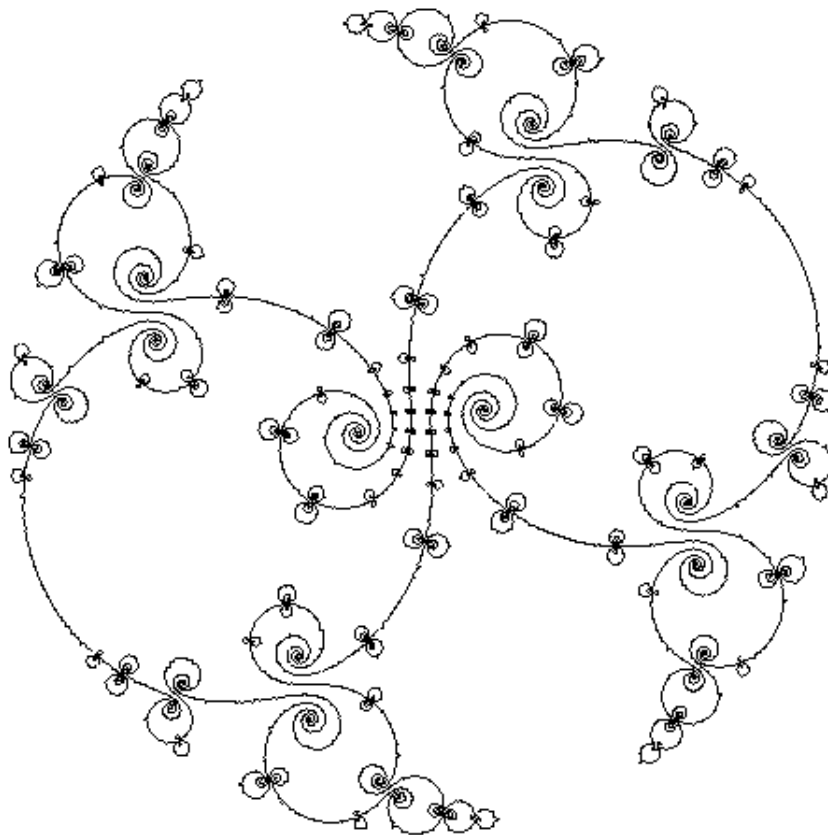


Marco Manetti

# Geometria Algebrica

Versione preliminare, 23 dicembre 2015

© 2015 Marco Manetti - Creative Commons **Attribution-NonCommercial 2.0**.  
Alcuni diritti riservati.



*Per quanto speciose parer possano tali ragioni alla turba dei letterati, i quali si persuadono agevolmente, scrivendo nelle lingue dotte, di salire in fama a paro degli antichi maestri e di levare nel mondo una più gran vampa di ammirazione del proprio ingegno, sono pure in effetto i mal consigliati coloro che si mettono a scrivere in altra lingua fuorché nella lor propria e nativa. Diversi sono appresso nazioni diverse i pensamenti, i concetti, le fantasie; diversi i modi di apprendere le cose, di ordinarle, di esprimerle.*

Francesco Algarotti, Posdammo 1750.

*È probabile che la capacità di risolvere problemi possa venire migliorata, e di molto, con lo studio della matematica, [...].*

*Voglio però cogliere l'occasione per sostenere che il modesto gioco della dama impegna le migliori abilità di una mente riflessiva assai più a fondo del gioco degli scacchi, complicato e futile. La complessità degli scacchi, dove le mosse sono varie e bizzarre, viene scambiata (è un errore comune) per profondità.*

Edgar Allan Poe, I delitti della rue Morgue.

Questo lavoro è rilasciato sotto la **Attribution-NonCommercial-Coffeeware 2.0** licenza **Creative Commons**. Ognuno è libero:

- di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire o recitare l'opera,
- di creare opere derivate.

Alle seguenti condizioni:

**Attribution.** Di riconoscere il contributo dell'autore originario.

**NonCommercial.** Di non usare quest'opera per scopi commerciali.

**Coffeeware.** Se usate queste note e le trovate di vostro gradimento, l'autore sarà lieto di farsi offrire un caffè da voi alla prima occasione utile.

In occasione di ogni atto di riutilizzazione o distribuzione, bisogna chiarire agli altri i termini della licenza di quest'opera. Se si ottiene il permesso dal titolare del diritto d'autore, è possibile rinunciare ad ognuna di queste condizioni.

Queste note sono state scritte per passione e sono distribuite nella speranza che siano utili, ma **SENZA ALCUNA GARANZIA**. L'autore declina ogni responsabilità per le possibili conseguenze di qualsiasi uso di esse.

Marco Manetti  
 Dipartimento di Matematica "G. Castelnuovo",  
 Università di Roma "La Sapienza",  
 Piazzale Aldo Moro 5, I-00185 Roma, Italy.  
 manetti@mat.uniroma1.it,  
<http://www.mat.uniroma1.it/people/manetti/>

---

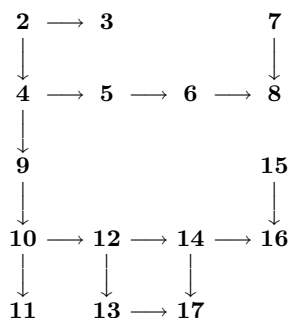
## Premessa

Questo libro è nato sotto forma di dispense per i corsi di Geometria Algebrica da me tenuti alla Scuola Normale Superiore negli anni 1995-96, 1997-98, all'Università di Roma "La Sapienza" nell'anno 2001-02 ed alla SMI di Perugia nell'agosto 2002. I corsi erano rivolti a studenti del corso di Laurea Specialistica in Matematica ed a studenti del primo anno del Dottorato di Ricerca in Matematica; per la comprensione delle note si richiede una buona conoscenza dei corsi istituzionali del corso di Laurea triennale in Matematica, in particolare dei corsi di Algebra e Geometria.

A partire dal 2003 il lavoro ed il tempo dedicato alla scrittura ed allo sviluppo del libro è andato progressivamente scemando e la convergenza verso la versione definitiva è diventata sempre più lenta. Questo fatto mi ha convinto a renderlo pubblico e libero, pur essendo ancora in forma non definitiva. Presumibilmente il numero di errori e incongruenze presenti è ancora alto: i lettori sono avvisati.

Ovviamente in futuro potranno esserci aggiornamenti, traduzioni in altre lingue e progetti derivati rivolti a diversi target.

Il materiale contenuto nel libro è più di quanto il numero di pagine possa far pensare. Le dimostrazioni sono spesso ridotte all'essenziale e non ci sono soluzioni degli esercizi proposti. In ogni modo non è necessaria la lettura in serie di tutti i capitoli e le propedeuticità sono organizzate in alcuni percorsi specifici descritti nella Tabella 0.1.



**Tabella 0.1.** *Leitfaden*: i numeri nella griglia si riferiscono ai capitoli di questo libro e le frecce denotano le propedeuticità consigliate.

Il Capitolo 1 contiene alcuni richiami di algebra ed è propedeutico a tutto il resto. Il Capitolo 18 contiene degli esercizi che non rispettano i percorsi di lettura esposti nella tabella.



---

# Indice

<b>1</b>	<b>Richiami di Algebra</b> .....	1
1.1	Il lemma di Zorn .....	1
1.2	Coefficienti binomiali .....	2
1.3	Anelli ed ideali .....	3
1.4	Il determinante di Vandermonde .....	5
1.5	Polinomi e fattorizzazione unica .....	7
1.6	Anelli graduati .....	11
1.7	Algebre e moduli .....	13
1.8	Esercizi complementari .....	15
<b>2</b>	<b>Spazi affini e proiettivi</b> .....	19
2.1	Combinazioni baricentriche .....	19
2.2	Spazi affini .....	20
2.3	Spazi proiettivi .....	25
2.4	Il birapporto .....	29
2.5	Esercizi complementari .....	30
<b>3</b>	<b>Forme binarie</b> .....	37
3.1	Risoluzione per radicali dell'equazione di terzo grado .....	37
3.2	Le funzioni simmetriche .....	39
3.3	Invarianti e covarianti di forme binarie .....	41
3.4	Il metodo simbolico di Cayley-Aronhold .....	46
3.5	Finita generazione dell'algebra dei covarianti .....	50
3.6	Esercizi complementari .....	56
<b>4</b>	<b>Teoria elementare dell'eliminazione</b> .....	61
4.1	Il risultante di due polinomi .....	61
4.2	Il discriminante .....	65
4.3	Anelli Noetheriani .....	67
4.4	La topologia di Zariski .....	69
4.5	Il teorema degli zeri di Hilbert .....	71
4.6	Esercizi complementari .....	73
4.7	Un lungo esercizio: il teorema di Lüroth .....	76
<b>5</b>	<b>Curve piane: nozioni base</b> .....	79
5.1	Definizioni principali .....	79
5.2	Retta tangente e molteplicità .....	82
5.3	Intersezione di curve piane .....	85

5.4	Sistemi lineari di curve piane . . . . .	91
5.5	Esercizi complementari . . . . .	95
5.6	Un lungo esercizio: il teorema di Bertini . . . . .	99
<b>6</b>	<b>Curve piane: argomenti scelti . . . . .</b>	<b>101</b>
6.1	Le coniche . . . . .	101
6.2	Corrispondenze e poligoni di Poncelet . . . . .	105
6.3	Flessi di cubiche piane e teorema di Salmon . . . . .	110
6.4	La legge di gruppo su di una cubica liscia . . . . .	114
6.5	Il teorema del resto . . . . .	119
6.6	Esercizi complementari . . . . .	123
<b>7</b>	<b>Aspetti algebrici delle serie di potenze . . . . .</b>	<b>129</b>
7.1	Serie di potenze . . . . .	129
7.2	Il teorema di preparazione di Weierstrass . . . . .	131
7.3	Il teorema fondamentale dell'algebra ed il teorema di Newton-Puiseux . . . . .	135
7.4	Il teorema delle funzioni implicite . . . . .	138
7.5	Archi e parametrizzazioni . . . . .	141
7.6	Esercizi complementari . . . . .	146
<b>8</b>	<b>Le singolarità delle curve piane da un punto di vista analitico . . . . .</b>	<b>151</b>
8.1	Ideali di Fitting . . . . .	151
8.2	Il lemma del serpente . . . . .	153
8.3	Definizioni alternative della molteplicità di intersezione . . . . .	154
8.4	Un lungo esercizio: il teorema $Af + B\phi$ di Max Noether . . . . .	157
8.5	Esercizi complementari . . . . .	158
<b>9</b>	<b>La topologia di Zariski . . . . .</b>	<b>161</b>
9.1	Esempi di spazi topologici . . . . .	161
9.2	L'immersione di Veronese . . . . .	164
9.3	Componenti irriducibili . . . . .	165
9.4	La dimensione combinatoria di uno spazio topologico . . . . .	168
9.5	La dimensione dello spazio affine . . . . .	170
9.6	La dimensione delle intersezioni . . . . .	172
9.7	La dimensione delle fibre . . . . .	176
9.8	Il grado: definizione geometrica . . . . .	178
9.9	Esercizi complementari . . . . .	181
<b>10</b>	<b>Varietà algebriche: nozioni base . . . . .</b>	<b>185</b>
10.1	Varietà affini . . . . .	185
10.2	Fasci strutturali . . . . .	189
10.3	Varietà quasiproiettive . . . . .	193
10.4	Le immersioni di Segre . . . . .	196
10.5	Prodotti . . . . .	199
10.6	Morfismi proiettivi . . . . .	201
10.7	Punti lisci e singolari, spazio tangente di Zariski . . . . .	203
10.8	Irriducibilità locale delle varietà lisce . . . . .	207
10.9	Esercizi complementari . . . . .	209

<b>11</b>	<b>Varietà algebriche: argomenti scelti</b> . . . . .	215
11.1	Le Grassmanniane . . . . .	215
11.2	Le varietà di incidenza . . . . .	219
11.3	Il teorema delle 27 rette . . . . .	222
11.4	Il teorema di Bertini-Sard . . . . .	224
11.5	Varietà duali . . . . .	226
11.6	Esercizi complementari . . . . .	229
<b>12</b>	<b>Piccolo bestiario di morfismi</b> . . . . .	233
12.1	Classi di morfismi e proprietà locale . . . . .	233
12.2	Morfismi affini e finiti . . . . .	235
12.3	Funzioni razionali . . . . .	239
12.4	Morfismi birazionali . . . . .	241
12.5	Estensioni separabili . . . . .	245
12.6	Morfismi separabili . . . . .	249
12.7	Esercizi complementari . . . . .	251
<b>13</b>	<b>Il polinomio di Hilbert</b> . . . . .	253
13.1	Decomposizioni irriducibili . . . . .	253
13.2	Il polinomio di Hilbert . . . . .	255
13.3	Varietà proiettive come sottoschemi . . . . .	259
13.4	Successioni regolari ed intersezioni complete . . . . .	264
13.5	Intersezioni trasverse e teorema di Bézout . . . . .	266
13.6	Semicontinuità del polinomio di Hilbert . . . . .	269
13.7	Esercizi complementari . . . . .	271
<b>14</b>	<b>Curve gobbe</b> . . . . .	275
14.1	Anelli di valutazione discreta . . . . .	275
14.2	Parametri locali su curve lisce . . . . .	276
14.3	Grado di morfismi di curve . . . . .	279
14.4	Divisori . . . . .	280
14.5	Sistemi lineari . . . . .	283
14.6	Il teorema del resto . . . . .	288
14.7	Esercizi complementari . . . . .	291
<b>15</b>	<b>Differenziali</b> . . . . .	293
15.1	(Alcune) Costruzioni universali in algebra e geometria . . . . .	293
15.2	Derivazioni universali e differenziali razionali . . . . .	298
15.3	Residui astratti (secondo Tate) . . . . .	300
15.4	Esercizi complementari . . . . .	304
15.5	Un lungo esercizio: il teorema di Krull . . . . .	306
<b>16</b>	<b>Il teorema di Riemann-Roch per curve lisce proiettive</b> . . . . .	309
16.1	Il teorema di Riemann-Roch, prima parte . . . . .	309
16.2	Prime applicazioni di Riemann-Roch . . . . .	314
16.3	Profilassi per caratteristiche positive . . . . .	314
16.4	Differenziali razionali su curve lisce . . . . .	315
16.5	Il teorema dei residui e seconda parte del teorema di Riemann-Roch . . . . .	318
16.6	Curve iperellittiche ed applicazione canonica . . . . .	321
16.7	Esercizi complementari . . . . .	323

VIII    Indice

<b>17</b>	<b>Genere aritmetico e disuguaglianza di Castelnuovo</b> .....	325
17.1	Il grado delle proiezioni .....	325
17.2	Modelli nonsingolari .....	326
17.3	Il teorema di posizione generale .....	327
17.4	La disuguaglianza di Castelnuovo .....	330
17.5	Il teorema di Max Noether .....	331
<b>18</b>	<b>Miscellanea di esercizi</b> .....	333
	<b>Riferimenti bibliografici</b> .....	335



---

## Prefazione

La geometria algebrica è una gigantesca montagna matematica, con molti punti di vista, svariati sentieri di scalata e con un grande dislivello tra le idee euristico-intuitive che stanno alla base di partenza ed i concetti astratti che formano gran parte delle ricerche contemporanee. Tutto questo rappresenta un serio ostacolo per chiunque voglia scrivere un trattato introduttivo e lo obbliga a delle scelte, sia per il linguaggio che per il livello di astrazione e generalità.

Già agli inizi del XX secolo, Federigo Enriques (prefazione di [EC1915]) negava, in virtù della *immane somma degli acquisti fatti*, la possibilità di dominare l'intera materia con una sola veduta. Tuttavia, egli poteva parlare della geometria algebrica come di una *dottrina qualitativa delle equazioni e delle funzioni algebriche, . . . , ove confluiscono il metodo delle coordinate, il metodo delle proiezioni e tutti i diversi ordini di concetti suggeriti dallo studio delle curve*.

Oggi questa definizione risulta indubbiamente inadeguata per descrivere lo stato dell'arte ma che tuttavia può essere presa in considerazione, con opportune imprescindibili modifiche, come percorso introduttivo alla materia. Le imprescindibili modifiche riguardano l'utilizzo dei metodi di algebra commutativa (studio degli anelli commutativi e dei loro ideali) e dei concetti di topologia algebrica, differenziale e generale.

Nella prima parte di queste note, l'obiettivo è quello di illustrare alcuni risultati che risalgono al XIX secolo e che sono all'origine di quel ramo della matematica che oggi viene comunemente chiamato Geometria Algebrica. Pur mantenendo un linguaggio moderno ed il necessario rigore, ho preferito, nei limiti del possibile, dimostrazioni che utilizzano le tecniche algebriche disponibili all'epoca. Tra i possibili approcci alla materia ho scelto quello puramente algebrico; per evitare le tentazioni topologiche ed analitico-complesse ho scelto di lavorare su di un campo arbitrario  $\mathbb{K}$  (sempre infinito e quasi sempre algebricamente chiuso). È tuttavia utile a fini didattici suggerire al lettore di farsi sempre un'idea intuitiva, aiutandosi con delle figure e se necessario introducendo concetti estranei alle note, di quello che succede sui numeri reali e complessi.

La seconda parte è una introduzione al linguaggio ed all'uso delle varietà quasiproiettive, cercando però di privilegiare l'aspetto geometrico-intuitivo e di limitare quanto più possibile il ricorso a strumenti di algebra commutativa.

Alle note sono stati aggiunti molti esercizi, molti dei quali non banali: alcuni asterischi (\*) indicano il livello di difficoltà: si tratta naturalmente di una valutazione del tutto personale che riflette in pieno le (in)capacità e le peculiarità dell'autore. Il simbolo (\*\*?) sta ad indicare un esercizio del quale non conosco alcuna ragionevole dimostrazione che utilizzi il materiale esposto nelle note (fino a quel punto). Gli esercizi complementari possono essere tralasciati ad una prima lettura e sono raccolti in apposite sezioni. Come ulteriore occasione di verifica sono stati disseminati errori di tutti i tipi: matematici, storici, di stampa, di grammatica, di uso trogloditico del L<sup>A</sup>T<sub>E</sub>X ecc.

## Regole del gioco, abbreviazioni, sigle e simboli

Per comodità espositiva, e salvo avviso contrario, useremo le seguenti convenzioni:

- Il simbolo  $\mathbb{N}$  denota l'insieme degli interi non negativi, ossia  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ .
- I simboli  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  denotano rispettivamente l'anello degli interi ed i campi dei numeri razionali, reali e complessi.
- Tutti gli anelli sono commutativi con unità e tutti i campi infiniti.
- Se  $A$  è un anello, l'ideale  $(1) = A$  è considerato un ideale primo.
- Ogni omomorfismo di anelli  $f: A \rightarrow B$  è unitario, cioè tale che  $f(1) = 1$ .

Assumeremo che il lettore abbia familiarità con le nozioni di dominio di integrità, di campo e di caratteristica di un campo.

Per facilitare il confronto con altri libri di testo, abbiamo deciso di scrivere le formule matematiche “in inglese”; scriveremo quindi GCD per massimo comun divisore, Ker per nucleo, rank per rango, trace per traccia eccetera.

Il simbolo  $\square$  indica la fine di una dimostrazione.

## Richiami di Algebra

---

In questo capitolo saranno richiamate, in modo estremamente conciso, alcune nozioni basilari di algebra allo scopo di facilitare il lettore e di fissare le notazioni. Per una trattazione più dettagliata e dimostrazioni complete rimandiamo a [Her1982], [Lang1984].

**Attenzione:** Salvo avviso contrario tutti gli anelli sono tacitamente considerati commutativi con unità e tutti i campi infiniti.

### 1.1 Il lemma di Zorn

In queste note accettiamo senza riserve la validità dell'assioma della scelta.

**Assioma della scelta.** Sia  $X = \cup\{X_i \mid i \in I\}$  l'unione di insiemi non vuoti, indicizzati da un insieme  $I$ . Allora esiste un'applicazione  $f: I \rightarrow X$  tale che  $f(i) \in X_i$  per ogni  $i \in I$ .

Prima di enunciare il lemma di Zorn nella forma di uso prevalente ricordiamo alcune definizioni:

1. Sia  $(S, \leq)$  un insieme (parzialmente) ordinato. Un sottoinsieme  $H \subset S$  si dice una **catena** se per ogni  $x, y \in H$ , vale  $x \leq y$  oppure  $y \leq x$ . In altri termini  $H \subset S$  è una catena se e solo se  $H$  è un insieme totalmente ordinato per la relazione di ordine indotta.
2. Sia  $(S, \leq)$  un insieme (parzialmente) ordinato,  $H \subset S$  un sottoinsieme e  $x \in S$ . Diremo che  $x$  è un **maggiorante** per  $H$  se  $y \leq x$  per ogni  $y \in H$ .
3. Sia  $(S, \leq)$  un insieme (parzialmente) ordinato e  $m \in S$ . Diremo che  $m$  è un **elemento massimale** per  $S$  se  $\{m\} = \{x \in S \mid m \leq x\}$ .

**Lemma 1.1.1.** Sia  $(S, \leq)$  un insieme ordinato. Allora ogni sottoinsieme  $H \subset S$  possiede elementi massimali se e solo se ogni catena ascendente numerabile  $\{x_0 \leq x_1 \leq \dots\}$  è stazionaria, cioè se esiste  $m \in \mathbb{N}$  tale che  $x_n = x_m$  per ogni  $n \geq m$ .

*Dimostrazione.* Se una catena ascendente numerabile  $x_n$  possiede un elemento massimale, diciamo  $x_m$ , allora necessariamente  $x_n = x_m$  per ogni  $n \geq m$ .

Viceversa, se esiste un sottoinsieme non vuoto  $H \subset S$  senza elementi massimali, allora, per ogni  $x \in H$ , il sottoinsieme  $H_x = \{y \in H \mid y > x\}$  è non vuoto. Per l'assioma della scelta esiste un'applicazione  $f: H \rightarrow H$  tale che  $f(x) > x$  per ogni  $x \in H$ . Preso comunque  $x_0 \in H$ , la catena  $x_n = f^n(x_0)$  non è stazionaria.  $\square$

**Lemma 1.1.2 (Lemma di Zorn).** *Sia  $(S, \leq)$  un insieme non vuoto parzialmente ordinato. Se ogni catena in  $S$  possiede un maggiorante, allora  $S$  possiede elementi massimali.*

Rimandiamo ai libri [Halm1960, Man2008] per la dimostrazione dell'equivalenza tra il lemma di Zorn e l'assioma della scelta.

Abbiamo enunciato l'assioma della scelta e il lemma di Zorn esclusivamente come richiamo di argomenti che assumiamo ben assodati nel lettore. In particolare queste note conterranno molti ragionamenti "informali" che hanno a che fare con quantità infinite, i quali possono essere facilmente formalizzati e resi precisi da qualsiasi persona dotata delle competenze matematiche di base.

## 1.2 Coefficienti binomiali

Dati due interi positivi  $n, d$ , il coefficiente binomiale

$$\binom{n}{d}$$

indica il numero dei sottoinsiemi di cardinalità  $d$  contenuti in un insieme di  $n$  elementi. Sono ben note le formule:

$$\binom{n}{d} = \frac{n!}{d!(n-d)!} = \frac{1}{d!} \prod_{i=0}^{d-1} (n-i), \quad (x+y)^n = \sum_{d=0}^n \binom{n}{d} x^d y^{n-d}.$$

**Lemma 1.2.1.** *Per ogni  $n, d \geq 0$  l'insieme*

$$P_{n,d} = \{(a_1, \dots, a_n) \in \mathbb{N}^n \mid a_1 + \dots + a_n \leq d\}$$

ha cardinalità  $\binom{d+n}{n}$ .

*Dimostrazione.* L'insieme  $Q_{n,d} = \{(b_1, \dots, b_n) \in \mathbb{N}^n \mid 1 \leq b_1 < b_2 < \dots < b_n \leq d+n\}$  ha cardinalità  $\binom{d+n}{n}$ , mentre l'applicazione

$$P_{n,d} \rightarrow Q_{n,d}, \quad (a_1, \dots, a_n) \mapsto (a_1 + 1, a_1 + a_2 + 2, \dots, a_1 + \dots + a_n + n),$$

è bigettiva. □

Si noti che esiste una bigezione naturale

$$\{(a_1, \dots, a_n) \in \mathbb{N}^n \mid a_1 + \dots + a_n \leq d\} \cong \{(a_0, \dots, a_n) \in \mathbb{N}^{n+1} \mid a_0 + \dots + a_n = d\}.$$

### Esercizi

1.1. Dimostrare che

$$\binom{d+n}{n} = \binom{d+n-1}{n-1} + \binom{d+n-1}{n} = \sum_{h=0}^d \binom{h+n-1}{n-1}.$$

1.2. Siano

$$F_0 = 0, \quad F_1 = 1, \quad F_2 = 1, \quad \dots \quad F_{n+1} = F_n + F_{n-1}, \quad \dots$$

i numeri di Fibonacci. Dimostrare che per ogni  $n \geq 0$  vale

$$F_{n+1} = \sum_{d \geq 0} \binom{n-d}{d}.$$

1.3. Dimostrare il seguente risultato, generalmente noto come *Principio di inclusione-esclusione*.

Denotiamo con  $C(a, n)$  la famiglia dei sottoinsiemi di cardinalità  $a$  di  $\{1, \dots, n\}$  e siano  $A_1, \dots, A_n$  sottoinsiemi di un insieme finito  $A$ ; per ogni  $I = \{i_1, \dots, i_a\} \in C(a, n)$  denotiamo con  $\alpha(I)$  la cardinalità di  $A_{i_1} \cap \dots \cap A_{i_a}$ . Dimostrare che la cardinalità di  $A_1 \cup \dots \cup A_n$  è uguale a

$$\sum_{a=1}^n (-1)^{a-1} \sum_{I \in C(a, n)} \alpha(I).$$

(Sugg.: un punto appartenente ad  $A_i$  per esattamente  $s$  indici  $i \in \{1, \dots, n\}$  viene contato, con molteplicità,  $1 - (1-1)^s$  volte.)

1.4. Dimostrare che per ogni  $s \geq 0$  vale lo sviluppo di Taylor

$$\frac{1}{(1-t)^{s+1}} = \sum_{n=0}^{+\infty} \binom{s+n}{s} t^n.$$

(Sugg.: induzione su  $s$ , derivando  $(1-t)^{-s}$  oppure utilizzando l'Esercizio 1.1.)

### 1.3 Anelli ed ideali

Con il termine anello intenderemo sempre un anello commutativo con unità e, salvo avviso contrario, ogni omomorfismo di anelli  $f: A \rightarrow B$  è unitario, cioè soddisfa la condizione  $f(1) = 1$ . Assumeremo che il lettore abbia familiarità con le nozioni di dominio di integrità, di campo e di caratteristica di un campo.

Dato un dominio di integrità  $A$ , il **campo delle frazioni** di  $A$  è il campo  $F$  formato dalle classi di equivalenza delle frazioni  $\frac{a}{b}$ , per  $a, b \in A$  e  $b \neq 0$ . La relazione di equivalenza  $\frac{a}{b} \sim \frac{c}{d}$  è valida se e solo se  $ad = bc$ . Le operazioni di somma e prodotto in  $F$  sono definite nel modo "naturale"

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}.$$

La caratteristica di un dominio di integrità è, per definizione, la caratteristica del suo campo delle frazioni [Her1982, 3.2]; se  $A$  è un dominio di caratteristica  $p > 0$ , l'applicazione  $x \mapsto x^p$  è un omomorfismo iniettivo di  $A$  in sé detto **morfismo di Frobenius**.

**Definizione 1.3.1.** *Un dominio di integrità si dice **perfetto** se ha caratteristica 0 oppure se ha caratteristica  $p > 0$  ed il morfismo di Frobenius è surgettivo.*

Un elemento  $x$  di un anello  $A$  si dice un **divisore di 0** se esiste  $y \in A - \{0\}$  tale che  $xy = 0$ . Un anello è un dominio di integrità se e solo se 0 è l'unico divisore di 0.

Dato un anello  $A$  ed un suo sottoinsieme  $E$ , denotiamo con  $(E) \subset A$  il più piccolo ideale di  $A$  contenente  $E$ . Si dimostra facilmente che ogni elemento di  $(E)$  si può scrivere

come una combinazione lineare finita di elementi di  $E$  a coefficienti in  $A$ . Diremo che un insieme  $E$  è un **insieme di generatori** dell'ideale  $I \subset A$  se  $I = (E)$ ; un ideale si dice **finitamente generato** se ammette un insieme finito di generatori; si dice **principale** se è generato da un solo elemento. Un anello si dice **Noetheriano** se ogni ideale è finitamente generato, si dice **ad ideali principali** se ogni ideale è principale. Esempi di anelli ad ideali principali sono i campi (gli unici ideali sono  $(1)$  e  $(0)$ ).

Intersezione di ideali è sempre un ideale mentre in generale l'unione di ideali non è un ideale. Se  $I, J \subset A$  sono ideali, denotiamo con  $I + J = (I \cup J)$  l'ideale generato da  $I$  e  $J$ . È facile vedere che  $I + J = \{x + y \mid x \in I, y \in J\}$ . Più in generale se  $I_\alpha$  è una famiglia arbitraria di ideali di  $A$  denotiamo con  $\sum_\alpha I_\alpha$  l'ideale generato da  $\cup_\alpha I_\alpha$ .

Un ideale  $I$  si dice **irriducibile** se per ogni coppia  $J_1, J_2$  di ideali tali che  $I = J_1 \cap J_2$  si ha che  $I = J_1$  oppure  $I = J_2$ . Un ideale  $\mathfrak{p}$  si dice **primo**<sup>1</sup> se  $ab \in \mathfrak{p}$  implica che  $a \in \mathfrak{p}$  oppure  $b \in \mathfrak{p}$ . Dato un ideale  $I \subset A$  si definisce il **radicale** di  $I$  come

$$\sqrt{I} = \{a \in A \mid a^n \in I \text{ per } n \gg 0\}.$$

Un **ideale radicale** è un ideale  $I$  tale che  $I = \sqrt{I}$ . Si noti che  $\sqrt{\sqrt{I}} = \sqrt{I}$  e che gli ideali primi sono radicali.

Un ideale **massimale** è un ideale proprio che è massimale rispetto alla relazione di inclusione. Ogni ideale massimale  $\mathfrak{m} \subset A$  è primo: infatti se  $ab \in \mathfrak{m}$  e né  $a$  né  $b$  appartengono a  $\mathfrak{m}$  allora  $\mathfrak{m} + (a) = \mathfrak{m} + (b) = (1)$  e quindi esistono  $m_1, m_2 \in \mathfrak{m}$ ,  $x_1, x_2 \in A$  tali che  $m_1 + ax_1 = m_2 + bx_2 = 1$ . Si ottiene che  $1 = m_1 m_2 + m_1 x_2 b + m_2 x_1 a + x_1 x_2 ab \in \mathfrak{m}$ , in contraddizione con il fatto che ogni ideale massimale è proprio.

Vediamo adesso due classiche ed istruttive applicazioni del lemma di Zorn. Altre ne saranno proposte negli esercizi.

**Lemma 1.3.2.** *Ogni ideale proprio di un anello  $A$  è contenuto in un ideale massimale.*

*Dimostrazione.* Sia  $I \subset A$  un ideale proprio e sia  $\mathcal{A}$  la famiglia degli ideali propri che contengono  $I$ . Ovviamente  $I \in \mathcal{A}$  che quindi non è vuota; se  $\{I_\alpha\}$  è una catena in  $\mathcal{A}$  allora  $\cup_\alpha I_\alpha = J$  è un ideale e, siccome  $1 \notin I_\alpha$  per ogni  $\alpha$ , ne segue che  $1 \notin J$ , cioè che  $J$  è un ideale proprio. Per il lemma di Zorn  $\mathcal{A}$  possiede elementi massimali.  $\square$

**Lemma 1.3.3.** *Sia  $I \subset A$  un ideale. Allora  $\sqrt{I}$  è l'intersezione di tutti gli ideali primi che contengono  $I$ .*

*Dimostrazione.* Se  $\mathfrak{p}$  è un ideale primo che contiene  $I$ , allora  $\sqrt{I} \subset \sqrt{\mathfrak{p}} = \mathfrak{p}$ .

Viceversa, fissiamo un elemento  $f \notin \sqrt{I}$  e denotiamo con  $\mathcal{A}$  la famiglia degli ideali radicali che contengono  $I$  e non contengono  $f$ .  $\mathcal{A}$  non è vuota perché contiene  $\sqrt{I}$ ; se  $J_\alpha$  è una catena in  $\mathcal{A}$  allora anche  $\cup J_\alpha \in \mathcal{A}$  (verifica per esercizio) e quindi per il lemma di Zorn  $\mathcal{A}$  possiede un elemento massimale  $\mathfrak{p}$ : vogliamo dimostrare che  $\mathfrak{p}$  è un ideale primo. Sia  $ab \in \mathfrak{p}$  e supponiamo per assurdo che  $a \notin \mathfrak{p}$  e  $b \notin \mathfrak{p}$ . Allora gli ideali  $\sqrt{(a) + \mathfrak{p}}$  e  $\sqrt{(b) + \mathfrak{p}}$  non appartengono ad  $\mathcal{A}$  e, poiché contengono  $I$ , dovranno contenere anche  $f$ . Esisteranno quindi interi positivi  $n, m$  tali che  $f^n \in (a) + \mathfrak{p}$  e  $f^m \in (b) + \mathfrak{p}$ . Prendendo il prodotto otteniamo  $f^{n+m} \in (ab) + \mathfrak{p} = \mathfrak{p}$  che contraddice l'appartenenza di  $\mathfrak{p}$  ad  $\mathcal{A}$ .  $\square$

**Definizione 1.3.4.** *Il **nilradicale** di un anello commutativo è l'intersezione di tutti gli ideali primi.*

Per il Lemma 1.3.3 il nilradicale coincide con l'insieme degli elementi nilpotenti  $\sqrt{0}$ .

<sup>1</sup> In queste note, non è richiesto agli ideali primi di essere propri.

**Definizione 1.3.5.** *Un anello si dice **locale** se contiene un solo ideale massimale. L'unico campo quoziente di un anello locale si dice **campo residuo**.*

Se  $f: A \rightarrow B$  è un omomorfismo di anelli e  $J \subset B$  è un ideale, allora anche  $f^{-1}(J)$  è un ideale di  $A$ ; se  $J$  è primo allora anche  $f^{-1}(J)$  è primo, mentre se  $J$  è massimale non è detto che anche  $f^{-1}(J)$  sia massimale: si consideri ad esempio l'inclusione  $\mathbb{Z} \rightarrow \mathbb{Q}$  e l'ideale nullo  $J = 0$ . Se  $I \subset A$  è un ideale e  $f$  non è surgettivo, allora in generale  $f(I)$  non è un ideale.

**Proposizione 1.3.6.** *Sia  $f: A \rightarrow B$  un omomorfismo surgettivo di anelli con nucleo  $K$ .*

1. *Se  $I \subset A$  è un ideale, allora  $f(I)$  è un ideale e  $f^{-1}(f(I)) = I + K$ . In particolare,  $f(I)$  è un ideale proprio se e solo se  $1 \notin I + K$ .*
2.  *$f^{-1}$  induce una biiezione tra l'insieme degli ideali di  $B$  e l'insieme degli ideali di  $A$  che contengono  $K$ .*
3. *Un ideale  $J \subset B$  è primo (risp.: massimale, radicale, irriducibile) se e solo se  $f^{-1}(J) \subset A$  è primo (risp.: massimale, radicale, irriducibile).*

*Dimostrazione.* Esercizio. □

In più di un'occasione utilizzeremo la seguente notazione: se  $A$  è un anello ed  $a \in A$ , allora  $O(a)$  indica un elemento imprecisato dell'ideale  $(a)$ ; scriveremo ad esempio  $(x + a)^3 = x^3 + 3x^2a + O(a^2)$  e più in generale  $b = c + O(a)$  se  $b \equiv c \pmod{a}$ .

**Esercizi**

**1.5.** Dimostrare che ogni ideale primo è irriducibile. Verificare che l'ideale  $0$  nell'anello  $\frac{\mathbb{R}[x]}{(x^2)}$  è irriducibile ma non è primo.

**1.6.** Sia  $\mathfrak{m}$  un ideale massimale di un anello  $A$ . Dimostrare che  $A$  è locale se e solo se  $1 - a$  è invertibile per ogni  $a \in \mathfrak{m}$ .

**1.7.** Sia  $\text{rad}$  l'intersezione di tutti gli ideali massimali di un anello commutativo  $A$ . Dimostrare che  $a \in \text{rad}$  se e solo se  $1 + ab$  è invertibile in  $A$  per ogni  $b \in A$ .

**1.4 Il determinante di Vandermonde**

Sia  $B = (b_{ij})$  una matrice quadrata di ordine  $n$  a coefficienti in un anello  $A$ . Come per le matrici a coefficienti in un campo si definisce il determinante di  $B$  nel modo seguente

$$\det(B) = |b_{ij}| = \sum_{\sigma \in \Sigma_n} (-1)^\sigma b_{1\sigma(1)} \cdots b_{n\sigma(n)}$$

dove  $\Sigma_n$  è il gruppo simmetrico delle permutazioni di  $\{1, \dots, n\}$  e  $(-1)^\sigma$  è la segnatura di  $\sigma$ . Continuano a valere le seguenti proprietà:

1. (Sviluppo di Laplace.) Se  $B^{ij}$  indica il determinante minore  $(n-1) \times (n-1)$  calcolato togliendo a  $B$  la  $i$ -esima riga e la  $j$ -esima colonna, allora valgono le formule

$$\det(B) = \sum_{j=1}^n (-1)^{h+j} B^{hj} b_{hj} = \sum_{i=1}^n b_{ih} (-1)^{i+h} B^{ih}, \quad \text{per ogni } h = 1, \dots, n.$$

$$\sum_{j=1}^n b_{kj} (-1)^{h+j} B^{hj} = \sum_{i=1}^n (-1)^{i+h} B^{ih} b_{ik} = 0, \quad \text{se } h \neq k.$$

2. Moltiplicando una riga od una colonna di  $B$  per un elemento  $a \in A$ , anche  $\det(B)$  viene moltiplicato per  $a$ .
3. Il determinante  $\det(B)$  non cambia se ad una colonna viene aggiunto un multiplo di un'altra colonna. Lo stesso per le righe.
4. Se la matrice  $B$  possiede due colonne uguali, allora  $\det(B) = 0$ .
5. Vale il teorema di Binet, e cioè  $\det(AB) = \det(A)\det(B)$ .

Come esempio di applicazione delle precedenti regole, calcoliamo il determinante della matrice di Vandermonde: proviamo che

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{vmatrix} = \prod_{i>j} (x_i - x_j)$$

Ragioniamo per induzione su  $n$ , considerando il polinomio

$$p(t) = \prod_{j=0}^{n-1} (t - x_j) = t^n + \sum_{i=0}^{n-1} a_i t^i.$$

Sommando all'ultima riga della matrice di Vandermonde la combinazione lineare a coefficienti  $a_i$  delle rimanenti righe si ottiene

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ p(x_0) & p(x_1) & \cdots & p(x_n) \end{vmatrix}$$

Dato che  $p(x_i) = 0$  per ogni  $i < n$  e  $p(x_n) = \prod_{n>j} (x_n - x_j)$  si ha

$$\begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_n^{n-1} \\ x_0^n & x_1^n & \cdots & x_n^n \end{vmatrix} = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_0 & x_1 & \cdots & x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{n-1} & x_1^{n-1} & \cdots & x_{n-1}^{n-1} \end{vmatrix} \cdot \prod_{n>j} (x_n - x_j)$$

Denotiamo con  $\tilde{B} = (\tilde{b}_{ij})$  la matrice di coefficienti  $\tilde{b}_{ij} = (-1)^{i+j} B^{ji}$ . Se  $I$  indica la matrice identità, allora segue dallo sviluppo di Laplace che

$$B \cdot \tilde{B} = \tilde{B} \cdot B = \det(B) \cdot I \quad (\text{prodotto righe per colonne}).$$

La matrice  $\tilde{B}$  viene detta **matrice aggiunta** di  $B$ .

### Esercizi

**1.8.** Sia  $B = (b_{ij})$  una matrice le cui colonne sono linearmente dipendenti su  $A$ , provare che  $\det(B)$  è un divisore di 0.



**1.9.** Sia  $B = (b_{ij})$  una matrice  $n \times (n + 1)$  a coefficienti in un anello  $A$  e denotiamo con  $d_j$  il determinante minore  $n \times n$  calcolato togliendo a  $B$  la  $j$ -esima colonna. Dimostrare che

$$B \begin{pmatrix} d_1 \\ -d_2 \\ d_3 \\ \vdots \end{pmatrix} = 0.$$

(Sugg.: calcolare i determinanti delle matrici  $(n + 1) \times (n + 1)$  ottenute duplicando le righe di  $B$ .)

### 1.5 Polinomi e fattorizzazione unica

Sia  $A$  un dominio di integrità, un elemento  $a \in A$  si dice **irriducibile** se non è invertibile e se  $a = bc$ , allora uno dei due elementi  $b, c \in A$  è invertibile. Un elemento non invertibile  $a \in A$  si dice **primo** se ogniqualvolta  $a$  divide  $bc$  si ha che  $a$  divide almeno uno dei due elementi  $b, c$ . È facile dimostrare che ogni primo è irriducibile, il viceversa è generalmente falso (vedi Esercizio 1.22).

Un dominio di integrità si dice a **fattorizzazione unica** se:

1. Ogni elemento diverso da 0 è invertibile oppure si può scrivere come prodotto di un numero finito di elementi irriducibili.
2. Gli elementi irriducibili nominati al punto 1 sono unicamente determinati, a meno dell'ordine e di moltiplicazione per invertibili.

I campi sono domini a fattorizzazione unica. Più in generale, è ben noto che i domini di integrità a ideali principali sono domini a fattorizzazione unica (cfr. Esercizio 1.33).

Se  $A$  è un anello, indicheremo con  $A[x_1, \dots, x_n]$  l'anello dei polinomi a coefficienti in  $A$  nelle indeterminate  $x_1, \dots, x_n$ . La proprietà caratterizzante di  $A[x_1, \dots, x_n]$  è che *per ogni omomorfismo di anelli  $\phi: A \rightarrow B$  e per ogni  $n$ -upla  $b_1, \dots, b_n \in B$  esiste unica una estensione di  $\phi$  ad un omomorfismo, detto di **specializzazione**,  $\hat{\phi}: A[x_1, \dots, x_n] \rightarrow B$  tale che  $\hat{\phi}(x_i) = b_i$ .*

Un polinomio  $p(t) \in A[t]$  si dice **monico** se il coefficiente della potenza più alta di  $t$  è uguale a 1. Ossia,  $p(t)$  è monico di grado  $d$  se e solo se si può scrivere

$$p(t) = t^d + a_1 t^{d-1} + \dots + a_d, \quad a_1, \dots, a_d \in A.$$

**Definizione 1.5.1.** Sia  $A$  un dominio a fattorizzazione unica; un polinomio  $f \in A[t]$  si dice **primitivo** se i coefficienti di  $f$  non hanno fattori comuni.

**Lemma 1.5.2 (di Gauss).** Sia  $A$  un dominio a fattorizzazione unica con campo delle frazioni  $\mathbb{K}$ . Allora il prodotto di polinomi primitivi è primitivo, ed inoltre:

1. Se  $f, g \in A[t]$ , con  $f$  primitivo che divide  $g$  in  $\mathbb{K}[t]$ , allora  $f$  divide  $g$  in  $A[t]$ .
2. Se  $f, g \in \mathbb{K}[t]$  sono polinomi monici e  $fg \in A[t]$ , allora  $f, g \in A[t]$
3.  $A[t]$  è un dominio a fattorizzazione unica.

*Dimostrazione.* (vedi anche l'Esercizio 13.28) Siano  $f = \sum_{i=0}^n a_i t^i$  e  $g = \sum_{j=0}^m b_j t^j$  due polinomi primitivi in  $A[t]$  e assumiamo per assurdo che esista  $c \in A$  non invertibile che divide il prodotto  $fg$ . Siano  $r \leq n$  e  $s \leq m$  due interi tali che  $c|a_i$  per  $i < r$ ,  $c \nmid a_r$ ,  $c|b_j$  per  $j < s$  e  $c \nmid b_s$ . Il coefficiente di  $t^{r+s}$  nel prodotto  $fg$  è uguale a

$$a_r b_s + \sum_{i < r} a_i b_{r+s-i} + \sum_{j < s} a_{r+s-j} b_j$$

e quindi  $c$  divide  $a_r b_s$ . Poiché  $A$  è a fattorizzazione unica, questa è una contraddizione.

[1] Sia  $f \in A[t]$  primitivo,  $g \in \mathbb{K}[t]$  e  $fg \in A[t]$ ; mettendo i coefficienti di  $g$  a denominatore comune, possiamo trovare  $a, b \in A$  senza fattori comuni tali che  $h = \frac{ag}{b}$  è un

polinomio primitivo in  $A[t]$ . Dunque  $fh = \frac{agf}{b}$  è primitivo, da cui segue che  $a$  è invertibile e quindi  $g = hb/a \in A[t]$ .

[2] Se  $f, g \in \mathbb{K}[t]$  sono polinomi monici, esistono  $a, b \in A$  tali che  $af, bg \in A[t]$  sono primitivi. Quindi  $abfg \in A[t]$  è primitivo e di conseguenza  $ab$  è invertibile.

[3] La dimostrazione del terzo punto segue facilmente dai primi due e dal fatto che  $\mathbb{K}[t]$  è un dominio a fattorizzazione unica. I dettagli sono lasciati per esercizio al lettore.  $\square$

**Lemma 1.5.3 (Divisione Euclidea).** *Sia  $A$  un dominio di integrità e  $p \in A[x]$  un polinomio monico di grado  $n > 0$ . Allora per ogni  $f \in A[x]$  esistono unici  $g, r \in A[x]$ , con  $r$  di grado minore di  $n$ , tali che  $f = gp + r$ .*

*Dimostrazione.* Esercizio.  $\square$

**Lemma 1.5.4 (regola di Ruffini).** *Sia  $A$  un dominio di integrità,  $f \in A[x]$  e  $a \in A$  tale che  $f(a) = 0$ . Allora  $(x - a)$  divide  $f$ ; in particolare esistono in  $A$  al più  $\deg(f)$  radici.*

*Dimostrazione.* Esercizio.  $\square$

**Lemma 1.5.5.** *Sia  $A$  un dominio a fattorizzazione unica con campo delle frazioni  $\mathbb{K}$  e siano  $f, g \in A[x]$  polinomi di grado positivo. Allora  $f$  e  $g$  hanno un fattore comune in  $A[x]$  di grado positivo se e solo se  $f$  e  $g$  hanno una radice comune nella chiusura algebrica di  $\mathbb{K}$ .*

*Dimostrazione.* Una implicazione è evidente. Viceversa supponiamo che  $f$  e  $g$  abbiano una radice comune in  $\overline{\mathbb{K}}$  e dimostriamo, per induzione sulla somma dei gradi, che  $f$  e  $g$  hanno un fattore comune di grado positivo; non è restrittivo supporre  $f$  e  $g$  polinomi primitivi. Se  $f$  e  $g$  hanno entrambi grado 1, diciamo  $f = ax + b$  e  $g = cx + d$ , allora  $\frac{b}{a} = \frac{d}{c}$  e quindi esiste un invertibile  $e$  tale che  $a = ec$  e  $b = ed$ . Se la somma dei gradi è maggiore di 2 e, tanto per fissare le idee,  $\deg f \geq \deg g$ , allora esistono  $a \in A - \{0\}$  ed un polinomio  $h \in A[x]$  di grado  $\deg f - \deg g$  tali che

$$\deg(af - hg) < \deg f.$$

I polinomi  $g$  e  $af - hg$  hanno una radice comune e per l'ipotesi induttiva esiste un polinomio irriducibile  $q \in A[x]$  di grado positivo che divide  $g$  e  $af$ .  $\square$

Dal Lemma 1.5.4 segue il seguente criterio di cui faremo uso in seguito: *se  $A$  è un dominio di integrità infinito ed  $f \in A[t]$  allora  $f = 0$  se e solo se  $f(a) = 0$  per infiniti  $a \in A$ .*

Dato un qualsiasi anello  $A$ , per ogni  $i = 1, \dots, s$  esiste unica un'applicazione

$$\frac{\partial}{\partial x_i}: A[x_1, \dots, x_s] \rightarrow A[x_1, \dots, x_s]$$

che chiameremo **derivata parziale** e che soddisfa le seguenti 4 condizioni:

1.  $\frac{\partial}{\partial x_i}(a) = 0$  per ogni  $a \in A$ .
2. (additività)  $\frac{\partial}{\partial x_i}(b_1 + b_2) = \frac{\partial}{\partial x_i}(b_1) + \frac{\partial}{\partial x_i}(b_2)$  per ogni  $b_1, b_2 \in A[x_1, \dots, x_s]$ .

3. (Leibniz)  $\frac{\partial}{\partial x_i}(b_1 b_2) = b_1 \frac{\partial}{\partial x_i}(b_2) + b_2 \frac{\partial}{\partial x_i}(b_1)$  per ogni  $b_1, b_2 \in A[x_1, \dots, x_s]$ .
4.  $\frac{\partial}{\partial x_i}(x_j) = \delta_{ij}$  (delta di Kronecker).

Si vede facilmente che  $\frac{\partial}{\partial x_i}$  è ben definita e unica. Scriveremo spesso  $\frac{\partial b}{\partial x_i}$  in luogo di  $\frac{\partial}{\partial x_i}(b)$ .

Più in generale dato un morfismo di anelli  $A \rightarrow B$ , un'applicazione  $d: B \rightarrow B$  che soddisfa le precedenti condizioni 1), 2) e 3) si dice una **A-derivazione**. Se  $A = \mathbb{R}$  le applicazioni  $\frac{\partial}{\partial x_i}$  coincidono con le usuali derivate parziali.

**Lemma 1.5.6.** *Sia  $A$  un dominio perfetto a fattorizzazione unica e  $f \in A[x_1, \dots, x_s]$ . Allora  $f$  possiede un fattore multiplo di grado positivo se e solo se  $f, \frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_s}$  hanno un fattore comune di grado positivo.*

*Dimostrazione.* Se  $h^2$  divide  $f$ , segue immediatamente dalla regola di Leibniz che  $h$  divide tutte le derivate parziali. Viceversa sia  $f = f_1 f_2 \cdots f_n$  con i polinomi  $f_i$  irriducibili e senza fattori in comune; si assuma per assurdo che  $f_1$  abbia grado positivo e divida tutte le derivate parziali di  $f$ . Di nuovo per Leibniz segue che  $f_1$  divide  $\frac{\partial f_1}{\partial x_i}$  per ogni  $i$  e quindi, siccome il grado della derivata è strettamente inferiore, deve essere necessariamente  $\frac{\partial f_1}{\partial x_i} = 0$  per ogni  $i$ .

Basta quindi dimostrare che se  $f$  è irriducibile di grado positivo, allora possiede almeno una derivata parziale non nulla. L'asserzione è evidente in caratteristica 0, mentre se la caratteristica è  $p > 0$  e le tutte derivate parziali sono nulle, allora  $f \in A[x_1^p, \dots, x_s^p]$ . Siccome  $A$  è perfetto, si ha che  $f$  appartiene all'immagine del morfismo di Frobenius  $A[x_1, \dots, x_s] \rightarrow A[x_1, \dots, x_s]$  e quindi esiste  $h \in B$  tale che  $f = h^p$ .  $\square$

Una **serie formale** a coefficienti in  $A$  nelle indeterminate  $x_1, \dots, x_n$  è una espressione del tipo

$$\phi = \sum_I a_I x^I \quad a_I \in A, \quad I \in \mathbb{N}^n$$

dove, se  $I = (i_1, \dots, i_n)$ , si è posto  $x^I = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ ; chiaramente un polinomio può essere pensato come una serie formale in cui  $a_I \neq 0$  per al più un numero finito di multiindici. Con le ben note regole di somma e di prodotto di Cauchy<sup>2</sup> le serie formali formano un anello commutativo denotato  $A[[x_1, \dots, x_n]]$ . È talvolta utile considerare  $A[x_1, \dots, x_n]$  come un sottoanello di  $A[[x_1, \dots, x_n]]$ . Ad esempio se  $a \in A$ , allora  $1 - ta \in A[[t]]$  è invertibile in  $A[[t]]$  con inverso  $\sum_{i \geq 0} a^i t^i$ ; si deduce immediatamente che  $1 - at$  è invertibile in  $A[[t]]$  se e solo se  $a$  è nilpotente.

### Esercizi

**1.10.** Siano  $A$  un anello,  $0 \leq r < n$  interi e  $a_{r+1}, \dots, a_n \in A$ . Mostrare che l'applicazione

---

2

$$\sum a_I x^I + \sum b_I x^I = \sum (a_I + b_I) x^I, \quad (\sum a_I x^I)(\sum b_I x^I) = \sum_H \left( \sum_{I+J=H} a_I b_J \right) x^H$$

$$\phi: A[x_1, \dots, x_n] \rightarrow A[x_1, \dots, x_r], \quad \phi(f(x_1, \dots, x_n)) = f(x_1, \dots, x_r, a_{r+1}, \dots, a_n)$$

è un omomorfismo surgettivo di anelli e che il nucleo di  $\phi$  è l'ideale generato da  $x_{r+1} - a_{r+1}, \dots, x_n - a_n$ . (Sugg.: scrivere  $x_i = y_i + a_i$ .)

**1.11.** Sia  $A = \mathbb{K}[t^2, t^3] \subset \mathbb{K}[t]$  il sottoanello dei polinomi con il coefficiente di  $t$  nullo. Provare che  $A$  non è un dominio a fattorizzazione unica e che il Lemma 1.5.5 non vale in  $A[x]$ .

**1.12.** Siano  $d_1, d_2: A[x_1, \dots, x_s] \rightarrow A[x_1, \dots, x_s]$  due  $A$ -derivazioni. Dimostrare che  $d_1 = d_2$  se e solo se  $d_1(x_i) = d_2(x_i)$  per ogni  $i = 1, \dots, s$ .

**1.13.** La **derivazione di Eulero** è l'unica  $A$ -derivazione

$$E: A[x_1, \dots, x_s] \rightarrow A[x_1, \dots, x_s]$$

tale che  $E(x_i) = x_i$  per ogni  $i$ . Dimostrare che  $E = \sum_i x_i \frac{\partial}{\partial x_i}$ .

**1.14.** Siano  $f \in A[x_1, \dots, x_s]$  e  $g_1, \dots, g_s \in A[t]$ , provare che

$$\frac{\partial}{\partial t} f(g_1(t), \dots, g_s(t)) = \sum_{i=1}^s \frac{\partial f}{\partial x_i}(g_1(t), \dots, g_s(t)) \frac{\partial g_i}{\partial t}(t)$$

**1.15.** Provare che in  $A[x_1, \dots, x_s]$  gli operatori  $\frac{\partial}{\partial x_i}$  commutano tra loro.

**1.16.** Sia  $A \rightarrow B$  un morfismo di anelli e siano  $f, g, h: B \rightarrow B$  tre  $A$ -derivazioni. Provare che:

1.  $f + g$  e  $bf$  sono  $A$ -derivazioni per ogni  $b \in B$ .
2.  $[f, g] := f \circ g - g \circ f$  è una  $A$ -derivazione.
3.  $[f \circ g, h] = f \circ [g, h] + [f, h] \circ g$ .

**1.17 (Lo Pfaffiano, I).** Sia  $\mathbb{K}$  un campo di caratteristica 0,  $V$  uno spazio vettoriale su  $\mathbb{K}$  di dimensione  $n = 2d$  e  $e_1, \dots, e_n$  una base di  $V$ . Data una matrice antisimmetrica  $A = (A_{ij})$  di ordine  $n$  a coefficienti in  $\mathbb{K}$ , si consideri la forma

$$\eta = \frac{1}{2} \sum_{i,j} A_{ij} e_i \wedge e_j \in \bigwedge^2 V.$$

Lo Pfaffiano di  $A$  è lo scalare  $Pf(A) \in \mathbb{K}$  definito dalla formula

$$\frac{1}{d!} \eta^{\wedge d} = Pf(A) e_1 \wedge \dots \wedge e_n.$$

Esplicitare lo Pfaffiano di una matrice antisimmetrica  $4 \times 4$ .

**1.18.** Sia  $R$  un dominio a fattorizzazione unica di caratteristica  $\neq 2$  e  $A = (A^{ij})$  una matrice simmetrica  $n \times n$  di rango 1 a coefficienti in  $R$ . Dimostrare che esistono, e che sono unici a meno di moltiplicazione per invertibili, elementi  $a, p_1, \dots, p_n \in R$  tali che  $\text{GCD}(p_1, \dots, p_n) = 1$  e  $A^{ij} = ap_i p_j$ .

**1.19 (Lo Pfaffiano II, \*).** Si consideri l'anello  $R = \mathbb{Z}[a_{ij}]$ , per  $1 \leq i < j \leq n$  e sia  $A = (A_{ij})$  la matrice antisimmetrica tale che  $A_{ij} = a_{ij}$  se  $i < j$ . Denotiamo con  $\tilde{A} = (A^{ij})$  la matrice aggiunta di  $A$ . Provare che:

- 1) Se  $n$  è dispari, allora  $A$  ha rango  $n - 1$ ,  $\tilde{A}$  è simmetrica di rango 1 e  $\text{GCD}(A^{ij}) = 1$ . Per l'Esercizio 1.18 si può scrivere  $A^{ij} = ap_i p_j$ . Mostrare che  $a = 1$ , che il vettore  $(p_1, \dots, p_n)$  è unicamente determinato a meno del segno e che vale  $\sum_j A_{ij} p_j = 0$  per ogni  $i = 1, \dots, n$ .
- 2) Se  $n = 2d$  è pari allora  $A$  ha rango  $n$  ed esiste  $Pf \in R$ , determinato a meno del segno, tale che  $\det A = Pf^2$ .
- 3) Esiste una determinazione del segno per  $Pf$  tale che ogni sua specializzazione  $Pf(A)$  ad una matrice antisimmetrica  $A$  di ordine pari su di un campo di caratteristica 0 coincide con lo Pfaffiano definito nell'Esercizio 1.17. (Sugg.: nelle notazioni dell'Esercizio 1.17 esiste una matrice  $B$  tale che  $\eta = Be_1 \wedge Be_2 + Be_e \wedge Be_4 + \dots + Be_{n-1} \wedge Be_n$ .)

**1.20.** Sia  $A(t)$  una matrice quadrata a coefficienti in  $\mathbb{K}[t]$ . Se  $r$  è la dimensione su  $\mathbb{K}$  del nucleo di  $A(0)$ , allora  $t^r$  divide il determinante di  $A(t)$ .

## 1.6 Anelli graduati

Un anello  $A$  si dice **graduato** se come gruppo abeliano ammette una decomposizione in somma diretta

$$A = \bigoplus_{d=-\infty}^{+\infty} A_d$$

tale che  $A_n A_m \subset A_{n+m}$  per ogni  $n, m \in \mathbb{Z}$ . Gli elementi di  $A_d \subset A$  si dicono **omogenei** di grado  $d$ . Un ideale  $I$  di un anello graduato  $A$  si dice **omogeneo** se ogniqualvolta  $a \in I$  accade che anche tutte le componenti omogenee di  $a$  appartengono a  $I$ : in altre parole  $I$  è omogeneo se e solo se  $I = \bigoplus_{d=-\infty}^{+\infty} (I \cap A_d)$ ; si dimostra facilmente che un ideale è omogeneo se e solo se è generato da elementi omogenei.

Se  $A$  è un dominio di integrità graduato e  $f, g \in A$  sono tali che il loro prodotto  $fg$  è omogeneo, allora  $f$  e  $g$  sono necessariamente omogenei: infatti se  $f = f_n + f_{n+1} + \dots + f_N$  e  $g = g_r + g_{r+1} + \dots + g_R$  sono le decomposizioni in componenti omogenee, con  $f_n, f_N, g_r, g_R \neq 0$ , allora  $fg = f_N g_R + f_n g_r + C$ , dove  $C$  è una combinazione lineare di elementi omogenei di gradi strettamente compresi fra  $n+r$  e  $N+R$ . Siccome  $fg$  è omogeneo deve necessariamente essere  $n+r = N+R$  e quindi  $n = N, r = R$ .

Per ogni anello commutativo  $A$ , l'anello dei polinomi  $A[x_1, \dots, x_n]$  possiede una graduazione naturale

$$A[x_1, \dots, x_n] = \bigoplus_{d=0}^{+\infty} A_d,$$

dove  $A_d$  è l'insieme dei polinomi omogenei di grado  $d$ , ossia l'insieme delle combinazioni lineari a coefficienti in  $A$  di monomi  $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$  con  $i_1 + \dots + i_n = d$ . A volte è utile associare ad ogni variabile  $x_i$  un peso  $w(x_i) \in \mathbb{N}$ ; in tal caso diremo che un polinomio è **isobaro di peso**  $m$ , rispetto ai pesi  $w(x_i)$ , se è combinazione lineare a coefficienti in  $A$  di monomi  $x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$  con  $i_1 w(x_1) + \dots + i_n w(x_n) = m$ .

Il ragionamento precedente mostra che se  $A$  è un dominio a fattorizzazione unica, allora i fattori irriducibili di un polinomio omogeneo (resp.: isobaro)  $f \in A[x_1, \dots, x_n]$  sono omogenei (resp.: isobari).

**Lemma 1.6.1.** *Sia  $A$  un dominio di integrità infinito e sia  $f \in A[x_1, \dots, x_s]$ . Allora  $f$  è omogeneo di grado  $n$  se e solo se*

$$f(tx_1, \dots, tx_s) = t^n f(x_1, \dots, x_s)$$

per ogni  $t \in A$ .

*Dimostrazione.* Se  $f$  è omogeneo la relazione precedente è evidente. Viceversa scriviamo  $f = f_0 + f_1 + \dots + f_N$  con  $f_i$  omogeneo di grado  $i$ . Il polinomio  $P = f_0 + tf_1 + \dots + t^N f_N - t^n f \in A[x_1, \dots, x_s, t]$  si annulla per infiniti valori di  $t \in A \subset A[x_1, \dots, x_s]$  e quindi deve necessariamente essere  $f_n = f$  e  $f_i = 0$  per  $i \neq n$ .  $\square$

**Lemma 1.6.2.** *Un ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$  è omogeneo se e solo se per ogni  $f \in I$  e per ogni  $t \in \mathbb{K}$ , il polinomio  $f_t(x_1, \dots, x_n) := f(tx_1, \dots, tx_n)$  appartiene all'ideale  $I$ .*

*Dimostrazione.* Dimostriamo il lemma utilizzando il cosiddetto *argomento di Vandermonde*: tale metodo sarà usato nuovamente in seguito.

Scriviamo  $f = f_0 + f_1 + \dots + f_s$ , dove  $f_i$  è omogeneo di grado  $i$ . Per ogni scelta di  $t_0, t_1, \dots, t_s \in \mathbb{K}$  vale  $f_{t_i} = \sum_j t_i^j f_j$ . Siccome  $\mathbb{K}$  è infinito, possiamo scegliere gli scalari  $t_0, t_1, \dots, t_s$  distinti. Quindi il determinante della matrice di Vandermonde  $(t_i^j)$  è invertibile, esiste la matrice inversa  $(a_j^i) = (t_i^j)^{-1}$  e, per ogni  $j = 0, \dots, s$ , vale  $f_j = \sum_i a_j^i f_{t_i} \in I$ .  $\square$

**Lemma 1.6.3 (Formula di Eulero).** *Se  $f \in A[x_1, \dots, x_s]$  è omogeneo di grado  $n$ , allora vale*

$$nf = \sum_{i=1}^s x_i \frac{\partial f}{\partial x_i}.$$

*Dimostrazione.* Induzione su  $n$ . Se  $n = 0$ , allora  $f \in A$  e la formula è chiara. Sia  $n > 0$  e supponiamo la formula vera per polinomi omogenei di grado  $n - 1$ ; per linearità basta provare la formula nel caso in cui  $f$  è un monomio, si può quindi scrivere  $f = x_j f'$  per qualche  $j = 1, \dots, s$  e  $f'$  omogeneo di grado  $n - 1$ . Quindi per induzione

$$\sum_{i=1}^s x_i \frac{\partial f}{\partial x_i} = \sum_{i=1}^s x_j x_i \frac{\partial f'}{\partial x_i} + x_j f' = (n-1)x_j f' + x_j f' = nx_j f' = nf.$$

$\square$

## Esercizi

**1.21.** Siano  $m$  e  $n$  interi positivi fissati e sia  $\mathbb{K}$  un campo di caratteristica 0 oppure maggiore di  $m$ . Dimostrare che l'insieme

$$\{p^m \mid p \in \mathbb{K}[x_1, \dots, x_n]\},$$

delle potenze  $m$ -esime dei polinomi genera  $\mathbb{K}[x_1, \dots, x_n]$  come  $\mathbb{K}$ -spazio vettoriale (Sugg.: Vandermonde).

**1.22.** Sia  $A = \mathbb{K}[x, y, z]/(xy - z^2)$ . Provare che  $A$  è un dominio di integrità e che  $z \in A$  è irriducibile ma non è primo. (Sugg.: l'anello  $A$  è graduato).

**1.23.** Sia  $A$  un dominio a fattorizzazione unica. Provare che il **determinante universale**  $\det(a_{ij}) \in A[a_{ij}]$  è irriducibile nell'anello dei polinomi a coefficienti in  $A$  nelle indeterminate  $a_{ij}$ , con  $i, j = 1, \dots, n$ . (Sugg.: induzione su  $n$ , essendo ovvio per  $n \leq 2$ . Sia per assurdo  $n > 2$  e  $f$  irriducibile omogeneo di grado  $d \leq n/2$  che divide  $\det(a_{ij})$  e specializziamo ponendo  $a_{1i} = 0$  per  $i = 2, \dots, n$ . La specializzazione di  $f$  divide  $a_{11}p$  dove  $p = \det(a_{ij})$ ,  $i, j \geq 2$  è un determinante universale e quindi irriducibile per l'ipotesi induttiva. Se ne deduce che  $d \leq 1$  ed adesso è facile concludere.)

**1.24 (Lo Pfaffiano III, \*).** Sia  $n = 2d$  un intero pari e sia  $Pf \in \mathbb{Z}[a_{ij}]$ ,  $1 \leq i < j \leq n$ , lo Pfaffiano universale definito nell'Esercizio 1.19. Dimostrare che  $Pf$  è omogeneo di grado  $d$  e che, se ad  $a_{ij}$  assegniamo il peso  $w(a_{ij}) = i + j$ , allora  $Pf$  è isobaro di peso  $d(n+1)$ . Si provi inoltre che  $Pf$  è irriducibile. (Sugg.: si usi la omogeneità di  $Pf$  e si consideri la specializzazione  $A_{ij} = A_{ji} = 0$  se  $i > d$  oppure se  $j < d$ .)

## 1.7 Algebre e moduli

Sia  $A$  un anello, un  **$A$ -modulo** è il dato di un gruppo abeliano  $M$ , con operazione di somma  $+$  ed elemento neutro  $0$ , e di un prodotto  $A \times M \rightarrow M$  tale che:

1.  $a(m_1 + m_2) = am_1 + am_2$  per ogni  $a \in A, m_1, m_2 \in M$ .
2.  $(a_1 + a_2)m = a_1m + a_2m$  per ogni  $a_1, a_2 \in A, m \in M$ .
3.  $(ab)m = a(bm)$  per ogni  $a, b \in A, m \in M$ .
4.  $1m = m$  e  $0m = 0$  per ogni  $m \in M$ .

Dati un  $A$ -modulo  $M$ , un ideale  $I \subset A$  ed un sottoinsieme  $E \subset M$  denotiamo con  $IE \subset M$  l'insieme delle combinazioni lineari finite di elementi di  $E$  a coefficienti in  $I$ . Chiaramente  $IE$  è chiuso per la somma e per il prodotto per scalare.

Dato un  $A$ -modulo  $M$ , un sottogruppo  $N \subset M$  si dice un **sottomodulo** se  $AN \subset N$ .

*Esempio 1.7.1.* Ogni anello  $A$  è un  $A$ -modulo in modo banale, i sottomoduli di  $A$  corrispondono agli ideali.

Dati due sottomoduli  $N_1, N_2 \subset M$ , la loro intersezione  $N_1 \cap N_2$  e la loro somma

$$N_1 + N_2 := \{n_1 + n_2 \mid n_1 \in N_1, n_2 \in N_2\}$$

sono ancora sottomoduli. Se  $N \subset M$  è un sottomodulo e  $I \subset A$  è un ideale allora  $IN$  è ancora un sottomodulo. Se  $N \subset M$  è un sottomodulo, allora il gruppo quoziente  $M/N$  possiede una struttura naturale di  $A$ -modulo.

Un insieme di generatori per  $M$  è un sottoinsieme  $E \subset M$  tale che  $M = AE$ . Un modulo che ammette un insieme finito di generatori si dice **finitamente generato**.

**Teorema 1.7.2 (Lemma di Nakayama).** *Siano  $A$  un anello,  $I \subset A$  un ideale,  $M$  un  $A$ -modulo finitamente generato e  $N \subset M$  un sottomodulo. Se  $IM + N = M$ , allora esiste  $a \in I$  tale che  $(1 + a)M \subset N$ .*

*Dimostrazione.* Sia  $e_1, \dots, e_r$  un insieme finito di generatori di  $M$ , dato che  $IM + N = M$ , per ogni  $i = 1, \dots, r$  si può scrivere  $e_i = \sum a_{ij}e_j + n_i$ , con  $a_{ij} \in I$  e  $n_i \in N$ . Se  $B$  è la matrice di coefficienti  $B_{ij} = \delta_{ij} - a_{ij}$ , allora si può scrivere la precedente relazione come un prodotto righe per colonne

$$B \begin{pmatrix} e_1 \\ \vdots \\ e_r \end{pmatrix} = \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix}$$

Moltiplicando a sinistra entrambi i membri per la matrice aggiunta di  $B$  si ottiene  $\det(B)e_i \in N$  per ogni  $i = 1, \dots, r$  e quindi  $\det(B)M \subset N$ . Basta adesso osservare che si può scrivere  $\det(B) = 1 + a$ , dove  $a$  appartiene all'ideale generato dagli  $a_{ij}$ .  $\square$

**Corollario 1.7.3.** *Sia  $\mathfrak{rad} \subset A$  l'intersezione di tutti gli ideali massimali e sia  $M$  un  $A$ -modulo finitamente generato: se vale  $\mathfrak{rad}M = M$ , allora  $M = 0$ .*

*Dimostrazione.* Applichiamo il Teorema 1.7.2 con  $I = \mathfrak{rad}$  e  $N = 0$ . Dunque esiste  $a \in \mathfrak{rad}$  tale che  $(1 + a)M = 0$ . Siccome  $a$  appartiene a  $\mathfrak{rad}$ , ne segue che  $1 + a$  non appartiene ad alcun ideale massimale e quindi è invertibile.  $\square$

Un applicazione  $f: M \rightarrow N$  tra due  $A$ -moduli si dice  $A$ -lineare o un morfismo di  $A$ -moduli se vale  $f(a_1m_1 + a_2m_2) = a_1f(m_1) + a_2f(m_2)$  per ogni  $m_1, m_2 \in M$  e  $a_1, a_2 \in A$ . È facile verificare che  $\text{Ker}(f) = \{m \in M \mid f(m) = 0\}$  e  $\text{Im}(f) = f(M) \subset N$  sono sottomoduli, mentre si definisce il **conucleo** di  $f$  come il modulo quoziente

$$\text{Coker}(f) = N/\text{Im}(f) = N/f(M).$$

Una successione di morfismi di  $A$ -moduli

$$\cdots \longrightarrow M_n \xrightarrow{d_n} M_{n+1} \xrightarrow{d_{n+1}} M_{n+2} \longrightarrow \cdots, \quad n \in \mathbb{Z},$$

si dice un **complesso** se  $d_{n+1} \circ d_n = 0$ , o equivalentemente se  $\text{Im}(d_n) \subset \text{Ker}(d_{n+1})$ , per ogni  $n$ . Si dice invece una **successione esatta** se  $\text{Im}(d_n) = \text{Ker}(d_{n+1})$  per ogni  $n$ .

La somma diretta di due moduli  $M$  ed  $N$  si indica con  $M \oplus N$  ed è data dall'insieme delle coppie  $(m, n)$ , dove  $m \in M$  e  $n \in N$ . La struttura di  $A$ -modulo è data dalle operazioni

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2), \quad a(m, n) = (am, an).$$

Notiamo che esiste una successione esatta

$$0 \longrightarrow M \xrightarrow{i} M \oplus N \xrightarrow{p} N \longrightarrow 0,$$

dove  $i(m) = (m, 0)$  e  $p(m, n) = n$ . Più in generale se  $\{M_i \mid i \in I\}$  è una famiglia qualsiasi di  $A$ -moduli, la somma diretta  $\oplus \{M_i \mid i \in I\}$  è per definizione l'insieme delle successioni  $\{m_i\}$ , con  $m_i \in M_i$  e  $m_i \neq 0$  per al più un numero finito di indici  $i \in I$ .

Un  $A$ -modulo si dice **libero** se è isomorfo ad una somma diretta di  $A$ -moduli isomorfi ad  $A$ . Il modulo  $A^r = \oplus_{i=1}^r A$  viene detto  $A$ -modulo libero di rango  $r$ . Osserviamo che un  $A$ -modulo  $M$  può essere generato da  $r$  elementi se e solo se esiste un morfismo surgettivo di moduli  $A^r \rightarrow M$ . Esiste una ovvia bigezione tra matrici a coefficienti in  $A$  e omomorfismi di  $A$ -moduli liberi di rango finito.

**Corollario 1.7.4.** *Sia  $A$  un anello,  $M$  un  $A$ -modulo finitamente generato e  $f: M \rightarrow M$  un morfismo surgettivo di moduli. Allora  $f$  è anche iniettivo e quindi un isomorfismo.*

*Dimostrazione.* L'endomorfismo  $f$  permette di considerare  $M$  come  $A[t]$ -modulo, dove la moltiplicazione per  $t$  è data da  $tm = f(m)$ . Per ipotesi  $(t)M = M$  e quindi esiste  $g \in A[t]$  tale che  $(1 + gt)M = 0$ . Per dimostrare che  $f$  è iniettiva basta dimostrare che ogni  $m \in \text{Ker}(f)$  è uguale a 0, e questo segue dalle uguaglianze

$$0 = (1 + gt)m = m + gf(m) = m.$$

□

**Definizione 1.7.5.** *Dato un  $A$ -modulo  $M$ , il suo **annullatore**  $\text{Ann}(M) \subset A$  è l'ideale formato dagli elementi  $a \in A$  tali che  $aM = 0$ .*

Osserviamo che  $\text{Ann}(M) \cap \text{Ann}(N) = \text{Ann}(M \oplus N)$ .

**Teorema 1.7.6 (Cayley-Hamilton).** *Sia  $A = (a_{ij})$  una matrice quadrata a coefficienti in un anello commutativo  $R$  con unità e denotiamo con  $p_A = \det(tI - A) \in R[t]$  il suo polinomio caratteristico. Allora  $p_A(A) = 0$ .*

*Dimostrazione.* Sia  $n$  l'ordine della matrice  $A$ , allora  $M = R^n$  possiede una struttura di  $R[t]$ -modulo ponendo la moltiplicazione per  $t$  uguale all'azione dell'endomorfismo indotto dalla matrice  $A$ . Bisogna dimostrare che  $p_A$  appartiene all'annullatore di  $M$ . Sia  $e_1, \dots, e_n$  la base canonica di  $M$ : in tale base si ha  $te_j = \sum_i a_{ij}e_i$ . Denotiamo con  $\delta_j^i$  la funzione delta di Kronecker e consideriamo la matrice  $B = b_{ij} = t\delta_j^i - a_{ij}$ ; notiamo che  $\det(B) = p_A$  e che  $B$  induce un morfismo di  $R[t]$ -moduli  $B: M^n \rightarrow M^n$  con la regola del prodotto riga per colonne

$$(m_1, \dots, m_n) \mapsto (m_1, \dots, m_n)B, \quad m_i \in M.$$



Per costruzione  $(e_1, \dots, e_n)B = 0$ , moltiplicando a destra per la matrice aggiunta si ottiene  $p_A e_i = 0$  per ogni  $i = 1, \dots, n$ .  $\square$

Un  $A$ -modulo  $B$  si dice una  **$A$ -algebra** se  $B$  possiede una struttura di anello compatibile con la struttura di  $A$ -modulo. In particolare deve valere la proprietà associativa del prodotto  $a(bc) = (ab)c$  per ogni  $a \in A, b, c \in B$ . Se  $f: A \rightarrow B$  è un omomorfismo di anelli, allora  $B$  ha una struttura naturale di  $A$ -algebra indotta dal prodotto  $ab = f(a)b$ . Viceversa se  $A, B$  sono anelli unitari, allora ogni struttura di  $A$ -algebra su  $B$  è indotta dall'omomorfismo  $f(a) = a1$ , dove  $a \in A$  e  $1$  indica l'unità in  $B$ .

Se  $B, C$  sono  $A$ -algebre, un morfismo  $B \rightarrow C$  si dice un **morfismo di  $A$ -algebre** se è contemporaneamente un omomorfismo di anelli ed un morfismo di  $A$ -moduli. Ad esempio, l'anello  $A[x_1, \dots, x_n]$  è una  $A$ -algebra ed i morfismi di  $A$ -algebre  $A[x_1, \dots, x_n] \rightarrow B$  sono in corrispondenza biunivoca con le  $n$ -uple ordinate di elementi di  $B$ . Una  $A$ -algebra si dice finitamente generata se è isomorfa ad un quoziente di un'algebra di polinomi in un numero finito di variabili.

## Esercizi

**1.25.** Sia  $A$  un anello,  $(f_{ij}) \in M(n, m, A)$  una matrice a coefficienti in  $A$  e  $f: A^m \rightarrow A^n$  il morfismo di moduli liberi corrispondente. Provare:

1. Se  $f$  è surgettivo, allora  $m \geq n$ . In particolare  $A^n$  è isomorfo ad  $A^m$  se e solo se  $n = m$ . (Sugg.: Corollario 1.7.4.)
2. Se  $f$  è iniettivo, allora esiste un determinante minore  $m \times m$  della matrice  $(f_{ij})$  che è diverso da 0; in particolare  $m \leq n$ . (Sugg.: induzione su  $m$  ed Esercizio 1.9.)
3. (\*) Il morfismo  $f$  è surgettivo se e solo se i determinanti minori  $n \times n$  della matrice  $(f_{ij})$  generano l'ideale unitario.

**1.26.** Sia  $R \subset \mathbb{K}[x, y]$  la sottoalgebra generata da tutti i monomi  $xy^a$ , con  $a \geq 0$ . Dimostrare che  $R$  non è finitamente generata.

**1.27.** Sia  $A \rightarrow B$  un morfismo di anelli unitari. Se  $B$  è generato come  $A$ -modulo da  $n$  elementi, allora per ogni  $b \in B$  esiste un polinomio  $p(t) \in A[t]$  monico di grado  $n$  tale che  $p(b) = 0$ . (Sugg.: Cayley-Hamilton.)

## 1.8 Esercizi complementari

**1.28 (Teoria delle basi).** Sia  $X$  un insieme non vuoto, si denoti con  $\mathcal{P}(X)$  la famiglia di tutti i sottoinsiemi di  $X$  e con  $\mathcal{P}_0(X)$  a famiglia di tutti i sottoinsiemi finiti di  $X$ .

Sia dato un operatore “di generazione”

$$\langle - \rangle: \mathcal{P}_0(X) \rightarrow \mathcal{P}(X)$$

con le seguenti proprietà:

1.  $A \subset \langle A \rangle$  per ogni  $A \subset X$  sottoinsieme finito.
2.  $\langle A \rangle \subset \langle B \rangle$  se e solo se  $\langle B \rangle$  contiene  $A$ .
3. Per ogni sottoinsieme finito  $A \subset X$  la relazione

$$x \sim y \quad \text{se e solo se} \quad x \in \langle A \cup \{y\} \rangle - \langle A \rangle$$

è simmetrica.

Provare che le condizioni 1,2 e 3 sono soddisfatte nei seguenti casi:

- $X$  spazio vettoriale e  $\langle A \rangle$  sottospazio vettoriale generato di  $A$ .
- $F \subset X$  estensione di campi e  $\langle A \rangle = \{x \in X \mid x \text{ algebrico su } F(A)\}$ .

Estendiamo l'operatore  $\langle - \rangle$  a tutti i sottoinsiemi di  $X$  ponendo

$$\langle A \rangle = \cup \{ \langle B \rangle \mid B \subset A \text{ finito} \}.$$

Diremo che un sottoinsieme  $A \subset X$  è un **insieme di generatori** se  $\langle A \rangle = X$ . Diremo che un sottoinsieme  $A \subset V$  è **indipendente** se per ogni sottoinsieme finito  $B \subset A$  ed ogni  $b \in B$  vale  $b \notin \langle B - \{b\} \rangle$ .

Sia  $A \subset X$  indipendente e sia  $x \in X$ . Dimostrare che  $A \cup \{x\}$  è indipendente se e solo se  $x \notin \langle A \rangle$ .

Sia  $\mathcal{B}$  la famiglia di tutti i sottoinsiemi indipendenti di  $X$ ; ordiniamo  $\mathcal{B}$  per inclusione, ossia  $A \leq B$  se  $A \subset B$ . Chiameremo **base** qualsiasi elemento massimale di  $\mathcal{B}$ . Dimostrare che le basi esistono e che per ogni base  $B$  vale  $\langle B \rangle = X$ , ossia che ogni base è anche un insieme di generatori. Dimostrare che ogni insieme indipendente si può estendere ad una base e che ogni insieme di generatori contiene basi.

Siano  $B \subset V$  un insieme di generatori ed  $A \subset V$  un insieme indipendente. Consideriamo l'insieme  $\mathcal{C}$  formato dalle coppie  $(S, f)$ , dove  $S \subset A$  ed  $f: S \rightarrow B$  è un'applicazione iniettiva tale che l'insieme  $(A - S) \cup f(S)$  è linearmente indipendente. Chiediamo inoltre che  $A \cap B \subset S$  e che  $f(v) = v$  per ogni  $v \in A \cap B$ . Ordiniamo  $\mathcal{C}$  per estensione, ossia  $(S, f) \leq (T, g)$  se  $S \subset T$  e  $g$  estende  $f$ . Dimostrare che  $\mathcal{C}$  è non vuoto, che possiede elementi massimali e che se  $(S, f)$  è massimale, allora  $S = A$ . (Sugg.: se esiste  $v \in A - S$ , allora  $B$  non è contenuto in  $\langle (A - (S \cup \{v\})) \cup f(S) \rangle$ .)

Dimostrare che due basi hanno la stessa cardinalità.

**1.29.** Sia  $F$  un campo infinito:

1. Se  $F \subset E$  è una estensione algebrica, provare che  $E$  ha, come insieme, la stessa cardinalità di  $F$ . (La dimostrazione richiede una certa conoscenza dell'aritmetica cardinale, vedi ad esempio [Halm1960]; il lettore ignaro può assumere questo punto come un dato di fatto e passare al successivo.)
2. Sia  $U$  un insieme di cardinalità strettamente maggiore di  $F$  e sia  $F \subset U$  una inclusione fissata. Denotiamo con  $\mathcal{A}$  l'insieme delle triple  $(E, +, \cdot)$  tali che  $F \subset E \subset U$  e  $+, \cdot: E \times E \rightarrow E$  sono operazioni binarie che inducono una struttura di campo su  $E$  che sia inoltre una estensione algebrica di  $F$ . Poniamo su  $\mathcal{A}$  la relazione di ordine  $(E, +, \cdot) \leq (E', +', \cdot')$  se e solo se  $E$  è un sottocampo di  $E'$ . Provare che  $\mathcal{A}$  possiede elementi massimali e che ogni elemento massimale è una chiusura algebrica di  $F$ .

**1.30.** Siano  $I, J$  ideali di un anello  $A$ . Provare che  $(I : J) = \{x \in A \mid xJ \subset I\}$  è un ideale. Tale ideale viene detto **ideale quoziente**.

**1.31.** Siano  $I_1, \dots, I_n$  ideali in un anello  $A$ . Provare che gli ideali  $I_1 I_2 \cdots I_n$  e  $I_1 \cap I_2 \cap \cdots \cap I_n$  hanno lo stesso radicale.

**1.32 (\*)**. Dimostrare che un dominio di integrità è a fattorizzazione unica se e solo se sono soddisfatte entrambe le seguenti condizioni:

1. Ogni elemento irriducibile è primo.
2. Ogni famiglia non vuota di ideali principali possiede un elemento massimale.

**1.33.** Dedurre dall'Esercizio 1.32 che ogni dominio ad ideali principali è a fattorizzazione unica.

**1.34.** Dimostrare che ogni dominio di integrità finito è un campo.

**1.35.** Dimostrare che i campi finiti sono perfetti; dimostrare inoltre che, in ogni caratteristica positiva, esistono campi non perfetti e domini perfetti che non sono campi.

**1.36.** Provare che il polinomio  $x^3 + 2x^2 + 2x - 88$  non ha radici razionali positive.

**1.37.** Sia  $A$  un anello commutativo e  $f = a_0x^n + \dots + a_n \in A[x]$  un polinomio a coefficienti in  $A$ . Provare che:

1.  $f$  è nilpotente se e solo se  $a_i$  è nilpotente per ogni  $i$ .
2.  $f$  è invertibile se e solo se  $a_n$  è invertibile e  $a_0, \dots, a_{n-1}$  sono nilpotenti.

**1.38.** Sia  $A$  un anello commutativo con unità e siano

$$\mathfrak{rad} = \{x \in A \mid 1 + xy \text{ è invertibile per ogni } y \in A\} \quad (\text{vedi Esercizio 1.7}),$$

$$\mathfrak{n} = \sqrt{0} = \{x \in A \mid x \text{ è nilpotente}\}, \quad E(A) = \{x \in A \mid x^2 = x\}.$$

Provare che:

1. Sia  $I \subset \mathfrak{rad}$  un ideale e sia  $a \in A$ . Provare che  $a$  è invertibile in  $A$  se e solo se la sua proiezione in  $A/I$  è invertibile.
2. (\*) Sia  $I \subset A$  ideale e  $\alpha: E(A) \rightarrow E(A/I)$  la proiezione al quoziente. Dimostrare che se  $I \subset \mathfrak{rad}$ , allora  $\alpha$  è iniettiva e che se  $I \subset \mathfrak{n}$ , allora  $\alpha$  è bigettiva. (Sugg.: per provare la surgettività di  $\alpha$  non è restrittivo supporre  $I$  principale a quadrato nullo; può risultare utile dimostrare che  $1 - 2x$  è invertibile nell'anello  $\mathbb{Z}[x]/(x^2 - x)$ .)

**1.39.** Sia  $B$  una matrice  $n \times n$  a coefficienti in un anello  $A$  e  $\tilde{B}$  la sua matrice aggiunta. Provare che per ogni vettore riga  $v$  e per ogni vettore colonna  $w$  di  $A^n$  vale

$$v\tilde{B}w + \det \begin{pmatrix} B & w \\ v & 0 \end{pmatrix} = 0$$

**1.40.** Sia  $D$  l'insieme dei divisori di 0 di un anello  $A$  e sia  $\mathcal{F}$  la famiglia degli ideali contenuti in  $D$ . Provare che  $\mathcal{F}$  possiede elementi massimali rispetto all'inclusione, ognuno dei quali è un ideale primo.

**1.41.** Dimostrare che la famiglia degli ideali primi di un anello commutativo possiede elementi minimali rispetto all'inclusione.

**1.42.** Sia  $f \in \mathbb{K}[x_1, \dots, x_s]$  un polinomio omogeneo di grado  $n$ . Differenziare la relazione  $t^n f(x_1, \dots, x_s) = f(tx_1, \dots, tx_s)$  e riottenere la formula di Eulero.

**1.43.** Provare che l'unica  $\mathbb{R}$ -derivazione su  $\mathbb{C}$  è quella nulla. Più in generale se  $A$  è un dominio perfetto e  $f \in A[t]$  è irriducibile, allora ogni  $A$ -derivazione su  $A[t]/(f)$  è nulla.

**1.44.** Provare che un dominio a fattorizzazione unica  $A$  è perfetto se e solo se per ogni  $f \in A[t]$  irriducibile vale  $\frac{df}{dt} \neq 0$ .

**1.45.** Sia  $A \rightarrow B$  un morfismo di anelli,  $a, b \in B$  e siano  $D, D': B \rightarrow B$  due  $A$ -derivazioni; allora vale

$$[aD, bD'] = ab[D, D'] + aD(b)D' - bD'(a)D.$$

**1.46.** Sia  $\mathbb{Q} \rightarrow A$  un morfismo di anelli,  $D: A \rightarrow A$  una  $\mathbb{Q}$ -derivazione e sia  $x \in A$  tale che  $Dx = 1$  e  $\bigcap_{i=1}^{\infty} (x^i) = 0$ . Provare che  $x$  non è un divisore di 0.

**1.47.** Enunciare e provare l'analogo della formula di Eulero (Lemma 1.6.3) per i polinomi isobari.

**1.48.** Sia  $\mathbb{K}$  un campo di caratteristica 0 e  $S = \mathbb{K}[x_1, \dots, x_n] = \bigoplus S_d$ , dove  $S_d$  denota lo spazio vettoriale dei polinomi omogenei di grado  $d$ . Denotiamo  $\partial_i = \frac{\partial}{\partial x_i} : S \rightarrow S$ , per  $i = 1, \dots, n$ , le derivate parziali e  $T = \mathbb{K}[\partial_1, \dots, \partial_n] = \bigoplus T_d$ , dove  $T_d$  è per definizione lo spazio vettoriale degli operatori differenziali omogenei di grado  $d$ . Provare:

1. Per ogni intero positivo  $d$ , le naturali applicazioni bilineari  $S_d \times T_d \rightarrow \mathbb{K}$  sono nondegeneri.
2. Un operatore  $D \in T_d$  è nullo se e solo se  $D(f^d) = 0$  per ogni  $f \in S_1$ .
3. Le  $d$ -esime potenze di elementi di  $S_1$  generano  $S_d$  come  $\mathbb{K}$ -spazio vettoriale.

(Sugg.: due qualsiasi delle precedenti affermazioni implicano la terza; all'autore è riuscito più facile dimostrare 1. e 2. ricordandosi che  $\mathbb{K}$  è infinito.)

**1.49 (Teorema di Macaulay).** (caratteristica 0) Nelle notazioni dell'Esercizio 1.48, data  $f \in S_n$ ,  $f \neq 0$ , si definisce  $f^\perp = \{D \in T \mid Df = 0\}$ . Provare:

1.  $f^\perp$  è un ideale omogeneo di  $T$ .
2. Se  $g \in S$  è omogeneo e  $f^\perp = g^\perp$  allora  $g = af$ ,  $a \in \mathbb{K}$ .

Si denoti  $I_d = f^\perp \cap T_d$ , per il punto 1)  $f^\perp = \bigoplus I_d$ . Sia  $A = T/f^\perp = \bigoplus A_d$  dove  $A_d = T_d/I_d$ . Provare:

3.  $A_n = \mathbb{K}$  e  $A_d = 0$  per ogni  $d > n$ .
4.  $\text{Zoccolo}(A) := \{a \in A \mid aA_d = 0 \text{ per ogni } d > 0\} = A_n$ .
5. Viceversa ogni ideale omogeneo  $I \subset T$  tale che l'anello  $A = T/I$  soddisfa le precedenti condizioni 3) e 4) è del tipo  $f^\perp$  per qualche  $f \in S_n$ . (Sugg.:  $I$  è unicamente determinato da  $I_n$ ).

**1.50.** (caratteristica 0) Dimostrare che per ogni intero  $n \geq 3$  non esistono polinomi  $p, q, r \in \mathbb{K}[x]$  relativamente primi e non costanti tali che  $p^n + q^n = r^n$ . (Sugg.: siano per assurdo  $p, q, r$  come sopra e tali che  $\deg(p) \geq \max(1, \deg(q))$ ; considerare la derivata rispetto a  $x$  e dedurre che  $p^{n-1}$  divide  $qr' - rq'$ .)

**1.51.** Dato un  $A$ -modulo  $M$  si consideri  $B = A \oplus M$  dotato delle operazioni  $(a, m) + (b, n) = (a + b, m + n)$  e  $(a, m)(b, n) = (ab, an + bm)$ . Provare che  $B$  è un anello.

**1.52.** Si consideri l'anello  $B = \mathbb{K}[x, y]/(x - y^2)$ .

1. Si provi che  $B$  è un  $\mathbb{K}[x]$ -modulo libero di rango 2 ed un  $\mathbb{K}[y]$ -modulo libero di rango 1.
2. Siccome  $\mathbb{K}[x]$  è isomorfo a  $\mathbb{K}[y]$  e due moduli liberi isomorfi hanno lo stesso rango ne segue che  $1=2$ ; dove sta l'errore?

## Spazi affini e proiettivi

### 2.1 Combinazioni baricentriche

Sia  $V$  uno spazio vettoriale su di un campo  $\mathbb{K}$ . Una combinazione lineare  $a_0v_0 + \dots + a_nv_n$  di vettori  $v_i \in V$  si dice una **combinazione baricentrica** se  $\sum a_i = 1$ . Un sottoinsieme di  $V$  si dice un **sottospazio affine** se è chiuso per combinazioni baricentriche. Ogni sottospazio vettoriale è anche un sottospazio affine.

Notiamo che combinazione baricentrica di combinazioni baricentriche è ancora baricentrica; in particolare l'insieme di tutte le combinazioni baricentriche di un numero finito di vettori è un sottospazio affine. Intersezione di sottospazi affini è ancora un sottospazio affine.

**Lemma 2.1.1.** *Sia  $K$  un sottospazio affine non vuoto di uno spazio vettoriale  $V$ . Allora:*

1. *Per ogni  $v \in V$  il sottoinsieme  $v + K = \{v + x \mid x \in K\}$  è ancora un sottospazio affine detto il **traslato di  $K$  tramite  $v$** .*
2. *Il sottoinsieme  $W = \{u - v \mid u, v \in K\} \subset V$  è un sottospazio vettoriale e vale  $K = v + W$  per ogni  $v \in K$ . In particolare  $K$  è un sottospazio vettoriale se e solo se  $0 \in K$ .*

*Dimostrazione. Esercizio.* □

Segue dal Lemma 2.1.1 che per ogni sottospazio affine non vuoto  $K \subset V$  esiste unico un sottospazio vettoriale  $W$  tale che  $K = v + W$  per ogni  $v \in K$ . Si definisce la dimensione di  $K$  come la dimensione di  $W$ . Se  $K = \emptyset$  allora si pone per convenzione  $\dim K = -1$ .

Un'applicazione  $f: V \rightarrow W$  tra spazi vettoriali si dice **affine** se commuta con le combinazioni baricentriche, cioè se per ogni  $v_0, \dots, v_n \in V$  e per ogni  $a_0, \dots, a_n \in \mathbb{K}$  tali che  $\sum a_i = 1$  vale  $f(\sum a_i v_i) = \sum a_i f(v_i)$ . Ogni applicazione lineare è a maggior ragione affine, viceversa se  $f: V \rightarrow W$  è affine e  $f(0) = 0$ , allora  $f$  è lineare. Infatti, dati comunque  $u, v \in V$  e  $a, b \in \mathbb{K}$ , ponendo  $c = 1 - a - b$  si ha

$$f(au + bv) = f(au + bv + c0) = af(u) + bf(v) + cf(0) = af(u) + bf(v).$$

Le traslazioni in uno spazio vettoriale sono applicazioni affini invertibili e composizione di applicazioni affini è ancora affine. Poiché le applicazioni lineari sono esattamente le applicazioni affini  $f$  tali che  $f(0) = 0$  si ha che ogni applicazione affine è la composizione di una applicazione lineare e di una traslazione.

**Esercizi**

**2.1.** Sia  $E$  un sottoinsieme di uno spazio vettoriale su di un campo  $\mathbb{K}$  con almeno tre elementi. Provare che  $E$  è un sottospazio affine se e solo se per ogni  $u, v \in E$  e per ogni  $a \in \mathbb{K}$  vale  $au + (1 - a)v \in E$ .

**2.2.** Sia  $V$  uno spazio vettoriale su di un campo  $\mathbb{K}$ . Provare che se  $\mathbb{K}$  possiede almeno  $n + 1$  elementi, allora  $V$  non è unione di  $n$  sottospazi affini propri. In particolare uno spazio vettoriale su di un campo infinito non è unione finita di sottospazi affini propri. (Sugg.: induzione su  $n$ ; sia per assurdo  $V = \cup_{i=1}^n V_i$ , allora a meno di traslazioni possiamo supporre  $0 \in V_n$ . Se  $V_n \subset V_i$  per qualche  $i < n$  abbiamo finito, altrimenti scegliamo  $v \in V_n - \cup_{i=1}^{n-1} (V_n \cap V_i)$ ,  $h \in V - V_n$  e consideriamo la retta affine  $L = \{tv + (1-t)h \mid t \in \mathbb{K}\}$ . Esiste allora un indice  $i$  tale che  $L$  interseca  $V_i$  in almeno due punti.)

**2.3.** Sia  $f: V \rightarrow W$  una applicazione affine tra spazi vettoriali e  $K \subset V$  un sottospazio affine. Dimostrare che esiste un sottospazio vettoriale  $W \subset V$  tale che

$$f^{-1}(f(v)) \cap K = v + W$$

per ogni  $v \in K$ .

**2.4.** Sia  $f: V \rightarrow W$  una applicazione affine. Dimostrare che:

1. Se  $E \subset V$  è un sottospazio affine, allora  $f(E)$  è un sottospazio affine.
2. Se  $H \subset W$  è un sottospazio affine, allora  $f^{-1}(H)$  è un sottospazio affine.

**2.5.** Sia  $f: \mathbb{K}^n \rightarrow \mathbb{K}^m$  un'applicazione affine e siano  $f(0) = (b_1, \dots, b_m)$ ,  $f(\delta^i) - f(0) = (a_{1i}, \dots, a_{mi})$ , dove  $\delta^1, \dots, \delta^n$  indica la base canonica di  $\mathbb{K}^n$ . Provare che  $f$  manda il punto  $(x_1, \dots, x_n)$  nel punto  $(y_1, \dots, y_m)$  che soddisfa la relazione

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \\ 0 & \dots & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 1 \end{pmatrix}.$$

Caratterizzare inoltre le matrici  $(n + 1) \times (n + 1)$  corrispondenti alle traslazioni in  $\mathbb{K}^n$ .

**2.6.** Sia  $H \subset \mathbb{K}^n$  un sottospazio affine non contenente  $0$  e  $f: H \rightarrow \mathbb{K}^m$  un'applicazione affine. Dimostrare che  $f$  è la restrizione ad  $H$  di un'applicazione lineare  $g: \mathbb{K}^n \rightarrow \mathbb{K}^m$ .

**2.7.** Siano  $P_1 = (1, 2)$ ,  $P_2 = (3, 1)$  e  $P_3 = (3, 3)$ . Siano inoltre  $Q_1 = (1, 8)$ ,  $Q_2 = (0, 7)$  e  $Q_3 = (7, 3)$ . Si determini l'applicazione affine  $\mathbb{R}^2 \rightarrow \mathbb{R}^2$  che trasforma  $P_i$  in  $Q_i$  per  $i = 1, 2, 3$ .

**2.2 Spazi affini**

Definiamo il **simpleso  $n$ -dimensionale standard**

$$\Delta^n = \{(t_0, \dots, t_n) \in \mathbb{K}^{n+1} \mid \sum t_i = 1\}.$$

Osserviamo che  $\Delta^n$  è un sottospazio affine e coincide con l'insieme di tutte le combinazioni baricentriche della base canonica  $\delta^0 = (1, 0, \dots, 0)$ ,  $\delta^1 = (0, 1, 0, \dots, 0)$  ecc. di  $\mathbb{K}^{n+1}$ .

Introduciamo adesso la nozione astratta di spazio affine.

**Definizione 2.2.1.** Un prespazio affine su di un campo  $\mathbb{K}$  è il dato di un insieme  $A$  e di una successione di applicazioni

$$b_n: A^{n+1} \times \Delta^n \rightarrow A, \quad \text{per } n \geq 1.$$

È conveniente definire  $b_0$  come l'identità su  $A$  e, per semplicità notazionale, scrivere

$$b_n(p_0, \dots, p_n, t_0, \dots, t_n) = t_0 p_0 + \dots + t_n p_n.$$

Chiameremo le applicazioni  $b_n$ ,  $n \geq 0$ , **combinazioni baricentriche**.

**Definizione 2.2.2.** Un prespazio affine  $A$  su di un campo  $\mathbb{K}$  si dice uno **spazio affine** se:

1. Per ogni  $p_0, \dots, p_n \in A$  e per ogni  $i = 0, \dots, n$  vale

$$0p_0 + \dots + 1p_i + \dots + 0p_n = p_i.$$

2. Per ogni  $p_0, \dots, p_n, q_0, \dots, q_m \in A$  l'insieme

$$\{(t_0, \dots, t_n, s_0, \dots, s_m) \in \Delta^n \times \Delta^m \mid t_0 p_0 + \dots + t_n p_n = s_0 q_0 + \dots + s_m q_m\}$$

è un sottospazio affine di  $\Delta^n \times \Delta^m \subset \mathbb{K}^{n+m+2}$ .

*Esempio 2.2.3.* Ogni spazio vettoriale  $V$  ha una struttura naturale di spazio affine, dove  $b_n$  è la combinazione baricentrica usuale. Denoteremo  $\mathbb{A}_{\mathbb{K}}^n$  lo spazio affine associato a  $\mathbb{K}^n$ .

*Esempio 2.2.4.* Sia  $V$  uno spazio vettoriale su  $\mathbb{K}$ , sia  $H \subset V$  un iperpiano e sia  $A$  l'insieme delle rette (sottospazi lineari di dimensione 1) di  $V$  che non sono contenute in  $H$ . L'insieme  $A$  possiede una naturale struttura di spazio affine con le combinazioni baricentriche definite nel modo seguente: date  $n+1$  rette  $L_0, \dots, L_n \in A$  scegliamo  $n+1$  vettori  $v_0, \dots, v_n$  tali che  $v_i \in L_i - \{0\}$  e  $v_i - v_0 \in H$  per ogni  $i = 0, \dots, n$ . Definiamo quindi  $t_0 L_0 + \dots + t_n L_n$  come la retta generata dal vettore  $\sum t_i v_i$ . Lasciamo per esercizio la semplice verifica che tali combinazioni baricentriche sono ben definite e definiscono una struttura di spazio affine su  $A$ .

*Esempio 2.2.5.* Sia  $E$  un sottospazio di uno spazio vettoriale  $V$  e denotiamo con  $\pi: V \rightarrow V/E$  la proiezione al quoziente. Vogliamo mostrare che l'insieme  $A$ , dei sottospazi vettoriali  $H \subset V$  tali che la proiezione  $\pi: H \rightarrow V/E$  è un isomorfismo (cioè tali che  $V = E \oplus H$ ), possiede una struttura di spazio affine.

Sia  $\{u_i \mid i \in \mathcal{I}\}$  una base dello spazio quoziente  $V/E$ ; per ogni  $H \in A$  e per ogni  $i \in \mathcal{I}$  denotiamo  $v_i(H) = H \cap \pi^{-1}(u_i)$ . Dati  $H_0, \dots, H_n \in A$  e  $(t_0, \dots, t_n) \in \Delta^n$ , definiamo  $t_0 H_0 + \dots + t_n H_n$  come il sottospazio  $H$  generato dall'insieme di vettori  $\{\sum_j t_j v_i(H_j) \mid i \in \mathcal{I}\}$ . Poiché  $\pi(\sum_j t_j v_i(H_j)) = u_i$ , la proiezione  $H \rightarrow V/E$  risulta bigettiva e quindi  $H \in A$ . Infine si dimostra facilmente che  $H$  non dipende dalla scelta della base  $\{u_i\}$  e che le combinazioni baricentriche inducono una struttura affine su  $A$ .

**Lemma 2.2.6.** In ogni spazio affine le combinazioni baricentriche sono simmetriche e commutano con le combinazioni baricentriche sui semplici standard.

Prima di passare alla dimostrazione precisiamo meglio il senso dell'enunciato. Sia  $A$  uno spazio affine, dire che le combinazioni baricentriche sono simmetriche significa che per ogni  $p_0, \dots, p_n \in A$ , ogni  $(t_0, \dots, t_n) \in \Delta^n$  ed ogni permutazione  $\sigma \in \Sigma_{n+1}$  vale

$$t_0 p_0 + \dots + t_n p_n = t_{\sigma(0)} p_{\sigma(0)} + \dots + t_{\sigma(n)} p_{\sigma(n)}$$

e quindi acquista significato l'espressione  $\sum_i t_i p_i$ . Dire che le combinazioni baricentriche commutano con le combinazioni baricentriche sui semplici standard significa che per ogni  $p_0, \dots, p_n \in A$ , ogni  $(m+1)$ -upla di vettori  $t^0, \dots, t^m \in \Delta^n$  ed ogni  $s \in \Delta^m$  vale

$$\sum_{j=0}^m s_j \left( \sum_{i=0}^n t_i^j p_i \right) = \sum_{i=0}^n \left( \sum_{j=0}^m s_j t_i^j \right) p_i.$$

*Dimostrazione.* Dimostriamo prima che le combinazioni baricentriche sullo spazio affine commutano con quelle sui semplici standard. Denotiamo  $q_j = t_0^j p_0 + \dots + t_m^j p_m$ ; per la Definizione 2.2.2 abbiamo che

$$H = \{(v, w) \in \Delta^n \times \Delta^m \mid v_0 p_0 + \dots + v_n p_n = w_0 q_0 + \dots + w_m q_m\}$$

è un sottospazio affine che contiene i vettori  $(t^j, \delta^j)$ , per  $j = 0, \dots, m$ . Quindi per ogni  $s = (s_0, \dots, s_m) \in \Delta^m$  si ha che  $(\sum_j s_j t^j, s) \in H$  e perciò

$$\left( \sum_j s_j t_0^j \right) p_0 + \dots + \left( \sum_j s_j t_n^j \right) p_n = s_0 q_0 + \dots + s_m q_m.$$

Per mostrare la simmetria, per ogni permutazione  $\sigma$  basta applicare il punto precedente ai vettori  $t^j = \delta^{\sigma(j)}$ .  $\square$

**Lemma 2.2.7.** *In ogni spazio affine le combinazioni baricentriche soddisfano le proprietà distributive, ossia vale*

$$0p_0 + t_1 p_1 + \dots + t_n p_n = t_1 p_1 + \dots + t_n p_n,$$

e se  $p_0 = p_1$ , allora

$$t_0 p_0 + t_1 p_1 + \dots + t_n p_n = (t_0 + t_1) p_1 + \dots + t_n p_n.$$

*Dimostrazione.* Per il Lemma 2.2.6 possiamo scrivere

$$t_1 p_1 + \dots + t_n p_n = \sum_{j=1}^n t_j \left( \sum_{i=0}^n \delta_i^j p_i \right) = \sum_{i=0}^n \left( \sum_{j=1}^n t_j \delta_i^j \right) p_i = 0p_0 + t_1 p_1 + \dots + t_n p_n.$$

Supponiamo adesso  $p_0 = p_1 = p$ ; allora

$$H = \left\{ (v, w) \in \mathbb{K}^3 \times \mathbb{K}^2 \mid \begin{array}{l} v_0 p + v_1 p + v_2 p + \sum_{i \geq 2} t_i p_i = w_0 p + w_1 p + \sum_{i \geq 2} t_i p_i, \\ v_0 + v_1 + v_2 = w_0 + w_1 = t_0 + t_1. \end{array} \right\}$$

è un sottospazio affine che contiene i vettori

$$a = ((t_0, 0, t_1), (t_0, t_1)), \quad b = ((0, t_1, t_0), (t_1, t_0)), \quad c = ((0, 0, t_0 + t_1), (0, t_0 + t_1))$$

e quindi contiene anche la combinazione baricentrica

$$a + b - c = ((t_0, t_1, 0), (t_0 + t_1, 0)).$$

$\square$

Dunque le combinazioni baricentriche in uno spazio affine hanno tutte le buone proprietà che è lecito aspettarsi dalla notazione adottata.

Poiché in queste note tutti i campi saranno (tranne avviso contrario) infiniti, giova dimostrare il seguente risultato.



**Proposizione 2.2.8.** *Sia  $A$  uno spazio affine su  $\mathbb{K}$ . Se  $\mathbb{K}$  possiede almeno 3 elementi, allora le combinazioni baricentriche sono univocamente determinate dalle combinazioni baricentriche a due termini, ossia  $b_1$  determina  $b_n$  per ogni  $n$ .*

*Dimostrazione.* Siano  $p_0, \dots, p_n \in A$ , con  $n > 1$  e  $v = (v_0, \dots, v_n) \in \Delta^n$ . Scegliamo un elemento  $a \in \mathbb{K}$  diverso da 0 e da  $v_0$  e consideriamo i vettori

$$u = (a, 1 - a, 0, \dots, 0), \quad w = \frac{a}{a - v_0} \left( v - \frac{v_0}{a} u \right) = (0, w_1, \dots, w_n).$$

Siccome  $w_0 = 0$ , per induzione su  $n$  i punti  $q_0 = w_0 p_0 + \dots + w_n p_n$  e  $q_1 = a p_0 + (1 - a) p_1$  sono determinati da  $b_1$  e quindi lo è anche

$$v_0 p_0 + \dots + v_n p_n = \left( 1 - \frac{v_0}{a} \right) q_0 + \frac{v_0}{a} q_1.$$

□

**Definizione 2.2.9.** *Un sottoinsieme  $E$  di uno spazio affine  $A$  si dice un **sottospazio affine** se è chiuso per combinazioni baricentriche.*

Intersezione di sottospazi affini è ancora un sottospazio affine e per ogni sottoinsieme  $S \subset A$  il sottospazio affine generato  $\langle S \rangle$  è l'intersezione di tutti i sottospazi affini contenenti  $S$ . Equivalentemente  $\langle S \rangle$  è uguale all'insieme di tutte le combinazioni baricentriche finite di elementi di  $S$ .

**Definizione 2.2.10.** *Sia  $A$  uno spazio affine;  $n + 1$  punti  $p_0, \dots, p_n \in A$  si dicono **linearmente indipendenti** se l'applicazione*

$$\Delta^n \rightarrow A, \quad (t_0, \dots, t_n) \mapsto t_0 p_0 + \dots + t_n p_n$$

è iniettiva. In caso contrario si dicono **linearmente dipendenti**. La **dimensione** di uno spazio affine non vuoto  $A$  è definita come

$$\dim A = \sup\{n \geq 0 \mid \text{esistono } p_0, \dots, p_n \in A \text{ linearmente indipendenti}\}.$$

La dimensione dello spazio affine vuoto si pone per convenzione uguale a  $-1$ .

Se  $K$  è un sottospazio affine di uno spazio vettoriale  $V$ . Dati  $p_0, \dots, p_n \in K$  e  $a_1, \dots, a_n \in \mathbb{K}$  si ha

$$p_0 + \sum_{i=1}^n a_i (p_i - p_0) = \left( 1 - \sum_{i=1}^n a_i \right) p_0 + a_1 p_1 + \dots + a_n p_n$$

e quindi  $p_0, \dots, p_n$  sono linearmente indipendenti nello spazio affine  $K$  se e solo se  $p_1 - p_0, \dots, p_n - p_0$  solo linearmente indipendenti nello spazio vettoriale  $V$ . Ne segue che per sottospazi affini di uno spazio vettoriale la Definizione 2.2.10 coincide con la definizione di dimensione data nella Sezione 2.1.

**Definizione 2.2.11.** *Un'applicazione affine è un'applicazione tra spazi affini che commuta con le combinazioni baricentriche. Un **isomorfismo affine** è un'applicazione affine e bigettiva. Un isomorfismo affine di uno spazio affine in sé si dice una **affinità**.*

Se  $f: A \rightarrow B$  è un isomorfismo affine, allora anche la sua inversa  $f^{-1}: B \rightarrow A$  è un isomorfismo affine. L'insieme di tutte le affinità di uno spazio affine  $A$ , dotato del prodotto di composizione, è un gruppo che denoteremo  $\text{GA}(A)$ .

*Esempio 2.2.12.* Nelle notazioni dell'Esempio 2.2.4, se  $v \in V - H$ , allora l'applicazione  $H \rightarrow A$ , data da  $h \mapsto [v + h]$ , è un isomorfismo affine (qui  $[w]$  denota la retta generata dal vettore  $w$ ).

**Definizione 2.2.13.** Chiameremo **traslazione** in uno spazio affine  $A$  qualunque applicazione del tipo

$$t_{\overline{pq}}: A \rightarrow A, \quad t_{\overline{pq}}(x) = x + q - p.$$

per qualche coppia di punti  $p, q \in A$ .

Dalla proprietà distributiva delle combinazioni baricentriche segue che la traslazione  $t_{\overline{pq}}$  è un'applicazione affine invertibile con inversa  $t_{\overline{qp}}$ . Denotiamo con  $T(A)$  l'insieme di tutte le traslazioni in  $A$ .

Giova osservare che, poiché le traslazioni sono definite in termini di combinazioni baricentriche, esse commutano con tutte le applicazioni affini: più precisamente se  $f: A \rightarrow B$  è una applicazione affine, allora per ogni  $p, q \in A$  vale  $f \circ t_{\overline{pq}} = t_{\overline{f(p)f(q)}} \circ f$ . In particolare ogni isomorfismo affine induce una bigezione tra i rispettivi insiemi di traslazioni. Si intuisce che diverse coppie  $p, q$  possono dare le medesime traslazioni; il come è spiegato nel seguente lemma.

**Lemma 2.2.14.** Nelle notazioni precedenti, per ogni  $p, q \in A$  vale:

1.  $t_{\overline{pp}} = Id$ .
2.  $t_{\overline{pq}}(p) = q$ , in particolare le traslazioni agiscono transitivamente su  $A$ .
3. Sia  $f$  una traslazione e  $r \in A$  un qualsiasi punto; se  $f(r) = s$ , allora  $f = t_{\overline{rs}}$ .  
In particolare se  $f(r) = r$ , allora  $f = t_{\overline{rr}} = Id$  e quindi ogni traslazione diversa dall'identità non ha punti fissi.
4. Le traslazioni formano un sottogruppo normale abeliano  $T(A) \subset GA(A)$  del gruppo delle affinità di  $A$ .

*Dimostrazione.* [1] e [2] sono banali.

[3] Per ipotesi  $f$  è una traslazione e quindi  $f = t_{\overline{pq}}$  per qualche coppia di punti  $p, q$  tali che  $q + r - p = s$ ; quindi per ogni  $x \in A$

$$t_{\overline{rs}}(x) = x + s - r = x + (q + r - p) - r = x + q - p = t_{\overline{pq}}(x) = f(x).$$

[4] Siano  $f, g$  due traslazioni, scegliamo un punto  $p \in A$  e poniamo  $q = f(p)$ ,  $r = g(q)$ . Allora per ogni  $x$  vale

$$g(f(x)) = g(x + q - p) = x + q - p + r - q = x + r - p,$$

$$f(g(x)) = f(x + r - q) = x + r - q + q - p = x + r - p$$

e quindi  $T(A)$  è un sottogruppo abeliano di  $GA(A)$ . Se  $f: A \rightarrow A$  è una affinità, allora per ogni  $x$  si ha

$$f(t_{\overline{pq}}(x)) = f(-p + q + x) = -f(p) + f(q) + f(x) = t_{\overline{f(p)f(q)}}(f(x))$$

e quindi  $f t_{\overline{pq}} f^{-1} = t_{\overline{f(p)f(q)}}$ . □

**Esercizi**

**2.8.** Sia  $A$  uno spazio affine su  $\mathbb{K}$  di dimensione finita  $n$  e siano  $p_0, \dots, p_n \in A$  dei punti linearmente indipendenti. Dimostrare che l'applicazione

$$\Delta^n \rightarrow A, \quad (t_0, \dots, t_n) \mapsto t_0 p_0 + \dots + t_n p_n$$

è un isomorfismo affine.

**2.9.** Siano  $A$  e  $B$  spazi affini su di un campo  $\mathbb{K}$  con almeno 3 elementi. Provare che un'applicazione  $f: A \rightarrow B$  è affine se e solo se per ogni  $p, q \in A$  e per ogni  $a \in \mathbb{K}$  vale  $f(ap + (1-a)q) = af(p) + (1-a)f(q)$ .

**2.10.** Siano  $A$  e  $B$  spazi affini. Provare che:

1. Il prodotto cartesiano  $A \times B$  è uno spazio affine.
2. L'insieme di tutte le applicazioni affini  $f: A \rightarrow B$  è uno spazio affine.

**2.11.** Se  $A$  è uno spazio affine su  $\mathbb{K}$ , un'applicazione  $f: A \rightarrow \mathbb{K}$  si dice *polinomiale* se per ogni scelta di  $p_0, \dots, p_n \in A$  fissati, si ha che  $f(t_0 p_0 + \dots + t_n p_n)$  è un polinomio nelle variabili  $t_0, \dots, t_n$ . Provare che:

1. Se  $f: A \rightarrow B$  è un'applicazione affine e  $g: B \rightarrow \mathbb{K}$  è polinomiale allora anche  $gf: A \rightarrow \mathbb{K}$  è polinomiale.
2. Le funzioni polinomiali sullo spazio affine  $\mathbb{A}_{\mathbb{K}}^n \cong \mathbb{K}^n$  sono tutte e sole quelle rappresentate da polinomi nelle coordinate di  $\mathbb{K}^n$ .

**2.12.** Sia  $V$  uno spazio vettoriale. Provare che il quoziente  $\text{GA}(V)/\text{T}(V)$  è isomorfo a  $\text{GL}(V)$ .

**2.13.** Dire se esiste un'affinità  $f: \mathbb{C}^2 \rightarrow \mathbb{C}^2$  tale che  $f(L) \neq L$  per ogni retta affine  $L \subset \mathbb{C}^2$ .

**2.3 Spazi proiettivi**

Sia  $\mathbb{K}$  un campo e  $V$  uno spazio vettoriale su  $\mathbb{K}$ ; definiamo il **proiettivizzato** di  $V$

$$\mathbb{P}(V) = (V - \{0\}) / \sim$$

come il quoziente di  $V - \{0\}$  per la relazione di equivalenza

$$v \sim w \quad \text{se e solo se} \quad v = \lambda w \quad \text{per qualche } \lambda \in \mathbb{K} - \{0\}.$$

L'insieme  $\mathbb{P}(V)$  è in bigezione naturale con l'insieme dei sottospazi vettoriali di dimensione 1 (rette per l'origine) di  $V$ . Notiamo, ad uso esclusivo degli esercizi complementari, che la definizione di  $\mathbb{P}(V)$  ha senso anche per spazi vettoriali sinistri su di un corpo non-commutativo. Dato un vettore  $v \in V - \{0\}$  si è soliti denotare con  $[v] \in \mathbb{P}(V)$  la classe di equivalenza corrispondente.

Chiameremo  $\mathbb{P}_{\mathbb{K}}^n = \mathbb{P}(\mathbb{K}^{n+1})$  **spazio proiettivo** di dimensione  $n$  sul campo  $\mathbb{K}$ . In assenza di ambiguità sul campo  $\mathbb{K}$  scriveremo più semplicemente  $\mathbb{P}^n$  in luogo di  $\mathbb{P}_{\mathbb{K}}^n$ . Diremo che un sottoinsieme  $M \subset V$  è un cono se  $0 \in M$  e se  $v \in M$  implica che  $\lambda v \in M$  per ogni  $\lambda \in \mathbb{K}$ . Se  $M \subset V$  è un cono definiamo il suo proiettivizzato come

$$\mathbb{P}(M) = \{[v] \mid v \in M - \{0\}\} \subset \mathbb{P}(V),$$

mentre, se  $S \subset \mathbb{P}(V)$  è un sottoinsieme definiamo il suo **cono affine** come

$$C(S) = \{v \in V - \{0\} \mid [v] \in S\} \cup \{0\}.$$

È immediato osservare che le applicazioni

$$\{\text{coni in } V\} \xrightarrow{\mathbb{P}} \{\text{sottoinsiemi di } \mathbb{P}(V)\} \xrightarrow{C} \{\text{coni in } V\}$$

sono bigettive ed una l'inversa dell'altra. Se  $W \subset V$  è un sottospazio lineare, chiameremo  $\mathbb{P}(W)$  **sottospazio proiettivo** di  $\mathbb{P}(V)$ . Si noti che ogni punto di uno spazio proiettivo è un sottospazio. Se  $W \subset V$  è un iperpiano diremo che  $\mathbb{P}(W)$  è un **iperpiano** di  $\mathbb{P}(V)$ . Poiché  $\mathbb{P}(\cap_i M_i) = \cap_i \mathbb{P}(M_i)$  per ogni famiglia di coni  $\{M_i\}$ , si ha in particolare che intersezione di sottospazi proiettivi è ancora un sottospazio proiettivo.

Se  $W_1, W_2 \subset V$  sono sottospazi scriveremo  $\langle \mathbb{P}(W_1), \mathbb{P}(W_2) \rangle = \mathbb{P}(W_1 + W_2)$ ; in altri termini, se  $H_1, H_2 \subset \mathbb{P}(V)$  sono sottospazi proiettivi, allora  $\langle H_1, H_2 \rangle$  è il più piccolo sottospazio proiettivo di  $\mathbb{P}(V)$  che li contiene. Se  $p, q \in \mathbb{P}(V)$  sono punti distinti, scriveremo talvolta  $\overline{pq}$  per denotare  $\langle p, q \rangle$ .

Per l'Esempio 2.2.4, dato un iperpiano  $H \subset \mathbb{P}(V)$ , il complementare  $E = \mathbb{P}(V) - H$  possiede una struttura naturale di spazio affine. Inoltre se  $v \in V - C(H)$  la composizione della traslazione  $t_v: C(H) \rightarrow V - H$ ,  $t_v(x) = x + v$ , e della proiezione  $\pi: V - \{0\} \rightarrow \mathbb{P}(V)$  induce un isomorfismo affine  $C(H) \rightarrow E$  (Esempio 2.2.12). In particolare  $E$  ha dimensione finita se e solo se  $V$  ha dimensione finita e vale  $\dim_{\mathbb{K}} E = \dim_{\mathbb{K}} V - 1$ . Se  $K \subset \mathbb{P}(V)$  è un sottospazio proiettivo, allora  $\pi$  induce un isomorfismo tra  $t_v(C(H)) \cap C(K)$  ed  $E \cap K$ ; in particolare  $E \cap K$  è un sottospazio affine di  $E$ .

Se lo spazio vettoriale  $V$  ha dimensione finita, definiamo la dimensione di  $\mathbb{P}(V)$  mediante la formula  $\dim \mathbb{P}(V) = \dim V - 1$  (in particolare  $\dim \emptyset = -1$ ). Spazi proiettivi di dimensione 1 e 2 si dicono rispettivamente **rette** e **piani** proiettivi. Punti contenuti in una medesima retta vengono detti **allineati**, punti (o rette) contenuti in un medesimo piano si dicono **complanari**, rette passanti per un medesimo punto si dicono **concorrenti**.

Due sottospazi proiettivi  $H, K \subset \mathbb{P}(V)$  si dicono **incidenti** se  $H \cap K \neq \emptyset$ , altrimenti si dicono **sghembi**; poiché  $C(\langle H, K \rangle) = C(H) + C(K)$  e  $\dim H = \dim C(H) - 1$  vale la **formula di Grassmann**

$$\dim(H \cap K) + \dim \langle H, K \rangle = \dim H + \dim K$$

e quindi  $H$  e  $K$  sono sghembi se e solo se  $\dim \langle H, K \rangle = \dim H + \dim K + 1$ .

**Definizione 2.3.1.** Diremo che  $s + 1$  punti  $p_0, \dots, p_s \in \mathbb{P}(V)$  sono **proiettivamente indipendenti** se il sottospazio  $\langle p_0, \dots, p_s \rangle$  da essi generato ha dimensione esattamente  $s$ .

Ad esempio, tre punti in  $\mathbb{P}^2$  sono proiettivamente indipendenti se e solo se non sono allineati. È fondamentale osservare che, se  $v_0, \dots, v_s \in V - \{0\}$ , allora i punti  $[v_0], \dots, [v_s]$  sono proiettivamente indipendenti se e solo se i vettori  $v_0, \dots, v_s$  sono linearmente indipendenti.

**Definizione 2.3.2.** Diremo che  $n + 2$  punti  $p_0, \dots, p_{n+1} \in \mathbb{P}(V)$  sono un **sistema di riferimento** se  $\dim V = n + 1$  e se per ogni indice  $i$  fissato, i punti  $p_j$ , per  $j \neq i$ , sono proiettivamente indipendenti.

Sono esempi di sistemi di riferimento:

- tre punti distinti di  $\mathbb{P}^1$ ;
- quattro punti di  $\mathbb{P}^2$ , tre dei quali non siano allineati;
- cinque punti di  $\mathbb{P}^3$ , quattro dei quali non siano complanari.

**Lemma 2.3.3.** Sia  $V$  uno spazio vettoriale di dimensione  $n + 1$ . Allora  $n + 2$  punti  $p_0, \dots, p_{n+1} \in \mathbb{P}(V)$  sono un sistema di riferimento se e solo se esiste una base  $e_0, \dots, e_n \in V$  tale che  $p_i = [e_i]$  per  $i = 0, \dots, n$  e  $p_{n+1} = [e_0 + e_1 + \dots + e_n]$ .

*Dimostrazione.* Se  $e_0, \dots, e_n \in V$  è una base, allora è facile osservare che i punti  $p_i = [e_i]$  per  $i = 0, \dots, n$  e  $p_{n+1} = [e_0 + e_1 + \dots + e_n]$  formano un sistema di riferimento

Sia viceversa  $p_0, \dots, p_{n+1}$  un sistema di riferimento e scegliamo vettori  $v_0, \dots, v_n \in V$  tali che  $p_i = [v_i]$  per ogni  $i = 0, \dots, n$ . Siccome  $p_0, \dots, p_n$  sono indipendenti, ne segue che  $v_0, \dots, v_n$  è una base di  $V$  e quindi esistono  $a_0, \dots, a_n \in \mathbb{K}$  tali che  $p_{n+1} = [e_{n+1}]$ , dove  $e_{n+1} = a_0 v_0 + \dots + a_n v_n$ . Se fosse  $a_i = 0$  per qualche indice  $i$ , allora i vettori  $e_{n+1}$  e  $v_j$ , per  $j \neq i$ , sarebbero linearmente dipendenti e quindi  $p_0, \dots, p_{n+1}$  non potrebbe essere un sistema di riferimento. Quindi  $a_i \neq 0$  per ogni  $i$  ed è sufficiente considerare la base  $e_i = a_i v_i$ .  $\square$

Per finire, definiamo lo spazio proiettivo duale  $\mathbb{P}(V)^\vee$  come l'insieme di tutti gli iperpiani di  $\mathbb{P}(V)$ . Per definizione gli iperpiani di  $\mathbb{P}(V)$  sono in corrispondenza biunivoca con gli iperpiani di  $V$  che a loro volta sono in bigezione con le classi di omotetia di funzionali lineari non nulli  $V \rightarrow \mathbb{K}$ . Esiste quindi una bigezione naturale  $\mathbb{P}(V)^\vee = \mathbb{P}(V^\vee)$ .

I sottospazi proiettivi di  $\mathbb{P}(V)^\vee$  sono anche detti **sistemi lineari di iperpiani**. Un sistema lineare di dimensione 1 è detto anche **fascio** (più raramente *pennello* o *schiera*) di iperpiani; un sistema lineare di dimensione 2 è detto **rete**.

Se  $H \subset \mathbb{P}(V)$  è un sottospazio proiettivo, denotiamo con  $H^\perp \subset \mathbb{P}(V)^\vee$  l'insieme degli iperpiani di  $\mathbb{P}(V)$  che contengono  $H$ . L'insieme  $H^\perp$  è il proiettivizzato dell'annullatore di  $C(H)$  ed è quindi un sistema lineare di iperpiani. Se  $V$  ha dimensione finita, allora esiste un isomorfismo naturale  $\mathbb{P}(V)^{\vee\vee} = \mathbb{P}(V)$  tramite il quale si ha  $H^{\perp\perp} = H$  per ogni sottospazio proiettivo  $H$ .

**Definizione 2.3.4.** *Un'applicazione  $\phi: \mathbb{P}(V) \rightarrow \mathbb{P}(W)$  si dice una **proiettività** se è indotta per passaggio al quoziente da una applicazione lineare iniettiva  $f: V \rightarrow W$ ; scriveremo in tal caso  $\phi = [f]$ . Un **isomorfismo proiettivo** è una proiettività bigettiva.*

È un facile esercizio di algebra lineare osservare che, date due applicazioni  $f, g: V \rightarrow W$  lineari iniettive, vale  $[f] = [g]$  se e solo se esiste  $a \in \mathbb{K} - \{0\}$  tale che  $f = ag$ .

Se  $V$  ha dimensione finita, allora ogni proiettività  $\mathbb{P}(V) \rightarrow \mathbb{P}(V)$  possiede una proiettività inversa: denotiamo con  $\text{Aut}(\mathbb{P}(V))$  il gruppo delle proiettività di  $\mathbb{P}(V)$  in sé.

Dunque, se  $\text{GL}(V)$  denota il gruppo degli automorfismi lineari di  $V$  in sé, esiste un omomorfismo surgettivo di gruppi

$$\text{GL}(V) \rightarrow \text{Aut}(\mathbb{P}(V))$$

che ha come nucleo i multipli dell'identità e quindi fattorizza ad un isomorfismo

$$\text{PGL}(V) := \frac{\text{GL}(V)}{\mathbb{K} * Id} \cong \text{Aut}(\mathbb{P}(V)).$$

Spesso si usa la notazione  $\text{PGL}(n, \mathbb{K}) = \text{PGL}(\mathbb{K}^n)$ .

Chiameremo **sistema di coordinate omogenee** su  $\mathbb{P}(V)$  un qualsiasi sistema di coordinate lineari su  $V$ . Se  $\mathbb{P}(V)$  ha dimensione finita  $n$ , la scelta di un sistema di coordinate omogenee definisce un isomorfismo proiettivo  $\mathbb{P}(V) = \mathbb{P}^n$  e quindi permette di rappresentare ogni punto  $p \in \mathbb{P}(V)$  nella forma  $p = [a_0, \dots, a_n]$ , con i numeri  $a_i \in \mathbb{K}$  non tutti nulli. Tale rappresentazione non è unica: infatti vale  $[a_0, \dots, a_n] = [\lambda a_0, \dots, \lambda a_n]$  se e solo se esiste  $\lambda \in \mathbb{K} - \{0\}$  tale che  $b_i = \lambda a_i$  per ogni  $i$ .

**Proposizione 2.3.5.** *Dati due sistemi di riferimento  $p_0, \dots, p_{n+1}$  e  $q_0, \dots, q_{n+1}$  di  $\mathbb{P}^n$ , esiste unica una proiettività  $\varphi: \mathbb{P}^n \rightarrow \mathbb{P}^n$  tale che  $\varphi(p_i) = q_i$  per ogni  $i$ .*

*Dimostrazione.* L'esistenza segue immediatamente dal Lemma 2.3.3, mentre per dimostrare l'unicità non è restrittivo supporre  $p_i = q_i$  per ogni  $i$ . Sia  $e_0, \dots, e_n$  una base di

$\mathbb{K}^{n+1}$  tale che  $p_i = [e_i]$  con  $e_{n+1} = \sum e_i$  e  $f \in \text{GL}(n+1)$  tale che  $[f]p_i = p_i$  per ogni  $i$ . Allora esistono costanti  $a_0, \dots, a_{n+1} \in \mathbb{K}$  tali che  $f(e_i) = a_i e_i$  per ogni  $i$ . Poiché  $e_0, \dots, e_n$  sono una base segue necessariamente che  $a_i = a_{n+1}$  per ogni  $i = 0, \dots, n$  e quindi  $f$  è un multiplo dell'identità.  $\square$

Si consideri adesso una decomposizione in somma diretta di sottospazi  $V = K \oplus W$  e sia  $\pi: V \rightarrow W$  la proiezione sul secondo fattore. Per passaggio al quoziente otteniamo una mappa  $[\pi]: \mathbb{P}(V) - \mathbb{P}(K) \rightarrow \mathbb{P}(W)$  detta **proiezione** su  $\mathbb{P}(W)$  di centro  $\mathbb{P}(K)$ . Da un punto di vista più geometrico, se  $p \in \mathbb{P}(V) - \mathbb{P}(K)$ , allora  $[\pi](p)$  è il punto di intersezione di  $\mathbb{P}(W) \subset \mathbb{P}(V)$  e di  $\langle \mathbb{P}(K), p \rangle$ . Lo spazio proiettivo  $\mathbb{P}(V/K)$  può essere pensato come l'insieme dei sottospazi proiettivi di  $\mathbb{P}(V)$  di dimensione uguale alla dimensione di  $K$  che contengono  $\mathbb{P}(K)$ ; in tale interpretazione l'isomorfismo naturale  $\mathbb{P}(W) \rightarrow \mathbb{P}(V/K)$  associa al punto  $p \in \mathbb{P}(W)$  il sottospazio  $\langle \mathbb{P}(K), p \rangle$ .

Sia  $x_0, \dots, x_n$  un sistema di coordinate omogenee su  $\mathbb{P}^n$  e scriviamo  $\mathbb{P}^n = \mathbb{A}_0^n \cup H_0$ , dove  $\mathbb{A}_0^n = \{[x_0, \dots, x_n] \mid x_0 \neq 0\}$  è la "parte affine" e  $H_0 = \{[x_0, \dots, x_n] \mid x_0 = 0\}$  è "l'iperpiano all'infinito". L'applicazione  $\mathbb{K}^n \rightarrow \mathbb{A}_0^n$ , data da  $(a_1, \dots, a_n) \mapsto [1, a_1, \dots, a_n]$ , è bigettiva e determina una struttura di spazio affine di dimensione  $n$  su  $\mathbb{A}_0^n$ . Non è difficile mostrare che il sottogruppo di  $\text{Aut}(\mathbb{P}^n)$ , formato dalle proiettività che preservano la decomposizione  $\mathbb{P}^n = \mathbb{A}_0^n \cup H_0$ , coincide con il gruppo delle trasformazioni affini di  $\mathbb{A}_0^n$ .

Per  $n = 1$  possiamo scrivere  $\mathbb{P}^1 = \mathbb{K} \cup \{\infty\}$ , dove  $\mathbb{K} = \{[t, 1] \mid t \in \mathbb{K}\}$  e  $\infty = [1, 0]$  (intuitivamente  $[1, 0]$  è il limite per  $t \rightarrow \infty$  di  $[1, 1/t] = [t, 1]$ ). Ogni proiettività  $\phi$  di  $\mathbb{P}^1$  in sé è rappresentata da una matrice invertibile

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{dove } ad - bc \neq 0,$$

e quindi  $\phi([x_0, x_1]) = [ax_0 + bx_1, cx_0 + dx_1]$  che, nella coordinata affine  $t$  diventa

$$\phi(t) = \frac{at + b}{ct + d}, \quad \text{con } ad - bc \neq 0.$$

## Esercizi

**2.14.** Sia  $V$  uno spazio vettoriale di dimensione  $n + 1$ . Provare che ogni sottospazio proiettivo di  $\mathbb{P}(V)$  di dimensione  $k$  è intersezione di  $n - k$  iperpiani proiettivi.

**2.15.** Se  $H, K$  sono sottospazi non vuoti di uno spazio proiettivo, provare che

$$\langle H, K \rangle = \bigcup_{p \in H, q \in K} \overline{pq}.$$

**2.16.** Dato un sottoinsieme  $W \subset \mathbb{P}(V)$ , denotiamo con  $\langle W \rangle$  il sottospazio generato da  $W$ , con  $\text{Sec}(W) = \cup \{\overline{pq} \mid p, q \in W\}$  e definiamo induttivamente  $\text{Sec}^n(W) = \text{Sec}(\text{Sec}^{n-1}(W))$ . Provare che  $\langle W \rangle = \cup_{n > 0} \text{Sec}^n(W)$  e che, se  $\langle W \rangle$  ha dimensione minore od uguale a  $n$ , allora  $\langle W \rangle = \text{Sec}^n(W)$ .

**2.17.** Siano  $H, K$  sottospazi di uno spazio proiettivo di dimensione  $n$ . Definiamo il **difetto incidente** di  $H$  e  $K$  tramite la formula

$$\text{DI}(H, K) = \begin{cases} \dim(H \cap K) + 1 & \text{se } \dim H + \dim K \leq n - 1, \\ n - \dim \langle H, K \rangle & \text{se } \dim H + \dim K \geq n - 1. \end{cases}$$

Provare che il difetto incidente è ben definito e che  $\text{DI}(H, K) = \text{DI}(H^\perp, K^\perp)$ .

**2.18.** Siano  $H, K$  sottospazi di uno spazio proiettivo di dimensione  $n$ . Definiamo il **difetto secante** di  $H$  e  $K$  come

$$DS(H, K) = \dim H + \dim K + 1 - \dim \langle H, K \rangle$$

Provare che, se  $\dim H + \dim K \leq n - 1$ , allora il difetto secante è uguale al difetto incidente.

**2.19.** Determinare le proiettività di  $\mathbb{P}_{\mathbb{C}}^1 = \mathbb{C} \cup \{\infty\}$  in sé che preservano i seguenti sottoinsiemi di  $\mathbb{C}$ :  $\mathbb{R} = \{x + iy \mid y = 0\}$ ,  $H = \{x + iy \mid y > 0\}$ ,  $\overline{H} = \{x + iy \mid y \geq 0\}$ ,  $\Delta = \{x + iy \mid x^2 + y^2 < 1\}$  e  $\overline{\Delta} = \{x + iy \mid x^2 + y^2 \leq 1\}$ .

Provare inoltre che la proiettività  $\phi(t) = \frac{t-i}{t+i}$  trasforma il semipiano  $H$  nel disco  $\Delta$ .

## 2.4 Il birapporto

Dati quattro punti distinti  $p_1, \dots, p_4 \in \mathbb{P}^1 = \mathbb{K} \cup \{\infty\}$ , esistono un'unica proiettività  $\phi \in \text{Aut}(\mathbb{P}^1)$  ed un elemento  $\lambda \in \mathbb{K} - \{0, 1\}$  tali che

$$\phi(p_1) = \lambda, \quad \phi(p_2) = 1, \quad \phi(p_3) = 0 \quad \text{e} \quad \phi(p_4) = \infty.$$

Il numero  $\lambda$  dipende solo dalla quaterna ordinata  $p_1, \dots, p_4$  ed è invariante per proiettività.

**Definizione 2.4.1.** La quantità  $\lambda = [p_1, p_2; p_3, p_4]$  si dice **birapporto**<sup>1</sup> della quaterna ordinata  $p_1, \dots, p_4$ .

Per costruzione, il birapporto può assumere qualsiasi valore in  $\mathbb{K} - \{0, 1\}$ . È inoltre conseguenza immediata della definizione che due quaterne ordinate di punti distinti di  $\mathbb{P}^1$  hanno lo stesso birapporto se e solo se esiste una proiettività che l'una nell'altra. Il nome birapporto è motivato dalla seguente proposizione.

**Proposizione 2.4.2.** Siano  $p_1 = [x_1, y_1], \dots, p_4 = [x_4, y_4]$  punti distinti di  $\mathbb{P}^1$ . Allora vale la formula

$$[p_1, p_2; p_3, p_4] = \frac{x_1 y_3 - x_3 y_1}{x_2 y_3 - x_3 y_2} : \frac{x_1 y_4 - x_4 y_1}{x_2 y_4 - x_4 y_2}$$

che in coordinate affini, ossia considerando  $p_i \in \mathbb{K} \cup \{\infty\}$ , diventa

$$[p_1, p_2; p_3, p_4] = \frac{p_1 - p_3}{p_2 - p_3} : \frac{p_1 - p_4}{p_2 - p_4}.$$

*Dimostrazione.* Esercizio. □

Il gruppo simmetrico su 4 elementi  $\Sigma_4$  agisce sulla quaterna  $p_1, \dots, p_4$  permutando gli indici; è naturale chiedersi come agisce  $\Sigma_4$  sul birapporto.

**Definizione 2.4.3.** Il **gruppo trirettangolo**<sup>2</sup>  $\Gamma_4$  è il sottogruppo di  $\Sigma_4$  formato dall'identità e dalle tre permutazioni<sup>3</sup> di ordine 2

$$\sigma_1 = (2, 1, 4, 3), \quad \sigma_2 = (3, 4, 1, 2), \quad \sigma_3 = (4, 3, 2, 1).$$

**Lemma 2.4.4.** Il birapporto di una quaterna di punti distinti di  $\mathbb{P}^1$  è invariante per l'azione del gruppo trirettangolo. Se  $[p_1, p_2; p_3, p_4] = \lambda$ , allora sotto l'azione del gruppo simmetrico il birapporto assume i valori

$$\lambda, \quad \frac{1}{\lambda}, \quad 1 - \lambda, \quad 1 - \frac{1}{\lambda}, \quad \frac{1}{1 - \lambda}, \quad \frac{\lambda}{\lambda - 1}.$$

<sup>1</sup> In inglese *cross ratio*; in francese *rapport anharmonique*.

<sup>2</sup> In inglese *Klein fourgroup*.

<sup>3</sup> Con la notazione  $\sigma = (a_1, \dots, a_n)$  si intende la permutazione tale che  $\sigma(i) = a_i$ .

*Dimostrazione.* Esercizio. □

In generale le sei espressioni elencate nel Lemma 2.4.4 forniscono sei birapporti distinti; si hanno tuttavia le seguenti eccezioni:

1. Caratteristica  $\neq 2$  e  $\lambda = -1, 2, \frac{1}{2}$ . In questo caso la quaterna è detta **armonica**.
2. Caratteristica  $\neq 3$ ,  $\xi^2 - \xi + 1 = 0$  e  $\lambda = \xi, \xi^{-1}$ . In questo caso la quaterna è detta **equianarmonica**<sup>4</sup>.

Notiamo che:

1. Dati  $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K} - \{0\}$  vale  $[0, \lambda_1; \lambda_2, \lambda_3] = [\infty, \lambda_1^{-1}; \lambda_2^{-1}, \lambda_3^{-1}] = \frac{1}{2}$  se e solo se  $\lambda_3$  è la media armonica di  $\lambda_1, \lambda_2$ .
2. In caratteristica 3 si hanno le uguaglianze  $\xi^2 - \xi + 1 = (1 + \xi)^2 = (1 - 2\xi)^2 = (2 - \xi)^2$ .
3. Su  $\mathbb{C}$ , rappresentato dal piano di Gauss, la quaterna formata dai vertici di un triangolo equilatero e dal suo baricentro è equianarmonica, mentre i vertici di un quadrato formano una quaterna armonica.

## Esercizi

**2.20.** Sia  $\mathbb{K}$  un campo infinito. Provare che per ogni  $n \geq 5$  esiste un insieme  $S \subset \mathbb{P}^1$  di  $n$  punti tale che, se  $\phi \in \text{Aut}(\mathbb{P}^1)$  e  $\phi(S) \subset S$ , allora  $\phi = Id$ .

**2.21.** Sia  $p \in \mathbb{P}^n$  e  $G \subset \text{Aut}(\mathbb{P}^n)$  il sottogruppo delle proiettività  $\phi$  tali che  $\phi(H) \subset H$  per ogni iperpiano  $H$  contenente  $p$ . Provare che  $G$  agisce transitivamente sull'insieme degli iperpiani di  $\mathbb{P}^n$  che non contengono  $p$ .

**2.22 (quadrilatero armonico).** Sia  $\mathbb{P}^2$  il piano proiettivo su di un campo di caratteristica  $\neq 2$ , siano  $a_1, a_2, a_3 \in \mathbb{P}^2$  punti non allineati e  $b_2 \in \overline{a_2 a_3}$ ,  $b_3 \in \overline{a_3 a_1}$  tali che  $b_i \neq a_j$  per ogni  $i, j$ . Indichiamo con  $c$  il punto di intersezione di  $\overline{a_1 b_2}$  e  $\overline{a_2 b_3}$ , con  $b_1$  il punto di intersezione di  $\overline{a_1 a_2}$  e  $\overline{a_3 c}$  e con  $d$  il punto di intersezione di  $\overline{a_1 a_2}$  e  $\overline{b_2 b_3}$  (vedi Figura 2.1). Provare che  $[a_1, a_2; b_1, d] = -1$ . (Sugg.: fissare un sistema di coordinate omogenee tali che  $a_1 = [0, 0, 1]$ ,  $a_2 = [2, 0, 1]$ ,  $d = [1, 0, 0]$ ,  $a_3 = [0, 1, 0]$  e provare che  $b_1 = [1, 0, 1]$ .)

## 2.5 Esercizi complementari

**2.23.** Siano  $a, b, c, d$  quattro punti distinti del piano affine reale  $\mathbb{A}_{\mathbb{R}}^2 = \mathbb{R}^2$ . Provare che esiste un'affinità  $f$  del piano affine in sé tale che  $f(a) = b$ ,  $f(b) = c$ ,  $f(c) = d$  e  $f(d) = a$  se e solo se  $a, b, c, d$  sono i vertici di un parallelogramma.

**2.24.** Dare una definizione “sensata” di parallelogramma su di un piano affine su di un campo arbitrario  $\mathbb{K}$  e generalizzare l'Esercizio 2.23 .

**2.25.** Siano dati  $a, b \in \mathbb{K}$ ; denotiamo con  $L_1 \subset \mathbb{A}^2$  la retta passante per i punti di coordinate  $(a, 0)$ ,  $(1, b)$  e con  $L_2 \subset \mathbb{A}^2$  la retta passante per i punti di coordinate  $(a, 1)$ ,  $(0, b)$ .

Provare che il punto di intersezione di  $L_1$  ed  $L_2$  appartiene alla diagonale  $x = y$ . (Sugg.: per semplificare i conti scrivere le equazioni delle due rette nella forma  $\alpha x + \beta y = ab$  per opportuni  $\alpha, \beta \in \mathbb{K}$ .)

<sup>4</sup> Tale definizione si trova a pagina 22 di [Cre1862]: Luigi Cremona (Pavia 1830-Roma 1903) è stato il fondatore della scuola italiana di Geometria Algebrica.



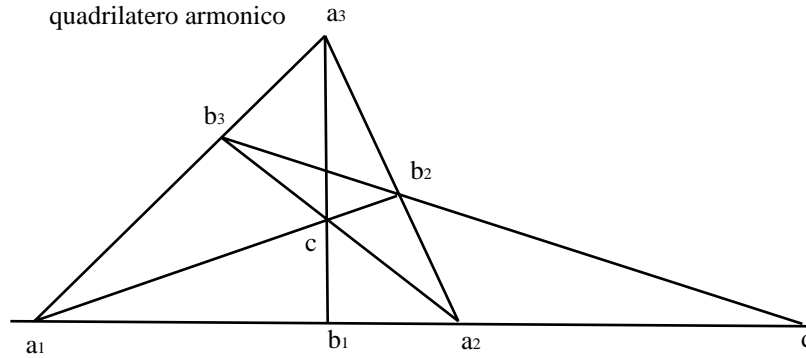


Figura 2.1. (Esercizio 2.22).

**2.26 (Rapporto semplice).** Siano  $a, b, c \in \mathbb{A}^n$  punti allineati tali che  $b \neq c$ ; esistono quindi, e sono unici, un vettore  $v \in \mathbb{K}^n$  ed uno scalare  $t \in \mathbb{K}$  tali che  $b = c + v$  e  $a = c + tv$ . La quantità  $t = (abc) = \frac{a-c}{b-c}$  viene detta **rapporto semplice** della terna ordinata  $a, b, c$ . Provare che se  $f: \mathbb{A}^n \rightarrow \mathbb{A}^m$  è una applicazione affine tale che  $f(b) \neq f(c)$ , allora vale  $(f(a)f(b)f(c)) = (abc)$ .

**2.27.** Sia  $\mathbb{K}$  un campo con almeno tre elementi. Provare che un'applicazione bigettiva  $f: \mathbb{K}^n \rightarrow \mathbb{K}^n$  è un'affinità se e soltanto se trasforma rette affini in rette affini (cioè se conserva gli allineamenti) e preserva i rapporti semplici.

**2.28 (Spazi affini modellati).** Sia  $V$  uno spazio vettoriale su di un campo  $\mathbb{K}$ . Uno **spazio affine modellato** su  $V$  è una terna  $(A, V, \rightarrow)$ , dove  $A$  è un insieme e  $A \times A \rightarrow V$  è un'applicazione che soddisfa gli assiomi:

1. Per ogni  $p \in A$  vale  $\overrightarrow{pp} = 0$ .
2. (*Relazione di Chasles*) Per ogni  $p, q, r \in A$  vale  $\overrightarrow{pq} + \overrightarrow{qr} + \overrightarrow{rp} = 0$ .
3. Per ogni  $p \in A$  e per ogni  $v \in V$  esiste unico un punto  $q \in A$  tale che  $\overrightarrow{pq} = v$ .

L'unico punto  $q$  descritto al punto 3 si dice traslato di  $p$  mediante  $v$  e si indica con  $q = v + p$ .

Definiamo una struttura di prespazio affine ponendo, per  $p_0, \dots, p_n \in A$  e  $(t_0, \dots, t_n) \in \Delta^n$

$$t_0 p_0 + \dots + t_n p_n = \left( \sum_i t_i \overrightarrow{p_0 p_i} \right) + p_0.$$

Mostrare che tale struttura definisce uno spazio affine.

**2.29.** Provare che se  $A$  è uno spazio affine modellato su di uno spazio vettoriale  $V$ , allora  $p_0, \dots, p_n$  sono linearmente indipendenti in  $A$  se e solo se gli  $n$  vettori  $\overrightarrow{p_0 p_i} \in V$  sono linearmente indipendenti.

**2.30.** Siano  $(A, V, \rightarrow)$  e  $(B, W, \rightarrow)$  spazi affini modellati. Mostrare che un'applicazione  $f: A \rightarrow B$  è affine se e solo se esiste un'applicazione lineare  $g: V \rightarrow W$  tale che  $\overrightarrow{f(p)f(q)} = g(\overrightarrow{pq})$  per ogni  $p, q \in A$ .

**2.31.** Sia  $A$  uno spazio affine: per ogni coppia di punti  $p, q \in A$  e per ogni  $a \in \mathbb{K}$  definiamo l'applicazione

$$t_{pq}^a: A \rightarrow A, \quad t_{pq}^a(x) = -ap + aq + x.$$

Dimostrare che, nelle notazioni precedenti, per ogni  $p, q \in A$ :

1.  $t_{\overline{pq}}^0 = Id$ .
2. Se  $r = (1 - a)p + aq$ , allora  $t_{\overline{pq}}^a$  è la traslazione  $t_{\overline{pr}}$ .
3.  $t_{\overline{qr}}^a \circ t_{\overline{pq}}^a = t_{\overline{pq}}^a \circ t_{\overline{qr}}^a = t_{\overline{pr}}^a$  per ogni  $a \in \mathbb{K}$  e  $p, q, r \in A$ .

**2.32.** Sia  $A \neq \emptyset$  uno spazio affine su  $\mathbb{K}$ . Mostrare che esiste una struttura di spazio vettoriale sul gruppo abeliano delle traslazioni  $T(A)$  tale che l'azione naturale  $T(A) \times A \rightarrow A$  rappresenta  $A$  come spazio affine modellato su  $T(A)$ . (Sugg.: definire il prodotto per scalare mediante la formula (vedi Esercizio 2.31)

$$at_{\overline{pq}} = t_{\overline{pq}}^a = t_{\overline{pr}}, \text{ dove } r = (1 - a)p + aq.$$

**2.33.** Dimostrare che un'applicazione  $f: A \rightarrow B$  tra spazi affini non vuoti è affine se e solo se esiste un'applicazione lineare  $g: T(A) \rightarrow T(B)$  tale che  $g(t_{\overline{pq}}) = t_{\overline{f(p)f(q)}}$  per ogni  $p, q \in A$ .

**2.34.** Sia  $V$  uno spazio vettoriale su di un campo con almeno tre elementi. Provare che un sottoinsieme  $K \subset \mathbb{P}(V)$  è un sottospazio proiettivo se e solo se  $K - H$  è un sottospazio affine di  $\mathbb{P}(V) - H$  per ogni iperpiano  $H \subset \mathbb{P}(V)$ .

**2.35.** Siano date  $n$  rette proiettive  $L_1, \dots, L_n \subset \mathbb{P}^n = \mathbb{A}_0^n \cup H_0$  e si assuma che nessuna delle rette  $L_i$  sia contenuta nell'iperpiano  $H_0 = \{x_0 = 0\}$ . Allora per ogni  $i = 1, \dots, n$  esiste una rappresentazione parametrica della retta  $L_i \cap \mathbb{A}_0^n$  che possiamo scrivere nella forma

$$L_i = \{ [1, a_{i1}t + b_{i1}, \dots, a_{in}t + b_{in}] \mid t \in \mathbb{K} \}.$$

Provare che gli  $n$  punti di intersezione delle rette  $L_1, \dots, L_n$  con l'iperpiano  $H_0$  sono proiettivamente indipendenti se e solo se  $\det(a_{ij}) \neq 0$ .

**2.36 (\*)**. Sia  $\mathbb{K}$  un campo algebricamente chiuso di caratteristica  $\neq 2$ , e siano date quattro rette  $L_1, \dots, L_4 \subset \mathbb{P}^3$ . Provare che esiste almeno una retta in  $\mathbb{P}^3$  che le interseca tutte e quattro. (Sugg.: se esiste un punto  $o$  appartenente all'intersezione di due rette distinte  $L_i, L_j$  considerare la proiezione di centro  $o$ . Altrimenti si prendano coordinate omogenee tali che  $L_4 = \{x_0 = x_1 = 0\}$ ,  $L_1 = \{x_2 = x_3 = 0\}$  e si consideri l'intersezione delle rette con i piani del fascio  $F_t = \{x_1 = tx_0\}$ , per  $t \in \mathbb{K}$ . Ad un certo punto servirà il risultato dell'Esercizio 2.35.)

**2.37.** Se  $\phi: \mathbb{P}^n - K \rightarrow H$  è una proiezione e  $L \subset \mathbb{P}^n$  è un sottospazio proiettivo tale che  $K \cap L = \emptyset$ , allora la restrizione  $\phi: L \rightarrow H$  è una proiettività tale che  $\phi(p) = p$  per ogni  $p \in L \cap H$ . Viceversa, si dimostri che ogni proiettività  $\psi: L \rightarrow H$  tale che  $\psi(p) = p$  per ogni  $p \in L \cap H$  è ottenuta come restrizione di una opportuna proiezione (di centro non necessariamente  $K$ ). Discutere inoltre se il risultato continua ad essere vero sugli spazi proiettivi definiti su corpi noncommutativi (per questo si consiglia di analizzare il caso  $H, L$  rette in  $\mathbb{P}^2$ ).

**2.38.** Siano  $L, H \subset \mathbb{P}^2$  rette distinte,  $p = L \cap H$  e  $\phi: L \rightarrow H$  una proiettività tale che  $\phi(p) \neq p$ . Provare che  $\phi$  è composizione di due proiezioni. (Sugg.: considerare la retta passante per i punti  $\phi(p), \phi^{-1}(p)$ .)

**2.39 (Prospettive)**. Sia  $V$  spazio vettoriale di dimensione finita  $n$  e  $f: V \rightarrow V$  un'applicazione lineare invertibile. La proiettività indotta  $[f]: \mathbb{P}(V) \rightarrow \mathbb{P}(V)$  si dice una **prospettiva** se esiste  $\lambda \in \mathbb{K}$  tale che  $\text{rank}(f - \lambda I) \leq 1$ . Provare che le seguenti condizioni sono equivalenti:

1.  $[f]$  è una prospettiva.
2.  $[f^t]: \mathbb{P}(V^\vee) \rightarrow \mathbb{P}(V^\vee)$  è una prospettiva.

3. Esiste un iperpiano  $H \subset \mathbb{P}(V)$  tale che  $[f]q = q$  per ogni  $q \in H$ .
4. Esiste  $p \in \mathbb{P}(V)$  tale che  $[f]q \in \overline{pq}$  per ogni  $q \in \mathbb{P}(V) - \{p\}$ .
5. Esiste un sistema di riferimento  $p_0, \dots, p_n \in \mathbb{P}(V)$  tale che  $[f]p_0 = p_0$  e  $[f]p_i \in \overline{p_0 p_i}$  per ogni  $i = 1, \dots, n$ .

**2.40 (Centro di prospettiva).** Sia  $[f]: \mathbb{P}(V) \rightarrow \mathbb{P}(V)$  una prospettiva diversa dall'identità. Provare che esiste un unico punto  $p \in \mathbb{P}(V)$  tale che  $[f]q \in \overline{pq}$  per ogni  $q \in \mathbb{P}(V) - \{p\}$ . Un tale punto  $p$  viene chiamato **centro di prospettiva**. Anticamente una prospettiva veniva chiamata *omologia* se  $p \notin H$ ; *elazione* od *omologia speciale* se  $p \in H$ .

**2.41.** Provare che, per una proiettività  $\phi: \mathbb{P}^n \rightarrow \mathbb{P}^n$ , le seguenti condizioni sono equivalenti:

1. Esiste un sottospazio  $H \subset \mathbb{P}^n$  di codimensione  $r$  tale che  $\phi(p) = p$  per ogni  $p \in H$ .
2. Esiste un sottospazio  $L$  di dimensione  $r - 1$  tale che  $\phi(q) \in \langle q, L \rangle$  per ogni  $q \in \mathbb{P}^n$ .
3.  $\phi$  è composizione di  $r$  prospettive.

**2.42.** Utilizzare l'Esercizio 2.39 (nel caso  $n = 3$ ) per dimostrare il teorema di Desargues (1648), vedi Figura 2.2.

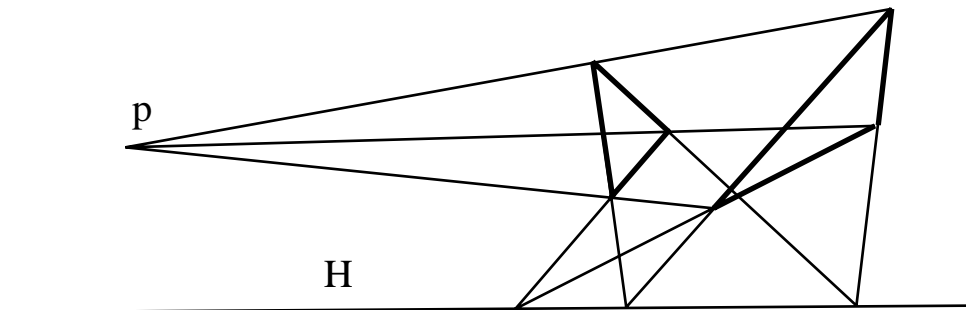


Figura 2.2. Il teorema di Desargues

**2.43.** Discutere la validità della Proposizione 2.3.5 su corpi noncommutativi. In particolare si determini il sottogruppo di  $\text{PGL}(2)$  che lascia fissi tre punti distinti di  $\mathbb{P}^1$ .

**2.44 (Teorema di Pappo, III sec. d.C.).** Siano  $p_1, p_2, p_3 \in \mathbb{P}^2$  e  $q_1, q_2, q_3 \in \mathbb{P}^2$  due terne di punti allineati, tra loro distinti ed appartenenti a rette distinte. Provare che i punti

$$r = \overline{p_1 q_2} \cap \overline{p_2 q_1}, \quad s = \overline{p_2 q_3} \cap \overline{p_3 q_2}, \quad t = \overline{p_3 q_1} \cap \overline{p_1 q_3}$$

sono allineati. (Sugg.: scegliere un sistema di coordinate omogenee tali che  $p_1 = [0, 1, 0]$ ,  $q_1 = [0, 0, 1]$ ,  $p_2 = [1, 1, 0]$ ,  $q_2 = [1, 0, 1]$ , prendere  $\overline{p_1 q_1}$  come retta all'infinito ed applicare l'Esercizio 2.25.)

**2.45.** Sia  $\lambda \in \mathbb{K} - \{0, 1\}$  fissato,  $L \subset \mathbb{P}^2$  una retta e  $\pi: \mathbb{P}^2 - \{o\} \rightarrow L$  la proiezione di centro  $o \notin L$ .

Definiamo un'applicazione  $\phi: \mathbb{P}^2 \rightarrow \mathbb{P}^2$  nel modo seguente:  $\phi(o) = o$  e  $\phi(p) = p$  per ogni  $p \in L$ ; se  $p \neq o$  e  $p \notin L$ , allora si pone  $r = \pi(p)$  e  $\phi(p) = q$ , dove  $q \in \overline{op}$  è l'unico punto tale che  $[o, r; p, q] = \lambda$ . Provare che  $\phi$  è una proiettività. Provare inoltre che ogni omologia (Esercizio 2.40) del piano ha questa forma e che  $\phi$  è una involuzione (cioè  $\phi^2 = Id$ ) se e solo se  $\lambda = -1$ .

**2.46.** Nelle notazioni dell'Esercizio 2.22, sia  $e = \overline{a_3 b_1} \cap \overline{b_2 b_3}$ ; provare che  $[a_1, a_2; b_1, d] = [b_2, b_3; e, d] = [a_2, a_1; b_1, d]$  e dedurne che  $[a_1, a_2; b_1, d]^2 = 1$ .

**2.47 (Rapporti plurisezionali).** Sia  $n \geq 2$  un intero e  $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{P}^1$  tali che  $b_i \neq a_{i+1}$ ; si definisce il rapporto  $n$ -sezionale come

$$[a_1, a_2, \dots, a_n; b_1, b_2, \dots, b_n] = \prod_{i=1}^n (a_i a_{i+1} b_i) = \prod_{i=1}^n \frac{a_i^0 b_i^1 - a_i^1 b_i^0}{a_{i+1}^0 b_i^1 - a_{i+1}^1 b_i^0}$$

dove si è posto  $a_{n+1} = a_1$  e  $b_{n+1} = b_1$ , mentre  $a_i = [a_i^0, a_i^1]$  e  $b_i = [a_i^0, a_i^1]$  sono le rappresentazioni in coordinate omogenee. Provare che il rapporto  $n$ -sezionale è invariante per proiettività e che se  $b_n = b_{n-1}$ , allora  $[a_1, a_2, \dots, a_n; b_1, b_2, \dots, b_n] = [a_1, a_2, \dots, a_{n-1}; b_1, b_2, \dots, b_{n-1}]$ .

Se invece  $a_1, \dots, a_n \in \mathbb{P}^2$  e  $b_i \in \overline{a_i a_{i+1}}$ , con  $b_i \neq a_{i+1}$  per ogni  $i = 1, \dots, n$ , allora, fissato un punto  $p \in \mathbb{P}^2$  non appartenente all'unione delle rette  $\overline{a_i a_{i+1}}$  si definisce  $[a_1, a_2, \dots, a_n; b_1, b_2, \dots, b_n]$  come il rapporto plurisezionale delle rispettive immagini in  $\mathbb{P}^1$  tramite la proiezione di centro  $p$ . Provare che si tratta di una buona definizione e che quindi il rapporto plurisezionale è invariante per proiettività. (Sugg.: siano  $p, q$  due centri di proiezione e si prendano coordinate affini tali che  $\overline{pq}$  sia la retta all'infinito. Non è restrittivo assumere che  $\overline{pq}$  non contenga alcun punto  $a_i$ ; si scriva quindi  $[a_1, a_2, \dots, a_n; b_1, b_2, \dots, b_n]$  come un prodotto di rapporti semplici.)

**2.48 (Teorema di Menelao, I sec. d.C.).** Siano  $a_1, a_2, a_3 \in \mathbb{P}^2$  i vertici di un triangolo e  $b_i \in \overline{a_i a_{i+1}}$  punti distinti dai vertici. Provare che  $b_1, b_2, b_3$  sono allineati se e solo se  $[a_1, a_2, a_3; b_1, b_2, b_3] = 1$  (Sugg.: considerare  $b_1 b_2$  come retta all'infinito).

**2.49 (Teorema di Ceva, 1678).** Siano  $a_1, a_2, a_3 \in \mathbb{P}^2$  non allineati e  $b_i \in \overline{a_i a_{i+1}}$  punti distinti dai vertici. Provare che le rette  $L_i = \overline{a_i b_{i+1}}$  sono concorrenti se e solo se  $[a_1, a_2, a_3; b_1, b_2, b_3] = -1$  (Sugg.: sia  $p$  un punto generico contenuto nella retta  $\overline{b_2 b_3}$  e si consideri la proiezione di centro  $p$  sulla retta  $\overline{a_1 a_2}$ ).

**2.50.** Sia  $\mathbb{K}$  algebricamente chiuso e  $\phi \in \text{Aut}(\mathbb{P}^1)$  una proiettività di ordine finito e non divisibile per la caratteristica di  $\mathbb{K}$ . Provare che  $\phi$  ha esattamente due punti fissi.

**2.51.** (caratteristica  $\neq 2$ ) Una quaterna ordinata  $p_1, \dots, p_4$  di punti distinti di  $\mathbb{P}^1$  definisce un omomorfismo iniettivo di gruppi  $h: \Gamma_4 \rightarrow \text{PGL}(2, \mathbb{K}) = \text{Aut}(\mathbb{P}^1)$  caratterizzato dalla proprietà che per ogni permutazione  $\sigma \in \Gamma_4$  vale  $h(\sigma)(p_i) = p_{\sigma(i)}$ . Provare che non esiste alcun sollevamento di  $h$  ad un omomorfismo  $\Gamma_4 \rightarrow \text{GL}(2, \mathbb{K})$ . (Sugg.: non è restrittivo assumere  $\mathbb{K}$  algebricamente chiuso; si prenda una coordinata affine tale che la quaterna sia  $1, -1, a, -a$  con  $a \neq \pm 1$ .)

**2.52.** Trovare un elemento di ordine 2 di  $\text{PGL}(2, \mathbb{Q})$  che non si rappresenta con elementi di ordine finito di  $\text{GL}(2, \mathbb{Q})$ .

**2.53.** Sia  $\mathbb{K}^* = \mathbb{K} - \{0\}$  il gruppo moltiplicativo,  $n \geq 2$  un intero e si assuma che esista un sottogruppo finito  $H \subset \mathbb{K}^*$  di ordine  $d$  tale che  $\mathbb{K}^*$  è generato da  $H$  e dalle potenze  $n$ -esime di elementi di  $\mathbb{K}^*$ . Sia inoltre  $h$  il massimo divisore di  $n$  non divisibile dalla caratteristica di  $\mathbb{K}$ . Dimostrare che per ogni sottogruppo finito  $\Gamma \subset \text{PGL}(n, \mathbb{K})$  di ordine  $m$  esiste un sottogruppo finito  $\Gamma' \subset \text{GL}(n, \mathbb{K})$  di ordine  $\leq hdm$  che si surietta su  $\Gamma$  tramite la proiezione naturale  $\text{GL}(n, \mathbb{K}) \rightarrow \text{PGL}(n, \mathbb{K})$ .

**2.54.** (caratteristica  $\neq 2, 3$ ) Sia  $p_1, \dots, p_4$  una quaterna di punti distinti di  $\mathbb{P}^1$ . Provare che:

- La quaterna è armonica se e solo se il birapporto  $[p_1, p_2; p_3, p_4]$  è invariante per l'azione di un sottogruppo di ordine 8 di  $\Sigma_4$ . Dedurre che il gruppo simmetrico  $\Sigma_4$  contiene esattamente tre sottogruppi di ordine 8 (2-Sylow) tra loro coniugati ed isomorfi al gruppo diedrale  $D_4$ .
- La quaterna è equianarmonica se e solo se il birapporto  $[p_1, p_2; p_3, p_4]$  è invariante per l'azione del gruppo alterno  $A_4$ .

**2.55.** Si consideri l'applicazione  $v_n: \mathbb{P}^1 \rightarrow \mathbb{P}^n$ , definita in coordinate omogenee da

$$v_n([x_0, x_1]) = [x_0^n, x_0^{n-1}x_1, \dots, x_0x_1^{n-1}, x_1^n].$$

Provare che, se  $p_0, \dots, p_{n+1}$  sono  $n+2$  punti distinti di  $\mathbb{P}^1$ , allora  $v_n(p_0), \dots, v_n(p_{n+1})$  è un sistema di riferimento su  $\mathbb{P}^n$ . L'applicazione  $v_n$  è detta **applicazione di Veronese**.

**2.56.** Si consideri il piano  $\mathbb{R}^2$  con la metrica euclidea usuale, per ogni  $p \in \mathbb{R}^2$  sia  $F_p \cong \mathbb{P}_{\mathbb{R}}^1$  il fascio di rette passanti per il punto  $p$ . Verificare che l'applicazione  $F_p \rightarrow F_p$  che manda ogni retta nella sua perpendicolare è una proiezione. Tale proiezione è chiamata **involuzione degli angoli retti**.

**2.57 (Luogo polare, [Cre1862, Art.III]).** Sia  $o \in \mathbb{P}^1$  e  $G$  un insieme di  $n$  punti distinti  $p_1, \dots, p_n$  di  $\mathbb{P}^1$ , con  $n \geq 2$ . Si definisce il luogo polare di  $o$  rispetto a  $G$  come l'insieme dei punti  $q \in \mathbb{P}^1$  tali che

$$\sum_{i=1}^n [o, q; p_i, \hat{o}] = 0$$

per ogni  $\hat{o} \neq o$ . Provare che se  $o = \{\infty\}$  e  $p_1, \dots, p_n \in \mathbb{K}$  sono le radici di un polinomio monico  $f$  di grado  $n$ , allora il luogo polare di  $\{\infty\}$  rispetto a  $p_1, \dots, p_n$  è l'insieme delle radici della derivata  $f'$  di  $f$ .

**2.58 (\*)**. Con l'utilizzo della sola riga dividere un rettangolo del piano euclideo in  $n$  parti uguali, per ogni  $n \geq 2$ . (Sugg.: quadrilatero armonico.)

**2.59.** Siano  $L, H, T$  tre rette distinte di  $\mathbb{P}^2$  concorrenti in un punto  $p$  e siano  $q, r \in T$  punti distinti da  $p$ . Si consideri le proiezioni  $\phi: L \rightarrow H$  e  $\psi: H \rightarrow L$  ottenute per proiezione di centro  $q$  ed  $r$  rispettivamente. Detta  $\eta: L \rightarrow L$  la composizione di  $\phi$  e  $\psi$  calcolare il valore del birapporto  $[p, s; \eta(s), \eta^2(s)]$  al variare di  $s$  in  $L - \{p\}$ .



## Forme binarie

Uno dei settori trainanti della geometria algebrica nel periodo 1840-1890 è stato senza dubbio la teoria algebrica degli invarianti. In questo capitolo ripercorriamo alcune delle principali conquiste di quel periodo, culminate con i teoremi della base e degli zeri di Hilbert, studiando gli invarianti di forme binarie. Riprendendo la terminologia usata all'epoca, useremo il termine forma (binaria, ternaria ecc.) per indicare un polinomio omogeneo (in due, tre ecc.) variabili.

Supporremo per semplicità  $\mathbb{K}$  campo di caratteristica 0 o sufficientemente alta (rispetto ai gradi dei polinomi considerati).

### 3.1 Risoluzione per radicali dell'equazione di terzo grado

In questo paragrafo  $\mathbb{K}$  denoterà un campo algebricamente chiuso di caratteristica  $\neq 2, 3$ .

Sia  $f(x) = x^3 + 3a_1x^2 + 3a_2x + a_3$  un polinomio di grado 3 a coefficienti in  $\mathbb{K}$ . Essendo  $\mathbb{K}$  algebricamente chiuso si può scrivere

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3), \quad \alpha_1, \alpha_2, \alpha_3 \in \mathbb{K}.$$

A meno di sostituire  $x$  con  $x - a_1$  si può assumere  $a_1 = 0$  e quindi

$$f(x) = x^3 + 3a_2x + a_3.$$

Esistono tre casi in cui l'equazione  $f(x) = 0$  è particolarmente semplice da risolvere.

- Se  $a_2 = 0$ , allora  $x = \sqrt[3]{-a_3}$ .
- Se  $a_3 = 0$ , allora  $x = 0, \sqrt{-3a_2}$ .
- Se  $f(x)$  e  $f'(x) = 3(x^2 + a_2)$  hanno un fattore comune, allora l'equazione si riduce ad una equazione di secondo grado.

Supponiamo di non essere in alcuno dei tre casi precedenti, in particolare  $f(x)$  avrà tre radici distinte.

È buona regola, di fronte ad equazioni di qualsiasi tipo e grado, cercare le simmetrie del sistema, cioè i gruppi di trasformazioni che lasciano invariate (nella sostanza) le equazioni date. Su  $\mathbb{K}$  è naturale considerare i seguenti gruppi:

- 1) Trasformazioni lineari: sono le trasformazioni del tipo  $x \mapsto \lambda x$ ; si vede subito che  $f(x)$  è invariante per una tale trasformazione se e solo se  $a_2 = 0, \lambda^3 = 1$  oppure  $a_3 = 0, \lambda^2 = 1$  oppure  $a_2 = a_3 = 0$ .
- 2) Trasformazioni affini: sono le trasformazioni del tipo  $x \mapsto \lambda x + \eta$ ; si vede subito che  $f(x)$  può essere invariante solo se  $\eta = 0$ , cioè solo se la trasformazione è lineare.
- 3) Trasformazioni proiettive: sono le trasformazioni del tipo

$$x \mapsto \frac{ax+b}{cx+d}, \quad ad \neq bc.$$

Una tale trasformazione agisce sul proiettivizzato dello spazio vettoriale dei polinomi di grado  $\leq 3$  e trasforma la classe  $[g(x)]$  in

$$\left[ g\left(\frac{ax+b}{cx+d}\right)(cx+d)^3 \right].$$

Siccome le tre radici  $\alpha_1, \alpha_2$  e  $\alpha_3$  di  $f(x)$  sono distinte, esiste unica una proiettività  $\psi$  tale che  $\psi(\alpha_1) = \alpha_2$ ,  $\psi(\alpha_2) = \alpha_3$  e  $\psi(\alpha_3) = \alpha_1$ . Evidentemente  $\psi^3 = Id$  e  $[f(x)]$  è un punto fisso per l'azione di  $\psi$  sul proiettivizzato dello spazio dei polinomi grado  $\leq 3$ . Per le ipotesi fatte su  $f(x)$  sappiamo che  $\psi$  non è una affinità, cioè il punto all'infinito non è un punto fisso di  $\psi$ . Siano  $n, m \in \mathbb{K}$  i punti fissi di  $\psi$ . Siccome  $n \neq m$  esiste un polinomio  $g(y)$  di grado al più tre tale che

$$f(x) = g\left(\frac{x-n}{x-m}\right)(x-m)^3.$$

Geometricamente, il polinomio  $g(y)$  è ottenuto da  $f(x)$  mediante il cambio di coordinate omogenee che trasforma  $n$  in  $0$  e  $m$  in  $\infty$ . Ne segue che  $[g(y)]$  è un punto fisso per l'azione della proiettività di ordine tre che ha come punti fissi  $\{0\}$  e  $\{\infty\}$ : tale proiettività è data da  $y \mapsto \xi y$ , dove  $\xi$  è una radice primitiva cubica di  $1$ . Dunque  $g(y)$  deve essere necessariamente del tipo  $ay^3 + b$ . Abbiamo quindi dimostrato la seguente proposizione.

**Proposizione 3.1.1.** *Sia  $f(x)$  un polinomio di terzo grado con radici distinte e siano  $n, m$  i punti fissi della proiettività che induce una permutazione ciclica delle radici di  $f(x)$ . Allora esistono due costanti  $a, b$  tali che  $f(x) = a(x-n)^3 + b(x-m)^3$ .*

Da tale risultato è facile ricavare la formula risolutiva dell'equazione di terzo grado: abbiamo infatti

$$x^3 + 3a_2x + a_3 = t(x-n)^3 + (1-t)(x-m)^3$$

che equivale al sistema

$$\begin{cases} tn + (1-t)m = 0 \\ tn^2 + (1-t)m^2 = a_2 \\ tn^3 + (1-t)m^3 = -a_3 \end{cases}$$

Dato che  $n - m \neq 0$ , possiamo ricavare il valore di  $t$  dalla prima equazione e sostituirlo nelle altre due; semplificando si ottiene

$$\begin{cases} \frac{m}{m-n} = t \\ nm = -a_2 \\ \frac{mn^3 - nm^3}{m-n} = -a_3. \end{cases}$$

Mettendo nella terza equazione  $-a_2$  al posto di  $nm$  e semplificando si ottiene

$$\begin{cases} \frac{m}{m-n} = t \\ nm = -a_2 \\ n+m = -\frac{a_3}{a_2}. \end{cases}$$

Si tratta di un sistema di secondo grado simmetrico dal quale si può ricavare  $n, m$  e  $t$ . Le radici di  $f$  sono quindi le radici dell'equazione



$$\left(\frac{x-n}{x-m}\right)^3 = \frac{t-1}{t} = \frac{n}{m}$$

che si calcolano esattamente e, fissate due radici cubiche  $\sqrt[3]{m}$ ,  $\sqrt[3]{n}$  di  $m$  e  $n$  rispettivamente, sono date dalla formula:

$$\alpha_i = \frac{m\sqrt[3]{n} - n\xi^i\sqrt[3]{m}}{\sqrt[3]{n} - \xi^i\sqrt[3]{m}}, \quad i = 0, 1, 2, \quad (3.1)$$

dove  $\xi$  è una radice primitiva cubica di 1.

Nel Capitolo 5 useremo uno stratagemma per ridurre l'equazione generale di quarto grado ad una di terzo grado (equazione risolvente) ed a due equazioni di secondo grado. È ben noto che per polinomi di grado  $\geq 5$  non esiste la risolubilità per radicali (cfr. [Her1982]).

Un problema intermedio (rispetto al problema della risolubilità delle equazioni) è il seguente: *dati due polinomi  $f(x), g(x)$  di grado  $n$  a radici distinte, esiste una proiettività  $\psi$  che trasforma le radici di  $f$  nelle radici di  $g$ ?*

Tale problema ha senso per ogni  $n \geq 4$  ed è perfettamente risolubile, anche se in caso di risposta positiva non esiste alcuna formula generale in grado di determinare  $\psi$ . Di tale problema inizieremo ad occuparci a partire dalla prossima sezione.

### Esercizi

**3.1.** Dimostrare che, se  $f$  possiede una radice multipla, allora l'equazione 3.1 degenera alla forma  $\alpha_i = \frac{0}{0}$ .

**3.2.** Sia  $f$  un polinomio di grado 4 senza radici multiple. Provare che  $f$  è autovettore per almeno tre proiettività distinte  $\psi_1, \psi_2, \psi_3$  tali che  $\psi_i^2 = Id$ .

**3.3.** Sia  $\mu_n \subset \mathbb{C}$  l'insieme delle radici  $n$ -esime di 1. Determinare il gruppo delle proiettività  $\phi$  di  $\mathbb{P}_\mathbb{C}^1$  tali che  $\phi(\mu_n) = \mu_n$ .

## 3.2 Le funzioni simmetriche

Il gruppo  $\Sigma_n$  delle permutazioni dell'insieme  $\{1, \dots, n\}$  agisce naturalmente sull'anello  $\mathbb{Z}[x_1, \dots, x_n]$ . Infatti, se  $A$  denota l'insieme delle applicazioni  $\phi: \{1, \dots, n\} \rightarrow \mathbb{Z}$ , allora possiamo interpretare  $\mathbb{Z}[x_1, \dots, x_n]$  come un sottoanello dell'anello di tutte le applicazioni  $f: A \rightarrow \mathbb{Z}$ , dove per ogni indice  $i$  si ha

$$x_i: A \rightarrow \mathbb{Z}, \quad x_i(\phi) = \phi(i).$$

Se adottiamo la convenzione che  $\Sigma_n$  agisce a sinistra su  $\{1, \dots, n\}$ , ossia che  $\sigma\tau(i) = \sigma(\tau(i))$ , allora  $\Sigma_n$  agisce a destra su  $A$  mediante la regola  $\phi^\sigma(i) = \phi(\sigma(i))$  e di conseguenza agisce a sinistra su  $\mathbb{Z}[x_1, \dots, x_n]$  mediante la regola

$$\sigma(p)(x_1, \dots, x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

**Definizione 3.2.1.** *Un polinomio  $p \in \mathbb{Z}[x_1, \dots, x_n]$  si dice **simmetrico** se è invariante per l'azione del gruppo simmetrico, ossia se  $\sigma p = p$  per ogni  $\sigma \in \Sigma_n$ .*

Notiamo che un polinomio è simmetrico se e solo se tutte le sue componenti omogenee sono simmetriche.

**Definizione 3.2.2.** Le *funzioni simmetriche elementari*  $\sigma_1, \dots, \sigma_n \in \mathbb{Z}[x_1, \dots, x_n]$  sono i polinomi simmetrici definiti dalla relazione

$$t^n + \sum \sigma_i t^{n-i} = \prod (t + x_i).$$

**Teorema 3.2.3.** Le funzioni simmetriche elementari generano la sottoalgebra dei polinomi simmetrici.

*Dimostrazione.* Sia  $f \in \mathbb{Z}[x_1, \dots, x_n]$  simmetrico e sia  $f = f_0 + \dots + f_m$  la decomposizione in componenti isobare rispetto ai pesi  $w(x_i) = i$ , con  $f_i$  di peso  $i$  ed  $f_m \neq 0$ . Dimostriamo per induzione su  $m$  che  $f$  è un polinomio nelle funzioni simmetriche elementari.

Per ogni  $i$  il monomio di peso massimo di  $\sigma_i$  è uguale a  $x_{n-i+1}x_{n-i+2} \cdots x_n$ .

Ogni monomio di  $f_m$  è del tipo  $ax_1^{i_1}x_2^{i_2} \cdots x_n^{i_n}$  con  $i_1 \leq i_2 \leq \dots \leq i_n$ ; quindi, se poniamo  $y_i = x_{n-i+1}x_{n-i+2} \cdots x_n$ , esiste un polinomio  $g \in \mathbb{Z}[y_1, \dots, y_n]$  tale che  $f_m(x_1, \dots, x_n) = g(y_1, \dots, y_n)$ . Il polinomio  $f(x_1, \dots, x_n) - g(\sigma_1, \dots, \sigma_n)$  è simmetrico di peso  $< m$  e si può applicare l'ipotesi induttiva.  $\square$

Negli esercizi di questa sezione indicheremo con  $\sigma_i, \psi_h \in \mathbb{Z}[x_1, \dots, x_n]$ , per  $i \in \mathbb{Z}$  e  $h \in \mathbb{N}$ , le funzioni simmetriche definite dalle formule

$$\prod_{i=1}^n (t + x_i) = \sum_{i=-\infty}^{+\infty} t^{n-i} \sigma_i, \quad \psi_h = \sum_{i=1}^n x_i^h.$$

Si noti che  $\psi_0 = n$  e  $\sigma_i = 0$  per  $i < 0$  e per  $i > n$ .

### Esercizi

**3.4.** Siano  $s < n$  e

$$\pi: \mathbb{Z}[x_1, \dots, x_n] \rightarrow \mathbb{Z}[x_1, \dots, x_s], \quad \text{dove } \pi(x_i) = 0 \text{ per } i = s+1, \dots, n,$$

la proiezione. Provare che  $\pi(\sigma_i) = \sigma_i$  per ogni  $i \in \mathbb{Z}$ .

**3.5.** Sia  $A \subset \mathbb{N}^n$  il sottoinsieme (di cardinalità  $n!$ ) formato dai multiindici  $a = (a_1, \dots, a_n)$  tali che  $0 \leq a_i < i$ . Per ogni vettore  $p = (p_1, \dots, p_n) \in \mathbb{Q}^n$ , per ogni permutazione  $\sigma \in \Sigma_n$  e per ogni  $a = (a_1, \dots, a_n) \in A$  poniamo  $p_\sigma^a = p_{\sigma(1)}^{a_1} \cdots p_{\sigma(n)}^{a_n}$ . Provare:

1. Se  $p_i \neq p_j$  per ogni  $i \neq j$ , allora la matrice  $(p_\sigma^a)$  ha rango  $n!$ .
2. (\*) Il determinante di  $(p_\sigma^a)$  è una potenza di  $\prod_{i>j} (p_i - p_j)$  (determinante della matrice di Vandermonde).

**3.6 (\*)**. Si denoti con  $I_n \subset \mathbb{Z}[x_1, \dots, x_n]$  l'ideale generato dalle funzioni  $\sigma_1, \dots, \sigma_n$ . Provare:

1. Per ogni  $i = 1, \dots, n$  vale

$$x_i^i \equiv \sum_{h=1}^i (-1)^{h-1} \sigma_h x_i^{i-h} \pmod{x_{i+1}, \dots, x_n}.$$

2. Ogni polinomio  $f \in \mathbb{Z}[x_1, \dots, x_n]$  è equivalente modulo  $I_n$  ad una combinazione lineare, a coefficienti in  $\mathbb{Z}$ , di monomi della forma

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}, \quad \text{con } 0 \leq a_i < i.$$

3.  $x_i^n \in I_n$  per ogni  $i$ .

4. Ogni polinomio omogeneo  $f \in \mathbb{Z}[x_1, \dots, x_n]$  di grado strettamente maggiore di  $\frac{1}{2}n(n-1)$  appartiene all'ideale  $I_n$ .
5.  $\mathbb{Z}[x_1, \dots, x_n]$  è uno  $\mathbb{Z}[\sigma_1, \dots, \sigma_n]$ -modulo libero di rango  $n!$  con base  $x_1^{a_1} \cdots x_n^{a_n}$ , per  $a_i < i$ . (Sugg.: usare il punto 2 e induzione sul grado per mostrare che i monomi generano. Usare l'Esercizio 3.5 per mostrare che sono indipendenti.)

**3.7.** Si consideri la serie generatrice

$$\psi(t) = \sum_{h=1}^{\infty} \frac{t^h}{h} \sum_{i=1}^n x_i^h = \sum_{h=1}^{\infty} \frac{t^h}{h} \psi_h \in \mathbb{Q}[x_1, \dots, x_n][[t]]$$

e si dimostrino le uguaglianze

$$\sum_{i=1}^n (-t)^i \sigma_i = e^{-\psi(t)} - 1, \quad \psi(t) = -\log \left( 1 + \sum_{i=1}^n (-t)^i \sigma_i \right).$$

Dalla prima uguaglianza segue che ogni funzione  $\sigma_i$  si scrive come un polinomio a coefficienti razionali in  $\psi_1, \dots, \psi_i$ ; la seconda fornisce una descrizione esplicita delle  $\psi_h = \sum x_i^h$  come polinomi nelle  $\sigma_i$ .

**3.8.** Si consideri la matrice a coefficienti in  $\mathbb{Z}[x_1, \dots, x_n]$

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & \sigma_n \\ -1 & 0 & \cdots & 0 & \sigma_{n-1} \\ 0 & -1 & \cdots & 0 & \sigma_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & \sigma_1 \end{pmatrix}$$

Si provi che  $\psi_h$  è uguale alla traccia di  $A^h$ , per ogni  $h \geq 0$ . (Sugg.: la matrice  $A$  rappresenta, in una opportuna base, la moltiplicazione per  $t$  nel modulo  $\mathbb{Z}[x_1, \dots, x_n][t]/(\prod_{i=1}^n (t - x_i))$ .)

### 3.3 Invarianti e covarianti di forme binarie

Il paragrafo precedente rappresenta un esempio di come la geometria della retta proiettiva si applica allo studio delle equazioni polinomiali  $f(x) = 0$ . In tale contesto è utile considerare al posto dei polinomi le forme binarie.

**Definizione 3.3.1.** Una **forma binaria** di grado  $n$  è un polinomio omogeneo di grado  $n$  in due variabili.

Denotiamo con  $V_n$  lo spazio vettoriale delle forme binarie di grado  $n$ . Ogni forma binaria  $f$  può essere pensata come una applicazione  $f: \mathbb{K}^2 \rightarrow \mathbb{K}$ ; per ragioni di convenienza notazionale, che appariranno più chiare in seguito, se  $x_0, x_1$  sono le coordinate di  $\mathbb{K}^2$ , scriveremo ogni forma binaria nella forma

$$f(x_0, x_1) = a_0 x_0^n + \binom{n}{1} a_1 x_0^{n-1} x_1 + \cdots + \binom{n}{i} a_i x_0^{n-i} x_1^i + \cdots + a_n x_1^n$$

e quindi  $a_0, \dots, a_n \in V_n^\vee = \text{Hom}_{\mathbb{K}}(V_n, \mathbb{K})$  sono le coordinate di  $f$ . In particolare  $V_n$  ha dimensione  $n+1$  su  $\mathbb{K}$ .

Esiste una naturale applicazione bilineare  $V_a \times V_b \rightarrow V_{a+b}$  data dalla moltiplicazione. Per ogni  $n \geq 0$  esiste un isomorfismo naturale fra  $V_n$  e lo spazio vettoriale dei polinomi di grado  $\leq n$  in una variabile  $x$ . Dato un polinomio omogeneo  $f(x_0, x_1) \in V_n$ , il suo disomogeneizzato  $p(x) = f(x, 1)$  è un polinomio di grado  $\leq n$ . Viceversa, dato un polinomio  $p(x)$  di grado  $\leq n$ , il suo omogeneizzato è il polinomio omogeneo definito dalla formula

$$f(x_0, x_1) = x_1^n p\left(\frac{x_0}{x_1}\right).$$

Dal fatto che gli isomorfismi di omogeneizzazione commutano con le operazioni di somma e prodotto, segue immediatamente che, se  $\mathbb{K}$  è algebricamente chiuso, allora ogni forma binaria è il prodotto di forme binarie di grado 1 e quindi ogni forma binaria non nulla di grado  $n$  possiede esattamente  $n$  radici (contate con molteplicità) su  $\mathbb{P}^1 = \mathbb{P}(V_1^\vee)$ . È inoltre chiaro che le radici di  $f(x, 1)$  sono esattamente le radici di  $f(x_0, x_1)$  che stanno nella parte affine  $\{x_1 \neq 0\}$  di  $\mathbb{P}^1$ .

**Lemma 3.3.2.** *Due forme binarie non nulle hanno le stesse radici nella chiusura algebrica di  $\mathbb{K}$ , contate con molteplicità, se e solo se sono proporzionali.*

*Dimostrazione.* Evidente. □

Si noti che il Lemma 3.3.2 definisce, su campi algebricamente chiusi, una bigezione fra  $\mathbb{P}^n = \mathbb{P}(V_n)$  ed il quoziente di  $(\mathbb{P}^1)^n$  per l'azione del gruppo simmetrico  $\Sigma_n$ .

La ovvia azione sinistra di  $\mathrm{GL}(2, \mathbb{K})$  su  $\mathbb{K}^2$  induce per composizione delle azioni destre

$$V_n \times \mathrm{GL}(2, \mathbb{K}) \rightarrow V_n, \quad (f, A) \mapsto f^A,$$

che sono compatibili con i prodotti  $V_a \times V_b \rightarrow V_{a+b}$ . In concreto, se  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ,  $f \in V_n$  e  $g$  è il disomogeneizzato di  $f$  si ha:

$$f^A(x_0, x_1) = f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}\right) = f(ax_0 + bx_1, cx_0 + dx_1),$$

$$g^A(x) = g\left(\frac{ax+b}{cx+d}\right) (cx+d)^n.$$

Ogni polinomio  $p(a_0, \dots, a_n)$  può essere pensato come una funzione  $p: V_n \rightarrow \mathbb{K}$ ; esiste allora una ovvia azione sinistra di  $\mathrm{GL}(2, \mathbb{K})$  su  $\mathbb{K}[a_0, \dots, a_n]$  data da:

$$Ap(f) = p(f^A), \quad \text{dove } A \in \mathrm{GL}(2, \mathbb{K}), \quad p \in \mathbb{K}[a_0, \dots, a_n] \quad \text{e } f \in V_n.$$

*Esempio 3.3.3.* Se

$$n = 2, \quad p = a_0 a_2 - a_1^2, \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

allora si ha  $Ap = p \det^2 A = p \det A^2$ . Infatti,

$$\begin{aligned} Ap(a_0 x_0^2 + 2a_1 x_0 x_1 + a_2 x_1^2) &= \\ p(a_0(ax_0 + bx_1)^2 + 2a_1(ax_0 + bx_1)(cx_0 + dx_1) + a_2(cx_0 + dx_1)^2) &= \\ (a_0 a^2 + 2a_1 ac + a_2 c^2)(a_0 b^2 + 2a_1 bd + a_2 d^2) - (a_0 ab + a_1(ad + bc) + a_2 cd)^2 &= \\ (a_0 a_2 - a_1^2)(ad - bc)^2 = p(a_0 x_0^2 + 2a_1 x_0 x_1 + a_2 x_1^2) \det A^2. \end{aligned}$$

Notiamo che  $p(f) = 0$  se e solo se  $f$  ha una radice doppia.

**Definizione 3.3.4.** Un polinomio  $p(a_0, \dots, a_n)$  si dice una **forma covariante di peso**  $m$  su  $V_n$  se, per ogni  $A \in \text{GL}(2, \mathbb{K})$ , vale  $Ap = p \det^m A$ .

Il termine **covariante** sarà spesso utilizzato come sinonimo di forma covariante. L'Esempio 3.3.3 mostra che  $a_0 a_2 - a_1^2$  è un covariante di peso 2 su  $V_2$ . Si noti che ogni covariante è costante sulle orbite di  $\text{SL}(2, \mathbb{K})$ . In particolare, le uniche forme covarianti su  $V_1$  sono le costanti.

**Teorema 3.3.5.** Sia  $p(a_0, \dots, a_n)$  una forma covariante di peso  $m$  su  $V_n$ . Allora  $p$  è un polinomio omogeneo di grado  $\frac{2m}{n}$  ed isobaro di peso  $m$  rispetto ai pesi  $w(a_i) = i$ . In particolare, ogni monomio che appare in  $p$  con coefficiente non nullo contiene un fattore  $a_i$  per qualche  $i \geq \frac{n}{2}$ .

*Dimostrazione.* Vale  $Ap = p \det A^m$  per ogni matrice  $A$  diagonale. Sia  $A = \text{diag}(\alpha, \beta)$  e sia  $q = a_0^{i_0} \cdots a_n^{i_n}$  un monomio di grado  $d = i_0 + \cdots + i_n$  e peso  $m = i_1 + 2i_2 + \cdots + ni_n$ . Vale  $\det A = \alpha\beta$  e  $Aq = q\alpha^{dn-m}\beta^m$  e quindi  $q$  può comparire in  $p$  solo se  $dn - m = m$ . Si noti infine che la condizione  $dn = 2m$  implica necessariamente  $i_s > 0$  per qualche  $s \geq \frac{n}{2}$ .  $\square$

**Definizione 3.3.6.** Un polinomio  $p \in \mathbb{K}[a_0, \dots, a_n]$  viene detto **SL-invariante** se  $Ap = p$  per ogni  $A \in \text{SL}(2, \mathbb{K})$ . I polinomi SL-invarianti formano una sottoalgebra  $R \subset \mathbb{K}[a_0, \dots, a_n]$  detta **algebra dei covarianti** su  $V_n$ .

Non è difficile dimostrare (Esercizio 3.9) che l'algebra dei covarianti coincide con la sottoalgebra generata dalle forme covarianti.

**Corollario 3.3.7.** Sia  $p$  un covariante su  $V_n$  e sia  $f \in V_n$ . Se  $f$  possiede una radice di molteplicità  $> \frac{n}{2}$  allora  $p(f) = 0$ .

*Dimostrazione.* Siccome  $p$  è covariante basta dimostrare che  $p(f^A) = 0$  per qualche  $A \in \text{GL}(2, \mathbb{K})$ ; non è quindi restrittivo supporre che  $f$  abbia in 0 una radice di molteplicità  $d > n/2$ . Quindi, se  $a_0, \dots, a_n$  sono le coordinate di  $f$ , vale  $a_s = 0$  per ogni  $s > n - d$  e la tesi segue dal Teorema 3.3.5.  $\square$

È utile osservare che  $p$  è un covariante di peso  $m$  se e solo se  $Ap = p \det^m A$  per ogni  $A$  appartenente ad un insieme fissato di generatori del gruppo  $\text{GL}(2, \mathbb{K})$ . Un conveniente insieme di generatori è dato dall'unione dei seguenti tre insiemi:

1. Matrici diagonali  $x_i \mapsto \lambda_i x_i$ ,  $i = 0, 1$ .
2. Inversione  $x_0 \mapsto x_1$ ,  $x_1 \mapsto x_0$ .
3. Traslazioni  $x_0 \mapsto x_0 + ax_1$ ,  $x_1 \mapsto x_1$ .

Dimostreremo in seguito il, tutt'altro che evidente, fatto che è sufficiente verificare la covarianza per le diagonali e le traslazioni.

Usiamo adesso il Teorema 3.2.3 sulle funzioni simmetriche per costruire in modo intuitivo (ma poco rigoroso) alcuni covarianti non banali su  $V_n$  per ogni  $n \geq 2$ ; si assuma per semplicità  $\mathbb{K} = \mathbb{R}, \mathbb{C}$ .

Siano  $\alpha_1, \dots, \alpha_n$  le radici di un polinomio  $f(x) = a_0 x^n + na_1 x^{n-1} + \cdots + a_n$ , si assuma  $a_0 a_n \neq 0$  e si consideri

$$D = \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Si tratta di un polinomio simmetrico in  $\alpha_1, \dots, \alpha_n$  e quindi si può scrivere  $D = D(\sigma_1, \dots, \sigma_n)$  dove  $\sigma_i = (-1)^i \binom{n}{i} \frac{a_i}{a_0}$  indica la  $i$ -esima funzione simmetrica elementare. Dimostriamo adesso che  $\Delta = a_0^{2(n-1)} D$  è un polinomio in  $a_0, \dots, a_n$  covariante di peso  $n(n-1)$  su  $V_n$ . Il polinomio  $\Delta(f)$  viene detto **discriminante** di  $f$ . La dimostrazione completa e rigorosa che  $\Delta$  è un polinomio, cioè che non contiene potenze di  $a_0$  al denominatore sarà data nel Capitolo 4. Si tratta comunque di un fatto abbastanza ovvio dal punto di vista intuitivo: infatti, per ogni polinomio monico fissato  $g(x)$  di grado  $n-1$  con radici  $\beta_1, \dots, \beta_{n-1}$ , esiste una costante  $C$  dipendente da  $g$  tale, che posto  $f(x) = (a_0x - 1)g(x)$ , vale  $\Delta(f) = C a_0^{2(n-1)} \prod_{i=1}^{n-1} (a_0^{-1} - \beta_i)^2$  e quindi esiste finito il limite di  $\Delta(f)$  per  $a_0 \rightarrow 0$ . La covarianza di  $\Delta$  rispetto alle traslazioni è evidente dalla definizione, rimane da verificare la covarianza rispetto alle matrici diagonali ed all'inversione. Sia  $A = \text{diag}(\lambda, \xi)$ , allora  $A(x_0 - \alpha_i x_1) = \lambda x_0 - \alpha_i \xi x_1$  e quindi  $A$  trasforma la radice  $\alpha_i$  in  $\lambda^{-1} \xi \alpha_i$ , mentre trasforma il coefficiente  $a_0$  in  $\lambda^n a_0$ , ne segue che

$$A\Delta = \Delta(\lambda^{-1}\xi)^{n(n-1)} \lambda^{2n(n-1)} = \Delta \det A^{n(n-1)}.$$

L'inversione manda  $\alpha_i$  in  $\alpha_i^{-1}$  e  $a_0$  in  $a_n$ , dunque

$$A\Delta = a_n^{2(n-1)} \prod_{i \neq j} \frac{(\alpha_i - \alpha_j)}{\alpha_i \alpha_j} = \Delta$$

dove nell'ultima uguaglianza abbiamo fatto uso della relazione  $a_n = (-1)^n a_0 \alpha_1 \dots \alpha_n$ . Siccome le  $f \in V_n$  con  $a_0 a_n \neq 0$  sono un aperto denso, la relazione  $\Delta(f^A) = \Delta(f) \det A^{n(n-1)}$  vale per ogni  $f$  ed  $A$ . Quindi  $\Delta$  è un covariante.

Usando la stessa idea si possono costruire altri covarianti di peso multiplo di  $n$ : diamo qui solo l'algoritmo di costruzione lasciando per esercizio le verifiche di covarianza. Si consideri una tabella quadrata  $T = \{(i, j) \in \mathbb{N}^2 \mid 1 \leq i, j \leq n\}$  e sia  $S \subset T$  un sottoinsieme con le seguenti proprietà:

1. Se  $(i, j) \in S$ , allora  $i < j$ .
2. Se  $r_i$  (resp.:  $c_i$ ) indica il numero di elementi di  $S$  sulla  $i$ -esima riga (resp.: colonna), allora  $r_i + c_i = m$  non dipende da  $i$ .

Le seguenti due tabelle forniscono due esempi di tali insiemi per  $n = 4$ :

			*
		*	

	*	*	*
		*	*
			*

Un covariante di peso  $nm$  è allora dato da:

$$\Delta_S = a_0^{2m} \sum_{\sigma \in \Sigma_n} \prod_{(i,j) \in S} (\alpha_{\sigma(i)} - \alpha_{\sigma(j)})^2.$$

Si noti che  $\Delta_S$  non è identicamente nullo, come si vede considerando un polinomio a radici razionali distinte.

*Esempio 3.3.8.* Con un conto che omettiamo si calcola il discriminante di una forma di terzo grado che, a meno di uno scalare, vale:

$$\Delta = a_0^2 a_3^2 - 3a_1^2 a_2^2 + 4a_1^3 a_3 + 4a_0 a_2^3 - 6a_0 a_1 a_2 a_3.$$

Dati due covarianti  $P, Q$  su  $V_n$  dello stesso peso, con  $Q \neq 0$ , il quoziente  $\frac{P}{Q}$  si dice un **invariante razionale** su  $V_n$ . Se  $U \subset V_n$  denota l'insieme delle forme  $f$  tali che  $Q(f) \neq 0$ , allora  $f^A \in U$  per ogni  $f \in U$  ed ogni  $A \in \text{GL}(2, \mathbb{K})$ . È definita una funzione:

$$\frac{P}{Q}: U \rightarrow \mathbb{K}, \quad \frac{P}{Q}(f) = \frac{P(f)}{Q(f)},$$

con le proprietà:

1.  $\frac{P}{Q}(f^A) = \frac{P}{Q}(f)$  per ogni  $A \in \text{GL}(2, \mathbb{K})$ .
2.  $\frac{P}{Q}(\lambda f) = \frac{P}{Q}(f)$  per ogni  $\lambda \in \mathbb{K}^*$ .

Le proprietà 1 e 2 implicano tra l'altro che, se  $f, g \in U$  ed esiste una proiettività di  $\mathbb{P}^1$  che trasforma gli zeri di  $f$  (contati con molteplicità) negli zeri di  $g$ , allora  $\frac{P}{Q}(f) = \frac{P}{Q}(g)$ .

**Proposizione 3.3.9.** *Le algebre dei covarianti su  $V_2$  e  $V_3$  sono generate dal discriminante.*

*Dimostrazione.* Consideriamo il caso  $V_3$ : la dimostrazione nel caso  $V_2$  è sostanzialmente identica. Sia  $P$  un covariante, esistono allora interi positivi  $r, s$  tali che  $P^r$  e  $\Delta^s$  hanno lo stesso peso e quindi  $\phi = \frac{P^r}{\Delta^s}$  è un invariante razionale. Detto  $U = \{f \mid \Delta(f) \neq 0\}$  si ha che  $f \in U$  se e solo se  $f$  possiede tre radici distinte; siccome due terne su  $\mathbb{P}^1$  sono sempre proiettivamente equivalenti  $\phi$  è uguale su  $U$  ad una costante  $c$ . Basta adesso osservare che  $\Delta$  è irriducibile e che  $\Delta(P^r - c\Delta^s) = \Delta P^r - c\Delta^{s+1} = 0$ .  $\square$

**Esercizi**

**3.9.** Provare che un polinomio omogeneo  $p \in \mathbb{K}[a_0, \dots, a_n]$  è un covariante se e solo se  $Ap = p$  per ogni  $A \in \text{SL}(2, \mathbb{K})$ .

**3.10.** Dimostrare che se  $p$  è una forma covariante di peso  $m$ , allora vale

$$p(a_n, a_{n-1}, \dots, a_0) = (-1)^m p(a_0, \dots, a_n).$$

**3.11.** Provare che una forma non nulla di grado  $n$

$$f(x_0, x_1) = a_0 x_0^n + \binom{n}{1} a_1 x_0^{n-1} x_1 + \dots + \binom{n}{i} a_i x_0^{n-i} x_1^i + \dots + a_n x_1^n$$

possiede una radice di molteplicità  $n$  se e solo se

$$\text{rank} \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = 1.$$

**3.12.** Sia  $f(x_0, x_1)$  una forma binaria di grado  $n$  a coefficienti numeri complessi. Provare che  $f = (ax_0 + bx_1)^n$  se e solo se il determinante Hessiano

$$\begin{vmatrix} f_{00} & f_{01} \\ f_{10} & f_{11} \end{vmatrix}$$

è identicamente nullo.

### 3.4 Il metodo simbolico di Cayley-Aronhold

Nella base standard di  $V_n$ , data dai monomi  $\binom{n}{i}x_0^i x_1^{n-i}$ , l'elevazione alla  $n$ -esima potenza  $V_1 \rightarrow V_n$  è rappresentata in coordinate da

$$(t_0, t_1) \mapsto (t_0^n, t_0^{n-1}t_1, \dots, t_0^{n-i}t_1^i, \dots, t_1^n).$$

In particolare, ogni applicazione lineare  $F: V_n \rightarrow \mathbb{K}$  induce una applicazione  $\tilde{F}: V_1 \rightarrow \mathbb{K}$  che è omogenea di grado  $n$  ed è data da  $\tilde{F}(p) = F(p^n)$ .

Viceversa, ogni applicazione  $\tilde{G}: V_1 \rightarrow \mathbb{K}$  omogenea di grado  $d$  è indotta da un'unica applicazione lineare  $G: V_d \rightarrow \mathbb{K}$ . Infatti, si ha  $\tilde{G}(\alpha_0 x_0 + \alpha_1 x_1) = \tilde{g}(\alpha_0, \alpha_1)$  con  $\tilde{g}$  polinomio omogeneo di grado  $d$ ; detto  $a_i = \alpha_0^{d-i} \alpha_1^i$  si può scrivere in modo unico  $\tilde{g}(\alpha_0, \alpha_1) = g(a_0, \dots, a_d)$ , con  $g$  omogeneo di grado 1. Ponendo

$$G\left(\sum a_i \binom{d}{i} x_0^{d-i} x_1^i\right) = g(a_0, \dots, a_d),$$

si verifica immediatamente che  $G(p^d) = \tilde{G}(p)$  per ogni  $p \in V_1$ . Si prova similmente che l'applicazione  $F \mapsto \tilde{F}$  definisce un isomorfismo di spazi vettoriali.

Si consideri adesso uno spazio vettoriale  $V$  di dimensione finita. Data un'applicazione

$$\hat{F}: \underbrace{V \times \dots \times V}_{d \text{ fattori}} \rightarrow \mathbb{K}$$

multilineare simmetrica si definisce in modo naturale una  $F: V \rightarrow \mathbb{K}$  omogenea di grado  $d$  ponendo  $F(v) = \hat{F}(v, \dots, v)$ . Il procedimento  $\hat{F} \mapsto F$  prende il nome di **restituzione**.

Viceversa, data una  $F: V \rightarrow \mathbb{K}$  omogenea di grado  $d$  e  $v_1, \dots, v_d \in V$  esiste unico un polinomio omogeneo simmetrico  $f \in \mathbb{K}[\lambda_1, \dots, \lambda_d]$  di grado  $d$  tale che

$$F(\lambda_1 v_1 + \dots + \lambda_d v_d) = f(\lambda_1, \dots, \lambda_d).$$

Definiamo quindi  $\hat{F}(v_1, \dots, v_d)$  come il coefficiente di  $\lambda_1 \dots \lambda_d$  in  $f$  diviso per  $d!$ . Il procedimento  $F \mapsto \hat{F}$  si dice di **polarizzazione**.

**Proposizione 3.4.1.** *La polarizzazione è l'inverso della restituzione: in particolare la polarizzata di un'applicazione omeogena è multilineare simmetrica.*

*Dimostrazione.* Sia  $F: V \rightarrow \mathbb{K}$  omogenea di grado  $d$ . È chiaro che la sua polarizzata  $\hat{F}$  è simmetrica; per dimostrare la multilinearità basta dimostrare che

$$\hat{F}(aw_1 + bw_2, v_2, \dots, v_d) = a\hat{F}(w_1, v_2, \dots, v_d) + b\hat{F}(w_2, v_2, \dots, v_d).$$

Sia  $c_i = d!\hat{F}(w_i, v_2, \dots, v_d)$ , per  $i = 1, 2$ , allora dal fatto che  $F$  è omogeneo di grado  $d$  segue che il coefficiente di  $\lambda_2 \dots \lambda_d$  in  $F(aw_1 + bw_2 + \lambda_2 v_2 + \dots + \lambda_d v_d)$  è una forma lineare in  $a$  e  $b$  che dovrà necessariamente essere  $c_1 a + c_2 b$ . Basta adesso notare che, per ogni  $d$ -upla  $z_1, \dots, z_d \in V$ , il valore  $d!\hat{F}(z_1, \dots, z_d)$  può essere definito come il coefficiente di  $\lambda_2 \dots \lambda_d$  in  $f(1, \lambda_2, \dots, \lambda_d) = F(z_1 + \lambda_2 z_2 + \dots + \lambda_d z_d)$  e quindi  $\hat{F}(aw_1 + bw_2, v_2, \dots, v_d) = c_1 a + c_2 b$ . Indichiamo con  $R$  l'operatore di restituzione e con  $P$  quello di polarizzazione. Data una  $F: V \rightarrow \mathbb{K}$  omogenea di grado  $d$  e  $v \in V$  si ha  $F(\lambda_1 v + \dots + \lambda_d v) = (\lambda_1 + \dots + \lambda_d)^d F(v)$  ed il coefficiente di  $\lambda_1 \dots \lambda_d$  in  $(\lambda_1 + \dots + \lambda_d)^d$  è esattamente  $d!$ , questo prova che  $R \circ P = Id$ .

Viceversa sia  $\hat{F}$  multilineare simmetrica e siano  $v_1, \dots, v_d \in V$  fissati, allora detto  $w = \lambda_1 v_1 + \dots + \lambda_d v_d$  si ha

$$\hat{F}(w, \dots, w) = \hat{f}(\lambda_1, \dots, \lambda_d)$$



per un opportuno polinomio omogeneo  $\hat{f}$ . Essendo  $\hat{F}$  simmetrica, il coefficiente di  $\lambda_1 \cdots \lambda_d$  in  $\hat{f}$  è esattamente  $d!\hat{F}(v_1, \dots, v_d)$ , questo prova che  $P \circ R = Id$ .  $\square$

Si noti che le operazioni di polarizzazione e restituzione commutano con l'azione naturale del gruppo  $GL(V, \mathbb{K})$  su  $V$ .

Ritorniamo agli spazi  $V_d$ ; un ragionamento analogo al precedente mostra che esiste una bigezione naturale fra le

$$\phi: V_d \times \cdots \times V_d \rightarrow \mathbb{K} \quad \text{multilineari simmetriche}$$

e le

$$\tilde{\phi}: V_1 \times \cdots \times V_1 \rightarrow \mathbb{K} \quad \text{multiomogenee simmetriche di grado } d.$$

La bigezione è data dalla relazione  $\tilde{\phi}(p_1, \dots, p_s) = \phi(p_1^d, \dots, p_s^d)$ .

Riassumendo, abbiamo trovato un procedimento, detto **metodo simbolico** che, partendo da una  $\tilde{F}: V_1^s \rightarrow \mathbb{K}$  multiomogenea simmetrica di grado  $d$ , si passa da una  $\hat{F}: V_d^s \rightarrow \mathbb{K}$  multilineare simmetrica e si arriva ad una  $F: V_d \rightarrow \mathbb{K}$  omogenea di grado  $s$ . Se inoltre  $\tilde{F}$  è  $SL(2, \mathbb{K})$ -invariante, allora anche  $F$  lo è. Concretamente, se  $v_i = \alpha_i x_0 + \beta_i x_1$ , per  $i = 1, \dots, s$ , allora si ha  $\tilde{F}(v_1, \dots, v_s) = \tilde{f}(\alpha_1, \beta_1, \dots, \alpha_s, \beta_s)$ , dove  $\tilde{f}$  è un polinomio multiomogeneo simmetrico di grado  $d$ . Per passare da  $\tilde{F}$  a  $\hat{F}$  si esegue la sostituzione  $a_{ij} = \alpha_i^{d-j} \beta_j^j$  e si ottiene  $\tilde{f}(\alpha_i, \beta_i) = \hat{f}(a_{ij})$ . Infine si pone  $a_j = a_{ij}$  e si ottiene  $f(a_0, \dots, a_d) = \hat{f}(a_{ij})$ , con  $f$  polinomio omogeneo di grado  $s$  e, usando l'isomorfismo standard si ha infine

$$F \left( \sum a_i \binom{d}{i} x_0^{d-i} x_1^i \right) = f(a_0, \dots, a_d).$$

Come esempio costruiamo due forme covarianti su  $V_4$  di gradi 2 e 3 ottenute partendo da dei covarianti  $\tilde{F}: V_1^s \rightarrow \mathbb{K}$  multiomogenei simmetrici di grado 4. Per  $s = 1$  non ci sono covarianti di peso positivo, ciò segue immediatamente dal fatto che  $V_1 - \{0\}$  è un'orbita dell'azione di  $SL(2, \mathbb{K})$ . Per  $s = 2$  un covariante naturale è  $g_2: V_1^2 \rightarrow \mathbb{K}$ , definito da

$$g_2 = \frac{1}{2} \begin{vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{vmatrix}^4.$$

Per  $s = 3$  abbiamo  $g_3: V_1^3 \rightarrow \mathbb{K}$ , definito da

$$g_3 = \frac{1}{6} \begin{vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{vmatrix}^2 \begin{vmatrix} \alpha_2 & \alpha_3 \\ \beta_2 & \beta_3 \end{vmatrix}^2 \begin{vmatrix} \alpha_3 & \alpha_1 \\ \beta_3 & \beta_1 \end{vmatrix}^2.$$

I covarianti  $g_2, g_3$  sono detti di **Eisenstein**. Applicando il metodo simbolico si ottiene

$$\begin{aligned} g_2 &= \frac{1}{2} (\alpha_1 \beta_2 - \alpha_2 \beta_1)^4 = \\ &= \frac{1}{2} (\alpha_1^4 \beta_2^4 - 4\alpha_1^3 \beta_1 \alpha_2 \beta_2^3 + 6\alpha_1^2 \beta_1^2 \alpha_2^2 \beta_2^2 - 4\alpha_1 \beta_1^3 \alpha_2^3 \beta_2 + \beta_1^4 \alpha_2^4) = \\ &= \frac{1}{2} (a_{10} a_{24} - 4a_{11} a_{23} + 6a_{12} a_{22} - 4a_{13} a_{21} + a_{14} a_{20}) = \\ &= \frac{1}{2} (a_0 a_4 - 4a_1 a_3 + 6a_2^2 - 4a_3 a_1 + a_4 a_0) = a_0 a_4 - 4a_1 a_3 + 3a_2^2. \end{aligned}$$

A rimarcare il valore matematico del metodo simbolico osserviamo che non è per nulla evidente come dall'espressione  $g_2 = a_0 a_4 - 4a_1 a_3 + 3a_2^2$  segua la covarianza di  $g_2$ . Prima di affrontare il calcolo esplicito di  $g_3$  osserviamo che, essendo in ogni monomio la somma dei gradi di  $\alpha_i$  e  $\beta_i$  uguale a 4 possiamo disomogeneizzare il tutto ponendo  $\alpha_i = 1$ . Si ha quindi

$$6g_3 = (\beta_1 - \beta_2)^2(\beta_2 - \beta_3)^2(\beta_3 - \beta_1)^2.$$

Dopo aver scritto i 27 addendi di  $g_3$  bisogna sostituire il monomio  $\beta_1^i \beta_2^j \beta_3^k$  con  $a_i a_j a_k$ ; si ottiene quindi una grande semplificazione da cui segue

$$g_3 = a_0 a_2 a_4 - a_0 a_3^2 + 2a_1 a_2 a_3 - a_2^3 - a_1^2 a_4.$$

Come prima non è affatto evidente da questa ultima espressione che si tratti di un covariante. Una piccola sfida intellettuale può venire dall'osservazione che  $g_2$  e  $g_3$  sono rispettivamente, a meno di costanti moltiplicative, lo Pfaffiano ed il determinante delle matrici

$$\begin{pmatrix} 0 & a_0 & 2a_1 & 3a_2 \\ -a_0 & 0 & a_2 & 2a_3 \\ -2a_1 & -a_2 & 0 & a_4 \\ -3a_2 & -2a_3 & -a_4 & 0 \end{pmatrix}, \quad \begin{pmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{pmatrix}.$$

**Lemma 3.4.2.** *I covarianti  $g_2, g_3 \in \mathbb{K}[a_0, \dots, a_4]$  sono algebricamente indipendenti su  $\mathbb{K}$ .*

*Dimostrazione.* È sufficiente dimostrare l'indipendenza algebrica di una qualunque specializzazione. Se poniamo  $a_0 = 1$  e  $a_1 = a_2 = 0$ , allora i covarianti diventano  $g_2 = a_4$  e  $g_3 = -a_3^2$  che si verifica facilmente essere algebricamente indipendenti.  $\square$

Vedremo più avanti che  $g_2$  e  $g_3$  generano l'algebra dei covarianti di  $V_4$ .

**Teorema 3.4.3.** *Ogni forma binaria di grado 4 a radici distinte, con covarianti  $g_2$  e  $g_3$  è equivalente alla forma di equazione non omogenea*

$$4x^3 - g_2x - g_3.$$

*Dimostrazione.* Sia  $f$  un forma di quarto grado senza radici multiple e sia  $x = \frac{x_0}{x_1}$  una coordinata affine sulla retta proiettiva. Con una opportuna proiettività possiamo mandare una radice all'infinito ed il baricentro delle altre 3 nello 0 e dunque  $f$  è proiettivamente equivalente ad una forma binaria del tipo  $4a_1x^3 + 4a_3x + a_4$ , con  $a_1 \neq 0$ . A meno di moltiplicare  $f$  per uno scalare possiamo supporre  $a_1 = 1$ ; si ottiene quindi la **forma canonica** delle forme binarie di grado 4 senza radici multiple

$$4x^3 - px - q, \quad \text{ossia } a_0 = a_2 = 0, a_1 = 1, a_3 = -\frac{p}{4}, a_4 = -q.$$

Si ha quindi  $g_2 = a_0 a_4 - 4a_1 a_3 + 3a_2^2 = p$  e  $g_3 = a_0 a_2 a_4 - a_0 a_3^2 + 2a_1 a_2 a_3 - a_2^3 - a_1^2 a_4 = q$ .  $\square$

**Teorema 3.4.4.** *Sia  $f \in V_4$ . Allora la forma  $f$  possiede radici multiple se e solo se  $(g_2^3 - 27g_3^2)(f) = 0$ .*

*Dimostrazione.* Se  $f$  possiede una radice multipla allora  $f$  è equivalente ad una forma binaria in cui  $a_0 = a_1 = 0$ : per tale forma si ha  $g_2 = 3a_2^2$ ,  $g_3 = -a_2^3$  e quindi  $g_2^3 = 27g_3^2$ .

Viceversa se  $f$  non ha radici multiple il polinomio  $p(x) = 4x^3 - g_2x - g_3$  non ha radici in comune con la sua derivata  $p'(x) = 12x^2 - g_2$ , cioè:

$$0 \neq p\left(\pm\sqrt{\frac{g_2}{12}}\right) = \pm\left(\frac{g_2}{27}\right)^{\frac{3}{2}} - g_3$$

e quindi  $27g_3^2 \neq g_2^3$ .  $\square$

Si definisce l'invariante  $j$  di una forma binaria di grado 4 come

$$j = 1728 \frac{g_2^3}{g_3^3 - 27g_2^2}.$$

La presenza del coefficiente  $1728 = 12^3$  è motivata dalla teoria delle curve ellittiche su campi di caratteristica 2 e 3, cfr. [Sil1986].

**Corollario 3.4.5.** *Due forme binarie di grado 4 a radici distinte sono equivalenti se e solo se hanno lo stesso invariante  $j$ .*

*Dimostrazione.* Siano  $f_1, f_2 \in V_4$  senza radici multiple con lo stesso invariante  $j$ , non è restrittivo supporre  $f_1, f_2$  in forma canonica, cioè

$$f_1 = 4x^3 - p_1x - q_1 \quad \text{e} \quad f_2 = 4x^3 - p_2x - q_2.$$

Con tali forme l'uguaglianza dell'invariante  $j$  equivale alla relazione  $p_1^3q_2^2 = p_2^3q_1^2$ . Dimostriamo che esiste  $t \in \mathbb{K}^*$  tale che  $f_2(x) = t^3f_1(t^{-1}x)$  o in termini equivalenti che  $p_2 = t^2p_1$  e  $q_2 = t^3q_1$ . Se  $p_1 = 0$ , allora  $q_1 \neq 0$  e dunque anche  $p_2 = 0$  e  $t$  esiste. Se  $p_1 \neq 0$ , allora anche  $p_2 \neq 0$  e con un opportuno  $t$  si può assumere  $p_1 = p_2$  e quindi  $q_1 = \pm q_2$ ; basta quindi considerare  $t = \pm 1$ .  $\square$

Data una quaterna non ordinata di punti  $Q = \{p_1, \dots, p_4\} \subset \mathbb{P}^1$ , con  $p_i \neq p_j$ , è ben definito  $j(Q) \in \mathbb{K}$  come il valore dell'invariante  $j$  di una forma binaria che ha come zeri esattamente  $p_1, \dots, p_4$ . Il Corollario 3.4.5 afferma che due quaterne non ordinate sono proiettivamente equivalenti se e solo se hanno lo stesso invariante  $j$ . Dunque  $j$  ha la stessa funzione che ha il birapporto rispetto alle quaterne ordinate di punti.

**Proposizione 3.4.6.** *Una quaterna non ordinata  $Q$  di punti distinti è:*

- *Armonica se e solo se  $g_3 = 0$  (Salmon, 1859).*
- *Equianarmonica se e solo se  $g_2 = 0$  (Painvin, 1861).*

*Dimostrazione.* I covarianti  $g_2$  e  $g_3$  di  $4x(x-1)(x-\lambda)$  sono

$$g_2 = \frac{4}{3}(\lambda^2 - \lambda + 1), \quad g_3 = \frac{4}{27}(\lambda + 1)(\lambda - 2)(2\lambda - 1).$$

$\square$

## Esercizi

**3.13.** Siano  $\alpha_1, \alpha_2, \alpha_3$  le radici di  $4x^3 - g_2x - g_3$ . Provare che

$$g_2^3 - 27g_3^2 = 16(\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2$$

e dedurre che  $g_2^3 - 27g_3^2$  differisce per una costante moltiplicativa dal discriminante  $\Delta$ .

**3.14.** Sia  $f(x) = x(x-1)(x-\lambda)$ , con  $\lambda \neq 0, 1$ . Provare che

$$j(f) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

**3.15.** Sia  $j \in \mathbb{K}$  e sia  $\lambda$  una radice del polinomio di sesto grado

$$f(x) = 2^8(x^2 - x + 1)^3 - jx^2(x-1)^2.$$

Provare che le sei radici di  $f(x)$ , contate con molteplicità, sono esattamente:

$$\lambda, \quad \frac{1}{\lambda}, \quad 1 - \lambda, \quad 1 - \frac{1}{\lambda}, \quad \frac{1}{1 - \lambda}, \quad \frac{\lambda}{\lambda - 1}.$$

Mostrare inoltre che  $f(x)$  possiede radici multiple se e solo se  $j = 0$  o  $j = 1728$ . Confrontare questo risultato con l'Esercizio 3.14 e con i possibili birapporti di una quaterna non ordinata di punti.

### 3.5 Finita generazione dell'algebra dei covarianti

In questa sezione  $n$  sarà un intero positivo fissato. Denotiamo con  $S_d$  lo spazio vettoriale dei polinomi omogenei di grado  $d$  in  $a_0, \dots, a_n$  e con  $S_{d,m} \subset S_d$  il sottospazio vettoriale dei polinomi isobari di peso  $m$ . Vale  $S_{d,m} \neq 0$  se e solo se  $0 \leq m \leq nd$ . Abbiamo visto (Esercizio 1.26) che le sottoalgebre di  $\mathbb{K}[a_0, \dots, a_n] = \bigoplus S_d$  non sono in generale finitamente generate. In questa sezione mostreremo invece che l'algebra dei covarianti è finitamente generata. Per fare ciò abbiamo bisogno di caratterizzare i covarianti su  $V_n$  come soluzioni di certe equazioni differenziali.

**Lemma 3.5.1.** *Il gruppo  $\mathrm{GL}(2, \mathbb{K})$  è generato dalle matrici triangolari inferiori e dalla matrice*

$$T = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

(Notare che  $T = T^{-1}$ .)

*Dimostrazione.* Basta osservare che per ogni scelta di coefficienti  $a, b, c, d$  con  $b \neq 0$  la matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} b & 0 \\ b - a & b \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

è triangolare inferiore. □

**Corollario 3.5.2.** *Il gruppo  $\mathrm{GL}(2, \mathbb{K})$  è generato dalle matrici diagonali invertibili e dalle matrici triangolari aventi 1 sulla diagonale.*

*Dimostrazione.* Evidente. □

Per ogni  $t \in \mathbb{K}$  definiamo

$$d(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad \delta(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

**Proposizione 3.5.3.** *Sia  $P \in \mathbb{K}[a_0, \dots, a_n]$  un polinomio omogeneo di grado  $d$  ed isobaro di peso  $\frac{1}{2}nd$ . Allora  $P$  è un covariante se e solo se  $d(t)P = \delta(t)P = P$  per ogni  $t \in \mathbb{K}$ .*

*Dimostrazione.* Le condizioni sul grado e sul peso equivalgono alla covarianza di  $P$  rispetto al sottogruppo delle matrici diagonali. Basta adesso applicare il Corollario 3.5.2. □

Studiamo adesso l'invarianza rispetto alle matrici triangolari superiori  $d(t)$ ; per quelle inferiori  $\delta(t)$  basterà scambiare  $x_0$  con  $x_1$  e  $a_i$  con  $a_{n-i}$ . Si noti che  $d(t)(P + Q) = d(t)P + d(t)Q$  e  $d(s)(d(t)P) = d(t + s)P$ .

Si osserva facilmente che lo spazio  $S_d$  è stabile per l'azione di  $\mathrm{GL}(2, \mathbb{K})$ , in particolare esiste un'applicazione polinomiale

$$\mathbb{K} \times S_d \rightarrow S_d, \quad (t, P) \mapsto d(t)P.$$

È possibile interpretare  $t$  come una indeterminata e quindi  $d(t)P \in \mathbb{K}[a_0, \dots, a_n, t]$ . Poiché  $d(0)P = P$  lo sviluppo di Taylor rispetto a  $t$  assume la forma

$$d(t)P = P + tP' + \frac{1}{2}t^2P'' + \dots + \frac{1}{d!}t^dP^{(d)},$$

dove  $P^{(i)} \in S_d$  e  $P' = \frac{\partial d(t)P}{\partial t} \Big|_{t=0}$ .

**Lemma 3.5.4.** *Nelle notazioni precedenti, vale  $d(t)P = P$  per ogni  $t \in \mathbb{K}$  se e solo se  $P' = 0$ .*

*Dimostrazione.* Una implicazione è ovvia. Se  $P' = 0$  allora per ogni  $c \in \mathbb{K}$  vale:

$$d(c+t)P = d(c)(d(t)P) = d(c)P + \frac{1}{2}(d(c)P'')t^2 + \dots$$

Dunque  $\frac{\partial}{\partial t}d(t)P|_{t=c} = 0$  e, siccome  $c$  è arbitrario, ne segue che  $d(t)P$  non dipende da  $t$ .  $\square$

Dato che  $d(t)P(a_0, \dots, a_n) = P(d(t)a_0, \dots, d(t)a_n)$  e

$$d(t)a_i = a_i + \binom{n}{i}^{-1} \binom{n}{i-1} (n-i+1)ta_{i-1} + \dots,$$

si ha  $a'_i = ia_{i-1}$  e, per la regola di derivazione della funzione composta,

$$P' = \sum_{i=0}^n \frac{\partial P}{\partial a_i} a'_i = \sum_{i=0}^n ia_{i-1} \frac{\partial P}{\partial a_i}.$$

La precedente relazione si può scrivere come  $P' = DP$ , dove  $D$  è l'operatore differenziale lineare del primo ordine

$$D = \sum_{i=0}^n ia_{i-1} \frac{\partial}{\partial a_i}.$$

Scambiando  $x_0$  con  $x_1$  e  $a_i$  con  $a_{n-i}$ , l'operatore  $D$  si trasforma nell'operatore

$$\Delta = \sum_{i=0}^n ia_{n-i+1} \frac{\partial}{\partial a_{n-i}} = \sum_{i=0}^n (n-i)a_{i+1} \frac{\partial}{\partial a_i}.$$

Notiamo che  $DS_{d,m} \subset S_{d,m-1}$  e  $\Delta S_{d,m} \subset S_{d,m+1}$ . È conveniente introdurre un operatore

$$H: S_{d,m} \rightarrow S_{d,m}, \quad HP = (nd - 2m)P.$$

Si estendono poi per linearità gli operatori  $H, D, \Delta$  ad operatori definiti su  $\mathbb{K}[a_0, \dots, a_n]$ : si verifica facilmente che  $H, D, \Delta$  sono  $\mathbb{K}$ -derivazioni e, per i risultati precedenti, un polinomio  $P$  appartiene all'algebra dei covarianti se e solo se  $HP = DP = \Delta P = 0$ .

**Lemma 3.5.5.** *Valgono le seguenti regole di commutazione:*

1.  $[D, \Delta] = D\Delta - \Delta D = H,$
2.  $[H, D] = 2D,$
3.  $[H, \Delta] = -2\Delta.$

*Dimostrazione.* Dimostriamo solo 1), la dimostrazione di 2) e 3) è simile ed è lasciata per esercizio. Essendo  $[D, \Delta]$  ed  $H$  entrambe derivazioni basta verificare la relazione sui generatori  $a_i$ : in tal caso vale

$$\begin{aligned} [D, \Delta]a_i &= D(n-i)a_{i+1} - \Delta ia_{i-1} = \\ &= ((i+1)(n-i) - i(n-i+1))a_i = (n-2i)a_i = Ha_i. \end{aligned}$$

$\square$

*Osservazione 3.5.6.* La maggior parte dei lettori avrà riconosciuto nel Lemma 3.5.5 le regole di commutazione dell'algebra di Lie  $\mathfrak{sl}(2)$  [Hum1973].

Lo scambio  $x_i \mapsto x_{1-i}$  di coordinate su  $V_1$  induce l'operatore

$$T: \mathbb{K}[a_0, \dots, a_n] \rightarrow \mathbb{K}[a_0, \dots, a_n], \quad T(a_i) = a_{n-i}.$$

Si osserva facilmente che  $TD = \Delta T$ ,  $T\Delta = DT$  e  $TH = -HT$ . Siano  $D^k: S_{d,m} \rightarrow S_{d,m-k}$  e  $\Delta^k: S_{d,m} \rightarrow S_{d,m+k}$  le iterate di  $D$  e  $\Delta$ .

**Lemma 3.5.7.** *Per ogni  $k > 0$  vale:*

1.  $[D^k, \Delta] = D^{k-1}(kH + k(k-1))$ .
2.  $[D, \Delta^k] = \Delta^{k-1}(kH - k(k-1))$ .

*Dimostrazione.* [1] Se  $k = 1$  ritroviamo esattamente il Lemma 3.5.5. Usando induzione su  $k$  e la regola di Leibniz per la derivata di Lie  $[AB, C] = A[B, C] + [A, C]B$ , si ottiene

$$\begin{aligned} [D^{k+1}, \Delta] &= D^k[D, \Delta] + [D^k, \Delta]D = \\ &= D^kH + D^{k-1}(kH + k(k-1))D = D^k((k+1)H + (k+1)k). \end{aligned}$$

[2] Si dimostra coniugando con l'operatore  $T$  l'uguaglianza al punto 1.  $\square$

**Teorema 3.5.8.** *Un polinomio  $P \in S_d$  è covariante se e solo se soddisfa due delle seguenti tre condizioni:*

1.  $HP = 0$ .
2.  $DP = 0$ .
3.  $\Delta P = 0$ .

*Dimostrazione.* Abbiamo già provato che un polinomio omogeneo  $P$  è un covariante se e solo se soddisfa le tre condizioni. Basta quindi dimostrare che due condizioni implicano la terza. Denotiamo con  $m = \frac{1}{2}nd$ .

[2] + 3)  $\Rightarrow$  1)] segue subito da  $[D, \Delta] = H$ .

[1] + 2)  $\Rightarrow$  3)]. Dalla condizione  $HP = 0$  segue che  $P$  è isobaro di peso  $m$ . Siccome  $S_{d,m+i} = 0$  per ogni  $i > m$ , esiste un intero  $k > 0$  tale che  $\Delta^k P = 0$  e  $\Delta^{k-1} P \neq 0$ . Allora vale  $0 = [D, \Delta^k]P = \Delta^{k-1}k(k-1)P$  da cui segue che  $k = 1$ .

[1] + 3)  $\Rightarrow$  2)]. Sia  $HP = \Delta P = 0$ , allora vale  $H(TP) = D(TP) = 0$  e per il punto precedente si ha  $\Delta(TP) = 0$ , da cui segue  $DP = 0$ .  $\square$

**Lemma 3.5.9.** *Siano  $d, k \geq 0$  interi fissati, poniamo  $m = \frac{1}{2}nd$  e sia  $Q \in S_{d,m-k}$  tale che  $DQ = 0$ . Allora per ogni  $i = 0, \dots, k$  vale*

$$D^i \Delta^k Q = \frac{(k+i)!}{(k-i)!} \Delta^{k-i} Q$$

ed in particolare

$$D^k \Delta^k Q = (2k)! Q$$

Si noti che nella formula appare solamente  $k$ .

*Dimostrazione.* Induzione su  $i$ : per  $i = 0$  non c'è nulla da dimostrare.

$$\begin{aligned}
 D^{i+1} \Delta^k Q &= \frac{(k+i)!}{(k-i)!} D \Delta^{k-i} Q \\
 &= \frac{(k+i)!}{(k-i)!} \Delta^{k-i-1} ((k-i)H - (k-i)(k-i-1))Q \\
 &= \frac{(k+i)!}{(k-i)!} (k-i) \Delta^{k-i-1} ((nd - 2(m-k)) - (k-i-1))Q \\
 &= \frac{(k+i)!}{(k-i)!} (k-i)(k+i+1) \Delta^{k-i-1} Q.
 \end{aligned}$$

□

**Proposizione 3.5.10.** *Siano  $Q, P_1, \dots, P_r$  forme covarianti su  $V_n$  di pesi  $q, m_1, \dots, m_r$  e siano  $A_1, \dots, A_r \in \mathbb{K}[a_0, \dots, a_n]$  tali che  $Q = \sum A_i P_i$ . Allora esistono covarianti  $B_1, \dots, B_r$  di pesi  $q - m_1, \dots, q - m_r$  tali che  $Q = \sum B_i P_i$ .*

*Dimostrazione.* Non è restrittivo supporre ogni polinomio  $A_i$  omogeneo ed isobaro di peso  $q - m_i$ , e quindi  $HA_i = 0$  per ogni  $i$ . Usando induzione su  $r$ , basta dimostrare che si può trovare una espressione del tipo  $Q = \sum B_i P_i$ , con  $B_1$  covariante; fatto questo si sostituisce  $Q$  con  $Q - B_1 P_1$ . Dimostriamo che tale espressione esiste per induzione sul minimo intero  $k$  tale che  $D^{k+1} A_1 = 0$ ; se  $k = 0$  allora  $A_1$  è un covariante e non c'è nulla da dimostrare. Se  $k > 0$ , denotiamo con  $R = D^k A_1$ ; per il Lemma 3.5.9 vale

$$D^k \Delta^k R = (2k)! R, \quad D^k \left( A_1 - \frac{1}{(2k)!} \Delta^k D^k A_1 \right) = 0.$$

Essendo i polinomi  $Q, P_1, \dots, P_r$  covarianti, per la regola di Leibniz vale

$$0 = \Delta^k D^k \left( \sum A_i P_i \right) = \sum (\Delta^k D^k A_i) P_i$$

e quindi

$$Q = \sum_{i=1}^r \left( A_i - \frac{1}{(2k)!} \Delta^k D^k A_i \right) P_i.$$

Si può adesso applicare l'ipotesi induttiva su  $k$  e trovare un'espressione con  $A_1$  covariante. □

Possiamo adesso dimostrare il teorema principale della sezione.

**Teorema 3.5.11 (Gordan 1868).** *L'algebra dei covarianti su  $V_n$  è finitamente generata su  $\mathbb{K}$ .*

La dimostrazione originale di Gordan e le semplificazioni dei contemporanei erano basate sul metodo simbolico e sulla rappresentazione dei covarianti come funzioni simmetriche delle differenze delle radici (cfr. [Hilb1993], [KR1984]). Di tali dimostrazioni sopravvive oggi un lemma sulla geometria dei coni poliedrali (Esercizio 4.33) di fondamentale importanza nello studio delle varietà toriche. La dimostrazione che presentiamo si deve sostanzialmente a David Hilbert e si basa sul seguente risultato la cui dimostrazione verrà data nella Sezione 4.3.

**Teorema 3.5.12 (Della base di Hilbert, 1890).** *Ogni ideale di  $\mathbb{K}[a_0, \dots, a_n]$  è finitamente generato.*

*Dimostrazione (del Teorema 3.5.11).* Sia  $I \subset \mathbb{K}[a_0, \dots, a_n]$  l'ideale generato dai covarianti di peso positivo, per il teorema della base di Hilbert  $I$  è generato da un numero finito  $P_1, \dots, P_r$  di covarianti. Sia  $Q$  un covariante di peso  $q$ , dimostriamo per induzione su  $q$  che si può scrivere  $Q$  come un polinomio nei  $P_i$  a coefficienti in  $\mathbb{K}$ . Se  $q \leq 0$  allora  $Q$  è una costante. Se  $q > 0$  allora  $Q \in I$  ed esistono  $A_1, \dots, A_r \in \mathbb{K}[a_0, \dots, a_n]$  tali che  $Q = \sum A_i P_i$ . Per la Proposizione 3.5.10 si può scrivere  $Q = \sum B_i P_i$  dove ogni  $B_i$  è un covariante di peso  $< q$  e quindi un polinomio nei  $P_i$ .  $\square$

Denotiamo con  $s_n(d, m)$  la dimensione su  $\mathbb{K}$  dello spazio vettoriale  $S_{d,m}$  e con  $w_n(d, m)$  la dimensione dello spazio vettoriale dei covarianti di peso  $m$  e grado  $d$ .

**Teorema 3.5.13.** *Vale la formula:*

$$w_n(d, m) = \begin{cases} s_n(d, m) - s_n(d, m-1) & \text{se } 2m = nd, \\ 0 & \text{altrimenti} \end{cases}$$

*Dimostrazione.* Basta dimostrare che se  $2m = nd$ , allora  $D: S_{d,m} \rightarrow S_{d,m-1}$  è surgettiva. Dimostriamo per induzione decrescente su  $k$  che  $D^k: S_{d,m} \rightarrow S_{d,m-k}$  è surgettiva per ogni  $k \geq 0$ . Se  $k > m$  il risultato è banale. Un semplice ragionamento di algebra lineare mostra che  $D^k$  è surgettiva se:

1.  $D^{k+1}$  è surgettiva e,
2. l'immagine di  $D^k$  contiene il nucleo di  $D: S_{d,m-k} \rightarrow S_{d,m-k-1}$ .

La 1) è vera per induzione mentre la 2) segue immediatamente dal Lemma 3.5.9.  $\square$

**Corollario 3.5.14.** *Sia  $2m = nd$ , allora  $w_n(d, m)$  è uguale al coefficiente di  $x^m$  nello sviluppo in serie di*

$$(1-x) \prod_{i=1}^d \frac{(1-x^{n+i})}{(1-x^i)}.$$

*Dimostrazione.* Se

$$\prod_{i=1}^d \frac{(1-x^{n+i})}{(1-x^i)} = \sum_{h=0}^{\infty} c_h x^h,$$

allora

$$(1-x) \prod_{i=1}^d \frac{(1-x^{n+i})}{(1-x^i)} = \sum_{h=0}^{\infty} (c_h - c_{h-1}) x^h.$$

Per il Teorema 3.5.13 basta quindi dimostrare che  $c_h = s_n(d, h)$ , per ogni  $h \geq 0$ . Sia

$$\phi(x, y) = \prod_{i=0}^n \left( \sum_{h=0}^{\infty} (x^i y)^h \right) = \prod_{i=0}^n \frac{1}{(1-x^i y)}.$$

Allora  $\phi(x, y) = \sum_{d,m} s_n(d, m) y^d x^m$ : infatti, il coefficiente di  $x^m y^d$  nello sviluppo di  $\phi$  coincide con il numero dei multiindici  $(i_0, \dots, i_n)$  di grado  $d$  e peso  $m$ . Si ha poi

$$(1-y)\phi(x, y) = \prod_{i=1}^n \frac{1}{(1-x^i y)} = (1-x^{n+1}y) \prod_{i=1}^{n+1} \frac{1}{(1-x^i y)} = (1-x^{n+1}y)\phi(x, xy).$$

Da tale equazione ne segue che, scrivendo  $\phi(x, y) = \sum G_i(x) y^i$ , vale  $G_0 = 1$  e

$$(1-y) \sum G_i(x) y^i = (1-x^{n+1}y) \sum G_i(x) x^i y^i.$$



Eguagliando i coefficienti di  $y^i$  si ottiene

$$G_i - G_{i-1} = G_i x^i - G_{i-1} x^{n+i}$$

e per induzione su  $i$  si deduce quindi che

$$G_i(x) = \frac{(1 - x^{n+i})}{(1 - x^i)} G_{i-1}(x) = \prod_{j=1}^i \frac{(1 - x^{n+j})}{(1 - x^j)}.$$

In particolare  $G_d(x) = \sum c_h x^h$  e la dimostrazione è conclusa.  $\square$

Nei prossimi esempi scriveremo  $\{f(x)\}_{x^i}$  per indicare il coefficiente di  $x^i$  nello sviluppo in serie di  $f(x)$ , cioè se  $f(x) = \sum a_i x^i$ , allora  $\{f(x)\}_{x^i} = a_i$ .

*Esempio 3.5.15.* Applichiamo il Corollario 3.5.14 per calcolare  $w_4(d, 2d)$ .

$$\begin{aligned} w_4(d, 2d) &= \left\{ (1-x) \prod_{i=1}^d \frac{(1-x^{4+i})}{(1-x^i)} \right\}_{x^{2d}} \\ &= \left\{ \frac{(1-x^{d+1})(1-x^{d+2})(1-x^{d+3})(1-x^{d+4})}{(1-x^2)(1-x^3)(1-x^4)} \right\}_{x^{2d}} \end{aligned}$$

Possiamo manipolare la formula togliendo termini che non influenzano il coefficiente di  $x^{2d}$ . Possiamo scrivere

$$\begin{aligned} w_4(d, 2d) &= \left\{ \frac{1-x^{d+1}-x^{d+2}-x^{d+3}-x^{d+4}}{(1-x^2)(1-x^3)(1-x^4)} \right\}_{x^{2d}} \\ &= \left\{ \frac{1}{(1-x^2)(1-x^3)(1-x^4)} \right\}_{x^{2d}} - \left\{ \frac{x(1+x+x^2+x^3)}{(1-x^2)(1-x^3)(1-x^4)} \right\}_{x^d}, \end{aligned}$$

dove abbiamo usato l'ovvio fatto che  $\{x^a \phi(x)\}_{x^b} = \{\phi(x)\}_{x^{b-a}}$ . Dato che  $1-x^4 = (1-x)(1+x+x^2+x^3)$  si ha:

$$\begin{aligned} w_4(d, 2d) &= \left\{ \frac{1}{(1-x^2)(1-x^3)(1-x^4)} \right\}_{x^{2d}} - \left\{ \frac{x}{(1-x^2)(1-x^3)(1-x)} \right\}_{x^d} \\ &= \left\{ \frac{1}{(1-x^2)(1-x^3)(1-x^4)} - \frac{x^2}{(1-x^2)(1-x^4)(1-x^6)} \right\}_{x^{2d}} \\ &= \left\{ \frac{1+x^3-x^2}{(1-x^2)(1-x^4)(1-x^6)} \right\}_{x^{2d}}. \end{aligned}$$

Siccome nello sviluppo del denominatore compaiono solo potenze pari di  $x$  si può togliere  $x^3$  dal numeratore e si ottiene la formula finale

$$w_4(d, 2d) = \left\{ \frac{1}{(1-x^4)(1-x^6)} \right\}_{x^{2d}} = \{(a, b) \in \mathbb{N}^2 \mid 4a + 6b = 2d\}.$$

Ricordiamo che i covarianti  $g_2^a g_3^b$  sono linearmente indipendenti e dalla formula precedente segue che quelli di grado  $d$  sono esattamente  $w_4(d, 2d)$ ; quindi  $g_2, g_3$  generano l'algebra dei covarianti di  $V_4$ .

**Proposizione 3.5.16.** *Siano  $Q \in \mathbb{K}[a_0, \dots, a_n]$ ,  $f_1, \dots, f_s \in V_n$ ,  $c_1, \dots, c_s \in \mathbb{K}$  tali che  $AQ(f_i) = Q(f_i^A) = c_i$  per ogni  $A \in \text{SL}(2, \mathbb{K})$  e per ogni  $i = 1, \dots, s$ . Allora esiste un SL-invariante  $P$  tale che  $P(f_i) = c_i$  per ogni  $i = 1, \dots, s$ .*

*Dimostrazione.* Per  $t \neq 0$  definiamo

$$h(t) = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \in \mathrm{SL}(2, \mathbb{K}).$$

Scriviamo  $Q = \sum Q_l$ , dove  $HQ_l = lQ_l$ : si verifica facilmente che  $h(t)Q = \sum t^l Q_l$  e quindi per ogni  $A \in \mathrm{SL}(2, \mathbb{K})$  fissato vale

$$h(t)Q(f_i^A) = \sum t^l Q_l(f_i^A) = c_i,$$

da cui segue che  $Q_0(f_i^A) = c_i$ . A meno di sostituire  $Q$  con  $Q_0$  si può supporre  $Q = Q_0$  e quindi  $HQ = 0$ . Dalla definizione degli operatori  $D$  e  $\Delta$  si ha che per ogni  $P \in \mathbb{K}[a_0, \dots, a_n]$  e per ogni  $f \in V_n$  vale

$$DP(f) = \frac{\partial}{\partial t|_{t=0}} d(t)P(f), \quad \Delta P(f) = \frac{\partial}{\partial t|_{t=0}} \delta(t)P(f)$$

da cui si deduce che  $DQ(f_i) = \Delta Q(f_i) = 0$  e, per induzione su  $k$ , che  $\Delta^k D^k Q(f_i) = 0$ . Sia  $k$  il più piccolo intero positivo tale che  $D^{k+1}Q = 0$ , allora, posto  $\hat{Q} = Q - \frac{1}{(2k)!} \Delta^k D^k Q$ , vale  $D^k(\hat{Q}) = 0$  e  $\hat{Q}(f_i^A) = c_i$ . La dimostrazione si conclude con la solita induzione decrescente su  $k$ .  $\square$

## Esercizi

**3.16.** Si provi che ogni fattore irriducibile di un covariante è covariante.

**3.17.** Sia  $n = 2d$  e sia  $a_{ij} = a_{i+j}$ , per  $0 \leq i, j \leq d$ . Dimostrare che il determinante  $P = \det(a_{ij})$  è un covariante non banale su  $V_n$ . (Sugg.: si consideri la matrice  $b_{ij} = a_{i+j} + t(i+j)a_{i+j-1}$ , provare che  $\det(b_{ij}) \equiv \det(a_{ij}) \pmod{t^2}$  e dedurre che  $P' = 0$ .)

**3.18.** Sia  $n = 4d$  e sia  $a_{ij} = (j-i)a_{i+j-1}$ ,  $0 \leq i, j \leq 2d+1$ , mostrare che il determinante e lo Pfaffiano della matrice  $(a_{ij})$  sono covarianti non banali su  $V_n$ . (Sugg.: vedi Esercizio 3.17.)

## 3.6 Esercizi complementari

**3.19.** Classificare i polinomi  $f \in \mathbb{C}[x]$  di grado  $n$  tali che

$$nf f'' = (n-1)(f')^2.$$

**3.20 (\*).** Un'applicazione ologomorfa fra due varietà complesse  $f: X \rightarrow Y$  si dice una immersione chiusa se è propria, iniettiva ed ha differenziale iniettivo in ogni punto.

Siano  $f_0, f_1, f_2 \in \mathbb{C}[x_0, x_1]$  omogenei di grado 3 senza zeri comuni: si provi che l'applicazione  $f: \mathbb{P}_{\mathbb{C}}^1 \rightarrow \mathbb{P}_{\mathbb{C}}^2$ , definita in coordinate omogenee da

$$f([x_0, x_1]) = [f_0(x_0, x_1), f_1(x_0, x_1), f_2(x_0, x_1)],$$

non è una immersione chiusa (Sugg.: usare 3.1.1.)

**3.21.** Sia  $d \geq 3$  un intero e  $p(x_0, x_1) = x_0^{d-1}x_1 - x_0x_1^{d-1}$ . Mostrare che le derivate parziali di  $p$  non hanno zeri comuni.

**3.22.** Siano  $f, g \in V_2$  forme binarie di grado 2 senza zeri comuni e sia  $J = f_1g_2 - f_2g_1 \in V_2$  il loro Jacobiano. Provare che le radici di  $fJ \in V_4$  formano una quaterna armonica.

**3.23 (Metodo di Hermite per l'integrazione delle funzioni razionali).** Siano  $\alpha_1, \dots, \alpha_r \in \mathbb{K}$  e  $a_1, \dots, a_r$  interi positivi. Per ogni  $p(t) \in \mathbb{K}[t]$  la funzione razionale

$$\frac{p(t)}{\prod_{i=1}^r (t - \alpha_i)^{a_i}}$$

si scrive in modo unico come somma di un polinomio e di una combinazione lineare delle funzioni razionali  $1/(t - \alpha_i)^j$ , per  $i = 1, \dots, r$  e  $1 \leq j \leq a_i$ . (Sugg.: sia  $m = \sum a_i$ ,  $f(t) = \prod (t - \alpha_i)^{a_i}$ , provare che le  $m$  funzioni razionali  $1/(t - \alpha_i)^j$  sono linearmente indipendenti in  $\mathbb{K}(t)$  e generano il sottospazio delle funzioni razionali  $g/f$  con  $g$  polinomio di grado  $< m$ .)

**3.24 (\*).** Sia  $\mathbb{K}$  campo di caratteristica 0. Dati  $n + 1$  polinomi  $f_0, \dots, f_n \in \mathbb{K}[x]$  sia  $W \in \mathbb{K}[x]$  il relativo determinante Wronskiano,

$$W = \begin{vmatrix} \partial^i f_j \\ \partial x^i \end{vmatrix} \quad i, j = 0, \dots, n$$

Provare che  $W = 0$  se e solo se  $f_0, \dots, f_n$  sono linearmente dipendenti in  $\mathbb{K}[x]$  (Sugg.: se i polinomi sono linearmente indipendenti e  $d_i$  è il grado di  $f_i$ , allora non è restrittivo assumere  $d_0 < d_1 < \dots < d_n$ : provare che la derivata  $(d_0 + \dots + d_n)$ -esima di  $W$  è diversa da 0.)

**3.25 (\*).** Sia  $A = (a_{ij})$ , per  $i, j = 0, \dots, n$ , la matrice di coefficienti

$$a_{ij} = (-1)^{n-i} \binom{n-j}{i}.$$

Dimostrare che  $A^3 = I$ . (Sugg.: studiare l'azione della proiettività  $x \mapsto -1/(x - 1)$  sulle forme binarie di grado  $n$ .)

**3.26.** Sia dato un polinomio monico  $f \in \mathbb{R}[t]$  di grado  $n$  e, per ogni  $h = 1, \dots, n$ , sia  $\psi_h \in \mathbb{K}$  la somma delle potenze  $h$ -esime delle radici di  $f$ ; gli Esercizi 3.7 e 3.8 forniscono una formula per esprimere  $\psi_1, \dots, \psi_n$  in funzione dei coefficienti di  $f$ , senza bisogno di calcolarne le radici.

Si consideri la matrice simmetrica  $B = (b_{ij})$ , per  $i, j = 0, \dots, n - 1$ , definita da  $b_{ij} = \psi_{i+j}$  (per convenzione  $\psi_0 = n$ ). Provare che il rango di  $B$  è uguale al numero di radici distinte di  $f$ . (Sugg.: dimostrare un risultato analogo per la matrice  $V$  di Vandermonde delle radici di  $f$  e osservare che  $B = VV^t$ .)

**3.27.** Una funzione  $f \in \mathbb{Z}[x_1, \dots, x_n]$  si dice antisimmetrica se per ogni permutazione  $\xi$  vale  $f(x_{\xi(1)}, \dots, x_{\xi(n)}) = (-1)^\xi f(x_1, \dots, x_n)$ . Mostrare che ogni funzione antisimmetrica è divisibile per il determinante della matrice di Vandermonde.

**3.28 (\*).** Sia  $\mathbb{K}$  un campo di caratteristica  $\neq 2$  e  $A \subset \mathbb{K}[x_0, \dots, x_n]$  la sottoalgebra delle funzioni invarianti per l'azione del gruppo alterno  $A_{n+1}$ . Provare che  $A$  è generata dalle funzioni simmetriche elementari e dal determinante della matrice di Vandermonde. (Sugg.: utilizzare l'Esercizio 3.27 oppure procedere così: per ogni  $a \geq 0$  scrivere

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ x_0^{a+1} & x_1^{a+1} & \dots & x_n^{a+1} \\ x_0^{a+2} & x_1^{a+2} & \dots & x_n^{a+2} \\ \vdots & \vdots & \ddots & \vdots \\ x_0^{a+n} & x_1^{a+n} & \dots & x_n^{a+n} \end{vmatrix} = P_a(x_0, \dots, x_n) - D_a(x_0, \dots, x_n)$$

dove  $P_a$  e  $D_a$  indicano le somme dei termini presenti nello sviluppo del determinante, relativi alle permutazioni di segnatura pari e dispari rispettivamente. Provare dapprima che  $A$  è generata dalle funzioni simmetriche e dalle funzioni  $D_a$ , per  $a \geq 0$ .)

**3.29 (Funzioni di Schur, \*).** Per ogni  $n$ -upla nondecrecente di numeri naturali  $\lambda : 0 \leq m_1 \leq m_2 \leq \dots \leq m_n$  la funzione

$$A_\lambda(x_1, \dots, x_n) = \begin{vmatrix} x_1^{m_1} & x_2^{m_1} & \dots & x_n^{m_1} \\ x_1^{m_2+1} & x_2^{m_2+1} & \dots & x_n^{m_2+1} \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{m_n+n-1} & x_2^{m_n+n-1} & \dots & x_n^{m_n+n-1} \end{vmatrix}$$

è antisimmetrica ed è quindi divisibile per il determinante della matrice di Vandermonde  $V(x_1, \dots, x_n)$  (vedi Esercizio 3.27). Le funzioni (dette *di Schur*)

$$S_\lambda := \frac{A_\lambda(x_1, \dots, x_n)}{V(x_1, \dots, x_n)}$$

sono quindi simmetriche. Provare che le funzioni di Schur sono una  $\mathbb{Z}$ -base dello spazio di tutte le funzioni simmetriche. Mostrare inoltre che  $\sigma_i = S_{(0, \dots, 0, 1, \dots, 1)}$  e che  $\psi_h = S_{(0, \dots, 0, h)}$ . (Sugg.: la funzione  $S_{(m_1, \dots, m_n)}$  è omogenea di grado  $m_1 + \dots + m_n$  ed ha  $x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}$  come addendo di peso più alto.)

**3.30.** Sia  $p \in \mathbb{Z}[t]$  un polinomio monico,  $p(t) = \prod_i (t - \alpha_i)$ , con  $\alpha_i \in \mathbb{C}$ . Provare che se tutte le radici  $\alpha_i$  hanno norma 1, allora sono radici dell'unità. (Sugg.: i polinomi  $p_k(t) = \prod_i (t - \alpha_i^k)$ , per  $k \in \mathbb{Z}$ , sono in numero finito.)

**3.31.** Provare che il gruppo  $GL(n, \mathbb{K})$  è generato dalle matrici triangolari.

**3.32.** Determinare un insieme minimale di generatori della sottoalgebra di  $\mathbb{Q}[x_0, \dots, x_3]$  formata dalle funzioni invarianti per l'azione del gruppo trirettangolo.

**3.33 (\*).** Un modo alternativo per dimostrare che ogni covariante  $p(a_0, \dots, a_4)$  di grado  $d$  su  $V_4$  si può scrivere come polinomio in  $g_2$  e  $g_3$ , si ottiene dimostrando nell'ordine i seguenti punti:

1. Se  $d$  è dispari, allora  $p(0, 1, 0, -1, 0) = 0$ .
2. Se  $d = 2h$ , allora a meno di sostituire  $p$  con  $p - cg_2^h$  per un'opportuna costante  $c$  si può supporre  $p(0, 1, 0, -1, 0) = 0$ .
3. Se  $p(0, 1, 0, -1, 0) = 0$ , allora  $p$  si annulla su tutte le forme le cui radici formano una quaterna armonica.
4. Se  $p(0, 1, 0, -1, 0) = 0$ , allora  $g_3$  divide  $p$ . (Sugg.: siccome  $-4g_3 = 4a_3^2 - h_2a_2 - h_3$ , con  $h_2, h_3 \in \mathbb{K}[a_0, a_1, a_3, a_4]$ , per la divisione euclidea si può scrivere  $p = qg_3 + r$  con  $r$  di grado  $\leq 2$  rispetto alla variabile  $a_2$ . Immergere  $\mathbb{K}$  in una chiusura algebrica e considerare le famiglie ad un parametro di forme  $f + tx_0^2x_1^2$  per provare, utilizzando la Proposizione 3.4.6, che  $(g_2^3 - 27g_3^2)(h_2^3 - 27h_3^2)r = 0$ .)

**3.34 (\*).** Dimostrare che

$$w_2(d, d) = \left\{ \frac{1}{(1-x^2)} \right\}_{x^d}, \quad w_3\left(d, \frac{3}{2}d\right) = \left\{ \frac{1}{(1-x^4)} \right\}_{x^d}.$$

(Sugg.: vedi [Hilb1993].)

**3.35.** Caratterizzare  $s_n(d, m)$  come il numero di sottotabelle  $S$  di una tabella rettangolare  $n \times d$  tali che:

1.  $S$  contiene  $m$  elementi.
2. Se  $(i, j) \in S$  allora  $(h, l) \in S$  per ogni  $h \leq i, l \leq j$ .

Dedurne le **leggi di reciprocità di Hermite**:  $s_n(d, m) = s_d(n, m)$  e  $w_n(d, m) = w_d(n, m)$ .

*Osservazione 3.6.1.* Una sottotabella  $S$  definita come sopra viene detta anche **Diagramma di Young**.

**3.36.** Dimostrare le leggi di reciprocità di Hermite utilizzando il Corollario 3.5.14.

**3.37.** Una forma binaria  $f$  si dice:

- *instabile* se  $P(f) = 0$  per ogni covariante  $P$  di grado positivo. (il termine instabile è recente, la denominazione precedente era *nullform*).
- *semistabile* se non è instabile.
- *stabile* se è semistabile e se  $\{A \in \text{SL}(2, \mathbb{K}) \mid f^A = f\}$  è un sottogruppo finito di  $\text{SL}(2, \mathbb{K})$ .

Si diano esempi di forme stabili, instabili e semistabili nonstabili. Si classifichino inoltre le forme binarie di grado  $\leq 4$  secondo le precedenti definizioni.

**3.38 (I Cumulanti).** Sia  $\mathbb{K}$  algebricamente chiuso di caratteristica 0 e sia  $V$  lo spazio affine dei polinomi monici di grado  $n$  nella variabile  $x$ . Dato  $f = \prod_{i=1}^n (x - \lambda_i) = x^n - \sigma_1 x^{n-1} + \dots + (-1)^n \sigma_n$ , si definisce per ogni  $k \geq 0$

$$s_k = \frac{1}{n} \sum_{i=1}^n \lambda_i^k = s_k(\sigma_1, \dots, \sigma_n), \quad s_0 = 1, s_1 = \frac{1}{n} \sigma_1, \dots$$

$$\sum_{k=1}^{\infty} c_k \frac{t^k}{k} = \log \left( \sum_{k=0}^{\infty} s_k \frac{t^k}{k!} \right)$$

Si provi che per ogni  $k \geq 2$ ,  $c_k(\sigma_1, \dots, \sigma_n)$  è un covariante per l'azione naturale su  $V$  del gruppo delle affinità di  $\mathbb{K}$  in sé.

**3.39.** Provare che non esistono covarianti nonbanali di grado 3 su  $V_{22}$ .

**3.40.** Sia  $R_m \subset \mathbb{K}[a_0, \dots, a_n]$  lo spazio dei covarianti di peso  $m$  e siano  $P_1 \in R_{m_1}, \dots, P_d \in R_{m_d}$  un insieme di generatori dell'algebra  $\bigoplus_{k \geq 0} R_k$ . Detto  $N$  il prodotto di  $d$  e del minimo comune multiplo di  $m_1, \dots, m_d$ , provare che  $\bar{R}_N$  genera la sottoalgebra  $\bigoplus_{k \geq 0} R_{kN}$ .

**3.41 (Azioni di Nagata).** Si consideri la naturale azione lineare del gruppo  $\text{SL}(m, \mathbb{K})$  sullo spazio vettoriale  $S = \mathbb{K}[x_1, \dots, x_m]$  e per ogni sottogruppo  $G \subset \text{SL}(m, \mathbb{K})$  denotiamo con  $S^G \subset S$  la  $\mathbb{K}$ -algebra dei polinomi invarianti per l'azione di  $G$  indotta. Si osservi ad esempio che se  $m = 2$  e  $G = \text{SL}(2, m)$  allora  $S^G = \mathbb{K}$  mentre se  $G$  è il gruppo delle matrici diagonali a determinante 1 allora  $S^G$  è la sottoalgebra generata da  $x_1 x_2 \dots x_m$ . Consideriamo adesso il caso  $m = 2n$ , scriviamo  $S = \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_n]$  e prendiamo come  $G$  l'immagine di  $\rho: \mathbb{K}^n \rightarrow \text{SL}(2n, \mathbb{K})$

$$\rho(t_1, \dots, t_n) \begin{cases} x_i \mapsto x_i \\ y_i \mapsto y_i + t_i x_i \end{cases}$$

Provare che:

- 1) Rispetto alla struttura additiva su  $\mathbb{K}^n$ ,  $\rho$  è un omomorfismo iniettivo di gruppi.
- 2)  $S^G = \mathbb{K}[x_1, \dots, x_n]$ .

Identifichiamo tramite  $\rho$  il sottogruppo  $G$  con  $\mathbb{K}^n$  e sia  $V \subset S^G$  un sottospazio vettoriale

di dimensione  $s$ .

3) Esiste una decomposizione in somma diretta  $S^V = \oplus S_{d_1, \dots, d_n, d}^V$ , con  $d_1, \dots, d_n, d \in \mathbb{N}$  e dove ogni  $f \in S_{d_1, \dots, d_n, d}^V$  è combinazione lineare di monomi della forma  $x_1^{i_1} \cdots x_n^{i_n} y_1^{j_1} \cdots y_n^{j_n}$ , con  $i_h + j_h = d_h$  e  $j_1 + j_2 + \cdots + j_n = d$ .

4) Se  $s < n$  e  $(a_{i1}, \dots, a_{in}) \in \mathbb{K}^n$ , per  $i = 1, \dots, s$ , è una base di  $V$ , allora i determinanti minori di ordine  $s + 1$  della matrice

$$\begin{pmatrix} a_{11}x_1 & \cdots & a_{1n}x_n \\ \vdots & \ddots & \vdots \\ a_{s1}x_1 & \cdots & a_{sn}x_n \\ y_1 & \cdots & y_n \end{pmatrix}$$

appartengono a  $S_{1,1,\dots,1}$ .

*Osservazione 3.6.2.* In uno dei suoi celebri problemi (il 14°), David Hilbert si chiedeva se per ogni sottogruppo algebrico<sup>1</sup>  $G \subset \text{SL}(m, \mathbb{K})$ , la sottoalgebra  $S^G$  fosse sempre finitamente generata: egli stesso aveva dimostrato la finita generazione in molti casi particolari. Il problema ha avuto risposta negativa nel 1958 ad opera del matematico giapponese Nagata il quale, nelle notazioni dell'Esercizio 3.41, dimostrò che per  $n = 16$  esistevano sottospazi  $V$  di dimensione 13 per i quali  $S^V$  non è finitamente generata. Nel 2001 Mukai ha trovato ulteriori esempi con  $n = 9$  e  $s = 3$ . È stato inoltre dimostrato che se  $s \leq 2$  l'algebra  $S^V$  è finitamente generata e per  $s = 1$  è facile descriverne i generatori: vedi in proposito l'Esercizio 18.1.

<sup>1</sup> Algebrico significa che è formato dalle matrici i cui coefficienti soddisfano un opportuno insieme di equazioni algebriche, ad esempio formano un sottogruppo algebrico le matrici ortogonali e le matrici triangolari con tutti 1 sulla diagonale principale

## Teoria elementare dell'eliminazione

Nello studio delle soluzioni di un sistema di equazioni algebriche

$$f_i(x_1, \dots, x_n) = 0, \quad i = 1, \dots, m, \quad f_i \in \mathbb{K}[x_1, \dots, x_n],$$

è naturale adottare alcune manipolazioni algebriche in modo da ottenere nuove equazioni di più facile comprensione; un caso tipico è il metodo di riduzione a forma trapezoidale dei sistemi di equazioni lineari (eliminazione di Gauss). È generalmente utile considerare delle espressioni  $g_j = \sum h_{ji} f_i$  nelle quali alcune delle variabili  $x_1, \dots, x_n$  non compaiono. Le ricette per esplicitare, se esistono, dei polinomi  $g_j$  come sopra fanno parte della teoria dell'eliminazione. In termini un po' più astratti possiamo dire che la teoria dell'eliminazione si occupa del seguente problema.

*Dato un anello  $A$  ed un ideale  $I \subset A[x_1, \dots, x_n]$ , determinare quando l'ideale  $I \cap A$  è diverso da 0, ed in tal caso esplicitarne elementi non banali.*

Lo strumento "basic" per eccellenza in teoria dell'eliminazione è il risultante, con il quale si riesce a dare una risposta più che soddisfacente al suddetto problema nel caso  $n = 1$ . Il risultante sarà inoltre uno degli strumenti tecnici più usati nel resto di queste note. Il risultato di maggior rilievo teorico in teoria dell'eliminazione è invece il teorema degli zeri di Hilbert, del quale daremo una dimostrazione nella Sezione 4.5.

### 4.1 Il risultante di due polinomi

Sia  $A$  un anello e siano  $m, n$  due interi positivi fissati. Indichiamo con  $M \subset A[x]$  il sottomodulo libero dei polinomi di grado  $\leq n+m-1$ . Identifichiamo  $M$  con  $A^{n+m}$  tramite l'isomorfismo di  $A$ -moduli che associa ad ogni vettore riga  $p = (a_0, \dots, a_{n+m-1}) \in A^{n+m}$  il polinomio  $p = \sum a_i x^{n+m-1-i} \in M$ .

Sia dato un insieme ordinato di  $n+m$  polinomi  $p_0, \dots, p_{n+m-1} \in M$ , rappresentati dai vettori riga  $p_i = (a_{i,0}, \dots, a_{i,n+m-1})$ ; è allora possibile considerare la matrice quadrata  $\Delta = (a_{i,j})$  ed il suo determinante  $J(p_0, \dots, p_{n+m-1}) = \det(\Delta)$ .

**Proposizione 4.1.1.** *Nelle notazioni precedenti, dati  $p_0, \dots, p_{n+m-1} \in M$ , esistono  $c_0, \dots, c_{n+m-1} \in A$  tali che*

$$J(p_0, \dots, p_{n+m-1}) = c_0 p_0 + \dots + c_{n+m-1} p_{n+m-1}.$$

*Dimostrazione.* Siano  $\Delta^i$  i vettori colonna della matrice  $\Delta$ , allora vale

$$P = \begin{pmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n+m-1} \end{pmatrix} = \Delta^0 x^{n+m-1} + \Delta^1 x^{n+m-2} + \dots + \Delta^{n+m-1}.$$





6. Esistono  $F, G \in A[x]$  polinomi tali che  $\deg(F) \leq n-1$ ,  $\deg(G) \leq m-1$  e  $R_{n,m}(f, g) = Gf + Fg$ ; in particolare  $R(f, g)$  appartiene all'ideale generato da  $f$  e  $g$ .
7. Se  $f$  è monico di grado  $n$  e  $(a_{ij})$  è la matrice quadrata di ordine  $n$  a coefficienti in  $A$  tale che per ogni  $i = 0, \dots, n-1$  vale

$$x^i g = h_i f + \sum_{j=0}^{n-1} a_{ij} x^j, \quad \text{con } h_i \in A[x],$$

allora  $R(f, g) = \det(a_{ij})$ . In particolare per ogni polinomio monico  $f$  il risultante  $R(f, g)$  dipende solo dalla classe di  $g$  in  $A[x]/(f)$ .

*Dimostrazione.* Le proprietà 1, 2, 3, 4 e 5 seguono da 4.1 e dalle proprietà elementari del determinante, mentre 6 è una conseguenza immediata della Proposizione 4.1.1. Per il punto 7 basta osservare che, se  $m$  è il grado di  $g$ , allora ogni polinomio  $h_i f$  è una combinazione lineare a coefficienti in  $A$  di  $f, xf, \dots, x^{m-1}f$ . È dunque possibile sommare ad ognuna delle ultime  $n$  righe della matrice  $S_{n,m}(f, g)$  dei multipli delle prime  $m$  righe in modo tale che diventi una matrice della forma

$$\begin{pmatrix} T & * \\ 0 & a_{ij} \end{pmatrix},$$

dove  $T$  è una matrice triangolare superiore di ordine  $m$  con i coefficienti della diagonale tutti uguali a 1.  $\square$

La matrice  $S_{n,m}(f, g)$  si dice **matrice di Sylvester** della coppia  $(f, g)$  e l'espressione del risultante come determinante di  $S_{n,m}(f, g)$  viene detta formula di Sylvester.

Il risultante è chiaramente funtoriale in  $A$ : ciò significa che, se  $\phi: A \rightarrow B$  è un omomorfismo di anelli, allora  $\phi$  si estende naturalmente ad un omomorfismo  $\phi: A[x] \rightarrow B[x]$  tale che  $\phi(x) = x$  e vale  $R(\phi(f), \phi(g)) = \phi(R(f, g))$ .

**Proposizione 4.1.3 (Invarianza per traslazione).** Per ogni  $f, g \in A[x]$  e per ogni  $a \in A$  vale

$$R(f(x-a), g(x-a)) = R(f(x), g(x)).$$

*Dimostrazione.* Sia  $M_d \subset A[x]$  il modulo dei polinomi di grado  $\leq d-1$ ; il modulo  $M_d$  è libero ed ha come una base canonica  $1, x, \dots, x^{d-1}$ . Il risultante è esattamente il determinante dell'applicazione

$$M_m \oplus M_n \rightarrow M_{n+m}, \quad (p, q) \mapsto fp + gq,$$

calcolato rispetto alle basi canoniche. Basta quindi osservare che l'isomorfismo di traslazione  $T_a: A[x] \rightarrow A[x]$ , dove  $T_a(x) = x-a$  e  $T_a(b) = b$  per ogni  $b \in A$ , preserva i sottomoduli  $M_d$  e su ciascuno di essi si rappresenta nella base canonica con una matrice triangolare con tutti 1 sulla diagonale ed ha quindi determinante 1.  $\square$

**Corollario 4.1.4.** Siano  $f, g \in A[x]$  polinomi. Se  $f = a_0 \prod_{i=1}^n (x - \alpha_i)$ , allora

$$R_{n,m}(f, g) = a_0^m \prod_{i=1}^n g(\alpha_i)$$

e quindi se  $g = b_0 \prod_{i=1}^m (x - \beta_i)$ , allora vale

$$R_{n,m}(f, g) = a_0^m b_0^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j).$$

In particolare valgono le relazioni di bilinearità:

$$R_{n+n',m}(ff', g) = R_{n,m}(f, g)R_{n',m}(f', g), \quad R_{n,m+m'}(f, gg') = R_{n,m}(f, g)R_{n,m'}(f, g').$$

*Dimostrazione.* Per la Proposizione 4.1.2 non è restrittivo supporre  $a_0 = 1$ ; dimostriamo che vale  $R_{n,m}(f, g) = a_0^m \prod_{i=1}^n g(\alpha_i)$  per induzione su  $n$ : se  $n = 0$  non c'è nulla da dimostrare. Sia dunque  $n > 0$  e scriviamo  $f = (x - \alpha_1)f'$ ; l'invarianza per traslazione dà

$$R_{n,m}(f, g) = R_{n,m}((x - \alpha_1)f'(x), g(x)) = R_{n,m}(xf'(x + \alpha_1), g(x + \alpha_1)),$$

e per 4.1.2 si ha dunque

$$R_{n,m}(f, g) = g(\alpha_1)R_{n-1,m}(f'(x + \alpha_1), g(x + \alpha_1)) = g(\alpha_1)R_{n-1,m}(f'(x), g(x)).$$

Le relazioni di bilinearità sono chiaramente funtoriali, si può quindi assumere senza perdita di generalità che  $A = \mathbb{Z}[a_i, a'_i, b_i]$  dove  $a_i, a'_i, b_i$  sono indeterminate che rappresentano i coefficienti di  $f, f'$  e  $g$ . Dunque non è restrittivo assumere  $A$  dominio di integrità. Basta adesso immergere  $A$  in una chiusura algebrica del suo campo delle frazioni per avere la completa riducibilità di  $f, f'$  e  $g$ . La dimostrazione della bilinearità è allora una conseguenza immediata della rappresentazione di  $R$  come funzione della differenza delle radici.  $\square$

**Corollario 4.1.5.** *Sia  $A$  un dominio a fattorizzazione unica e  $f, g \in A[x]$ . Allora  $f$  e  $g$  possiedono un fattore comune di grado positivo se e solo se  $R(f, g) = 0$ .*

*Dimostrazione.* Sia  $\mathbb{K}$  la chiusura algebrica del campo delle frazioni di  $A$ , è allora ben noto che  $f$  e  $g$  hanno un fattore comune di grado positivo se e solo se hanno una radice comune in  $\mathbb{K}$ . La tesi segue immediatamente da 4.1.4.  $\square$

**Proposizione 4.1.6.** *Sia  $R_{n,m} \in \mathbb{Z}[a_0, \dots, a_n, b_0, \dots, b_m]$  il risultante universale, cioè il determinante della matrice di Sylvester (4.1) i cui coefficienti  $a_i, b_j$  sono elementi algebricamente indipendenti. Se le variabili  $a_i, b_i$  hanno grado 1 e peso  $i$ , allora  $R_{n,m}$  è omogeneo di grado  $n + m$  ed isobaro di peso  $nm$ .*

*Dimostrazione.* Sia  $S_{n,m}$  la matrice di Sylvester universale (4.1), moltiplicare  $a_i$  e  $b_i$  per  $t^i$  equivale a eseguire nell'ordine le seguenti operazioni:

- 1) moltiplicare per  $t^i$  la  $i$ -esima colonna di  $S_{n,m}$ .
- 2) dividere per  $t^i$  la  $i$ -esima riga di  $S_{n,m}$  se  $i \leq m$ .
- 3) dividere per  $t^{i-m}$  la  $i$ -esima riga di  $S_{n,m}$  se  $i > m$ .

Alla fine il determinante di  $S_{n,m}$  risulta moltiplicato per  $t^e$ , dove

$$e = \sum_{i=1}^{n+m} i - \sum_{i=1}^m i - \sum_{i=1}^n i = nm.$$

$\square$

**Lemma 4.1.7.** *Sia  $A$  un dominio di integrità e  $0 \neq \mathfrak{p} \subset A[x]$  un ideale primo tale che  $\mathfrak{p} \cap A = 0$ . Sia  $\mathbb{K}$  il campo delle frazioni di  $A$  e sia  $\mathfrak{p}^e \subset \mathbb{K}[x]$  l'ideale generato da  $\mathfrak{p}$ . Allora  $\mathfrak{p}^e$  è un ideale primo e  $\mathfrak{p}^e \cap A[x] = \mathfrak{p}$ .*

*Dimostrazione.* Si prova facilmente che  $\mathfrak{p}^e = \left\{ \frac{p}{a} \mid p \in \mathfrak{p}, a \in A - \{0\} \right\}$ . Sia  $\frac{p_1}{a_1} \frac{p_2}{a_2} \in \mathfrak{p}^e$  con  $p_i \in A[x]$  e  $a_i \in A$ ; allora esiste  $a \in A - \{0\}$  tale che  $ap_1p_2 \in \mathfrak{p}$ . Siccome  $\mathfrak{p} \cap A = 0$  deve essere  $p_1 \in \mathfrak{p}$  oppure  $p_2 \in \mathfrak{p}$ ; questo prova che  $\mathfrak{p}^e$  è primo. Sia  $q \in \mathfrak{p}^e \cap A[x]$ , come sopra esiste  $a \in A - \{0\}$  tale che  $aq \in \mathfrak{p}$  e quindi  $q \in \mathfrak{p}$ .  $\square$

**Lemma 4.1.8.** *Siano  $A, \mathfrak{p} \subset A[x]$  come nel Lemma 4.1.7. Allora esiste  $f \in \mathfrak{p}$  tale che  $R(f, g) \neq 0$  per ogni  $g \notin \mathfrak{p}$ .*

*Dimostrazione.* Per il Lemma 4.1.7 esiste  $f \in \mathfrak{p}$  irriducibile in  $\mathbb{K}[x]$  tale che  $\mathfrak{p}^e = (f) \subset \mathbb{K}[x]$ . Essendo  $g \notin \mathfrak{p}^e$  si ha  $R(f, g) \neq 0$ .  $\square$

**Teorema 4.1.9.** *Sia  $A$  un anello,  $\mathfrak{p} \subset A[x]$  un ideale primo e  $\mathfrak{q} = A \cap \mathfrak{p}$ . Se  $\mathfrak{p} \neq \mathfrak{q}[x]$ , allora esiste  $f \in \mathfrak{p}$  tale che  $R(f, g) \notin \mathfrak{q}$  per ogni  $g \notin \mathfrak{p}$ .*

*Dimostrazione.* Siccome  $\mathfrak{q}[x] \subset \mathfrak{p}$ , l'immagine di  $\mathfrak{p}$  in  $(A/\mathfrak{q})[x] = A[x]/\mathfrak{q}[x]$  è un ideale primo che soddisfa le ipotesi del Lemma 4.1.8.  $\square$

**Corollario 4.1.10.** *Siano  $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset A[x]$  ideali primi tali che  $1 \notin \mathfrak{p}_2$  e  $\mathfrak{p}_1$  contenga un polinomio monico. Allora  $\mathfrak{p}_1 \cap A = \mathfrak{p}_2 \cap A$  se e solo se  $\mathfrak{p}_1 = \mathfrak{p}_2$ .*

*Dimostrazione.* Sia  $\mathfrak{q} = \mathfrak{p}_1 \cap A = \mathfrak{p}_2 \cap A$ , siccome  $\mathfrak{q}$  è un ideale proprio di  $A$ ,  $\mathfrak{q}[x]$  non contiene polinomi monici e quindi  $\mathfrak{q}[x] \neq \mathfrak{p}_1$ . Se per assurdo esistesse  $g \in \mathfrak{p}_2 - \mathfrak{p}_1$ , allora per il Teorema 4.1.9 esisterebbe  $f \in \mathfrak{p}_1$  tale che  $R(f, g) \notin \mathfrak{q}$  in contraddizione con il fatto che  $R(f, g) \in (f, g) \subset \mathfrak{p}_2$ .  $\square$

## Esercizi

**4.1 ( $k$ -risultanti).** Sia  $A$  un dominio a fattorizzazione unica,  $f, g \in A[x]$  polinomi,  $\deg(f) = n$ ,  $\deg(g) = m$ . Per ogni  $k \geq 0$  si definisce il  $k$ -risultante  $R_k(f, g)$  come il determinante della matrice quadrata di ordine  $n + m - 2k$  ricavata eliminando dalla matrice di Sylvester  $S_{n,m}(f, g)$  le righe  $1, 2, \dots, k, m + 1, \dots, m + k$  e le colonne  $1, 2, \dots, k, n + m, n + m - 1, \dots, n + m - k + 1$ .

Dimostrare che  $f$  e  $g$  hanno un fattore comune di grado  $> k$  se e solo se  $R_0(f, g) = R_1(f, g) = \dots = R_k(f, g) = 0$ . (Sugg.: induzione su  $k$ : la condizione  $R_k(f, g) = 0$  equivale all'esistenza di due polinomi  $A_k, B_k$  di grado  $< m - k, n - k$  rispettivamente tali che  $A_k f + B_k g$  ha grado  $< k$ .)

**4.2.** Calcolare esplicitamente il risultante di due polinomi di secondo grado.

**4.3.** Sia  $A$  un dominio di integrità,  $f, g \in A[x]$  e  $s \in (f, g) \cap A$ . Provare che  $s^3 \in (f^2, g^2) \cap A$  e che  $R(f^2, g^2) = R(f, g)^4$ . Dedurre che, in generale, il risultante non genera l'ideale contratto  $(f, g) \cap A$ .

## 4.2 Il discriminante

Per semplicità espositiva consideriamo esclusivamente il caso in cui  $A$  è un dominio di integrità perfetto oppure di caratteristica sufficientemente alta, lasciando le possibili generalizzazioni per esercizio al lettore interessato.

Dato un polinomio  $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n \in A[x]$ , con  $a_0 \neq 0$ , e considerando la sua derivata formale  $f'(x) = n a_0 x^{n-1} + \dots + a_{n-1}$  si osserva che la prima colonna della matrice di Sylvester della coppia  $(f, f')$  è divisibile per  $a_0$ . Esiste dunque unico un elemento  $\Delta(f) \in A$  detto **discriminante** di  $f$ , tale che

$$\Delta(f) = \frac{1}{a_0} R(f, f') = \frac{1}{a_0} R(f', f).$$

Se  $A$  è un dominio a fattorizzazione unica, segue dal Corollario 4.1.5 che  $f$  possiede un fattore multiplo di grado positivo se e solo se  $\Delta(f) = 0$ . Come conseguenza immediata della Proposizione 4.1.6 abbiamo che, se  $A = \mathbb{K}[a_0, \dots, a_n]$ , allora il discriminante di  $a_0 x^n + \dots + a_n$  è un polinomio omogeneo di grado  $2n - 2$  ed isobaro di peso  $n(n - 1)$ . Dato

che la derivazione rispetto ad  $x$  ed il risultante commutano con le traslazioni  $x \mapsto x - a$ , si ha  $\Delta(f(x)) = \Delta(f(x-a))$  per ogni  $a \in A$ ; dai risultati del Capitolo 3 segue dunque che  $\Delta$  è un covariante. Per confrontare la presente definizione di  $\Delta$  con quella data a Pagina 44 come funzione delle differenze delle radici, scriviamo

$$f = a_0 \prod_{i=1}^n (x - \alpha_i), \quad f' = a_0 \sum_{i=1}^n \prod_{j \neq i} (x - \alpha_j)$$

da cui  $f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j)$  e, per il Corollario 4.1.4, si ha

$$\Delta(f) = a_0^{-1} R(f, f') = a_0^{n-2} \prod_{i=1}^n f'(\alpha_i) = a_0^{2n-2} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Naturalmente, se  $\beta_1, \dots, \beta_{n-1}$  sono le radici della derivata  $f'$ , allora vale anche la formula  $\Delta(f) = n^n a_0^{n-1} \prod f(\beta_i)$ .

*Esempio 4.2.1.* (caratteristica  $\neq 2$ ) Se  $f = ax^2 + bx + c$ , allora  $-\frac{b}{2a}$  è la radice di  $f'$  e vale

$$\Delta(f) = 2^2 a f \left( -\frac{b}{2a} \right) = 4ac - b^2.$$

*Esempio 4.2.2.* (caratteristica  $\neq 2, 3$ ) Se  $f = x^3 - px - q$ , allora le radici di  $f'$  sono  $\pm \sqrt{\frac{p}{3}}$  e quindi il discriminante vale

$$\Delta(f) = 27 f \left( \sqrt{\frac{p}{3}} \right) f \left( -\sqrt{\frac{p}{3}} \right) = 27q^2 - 4p^3.$$

*Esempio 4.2.3.* Per la Proposizione 4.1.2, vale  $\Delta(x^n + a) = n^n a^{n-1}$ .

Un utile trucco per calcolare  $\Delta(f)$  quando  $f$  è un polinomio monico, consiste nell'applicare l'algoritmo euclideo per determinare il massimo comune divisore fra  $f$  e  $f'$  e poi moltiplicare per uno scalare in modo da avere la relazione dell'Esempio 4.2.3 soddisfatta. Ad esempio se  $f = x^4 + cx^2 + bx + a$  si ha  $27\Delta(f) = 4(c^2 + 12a)^3 - (2c^3 - 72ac + 27b^2)^2$ .

## Esercizi

**4.4.** Siano  $\mathbb{K}$  un campo perfetto e  $f, g \in \mathbb{K}[x]$  polinomi senza fattori comuni. Dimostrare che vale una delle seguenti possibilità:

1. Il polinomio  $tf(x) + g(x)$  ha radici multiple per al più finiti valori di  $t \in \mathbb{K}$ .
2. La caratteristica di  $\mathbb{K}$  è  $p > 0$  ed esistono  $\tilde{f}, \tilde{g} \in \mathbb{K}[x]$  tali che  $f = \tilde{f}^p, g = \tilde{g}^p$ .

**4.5.** (caratteristica 0) Sia  $A$  un dominio di integrità di caratteristica 0 e  $f \in A[x]$  un polinomio di grado  $n$ . Provare che

$$\Delta(f) = \frac{R_{n-1, n-1}(nf - xf', f')}{n^{n-1}}.$$

### 4.3 Anelli Noetheriani

In questa sezione dimostreremo il teorema della base di Hilbert. Per future applicazioni è conveniente inquadrare il teorema in un ambito più astratto di quello considerato precedentemente.

**Definizione 4.3.1.** *Un anello in cui ogni ideale è finitamente generato si dice **Noetheriano**.*

**Lemma 4.3.2.** *Per un anello  $A$  le seguenti condizioni sono equivalenti:*

1.  $A$  è Noetheriano.
2. Ogni catena ascendente di ideali in  $A$  è stazionaria.
3. Ogni catena ascendente numerabile di ideali in  $A$  è stazionaria.
4. Ogni famiglia di ideali di  $A$  contiene un elemento massimale.

*Dimostrazione.* [1  $\Rightarrow$  2] Sia  $\{I_v \mid v \in V\}$  una catena ascendente di ideali e sia  $I = \cup\{I_v \mid v \in V\}$ . L'ideale  $I$  è finitamente generato, diciamo da  $a_1, \dots, a_n$ . Se  $a_i \in I_{v_i}$ , per  $i = 1, \dots, n$ , allora detto  $w$  il massimo di  $v_1, \dots, v_n$  si ha che  $I \subset I_w \subset I_v \subset I$  per ogni  $v \geq w$  e quindi la catena è stazionaria.

[2  $\Rightarrow$  3] è ovvio e [3  $\Rightarrow$  4] è una immediata applicazione del Lemma 1.1.1.

[4  $\Rightarrow$  1] Sia  $I$  un ideale e sia  $J \subset I$  un elemento massimale della famiglia degli ideali finitamente generati contenuti in  $I$ , dimostriamo che  $J = I$ . Sia  $a \in I$  allora l'ideale  $J+(a) \subset I$  è ancora finitamente generato e per la massimalità di  $J$  si deve avere  $a \in J$ .  $\square$

Emmy Noether è stata la prima a introdurre nel 1923 la nozione di catena ascendente di ideali ed a studiare la classe degli anelli, oggi chiamati in suo onore, Noetheriani. I campi e gli anelli ad ideali principali sono tutti Noetheriani.

**Teorema 4.3.3 (Della base di Hilbert).** *Se  $A$  è un anello Noetheriano, allora anche  $A[x]$  è Noetheriano.*

*Dimostrazione.* Dato un polinomio  $f \in A[x]$  di grado  $r \geq 0$  chiameremo coefficiente direttore di  $f$  il coefficiente di  $x^r$  in  $f$ ; è utile osservare che i polinomi  $f, xf, x^2f, \dots$  hanno tutti lo stesso coefficiente direttore.

Sia  $I \subset A[x]$  un ideale e, per ogni  $m \geq 0$ , denotiamo con  $J_m \subset A$  l'insieme formato dallo 0 e dai coefficienti direttori dei polinomi di grado  $m$  contenuti in  $I$ . Si osserva immediatamente che  $J_m$  è un ideale e che  $J_m \subset J_{m+1}$  per ogni  $m$ . Per ipotesi l'anello  $A$  è Noetheriano, dunque gli ideali  $J_m$  sono tutti finitamente generati e la catena ascendente  $\{J_m \mid m \in \mathbb{N}\}$  è stazionaria. Sia  $N > 0$  tale che  $J_m = J_N$  per ogni  $m \geq N$  e, per ogni  $i = 0, \dots, N$ , siano  $f_1^i, \dots, f_j^i \in I$  polinomi di grado  $i$  i cui coefficienti direttori generano  $J_i$ . Sia  $H \subset I$  l'ideale generato dai polinomi  $f_j^i$ , per  $i = 0, \dots, N$ , e proviamo che  $H = I$ . Infatti, sia  $f \in I$  e scriviamo  $f = h + g$  con  $h \in H$ ,  $g$  di grado minimo e si assuma per assurdo  $g \neq 0$ . Sia  $r = \min(\deg(g), N)$ , allora il coefficiente direttore di  $g$  appartiene a  $J_r$  e quindi esistono  $a_1, \dots, a_j \in A$  tali che, detto  $s = \deg(g) - r$ , il polinomio  $g - (a_1 f_1^r + \dots + a_j f_j^r)x^s$  ha grado minore del grado di  $g$ . Dato che  $\sum a_i f_i^r \in H$  l'assurdo è servito.  $\square$

**Proposizione 4.3.4.** *Sia  $A$  un anello Noetheriano e  $I$  un ideale. Allora l'anello quoziente  $A/I$  è Noetheriano.*

*Dimostrazione.* Sia  $\pi: A \rightarrow A/I$  la proiezione al quoziente, una catena ascendente di ideali  $\{J_v\} \subset A/I$  è stazionaria se e solo se la catena  $\{\pi^{-1}(J_v)\} \subset A$  è stazionaria.  $\square$

**Corollario 4.3.5.** Per ogni campo  $\mathbb{K}$  e per ogni ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$ , l'anello quoziente  $\mathbb{K}[x_1, \dots, x_n]/I$  è Noetheriano.

*Dimostrazione.* Il campo  $\mathbb{K}$  è Noetheriano, per il teorema della base di Hilbert e per induzione su  $n$  si ha che  $\mathbb{K}[x_1, \dots, x_n]$  è Noetheriano. Basta adesso applicare la Proposizione 4.3.4.  $\square$

**Teorema 4.3.6 (Lemma di Artin-Rees).** Sia  $A$  un anello Noetheriano e siano  $I, M \subset A$  ideali. Allora esiste un intero  $k \geq 0$  tale che, per ogni  $n \geq k$  vale

$$I \cap M^n = M^{n-k}(I \cap M^k)$$

e quindi  $M^n I \subset I \cap M^n \subset M^{n-k} I$ .

*Dimostrazione.* L'inclusione  $\supset$  è evidente per ogni  $n, k$ , proviamo che vale  $\subset$ . Fissiamo un insieme di generatori  $a_1, \dots, a_r$  dell'ideale  $M$  e consideriamo l'omomorfismo di anelli  $f: A[t_1, \dots, t_r] \rightarrow A$  tale che  $f(t_i) = a_i$  per  $i = 1, \dots, r$  e  $f(a) = a$  per ogni  $a \in A$ . Notiamo che  $M^n$  è l'immagine tramite  $f$  dell'insieme dei polinomi omogenei di grado  $n$ . Per ogni  $n \geq 0$  sia  $J_n \subset A[t_1, \dots, t_r]$  l'ideale generato dai polinomi omogenei  $p$  di grado  $\leq n$  tali che  $f(p) \in I$ ; per il teorema della base l'anello  $A[t_1, \dots, t_r]$  è Noetheriano e la catena  $J_0 \subset J_1 \subset \dots$  è stazionaria.

Fissiamo un intero  $k$  tale che  $J_k = J_n$  per ogni  $n \geq k$ . Dato  $n \geq k$  e  $a \in I \cap M^n$  esiste  $p \in J_n$  polinomio omogeneo di grado  $n$  tale che  $a = f(p)$ ; siccome  $J_n = J_k$  vale  $p = \sum p_i q_i$ , dove ogni  $p_i \in J_k$  è omogeneo di grado  $k$  e ogni  $q_i$  è omogeneo di grado  $n - k$ ; quindi  $f(p_i) \in I \cap M^k$ ,  $f(q_i) \in M^{n-k}$  e la tesi è dimostrata.  $\square$

**Corollario 4.3.7.** Sia  $A$  un anello Noetheriano e  $M \subset A$  un ideale. Se  $1 + M$  non contiene divisori di 0 allora

$$\bigcap_{n \geq 0} M^n = 0$$

*Dimostrazione.* Sia  $J = \bigcap_{n \geq 0} M^n$ ; per il lemma di Artin-Rees 4.3.6 esiste  $k \geq 0$  tale che  $J = J \cap M^{k+1} = M(J \cap M^k) = MJ$ . Per il lemma di Nakayama esiste  $a \in M$  tale che  $(1 - a)J = 0$  e quindi  $J = 0$ .  $\square$

**Corollario 4.3.8.** Sia  $A$  un anello locale Noetheriano con ideale massimale  $\mathfrak{m}$ . Allora per ogni ideale  $I \subset \mathfrak{m}$  vale

$$\bigcap_{n \geq 0} (I + \mathfrak{m}^n) = I.$$

*Dimostrazione.* Basta applicare il Corollario 4.3.7 all'anello quoziente  $A/I$  ed al suo ideale massimale.  $\square$

## Esercizi

**4.6.** Provare che l'anello delle funzioni continue  $f: [0, 1] \rightarrow \mathbb{R}$  non è Noetheriano.

**4.7.** Siano  $A$  un anello Noetheriano ed  $E \subset A$  un sottoinsieme. Provare che esiste un sottoinsieme finito  $E_0 \subset E$  tale che  $(E) = (E_0)$ .

**4.8.** Siano  $A$  un anello Noetheriano e  $f: A \rightarrow A$  un endomorfismo surgettivo di anelli. Provare che  $f$  è un isomorfismo.

**4.9 (Moduli Noetheriani).** Un modulo si dice **Noetheriano** se ogni suo sottomodulo è finitamente generato. Si provi:

1. Sia  $M$  un modulo e  $N \subset M$  un sottomodulo. Allora  $M$  è Noetheriano se e solo se  $N$  e  $M/N$  sono Noetheriani.
2. Se  $M, N$  sono Noetheriani, allora  $M \oplus N$  è Noetheriano.
3. Se  $A$  è un anello Noetheriano, allora ogni  $A$ -modulo finitamente generato è Noetheriano. (Sugg.: ogni modulo finitamente generato è quoziente di un modulo libero di rango finito.)

**4.10.** Sia  $A$  un anello locale Noetheriano con ideale massimale  $\mathfrak{m}$  tale che  $\mathfrak{m}^n = \mathfrak{m}^{n+1}$  per qualche intero  $n \geq 0$ . Provare che  $\mathfrak{m}^n = 0$  (Sugg.: Nakayama) e che ogni catena discendente di ideali è stazionaria (Sugg.: induzione su  $n$ ). Un anello con queste caratteristiche si dice **locale Artiniano**.

**4.11.** Sia  $A$  un anello e denotiamo con  $\mathcal{V}$  la famiglia degli ideali di  $A$  che non sono finitamente generati. Provare che se  $\mathcal{V} \neq \emptyset$ , cioè se  $A$  non è Noetheriano, allora  $\mathcal{V}$  contiene elementi massimali rispetto all'inclusione. Dimostrare inoltre gli elementi massimali di  $\mathcal{V}$  sono ideali primi di  $A$ . (Sugg.: se  $I$  è un ideale,  $xy \in I$  e  $J \subset I$  un ideale tale che  $I + (x) = J + (x)$ , allora vale  $I = J + x(I : x)$ , dove  $(I : x) = \{y \in A \mid xy \in I\}$ .)

## 4.4 La topologia di Zariski

Sia  $\mathbb{K}$  un campo (infinito) fissato e  $\mathbb{A}^n \cong \mathbb{K}^n$  lo spazio affine su  $\mathbb{K}$  di dimensione  $n$ . L'anello  $\mathbb{K}[x_1, \dots, x_n]$  è un'algebra di funzioni su  $\mathbb{A}^n$  a valori in  $\mathbb{K}$  ed è naturale pensare ogni sottoinsieme di  $\mathbb{K}[x_1, \dots, x_n]$  come un insieme di equazioni algebriche nelle variabili  $x_1, \dots, x_n$ .

Il **luogo di zeri** di un sottoinsieme  $E \subset \mathbb{K}[x_1, \dots, x_n]$  è definito come

$$V(E) = \{(a_1, \dots, a_n) \in \mathbb{A}^n \mid f(a_1, \dots, a_n) = 0 \text{ per ogni } f \in E\}.$$

Dalla definizione appare chiaro che, se  $(E)$  è l'ideale generato da  $E$ , allora  $E$  ed  $(E)$  hanno lo stesso luogo di zeri, cioè  $V(E) = V((E))$ . Ne segue che non è restrittivo considerare esclusivamente luoghi di zeri di ideali di  $\mathbb{K}[x_1, \dots, x_n]$ .

**Definizione 4.4.1.** Un sottoinsieme  $X \subset \mathbb{A}^n$  si dice **algebrico** se è  $X = V(I)$  per qualche ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$ .

Non tutti i sottoinsiemi di  $\mathbb{A}^n$  sono algebrici: ad esempio un sottoinsieme proprio di  $\mathbb{A}^1$  è algebrico se e solo se è finito. Le seguenti proprietà sono di immediata verifica:

1.  $V(0) = \mathbb{A}^n$  e  $V(\mathbb{K}[x_1, \dots, x_n]) = \emptyset$ .
2. Se  $I \subset J$  sono ideali, allora  $V(J) \subset V(I)$ .
3. Per ogni ideale  $I$ , vale  $V(I) = V(\sqrt{I})$ .
4. Dati  $I, J$  ideali, vale  $V(IJ) = V(I) \cup V(J)$ .
5. Data una famiglia qualsiasi  $\{I_\alpha\}$  di ideali, vale  $V(\sum I_\alpha) = \cap V(I_\alpha)$ .

Le proprietà 1), 4) e 5) mostrano che i sottoinsiemi algebrici di  $\mathbb{A}^n$  sono i chiusi di una topologia, detta **topologia di Zariski**.

6. Se  $\mathbb{K} = \overline{\mathbb{K}}$  è algebricamente chiuso e  $I \subset \mathbb{K}[t]$  è un ideale proprio, allora il luogo di zeri  $V(I) \subset \mathbb{A}^1$  è non vuoto (poiché  $\mathbb{K}[t]$  è un anello ad ideali principali ogni ideale proprio è della forma  $(f)$ , con  $f$  polinomio di grado positivo e  $V(f)$  è l'insieme delle radici di  $f$ ).

7. Se  $\mathbb{K} = \overline{\mathbb{K}}$  è algebricamente chiuso,  $n \geq 2$  e  $f \in \mathbb{K}[x_1, \dots, x_n]$  è un polinomio di grado positivo, allora  $V(f) \subset \mathbb{A}^n$  è infinito. Infatti se, tanto per fissare le idee,  $f$  ha grado  $d > 0$  nella variabile  $x_n$ , allora  $f = f_0(x_1, \dots, x_{n-1})x_n^d + \dots$  e per ogni  $a \in \mathbb{A}^{n-1}$  tale che  $f_0(a) \neq 0$  esiste  $a_n \in \mathbb{K}$  tale che  $f(a, a_n) = 0$ .

**Lemma 4.4.2 (di preparazione).** *Siano  $\mathbb{K}$  un campo infinito e  $f \in \mathbb{K}[x_1, \dots, x_n]$  un polinomio non nullo di grado  $d \geq 0$ . Allora:*

1. *L'aperto  $\mathbb{A}_f^n = \{a \in \mathbb{A}^n \mid f(a) \neq 0\}$  è non vuoto.*
2. *Esiste un cambio lineare di coordinate  $x_i = \sum a_{ij}y_j$  ed una costante  $c \in \mathbb{K}$  tale che il polinomio  $cf$  è monico di grado  $d$  rispetto alla variabile  $y_n$ .*

*Dimostrazione.* [1] Lavoriamo per induzione su  $n$ , assumiamo l'enunciato vero per polinomi in  $\mathbb{K}[x_1, \dots, x_{n-1}]$  e scriviamo  $f = \sum f_i x_n^i$ , con i polinomi  $f_i \in \mathbb{K}[x_1, \dots, x_{n-1}]$  non tutti nulli. Sia  $a \in \mathbb{A}^{n-1}$  tale che i valori  $f_0(a), f_1(a), \dots$  non siano tutti nulli. Allora il polinomio  $f(a, x_n)$  non è nullo in  $\mathbb{K}[x_n]$  ed ha al più un numero finito di radici.

[2] Sia  $f_d$  la componente omogenea di grado  $d$  di  $f$ . Per il punto 1) esiste un punto  $a \in \mathbb{A}^n$  tale che  $f_d(a) \neq 0$ ; scegliamo un sistema di coordinate  $y_1, \dots, y_n$  tale che il punto  $a$  corrisponda a  $(0, 0, \dots, 0, 1)$ . Nel nuovo sistema di coordinate il polinomio  $f(0, \dots, 0, y_n)$  ha grado  $d$  e basta quindi prendere come costante  $c = 1/f_d(0, \dots, 0, 1)$ .  $\square$

Le proiezioni affini non sono applicazioni chiuse; consideriamo ad esempio l'iperbole  $X = V(xy - 1) \subset \mathbb{A}^2$  e sia  $\pi: \mathbb{A}^2 \rightarrow \mathbb{A}^1$  la proiezione sulla prima coordinata. Si vede immediatamente che  $\pi(X)$  non è un chiuso di Zariski. Similmente se facciamo la proiezione sulla seconda coordinata. Però, se prima si effettua un cambio lineare di coordinate  $x = au + bv$ ,  $y = cu + dv$ , con  $ad - bc \neq 0$ , si trova che  $X = V(bdv^2 + vu(ad + bc) + acu^2 - 1)$  e, se  $bd \neq 0$ , allora la proiezione di  $X$  sul primo asse coordinato è  $\mathbb{A}^1$ , che è quindi chiuso. Abbiamo quindi sperimentato che *la generica proiezione di  $X$  su di un sottospazio affine è un chiuso*. Quanto appena visto è un caso particolare di un fatto molto più generale che viene detto *Lemma di normalizzazione di Noether*.

**Lemma 4.4.3 (di proiezione).** *Siano  $\mathbb{K} = \overline{\mathbb{K}}$  un campo algebricamente chiuso,  $J \subset \mathbb{K}[x_1, \dots, x_n]$  un ideale,  $J^c = J \cap \mathbb{K}[x_1, \dots, x_{n-1}]$  e  $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$  la proiezione sulle prime coordinate. Se esiste un polinomio  $F \in J$  monico rispetto a  $x_n$  (e.g. se  $\deg_{x_n} F = \deg F$ ), allora  $\pi: V(J) \rightarrow V(J^c)$  è chiusa e surgettiva.*

*Dimostrazione.* Se  $(a_1, \dots, a_n) \in V(J)$ , allora  $f(a_1, \dots, a_n) = 0$  per ogni  $f \in J^c$  e quindi  $(a_1, \dots, a_{n-1}) \in V(J^c)$ .

Proviamo adesso la surgettività: si consideri un punto  $(a_1, \dots, a_{n-1}) \in V(J^c)$  e sia  $M \subset \mathbb{K}[x_1, \dots, x_n]$  l'ideale generato da  $x_1 - a_1, \dots, x_{n-1} - a_{n-1}$ . Siccome

$$V(J + M) = V(J) \cap V(M) \subset V(M) = \pi^{-1}(a_1, \dots, a_{n-1}),$$

basta dimostrare che  $V(J + M)$  è non vuoto. Mostriamo come primo passo che  $1 \notin J + M$ : infatti, se per assurdo  $1 = f + \sum (x_i - a_i)g_i$  per qualche  $f \in J$  e  $g_1, \dots, g_{n-1} \in \mathbb{K}[x_1, \dots, x_n]$ , allora  $f(a_1, \dots, a_{n-1}, t) = 1$  per ogni  $t \in \mathbb{K}$  e quindi, se

$$f(x_1, \dots, x_{n-1}, t) = \sum f_i(x_1, \dots, x_{n-1})t^i,$$

deve essere  $f_0(a_1, \dots, a_{n-1}) = 1$  e  $f_i(a_1, \dots, a_{n-1}) = 0$  per ogni  $i > 0$ . Si consideri adesso il risultante  $R = R(F, f) \in J^c$  dell'eliminazione della variabile  $x_n$  da  $F$  e  $f$ . Vale  $R = \det S(F, f)$ , dove  $S(F, f)$  è la matrice di Sylvester della coppia  $F, f$ . Siccome  $S(F, f)(a_1, \dots, a_{n-1})$  è una matrice triangolare superiore con tutti 1 sulla diagonale si ha  $R(F, f)(a_1, \dots, a_{n-1}) = 1$  in contraddizione con l'appartenenza a  $J^c$ , dunque  $1 \notin J + M$ .



Si consideri adesso l'omomorfismo surgettivo  $\phi: \mathbb{K}[x_1, \dots, x_n] \rightarrow \mathbb{K}[t]$  definito da  $\phi(x_n) = t$  e  $\phi(x_i) = a_i$ ; è chiaro che  $M = \text{Ker}(\phi)$  (cfr. Esercizio 1.10) e quindi che  $\phi^{-1}(\phi(J)) = J + M$ . Dato che  $1 \notin J + M$  ne segue che  $\phi(J)$  è un ideale proprio e quindi esiste  $a_n \in \mathbb{K}$  tale che per ogni  $f \in J$  vale  $f(a_1, \dots, a_n) = \phi(f)(a_n) = 0$ .

Sia  $X \subset V(J)$  un chiuso di Zariski, allora  $X = V(I) \cap V(J) = V(I + J)$ ; a meno di sostituire  $I$  con  $I + J$  non è restrittivo supporre  $J \subset I$ : in particolare  $F \in I$  e  $\pi(X) = V(I^c)$ .  $\square$

Due dimostrazioni alternative del lemma di proiezione saranno presentate negli Esercizi 4.16 e 4.45.

### Esercizi

**4.12.** Provare che la topologia di Zariski non è di Hausdorff.

**4.13.** Provare che i sottoinsiemi  $\mathbb{A}_f^n = \{a \in \mathbb{A}^n \mid f(a) \neq 0\}$  formano, al variare di  $f \in \mathbb{K}[x_1, \dots, x_n]$ , una base di aperti della topologia di Zariski.

**4.14.** Sia  $I \subset \mathbb{K}[x_1, \dots, x_n]$  un ideale e  $X \subset \mathbb{A}^n$  un sottoinsieme finito tale che  $X \cap V(I) = \emptyset$ . Provare che esiste un polinomio  $f \in I$  tale che  $f(x) \neq 0$  per ogni  $x \in X$ . Provare inoltre che se  $I$  è un ideale omogeneo, allora è possibile scegliere  $f$  omogeneo. (Sugg.: poiché  $X$  è finito esistono  $f_1, \dots, f_s \in I$  tali che, per ogni  $x \in X$ , esiste un indice  $i$  per cui  $f_i(x) \neq 0$ . Ne segue che l'insieme dei vettori  $a = (a_1, \dots, a_s) \in \mathbb{K}^s$  per cui  $V(\sum a_i f_i) \cap X \neq \emptyset$  è unione di un numero finito di iperpiani.)

**4.15.** Sia  $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$  la proiezione sulle prime coordinate. Mostrare che, nella topologia di Zariski,  $\pi$  è aperta. (Sugg.: se  $f(x_1, \dots, x_n) = \sum_i f_i(x_1, \dots, x_{n-1})x_n^i$  mostrare che  $\pi(\mathbb{A}_f^n) = \cup_i \mathbb{A}_{f_i}^{n-1}$ .)

**4.16.** *Prima dimostrazione alternativa del lemma di proiezione 4.4.3.* Questa dimostrazione è interamente basata sulle proprietà del risultante. Nelle notazioni del Lemma 4.4.3 sia  $a = (a_1, \dots, a_{n-1}) \in V(J^c)$  e denotiamo  $X = V(F) \cap \pi^{-1}(a)$ . Mostrare che  $X$  è un insieme finito. Supponiamo quindi per assurdo che  $X \cap V(I) = \emptyset$ ; per l'Esercizio 4.14 esiste  $f \in I$  tale che  $X \cap V(f) = \emptyset$ : questo significa che i due polinomi  $F(a, x_n), f(a, x_n) \in \mathbb{K}[x_n]$  non hanno zeri comuni ed il loro risultante  $R(F, f)$  non si annulla in  $a$ .

## 4.5 Il teorema degli zeri di Hilbert

Dato un qualsiasi sottoinsieme  $X \subset \mathbb{A}^n$ , si definisce

$$I(X) = \{f \in \mathbb{K}[x_1, \dots, x_n] \mid f(a) = 0 \text{ per ogni } a \in X\}.$$

L'insieme  $V(I(X))$  è uguale alla chiusura di  $X$  nella topologia di Zariski. Infatti si ha  $X \subset V(I(X))$  e, se  $V(J)$  è un chiuso che contiene  $X$ , allora  $J \subset I(X)$  e quindi  $V(I(X)) \subset V(J)$ .

L'applicazione  $X \mapsto I(X)$  soddisfa inoltre le proprietà:

1.  $I(\emptyset) = \mathbb{K}[x_1, \dots, x_n]$  e  $I(\mathbb{A}^n) = 0$ .
2. Se  $X \subset Y$ , allora  $I(Y) \subset I(X)$ .
3. Per ogni sottoinsieme chiuso  $X \subset \mathbb{A}^n$ , vale  $I(X) = \sqrt{I(X)}$  e  $X = V(I(X))$ .
4. Per ogni ideale  $J \subset \mathbb{K}[x_1, \dots, x_n]$ , vale  $\sqrt{J} \subset I(V(J))$ .

L'inclusione del punto 4) è in generale propria: ad esempio, se  $\mathbb{K} = \mathbb{R}$ ,  $n = 1$  e  $J = (x^2 + 1)$ , allora  $V(J) = \emptyset$  e  $I(V(J)) = \mathbb{R}[x] \neq \sqrt{J}$ .

**Teorema 4.5.1 (degli zeri di Hilbert (1892), forma debole).** *Se il campo  $\mathbb{K}$  è algebricamente chiuso e  $J \subset \mathbb{K}[x_1, \dots, x_n]$  è un ideale, allora vale  $V(J) = \emptyset$  se e solo se  $1 \in J$ .*

*Dimostrazione.* L'enunciato è ovvio se  $1 \in J$  oppure se  $J = 0$ . Supponiamo quindi  $0 \neq J \neq \mathbb{K}[x_1, \dots, x_n]$  e proviamo che  $V(J)$  è non vuoto.

Se  $n = 1$ , allora l'ideale  $J$  è principale, diciamo  $J = (f)$ , e quindi  $V(J)$  è l'insieme delle radici di  $f$ . Siccome  $f$  non è invertibile deve avere grado positivo e quindi possiede radici.

Se  $n > 1$ , ragioniamo per induzione e supponiamo il teorema vero in  $\mathbb{A}^{n-1}$ . Sia  $F \in J$  un polinomio di grado  $m > 0$ . Per il lemma di preparazione 4.4.2, a meno di un cambio lineare di coordinate e di moltiplicazione per una costante, possiamo supporre che  $F$  sia un polinomio monico di grado  $m$  rispetto a  $x_n$ . Consideriamo l'ideale  $J^c = J \cap \mathbb{K}[x_1, \dots, x_{n-1}]$ ; per l'ipotesi induttiva  $V(J^c) \neq \emptyset$ . Denotando con  $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$  la proiezione sulle prime  $n - 1$  coordinate, per il Lemma 4.4.3, vale  $\pi(V(J)) = V(J^c)$  e perciò  $V(J) \neq \emptyset$ .  $\square$

**Corollario 4.5.2.** *Se il campo  $\mathbb{K}$  è algebricamente chiuso, allora gli ideali massimali di  $\mathbb{K}[x_1, \dots, x_n]$  sono tutti e soli gli ideali del tipo  $I(p)$ , per  $p \in \mathbb{A}^n$ . Esiste dunque una biiezione naturale fra  $\mathbb{A}^n$  e l'insieme degli ideali massimali di  $\mathbb{K}[x_1, \dots, x_n]$ .*

*Dimostrazione.* Sia  $\mathfrak{m} \subset \mathbb{K}[x_1, \dots, x_n]$  massimale e  $p \in V(\mathfrak{m})$ ; allora  $\mathfrak{m} \subset I(p)$  da cui segue  $\mathfrak{m} = I(p)$ . Viceversa se  $p \in \mathbb{A}^n$  e  $I(p) \subset \mathfrak{m}$ , con  $\mathfrak{m}$  massimale, allora esiste  $q \in \mathbb{A}^n$  tale che  $I(p) \subset \mathfrak{m} = I(q)$ , da cui  $\{q\} \subset \{p\}$  e quindi  $p = q$ .  $\square$

**Teorema 4.5.3 (degli zeri di Hilbert (1892), forma forte).** *Se il campo  $\mathbb{K}$  è algebricamente chiuso, allora per ogni ideale  $J \subset \mathbb{K}[x_1, \dots, x_n]$  vale  $\sqrt{J} = I(V(J))$ .*

*Dimostrazione.* Siccome  $X = V(J) = V(\sqrt{J})$  si può supporre senza perdita di generalità che  $J = \sqrt{J}$ , cioè che  $S = \mathbb{K}[x_1, \dots, x_n]/J$  non possiede elementi nilpotenti. Dobbiamo dimostrare che se  $F \notin J$  allora esiste  $x \in X$  tale che  $F(x) \neq 0$ . Sia  $F$  come sopra fissato,  $\alpha: \mathbb{K}[x_1, \dots, x_n] \rightarrow S$  la proiezione al quoziente,  $f = \alpha(F)$ . Si noti che  $1 - tf$  è invertibile in  $S[[t]]$  con inverso  $\sum_{i=0}^{\infty} t^i f^i$  e quindi  $1 - tf$  è invertibile in  $S[t]$  se e solo se  $f$  è nilpotente. Per ipotesi  $S$  è ridotto e quindi  $(1 - tf)$  è un ideale proprio di  $S[t]$  e di conseguenza  $J$  e  $1 - tF$  generano un ideale proprio di  $\mathbb{K}[x_1, \dots, x_n, t]$ . Per la forma debole del teorema degli zeri esistono  $a_0, \dots, a_n, t_0$  tali che  $g(a_0, \dots, a_n) = 0$  per ogni  $g \in J$  e  $1 - t_0 F(a_0, \dots, a_n) = 0$ . Dunque  $x = (a_0, \dots, a_n) \in X$  e  $F(x) \neq 0$ .  $\square$

**Corollario 4.5.4.** *Supponiamo  $\mathbb{K}$  algebricamente chiuso e siano  $f, g \in \mathbb{K}[x_1, \dots, x_n]$  con  $f$  irriducibile. Se  $V(f) \subset V(g)$ , allora  $f$  divide  $g$ .*

*Dimostrazione.* Per il teorema degli zeri vale  $g \in I(V(f)) = \sqrt{(f)} = (f)$ .  $\square$

Ricordiamo che un ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$  si dice omogeneo se è generato da polinomi omogenei; se  $S_d \subset \mathbb{K}[x_1, \dots, x_n]$  è il sottospazio dei polinomi omogenei di grado  $d$  si verifica facilmente che  $I$  è omogeneo se e solo se  $I = \bigoplus (I \cap S_d)$ . Sia infine  $0 = (0, \dots, 0) \in \mathbb{A}^n$ ; notiamo che se  $I$  è omogeneo e  $V(I) \neq \emptyset$ , allora  $0 \in V(I)$ .

**Corollario 4.5.5 (Teorema degli zeri omogeneo).** *Se il campo  $\mathbb{K}$  è algebricamente chiuso e  $I \subset \mathbb{K}[x_1, \dots, x_n]$  è un ideale omogeneo proprio, allora  $V(I) = \{0\}$  se e solo se esiste  $d > 0$  tale che  $S_d \subset I$ .*

*Dimostrazione.* Se  $S_d \subset I$ , allora per ogni  $i$  si ha  $x_i^d \in I$ , quindi  $x_i \in \sqrt{I}$  e perciò  $V(I) = V(\sqrt{I}) = \{0\}$ .

Viceversa, se  $V(I) = \{0\}$ , allora per il teorema degli zeri  $\sqrt{I} = I(\{0\}) = (x_1, \dots, x_n)$ . Esiste dunque  $d > 0$  tale che  $x_i^d \in I$  per ogni  $i$  e quindi  $S_{dn-n+1} \subset I$ .  $\square$

Un risultato collegato al teorema degli zeri omogeneo, che riportiamo senza dimostrazione è il seguente.

**Teorema 4.5.6.** *Sia  $I \subset \mathbb{K}[x_0, \dots, x_n]$  un ideale generato da  $n + 1$  polinomi omogenei di gradi  $d_0, \dots, d_n$ . Se  $\sqrt{I} = (x_0, \dots, x_n)$ , allora la dimensione di  $S_h \cap I$  dipende solo dai numeri  $h, n, d_0, \dots, d_n$  e non dall'ideale  $I$ . In particolare  $S_d \subset I$  se e solo se  $d \geq \sum d_i - n$ .*

Dimostreremo più avanti tale risultato come semplice corollario del Teorema 13.4.6 (vedi Esercizio 13.13).

**Esercizi**

**4.17.** Sia  $Y \subset \mathbb{A}^3$  l'unione dei tre piani coordinati e  $X \subset \mathbb{A}^3$  l'unione dei tre assi coordinati. Provare che  $I(Y) = (xyz)$  e che  $I(X) = (xy, yz, zx)$ . (Sugg.: se  $f \in I(X)$  considerare  $f(x, y, z) - f(0, y, z) - f(x, 0, z) - f(x, y, 0)$ .)

**4.18.** Sia  $J \subset S = \mathbb{K}[x_1, \dots, x_n]$  un ideale e  $X = V(J)$ . Provare che se  $f \in I(X)$  allora  $1 + f$  è invertibile in  $S/J$ .

**4.19.** Dimostrare che ogni ideale primo di  $\mathbb{C}[x_1, \dots, x_n]$  è intersezione di ideali massimali.

**4.6 Esercizi complementari**

**4.20.** Sia  $f \in A[x]$  un polinomio monico. Provare che per ogni coppia di polinomi  $g, h \in A[x]$  vale  $R(f, g) = R(f, g + hf)$ .

**4.21.** Provare che  $R_{n,m}(f(x), g(x)) = \pm R_{n,m}(x^n f(x^{-1}), x^m g(x^{-1}))$ .

**4.22.** Siano  $f(x, y)$  e  $g(x, y)$  due forme binarie non nulle di gradi  $n$  e  $m$  a coefficienti in un campo  $\mathbb{K}$ . Provare che  $f$  e  $g$  hanno un fattore comune se e solo se  $R(f, g) = R_{n,m}(f(x, 1), g(x, 1)) = 0$ . Mostrare inoltre che per ogni  $A \in \text{SL}(2, \mathbb{K})$  vale  $R_{n,m}(Af, Ag) = R_{n,m}(f, g)$ . (Sugg.: imitare la dimostrazione di 4.1.3.)

**4.23.** Sia  $A$  un dominio a fattorizzazione unica e siano  $f, g \in A[x]$  polinomi di gradi  $\deg(f) = n, \deg(g) = m$ . Dimostrare che  $f$  e  $g$  hanno un fattore comune di grado  $> k$ , con  $0 \leq k \leq \min(n, m)$ , se e solo se la matrice

$$\begin{pmatrix} x^{m-k-1}f \\ \vdots \\ f \\ x^{n-k-1}g \\ \vdots \\ g \end{pmatrix} \in M(n + m - 2k, n + m - k, A)$$

non ha rango massimo.

**4.24.** Sia  $S(f, g)$  la matrice di Sylvester di due forme binarie  $f, g$  di gradi  $n, m$ . Provare che se  $f, g$  hanno un fattore comune di grado  $r$  allora la dimensione del nucleo di  $S(f, g)$  è almeno  $r$ .

**4.25 (\*)**. Esistono altre rappresentazioni del risultante: qui ne proponiamo due come esercizi, rimandando a [GKZ1994, p. 401] per suggerimenti e soluzioni.

- Data una serie formale  $\phi = \sum_{i=-\infty}^{+\infty} r_i x^i$ , per ogni coppia di interi positivi  $n, m$  si definisce la matrice (detta di Toeplitz)  $S_{n,m}(\phi) = (a_{ij})$ , dove  $a_{ij} = r_{n+j-i}$  e  $1 \leq i, j \leq m$ . Siano  $f, g \in A[x]$  con  $f(0) = 1$  e  $\phi = \frac{g}{f} \in A[[x]]$ . Provare che il determinante di  $S_{n,m}(\phi)$  è uguale a  $R_{n,m}(f, g)$ .
- (Formula di Bézout-Cayley) Siano  $f, g$  polinomi di grado  $n$  e sia

$$\frac{f(x)g(y) - g(x)f(y)}{x - y} = \sum_{i,j=0}^{n-1} c_{ij} x^i y^j.$$

Provare che  $R_{n,n}(f, g) = \det(c_{ij})$ .

**4.26**. Siano  $I_1, \dots, I_r \in \mathbb{N}^n$  multiindici distinti e  $\mathbb{K}$  un campo infinito. Mostrare che l'immagine di  $\mathbb{K}^n \rightarrow \mathbb{K}^r$ ,  $x \mapsto (x^{I_1}, \dots, x^{I_r})$  contiene una base dello spazio vettoriale  $\mathbb{K}^r$ .

**4.27 (Sistemi risultanti)**. Siano  $A$  un dominio a fattorizzazione unica,  $f, g_1, \dots, g_r \in A[x]$  polinomi,  $a_1, \dots, a_r$  indeterminate e sia  $R \in A[a_1, \dots, a_r]$  il risultante dell'eliminazione di  $x$  dai polinomi  $f$  e  $a_1 g_1 + \dots + a_r g_r$ . Provare che  $R = 0$  se e solo se gli  $r + 1$  polinomi  $f, g_1, \dots, g_r$  hanno un fattore comune di grado positivo. Provare inoltre che i coefficienti di  $R(a_1, \dots, a_r)$  appartengono a  $A \cap (f, g_1, \dots, g_r)$ .

**4.28**. Dato un polinomio monico  $f$  a coefficienti reali, senza radici multiple, determinare la relazione tra il segno del discriminante, il grado del polinomio e la classe di resto modulo 4 del numero di radici reali. In particolare si provi che se il grado di  $f$  è 3 allora  $f$  possiede tre radici reali distinte se e solo se  $\Delta(f) < 0$ .

**4.29**. Provare che se  $f, g \in \mathbb{K}[x]$  hanno gradi  $n, m$  allora vale la formula di polarizzazione

$$R(f, g)^2 = (-1)^{nm} \frac{\Delta(fg)}{\Delta(f)\Delta(g)}.$$

**4.30**. Sia  $f = \sum a_i x^{n-i} y^i$  un polinomio omogeneo di grado  $n$  a coefficienti in un campo di caratteristica 0 e siano  $f_x, f_y$  le derivate di  $f$  rispetto a  $x$  e  $y$  rispettivamente. Provare che:

$$R_{n,n-1}(f, f_x) = \frac{a_0}{n^{n-2}} R_{n-1,n-1}(f_x, f_y), \quad \Delta(f) = \frac{1}{n^{n-2}} R_{n-1,n-1}(f_x, f_y).$$

**4.31**. Siano  $f, g, q \in \mathbb{K}[x]$  polinomi senza fattori comuni di gradi  $n, n, m$  rispettivamente, con  $m < n$ . Provare che  $R(f + \lambda q, g + \mu q) \in \mathbb{K}[\lambda, \mu]$  è un polinomio di grado  $\leq n$ . (Sugg.: non è restrittivo supporre  $\mathbb{K}$  algebricamente chiuso, si considerino allora gli omomorfismi  $\mathbb{K}[\lambda, \mu] \rightarrow \mathbb{K}[t]$  dati da  $\lambda \mapsto at, \mu \mapsto bt$ , al variare di  $a, b \in \mathbb{K}$ .)

**4.32 (Implicitizzazione delle curve razionali nel piano)**. Dati  $f, g, q \in \mathbb{K}[t]$  polinomi senza fattori comuni, provare che esiste  $F \in \mathbb{K}[x_1, x_2]$  polinomio irriducibile tale che

$$\left\{ \left( \frac{f(t)}{q(t)}, \frac{g(t)}{q(t)} \right) \mid t \in \mathbb{K}, q(t) \neq 0 \right\} \subset V(F).$$

(Sugg.: Esercizio 4.31.)

**4.33 (Il lemma di Gordan, \*).** Ricordiamo (vedi Pagina 25) che un sottoinsieme  $C \subset \mathbb{R}^n$  si dice un cono se  $0 \in C$  e  $tC \subset C$  per ogni numero reale  $t > 0$ . Si denoti  $x \cdot y$  il prodotto scalare usuale in  $\mathbb{R}^n$ ; esempi di coni sono le semirette  $R = \{ax \mid a \geq 0\}$  e i semispazi chiusi  $H = \{y \mid y \cdot x \geq 0\}$ .

Il duale di un cono  $C$  è per definizione

$$C^\vee = \{x \in \mathbb{R}^n \mid x \cdot y \geq 0 \text{ per ogni } y \in C\}.$$

1. Dimostrare che per ogni cono  $C \subset \mathbb{R}^n$ , il suo duale  $C^\vee$  è un cono chiuso e convesso.
2. Provare che un cono è chiuso e convesso se e solo se è intersezione di semispazi chiusi. (Sugg.: se  $C$  cono chiuso e convesso e  $p \notin C$ , sia  $q \in C$  il punto che minimizza  $(q-p) \cdot (q-p)$ . Mostrare che  $q \cdot (q-p) = 0$  e si consideri l'iperpiano ortogonale a  $q-p$ .)
3. Se  $C$  è un cono chiuso e convesso, provare che  $C = C^{\vee\vee}$ .

Un cono  $C \subset \mathbb{R}^n$  si dice poliedrale se esistono  $x_1, \dots, x_s \in \mathbb{R}^n$  tali che  $C$  è dato dall'insieme di tutte le combinazioni lineari

$$t_1x_1 + \dots + t_sx_s, \quad t_i \in \mathbb{R}, \quad t_i \geq 0.$$

Se è possibile scegliere  $x_1, \dots, x_s \in \mathbb{Q}^n$  diremo che il cono poliedrale  $C$  è razionale.

3. Provare che un semispazio chiuso  $H \subset \mathbb{R}^n$  è razionale se e solo se esiste  $y \in \mathbb{Q}^n$  tale che  $H = \{x \in \mathbb{R}^n \mid x \cdot y \geq 0\}$ .
4. Provare che l'intersezione di un numero finito di semispazi chiusi e razionali è un cono poliedrale razionale (Sugg.: induzione sul numero di semispazi.)
5. Se  $C$  è un cono poliedrale razionale, allora  $C^\vee$  è poliedrale razionale. Dedurre che ogni cono poliedrale razionale è intersezione finita di semispazi razionali.
6. Dato un cono  $C$  sia  $\mathbb{K}[C] \subset \mathbb{K}[x_1, x_1^{-1}, \dots, x_n, x_n^{-1}]$  la sottoalgebra generata dai monomi  $x^I$ , al variare di  $I \in C \cap \mathbb{Z}^n$ . Provare che se  $C$  è poliedrale razionale, allora  $\mathbb{K}[C]$  è finitamente generata.

**4.34 (\*).** Un anello si dice **Artiniano** se ogni catena discendente di ideali è stazionaria. Dimostrare che ogni anello Artiniano è anche Noetheriano ma che non vale il viceversa.

**4.35.** Sia  $I \subset \mathbb{K}[x_1, \dots, x_n]$  un ideale proprio,  $\mathbb{K} \subset L$  una estensione di campi e  $I^e = IL[x_1, \dots, x_n]$  l'estensione di  $I$ . Mostrare che  $1 \notin I^e$ .

Più in generale mostrare che  $I^e \cap \mathbb{K}[x_1, \dots, x_n] = I$ . (Sugg.: teorema di Rouché-Capelli.)

**4.36.** Sia  $I \subset \mathbb{K}[x_1, \dots, x_n]$  un ideale proprio. Dimostrare che esiste una estensione finita di campi  $\mathbb{K} \subset L$  tale che  $V(I^e) \neq \emptyset$ , dove  $I^e$  denota l'ideale esteso  $I^e = IL[x_1, \dots, x_n]$ .

**4.37.** Dimostrare che se  $\mathbb{K} \subset L$  è una estensione di campi e  $L$  è una  $\mathbb{K}$ -algebra finitamente generata, allora  $L$  è una estensione algebrica finita di  $\mathbb{K}$ . (Sugg.: sia  $L = \mathbb{K}[x_1, \dots, x_n]/I$ ; mostrare che esiste un omomorfismo di  $\mathbb{K}$  algebre  $\phi: \mathbb{K}[x_1, \dots, x_n] \rightarrow \overline{\mathbb{K}}$  tale che  $\phi(I) = 0$ .)

**4.38 (caso particolare del Teorema 4.5.6, \*).** Siano  $f, g \in \mathbb{K}[x, y]$  omogenei di grado  $d$  senza fattori comuni. Provare che  $S_n \subset (f, g)$  se e solo se  $n \geq 2d - 1$ . (Sugg.: usare 4.1.2.6.)

**4.39.** Dimostrare che nel Teorema 4.5.6 non è restrittivo supporre  $\mathbb{K}$  campo algebricamente chiuso.

**4.40 (Lemma di Gieseker).** Sia  $I \subset \mathbb{K}[x, y]$  un ideale omogeneo e scriviamo  $I = \bigoplus_{d \geq 0} I_d$ , dove  $I_d = I \cap S_d$ . Dimostrare che se  $\dim I_{d+1} \leq \dim I_d + 1$ , allora esistono  $h \leq d$  e  $f \in S_{d-h}$  tale che  $I_d = fS_h$ . (Sugg.: sia  $f_0, \dots, f_n$  una base di  $I_d$  tale che  $f_i = x^{r_i}g_i$  con  $g_i(0, 1) = 1$  e  $r_i < r_{i+1}$  per ogni  $i = 0, \dots, n$ . Si consideri l'insieme  $A = \{i \mid g_n \nmid g_i\} \cup \{i \mid r_{i+1} \geq r_i + 2\}$ ; se  $A \neq \emptyset$  sia  $s = \max(A)$  e si provi che  $yf_0, xf_0, \dots, xf_s, yf_{s+1}, xf_{s+1}, \dots, xf_n$  sono linearmente indipendenti.)

**4.41.** Nelle notazioni di 4.5.6, siano  $V \subset S_a$ ,  $W \subset S_b$  sottospazi vettoriali e  $\mu: V \otimes W \rightarrow S_{a+b}$  la mappa di moltiplicazione  $\mu(f \otimes g) = fg$ . Provare che il rango di  $\mu$  è almeno  $\dim V + \dim W - 1$ . (Sugg.: usare la fattorizzazione unica in  $\mathbb{K}[x_1, \dots, x_n]$ .)

**4.42 (Teorema di Hopf).** Siano  $A, B, C$  spazi vettoriali di dimensione finita su un campo algebricamente chiuso e sia  $\mu: A \otimes B \rightarrow C$  un'applicazione lineare e separatamente iniettiva, cioè tale che  $\mu(a \otimes b) = 0$  se e solo se  $a \otimes b = 0$ .

1. (\*) Provare che se  $\dim A = 2$ , allora  $\dim C > \dim B$ . (Sugg.: sia per assurdo  $\mu: A \otimes B \rightarrow B$  come sopra,  $e_1, e_2$  una base di  $A$ ,  $f_i(b) = \mu(e_i \otimes b)$  e si considerino gli endomorfismi  $\lambda f_1 + \eta f_2$ , con  $[\lambda, \eta] \in \mathbb{P}^1$ .)
2. (\*\*?) Provare che  $\dim C \geq \dim A + \dim B - 1$  (vedi Esercizio 10.27).

**4.43.** Sia  $\mathbb{K}$  un campo sul quale vale il teorema di Hopf (punto 2 dell'Esercizio 4.42) e siano  $A, B, C, \mu$  come in 4.42. Mostrare che, se vale  $\dim C = \dim A + \dim B - 1$ , allora per ogni  $c \in C$  esistono  $a, b$  tali che  $c = \mu(a \otimes b)$ . Utilizzare questo fatto per mostrare che ogni forma binaria di grado  $\geq 2$  a coefficienti in  $\mathbb{K}$  non è irriducibile e quindi che  $\mathbb{K}$  è algebricamente chiuso.

**4.44.** Sia  $A$  un anello,  $I \subset A[x]$  un ideale e  $B = A[x]/I$ . Provare che  $I$  contiene un polinomio monico se e solo se  $B$  è un  $A$ -modulo finitamente generato.

**4.45 (Seconda dimostrazione alternativa del lemma di proiezione 4.4.3).** Questa dimostrazione sostituisce, grazie all'Esercizio 4.44, l'utilizzo del risultante con il lemma di Nakayama 1.7.2 (cfr. [Reid1988, Esercizio II.3.15]).

Per dimostrare che  $(a_1, \dots, a_{n-1}) \in V(J^e)$  appartiene alla proiezione di  $V(J)$  occorre dimostrare, come in 4.4.3, che  $1 \notin \phi(J)$ . Considerare, nelle notazioni di 1.7.2,  $A = \mathbb{K}[x_1, \dots, x_{n-1}]$ ,  $M = \mathbb{K}[x_1, \dots, x_n]/J$ ,  $N = 0$  e  $I = (x_1 - a_1, \dots, x_{n-1} - a_{n-1}) \subset A$ . Se per assurdo  $1 \in J + I\mathbb{K}[x_1, \dots, x_n]$  allora  $IM = M$  e applicare 1.7.2 per arrivare ad una contraddizione.

**4.46.** Siano  $A \subset B$  anelli Noetheriani con  $B$  finitamente generato come  $A$ -modulo. Provare:

1. Ogni  $x \in B$  è radice di un polinomio monico a coefficienti in  $A$ . (Sugg.: polinomio caratteristico della moltiplicazione per  $x$ .)
2. Se  $I \subset A$  è un ideale proprio, allora  $IB \neq B$ . (Sugg. Nakayama.)
3. Se  $\mathbb{K}$  è un campo algebricamente chiuso, allora ogni morfismo  $A \rightarrow \mathbb{K}$  si estende ad un morfismo  $B \rightarrow \mathbb{K}$ . (Sugg.: usare il lemma di Zorn ed il punto 2 per ricondursi al caso  $A$  campo e  $B = A[x]$ , con  $x$  algebrico su  $A$ .)

## 4.7 Un lungo esercizio: il teorema di Lüroth

Gli esercizi di questa sezione, svolti nella sequenza proposta forniranno una dimostrazione del seguente celebre teorema.

**Teorema 4.7.1 (Lüroth (1875)).** *Sia  $\mathbb{K}$  un campo algebricamente chiuso e  $L \subset \mathbb{K}(x)$  un sottocampo. Se  $\mathbb{K}$  è strettamente contenuto in  $L$ , allora  $L$  è una estensione puramente trascendente di  $\mathbb{K}$ .*

**Esercizi**

**4.47 (versione geometrica, \*).** Sia  $\mathbb{K}$  un campo algebricamente chiuso e  $F(x, y) \in \mathbb{K}[x, y]$  un polinomio con le seguenti proprietà:

1. La relazione  $\sim$  così definita:  

$$a \sim b \quad \text{se e solo se } (a, b) \in V(F) \subset \mathbb{K}^2,$$
è una relazione di equivalenza su  $\mathbb{K}$ .
2.  $F$  è combinazione lineare di monomi  $x^a y^b$ , con  $a, b \leq n$ .
3. Esiste  $x_0 \in \mathbb{K}$  tale che il polinomio  $F(x_0, y) \in \mathbb{K}[y]$  possiede  $n$  radici semplici distinte.

Provare che esistono  $f, g \in \mathbb{K}[t]$  di grado  $\leq n$  tali che  $F(x, y) = f(x)g(y) - f(y)g(x)$ . (Sugg.: svolgere nell'ordine i seguenti punti:

1. Non è restrittivo supporre che  $F$  non contenga fattori del tipo  $x - a, y - b$ .
2. Il polinomio  $F$  è ridotto e  $F(x, y) = \delta F(y, x)$ , con  $\delta \in \mathbb{K}$  tale che  $\delta^2 = 1$ .
3. Esistono  $n$  punti distinti  $a_1, \dots, a_n \in \mathbb{K}$  tali che  $F(a_i, y) = c_i F(a_1, y)$  per opportune costanti  $c_2, \dots, c_n \in \mathbb{K}$ .
4. Sia  $V \subset \mathbb{K}[y]$  il sottospazio vettoriale dei polinomi di grado  $\leq n$ ; dimostrare che l'immagine dell'applicazione  $\mathbb{K} \rightarrow V, a \mapsto F(a, y)$ , è contenuta in un piano  $P \subset V$ .
5. Sia  $f, g$  una base di  $P$ . Per ogni  $a \in \mathbb{K}$  esistono costanti  $\alpha, \beta$  tali che  $F(a, y) = \alpha f(y) - \beta g(y)$ . Se  $g(a)f(a) \neq 0$  esiste una costante  $c_a$  tale che  $F(a, y) = c_a(g(a)f(y) - f(a)g(y))$ .
6. Utilizzare la simmetria di  $F$  (punto 2) per mostrare che  $c_a = c$  non dipende da  $a$ .

**4.48 (\*).** Siano  $p, q \in \mathbb{K}[x]$  senza fattori comuni e sia  $n$  il massimo dei gradi di  $p$  e  $q$ . Si ponga  $\phi = \frac{p}{q} \in \mathbb{K}(x)$ ,  $F(x, y) = p(x)q(y) - p(y)q(x)$  e

$$\Sigma(F) = \left\{ \frac{r(x)}{s(x)} \mid F(x, y) \text{ divide } r(x)s(y) - r(y)s(x) \right\}.$$

Provare che  $\Sigma(F) = \mathbb{K}(\phi)$  e che  $\Sigma(F) \subset \mathbb{K}(x)$  è una estensione algebrica finita di grado  $n$ . Si noti che  $n$  è il grado di  $F$  rispetto alla variabile  $y$ . (Sugg.: provare nell'ordine i seguenti punti:

1.  $\Sigma$  è un campo contenente  $\mathbb{K}(\phi)$ .
2. L'estensione  $\mathbb{K}(\phi) \subset \mathbb{K}(x)$  ha grado  $\leq n$ .
3. Siano  $r, s \in \mathbb{K}[x]$  senza fattori comuni, se  $r(x)s(y) - r(y)s(x)$  non è ridotto, allora  $\text{char} \mathbb{K} = p > 0$  e  $r, s \in \mathbb{K}[x]^p = \mathbb{K}[x^p]$ ; dedurre che in caratteristica  $p$  vale  $\Sigma(F^p) = \Sigma(F)^p$  e quindi che le estensioni  $\Sigma(F^p) \subset \mathbb{K}(x^p)$  e  $\Sigma(F) \subset \mathbb{K}(x)$  hanno lo stesso grado.
4. Se  $F$  è ridotto, allora l'estensione  $\Sigma(F) \subset \mathbb{K}(x)$  ha grado  $\geq n$ : se

$$g(t, x) = t^h + \sum_{i=0}^{h-1} t^i \frac{r_i(x)}{s_i(x)}$$

è il polinomio minimo di  $x$  su  $\Sigma(F)$ , e se  $a \in \mathbb{K}$  è tale che  $s_i(a) \neq 0$  e  $F(x, a)$  possiede  $n$  radici distinte  $a = a_1, \dots, a_n$ , allora  $g(a_i, a) = 0$  per ogni  $i = 1, \dots, n$ .

**4.49 (versione algebrica effettiva, \*).** Sia  $\mathbb{K}$  algebricamente chiuso e siano  $f_1, \dots, f_d \in \mathbb{K}(x)$ ; scriviamo  $f_i = \frac{p_i}{q_i}$ , con  $p_i, q_i \in \mathbb{K}[x]$  senza fattori comuni. Poniamo  $F_i(x, y) = p_i(x)q_i(y) - p_i(y)q_i(x)$  e sia  $F$  il massimo comune divisore di  $F_1, \dots, F_d$ . Se il polinomio  $F_1$  soddisfa le ipotesi della versione geometrica (Esercizio 4.47), allora anche  $F$  le soddisfa e, nelle notazioni dell'Esercizio 4.48, vale  $\mathbb{K}(f_1, \dots, f_d) = \Sigma(F) = \mathbb{K}(\phi)$  per

qualche  $\phi \in \mathbb{K}(x)$ . (Sugg.: basta dimostrare che  $\mathbb{K}(f_1, \dots, f_d) = \Sigma(F)$ , essendo le rimanenti asserzioni conseguenze immediate della versione geometrica del teorema di Lüroth. Dall'Esercizio 4.48 segue che  $\mathbb{K}(f_i) = \Sigma(F_i) \subset \Sigma(F)$  e quindi  $\mathbb{K}(f_1, \dots, f_d) \subset \Sigma(F)$ . Per il lemma di Gauss (1.5.2)  $F$  coincide con il massimo comune divisore di  $F_1, \dots, F_d$  nell'anello  $\mathbb{K}(x)[y]$ . Sia  $g(y) \in \mathbb{K}(f_1, \dots, f_d)[y]$  il polinomio minimo di  $x$ ; dato che  $g$  divide i polinomi  $p_i(y) - f_i q_i(y)$  in  $\mathbb{K}(x)[y]$ , ne segue che  $g$  divide  $F$  in  $\mathbb{K}(x)[y]$  e quindi il grado dell'estensione  $\mathbb{K}(f_1, \dots, f_d) \subset \mathbb{K}(x)$  è minore o uguale al grado di  $F$  rispetto ad  $y$ . Applicare adesso l'Esercizio 4.48.)

**4.50 (versione nazionalpopolare).** Sia  $\mathbb{K}$  un campo algebricamente chiuso e  $L \subset \mathbb{K}(x)$  un sottocampo. Provare che se  $\mathbb{K}$  è strettamente contenuto in  $L$ , allora  $L$  è una estensione puramente trascendente di  $\mathbb{K}$ . (Sugg.: sia  $f_1 \in L - \mathbb{K}$ , allora  $\mathbb{K}(f_1) \subset \mathbb{K}(x)$  è una estensione finita; a maggior ragione  $\mathbb{K}(f_1) \subset L$  è finita e quindi  $L = \mathbb{K}(f_1, \dots, f_d)$ . Se  $\mathbb{K}$  ha caratteristica  $p > 0$ , allora a meno di sostituire  $x$  con  $x^{p^e}$  per un opportuno  $e \geq 0$ , si può prendere  $f_1 \notin \mathbb{K}(x^p)$ .)



## Curve piane: nozioni base

In tutto il capitolo indicheremo con  $\mathbb{K}$  un campo *algebricamente chiuso*. Denoteremo inoltre  $\mathbb{P}^2 = \mathbb{P}_{\mathbb{K}}^2$  il piano proiettivo su  $\mathbb{K}$ .

### 5.1 Definizioni principali

In prima approssimazione possiamo definire una curva algebrica piana come il luogo dei punti di  $\mathbb{P}^2$  che annullano un polinomio omogeneo nelle coordinate omogenee di  $\mathbb{P}^2$ . Questa definizione, sebbene semplice, non è sufficientemente precisa e presenta qualche difficoltà operativa.

Già nella teoria dei fasci di coniche proiettive si incontrano certi oggetti detti “rette doppie” che, insiemisticamente sono rette, ma che appartengono allo spazio delle coniche di  $\mathbb{P}^2$ .

**Definizione 5.1.1.** *Sia  $x_0, x_1, x_2$  un sistema di coordinate omogenee su  $\mathbb{P}^2$ . Un sottoinsieme  $C \subset \mathbb{P}^2$  si dice una **curva irriducibile** di grado  $n$  se esiste un polinomio irriducibile omogeneo  $F(x_0, x_1, x_2)$  di grado  $n$  tale che  $C = V(F)$ , cioè*

$$C = \{[x_0, x_1, x_2] \in \mathbb{P}^2 \mid F(x_0, x_1, x_2) = 0\}.$$

Ad esempio le rette di  $\mathbb{P}^2$  sono curve irriducibili di grado 1. La definizione di curva irriducibile non dipende dal particolare sistema di coordinate omogenee. Sia infatti  $y_0, y_1, y_2$  un altro sistema e  $x_i = \sum a_{ij}y_j$  con la matrice  $a_{ij}$  invertibile; se  $F(x_0, x_1, x_2) = G(y_0, y_1, y_2)$ , allora vale

$$G(y_0, y_1, y_2) = 0 \quad \text{se e solo se} \quad [y_0, y_1, y_2] \in C.$$

Inoltre il grado di  $F$  è uguale al grado di  $G$  e  $F$  è irriducibile se e solo se  $G$  è irriducibile.

Fissato un sistema di coordinate omogenee  $x_i$ , una curva irriducibile  $C$  determina a meno di costante moltiplicativa il polinomio  $F$  di cui è luogo di zeri. Infatti se  $G(x_0, x_1, x_2) = 0$  per ogni  $[x] \in C$  allora, per il teorema degli zeri 4.5.4,  $F$  divide  $G$  e se  $G$  è irriducibile allora  $G = aF$  per qualche  $a \in \mathbb{K}$ .

**Definizione 5.1.2.** *Una **curva irriducibile con molteplicità** è una coppia  $(C, m)$  dove  $C$  è una curva irriducibile e  $m \in \mathbb{N} - \{0\}$  è un numero intero positivo. Una **curva algebrica piana**  $C$  è un insieme finito di curve irriducibili con molteplicità  $\{(C_1, m_1), \dots, (C_r, m_r)\}$ , con  $C_i \neq C_j$  per ogni  $i \neq j$ .*

Una notazione molto conveniente, che inizieremo ad usare da subito, è quella di rappresentare la curva  $\{(C_1, m_1), \dots, (C_r, m_r)\}$  tramite la combinazione lineare formale  $C = m_1C_1 + m_2C_2 + \dots + m_rC_r$ . La terminologia di base delle curve piane è esposta nella prossima definizione.

**Definizione 5.1.3.** Sia  $C = m_1C_1 + m_2C_2 + \dots + m_rC_r$  una curva algebrica piana. Allora:

- Le curve  $C_i$  si dicono le **componenti irriducibili** di  $C$ .
- Per ogni  $i = 1, \dots, r$ , il numero  $m_i$  viene detto la **molteplicità** della componente  $C_i$ .
- Il sottoinsieme  $\text{Supp}(C) = \cup C_i \subset \mathbb{P}^2$  è detto il **supporto** della curva. Con un leggero abuso di notazione, se  $C$  è una curva e  $p \in \mathbb{P}^2$ , scriveremo  $p \in C$  per indicare che  $p \in \text{Supp}(C)$ .
- Se  $n_1, \dots, n_r$  sono i gradi delle componenti irriducibili  $C_1, \dots, C_r$ , allora il numero  $\text{deg}(C) = n_1m_1 + \dots + n_rm_r$  è detto il **grado** di  $C$ .
- Una componente irriducibile  $C_i$  si dice **multipla** se la sua molteplicità  $m_i$  è maggiore di 1; la curva  $C$  si dice **ridotta** se non possiede componenti multiple, ovvero se  $m_i = 1$  per ogni  $i$ .

Se  $C$  e  $D$  sono curve, la loro “somma”  $C + D$  è la curva che ha come componenti irriducibili l’unione delle componenti di  $C$  e  $D$  e come molteplicità la somma delle stesse, dove si intende che la molteplicità di una curva irriducibile è uguale a 0 se tale curva non è una componente. Il grado della somma è uguale alla somma dei gradi.

Nel resto del capitolo, con il termine curva intenderemo sempre una curva algebrica piana. Le curve di grado 1, 2, 3, 4, 5 e 6 si possono anche chiamare rispettivamente rette, coniche, cubiche, quartiche, quintiche e sestiche.

Fissato un sistema di coordinate omogenee  $x_0, x_1, x_2$ , esiste una bigezione fra l’insieme delle curve algebriche di grado  $n$  ed il proiettivizzato dello spazio vettoriale dei polinomi omogenei di grado  $n$  nelle variabili  $x_0, x_1, x_2$ . Infatti, se  $F$  è un polinomio omogeneo di grado  $n$ , allora esiste una decomposizione in fattori irriducibili  $F = F_1^{m_1} \dots F_r^{m_r}$ : possiamo quindi associare ad  $F$  la curva le cui componenti irriducibili  $C_i$  sono i luoghi di zeri dei polinomi  $F_i$  aventi molteplicità  $m_i$ . Per l’unicità della fattorizzazione, tale curva risulta ben definita.

Sia data viceversa una curva  $C = \sum m_iC_i$ ; per definizione di curva irriducibile possiamo scrivere  $C_i = V(F_i)$ , con  $F_i$  polinomio omogeneo irriducibile per ogni  $i$  e considerare il prodotto  $F = \prod F_i^{m_i}$ . Essendo il polinomio  $F_i$  definito a meno di costante moltiplicativa, anche  $F$  è definito a meno di costante moltiplicativa. Diremo che  $F$  è una equazione di  $C$ . Si noti che in tale corrispondenza biunivoca vale la relazione  $\text{Supp}(C) = V(F)$ .

**Teorema 5.1.4.** (Forma debole del teorema di Bézout) *Siano  $C$  e  $D$  due curve algebriche di gradi  $n$  e  $m$  rispettivamente. Allora:*

1.  $\text{Supp}(C) \cap \text{Supp}(D) \neq \emptyset$ .
2. Se  $\text{Supp}(C) \cap \text{Supp}(D)$  contiene più di  $nm$  punti, allora  $C$  e  $D$  hanno una componente irriducibile in comune.

*Dimostrazione.* Denotiamo  $V = \text{Supp}(C) \cap \text{Supp}(D)$  e sia  $\{p_1, \dots, p_s\} \subset V$  un sottoinsieme di cardinalità  $s$  uguale al minimo fra la cardinalità di  $V$  e  $nm + 1$ . Detta  $L_{ij} = \overline{p_i p_j}$  la retta passante per  $p_i$  e  $p_j$ , possiamo trovare un punto  $q \notin \text{Supp}(C) \cup \text{Supp}(D) \cup_{i \neq j} L_{ij}$  ed un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che  $q = [0, 0, 1]$ . Siano  $F$  e  $G$  equazioni di  $C$  e  $D$  in tali coordinate: si può scrivere

$$F = A_0x_2^n + A_1x_2^{n-1} + \dots + A_n, \quad G = B_0x_2^m + B_1x_2^{m-1} + \dots + B_m,$$

dove  $A_i$  e  $B_i$  sono polinomi omogenei di grado  $i$  nelle coordinate  $x_0, x_1$ ; siccome  $[0, 0, 1] \notin \text{Supp}(C) \cup \text{Supp}(D)$  si ha  $A_0B_0 \neq 0$ . Indichiamo con  $R(x_0, x_1)$  il risultante dell’eliminazione di  $x_2$  da  $F$  e  $G$ . Allora vale  $R(a, b) = 0$  se e solo se i polinomi  $F(a, b, x_2), G(a, b, x_2)$  hanno una radice comune  $x_2 = c$ : questo prova che la cardinalità di  $V$  è maggiore o uguale al numero di radici distinte di  $R$ . Per la Proposizione 4.1.6, il polinomio  $R$  è omogeneo di grado  $nm$  ed è identicamente nullo se e solo se  $F$  e  $G$  hanno un fattore comune. Basta quindi dimostrare che  $R$  si annulla in almeno  $s$  punti distinti di  $\mathbb{P}^1$ .

Sia  $p_i = [a_i, b_i, c_i]$ , allora i polinomi  $F(a_i, b_i, x_2)$  e  $G(a_i, b_i, x_2)$  hanno una radice comune  $x_2 = c_i$  e quindi  $R(a_i, b_i) = 0$  per ogni  $i$ ; siccome  $[0, 0, 1] \notin \cup L_{i_j}$  ne segue che, se  $i \neq j$ , allora  $[a_i, b_i] \neq [a_j, b_j]$ .  $\square$

**Corollario 5.1.5.** *Due curve irriducibili distinte di gradi  $n, m$  hanno al più  $nm$  punti in comune.*

*Dimostrazione.* Immediata.  $\square$

Sia  $F(x_0, x_1, x_2)$  un'equazione di una curva  $C$  e sia  $p = [v_0, v_1, v_2] \in \mathbb{P}^2$ . Diremo che  $p$  è un **punto singolare** di  $C$  se

$$F(v_0, v_1, v_2) = 0 \quad \text{e} \quad \frac{\partial F}{\partial x_i}(v_0, v_1, v_2) = 0 \quad \text{per ogni } i = 0, 1, 2.$$

Si noti che:

1) La definizione di punto singolare è una buona definizione: infatti essendo  $F$  omogeneo, anche le sue derivate parziali sono omogenee. Inoltre se  $y_0, y_1, y_2$  è un diverso sistema di coordinate e  $G$  è un'equazione di  $C$  nelle coordinate  $y_i$ , allora si ha  $G(y) = aF(x)$  per qualche  $a \in \mathbb{K}$  e quindi

$$\frac{\partial G}{\partial y_i} = a \sum_{j=0}^2 \frac{\partial F}{\partial x_j} \frac{\partial x_j}{\partial y_i}$$

2) Se il campo  $\mathbb{K}$  ha caratteristica 0, dalla formula di Eulero (Lemma 1.6.3) segue che un punto  $p$  è singolare per la curva di equazione  $F$  se e solo se  $p$  annulla tutte le derivate parziali di  $F$ .

3) Se  $C$  è irriducibile di grado  $n$  e di equazione  $F$  allora, essendo  $\mathbb{K}$  algebricamente chiuso e quindi perfetto, esiste una derivata parziale non nulla e quindi per Bézout debole (Teorema 5.1.4)  $C$  ha al più  $n(n-1)$  punti singolari. Più avanti miglioreremo questo risultato dimostrando che una curva irriducibile di grado  $n$  può avere al più  $\frac{1}{2}(n-1)(n-2)$  punti singolari.

I punti di una curva che non sono singolari si dicono **lisci**. Una curva **singolare** è una curva che contiene almeno un punto singolare. Una curva che non ha punti singolari si dice **non singolare** oppure **liscia**.

**Proposizione 5.1.6.** *Siano  $C_1, \dots, C_r$  curve algebriche (non necessariamente irriducibili) e sia  $C = C_1 + \dots + C_r$ . Allora:*

1. *Se  $p \in C_i \cap C_j$  per qualche  $i \neq j$ , allora  $p$  è un punto singolare di  $C$ .*
2. *Se  $p \in C_i$  e  $p \notin C_j$  per ogni  $j \neq i$ , allora  $p$  è un punto singolare di  $C$  se e solo se è un punto singolare di  $C_i$ .*
3. *Una curva è ridotta se e solo se possiede un numero finito di punti singolari.*

*Dimostrazione.* Sia  $F_i$  un'equazione della curva  $C_i$ , allora  $F = F_1 \cdots F_r$  è un'equazione per  $C$ . Se  $p \in C_i \cap C_j$ , con  $i \neq j$ , allora  $F_i(p) = F_j(p) = 0$  e per la regola di Leibniz ogni derivata parziale di  $F$  si annulla in  $p$ ; questo prova 1). Se invece  $F_i(p) = 0$  e  $F_j(p) \neq 0$  per ogni  $j \neq i$ , allora la regola di Leibniz implica che, per ogni  $h = 0, 1, 2$  vale  $\frac{\partial F}{\partial x_h}(p) = 0$  se e solo se  $\frac{\partial F_i}{\partial x_h}(p) = 0$ . Siccome una curva  $C = C_1 + \dots + C_r$ , con le  $C_i$  irriducibili, è ridotta se e solo se le  $C_i$  sono distinte, il punto 3) segue dai punti precedenti e dal fatto che ogni curva irriducibile possiede un numero finito di punti singolari.  $\square$

**Esercizi**

**5.1.** Provare che per ogni curva algebrica  $C$ , il supporto  $\text{Supp}(C)$  è un sottoinsieme proprio e infinito di  $\mathbb{P}^2$ .

**5.2.** Mostrare che in caratteristica 0 la curva di Fermat  $x_0^n + x_1^n + x_2^n = 0$  è liscia.

**5.3.** In caratteristica  $\neq 2, 3$ , determinare per quali valori del parametro  $\lambda \in \mathbb{K}$  risultano singolari le cubiche di equazioni

$$x_0x_2^2 = x_1(x_1 + x_0)(x_1 + \lambda x_0), \quad x_0^3 + x_1^3 + x_2^3 - 3\lambda x_0x_1x_2 = 0.$$

**5.4.** Siano  $C_1, \dots, C_r$  curve piane di gradi  $n_1 \geq n_2 \geq \dots \geq n_r$  e sia  $V = C_1 \cap \dots \cap C_r$ . Dimostrare che se  $V$  è finito, allora contiene al più  $n_1 n_r$  punti.

**5.5.** Determinare e descrivere i punti singolari (su  $\mathbb{C}$ ) delle curve di equazioni  $y^3(4z - y)^3 - 4x^4(x + 3z)^2 = 0$ ,  $(8y - x - z)^3 = 216xyz$ ,  $(x^2 - z^2)^2y = (y^2 - z^2)^2x$ .

**5.2 Retta tangente e molteplicità**

Sia  $C$  una curva algebrica piana di grado  $n$  ed equazione  $F$  e sia  $L \subset \mathbb{P}^2$  una retta. Se  $L$  è contenuta nel supporto di  $C$ , allora  $L$  è una componente irriducibile di  $C$ ; se invece  $L$  non è una componente irriducibile di  $C$ , allora presi due punti distinti  $p = [p_0, p_1, p_2]$  e  $q = [q_0, q_1, q_2]$  sulla retta  $L$ , il polinomio

$$f(t_0, t_1) = F(t_0p_0 + t_1q_0, t_0p_1 + t_1q_1, t_0p_2 + t_1q_2)$$

è non nullo ed omogeneo di grado  $n$ . Esistono dunque  $n$  punti di  $L$ , contati con molteplicità in cui  $f = 0$ : chiaramente tali punti corrispondono all'intersezione della curva  $C$  con la retta  $L$ . Per ogni punto  $p \in L$  definiamo il numero  $\nu_p(L, C)$  come la molteplicità della radice  $p$  nel polinomio  $f$ : si vede facilmente che il tutto è ben definito.

*Esempio 5.2.1.* Il punto  $p = [0, 0, 1]$  appartiene all'intersezione della cubica  $C$  di equazione  $F = x_0x_2^2 - x_1^3 - x_0^3$  col la retta  $L$  di equazione  $x_0 + x_1 = 0$ . Calcoliamo  $\nu_p(L, C)$ . Il punto  $q = [1, -1, 0]$  appartiene a  $L$  e quindi  $\nu_p(L, C)$  è la molteplicità in  $t = 0$  del polinomio  $f(t) = F(t, -t, 1)$ . Dato che  $f(t) = t$ , si ha  $\nu_p(L, C) = 1$ . Notiamo inoltre che il polinomio di terzo grado  $f(t)$  ha molteplicità 2 all'infinito e quindi che  $\nu_q(L, C) = 2$ .

**Definizione 5.2.2.** Siano  $L$  una retta,  $C$  una curva e  $p \in L \cap C$ . Se  $\nu_p(L, C) = 1$  diremo che  $L$  è **trasversale** a  $C$  nel punto  $p$ ; se  $\nu_p(L, C) > 1$  diremo che  $L$  è **tangente** a  $C$  nel punto  $p$ . Diremo che  $L$  è tangente a  $C$  se lo è in qualche punto; diremo che è trasversale se non è tangente.

Notiamo che, se esiste una retta trasversale ad una curva  $C$ , allora  $C$  deve essere necessariamente ridotta. Se  $p \in L \subset C$ , poniamo per convenzione  $\nu_p(L, C) = +\infty$ , mentre se  $p \notin C \cap L$  si pone  $\nu_p(L, C) = 0$ .

**Proposizione 5.2.3.** Siano dati una curva  $C$  di equazione  $F$  e due punti distinti  $p = [x_0, x_1, x_2]$  e  $q = [y_0, y_1, y_2]$ , con  $p \in C$ . Allora la retta  $L = \overline{pq}$  è tangente a  $C$  in  $p$  se e solo se

$$F_q(x_0, x_1, x_2) := \sum_{i=0}^2 y_i \frac{\partial F}{\partial x_i}(x_0, x_1, x_2) = 0.$$

*Dimostrazione.* La retta  $L$  è tangente a  $C$  in  $p$  se e solo se  $t = 0$  è una radice multipla di  $f(t) = F(x_0 + ty_0, x_1 + ty_1, x_2 + ty_2)$ , cioè se e solo se  $f'(0) = 0$ , dove  $f'$  denota la derivata di  $f$  rispetto a  $t$ . Basta adesso applicare la regola di derivazione della funzione composta.  $\square$

**Definizione 5.2.4.** La curva  $C_q$  di equazione  $F_q = \sum_{i=0}^2 y_i \frac{\partial F}{\partial x_i}$  si dice la **polare** di  $q$  rispetto a  $C$  (cfr. Esercizio 2.57).

La classe di omotetia di  $F_q$  è ben definita per qualsiasi  $q \in \mathbb{P}^2$ . Lasciamo al lettore la facile verifica che la definizione di  $C_q$  non dipende dal particolare sistema di coordinate omogenee. È possibile che il polinomio  $F_q$  sia identicamente nullo (per esempio se  $C$  è unione di rette passanti per  $q$ ): in tal caso diremo che la polare  $C_q$  è indeterminata.

**Corollario 5.2.5.** Sia  $C$  una curva ridotta di grado  $n$  ed equazione  $F$ . Allora:

1. Se per un punto  $q \notin C$  passano infinite rette tangenti a  $C$ , allora la caratteristica del campo  $\mathbb{K}$  è positiva.
2. Se per un punto  $q \notin C$  passano al più un numero finito di rette tangenti a  $C$ , allora tale numero non supera  $n(n - 1)$ .
3. Esistono infiniti punti  $q \in \mathbb{P}^2 - C$  per cui vale la condizione 2 precedente.

*Dimostrazione.* [1], [2] Le rette tangenti a  $C$  passanti per  $q$  sono tutte e sole quelle  $\overline{qp}$  dove  $F(p) = F_q(p) = 0$ . Dato che  $F_q$  ha grado  $n - 1$ , in virtù del teorema di Bézout, è sufficiente determinare quando  $F$  e  $F_q$  non hanno componenti in comune. Per fare ciò prendiamo un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che  $q = [0, 0, 1]$ ; allora si può scrivere

$$F = A_0 x_2^n + A_1 x_2^{n-1} + \dots + A_n, \quad \text{con } A_0 \neq 0 \quad \text{e } F_q = \frac{\partial F}{\partial x_2}.$$

Se  $F$  e  $F_q$  non hanno fattori comuni, e questo è vero in caratteristica 0 poiché  $F$  non ha fattori multipli, allora per Bézout  $F$  e  $F_q$  hanno al più  $n(n - 1)$  punti di intersezione, questo prova i punti 1 e 2.

[3] Prendiamo come sopra un sistema di coordinate tali che il punto  $[0, 0, 1]$  non appartenga a  $C$ ; si ha quindi che ogni fattore irriducibile di  $F$  ha grado positivo rispetto a  $x_2$ . Siccome il campo  $\mathbb{K}$  è perfetto e  $F$  non ha fattori multipli, i polinomi  $F, \frac{\partial F}{\partial x_0}, \frac{\partial F}{\partial x_1}$  e  $\frac{\partial F}{\partial x_2}$  non hanno fattori comuni e quindi il risultante  $R(a, b, c, x_0, x_1)$  dei polinomi  $F$  e  $a \frac{\partial F}{\partial x_0} + b \frac{\partial F}{\partial x_1} + c \frac{\partial F}{\partial x_2}$  non è nullo; in particolare esistono infiniti punti  $q = [a, b, c] \in \mathbb{P}^2 - C$  tali che  $R(a, b, c, x_0, x_1) \neq 0$  e quindi tali che  $F$  e  $F_q$  non hanno fattori comuni.  $\square$

**Corollario 5.2.6.** Sia  $p$  un punto di una curva  $C$ :

1. Se  $p$  è singolare, allora ogni retta per  $p$  è tangente a  $C$  in  $p$ .
2. Se  $p$  è liscio, allora esiste unica una retta tangente a  $C$  in  $p$ .

*Dimostrazione.* Conseguenza immediata della Proposizione 5.2.3.  $\square$

**Definizione 5.2.7.** Sia  $C$  curva e  $p \in \mathbb{P}^2$ ; si definisce  $\text{mult}_p(C)$  come il minimo dei  $\nu_p(L, C)$  al variare di  $L$  tra le rette passanti per  $p$ . Il numero  $\text{mult}_p(C) \in \mathbb{N}$  viene detto **molteplicità** di  $C$  nel punto  $p$

Si noti che  $\text{mult}_p(C) > 0$  se e solo se  $p \in C$  e vale  $\text{mult}_p(C) > 1$  se e solo se  $p$  è un punto singolare di  $C$ .

Sia  $\mathbb{A}^2 \subset \mathbb{P}^2$  il piano affine ottenuto dal piano proiettivo togliendo la retta all'infinito. Una curva affine è per definizione la restrizione ad  $\mathbb{A}^2$  di una curva algebrica piana  $C$ , più precisamente se  $C = m_1 C_1 + \dots + m_r C_r$ , si pone

$$C \cap \mathbb{A}^2 = m_1(C_1 \cap \mathbb{A}^2) + \dots + m_r(C_r \cap \mathbb{A}^2).$$

Assumiamo che la retta all'infinito non sia una componente irriducibile di  $C$  e sia  $x_0, x_1, x_2$  un sistema di coordinate omogenee tali  $\mathbb{A}^2 = \{x_0 \neq 0\}$ . Il sistema di coordinate affini corrispondente è quindi  $y_1 = \frac{x_1}{x_0}, y_2 = \frac{x_2}{x_0}$ . Denotiamo con  $F$  l'equazione proiettiva di  $C$  e consideriamo il polinomio  $f(y_1, y_2) = F(1, y_1, y_2)$ . Il polinomio  $f$  ha lo stesso grado di  $F$ , e quindi della curva  $C$ . Esiste una corrispondenza biunivoca tra i fattori irriducibili di  $f$  e quelli di  $F$ . Infatti se  $H|F$ , allora  $x_0$  non divide  $H$  e denotando  $h(y_1, y_2) = H(1, y_1, y_2)$  si ha che  $h$  divide  $f$ . Viceversa se un polinomio  $h \in \mathbb{K}[y_1, y_2]$  ha grado  $r$  e divide  $f$ , allora  $H(x_0, x_1, x_2) = x_0^r h\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$  è un polinomio omogeneo che divide  $F$ . In particolare  $F$  è irriducibile se e solo se  $f$  è irriducibile. Chiameremo  $f$  equazione della curva affine  $C \cap \mathbb{A}^2$ .

Siano  $p$  un punto di  $\mathbb{P}^2$  e scegliamo un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che  $p = [1, 0, 0]$ . Sia  $C$  una curva algebrica piana di grado  $n$  e di equazione  $F$ , allora possiamo scrivere l'equazione della curva affine  $C \cap \mathbb{A}^2$  come

$$f(y_1, y_2) = f_m(y_1, y_2) + f_{m+1}(y_1, y_2) + \dots + f_n(y_1, y_2),$$

dove  $f_m \neq 0$  e  $f_i$  è omogeneo di grado  $i$  per ogni  $i = m, \dots, n$ . Dimostriamo che il numero intero  $m \geq 0$  è uguale alla molteplicità  $\text{mult}_p(C)$ . Infatti, per definizione di molteplicità  $\text{mult}_p(C)$  è la minima molteplicità in  $t = 0$  dei polinomi  $f(ty_1, ty_2) = t^m f_m(y_1, y_2) + t^{m+1} \dots$  al variare di  $[y_1, y_2] \in \mathbb{P}^1$ . Notiamo che  $[y_1, y_2] \in \mathbb{P}^1$  è una radice della forma binaria  $f_m$  se e solo se la retta  $L = p + [0, y_1, y_2]$  è tale che  $\nu_p(L, C) > \text{mult}_p(C)$ ; ne deduciamo che tali rette sono in numero finito e sono le componenti irriducibili di una curva di grado  $m = \text{mult}_p(C)$  ed equazione  $f_m$ , chiamata **cono tangente** a  $C$  nel punto  $p$ .

**Proposizione 5.2.8.** *Sia  $C \subset \mathbb{P}^2$  una curva ridotta di grado  $n$  e  $p$  un punto di  $\mathbb{P}^2$ . Se il campo  $\mathbb{K}$  ha caratteristica 0 oppure  $> n$ , allora esiste una retta passante per  $p$  e che interseca  $C - \{p\}$  in esattamente  $n - \text{mult}_p(C)$  punti distinti.*

*Dimostrazione.* Prendiamo un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che  $p = [1, 0, 0]$ . Se  $m = \text{mult}_p(C)$ , allora l'equazione di  $C$  è

$$F = A_m x_0^{n-m} + A_{m+1} x_0^{n-m-1} + \dots + A_n, \quad \text{con } A_i \in \mathbb{K}[x_1, x_2] \text{ e } A_m \neq 0.$$

Sia  $\Delta(x_1, x_2)$  il discriminante di  $F$  considerato come un polinomio di grado  $n - m$  in  $x_0$ : poiché  $F$  non ha fattori multipli e la caratteristica di  $\mathbb{K}$  è uguale a 0 oppure maggiore di  $n - m$ , è facile dedurre che  $\Delta \neq 0$  e vale  $\Delta(v_1, v_2) = 0$  se e solo se  $f(t) = F(t, v_1, v_2) = 0$  ha una radice multipla. Per dimostrare la proposizione è quindi sufficiente considerare una retta di equazione  $x_1 v_2 = x_2 v_1$ , dove la coppia  $(v_1, v_2)$  non annulla il discriminante  $\Delta$ .  $\square$

Un punto di molteplicità 2 si dice un **punto doppio**. Un punto doppio si dice un **nodo** se il cono tangente formato da due rette distinte, altrimenti si dice una **cuspid**; ad esempio la curva affine di equazione  $y^2 = x^2 + x^3$  ha un nodo nel punto di coordinate  $(0, 0)$ , mentre la curva affine  $y^2 = x^n$ , con  $n \geq 3$ , possiede una cuspid in  $(0, 0)$ . Diremo che  $C$  ha una singolarità **ordinaria** in  $p$  se il cono tangente di  $C$  in  $p$  è ridotto: equivalentemente, se  $x, y$  sono coordinate affini tali che  $p = (0, 0)$  e l'equazione affine di  $C$  è  $f = f_m + f_{m+1} + \dots$ , allora  $m = \text{mult}_p(C)$  e la singolarità è ordinaria se e solo se  $f_m$  non ha radici multiple.

**Definizione 5.2.9.** Data una curva  $C$  ed un suo punto liscio  $p$  denoteremo con  $\mathbb{T}_p C$  la retta tangente a  $C$  in  $p$ . Diremo che un punto liscio  $p \in C$  è un **flesso**, o un **punto di flessione**, di  $C$  se  $3 \leq \nu_p(C, \mathbb{T}_p C) < +\infty$ . Chiameremo il numero naturale  $\nu_p(C, \mathbb{T}_p C) - 2$  **molteplicità di flesso**<sup>1</sup> di  $p$ .

Per la Proposizione 5.2.3, se  $F(x_0, x_1, x_2)$  è l'equazione di  $C$  e  $p = [v]$ , allora l'equazione di  $\mathbb{T}_p C$  è

$$x_0 \frac{\partial F}{\partial x_0}(v) + x_1 \frac{\partial F}{\partial x_1}(v) + x_2 \frac{\partial F}{\partial x_2}(v) = 0.$$

### Esercizi

**5.6.** Calcolare il grado del discriminante calcolato nella dimostrazione della Proposizione 5.2.8. Provare inoltre che in caratteristica positiva tale proposizione è generalmente falsa.

**5.7.** Sia  $C$  curva di grado  $n$ . Provare che per ogni  $p \in \mathbb{P}^2$  vale  $\text{mult}_p(C) \leq n$  e che vale  $\text{mult}_p(C) = n$  se e solo se ogni componente irriducibile di  $C$  è una retta passante per il punto  $p$ .

**5.8.** Si determini il numero di rette passanti per il punto  $[1, 1, 0]$  e tangenti alla curva di Fermat  $x_0^n + x_1^n + x_2^n = 0$ , con  $n$  non divisibile dalla caratteristica di  $\mathbb{K}$ .

**5.9 (Teorema di Carnot, 1803).** Sia  $C \subset \mathbb{P}^2$  una curva piana di grado  $m$  e siano  $a_1, \dots, a_n \in \mathbb{P}^2 - C$ . Per ogni  $i = 1, \dots, n$  siano  $b_{i1}, \dots, b_{im}$  i punti di intersezione, contati con molteplicità, di  $C$  con la retta  $\overline{a_i a_{i+1}}$  (intendendo  $a_{n+1} = a_1$ ). Provare che

$$\prod_{j=1}^m [a_1, \dots, a_n; b_{1j}, \dots, b_{nj}] = 1.$$

(Sugg.: prendere un sistema di coordinate affini  $x, y$  tali che la retta all'infinito non contenga alcuno degli  $n(m+1)$  punti  $a_i, b_{ij}$ . Detta  $f$  l'equazione affine di  $C$  si provi che vale

$$\prod_{j=1}^m (a_i a_{i+1} b_{ij}) = \frac{f(a_i)}{f(a_{i+1})}.)$$

**5.10.** Provare che in caratteristica positiva esistono curve irriducibili  $C$  e punti  $q \notin C$  tali che ogni retta passante per  $q$  è tangente a  $C$ .

**5.11.** (caratteristica 0) Sia  $C$  una curva piana e  $p \in C$ . Provare che per un generico punto  $q \in \mathbb{P}^2$  vale  $\text{mult}_p(C_q) = \text{mult}_p(C) - 1$ .

## 5.3 Intersezione di curve piane

Nel paragrafo precedente abbiamo visto che una curva piana  $C \subset \mathbb{P}^2$  interseca una retta  $L$  in esattamente  $\text{deg}(C)$  punti contati con molteplicità, a meno che  $L$  non sia una componente irriducibile di  $C$ . Inoltre, nella dimostrazione della forma debole del teorema di Bézout abbiamo costruito una bigezione fra l'insieme dei punti in comune a due curve  $C, D$  di gradi  $n, m$  senza componenti comuni e l'insieme delle radici su  $\mathbb{P}^1$  di un polinomio risultante  $R$  omogeneo di grado  $nm$ . Queste considerazioni fanno ben sperare nella validità del seguente risultato.

<sup>1</sup> Alcuni autori distinguono i punti di flessione in flessi ordinari e flessi multipli: i primi hanno molteplicità di flesso uguale a 1, i secondi maggiore di 1.

**Teorema 5.3.1 (di Bézout<sup>2</sup>).** *Due curve piane proiettive, senza componenti comuni, di gradi  $n$  e  $m$  si intersecano in  $nm$  punti contati con molteplicità.*

Naturalmente occorre definire con precisione cosa intendiamo per molteplicità di un punto di intersezione. Le principali definizioni (tutte equivalenti) che vedremo in queste note sono:

1. Definizione per proiezione generica (Definizione 5.3.2).
2. Definizione analitica (Corollario 8.3.2).
3. Definizione parametrica (Teorema 8.3.4: si tratta della definizione data nel paragrafo precedente quando una delle due curve è una retta).

La definizione per proiezione generica è la più elementare ed è motivata dalla dimostrazione di Bézout debole.

Siano dunque  $C$  e  $D$  due curve piane proiettive senza componenti comuni di gradi  $n$ ,  $m$  ed equazioni  $F$ ,  $G$  rispettivamente. Denotiamo con  $p_1, \dots, p_r$ , i loro punti di intersezione; abbiamo già dimostrato che  $r \leq nm$ . Per ogni coppia di indici  $i \neq j$  indichiamo con  $L_{ij}$  la retta  $\overline{p_i p_j}$ . Diremo provvisoriamente che un punto  $q \in \mathbb{P}^2$  è *generico* se non appartiene all'unione di  $C, D$  e delle rette  $L_{ij}$ . Prendiamo un qualsiasi punto generico  $q$  e fissiamo un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che  $q = [0, 0, 1]$ . Se  $p_i = [a_i, b_i, c_i]$ , per  $i = 1, \dots, r$ , allora poiché  $[0, 0, 1] \notin \cup L_{ij}$  ne segue che  $[a_i, b_i] \neq [a_j, b_j]$  per ogni  $i \neq j$  e si ha

$$F = A_0 x_2^n + A_1 x_2^{n-1} + \dots + A_n, \quad G = B_0 x_2^m + B_1 x_2^{m-1} + \dots + B_m,$$

dove  $A_i$  e  $B_i$  sono polinomi omogenei di grado  $i$  nelle coordinate  $x_0, x_1$  e  $A_0 B_0 \neq 0$ . Denotiamo con  $R(x_0, x_1)$  il risultante di  $F$  e  $G$  calcolato eliminando la variabile  $x_2$ , allora, per ogni  $i = 1, \dots, r$ , i due polinomi  $F(a_i, b_i, x_2)$  e  $G(a_i, b_i, x_2)$  hanno una radice comune  $x_2 = c_i$  e quindi  $R(a_i, b_i) = 0$ .

**Definizione 5.3.2.** *Nelle notazioni precedenti si definisce la **molteplicità di intersezione** di  $C$  e  $D$  nel punto  $p_i$  come:  $\nu_{p_i}(C, D) = \text{molteplicità della radice } [a_i, b_i] \text{ in } R$ .*

Dal prossimo Teorema 5.3.3 seguirà che si tratta di una buona definizione, cioè che i numeri  $\nu_{p_i}(C, D)$  non dipendono dalla scelta del punto generico e del sistema di coordinate omogenee. Mostrato questo, il teorema di Bézout diventa una conseguenza immediata del fatto che  $R$  è omogeneo di grado  $nm$ .

**Teorema 5.3.3 (Regola di Halphen, 1873).** *La molteplicità di intersezione di due curve in un punto è ben definita.*

*Dimostrazione.* Vediamo per prima cosa che la molteplicità non dipende dal particolare sistema di coordinate. Sia infatti  $y_0, y_1, y_2$  un secondo sistema di coordinate tali che  $q = \{y_0 = y_1 = 0\}$  e legato al precedente dalle relazioni

$$\begin{cases} x_0 = ay_0 + by_1 \\ x_1 = cy_0 + dy_1 \\ x_2 = hy_0 + ky_1 + y_2 \end{cases} \quad ad \neq bc.$$

<sup>2</sup> L'enunciato del Teorema 5.3.1 risale a Mac-Laurin (1720), i primi accenni di dimostrazione si devono a Eulero (1748) e Cramer (1750); una trattazione più completa fu data da Bézout (1779), mentre per la prima dimostrazione completa e rigorosa bisogna aspettare il teorema fondamentale dell'algebra (Gauss 1799) e la nozione corretta di molteplicità di intersezione (Halphen 1873). Spesso (e.g. [Cre1862]) il Teorema 5.3.1 veniva ammesso come principio evidente.



Consideriamo un terzo sistema di coordinate omogenee  $z_0, z_1, z_2$  legato ai precedenti dalle relazioni:

$$\begin{cases} z_0 = y_0 \\ z_1 = y_1 \\ z_2 = hy_0 + ky_1 + y_2, \end{cases} \quad (5.1)$$

$$\begin{cases} x_0 = az_0 + bz_1 \\ x_1 = cz_0 + dz_1 \\ x_2 = z_2 \end{cases} \quad ad \neq bc. \quad (5.2)$$

Dall'invarianza rispetto alle traslazioni del risultante (Proposizione 4.1.3) segue l'invarianza di  $R$  per la trasformazione (5.1), mentre dalla funtorialità del risultante segue che la trasformazione (5.2) lascia invariate le molteplicità delle radici di  $R$  e quindi non cambia le molteplicità di intersezione.

Adesso bisogna dimostrare che la molteplicità non dipende dalla scelta del punto generico  $q$ . Sia  $q'$  un altro punto generico e si prenda un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che  $q = [0, 0, 1]$ ,  $q' = [0, 1, 0]$ ,  $p_1 = [a, 1, 1]$  per qualche  $a \in \mathbb{K}$  e

$$[1, 0, 0] \notin C \cup D \cup_{i \neq j} \overline{p_i p_j} \cup_i \overline{q p_i} \cup_i \overline{q' p_i}.$$

In tale sistema di coordinate, siano  $R_1, R_2$  i risultanti di  $F, G$  ottenuti eliminando  $x_1, x_2$  rispettivamente; per dimostrare che  $\nu_{p_1}(C, D)$  è ben definita bisogna dimostrare che  $[a, 1]$  è radice di eguale molteplicità dei polinomi  $R_1(x_0, x_2)$  e  $R_2(x_0, x_1)$ . Per fare questo introduciamo la curva di Chow  $\text{Ch}(C, D) \subset (\mathbb{P}^2)^\vee$  della coppia  $C, D$ . Se  $\lambda = (\lambda_1, \lambda_2) \in \mathbb{K}^2$ , denotiamo con  $L_\lambda \subset \mathbb{P}^2$  la retta di equazione  $x_0 = \lambda_1 x_1 + \lambda_2 x_2$ ; si noti che le rette  $L_\lambda$  sono, al variare di  $\lambda \in \mathbb{K}^2$ , tutte e sole le rette che non passano per il punto  $[1, 0, 0]$ . Si considerino adesso i polinomi:

$$\begin{aligned} f(\lambda_1, \lambda_2, x_1, x_2) &= f_\lambda(x_1, x_2) = F(\lambda_1 x_1 + \lambda_2 x_2, x_1, x_2), \\ g(\lambda_1, \lambda_2, x_1, x_2) &= g_\lambda(x_1, x_2) = G(\lambda_1 x_1 + \lambda_2 x_2, x_1, x_2) \end{aligned}$$

e sia  $R(\lambda_1, \lambda_2)$  il risultante delle forme binarie  $f_\lambda, g_\lambda$ . Si definisce  $\text{Ch}(C, D)$  come la chiusura proiettiva della curva affine definita dall'equazione  $R(\lambda_1, \lambda_2)$ . Poiché  $R(\lambda_1, \lambda_2) = 0$  se e solo se  $L_\lambda$  contiene almeno un punto di intersezione di  $C$  e  $D$ , ne deriva che le componenti irriducibili di  $\text{Ch}(C, D)$  sono tutte e sole i fasci di rette passanti per i punti di intersezione di  $C$  e  $D$ . Sia  $\nu_1$  la molteplicità, come componente di  $\text{Ch}(C, D)$ , del fascio di rette  $\{\lambda_1 + \lambda_2 = a\}$  di centro  $p_1$  e dimostriamo che  $\nu_1$  coincide con le molteplicità di intersezione di  $C$  e  $D$  calcolate rispetto alle proiezioni dai punti generici  $q, q'$ . Iniziamo con l'osservare che se  $E_j$  indica il fascio di rette per  $p_j$ , allora, dato che  $q, q'$  sono generici, si ha che  $(a, 0), (0, a) \in E_1 - \cup_{j \neq 1} E_j$  ed i polinomi  $R(t, 0), R(0, t)$  non sono identicamente nulli. Si noti che  $R(t, 0), R(0, t)$  rappresentano le restrizioni di  $R$  ai fasci di rette passanti per  $q, q'$ . Dunque  $\nu_1$  è uguale alla molteplicità della radice  $t = a$  in entrambi i polinomi  $R(t, 0)$  e  $R(0, t)$ . Siccome  $R(t, 0)$  è il risultante delle forme

$$F(tx_1, x_1, x_2) = A_0(t, 1)x_2^n + A_1(t, 1)x_1x_2^{n-1} + \cdots + A_n(t, 1)x_1^n,$$

$$G(tx_1, x_1, x_2) = B_0(t, 1)x_2^m + B_1(t, 1)x_1x_2^{m-1} + \cdots + B_m(t, 1)x_1^m$$

vale  $R(t, 0) = \pm R_2(t, 1)$ . Allo stesso modo si prova  $R(0, t) = \pm R_1(t, 1)$  e per quanto visto questo conclude la dimostrazione della regola di Halphen.  $\square$

Si noti che dal teorema di Bézout segue che il grado della curva di Chow  $\text{Ch}(C, D)$  è uguale al prodotto dei gradi di  $C$  e  $D$ . Poniamo per convenzione  $\nu_p(C, D) = +\infty$  se  $C$  e  $D$  hanno una componente irriducibile comune passante per  $p$ . Dalle proprietà del risultante seguono immediatamente le seguenti proprietà delle molteplicità di intersezione:

- $\nu_p(C, D) \geq 0$  e vale 0 se e solo se  $p \notin C \cap D$ , (positività).
- $\nu_p(C, D) = \nu_p(D, C)$ , (simmetria).
- $\nu_p(C, D + E) = \nu_p(C, D) + \nu_p(C, E)$ , (bilinearità).

**Teorema 5.3.4.** *Sia  $p$  un punto appartenente all'intersezione di due curve piane  $C$  e  $D$ . Allora  $\nu_p(C, D) \geq \text{mult}_p(C) \text{mult}_p(D)$  e l'uguaglianza vale se e solo se i coni tangenti di  $C$  e  $D$  in  $p$  non hanno componenti comuni.*

*Dimostrazione.* Siano  $F, G$  rispettivamente le equazioni di  $C, D$  in un sistema  $x_0, x_1, x_2$  di coordinate tali che  $p = [1, 0, 0]$  e tali che il punto  $[0, 0, 1]$  sia generico e non appartenente all'unione dei coni tangenti delle due curve nel punto  $p$ . In particolare  $p$  è l'unico punto di intersezione di  $C$  e  $D$  sulla retta  $L = \{x_1 = 0\}$ . Denotiamo  $r = \text{mult}_p(C) = \nu_p(L, C)$  e  $s = \text{mult}_p(D) = \nu_p(L, D)$ . Per definizione, la molteplicità di intersezione  $\nu_p(C, D)$  è uguale alla molteplicità della radice  $x = 0$  nel risultante  $R(x)$  dell'eliminazione di  $y$  dai polinomi

$$f(x, y) = F(1, x, y), \quad g(x, y) = G(1, x, y).$$

Tenendo conto delle molteplicità delle due curve nel punto  $p$ , si può scrivere in modo unico:

$$\begin{aligned} f &= f_0x^r + f_1x^{r-1}y + \dots + f_r y^r + f_{r+1}y^{r+1} + \dots + f_n y^n, \\ g &= g_0x^s + g_1x^{s-1}y + \dots + g_s y^s + g_{s+1}y^{s+1} + \dots + g_m y^m, \end{aligned}$$

per opportuni polinomi  $f_i, g_i \in \mathbb{K}[x]$ . Dunque il risultante  $R(x)$  è il determinante della matrice di Sylvester  $S(f, g)$  che assume la forma

$$\begin{pmatrix} f_0x^r f_1x^{r-1} \dots & \cdot & \cdot & \cdot & \dots & \cdot & f_n & & & \\ & f_0x^r & \dots & \cdot & \cdot & \cdot & \dots & \cdot & & f_n \\ & & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots \\ & & & f_0x^r f_1x^{r-1} f_2x^{r-2} \dots & \cdot & \cdot & \cdot & \dots & f_n & \\ g_0x^s g_1x^{s-1} \dots & \cdot & g_m & & & & & & & \\ & g_0x^s & \dots & \cdot & g_m & & & & & \\ & & \ddots & \vdots & \vdots & \vdots & \ddots & & & \\ & & & g_0x^s g_1x^{s-1} g_2x^{s-2} \dots & g_m & & & & & \\ & & & & g_0x^s g_1x^{s-1} \dots & \cdot & g_m & & & \\ & & & & & g_0x^s & \dots & \cdot & & g_m \\ & & & & & & \ddots & \vdots & \vdots & \ddots \\ & & & & & & & g_0x^s g_1x^{s-1} g_2x^{s-2} \dots & g_m & \end{pmatrix}.$$

Per dimostrare che il monomio  $x^{rs}$  divide  $R(x)$ , ripetiamo nella sostanza la dimostrazione del fatto che il risultante è isobaro. Sia  $\Delta$  la matrice ottenuta da  $S(f, g)$  eseguendo nell'ordine le seguenti operazioni:

1. Se  $1 \leq i \leq s$ , moltiplicare la  $i$ -esima riga per  $x^{s-i+1}$ .
2. Se  $m + 1 \leq i \leq m + r$ , moltiplicare la  $i$ -esima riga per  $x^{m+r-i+1}$ .
3. Se  $1 \leq i \leq r + s$ , dividere la  $i$  esima colonna per  $x^{r+s-i+1}$ .

Si vede facilmente che i coefficienti di  $\Delta$  sono polinomi e che  $R(x) = x^{rs} \det \Delta(x)$ . Rimane da dimostrare che  $\Delta(0)$  è invertibile se e solo se i coni tangenti non hanno componenti comuni. Denotando  $a_i = f_i(0)$  e  $b_i = g_i(0)$ , La matrice  $\Delta(0)$  è uguale a:



*Dimostrazione.* Sia  $F$  l'equazione di  $C$ , per il Corollario 5.2.5 esiste un punto  $q$  tale che l'equazione  $F_q$  della polare  $C_q$  è non nulla e senza componenti in comune con  $F$ . Dato che il grado di  $F_q$  è uguale a  $n - 1$ , è sufficiente dimostrare che per ogni punto  $p$  vale  $\text{mult}_p(F_q) \geq \text{mult}_p(F) - 1$ . Prendiamo un sistema di coordinate omogenee  $x_0, x_1, x_2$  tale che  $q = [0, 0, 1]$  e  $p = [1, 0, 0]$ . Se  $f(x, y) = F(1, x, y)$ , allora l'equazione affine della polare  $C_q$  è uguale alla derivata di  $f$  rispetto a  $y$ ; è allora chiaro che la molteplicità diminuisce al più di 1.  $\square$

**Corollario 5.3.7.** *Siano  $C$  e  $D$  curve piane senza componenti comuni e denotiamo con  $L = \mathbb{T}_p C \subset \mathbb{P}^2$  la retta tangente a  $C$  in un suo punto liscio  $p \in C$ . Se  $\nu_p(L, D) \leq \text{mult}_p(D) + \nu_p(L, C) - 2$ , allora vale  $\nu_p(L, D) = \nu_p(C, D)$ .*

*Osservazione 5.3.8.* Se  $\nu_p(L, C) = 2$  (caso generico) il Corollario 5.3.7 non aggiunge nulla al Teorema 5.3.4. Del Corollario 5.3.7 è interessante anche il metodo di dimostrazione.

*Dimostrazione.* Sia  $q \notin L$  un punto generico (nel senso della Definizione 5.3.2) e siano  $x_0, x_1, x_2$  coordinate omogenee tali che  $p = [0, 0, 1]$ ,  $q = [0, 1, 0]$  e  $L$  sia la retta  $\{x_1 = 0\}$ . Dette  $F, G$  le equazioni di  $C$  e  $D$  nelle coordinate  $x_i$  si ha che  $\nu_p(C, D) =$  molteplicità in 0 del risultante dell'eliminazione di  $y$  dai polinomi  $f(x, y) = F(x, y, 1)$  e  $g(x, y) = G(x, y, 1)$ . Siccome il punto  $q$  non appartiene a  $C \cup D$ , a meno di moltiplicazione per costanti possiamo supporre  $f$  e  $g$  polinomi monici in  $y$ .

Abbiamo visto nel capitolo sul risultante che in tali ipotesi  $R(f, g) = R(f, g + hf)$  per ogni polinomio  $h \in \mathbb{K}[x, y]$ . In base al Teorema 5.3.4 possiamo quindi affermare che la molteplicità in 0 di  $g + hf$  non supera  $\nu_p(C, D)$  per ogni scelta di  $h$ . Dato che  $C$  è liscia in 0 con retta tangente  $y = 0$  si può scrivere  $f = y + \tilde{f}(x, y)$  con  $\text{mult}_0(\tilde{f}) \geq 2$  e  $g(x, y) = g(x, 0) + y\tilde{g}(x, y)$ . Si noti che  $\nu_p(L, D), \nu_p(L, C)$  sono rispettivamente le molteplicità in 0 di  $g(x, 0)$  e  $\tilde{f}(x, 0)$ . Definiamo per ricorrenza dei polinomi  $g_i, \tilde{g}_i$  ponendo:

$$g_0(x, y) = g(x, y), \quad g_i(x, y) = g_i(x, 0) + y\tilde{g}_i(x, y),$$

$$g_{i+1}(x, y) = g_i(x, y) - \tilde{g}_i(x, y)f(x, y) = g_i(x, 0) - \tilde{g}_i(x, y)\tilde{f}(x, y).$$

Si noti che  $g_{i+1}(x, 0) = g_i(x, 0) - \tilde{g}_i\tilde{f}(x, 0)$ ,  $\tilde{g}_i(x, y)\tilde{f}(x, y) = u_i(x, 0) - yg_{i+1}(x, y)$  e che la molteplicità di  $\tilde{g}_i$  in 0 è una funzione strettamente crescente di  $i$ . Dall'esistenza del massimo delle molteplicità di  $g + hf$  si deduce che dopo un numero finito di passi la molteplicità di  $\tilde{g}_i$  è maggiore o uguale a quella di  $g_i(x, 0)$  e quindi la retta  $L$  non appartiene al cono tangente di  $g_i$  nel punto 0. Abbiamo quindi dimostrato che  $\nu_p(C, D) = \text{mult}_0(g_i) = \text{mult}_0(g_i(x, 0))$  per  $i$  sufficientemente grande.

Per finire la dimostrazione basta osservare che la molteplicità di  $\tilde{g}_i$  è maggiore o uguale ad  $\text{mult}_p(D) - 1$  per ogni  $i$  e che quindi la molteplicità di  $\tilde{g}_i f(x, 0)$  è almeno  $\nu_p(L, C) + \text{mult}_p(D) - 1$ . Se  $\nu_p(L, D) \leq \text{mult}_p(D) + \nu_p(L, C) - 2$ , allora i polinomi  $g_i(x, 0)$  hanno quindi tutti la stessa molteplicità in 0.  $\square$

Facendo un po' di attenzione alla dimostrazione di 5.3.7, ci accorgiamo che nell'uguaglianza  $\nu_p(L, D) = \nu_p(C, D)$  il termine a sinistra è definito per via parametrica, mentre il termine a destra è definito per proiezione generica (5.3.2). Quindi, se  $C = L$ , allora l'enunciato non è tautologico e ci dà una dimostrazione dell'equivalenza delle due definizioni di  $\nu_p(L, D)$  (Esercizio 5.12).

## Esercizi

**5.12.** Provare che se  $D$  è una retta, allora la Definizione 5.3.2 è equivalente alla definizione parametrica (vedi in proposito la dimostrazione del Corollario 5.3.7).

**5.13.** Trovare i punti di intersezione delle curve definite, nelle coordinate omogenee  $x, y, z$ , dalle equazioni  $x(y^2 - xz)^2 - y^5 = 0$  e  $y^4 + y^3z + x^2z^2 = 0$ .

**5.14 (Trucco di Berzolari).** Sia  $C$  una curva piana ridotta di grado  $n$  e siano  $L_1, \dots, L_n$  rette tre a tre non concorrenti e tali che  $C$  interseca  $L_1 + L_2 + \dots + L_n$  in  $n^2$  punti distinti. Si costruisca un sottoinsieme  $S \subset C$  di cardinalità  $\frac{1}{2}n(n+3)$  prendendo un punto  $p \in C$  esterno alla curva  $L_1 + L_2 + \dots + L_n$ , gli  $n$  punti di intersezione di  $C$  con  $L_1$  e scegliendo  $r$  punti di  $L_r \cap C$  per ogni  $r = 2, \dots, n$ . Provare che  $C$  è l'unica curva di grado  $n$  che contiene  $S$ .

**5.15 (Trasformata di Tschirnhausen, 1861).** In caratteristica 0, mediante la risoluzione di alcune equazioni di secondo grado è possibile ricondurre la soluzione di una equazione algebrica  $f(x) = x^n + a_1x^{n-1} + \dots + a_n = 0$  alla soluzione di una equazione  $g(y) = y^n + b_3y^{n-3} + \dots + b_n$ . (Sugg.: si consideri il polinomio  $h = y - rx^2 - sx - t$  e sia  $g(y) = \sum b_i y^{n-i}$  il risultante dell'eliminazione di  $x$  da  $f$  e  $h$ . Provare che  $b_i$  è un polinomio omogeneo di grado  $i$  in  $r, s, t$ .)

**5.16.** Utilizzare la trasformata di Tschirnhausen (Esercizio 5.15) per ricondurre la soluzione dell'equazione di quarto grado alla soluzione di una equazione di terzo grado ed una equazione biquadratica  $y^4 + by^2 + c = 0$ .

## 5.4 Sistemi lineari di curve piane

Abbiamo già osservato che le curve piane di grado  $n$  sono in corrispondenza biunivoca con il proiettivizzato dello spazio vettoriale dei polinomi omogenei di grado  $n$ . Più precisamente, alla curva di equazione  $\sum_{ijk} a_{ijk} x_0^i x_1^j x_2^k$  corrisponde il punto di  $\mathbb{P}^N$  di coordinate omogenee  $[a_{ijk}]$ . Chiaramente  $N+1$  è uguale al numero di monomi di grado  $n$  in tre variabili e quindi  $1+N = \frac{1}{2}(n+1)(n+2)$  da cui  $N = \frac{1}{2}n(n+3)$ . Indichiamo con  $|\mathcal{O}(n)|$  lo spazio proiettivo delle curve di grado  $n$ ; un sottospazio proiettivo di  $|\mathcal{O}(n)|$  si dice un **sistema lineare** di curve di grado  $n$ . Lo stesso spazio  $|\mathcal{O}(n)|$  è un sistema lineare che viene detto **completo**. Se  $D_1, \dots, D_r$  sono curve di grado  $n$  denotiamo con  $\langle D_1, \dots, D_r \rangle \subset |\mathcal{O}(n)|$  il sistema lineare da esse generato. Se  $V$  è un sistema lineare, indicheremo con  $\dim V$  la sua dimensione: un sistema lineare di dimensione 1 si dice un **fascio**<sup>3</sup>.

Sia  $V \subset |\mathcal{O}(n)|$  un sistema lineare, un punto  $p \in \mathbb{P}^2$  si dice un **punto base** di  $V$  se per ogni curva  $D \in V$  vale  $p \in D$ ; denoteremo  $BS(V)$  l'insieme dei punti base di  $V$ . Se  $V$  è un sistema lineare di dimensione  $r$  e  $F_0, \dots, F_r$  sono equazioni di un insieme di curve indipendenti di  $V$ , allora le curve di  $V$  sono tutte e sole quelle di equazione  $\sum \lambda_i F_i$ . L'equazione di un iperpiano in  $|\mathcal{O}(n)|$  si dice una **condizione lineare** sulle curve di grado  $n$ .

*Esempio 5.4.1.* Sia  $p \in \mathbb{P}^2$  un punto. La relazione  $p \in D$ , con  $D \in |\mathcal{O}(n)|$ , viene detta **condizione di passaggio per  $p$  su  $|\mathcal{O}(n)|$** . Essa impone una condizione lineare su  $|\mathcal{O}(n)|$ : infatti se  $p = [v_0, v_1, v_2]$ , allora una curva di equazione  $\sum a_{ijk} x_0^i x_1^j x_2^k$  contiene  $p$  se e solo se vale  $\sum a_{ijk} v_0^i v_1^j v_2^k = 0$  e quest'ultima condizione è esattamente l'equazione, nelle coordinate omogenee  $\{a_{ijk}\}$ , di un iperpiano in  $|\mathcal{O}(n)|$ .

Più in generale, sia  $\mathcal{P}$  una proprietà definita sulle curve di grado  $n$  e  $V \subset |\mathcal{O}(n)|$  un sistema lineare; diremo che  $\mathcal{P}$  impone  $r$  condizioni lineari su  $V$  se l'insieme delle  $D \in V$  che soddisfano  $\mathcal{P}$  è un sottospazio proiettivo di codimensione  $r$ . Ad esempio la condizione

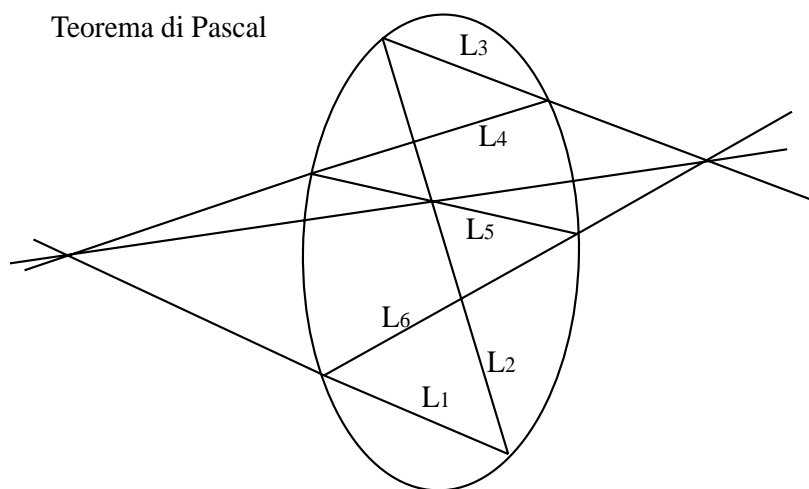
<sup>3</sup> In inglese **pencil**, in francese **pinceau**, in romeno **fascicul**.

di passaggio per un punto  $p$  (il termine passaggio nasce dal fatto di pensare intuitivamente un sistema lineare come una curva che si muove in  $\mathbb{P}^2$  con uno spazio dei parametri che è uno spazio proiettivo) induce una condizione lineare su un sistema  $V$  se e solo se  $p$  non è un punto base di  $V$ .

Un insieme finito di punti  $S \subset \mathbb{P}^2$  si dice in **posizione generica** se per ogni coppia di interi positivi  $m, n$  tali che  $m \leq \frac{1}{2}(n+1)(n+2)$  e per ogni sottoinsieme  $A \subset S$  di cardinalità  $m$ , la condizione di passaggio per i punti di  $A$  impone  $m$  condizioni lineari sulle curve di grado  $n$ . Se  $r \leq n$  e  $p \in \mathbb{P}^2$ , allora  $V = \{D \in |\mathcal{O}(n)| \mid \text{mult}_p(D) \geq r\}$  è un sistema lineare di codimensione  $\frac{1}{2}r(r+1)$ : infatti in un sistema di coordinate omogenee tali che  $p = [1, 0, 0]$ , una curva  $D$  di equazione affine  $0 = a_{00} + a_{10}x + a_{01}y + \dots + a_{ij}x^i y^j + \dots$  soddisfa  $\text{mult}_p(D) \geq r$  se e solo se  $a_{ij} = 0$  per ogni  $i + j < r$ .

**Teorema 5.4.2 (Gergonne, 1827).** *Siano  $C$  e  $D$  due curve piane di grado  $n$  che si intersecano in esattamente  $n^2$  punti distinti. Se  $nm$  di questi punti appartengono ad una curva  $E$  di grado  $m \leq n$ , allora i restanti  $n(n-m)$  punti appartengono ad una curva  $H$  di grado  $n-m$ .*

*Dimostrazione.* Siano  $p_1, \dots, p_{n^2}$  i punti di intersezione di  $C$  e  $D$ , dal teorema di Bézout segue che necessariamente  $C, D, E$  sono curve ridotte e che per ogni  $i$ , il punto  $p_i$  è liscio per  $C$  e  $D$ . Siano  $C_t$ , con  $t \in \mathbb{P}^1$ , le curve del fascio  $V$  generato da  $C$  e  $D$ ; notiamo che  $C \cap D = BS(V)$ . Sia  $E = E_1 + \dots + E_r$  la decomposizione in componenti irriducibili e denotiamo con  $m_i$  il grado di  $E_i$ . Per ogni  $i = 1, \dots, m$ , sia  $q_i \in E_i - BS(V)$  un punto fissato, allora esiste un unico  $t_i \in \mathbb{P}^1$  tale che  $q_i \in C_{t_i}$ . Siccome  $E_i \cap C \cap D$  deve necessariamente contenere  $nm_i$  punti, ne segue che  $E_i \cap C_{t_i}$  contiene almeno  $nm_i + 1$  punti e quindi  $E_i$  è una componente di  $C_{t_i}$ . Osserviamo che se  $q = q_i = q_j \in E_i \cap E_j$ , con  $i \neq j$ , allora  $q$  è un punto singolare di  $E$  e quindi non appartiene ai punti base di  $V$ , ragionando come sopra ne segue che  $t_i = t_j = t$  per ogni  $i, j$ . Dunque  $E$  è contenuta in una curva  $C_t$  del fascio, basta quindi prendere  $H = C_t - E$ .  $\square$



**Figura 5.1.** Il teorema di Pascal

**Corollario 5.4.3.** (Teorema di Pappo-Pascal, III sec d.C.-1640) *Le coppie di lati opposti di un esagono inscritto in una conica ridotta si intersecano in punti allineati.*

*Dimostrazione.* (Plücker, 1828)<sup>4</sup> Siano  $L_1, L_2, \dots, L_6$  i lati successivi di un esagono inscritto in una conica  $E$ . In virtù del teorema di Gergonne 5.4.2, basta osservare che le due cubiche  $C = L_1 + L_3 + L_5$  e  $D = L_2 + L_4 + L_6$  si intersecano in 9 punti e 6 di questi appartengono a  $E$ .  $\square$

Lo studio dei sistemi lineari e delle condizioni lineari è un ottimo strumento per stabilire l'esistenza di curve con opportune caratteristiche. Ad esempio, si considerino  $k$  punti  $p_1, \dots, p_k \in \mathbb{P}^2$  e  $k$  interi positivi  $r_1, \dots, r_k$ . Se  $n(n+3) \geq \sum r_i(r_i+1)$ , allora esiste una curva  $C$  di grado  $n$  tale che  $\text{mult}_{p_i}(C) \geq r_i$  per ogni  $i$ : infatti la dimensione di  $|\mathcal{O}(n)|$  è  $\frac{1}{2}n(n+3)$ , mentre la costrizione  $\text{mult}_{p_i}(C) \geq r_i$  induce al più  $\frac{1}{2} \sum r_i(r_i+1)$  condizioni lineari.

**Teorema 5.4.4 (MacLaurin, 1720).** *Siano  $p_1, \dots, p_k$  i punti singolari di una curva irriducibile di grado  $n$  e siano  $r_1, \dots, r_k$  le rispettive molteplicità. Allora vale la disuguaglianza*

$$(n-1)(n-2) \geq \sum_{i=1}^k r_i(r_i-1).$$

*Dimostrazione.* Indichiamo con  $C$  la curva e definiamo

$$h = \frac{1}{2}((n-1)(n+2) - \sum r_i(r_i-1)).$$

Abbiamo già osservato come dal teorema di Bézout segue  $n(n-1) \geq \sum r_i(r_i-1)$  e, siccome  $(n-1)(n+2) \geq n(n-1)$ , vale  $h \geq 0$ . Siano  $q_1, \dots, q_h$  punti non singolari della curva  $C$ ; per quanto osservato precedentemente esiste una curva  $D$  di grado  $n-1$  passante per  $q_1, \dots, q_h$  e tale che  $\text{mult}_{p_i}(D) \geq r_i-1$  per ogni  $i = 1, \dots, k$ . Dato che  $C$  è irriducibile e distinta da  $D$  vale il teorema di Bézout

$$\begin{aligned} n(n-1) &\geq \sum_{i=1}^k \text{mult}_{p_i}(C) \text{mult}_{p_i}(D) + \sum_{i=1}^h \text{mult}_{q_i}(C) \text{mult}_{q_i}(D) \geq \\ &\geq \sum_{i=1}^k r_i(r_i-1) + h = \frac{1}{2}((n-1)(n+2) + \sum_{i=1}^k r_i(r_i-1)) \end{aligned}$$

da cui segue tutto.  $\square$

Esistono dei casi in cui vale l'uguaglianza nel Teorema 5.4.4. Ad esempio la curva di equazione affine  $y^{n-1} = x^n$  è irriducibile e possiede un punto di molteplicità  $n-1$ .

**Proposizione 5.4.5.** *Siano  $V$  un fascio di curve piane e  $p$  punto base di  $V$ ; allora per ogni terna distinta  $C, D, E \in V$  vale  $\nu_p(C, D) = \nu_p(C, E) = \nu_p(D, E)$ .*

*Dimostrazione.* Segue immediatamente dalle proprietà del risultante, in particolare per il punto 4 della Proposizione 4.1.2.  $\square$

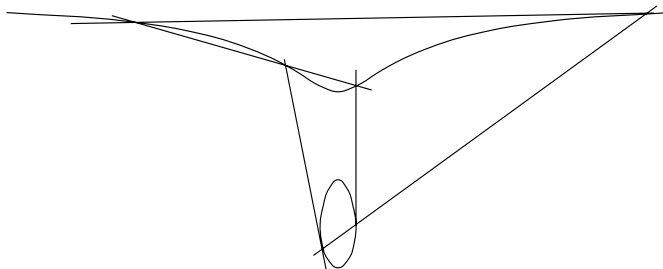
Un'altra significativa applicazione dei sistemi lineari si ha nel seguente:

**Teorema 5.4.6 (Dei tangenziali di MacLaurin, 1748).** *Sia  $C$  una cubica irriducibile; per ogni punto nonsingolare  $p \in C$  si definisce il tangenziale di  $p$  come il terzo punto di intersezione di  $C$  con la retta tangente alla cubica nel punto  $p$ . Se tre punti lisci di  $C$  sono allineati, allora anche i loro tangenziali sono allineati.*

<sup>4</sup> Un'altra elegante dimostrazione sarà proposta nell'Esercizio 6.37. Altre dimostrazioni del teorema di Pascal sono riportate in [Sev1906, §11]. L'argomento utilizzato da Pascal, che nel 1640 aveva 16 anni, per la dimostrazione era quello di ricondursi ad un cerchio mediante una proiezione centrale e poi usare le proprietà metriche della geometria euclidea. Pascal chiamò il Corollario 5.4.3 con il nome di *teorema dell'esagramma mistico*.

*Dimostrazione.* Siano  $p_1, p_2, p_3 \in C$  tre punti lisci ed allineati e sia  $L$  la retta che li contiene: dicendo questo si intende che  $p_1, p_2, p_3$  sono i punti di intersezione di  $L$  e  $C$  contati con molteplicità. Se  $p_1 = p_2$  allora  $p_3$  è per definizione il tangenziale di  $p_1$  e  $p_2$  ed il teorema è banale. Possiamo quindi supporre che la retta  $L$  interseca  $C$  in tre punti distinti.

Siano  $T_1, T_2, T_3$  le rette tangenti a  $C$  nei punti  $p_1, p_2, p_3$  rispettivamente e sia  $V$  il fascio di cubiche generato da  $C$  e  $T_1 + T_2 + T_3$ . Preso un punto  $q \in L - C$  esiste una cubica  $D \in V$  che contiene  $q$ ; poiché i tangenziali sono punti base del fascio  $V$ , essi appartengono anche alla curva  $D$  e, se proviamo che  $D = 2L + R$ , allora sono contenuti nella retta  $R$ . La retta  $L$  interseca  $D$  in almeno quattro punti distinti,  $p_1, p_2, p_3, q$  e per Bézout si ha  $D = L + Q$ , dove  $Q$  è una conica. Per ogni  $i$  vale  $\nu_{p_i}(C, D) = \nu_{p_i}(C, T_1 + T_2 + T_3) \geq 2$  e  $\nu_{p_i}(C, L) = 1$ , si ha quindi che i punti  $p_i$  devono necessariamente appartenere alla conica  $Q$  che deve quindi avere  $L$  come componente.  $\square$



**Figura 5.2.** Tangenziali di MacLaurin

### Esercizi

**5.17.** Calcolare la dimensione del sistema lineare delle coniche passanti per 4 punti non allineati.

**5.18.** Mostrare che, se  $n \geq 2$ , allora non tutte le condizioni lineari su  $|\mathcal{O}(n)|$  sono indotte dal passaggio per un punto.

**5.19.** Provare che il passaggio per  $r$  punti distinti di  $\mathbb{P}^2$  induce  $s$  condizioni lineari su  $|\mathcal{O}(n)|$ , con  $s \leq r$ . Quante condizioni lineari impongono 4 punti allineati su  $|\mathcal{O}(2)|$ ?

**5.20 (Teorema di Gua de Malves, 1740).** Sia  $C$  una cubica irriducibile e  $p, q \in C$  punti lisci di flessione. Provare che il terzo punto di intersezione di  $C$  con la retta  $\overline{pq}$  è ancora un flesso. (Sugg.: tangenziali di MacLaurin.)

**5.21.** Provare che, se  $k$  punti di  $\mathbb{P}^2$  inducono  $k$  condizioni lineari sulle curve di grado  $n$ , allora inducono  $k$  condizioni lineari su  $|\mathcal{O}(m)|$  per ogni  $m \geq n$ .

**5.22 (Principio di Lamé, 1818).** Siano  $C$  e  $D$  curve piane di grado  $n$  che si intersecano in  $n^2$  punti distinti  $p_1, \dots, p_{n^2}$ . Dimostrare che ogni curva di grado  $n$  passante per  $p_1, \dots, p_{n^2}$  appartiene al fascio generato da  $C$  e  $D$ .

**5.23.** Provare che  $n + 1$  punti distinti di  $\mathbb{P}^2$  inducono  $n + 1$  condizioni lineari sul sistema lineare delle curve di grado  $n$ . Si deduca quindi per induzione su  $n$  che la dimensione di  $|\mathcal{O}(n)|$  è  $\frac{1}{2}n(n + 3)$ .



**5.24 (Teorema di Jacobi, 1836).** Si considerino una curva piana di grado  $n$  ed una curva irriducibile di grado  $m \leq n$  che si intersecano in  $nm$  punti distinti  $p_1, \dots, p_{nm}$ . Dimostrare che i punti  $p_1, \dots, p_{nm}$  inducono  $mn - \frac{1}{2}(m-1)(m-2)$  condizioni lineari indipendenti sullo spazio delle curve di grado  $n$ .

*Osservazione 5.4.7.* I teoremi di Gergonne, Jacobi ed il principio di Lamé sono casi particolari del *teorema  $Af + B\phi$  di Max Noether (1872)* che affronteremo e dimostreremo nei prossimi capitoli.

*Osservazione 5.4.8.* (cfr. [EC1915, L 2°, §15]) Può sembrare strano ma, mentre la teoria delle curve algebriche piane è stata uno dei temi centrali della matematica del XVIII secolo, lo sviluppo dell'algebra lineare e degli spazi a più dimensioni nasce invece all'inizio del secolo XIX. Si capisce quindi come nel 1750, Cramer considerasse un paradosso il fatto che  $\frac{1}{2}n(n+3)$  punti contenuti nell'intersezione di due curve non determinano univocamente una curva di grado  $n$  passante per essi.

## 5.5 Esercizi complementari

**5.25.** Sia  $F$  l'equazione di una curva irriducibile di grado  $n$ ; provare che  $F$  possiede almeno due derivate parziali non nulle. (Sugg.: ricordarsi che il campo è perfetto.)

**5.26.** Provare che per le curve ottenute per unione di rette distinte vale l'uguaglianza nella formula del Corollario 5.3.6.

**5.27.** Trovare una quartica irriducibile con tre nodi.

**5.28.** Dati 4 punti distinti del piano proiettivo, tre dei quali non allineati, determinare tutte le quartiche che sono singolari in tali punti. (Sugg.: per il Teorema 5.4.4 tali quartiche non possono essere irriducibili).

**5.29.** (caratteristica  $\neq 2, 3$ ) Provare che ogni cubica irriducibile possiede al più un punto singolare e che ogni cubica irriducibile singolare si può scrivere in un opportuno sistema di coordinate affini come  $y^2 = x^3$  oppure  $y^2 = x^3 + x^2$ .

**5.30.** (caratteristica  $\neq 2, 3$ ) Sia  $f(x, y)$  un polinomio omogeneo di terzo grado. Mostrare che esistono  $\alpha, \beta \in \mathbb{K}$  tali che  $f(x, y) + \alpha(x^3 + xy^2) + \beta(x^2y + y^3)$  è il cubo di un binomio.

**5.31.** Siano  $f_0, f_1, f_2 \in \mathbb{K}[x_0, x_1]$  polinomi omogenei di grado  $n$  senza fattori comuni e consideriamo l'applicazione

$$\phi: \mathbb{P}^1 \rightarrow \mathbb{P}^2, \quad \phi([x_0, x_1]) = [f_0(x_0, x_1), f_1(x_0, x_1), f_2(x_0, x_1)].$$

Provare che l'immagine di  $\phi$  è una curva irriducibile; se inoltre esiste  $c \in \phi(\mathbb{P}^1)$  tale che  $\phi^{-1}(c)$  contiene un solo punto (contato con molteplicità), allora  $\phi(\mathbb{P}^1)$  ha grado  $n$ . (Sugg.: il punto  $[v_0, v_1, v_2]$  appartiene all'immagine di  $\phi$  se e solo se le forme binarie  $v_i f_j - v_j f_i$  hanno una radice comune.)

**5.32.** Precisare il concetto di molteplicità usato nell'Esercizio 5.31.

**5.33.** Sia  $f \in \mathbb{C}[x, y, z]$  irriducibile ed omogeneo di grado  $n$  e sia

$$V_{\mathbb{R}}(f) = \{[x, y, z] \in \mathbb{P}_{\mathbb{R}}^2 \mid f(x, y, z) = 0\}.$$

Provare che vale almeno una delle seguenti possibilità:

1. Esiste una costante  $a \in \mathbb{C} - \{0\}$  tale che  $af \in \mathbb{R}[x, y, z]$ .
2. L'insieme  $V_{\mathbb{R}}(f)$  contiene al più  $n^2$  punti.

**5.34.** Si disegni (approssimativamente) la parte affine reale delle curve di equazioni  $y^2 + x^3(x^2 - 1)^2(x - 2)$ ,  $y^2 = x^2(x - 1)$  e  $y^2 = x^2(x^2 - 2x - 3)$ .

**5.35.** Siano  $L$  una retta in  $\mathbb{P}^2$  e  $u(x, y, z)$  un polinomio omogeneo di grado  $2n - 2$ . Denotiamo con  $[x_i, y_i, z_i] \in \mathbb{P}^2$ , per  $i = 0, \dots, 2n$ , i punti di intersezione, contati con molteplicità, della retta  $L$  con la curva di equazione  $x^{2n+1} + y^{2n+1} + z^{2n+1} = xyz u$ . Provare che vale  $x_0 x_1 \cdots x_{2n} + y_0 \cdots y_{2n} + z_0 \cdots z_{2n} = 0$ .

**5.36.** (caratteristica  $\neq 2, 3$ ) Siano  $F(x_0, x_1, x_2)$  e  $G(x_0, x_1, x_2)$  polinomi omogenei di gradi 2 e 3 rispettivamente. Studiare le singolarità della sestica di equazione  $F^3 - G^2 = 0$ .

**5.37.** Dedurre il teorema dei tangenziali di MacLaurin dal teorema di Carnot (Esercizio 5.9) e dal teorema di Menelao (Esercizio 2.48).

**5.38 (Teorema di Newton).** Sia  $C \subset \mathbb{R}^2$  una conica e siano  $L, M \subset \mathbb{R}^2$  due rette. Per ogni punto  $u \in \mathbb{R}^2$  denotiamo:

- $l_1, l_2$  i punti di intersezione di  $C$  con la retta parallela ad  $L$  e passante per  $u$ .
- $m_1, m_2$  i punti di intersezione di  $C$  con la retta parallela ad  $M$  e passante per  $u$ .

Supponendo che nessuno dei quattro punti  $l_1, l_2, m_1, m_2$  si trovi all'infinito, dimostrare che il rapporto

$$\alpha = \frac{ul_1 \cdot ul_2}{um_1 \cdot um_2}$$

non dipende da  $u$ . (Sugg.: Teorema di Carnot con  $a_1 = u$  e  $a_2, a_3$  i punti all'infinito di  $L, M$ ). Se  $C$  è un cerchio, allora  $\alpha = 1$  (basta calcolarlo per  $u$  uguale al centro): provare che da questo seguono molti teoremi presenti negli Elementi di Euclide e nei testi di geometria delle scuole medie.

**5.39.** Provare che ogni insieme di  $n + 1$  punti del piano proiettivo è contenuto in una curva irriducibile di grado  $\leq n$ . Trovare inoltre, per ogni  $n > 0$ , un insieme di  $n + 1$  punti che non è contenuto in alcuna curva irriducibile di grado  $< n$ . (Sugg.: si possono supporre i punti  $p_0, \dots, p_n$  nel piano affine e  $p_i = (x_i, y_i)$ , con le ascisse  $x_i$  distinte. Si consideri una curva affine di equazione  $y - \sum a_i x^i$ .)

**5.40.** Trovare due polinomi  $f, g \in \mathbb{C}[x, y]$  monici rispetto a  $y$  e senza fattori comuni tali che il risultante di  $f - u$  e  $g - v$  abbia un fattore multiplo in  $\mathbb{C}[x, u, v]$ .

**5.41 (\*).** Sia data una curva irriducibile  $C$  con al più singolarità ordinarie ed un punto  $q \in \mathbb{P}^2$  tale che la polare  $C_q$  sia indeterminata, o equivalentemente tale che tutte le rette tangenti a  $C$  nei suoi punti lisci passano per  $q$  (una curva siffatta si dice *strana*).

Assumendo che  $\text{mult}_q(C) \leq 1$ , si provi che  $C$  è una retta oppure una conica in caratteristica 2 (il risultato è vero anche senza l'ipotesi  $\text{mult}_q(C) \leq 1$ , ma la dimostrazione sembrerebbe richiedere strumenti non ancora visti). (Sugg.: trattare separatamente i casi  $q \in C$  e  $q \notin C$ . Nel primo caso si prendano coordinate affini  $x, y$  tali che  $q = (0, 0)$  e, detta  $f$  l'equazione affine di  $C$ , provare che  $f$  divide  $xf_x + yf_y$ . Nel secondo caso siano  $x, y, z$  coordinate omogenee tali che  $q = [0, 0, 1]$  e, detti  $n, F$  il grado e l'equazione di  $C$ , si provi che la caratteristica di  $\mathbb{K}$  divide  $n$  e che  $F_x, F_y$  hanno un fattore comune di grado  $n - 2$ .)

**5.42.** (caratteristica 0) Sia  $C$  una curva ridotta e  $p \in C$  un suo punto liscio. Provare che esistono al più  $n(n - 1) - 1$  rette tangenti a  $C$  passanti per  $p$ . (Sugg.: nelle notazioni del Corollario 5.2.5 calcolare il grado del risultante di  $F, F_q$  quando  $A_0 = 0$ .)

**5.43 (\*\*?).** (caratteristica 0) Data una curva  $C$  di grado  $n$ , una retta  $L$  si dice una tangente semplice a  $C$  se  $L \cap C$  contiene esattamente  $n - 1$  punti. Equivalentemente, una retta  $L$  si dice una tangente semplice a  $C$  se  $L \cap C$  contiene 1 punto di molteplicità 2 e  $n - 2$  punti di molteplicità 1. Provare che se  $C$  è liscia esistono al più un numero finito di rette che non sono né trasversali né tangenti semplici a  $C$ . (Questo esercizio potrà essere risolto agevolmente con i risultati della Sezione 11.5.)

**5.44 (\*).** Sia  $p$  un punto contenuto nell'intersezione di due curve piane  $C, D$  e indichiamo con  $t$  il numero (contato con molteplicità) delle componenti comuni ai conici tangenti a  $C$  e  $D$  nel punto  $p$ . Dimostrare che  $\nu_p(C, D) \geq \text{mult}_p(C) \text{mult}_p(D) + t$ . (Sugg.: nella dimostrazione del Teorema 5.3.4 valutare il rango della matrice  $\Delta(0)$  ed utilizzare l'Esercizio 1.20.)

**5.45.** (caratteristica  $\neq 2$ ) Sia  $C$  una curva affine di equazione  $f(x, y) = 0$  avente una cuspidale in  $o = (0, 0)$  e sia  $L$  l'unica componente del cono tangente a  $C$  in  $o$ . Mostrare che le seguenti condizioni sono equivalenti:

1.  $\nu_o(C, L) = 3$ .
2. A meno di un cambio lineare di coordinate si ha

$$f = y^2 + x^3 + \sum \text{monomi di grado} \geq 4.$$

Una cuspidale con tali caratteristiche si dice **cuspidale semplice**.

**5.46.** (caratteristica  $\neq 2, 3$ ) Trovare le tangenti dal punto  $[1, 1, 1]$  alle cubiche di equazioni  $(x^2 + y^2)z = 2x^3$  e  $x^3 + y^3 = 2z^3$ .

**5.47.** Sia  $C$  una curva di grado  $n$ . Provare che, se la caratteristica del campo è uguale a 0 oppure maggiore di  $n$ , allora la polare  $C_q$  è indeterminata se e solo se  $C$  è unione di rette passanti per  $q$ .

**5.48.** 1. (tratto da [Cia1919]) Abbiassi un triangolo  $C$ , sul piano proiettivo complesso, di vertici  $a, b, c$  che chiameremo fondamentale e un punto qualunque  $r$  del suo piano. Siano  $r_1, r_2, r_3$  le proiezioni di  $r$  fatte da ciascun vertice del triangolo fondamentale sul lato opposto, di guisa che  $r_1$  sia la proiezione sopra  $\overline{bc}$ ,  $r_2$  quella sopra  $\overline{ca}$ ,  $r_3$  quella sopra  $\overline{ab}$ . Indichiamo con  $r'_1$  il coniugato armonico di  $r_1$  rispetto a  $b, c$  (cioè  $[b, c; r_1, r'_1] = -1$ ), con  $r'_2$  il coniugato armonico di  $r_2$  rispetto a  $c, a$ , con  $r'_3$  il coniugato armonico di  $r_3$  rispetto a  $a, b$ . Ebbene si dimostri che i tre punti  $r'_1, r'_2, r'_3$  esistono su di una medesima retta  $R$ .

2. Provare che la retta  $R$  costruita in 1 coincide con la polare seconda  $C_{rr}$ .

**5.49.** Per ogni intero  $n \geq 0$  si determini il massimo intero  $k = k(n)$  tale che, presi comunque  $k$  punti distinti  $p_1, \dots, p_k \in \mathbb{P}^2$ , il passaggio per  $p_1, \dots, p_k$  impone esattamente  $k$  condizioni lineari sulle curve di grado  $n$  (esempio  $k(2) = 3$ ).

**5.50.** Siano  $a, b, c$  tre punti distinti di una conica irriducibile e siano  $A, B, C$  le rispettive rette polari. Dimostrare che i punti  $p = A \cap \overline{bc}$ ,  $q = B \cap \overline{ca}$  e  $q = C \cap \overline{ab}$  sono allineati.

**5.51.** Sia  $L \subset \mathbb{P}^2$  una retta e  $p \in L$  un suo punto. Siano  $C$  e  $D$  curve piane dello stesso grado senza componenti comuni. Provare che:

1. Esiste al più una curva  $C' \in \langle C, D \rangle$  contenente  $L$ .
2. Per ogni  $C' \in \langle C, D \rangle$  si ha  $\nu_p(L, C') \geq \min(\nu_p(L, C), \nu_p(L, D))$ : mostrare inoltre che la disuguaglianza  $\nu_p(L, C') > \min(\nu_p(L, C), \nu_p(L, D))$  vale per al più un numero finito di curve  $C'$  del fascio.

Dire inoltre se i punti 1 e 2 continuano a valere se si considera una curva irriducibile  $E$  al posto della retta  $L$ ?

**5.52.** Costruire un sistema lineare di quartiche di dimensione 3 con esattamente 12 punti base.

**5.53.** Siano  $C, D, C'$  curve piane dello stesso grado e supponiamo che: la curva  $C'$  è irriducibile, le curve  $C$  e  $D$  non hanno componenti comuni e, per ogni punto  $p \in C \cap D$ , vale  $\nu_p(C, D) = \nu_p(C', D) = \nu_p(C', C)$ . Provare allora che  $C' \in \langle C, D \rangle$ . Mostrare inoltre che il risultato è in generale falso se  $C'$  ha delle componenti multiple.

**5.54.** Sia dato un quadrilatero in  $\mathbb{P}^2$  di vertici  $a, b, c, d$  e siano  $e, f, g$  i punti di intersezione delle diagonali. Dimostrare che due cubiche passanti per  $a, b, c, d, e, f, g$  ed aventi un contatto multiplo in  $e$  hanno il nono punto di intersezione sulla retta  $fg$ .

**5.55.** (caratteristica 0) Sia dato un fascio di curve di grado  $n$  e sia  $L$  una retta che non ne interseca il luogo base. Provare che vi sono al più  $2n - 2$  curve del fascio che sono tangenti a  $L$ . Mostrare inoltre con un esempio che lo stesso risultato è generalmente falso in caratteristica positiva.

**5.56.** Siano  $p_1, \dots, p_8 \in \mathbb{P}^2$  otto punti in posizione generica e sia  $S$  una sestica con 8 punti doppi in  $p_1, \dots, p_8$ . Provare che l'equazione di  $S$  può essere scritta nella forma  $aU^2 + bUV + cV^2 = CQ$ , dove  $U, V$  sono equazioni di cubiche passanti per  $p_1, \dots, p_8$  e  $C$  è l'equazione della conica passante per  $p_1, \dots, p_5$ .

**5.57.** (caratteristica  $\neq 2$ ) Provare che esistono quartiche irriducibili con tre cuspidi. (Sugg.: si determini il sistema lineare delle quartiche aventi punti singolari in  $[1, 0, 0]$ ,  $[0, 1, 0]$  e  $[0, 0, 1]$ .)

**5.58.** Sia  $Q$  una quartica irriducibile con tre cuspidi in  $p_1, p_2, p_3$ . Provare che i coni tangenti a  $Q$  in  $p_1, p_2, p_3$  sono rette concorrenti.

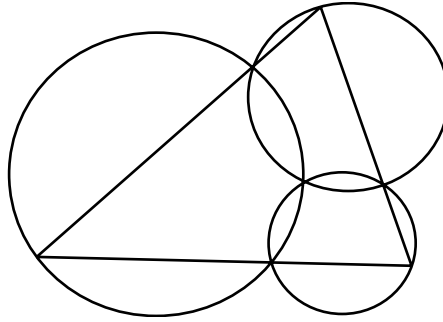
**5.59.** Sia  $F \in \mathbb{C}[x_0, x_1, x_2]$  omogeneo di grado 2 e sia  $C \subset \mathbb{C}^2$  la curva affine di equazione  $f(x, y) = F(x, y, 1)$ . Provare che le seguenti condizioni sono equivalenti:

1.  $C \cap \mathbb{R}^2$  è un cerchio.
2.  $F(1, i, 0) = F(1, -i, 0) = 0$  e  $C \cap \mathbb{R}^2$  contiene almeno tre punti non allineati.

I due punti all'infinito  $[1, \pm i, 0]$  si dicono **punti ciclici**.

**5.60 (Teorema di Miquel, 1838).** Siano  $A_{11}, A_{22}$  e  $A_{33}$  i vertici di un triangolo in  $\mathbb{R}^2$  e per ogni coppia  $(i, j)$  sia  $A_{ij} = A_{ji}$  un punto interno al lato di estremi  $A_{ii}$  e  $A_{jj}$ . Detto  $C_i \subset \mathbb{R}^2$  il cerchio passante per i tre punti  $A_{i1}, A_{i2}, A_{i3}$ , provare che  $C_1 \cap C_2 \cap C_3 \neq \emptyset$  (Figura 5.3). (Sugg.: sia  $L_i$  la retta contenente il lato del triangolo opposto ad  $A_{ii}$  e si considerino le curve  $B_i = C_i + L_i$ , per  $i = 1, 2, 3$ . Per continuità si può assumere che esista una coppia  $i, j$  tale che  $B_i$  interseca  $B_j$  in 9 punti distinti di  $\mathbb{P}_{\mathbb{C}}^2$ . Usare quindi il teorema di Gergonne e l'Esercizio 5.59.)

**5.61 (\*).** Un sistema lineare bidimensionale  $V$  di curve piane si dice una **rete di Laguerre** se esiste un isomorfismo proiettivo  $\phi: \mathbb{P}^2 \rightarrow V$  tale che  $p \in \phi(p)$  per ogni  $p \in \mathbb{P}^2$ . Dati 7 punti di  $\mathbb{P}^2$  in posizione generica (cioè nessuna terna allineata e nessuna sestupla in una conica) provare che le cubiche passanti per i sette punti formano una rete di Laguerre. (Sugg.: Siano  $C_1, C_2$  cubiche generiche per i 7 punti di equazione  $F_1, F_2$  e siano  $a, b$  i rimanenti punti di intersezione; provare che la retta  $L = \overline{ab}$  non contiene alcuno dei sette punti base. Esistono coordinate omogenee  $x_0, x_1, x_2$  tali che  $L = \{x_0 = 0\}$  e  $x_1F_1 + x_2F_2$  è nulla su  $L$ .)



**Figura 5.3.** Teorema di Miquel

**5.62.** Siano  $C$  e  $D$  curve di grado  $n$  tali che  $\text{Sing}(C) \cap D = \emptyset$ . Provare che, se  $E$  è una curva di grado  $n$  tale che  $\nu_p(C, D) = \nu_p(C, E)$  per ogni  $p \in C$ , allora  $C$  è ridotta e appartiene al fascio di curve generato da  $E$  e  $D$ . Provare inoltre che tale risultato è generalmente falso se  $D$  contiene un punto singolare di  $C$ .

### 5.6 Un lungo esercizio: il teorema di Bertini

Gli esercizi di questa sezione, svolti nella sequenza proposta, permettono di dimostrare in modo abbastanza elementare il teorema di Bertini per i sistemi lineari di curve piane. La versione generale del teorema sarà dimostrata nella Sezione 11.4.

**Teorema 5.6.1 (di Bertini).** *In caratteristica 0, il generico elemento di un sistema lineare di curve piane è liscio al di fuori del luogo base.*

#### Esercizi

**5.63.** Sia  $M(n, n + 1)$  lo spazio vettoriale delle matrici  $A = (a_{ij})$ , con  $i = 1, \dots, n$  e  $j = 0, \dots, n$ . Per ogni  $A = (a_{ij}) \in M(n, n + 1)$  denotiamo con  $A^k = \det(a_{ij})_{j \neq k}$ , per  $k = 0, \dots, n$ , i determinanti minori di ordine  $n$ .

Sia  $f: M(n, n + 1) \rightarrow \mathbb{K}$  una funzione polinomiale tale che  $f(GA) = \det(G)^d f(A)$  per ogni  $A \in M(n, n + 1)$  ed ogni  $G \in \text{GL}(n)$ ; provare che esiste un unico polinomio omogeneo  $g(y_0, \dots, y_n)$  di grado  $d$  tale che  $f(A) = g(A^0, \dots, A^n)$ .

**5.64.** (caratteristica 0) Sia  $F(x_0, x_1, x_2)$  un polinomio omogeneo irriducibile di grado  $n$  e sia  $C = V(F) \subset \mathbb{P}^2$  la curva associata.

1. Provare che esiste un polinomio omogeneo  $F^\vee(y_0, y_1, y_2)$  di grado  $n(n - 1)$  tale che  $F^\vee(a_0, a_1, a_2) = 0$  se e solo se la retta  $a_0x_0 + a_1x_1 + a_2x_2 = 0$  è tangente a  $C$ . (Sugg.: nelle notazioni dell'Esercizio 5.63, per ogni matrice  $(a_{ij}) \in M(2, 3)$  sia  $f(A)$  il discriminante della forma binaria di grado  $n$

$$F_A(t_1, t_2) = F(t_1a_{10} + t_2a_{20}, t_1a_{11} + t_2a_{21}, t_1a_{12} + t_2a_{22}).$$

Osservare che, se  $A$  ha rango 2, allora l'immagine della proiettività  $\mathbb{P}^1 \rightarrow \mathbb{P}^2$  indotta dalla matrice  $A$  è la retta  $L_A$  di equazione  $A^0x_0 + A^1x_1 + A^2x_2 = 0$  e che  $f(A) = 0$  se e solo se la retta  $L_A$  è tangente a  $C$ .)

2. Sia  $T \subset (\mathbb{P}^2)^\vee$  la curva di equazione  $F^\vee$  e sia  $L$  una retta di  $\mathbb{P}^2$ ; provare che la molteplicità  $\text{mult}_L(T)$  di  $L$  in  $T$  è uguale a

$$\sum_{p \in L \cap C} \nu_p(C, C_q),$$

dove  $q$  è un generico punto di  $L$ . Caratterizzare le rette corrispondenti a punti lisci di  $T$ .

*Osservazione 5.6.2.* Proveremo nella Sezione 11.5 che, se  $C$  ha grado  $> 1$ , allora  $V(F^\vee) = C^\vee + \sum_i \delta_i F_i$ , dove  $C^\vee$  è una curva irriducibile detta **curva duale** e gli  $F_i$  sono i fasci di rette passanti per i punti singolari di  $C$ . Il grado di  $C^\vee$  viene detto la **classe** di  $C$ .

**5.65.** (caratteristica 0) Si consideri un fascio  $\{D_t \mid t = [t_0, t_1] \in \mathbb{P}^1\}$  di curve piane di grado  $m$  ed equazioni  $t_0 G(x_0, x_1, x_2) + t_1 H(x_0, x_1, x_2)$ ; denotiamo con  $B \subset \mathbb{P}^2$  il luogo base del fascio. Sia  $C \subset \mathbb{P}^2$  una curva irriducibile di grado  $n$  non contenuta in alcuna curva  $D_t$  del fascio.

Provare che esiste una retta  $L$ , trasversale a  $C$ , tale che  $L \cap B \cap C = \emptyset$  e per gli  $n$  punti distinti di  $L \cap C$  passano  $n$  curve distinte del fascio. (Sugg.: sia  $F$  l'equazione di  $C$  e  $R(y_1, y_2, t_0, t_1)$  il risultante delle forme binarie in  $x_1, x_2$

$$F(y_1 x_1 + y_2 x_2, x_1, x_2), \quad (t_0 G + t_1 H)(y_1 x_1 + y_2 x_2, x_1, x_2).$$

Sia  $U \subset (\mathbb{P}^2)^\vee$  l'insieme delle rette  $L$  trasversali a  $C$  tali che  $L \cap C \cap B = \emptyset$ ,  $U$  è il complementare di una curva piana e per ogni  $s = [s_0, s_1]$  fissato esistono finite rette in  $U$  di equazione  $x_0 = ax_1 + bx_2$  tali che  $R(a, b, t_0, t_1)$  ha una radice multipla in  $s$ . Dedurre che  $R$  non può avere fattori multipli di grado positivo in  $t_0, t_1$ .)

**5.66.** Nelle stessa situazione dell'Esercizio 5.65, provare che esiste un punto  $p \in C - B$  tale che  $\nu_p(C, D_t) \leq 1$  per ogni  $t$ . (Sugg.: fissiamo un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che  $[1, 0, 0] \notin C \cup B$  e la retta  $L = \{x_2 = 0\}$  soddisfi le condizioni dell'Esercizio 5.65. Detto  $R(x_1, x_2, t_0, t_1)$  il risultante dell'eliminazione di  $x_0$  da  $F$  e  $t_0 G + t_1 H$ , provare che si può scrivere

$$R(x_1, x_2, t_0, t_1) = A(x_1, x_2)B(x_1, x_2, t_0, t_1)$$

con  $B$  polinomio ridotto senza fattori di grado 0 in  $t$ .)

**5.67.** Nelle notazioni precedenti, per quasi tutti i  $t \in \mathbb{P}^1$  (cioè eccetto un numero finito) la curva  $D_t$  è liscia al di fuori di  $B$ . (Sugg.: siano  $G_i, H_i$ , per  $i = 0, 1, 2$ , le derivate parziali rispetto alle variabili  $x_i$ . Utilizzare l'Esercizio 5.66 e la formula di Eulero per provare che il luogo dei punti  $p \in \mathbb{P}^2$  tali che

$$\text{rank} \begin{pmatrix} H_0(p) & H_1(p) & H_2(p) \\ G_0(p) & G_1(p) & G_2(p) \end{pmatrix} \leq 1$$

è contenuto nell'unione di un numero finito di curve del fascio.)

**5.68.** (caratteristica 0) siano  $D_0, D_\infty \subset \mathbb{P}^2$  curve piane di grado  $m$  senza componenti comuni e sia  $D_t$  il fascio da esse generato. Provare che per quasi tutti i  $t$  la curva  $D_t$  è liscia al di fuori di  $\text{Sing}(D_0) \cap \text{Sing}(D_\infty)$  e dedurre il Teorema di Bertini 5.6.1.

## Curve piane: argomenti scelti

### 6.1 Le coniche

In questa sezione assumeremo, salvo avviso contrario, che  $\mathbb{K}$  sia un campo algebricamente chiuso di caratteristica diversa da 2.

Una conica è una curva algebrica piana di grado 2. Due coniche si dicono proiettivamente equivalenti se esiste una proiettività di  $\mathbb{P}^2$  che trasforma l'una nell'altra. Una conica non irriducibile è unione di due rette che possono essere distinte o coincidenti. Chiameremo **rango** di una conica di equazione  $F(x_0, x_1, x_2) = 0$ , il rango della matrice Hessiana

$$H = \begin{pmatrix} F_{00} & F_{01} & F_{02} \\ F_{10} & F_{11} & F_{12} \\ F_{20} & F_{21} & F_{22} \end{pmatrix} \in M(3, 3, \mathbb{K}), \quad F_{ij} = \frac{\partial^2 F}{\partial x_i \partial x_j}.$$

Il rango di una conica non dipende dalla scelta del sistema di coordinate omogenee.

**Teorema 6.1.1.** *Due coniche sono proiettivamente equivalenti se e solo se hanno lo stesso rango. In particolare ogni conica è proiettivamente equivalente ad una delle seguenti:*

1.  $x_0^2 = 0$ , retta doppia.
2.  $x_0 x_1 = 0$ , rette incidenti.
3.  $x_0 x_2 = x_1^2$ , conica liscia.

*Dimostrazione.* Sia  $C$  una conica di equazione  $F(x_0, x_1, x_2)$  e matrice Hessiana  $H$ . Un punto  $p = [v_0, v_1, v_2] = [v] \in \mathbb{P}^2$  è un punto singolare di  $C$  se e solo se  $Hv = (F_0(v), F_1(v), F_2(v)) = 0$ . Se il rango di  $H$  è 1, allora esiste una retta  $L$  composta di punti singolari di  $C$  e quindi deve necessariamente essere  $C = 2L$ . Se il rango è 2, allora esiste un unico punto singolare  $p = [v]$ : proviamo che  $C$  è unione di rette passanti per  $p$ , per ragioni di grado tali rette dovranno essere esattamente due. Se  $q = [y] \in C$ , allora per ogni  $a, b \in \mathbb{K}$  vale

$$2F(av + by) = (av + by)^T H(av + by) = b^2 y^T H y = 0.$$

Infine se il rango è 3 la conica è liscia; siano  $p, q$  e  $r$  tre punti distinti di  $C$  e denotiamo con  $o = \mathbb{T}_p C \cap \mathbb{T}_q C$  il punto di intersezione delle rette tangenti a  $C$  nei punti  $p$  e  $q$  rispettivamente. La quaterna  $p, q, r, o$  è un sistema di riferimento di  $\mathbb{P}^2$ , esiste quindi un unico sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che

$$p = [1, 0, 0], \quad q = [0, 0, 1], \quad r = [1, 1, 1], \quad o = [0, 1, 0].$$

Sia  $F$  l'equazione di  $C$  in tale sistema di coordinate, dalla condizione  $p, q \in C$  si deduce che  $F_{00} = F_{22} = 0$ . Le equazioni di  $\mathbb{T}_p C = \overline{op}$  e  $\mathbb{T}_q C = \overline{oq}$  sono rispettivamente  $x_2 = 0$  e

$x_0 = 0$ ; si deduce quindi che  $F_{01} = F_{12} = 0$  e si ha  $F = ax_0x_2 - bx_1^2$ . La condizione  $r \in C$  impone infine che  $a = b$ .  $\square$

La dimostrazione appena terminata è costruttiva e fornisce un metodo effettivo per il calcolo della proiettività che trasforma una conica nella sua forma canonica. Tale calcolo richiede la soluzione di una equazione di secondo grado ed alcuni sistemi di equazioni lineari.

**Corollario 6.1.2.** *Siano  $p, q, r$  tre punti distinti di una conica irriducibile  $C$ . Allora esiste un sistema di coordinate omogenee  $x_0, x_1, x_2$  tale che  $p = [1, 0, 0]$ ,  $q = [0, 0, 1]$ ,  $r = [1, 1, 1]$  e l'equazione di  $C$  è  $x_0x_2 = x_1^2$ .*

*Dimostrazione.* Basta osservare che, nella dimostrazione del Teorema 6.1.1, la scelta dei punti  $p, q$  e  $r$  è arbitraria.  $\square$

Si consideri adesso l'applicazione  $v: \mathbb{P}^1 \rightarrow \mathbb{P}^2$  descritta in coordinate omogenee da  $v([t_0, t_1]) = [t_0^2, t_0t_1, t_1^2]$ . Si vede facilmente che  $v$  è iniettiva ed ha come immagine la conica di equazione  $x_0x_2 = x_1^2$ .

**Corollario 6.1.3.** *Sia  $C \subset \mathbb{P}^2$  una conica liscia. Esiste allora una base  $h_0, h_1, h_2$  dello spazio vettoriale dei polinomi omogenei di grado 2 nelle variabili  $t_0, t_1$  tale che l'applicazione  $h: \mathbb{P}^1 \rightarrow \mathbb{P}^2$ , definita in coordinate omogenee da*

$$h([t_0, t_1]) = [h_0(t_0, t_1), h_1(t_0, t_1), h_2(t_0, t_1)]$$

*induce una bigezione tra  $\mathbb{P}^1$  e  $C$ . Inoltre  $h$  è unica a meno di proiettività di  $\mathbb{P}^1$  e, per ogni curva  $D \subset \mathbb{P}^2$  di grado  $m$  ed equazione  $G$  i punti di intersezione, contati con molteplicità, di  $C$  e  $D$  sono in bigezione con le  $2m$  radici del polinomio omogeneo*

$$g(t_0, t_1) = G(h_0(t_0, t_1), h_1(t_0, t_1), h_2(t_0, t_1)).$$

*Dimostrazione.* Dato che  $t_0^2, t_0t_1, t_1^2$  formano una base dello spazio vettoriale dei polinomi omogenei di grado 2 in  $t_0, t_1$ , dal Corollario 6.1.2 segue l'esistenza di un tale morfismo  $h$ . Per dimostrare l'unicità si può assumere che  $C$  sia la conica di equazione  $x_0x_2 = x_1^2$ . A meno di comporre  $h$  con una proiettività di  $\mathbb{P}^1$  si può assumere che  $h([1, 0]) = [1, 0, 0]$ ,  $h([0, 1]) = [0, 0, 1]$  e  $h([1, 1]) = [1, 1, 1]$ . Si deve quindi avere  $h_0 = t_0f$ ,  $h_1 = t_0t_1a$ ,  $h_2 = t_1g$  con  $a$  costante e  $f, g$  polinomi omogenei di grado 1 tali che  $f(1, 0) \neq 0$ ,  $g(0, 1) \neq 0$ ,  $f(1, 1) = g(1, 1) = a$  e  $gf = a^2t_0t_1$ . Infine sia  $p \in C \cap D$ , per il Corollario 6.1.2 possiamo scegliere un sistema di coordinate omogenee tali che  $p = [1, 0, 0]$ ,  $[0, 1, 0] \notin C \cup D$ , la conica  $C$  abbia equazione  $x_0x_2 = x_1^2$  e la retta  $x_2 = 0$  non contenga altri punti di intersezione di  $C$  e  $D$  oltre  $p$ . Nelle coordinate affini  $x = x_1x_0^{-1}$ ,  $y = x_2x_0^{-1}$  l'equazione di  $C$  è  $y = x^2$  e quella di  $D$  è  $g(x, y) = G(1, x, y)$ . La molteplicità di intersezione  $\nu_p(C, D)$  è uguale alla molteplicità in  $y = 0$  del risultante  $R(y)$  dell'eliminazione di  $x$  dai polinomi  $x^2 - y$ ,  $g(x, y)$ . Sia  $\phi(t) = g(t, t^2)$ , per dimostrare che  $\nu_p(C, D)$  è uguale alla molteplicità in 0 di  $\phi$  basta dimostrare che  $R(t^2) = \phi(t)\phi(-t)$ . Per le proprietà di funtorialità del risultante  $R(t^2)$  è uguale al risultante di  $x^2 - t^2$  e  $g(x, t^2)$  che, per il Corollario 4.1.4, è uguale a  $g(t, t^2)g(-t, t^2)$ .  $\square$

Il Corollario 6.1.3 permette di definire sulla conica liscia  $C$  una struttura di retta proiettiva; in particolare è ben definito il birapporto di una quaterna ordinata di punti su  $C$ . Su tale struttura si basa il ben noto teorema di Steiner.

**Teorema 6.1.4 (Steiner, 1832).** *Siano  $p$  e  $q$  due punti di una conica liscia  $C$  e denotiamo con  $F_p$  e  $F_q$  i fasci di rette passanti per  $p$  e  $q$  rispettivamente. Allora l'applicazione  $F_p \rightarrow F_q$  definita da  $F_p \ni L \mapsto \overline{qs}$ , dove  $s$  è il punto di intersezione di  $L$  con  $C$  diverso da  $p$ , è una proiettività.*



*Dimostrazione.* Non è restrittivo supporre che  $C$  sia la conica di equazione  $x_0x_2 = x_1^2$  e che la struttura di retta proiettiva sia indotta dal morfismo  $v: \mathbb{P}^1 \rightarrow C$  dato da  $v([t_0, t_1]) = [t_0^2, t_0t_1, t_1^2]$ . Dato un punto  $[a, b] \in \mathbb{P}^1$ , la retta di  $\mathbb{P}^2$  di equazione  $bx_1 - ax_2$  interseca  $C$  nei punti  $p = [1, 0, 0]$  e  $v([a, b])$ . L'applicazione  $[a, b] \mapsto ax_1 - bx_2$  è una proiettività tra  $\mathbb{P}^1$  ed il fascio di rette passanti per  $p$ ; similmente l'applicazione  $[a, b] \mapsto ax_1 - bx_0$  è una proiettività tra  $\mathbb{P}^1$  ed il fascio di rette passanti per il punto  $q = [0, 0, 1]$ .  $\square$

È facile dimostrare che ogni fascio di coniche contiene almeno una conica singolare. Infatti siano  $C_1, C_2$  coniche di equazioni  $F_1, F_2$  e matrici Hessiane  $H_1, H_2$  rispettivamente. Se  $C_2$  è singolare abbiamo finito. Altrimenti si ha che la conica di equazione  $F_1 - tF_2$  è singolare se e solo se  $p(t) = \det(H_1 - tH_2) = 0$ ; Il polinomio  $p(t)$  ha grado 3 e quindi ammette radici. Se vogliamo determinare i punti di intersezione di due coniche  $C_1, C_2$  si può procedere in almeno tre modi distinti.

1. Prendere un sistema di coordinate omogenee in cui il punto  $[0, 0, 1]$  non appartiene all'unione  $C_1 \cup C_2$ , calcolare il risultante rispetto a  $x_2$  delle equazioni di  $C_1$  e  $C_2$  e determinarne le radici.
2. Se  $C_2$  è singolare se ne determinano le componenti irriducibili e quindi l'intersezione di queste con  $C_1$ . Se  $C_2$  è liscia,  $h: \mathbb{P}^1 \rightarrow C_2$  è una proiettività (cfr. Corollario 6.1.3) e  $F_1$  è un'equazione per  $C_1$ , allora i punti di intersezione sono in bigezione naturale con le radici del polinomio omogeneo in due variabili  $F(h(t_0, t_1))$ .
3. Determinare una conica singolare  $C_0$  appartenente al fascio generato da  $C_1$  e  $C_2$  e quindi ricondursi al caso particolare del punto 2) ricordandosi che, se  $C_0 \neq C_2$ , allora  $C_1 \cap C_2 = C_0 \cap C_2$ .

I metodi 1) e 2) richiedono in generale la soluzione di una equazione di quarto grado mentre il metodo 3) richiede solamente la soluzione di una equazione di terzo grado e di tre equazioni di secondo grado.

*Esempio 6.1.5.* Il generico polinomio monico di quarto grado

$$R(x) = x^4 + ax^3 + bx^2 + cx + d$$

può essere visto come il risultante dell'eliminazione di  $y$  dai polinomi

$$f_1(x, y) = y^2 + axy + by + cx + d, \quad f_2(x, y) = y - x^2$$

e quindi le radici di  $R(x)$  sono in corrispondenza biunivoca con le intersezioni delle coniche affini di equazioni  $f_1 = 0$  e  $f_2 = 0$ . Le matrici Hessiane di  $f_1$  e  $f_2$  (o più precisamente dei loro omogeneizzati) sono rispettivamente

$$H_1 = \begin{pmatrix} 0 & a & c \\ a & 2 & b \\ c & b & 2d \end{pmatrix}, \quad H_2 = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

e quindi

$$p(t) = \det(H_1 - tH_2) = \begin{vmatrix} 2t & a & c \\ a & 2 & b-t \\ c & b-t & 2d \end{vmatrix}.$$

Se avete letto il Capitolo 3, allora troverete interessante assumere la caratteristica di  $\mathbb{K}$  diversa da 2 e da 3, porre  $a_0 = 1$ ,  $4a_1 = a$ ,  $6a_2 = b$ ,  $4a_3 = c$ ,  $a_4 = d$  ed eseguire la "misteriosa" sostituzione  $t = 4(s + a_2)$ . Un semplice conto che omettiamo ci dà

$$q(s) = -\frac{p(4(s + a_2))}{32} = 4s^3 - g_2s - g_3,$$

dove  $g_2 = a_0a_4 - 4a_1a_3 + 3a_2^2$  e  $g_3 = a_0a_2a_4 - a_0a_3^2 + 2a_1a_2a_3 - a_2^3 - a_1^2a_4$ . Il polinomio  $q(s)$  viene talvolta detto **risolvente** di  $R(x)$  e, come abbiamo visto nel Capitolo 3, la quaterna delle radici di  $R(x)$  è proiettivamente equivalente alla quaterna formata dalle radici di  $q(x)$  più il punto all'infinito.

Dato che lo spazio delle coniche ha dimensione 5, per cinque punti distinti di  $\mathbb{P}^2$  passa almeno una conica; inoltre tale conica è unica se i punti sono presi in posizione generica.

**Proposizione 6.1.6.** *Se per cinque punti distinti di  $\mathbb{P}^2$  passano due coniche distinte allora quattro di essi sono allineati.*

*Dimostrazione.* Per Bézout le due coniche devono avere una retta  $L$  in comune e le due coniche possono avere al più un punto di intersezione al di fuori di  $L$ .  $\square$

Si noti che il teorema di Steiner 6.1.4 può essere interpretato come una condizione necessaria e sufficiente sulle sestuple di punti distinti affinché siano contenute in una conica.

Se  $C$  è una conica liscia di equazione  $F(x_0, x_1, x_2) = 0$  e  $p = [y_0, y_1, y_2]$ , allora la curva polare di  $p$  rispetto a  $C$  è la retta  $C_p$  di equazione  $F_p(x) = y^T Hx = 0$ , dove  $H$  indica la matrice Hessiana di  $F$ . Dato che  $C$  è liscia, la matrice  $H$  è invertibile e quindi l'applicazione  $p \mapsto C_p$  definisce una proiettività  $\mathbb{P}^2 \rightarrow (\mathbb{P}^2)^\vee$ .

**Lemma 6.1.7.** *Nelle notazioni precedenti  $p \in C_q$  se e solo se  $q \in C_p$ .*

*Dimostrazione.* La matrice Hessiana è simmetrica.  $\square$

*Esempio 6.1.8.* Siano  $L \subset \mathbb{P}^2$  una retta,  $C \subset \mathbb{P}^2$  una conica liscia,  $p, q \in L$  punti distinti e  $r = C_p \cap C_q$ . Per il Lemma 6.1.7 si ha  $p, q \in C_r$  e quindi  $L = C_r$ .

**Teorema 6.1.9.** *Siano  $C$  una conica liscia e  $p$  un punto del piano.*

1. *Se  $p \in C$ , allora la polare  $C_p$  è la retta tangente a  $C$  nel punto  $p$ .*
2. *Se  $p \notin C$ , allora la polare  $C_p$  interseca  $C$  in due punti distinti e per  $p$  passano esattamente due rette distinte tangenti a  $C$ .*

*Dimostrazione.* Se  $p \in C$ ,  $q \in C_p$  e  $q \neq p$ , allora  $p \in C_q \cap C$  e quindi  $\overline{pq} = C_p$  è tangente a  $C$  in  $p$ . Se  $p \in \mathbb{P}^2$  e  $C_p$  è tangente a  $C$  nel punto  $q \in C$ , allora per il punto precedente  $C_p = C_q$  e  $p = q$ . Per la formula di Eulero, se  $p \notin C$ , allora  $p \notin C_p$  e quindi i punti di intersezione di  $C_p$  con  $C$  non sono allineati con  $p$ .  $\square$

Quanto dimostrato mostra in particolare che, data una conica liscia  $C \subset \mathbb{P}^2$ , l'insieme delle sue rette tangenti  $C^\vee = \{C_p \in (\mathbb{P}^2)^\vee \mid p \in C\}$  è una conica detta **conica duale** di  $C$ . Si ha inoltre  $C^{\vee\vee} = C$ .

## Esercizi

**6.1.** Provare che il Corollario 6.1.2 è vero anche in caratteristica 2.

**6.2.** Trovare le componenti irriducibili della conica di equazione

$$3x_0^2 + 5x_0x_1 + 2x_0x_2 + 2x_1^2 + x_1x_2 - x_2^2 = 0.$$

**6.3.** Sia dato un fascio di coniche generato da due rette doppie. Provare che ogni conica di tal fascio è singolare.

**6.4.** Calcolare i punti di intersezione delle coniche di equazioni

$$x_0^2 + x_1^2 + x_2^2 = 0, \quad x_1^2 + x_2^2 - x_0x_1 - x_0x_2 = 0.$$

**6.5.** Scrivere l'equazione della conica affine passante per i punti  $(0,0)$ ,  $(1,0)$ ,  $(0,1)$  e tangente alla retta  $x + y = 4$  nel punto  $(2,2)$ .

**6.6.** Sia  $\mathbb{P}^5$  lo spazio di tutte le coniche e sia  $v_2: (\mathbb{P}^2)^\vee \rightarrow \mathbb{P}^5$  l'applicazione data da  $v_2(L) = 2L$ . L'immagine di  $v_2$  è detta **superficie di Veronese**. Provare che se  $p, q \in v_2((\mathbb{P}^2)^\vee)$ , allora la retta  $\overline{pq}$  è contenuta nel luogo delle coniche singolari.

**6.7 (Variante al teorema di Steiner, 1832, \*).** Data una conica liscia  $C$ , un triangolo (terna di punti non allineati)  $T = \{p_1, p_2, p_3\}$  si dice autoconiugato rispetto a  $C$  se  $C_{p_i} = \overline{p_j p_k}$ , dove  $j, k \neq i$ . Dati sei punti distinti  $p_1, p_2, p_3, q_1, q_2, q_3 \in \mathbb{P}^2$ , tre a tre non allineati, considerare i due triangoli  $P = \{p_1, p_2, p_3\}$ ,  $Q = \{q_1, q_2, q_3\}$ . Provare che le seguenti condizioni sono equivalenti:

1.  $P$  e  $Q$  sono autoconiugati rispetto ad una conica liscia.
2.  $P$  e  $Q$  sono inscritti in una conica liscia.
3.  $P$  e  $Q$  sono circoscritti ad una conica liscia.

(Sugg.: per dualità basta dimostrare che (1) è equivalente a (2) Se vale (1), si considerino le intersezioni dei fasci di rette di centri  $p_1$  e  $q_1$  con la retta  $\overline{p_2 p_3}$ , quindi si provi l'uguaglianza dei birapporti delle quaterne ordinate  $(\overline{p_1 p_2}, \overline{p_1 p_3}, \overline{p_1 q_2}, \overline{p_1 q_3})$ ,  $(\overline{p_1 p_3}, \overline{p_1 p_2}, \overline{p_1 q_3}, \overline{p_1 q_2})$  e  $(\overline{q_1 p_2}, \overline{q_1 q_3}, \overline{q_1 q_2}, \overline{q_1 p_3})$ . Viceversa se vale (2), si provi che esiste una conica liscia  $C$  tale che  $C_{p_i} = \overline{p_j p_k}$  e  $C_{q_i} = \overline{q_2 q_3}$ . Si mostri quindi che  $C_{q_2} = \overline{q_1 q_3}$  usando l'unicità della conica passante per  $p_1, p_2, p_3, q_1$  e  $q_2$ .)

*Osservazione 6.1.10.* L'equivalenza fra le condizioni (2) e (3) dell'Esercizio 6.7 è conosciuta con il nome di *teorema di Brianchon (1817)*.

## 6.2 Corrispondenze e poligoni di Poncelet

In questa sezione daremo una dimostrazione del celebre teorema dei poligoni di Poncelet; le idee principali di questa dimostrazione sono state indicate da Cayley nel 1871 ([Cay1871], [EC1915, Libro II p. 164], [An1977]) e riposano sulla teoria delle corrispondenze su  $\mathbb{P}^1$ .

**Definizione 6.2.1.** Sia  $F(x_0, x_1, y_0, y_1)$  un polinomio biomogeneo irriducibile di bigrado  $(a, b)$ . L'insieme

$$V(F) = \{([x_0, x_1], [y_0, y_1]) \in \mathbb{P}^1 \times \mathbb{P}^1 \mid F(x_0, x_1, y_0, y_1) = 0\}$$

si dice una **corrispondenza irriducibile di tipo  $(a, b)$** .

Per il teorema degli zeri di Hilbert, ogni corrispondenza irriducibile  $V(F)$  determina la sua equazione  $F$  a meno di una costante moltiplicativa. Per esempio, la diagonale

$$\Delta = \{([x_0, x_1], [y_0, y_1]) \in \mathbb{P}^1 \times \mathbb{P}^1 \mid x_0 y_1 - x_1 y_0 = 0\}$$

è una corrispondenza irriducibile di tipo  $(1, 1)$ . Più in generale, se  $f(x_0, x_1)$  e  $g(x_0, x_1)$  sono polinomi omogenei di grado  $n$  senza fattori comuni, l'insieme

$$\Gamma = \{([x_0, x_1], [y_0, y_1]) \in \mathbb{P}^1 \times \mathbb{P}^1 \mid y_0 g(x_0, x_1) - y_1 f(x_0, x_1) = 0\}$$

è una corrispondenza irriducibile di tipo  $(n, 1)$ . Si noti che  $\Gamma$  è il grafico dell'applicazione  $\gamma: \mathbb{P}^1 \rightarrow \mathbb{P}^1$  data in coordinate omogenee da  $\gamma([x_0, x_1]) = [f(x_0, x_1), g(x_0, x_1)]$ .

**Definizione 6.2.2.** Una **corrispondenza** è una combinazione lineare formale finita di corrispondenze irriducibili a coefficienti interi positivi. In altri termini, una corrispondenza è  $C = m_1 C_1 + \dots + m_k C_k$ , con le  $C_i$  corrispondenze irriducibili e gli  $m_i$  interi positivi.

Ragionando come per le curve piane si dimostra che esiste una bigezione naturale tra l'insieme delle corrispondenze di tipo  $(a, b)$  ed il proiettivizzato dello spazio dei polinomi biomogenei di bigrado  $(a, b)$ . Se  $C$  è una corrispondenza di equazione  $F(x, y) = 0$  si definisce la sua **inversa**  $C^{-1}$  come la corrispondenza di equazione  $F(y, x) = 0$ . Il nome di corrispondenza inversa è motivato esclusivamente da ragioni storiche (cfr. [GH1978, p. 283]): sarebbe infatti molto più sensato chiamarla corrispondenza trasposta. Si osservi ad esempio che  $(C_1 + C_2)^{-1} = C_1^{-1} + C_2^{-1}$ . Il nome di corrispondenza inversa è inoltre in contraddizione con la seguente (ugualmente storica)

**Definizione 6.2.3.** Una corrispondenza  $C$  si dice **simmetrica** se  $C = C^{-1}$ .

Si noti che se  $C$  è di tipo  $(a, b)$ , allora  $C^{-1}$  è di tipo  $(b, a)$ . Una corrispondenza di equazione  $F$  è simmetrica se e solo se  $F(x, y) = \pm F(y, x)$ .

**Definizione 6.2.4.** I **punti fissi** di una corrispondenza  $C$  sono i punti di intersezione di  $C$  con la diagonale  $\Delta$ .

**Lemma 6.2.5 (Principio di Chasles).** Sia  $C$  una corrispondenza di tipo  $(a, b)$ . Se la diagonale  $\Delta$  non è una componente di  $C$ , allora  $C$  contiene  $a + b$  punti fissi contati con molteplicità.

*Dimostrazione.* Se  $F$  è l'equazione della corrispondenza  $C$ , allora le radici in  $\mathbb{P}^1$  della forma binaria  $f(x_0, x_1) = F(x_0, x_1, x_0, x_1)$  sono in bigezione con i punti fissi di  $C$ ; basta osservare che il grado di  $f$  è  $a + b$ .  $\square$

**Lemma 6.2.6.** Sia  $C$  una corrispondenza di tipo  $(a, b)$  senza componenti multiple. Se la caratteristica di  $\mathbb{K}$  è uguale a 0 oppure maggiore di  $b$ , allora esistono  $2a(b - 1)$  punti  $p \in \mathbb{P}^1$ , contati con molteplicità, tali che la retta  $\{p\} \times \mathbb{P}^1$  è tangente a  $C$ .

*Dimostrazione.* Sia  $F(x_0, x_1, y_0, y_1)$  l'equazione di  $C$ ; se pensiamo  $F$  come una forma binaria di grado  $b$  a coefficienti in  $\mathbb{K}[x_0, x_1]$ , allora i punti  $p$  cercati sono le radici del discriminante  $\Delta(x_0, x_1)$  di  $F$ . Siccome il discriminante di una forma di grado  $b$  è omogeneo di grado  $2b - 2$  nei coefficienti della forma, ne segue che  $\Delta(x_0, x_1)$  è omogeneo di grado  $2a(b - 1)$  nelle variabili  $x_0, x_1$ .  $\square$

Classicamente una corrispondenza  $C$  di tipo  $(a, b)$  veniva interpretata come una applicazione "algebraica" di grado  $a$  definita su  $\mathbb{P}^1$  a valori nello spazio proiettivo delle  $b$ -uple non ordinate di punti di  $\mathbb{P}^1$ . Più precisamente, al punto  $p \in \mathbb{P}^1$  si associava la  $b$ -upla  $C_p = C \cap (\{p\} \times \mathbb{P}^1)$ . In tale formalismo si aveva quindi:

1.  $p \in C_p$  se e solo se  $p$  è un punto fisso.
2.  $p \in C_q$  se e solo se  $q \in C_p^{-1}$ .

Se  $C$  e  $D$  sono due corrispondenze, viene spontaneo definire la loro composizione  $D \circ C$  in modo tale che per ogni punto  $p \in \mathbb{P}^1$  si abbia

$$(D \circ C)_p = \cup \{D_q \mid q \in C_p\}.$$

In termini più rigorosi, si definisce la composizione mediante l'uso del risultante. Se il polinomio  $F$  di bigrado  $(a, b)$  è l'equazione di  $C$  ed il polinomio  $G$  di bigrado  $(m, n)$  è l'equazione di  $D$ , allora si definisce  $D \circ C$  come la corrispondenza di equazione

$$H(x_0, x_1, y_0, y_1) = R_{b,m}(F(x_0, x_1, z_0, z_1), G(z_0, z_1, y_0, y_1)),$$

dove il risultante è fatto considerando  $F$  e  $G$  come forme binarie nelle variabili  $z_0, z_1$ .

Tale definizione è perfettamente compatibile con la descrizione intuitiva di corrispondenza composta, infatti se  $p = [u_0, u_1]$  è un punto fissato tale che  $\{p\} \times \mathbb{P}^1$  non è una componente di  $C$ , allora, a meno di costanti moltiplicative si ha

$$H(u_0, u_1, y_0, y_1) = \prod_{i=1}^b G(\alpha_i, \beta_i, y_0, y_1),$$

dove  $[\alpha_i, \beta_i] \in \mathbb{P}^1$ , per  $i = 1, \dots, b$ , sono tutte e sole le radici della forma binaria  $F(u_0, u_1, z_0, z_1)$ . Dalle proprietà basilari del risultante segue immediatamente che:

1. Siano  $R, S$  e  $T$  tre copie della retta proiettiva,  $C$  una corrispondenza su  $R \times S$  e  $D$  una corrispondenza su  $S \times T$ . Allora  $D \circ C$  è una corrispondenza su  $R \times T$ .
2. Se  $C$  è di tipo  $(a, b)$  e  $D$  è di tipo  $(m, n)$ , allora  $D \circ C$  è di tipo  $(am, bn)$ .
3.  $(D \circ C)^{-1} = C^{-1} \circ D^{-1}$  e quindi  $C^{-1} \circ C$  è simmetrica.
4.  $D \circ (C_1 + C_2) = D \circ C_1 + D \circ C_2$ ,  $(D_1 + D_2) \circ C = D_1 \circ C + D_2 \circ C$ .

Si considerino adesso due coniche lisce  $Q_1, Q_2 \subset \mathbb{P}^2$  e identifichiamo  $Q_1$  con  $\mathbb{P}^1$  tramite una proiettività fissata. Si assuma inoltre la caratteristica del campo diversa da 2. Vogliamo mostrare che esiste unica una corrispondenza  $B \subset Q_1 \times Q_1$  simmetrica di tipo  $(2, 2)$  tale che  $(p, q) \in B$  se e solo se la retta  $L \subset \mathbb{P}^2$  tale che  $L \cap Q_1 = \{p, q\}$  è tangente a  $Q_2$ . Per mostrare ciò fissiamo un sistema di coordinate omogenee su  $\mathbb{P}^2$ , sia  $H$  la matrice Hessiana di  $Q_2$  e  $f = (f_0, f_1, f_2): \mathbb{P}^1 \rightarrow Q_1$  una proiettività fissata; i polinomi  $f_i \in \mathbb{K}[t_0, t_1]$  sono omogenei di grado 2. Fissiamo un punto  $p = [u] = [u_0, u_1, u_2] \in \mathbb{P}^2$ , poiché la retta  $p + [x]$  è tangente a  $Q_2$  se e solo se il polinomio  $g(t) = (u + tx)^T H(u + tx)$  ha una radice doppia, si ha che la conica  $S_p$  di equazione

$$(u^T Hx)^2 - (u^T Hu)(x^T Hx) = 0$$

è l'unione delle due rette (possibilmente coincidenti) passanti per  $p$  e tangenti a  $Q_2$ . In particolare se  $p \in Q_1$  si ha:

1.  $\nu_p(S_p, Q_1) = 4$  se  $p \in Q_2$  e  $\mathbb{T}_p Q_1 = \mathbb{T}_p Q_2$ .
2.  $\nu_p(S_p, Q_1) = 3$  se  $p \notin Q_2$  e  $\mathbb{T}_p Q_1$  è tangente a  $Q_2$  in un punto  $q \neq p$ .
3.  $\nu_p(S_p, Q_1) = 2$  in tutti gli altri casi, cioè se  $\mathbb{T}_p Q_1$  non è tangente a  $Q_2$ .

Dunque se  $S \subset Q_1 \times Q_1$  è la corrispondenza di tipo  $(4, 4)$  di equazione

$$(f(x_0, x_1)^T Hf(y_0, y_1))^2 - (f(x_0, x_1)^T Hf(x_0, x_1))(f(y_0, y_1)^T Hf(y_0, y_1)) = 0,$$

si ha per il Corollario 6.1.3 che  $S = B + 2\Delta$  dove  $B$  è la corrispondenza cercata.

Fissato un intero  $n > 0$  ed un punto  $p \in Q_1$  possiamo costruire due punti  $p_1^{(n)}, p_2^{(n)} \in Q_1$  nel modo seguente. Siano  $L_1, L_2$  le rette per  $p$  tangenti a  $Q_2$ . Si definisce  $p'_1$  come il secondo punto di intersezione di  $L_1$  con  $Q_1$  e  $L'_1$  come la seconda retta per  $p'_1$  tangente a  $Q_2$ . Si definisce poi  $p''_1$  come il secondo punto di intersezione di  $L'_1$ ; proseguendo per  $n$  passi si arriva a definire  $p_1^{(n)}$ . Ripetendo la stessa procedura partendo da  $L_2$  si definisce  $p_2^{(n)}$ . Si vede facilmente che l'applicazione  $p \mapsto \{p_1^{(n)}, p_2^{(n)}\}$  è indotta da una corrispondenza simmetrica  $B^{(n)}$  di tipo  $(2, 2)$ , basta infatti definire per ricorrenza  $B^{(0)} = 2\Delta$ ,  $B^{(1)} = B$  e per ogni  $n \geq 2$   $B^{(n)} = B \circ B^{(n-1)} - B^{(n-2)}$ .

Si possono verificare due casi. Nel primo la diagonale  $\Delta$  è una componente di  $B^{(n)}$  e quindi ogni punto di  $Q_1$  è vertice di un poligono chiuso di  $n$  lati inscritto a  $Q_1$  e circoscritto a  $Q_2$ . Nel secondo caso la diagonale non è una componente di  $B^{(n)}$  e quindi esistono  $4 = 2 + 2$  punti fissi di  $B^{(n)}$  contati con molteplicità.

**Teorema 6.2.7 (degli  $n$ -goni di Poncelet, 1822).** *Sia  $n$  un intero maggiore di 2 e siano  $Q_1, Q_2 \subset \mathbb{P}^2$  due coniche lisce definite su di un campo algebricamente chiuso di caratteristica  $\neq 2$ . Per ogni punto  $p \in Q_1$  si consideri la seguente proprietà:*

(P) Il punto  $p$  è il vertice di un  $n$ -gono inscritto a  $Q_1$  e circoscritto a  $Q_2$ , o equivalentemente esiste una  $n$ -upla ordinata di punti distinti  $p_1, p_2, \dots, p_n \in Q_1$  tali che  $p = p_i$  per qualche  $i$  e le  $n$  rette  $\overline{p_i p_{i+1}}$ , per  $i = 1, \dots, n$  e  $p_{n+1} = p_1$ , sono tangenti a  $Q_2$ .

Se la proprietà (P) è vera per un punto, allora è vera per tutti i punti di  $Q_1$  eccetto un insieme finito.

*Dimostrazione.* Si assuma vera la (P) per un punto  $p$  e siano  $p = p_1, \dots, p_n$  i vertici dell' $n$ -gono relativo; si osserva innanzitutto che la (P) è soddisfatta da  $p_1, \dots, p_n$ . Siccome i punti  $p_1, \dots, p_n$  sono distinti, si ha che per ogni  $i = 1, \dots, n - 1$  la corrispondenza  $B^{(i)}$  non contiene la diagonale e quindi esistono al più finiti  $n$ -goni inscritti a  $Q_1$ , circoscritti a  $Q_2$  ed aventi almeno un vertice che è anche un punto fisso della corrispondenza  $B^{(i)}$ , per qualche  $i = 1, \dots, n - 1$ ; denotiamo con  $R \subset Q_1$  l'unione dei vertici di tali  $n$ -goni. Dalle definizioni segue subito che un punto  $p$  ha la proprietà (P) se e solo se è un punto fisso di  $B^{(n)}$  e non appartiene a  $R$ . Basta quindi dimostrare che  $B^{(n)}$  contiene la diagonale. Distinguiamo tre casi:

1)  $n \geq 5$ : la corrispondenza  $B^{(n)}$  ha almeno  $n$  punti fissi e quindi deve contenere la diagonale.

2)  $n = 4$ : basta dimostrare che esiste un punto fisso di  $B^{(4)}$  distinto da  $p_1, \dots, p_4$ . Sia  $q \in Q_1 \cap Q_2$  e denotiamo con  $q_1 \in Q_1$  il secondo punto dell'intersezione di  $Q_1$  e  $\mathbb{T}_q Q_2$ , con  $L$  la seconda retta per  $q_1$  tangente a  $Q_2$  e con  $q_2$  il secondo punto di intersezione di  $Q_1$  con  $L$ . Lasciamo al lettore la semplice verifica che  $q_2$  è un punto fisso di  $B^{(4)}$  distinto dai punti  $p_i$ .

3)  $n = 3$ : Occorre trovare due ulteriori punti fissi di  $B^{(3)}$ . Distinguiamo due sottocasi:

3.1) Esiste un punto di contatto multiplo tra  $Q_1$  e  $Q_2$ , cioè esiste  $q \in Q_1 \cap Q_2$  tale che  $\mathbb{T}_q Q_1 = \mathbb{T}_q Q_2$ . Lasciamo per esercizio al lettore provare che  $q$  è un punto fisso di molteplicità  $\geq 2$  per ogni corrispondenza  $B^{(i)}$ ,  $i \geq 1$ .

3.2)  $Q_1$  e  $Q_2$  si intersecano trasversalmente. Dalla teoria della polarità (Teorema 6.1.9) segue che anche le coniche duali si intersecano trasversalmente e quindi esistono esattamente quattro rette distinte  $L_1, \dots, L_4$  che sono contemporaneamente tangenti a  $Q_1$  e  $Q_2$ . Per ogni  $i$  sia  $q_i$  il punto di intersezione di  $L_i$  con  $Q_1$ ,  $L'_i$  la seconda retta per  $q_i$  tangente a  $Q_2$  e  $s_i$  il secondo punto di intersezione di  $L'_i$  con  $Q_1$ . I punti  $s_1, \dots, s_4$  sono punti fissi di  $B^{(3)}$  e non possono essere tutti coincidenti.

Concludiamo la dimostrazione osservando che se  $p \in R$ , allora l' $n$ -gono di Poncelet con vertice in  $p$  è ancora chiuso ma può avere lati e vertici ripetuti.  $\square$

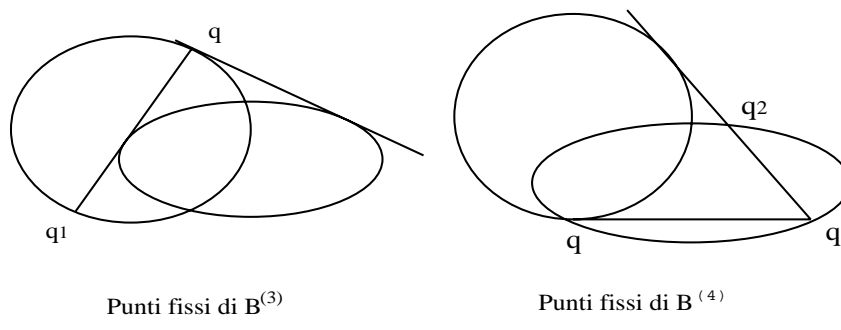
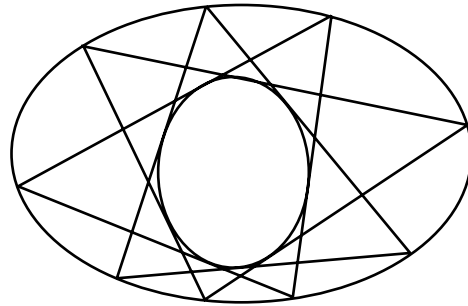


Figura 6.1. Punti fissi delle corrispondenze  $B^{(3)}$  e  $B^{(4)}$

Per una dimostrazione (non banale) di 6.2.7 che utilizza i metodi classici della geometria proiettiva rimandiamo a [Sev1906, p. 226].

Triangoli di Poncelet



**Figura 6.2.** Triangoli di Poncelet

Si noti come nel caso  $n = 3$  il teorema dei triangoli di Poncelet segue facilmente dal teorema di Brianchon (Esercizio 6.7), (cfr. [EC1915] libro III, p. 69.)

Introduciamo adesso le corrispondenze associate ad una curva piana. Siano  $a, b$  punti distinti di  $\mathbb{P}^2$ , denotiamo con  $L = \overline{ab}$  la retta passante per essi e con  $F_a$  e  $F_b$  i fasci di rette passanti per  $a$  e  $b$  rispettivamente. Per ogni curva  $C \subset \mathbb{P}^2$  di grado  $n$  si può associare in modo naturale una corrispondenza  $C_{a,b} \subset F_a \times F_b$  di tipo  $(n, n)$ :

Dal punto di vista sintetico, una coppia  $(L_1, L_2) \in F_a \times F_b$  appartiene a  $C_{a,b}$  se e solo se  $C \cap L_1 \cap L_2 \neq \emptyset$ .

Dal punto di vista algebrico, se  $x_0, x_1, x_2$  è un sistema di coordinate omogenee tali che  $a = [1, 0, 0]$  e  $b = [0, 1, 0]$  (e quindi  $L = \{x_2 = 0\}$  è la retta all'infinito), allora il punto di intersezione di una generica coppia di rette  $L_1 \in F_a, L_2 \in F_b$  si ottiene risolvendo il sistema lineare omogeneo

$$\begin{cases} u_0x_1 - u_1x_2 = 0 \\ v_0x_0 - v_1x_2 = 0 \end{cases}$$

che, se  $(u_0, v_0) \neq (0, 0)$ , ha come soluzione

$$[x_0, x_1, x_2] = [u_0v_1, v_0u_1, u_0v_0].$$

Si definisce quindi  $C_{a,b}$  come la corrispondenza di equazione

$$G(u_0, u_1, v_0, v_1) = F(u_0v_1, v_0u_1, u_0v_0).$$

Si noti che se  $a \in C$  (risp.:  $b \in C$ ), allora  $F_a \times \{L\}$  (risp.:  $\{L\} \times F_b$ ) è una componente di  $C_{a,b}$ ; notiamo inoltre che  $C_{a,b}^{-1} = C_{b,a}$ . L'equazione affine di  $C_{a,b}$  nello spazio affine  $(F_a - \{L\}) \times (F_b - \{L\}) = \{u_0v_0 \neq 0\}$  è

$$g(x, y) = G(1, x, 1, y) = F(y, x, 1)$$

e quindi le due curve affini  $C_{a,b} - (F_a \times \{L\} \cup \{L\} \times F_b)$  e  $C - \{L\}$  sono isomorfe. È quindi possibile ricostruire  $C$  conoscendo  $C_{a,b}$ . Infatti se  $C_{a,b}$  ha tipo  $(n, n)$  basta aggiungere un certo numero di volte la retta  $L$  alla curva di equazione affine  $G(1, x, 1, y) = F(y, x, 1)$  in modo da ottenere una curva  $C$  di grado  $n$ .

### Esercizi

**6.8.** Sia  $C$  una corrispondenza simmetrica non contenente la diagonale  $\Delta$ . Dimostrare che  $(p, p)$  è un punto fisso multiplo se e solo se la retta  $\{p\} \times \mathbb{P}^1$  è tangente a  $C$  nel punto  $(p, p)$ . (Sugg.: detta  $F$  è l'equazione di  $C$ , provare che  $F(x, y) = F(y, x)$ .)

**6.9.** Siano  $C$  e  $D$  corrispondenze irriducibili. Dimostrare che se per infiniti punti  $p \in \mathbb{P}^1$  vale  $C_p \subset D_p$ , allora  $C = D$ .

**6.10 (Teorema di Bézout per le corrispondenze).** Dimostrare che due corrispondenze senza componenti comuni di tipo  $(a, b)$  e  $(m, n)$  si intersecano in  $an + bm$  punti contati con molteplicità.

**6.11.** Sia  $C \subset \mathbb{P}^2$  una curva di grado  $n$ , siano  $a, b \in \mathbb{P}^2$  e  $C_{a,b} \subset F_a \times F_b$  la corrispondenza di tipo  $(n, n)$  formata dalle coppie di rette che si intersecano in  $C$ . Si denoti inoltre  $L = \overline{ab}$ . Provare che:

1. Se  $a \in C$  è un punto di molteplicità  $m$ , allora  $F_a \times \{L\}$  è una componente di molteplicità  $m$  in  $C_{a,b}$ .
2. La molteplicità di  $(L, L)$  in  $C_{a,b}$  è maggiore od uguale ad  $n$ ; è uguale ad  $n$  se e solo se  $L$  non è una componente di  $C$ .
3. Se  $L$  non è una componente di  $C$ , allora esiste una bigezione naturale fra  $L \cap C$  e le componenti del cono tangente a  $C_{a,b}$  nel punto  $(L, L)$ .
4. Se  $C$  è una cubica liscia e  $a, b \in C$ , allora  $C_{a,b} - (F_a \times \{L\} \cup \{L\} \times F_b)$  è una corrispondenza liscia di tipo  $(2, 2)$ .

**6.12 (Regola di Zeuthen, 1873).** Sia  $p$  un punto di intersezione di due curve  $C, D$  senza componenti comuni e siano  $a, b$  punti di  $\mathbb{P}^2$  in posizione generica. Dimostrare che  $\nu_p(C, D)$  è uguale alla molteplicità della retta  $\overline{ap}$  come punto fisso della corrispondenza  $D_{b,a} \circ C_{a,b}$ . Se  $C$  e  $D$  hanno rispettivamente gradi  $n$  e  $m$ , dimostrare che la retta  $\overline{ab}$  è un punto fisso di  $D_{b,a} \circ C_{a,b}$  di molteplicità  $nm$  e si deduca il teorema di Bézout dal principio di Chasles.

### 6.3 Flessi di cubiche piane e teorema di Salmon

Nel seguito supporremo  $C \subset \mathbb{P}^2$  una cubica liscia fissata su di un campo algebricamente chiuso  $\mathbb{K}$  di caratteristica diversa da 2 e da 3. Se  $p, q \in C$  indicheremo con  $\overline{pq}$  la retta passante per i punti  $p$  e  $q$  quando  $p \neq q$ , e la retta tangente a  $C$  in  $p$  quando  $p = q$ .

**Lemma 6.3.1.** *I punti di flessione di una cubica piana liscia sono tutti ordinari, cioè hanno tutti molteplicità di flesso uguale a 1.*

*Dimostrazione.* Sia  $C$  una cubica piana liscia e  $p$  un suo flesso. Per definizione la molteplicità di flesso è uguale a  $\nu_p(C, \mathbb{T}_p C) - 2$  e se tale numero fosse maggiore di 1, allora  $\nu_p(C, \mathbb{T}_p C) \geq 4$  e la retta  $\mathbb{T}_p C$  sarebbe una componente di  $C$ .  $\square$

Per ogni  $p \in \mathbb{P}^2$  denotiamo con  $C_p$  la conica polare di  $C$  rispetto al punto  $p$ .

**Proposizione 6.3.2.** *Sia  $p$  un punto di una cubica piana liscia  $C$ :*

1. Se  $q \neq p$  e  $q \in C \cap C_p$ , allora  $\nu_q(C, C_p) = 1$ .
2. La polare  $C_p$  è liscia in  $p$  e vale  $\nu_p(C, C_p) = \nu_p(C, \mathbb{T}_p C)$ .
3. Il punto  $p$  è un flesso se e solo se la conica  $C_p$  è singolare.

*Dimostrazione.* Sia  $F$  l'equazione di  $C$  in un sistema di coordinate omogenee fissato e siano  $p = [u]$ ,  $q = [v]$ , dove  $u, v \in \mathbb{K}^3 - 0$ . Il polinomio  $f(t) = F(v + tu)$  è non nullo ed ha grado  $\leq 2$  poiché  $F(u) = 0$ ; la sua derivata rispetto a  $t$  è  $f'(t) = F_p(v + tu)$ . Vediamo che cosa succede al variare di  $q$ .

Se  $q \notin \mathbb{T}_p C$ , allora il grado di  $f$  è esattamente 2; quindi il grado di  $f'$  è 1 e la retta  $\overline{pq}$  è trasversale a  $C_p$ . Questo implica tra l'altro che la polare  $C_p$  è liscia in  $p$  con retta tangente uguale a  $\mathbb{T}_p C_p = \mathbb{T}_p C$ .



Se  $q \neq p$  e  $q \in C \cap C_p$ , allora  $\mathbb{T}_q C = \overline{pq}$  e  $f(t)$  ha  $t = 0$  come radice di molteplicità 2. Deve quindi essere  $f(t) = at^2$ , e derivando rispetto a  $t$  si ha  $2at = f'(t) = F_p(v + tu)$ ; questo prova che la retta tangente a  $C$  in  $q$  è trasversa a  $C_p$  e quindi il punto 1).

Si fissi adesso un punto  $q \in \mathbb{T}_p C$ , sono possibili due casi: se  $p$  è un flesso di  $C$ , allora  $f$  è costante, ovvero  $f' = 0$  e  $\mathbb{T}_p C$  è una componente di  $C_p$ . La restante componente di  $C_p$  non può contenere il punto  $p$  e quindi  $\nu_p(C, C_p) = \nu_p(C, \mathbb{T}_p C) = 3$ . Se invece  $p$  non è un flesso, allora  $\mathbb{T}_p C$  non è una componente di  $C_p$  pur essendone tangente in un suo punto liscio, questo implica che  $C_p$  è liscia e prova il punto 3). Per il calcolo di  $\nu_p(C, C_p)$  prendiamo un sistema di coordinate omogenee  $x_0, x_1, x_2$  nelle quali  $p = [1, 0, 0]$  e  $\mathbb{T}_p C$  è la retta di equazione  $x_2 = 0$ . In tali coordinate le equazioni di  $C$  e  $C_p$  sono rispettivamente

$$F = x_2 x_0^2 + 2B(x_1, x_2)x_0 + C(x_1, x_2), \quad \frac{1}{2}F_p = x_2 x_0 + B(x_1, x_2),$$

che nelle coordinate affini  $x = x_1/x_0$  e  $y = x_2/x_0$  diventano

$$f = y + 2B(x, y) + C(x, y), \quad g = y + B(x, y).$$

La condizione che  $p$  non sia un flesso significa che  $y$  non divide il polinomio omogeneo  $B(x, y)$  o equivalentemente che la retta  $y = 0$  non è una componente del cono tangente di  $f - g = B(x, y) + C(x, y)$ . Dal Teorema 5.3.4 segue dunque che  $f$  e  $g$  hanno molteplicità di intersezione 2 in  $p$ .  $\square$

L'apparentemente innocua Proposizione 6.3.2 permette di dimostrare facilmente due interessanti corollari.

**Corollario 6.3.3.** *Ogni cubica piana liscia contiene esattamente 9 flessi distinti. Ogni retta passante per due flessi ne contiene un terzo.*

*Dimostrazione.* Dimostriamo solo la prima asserzione: la seconda (teorema di Gua de Malves, Esercizio 5.20) è un caso particolare del teorema dei tangenziali di Mac-Laurin.

Sia  $C$  una cubica piana liscia e definiamo  $H \subset \mathbb{P}^2$  come l'insieme dei punti  $p$  tali che la polare  $C_p$  è una conica singolare; per Bézout basta dimostrare che  $H$  è una cubica che interseca trasversalmente  $C$ . In un sistema di coordinate omogenee  $x_0, x_1, x_2$ , detta  $F = 0$  l'equazione di  $C$  e  $H_i$  la matrice Hessiana della conica  $\frac{\partial F}{\partial x_i}$ , per  $i = 0, 1, 2$ , si ha che  $H$  è la curva di equazione  $\det(x_0 H_0 + x_1 H_1 + x_2 H_2) = 0$  che ha evidentemente grado 3.

Sia ora  $p \in C \cap H$  un flesso di  $C$  e prendiamo un sistema di coordinate omogenee tali che  $p = [1, 0, 0]$  e  $C_p$  è la conica di equazione  $x_0 x_2 = 0$ ; la retta  $L$  di equazione  $x_2 = 0$  è la retta tangente a  $C$  in  $p$  e quindi  $\nu_p(C, H) = 1$  se e solo se  $\nu_p(L, H) = 1$ , cioè se e solo se  $t = 0$  è una radice semplice di  $\det(H_0 + tH_1) = 0$ . Si noti adesso che il punto  $q = [0, 1, 0]$  non appartiene a  $C$  e per la formula di Eulero  $q$  non appartiene nemmeno a  $C_q$ ; questo prova che se  $H_1 = (a_{ij})_{i,j=0,1,2}$ , allora  $a_{11} \neq 0$  e, tenendo presente che

$$H_0 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

si ha che  $\det(H_0 + tH_1) = -a_{11}t + t^2(\dots)$ .  $\square$

**Corollario 6.3.4.** *Sia dato un punto  $p$  di una cubica piana liscia  $C$  e denotiamo con  $\{p, p, q_1, q_2, q_3, q_4\}$  i sei punti, contati con molteplicità, di  $C \cap C_p$ . Allora le quattro rette  $L_i = \overline{pq_i}$ , per  $i = 1, \dots, 4$ , sono distinte.*

*Dimostrazione.* Dalla Proposizione 6.3.2 segue che i punti  $q_1, \dots, q_4$  sono distinti e quindi, se fosse  $L_i = L_j$ , allora si avrebbe una retta tangente a  $C$  nei punti  $q_i$  e  $q_j$  in contraddizione con il teorema di Bézout.  $\square$

**Definizione 6.3.5.** *Nelle notazioni del Corollario 6.3.4 e denotando con  $F_p$  è il fascio delle rette passanti per  $p$ , chiameremo **quaterna di Salmon** della coppia  $(C, p)$  la quaterna non ordinata  $\{L_1, L_2, L_3, L_4\} \subset F_p$ .*

È molto facile descrivere algebricamente la forma binaria di quarto grado le cui soluzioni formano la quaterna di Salmon di  $(C, p)$ . Siano infatti  $x_0, x_1, x_2$  coordinate omogenee tali che  $p = [1, 0, 0]$  e consideriamo l'isomorfismo  $F_p \cong \mathbb{P}^1$  che al punto di coordinate omogenee  $[a, b]$  associa la retta di rappresentazione parametrica  $t \mapsto [t, a, b]$ . Se  $F(x_0, x_1, x_2) = A(x_1, x_2)x_0^2 + 2B(x_1, x_2)x_0 + C(x_1, x_2)$  è l'equazione di  $C$ , allora la retta  $[a, b] \in F_p$  appartiene alla quaterna di Salmon se e solo se  $f(t) = F(t, a, b)$  è costante oppure ha una radice doppia; ne segue che le rette  $L_i$  sono in bigezione con le radici del discriminante  $B^2 - AC$ .

**Teorema 6.3.6 (Salmon, 1851).** *Per ogni coppia di punti  $p, q$  di una cubica liscia  $C$  esiste una proiettività di fasci  $\phi: F_p \rightarrow F_q$  che trasforma l'una nell'altra le quaterne di Salmon delle coppie  $(C, p)$  e  $(C, q)$ .*

*Dimostrazione.* La dimostrazione che daremo risale a Luigi Cremona (1861); non si tratta della dimostrazione più semplice possibile, ma ha il vantaggio di fornire una costruzione esplicita di  $\phi$ . A meno di scambiare  $p$  e  $q$  possiamo supporre che la retta  $L = \overline{pq}$  non sia tangente a  $C$  nel punto  $p$ . Indichiamo con  $r$  il terzo punto di intersezione di  $L$  con  $C$ , con  $s$  un punto tale che  $\mathbb{T}_s C \cap C = \{s, s, r\}$  e denotiamo  $M = \overline{rs}$ . Si noti che, avendo supposto  $L \neq \mathbb{T}_p C$ , si ha che  $r \neq p$  e di conseguenza  $M \neq \mathbb{T}_s C$ . Dati due punti  $a, b \in C$  si definisce  $\hat{C}_{a,b} = C_{a,b} - (\{\overline{ab}\} \times F_b) - (F_a \times \{\overline{ab}\})$ , dove  $C_{a,b}$  è la corrispondenza di tipo (3, 3) definita a pagina 109. Si consideri la corrispondenza di tipo (4, 4), composizione delle due corrispondenze di tipo (2, 2)

$$\hat{C}_{s,q} \circ \hat{C}_{p,s} \subset F_p \times F_q.$$

È chiaro che tale corrispondenza contiene come componente la corrispondenza  $\hat{C}_{p,q}$ , si definisce quindi

$$B = \hat{C}_{s,q} \circ \hat{C}_{p,s} - \hat{C}_{p,q} \subset F_p \times F_q.$$

Per meglio capire la corrispondenza  $B$  ragioniamo sinteticamente: per ogni  $N \in F_p$  siano  $p, p_1, p_2$  i punti di intersezione di  $N$  con  $C$ ; siano poi  $q_1$  il terzo punto di intersezione di  $C$  con la retta  $\overline{sp_1}$  e  $q_2$  il terzo punto di intersezione di  $C$  con la retta  $\overline{sp_2}$ . Allora vale  $B_N = \{\overline{q_1q_1}, \overline{q_1q_2}\}$ . Se  $L_i$  appartiene alla quaterna di Salmon di  $(C, p)$ , allora segue dal teorema dei tangenziali di Mac-Laurin che  $B_{L_i} = \{V, V\}$ , dove  $V$  appartiene alla quaterna di Salmon di  $(C, q)$ . Inoltre  $B_M = \{L, L\}$  e quindi esistono almeno cinque rette verticali distinte tangenti a  $B$ : per il Lemma 6.2.6 esiste una corrispondenza  $\phi$  di tipo (1, 1) tale che  $B = 2\phi$  ed una tale  $\phi$  è esattamente la proiettività cercata.  $\square$

Se  $C$  e  $D$  sono due cubiche lisce proiettivamente equivalenti, allora per ogni  $p \in C$  e  $q \in D$  le quaterne di Salmon delle coppie  $(C, p)$  e  $(D, q)$  sono a loro volta proiettivamente equivalenti. Il prossimo teorema mostra che vale anche il viceversa.

**Teorema 6.3.7.** *Siano  $C, D \subset \mathbb{P}^2$  due cubiche lisce,  $p \in C$ ,  $q \in D$ . Allora  $C$  e  $D$  sono proiettivamente equivalenti se e solo se le quaterne di Salmon delle coppie  $(C, p)$  e  $(D, q)$  sono proiettivamente equivalenti.*

*Dimostrazione.* Assumiamo le due quaterne di Salmon proiettivamente equivalenti: per il Corollario 6.3.3 ed il Teorema 6.3.6 non è restrittivo supporre  $p$  e  $q$  punti di flessione di  $C$  e  $D$  rispettivamente. Sia  $\phi: F_p \rightarrow F_q$  la proiettività che trasforma l'una nell'altra le quaterne di Salmon di  $C$  e  $D$ , a meno di un'azione del gruppo trirettangolo sulle quaterne possiamo supporre che  $\phi$  trasforma la retta tangente a  $C$  in  $p$  nella retta tangente a  $D$  in  $q$ . Agendo su  $D$  con una opportuna proiettività di  $\mathbb{P}^2$  possiamo assumere che  $p = q$  e che le due quaterne di Salmon coincidano, in particolare  $C$  e  $D$  avranno la stessa retta tangente  $L$  in  $p$ . Agendo ancora su  $D$  con una proiettività che lascia fissa ogni retta del fascio  $F_p$  si può assumere che  $C_p = D_p = L + M$  (vedi Esercizio 2.21). Prendiamo adesso un sistema di coordinate omogenee tali che  $p = [0, 0, 1]$ ,  $L = \{x_0 = 0\}$  e  $M = \{x_2 = 0\}$ . Un facile conto mostra che nelle coordinate affini  $x = x_1/x_0$  e  $y = x_2/x_0$  le equazioni di  $C$  e  $D$  sono rispettivamente

$$y^2 = c(x), \quad y^2 = d(x),$$

con  $c$  e  $d$  polinomi di grado 3. Se  $\alpha$  è una radice di  $c$ , allora la retta  $\{x = \alpha\}$  appartiene alla quaterna di Salmon di  $(C, p)$ , ne segue che polinomi  $c$  e  $d$  hanno le stesse radici e differiscono per una costante moltiplicativa  $a^2$ . La trasformazione affine  $y \mapsto ay$  trasforma infine  $C$  in  $D$ .  $\square$

*Osservazione 6.3.8.* La dimostrazione del Teorema 6.3.7 mostra inoltre che ogni cubica liscia è proiettivamente equivalente ad una cubica di equazione affine

$$y^2 = 4x^3 - g_2x - g_3 \tag{6.1}$$

che viene detta in **forma normale di Weierstrass**. Per quanto visto nel Capitolo 3, se la cubica  $C$  è in forma normale di Weierstrass (6.1), allora l'invariante  $j$  associato alle quaterne di Salmon di  $C$  si calcola facilmente tramite la formula

$$j = 1728 \frac{g_2^3}{g_2^3 - 27g_3^2}.$$

### Esercizi

**6.13.** Sia  $E \subset \mathbb{R}^2$  un sottoinsieme finito tale che per ogni coppia di punti di  $E$  la retta passante per essi contiene almeno un altro punto di  $E$ . Provare che i punti di  $E$  sono allineati. Dedurre che una cubica affine liscia  $C \subset \mathbb{C}^2$  di equazione  $F \in \mathbb{R}[x, y]$  possiede al più tre flessi a coordinate reali. (Sugg.: sia  $S$  l'insieme delle rette che contengono almeno due punti di  $E$  e sia  $A = \{(L, p) \in S \times E \mid p \notin L\}$ . Se per assurdo  $A \neq \emptyset$  si prenda un elemento  $(L_0, p_0)$  tale che la distanza tra  $p_0$  e  $L_0$  sia minima.)

**6.14.** Sia  $\phi: F_p \rightarrow F_q$  la proiettività costruita nella dimostrazione del Teorema 6.3.6 e sia  $Q$  la conica proiettivamente generata da  $\phi$ . Determinare le tangenti a  $Q$  nei punti  $p, q$  e la polare di  $s$  rispetto a  $Q$ .

**6.15 (Forme canoniche dell'equazione cubica, \*).** Nel presente esercizio  $C$  denoterà una cubica piana liscia su un campo algebricamente chiuso. Dimostrare che:

1. Siano  $p, q, r \in C$  tre flessi distinti e allineati, allora  $\mathbb{T}_p C \cap \mathbb{T}_q C \cap \mathbb{T}_r C = \emptyset$ .
2. In un opportuno sistema di coordinate affini, l'equazione di  $C$  assume la **forma canonica di Deuring**

$$y^2 + y + \delta xy = x^3.$$

(Sugg.: siano  $p = [0, 0, 1]$ ,  $q = [1, 0, 0]$  due flessi e  $[0, 1, 0] = \mathbb{T}_p C \cap \mathbb{T}_q C$ ).

3. In un opportuno sistema di coordinate omogenee l'equazione di  $C$  assume la forma

$$(x_0 + x_1 + x_2)^3 + lx_0x_1x_2 = 0.$$

(Sugg.: sia  $L$  retta,  $p_0, p_1, p_2 \in C \cap L$  flessi allineati e  $\mathbb{T}_{p_i}C = \{x_i = 0\}$ ,  $L = \{x_0 + x_1 + x_2 = 0\}$ .)

4. In opportuni sistemi di coordinate omogenee l'equazione di  $C$  assume le forme

$$\begin{aligned} x_0^3 + x_1^3 + x_2^3 + mx_0x_1x_2 &= 0, \\ (x_0^2 + x_1^2 + x_2^2)(x_0 + x_1 + x_2) - (x_0^3 + x_1^3 + x_2^3) + nx_0x_1x_2 &= 0, \\ x_0^3 + x_1^3 + x_2^3 &= h(x_0 + x_1 + x_2)^3. \end{aligned}$$

(Sugg.: considerare il generico cambio di coordinate omogenee che commuta con l'azione del gruppo simmetrico  $\Sigma_3$ ; tale cambio di coordinate è rappresentato da una matrice

$$\begin{pmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{pmatrix}, \quad \alpha \in \mathbb{K}.$$

Sostituire in 3) e risolvere in  $\alpha$ .)

## 6.4 La legge di gruppo su di una cubica liscia

In questa sezione denoteremo con  $\mathbb{K}$  un campo algebricamente chiuso di caratteristica arbitraria. Se  $C$  è una curva piana e  $p \in \mathbb{P}^2$  denoteremo come al solito con  $C_p$  la curva polare di  $p$  rispetto a  $C$ . Date tre curve  $C, D, E \subset \mathbb{P}^2$  si può considerare l'insieme

$$Z = \{(p, q) \in \mathbb{P}^2 \times \mathbb{P}^2 \mid p \in C_q \cap D_q \cap E_q\}$$

assieme alle sue proiezioni  $J(C, D, E) \subset \mathbb{P}^2$  e  $S(C, D, E) \subset \mathbb{P}^2$  sul primo e sul secondo fattore rispettivamente. Si può dimostrare che “in generale”  $J$  e  $S$  sono curve piane e tra poco calcoleremo esattamente l'equazione di  $J$ .

**Definizione 6.4.1 (Sylvester 1853).** *La curva  $J(C, D, E)$  si dice la **Jacobiana**<sup>1</sup> della terna  $C, D, E$ .*

**Definizione 6.4.2 (Cremona 1862, [Cre1862, pag. 68]).** *La curva  $S(C, D, E)$  si dice la **Steineriana** della terna  $C, D, E$ .*

Se  $J(C, D, E) = \mathbb{P}^2$  diremo che la Jacobiana della terna è indeterminata; similmente per la Steineriana. Seguirà a posteriori che la Jacobiana è molto più interessante della Steineriana, nonché più facile da studiare: per questo motivo ci occuperemo in queste note solamente delle Jacobiane. Un'altra curva storicamente associata alla terna  $C, D, E$  è la **Cayleyana**, definita come l'involuppo delle rette  $\overline{pq}$  al variare di  $(p, q) \in Z$ .

**Lemma 6.4.3.** *Siano  $C, D, E$  curve piane di gradi  $n, m, l$ . Se la Jacobiana  $J(C, D, E)$  non è indeterminata, allora è una curva piana di grado  $n + m + l - 3$ .*

<sup>1</sup> Non bisogna assolutamente confondere la curva Jacobiana di una terna con la varietà Jacobiana di una curva, vedi [GH1978, p.333].

*Dimostrazione.* Siano  $F, G, H$  le equazioni di  $C, D, E$  in un sistema di coordinate omogenee fissato  $x_0, x_1, x_2$ ; denotiamo con  $F_i, G_i, H_i$  le derivate parziali di  $F, G, H$  rispetto alla variabile  $x_i$ , per  $i = 0, 1, 2$ . La coppia  $([u], [v])$  appartiene a  $Z$  se e solo se vale

$$\begin{cases} v_0 F_0(u) + v_1 F_1(u) + v_2 F_2(u) = 0 \\ v_0 G_0(u) + v_1 G_1(u) + v_2 G_2(u) = 0 \\ v_0 H_0(u) + v_1 H_1(u) + v_2 H_2(u) = 0 \end{cases}$$

e quindi  $J(C, D, E)$  è l'insieme dei punti  $p = [u]$  tali che il precedente sistema lineare nelle incognite  $v_i$  possiede una soluzione non banale. È quindi evidente che l'equazione di  $J(C, D, E)$  è

$$\det \begin{pmatrix} F_0 & G_0 & H_0 \\ F_1 & G_1 & H_1 \\ F_2 & G_2 & H_2 \end{pmatrix} = 0.$$

□

È chiaro che se le tre curve  $C, D, E$  hanno lo stesso grado, allora  $J(C, D, E)$  dipende solo dal sistema lineare generato dalle tre curve.

**Lemma 6.4.4.** *Sia  $p$  un punto liscio di una curva piana  $C$  e siano  $d, m$  interi positivi. Allora l'insieme delle curve  $D$  di grado  $m$  tali che  $\nu_p(C, D) \geq d$  è un sistema lineare di codimensione  $\leq d$  nello spazio  $|\mathcal{O}(m)|$ .*

*Dimostrazione.* Basta mostrare che se  $V \subset |\mathcal{O}(m)|$  è un sistema lineare e  $a$  è il minimo valore di  $\nu_p(C, D)$  al variare di  $D \in V$ , allora  $W = \{D \in V \mid \nu_p(C, D) > a\}$  è un iperpiano in  $V$ . Siano  $x, y$  coordinate affini tali che  $p = (0, 0)$  e la retta  $y = 0$  sia tangente a  $C$  in  $p$ . Sia  $r$  la dimensione di  $V$ , sia  $f$  l'equazione affine di  $C$  e siano  $g_0, \dots, g_r$  le equazioni affini di un sistema di generatori di  $V$  tali che  $\nu_p(f, g_0) = a$ . Esistono costanti  $\alpha_1, \dots, \alpha_r \in \mathbb{K}$  tali che  $\nu_p(f, g_i - \alpha_i g_0) > a$ : infatti, come nella dimostrazione di 5.3.5, per ogni  $i = 0, \dots, r$  esiste un polinomio  $h_i$  tale che

$$g_i - h_i f = \beta_i x^a + \sum \{\text{monomi di grado } > a\}.$$

Dato che  $\beta_0 \neq 0$ , basta prendere  $\alpha_i = \beta_i \beta_0^{-1}$ . □

Vogliamo adesso studiare la molteplicità di intersezione  $\nu_p(C, J)$ , dove  $J = J(C, D, E)$ , nelle seguenti ipotesi:

1.  $C$  curva di grado  $n$  e  $p \in C$  punto liscio.
2.  $D, E$  hanno lo stesso grado  $m$  e generano un fascio  $V$ .
3.  $\nu_p(C, D) < +\infty$ .

Per il Lemma 6.4.4 possiamo assumere che  $d = \nu_p(C, D) < \nu_p(C, E) = e \leq +\infty$  ed  $E$  è l'unica curva di  $V$  ad avere molteplicità di intersezione con  $C$  in  $p$  maggiore di  $d$ .

**Definizione 6.4.5.** *Nelle notazioni precedenti, diremo che  $p \in C$  è un **punto di ramificazione** per il fascio  $V$  se  $e \geq d + 2$ .*

**Lemma 6.4.6.** *Nelle notazioni precedenti, se  $m$  non è divisibile per la caratteristica di  $\mathbb{K}$ , allora:*

1.  $\nu_p(C, J) \geq d + e - 1$ . Inoltre vale  $\nu_p(C, J) = d + e - 1$  se e solo se  $e = +\infty$  oppure se  $e < +\infty$  e la caratteristica di  $\mathbb{K}$  non divide  $e - d$ .
2.  $\nu_p(C, J) \geq 2d$ . Inoltre vale  $\nu_p(C, J) = 2d$  se e solo se  $p$  non è un punto di ramificazione per il fascio  $V$ .

*Dimostrazione.* [1] Siano  $F, G, H$  le equazioni di  $C, D, E$  in un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che  $p = [1, 0, 0]$  e la retta tangente a  $C$  in  $p$  ha equazione  $x_2 = 0$ . Per la formula di Eulero vale

$$\begin{aligned} x_0 F_0 - (n - m)F &= mF - x_1 F_1 - x_2 F_2, \\ x_0 G_0 &= mG - x_1 G_1 - x_2 G_2, & x_0 H_0 &= mH - x_1 H_1 - x_2 H_2 \end{aligned}$$

e quindi

$$mx_0 \begin{vmatrix} F_0 & G_0 & H_0 \\ F_1 & G_1 & H_1 \\ F_2 & G_2 & H_2 \end{vmatrix} \equiv \begin{vmatrix} F & G & H \\ F_1 & G_1 & H_1 \\ F_2 & G_2 & H_2 \end{vmatrix} \pmod{F}.$$

Passando alle coordinate affini  $x = \frac{x_1}{x_0}$  e  $y = \frac{x_2}{x_0}$  si ha  $\nu_p(C, J) = \nu_p(f, \phi)$ , dove  $f, g, h$  sono le equazioni affini di  $C, D, E$  rispettivamente e

$$\phi = \begin{vmatrix} f & g & h \\ f_x & g_x & h_x \\ f_y & g_y & h_y \end{vmatrix}.$$

Aggiungendo a  $g$  ed  $h$  elementi dell'ideale principale  $(f) \subset \mathbb{K}[x, y]$  otteniamo un nuovo  $\phi$  che è congruo al precedente modulo  $f$ . Tenendo presente che  $f = y + \sum\{\text{monomi di grado} > 1\}$ , non è restrittivo supporre che  $g = x^d + \sum\{\text{monomi di grado} > d\}$  e, qualora  $e < +\infty$ , anche che  $h = x^e + \sum\{\text{monomi di grado} > e\}$ . Un semplice conto mostra che  $\phi = (e - d)x^{d+e-1} + \sum\{\text{monomi di grado} > d + e - 1\}$  che prova il teorema nel caso  $e < +\infty$ . Se invece  $e = +\infty$ , allora  $f$  e  $h$  hanno un fattore comune  $f_1$  tale che  $f_1(0, 0) = 0$  e lo sviluppo del determinante mostra che  $\phi \in (f_1)$  e quindi  $\nu_p(f, \phi) = +\infty$ .

[2] Il secondo punto è conseguenza immediata del primo.  $\square$

**Teorema 6.4.7.** *Sia  $C$  una curva liscia di grado  $n \geq 3$  e siano  $D, E$  curve di grado  $m$  che non contengono  $C$  come componente. Siano  $p_1, \dots, p_{nm}$  i punti di intersezione di  $C$  e  $D$  contati con molteplicità. Se  $E \cap C$  contiene  $nm - 1$  punti di  $C \cap D$ , allora:*

1.  $D = E$  oppure,
2.  $D \neq E$  ed esiste una curva del fascio generato da  $D$  ed  $E$  che contiene  $C$  come componente.

*In entrambi i casi  $D$  ed  $E$  hanno gli stessi punti di intersezione con  $C$ , contati con molteplicità.*

*Dimostrazione.* Assumiamo che  $D \neq E$  e proviamo che vale l'opzione 2. Non è restrittivo supporre che la caratteristica di  $\mathbb{K}$  non divida  $m$ , altrimenti basta considerare al posto di  $D$  e  $E$  le curve  $D + L$  ed  $E + L$ , dove  $L$  è una retta generica. Proviamo per prima cosa che  $\nu_p(C, D) = \nu_p(C, E)$  per ogni punto  $p \in C$ . Se così non fosse, detto  $\{p_1, \dots, p_r\} = C \cap D$  si avrebbe, a meno di permutazioni degli indici,

$$\begin{cases} \nu_{p_i}(C, E) \geq \nu_{p_i}(C, D) & \text{per } i = 1, \dots, r - 1, \\ \nu_{p_r}(C, E) = \nu_{p_r}(C, D) - 1. \end{cases}$$

Per il teorema di Bézout e per il Lemma 6.4.4 si ha che  $C$  non contiene punti di ramificazione per il fascio  $\langle D, E \rangle$  ed in particolare la Jacobiana  $J$  della terna  $C, D, E$  non è indeterminata e non contiene  $C$  come componente. Ora il grado di  $J$  è  $2m + (n - 3) \geq 2m$  e per Bézout

$$\sum_p \nu_p(C, J) \geq 2nm > \sum_p 2 \min(\nu_p(C, D), \nu_p(C, E)).$$

Quindi esiste un punto  $p \in C$  tale che  $\nu_p(C, J) > 2\min(\nu_p(C, D), \nu_p(C, E))$  e per il Lemma 6.4.6, il punto  $p$  è di ramificazione per il fascio  $\langle D, E \rangle$ .

Abbiamo dunque stabilito che  $\nu_p(C, D) = \nu_p(C, E)$  per ogni  $p \in C$ ; preso  $q \in C - D$  allora l'unica curva di  $\langle D, E \rangle$  che contiene  $q$  deve contenere  $C$  come componente.  $\square$

Una delle applicazioni più piacevoli del Teorema 6.4.7 è senza dubbio la verifica della struttura di gruppo sulle cubiche lisce. Sia  $C \subset \mathbb{P}^2$  una cubica liscia e sia  $o \in C$  un punto fissato; definiamo un'applicazione simmetrica "di somma"  $C \times C \xrightarrow{\oplus} C$ , dipendente dalla scelta di  $o$ , nel modo seguente.

Innanzitutto, per ogni  $a \in C$  denotiamo con  $\hat{a} \in C$  il terzo punto di intersezione di  $C$  con la retta  $\overline{o\hat{a}}$ ; poi per ogni coppia di punti  $a, b \in C$  si definisce  $a \oplus b = \hat{r}$ , dove  $r$  è il terzo punto di intersezione di  $C$  con la retta  $\overline{ab}$ . Osserviamo che l'applicazione  $\oplus$  è simmetrica, cioè  $a \oplus b = b \oplus a$  e che  $\hat{o}$  coincide con il tangenziale di  $o$ .

**Teorema 6.4.8.** *L'applicazione  $\oplus$  sopra definita induce su  $C$  una struttura di gruppo abeliano con elemento neutro  $o$ .*

*Dimostrazione.* Verifichiamo che gli assiomi di gruppo sono soddisfatti.

*Elemento neutro.* Per definizione si ha  $o \oplus a = a \oplus o = \hat{\hat{a}} = a$ .

*Esistenza dell'inverso.* Per ogni  $a \in C$  definiamo  $\ominus a$  come il terzo punto di intersezione di  $C$  con la retta  $\overline{a\hat{o}}$ . Allora  $(\ominus a) \oplus a = a \oplus (\ominus a) = \hat{\hat{o}} = o$ .

*Associatività.* Siano  $a, b, c \in C$  e denotiamo  $d = a \oplus b, e = b \oplus c, f = d \oplus c, g = a \oplus e$ ; bisogna dimostrare che  $f = g$  o equivalentemente che  $\hat{f} = \hat{g}$ .

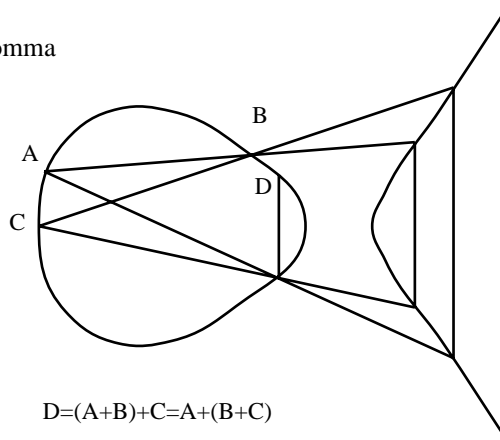
Consideriamo l'esagono inscritto a  $C$  di vertici  $a, b, c, d, o$  ed  $e$ ; i suoi lati sono le rette  $L_1 = \overline{ab}, L_2 = \overline{bc}, L_3 = \overline{cd}, L_4 = \overline{do}, L_5 = \overline{oe}$  e  $L_6 = \overline{ea}$ . Guardiamo alle intersezioni di  $C$  con le due cubiche formate rispettivamente dai lati pari e dispari dell'esagono, esse sono:

$$C \cap (L_1 + L_3 + L_5) = \{a, b, \hat{d}, c, d, \hat{f}, o, e, \hat{e}\},$$

$$C \cap (L_2 + L_4 + L_6) = \{b, c, \hat{e}, d, o, \hat{d}, e, a, \hat{g}\}.$$

Le due intersezioni hanno otto dei nove punti in comune e, per il Teorema 6.4.7, devono avere in comune anche il nono e quindi  $\hat{f} = \hat{g}$ .  $\square$

Associatività della somma



**Figura 6.3.** L'associatività nella cubica

Il riconoscimento della struttura di gruppo sulla cubica si deve allo sviluppo della teoria degli integrali ellittici avvenuto principalmente per opera di Jakob Bernoulli (1679), Johann Bernoulli (1698), Fagnano (1714), Euler (1756), Abel e Jacobi (1829).

Segue immediatamente dalla definizione della struttura di gruppo su una cubica piana liscia con elemento neutro  $o$  che la somma di tre punti allineati è sempre uguale a  $\hat{o}$ . Più in generale, è anche vero che la somma dei  $3m$  punti di intersezione di  $C$  con una qualsiasi curva  $D$  di grado  $m$  è indipendente da  $D$ . Per dimostrare questo fatto abbiamo però bisogno di introdurre il concetto di divisore e dare una diversa caratterizzazione della struttura di gruppo su  $C$ .

**Definizione 6.4.9.** Sia  $C \subset \mathbb{P}^2$  una curva liscia, il **gruppo dei divisori** su  $C$  si denota con  $\text{Div}(C)$  ed è il gruppo abeliano libero generato dai punti di  $C$ . I **divisori** su  $C$  sono gli elementi di  $\text{Div}(C)$  e non sono altro che combinazioni lineari formali finite  $\sum_{i=1}^r n_i p_i$ , con  $n_i \in \mathbb{Z}$  e  $p_i \in C$  per ogni  $i = 1, \dots, r$ .

Un divisore  $\phi = \sum n_i p_i$  si dice **effettivo** se  $n_i \geq 0$  per ogni  $i$ ; il divisore nullo è l'elemento neutro di  $\text{Div}(C)$  e sarà indicato con  $0$ . Il **grado** di un divisore  $\phi = \sum n_i p_i$  è per definizione la somma  $\deg(\phi) = \sum n_i \in \mathbb{Z}$ . I divisori di grado 0 formano un sottogruppo  $\text{Div}^0(C) \subset \text{Div}(C)$ .

Se  $D \subset \mathbb{P}^2$  è una curva che non contiene  $C$  come componente, si definisce un divisore effettivo  $D|_C \in \text{Div}(C)$  ponendo

$$D|_C = \sum_{p \in C \cap D} \nu_p(C, D)p.$$

Chiameremo **divisori aggiunti** i divisori su  $C$  della forma  $D|_C$ . Notiamo incidentalmente che nella dimostrazione del Teorema 6.4.7 si è provato che, se  $D|_C = E|_C$ , allora o  $E = D$ , oppure esiste una curva nel fascio generato da  $D$  ed  $E$  che contiene  $C$  come componente. Per il teorema di Bézout  $\deg(D|_C) = \deg(C) \deg(D)$ .

**Definizione 6.4.10.** Due divisori  $\phi$  e  $\psi$  su una curva liscia  $C$  si dicono **linearmente equivalenti** se esistono due curve piane  $D$  ed  $E$  dello stesso grado, che non contengono  $C$  come componente e tali che  $\phi + D|_C = \psi + E|_C$ .

Lasciamo per esercizio al lettore la facile verifica che l'equivalenza lineare è una relazione di equivalenza che denoteremo con il simbolo  $\sim$ . È inoltre immediato osservare che divisori linearmente equivalenti hanno lo stesso grado e che la relazione  $\sim$  commuta con le operazioni di somma e differenza di divisori.

**Teorema 6.4.11.** Siano  $p$  e  $q$  due punti di una curva piana liscia di grado  $\geq 3$ . Allora vale  $p \sim q$  (come divisori) se e solo se  $p = q$ .

*Dimostrazione.* Indichiamo con  $C$  la curva, sia  $n$  il suo grado e supponiamo  $p$  e  $q$  linearmente equivalenti: allora esistono due curve  $D, E$  dello stesso grado  $m$  tali che  $p + D|_C = q + E|_C$ . Ne segue che le intersezioni di  $D$  ed  $E$  con  $C$  hanno almeno  $nm - 1$  punti in comune e, per il Teorema 6.4.7, si ha  $D|_C = E|_C$  da cui segue  $p = q$ .  $\square$

**Definizione 6.4.12.** Il **gruppo delle classi** di una curva liscia  $C$  si denota con  $\text{Cl}(C)$  ed è il quoziente di  $\text{Div}(C)$  per la relazione di equivalenza lineare. Con  $\text{Cl}^0(C) \subset \text{Cl}(C)$  viene indicato il sottogruppo delle classi di equivalenza lineare di divisori di grado 0, ovvero il quoziente di  $\text{Div}^0(C)$  per la relazione di equivalenza lineare.

**Teorema 6.4.13.** Sia  $C$  curva liscia di grado  $n \geq 3$  e sia  $o \in C$  un punto fissato. Allora l'applicazione

$$\mu: C \rightarrow \text{Cl}^0(C), \quad \mu(p) = p - o,$$

è iniettiva. Se  $n = 3$  e consideriamo su  $C$  la struttura di gruppo avente  $\oplus$  come prodotto e  $o$  come elemento neutro, allora  $\mu$  è un isomorfismo di gruppi.



*Dimostrazione.* L'iniettività di  $\mu$  non è altro che una riformulazione del Teorema 6.4.11. Se  $C$  è una cubica occorre provare che:

1.  $\mu(a \oplus b) = \mu(a) + \mu(b)$ .
2. L'immagine di  $\mu$  contiene un insieme di generatori di  $\text{Cl}^0(C)$ .

Per dimostrare 1. basta osservare che, se  $c = a \oplus b$  allora esistono due rette  $L$  e  $N$  tali che  $L|_C = a + b + (\hat{c})$  e  $N|_C = o + c + (\hat{c})$ ; ne segue che  $a + b - o + N|_C = c + L|_C$  e quindi  $a + b - 2o \sim c - o$ . Per dimostrare 2. basta osservare che ogni divisore di grado 0 si può scrivere come combinazione lineare a coefficienti interi di divisori del tipo  $p - o$ , con  $p \in C$ .  $\square$

### Esercizi

**6.16.** Dimostrare che, nelle notazioni del Lemma 6.4.3, se la caratteristica di  $\mathbb{K}$  divide  $n, m$  e  $l$ , allora la Jacobiana è indeterminata; se la caratteristica di  $\mathbb{K}$  divide  $m$  e  $l$ , allora  $C \subset J(C, D, L)$ .

**6.17 (La Hessiana, \*).** (caratteristica 0) Sia  $C$  una curva piana irriducibile di grado  $n \geq 2$  e di equazione  $F(x_0, x_1, x_2) = 0$ . La **Hessiana** di  $C$  è la curva di grado  $3(n - 2)$  e di equazione

$$\det \begin{pmatrix} F_{00} & F_{01} & F_{02} \\ F_{10} & F_{11} & F_{12} \\ F_{20} & F_{21} & F_{22} \end{pmatrix} = 0.$$

Provare che  $H$  non è indeterminata e non contiene  $C$  come componente. Se  $p \in C$  è un punto liscio e  $L$  è la retta tangente a  $C$  in  $p$ , si provi che  $\nu_p(C, L) = \nu_p(C, H) + 2$  e si deduca che una curva liscia di grado  $n$  possiede  $3n(n - 2)$  flessi contati con molteplicità. (Sugg.: mostrare che  $\nu_p(C, L) > 2$  se e solo se  $p \in H$  e poi usare 5.3.7. Vedi anche [Walk1950]).

**6.18.** Provare che se una curva liscia  $C$  ha grado  $\leq 2$ , allora  $\text{Cl}^0(C) = 0$  e la funzione grado induce un isomorfismo tra  $\text{Cl}(C)$  e  $\mathbb{Z}$ .

## 6.5 Il teorema del resto

In questa sezione vedremo una versione debole (ma non troppo) del teorema  $Af + B\phi$  di Max Noether. La versione completa sarà proposta come esercizio nella Sezione 8.4.

**Teorema 6.5.1 (Max Noether, 1872).** *Siano  $C, D$  ed  $E$  curve piane di equazioni  $F, \Phi$  ed  $H$  rispettivamente. Si assuma inoltre che  $C$  e  $D$  siano senza componenti comuni e che  $D$  non contenga punti singolari di  $C$ . Allora vale  $\nu_p(C, E) \geq \nu_p(C, D)$  per ogni  $p \in C$  se e solo se  $H = AF + B\Phi$  per opportuni polinomi omogenei  $A$  e  $B$ .*

*Dimostrazione.* L'implicazione “se” è chiara, dimostriamo il “solo se” e quindi supponiamo che  $\nu_p(C, E) \geq \nu_p(C, D)$  per ogni  $p \in C$ ; per ipotesi  $D$  non interseca gli eventuali punti singolari di  $C$  e questo implica in particolare che  $C$  è una curva ridotta. Indichiamo con  $n, m$  e  $l$  i gradi delle curve  $C, D$  ed  $E$  rispettivamente. Al fine di alleggerire la dimostrazione identificheremo liberamente una curva piana con la sua equazione, in particolare se  $P, Q$  sono polinomi omogenei e  $q \in \mathbb{P}^2$  denoteremo con  $\nu_p(P, Q)$  la molteplicità di intersezione in  $q$  delle curve di equazione  $P$  e  $Q$ . Daremo due distinte dimostrazioni del teorema: la prima, di natura più algebrica, è presa da [Walk1950] e vale in caratteristica 0, mentre la seconda, più geometrica, è presa da [EC1915].

*Prima dimostrazione:* Caratteristica 0. Proviamo dapprima il teorema in alcuni casi particolari.

a) Esiste un punto  $q \notin C$  tale che  $\text{mult}_q(E) > l - n$  e  $D = \sum a_i L_i$  con  $L_i$  retta passante per  $q$  e trasversale a  $C$ . In questo caso  $\Phi$  divide  $H$ , cioè per ogni  $i$  la retta  $L_i$  è una componente di  $E$  di molteplicità almeno  $a_i$ ; sia infatti  $E = b_1 L_1 + E_1$  con  $b_1 < a_1$  e proviamo che  $L_1$  è una componente di  $E_1$ . Siano  $p_1, \dots, p_n$  i punti di intersezione di  $C$  con  $L_1$ , vale  $\nu_{p_i}(C, E) \geq \nu_{p_i}(C, D) = a_1$  e quindi, essendo  $b_1 < a_1$ , i punti  $p_1, \dots, p_n$  appartengono anche alla curva  $E_1$ . Inoltre  $\text{mult}_q(E_1) > l - n - b_1$  e quindi  $\nu_q(E_1, L_1) + \sum_i \nu_{p_i}(L_1, E_1) > l - b_1 = \text{deg}(b_1)$  e per Bézout  $L_1$  è una componente di  $E_1$ .

b) La curva  $D$  è come al punto a) e la curva  $E$  qualsiasi. Fissiamo un sistema di coordinate omogenee tali che  $q = [0, 0, 1]$ ; dato che  $q \notin C$  il polinomio  $F$  è, a meno di scalari, monico rispetto alla variabile  $x_2$  e quindi esistono unici  $Q, T$  tali che  $H = QF + T$  con  $T$  di grado  $< n$  rispetto alla variabile  $x_2$ , e quindi  $\text{mult}_q(T) > l - n$ . Possiamo tranquillamente scambiare  $H$  con  $T$  e ricondurci al punto a).

In generale siano  $p_1, \dots, p_r$  i punti di intersezione di  $C$  e  $D$ , siccome i punti  $p_i$  sono lisci per  $C$ , per ogni punto  $p_i$  passano finite rette contenenti un  $p_j$ , per  $i \neq j$  e tangenti a  $C$  (qui si usa la caratteristica 0). Sia  $q \in \mathbb{P}^2$  un punto non appartenente all'unione di  $C, D$  e delle rette sopra descritte. Fissato un sistema di coordinate omogenee tali che  $q = [0, 0, 1]$  sia  $R(x_0, x_1) = QF + U\Phi$  il risultante di  $F$  e  $\Phi$  rispetto alla variabile  $x_2$ , data la scelta di  $q$ , la curva  $R$  soddisfa le stesse condizioni della curva  $\Phi$  nel precedente caso particolare b), in particolare  $R$  e  $F$  non hanno fattori comuni.

Dato che  $\nu_p(F, UH) \geq \nu_p(F, U\Phi) = \nu_p(F, R)$  per ogni  $p \in C$  ci siamo ricondotti al punto b) e quindi  $UH = AF + BR = (A + BQ)F + UB\Phi$ ; notiamo infine che  $F$  e  $U$  non hanno fattori comuni e quindi  $U$  divide  $A + BQ$  ed il teorema è dimostrato.

*Seconda dimostrazione (Angas Scott<sup>2</sup>, 1899).* Dividiamo la dimostrazione in due passi; nel primo proviamo il teorema quando  $l \geq nm$  e nel secondo proviamo che, se il teorema vale per la terna di gradi  $(n, m, l)$ , allora vale anche per  $(n, m, l - 1)$ . Sia dunque  $l \geq nm$  e denotiamo con  $V$  il sistema lineare delle curve  $E$  di grado  $l$  tali  $\nu_p(C, E) \geq \nu_p(C, D)$  per ogni  $p \in C$ . Proviamo che la codimensione di  $V$  è esattamente  $nm$  e quindi che la dimensione di  $V$  è  $\frac{1}{2}l(l + 3) - nm$ . Siano  $p_1, \dots, p_{nm}$  i punti di intersezione di  $C$  e  $D$  contati con molteplicità e, per ogni  $i$ , sia  $L_i$  una retta generica passante per  $p_i$ . Detta  $L$  una retta tale che  $L \cap C \cap D = \emptyset$  si ha che per ogni  $j < nm$  la curva  $L_1 + \dots + L_j + (l - j)L$  ha grado  $l$ , passa per  $p_1, \dots, p_j$  ma non per i rimanenti  $p_{j+1}, \dots, p_{nm}$ ; questo prova che le  $nm$  condizioni di passaggio per i punti  $p_i$  inducono condizioni lineari indipendenti sulle curve di grado  $l \geq nm$ . Sia ora  $V' \subset V$  il sistema lineare delle curve  $H = AF + B\Phi$  al variare di  $A$  e  $B$  nello spazio dei polinomi di grado  $l - n$  e  $l - m$  rispettivamente. Si ha  $V' = \mathbb{P}(W_F + W_\Phi)$ , dove  $W_F$  (resp.  $W_\Phi$ ) è lo spazio vettoriale dei polinomi di grado  $l$  divisibili per  $F$  (resp.  $\Phi$ ). Vale quindi  $(W_F \cap W_\Phi) = W_{F\Phi}$  e

$$\dim W_F = \binom{l - n + 2}{2}, \quad \dim W_\Phi = \binom{l - m + 2}{2}, \quad \dim W_{F\Phi} = \binom{l - n - m + 2}{2}.$$

Una semplice addizione, che omettiamo, mostra che  $V'$  e  $V$  hanno la stessa dimensione e questo prova il primo passo.

Proviamo adesso il teorema assumendolo vero per la terna di gradi  $(n, m, l + 1)$ . Sia  $L$  l'equazione di una retta trasversale a  $C$  e non passante per i punti di intersezione di  $C$  e  $D$ ; per induzione esistono  $\hat{A}, \hat{B}$  tali che  $HL = \hat{A}F + \hat{B}\Phi$ . Dato che  $\nu_p(F, \hat{B}) \geq \nu_p(F, L)$  per ogni  $p \in C$ , se il grado di  $\hat{B}$  è minore di  $n$  allora  $L$  divide  $\hat{B}$  mentre se il grado di  $\hat{B}$  è maggiore o uguale a  $n$  per il primo passo si ha  $\hat{B} = UF + BL$ . Sostituendo nell'espressione di  $HL$  e tenendo presente che  $L$  non divide  $F$  si arriva alla conclusione cercata.  $\square$

<sup>2</sup> Charlotte Angas Scott 1858-1931, Inglese, allieva di Cayley: per quanto mi risulta, la prima donna ad occuparsi profittevolmente di geometria algebrica

**Teorema 6.5.2 (Teorema del resto di Brill e Noether, 1873).** *Siano  $\varphi, \psi$  ed  $\eta$  divisori effettivi su una curva piana liscia  $C$ , con  $\varphi$  e  $\psi$  linearmente equivalenti. Allora  $\varphi + \eta$  è aggiunto se e solo se  $\psi + \eta$  è aggiunto.*

*Dimostrazione.* L'enunciato è simmetrico in  $\varphi$  e  $\psi$ ; assumiamo che  $\varphi + \eta$  sia aggiunto. Per definizione di equivalenza lineare esistono divisori aggiunti  $\xi, \zeta$  tali che

$$\varphi + \eta + \xi = \psi + \eta + \zeta$$

e quindi  $\psi + \eta = \varphi + \eta + \xi - \zeta$  è la differenza di due divisori aggiunti, diciamo  $\psi + \eta = E|_C - D|_C$ . Essendo  $\psi + \eta$  effettivo si ha  $\nu_p(C, E) \geq \nu_p(C, D)$  per ogni  $p \in C$  e, per il teorema di  $Af + B\phi$  di Max Noether, segue che  $\psi + \eta$  è aggiunto.  $\square$

**Corollario 6.5.3.** *Siano  $\varphi$  e  $\psi$  divisori effettivi linearmente equivalenti su una curva piana liscia  $C$ . Allora  $\psi$  è aggiunto se e solo se  $\varphi$  è aggiunto.*

*Dimostrazione.* È sufficiente mettere  $\eta = 0$  nel Teorema 6.5.2.  $\square$

Nella Sezione 6.4 abbiamo introdotto il gruppo delle classi di una curva piana liscia e definito una applicazione  $\mu: C \rightarrow \text{Cl}^0(C)$ . Più in generale, per ogni  $s > 0$  possiamo definire un'applicazione

$$\mu_s: C^s \rightarrow \text{Cl}^0(C), \quad \mu_s(p_1, \dots, p_s) = p_1 + \dots + p_s - so.$$

Una differente scelta del “punto base”  $o \in C$  fornisce una nuova applicazione  $\mu_s$  che differisce dalla precedente per una traslazione in  $\text{Cl}^0(C)$ .

**Definizione 6.5.4 (Weierstrass).** *Si dice **genere** della curva  $C$  il più piccolo intero positivo  $g$  tale che  $\mu_g: C^g \rightarrow \text{Cl}^0(C)$  è surgettiva.<sup>3</sup>*

Naturalmente la definizione precedente non dipende dalla scelta del punto  $o \in C$  e ha senso solamente dopo aver provato che  $\mu_s$  è surgettiva per  $s \gg 0$ .

**Teorema 6.5.5.** *Il genere di una curva piana e liscia di grado  $n > 0$  è uguale a  $\frac{1}{2}(n-1)(n-2)$ .*

*Dimostrazione.* Abbiamo già osservato che se  $C$  è una retta o una conica liscia allora  $\text{Cl}^0(C) = 0$  e quindi il genere di  $C$  è uguale a 0. Assumiamo quindi che  $C$  sia una curva liscia fissata di grado  $n \geq 3$  e consideriamo il numero intero  $g = \frac{1}{2}(n-1)(n-2)$ . La dimostrazione è divisa in due passi: nel primo si prova che  $\mu_g$  è surgettiva, nel secondo che  $\mu_{g-1}$  non è surgettiva.

Per ogni  $m > 0$  fissato sia  $P_m \subset \text{Div}(C)$  l'insieme dei divisori aggiunti di grado  $nm$ . Esiste una struttura naturale di spazio proiettivo su  $P_m$ . Infatti detto  $S_d \subset \mathbb{K}[x_0, x_1, x_2]$  il sottospazio vettoriale dei polinomi omogenei di grado  $d$  e  $F \in S_n$  l'equazione di  $C$  esiste una bigezione naturale  $\alpha: \mathbb{P}(S_m/FS_{m-n}) \rightarrow P_m$ . Per ogni  $G \in S_m - FS_{m-n}$  si pone  $\alpha([G]) = D|_C$  dove  $D$  è la curva di equazione  $G$ . In base al Teorema 6.5.1 l'applicazione  $\alpha$  è ben definita e bigettiva. Se  $m \geq n$  la dimensione di  $P_m$  si calcola facilmente ed è uguale a

<sup>3</sup> È sicuramente più nota al grande pubblico la definizione di Riemann del genere di una curva come “numero di manici”  $= 1 - \frac{e}{2}$ , dove  $e$  indica la caratteristica di Eulero-Poincaré. Le due definizioni sono apparentemente indipendenti (non a caso Riemann chiamava il suo invariante *Klassenzahl*, mentre Weierstrass lo chiamava *Rang*) e rimandiamo all'Esercizio 6.25 per il calcolo del “Klassenzahl” delle curve piane non singolari. Il nome genere è stato introdotto da Clebsch.

$$\frac{1}{2}m(m+3) - \frac{1}{2}(m-n)(m-n+3) - 1 = mn - g.$$

Da questo semplice conto di dimensioni si ha che per ogni  $m \geq n$  valgono le seguenti due proprietà:

1. Dato comunque un divisore effettivo  $\varphi$  su  $C$  di grado  $nm - g$ , esiste una curva  $D$  di grado  $m$  tale che  $D|_C \geq \varphi$ .
2. Dato un punto  $o \in C$ , esistono  $nm - g$  punti  $p_i$  su  $C$  tali che ogni curva  $D$  di grado  $m$  che contiene  $o, p_1, \dots, p_{nm-g}$  contiene anche  $C$  come componente. Basta infatti prendere  $p_i$  che inducono condizioni indipendenti sull'iperpiano di  $P_m$  formato dai divisori che contengono  $o$ .

Adesso dobbiamo dimostrare che ogni divisore di grado 0 è linearmente equivalente ad un divisore del tipo  $\varphi - go$  con  $\varphi$  divisore effettivo di grado  $g$ . Sia  $\psi = \psi_0 - \psi_\infty$  con  $\psi_0, \psi_\infty$  divisori effettivi dello stesso grado. Esiste allora una curva  $D$  di grado  $m$  sufficientemente elevato tale che  $D|_C = \psi_0 + go + \eta$  con  $\eta$  divisore effettivo, per il punto 1 esiste una curva  $E$  di grado  $m$  tale che  $E|_C = \eta + \psi_\infty + \varphi$  con  $\varphi$  divisore effettivo di grado  $g$ . Dato che  $\psi + E|_C = \varphi - go + D|_C$  si ha che  $\psi \sim \varphi - go$ .

Proviamo adesso che  $\mu_{g-1}$  non è surgettiva. Sia  $m \geq n$  un intero fissato e siano  $p_1, \dots, p_{nm-g} \in C$  punti distinti come al punto 2), esiste allora un divisore effettivo  $\varphi$  di grado  $g$  tale che  $\varphi + \sum p_i \in P_m$ . Proviamo che  $\varphi - go$  non appartiene all'immagine di  $\mu_{g-1}$ ; infatti se così non fosse avremo un divisore effettivo  $\psi$  di grado  $g-1$  tale che  $\varphi - go \sim \psi - (g-1)o$  da cui  $\psi + o + \sum p_i \sim \varphi + \sum p_i = D|_C$  e, per il Corollario 6.5.3, esisterebbe una curva  $E$  tale che  $E|_C = \psi + o + \sum p_i$  in aperta e dichiarata contraddizione con la scelta dei punti  $p_i$ .  $\square$

### Esercizi

**6.19.** Provare che il teorema del resto implica il teorema  $Af + B\phi$  di Max Noether nel caso di  $C$  curva liscia.

**6.20.** Dimostrare che i tangenziali dei  $3m$  punti di intersezione di una curva di grado  $m$  con una cubica liscia  $C$  appartengono ad una curva di grado  $m$ .

**6.21.** (caratteristica 0) Siano  $C$  curva irriducibile di grado  $n \geq 2$ ,  $p \in \mathbb{P}^2$ , e  $q \in C \cap C_p$  un punto liscio di  $C$  distinto da  $p$ . Provare che  $\nu_q(C, C_p) = \nu_q(\mathbb{T}_q C, C_p) = \nu_q(\mathbb{T}_q C, C) - 1$ .

**6.22.** (caratteristica 0) Sia  $C$  una curva liscia di grado  $n$ , fissiamo un punto  $p \notin C$  e siano  $L_1, \dots, L_r$  le rette passanti per  $p$  tangenti a  $C$ . Denotiamo con  $a_i$  la molteplicità di  $L_i$  come componente della curva risultante di  $C$  e  $C_p$  per la proiezione di centro  $p$ . Per la formula della classe vale  $\sum a_i = n(n-1)$ . Provare che  $L_i$  interseca  $C$  in esattamente  $n - a_i$  punti distinti e che quindi  $L_1 + \dots + L_r$  interseca  $C$  in esattamente  $n(r - n + 1)$  punti distinti (Sugg.: Esercizio 6.21).

**6.23 (Teorema di Cayley, 1843).** Siano  $q_1, \dots, q_{nm}$  punti distinti di intersezione di due curve irriducibili di gradi  $n, m$ . Se  $0 < p \leq \min(n, m)$ , provare che il passaggio per  $q_1, \dots, q_{nm}$  induce

$$mn - \frac{(p-1)(p-2)}{2}$$

condizioni lineari sulle curve di grado  $n + m - p$ .

*Osservazione 6.5.6.* La dimostrazione corretta del risultato del precedente esercizio richiede il teorema  $Af + B\phi$  datato 1872: tale teorema fu assunto da Cayley come fatto evidente e senza alcun commento, vedi [EGH1996]. È invece facile rendersi conto che la dimostrazione presentata in [Cre1862, pag. 38] non è corretta. Il teorema di Cayley è stato generalizzato da Bacharach nel 1886 (vedi Esercizio 6.24 per una versione debole).

**6.24 (Teorema di Cayley-Bacharach, 1886).** Ecco una interessante applicazione del teorema del resto di Brill e Noether. Siano  $C, D$  curve piane lisce di gradi  $n, m$  che si interscano trasversalmente, cioè in  $nm$  punti distinti, e sia  $0 \leq l < \min(n, m)$  un intero. Per Bézout non esiste alcuna curva di grado  $l$  contenente  $C \cap D$  ed è quindi possibile trovare un sottoinsieme  $A \subset C \cap D$  di cardinalità  $\frac{1}{2}(l+1)(l+2) = \frac{1}{2}l(l+3) + 1$  che non è contenuto in alcuna curva di grado  $l$ ; sia  $B \subset C \cap D$  il complementare di  $A$ . Dimostrare che ogni curva di grado  $n+m-l-3$  che contiene  $B$  contiene anche  $A$ . (Sugg.: si assuma  $n \geq m$  per fissare le idee, sia  $H$  una curva fissata di grado  $n+m-l-3$  che contiene  $B$  e sia  $p \in A$ ; bisogna dimostrare che  $p \in H$ . Si prenda  $L$  una retta generica per  $p$  e sia  $E$  l'unica curva di grado  $l$  contenente  $A-p$ . Possiamo scrivere  $H|_D = B + \eta$ ,  $(E+L)|_D = A + \mu$  con  $\eta, \mu$  divisori effettivi su  $D$ . Per il teorema del resto 6.5.2 esiste una curva  $F$  di grado  $m-2$  tale che  $F|_D = \mu + \eta$ . Provare che  $L$  è una componente di  $F$  e quindi che  $p \in \eta$ )

**6.25.** (In questo esercizio sono richieste nozioni di topologia algebrica e di teoria dei rivestimenti).

Se  $\mathbb{K} = \mathbb{C}$  usare l'Esercizio 6.22 per dimostrare che la caratteristica di Eulero-Poincaré topologica  $e$  di una curva liscia  $C$  di grado  $n$  è uguale a  $3n - n^2 = 2 - 2g(C)$ . (Sugg.: se  $A \subset C$  è un insieme finito di  $a$  punti si ha  $e(C-A) = e(C) - a$ , si consideri la restrizione a  $C$  della proiezione di centro  $p \notin C$  su di una retta  $\mathbb{P}^1 \subset \mathbb{P}^2 - \{p\}$ .)

## 6.6 Esercizi complementari

### Esercizi sulle Coniche

Salvo avviso contrario, in tutti gli esercizi di questa sottosezione si assume il campo base di **caratteristica diversa da 2**.

**6.26 (La *propriété merveilleuse* di Pascal, 1640).**

1) Sia  $\mathbb{K}$  un campo algebricamente chiuso di caratteristica  $\neq 2$  e siano  $f, g \in \mathbb{K}[x_0, x_1]$  polinomi omogenei di grado 2 senza fattori comuni. Dimostrare che esiste una involuzione non banale  $\sigma: \mathbb{P}^1 \rightarrow \mathbb{P}^1$  che scambia le radici del polinomio  $af + bg$ , per ogni scelta di  $a, b \in \mathbb{K}$  non entrambi nulli.

2) Sia  $p_1, p_2, p_3, p_4 \in \mathbb{P}^2$  un sistema di riferimento e sia  $L \subset \mathbb{P}^2$  una retta non contenente alcuno dei punti  $p_i$ . Dimostrare che esiste una involuzione non banale  $\sigma: L \rightarrow L$  che scambia i punti di intersezione di  $L$  con ogni conica passante per  $p_1, p_2, p_3, p_4$ .

**6.27.** Siano  $C$  conica liscia,  $p \notin C$  e  $C_p$  la polare di  $p$  rispetto a  $C$ . Provare che per ogni retta  $L \subset \mathbb{P}^2$  passante per  $p$  e trasversale a  $C$  i quattro punti  $\{p, C \cap L, C_p \cap L\}$  formano una quaterna armonica.

**6.28.** Sia  $S^1 \subset \mathbb{C}$  l'insieme dei numeri complessi di norma 1. Dati quattro punti distinti di  $S^1$  ha senso definire due tipi di birapporto:

- Il birapporto complesso - pensando  $S^1$  come un sottoinsieme di  $\mathbb{P}_{\mathbb{C}}^1$ .
- Il birapporto di Steiner - pensando  $S^1$  come una conica liscia di  $\mathbb{P}_{\mathbb{R}}^2$ .

Provare che i due birapporti coincidono.

**6.29.** (caratteristica  $\neq 2$ ) Sia  $C \subset \mathbb{P}^2$  una conica liscia e  $p \notin C$ . Si consideri l'applicazione  $\phi_p: C \rightarrow C$  che manda il punto  $q$  nel rimanente punto di intersezione di  $C$  con la retta  $\overline{pq}$ . Provare che  $\phi$  è una proiezione di  $C$  in sé. (Sugg.: considerare coordinate omogenee tali che  $p = [1, 0, 0]$  e la polare  $C_p$  sia la retta  $x_0 = 0$ ).

**6.30 (Punto di Frégier, 1816).** Sia  $C \subset \mathbb{R}^2$  un'ellisse e  $p \in C$  un punto fissato. Provare che tutte le corde di  $C$  che vedono un angolo retto in  $p$  passano per uno stesso punto  $q$ , situato sulla normale a  $C$  in  $p$  ed interno alla conica. (Sugg.: sia  $q$  il punto di intersezione di due tali corde e sia  $\phi_q$  l'involuzione definita all'Esercizio 6.29. Provare che  $\phi_q$  induce sul fascio delle rette per  $p$  l'involuzione degli angoli retti, vedi Esercizio 2.56).

**6.31 (Problema di Staudt, 1831).** Date due coniche lisce distinte, determinare il luogo dei punti  $p$  tali che le quattro rette del fascio per  $p$  e tangenti alle coniche date, formano una quaterna armonica.

**6.32.** Determinare per quali valori di  $a \in \mathbb{C}$ , la conica nel piano affine complesso  $\mathbb{C}^2$  di equazione

$$(ia - 1)(x^2 + y^2 + 1) + 2(a - i)xy, \quad i = \sqrt{-1},$$

contiene infiniti punti a coordinate reali. (Sugg.: per una soluzione elegante dell'esercizio suggeriamo l'uso dei ben noti isomorfismi conformi tra il disco unitario di  $\mathbb{C}$  ed il semipiano superiore.)

**6.33.** Siano  $C, D \subset \mathbb{R}^2$  due cerchi che si intersecano in due punti distinti  $p, q$  e siano  $c \in C$  e  $d \in D$  punti fissati. Per ogni retta  $L$  passante per  $c$  denotiamo con  $l \in C$  il secondo punto di intersezione di  $C$  e  $L$ , con  $l'$  il secondo punto di intersezione di  $D$  e  $\overline{pl}$  e con  $l''$  il punto di intersezione di  $L$  e  $\overline{dl'}$ . Provare che, al variare della retta  $L$  tra quelle passanti per  $c$ , il luogo dei punti  $l''$  è il cerchio passante per  $c, d, q$ .

Convincersi inoltre che questo risultato è sostanzialmente equivalente al teorema di Miquel, Esercizio 5.60. (Sugg.: utilizzare la generazione proiettiva delle coniche per dimostrare che tale luogo è una conica passante per  $c, d$  e per i punti di intersezione di  $C, D$  diversi da  $p$ .)

**6.34.** Siano  $p_1, p_2, p_3 \in \mathbb{R}^2$  punti non allineati,  $L_1, L_2$  le bisettrici degli angoli in  $p_3$  formati dalle rette  $\overline{p_1p_3}$  e  $\overline{p_2p_3}$ ,  $a = L_1 \cap \overline{p_1p_2}$ ,  $b = L_2 \cap \overline{p_1p_2}$ ,  $C_1$  la circonferenza passante per  $p_1, p_2, p_3$ ,  $C_2$  la circonferenza passante per  $a, b, p_3$  e  $p_4 \neq p_3$  il secondo punto di intersezione di  $C_1$  e  $C_2$ . Provare che  $p_1, p_2, p_3, p_4$  è una quaterna armonica della conica liscia  $C_1$ . (Sugg.: siano  $s \in C_1 \cap L_1$ ,  $t = C_1 \cap L_2$ ,  $s, t \neq p_3$ , provare che  $\overline{ab}$  è un diametro di  $C_2$  e che  $\overline{st}$  è un diametro di  $C_1$ . Detti  $c \in C_1 \cap \overline{at}$ ,  $d \in C_1 \cap \overline{bs}$  i rimanenti punti di intersezione, provare che

$$[p_1, p_2; a, b] = [p_1, p_2; c, p_3] = [p_1, p_2; p_3, d] = -1$$

e dedurre che  $c = d = p_4$ .)

### Esercizi sulle corrispondenze

**6.35.** Sia  $C$  una corrispondenza simmetrica di tipo  $(a, a)$ . Dimostrare che  $C^2 = C \circ C$  contiene la diagonale  $\Delta$  con molteplicità  $\geq a$ .

**6.36.** Sia  $C(r, d) = \{(x, y) \in \mathbb{R}^2 \mid (x - d)^2 + y^2 = r^2\}$ . Descrivere le coppie  $(d, r)$  per le quali esiste un triangolo inscritto a  $C(1, 0)$  e circoscritto a  $C(r, d)$ .

**6.37 (Dimostrazione di Dandelin (1826) del teorema di Pascal 5.4.3).** Premettiamo alcune semplici osservazioni:

a) Dato un piano  $\Pi \subset \mathbb{P}^3$  e tre punti distinti  $p, q, r \in \mathbb{P}^3 - \Pi$ , allora i punti di intersezione di  $\Pi$  con i lati del triangolo di vertici  $p, q, r$  sono allineati.

b) Siano  $\mathbb{P}^1, \mathbb{P}^1$  e  $\mathbb{P}^3$  spazi proiettivi dotati dei sistemi di coordinate omogenee  $x_0, x_1; y_0, y_1; u_{00}, u_{01}, u_{10}, u_{11}$  e si consideri la mappa di Segre (vedi Definizione 10.4.3)

$$s: \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^3, \quad s([x_0, x_1], [y_0, y_1]) = [x_0y_0, x_0y_1, x_1y_0, x_1y_1].$$

Si osservi che  $s$  induce una bigezione tra  $\mathbb{P}^1 \times \mathbb{P}^1$  e la quadrica  $Q$  di equazione  $u_{00}u_{11} = u_{10}u_{01}$ . Tale bigezione identifica la diagonale  $\Delta$  con la conica liscia  $C$  ottenuta per intersezione di  $Q$  con il piano  $H = \{u_{10} - u_{01} = 0\}$ .

c) Sostituendo  $x_i y_j$  al posto di  $u_{ij}$  nell'equazione di un piano di  $\mathbb{P}^3$  si ottiene l'equazione di una corrispondenza di tipo  $(1, 1)$  su  $\mathbb{P}^1 \times \mathbb{P}^1$  ed esiste una bigezione naturale tra  $(\mathbb{P}^3)^\vee$  e lo spazio di tutte le corrispondenze di tipo  $(1, 1)$ .

Siano  $p_1, \dots, p_6$  punti distinti sulla conica  $C$  e siano  $q_1, \dots, q_6 \in \mathbb{P}^1$  tali che  $s^{-1}(p_i) = (q_i, q_i)$  per ogni  $i$ . Denotiamo  $a = s(q_1, q_4)$ ,  $b = s(q_3, q_6)$  e  $c = s(q_5, q_2)$ . Dimostrare che

$$\begin{cases} \overline{ab} \cap H = \overline{p_3 p_4} \cap \overline{p_6 p_1} \\ \overline{ac} \cap H = \overline{p_4 p_5} \cap \overline{p_1 p_2} \\ \overline{bc} \cap H = \overline{p_2 p_3} \cap \overline{p_5 p_6} \end{cases}$$

e dedurre il Teorema di Pascal. (Sugg.: ragionare in termini di corrispondenze per provare che  $c$  appartiene al piano  $\langle a, p_1, p_2 \rangle$  e che  $a$  appartiene al piano  $\langle c, p_4, p_5 \rangle$ .)

**6.38.** Trovare l'errore nell'argomentazione del seguente sofisma. *Esiste una corrispondenza  $\emptyset \neq C \subset \mathbb{P}^1 \times \mathbb{P}^1$  che non interseca la diagonale.* Infatti, siano  $p_1, p_2 \in \mathbb{P}^1$  punti distinti e sia  $C$  l'insieme delle coppie  $(p_3, p_4) \in \mathbb{P}^1 \times \mathbb{P}^1$  tali che  $[p_1, p_2; p_3, p_4] = -1$  (quaterna armonica). Tale insieme è chiaramente non vuoto ed è definito da una equazione algebrica, dunque  $C$  è una corrispondenza. Poiché il birapporto di quattro punti due dei quali coincidenti non può essere uguale a  $-1$ , il sofisma è provato.

### Esercizi sulle cubiche

Salvo avviso contrario, in tutti gli esercizi di questa sottosezione si assume il campo base di **caratteristica diversa da 2 e da 3**.

**6.39 (Steiner, 1846).** Sia  $C$  una cubica piana liscia, un punto  $p \in C$  si dice **sestatico** se esiste una conica ridotta  $Q$  tale che  $\nu_p(C, Q) = 6$ . Provare che se  $p$  è un flesso e  $C \cap C_p = \{p, p, p, q_1, q_2, q_3\}$ , allora i punti  $q_i$  sono sestatici. Viceversa, dimostrare che ogni punto sestatico si ottiene in questo modo e quindi  $C$  ha esattamente 27 punti sestatici distinti. (Sugg.: se  $q$  è sestatico e  $Q$  è una conica tale che  $\nu_q(C, Q) = 6$ , provare che  $Q$  è liscia in  $q$  e considerare il sistema lineare generato da  $C$  e da  $3\mathbb{T}_q C$ .)

**6.40.** Nelle notazioni della dimostrazione del Teorema 6.3.6, se  $s = r$  è un flesso e  $C_r = \mathbb{T}_r C + L$ , provare che  $\phi$  è indotta dalla proiezione di centro  $L \in (\mathbb{P}^2)^\vee$ .

**6.41 (Poncelet, 1832).** Sia  $C$  cubica piana liscia; dimostrare che un punto  $p \in C$  è un flesso se e solo se le tre coppie di punti di  $C$  segate da tre rette trasversali passanti per  $p$  appartengono ad una conica.

**6.42 (Hesse, 1844).** Provare che nove punti del piano, tali che la retta che ne congiunge due ne contiene un terzo (ma non un quarto), appartengono ad un fascio di cubiche di cui sono i flessi. (Sugg.: Esercizio 6.41).

**6.43 (Polare armonica del flesso).** Sia  $C$  cubica liscia e  $p \in C$  un flesso. Per ogni retta  $L$  passante per  $p$  e trasversa a  $C$  siano  $q, r$  i rimanenti punti di intersezione e sia  $o \in L$  il quarto armonico,  $[p, o; q, r] = -1$ . Provare che al variare di  $L$ , i punti  $o$  sono contenuti in una retta  $R$ .

**6.44.** Date due cubiche lisce, provare che esiste una proiettività di  $\mathbb{P}^2$  che manda i flessi dell'una nei flessi dell'altra. (Sugg.: determinare i flessi della cubica di equazione  $x_0^3 + x_1^3 + x_2^3 + mx_0 x_1 x_2 = 0$ .)

**6.45.** Mostrare che ogni cubica liscia è l'Hessiana (Esercizio 6.17) di un'altra cubica liscia.

**6.46 (\*)**. Sia  $C$  una cubica liscia fissata e denotiamo con  $G$  il gruppo delle proiettività  $\phi$  di  $\mathbb{P}^2$  tali che  $\phi(C) = C$ . Dimostrare che:

1.  $G$  è finito (se  $\phi(C) = C$ , allora  $\phi$  manda flessi in flessi).
2.  $G$  agisce transitivamente sull'insieme dei nove flessi di  $C$ .
3. Fissato un flesso  $p \in C$  sia  $G_p \subset G$  lo stabilizzatore di  $p$  e  $H_p \subset G_p$  lo stabilizzatore della quaterna di Salmon di  $(C, p)$ . Allora  $H_p = \mathbb{Z}/2$ .
4. La cardinalità di  $G$  è uguale a:
  - a) 54 se la quaterna di Salmon è equianarmonica.
  - b) 36 se la quaterna di Salmon è armonica.
  - c) 18 in tutti gli altri casi.
5. Se  $|G| = 18$ , allora ogni elemento di  $G$  è prodotto di al più due involuzioni.
6. Esiste una bigezione tra l'insieme dei flessi ed il gruppo  $T = \mathbb{Z}/3 \times \mathbb{Z}/3$  tale che tre flessi risultano allineati se e solo se la somma dei corrispondenti elementi di  $T$  è uguale a 0.
7. Esiste un sottogruppo normale di  $G$  isomorfo a  $T$ .
8. Esplicitare  $G$  in un sistema di coordinate omogenee nelle quali  $C$  ha equazione  $x^3 + y^3 + z^3 + mxyz = 0$ .
9. L'inclusione  $G \hookrightarrow \text{PGL}(3, \mathbb{K})$  non si solleva ad una inclusione  $G \hookrightarrow \text{GL}(3, \mathbb{K})$ .

**6.47.** Sia  $F(x_0, x_1, x_2)$  l'equazione di una cubica liscia e sia  $S \subset \mathbb{P}^3$  l'insieme dei punti  $[x_0, \dots, x_3]$  tali che  $x_3^3 = F(x_0, x_1, x_2)$ . Provare che  $S$  contiene esattamente 27 rette distinte e che ogni retta ne interseca altre 10 (Sugg.:  $27 = 9 \times 3$ ;  $10 = (9 - 1) + (3 - 1)$ ).

**6.48 (Steiner, 1853)**. Sia  $C$  una cubica liscia e  $p \in \mathbb{P}^2$ . Provare che se la conica polare  $C_p$  è singolare in  $q$ , allora  $C_q$  è singolare in  $p$ .

**6.49 (Le Poloconiche)**. Sia  $C$  una cubica liscia e  $L$  una retta. Per ogni  $p \in L$  sia  $C_{pp} = (C_p)_p$  la polare doppia di  $p$  rispetto a  $C$ . Provare che le rette  $C_{pp}$ , per  $p \in L$ , sono tutte tangenti ad una conica  $Q$  detta **Poloconica** di  $L$ .

**6.50.** Due cubiche lisce si dicono **sizigetiche** se hanno in comune i nove flessi. Provare che nel fascio generato da due cubiche sizigetiche vi sono quattro cubiche singolari, ognuna delle quali è unione di tre rette.

**6.51.** Sia  $B$  la corrispondenza costruita nella dimostrazione del teorema di Salmon. Usare la legge di gruppo della cubica per provare che  $B = 2\phi$ .

**6.52.** Data una cubica  $C$  ed una retta  $L$ , la retta  $L'$  che contiene i tangenziali dei punti di intersezione di  $C$  con  $L$  si dice **retta satellite** di  $L$ .

Sia  $L$  una retta che interseca  $C$  in tre punti distinti nessuno dei quali sia un flesso. Provare che  $L$  è satellite di 16 rette distinte concorrenti a gruppi di 4 in 12 punti. Inoltre ognuna delle 16 rette contiene esattamente 3 dei suddetti punti.

**6.53.** Forse il modo più semplice per dimostrare che le quaterne di Salmon di una cubica liscia  $C$  sono tutte proiettivamente equivalenti è quello di usare la forza bruta e dimostrare che l'invariante  $j$  è costante. Per facilitare il conto, se  $p, q \in C$ , non è restrittivo supporre  $\overline{pq}$  trasversale a  $C$  e si può prendere un sistema di coordinate omogenee tali che  $p = [1, 0, 0]$ ,  $q = [0, 1, 0]$ ,  $\mathbb{T}_p C \cap \mathbb{T}_q C = [0, 0, 1]$  e  $C$  è definita dall'equazione

$$x_2^3 + x_2^2(x_0 + x_1) + x_0x_1(ax_0 + bx_1 + cx_2) = 0.$$

**6.54.** Sia  $C$  una cubica liscia e  $p, q \in C$  due punti distinti. Provare che esistono 4 coniche, ognuna delle quali è tangente a  $C$  nei punti  $p, q$  ed in un terzo punto  $r$ .



**Esercizi sulle curve di grado superiore**

**6.55.** Sia  $\mathbb{K}$  algebricamente chiuso di caratteristica 3; mostrare che ogni punto della quartica piana di equazione  $x^3y + y^3z + z^3x = 0$  è non singolare ed è un flesso.

**6.56.** Provare:

1. Nelle notazioni del Lemma 6.4.3, se esiste  $\psi \in \mathbb{K}[w_0, w_1, w_2]$  tale che  $\psi(F, G, H) = 0$ , allora  $J(C, D, E)$  è indeterminata.
2. (\*\*?) In caratteristica 0 vale anche il viceversa del punto 1. (Suggerimento per gli esperti:  $F, G, H$  definiscono un'applicazione razionale da  $\mathbb{P}^2$  in uno spazio proiettivo pesato).

**6.57** (\*\*?). Nelle notazioni di 6.4.3, se la Steineriana non è indeterminata, allora è una curva piana di grado  $(n-1)(m-1) + (m-1)(l-1) + (l-1)(n-1)$ .

**6.58** (\*\*?). Se la Steineriana  $S(C, D, E)$  è determinata, mentre la Jacobiana  $J(C, D, E)$  è indeterminata, provare che esistono infiniti punti  $q$  tali che  $C_q, D_q, E_q$  hanno una componente comune.

**6.59** (\*). (caratteristica 0) Se tre curve piane  $C, D, E$  hanno lo stesso grado, provare che la Steineriana è indeterminata se e solo se esiste  $p \in \mathbb{P}^2$  che è singolare per  $C, D$  ed  $E$ . (Sugg.: Teorema di Bertini 5.6.1.)

**Esercizi sul teorema di Riemann**

Enunceremo, dimostreremo e daremo qualche applicazione del teorema di Riemann per curve piane lisce. Nel Capitolo 16 estenderemo il risultato sia in termini di enunciato (contributo di Roch, allievo di Riemann) sia in termini di applicabilità (la classe di tutte le curve lisce proiettive).

**6.60.** Sia  $C$  una curva piana liscia di grado  $n \geq 3$  e sia  $g = (n-1)(n-2)/2$  il suo genere. Dato un divisore effettivo  $\varphi$  su  $C$  scegliamo un altro divisore effettivo  $\eta$  tale che  $\varphi + \eta$  sia aggiunto di grado  $mn$ , con  $m \geq n$ . Per il teorema del resto, l'insieme  $|\varphi|$  dei divisori effettivi linearmente equivalenti a  $\varphi$  è in bigezione naturale con l'insieme dei divisori aggiunti di grado  $mn$  maggiore o uguali a  $\eta$  ed è quindi uno spazio proiettivo di dimensione finita. Dimostrare che:

1. La struttura proiettiva su  $|\varphi|$  non dipende dalla scelta di  $\eta$ . In particolare la dimensione  $\dim |\varphi|$  è ben definita.
2. (Disuguaglianza di Riemann) Per ogni divisore effettivo  $\varphi$  vale

$$\deg(\varphi) \geq \dim |\varphi| \geq \deg(\varphi) - g.$$

3. (Teorema di Riemann<sup>4</sup>, 1857)

Se  $\deg(\varphi) \geq 2g - 1$ , allora vale  $\dim |\varphi| = \deg(\varphi) - g$

(Sugg.: [1] teorema del resto. [2] se  $\xi$  è un divisore effettivo, provare che l'insieme dei divisori effettivi linearmente equivalenti a  $\varphi$  che contengono  $\xi$  è un sottospazio proiettivo di  $|\varphi|$ . Per [3] si ha  $\dim |\varphi + \eta| = nm - g$  (vedi dimostrazione di 6.5.5), se  $\alpha$  è un divisore generico di grado  $nm - g + 1$  si ha che  $\alpha - \eta$  ha grado  $\deg(\varphi) - g + 1 \geq g$  ed è quindi linearmente equivalente ad un divisore effettivo  $\psi$  tale che  $|\varphi - \psi| = \emptyset$ .)

<sup>4</sup> A rigore, il vero teorema di Riemann è leggermente più forte di questo: rimandiamo al Corollario 16.2.1 per la versione filologicamente corretta.

**6.61 (\*)**. La definizione originale di Weierstrass del genere di una curva liscia è, rispetto alla Definizione 6.5.4, diversa nella forma ma equivalente nella sostanza (vedi [EC1915] Libro V, p. 141-148). Per Weierstrass, il genere di una curva  $C$  è più piccolo intero  $p$  tale che, per ogni divisore effettivo  $\varphi$  di grado  $p + 1$ , l'insieme  $|\varphi|$  dei divisori effettivi linearmente equivalenti a  $\varphi$  è uno spazio proiettivo di dimensione positiva. Dimostrare l'equivalenza tra la Definizione 6.5.4 e la definizione originale di Weierstrass. (Sugg.: utilizzare il teorema di Riemann (Esercizio 6.60) per dimostrare che la definizione di Weierstrass ha senso dopodiché, per  $p$  definito come sopra, provare la disuguaglianza di Riemann  $\dim |\varphi| \geq \deg(\varphi) - p$ ).

**6.62 (Zariski [Zar1962, pp. 562-563], \*)**. Sia  $C \subset \mathbb{P}^2$  una cubica liscia di equazione  $F$  e siano  $p_1, \dots, p_{12} \in C$  dodici punti distinti. Si assuma per ipotesi che per ogni  $n > 0$  il divisore (di grado  $12n$ )  $np_1 + np_2 + \dots + np_{12}$  non sia aggiunto<sup>5</sup>. Per ogni coppia di numeri naturali  $a, b$  denotiamo con  $V_{a,b} \subset \mathbb{K}[x_0, x_1, x_2]$  il sottospazio vettoriale dei polinomi omogenei di grado  $a + 3b$  che si annullano con molteplicità  $\geq b$  su ciascuno dei dodici punti  $p_i$ .

Dimostrare che la sottoalgebra  $V = \bigoplus_n V_{n,n} \subset \mathbb{K}[x_0, x_1, x_2]$  non è finitamente generata. (Sugg.: svolgere nell'ordine:

1. Se  $a \leq b$  allora ogni elemento di  $V_{a,b}$  si annulla su  $C$ .
2.  $\dim V_{a,b} \geq \dim V_{a+3b,0} - 6b(b+1)$ .
3. Usare induzione su  $b$  e l'applicazione  $V_{a,b} \rightarrow V_{a,b+1}$  indotta dalla moltiplicazione per  $F$ , per dimostrare che se  $b < a$ , allora vale  $\dim V_{a,b} \leq \dim V_{a+3b,0} - 6b(b+1)$ .
4. Il generico polinomio di  $V_{n,n-1}$  non si annulla in  $C$ .
5. Dedurre da 1) e 4) che  $V$  non può essere finitamente generata come  $\mathbb{K}$ -algebra.)

---

<sup>5</sup> Sul campo dei numeri complessi, tale assunto è verificato per ogni scelta generica dei dodici punti.

## Aspetti algebrici delle serie di potenze

### 7.1 Serie di potenze

Sia  $\mathbb{K}$  un campo, una **norma** su  $\mathbb{K}$  è un'applicazione  $|\cdot|: \mathbb{K} \rightarrow \mathbb{R}$  che soddisfa le seguenti proprietà:

1.  $|a| \geq 0$  per ogni  $a \in \mathbb{K}$ .
2.  $|a| = 0$  se e solo se  $a = 0$ .
3.  $|a + b| \leq |a| + |b|$  per ogni  $a, b \in \mathbb{K}$  (disuguaglianza triangolare).
4.  $|ab| = |a||b|$  per ogni  $a, b \in \mathbb{K}$ .

Si noti che  $|1| = |-1| = 1$ . Ogni norma induce una struttura di spazio metrico con distanza  $d(a, b) = |a - b|$ ; il campo normato  $(\mathbb{K}, |\cdot|)$  si dice completo se lo spazio metrico  $(\mathbb{K}, d)$  è completo.

*Esempio 7.1.1.* Se  $\mathbb{K}$  è un sottocampo di  $\mathbb{C}$ , allora il valore assoluto usuale induce una norma su  $\mathbb{K}$ . Tale norma viene talvolta indicata con  $|\cdot|_\infty$ .

*Esempio 7.1.2.* Sia  $\mathbb{K}$  un campo qualsiasi, la funzione  $|0| = 0$ ,  $|a| = 1$  per ogni  $a \neq 0$ , è una norma che induce la topologia discreta.

*Esempio 7.1.3.* Sia  $\mathbb{K} = \mathbb{Q}$  e sia  $p$  un numero primo. La norma  $p$ -adica  $|\cdot|_p: \mathbb{Q} \rightarrow \mathbb{R}$  si definisce nel modo seguente: se  $a = p^r \frac{b}{c}$  con  $b, c, r \in \mathbb{Z}$  e  $b, c$  non divisibili per  $p$ , si pone  $|a|_p = p^{-r}$ . Non è arduo dimostrare che si tratta di una norma.

Sia  $n$  un intero positivo fissato, un multiindice  $I = (i_1, \dots, i_n)$  è un elemento di  $\mathbb{N}^n$ ; il grado di  $I$  è per definizione uguale a  $|I| = i_1 + \dots + i_n$ .

Un multiraggio  $r = (r_1, \dots, r_n)$  è una successione finita di numeri reali positivi. Se  $r = (r_1, \dots, r_n)$  è un multiraggio e  $I = (i_1, \dots, i_n)$  un multiindice si pone  $r^I = r_1^{i_1} r_2^{i_2} \dots r_n^{i_n}$ .

Una **serie formale** a coefficienti in  $\mathbb{K}$  nelle indeterminate  $x_1, \dots, x_n$  è una espressione del tipo

$$\phi = \sum_{I \in \mathbb{N}^n} a_I x^I, \quad \text{dove } a_I \in \mathbb{K} \text{ per ogni } I \in \mathbb{N}^n$$

e si conviene che  $x^I = x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ ; ogni serie formale si scrive in modo unico come  $\phi = \sum_{i \geq 0} \phi_i$ , dove  $\phi_i \in \mathbb{K}[x_1, \dots, x_n]$  è un polinomio omogeneo di grado  $i$ . Chiaramente un polinomio può essere pensato come una serie formale in cui i coefficienti sono diversi da 0 per al più un numero finito di multiindici.

**Definizione 7.1.4.** La **molteplicità** di una serie formale  $\phi = \sum_{i \geq 0} \phi_i$  è data da

$$\nu(\phi) = \sup\{n \in \mathbb{N} \mid \phi_i = 0 \text{ per ogni } i < n\} \in \mathbb{N} \cup \{+\infty\}.$$

Si noti che  $\nu(\phi) = +\infty$  se e solo se  $\phi = 0$ ; se  $\phi \neq 0$ , allora  $\nu(\phi)$  è uguale al più piccolo intero  $m \geq 0$  tale che  $\phi_m \neq 0$ .

Con le ben note regole di somma e di prodotto di Cauchy<sup>1</sup> le serie formali formano un anello commutativo denotato con  $\mathbb{K}[[x_1, \dots, x_n]]$ .

Sia ora  $\|\cdot\|$  una norma fissata su  $\mathbb{K}$ , una serie formale  $\phi = \sum a_I x^I$  si dice **convergente** se esiste un multiraggio  $r$  tale che

$$\|\phi\|_r := \sum_I |a_I| r^I < +\infty.$$

Se  $\mathbb{K} = \mathbb{R}, \mathbb{C}$  questa definizione coincide con la classica nozione di serie totalmente convergente. Denotiamo  $\mathbb{K}\{x_1, \dots, x_n\} \subset \mathbb{K}[[x_1, \dots, x_n]]$  il sottoinsieme delle serie convergenti e, per ogni multiraggio  $r = (r_1, \dots, r_n)$  poniamo

$$B_r = \{\phi \in \mathbb{K}\{x_1, \dots, x_n\} \mid \|\phi\|_r < +\infty\}.$$

**Lemma 7.1.5.** *Siano  $\phi, \psi$  serie convergenti e sia  $r$  un multiraggio tale che  $\|\phi\|_r < +\infty$ ,  $\|\psi\|_r < +\infty$ . Allora*

1.  $\|\phi + \psi\|_r \leq \|\phi\|_r + \|\psi\|_r$ .
2.  $\|\phi\psi\|_r \leq \|\phi\|_r \|\psi\|_r$ .

*In particolare, per ogni  $n$  e  $r$ , gli insiemi  $\mathbb{K}\{x_1, \dots, x_n\}$  e  $B_r$  sono sottoanelli di  $\mathbb{K}[[x_1, \dots, x_n]]$*

*Dimostrazione.* 1) è immediato. Se  $\psi$  è un monomio è ovvio che  $\|\phi\psi\|_r = \|\phi\|_r \|\psi\|_r$  e quindi se  $\psi$  è un polinomio il punto 2) segue immediatamente da 1). Dunque se  $\psi = \sum a_I x^I$ , per ogni  $s > 0$  si ha  $\|\phi \sum_{|I| < s} a_I x^I\|_r \leq \|\phi\|_r \|\psi\|_r$  e, passando al limite per  $s \rightarrow +\infty$ , si ottiene la tesi.  $\square$

Per definizione, l'unione di tutti i  $B_r$  è l'anello delle serie convergenti; con la norma  $\|\cdot\|_r$ , il  $\mathbb{K}$ -spazio vettoriale  $B_r$  diventa uno spazio normato.

Un'altra importante conseguenza del Lemma 7.1.5 è la regola di composizione. Se  $f \in \mathbb{K}[[x_1, \dots, x_n]]$  e  $g_1, \dots, g_n \in \mathbb{K}[[y_1, \dots, y_m]]$  hanno molteplicità positiva allora è ben definita la serie composta  $\phi = f(g_1, \dots, g_n) \in \mathbb{K}[[y_1, \dots, y_m]]$ . Ebbene, se  $f, g_1, \dots, g_m$  sono convergenti allora anche  $\phi$  è convergente. Lasciamo la dimostrazione per esercizio al lettore.

*Osservazione 7.1.6.* Se  $\|\cdot\|$  è la norma discreta (Esempio 7.1.2), allora ogni serie formale è convergente; in particolare tutti i risultati validi per l'anello  $\mathbb{K}\{x_1, \dots, x_n\}$  delle serie convergenti rispetto ad una norma qualunque valgono anche per  $\mathbb{K}[[x_1, \dots, x_n]]$ .

L'applicazione  $\phi = \sum a_I x^I \mapsto \phi(0) = a_0$  definisce un omomorfismo surgettivo di anelli  $\mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}$  con nucleo  $\mathfrak{m} = (x_1, \dots, x_n)$ .

**Lemma 7.1.7.** *L'anello  $\mathbb{K}\{x_1, \dots, x_n\}$  è locale con ideale massimale  $\mathfrak{m}$ .*

*Dimostrazione.* Sia  $\phi \in \mathfrak{m}$ , dobbiamo dimostrare che  $1 - \phi$  è invertibile. La serie formale  $\psi = \sum_{i=0}^{+\infty} \phi^i$  è l'inverso di  $1 - \phi$  in  $\mathbb{K}[[x_1, \dots, x_n]]$ , rimane da vedere che  $\psi$  è convergente. Sia  $R$  un multiraggio tale che  $\|\phi\|_R < +\infty$ , siccome  $\phi(0) = 0$ , per ogni scalare positivo  $\delta \leq 1$  si ha  $\|\phi\|_{\delta R} \leq \delta \|\phi\|_R$  e quindi per  $\delta$  sufficientemente piccolo  $r = \delta R$  soddisfa la condizione  $\|\phi\|_r < 1$  e, per il Lemma 7.1.5, vale  $\|\psi\|_r < +\infty$ .  $\square$

<sup>1</sup>

$$\sum a_I x^I + \sum b_I x^I = \sum (a_I + b_I) x^I, \quad \left(\sum a_I x^I\right) \left(\sum b_I x^I\right) = \sum_H \left(\sum_{I+J=H} a_I b_J\right) x^H$$

**Corollario 7.1.8.** *L'anello  $\mathbb{K}\{t\}$  è un dominio ad ideali principali: più precisamente ogni ideale non banale è generato da  $t^n$  per qualche  $n \geq 0$ .*

*Dimostrazione.* Sia  $I \neq 0$  un ideale e sia  $f \in I$  di molteplicità minima  $m$ , siccome  $t^m$  divide ogni  $g \in I$  basta dimostrare che  $t^m \in I$ . Si può scrivere  $f = t^m \phi$  con  $\phi(0) \neq 0$ ; dato che  $\phi$  è invertibile vale  $t^m = f \phi^{-1} \in I$ .  $\square$

### Esercizi

**7.1.** Sia  $\mathbb{K}$  un campo completo di caratteristica 0. Provare che se  $|2| > 1$ , allora  $\mathbb{K}$  è connesso.

**7.2.** Sia  $s$  un intero positivo. Provare che una serie  $\sum a_I x^I$  è convergente se e solo se esiste un numero reale positivo  $R$  tale che  $|a_I| |I|^s \leq R^{|I|}$  per ogni multiindice  $I$ . Dedurre che le derivate parziali formali di una serie convergente sono convergenti.

**7.3.** Sia  $\phi \in \mathbb{K}[[x_1, \dots, x_n]]$  di molteplicità  $m$ ,  $r$  un multiraggio e  $a \in ]0, 1[$ . Provare che  $\|\phi\|_{ar} \leq a^m \|\phi\|_r$ .

**7.4.** Se  $(\mathbb{K}, |\cdot|)$  è un campo completo e  $\phi \in \mathbb{K}\{x_1, \dots, x_n\}$ , allora  $\phi$  definisce, in un intorno di 0 in  $\mathbb{K}^n$ , una funzione continua a valori in  $\mathbb{K}$ . (Nota: se il campo non è completo, una serie convergente non definisce in generale una funzione in un intorno di 0.)

**7.5.** Sia  $(\mathbb{K}, |\cdot|)$  un campo normato e siano  $a_1, \dots, a_n \in \mathbb{K}$  tali che  $|a_i| = 1$  per ogni  $i = 1, \dots, n$ ; denotiamo con  $A \subset \mathbb{K}$  il sottoanello unitario generato dalle funzioni simmetriche elementari di  $a_1, \dots, a_n$ . Provare che, se l'insieme  $\{a \in A \mid |a| \leq 2^{n-1}\}$  è finito, allora  $a_1, \dots, a_n$  sono radici dell'unità. (Sugg.: i polinomi  $p_r(x) = \prod_i (x - a_i^r)$ , con  $r \in \mathbb{Z}$ , non possono essere tutti distinti.)

Dedurre che le matrici ortogonali a coefficienti interi hanno ordine finito nel gruppo  $O(n, \mathbb{R})$ .

## 7.2 Il teorema di preparazione di Weierstrass

Sia

$$\phi = \sum_{i=0}^{+\infty} \phi_i(x) t^i \in \mathbb{K}\{x_1, \dots, x_n, t\}$$

una serie fissata e si assuma che esista un intero  $N \geq 0$  tale che  $\phi_i(0) = 0$  per ogni  $i < N$  e  $\phi_N(0) = 1$ . Si considerino le applicazioni (dipendenti da  $\phi$ )

$$L: \mathbb{K}\{x_1, \dots, x_n, t\} \rightarrow \mathbb{K}\{x_1, \dots, x_n, t\}, \quad L(\sum_{i \geq 0} f_i(x) t^i) = \sum_{i \geq N} f_i(x) t^{i-N}$$

$$V: \mathbb{K}\{x_1, \dots, x_n, t\} \rightarrow \mathbb{K}\{x_1, \dots, x_n, t\}, \quad V(f) = L(\phi f).$$

**Lemma 7.2.1.** *Sia  $r$  un multiraggio fissato. Allora esiste  $R \leq r$  tale che  $V: B_R \rightarrow B_R$  è bigettiva (ricordiamo che  $B_R = \{f \mid \|f\|_R < +\infty\}$ ).*

*Dimostrazione.* Scriviamo

$$\phi = t^N + t^N e(x, t) + \sum_{i=1}^N \phi_i(x) t^{N-i},$$

con  $e(0) = \phi_i(0) = 0$ . Sia  $\varepsilon = \frac{1}{2(N+1)}$ , a meno restringere  $r$  si può supporre  $\|e\|_r < \varepsilon$ , esiste inoltre una costante  $C$  tale che per ogni  $R < r$ ,  $R = (R_1, \dots, R_n, R_t)$ , vale  $\|\phi_i\|_R \leq C(R_1 + \dots + R_n)$ . Si noti che  $\|L(t^{N-i}g)\|_R \leq R_t^{-i}\|g\|_R$ , presi quindi  $R_1, \dots, R_n$  sufficientemente piccoli tali che  $\|\phi_i\|_R \leq \varepsilon R_t^i$  per ogni  $i = 1, \dots, N$  si ha

$$L(\phi g) - g = eg + \sum \phi_i L(t^{N-i}g)$$

$$\|g - V(g)\|_R = \|L(\phi g) - g\|_R \leq (N+1)\varepsilon\|g\|_R = \frac{1}{2}\|g\|_R.$$

Sia  $\mathfrak{m} \subset \mathbb{K}\{x_1, \dots, x_n, t\}$  l'ideale massimale,  $I = (x_1, \dots, x_n)$  e  $H = Id - V$ ,  $H(g) = g - L(\phi g)$ . Se  $g \in I^p \mathfrak{m}^s$  allora  $H(g) \in I^p \mathfrak{m}^{s+1} + I^{p+1} \mathfrak{m}^{s-N}$ , per induzione segue che per ogni  $g \in \mathbb{K}\{x_1, \dots, x_n\}$ ,  $i > 0$  vale

$$H^i(g) \in \sum_{p \geq 0} I^p \mathfrak{m}^{i-p(N+1)} \subset \mathfrak{m}^d,$$

dove  $d$  è la parte intera di  $\frac{i}{N+1}$ . Quindi per ogni  $g$ ,  $V^{-1}(g) = \sum_{i \geq 0} H^i(g)$  è ben definita come serie formale, essendo inoltre  $\|H^i(g)\|_R \leq 2^{-i}\|g\|_R$  si ha  $\|\sum_{i \geq 0} H^i(g)\|_R < +\infty$  e quindi  $V$  è bigettiva come applicazione di  $B_R$  in sé.  $\square$

**Teorema 7.2.2 (di divisione: Stickelberger, 1887).** *Siano  $\phi, N$  definiti come sopra, per ogni  $f \in \mathbb{K}\{x_1, \dots, x_n, t\}$  esistono unici  $g \in \mathbb{K}\{x_1, \dots, x_n, t\}$  e  $r \in \mathbb{K}\{x_1, \dots, x_n\}[t]$  di grado  $< N$  in  $t$  tali che*

$$f = \phi g + r.$$

*Dimostrazione.* Per il Lemma 7.2.1 esiste  $g$  tale che  $L(f) = L(\phi g)$  e quindi  $r = f - \phi g$  ha grado  $< N$  in  $t$ . Viceversa se  $f = \phi g + r$ , allora  $L(f) = L(\phi g)$  e per 7.2.1  $g$  è unica.  $\square$

**Teorema 7.2.3 (di preparazione: Weierstrass, 1860).** *Siano  $\phi, N$  come sopra, allora esiste unica  $e \in \mathbb{K}\{x_1, \dots, x_n, t\}$  invertibile tale che*

$$\phi e = t^N + \sum_{i=1}^N \psi_i(x) t^{N-i}, \quad \psi_i(0) = 0.$$

*Dimostrazione.* Per il teorema di divisione esiste unica una serie di potenze convergente  $e$  tale che  $t^N = e\phi + r$  con  $r$  polinomio in  $t$  di grado  $< N$ , basta quindi dimostrare che  $e(0) \neq 0$ ,  $r(0, t) = 0$ . Vale  $e(0, t)\phi(0, t) = e(0)t^N + \sum_{i > N} a_i t^i$  e quindi necessariamente  $r(0, t) = 0$  e  $e(0) = 1$ .  $\square$

Dimostriamo adesso che per ogni campo infinito  $\mathbb{K}$  l'anello  $\mathbb{K}\{x_1, \dots, x_n\}$  è un dominio Noetheriano a fattorizzazione unica; questo risultato si rivelerà di importanza fondamentale in seguito; se il campo è finito il risultato è ancora vero ma richiede una diversa dimostrazione. Premettiamo una definizione ed alcuni lemmi.

**Definizione 7.2.4.** *Una serie  $p(x, t) \in \mathbb{K}\{x_1, \dots, x_n, t\}$  si dice un **polinomio di Weierstrass** di grado  $N$  in  $t$  se:*

1.  $p \in \mathbb{K}\{x_1, \dots, x_n\}[t]$  è un polinomio monico di grado  $N$  in  $t$ , cioè si può scrivere

$$p(x, t) = t^N + \sum_{i=1}^N \phi_i(x) t^{N-i}, \quad \phi_i \in \mathbb{K}\{x_1, \dots, x_n\}.$$

2. Nelle notazioni di 1)  $\phi_i(0) = 0$  per ogni  $i = 1, \dots, N$ .

**Lemma 7.2.5.** *Siano  $f, g \in \mathbb{K}\{x_1, \dots, x_n\}[t]$  con  $g$  polinomio di Weierstrass. Se  $f = hg$  con  $h \in \mathbb{K}\{x_1, \dots, x_n, t\}$ , allora anche  $h \in \mathbb{K}\{x_1, \dots, x_n\}[t]$ .*

Si noti che se  $g$  non è di Weierstrass il risultato è falso, si consideri ad esempio il caso  $n = 0, f = t^3$  e  $g = t + t^2$ .

*Dimostrazione.* Sia  $g = t^s + \sum g_i(x)t^{s-i}, g_i(0) = 0, f = \sum_{i=0}^r f_i(x)t^{r-i}, h = \sum_i h_i(x)t^i$ , bisogna dimostrare che  $h_i = 0$  per ogni  $i > r - s$ . Si assuma per assurdo che esista  $j > r - s$  tale che  $h_j \neq 0$ , si può allora supporre che la molteplicità di  $h_j$  sia minima fra tutte le molteplicità di  $h_i, i > r - s$ . Vale l'uguaglianza  $0 = h_j + \sum g_i h_{j+i}$  e siccome tutte le  $g_i$  hanno molteplicità positiva si ottiene una contraddizione.  $\square$

**Lemma 7.2.6.** *Un polinomio di Weierstrass  $g \in \mathbb{K}\{x_1, \dots, x_n\}[t]$  è irriducibile in  $\mathbb{K}\{x_1, \dots, x_n, t\}$  se e solo se è irriducibile in  $\mathbb{K}\{x_1, \dots, x_n, t\}$ .*

Come in 7.2.5 il risultato è falso se  $g$  non è di Weierstrass.

*Dimostrazione.* Assumiamo  $g$  irriducibile in  $\mathbb{K}\{x_1, \dots, x_n, t\}$  e siano  $g_1, g_2 \in \mathbb{K}\{x_1, \dots, x_n\}[t]$  tali che  $g = g_1 g_2$ . A meno di moltiplicazione per costante e scambio di indici si può supporre  $g_1$  polinomio monico in  $t$  invertibile in  $\mathbb{K}\{x_1, \dots, x_n, t\}$ , cioè  $g_1(0) = a$  con  $a \in \mathbb{K} - \{0\}$ . Ma essendo  $g$  di Weierstrass deve necessariamente essere  $g_1(0, t) = t^s$  e quindi  $s = 0$  e  $g_1 = 1$ .

Viceversa supponiamo  $g$  irriducibile in  $\mathbb{K}\{x_1, \dots, x_n\}[t]$  e sia  $g = h_1 h_2$  con  $h_i \in \mathbb{K}\{x_1, \dots, x_n, t\}$ . Siccome  $h_1(0, t) \neq 0$  per il teorema di preparazione possiamo scrivere  $h_1 = e g_1$  con  $e$  invertibile e  $g_1$  polinomio di Weierstrass; per il Lemma 7.2.5  $g_1$  divide  $g$  in  $\mathbb{K}\{x_1, \dots, x_n\}[t]$  e quindi  $g = g_1, h_2$  invertibile oppure  $g_1 = 1, h_1$  invertibile.  $\square$

**Teorema 7.2.7 (E. Lasker, 1905).** *L'anello  $\mathbb{K}\{x_1, \dots, x_n, t\}$  è un dominio a fattorizzazione unica.*

*Dimostrazione.* Induzione su  $n$ ; per  $n = 0$  l'anello  $\mathbb{K}\{t\}$  è un dominio ad ideali principali e quindi è a fattorizzazione unica per fatti generali. Supponiamo  $n > 0$  e sia  $f \in \mathbb{K}\{x_1, \dots, x_n, t\}$  di molteplicità  $m$ , diciamo  $f = f_m + f_{m+1} + \dots$ . Per il lemma di preparazione 4.4.2, a meno di un possibile cambio di coordinate si può supporre  $f_m(0, \dots, 0, 1) \neq 0$  e per il teorema di preparazione si può supporre che  $f$  sia un polinomio di Weierstrass di grado  $m$  in  $t$ . Siccome  $\mathbb{K}\{x_1, \dots, x_n\}$  e  $\mathbb{K}\{x_1, \dots, x_n\}[t]$  sono domini a fattorizzazione unica si ha  $f = \prod f_i$ , con gli  $f_i$  polinomi di Weierstrass irriducibili. Sia  $g \in \mathbb{K}\{x_1, \dots, x_n, t\}$  irriducibile che divide  $f$ , allora  $g(0, t) \neq 0$  e per il teorema di preparazione si può assumere  $g$  polinomio di Weierstrass e quindi  $g = f_i$  per qualche  $i$ .  $\square$

**Teorema 7.2.8 (W. Rückert, 1931).** *L'anello  $\mathbb{K}\{x_1, \dots, x_n, t\}$  è Noetheriano.*

*Dimostrazione.* Induzione su  $n$ ; per  $n = 0$  l'anello  $\mathbb{K}\{t\}$  è un dominio ad ideali principali e quindi Noetheriano. Supponiamo  $n > 0$  e sia  $I \subset \mathbb{K}\{x_1, \dots, x_n, t\}$  un ideale. Se  $I = 0$ , allora  $I$  è finitamente generato. Se  $I \neq 0$ , allora, ragionando come nella dimostrazione del Teorema 7.2.7, si può supporre che esista  $f \in I$  polinomio di Weierstrass in  $t$  di grado  $s$ . Per l'ipotesi induttiva ed il teorema della base di Hilbert, l'anello  $\mathbb{K}\{x_1, \dots, x_n\}[t]$  è Noetheriano e quindi l'ideale  $J = I \cap \mathbb{K}\{x_1, \dots, x_n\}[t]$  è finitamente generato, diciamo da  $g_1, \dots, g_r$ . Dato  $h \in I$ , per il teorema di divisione 7.2.2 si può scrivere  $h = pf + q$  con  $p \in \mathbb{K}\{x_1, \dots, x_n, t\}$  e  $q \in J$ ; quindi  $I$  è generato da  $f, g_1, \dots, g_r$ .  $\square$

**Teorema 7.2.9 (Lemma di Hensel).** *Sia  $p(x, t) \in \mathbb{K}\{x_1, \dots, x_n\}[t]$  un polinomio monico di grado  $N$  in  $t$  e denotiamo  $p_0(t) = p(0, t) \in \mathbb{K}[t]$ . Siano  $h_0, k_0 \in \mathbb{K}[t]$  due polinomi monici senza fattori comuni tali che  $p_0 = h_0 k_0$  e di gradi  $a, b = N - a$  rispettivamente. Se il campo  $\mathbb{K}$  contiene tutte le radici di  $h_0$  allora esistono, e sono unici, due polinomi  $h, k \in \mathbb{K}\{x_1, \dots, x_n\}[t]$  di gradi rispettivi  $a, b$  in  $t$  tali che  $hk = p$  e  $h_0(t) = h(0, t)$ ,  $k_0(t) = k(0, t)$ .*

*Osservazione 7.2.10.* Il Lemma di Hensel continua ad essere valido anche senza l'ipotesi sulle radici di  $h_0$  ma richiede una diversa dimostrazione.

*Dimostrazione.* Per induzione su  $a$ ; se  $a = 0$  allora  $h_0 = 1$  e non c'è nulla da dimostrare. Se  $a > 0$  sia  $\alpha \in \mathbb{K}$  una radice di  $h_0$  e scriviamo  $h_0(t) = (t - \alpha)^m l_0(t)$ ,  $l_0(\alpha) \neq 0$ . Per ipotesi  $k_0(\alpha) \neq 0$ . Il polinomio  $q(x, t) = p(x, t + \alpha)$  è tale che  $q(0, t) = c_m t^m + c_{m+1} t^{m+1} + \dots$  con la costante  $c_m \neq 0$ . Per il teorema di preparazione di Weierstrass e per il Lemma 7.2.5 possiamo scrivere  $q =$  come il prodotto di un polinomio di Weierstrass  $q_1$  di grado  $m$  e di un polinomio  $q_2$ . Inoltre  $q_1, q_2$  sono unici. Quindi  $p(x, t) = p_1(x, t) p_2(x, t)$ , dove  $p_i(x, t) = q_i(x, t - \alpha)$ ,  $p_1(0, t) = (t - \alpha)^m$  e  $p_2(0, t) = l_0(t) k_0(t)$ . Poiché  $l_0$  ha grado  $< a$  è possibile applicare l'ipotesi induttiva a  $p_2(x, t)$ .  $\square$

**Corollario 7.2.11.** *Sia  $p(x, t) \in \mathbb{K}\{x_1, \dots, x_n\}[t]$  un polinomio monico in  $t$ . Se  $\alpha$  è una radice semplice di  $p(0, t)$  allora esiste unica una serie convergente  $\psi \in \mathbb{K}\{x_1, \dots, x_n\}$  tale che  $\psi(0) = \alpha$  e  $p(x, \psi(x)) = 0$ .*

*Dimostrazione.* Per il lemma di Hensel esiste una serie convergente  $\psi$  ed un polinomio  $p_1$  tale che  $p = (t - \psi)p_1$ ,  $t - \psi(0) = t - \alpha$  e  $p_1(0, \alpha) \neq 0$ . In particolare per ogni  $\psi_1 \in \mathbb{K}\{x_1, \dots, x_n\}$  tale che  $\psi_1(0) = \alpha$  si ha  $p_1(x, \psi_1(x)) \neq 0$  e quindi se  $p(x, \psi_1(x)) = 0$  deve necessariamente essere  $\psi_1 = \psi$ .  $\square$

**Proposizione 7.2.12.** *Siano  $\mathbb{K}$  un campo algebricamente chiuso e  $f \in \mathbb{K}\{x, y\}$  irriducibile di molteplicità positiva  $m$ . Se  $f = f_m + f_{m+1} + \dots$  indica la scomposizione in componenti omogenee, allora  $f_m$  è una potenza di un polinomio irriducibile.*

*Dimostrazione.* Supponiamo per assurdo  $f_m = g_a h_b$  con  $g_a, h_b$  omogenei di grado  $a, b > 0$  rispettivamente e senza fattori comuni; basta provare che esiste una decomposizione  $f = gh$  con  $g = g_a + g_{a+1} + \dots$ ,  $h = h_b + h_{b+1} + \dots$ . A meno di un cambio lineare di coordinate e moltiplicazione per invertibili possiamo supporre  $f, f_m, g_a, h_b$  polinomi di Weierstrass di gradi  $m, m, a, b$  rispettivamente nella variabile  $y$ . Detto  $\hat{f}(x, y) = \frac{f(x, y)}{x^m}$  vale  $\hat{f}(0, y) = \hat{f}_m(0, y) = \hat{g}_a(0, y) \hat{h}_b(0, y)$  e per il lemma di Hensel possiamo scrivere  $\hat{f} = \hat{g} \hat{h}$  con  $\hat{g}, \hat{h}$  polinomi monici in  $y$  di grado  $a, b$  rispettivamente; basta adesso riconsiderare  $g(x, y) = x^a \hat{g}\left(x, \frac{y}{x}\right)$ ,  $h(x, y) = x^b \hat{h}\left(x, \frac{y}{x}\right)$ .  $\square$

Se  $\mathbb{K}$  è algebricamente chiuso e  $f \in \mathbb{K}\{x, y\}$ ,  $f = f_m + f_{m+1} + \dots$ , si definisce il cono tangente di  $f$ ,  $C(f) \subset \mathbb{K}^2$ , come la curva affine di equazione  $f_m$ . Chiaramente il supporto di  $C(f)$  è unione di un numero finito di rette uguale al numero di radici distinte di  $f_m$  in  $\mathbb{P}^1$ . Il precedente risultato può essere allora riformulato nella seguente forma:

**Proposizione 7.2.13.** *Siano  $\mathbb{K}$  algebricamente chiuso e  $f \in \mathbb{K}\{x, y\}$ , allora il numero di fattori irriducibili distinti di  $f$  non è inferiore al numero di rette distinte contenute nel cono tangente  $C(f)$ .*

*Dimostrazione.* Basta applicare la Proposizione 7.2.12 ad ogni fattore irriducibile di  $f$ .  $\square$



**Esercizi**

**7.6 (Anelli Henseliani, \*\*).** Sia  $A$  un anello locale con ideale massimale  $\mathfrak{m}$  e campo residuo  $\mathbb{K}$ ; provare che le seguenti proprietà sono equivalenti:

1. Sia  $p \in A[x]$  un polinomio monico a coefficienti in  $A$  e sia  $\bar{p} \in \mathbb{K}[x]$  la sua riduzione modulo  $\mathfrak{m}$ . Se esistono  $\bar{p}_1, \bar{p}_2 \in \mathbb{K}[x]$  senza fattori comuni tali che  $\bar{p}_1\bar{p}_2 = \bar{p}$ , allora si può sollevare  $\bar{p}_1, \bar{p}_2$  a polinomi  $p_1, p_2 \in A[x]$  tali che  $p_1p_2 = p$ .
2. Per ogni omomorfismo di anelli  $A \rightarrow B$  per cui  $B$  sia finitamente generato come  $A$ -modulo, l'applicazione naturale tra gli insiemi degli idempotenti  $E(B) \rightarrow E(B/\mathfrak{m}B)$  è bigettiva (per definizione di  $E(B) = \{b \in B \mid b^2 = b\}$  vedi Esercizio 1.38).
3. Per ogni morfismo di anelli  $A \rightarrow B$ , con  $B$  finitamente generato come  $A$ -modulo, si può scrivere  $B$  come prodotto diretto di un numero finito di anelli locali.

Un anello con queste proprietà si dice **Henseliano**.

### 7.3 Il teorema fondamentale dell'algebra ed il teorema di Newton-Puiseux

In questa sezione daremo una dimostrazione del fatto che  $\mathbb{C}$  è un campo algebricamente chiuso che utilizza i concetti introdotti nelle Sezioni 7.1 e 7.2. Tale dimostrazione, sebbene più complicata di quelle tradizionali, ha il pregio di gettare luce sulla geometria dei polinomi complessi. Inoltre, con lievi modifiche (vedi esercizi), la stessa dimostrazione può essere utilizzata per dimostrare che un campo completo  $(\mathbb{K}, | \cdot |)$  è algebricamente chiuso se  $\mathbb{K} - \{0\}$  è connesso.

**Teorema 7.3.1 (Teorema fondamentale dell'algebra).** *Ogni polinomio  $p \in \mathbb{C}[t]$  di grado positivo è un prodotto di polinomi di grado 1.*

*Dimostrazione.* Si può chiaramente supporre  $p$  monico di grado  $n \geq 2$ ,

$$p(t) = t^n + a_1t^{n-1} + \dots + a_n.$$

Inoltre, a meno di effettuare la sostituzione  $t \mapsto t - \frac{a_1}{n}$ , si può assumere  $a_1 = 0$ . Per induzione su  $n$  si può assumere il teorema vero per ogni polinomio di grado  $< n$ . Dato un vettore  $a = (a_2, \dots, a_n) \in \mathbb{C}^{n-1}$  si pone  $p_a(t) = t^n + a_2t^{n-2} + \dots + a_n$ . Si considerino poi i due sottoinsiemi:

$W$  = insieme dei vettori  $a$  tali che  $p_a$  non ha radici.

$V$  = insieme dei vettori  $a$  tali che vale  $p_a = rs$  con  $r, s$  polinomi di grado positivo senza fattori comuni.

Per dimostrare il Teorema 7.3.1 occorre provare che  $W = \emptyset$ ; quest'ultimo fatto è una conseguenza dei seguenti tre lemmi.

**Lemma 7.3.2.** *Nelle notazioni precedenti vale  $V \neq \emptyset$ ,  $V \cap W = \emptyset$  e  $V \cup W = \mathbb{C}^{n-1} - \{0\}$ .*

**Lemma 7.3.3.** *L'insieme  $W$  è aperto nella topologia euclidea.*

**Lemma 7.3.4.** *L'insieme  $V$  è contenuto nella parte interna di  $\mathbb{C}^{n-1} - W$ .*

*Dimostrazione (di 7.3.2).* L'unica asserzione non banale è  $V \cup W = \mathbb{C}^{n-1} - \{0\}$ . Se  $a \notin V \cup W$ , allora  $p_a$  è una potenza di un polinomio irriducibile e quindi, per l'ipotesi induttiva, deve avere una radice di molteplicità  $n$ , cioè  $p_a = (t + b)^n$ . Siccome  $a_1 = nb = 0$ , deve essere  $b = 0$  e quindi  $a = 0$ .  $\square$

*Dimostrazione (di 7.3.3).* Siano  $[t_0, t_1]$  coordinate omogenee di  $\mathbb{P}_{\mathbb{C}}^1$  e si consideri il chiuso

$$H = \{(a, [t_0, t_1]) \in \mathbb{C}^{n-1} \times \mathbb{P}_{\mathbb{C}}^1 \mid t_1^n + \sum a_i t_0^i t_1^{n-i} = 0\}.$$

Indicando con  $\pi: \mathbb{C}^{n-1} \times \mathbb{P}_{\mathbb{C}}^1 \rightarrow \mathbb{C}^{n-1}$  la proiezione sul primo fattore, si ha  $\mathbb{C}^{n-1} - W = \pi(H)$  e, siccome  $\pi$  è un'applicazione propria, ne consegue che  $\pi(H)$  è un sottoinsieme chiuso.  $\square$

*Dimostrazione (di 7.3.4).* Sia  $a \in V$ , bisogna dimostrare che esiste un multiraggio  $R$  tale che per ogni vettore  $x = (x_2, \dots, x_n)$  con  $|x_i| < R_i$  si ha che  $p_{a+x}$  non è irriducibile. Sia  $\phi(x, t) = p_{a+x}(t)$ , siccome  $\phi(0, t)$  è il prodotto di due polinomi monici relativamente primi; per induzione  $\phi(0, t)$  è un prodotto di fattori di grado 1 e, per il lemma di Hensel, si ha  $\phi(x, t) = r(x, t)s(x, t)$  con  $r, s$  polinomi monici in  $t$  di grado positivo. Preso dunque un poliraggio  $R$  sufficientemente piccolo  $r$  ed  $s$  sono funzioni definite sul polidisco  $\Delta = \{x \in \mathbb{C}^{n-1} \mid |x_i| < R_i\}$  e quindi  $a + \Delta \cap W = \emptyset$ .  $\square$

I lemmi precedenti implicano che  $W = \emptyset$ : infatti da 7.3.2 e 7.3.4 segue che  $V$  è contenuto nella sua parte interna e quindi è un aperto non vuoto, adesso basta usare la connessione di  $\mathbb{C}^{n-1} - \{0\}$ .  $\square$

Consideriamo un polinomio monico  $p \in \mathbb{C}\{x\}[t]$ . Si osserva immediatamente che in generale non esiste alcuna fattorizzazione di  $p$  in pseudopolinomi di grado 1 in  $t$ , basta ad esempio considerare  $p = t^2 - x$ . Newton ebbe per primo l'intuizione che si può sempre scrivere (almeno formalmente)  $p(x, t) = \prod_i (t - \phi_i(x))$  dove  $\phi_i(x) = \sum a_j x^{\alpha_j}$  con gli esponenti  $\alpha_j$  non necessariamente interi. La dimostrazione completa di questo fatto si è avuta molto più tardi ad opera di Puiseux nel 1850.

**Teorema 7.3.5.** *Sia  $\mathbb{K}$  un campo algebricamente chiuso di caratteristica 0 e sia*

$$p(x, t) = t^N + \sum_{i=1}^N \phi_i(x) t^{N-i} \in \mathbb{K}\{x\}[t], \quad \text{con } N > 0.$$

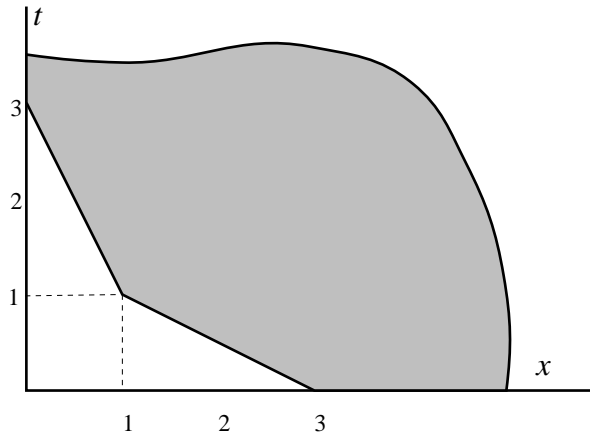
*Esiste allora un intero  $0 < s \leq N$  tale che  $p(\xi^s, t)$  è decomponibile in  $\mathbb{K}\{\xi\}[t]$ .*

*Dimostrazione.* Essendo  $\mathbb{K}$  di caratteristica 0 si può supporre senza perdita di generalità  $\phi_1 = 0$ . Se  $p = t^N$  la tesi è ovvia; altrimenti per ogni  $i \geq 2$  sia  $\alpha_i$  la molteplicità di  $\phi_i$  (per convenzione  $\alpha_i = +\infty$  se  $\phi_i = 0$ ). Sia  $j \geq 2$  un indice tale che  $\frac{\alpha_j}{j} \leq \frac{\alpha_i}{i}$  per ogni  $i$ . Se  $\alpha_j = 0$ , allora  $p(0, t)$  possiede almeno due radici distinte e per il lemma di Hensel  $p(x, t)$  si decompone nel prodotto di due polinomi monici in  $t$ . Se  $\alpha_j > 0$ , sia  $m$  il minimo comune multiplo di  $j$  e  $\alpha_j$  e denotiamo  $s = \frac{m}{\alpha_j}$ ,  $l = \frac{m}{j}$ . Vogliamo dimostrare che  $p(\xi^s, t)$  è decomponibile. Scriviamo  $p(\xi^s, t) = t^N + \sum \psi_i(\xi) t^{N-i}$ , dove  $\psi_i(\xi) = \phi_i(\xi^s)$ . Per ogni  $i$  la molteplicità di  $\psi_i$  è  $s\alpha_i \geq il$  ed esiste quindi un polinomio in  $t$  definito da

$$q(\xi, t) = p(\xi^s, \xi^l t) \xi^{-lN} = t^N + \sum \frac{\psi_i(\xi)}{\xi^{li}} t^{N-i} = t^N + \sum \eta_i(\xi) t^{N-i}.$$

Siccome  $\eta_j(0) \neq 0$ , per il lemma di Hensel si può scrivere  $q(\xi, t) = q_1(\xi, t)q_2(\xi, t)$  con  $q_i$  polinomio in  $t$  di grado  $N_i$ . Siano  $p_1, p_2$  due polinomi tali che  $p_i(\xi, \xi^l t) = q_i(\xi, t)\xi^{lN_i}$ , è allora chiaro che  $p(\xi^s, t) = p_1(\xi, t)p_2(\xi, t)$ .  $\square$

Data una serie in due variabili  $f = \sum a_{ij} x^i t^j$  si definisce il **poligono di Newton**  $N_f$  di  $f$  come l'involuppo convesso in  $\mathbb{R}^2$  del sottoinsieme di  $\mathbb{N}^2$  formato dalle coppie  $(i', j')$  tali che  $a_{ij} \neq 0$  per qualche  $i \leq i'$  e qualche  $j \leq j'$ .



**Figura 7.1.** Poligono di Newton di  $t^3 + x^3 + tx$

Si noti che nella dimostrazione del Teorema 7.3.5, gli interi  $s$  ed  $l$  sono determinati dal poligono di Newton  $N_p$ ; più precisamente  $s$  è il più piccolo intero positivo tale che il bordo di  $N_p$  contiene un punto di coordinate intere  $(l, N - s)$ . L'esponente  $s$  determinato dal poligono di Newton non è necessariamente il minimo indispensabile per fattorizzare  $p$ , si consideri ad esempio  $p = t^2 - x^4$ . Se il campo  $\mathbb{K}$  è di caratteristica positiva il Teorema 7.3.5 è generalmente falso (vedi Esercizi 7.7 e 7.8).

**Definizione 7.3.6.** Una *serie di Puiseux*  $\phi$  a coefficienti in  $\mathbb{K}$  è una combinazione formale

$$\phi = \sum_{i \in \mathbb{N}} a_i x^{\frac{i}{C}} \quad a_i \in \mathbb{K},$$

dove  $C$  è un intero positivo che dipende da  $\phi$ .

Ogni serie di Puiseux possiede una forma canonica  $\phi = \sum_{i=0}^{+\infty} a_i x^{\frac{i}{N}}$  determinata dalla condizione aggiuntiva che esistano interi  $i_1, \dots, i_d$  tali che  $a_{i_h} \neq 0$  per ogni  $h$  e  $\text{GCD}(N, i_1, \dots, i_d) = 1$ . L'intero  $N$  si dice **ordine di polidromia** della serie e, se definiamo per ricorrenza

$$\begin{cases} \tau_0 = N \\ \tau_{s+1} = \min\{i \mid a_i \neq 0, \text{GCD}(\tau_0, \dots, \tau_s) > \text{GCD}(\tau_0, \dots, \tau_s, i)\} \end{cases}$$

allora gli interi  $\tau_1, \dots, \tau_d$  si dicono **esponenti caratteristici** di  $\phi$ .

Una serie di Puiseux  $\phi = \sum a_i x^{\frac{i}{N}}$  si dice convergente se esiste un raggio  $r > 0$  tale che  $\sum |a_i| r^i < +\infty$ . Come nel caso delle serie di potenze si prova che le serie di Puiseux convergenti formano un anello  $P\{x\}$ . Esiste una ovvia inclusione  $\mathbb{K}\{x\} \subset P\{x\}$ .

**Corollario 7.3.7 (Newton-Puiseux).** Sia  $p \in \mathbb{K}\{t\}[x]$  un polinomio monico in  $t$  di grado  $N$  con  $\mathbb{K}$  algebricamente chiuso di caratteristica 0. Esistono allora serie di Puiseux convergenti  $\phi_1, \dots, \phi_N \in P\{x\}$  con ordine di polidromia  $\leq N$  tali che

$$p(x, t) = \prod_{i=1}^N (t - \phi_i(x)).$$

*Dimostrazione.* L'esistenza delle  $\phi_i$  segue immediatamente dal Teorema 7.3.5. Sia  $s$  l'ordine di polidromia di  $\phi_1$ , ciò significa che si può scrivere  $x = \xi^s$  e  $\phi_1(x) = \psi(\xi)$ , con

$\psi \in \mathbb{K}\{\xi\}$ . Se  $\epsilon$  è una radice  $s$ -upla primitiva di 1, allora le serie  $\psi(\epsilon^i \xi)$  descrivono al variare di  $i \in \mathbb{N}$ ,  $s$  radici distinte di  $p$ , dunque  $s \leq N$ . Si noti che, essendo  $P\{x\}$  un dominio di integrità, le serie  $\phi_i$  sono uniche a meno dell'ordine.  $\square$

### Esercizi

**7.7.** Sia  $\mathbb{K}$  campo algebricamente chiuso di caratteristica 3. Provare che  $x^3 + t^{2s}x + t^s$  è irriducibile in  $\mathbb{K}[[t]][x]$  per ogni  $s > 0$ .

**7.8.** Sia  $\mathbb{K}$  un campo di caratteristica  $p > 0$ . Provare che il polinomio di Weierstrass  $x^p + t^s x^{p-1} + t^s$  non ha radici in  $\mathbb{K}[[t]]$  per ogni  $s > 0$ . (Sugg.: si può assumere  $\mathbb{K}$  algebricamente chiuso, se esiste una radice  $\xi$ , allora deve essere del tipo  $\xi = \eta^p$  e  $p$  deve dividere  $s$ ; induzione su  $s$ .)

**7.9.** Scrivere le serie di Puiseux radici dei polinomi in  $\mathbb{C}\{t\}[x]$   $x^a - t^b$ ,  $x^2 - t^2 - t^3$  e  $x^3 + 3x^2t + 3xt^2 + t^4$ .

**7.10.** Mostrare che per ogni numero primo  $p$  esiste un campo di caratteristica 0, NON algebricamente chiuso nel quale ogni polinomio di grado  $< p$  possiede una radice. (Sugg.: Corollario 7.3.7.)

**7.11.** Per ogni coppia di interi positivi  $n, s \in \mathbb{N} - \{0\}$  siano  $A_n$  una copia di  $\mathbb{K}\{t\}$  e  $\rho_{n,s}: A_n \rightarrow A_{ns}$  l'omomorfismo di  $\mathbb{K}$  algebre definito da  $\rho_{s,n}(\phi)(t) = \phi(t^s)$ . Provare che  $P\{t\}$  è il limite diretto del sistema  $(A_n, \rho_{n,s})$ .

**7.12.** Sia  $p(t, x) = x^r + g_1(t)x^{r-1} + \dots + g_r \in \mathbb{C}\{t\}[x]$  un polinomio in  $x$  convergente e sia  $\phi(t) \in \mathbb{C}[[t]]$  tale che  $p(t, \phi(t)) = 0$ . Provare che  $\phi(t) \in \mathbb{C}\{t\}$  è convergente.

## 7.4 Il teorema delle funzioni implicite

Se  $\phi_1, \dots, \phi_n \in \mathbb{K}\{y_1, \dots, y_m\}$  sono serie di molteplicità positiva, è facile vedere che l'applicazione

$$\phi: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}\{y_1, \dots, y_m\}, \quad \phi(f) = f(\phi_1, \dots, \phi_n)$$

è un omomorfismo locale di  $\mathbb{K}$ -algebre.

**Lemma 7.4.1.** Sia  $\phi: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}\{y_1, \dots, y_m\}$  un omomorfismo di  $\mathbb{K}$ -algebre. Allora le serie  $\phi_i = \phi(x_i)$ , per  $i = 1, \dots, n$ , hanno molteplicità positiva e per ogni  $f \in \mathbb{K}\{x_1, \dots, x_n\}$  vale  $\phi(f) = f(\phi_1, \dots, \phi_n)$ .

*Dimostrazione.* Siano  $\mathfrak{m} = (x_1, \dots, x_n)$  e  $\mathfrak{n} = (y_1, \dots, y_m)$  gli ideali massimali di  $\mathbb{K}\{x_1, \dots, x_n\}$  e  $\mathbb{K}\{y_1, \dots, y_m\}$  rispettivamente. Se  $\phi: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}\{y_1, \dots, y_m\}$  è un morfismo di  $\mathbb{K}$ -algebre, allora  $\phi(\mathfrak{m}) \subset \mathfrak{n}$ : infatti se per assurdo esistesse  $f \in \mathfrak{m}$  tale che  $\phi(f) \notin \mathfrak{n}$ , allora  $\phi(f)(0) \neq 0$  e quindi  $f - \phi(f)(0)$  sarebbe invertibile in  $\mathbb{K}\{x_1, \dots, x_n\}$ ; ne seguirebbe che  $\phi(f - \phi(f)(0))$  sarebbe invertibile, in contraddizione con il fatto che  $\phi(f) - \phi(f)(0) \in \mathfrak{n}$ . In particolare le serie  $\phi(x_1), \dots, \phi(x_n)$  sono convergenti di molteplicità positiva; passando alle potenze degli ideali massimali, vale  $\phi(\mathfrak{m}^s) \subset \mathfrak{n}^s$  per ogni  $s > 0$ . Data una serie  $f \in \mathbb{K}\{x_1, \dots, x_n\}$ , le due serie  $\phi(f)$  e  $f(\phi(x_1), \dots, \phi(x_n))$  sono entrambe convergenti; per ogni  $s > 0$  si può scrivere  $f = p_s + q_s$ , dove  $p_s$  è un polinomio in  $x_1, \dots, x_n$  e  $q_s \in \mathfrak{m}^s$ . Dato che  $\bigcap_s \mathfrak{n}^s = 0$  e vale

$$\phi(f) = \phi(p_s) + \phi(q_s) \equiv \phi(p_s) = p_s(\phi(x_1), \dots, \phi(x_n)) \pmod{\mathfrak{n}^s}$$

$$f(\phi(x_1), \dots, \phi(x_n)) \equiv p_s(\phi(x_1), \dots, \phi(x_n)) \pmod{\mathfrak{n}^s},$$

passando al limite per  $s \rightarrow +\infty$  si ottiene l'uguaglianza  $\phi(f) = f(\phi(x_1), \dots, \phi(x_n))$ .  $\square$

**Lemma 7.4.2.** Sia  $f(x_1, \dots, x_n) \in \mathbb{K}\{x_1, \dots, x_n\}$  una serie di molteplicità positiva. Allora il nucleo dell'omomorfismo  $\phi: \mathbb{K}\{x_1, \dots, x_n, t\} \rightarrow \mathbb{K}\{x_1, \dots, x_n\}$  definito da

$$\phi(t) = f(x_1, \dots, x_n) \text{ e } \phi(x_i) = x_i \text{ per } i = 1, \dots, n,$$

è l'ideale generato da  $t - f(x)$ .

*Dimostrazione.* È ovvio che  $t - f(x_1, \dots, x_n) \in \text{Ker}(\phi)$ . Viceversa sia  $g(x_1, \dots, x_n, t) \in \mathbb{K}\{x_1, \dots, x_n, t\}$ ; per il teorema di divisione possiamo scrivere

$$g(x_1, \dots, x_n, t) = (t - f(x_1, \dots, x_n))h(x_1, \dots, x_n, t) + r(x_1, \dots, x_n)$$

e vale  $\phi(g) = r$ . □

**Teorema 7.4.3 (Teorema delle funzioni implicite).** Siano date  $m$  serie convergenti  $f_1, \dots, f_m \in \mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_m\}$  di molteplicità positiva e si consideri l'omomorfismo di  $\mathbb{K}$ -algebre

$$\phi: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \frac{\mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_m\}}{(f_1, \dots, f_m)}, \quad \phi(x_i) = x_i.$$

Allora sono equivalenti:

1.  $\phi$  è un isomorfismo.
2.  $\phi$  è surgettivo.
3.  $\det \left( \frac{\partial f_i}{\partial y_j}(0) \right) \neq 0$ .

*Dimostrazione.* [2  $\Rightarrow$  3] Se  $\phi$  è surgettivo, allora per ogni  $i = 1, \dots, m$  si può scrivere

$$y_i = h_i(x) + \sum_j k_j(x, y) f_j(x, y)$$

e quindi, denotando con  $h_i(x)_1, f_j(x, y)_1$  le parti lineari, si hanno le uguaglianze

$$y_i = h_i(x)_1 + \sum_j k_j(0, 0) f_j(x, y)_1$$

dalle quali segue che la matrice  $\left( \frac{\partial f_i}{\partial y_j}(0) \right)$  ha rango massimo.

[3  $\Rightarrow$  1] A meno di sostituire le serie  $f_i$  con opportune combinazioni lineari indipendenti di esse stesse, possiamo supporre, per ogni  $i = 1, \dots, m$ , che  $f_i = y_i + l_i(x) + h_i(x, y)$ , con le serie  $l_i$  di molteplicità positiva e le serie  $h_i$  di molteplicità  $\geq 2$ . Per il teorema di preparazione possiamo scrivere  $f_m = (y_m - g_m(x, y_1, \dots, y_{m-1}))e(x, y)$ , con  $e(0, 0) \neq 0$ . Per il Lemma 7.4.2 il nucleo dell'omomorfismo

$$\psi: \mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_m\} \rightarrow \mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_{m-1}\}, \quad y_m \mapsto g_m$$

è esattamente l'ideale generato da  $f_m$ , e quindi  $\psi$  induce un isomorfismo di anelli

$$\frac{\mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_m\}}{(f_1, \dots, f_m)} \rightarrow \frac{\mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_{m-1}\}}{(\hat{f}_1, \dots, \hat{f}_{m-1})}$$

dove  $\hat{f}_i = \psi(f_i) = y_i + l_i(x) + \psi(h_i)$ . Basta adesso usare induzione su  $m$ . □

**Corollario 7.4.4.** *Siano date  $m$  serie convergenti  $f_1, \dots, f_m \in \mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_m\}$  di molteplicità positiva tali che  $\det\left(\frac{\partial f_i}{\partial y_j}(0)\right) \neq 0$ . Allora esistono  $m$  serie convergenti  $\psi_1(x), \dots, \psi_m(x) \in \mathbb{K}\{x_1, \dots, x_n\}$  di molteplicità positiva tali che*

$$f_i(x_1, \dots, x_n, \psi_1(x), \dots, \psi_m(x)) = 0 \quad \text{per ogni } i = 1, \dots, m.$$

*Dimostrazione.* Per il Teorema 7.4.3 l'omomorfismo

$$\phi: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \frac{\mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_m\}}{(f_1, \dots, f_m)}, \quad \phi(x_i) = x_i,$$

è un isomorfismo. Basta allora definire  $\psi_i = \phi^{-1}(y_i)$ .  $\square$

**Teorema 7.4.5 (di invertibilità locale).** *Siano date  $f_1, \dots, f_n \in \mathbb{K}\{y_1, \dots, y_n\}$  di molteplicità positiva. L'omomorfismo di  $\mathbb{K}$ -algebre*

$$\phi: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}\{y_1, \dots, y_n\}, \quad \phi(x_i) = f_i$$

*è un isomorfismo se e solo se*

$$\det\left(\frac{\partial f_i}{\partial y_j}(0)\right) \neq 0.$$

*Dimostrazione.* Si consideri l'anello

$$A = \frac{\mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_n\}}{(x_1 - f_1, \dots, x_n - f_n)}$$

e gli omomorfismi

$$\begin{aligned} \alpha: \mathbb{K}\{x_1, \dots, x_n\} &\rightarrow A, & \alpha(x_i) &= x_i, \\ \beta: \mathbb{K}\{y_1, \dots, y_n\} &\rightarrow A, & \beta(y_i) &= y_i, \\ \gamma: A &\rightarrow \mathbb{K}\{y_1, \dots, y_n\}, & \gamma(x_i) &= f_i, \quad \gamma(y_i) = y_i. \end{aligned}$$

Si ha evidentemente  $\gamma\alpha = \phi$ ,  $\gamma\beta = Id$ ; per il teorema delle funzioni implicite  $\beta$  è invertibile e quindi  $\gamma = \beta^{-1}$ . Per il Teorema 7.4.3,  $\alpha$  è un isomorfismo se e solo se la matrice jacobiana è invertibile in 0.  $\square$

## Esercizi

**7.13 (Relazione di Reiss, [GH1978, pag. 675]).** (caratteristica  $\neq 2$ ) Sia  $f \in \mathbb{K}\{x\}[y]$  polinomio monico di grado  $n$  tale che  $f(0, y)$  abbia  $n$  radici distinte  $y_1, \dots, y_n$ . Provare che il coefficiente di  $x^2 y^{n-1}$  in  $f$  è uguale a

$$\frac{1}{2} \sum_{i=1}^n \frac{f_{xx} f_y^2 - 2f_{xy} f_x f_y + f_{yy} f_x^2}{f_y^3}(0, y_i),$$

dove come al solito si intende con  $f_x$  la derivata parziale rispetto a  $x$  ecc. (Sugg.: scrivere  $f = \prod(y + \phi_i(x))$ , derivare le relazioni  $f(x, -\phi_i(x)) = 0$  e rappresentare i singoli termini della sommatoria in funzione di  $\phi_1, \dots, \phi_n$ .)

**7.14.** Nell'Esercizio 7.13 si assuma  $\mathbb{K} = \mathbb{R}$  ed  $f$  convergente in una striscia  $(-\epsilon, \epsilon) \times \mathbb{R}$ . Descrivere i termini della sommatoria in funzione del versore tangente e della curvatura della curva piana  $f = 0$  nei punti di intersezione con l'asse  $x = 0$ .

**7.15.** Siano  $f \in \mathbb{K}\{x_1, \dots, x_n, t_1, \dots, t_m\}$  e  $g_1, \dots, g_m \in \mathbb{K}\{x_1, \dots, x_n\}$  serie di molteplicità positiva. Provare che l'ideale generato da  $f, t_1 - g_1, \dots, t_m - g_m$  coincide con l'ideale generato da  $f(x_1, \dots, x_n, g_1, \dots, g_m), t_1 - g_1, \dots, t_m - g_m$ .

**7.16.** Sia  $\phi: \mathbb{K}\{x_1, \dots, x_n, y_1, \dots, y_m\} \rightarrow \mathbb{K}\{x_1, \dots, x_n\}$  un morfismo di  $\mathbb{K}$ -algebre tale che  $\phi(x_i) = x_i$ . Provare che il nucleo di  $\phi$  è l'ideale generato dalle serie  $y_i - \phi(y_i)$ .

## 7.5 Archi e parametrizzazioni

**Definizione 7.5.1.** Un *germe di arco analitico*, detto più semplicemente *arco*, è un omomorfismo locale di  $\mathbb{K}$ -algebre

$$\alpha: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}\{t\}.$$

Un tale arco  $\alpha$  è unicamente determinato dalle  $n$  serie di potenze  $\alpha(x_i) \in (t)$ , dove  $(t) \subset \mathbb{K}\{t\}$  denota l'ideale massimale; se  $\alpha(x_i) = 0$  per ogni  $i$  chiameremo  $\alpha$  arco banale. Se  $f_1, \dots, f_n \in (t)$ , denoteremo con  $\alpha = (f_1, \dots, f_n)$  l'arco definito da  $\alpha(x_i) = f_i$ .

Diremo che un arco  $\alpha$  è **primitivo** o **irriducibile** se l'immagine di  $\alpha$  contiene un ideale non banale di  $\mathbb{K}\{t\}$ ; altrimenti si dirà **riducibile**.

*Esempio 7.5.2.* 1. Un arco  $\alpha: \mathbb{K}\{x\} \rightarrow \mathbb{K}\{t\}$  è primitivo se e solo se è un isomorfismo.

Infatti per ogni  $f \in \mathbb{K}\{x\}$  vale  $\nu(\alpha(f)) = \nu(f)\nu(\alpha(x))$ , mentre per il teorema di invertibilità locale  $\alpha$  è un isomorfismo se e solo se  $\alpha(x)$  ha molteplicità 1. (vedi anche Esercizio 7.18).

2. L'arco  $\alpha: \mathbb{K}[[x, y]] \rightarrow \mathbb{K}[[t]]$  definito da  $\alpha(x) = t^2$ ,  $\alpha(y) = t^3$  è primitivo: infatti l'immagine di  $\alpha$  contiene l'ideale  $(t^2)$ .

3. Siano  $\alpha: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}\{t\}$  e  $\xi: \mathbb{K}\{t\} \rightarrow \mathbb{K}\{t\}$  due archi. Se  $\xi \circ \alpha$  è primitivo, allora  $\xi$  è un isomorfismo.

Esiste un semplice criterio per stabilire se un arco è primitivo. Premettiamo alcuni lemmi:

**Lemma 7.5.3.** Sia  $H \subset \mathbb{N}$  un semigruppò, cioè un sottoinsieme chiuso per l'operazione di addizione. Allora sono equivalenti:

1. Il complementare di  $H$  è un insieme finito.
2. Esistono  $h_1, \dots, h_k \in H$  senza fattori comuni.
3.  $s, s + 1 \in H$  per qualche  $s \in \mathbb{N}$ .

*Dimostrazione.* [1  $\Rightarrow$  2] È evidente. [2  $\Rightarrow$  3] Se  $h_1, \dots, h_k \in H$  sono senza fattori comuni, allora esistono interi  $a_1, \dots, a_k$  tali che  $a_1 h_1 + \dots + a_k h_k = 1$ . Abbiamo dunque

$$s := \sum_{i=1}^k \max(0, -a_i) h_i \in H,$$

$$s + 1 = s + \sum_{i=1}^k a_i h_i = \sum_{i=1}^k \max(0, a_i) h_i \in H.$$

[3  $\Rightarrow$  1] Se  $h \geq s^2 - s$  possiamo scrivere  $h = as + r$  con  $a \geq s - 1$  e  $r \leq s - 1$ . Dunque  $h = (a - r)s + r(s + 1) \in H$ .  $\square$

*Esempio 7.5.4.* Se  $\alpha: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}\{t\}$  è un arco, allora il sottoinsieme

$$H = \{\nu(\alpha(f)) \in \mathbb{N} \mid f \in \mathbb{K}\{x_1, \dots, x_n\}\}$$

delle molteplicità degli elementi dell'immagine di  $\alpha$  è un semigruppato.

**Lemma 7.5.5.** *Siano  $g, f \in \mathbb{K}\{t\}$  serie di molteplicità positiva con  $f \neq 0$  e si considerino gli archi  $\alpha, \beta: \mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{t\}$  definiti da  $\alpha = (f, g)$  e  $\beta = (f, fg)$ . Allora  $\alpha$  è primitivo se e solo se  $\beta$  è primitivo.*

*Dimostrazione.* Osserviamo che  $\beta$  è la composizione di  $\alpha$  con l'omomorfismo di anelli  $\mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{x, y\}$  dato da  $x \mapsto x$  e  $y \mapsto xy$ ; in particolare l'immagine di  $\alpha$  contiene l'immagine di  $\beta$  e quindi, se  $\beta$  è primitivo, allora anche  $\alpha$  è primitivo.

Viceversa, se  $\alpha$  è primitivo, allora esiste un intero  $a > 0$  tale che  $\alpha(y^a) = \alpha(xp)$  per qualche  $p$  appartenente all'ideale massimale di  $\mathbb{K}\{x, y\}$  e dunque  $y^a - xp$  appartiene al nucleo di  $\alpha$ . Se  $m = \nu(f)$  e  $(t^N)$  è contenuto nell'immagine di  $\alpha$ , dimostriamo che  $(t^{N+am})$  è contenuto nell'immagine di  $\beta$ . Sia  $h = f^a h_1$ , con  $h_1 \in (t^N)$ , e sia  $h_1 = \alpha(q)$ ; per il teorema di divisione si ha  $q = q_1(y^a - xp) + r$ , con  $r$  polinomio in  $y$  di grado  $< a$ . Siccome  $\alpha(\phi(x)y^b)$  appartiene all'immagine di  $\beta$ , se la molteplicità di  $\phi$  è almeno  $b$ , allora si ha che  $h = \alpha(x^a q) = \alpha(x^a r)$  appartiene all'immagine di  $\beta$ .  $\square$

**Teorema 7.5.6.** *Un arco  $\alpha: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}\{t\}$  è primitivo se e solo se esistono  $g_1, \dots, g_k \in \mathbb{K}\{x_1, \dots, x_n\}$  tali che le molteplicità  $\nu(\alpha(g_1)), \dots, \nu(\alpha(g_k))$  non hanno fattori comuni.*

*Dimostrazione.* La condizione è chiaramente necessaria. Viceversa, per il Lemma 7.5.3 esistono  $p, q \in \mathbb{K}\{x_1, \dots, x_n\}$  tali che  $\nu(\alpha(p)) = \nu(\alpha(q)) + 1$ . Scriviamo  $f = \alpha(q)$  e  $fg = \alpha(p)$  con  $g \in \mathbb{K}\{t\}$  di molteplicità 1. Basta provare che l'arco  $\beta: \mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{t\}$  definito da  $\beta(x) = f$  e  $\beta(y) = fg$  è primitivo: questo segue dal Lemma 7.5.5 assieme al fatto che ogni elemento di  $\mathbb{K}\{t\}$  può essere rappresentato come una serie di potenze in  $g$ .  $\square$

**Definizione 7.5.7.** *Diremo che due archi sono **equivalenti** se differiscono per un automorfismo del loro codominio  $\mathbb{K}\{t\}$ . Una classe di equivalenza di archi primitivi si dice un **ramo**.*

**Proposizione 7.5.8.** *Sia  $\alpha: \mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{t\}$  un arco non banale. Allora  $\text{Ker}(\alpha) = (f)$ , con  $f \in \mathbb{K}\{x, y\}$  irriducibile.*

*Dimostrazione.* Proviamo per prima cosa che  $\text{Ker}(\alpha) \neq 0$ : se  $\alpha(xy) = 0$  abbiamo finito, altrimenti per il teorema di preparazione di Weierstrass possiamo moltiplicare per degli invertibili le due serie  $\alpha(x) - x \in \mathbb{K}\{t, x\}$ ,  $\alpha(y) - y \in \mathbb{K}\{t, y\}$  e ottenere due polinomi di Weierstrass  $f(x, t) \in \mathbb{K}\{x\}[t]$ ,  $g(y, t) \in \mathbb{K}\{y\}[t]$  in  $t$  tali che  $f(\alpha(x), t) = 0$  e  $g(\alpha(y), t) = 0$ . Il risultante  $R(f, g) \in \mathbb{K}\{x, y\} \cap (f, g)$  appartiene al nucleo di  $\alpha$ ; dato che  $f(x, 0)$ ,  $g(y, 0)$  non hanno fattori comuni in  $\mathbb{K}\{x, y\}$ , segue che  $f$  e  $g$  sono relativamente primi e quindi  $R \neq 0$ . Siccome  $\text{Ker}(\alpha)$  è un ideale primo non banale esiste  $f \in \mathbb{K}\{x, y\}$  irriducibile tale che  $\alpha(f) = 0$ . Supponiamo  $\alpha(g) = 0$  e proviamo che  $f$  divide  $g$ ; a meno di un cambio lineare di coordinate e di moltiplicazione per invertibili non è restrittivo assumere  $f$  e  $g$  polinomi di Weierstrass in  $y$ . Per il Lemma 7.2.6 il polinomio  $f$  è irriducibile in  $\mathbb{K}\{x\}[y]$ . Dato che  $f(0, y) = y^m$ , se fosse  $\alpha(x) = 0$  si avrebbe  $0 = \alpha(f) = \alpha(y)^m$  e quindi  $\alpha$  sarebbe banale contrariamente alle ipotesi. Dunque  $\alpha(x) \neq 0$  e la restrizione  $\alpha: \mathbb{K}\{x\} \rightarrow \mathbb{K}\{t\}$  è iniettiva. Sia  $R \in \mathbb{K}\{x\}$  il risultante di  $f$  e  $g$ : dato che  $\alpha(R) = 0$ , si ha  $R = 0$  e quindi  $f$  divide  $g$ .  $\square$



**Definizione 7.5.9.** Sia  $f \in \mathbb{K}\{x, y\}$  una serie irriducibile e  $\alpha: \mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{t\}$  un arco non banale. Diremo che  $\alpha$  è una **parametrizzazione** di  $f$  se  $\alpha(f) = 0$  (e quindi per la Proposizione 7.5.8 vale  $\text{Ker}(\alpha) = (f)$ ).

Proviamo adesso che, se il campo è algebricamente chiuso, allora ogni serie irriducibile ammette una parametrizzazione irriducibile sostanzialmente unica.

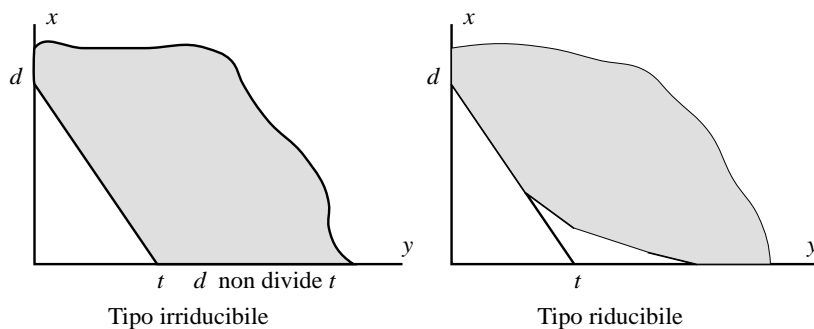
**Teorema 7.5.10.** Sia  $\mathbb{K}$  algebricamente chiuso e  $f \in \mathbb{K}\{x, y\}$  irriducibile. Esiste allora un arco primitivo  $\alpha: \mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{t\}$  tale che  $\alpha(f) = 0$ . Ogni altro arco  $\beta$  tale che  $\beta(f) = 0$  è la composizione di  $\alpha$  e di un endomorfismo di  $\mathbb{K}\{t\}$ ; esiste quindi una bigezione naturale tra l'insieme dei rami e l'insieme degli elementi irriducibili di  $\mathbb{K}\{x, y\}$ .

*Dimostrazione.* Induzione sulla molteplicità  $d = \nu(f)$  della serie  $f$ . Se  $d = 1$ , allora a meno di un cambio lineare di coordinate e per il teorema di preparazione di Weierstrass si ha

$$f(x, y) = (x - \phi(y))e(x, y), \quad e(0) \neq 0.$$

Un arco primitivo  $\alpha$  che annulla  $f$  è quindi dato da  $\alpha(x) = \phi(t)$ ,  $\alpha(y) = t$ . Se  $\beta$  è un altro arco primitivo che annulla  $f$  deve essere necessariamente  $\beta(x) = \phi(\beta(y))$  e quindi  $\beta$  è la composizione di  $\alpha$  e del morfismo  $\mathbb{K}\{t\} \rightarrow \mathbb{K}\{t\}$  dato da  $t \rightarrow \beta(y)$ . Si assuma adesso  $d > 0$  ed il teorema vero per serie irriducibili di molteplicità minore di  $d$ . A meno di un cambio lineare di coordinate e per il teorema di preparazione possiamo assumere

$$f(x, y) = x^d + \phi_1(y)x^{d-1} + \cdots + \phi_d(y), \quad \nu(\phi_i) \geq i, \quad \phi_d \neq 0$$



**Figura 7.2.**

*Asserzione:* A meno di un cambio di coordinate del tipo  $x \mapsto x - \psi(y)$ ,  $\psi \in \mathbb{K}[y]$ ,  $\psi(0) = 0$ ,  $y \mapsto y$  possiamo supporre che il poligono di Newton di  $f$  abbia una delle due forme illustrate nella Figura 7.2.

*Dimostrazione.* Si osservi innanzitutto che se  $r(y)$  è una serie di potenze di molteplicità sufficientemente alta il poligono di Newton di  $f$  è invariante per il cambio di coordinate  $x \mapsto x - r(y)$ ,  $y \mapsto y$  e quindi non è restrittivo provare l'esistenza di  $\psi$  come serie di potenze di molteplicità positiva. Dividiamo la dimostrazione in due casi.

1) La caratteristica di  $\mathbb{K}$  non divide  $d$ . A meno di sostituire  $x$  con  $x - \frac{\phi_1(y)}{d}$  si può supporre

$$f(x, y) = x^d + \phi_2(y)x^{d-2} + \cdots + \phi_d(y), \quad \nu(\phi_i) \geq i.$$

Essendo  $f$  irriducibile e  $d > 1$  deve essere  $\phi_d \neq 0$ . Se  $d$  non divide la molteplicità di  $\phi_d$  abbiamo finito. Se invece  $\nu(\phi_d) = ds$ , essendo  $\mathbb{K}$  algebricamente chiuso esiste un cambio

di coordinate del tipo  $x \mapsto x - ay^s$ ,  $a \in \mathbb{K}$ ,  $a \neq 0$ , che rende il poligono di Newton di tipo riducibile con  $t = ds$ .

2) Il campo  $\mathbb{K}$  ha caratteristica  $p > 0$  e  $p|d$ . Si consideri l'insieme  $E$  delle coppie  $(a, b)$  tali che il monomio  $x^{d-a}y^b$  compare in  $f$  con coefficiente non nullo e tali che  $a, b, p$  siano senza fattori comuni. Se  $E = \emptyset$  allora  $f$  sarebbe una potenza  $p$ -esima e quindi  $E \neq \emptyset$ . Ordiniamo  $E$  secondo l'ordinamento lessicografico:  $(a, b) < (c, d)$  se e solo se  $a < c$  oppure  $a = c$  e  $b < d$ . Sia  $(A, B)$  il punto di minimo di  $E$ . Proviamo adesso che  $(A, B)$  è invariante per cambi di coordinate del tipo  $x \mapsto x + g(y)$ ,  $y \mapsto y$ . Infatti se  $a < A$  allora  $\phi_a(y)x^{d-a}$  è una potenza  $p$ -esima e quindi  $\phi_a(y)(x + g(y))^{d-a}$  non contiene il monomio  $x^{d-A}y^B$ . Si assuma che il poligono di Newton non sia né di tipo irriducibile né di tipo riducibile, allora esiste  $0 < s \leq \frac{B}{A}$  tale che  $\nu(\phi_d) = ds$ . Con un cambio di coordinate di tipo  $x \mapsto x + ay^s$  si può aumentare la molteplicità di  $\phi_d$ . Se ancora non va bene si ripete il procedimento (con un  $s' > s$ ); la limitazione  $As \leq B$  implica che il procedimento finisce dopo un numero finito di passi.  $\square$

Ritorniamo alla dimostrazione del teorema. Si assuma il poligono di Newton di tipo riducibile o irriducibile e sia  $t \in \mathbb{Q}$  il punto di intersezione dell'asse delle ascisse con il prolungamento del primo segmento del poligono (vedi figura). Detta  $s \geq 1$  la parte intera di  $\frac{t}{d}$  si può considerare lo scoppiamento di  $f$  definito da

$$\tilde{f}(x, y) = \frac{f(xy^s, y)}{y^{ds}} \in \mathbb{K}\{y\}[x].$$

La molteplicità di  $\tilde{f}$  è chiaramente  $> 0$  e  $< d$ , per poter applicare l'ipotesi induttiva occorre dimostrare la seguente:

*Asserzione:  $\tilde{f}$  è irriducibile.*

*Dimostrazione.* Si assuma per assurdo che  $\tilde{f}$  abbia un fattore irriducibile  $g$  di molteplicità strettamente minore. Essendo  $g(x, 0) \neq 0$  non è restrittivo supporre  $g$  polinomio di Weierstrass. Per il Lemma 7.2.5 si ha  $\tilde{f} = gh$  con  $h$  polinomio. Detti  $a, b$  i gradi dei polinomi  $g, h$  rispettivamente si ha  $a + b = d$  e quindi

$$f(x, y) = y^{as}g\left(\frac{x}{y^s}, y\right)y^{bs}h\left(\frac{x}{y^s}, y\right)$$

contraddicendo la irriducibilità di  $f$ .  $\square$

Per induzione esiste un arco primitivo  $\alpha = (\alpha_1(t), \alpha_2(t))$  tale che  $\tilde{f}(\alpha_1(t), \alpha_2(t)) = 0$  con  $\alpha_2 \neq 0$ . Chiaramente  $f(\alpha_1\alpha_2^s(t), \alpha_2(t)) = 0$  e per il Lemma 7.5.5 l'arco  $(\alpha_1\alpha_2^s(t), \alpha_2(t))$  è primitivo. Se  $f(\beta_1(t), \beta_2(t)) = 0$  allora deve essere  $\nu(\beta_1) \geq s\nu(\beta_2)$  e quindi  $\gamma = \beta_1\beta_2^{-s} \in \mathbb{K}\{t\}$  e  $\tilde{f}(\gamma(t), \beta_2(t)) = 0$ . Per l'ipotesi induttiva l'arco  $\beta$  è la composizione di  $\alpha$  e di un endomorfismo di  $\mathbb{K}\{t\}$ .  $\square$

In caratteristica 0 il Teorema 7.5.10 poteva essere più facilmente dimostrato utilizzando il teorema di Newton-Puiseux. La dimostrazione riportata ha tuttavia il pregio di mostrare direttamente che ogni serie irriducibile  $f \in \mathbb{K}\{x, y\}$  si trasforma in una serie di molteplicità 1 mediante un numero finito di cambi di coordinate e scoppiamenti (Teorema di Hamburger-Weierstrass (1871)).

**Lemma 7.5.11 (Lemma della scelta degli archi<sup>2</sup>).** *Sia  $\mathbb{K}$  un campo algebricamente chiuso,  $\mathfrak{p} \subset \mathbb{K}\{x_0, \dots, x_n\}$  un ideale primo e  $h \notin \mathfrak{p}$ . Esiste allora un arco  $\alpha: \mathbb{K}\{x_0, \dots, x_n\} \rightarrow \mathbb{K}\{t\}$  tale che  $\alpha(\mathfrak{p}) = 0$  e  $\alpha(h) \neq 0$ .*

<sup>2</sup> Tentativo non troppo soddisfacente di tradurre il corrispondente termine inglese *curve selection lemma*.

*Dimostrazione.* Induzione su  $n$ , se  $n = 0$  gli unici ideali primi di  $\mathbb{K}\{x_0\}$  sono  $\mathfrak{p} = 0$  e  $\mathfrak{p} = (x_0)$ ; basta quindi prendere nel primo caso l'arco identità e nel secondo caso l'arco banale. L'anello  $\mathbb{K}\{x_0, \dots, x_n\}$  è Noetheriano e quindi l'ideale  $\mathfrak{p}$  è generato da un numero finito  $f_1, \dots, f_r$  di serie. A meno di un generico cambio lineare di coordinate e moltiplicazione per invertibili possiamo supporre  $h, f_1, \dots, f_r$  polinomi di Weierstrass rispetto alla variabile  $x_n$ . Denotiamo  $\mathfrak{q} = \mathfrak{p} \cap \mathbb{K}\{x_0, \dots, x_{n-1}\}$ ; per il Teorema 4.1.9 esiste  $g \in \mathfrak{p} \cap \mathbb{K}\{x_0, \dots, x_{n-1}\}[x_n]$  tale che  $R(h, g) \notin \mathfrak{q}$ , essendo  $R(h, g)$  il risultante dell'eliminazione di  $x_n$ . Per l'ipotesi induttiva esiste un arco  $\beta: \mathbb{K}\{x_0, \dots, x_{n-1}\} \rightarrow \mathbb{K}\{s\}$  tale che  $\beta(\mathfrak{q}) = 0$  e  $\beta(R(h, g)) \neq 0$ . È chiaro che le serie  $F_i(s, x_n) = f_i(\beta(x_0), \dots, \beta(x_{n-1}), x_n) \in \mathbb{K}\{s\}[x_n]$  sono ancora polinomi di Weierstrass nella variabile  $x_n$  e, dato che  $\beta$  annulla tutti i risultanti  $R(f_1, \sum a_j f_j)$ ,  $a_j \in \mathbb{K}$ , esiste un fattore irriducibile  $F \in \mathbb{K}\{s\}[x_n]$  che divide tutti gli  $F_i$ . L'arco  $\beta$  si estende naturalmente ad un omomorfismo locale di  $\mathbb{K}$ -algebre  $\beta: \mathbb{K}\{x_0, \dots, x_n\} \rightarrow \mathbb{K}\{s, x_n\}$  e, dato che  $g \in \mathfrak{p} = (f_1, \dots, f_r)$  abbiamo che  $F$  divide  $g(\beta(x_0), \dots, \beta(x_{n-1}), x_n)$  in  $\mathbb{K}\{s, x_n\}$  e quindi, siccome  $F$  è preparato in forma di Weierstrass lo divide pure in  $\mathbb{K}\{s\}[x_n]$ ; d'altra parte  $F$  non divide  $h(\beta(x_0), \dots, \beta(x_{n-1}), x_n)$ , altrimenti l'arco  $\beta$  annullerebbe il risultante  $R(h, g)$ . Se  $\gamma: \mathbb{K}\{s, x_n\} \rightarrow \mathbb{K}\{t\}$  è una parametrizzazione di  $F$ , vale  $\gamma(h(\beta(x_0), \dots, \beta(x_{n-1}), x_n)) \neq 0$  e basta quindi prendere  $\alpha$  come la composizione si  $\gamma$  e di  $\beta$ .  $\square$

### Esercizi

**7.17.** Sia  $f \in \mathbb{K}\{x, y\}$ . Provare che se  $\nu(f(0, y)) = n$ , allora  $\mathbb{K}\{x, y\}/(f)$  è un  $\mathbb{K}\{x\}$ -modulo libero di rango  $n$ . (Sugg.: teorema di divisione.)

**7.18.** Sia  $\alpha: \mathbb{K}\{x\} \rightarrow \mathbb{K}\{t\}$  un arco e sia  $n = \nu(\alpha(x))$ . Provare che, tramite  $\alpha$ ,  $\mathbb{K}\{t\}$  è un  $\mathbb{K}\{x\}$ -modulo libero di rango  $n$ . In particolare  $\alpha$  è un isomorfismo se e solo se  $n = 1$ .

**7.19.** Si consideri l'arco  $\alpha: \mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{t\}$  definito da

$$\alpha(x) = t^n, \quad \alpha(y) = \sum a_i t^i.$$

Dimostrare che se la caratteristica di  $\mathbb{K}$  non divide  $n$ , allora  $\alpha$  è primitivo se e solo se esistono indici  $h_1, \dots, h_k$  tali che  $a_{h_i} \neq 0$  per ogni  $i$  ed i  $k + 1$  numeri  $n, h_1, \dots, h_k$  non hanno fattori comuni. (Sugg.: induzione su  $\text{GCD}(n, \nu(\alpha(y)))$ .)

**7.20.** Per un arco  $\alpha: \mathbb{K}\{x_1, \dots, x_n\} \rightarrow \mathbb{K}\{t\}$  le seguenti affermazioni sono equivalenti:

1.  $\alpha$  è primitivo.
2. Il conucleo di  $\alpha$  è uno spazio vettoriale di dimensione finita.
3. Detto  $\mathfrak{m}$  l'ideale massimale di  $\mathbb{K}\{x_1, \dots, x_n\}$ , per ogni  $s > 0$  esiste un ideale non banale di  $\mathbb{K}\{t\}$  contenuto in  $\alpha(\mathfrak{m}^s)$ .

**7.21.** Sia  $\mathbb{K}$  un campo, provare che l'arco  $\alpha: \mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{t\}$ ,  $\alpha(x) = t^2 + t^3$ ,  $\alpha(y) = t^4$  è primitivo. (Sugg.: trattare separatamente il caso in cui  $\mathbb{K}$  ha caratteristica 2 e applicare il Teorema 7.5.6.)

**7.22 (Teorema degli zeri di Rückert).** Sia  $\mathbb{K}$  campo algebricamente chiuso, per ogni ideale  $I \subset \mathbb{K}\{x_0, \dots, x_n\}$  sia

$$\text{Arc}(I) = \{ \text{archi } \phi: \mathbb{K}\{x_0, \dots, x_n\} \rightarrow \mathbb{K}\{t\} \mid \phi(I) = 0 \}.$$

Provare che  $\text{Arc}(I) = \text{Arc}(J)$  se e solo se  $\sqrt{I} = \sqrt{J}$ . (Sugg.: Lemma 7.5.11.)

## 7.6 Esercizi complementari

**7.23.** Dimostrare che in un campo finito esiste un'unica norma (quella di 7.1.2).

**7.24.** Sia  $\mathbb{K}$  il campo delle frazioni globali di un dominio a fattorizzazione unica  $A$  e sia  $f \in A$  irriducibile. Mostrare che esiste un'unica norma su  $\mathbb{K}$  tale che  $|f| = \frac{1}{2}$  e  $|g| = 1$  per ogni  $g \in A$  non divisibile per  $f$ .

**7.25.** Mostrare che il completamento  $p$ -adico di  $\mathbb{Q}$  possiede infinite componenti connesse.

**7.26.** Sia  $|\cdot|$  una norma su  $\mathbb{Q}$  tale che  $|p| \leq 1$  per qualche primo  $p > 1$ . Dimostrare che  $|q| \leq 1$  per ogni numero intero. Provare inoltre che, se  $|p| < 1$  e  $p$  non divide  $q$ , allora  $|q| = 1$ . (Sugg.: scrivere  $q^n$  in base  $p$  e fare tendere  $n \rightarrow +\infty$ .)

**7.27 (Criterio valutativo di convergenza, (\*)).** Sia  $(\mathbb{K}, |\cdot|)$  un campo completo di caratteristica 0 contenente tutte le radici di 1. Dimostrare che una serie  $f \in \mathbb{K}[[x_1, \dots, x_s]]$  è convergente se e solo se per ogni  $\alpha_1, \dots, \alpha_s \in \mathbb{K}$ , la serie  $f(\alpha_1 t, \dots, \alpha_s t) \in \mathbb{K}[[t]]$  è convergente. (Sugg.: dimostrare nell'ordine i seguenti 6 punti:

a) (Formula di Cauchy). Sia  $P \in \mathbb{K}[x_1, \dots, x_s]$  un polinomio di grado  $\leq n$ ,  $p > n$  un numero primo e sia  $G \subset \mathbb{K}^*$  il sottogruppo delle radici  $p$ -esime di 1.

Se  $P = \sum a_I x^I$ , allora per ogni multiindice  $I = (i_1, \dots, i_s)$  tale che  $p > |i_1| + \dots + |i_s|$  vale

$$a_I = \frac{1}{p^s} \sum_{\epsilon \in G^s} \frac{P(\epsilon)}{\epsilon^I}.$$

b) Se  $P = \sum_{|I|=n} a_I x^I$  è un polinomio omogeneo di grado  $n$ , allora per ogni  $v \in \mathbb{K}$  ed ogni  $t \in \mathbb{K}^*$  vale

$$a_I = \frac{1}{t^n p^s} \sum_{\epsilon \in G^s} \frac{P(v + t\epsilon)}{\epsilon^I}.$$

c) Sia  $\{f_n\} \subset \mathbb{K}[x_1, \dots, x_s]$  una successione di polinomi, con  $f_n$  omogeneo di grado  $n$ .

Se  $\{f_n\}$  è uniformemente limitata in un aperto di  $\mathbb{K}^n$ , allora esiste una costante  $C > 0$  tale che per ogni  $n$  e per ogni coefficiente  $a$  di  $f_n$  vale  $|a| \leq C^n$ .

d) Sia  $f = \sum f_n \in \mathbb{K}[[x_1, \dots, x_s]]$  una serie non convergente. Per ogni  $R > 0$  sia

$$V_R = \{\alpha \in \mathbb{K}^n \mid \text{esiste } n \text{ tale che } |f_n(\alpha)| \geq R^n\}.$$

Provare che  $V_R$  è un aperto denso.

e) Usare il teorema di Baire per dedurre che  $\cap_R V_R \neq \emptyset$ .

f) Il teorema è generalmente falso se il campo  $\mathbb{K}$  non è completo. Ad esempio si provi che se  $\mathbb{K}$  è numerabile allora esiste  $f \in \mathbb{K}[[x, y]]$  non convergente tale che  $f(at, bt)$  è un polinomio in  $t$  per ogni  $a, b \in \mathbb{K}$ .

**7.28.** Sia  $p(y_1, \dots, y_s, x) \in \mathbb{C}\{y_1, \dots, y_s\}[x]$  un polinomio monico in  $x$  e sia  $\phi(y_1, \dots, y_s) \in \mathbb{C}[[y_1, \dots, y_s]]$  tale che  $p(y_1, \dots, y_s, \phi(y)) = 0$ . Dimostrare che la serie  $\phi$  è convergente.

**7.29.** Dimostrare che l'algebra delle serie convergenti  $\mathbb{C}\{x_1, \dots, x_n\}$  è integralmente chiusa nell'algebra delle serie formali  $\mathbb{C}[[x_1, \dots, x_n]]$ . (Sia data un'inclusione di anelli  $A \subset B$ . Allora  $A$  si dice integralmente chiuso in  $B$  se coincide con l'insieme degli elementi di  $B$  che sono radici di un polinomio monico a coefficienti in  $A$ , vedi ad esempio [AM1969, Cap. 5]).

**7.30 (Polinomi di Hermite).** Dato un polinomio  $f \in \mathbb{R}[x]$ , denotiamo con  $f^{(i)}$  la sua derivata  $i$ -esima rispetto a  $x$ . Per ogni intero positivo  $n$  e per ogni numero primo  $p > n$  siano

$$f_{n,p}(x) = \frac{x^{p-1}}{(p-1)!} \prod_{h=1}^n (h-x)^p, \quad F_{n,p}(x) = \sum_{i \geq 0} f_{n,p}^{(i)}(x) \in \mathbb{Q}[x].$$

Si noti che  $F_{n,p} - F'_{n,p} = f_{n,p}(x)$ . Si provi che:

1.  $F_{n,p}(0)$  è un intero non divisibile per  $p$ .
2. Per ogni  $h = 1, \dots, n$ , il numero intero  $F_{n,p}(h)$  è divisibile per  $p$ .
3. Sia  $x \in \mathbb{R}$ , allora

$$F_{n,p}(x) = \sum_{h=0}^{+\infty} \sum_{j=0}^h \frac{x^j}{j!} f_{n,p}^{(h)}(0).$$

(Sugg.: sviluppo di Taylor.)

**7.31 (La trascendenza di  $e$ ).** Nelle stesse notazioni dell'Esercizio 7.30 e con  $\|\cdot\|$  la norma usuale in  $\mathbb{C}$ . La serie esponenziale è data da

$$e^x = \sum_{h \geq 0} \frac{x^h}{h!} \in \mathbb{C}\{x\}.$$

Per ogni  $f = \sum a_i x^i \in \mathbb{R}[x]$  poniamo  $\|f\| = \sum |a_i|$ . Si provi:

1.  $|f^{(i)}(0)| \leq i! \|f\|$ .
2.  $\|f^i\| \leq \|f\|^i$ .
3. Per ogni  $n$  fissato esiste una costante  $C$  tale che  $\|f_{n,p}\| \leq \frac{C^p}{(p-1)!}$ .
4. Per ogni  $n$  fissato e per ogni  $h = 1, \dots, n$ , vale

$$\lim_{p \rightarrow +\infty} (F_{n,p}(h) - e^h F_{n,p}(0)) = 0.$$

(Sugg.: scrivere lo sviluppo in serie di  $e$  e usare il punto 3) dell'Esercizio 7.30.)

Dal punto 4) e dall'Esercizio 7.30 si può facilmente dedurre che  $e$  è trascendente. Sia infatti per assurdo  $a_0 + a_1 e + \dots + a_n e^n = 0$  con  $a_i \in \mathbb{Z}$ ; si ponga  $F_p = F_{n,p}$  e si consideri il limite per  $p \rightarrow +\infty$  di

$$\sum_{h=1}^n a_h (F_p(h) - e^h F_p(0)) \equiv a_0 F_0(p) \pmod{p}.$$

**7.32 (Le algebre ombra).** Sia  $\mathbb{K}$  un campo e  $\mathcal{P}$  lo spazio vettoriale di tutte le applicazioni lineari  $\mathbb{K}[x] \rightarrow \mathbb{K}$ . Allora esiste un isomorfismo naturale di  $\mathbb{K}$ -spazi vettoriali

$$\Phi: \mathcal{P} \rightarrow \mathbb{K}[[t]], \quad \Phi(L) = \sum_n L(x^n) t^n.$$

Tramite  $\Phi$  lo spazio vettoriale  $\mathcal{P}$  acquista una struttura di  $\mathbb{K}$ -algebra detta *algebra ombra*<sup>3</sup> e su tale circostanza si basa il calcolo ombra. Si assuma adesso il campo  $\mathbb{K}$  normato. I sottoinsiemi  $B(p, r, \epsilon) \subset \mathbb{K}[x]$ ,  $p \in \mathbb{K}[x]$ ,  $r, \epsilon > 0$

$$B(p, r, \epsilon) = \{q \mid \|q - p\|_r < \epsilon\}$$

sono una base per una topologia su  $\mathbb{K}[x]$ . Detto  $B_\delta \subset \mathbb{K}$  la palla di centro 0 e raggio  $\delta$ , un funzionale  $L \in \mathcal{P}$  è continuo se e solo se per ogni  $\delta > 0$  esistono  $\epsilon, r$  tali che  $L(B(0, r, \epsilon)) \subset B_\delta$ . Tramite l'isomorfismo  $\Phi$  le serie convergenti corrispondono ai funzionali continui.

<sup>3</sup> in inglese umbral algebra

**7.33.** Si interpreti il teorema degli zeri di Rückert (Esercizio 7.22) nella teoria dei germi di spazi complessi, vedi [GR1965].

**7.34 (\*)**. Sia  $\mathbb{K}$  un campo algebricamente chiuso di caratteristica 0, siano  $f, g \in \mathbb{K}\{x, y\}$  due serie di molteplicità positiva e sia  $J = f_x g_y - f_y g_x$  il determinante Jacobiano. Dimostrare che se  $J = 0$ , allora  $f$  e  $g$  hanno gli stessi fattori irriducibili (con molteplicità possibilmente diverse). Mostrare con un esempio che il viceversa è generalmente falso.

**7.35.** Sia  $H \subset \mathbb{N}$  un semigruppone contenente 0 e siano  $n_1 < n_2 < n_3 < \dots$  gli elementi di  $\mathbb{N} \setminus H$ . Provare che  $n_i \leq 2i - 1$  per ogni  $i$ . Dedurre che se  $\mathbb{N} \setminus H$  contiene  $g$  elementi, allora vale

$$\frac{g(g+1)}{2} \leq \sum_{n \notin H} n \leq g^2.$$

(Sugg.: se  $n_i \geq 2i$  considerare le coppie  $(j, n_i - j)$ , per  $j = 1, \dots, i$ .)

**7.36.** Sia  $\{a_n \mid n \in \mathbb{N}\}$  una successione di numeri reali non negativi tale che

$$a_{n+m} \leq \frac{1}{2}(a_n + a_m)$$

per ogni  $n, m \in \mathbb{N}$ . Dimostrare che tale successione è convergente. (Sugg.: Sia  $l$  il minimo limite della successione; provare che per ogni  $\epsilon > 0$  l'insieme  $H_\epsilon = \{n \mid a_n \leq l + \epsilon\}$  è un semigruppone cofinito.)

**7.37.** Nelle notazioni della Sezione 7.2. Dimostrare che se  $(\mathbb{K}, | \cdot |)$  è completo, allora  $(B_r, \| \cdot \|_r)$  è uno spazio di Banach per ogni multiraggio  $r$ .

**7.38 (\*)**. Provare che per ogni  $r > 0$ , l'anello  $B_r \subset \mathbb{C}\{x\}$  non è a fattorizzazione unica. (Sugg.: mostrare che esiste una catena non stazionaria di ideali principali.)

**7.39 (\*)**. Siano  $f, g \in \mathbb{K}\{x, t\}$  senza fattori comuni: dimostrare che il  $\mathbb{K}$ -spazio vettoriale  $\mathbb{K}\{x, t\}/(f, g)$  ha dimensione finita. (Sugg.: ridursi al caso  $f, g$  polinomi di Weierstrass e quindi mostrare che esiste  $N > 0$  tale che  $x^N, t^N$  appartengono all'ideale  $(f, g)$ .)

**7.40 (\*\*?)**. In caratteristica 0, se  $f \in \mathbb{K}\{x_1, \dots, x_n\}$  è irriducibile, allora  $f$  è ancora irriducibile in  $\mathbb{K}[[x_1, \dots, x_n]]$ . (Sugg.: una dimostrazione possibile utilizza il teorema di Artin [Art1968] sulla soluzione delle equazioni analitiche.)

**7.41.** Siano  $f, h \in \mathbb{K}[x_0, \dots, x_n]$  con  $h$  irriducibile e  $h(0) = f(0) = 0$ . Dimostrare che se  $h$  divide  $f$  in  $\mathbb{K}\{x_0, \dots, x_n\}$ , allora lo divide in  $\mathbb{K}[x_0, \dots, x_n]$ . (Sugg.: non è restrittivo assumere  $\mathbb{K}$  algebricamente chiuso; a meno di un cambio lineare di coordinate si può supporre  $h(0, \dots, 0, x_n) \neq 0$ . Usare il lemma di Hensel, il Lemma 7.2.5 e le proprietà del risultante.)

*Osservazione 7.6.1.* L'Esercizio 7.41 è un caso particolare di un Teorema di Krull (vedi Sezione 15.5).

**7.42.** Sia  $\mathbb{K}$  un campo di caratteristica 0 e siano  $h, f, g \in \mathbb{K}[x, y]$  con  $h$  irriducibile,  $h(0) = f(0) = 0$ ,  $h_y(0) \neq 0$  e  $g(0) = 1$ . Dimostrare che se  $h$  divide i polinomi  $fg_x - gf_x$  e  $fg_y - gf_y$ , allora  $h$  divide  $f$ . (Sugg.: usare l'Esercizio 7.41.)

### Esercizi sulle algebre analitiche locali

Sia  $\mathbb{K}$  un campo normato fissato (infinito). Una  **$\mathbb{K}$ -algebra analitica locale** è una  $\mathbb{K}$ -algebra isomorfa ad un quoziente di un'algebra di serie di potenze convergenti. Si noti che ogni  $\mathbb{K}$ -algebra analitica locale è un anello locale Noetheriano con campo residuo uguale a  $\mathbb{K}$ . Una  $\mathbb{K}$ -algebra analitica locale si dice **liscia** se è isomorfa a  $\mathbb{K}\{x_1, \dots, x_n\}$  per qualche  $n$ .

**7.43.** Provare che ogni algebra analitica è isomorfa a  $\mathbb{K}\{x_1, \dots, x_n\}/I$ , con  $I \subset \mathfrak{m}^2 = (x_1, \dots, x_n)^2$ .

**7.44.** Per ogni  $n \geq 2$  indichiamo con  $p_n: \mathbb{K}\{t\}/(t^n) \rightarrow \mathbb{K}\{t\}/(t^2)$  il morfismo di proiezione al quoziente. Provare che un'algebra analitica locale  $A$  è liscia se e solo se per ogni omomorfismo  $f: A \rightarrow \mathbb{K}\{t\}/(t^2)$  e per ogni  $n \geq 2$  esiste un omomorfismo  $g: A \rightarrow \mathbb{K}\{t\}/(t^n)$  tale che  $f = p_n g$ . (Sugg.: Esercizio 7.43.)

**7.45.** Siano  $A$  e  $B$  due  $\mathbb{K}$ -algebre analitiche locali con ideali massimali  $\mathfrak{m} \subset A$  e  $\mathfrak{n} \subset B$ . Sia  $f: A \rightarrow B$  un omomorfismo locale e denotiamo con  $f': \mathfrak{m}/\mathfrak{m}^2 \rightarrow \mathfrak{n}/\mathfrak{n}^2$  l'applicazione indotta. Provare:

- $f$  è surgettivo se e solo se  $f'$  è surgettivo.
- Se  $B$  è liscia e  $f'$  è iniettivo allora anche  $f$  è iniettivo.

**7.46 (Lemma di Cartan).** Siano  $g_1, \dots, g_n \in \mathbb{K}\{x_1, \dots, x_n\}$  serie la cui matrice Jacobiana in 0 è la matrice identità: questo significa che per ogni  $i = 1, \dots, n$  si può scrivere  $g_i = x_i + \hat{g}_i$ , con  $\hat{g}_i \in \mathfrak{m}^2$ . Sia  $\phi$  l'automorfismo di  $\mathbb{K}\{x_1, \dots, x_n\}$  dato da  $\phi(f)(x_1, \dots, x_n) = f(g_1(x), \dots, g_n(x))$ . Provare:

1. Se il campo  $\mathbb{K}$  ha caratteristica 0 e  $\phi^d = Id$  per qualche  $d > 0$ , allora  $\phi = Id$ .
2. Se la caratteristica di  $\mathbb{K}$  divide  $d$  il risultato del punto 1) è generalmente falso.

**7.47 (\*).** Dato un ideale  $I \subset \mathbb{K}\{x_1, \dots, x_n\}$  ed un numero naturale  $h$  si definisce  $J_h(I)$  come l'ideale generato dai determinanti minori di ordine  $h$  di tutte le matrici Jacobiane  $\left(\frac{\partial f_i}{\partial x_j}\right)$ , al variare di  $f_1, \dots, f_h \in I$ . Dimostrare:

1. La definizione dei  $J_h$  è invariante per automorfismi di  $\mathbb{K}\{x_1, \dots, x_n\}$ .
2. Se  $\mathbb{K}$  ha caratteristica 0 ed esiste  $h$  tale che  $J_{n-h}(I) = (1)$  e  $J_{n-h+1}(I) \subset I$ , allora la  $\mathbb{K}$ -algebra analitica  $\mathbb{K}\{x_1, \dots, x_n\}/I$  è isomorfa a  $\mathbb{K}\{y_1, \dots, y_h\}$ .
3. Il punto 2) è generalmente falso in caratteristica  $p > 0$ : è comunque vero sotto le stesse ipotesi che  $\mathbb{K}\{x_1, \dots, x_n\}/I$  è isomorfa a  $\mathbb{K}\{y_1, \dots, y_h\}/J$  dove  $J$  è un ideale contenuto in  $(y_1^p, \dots, y_h^p)$ .

### Esercizi sul poligono di Newton

Nei seguenti esercizi studieremo alcune proprietà del poligono di Newton  $N_f \subset [0, +\infty]^2$  di una serie  $f \in \mathbb{K}\{x, y\}$ . Per convenzione riportiamo sull'asse delle ascisse gli esponenti di  $y$  e sull'asse delle ordinate gli esponenti di  $x$ . Il campo  $\mathbb{K}$  è inoltre supposto algebricamente chiuso.

**7.48.** Siano  $e, f \in \mathbb{K}\{x, y\}$  con  $e(0) \neq 0$ . Provare che  $N_f = N_{fe}$  e dedurre che  $N_f$  dipende solo dall'ideale  $(f)$ .

In generale chiameremo poligono di Newton qualsiasi sottoinsieme convesso  $N \subset [0, +\infty]^2$  tale che  $N = N_f$  per qualche serie  $f$  di molteplicità positiva. Dato un poligono di Newton ed un suo lato  $l$  si definisce la pendenza  $0 \leq p(l) \leq \frac{\pi}{2}$  come l'angolo formato tra  $l$  e la retta verticale. Dato un poligono di Newton  $N$  è sempre possibile ordinare i suoi lati  $l_0, l_1, \dots, l_k$  in modo tale che  $0 = p(l_0) < p(l_1) < \dots < p(l_k) = \frac{\pi}{2}$ ; diremo infine che il poligono  $N$  è **preparato** se  $l_0$  e  $l_k$  sono contenuti negli assi coordinati (se  $N = N_f$  la condizione equivale a  $f(x, 0) \neq 0$  e  $f(0, y) \neq 0$ ). Dato un poligono di Newton preparato  $N$ , con lati  $l_0, \dots, l_k$ , si definisce la **pendenza minima e massima**  $\min(N) = p(l_1)$ ,  $\max(N) = p(l_{k-1})$ .

**7.49.** Siano  $N, M$  poligoni di Newton preparati con  $\max(N) < \min(M)$ . Provare che

$$N + M = \{n + m \mid n \in N, m \in M\} \subset [0, +\infty]^2$$

è ancora un poligono di Newton preparato.

**7.50.** Siano  $f, g, h \in \mathbb{K}\{x, y\}$  tali che i poligoni  $N_f, N_g$  siano preparati e  $\max(N_f) < \min(N_g)$ . Mostrare che  $N_h = N_f + N_g$  se e solo se  $N_h = N_{fg}$ .

**7.51.** Siano dati una serie  $f$  e due poligoni di Newton preparati  $N$  e  $M$  tali che  $N_f = N + M$  e  $\min(N) = \max(N) = \frac{\pi}{4} < \min(M)$ . Dimostrare che esiste  $g \in \mathbb{K}\{x, y\}$  tale che  $N_g = M$ ,  $g|f$  e  $M.C.D.(g, fg^{-1}) = 1$ . (Sugg.: usare lo scoppimento.)

**7.52.** Siano dati una serie  $f$  e due poligoni di Newton preparati  $N$  e  $M$  tali che  $N_f = N + M$  e  $\max(N) \leq \frac{\pi}{4} < \min(M)$ . Dimostrare che esiste  $g \in \mathbb{K}\{x, y\}$  tale che  $N_g = M$ ,  $g|f$  e  $M.C.D.(g, fg^{-1}) = 1$ . (Sugg.: usare il fatto che  $M$  è invariante per cambi di coordinate del tipo  $x \mapsto x, y \mapsto y + \phi(x)$  per ricondursi all'Esercizio 7.51.)

**7.53.** Sia  $\mathbb{K}$  campo infinito e  $f \in \mathbb{K}\{x, y\}$ . Dimostrare che il numero dei fattori irriducibili di  $f$  è maggiore o uguale del numero dei lati di  $N_f$  che non sono contenuti nell'unione degli assi coordinati. (Sugg.: Esercizio 7.52.)

**7.54.** Siano  $f_1, \dots, f_n \in \mathbb{K}\{x\}$  serie con molteplicità positive e strettamente crescenti, cioè  $0 < \nu(f_1) < \dots < \nu(f_n)$ . Descrivere il poligono di Newton di  $\prod_i (y - f_i(x))$ . Si raccomanda di fare almeno il caso  $n = 2$ .

**7.55 (\*).** Sia  $\mathbb{K}$  un campo di caratteristica  $\neq 2$  e  $f = y^2 - (x^a + y^b)^k \in \mathbb{K}\{x, y\}$ , con  $k, a > 0$  e  $b > 2$ . Provare che  $f$  è irriducibile se e solo se  $ak$  è dispari. (Sugg.: preparazione di Weierstrass e poligono di Newton.)



## Le singolarità delle curve piane da un punto di vista analitico

### 8.1 Ideali di Fitting

**Definizione 8.1.1.** Sia  $B = (b_{ij})$  una matrice ad  $n$  righe ed  $m$  colonne a valori in un anello  $A$ . Per ogni  $h \geq 0$  si definisce lo  $h$ -esimo **ideale di Fitting**<sup>1</sup> di  $B$  come l'ideale  $F_h(B) \subset A$  generato da tutti i determinanti minori di ordine  $(n - h)$  della matrice  $B$ . (Per convenzione, se  $j \leq 0$ , allora i determinanti minori di ordine  $j$  sono uguali a 1.)

È evidente che  $F_0(B) \subset F_1(B) \subset \cdots \subset F_n(B) = A$ . Ricordiamo che con mosse elementari su una matrice  $B$  a coefficienti in un anello  $A$  si intende una delle seguenti 6 mosse:

*Mosse elementari sulle righe:*

1. Permutare le righe.
2. Moltiplicare una riga per un invertibile di  $A$ .
3. Aggiungere ad una riga un multiplo di un'altra riga.

*Mosse elementari sulle colonne:*

1. Permutare le colonne.
2. Moltiplicare una colonna per un invertibile di  $A$ .
3. Aggiungere ad una colonna un multiplo di un'altra colonna.

Segue facilmente dalla regola di Laplace per il calcolo del determinante che gli ideali di Fitting sono invarianti per mosse elementari.

Ricordiamo che un anello  $A$  si dice **Euclideo** se è un dominio di integrità ed è definita un **funzione grado**  $d: A - \{0\} \rightarrow \mathbb{N}$  tale che:

1.  $d(a) \geq 0$  per ogni  $a \in A - \{0\}$ .
2.  $d(ab) \geq \max(d(a), d(b))$  per ogni  $a, b \in A - \{0\}$ .
3. Per ogni  $a, b \in A - \{0\}$  esistono  $p, r \in A$  tali che  $a = pb + r$ , dove  $r = 0$  oppure  $d(r) < d(b)$ .

**Teorema 8.1.2.** Sia  $A$  un anello Euclideo. Allora, mediante un numero finito di mosse elementari, è possibile trasformare ogni matrice a coefficienti in  $A$  in una matrice  $(c_{ij})$  tale che  $c_{ij} = 0$  se  $i \neq j$  e  $c_{ii} | c_{jj}$  se  $i \leq j$ .

*Inoltre i coefficienti  $c_{ii}$  sono univocamente determinati a meno di invertibili.*

*Osservazione 8.1.3.* Il Teorema 8.1.2 è vero più in generale per matrici a coefficienti in anello ad ideali principali (vedi ad esempio [Lang1984, XV.2]).

<sup>1</sup> Fitting è il nome di un matematico tedesco e non un termine inglese.

*Dimostrazione.* Sia  $B = (b_{ij})$  una matrice  $n \times m$  a coefficienti in  $A$ .

*Esistenza:* La prova dell'esistenza è costruttiva: eccone l'algoritmo.

1) A meno di permutazioni degli indici non è restrittivo assumere  $d(b_{11}) \leq d(b_{ij})$  per ogni  $i, j$ . Se  $b_{11}$  divide  $b_{ij}$  per ogni  $i, j$  (questo è vero se  $d(b_{11}) = 0$ ), allora zompriamo al punto 4, altrimenti passiamo al punto 2.

2) Se  $b_{11}$  divide  $b_{1j}$  per ogni  $j$ , allora andiamo direttamente al punto 3. Se invece  $b_{11}$  non divide  $b_{1j}$  per qualche  $j \geq 2$ , allora, aggiungendo alla  $j$ -esima colonna un opportuno multiplo della prima possiamo supporre  $d(b_{1j}) < d(b_{11})$ . Scambiamo la  $j$ -esima colonna con la prima e torniamo al punto 1.

3) Con mosse elementari di tipo 3 possiamo supporre  $b_{1j} = b_{11}$  per ogni  $j$ . Se  $b_{11}$  non divide  $b_{ij}$  per qualche  $i, j$ , con  $i > 1$ , allora, aggiungendo alla  $i$ -esima riga un opportuno multiplo della prima possiamo supporre  $d(b_{ij}) < d(b_{11})$ . Scambiamo la  $j$ -esima colonna con la prima colonna, la  $i$ -esima riga con la prima riga e torniamo al punto 1.

4) Con mosse elementari di tipo 3 possiamo supporre  $b_{1i} = b_{11} = 0$  per ogni  $i > 1$ . Restringiamoci alla sottomatrice di indici  $i, j > 1$  e ritorniamo all'inizio.

*Unicità:* Basta osservare che per ogni matrice  $(c_{ij})$  di ordine  $n \times m$ , come nell'enunciato si ha  $F_{n-h}(C) = (c_{11}c_{22} \cdots c_{hh})$  per ogni  $h \leq n$ . Adesso basta ricordarsi che gli ideali di Fitting sono invarianti per mosse elementari.  $\square$

**Corollario 8.1.4.** *Ogni matrice invertibile a coefficienti in un anello Euclideo è il prodotto di un numero finito di matrici rappresentanti mosse elementari.*

*Dimostrazione.* Basta applicare il Teorema 8.1.2 ed osservare che una matrice invertibile resta invertibile anche dopo una mossa elementare.  $\square$

**Corollario 8.1.5.** *Sia  $B$  una matrice  $n \times m$  a coefficienti in un anello Euclideo  $A$ . Allora esistono due matrici invertibili  $U_1 \in \text{GL}(n, A)$  e  $U_2 \in \text{GL}(m, A)$  tali che  $U_1 B U_2 = (c_{ij})$ , dove  $c_{ij} = 0$  se  $i \neq j$  e  $c_{ii} | c_{jj}$  se  $i \leq j$ .*

*Dimostrazione.* Basta osservare che ogni applicazione elementare sulle righe (risp.: colonne) si può ottenere moltiplicando a sinistra (risp.: destra) con una opportuna matrice invertibile.  $\square$

Il Corollario 8.1.5 viene chiamato talvolta **Teorema di Frobenius**.

Applichiamo i risultati precedenti all'anello Euclideo  $\mathbb{K}\{t\}$  attrezzato della molteplicità  $\nu$  come funzione grado. Dato un  $\mathbb{K}\{t\}$ -modulo  $M$  si definisce la **lunghezza** di  $M$  come

$$l(M) = \dim_{\mathbb{K}} M \in \mathbb{N} \cup \{+\infty\}.$$

Si noti che  $\frac{\mathbb{K}\{t\}}{(t^n)}$  ha lunghezza  $n$  e quindi per ogni  $f \in \mathbb{K}\{t\}$  vale  $l\left(\frac{\mathbb{K}\{t\}}{(f)}\right) = \nu(f)$ .

**Teorema 8.1.6.** *Siano  $A = \mathbb{K}\{t\}$  e  $\phi: A^n \rightarrow A^n$  un omomorfismo di  $A$ -moduli. Allora vale  $l(\text{Coker}(\phi)) = \nu(\det(\phi))$ , dove con  $\det(\phi)$  si intende il determinante della matrice che rappresenta  $\phi$  nella base canonica di  $A^n$ .*

*Dimostrazione.* Le mosse elementari lasciano invariati sia  $l(\text{Coker}(\phi))$  che  $\nu(\det(\phi))$ : non è quindi restrittivo dimostrare il teorema nel caso in cui  $\phi$  sia rappresentato da una matrice diagonale  $\phi = \text{diag}(a_1, \dots, a_n)$ , con  $a_i \in A$ . È chiaro che  $\nu(\det(\phi)) = \nu(a_1) + \dots + \nu(a_n)$ , che  $\text{Coker}(\phi) = A/(a_1) \oplus \dots \oplus A/(a_n)$  e quindi che  $l(\text{Coker}(\phi)) = l(A/(a_1)) + \dots + l(A/(a_n)) = \nu(a_1) + \dots + \nu(a_n)$ .  $\square$

### Esercizi

**8.1.** Sia  $A$  un anello Euclideo con funzione grado  $d$ . Dimostrare che  $A$  è un anello unitario ad ideali principali, che  $d(a) \geq d(1)$  per ogni  $a$  e che vale  $d(a) = d(1)$  se e solo se  $a$  è invertibile. (Sugg.: per ogni ideale scegliere un elemento di grado minimo. In particolare l'anello stesso è un ideale principale, diciamo  $A = (a)$ . Per la proprietà di divisione esiste  $u \in A$  tale che  $a = au$ .)

**8.2.** Sia  $A$  anello Euclideo. Dimostrare che ogni sottomodulo di  $A^n$  è libero di rango  $\leq n$ .

## 8.2 Il lemma del serpente

Il periodo 1940-1955 è stato caratterizzato da un forte sviluppo della topologia algebrica: molte idee maturate in quel periodo hanno influenzato enormemente tutta quanta la matematica degli anni a seguire. Basta citare ad esempio i concetti di Categoria e Funtore e l'utilizzo grafico delle frecce fino ad allora sconosciuto (sembra che il primo ad utilizzare una freccia per indicare un morfismo sia stato Hurewicz nel 1940: il libro di Walker [Walk1950], stampato nel 1949, è uno degli ultimi testi a non fare uso di frecce). Tra le nuove nozioni troviamo anche quella di successione esatta.

Una successione di morfismi di  $A$ -moduli

$$\cdots \longrightarrow M_n \xrightarrow{d_n} M_{n+1} \xrightarrow{d_{n+1}} M_{n+2} \longrightarrow \cdots, \quad n \in \mathbb{Z}, \quad (8.1)$$

si dice un **complesso** se  $\text{Im}(d_n) \subset \text{Ker}(d_{n+1})$  per ogni  $n$ , o equivalentemente se  $d_{n+1}d_n = 0$  per ogni  $n$ . Si dice una **successione esatta** se  $\text{Im}(d_n) = \text{Ker}(d_{n+1})$  per ogni  $n$ . Una successione esatta come in 8.1 si dice limitata se  $M_n = 0$  ad eccezione di un numero finito di interi  $n$ , mentre si dice **corta** se  $M_n = 0$  per ogni  $n \neq -1, 0, 1$ . Più familiarmente, una successione esatta corta è una successione esatta del tipo

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0.$$

Un morfismo di successioni esatte corte è un diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_1 & \longrightarrow & M_1 & \longrightarrow & P_1 & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & N_2 & \longrightarrow & M_2 & \longrightarrow & P_2 & \longrightarrow & 0, \end{array} \quad (8.2)$$

dove le righe sono successioni esatte corte. Si noti che un tale morfismo induce in modo naturale i due complessi

$$0 \longrightarrow \text{Ker}(\alpha) \longrightarrow \text{Ker}(\beta) \longrightarrow \text{Ker}(\gamma) \quad \text{e}$$

$$\text{Coker}(\alpha) \longrightarrow \text{Coker}(\beta) \longrightarrow \text{Coker}(\gamma) \longrightarrow 0.$$

**Lemma 8.2.1 (del serpente).** *Sia dato un morfismo di successioni esatte corte come in 8.2. Allora esiste un morfismo (di bordo)  $\delta: \text{Ker}(\gamma) \rightarrow \text{Coker}(\alpha)$  tale che la successione*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Ker}(\alpha) & \longrightarrow & \text{Ker}(\beta) & \longrightarrow & \text{Ker}(\gamma) \\ & & & & & & \downarrow \delta \\ & & & & & & \text{Coker}(\alpha) & \longrightarrow & \text{Coker}(\beta) & \longrightarrow & \text{Coker}(\gamma) & \longrightarrow & 0. \end{array}$$

è esatta.

*Dimostrazione.* Sia  $p \in P_1$  tale che  $\gamma(p) = 0$  e sia  $m \in M_1$  un sollevamento di  $p$ ; siccome il diagramma è commutativo, l'immagine di  $\beta(m)$  in  $P_2$  è nulla e quindi  $\beta(m) \in N_2$ . Definiamo  $\delta(p)$  come la classe di  $\beta(m)$  nel conucleo di  $\alpha$ . Lasciamo per esercizio al lettore la semplice verifica che  $\delta$  è un omomorfismo ben definito e che la successione è esatta.  $\square$

**Esercizi**

**8.3.** Sia

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & P & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & P & \longrightarrow & 0 \end{array}$$

un morfismo di successioni esatte corte di spazi vettoriali di dimensione finita su  $\mathbb{K}$ . Provare che la traccia di  $\beta$  è uguale alla somma delle tracce di  $\alpha$  e  $\gamma$ .

**8.4.** Una applicazione lineare  $\phi$  tra spazi vettoriali su un campo  $\mathbb{K}$  fissato si dice di Fredholm se  $\text{Ker}(\phi)$  e  $\text{Coker}(\phi)$  hanno dimensione finita; in tal caso si definisce l'indice  $i(\phi) = \dim \text{Coker}(\phi) - \dim \text{Ker}(\phi)$ . Sia

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_1 & \longrightarrow & M_1 & \longrightarrow & P_1 & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \longrightarrow & N_2 & \longrightarrow & M_2 & \longrightarrow & P_2 & \longrightarrow & 0 \end{array}$$

un morfismo di successioni esatte corte di spazi vettoriali su  $\mathbb{K}$ . Dimostrare che se  $\alpha$  e  $\gamma$  sono di Fredholm, allora anche  $\beta$  è di Fredholm e vale  $i(\beta) = i(\alpha) + i(\gamma)$ .

**8.5 (Lemma del 9).** Si consideri un diagramma commutativo con le colonne esatte

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & M_1 & \longrightarrow & P_1 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_2 & \xrightarrow{f} & M_2 & \xrightarrow{g} & P_2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_3 & \longrightarrow & M_3 & \longrightarrow & P_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

e si assuma che  $gf = 0$ . Provare che se due righe sono esatte allora è esatta anche la terza. (Sugg.: se la riga centrale è esatta applicare il lemma del serpente, altrimenti caccia al diagramma.)

**8.3 Definizioni alternative della molteplicità di intersezione**

Da ora in poi  $\mathbb{K}$  denoterà un campo algebricamente chiuso.

**Teorema 8.3.1.** *Siano  $f, g \in \mathbb{K}\{x\}[y]$  polinomi monici in  $y$  tali che  $f(0, y)$  e  $g(0, y)$  non abbiano radici in comune diverse da  $y = 0$ . Sia  $R = R(f, g) \in \mathbb{K}\{x\}$  il risultante di  $f$  e  $g$ , allora vale*

$$\nu(R) = \dim_{\mathbb{K}} \mathbb{K}\{x\}/(R) = \dim_{\mathbb{K}} \mathbb{K}\{x, y\}/(f, g).$$

*Dimostrazione.* Per il lemma di Hensel possiamo scrivere  $f = f_1 f_2$  e  $g = g_1 g_2$ , con  $f_i, g_i \in \mathbb{K}\{x\}[y]$ ,  $f_1$  e  $g_1$  polinomi di Weierstrass,  $f_2(0) \neq 0$  e  $g_2(0) \neq 0$ . Per ipotesi i polinomi  $f_2(0, y)$  e  $g_2(0, y)$  non hanno radici comuni e quindi i tre risultanti  $R(f_1, g_2)$ ,  $R(f_2, g_1)$  e  $R(f_2, g_2)$  sono tutti invertibili in  $\mathbb{K}\{x\}$  e  $\nu(R(f, g)) = \nu(R(f_1, g_1))$ . Essendo inoltre chiaro che  $(f, g) = (f_1, g_1) \subset \mathbb{K}\{x, y\}$  si deduce che non è restrittivo dimostrare il teorema nel caso particolare di  $f$  e  $g$  polinomi di Weierstrass. Sia  $f(0, y) = y^n$ , allora per il teorema di divisione  $\mathbb{K}\{x, y\}/(f)$  è un  $\mathbb{K}\{x\}$ -modulo libero con base canonica  $1, y, \dots, y^{n-1}$  e  $\mathbb{K}\{x, y\}/(f, g)$  è il conucleo della moltiplicazione per  $g$  in  $\mathbb{K}\{x, y\}/(f)$ . Nella base canonica la moltiplicazione per  $g$  è rappresentata dalla matrice  $m_{ij}$  i cui coefficienti soddisfano la relazione

$$y^i g = h_i f + \sum_{j=0}^{n-1} m_{ij} y^j, \quad i = 0, \dots, n-1, \quad h_i \in \mathbb{K}\{x\}[y].$$

In base a 4.1.2 il risultante di  $f$  e  $g$  è esattamente il determinante di  $m_{ij}$  e la dimostrazione si conclude usando il Teorema 8.1.6.  $\square$

**Corollario 8.3.2 (Definizione analitica della molteplicità di intersezione).** *Siano  $C$  e  $D$  due curve piane senza componenti comuni,  $p \in C \cap D$  e siano  $x, y$  coordinate affini centrate in  $p$ . Se  $f, g \in \mathbb{K}[x, y]$  sono le equazioni affini di  $C$  e  $D$  rispettivamente, allora vale*

$$\nu_p(C, D) = \dim_{\mathbb{K}} \frac{\mathbb{K}\{x, y\}}{(f, g)}.$$

*Dimostrazione.* A meno di un cambio lineare di coordinate non è restrittivo assumere che  $f$  e  $g$  soddisfano le ipotesi del Teorema 8.3.1; basta adesso ricordarsi che per definizione di molteplicità di intersezione vale  $\nu_p(C, D) = \nu(R)$ .  $\square$

È naturale estendere la molteplicità di intersezione di due curve affini ad un'applicazione

$$\nu: \mathbb{K}\{x, y\} \times \mathbb{K}\{x, y\} \rightarrow \mathbb{N} \cup \{+\infty\}, \quad \nu(f, g) = \dim_{\mathbb{K}} \frac{\mathbb{K}\{x, y\}}{(f, g)}.$$

Dato che una tale applicazione  $\nu$  è invariante per cambi analitici di coordinate e per moltiplicazione di  $f$  e  $g$  per elementi invertibili, ne segue che  $\nu$  è univocamente determinata dai valori  $\nu(f, g)$ , con  $f, g$  polinomi di Weierstrass in  $y$ . In tal caso, grazie a 8.3.1, la molteplicità di intersezione è uguale alla molteplicità del risultante. In particolare  $\nu(f, g) = +\infty$  se e solo se  $f$  e  $g$  hanno un fattore comune.

**Proposizione 8.3.3.** *L'applicazione  $\nu: \mathbb{K}\{x, y\}^2 \rightarrow \mathbb{N} \cup \{+\infty\}$  è univocamente determinata dalle seguenti proprietà:*

1.  $\nu(f, g) = \nu(g, f)$ .
2.  $\nu$  è invariante per cambi lineari di coordinate.
3.  $\nu(f, g + fh) = \nu(f, g)$  per ogni  $f, g, h \in \mathbb{K}\{x, y\}$ .
4. Se  $f \in \mathbb{K}\{x, y\}$  non è invertibile, allora  $\nu(0, f) = +\infty$ . Se  $e \in \mathbb{K}\{x, y\}$  è invertibile, allora  $\nu(e, g) = 0$  per ogni  $g$ .
5.  $\nu(x, y) = 1$ .
6.  $\nu(f, gh) = \nu(f, g) + \nu(f, h)$  per ogni  $f, g, h \in \mathbb{K}\{x, y\}$ .

*Dimostrazione.* Segue immediatamente dalla definizione e dal Teorema 8.3.1 che  $\nu$  soddisfa le condizioni 1, ..., 6. Una dimostrazione alternativa di 6 che non utilizzi la bilinearità del risultante può essere fatta osservando che, se  $f$  e  $gh$  non hanno fattori comuni, allora esiste una successione esatta corta

$$0 \longrightarrow \frac{\mathbb{K}\{x, y\}}{(f, h)} \xrightarrow{\alpha} \frac{\mathbb{K}\{x, y\}}{(f, gh)} \xrightarrow{\beta} \frac{\mathbb{K}\{x, y\}}{(f, g)} \longrightarrow 0,$$

dove  $\beta$  è la proiezione al quoziente e  $\alpha$  è indotta dalla moltiplicazione per  $g$ ; lasciamo per esercizio al lettore la verifica della esattezza. Si consideri adesso una  $\mu: \mathbb{K}\{x, y\}^2 \rightarrow \mathbb{N} \cup \{+\infty\}$  che soddisfa le condizioni 1, ..., 6 e proviamo che  $\mu = \nu$ .

Osserviamo dapprima che  $\mu(f, x) = \nu(f(0, y))$  per ogni  $f \in \mathbb{K}\{x, y\}$ . Infatti, se  $x$  divide  $f$ , allora  $f = xg$  e  $\mu(f, x) = \mu(f - xg, x) = \mu(0, x) = +\infty$ . Se invece  $x$  non divide  $f$ , allora per il teorema di preparazione si ha  $f = eh$ , con  $e$  invertibile e  $h = y^m + xh_1$  polinomio di Weierstrass in  $y$ ; dunque  $\mu(f, x) = \mu(h, x) = \mu(y^m, x) = m$ . Se  $g \in \mathbb{K}\{x\}$  è una serie di molteplicità  $d = \nu(g)$ , si può scrivere  $g = x^d g_1$  con  $g_1$  invertibile e quindi  $\mu(f, g) = \nu(g)\nu(f(0, y))$ . In generale siano  $f, g \in \mathbb{K}\{x, y\}$ , allora a meno di un cambio lineare di coordinate e moltiplicazione per invertibili non è restrittivo supporre  $f$  e  $g$  polinomi di Weierstrass in  $y$  con  $\deg f \leq \deg g$ . Proviamo per induzione sul grado di  $f$  che  $\mu(f, g) = \nu(f, g)$ . Per il teorema di divisione si ha  $g = fh + r$ , con  $r \in \mathbb{K}\{x\}[y]$ , da cui segue  $\mu(f, g) = \mu(f, r)$ . Se  $r \in \mathbb{K}\{x\}$  abbiamo già visto che  $\mu(f, r) = \nu(f, r)$ , altrimenti possiamo scrivere  $r = sep$  con  $s \in \mathbb{K}\{x\}$ ,  $e$  invertibile e  $p$  polinomio di Weierstrass in  $y$  di grado strettamente minore al grado di  $f$  e quindi  $\mu(f, g) = \mu(f, s) + \mu(f, p)$ .  $\square$

**Teorema 8.3.4 (Definizione parametrica della molteplicità di intersezione).** *Sia  $f \in \mathbb{K}\{x, y\}$  irriducibile e  $\alpha: \mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{t\}$  una parametrizzazione irriducibile di  $f$ . Allora per ogni  $g \in \mathbb{K}\{x, y\}$  vale  $\nu(f, g) = \nu(\alpha(g))$ .*

*Dimostrazione.* Il risultato è evidente se  $f$  divide  $g$ , basta quindi esaminare il caso in cui  $f$  e  $g$  non hanno fattori comuni e  $\alpha(g) \neq 0$ . Siano  $\phi: \mathbb{K}\{x, y\}/(f) \rightarrow \mathbb{K}\{x, y\}/(f)$  e  $\psi: \mathbb{K}\{t\} \rightarrow \mathbb{K}\{t\}$  le moltiplicazioni per  $g$  e  $\alpha(g)$  rispettivamente; i morfismi  $\phi$  e  $\psi$  sono iniettivi e  $\mathbb{K}$ -lineari. Il conucleo  $\text{Coker}(\alpha)$  ha dimensione finita ed esiste un morfismo di successioni esatte corte

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{K}\{x, y\}/(f) & \xrightarrow{\alpha} & \mathbb{K}\{t\} & \longrightarrow & \text{Coker}(\alpha) \longrightarrow 0 \\ & & \downarrow \phi & & \downarrow \psi & & \downarrow \gamma \\ 0 & \longrightarrow & \mathbb{K}\{x, y\}/(f) & \xrightarrow{\alpha} & \mathbb{K}\{t\} & \longrightarrow & \text{Coker}(\alpha) \longrightarrow 0. \end{array}$$

Per il lemma del serpente esiste una successione esatta di spazi vettoriali di dimensione finita

$$0 \longrightarrow \text{Ker}(\gamma) \longrightarrow \text{Coker}(\phi) \longrightarrow \text{Coker}(\psi) \longrightarrow \text{Coker}(\gamma) \longrightarrow 0.$$

Dato che  $\text{Coker}(\alpha)$  ha dimensione finita, si ha  $\dim \text{Ker}(\gamma) = \dim \text{Coker}(\gamma)$  e quindi  $\nu(f, g) = \dim \text{Coker}(\phi) = \dim \text{Coker}(\psi) = \nu(\alpha(g))$ .  $\square$

**Esercizi**

**8.6.** Sia  $x \mapsto \alpha_1(t)$ ,  $y \mapsto \alpha_2(t)$ , una parametrizzazione irriducibile di una serie irriducibile  $f \in \mathbb{K}\{x, y\}$ . Provare che la molteplicità di  $f$  è uguale al minimo delle molteplicità di  $\alpha_1(t)$  e  $\alpha_2(t)$ .

**8.7.** Sia  $f \in \mathbb{K}\{x, y\}$  polinomio di Weierstrass di grado  $m$  in  $y$  e si consideri il morfismo di  $\mathbb{K}$ -algebre

$$\alpha: \mathbb{K}\{u, v\} \rightarrow \mathbb{K}\{x, y\}/(f), \quad \alpha(g(u, v)) = g(x, xy).$$

Provare che la dimensione di  $\text{Coker}(\alpha)$  su  $\mathbb{K}$  è uguale a  $1 + 2 + \dots + (m - 1) = \frac{1}{2}m(m - 1)$ . (Sugg.: utilizzare il teorema di divisione per dimostrare che i monomi  $x^a y^b$ , al variare di  $0 \leq a < b < m$ , sono una base di  $\text{Coker}(\alpha)$ .)

**8.8 (Il numero di punti doppi, \*).** Dato un arco primitivo  $\alpha: \mathbb{K}\{x, y\} \rightarrow \mathbb{K}\{t\}$ , la dimensione  $\delta(\alpha) = \dim \text{Coker}(\alpha)$  del conucleo di  $\alpha$  è detta **numero di punti doppi** di  $\alpha$ . Per ogni  $f \in \mathbb{K}\{x, y\}$  si definisce:

1.  $\delta(f) = +\infty$  se  $f$  possiede una componente multipla.
2.  $\delta(f) = 0$  se  $f$  è invertibile.
3. Se  $f$  è ridotta di molteplicità  $\nu(f) > 0$  e  $\alpha_1, \dots, \alpha_k$  sono delle parametrizzazioni primitive delle componenti irriducibili di  $f$ , allora  $\delta(f)$  è uguale alla dimensione del conucleo di

$$\mathbb{K}\{x, y\} \xrightarrow{\oplus \alpha_i} \bigoplus_{i=1}^k \mathbb{K}\{t\}.$$

Dalla definizione segue immediatamente che se  $f$  è irriducibile ed  $\alpha$  è una sua parametrizzazione irriducibile, allora  $\delta(f) = \delta(\alpha)$ . Provare che:

1. Se  $f$  è ridotta, allora  $\delta(f) < +\infty$ .
2.  $\delta(fg) = \delta(f) + \delta(g) + \nu(f, g)$ .
3.  $\delta(f) = 0$  se e solo se  $\nu(f) \leq 1$ .
4. Nelle notazioni del Lemma 7.5.5, vale  $\delta(\beta) = \delta(\alpha) + \frac{1}{2}\nu(f)(\nu(f) - 1)$ .
5.  $\delta(f) \geq \frac{1}{2}\nu(f)(\nu(f) - 1)$ .

**8.9.** Dimostrare la validità della seguente ricetta induttiva per il calcolo della molteplicità di intersezione di due serie irriducibili  $f(x, y)$  e  $g(x, y)$  in funzione delle rispettive parametrizzazioni primitive  $\alpha = (\alpha_1, \alpha_2)$  e  $\beta = (\beta_1, \beta_2)$ .

Denotiamo  $\nu(\alpha, \beta) = \nu(f, g)$  e per ogni arco  $\gamma = (\gamma_1, \gamma_2)$  definiamo la sua molteplicità  $\nu(\gamma)$  come il minimo delle molteplicità delle due serie  $\gamma_1, \gamma_2$ . Con un opportuno cambio lineare sulle coordinate  $x, y$  si ha  $\nu(\alpha_1) < \nu(\alpha_2)$ ; in tali ipotesi

1.  $\nu(\alpha, \beta) = \nu(\alpha)\nu(\beta)$  se  $\nu(\beta_1) \geq \nu(\beta_2)$ .
2.  $\nu(\alpha, \beta) = \nu(\alpha)\nu(\beta) + \nu(\alpha', \beta')$  se  $\nu(\beta_1) < \nu(\beta_2)$ , dove si è posto  $\alpha' = (\alpha_1, \alpha_2\alpha_1^{-1})$  e  $\beta' = (\beta_1, \beta_2\beta_1^{-1})$ .

### 8.4 Un lungo esercizio: il teorema $Af + B\phi$ di Max Noether

Gli esercizi di questa sezione forniranno una dimostrazione della seguente generalizzazione del Teorema 6.5.1.

**Definizione 8.4.1.** Siano  $C, D \subset \mathbb{P}^2$  curve fissate senza componenti comuni di equazioni  $F$  e  $\Phi$  rispettivamente. Diremo che una curva  $E \subset \mathbb{P}^2$  di equazione  $H$  soddisfa la condizione  $Af + B\phi$  **globale** se esistono polinomi omogenei  $A, B$  tali che  $H = AF + B\Phi$ .

Diremo che  $E$  soddisfa la condizione  $Af + B\phi$  **locale** se per ogni  $p \in C \cap D$ , dette  $f, \phi, h$  le equazioni di  $C, D, E$  in un sistema di coordinate affini  $x, y$  centrate in  $p$ , si ha  $h \in (f, \phi) \subset \mathbb{K}\{x, y\}$ .

**Teorema 8.4.2.** Siano  $C, D \subset \mathbb{P}^2$  curve fissate senza componenti comuni di equazioni  $F$  e  $\Phi$  rispettivamente. Allora una curva  $E$  soddisfa la condizione  $Af + B\phi$  globale se e solo se soddisfa quella locale.

**Esercizi**

**8.10.** Sia  $\mathfrak{m} \subset \mathbb{K}\{x, y\}$  l'ideale massimale, e siano  $f, g \in \mathfrak{m}$  senza fattori comuni; indichiamo  $\nu(f, g) = d$ . Provare che  $\mathfrak{m}^d \subset (f, g)$  e quindi che  $\mathbb{K}\{x, y\}/(f, g)$  è generato come spazio vettoriale dai monomi  $x^a y^b$ , con  $a + b < d$ . (Sugg.: l'anello  $A = \mathbb{K}\{x, y\}/(f, g)$  è locale noetheriano con ideale massimale  $\mathfrak{n} = \mathfrak{m}/(f, g)$ , esiste  $h \leq d$  tale che  $\mathfrak{n}^h = \mathfrak{n}^{h+1} = \mathfrak{n} \cdot \mathfrak{n}^h$ , si usi il lemma di Nakayama.)

**8.11.** Siano  $f, g, h \in \mathbb{K}\{x, y\}$  con  $f$  di molteplicità 1. Provare che  $h \in (f, g)$  se e solo se  $\nu(h, f) \geq \nu(g, f)$ .

**8.12.** Siano  $f_1, \dots, f_r, g, h \in \mathbb{K}\{x, y\}$  con  $f_1, \dots, f_r$  di molteplicità 1 a tangenti distinte e denotiamo  $f = f_1 \cdots f_r$ . Provare che se  $\nu(h, f_i) \geq \nu(g, f_i) + r - 1$  per ogni  $i = 1, \dots, r$ , allora  $h \in (f, g)$ . (Sugg.: induzione su  $r$ .)

**8.13.** Dimostrare il Teorema 8.4.2. (Sugg.: siano  $n, m$  i gradi di  $C$  e  $D$ , provare che se  $d \geq nm$  le curve  $E$  di grado  $d$  che soddisfano la condizione locale formano un sistema lineare di dimensione  $\frac{1}{2}d(d+3) - nm$ . Ripetere la seconda dimostrazione del Teorema 6.5.1.)

**8.5 Esercizi complementari**

**8.14.** Utilizzare il teorema di Bertini 5.6.1 per dimostrare che, in caratteristica 0, se  $V$  è un fascio di curve piane senza componenti comuni e  $d$  è il massimo grado di una componente irriducibile contenuta in una curva del fascio, allora esiste al più un numero finito di curve in  $V$  aventi una componente irriducibile di grado  $< d$ .

**8.15.** Sia  $f \in \mathbb{K}\{t\}$  di molteplicità  $\nu(f) > 0$  non divisibile per la caratteristica di  $\mathbb{K}$ . Provare che

$$\nu\left(x - y, \frac{f(x) - f(y)}{x - y}\right) = \nu(f) - 1.$$

**8.16 (\*)**. Sia  $\mathbb{K}$  campo algebricamente chiuso,  $f \in \mathbb{K}\{x, y\}$  senza fattori multipli e sia  $f = f_1 \cdots f_n$  la scomposizione in fattori irriducibili. Per ogni multiindice  $I = (i_1, \dots, i_n) \in \mathbb{N}^n$  si consideri lo spazio vettoriale

$$V(I) = \left\{ g \in \mathbb{K}\{x, y\} \mid \nu(g, f_j) = \dim_{\mathbb{K}} \frac{\mathbb{K}\{x, y\}}{(g, f_j)} \geq i_j \text{ per ogni } j = 1, \dots, n \right\}.$$

Dimostrare che esiste un multiindice  $I_0$  tale che:

1.  $V(I_0)$  ha codimensione finita in  $\mathbb{K}\{x, y\}$ .
2. Per ogni  $I = (i_1, \dots, i_n) \in \mathbb{N}^n$ , lo spazio  $V(I_0 + I)$  ha codimensione  $|I| = i_1 + \dots + i_n$  in  $V(I_0)$ .
3.  $V(I_0 + I) + V(I_0 + H) = V(I_0 + I \wedge H)$ , dove

$$(i_1, \dots, i_n) \wedge (h_1, \dots, h_n) = (\min(i_1, h_1), \dots, \min(i_n, h_n)).$$

In particolare  $V(I_0 + I) = V(I_0 + H)$  se e solo se  $H = I$ .

**8.17.** Sia  $A$  un anello e  $f: M \rightarrow P$ ,  $g: N \rightarrow P$  due omomorfismi di  $A$ -moduli. Il **prodotto fibrato** di  $f$  e  $g$  è per definizione lo  $A$ -modulo

$$M \times_P N = \{(m, n) \in M \times N \mid f(m) = g(n)\}.$$



Denotiamo con  $f': M \times_P N \rightarrow N$  e  $g': M \times_P N \rightarrow M$  le due proiezioni. Dimostrare che per ogni diagramma commutativo di morfismi di  $A$ -moduli

$$\begin{array}{ccc} H & \xrightarrow{\alpha} & N \\ \downarrow \beta & & \downarrow g \\ M & \xrightarrow{f} & P \end{array}$$

esiste un unico omomorfismo di  $A$ -moduli  $\gamma: H \rightarrow M \times_P N$  tale che  $\beta = g'\gamma$  e  $\alpha = f'\gamma$ . Provare inoltre che  $\gamma$  è un isomorfismo se e soltanto se  $\text{Im}(\alpha) = \text{Im}(f')$  e  $\beta$  induce un isomorfismo tra  $\text{Ker}(\alpha)$  e  $\text{Ker}(f)$ .

**8.18.** Sia  $A$  un anello e  $f: M \rightarrow P$ ,  $g: M \rightarrow N$  due omomorfismi di  $A$ -moduli. Il **coprodotto fibrato** (detto anche **somma fibrata**) di  $f$  e  $g$  è per definizione lo  $A$ -modulo  $P \oplus_M N = (P \oplus N)/K$ , dove  $K = \{(f(m), -g(m)) \in P \oplus N \mid m \in M\}$ . In altri termini  $P \oplus_M N$  è il conucleo dell'omomorfismo  $(f, -g): M \rightarrow P \oplus N$ . Denotiamo con  $f': N \rightarrow P \oplus_M N$  e  $g': P \rightarrow P \oplus_M N$  i morfismi indotti dalle inclusioni nella somma diretta. Dimostrare che per ogni diagramma commutativo di morfismi di  $A$ -moduli

$$\begin{array}{ccc} M & \xrightarrow{f} & P \\ \downarrow g & & \downarrow \beta \\ N & \xrightarrow{\alpha} & H \end{array}$$

esiste un unico omomorfismo di  $A$ -moduli  $\gamma: P \oplus_M N \rightarrow H$  tale che  $\beta = \gamma g'$  e  $\alpha = \gamma f'$ . Provare inoltre che  $\gamma$  è un isomorfismo se e soltanto se  $\text{Ker}(\alpha) = \text{Ker}(f')$  e  $\beta$  induce un isomorfismo tra  $\text{Coker}(\alpha)$  e  $\text{Coker}(f)$ .

**8.19 (\*)**. Sia  $A$  un anello euclideo e consideriamo l'insieme  $M(m, n, A)$  delle matrici  $m \times n$  a coefficienti in  $A$  come un  $M(n, n, A)$ -modulo destro. Provare che se  $m \leq n$ , allora ogni sottomodulo di  $M(m, n, A)$  è generato da un solo elemento. (Sugg.: considerare  $M(m, n, A)$  come lo spazio delle applicazioni  $A$ -lineari  $A^n \rightarrow A^m$ . Per ogni sottomodulo  $N \subset M(m, n, A)$  sia  $V \subset A^n$  l'insieme dei  $f(v)$ ,  $f \in N$ ,  $v \in A^n$ . Considerare preliminarmente il caso  $V = A^n$ ; se  $V$  è libero di rango  $s \leq m$  esiste  $\phi \in M(m, s, A)$  tale che  $N = \phi M(s, n, A)$ .)

**8.20 (Proiettività normale delle curve piane lisce, \*\*)**. Sia  $F \in \mathbb{K}[x_0, x_1, x_2]$  l'equazione di una curva piana liscia  $C$ ,  $A = \mathbb{K}[x_0, x_1, x_2]/(F)$  e  $R(x) \in A[x]$  un polinomio monico. Provare:

1. Dati  $P = \hat{P} + P_r$ ,  $Q = \hat{Q} + Q_s$  polinomi in  $\mathbb{K}[x_0, x_1, x_2]$  con  $P_r$  (risp.  $Q_s$ ) omogeneo di grado  $r$  (risp.  $s$ ) e  $\hat{P}$  (risp.  $\hat{Q}$ ) di grado  $< r$  (risp.  $< s$ ). Se  $P/Q$  è una radice di  $R$  allora vale  $\nu_p(F, P_r) \geq \nu_p(F, Q_s)$  per ogni  $p \in C$ .
2. L'anello  $A$  è un integralmente chiuso (vedi Esercizio 7.29) nel suo campo delle frazioni. (Sugg.: usare il punto 1) ed il teorema  $Af + B\phi$  di Max Noether.)



## La topologia di Zariski

In tutto il capitolo  $\mathbb{K}$  denoterà un campo algebricamente chiuso. Chiameremo quasi-compatto uno spazio topologico tale che ogni ricoprimento aperto ammette un sottoricoprimento finito: riserveremo il termine compatto agli spazi quasicompatti di Hausdorff. Diremo che un'applicazione continua  $f: X \rightarrow Y$  tra spazi topologici è una **immersione topologica** se  $f: X \rightarrow f(X)$  è un omeomorfismo, dove  $f(X)$  ha la topologia di sottospazio. Notiamo che una applicazione continua  $f: X \rightarrow Y$  è iniettiva e chiusa se e solo se è una immersione topologica e  $f(X)$  è chiuso in  $Y$ . Similmente  $f$  è iniettiva ed aperta se e solo se è una immersione topologica e  $f(X)$  è aperto in  $Y$ .

### 9.1 Esempi di spazi topologici

Ricordiamo che il luogo di zeri di un ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$  è definito come

$$V(I) = \{a \in \mathbb{A}^n \mid f(a) = 0 \text{ per ogni } f \in I\}$$

e che l'ideale di un sottoinsieme  $X \subset \mathbb{A}^n$  è

$$I(X) = \{f \in \mathbb{K}[x_1, \dots, x_n] \mid f(a) = 0 \text{ per ogni } a \in X\}.$$

Il Teorema degli Zeri di Hilbert 4.5.3 afferma che per ogni ideale  $J \subset \mathbb{K}[x_1, \dots, x_n]$  vale  $I(V(J)) = \sqrt{J}$ . Abbiamo inoltre già osservato che gli insiemi  $V(I) = V(\sqrt{I})$  formano, al variare di  $I$  tra gli ideali di  $\mathbb{K}[x_1, \dots, x_n]$ , la famiglia dei chiusi di una topologia su  $\mathbb{A}^n$  detta **topologia di Zariski**.

**Definizione 9.1.1.** *Un sottoinsieme non vuoto  $X \subset \mathbb{A}^n$  si dice una **ipersuperficie affine** se  $X = V(f)$  per qualche polinomio  $f$  di grado positivo.*

Siccome ogni ideale di  $\mathbb{K}[x_1, \dots, x_n]$  è finitamente generato, si ha che ogni chiuso di Zariski è intersezione finita di ipersuperfici. Inoltre gli aperti  $\mathbb{A}_f^n := \mathbb{A}^n - V(f)$ , con  $f \in \mathbb{K}[x_1, \dots, x_n]$ , formano una base della topologia di Zariski.

In modo analogo è possibile definire la topologia di Zariski anche nello spazio proiettivo. Sia  $x_0, \dots, x_n$  un sistema di coordinate omogenee su  $\mathbb{P}^n$  e denotiamo

$$S = \oplus S_d = \mathbb{K}[x_0, \dots, x_n],$$

dove  $S_d$  denota lo spazio vettoriale dei polinomi omogenei di grado  $d$ . Dato un polinomio omogeneo  $f \in S$  è ben definita l'**ipersuperficie proiettiva**

$$V_{\mathbb{P}}(f) = \{[x] \in \mathbb{P}^n \mid f(x) = 0\}$$

e si definiscono i chiusi di Zariski come i sottoinsiemi che sono intersezione di ipersuperfici. Se  $I \subset S$  è un ideale omogeneo si definisce  $V_{\mathbb{P}}(I)$  come l'intersezione di tutte le ipersuperfici  $V_{\mathbb{P}}(f)$  al variare di  $f$  tra gli elementi omogenei di  $I$ . Per definizione gli insiemi  $V_{\mathbb{P}}(I)$ , al variare di  $I$  tra gli ideali omogenei, sono tutti e soli i chiusi di Zariski. la verifica che i chiusi di Zariski sono realmente i chiusi di una topologia è lasciata per esercizio.

Da ora in poi, salvo avviso contrario, qualsiasi affermazione riguardante la topologia dello spazio affine e/o proiettivo si intende relativa alla topologia di Zariski.

Denotiamo con  $\pi: \mathbb{A}^{n+1} - \{0\} \rightarrow \mathbb{P}^n$ ,  $\pi(x_0, \dots, x_n) = [x_0, \dots, x_n]$ , la proiezione al quoziente. Per ogni sottoinsieme  $X \subset \mathbb{P}^n$  si definisce il **cono affine** di  $X$  come

$$C(X) = \pi^{-1}(X) \cup \{0\}.$$

Si verifica immediatamente che se  $I \subset S_+ := \bigoplus_{d>0} S_d$  è un ideale omogeneo allora  $C(V_{\mathbb{P}}(I)) = V(I)$ . Viceversa se  $X \subset \mathbb{P}^n$  si definisce  $I(X) \subset S_+$  come l'ideale generato dai polinomi omogenei di grado positivo che si annullano su  $X$ .

**Lemma 9.1.2.** *Nelle notazioni precedenti, per ogni sottoinsieme  $X \subset \mathbb{P}^n$  vale  $I(X) = I(C(X))$ .*

*Dimostrazione.* Segue immediatamente dalla definizione che  $I(X)$  e  $I(C(X))$  contengono gli stessi polinomi omogenei, basta quindi dimostrare che l'ideale  $I(C(X))$  è omogeneo. Sia  $f \in I(C(X))$  di grado  $m$  e  $f = f_1 + \dots + f_m$  la decomposizione di  $f$  nelle sue componenti omogenee; bisogna dimostrare che  $f_i \in I(C(X))$  per ogni  $i = 1, \dots, m$ . Dato che  $C(X)$  è un cono di centro 0, per ogni  $t \in \mathbb{K}$  il polinomio  $f_t(x_0, \dots, x_n) = f(tx_0, \dots, tx_n)$  appartiene ancora all'ideale  $I(C(X))$ . Dato che  $f_t = tf_1 + \dots + t^m f_m$ , prendendo  $m$  valori distinti  $t_1, \dots, t_m \in \mathbb{K} - \{0\}$  e invertendo la matrice di Vandermonde  $(t_i^j)$  si può scrivere  $f_1, \dots, f_m$  come combinazione lineare dei polinomi  $f_{t_1}, \dots, f_{t_m}$ .  $\square$

**Teorema 9.1.3 (Teorema degli zeri proiettivo).** *Per ogni ideale omogeneo  $J \subset S_+$  vale  $I(V_{\mathbb{P}}(J)) = \sqrt{J}$ .*

*Dimostrazione.* Segue immediatamente dal Lemma 9.1.2 ed dal teorema degli zeri affine.  $\square$

Si osservi che l'enunciato del teorema degli zeri proiettivo sarebbe falso senza l'ipotesi  $J \subset S_+$ : ad esempio  $V_{\mathbb{P}}(S) = V_{\mathbb{P}}(S_+) = \emptyset$ .

**Corollario 9.1.4.** *Sia  $J = \bigoplus J_d \subset S_+ = \bigoplus_{d>0} S_d$  un ideale omogeneo. Allora vale  $V_{\mathbb{P}}(J) = \emptyset$  se e solo se esiste  $k$  tale che  $S_d = J_d$  per ogni  $d \geq k$ .*

*Dimostrazione.* Se  $S_d = J_d$  per qualche  $d$  allora  $V(J) = \emptyset$ . Viceversa se  $V(J) = \emptyset$ , allora per il teorema degli zeri  $\sqrt{J} = S_+$  e dato che  $S_+$  è finitamente generato esiste  $k > 0$  tale che  $S_+^k \subset J$ .  $\square$

**Corollario 9.1.5.** *Nelle notazioni precedenti, siano  $f_0, \dots, f_r \in S_+$  polinomi omogenei di gradi  $d_0 \geq d_1 \geq \dots \geq d_r > 0$  e, per ogni intero  $d > 0$ , si consideri l'applicazione lineare*

$$\phi_d: S_{d-d_0} \oplus \dots \oplus S_{d-d_r} \rightarrow S_d, \quad \phi_d(g_0, \dots, g_r) = g_0 f_0 + \dots + g_r f_r.$$

*Allora vale  $V(f_0) \cap \dots \cap V(f_r) = \emptyset$  se e solo se  $\phi_d$  è surgettiva per qualche  $d > 0$ .*

*Dimostrazione.* Ovvvia conseguenza di 9.1.4.  $\square$

*Osservazione 9.1.6.* È possibile dimostrare (Esercizio 13.14) che, nelle notazioni del Corollario 9.1.5, se  $V(f_0, \dots, f_r) = \emptyset$ , allora  $r \geq n$  e  $\phi_d$  è surgettiva per ogni  $d \geq d_0 + d_1 + \dots + d_n - n$ .

Molto utili per le applicazioni sono gli spazi misti affino-multiproiettivi

$$\mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_s} \times \mathbb{A}^m$$

sui quali si definisce la topologia di Zariski come l'unica topologia avente la seguente proprietà: per ogni scelta di iperpiani  $H_1 \subset \mathbb{P}^{n_1}, \dots, H_s \subset \mathbb{P}^{n_s}$ , la topologia indotta sul sottospazio  $(\mathbb{P}^{n_1} - H_1) \times \dots \times (\mathbb{P}^{n_s} - H_s) \times \mathbb{A}^m$  coincide con la topologia di Zariski su  $\mathbb{A}^{m+\sum n_i}$ .

In analogia con il caso di  $\mathbb{P}^n$ , possiamo definire una ipersuperficie in  $\mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_s} \times \mathbb{A}^m$  come il luogo di zeri di un polinomio separatamente omogeneo nelle coordinate omogenee di ciascun fattore  $\mathbb{P}^{n_i}$  e quindi definire i chiusi come intersezioni di ipersuperfici. Consideriamo per esempio il caso  $\mathbb{P}^n \times \mathbb{A}^m$ . Un polinomio  $f \in \mathbb{K}[x_0, \dots, x_n, y_1, \dots, y_m]$  risulta essere omogeneo rispetto alle variabili  $x_0, \dots, x_n$  se e solo se si può scrivere  $f(x, y) = \sum h_i(x)k_i(y)$ , con i polinomi  $h_i$  omogenei dello stesso grado. Per un tale polinomio è ben definita la corrispondente ipersuperficie  $V(f) \subset \mathbb{P}^n \times \mathbb{A}^m$ . Ricordiamo (vedi il Capitolo 1) che ogni fattore irriducibile di  $f$  è ancora omogeneo rispetto alle variabili  $x_0, \dots, x_n$  e quindi, se  $f = gh$ , allora  $V(f) = V(g) \cup V(h)$ .

**Teorema 9.1.7.** *La proiezione sul secondo fattore  $\pi: \mathbb{P}^n \times \mathbb{A}^m \rightarrow \mathbb{A}^m$  è un'applicazione chiusa.*

*Dimostrazione.* Sia  $X \subset \mathbb{P}^n \times \mathbb{A}^m$  un chiuso e siano  $x_0, \dots, x_n$  coordinate omogenee su  $\mathbb{P}^n$ . Allora  $X$  è intersezione di un numero finito di ipersuperfici  $V(f_0), \dots, V(f_r)$ , con i polinomi  $f_i(x, y)$  omogenei nelle variabili  $x_0, \dots, x_n$ . Un punto  $a \in \mathbb{A}^m$  appartiene a  $\pi(X)$  se e solo se i polinomi omogenei  $f_0(x, a), \dots, f_r(x, a) \in \mathbb{K}[x_0, \dots, x_n]$  hanno uno zero comune in  $\mathbb{P}^n$  e questo equivale a dire che per ogni intero positivo  $d$  l'applicazione lineare  $\phi_d(a)$ , definita nel Corollario 9.1.5, non è surgettiva. Se  $Y_d$  denota l'insieme dei punti  $a$  tali che  $\phi_d(a)$  non è surgettiva, allora vale  $X = \bigcap_d Y_d$  e quindi è sufficiente dimostrare che  $Y_d$  è chiuso per ogni  $d$ . L'applicazione lineare  $\phi_d(a)$  è rappresentata da una matrice i cui coefficienti dipendono in modo polinomiale da  $a$  e la condizione  $\phi_d(a)$  non surgettiva equivale all'annullarsi dei determinanti minori di ordine uguale alla dimensione di  $S_d$ . Questo prova la chiusura di  $Y_d$ .  $\square$

**Corollario 9.1.8.** *La proiezione*

$$\mathbb{P}^{n_0} \times \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_s} \times \mathbb{A}^m \rightarrow \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_s} \times \mathbb{A}^m$$

*è un'applicazione chiusa.*

*Dimostrazione.* Basta osservare che  $\mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_s} \times \mathbb{A}^m$  è ricoperto da un numero finito di spazi affini  $\mathbb{A}^{m+\sum n_i}$ .  $\square$

### Esercizi

**9.1.** Provare che  $\mathbb{A}^n$ , inteso come spazio topologico, è quasicompatto.

**9.2.** Dimostrare che per ogni scelta di  $p_1, \dots, p_s \in \mathbb{K}[x_1, \dots, x_n]$ , l'applicazione  $\mathbb{A}^n \rightarrow \mathbb{A}^s$ , definita da  $a \mapsto (p_1(a), \dots, p_s(a))$  è continua: in particolare le affinità di  $\mathbb{A}^n$  in sé sono omeomorfismi.

**9.3.** Mostrare che l'applicazione  $\mathbb{A}^n \rightarrow \mathbb{A}^{n+1}$ ,  $(a_1, \dots, a_n) \mapsto (a_1, \dots, a_n, 0)$ , è una immersione topologica chiusa.

**9.4.** Utilizzando la bigezione naturale  $\mathbb{A}^{n+m} \cong \mathbb{A}^n \times \mathbb{A}^m$ , confrontare la topologia di Zariski su  $\mathbb{A}^{n+m}$  con la topologia prodotto su  $\mathbb{A}^n \times \mathbb{A}^m$  e provare che se  $X \subset \mathbb{A}^n$  e  $Y \subset \mathbb{A}^m$  sono chiusi, allora  $X \times Y \subset \mathbb{A}^{n+m}$  è chiuso.

*Osservazione 9.1.9.* Il fatto che la topologia di Zariski su  $\mathbb{A}^{n+m}$  è strettamente più fine della topologia prodotto permette di supplire a certi inconvenienti tipici delle topologie non-Hausdorff. Ad esempio il grafico dell'applicazione definita nell'Esercizio 9.2 è un sottoinsieme chiuso di  $\mathbb{A}^{n+s}$ .

**9.5.** Dimostrare che le proiettività  $\mathbb{P}^n \rightarrow \mathbb{P}^n$  sono omeomorfismi e che l'applicazione  $\mathbb{A}^n \rightarrow \mathbb{P}^n$  definita da  $(a_1, \dots, a_n) \mapsto [1, a_1, \dots, a_n]$  è una immersione topologica aperta.

**9.6.** Provare che la proiezione sul secondo fattore  $\mathbb{P}^m \times \mathbb{A}^n \rightarrow \mathbb{A}^n$  è aperta. (Sugg.: applicare l'Esercizio 4.15 ad un opportuno ricoprimento aperto di  $\mathbb{P}^m \times \mathbb{A}^n$ .)

**9.7.** Siano  $X \subset \mathbb{A}^n$  un chiuso,  $I = I(X)$  il suo ideale,  $f \in \mathbb{K}[x_1, \dots, x_n]$  un polinomio e  $\Gamma \subset X \times \mathbb{A}^1 \subset \mathbb{A}^{n+1}$  il grafico dell'applicazione  $f: X \rightarrow \mathbb{A}^1$ . Dimostrare che  $\Gamma$  è chiuso e che  $I(\Gamma)$  è l'ideale generato da  $I$  e da  $x_{n+1} - f(x_1, \dots, x_n)$ .

## 9.2 L'immersione di Veronese

Siano  $f_0, \dots, f_s \in \mathbb{K}[x_0, \dots, x_n]$  polinomi omogenei dello stesso grado  $d$  senza zeri comuni, cioè tali che  $V(f_0, \dots, f_s) = \emptyset$ . Possiamo definire un'applicazione

$$f: \mathbb{P}^n \rightarrow \mathbb{P}^s, \quad f([x]) = [f_0(x), \dots, f_s(x)],$$

che si verifica immediatamente essere continua.

**Definizione 9.2.1.** *La  $d$ -esima immersione di Veronese*

$$v_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$$

è l'applicazione definita in coordinate omogenee da

$$v_d([x_0, \dots, x_n]) = [\dots, x^I, \dots],$$

al variare di  $I = (i_0, \dots, i_n) \in \mathbb{N}^{n+1}$  tra tutti i multiindici di grado  $|I| = i_0 + \dots + i_n = d$  e dove  $x^{(i_0, \dots, i_n)} = x_0^{i_0} \cdots x_n^{i_n}$ . Il numero  $N + 1$  è perciò uguale al numero di monomi di grado  $d$  nelle variabili  $x_0, \dots, x_n$  e quindi  $N = \binom{n+d}{d} - 1$ .

Ad esempio la seconda immersione di Veronese  $v_2: \mathbb{P}^2 \rightarrow \mathbb{P}^5$  è data da

$$[x_0, x_1, x_2] \mapsto [x_0^2, x_0x_1, x_0x_2, x_1^2, x_1x_2, x_2^2].$$

**Proposizione 9.2.2.** *Per ogni coppia di interi positivi  $n$  e  $d$ , la  $d$ -esima immersione di Veronese  $v_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$  è una immersione topologica chiusa e la sua immagine  $v_d(\mathbb{P}^n)$  è intersezione finita di quadriche proiettive.*

*Dimostrazione.* Iniziamo con l'osservare che per ogni proiettività  $\phi$  di  $\mathbb{P}^n$  esiste una proiettività indotta  $\psi$  su  $\mathbb{P}^N$  tale che  $v_d\phi = \psi v_d$ . Dato che  $v_d$  non è costante ed il gruppo delle proiettività di  $\mathbb{P}^n$  agisce in modo doppiamente transitivo (significa che  $\text{PGL}(n+1)$  agisce transitivamente su  $\mathbb{P}^n \times \mathbb{P}^n - \text{Diagonale}$ ) ne segue immediatamente che  $v_d$  è iniettiva. Il fatto che  $v_d$  è una applicazione chiusa può essere dedotto da un risultato generale

non costruttivo che dimostreremo in seguito. Per motivi didattici preferiamo dare qui una dimostrazione costruttiva della chiusura di  $v_d$ .

Sia  $y_{I_0}, \dots, y_{I_N}$  un sistema di coordinate omogenee su  $\mathbb{P}^N$  tale che l'equazioni  $y_{I_j} = x^{I_j}$  definiscono l'immersione di Veronese. Poniamo  $X = v_d(\mathbb{P}^n)$  dotato della topologia di sottospazio e proviamo prima che  $v_d: \mathbb{P}^n \rightarrow X$  è un omeomorfismo e poi che  $X$  è intersezione finita di quadriche in  $\mathbb{P}^N$ . Dato che ogni chiuso di  $\mathbb{P}^n$  è intersezione di ipersuperfici, è sufficiente provare che  $v_d(V(g))$  è chiuso in  $X$  per ogni polinomio omogeneo  $g$ . A meno di sostituire  $g$  con una sua potenza non è restrittivo supporre che il grado di  $g$  sia un multiplo di  $d$ . Esiste allora un polinomio  $P \in \mathbb{K}[y_0, \dots, y_N]$  tale che  $P(x^{I_0}, \dots, x^{I_N}) = g$ . È allora evidente che  $v_d(V(g)) = X \cap V(P)$ . Consideriamo il chiuso di  $\mathbb{P}^N$ , intersezione di (finite) quadriche

$$Y = \bigcap \{V(y_{I_1}y_{I_2} - y_{J_1}y_{J_2}) \mid I_1 + I_2 = J_1 + J_2\}.$$

È chiaro che  $X \subset Y$ ; proviamo che vale  $X = Y$ . Sia  $[y] \in Y$  e sia  $I = (i_0, \dots, i_n)$  un multiindice tale che  $y_I \neq 0$ . A meno di permutazioni degli indici si può supporre  $i_0 > 0$ ; se  $i_0 < d$  possiamo trovare due multiindici  $J = (j_0, \dots, j_n)$  e  $H$ , di grado  $d$ , tali che  $2I = J + H$  e  $j_0 > i_0$ . Siccome  $y_I^2 = y_J y_H$  si ha  $y_J \neq 0$ . Non è quindi restrittivo supporre  $I = (d, 0, 0, \dots, 0)$  e se definiamo  $x_0 = y_{(d,0,0,\dots,0)} = 1$  e  $x_j = y_{(d-1,0,\dots,1,\dots,0)}$  dove 1 è posto alla  $j$ -esima posizione si verifica facilmente che  $v_d([x_0, \dots, x_n]) = [y]$  (si noti che lo stesso argomento mostra che  $v_d: \mathbb{P}^n \rightarrow Y$  è bigettiva).  $\square$

**Esercizi**

**9.8 (Definizione intrinseca dell'immersione di Veronese).** Sia  $V$  uno spazio vettoriale e denotiamo con  $V_d$  lo spazio vettoriale delle forme  $f: V \rightarrow \mathbb{K}$  omogenee di grado  $d$  (cioè  $f$  si rappresenta con un polinomio omogeneo di grado  $d$  in ogni sistema di coordinate su  $V$ ). Per ogni  $p \in \mathbb{P}(V)$  denotiamo con  $L(-p) \subset V_d$  il sottospazio vettoriale delle forme che si annullano in  $p$ . Dimostrare che  $L(-p)$  è un iperpiano e che, in opportuni sistemi di coordinate, l'applicazione

$$\mathbb{P}(V) \rightarrow \mathbb{P}(V_d^\vee), \quad p \mapsto L(-p),$$

è la  $d$ -esima immersione di Veronese. (Sugg.: isomorfismi canonici  $(V^\vee)_d = (V_d)^\vee$ .)

**9.9.** Il complementare in  $\mathbb{P}^n$  di una ipersuperficie proiettiva è omeomorfo ad un chiuso di uno spazio affine. (Sugg.: immersione di Veronese.)

**9.10.** Provare che l'immagine della  $n$ -esima immersione di Veronese

$$\mathbb{P}^1 \rightarrow \mathbb{P}^n, \quad [x_0, x_1] \mapsto [x_0^n, \dots, x_1^n]$$

è il chiuso determinantale di equazione

$$\text{rank} \begin{pmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ y_1 & y_2 & \cdots & y_n \end{pmatrix} \leq 1.$$

**9.3 Componenti irriducibili**

In questa sezione svilupperemo alcune nozioni di topologia generale che ben si adattano alla topologia di Zariski.

Sia  $X$  uno spazio topologico, un sottoinsieme  $Z \subset X$  si dice **localmente chiuso** se per ogni  $z \in Z$  esiste un aperto  $U \subset X$  tale che  $z \in U$  e  $Z \cap U$  è chiuso in  $U$ . Ad esempio i sottoinsiemi aperti ed i sottoinsiemi chiusi sono anche localmente chiusi.

**Lemma 9.3.1.** *Sia  $X$  uno spazio topologico e  $Z \subset X$  un sottoinsieme. Allora sono fatti equivalenti:*

1.  $Z$  è localmente chiuso.
2.  $Z$  è aperto in  $\overline{Z}$  (rispetto alla topologia di sottospazio).
3.  $Z$  è intersezione di un chiuso e di un aperto di  $X$ .

*Dimostrazione.* [1  $\Rightarrow$  2] Per ogni punto  $z \in Z$  esiste un aperto  $z \in U \subset X$  tale che  $Z \cap U$  è chiuso in  $U$  e quindi esiste un chiuso  $C \subset X$  tale che  $C \cap U = Z \cap U$ ; a meno di sostituire  $C$  con  $C \cup (X - U)$  non è restrittivo supporre  $Z \subset C$ . Quindi  $Z \cap U \subset \overline{Z} \cap U \subset C \cap U = Z \cap U$  che implica  $\overline{Z} \cap U \subset Z$ .

Le implicazioni [2  $\Rightarrow$  3] e [3  $\Rightarrow$  1] sono banali.  $\square$

**Definizione 9.3.2.** *Uno spazio topologico  $X$  si dice **Noetheriano** se ogni famiglia di aperti possiede un elemento massimale rispetto all'inclusione.*

Per il Lemma 1.1.1 uno spazio topologico è Noetheriano se e solo se ogni catena numerabile ascendente di aperti è stazionaria: per passaggio al complementare si ha che uno spazio topologico è Noetheriano se e solo se ogni catena numerabile discendente di chiusi è stazionaria. Tutti gli spazi considerati nella Sezione 9.1 sono Noetheriani: infatti, ad una catena discendente di chiusi  $X_i$  dello spazio affine  $\mathbb{A}^n$  corrisponde una catena ascendente di ideali  $I(X_i)$  che, per il teorema della base di Hilbert, è stazionaria.

**Lemma 9.3.3.** *Sia  $X$  uno spazio topologico Noetheriano. Allora:*

1.  $X$  è quasicompatto.
2. Ogni immagine continua di  $X$  è Noetheriana.
3. Ogni sottospazio topologico di  $X$  è Noetheriano.

*Dimostrazione.* [1] Sia  $\mathcal{U}$  un ricoprimento di  $X$ ; per trovare un sottoricoprimento finito basta prendere un elemento massimale nella famiglia delle unioni finite di aperti di  $\mathcal{U}$ .

[2] È banale.

[3] Sia  $Y \subset X$  un sottospazio. Denotiamo con  $\mathcal{T}(X)$  e  $\mathcal{T}(Y) = \{U \cap Y \mid U \in \mathcal{T}(X)\}$  le famiglie di aperti di  $X$  e  $Y$  rispettivamente e con  $r: \mathcal{T}(X) \rightarrow \mathcal{T}(Y)$  la naturale mappa di restrizione. Sia  $\mathcal{F} \subset \mathcal{T}(Y)$  una collezione di aperti e sia  $U \in \mathcal{T}(X)$  un elemento massimale della famiglia  $r^{-1}(\mathcal{F})$ ; proviamo che  $r(U) = U \cap Y$  è massimale in  $\mathcal{F}$ . Se  $r(U) \subset r(V)$  e  $r(V) \in \mathcal{F}$  allora  $U \cup V \in r^{-1}(\mathcal{F})$  e per la massimalità di  $U$  vale  $V \subset U$  e quindi  $r(U) = r(V)$ .  $\square$

**Definizione 9.3.4.** *Uno spazio topologico si dice **irriducibile** se ogni coppia di aperti non vuoti ha intersezione non vuota. Equivalentemente uno spazio è irriducibile se non è unione finita di chiusi propri. Un sottospazio di uno spazio topologico si dice irriducibile se è irriducibile per la topologia indotta.*

Ad esempio l'insieme vuoto, i punti e, più in generale, qualsiasi spazio topologico dotato della topologia indiscreta è irriducibile.

**Lemma 9.3.5.** *Siano  $X$  uno spazio topologico e  $Y \subset X$  un sottospazio irriducibile. Allora:*

1. La chiusura topologica  $\overline{Y}$  è irriducibile.
2. Se  $U \subset X$  è un aperto, allora  $Y \cap U$  è irriducibile.
3. Se  $f: X \rightarrow Z$  è continua, allora  $f(Y)$  è irriducibile.

*Dimostrazione.* Esercizio (molto facile).  $\square$



**Lemma 9.3.6.** *Siano dati due spazi topologici irriducibili  $X, Y$  ed una topologia sul prodotto cartesiano  $X \times Y$  tale che per ogni  $(x_0, y_0) \in X \times Y$  le inclusioni*

$$X \rightarrow X \times Y, \quad x \mapsto (x, y_0),$$

e

$$Y \rightarrow X \times Y, \quad y \mapsto (x_0, y),$$

siano continue. Allora anche  $X \times Y$  è irriducibile.

*Dimostrazione.* Siano  $U_1, U_2 \subset X \times Y$  aperti non vuoti,  $(x_1, y_1) \in U_1, (x_2, y_2) \in U_2$ . Per ipotesi i sottoinsiemi  $V_1 = \{y \in Y \mid (x_1, y) \in U_1\}$  e  $V_2 = \{y \in Y \mid (x_2, y) \in U_2\}$  sono aperti non vuoti di  $Y$  e quindi esiste  $y_0 \in Y$  tale che  $(x_1, y_0) \in U_1$  e  $(x_2, y_0) \in U_2$ . Ne segue che  $W_1 = \{x \in X \mid (x, y_0) \in U_1\}$  e  $W_2 = \{x \in X \mid (x, y_0) \in U_2\}$  sono aperti non vuoti di  $X$  e quindi esiste  $x_0 \in X$  tale che  $(x_0, y_0) \in U_1 \cap U_2$ .  $\square$

**Definizione 9.3.7.** *Le componenti irriducibili di uno spazio topologico sono gli elementi massimali della famiglia dei chiusi irriducibili, ordinata rispetto all'inclusione.*

**Teorema 9.3.8.** *Sia  $X$  uno spazio topologico Noetheriano. Allora:*

1.  $X$  possiede un numero finito di componenti irriducibili  $X_1, \dots, X_n$ .
2.  $X = X_1 \cup \dots \cup X_n$ .
3. Per ogni indice  $i$ , la componente  $X_i$  non è contenuta nell'unione delle componenti  $X_j$ , per  $j \neq i$ .

*Dimostrazione.* Dimostriamo per cominciare che ogni chiuso di  $X$  si può scrivere come unione finita di chiusi irriducibili; a tal fine consideriamo la famiglia  $\mathcal{C}$  di tutti i chiusi di  $X$  e la sottofamiglia  $\mathcal{F} \subset \mathcal{C}$  dei chiusi che sono unioni finite di chiusi irriducibili. Se per assurdo  $\mathcal{F} \neq \mathcal{C}$ , allora esiste  $Z \in \mathcal{C} - \mathcal{F}$  minimale; poiché  $Z \notin \mathcal{F}$ , il chiuso  $Z$  non è irriducibile e quindi esistono due chiusi propri  $Z_1, Z_2$  tali che  $Z = Z_1 \cup Z_2$ . Per la minimalità di  $Z$  si ha che  $Z_1, Z_2 \in \mathcal{F}$  e quindi anche  $Z \in \mathcal{F}$ . Possiamo quindi scrivere  $X = X_1 \cup \dots \cup X_n$ , dove ogni  $X_i$  è un chiuso irriducibile ed in modo tale che la condizione 3) sia soddisfatta. Dimostriamo che  $X_1, \dots, X_n$  sono tutte e sole le componenti irriducibili di  $X$ . Sia  $Z \subset X$  un chiuso irriducibile, allora  $Z = (Z \cap X_1) \cup \dots \cup (Z \cap X_n)$  e quindi i chiusi  $Z \cap X_i$  non possono essere tutti propri, ovvero esiste un indice  $i$  tale che  $Z \subset X_i$ . Lo stesso vale se  $Z$  è una componente irriducibile e quindi, tenendo presente la massimalità deduciamo che ogni componente irriducibile di  $X$  è uguale ad un  $X_i$ .

Viceversa se  $X_i$  non è massimale esiste una inclusione propria  $X_i \subset Z$  con  $Z$  irriducibile; per l'argomento precedente  $Z$  è contenuto in qualche  $X_j$  in contraddizione con la condizione 3).  $\square$

### Esercizi

**9.11.** Dimostrare che l'intersezione finita di sottoinsiemi localmente chiusi è localmente chiusa.

**9.12.** Quali dei seguenti sottoinsiemi di  $\mathbb{A}^2$  sono localmente chiusi?

$$X = \{xy \neq 0\} \cup \{(0, 0)\}, \quad Y = (\{xy = 1\} \cap \{x \neq y\}) \cup \{(1, 1)\},$$

$$Z = \left\{ (x, y) \in \mathbb{A}^2 \mid \begin{pmatrix} x & 2x \\ y & y \end{pmatrix} \text{ è diagonalizzabile} \right\}.$$

**9.13.** Dimostrare che unione finita di spazi topologici Noetheriani è Noetheriana.

**9.14.** Dimostrare che in uno spazio topologico di Hausdorff ogni sottospazio irriducibile non vuoto è formato da un solo punto.

**9.15.** Sia  $f: X \rightarrow Y$  un'applicazione continua ed aperta. Se le fibre di  $f$  sono irriducibili e  $Z \subset Y$  è irriducibile, provare che  $f^{-1}(Z)$  è irriducibile.

**9.16.** Sia  $\{Y_i\}$  una catena ascendente di sottospazi irriducibili di uno spazio topologico (non necessariamente Noetheriano). Dimostrare che  $\cup Y_i$  e  $\overline{\cup Y_i}$  sono irriducibili. Utilizzare il Lemma di Zorn per dedurre che ogni chiuso irriducibile è contenuto in una componente irriducibile e che ogni spazio topologico è unione delle sue componenti irriducibili.

**9.17.** Sia  $X = X_1 \cup X_2$  con  $X_1, X_2$  aperti irriducibili non vuoti. Dimostrare che  $X$  è irriducibile se e solo se  $X_1 \cap X_2 \neq \emptyset$ .

**9.18.** Provare che ogni spazio topologico Noetheriano di Hausdorff è finito.

## 9.4 La dimensione combinatoria di uno spazio topologico

**Definizione 9.4.1.** Sia  $X$  uno spazio topologico e  $Y \subset X$  un sottospazio irriducibile. La **codimensione combinatoria**

$$\text{codim}(Y, X) \in \mathbb{N} \cup \{+\infty\}$$

di  $Y$  in  $X$  è per definizione l'estremo superiore dell'insieme dei numeri naturali  $n$  per i quali esiste una catena  $Y \subset Z_n \subset Z_{n-1} \subset \dots \subset Z_0 \subset X$ , dove gli  $Z_i$  sono chiusi irriducibili e  $Z_i \neq Z_{i-1}$  per ogni  $i$ .

Osserviamo che i punti sono irriducibili e quindi, se  $p \in X$  è un punto, allora ha senso considerarne la codimensione. Per definizione  $\text{codim}(p, X)$  è uguale all'estremo superiore dell'insieme dei numeri naturali  $n$  tali che esiste una catena  $p \in Z_n \subset Z_{n-1} \subset \dots \subset Z_0 \subset X$ , dove gli  $Z_i$  sono chiusi irriducibili e  $Z_i \neq Z_{i-1}$  per ogni  $i$ .

**Definizione 9.4.2.** La **dimensione combinatoria** di uno spazio topologico  $X$  è l'estremo superiore delle codimensioni combinatorie dei suoi punti, cioè

$$\dim X = \sup\{\text{codim}(p, X) \mid p \in X\}.$$

Se  $p \in X$  è un punto, la **dimensione di  $X$  in  $p$**  è l'estremo inferiore delle dimensioni degli aperti di  $X$  contenenti  $p$ , cioè

$$\dim_p X = \inf\{\dim U \mid p \in U \text{ e } U \subset X \text{ aperto}\}.$$

Poniamo per convenzione uguale a  $-1$  la dimensione dell'insieme vuoto. Conveniamo inoltre che se  $p \notin X$ , allora  $\dim_p X = \text{codim}(p, X) = -1$ .

Da ora in poi, quando non ci sarà rischio di confusione, scriveremo semplicemente **dimensione** (risp.: **codimensione**) intendendo la **dimensione** (risp.: **codimensione**) combinatoria.

Uno spazio avente la stessa dimensione in tutti i suoi punti è detto **equidimensionale** o di **dimensione pura**.

Sebbene le Definizioni 9.4.1 e 9.4.2 abbiano senso per qualsiasi spazio topologico, esse perdono tutto il loro significato geometrico e la sua utilità se applicate agli spazi di Hausdorff. Per tale motivo da ora in poi studieremo la dimensione esclusivamente per spazi topologici Noetheriani.

**Lemma 9.4.3.** *Siano  $\{X_i \mid i \in I\}$  le componenti irriducibili di uno spazio topologico Noetheriano  $X$ . Allora*

$$\dim X = \sup\{\dim X_i \mid i \in I\}$$

e per ogni punto  $p \in X$  vale

$$\dim_p X = \sup\{\dim_p X_i \mid p \in X_i\}, \quad \text{codim}(p, X) = \sup\{\text{codim}(p, X_i) \mid p \in X_i\}.$$

*Dimostrazione.* Esercizio. □

**Lemma 9.4.4.** *Siano  $X$  uno spazio topologico e  $Y \subset X$  un sottospazio. Allora*

$$\dim Y \leq \dim X$$

e per ogni punto  $p \in Y$  vale

$$\dim_p Y \leq \dim_p X, \quad \text{codim}(p, Y) \leq \text{codim}(p, X).$$

*Dimostrazione.* Sia  $Z \subset Y$  chiuso irriducibile e  $\bar{Z}$  la chiusura di  $Z$  in  $X$ . Dalla formula  $Z = Y \cap \bar{Z}$  segue che la chiusura in  $X$  trasforma inclusioni proprie di chiusi irriducibili di  $Y$  in inclusioni proprie di chiusi irriducibili di  $X$ . Questo prova che  $\text{codim}(p, Y) \leq \text{codim}(p, X)$  per ogni  $p \in Y$  e quindi che  $\dim Y \leq \dim X$ . Lo stesso argomento mostra che per ogni aperto  $U$  di  $X$  vale  $\dim(Y \cap U) \leq \dim U$  e quindi che  $\dim_p Y \leq \dim_p X$ . □

Segue immediatamente dal Lemma 9.4.4 che la dimensione in un punto è un invariante locale cioè, se  $U \subset X$  è un aperto contenente un punto  $p$ , allora  $\dim_p U = \dim_p X$ . La proprietà analoga per la codimensione richiede una diversa dimostrazione.

**Lemma 9.4.5.** *La codimensione di un punto è un invariante locale, cioè se  $U \subset X$  è un intorno di  $p$ , allora vale  $\text{codim}(p, U) = \text{codim}(p, X)$ .*

*Dimostrazione.* Per il Lemma 9.4.4 non è restrittivo supporre  $U$  aperto. Se  $p \in Z \subset X$  è un chiuso irriducibile e  $Z \cap U = Z_1 \cup Z_2$ , con  $Z_1, Z_2$  chiusi di  $U$ , allora  $Z = (Z - U) \cup \overline{(Z \cap U)} = Z = (Z - U) \cup \overline{Z_1} \cup \overline{Z_2}$  e, dato che  $p \notin Z - U$ , si ha che  $Z = \overline{Z_i}$  per qualche  $i$ . In particolare  $Z \cap U$  è irriducibile,  $Z = \overline{Z \cap U}$  e la restrizione ad  $U$  trasforma inclusioni proprie di chiusi irriducibili di  $X$  contenenti  $p$  in inclusioni proprie di chiusi irriducibili di  $U$ . □

**Corollario 9.4.6.** *Per ogni punto  $p$  di uno spazio topologico  $X$  vale*

$$\text{codim}(p, X) \leq \dim_p X.$$

*Dimostrazione.* Per ogni aperto  $U$  che contiene  $p$  vale  $\text{codim}(p, X) = \text{codim}(p, U) \leq \dim U$ . □

Mostreremo più avanti che se  $X$  è un sottoinsieme localmente chiuso di uno spazio affine o proiettivo, allora vale  $\text{codim}(p, X) = \dim_p X$  per ogni punto  $p$ . Esistono spazi topologici, molto importanti nella geometria algebrica più avanzata, dove la codimensione in un punto può essere strettamente minore della dimensione nello stesso punto (per un esempio vedere l'Esercizio 9.28).

Essendo le definizioni di dimensione e codimensione puramente topologiche, esse sono invarianti per omeomorfismo. Un utile lemma è il seguente:

**Lemma 9.4.7.** *Sia  $X$  uno spazio topologico irriducibile non vuoto di dimensione finita. Allora per ogni chiuso proprio  $Y \subset X$  e per ogni punto  $p \in Y$  vale  $\text{codim}(p, Y) < \text{codim}(p, X)$  e conseguentemente  $\dim Y < \dim X$ .*

*Dimostrazione.* Sia  $n < +\infty$  la codimensione di  $p$  in  $X$  e si assuma per assurdo che esista una catena di  $n$  inclusioni proprie di chiusi irriducibili di  $Y$  contenenti  $p$ , diciamo  $p \in Z_n \subset Z_{n-1} \subset \cdots \subset Z_0 \subset Y$ . Poiché  $X \neq Y$  si avrebbe che la catena di chiusi irriducibili  $p \in Z_n \subset \cdots \subset Z_0 \subset X$  sarebbe propria e quindi  $\text{codim}(p, X) \geq n + 1$ .  $\square$

*Osservazione 9.4.8.* Esistono spazi Noetheriani di dimensione infinita (cfr. Esercizio 9.27).

**Lemma 9.4.9.** *Sia  $f: X \rightarrow Y$  un'applicazione continua, chiusa e surgettiva tra spazi topologici Noetheriani e sia  $y \in Y$  un punto fissato. Allora per ogni numero naturale  $n \leq \text{codim}(y, Y)$  esiste un punto  $x \in X$ , dipendente da  $n$ , tale che  $f(x) = y$  e  $\text{codim}(x, X) \geq n$ .*

*Di conseguenza  $\dim X \geq \dim Y$  e, se la fibra su  $y$  contiene un solo punto  $x$ , cioè  $f^{-1}(y) = \{x\}$ , allora  $\text{codim}(x, X) \geq \text{codim}(y, Y)$ .*

*Dimostrazione.* Per ogni catena finita  $y \in Z_n \subset \cdots \subset Z_0$  di chiusi irriducibili di  $Y$  costruiamo una catena  $H_n \subset \cdots \subset H_0$  di chiusi irriducibili di  $X$  tali che  $f(H_i) = Z_i$ . Basterà poi considerare un qualsiasi punto  $x \in H_n \cap f^{-1}(y)$ . Essendo  $f^{-1}(Z_0)$  un chiuso in uno spazio Noetheriano esso è unione di un numero finito di componenti irriducibili, diciamo  $f^{-1}(Z_0) = W_1 \cup \cdots \cup W_s$ . I chiusi  $f(W_j)$  ricoprono  $Z_0$  e per l'irriducibilità esiste un indice  $j$  tale che  $f(W_j) = Z_0$ . Poniamo  $H_0 = W_j$  e ripetiamo il ragionamento con  $H_0$  al posto di  $X$  e  $Z_1$  al posto di  $Z_0$ .  $\square$

## Esercizi

**9.19.** Dato uno spazio topologico  $X$ , un'applicazione  $f: X \rightarrow \mathbb{N} \cup \{+\infty\}$  si dice semicontinua superiormente se per ogni  $p \in X$  esiste un aperto  $U \subset X$  tale che  $p \in U$  e  $f(q) \leq f(p)$  per ogni  $q \in U$ . Equivalentemente  $f$  è semicontinua superiormente se per ogni  $n \in \mathbb{N} \cup \{+\infty\}$  il sottoinsieme  $\{p \in X \mid f(p) \geq n\}$  è chiuso. Dimostrare che l'applicazione  $p \mapsto \dim_p X$  è semicontinua superiormente.

## 9.5 La dimensione dello spazio affine

Dimostriamo adesso che la dimensione di  $\mathbb{A}^n$  è uguale a  $n$ . Tale risultato, associato all'esistenza delle proiezioni normalizzate, permetterà di trovare un'utile caratterizzazione della dimensione dei chiusi affini e proiettivi.

**Lemma 9.5.1.** *Un sottoinsieme chiuso  $X \subset \mathbb{A}^n$  è irriducibile se e solo se  $I(X)$  è un ideale primo.*

*Dimostrazione.* Se  $X = X_1 \cup X_2$  con  $X_i$  chiusi propri, allora esistono  $f_i \in I(X_i) - I(X)$ ,  $i = 1, 2$ . Chiaramente  $f_1 f_2 \in I(X)$  e quindi  $I(X)$  non è primo.

Viceversa se  $f_1, f_2 \notin I(X)$  e  $f_1 f_2 \in I(X)$  allora possiamo scrivere  $X = X_1 \cup X_2$  dove  $X_i = X \cap V(f_i)$  è un chiuso proprio e dunque  $X$  non è irriducibile.  $\square$

**Corollario 9.5.2.** *Lo spazio affine  $\mathbb{A}^n$  è uno spazio topologico Noetheriano irriducibile.*

*Dimostrazione.* L'ideale  $I(\mathbb{A}^n) = 0$  è primo.  $\square$

**Definizione 9.5.3.** *Sia  $X \subset \mathbb{A}^n$  un chiuso di Zariski. Diremo che la proiezione lineare sulle prime  $s$  coordinate  $\mathbb{A}^n \rightarrow \mathbb{A}^s$  è **normalizzata** rispetto a  $X$  se per ogni indice  $i = s + 1, s + 2, \dots, n$  esiste un polinomio  $f_i \in I(X) \cap \mathbb{K}[x_1, \dots, x_s][x_i] \subset \mathbb{K}[x_1, \dots, x_n]$  che è monico di grado positivo rispetto alla variabile  $x_i$ .*

Segue dal Lemma di Proiezione 4.4.3 e da una semplice induzione su  $n - s$  che, se  $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^s$  è normalizzata rispetto a  $X$ , allora  $\pi: X \rightarrow \mathbb{A}^s$  è un'applicazione chiusa e  $I(\pi(X)) = I(X) \cap \mathbb{K}[x_1, \dots, x_s]$ .

**Lemma 9.5.4.** *Supponiamo che la proiezione sulle prime  $n-1$  coordinate  $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$  sia normalizzata rispetto ad un chiuso irriducibile non vuoto  $X \subset \mathbb{A}^n$ . Allora per ogni chiuso proprio  $Z \subset X$  vale  $\pi(Z) \neq \pi(X)$ .*

*Dimostrazione.* Per il Lemma 4.4.3, la proiezione  $\pi: X \rightarrow \mathbb{A}^{n-1}$  è un'applicazione chiusa,  $I(\pi(X)) = I(X) \cap \mathbb{K}[x_1, \dots, x_{n-1}]$  e  $I(\pi(Z)) = I(Z) \cap \mathbb{K}[x_1, \dots, x_{n-1}]$ . Dato che  $\pi(X)$  è irriducibile e  $Z$  è unione finita di irriducibili, non è restrittivo supporre  $Z$  irriducibile e non vuoto. Siccome  $I(X) \subset I(Z)$  sono ideali primi,  $1 \notin I(Z)$  e  $I(X)$  contiene un polinomio monico in  $x_n$ , per il Corollario 4.1.10 si ha  $I(X) \cap \mathbb{K}[x_1, \dots, x_{n-1}] \neq I(Z) \cap \mathbb{K}[x_1, \dots, x_{n-1}]$  e quindi  $\pi(X) \neq \pi(Z)$ .  $\square$

**Proposizione 9.5.5.** *Se la proiezione sulle prime coordinate  $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$  sia normalizzata rispetto ad un chiuso irriducibile non vuoto  $X \subset \mathbb{A}^n$ , allora  $\dim X = \dim \pi(X)$  e per ogni punto  $p \in X$  vale  $\text{codim}(p, X) \leq \text{codim}(\pi(p), \pi(X))$ .*

*Dimostrazione.* Per il Lemma 9.5.4, la proiezione  $\pi$  trasforma inclusioni proprie di chiusi irriducibili di  $X$  contenenti  $p$  in inclusioni proprie di chiusi irriducibili di  $\pi(X)$  contenenti  $\pi(p)$ : questo prova che  $\text{codim}(p, X) \leq \text{codim}(\pi(p), \pi(X)) \leq \dim \pi(X)$  e quindi  $\dim X \leq \dim \pi(X)$ . D'altronde per il Lemma 9.4.9  $\dim X \geq \dim \pi(X)$  e quindi  $\dim X = \dim \pi(X)$ .  $\square$

**Teorema 9.5.6.** *Sia  $X \subset \mathbb{A}^n$  un chiuso irriducibile. Allora  $\dim X + \text{codim}(X, \mathbb{A}^n) = n$  e quindi  $\dim \mathbb{A}^n = n - \text{codim}(\mathbb{A}^n, \mathbb{A}^n) = n$ . Inoltre se  $X \subset \mathbb{A}^n$  e  $Y \subset \mathbb{A}^m$  sono chiusi irriducibili, allora  $X \times Y \subset \mathbb{A}^{n+m}$  è irriducibile di dimensione  $\dim X \times Y = \dim X + \dim Y$ .*

*Dimostrazione.* Proviamo inizialmente, per induzione su  $n$  che  $\dim \mathbb{A}^n = n$ . Gli unici chiusi propri irriducibili di  $\mathbb{A}^1$  sono i punti, quindi il teorema è vero per  $n = 1$ ; per induzione possiamo supporre il teorema vero per  $\mathbb{A}^{n-1}$ . Esiste una ovvia catena di chiusi irriducibili  $0 = Z_n \subset \dots \subset Z_1 \subset Z_0 = \mathbb{A}^n$ , dove  $Z_i = \{x_1 = \dots = x_i = 0\}$ , dalla quale segue che  $\dim \mathbb{A}^n \geq n$ . Per ogni chiuso proprio irriducibile  $X \subset \mathbb{A}^n$  si ha  $\dim X < n$ ; infatti a meno di un cambio lineare di coordinate la proiezione  $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$  è normalizzata rispetto a  $X$  e per la Proposizione 9.5.5 si ha  $\dim X = \dim \pi(X) \leq \dim \mathbb{A}^{n-1} = n - 1$ . Questo prova che  $\dim \mathbb{A}^n = n$ . Consideriamo adesso due chiusi irriducibili  $X \subset \mathbb{A}^n$ ,  $Y \subset \mathbb{A}^m$ ; dal Lemma 9.3.6 segue che anche  $X \times Y$  è irriducibile. Quindi se  $Z \subset \mathbb{A}^{n-1}$  è un chiuso irriducibile, allora anche  $\pi^{-1}(Z) = Z \times \mathbb{A}^1$  è irriducibile in  $\mathbb{A}^n$ . Poiché  $\pi^{-1}(\pi(X)) \neq X$  si ha che  $\text{codim}(X, \mathbb{A}^n) \geq \text{codim}(\pi(X), \mathbb{A}^{n-1}) + 1$  e quindi per l'ipotesi induttiva

$$\dim(X) + \text{codim}(X, \mathbb{A}^n) \geq \dim \pi(X) + \text{codim}(\pi(X), \mathbb{A}^{n-1}) + 1 = n.$$

D'altra parte per ogni chiuso irriducibile  $X$  in uno spazio topologico  $Y$  vale  $\dim X + \text{codim}(X, Y) \leq \dim Y$  e quindi vale l'uguaglianza  $\dim(X) + \text{codim}(X, \mathbb{A}^n) = n$ . Consideriamo adesso due chiusi irriducibili  $X_a \subset \mathbb{A}^n$ ,  $Y_b \subset \mathbb{A}^m$  di dimensioni  $a = \dim X_a$ ,  $b = \dim Y_b$ . Esistono allora catene strettamente crescenti di chiusi irriducibili non vuoti

$$X_0 \subset \dots \subset X_a \subset \dots \subset X_n = \mathbb{A}^n, \quad Y_0 \subset \dots \subset Y_b \subset \dots \subset Y_m = \mathbb{A}^m.$$

Le catene

$$X_0 \times Y_0 \subset X_0 \times Y_1 \subset \dots \subset X_0 \times Y_b \subset X_1 \times Y_b \subset \dots \subset X_a \times Y_b$$

e

$$X_a \times Y_b \subset X_a \times Y_{b+1} \subset \cdots \subset X_a \times Y_m \subset X_{a+1} \times Y_m \subset \cdots \subset X_n \times Y_m$$

mostrano che  $\dim X_a \times Y_b \geq a + b$  e che  $\text{codim}(X_a \times Y_b, \mathbb{A}^{n+m}) \geq n + m - a - b$ .  $\square$

La dimostrazione di 9.5.5 fornisce, assieme al Teorema 9.5.6, una ricetta per il calcolo della dimensione di un chiuso affine  $X$ ; basta infatti eseguire una serie di proiezioni  $\pi_n: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}, \dots, \pi_{s+1}: \mathbb{A}^{s+1} \rightarrow \mathbb{A}^s$  normalizzate rispetto a  $X$ ,  $\pi_n(X)$  ecc... in modo tale che  $\pi_{s+1}\pi_{s+2}\cdots\pi_n(X) = \mathbb{A}^s$ . La dimensione di  $X$  sarà quindi uguale a  $s$ .

Concludiamo il paragrafo analizzando in dettaglio il caso delle ipersuperfici. Abbiamo già osservato che  $V(f)$  è irriducibile se  $f$  è irriducibile. In generale se  $f_1, \dots, f_r$  sono i fattori irriducibili di  $f$  vale  $V(f) = V(f_1) \cup \cdots \cup V(f_r)$  e i chiusi  $V(f_i)$  sono esattamente le componenti irriducibili di  $V(f)$ .

**Proposizione 9.5.7.** *Siano  $X \subset \mathbb{A}^n$  una ipersuperficie e  $p \in X$  un punto di essa. Allora vale  $\text{codim}(p, X) = n - 1$  e quindi  $X$  ha dimensione pura  $n - 1$ . Viceversa se  $X \subset \mathbb{A}^n$  è un chiuso irriducibile di dimensione  $n - 1$  allora  $X$  è un'ipersuperficie.*

*Dimostrazione.* Dato che tutte le componenti irriducibili di  $X$  sono ipersuperfici non è restrittivo supporre  $X = V(f)$  irriducibile. Se  $n = 1$  l'asserto è banale; possiamo quindi supporre  $n > 1$  ed assumere il teorema vero per ipersuperfici in  $\mathbb{A}^{n-1}$ . Poiché  $X$  è infinito, possiamo trovare un iperpiano affine  $H$  passante per  $p$  tale che  $H \cap X$  è strettamente contenuta sia in  $H$  che in  $X$ . L'intersezione  $X \cap H$  è una ipersuperficie in  $H = \mathbb{A}^{n-1}$  e per induzione

$$n - 2 = \text{codim}(p, X \cap H) < \text{codim}(p, X) < n = \dim \mathbb{A}^n.$$

Viceversa, se  $X \subset \mathbb{A}^n$  è irriducibile di dimensione  $n - 1$ , allora l'ideale  $I(X) \neq 0$  è primo e contiene un polinomio irriducibile  $f$ . Dunque  $X \subset V(f)$  e  $\dim X = \dim V(f) < +\infty$ . Dato che  $V(f)$  è irriducibile, il Lemma 9.4.7 implica che  $X = V(f)$ .  $\square$

## Esercizi

**9.20 (Lemma di normalizzazione di E. Noether).** Dimostrare:

1. Siano  $\pi_1: \mathbb{A}^n \rightarrow \mathbb{A}^s, \pi_2: \mathbb{A}^s \rightarrow \mathbb{A}^r$  proiezioni normalizzate rispetto a  $X$  e  $\pi_1(X)$  rispettivamente. Allora  $\pi_2 \circ \pi_1$  è normalizzata rispetto a  $X$ . (Sugg.: estensioni intere per gli esperti, induzione su  $s - r$  e risultante per gli inesperti.)
2. Sia  $X \subset \mathbb{A}^n$  un chiuso di dimensione  $s$ . Allora, a meno di un cambio lineare di coordinate, la proiezione sulle prime  $s$  coordinate è normalizzata rispetto a  $X$ .

## 9.6 La dimensione delle intersezioni

Una delle caratteristiche fondamentali degli spazi considerati nella geometria algebrica classica (pre teoria degli schemi) è che ogni punto possiede un sistema fondamentale di intorno omeomorfo a chiusi affini. D'altra parte ogni chiuso affine può essere pensato come un aperto di un chiuso proiettivo; è quindi possibile studiare le proprietà locali, come ad esempio la dimensione in un punto, restringendo la nostra attenzione alla classe dei chiusi proiettivi. Osserviamo innanzitutto che il gruppo delle proiettività agisce transitivamente su  $\mathbb{P}^n$  e che quindi  $\dim \mathbb{P}^n = \dim_p \mathbb{P}^n = \text{codim}(p, \mathbb{P}^n)$  per ogni punto  $p$ .

**Teorema 9.6.1.** *Lo spazio proiettivo  $\mathbb{P}^n$ , dotato della topologia di Zariski, è uno spazio irriducibile Noetheriano di dimensione pura  $n$ . Per ogni chiuso irriducibile non vuoto  $X \subset \mathbb{P}^n$  vale  $\dim X + \text{codim}(X, \mathbb{P}^n) = n$ .*

*Dimostrazione.* Siccome ogni punto possiede un intorno omeomorfo ad  $\mathbb{A}^n$  si deduce immediatamente che  $\dim \mathbb{P}^n = n$ . Se  $X$  è irriducibile e non vuoto, allora esiste un iperpiano  $H$  che non lo contiene e valgono le disuguaglianze  $\dim(X - H) \leq \dim X$  e  $\text{codim}(X - H, \mathbb{P}^n - H) \leq \text{codim}(X, \mathbb{P}^n)$ . Basta adesso osservare che

$$n = \dim(X - H) + \text{codim}(X - H, \mathbb{P}^n - H) \leq \dim(X) + \text{codim}(X, \mathbb{P}^n) \leq \dim \mathbb{P}^n = n.$$

□

Uno dei vantaggi dei chiusi proiettivi è la mancanza di asintoti e quindi la normalizzazione automatica delle proiezioni.

**Lemma 9.6.2.** *Siano  $X \subset \mathbb{P}^n$  un chiuso,  $o \notin X$  un punto e  $\pi: (\mathbb{P}^n - \{o\}) \rightarrow \mathbb{P}^{n-1}$  la proiezione di centro  $o$ . Allora:*

1. *Ogni fibra di  $\pi: X \rightarrow \pi(X)$  ha cardinalità finita.*
2.  *$\pi(X)$  è chiuso in  $\mathbb{P}^{n-1}$  e  $\dim X = \dim \pi(X)$ .*
3. *Per ogni  $p \in X$  si ha  $\text{codim}(p, X) \leq \text{codim}(\pi(p), \pi(X))$  e vale  $\text{codim}(p, X) = \text{codim}(\pi(p), \pi(X))$  se  $X$  interseca la retta  $\overline{op}$  solamente nel punto  $p$ .*

*Dimostrazione.* Siano  $x_0, \dots, x_n$  coordinate omogenee su  $\mathbb{P}^n$  tali che  $o = [1, 0, \dots, 0]$ , allora la proiezione si esprime in coordinate omogenee come  $\pi([x_0, \dots, x_n]) = [x_1, \dots, x_n]$ . Dato che  $o \notin X$ , esiste un polinomio omogeneo  $f \in I(X)$  tale che  $f(o) \neq 0$ . Necessariamente  $f$  è un multiplo scalare di un polinomio monico in  $x_0$ , basta quindi applicare i risultati del paragrafo precedente alle restrizioni  $\pi_i: X \cap \mathbb{A}_i^n \rightarrow H \cap \mathbb{A}_i^n = \mathbb{A}^{n-1}$  dove  $\mathbb{A}_i^n = \{x_i \neq 0\}$  per ogni  $i = 1, \dots, n$ . □

Nel seguente corollario continueremo ad usare la convenzione che la dimensione dell'insieme vuoto è  $-1$ .

**Corollario 9.6.3.** *Sia  $X \subset \mathbb{P}^n$  un chiuso e sia  $\mathcal{F}$  la famiglia dei sottospazi proiettivi di  $\mathbb{P}^n$  che non intersecano  $X$ . Se  $K \in \mathcal{F}$  è un elemento massimale rispetto all'inclusione, allora  $\dim X + \dim K = n - 1$ .*

*Dimostrazione.* Il risultato è banalmente vero se  $X = \emptyset, \mathbb{P}^n$  oppure  $n = 1$ . Se  $X \neq \emptyset, \mathbb{P}^n$ , allora prendiamo un punto  $o \in K$  e denotiamo con  $\pi: X \rightarrow \mathbb{P}^{n-1}$  la proiezione di centro  $o$ . Per il Lemma 9.6.2, i chiusi  $X$  e  $\pi(X)$  hanno la stessa dimensione, mentre  $\dim \pi(K) = \dim K - 1$ . Dato che  $\pi(K)$  è chiaramente massimale tra i sottospazi di  $\mathbb{P}^{n-1}$  che non intersecano  $\pi(X)$ , l'induzione su  $n$  conclude la dimostrazione. □

**Lemma 9.6.4.** *Siano  $X \subset \mathbb{P}^n$  un chiuso di dimensione  $\leq n - 2$  e  $p \in X$  un punto qualsiasi. Allora esiste un punto  $o \neq p$  tale che la retta  $\overline{op}$  interseca  $X$  solamente nel punto  $p$ .*

*Dimostrazione.* Per il Corollario 9.6.3 esiste una retta  $L \subset \mathbb{P}^n$  che non interseca  $X$ ; indichiamo con  $P$  il piano proiettivo generato dalla retta  $L$  e dal punto  $p$ . Dato che  $(X \cap P) \cap L = \emptyset$ , per il Corollario 9.6.3 la dimensione di  $X \cap P$  è uguale a 0. Dunque  $X \cap P$  è un insieme finito di punti ed esistono al più finiti punti  $o \in L$  che non soddisfano la condizione richiesta. □

**Teorema 9.6.5.** *Siano  $X \subset \mathbb{P}^n$  un chiuso,  $H$  un iperpiano e  $p \in X \cap H$  un punto:*

1. *Se  $p \in Z \subset X$  è un sottoinsieme chiuso irriducibile, allora  $\text{codim}(p, X) \geq \dim Z$ .*
2. *Se  $X$  è irriducibile, allora  $\text{codim}(p, X) = \dim_p X = \dim X$ .*
3.  *$\text{codim}(p, X \cap H) \geq \text{codim}(p, X) - 1$ . In particolare se  $X$  è irriducibile tutte le componenti di  $X \cap H$  hanno la stessa dimensione.*

*Dimostrazione.* Se  $n = 1$  il teorema è evidente, per induzione su  $n$  possiamo assumere vero il teorema per chiusi di  $\mathbb{P}^{n-1}$ . Osserviamo che se il teorema vale per ogni componente irriducibile di  $X$  allora vale anche per  $X$ , non è quindi restrittivo assumere  $X$  chiuso proprio irriducibile e  $Z = X$ .

Se  $X$  è una ipersuperficie abbiamo già dimostrato che  $\text{codim}(p, X) = \dim X = n - 1$  e  $X \cap H$  è ancora una ipersuperficie e quindi  $\text{codim}(p, X \cap H) \geq n - 2$ . Se  $X$  non è una ipersuperficie allora  $\dim X < n - 1$  e per il Lemma 9.6.4 esiste una proiezione  $\pi: X \rightarrow \mathbb{P}^{n-1}$  tale che  $\pi^{-1}(\pi(p)) = p$ ; per induzione su  $n$  si ricava

$$\text{codim}(p, X) = \text{codim}(\pi(p), \pi(X)) = \dim \pi(X) = \dim X.$$

Sia  $Y = X \cap H$ ; se  $X = Y$ , allora il punto 3) è banale; se  $Y$  è un chiuso proprio di  $X$ , allora  $\dim Y < \dim X$  e quindi  $\dim Y \leq \dim H - 2$ . Per 9.6.4 esiste una proiezione  $\pi: X \rightarrow \mathbb{P}^{n-1}$  di centro  $o \in H$  tale che  $\pi^{-1}(\pi(p)) = p$ . Dunque  $\text{codim}_p Y = \text{codim}(\pi(p), \pi(Y))$  e la conclusione segue osservando che  $\pi(Y)$  è una sezione iperpiana di  $\pi(X)$ .  $\square$

**Corollario 9.6.6.** *Sia  $U \subset \mathbb{P}^n$  un sottoinsieme localmente chiuso. Allora per ogni punto  $p \in U$  vale  $\text{codim}(p, U) = \dim_p U$  e, se  $U$  è irriducibile, allora  $U$  è equidimensionale.*

*Dimostrazione.* Sia  $X = \overline{U}$  la chiusura proiettiva di  $U$ . Poiché  $U$  è aperto in  $X$ , per il Lemma 9.4.5 vale  $\text{codim}(p, U) = \text{codim}(p, X)$  e  $\dim_p U = \dim_p X$ ; se  $U$  è irriducibile anche  $X$  è irriducibile e se  $X$  è equidimensionale anche  $U$  è equidimensionale. Non è quindi restrittivo assumere  $U = X$  chiuso. Sempre per il Lemma 9.4.5 possiamo assumere che ogni componente irriducibile di  $X$  passi per il punto  $p$ . Per il Teorema 9.6.5 si ha  $\text{codim}(p, X) \geq \dim Z$  per ogni componente irriducibile  $Z$  di  $X$  e quindi  $\text{codim}(p, X) \geq \dim X \geq \dim_p X \geq \text{codim}(p, X)$ .  $\square$

Da ora in poi, per semplicità notazionale ed economia di concetti, quando avremo a che fare con sottospazi localmente chiusi di  $\mathbb{P}^n$  useremo sempre la notazione  $\dim_p X$  anche quando dal contesto sarebbe più logico scrivere  $\text{codim}(p, X)$ .

Grazie all'immersione di Veronese, che sappiamo essere una immersione topologica chiusa, possiamo generalizzare immediatamente e senza fatica i precedenti risultati alle intersezioni di chiusi di  $\mathbb{P}^n$  con ipersuperfici.

**Corollario 9.6.7.** *Sia  $X \subset \mathbb{P}^n$  chiuso e  $H \subset \mathbb{P}^n$  ipersuperficie, allora se  $\dim X > 0$  vale  $X \cap H \neq \emptyset$  e per ogni  $p \in X \cap H$  si ha  $\dim_p(X \cap H) \geq \dim_p X - 1$ . In particolare  $n$  ipersuperfici in  $\mathbb{P}^n$  hanno intersezione non vuota.*

*Dimostrazione.* Supponiamo  $H = V(f)$ , con  $f$  polinomio omogeneo di grado  $d$ . Se  $v_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$  indica la  $d$ -esima immersione di Veronese, allora esiste un unico iperpiano  $W \subset \mathbb{P}^N$  tale che  $v_d^{-1}(W) = H$  e quindi  $v_d(X \cap H)$  è omeomorfo all'intersezione di  $v_d(X)$  con  $W$ .  $\square$

**Corollario 9.6.8 (Versione geometrica del teorema dell'ideale principale di Krull).** *Siano  $X \subset \mathbb{A}^n$  un chiuso e  $H \subset \mathbb{A}^n$  ipersuperficie affine. Allora per ogni  $p \in X \cap H$  vale  $\dim_p(X \cap H) \geq \dim_p X - 1$ .*

*Dimostrazione.* Immergiamo  $\mathbb{A}^n$  in uno spazio proiettivo  $\mathbb{P}^n$  e prendiamo le chiusure di  $X$  e  $H$ . Basta osservare adesso che la chiusura proiettiva di una ipersuperficie è ancora una ipersuperficie, più precisamente se  $f \in \mathbb{K}[x_1, \dots, x_n]$  ha grado  $d$  e  $H = V(f)$ , la chiusura di  $H$  in  $\mathbb{P}^n$  è l'ipersuperficie definita dall'omogeneizzato di  $f$  in  $\mathbb{K}[x_0, x_1, \dots, x_n]$ .  $\square$

**Teorema 9.6.9.** *Sia  $X \subset \mathbb{A}^n$  un chiuso affine. Allora la dimensione di  $X$  in un suo punto  $p$  è uguale al minimo intero  $s$  per il quale esistono  $s$  polinomi  $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$  ed un aperto  $U \subset X$  tali che  $U \cap V(f_1, \dots, f_s) = p$ .*



*Dimostrazione.* Se  $U \cap V(f_1, \dots, f_s) = p$ , allora per il Corollario 9.6.8  $0 = \dim\{p\} \geq \dim_p U - s$  e quindi  $\dim_p X \leq s$ . Viceversa se  $\dim_p X = d > 0$ , allora possiamo trovare un iperpiano  $H_1 = V(f_1)$  passante per  $p$  e non contenente alcuna componente irriducibile di  $X$ . Abbiamo  $\dim_p(X \cap H_1) = \dim_p X - 1$  e, ripetendo  $d$  volte il ragionamento, possiamo trovare  $d$  iperpiani  $H_1, \dots, H_d$  tali che  $\dim_p X \cap H_1 \cap \dots \cap H_d = 0$  e quindi  $d \geq s$ .  $\square$

*Osservazione 9.6.10.* Il Teorema 9.6.9 è la versione geometrica del teorema [AM1969, 11.14] di algebra commutativa secondo il quale la dimensione di un anello locale Noetheriano con ideale massimale  $\mathfrak{m}$  è uguale al minimo numero di generatori di un ideale  $\mathfrak{m}$ -primario (vedi Esercizio 13.15).

**Corollario 9.6.11.** *Siano  $X, Y \subset \mathbb{A}^n$  chiusi affini e  $p \in X \cap Y$ . Allora vale*

$$\dim_p(X \cap Y) \geq \dim_p X + \dim_p Y - n.$$

*Dimostrazione.* Non è restrittivo supporre  $p = (0, \dots, 0)$  e i chiusi  $X, Y$  irriducibili. L'applicazione diagonale  $\mathbb{A}^n \rightarrow \mathbb{A}^n \times \mathbb{A}^n$ ,  $x \mapsto (x, x)$ , è un'immersione topologica chiusa ed induce un omeomorfismo tra  $X \cap Y$  e l'intersezione di  $X \times Y$  con la diagonale  $\Delta$ . Per il Teorema 9.5.6  $\dim_0 X + \dim_0 Y = \dim_0(X \times Y)$  e, dato che  $\Delta$  è data dall'intersezione di  $n$  iperpiani, per il Corollario 9.6.8

$$\dim_0(X \cap Y) = \dim_0(X \times Y \cap \Delta) \geq \dim_0 X + \dim_0 Y - n.$$

$\square$

*Esempio 9.6.12 (Il cono tangente ridotto).* Consideriamo la moltiplicazione per scalare

$$\phi: \mathbb{A}^1 \times \mathbb{A}^n \rightarrow \mathbb{A}^n, \quad \phi(t, x) = tx$$

e per ogni chiuso affine  $X \subset \mathbb{A}^n$  denotiamo con  $\hat{X} \subset \mathbb{A}^1 \times \mathbb{A}^n$  l'unione delle componenti irriducibili di  $\phi^{-1}(X)$  che non sono contenute in  $\{0\} \times \mathbb{A}^n$  e con  $C_0(X) = \hat{X} \cap (\{0\} \times \mathbb{A}^n)$ . Notiamo che  $\hat{X}$  è la chiusura di Zariski dell'insieme delle coppie  $(t, x)$  tali che  $t \neq 0$  e  $tx \in X$  e di conseguenza che  $C_0(X \cup Y) = C_0(X) \cup C_0(Y)$  per ogni coppia di chiusi  $X, Y$ . Se  $f \in \mathbb{K}[x_1, \dots, x_n]$  scriviamo  $f = f_m + f_{m+1} + \dots$  con  $f_i$  omogeneo di grado  $i$  e  $f_m \neq 0$ ; chiameremo  $m = \text{mult}_0(f)$  la molteplicità di  $f$  in 0 e  $f_m$  la forma iniziale di  $f$ . Vogliamo adesso dimostrare che:

1. Se  $X = V(I)$  per qualche ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$ , allora  $C_0(X)$  è il luogo di zeri delle forme iniziali degli elementi di  $I$ .
2.  $C_0(X) \neq \emptyset$  se e solo se  $0 \in X$ .
3.  $\dim_0 X = \dim C_0(X)$ .

Per dimostrare (1), osserviamo che se  $X = V(I)$ , allora  $\phi^{-1}(X)$  è il luogo di zeri dei polinomi  $g(t, x) = f(tx)$  al variare di  $f \in I$  e quindi  $\hat{X}$  è il luogo di zeri dei polinomi  $\hat{f}(t, x) := \frac{f(tx)}{t^m}$ , dove  $m = \text{mult}_0(f)$  e  $f$  varia in  $I$ . Ne segue che  $C_0(X)$  è il luogo di zeri dei polinomi  $\hat{f}(0, x)$ , con  $f \in I$ . Basta adesso osservare che  $\hat{f}(0, x)$  è esattamente la forma iniziale di  $f$ . Per dimostrare (2) notiamo che  $0 \in X$  se e solo se ogni  $f \in I$  ha molteplicità in 0 positiva e questo è equivalente a dire che 0 annulla tutte le forme iniziali degli elementi di  $I$ . Per dimostrare (3) possiamo assumere  $X$  irriducibile e  $0 \in X$ ; in particolare  $\dim_0 X = \dim X$ . Siano  $Y_1, \dots, Y_s$  le componenti irriducibili di  $\hat{X}$ , è chiaro che nessuna delle  $Y_i$  è contenuta in un iperpiano  $t = \text{costante}$ . Applicando il Corollario 9.6.8 all'intersezione di  $\hat{X}$  con gli iperpiani  $t = 1$  e  $t = 0$  otteniamo le uguaglianze  $\dim \hat{X} - 1 = \dim X$  e  $\dim C_0(X) = \dim \hat{X} - 1$ . Il cono  $C_0(X)$  si dice **cono tangente ridotto** a  $X$  nel punto 0.

*Esempio 9.6.13 (Coni proiettivi).* Sia  $X \subset \mathbb{P}^n$  un chiuso: identifichiamo  $\mathbb{P}^n$  con un iperpiano di  $\mathbb{P}^{n+1}$  e prendiamo un punto  $o \in \mathbb{P}^{n+1} - \mathbb{P}^n$ . L'insieme  $C_{\mathbb{P}}(X) \subset \mathbb{P}^{n+1}$ , unione delle rette  $\overline{op}$  al variare di  $p \in X$  si dice **cono proiettivo** di  $X$ . Possiamo trovare coordinate omogenee  $x_0, \dots, x_{n+1}$  in  $\mathbb{P}^{n+1}$  tali che  $o = [1, 0, \dots, 0]$  e l'iperpiano  $\mathbb{P}^n$  abbia equazione  $x_0 = 0$ . Per costruzione, un polinomio omogeneo  $f = \sum_i x_0^i f_i(x_1, \dots, x_{n+1})$  si annulla su  $C_{\mathbb{P}}(X)$  se e solo se tutti i  $f_i$  si annullano su  $X$ . Dunque  $C_{\mathbb{P}}(X)$  è il chiuso proiettivo definito da tutti i polinomi omogenei in  $x_1, \dots, x_{n+1}$  che si annullano in  $X$ .

Mostriamo adesso che se  $X$  è irriducibile, allora anche  $C_{\mathbb{P}}(X)$  è irriducibile di dimensione  $\dim X + 1$ . Se  $U, V \subset C_{\mathbb{P}}(X)$  sono aperti non vuoti, allora esiste un iperpiano  $H$  che non contiene  $o$  e che li interseca entrambi; siccome la proiezione di centro  $o$  induce una proiettività tra  $X$  e  $C_{\mathbb{P}}(X) \cap H$ , ne segue che  $U \cap V \cap H \neq \emptyset$ . Il computo della dimensione segue dal fatto che  $X$  è una sezione iperpiana propria di  $C_{\mathbb{P}}(X)$ . Si noti che la restrizione di  $C_{\mathbb{P}}(X)$  all'aperto affine  $x_0 \neq 0$  è isomorfa al cono affine  $C(X)$ .

**Teorema 9.6.14.** *Siano  $X, Y \subset \mathbb{P}^n$  chiusi irriducibili. Se  $\dim X + \dim Y \geq n$  allora  $X \cap Y \neq \emptyset$  e in ogni punto  $p \in X \cap Y$  vale  $\dim_p X \cap Y \geq \dim X + \dim Y - n$ .*

*Dimostrazione.* Basta mostrare che  $X \cap Y \neq \emptyset$ , essendo la stima sulla dimensione locale di  $X \cap Y$  conseguenza immediata del Corollario 9.6.11. Nelle notazioni dell'Esempio 9.6.13

$$\dim_o(C_{\mathbb{P}}(X) \cap C_{\mathbb{P}}(Y)) \geq (\dim X + 1) + (\dim Y + 1) - (n + 1) > 0$$

e quindi  $C_{\mathbb{P}}(X) \cap C_{\mathbb{P}}(Y)$  contiene almeno una retta passante per  $o$  che interseca l'iperpiano  $\mathbb{P}^n$  in un punto di  $X \cap Y$ .  $\square$

## Esercizi

**9.21.** Siano  $f, g \in \mathbb{K}[x_1, \dots, x_n]$  polinomi omogenei non nulli dello stesso grado  $d > 0$  e denotiamo  $X = V(x_0^d + f, g) \subset \mathbb{P}^n$ . Dimostrare che il chiuso  $X$  ha dimensione  $n - 2$  e che il numero delle sue componenti irriducibili non supera  $d$  volte il numero di componenti irriducibili dell'ipersuperficie  $V(g)$ . In caratteristica 0, trovare  $f$  e  $g$  come sopra tali che  $X$  ha esattamente  $d^2$  componenti irriducibili.

**9.22.** Mostrare con un esempio che, se  $X, Y, Z$  sono chiusi irriducibili di  $\mathbb{P}^n$  con  $X \cup Y \subset Z$  e  $\dim X + \dim Y \geq \dim Z$ , è generalmente falso che  $X \cap Y \neq \emptyset$ .

**9.23.** Nelle notazioni dell'Esempio 9.6.12, mostrare che, se  $g_1, \dots, g_r$  sono generatori dell'ideale  $I(X)$ , allora in generale  $C_0(X)$  non è definito dalle parti iniziali di  $g_1, \dots, g_r$ .

## 9.7 La dimensione delle fibre

Il principale risultato di questa sezione è noto come teorema sulla dimensione delle fibre ed è la versione moderna dell'ottocentesco **principio di Plücker-Clebsch** sul quale rimandiamo a [EC1915, Libro I, p. 149] per maggiori informazioni.

**Teorema 9.7.1.** *Sia  $X \subset \mathbb{A}^m \times \mathbb{P}^n$  un chiuso,  $\pi: X \rightarrow \mathbb{A}^m$  la proiezione sul primo fattore e per ogni  $q \in \mathbb{A}^m$  denotiamo  $X_q = \pi^{-1}(q) = X \cap (\{q\} \times \mathbb{P}^n)$ . Allora:*

1. Per ogni  $p \in X$  vale  $\dim_p X \leq \dim_p X_q + \dim_q \pi(X)$ , dove  $q = \pi(p)$ .
2. Per ogni intero  $h$ , l'insieme  $Y_h = \{q \in \mathbb{A}^m \mid \dim X_q \geq h\}$  è un chiuso di Zariski.
3. Se  $X$  è irriducibile, allora esiste un aperto denso  $U \subset \pi(X)$  tale che  $\dim X_q = \dim X - \dim \pi(X)$  per ogni  $q \in U$ .

*Dimostrazione.* [1] Sia  $r = \dim_q \pi(X)$ , esistono allora  $r$  iperpiani  $H_1, \dots, H_r$  di  $\mathbb{A}^m$  passanti per  $q$  tali che  $q$  è un punto isolato di  $\pi(X) \cap H_1 \cap \dots \cap H_r$ ; si ha quindi  $\dim_p X_q = \dim_p (X \cap (H_1 \times \mathbb{P}^n) \cap \dots \cap (H_r \times \mathbb{P}^n))$  e, dato che  $H_i \times \mathbb{P}^n$  è un iperpiano per ogni  $i$ , si ha che  $\dim_p X_q \geq \dim_p X - r$ .

[2] Sappiamo che  $\pi$  è una applicazione chiusa: per ogni sottoinsieme  $Z \subset \pi(X)$  denotiamo con  $d_Z = \min\{\dim X_q \mid q \in Z\} \in \mathbb{N}$ . Poniamo  $X_0 = X$ ,  $Z_0 = \pi(X)$  e sia  $q \in Z_0$  tale che  $\dim X_q = d_{Z_0}$ . Sia  $H \subset \mathbb{P}^n$  un sottospazio proiettivo massimale che non interseca  $X_q$  e poniamo  $Z_1 = \pi(X_0 \cap (\mathbb{A}^m \times H))$ ,  $X_1 = \pi^{-1}(Z_1)$ . Segue immediatamente dalla costruzione che, se  $Z_0 \neq \emptyset$ , allora  $Z_1$  è un chiuso proprio di  $Z_0$  e  $\dim X_q = d_{Z_0}$  per ogni  $q \in Z_0 - Z_1$ . Ripetiamo il procedimento con  $X_1, Z_1$  al posto di  $X_0, Z_0$  e costruiamo  $X_2, Z_2$  al posto di  $X_1, Z_1$ . Iterando il procedimento troviamo una catena discendente di chiusi  $Z_0 \supset Z_1 \supset \dots \supset Z_i \supset \dots$  con le proprietà che  $Z_{i+1} \neq Z_i$ , eccetto il caso in cui  $Z_i = \emptyset$ , e  $\dim X_q = d_{Z_i}$  per ogni  $q \in Z_i - Z_{i+1}$ . Per Noetherianità  $Z_i = \emptyset$  per  $i \gg 0$  e gli insiemi  $Y_h$  corrispondono ai chiusi  $Z_i$  tali che  $d_{Z_i} > d_{Z_{i-1}}$ .

[3] Segue da [1] e [2] che l'insieme  $U$  dei punti  $q \in \pi(X)$  tali che  $\dim X_q = \dim X - \dim \pi(X)$  è aperto; dato che  $\pi(X)$  è irriducibile basta dimostrare che  $U$  non è vuoto. Dimostriamo il risultato per induzione su  $r = \dim \pi(X)$ . Se  $r = 0$  allora  $\pi(X)$  è un punto e l'asserto è banale. Si assuma  $r > 0$  e sia  $s = \dim X$ . Sia  $H \subset \mathbb{A}^m$  un iperpiano tale che  $\emptyset \neq H \cap \pi(X) \neq \pi(X)$ , per il Corollario 9.6.8 ogni componente irriducibile di  $\pi(X) \cap H$  (risp.:  $X \cap (H \times \mathbb{P}^n)$ ) ha dimensione  $r - 1$  (risp.:  $s - 1$ ). Sia  $Z$  una componente irriducibile fissata di  $\pi(X) \cap H$  e scriviamo  $X \cap (H \times \mathbb{P}^n) = X_1 \cup \dots \cup X_a \cup Y_1 \cup \dots \cup Y_b$ , dove  $X_i, Y_j$  sono le componenti irriducibili divise in modo tale che  $\pi(X_i) = Z$  e  $\pi(Y_j) \neq Z$ . Dato che  $\pi$  è chiusa e  $Z$  è irriducibile necessariamente dovrà aversi  $a > 0$ . Per l'ipotesi induttiva, per ogni  $i = 1, \dots, a$ , esiste un aperto non vuoto  $U_i \subset Z$  tale che le fibre di  $X_i$  sopra  $U_i$  hanno dimensione esattamente  $s - r$ . Per qualsiasi punto  $q \in (U_1 \cap \dots \cap U_a) - (\pi(Y_1) \cup \dots \cup \pi(Y_b))$  vale  $\dim X_q = s - r$ .  $\square$

**Corollario 9.7.2.** *Nelle notazioni del Teorema 9.7.1, se  $\pi(X)$  è irriducibile e se, al variare di  $q \in \pi(X)$ , le fibre  $X_q$  sono tutte irriducibili e della stessa dimensione, allora  $X$  è irriducibile.*

*Dimostrazione.* Siano  $Z_1, \dots, Z_a, W_1, \dots, W_b$  le componenti irriducibili di  $X$  ordinate in modo tale che  $\pi(Z_i) = \pi(X)$ ,  $\pi(W_i) \neq \pi(X)$  e  $\dim Z_1 \geq \dim Z_i$  per ogni  $i$ . Proviamo che  $X = Z_1$ . Dato che  $Y$  è irriducibile e  $\pi$  è chiusa deve essere  $a > 0$ , denotiamo con  $s$  e  $r$  le dimensioni di  $Z_1$  e  $\pi(X)$  rispettivamente. Per il Teorema 9.7.1 esiste un aperto denso  $U \subset \pi(X)$  tale che, per ogni  $q \in U$ , vale  $(W_i)_q = \emptyset$  e  $\dim(Z_i)_q = \dim Z_i - r$ ; ne segue in particolare che se  $q \in U$ , allora la dimensione di  $X_q$  è esattamente  $s - r$ . Per ipotesi le fibre  $X_q$  sono tutte irriducibili di dimensione  $s - r$  e quindi per ogni  $q \in \pi(X)$  vale  $(Z_1)_q \subset X_q$ ,  $\dim(Z_1)_q \geq s - r = \dim X_q$  e di conseguenza  $(Z_1)_q = X_q$ . Questo implica che  $Z_1 = X$ .  $\square$

Lo stesso argomento usato in 9.1.8 mostra che il Teorema 9.7.1 ed il suo Corollario 9.7.2 restano validi per sottoinsiemi chiusi  $X \subset \mathbb{P}^{n_0} \times \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_s} \times \mathbb{A}^m$  e per la proiezione  $\pi: X \rightarrow \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_s} \times \mathbb{A}^m$ .

Vediamo adesso alcune applicazioni dei precedenti risultati.

*Esempio 9.7.3 (Insiemi costruibili).* Un sottoinsieme di uno spazio topologico si dice **costruibile** se è unione finita di sottoinsiemi localmente chiusi. Lasciamo per esercizio al lettore dimostrare che la famiglia dei sottoinsiemi costruibili è la più piccola famiglia di sottoinsiemi che contiene gli aperti ed è chiusa per le operazioni di complemento e di unione finita.

Proviamo adesso che, nelle stesse notazioni di 9.7.1, se  $Z \subset \mathbb{A}^m \times \mathbb{P}^n$  è costruibile allora anche  $\pi(Z)$  è costruibile. Chiaramente non è restrittivo supporre  $Z$  localmente

chiuso ed irriducibile, ovvero  $Z = X \cap V$  con  $X$  chiuso irriducibile e  $V$  aperto. Se  $Z = \emptyset$  non c'è nulla da dimostrare; se  $Z \neq \emptyset$  allora vale  $X = Z \cup C$  con  $C$  chiuso di dimensione  $\dim C < \dim X$ . Per il Teorema 9.7.1 esiste un aperto non vuoto  $U \subset \pi(X)$  tale che per ogni  $q \in U$  vale  $\dim X_q = \dim X - \dim \pi(X)$  e  $\dim C_q < \dim X - \dim Y$ . Dunque  $U \subset \pi(Z)$  e quindi  $\pi(Z) = U \cup \pi(Z \cap \pi^{-1}(\pi(X) - U))$ ; siccome la chiusura di  $Z \cap \pi^{-1}(\pi(X) - U)$  è strettamente contenuta in  $X$  basta ragionare per induzione sulla dimensione di  $\bar{Z}$  per dedurre che  $\pi(Z \cap \pi^{-1}(\pi(X) - U))$  è costruibile e quindi che anche  $\pi(Z)$  è costruibile.

*Esempio 9.7.4 (Curve piane singolari).* Sia  $n$  un intero maggiore di 1 e sia  $\mathbb{P}^N$ , con  $N = \frac{1}{2}n(n+3)$ , lo spazio proiettivo delle curve piane di grado  $n$ . Dimostriamo che l'insieme  $Y \subset \mathbb{P}^N$  delle curve singolari è una ipersuperficie irriducibile. Consideriamo infatti l'insieme  $X \subset \mathbb{P}^2 \times \mathbb{P}^N$  formato dalle coppie  $(p, C)$  tali che  $p$  è un punto singolare di  $C$ . Si vede facilmente che  $X$  è un chiuso, infatti la coppia di punti di coordinate omogenee  $([x], [F])$ , con  $F$  equazione di  $C$ , appartiene a  $X$  se e solo se  $F(x) = F_0(x) = F_1(x) = F_2(x) = 0$ . Fissato un punto  $p \in \mathbb{P}^2$  le curve piane singolari in  $p$  formano un sistema lineare di dimensione  $N - 3$ , per i Teoremi 9.7.1 e 9.7.2 applicati alla proiezione  $X \rightarrow \mathbb{P}^2$ , o più precisamente alle restrizioni agli aperti affini di  $\mathbb{P}^2$ , abbiamo che  $X$  è irriducibile di dimensione  $N - 1$ . La fibra di  $\pi: X \rightarrow \mathbb{P}^N$  sopra la curva  $C$  consiste nell'insieme dei punti singolari di  $C$ , e siccome esiste almeno una curva di grado  $n$  con un punto singolare, per il Teorema 9.7.1 ricaviamo che  $Y = \pi(X)$  è un chiuso irriducibile di dimensione  $N - 1$  e quindi una ipersuperficie.

*Esempio 9.7.5 (Luoghi determinanti, cfr. Esercizio 11.16).* Sia  $n$  un intero positivo fisso: per ogni coppia di interi  $m \geq k \geq \max(0, m - n)$  denotiamo con  $M(n, m)$  lo spazio vettoriale delle matrici  $n \times m$  a coefficienti nel campo base  $\mathbb{K}$  e con  $M_{m,k} \subset \mathbb{P}(M(n, m))$  l'insieme delle classi di omotetia di matrici il cui nucleo ha dimensione  $\geq k$ . Proviamo per induzione su  $k$  che  $M_{m,k}$  è un chiuso irriducibile di dimensione  $(m - k)(n + k) - 1$ .

Se  $k = \max(0, m - n)$  allora  $M_{m,k} = \mathbb{P}(M(n, m))$ ,  $(m - k)(n + k) - 1 = nm - 1$  e l'asserto è banalmente verificato. Supponiamo quindi  $k > \max(0, m - n)$  e consideriamo

$$X_{m,k} = \{([A], [x]) \in \mathbb{P}(M(n, m)) \times \mathbb{P}^{m-1} \mid [A] \in M_{m,k}, Ax = 0\}.$$

Le fibre della proiezione  $X_{m,k} \rightarrow \mathbb{P}^{m-1}$  sono tutte isomorfe a  $M_{m-1,k-1}$  e quindi per l'ipotesi induttiva ed il Corollario 9.7.2  $X_{m,k}$  è irriducibile di dimensione  $(m - k)(n + k - 1) + (m - 1) - 1$ . La proiezione  $X_{m,k} \rightarrow M_{m,k}$  è surgettiva e quindi  $M_{m,k}$  è irriducibile. Inoltre le fibre sui punti dell'aperto non vuoto  $M_{m,k} - M_{m,k+1}$  sono isomorfe a  $\mathbb{P}^{k-1}$ ; per il Teorema 9.7.1 vale  $\dim M_{m,k} = \dim X_{m,k} - (k - 1) = (m - k)(n + k) - 1$ .

Altre significative applicazioni di 9.7.1 e 9.7.2 saranno esposte prossimamente utilizzando il linguaggio delle varietà algebriche.

## Esercizi

**9.24.** Sia  $Z$  un sottoinsieme costruibile di uno spazio topologico Noetheriano. Provare che  $Z$  contiene un aperto denso di  $\bar{Z}$ .

## 9.8 Il grado: definizione geometrica

Un attributo fondamentale dei sottoinsiemi chiusi di uno spazio proiettivo è il grado. Ricordiamo che il grado di una curva irriducibile  $C \subset \mathbb{P}^2$  è il più piccolo intero  $\deg(C)$  con la proprietà che, se una retta  $L$  interseca  $C$  in un numero finito di punti, allora la

cardinalità di  $L \cap C$  è al più  $\deg(C)$ . Abbiamo inoltre visto (Corollario 5.2.5) che esistono punti  $q \in \mathbb{P}^2 - C$  tali che la generica retta passante per  $q$  interseca  $C$  in esattamente  $\deg(C)$  punti.

Tale definizione si estende in modo naturale ad arbitrari sottoinsiemi chiusi irriducibili di  $\mathbb{P}^n$ .

**Definizione 9.8.1.** *Sia  $X \subset \mathbb{P}^n$  un chiuso irriducibile di dimensione  $h$ . Il **grado** di  $X$  è il più piccolo intero  $\deg(X)$  tale che, se  $H \subset \mathbb{P}^n$  è un sottospazio proiettivo di codimensione  $h$ , allora l'insieme  $H \cap X$  è infinito oppure ha cardinalità  $\leq \deg(X)$ .*

Mostriamo tra breve che la definizione di  $\deg(X)$  ha senso per ogni  $X$  irriducibile. Calcoliamo prima il grado in alcuni casi semplici. Osserviamo che il grado è invariante sotto l'azione del gruppo delle proiettività di  $\mathbb{P}^n$ .

*Esempio 9.8.2.* Se  $X$  è un sottospazio proiettivo, allora  $\deg(X) = 1$ .

*Esempio 9.8.3.* Siano  $X \subset \mathbb{P}^n$  un chiuso irriducibile,  $K \subset \mathbb{P}^n$  un sottospazio proiettivo di codimensione  $s + 1$  che non interseca  $X$  e denotiamo con  $\pi: X \rightarrow \mathbb{P}^s$  la proiezione di centro  $K$ . Allora  $\deg(\pi(X)) \leq \deg(X)$ .

Infatti, poiché ogni proiezione è la composizione di proiezioni con centro un punto, per il Lemma 9.6.2 vale  $\dim \pi(X) = \dim X$  e, se  $S \subset \pi(X)$  è un sottoinsieme finito, allora anche  $\pi^{-1}(S) \subset X$  è un sottoinsieme finito e  $\#\pi^{-1}(S) \geq \#S$ . Basta quindi considerare come  $S$  un insieme di  $\deg(\pi(X))$  punti contenuti nell'intersezione di  $\pi(X)$  con un sottospazio proiettivo di codimensione  $h$ .

*Esempio 9.8.4.* Se  $X = V(f)$  è una ipersuperficie, con  $f$  polinomio irriducibile di grado  $d$  in un sistema di coordinate omogenee  $x_0, \dots, x_n$ , allora  $\deg(X) = d$ .

La restrizione di  $f$  a una retta proiettiva è una forma binaria di grado  $d$  che, se non è nulla ha al più  $d$  radici: quindi  $\deg(X) \leq d$ . Mostriamo adesso che esiste una retta  $L$  che interseca  $V(f)$  in  $d$  punti distinti, questo proverà che  $d \leq \deg(X)$ . Per ipotesi  $f$  è irriducibile e quindi con almeno una derivata parziale non nulla. Fissiamo un punto  $y = (y_0, \dots, y_n) \in \mathbb{K}^{n+1}$  tale che  $f_y = \sum_i y_i \frac{\partial f}{\partial x_i} \neq 0$  e  $q = [y] \notin X$ . Essendo  $f$  irriducibile, ed  $f_y$  di grado  $d-1$ , la dimensione di  $X \cap V(f_y)$  è  $< n-1$ . Indichiamo con  $\pi: X \rightarrow \pi(X) = \mathbb{P}^{n-1}$  la proiezione di centro  $[q]$ . Lo stesso ragionamento fatto nella Proposizione 5.2.3 mostra che, per ogni  $p \in X$ , la retta  $\overline{pq}$  interseca  $X$  in  $d$  punti distinti se e solo se  $\overline{pq} \cap X \cap V(f_y) = \emptyset$ , ovvero se e solo se  $p \notin \pi(X \cap V(f_y))$ . Basta adesso osservare che  $\pi(X \cap V(f_y))$  è un chiuso di dimensione  $< n-1$ .

*Dimostrazione (che il grado è ben definito).* Denotiamo con  $M(s, n+1)$  lo spazio affine delle matrici  $s \times (n+1)$ . Per ogni  $a = (a_{ij}) \in M$  denotiamo con  $K_a \subset \mathbb{P}^n$  il proiettivizzato del nucleo dell'applicazione lineare definita da  $a$  e con  $\phi_a: \mathbb{P}^n - K_a \rightarrow \mathbb{P}^{s-1}$  la proiezione associata, ovvero

$$\phi_a([x_0, \dots, x_n]) = \left[ \sum_j a_{1j} x_j, \dots, \sum_j a_{sj} x_j \right].$$

Sia adesso  $X \subset \mathbb{P}^n$  un chiuso irriducibile di dimensione  $h < n$ , denotiamo  $M = M(h+2, n+1)$  e consideriamo il chiuso  $W \subset M \times \mathbb{P}^{h+1} \times \mathbb{P}^n$  formato dai punti  $(a, [y], [x])$  tali che  $[x] \in X$  e  $y_i (\sum_k a_{jk} x_k) = y_j (\sum_k a_{ik} x_k)$  per ogni  $i, j$ .  $W$  è evidentemente un chiuso e per il Teorema 9.1.7 anche la proiezione sui primi due fattori  $Y = p(W) \subset M \times \mathbb{P}^{h+1}$  è chiusa ed è quindi definita da un numero finito di polinomi  $f_i(a_{ij}, y_i)$  omogenei di gradi  $d_i$  nelle variabili  $y_i$ : mostriamo che  $\deg(X) \leq \max(d_i)$ . Per ogni matrice  $a \in M$

denotiamo con  $Y_a$  l'intersezione di  $Y$  con  $\{a\} \times \mathbb{P}^{h+1}$ . Se  $X \cap K_a \neq \emptyset$  allora  $Y_a = \mathbb{P}^n$  mentre se  $X \cap K_a = \emptyset$  allora, per il Lemma 9.6.2,  $Y_a$  è irriducibile di dimensione  $h$  (quindi una ipersuperficie) e di grado  $\leq \max(d_i)$ . Si consideri un sottospazio proiettivo  $H$  di codimensione  $h$  tale che  $H \cap X = \{p_1, \dots, p_s\}$  e sia  $a \in M$  di rango massimo tale che il sottospazio  $K_a$ , di codimensione  $h+2$ , è contenuto in  $H$  e non interseca alcuna delle rette  $\overline{p_i p_j}$ . Allora  $\phi_a: H \cap X \rightarrow \phi_a(H) \cap Y_a$  è bigettiva e quindi  $s \leq \deg(Y_a) \leq \max(d_i)$ .  $\square$

**Lemma 9.8.5.** *Sia  $X \subset \mathbb{P}^n$  un chiuso irriducibile di dimensione 1. Se  $\deg(X) = k < n$ , allora  $X$  è contenuto in un sottospazio proiettivo di dimensione  $k$ .*

*Dimostrazione.* Se  $X$  non è contenuto in alcun sottospazio di dimensione  $k$  possiamo costruire per ricorrenza una successione di punti  $p_0, \dots, p_k, p_{k+1} \in X$  tali che  $\dim(p_0 + \dots + p_i) = i$  per ogni  $i \leq k+1$ . Sia  $H$  un iperpiano contenente  $p_0, \dots, p_k$  ma non  $p_{k+1}$ ; allora  $X \cap H$  è un insieme finito di punti contenente  $p_0, \dots, p_k$ .  $\square$

Mostreremo nei prossimi capitoli che per “quasi tutti” i sottospazi  $H$  di codimensione uguale alla dimensione di  $X$ , la cardinalità di  $H \cap X$  è uguale al grado di  $X$ . Per il momento mostriamo con la prossima proposizione che di tali sottospazi ne possiamo trovare abbastanza tali da riuscire a dimostrare, negli esercizi, alcune interessanti applicazioni.

**Proposizione 9.8.6.** *Sia  $X \subset \mathbb{P}^n$  un chiuso irriducibile di dimensione  $h$  e grado  $d$ .*

1. *Sia  $K \subset \mathbb{P}^n - X$  un sottospazio proiettivo di codimensione  $h+1$  e  $\pi: X \rightarrow \mathbb{P}^h$  la proiezione di centro  $K$ . Allora l'insieme*

$$U = \{p \in \mathbb{P}^h \mid \#\pi^{-1}(p) = d\}$$

*è un aperto di Zariski (possibilmente vuoto).*

2. *Sia  $Z \subset X$  un sottoinsieme chiuso proprio. Allora esiste un sottospazio proiettivo  $H \subset \mathbb{P}^n$  di codimensione  $h$  tale che  $H \cap Z = \emptyset$  e  $\#(H \cap X) = d$ .*

*Dimostrazione.* Il punto [1] è già stato dimostrato per le ipersuperfici nell'Esempio 9.8.4 con l'aiuto delle varietà polari. Nel caso generale, se  $U = \emptyset$  non c'è nulla da dimostrare: altrimenti sia  $H$  un sottospazio di codimensione  $h$  contenente  $K$  che interseca  $X$  in  $d$  punti distinti  $p_1, \dots, p_d$  e sia  $T \subset K$  un sottospazio di codimensione  $h+2$  che non interseca alcuna delle rette  $\overline{p_i p_j}$ ,  $i \neq j$ . Denotiamo con  $\hat{\pi}: X \rightarrow \mathbb{P}^{h+1}$  la proiezione di centro  $T$ ,  $Y = \hat{\pi}(X)$  e con  $\hat{\pi}: Y \rightarrow \mathbb{P}^h$  la proiezione di centro  $\hat{\pi}(K)$ . Chiaramente  $\pi = \hat{\pi}\hat{\pi}$ , e per l'Esempio 9.8.3  $Y$  è una ipersuperficie di grado  $\leq d$ . D'altra parte,  $\hat{\pi}(H)$  è una retta che interseca  $Y$  in  $d$  punti distinti e quindi  $Y$  ha grado  $d$ . Per il caso già visto l'insieme

$$\tilde{U} = \{p \in \mathbb{P}^h \mid \#\hat{\pi}^{-1}(p) = d\}$$

è un aperto contenente  $\pi(H)$ ; basta quindi dimostrare che  $\tilde{U} \subset U$ , ma questo è ovvio perché per ogni  $p \in \mathbb{P}^h$  vale  $d \geq \#\pi^{-1}(p) \geq \#\hat{\pi}^{-1}(p)$ .

Mostriamo adesso che [1  $\Rightarrow$  2]. Sia infatti  $H$  un sottospazio di codimensione  $h$  tale che  $H \cap X = p_1, \dots, p_d$ ; se  $H \cap Z = \emptyset$  abbiamo finito, altrimenti scegliamo un sottospazio  $K \subset H$  di codimensione  $h+1$  che non interseca  $X$ . Considerando la proiezione di centro  $K$ ,  $\pi: X \rightarrow \mathbb{P}^h$ , si ha che  $\pi(Z)$  è un chiuso proprio mentre per il punto 1), l'insieme (non vuoto perché contiene  $H$ ) dei sottospazi di codimensione  $h$  contenenti  $K$  che intersecano  $X$  in  $d$  punti è un aperto che quindi non può essere contenuto in  $\pi(Z)$ .  $\square$

Per dimostrare risultati interessanti e validi in caratteristica arbitraria concernenti il grado, come ad esempio il teorema di Bézout per  $\mathbb{P}^n$ , occorre fare uno studio algebrico più approfondito: faremo questo nel Capitolo 13 osservando che  $\frac{\deg(X)}{\dim X!}$  è il coefficiente direttore di un attributo più generale dei chiusi proiettivi: il polinomio di Hilbert.

**Esercizi**

**9.25.** Se  $X$  ha grado 1 allora  $X$  è un sottospazio proiettivo. (Sugg.: se  $\dim X = h$ , per ogni sottospazio  $K \subset \mathbb{P}^n - X$  di codimensione  $h + 1$ , la proiezione di centro  $K$ ,  $\pi_K: X \rightarrow \mathbb{P}^h$  è iniettiva.)

**9.9 Esercizi complementari**

**9.26.** Uno spazio topologico si dice **Artiniano** se ogni famiglia di aperti contiene un elemento minimale. Sia  $X$  uno spazio topologico Artiniano, provare che:

1.  $X$  contiene un numero finito di punti chiusi.
2. Ogni chiuso di  $X$  è unione finita di componenti irriducibili.
3. Se  $X$  è irriducibile, l'unione dei chiusi propri di  $X$  è un chiuso proprio.
4. (\*) Se  $X$  è anche Noetheriano allora contiene un numero finito di aperti. (Sugg.: uno spazio Artiniano con infiniti chiusi contiene una catena discendente non stazionaria di chiusi.)

**9.27.** Mostrare che esistono spazi topologici Noetheriani e spazi topologici Artiniani di dimensione infinita.

**9.28 (Spazi di Zariski).** Ricordiamo che uno spazio topologico  $X$  soddisfa l'assioma di separazione  $T_0$  se per ogni coppia di punti distinti  $x, y \in X$  vale  $\bar{x} \neq \bar{y}$ . Un punto  $x \in X$  si dice **generico** se  $\bar{x} = X$ . Condizione necessaria affinché esista un punto generico è che  $X$  sia irriducibile; se  $X$  è  $T_0$  esiste al più un punto generico.

Sia  $X$  uno spazio topologico e per ogni chiuso  $C \subset X$  denotiamo con  $t(C)$  l'insieme dei chiusi irriducibili contenuti in  $C$ . Provare:

1. Gli insiemi  $t(C)$ , presi al variare di  $C \subset X$  chiuso, sono i chiusi di una topologia  $T_0$  su  $t(X)$ .
2. Si consideri l'applicazione naturale  $\phi: X \rightarrow t(X)$ ,  $\phi(x) = \bar{x}$ . Allora vale  $\phi^{-1}(t(C)) = C$  per ogni chiuso  $C \subset X$  e quindi  $\phi$  è continua,  $\phi(X)$  è denso in  $t(X)$  e  $\phi$  è iniettiva se e solo se  $X$  è  $T_0$ .
3. Se  $X$  è irriducibile (risp.: Noetheriano), allora  $t(X)$  è irriducibile (risp.: Noetheriano).
4. Uno spazio topologico si dice uno **spazio di Zariski** se è  $T_0$ , Noetheriano ed ogni chiuso irriducibile contiene un punto generico. Se  $X$  è Noetheriano allora  $t(X)$  è di Zariski e se  $X$  è di Zariski allora  $\phi$  è un omeomorfismo.
5. Ogni applicazione continua  $f: X \rightarrow Y$  induce una applicazione continua  $t(f): t(X) \rightarrow t(Y)$  che commuta con  $\phi_X: X \rightarrow t(X)$  e  $\phi_Y: Y \rightarrow t(Y)$ .
6. Sia  $C \subset \mathbb{A}^n$  un chiuso irriducibile, provare che

$$\text{codim}(C, t(\mathbb{A}^n)) = \text{codim}(C, \mathbb{A}^n), \quad \dim_C t(\mathbb{A}^n) = n.$$

7. Dare una descrizione di  $t(\mathbb{A}^n)$  e della sua topologia in funzione degli ideali di  $\mathbb{K}[x_1, \dots, x_n]$  e delle relazioni di inclusione tra di essi.

**9.29.** Tradurre:

Teorema: Seja  $E$  um espaço irredutível e  $U$  um aberto não vazio de  $E$ . Então,  $U$  é denso em  $E$ , isto é, o fecho  $\bar{U}$  de  $U$  é igual a  $E$ . Demonstração: Se  $E$  é aberto e não vazio então,  $U = E - F$ , onde  $F$  é fechado e distinto de  $E$ . Como  $E = U \cup F = \bar{U} \cup F$  e  $E$  é irredutível resulta que  $\bar{U} = E$ .

**9.30.** Sia  $X$  uno spazio topologico Noetheriano. Provare che un sottoinsieme  $A \subset X$  è aperto se e solo se per ogni chiuso irriducibile  $E \subset X$  esiste un sottoinsieme  $S \subset E$  aperto in  $E$  tale che  $S \subset A \cap E \subset \bar{S}$ . (Sugg.: si consideri la famiglia dei chiusi  $C$  di  $X$  tali che  $C - A$  non è chiuso.)

**9.31.** Descrivere l'immagine dell'applicazione  $f: \mathbb{A}^2 \rightarrow \mathbb{A}^2$ ,  $f(x, y) = (x, xy)$  e dire se è chiusa, aperta, localmente chiusa, costruibile o niente di tutto ciò.

**9.32.** (caratteristica  $\neq 2$ ) Determinare le componenti irriducibili di

$$X = \{x^2 + y^2 + z^2 = x^2 + 1 - y^2 - z^2 = 0\} \subset \mathbb{A}^3.$$

**9.33.** Nelle notazioni del Corollario 9.1.5, se  $n = 2, r = 1$  e  $f_0, f_1$  sono senza fattori comuni, determinare la dimensione del conucleo di  $\phi_d$  per  $d \gg 0$ . (Sugg.: descrivere il nucleo di  $\phi_d$ .)

**9.34.** Siano  $p, q \in \mathbb{N}$  senza fattori comuni,  $X = \{x^p = y^q\} \subset \mathbb{A}^2$  e  $\phi: \mathbb{A}^1 \rightarrow X$  definita da  $\phi(t) = (t^q, t^p)$ . Provare che  $\phi$  è un omeomorfismo. (Sugg.: esistono interi  $n, m$  tali che  $np + mq = 1$ .)

**9.35.** Si consideri l'applicazione  $\phi: \mathbb{A}^1 \rightarrow \mathbb{A}^3$ ,  $\phi(t) = (t, t^2, t^3)$ ; dimostrare che  $X = \phi(\mathbb{A}^1)$  è chiuso e si determini  $I(X)$ .

**9.36.** Enunciare e dimostrare il teorema degli zeri di Hilbert per  $\mathbb{P}^n \times \mathbb{P}^m$ .

**9.37.** Dimostrare che:

1. Ogni sottoinsieme costruibile di  $\mathbb{A}^n$  è della forma  $\pi(X)$ , dove  $X \subset \mathbb{A}^{n+1}$  è un sottoinsieme chiuso e  $\pi$  è la proiezione sulle prime  $n$  coordinate. (Sugg.: mostrare prima che ogni sottoinsieme localmente chiuso di  $\mathbb{A}^n$  è della forma  $\pi(X)$ .)
2. Un sottoinsieme costruibile  $Z \subset \mathbb{A}^n$  è chiuso se e solo se  $Z \cap C$  è chiuso per ogni chiuso irriducibile  $C \subset \mathbb{A}^n$  di dimensione 1.
3. Il risultato di 2) è generalmente falso senza l'ipotesi che  $Z$  sia costruibile.

**9.38.** Nelle stesse notazioni del Teorema 9.7.1 si provi che la funzione

$$\mathbb{A}^m \times \mathbb{P}^n \rightarrow \mathbb{Z}, \quad p \mapsto \dim_p X_{\pi(p)}$$

è semicontinua superiormente. (Sugg.: se l'asserzione è vera per due sottoinsiemi chiusi di  $\mathbb{A}^m \times \mathbb{P}^n$  allora è vera anche per la loro unione; non è quindi restrittivo supporre  $X$  irriducibile. Ragionare per induzione sulla dimensione di  $\pi(X)$  utilizzando 9.7.1.)

**9.39.** Sia  $X \subset \mathbb{A}^n$  un chiuso e  $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$  la proiezione sulle prime  $n - 1$  coordinate. Provare che se  $f = \sum_{i \geq 0} g_i(x_1, \dots, x_{n-1})x_n^{d-i} \in I(X)$ , allora  $\pi(X) - V(g_0)$  è chiuso in  $\mathbb{A}^{n-1} - V(g_0)$  e dedurre che  $\pi(X)$  contiene un aperto di  $\overline{\pi(X)}$ . (Sugg.: si può ripetere sostanzialmente la dimostrazione del lemma di proiezione oppure si può considerare il chiuso  $\tilde{X} \subset \mathbb{A}^n \times \mathbb{A}$  definito da  $I(X)$  e  $1 - tg_0$ .)

**9.40.** Provare che  $\mathbb{A}^2$  e  $\mathbb{P}^2$ , dotati della topologia di Zariski, non sono omeomorfi. Più in generale se  $n \geq 2$  e  $X \subset \mathbb{P}^n$  è chiuso di dimensione  $\leq n - 3$ , si provi che  $\mathbb{A}^n$  e  $\mathbb{P}^n - X$  non sono omeomorfi.

**9.41.** (caratteristica  $\neq 2$ ) Sia  $X \subset \mathbb{A}^3$  il chiuso definito dalle equazioni  $xy - z^2 = y^3 - x^5 = 0$ . Provare che  $X$  ha due componenti irriducibili.



**9.42.** (caratteristica 0) Sia  $F(x_1, \dots, x_n)$  un polinomio omogeneo di grado  $m > 0$  senza fattori multipli; poniamo  $C = V(F) \subset \mathbb{A}^n$  e sia  $\mathcal{A}$  l'insieme dei sottospazi affini di  $\mathbb{A}^n$  contenuti in  $C$ . Definiamo infine  $C_0$  come l'intersezione dei sottospazi in  $\mathcal{A}$  che sono massimali rispetto all'inclusione. Provare:

1.  $C_0$  è un sottospazio affine contenente l'origine  $(0, \dots, 0)$ .
2. A meno di un cambio lineare di coordinate si può assumere che esista  $s \leq n$  tale che  $\frac{\partial F}{\partial x_i} = 0$  per ogni  $i > s$  e i polinomi  $\frac{\partial F}{\partial x_1}, \dots, \frac{\partial F}{\partial x_s}$  linearmente indipendenti su  $\mathbb{K}$ .
3. (\*) In un sistema di coordinate come al punto 2) vale  $C_0 = \{x_1 = \dots = x_s = 0\}$ .

**9.43.** Sia  $M = M(n, n, \mathbb{K})$  lo spazio affine delle matrici  $n \times n$  e sia  $X \subset \mathbb{P}(M)$  il proiettivizzato dell'insieme delle matrici  $A$  che hanno un autovalore  $\lambda \neq 0$  tale che  $\lambda^n + (-1)^n \det(A) = 0$ .

1. Provare che  $X$  è una ipersuperficie irriducibile.
2. (\*) Determinare il grado di  $X$ .

**9.44** (\*). Dimostrare che ogni chiuso proprio in  $\mathbb{P}^n$  è intersezione (insiemistica) di al più  $n + 1$  ipersuperfici. (Sugg.: Esercizio 4.14.)

**9.45.** Sia  $S_d \subset \mathbb{K}[x_0, \dots, x_n]$  lo spazio vettoriale dei polinomi omogenei di grado  $d$  e  $v_n: \mathbb{P}^1 \rightarrow \mathbb{P}^n$  la  $n$ -esima immersione di Veronese. Determinare la dimensione dello spazio vettoriale  $V_d = \{f \in S_d \mid v_n(\mathbb{P}^1) \subset V(f)\}$  per ogni  $d > 0$ .

**9.46.** (caratteristica 0) Sia  $X \subset M(4, 4, \mathbb{K}) = \mathbb{A}^{16}$  il sottoinsieme delle matrici  $A$  tali che  $I, A$  e  $A^2$  sono vettori linearmente dipendenti in  $M(4, 4, \mathbb{K})$ . Dimostrare:

1.  $X$  è chiuso.
2.  $X$  non è irriducibile (Sugg.: polinomio caratteristico).

**9.47 (Lo scoppimento).** Sia  $X \subset \mathbb{A}^n$  un chiuso e denotiamo con:  $Y = X - \{0\}$ , con  $\tilde{Y} \subset (\mathbb{A}^n - \{0\}) \times \mathbb{P}^{n-1}$  l'insieme dei punti  $\{(y, [y])\}$  al variare di  $y \in Y$ , con  $\tilde{X} \subset \mathbb{A}^n \times \mathbb{P}^{n-1}$  la chiusura di Zariski di  $\tilde{Y}$  e con  $E = (\{0\} \times \mathbb{P}^{n-1}) \cap \tilde{X}$ .

1. Dimostrare che  $\tilde{Y}$  è un chiuso di  $(\mathbb{A}^n - \{0\}) \times \mathbb{P}^{n-1}$  omeomorfo a  $Y$ . (Sugg.: considerare dapprima il caso  $X = \mathbb{A}^n$ .)
2. Descrivere esplicitamente  $\tilde{X}$  ed  $E$  nei casi  $X = \mathbb{A}^n$  e  $X$  ipersuperficie.
3. Se  $X$  è unione di due chiusi  $X_1$  e  $X_2$ , provare che  $\tilde{X} = \tilde{X}_1 \cup \tilde{X}_2$ .
4. Mostrare che, se  $0 \in X$ , allora il cono affine di  $E$  coincide con il cono tangente ridotto  $C_0(X)$  e quindi  $\dim_0 X = \dim E + 1$ .

**9.48 (Scoppimento lungo sottospazi proiettivi).** Sia  $K \subset \mathbb{P}^n$  un sottospazio proiettivo di codimensione  $h + 1$ , con  $h > 0$ ; denotiamo con  $\mathbb{P}^h$  lo spazio proiettivo dei sottospazi di  $\mathbb{P}^n$  di codimensione  $h$  che contengono  $K$  e con

$$\text{Bl}_K \mathbb{P}^n = \{(p, H) \in \mathbb{P}^n \times \mathbb{P}^h \mid p \in H\}.$$

(Si noti che  $K \times \mathbb{P}^h \subset \text{Bl}_K \mathbb{P}^n$ .) Indichiamo con  $\pi_1: \text{Bl}_K \mathbb{P}^n \rightarrow \mathbb{P}^n$  e  $\pi_2: \text{Bl}_K \mathbb{P}^n \rightarrow \mathbb{P}^h$  le proiezioni sui fattori.

- 1) Mostrare che per ogni sottospazio  $H$  di codimensione  $h$  vale  $\pi_1 \pi_2^{-1}(H) = H$  e che, se  $p \notin K$  allora  $\pi_2 \pi_1^{-1}(p) = K + p$ .
- 2) Se  $K$  è definito dalle  $h + 1$  equazioni lineari indipendenti  $f_i(x_0, \dots, x_n) = 0$ , con  $i = 0, \dots, h$ , provare che  $\text{Bl}_K \mathbb{P}^n$  è il chiuso definito dalle  $\binom{h+1}{2}$  equazioni  $y_i f_j(x_0, \dots, x_n) = y_j f_i(x_0, \dots, x_n)$ , con  $0 \leq i < j \leq h$ .
- 3) Sia  $X \subset \mathbb{P}^n$  un chiuso tale che alcuna componente irriducibile di  $X$  sia contenuta in  $K$ .

Allora si definisce  $\text{Bl}_K X \subset \text{Bl}_K \mathbb{P}^n$  come l'unione delle componenti irriducibili di  $\pi_1^{-1}(X)$  che non sono contenute in  $\pi_1^{-1}(K)$ .

Dimostrare che la proiezione  $\pi_1: \text{Bl}_K X \rightarrow X$  è surgettiva ed induce una bigezione tra le rispettive famiglie di componenti irriducibili. Provare inoltre che  $\dim \text{Bl}_K X = \dim X$  e  $\dim(\pi_1^{-1}(K) \cap \text{Bl}_K X) < \dim X$ .

4) Provare che  $\pi_2 \text{Bl}_K X = \overline{\pi_K(X - K)}$ , dove  $\pi_K$  indica la proiezione di centro  $K$ .

**9.49.** Siano  $Y \subset \mathbb{P}^n$  un chiuso irriducibile di dimensione  $h < n$  e grado  $d > 1$  e  $H$  un sottospazio proiettivo di codimensione  $h$  che interseca  $Y$  in esattamente  $d$  punti. Sia  $o \in H \cap Y$  e denotiamo con  $\pi_o$  la proiezione di centro  $o$ . Dimostrare che  $X = \overline{\pi_o(X - o)}$  ha dimensione  $h$  e grado  $< d$ . (Sugg.: nelle notazioni dell'Esercizio 9.48 si ha  $X = \pi_2(\text{Bl}_o Y)$  e  $0 < \sharp(\text{Bl}_o Y \cap \pi_2^{-1}(H)) < +\infty$ . Applicare la Proposizione 9.8.6 al chiuso proprio  $\pi_2(\text{Bl}_o Y \cap \pi_1^{-1}(o)) \subset X$ .)

**9.50.** Sia  $X \subset \mathbb{P}^n$  un chiuso irriducibile. Dimostrare che se  $X$  non è contenuto in alcun iperpiano, allora vale  $\dim X + \deg(X) \geq n + 1$ . (Sugg.: Esercizio 9.49 e induzione sulla codimensione di  $X$ .)

**9.51 (Varietà secante).** Si considerino due spazi proiettivi  $\mathbb{P}^{2n+1}$  e  $\mathbb{P}^n$  aventi rispettivamente coordinate omogenee  $x_0, \dots, x_n, y_0, \dots, y_n$  e  $t_0, \dots, t_n$ . Dati due chiusi irriducibili non vuoti  $X, Y \subset \mathbb{P}^n$ , sia  $\tilde{V}$  l'insieme delle coppie  $([t], [x, y]) \in \mathbb{P}^n \times \mathbb{P}^{2n+1}$  tali che  $x \in C(X)$ ,  $y \in C(Y)$  e  $t_i(x_j - y_j) = t_j(x_i - y_i)$  per ogni  $i, j$ . Siano  $p: \tilde{V} \rightarrow \mathbb{P}^n$ ,  $q: \tilde{V} \rightarrow \mathbb{P}^{2n+1}$  le proiezioni sui fattori. Mostrare che  $\tilde{V}$  è un chiuso ed esiste una unica componente irriducibile  $V \subset \tilde{V}$  tale che  $q(V)$  non è contenuta in  $H = \{x_i = y_i \forall i\}$ . Detti  $S(X, Y) = p(V)$ ,  $J(X, Y) = q(V)$ , mostrare che  $J(X, Y)$ ,  $S(X, Y)$  sono chiusi irriducibili,  $\dim S(X, Y) \leq \dim J(X, Y) = \dim V = \dim X + \dim Y + 1$  e che  $S(X, Y)$  contiene come sottoinsieme denso l'unione di tutte le rette  $\overline{ab}$  al variare di  $a \in X$ ,  $b \in Y$ ,  $a \neq b$ .

I chiusi  $S(X, Y)$  e  $J(X, Y)$  sono detti rispettivamente **join** e **join astratto** di  $X$  e  $Y$ , mentre  $S(X, X)$  è detto **varietà secante** di  $X$ . Descrivere la varietà secante dell'immagine della seconda immersione di Veronese  $v_2: \mathbb{P}^2 \rightarrow \mathbb{P}^5$ .

**9.52 (\*).** Sia  $X \subset \mathbb{P}^n$  irriducibile di dimensione  $h \leq n - 2$ . Provare che esiste un aperto non vuoto  $U \subset \mathbb{P}^n - X$  tale che, per ogni  $o \in U$ ,  $\deg(\pi_o(X)) = \deg(X)$ , dove  $\pi_o$  è la proiezione di centro  $o$ . (Sugg.: siano  $H$  un sottospazio di codimensione  $h$  che interseca  $X$  in  $d = \deg(X)$  punti distinti,  $K \subset H$  sottospazio di codimensione  $h + 1$  che non interseca  $X$  e  $Z \subset \text{Bl}_K \mathbb{P}^n$  l'insieme tale che  $\pi_2^{-1}(H) = S(X \cap H, X \cap H)$  (nelle notazioni degli Esercizi 9.48 e 9.51). Mostrare che  $Z$  è un chiuso proprio e che esiste un aperto non vuoto  $V \subset \mathbb{P}^h$  tale che ogni  $o \in \pi_1(\pi_2^{-1}(V) - Z - K \times \mathbb{P}^h)$  soddisfa la condizione  $\deg(\pi_o(X)) = \deg(X)$ .)

**9.53.** Sia  $v_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$  la  $d$ -esima immersione di Veronese. Provare:

1. Il grado di  $v_d(\mathbb{P}^n)$  è  $\geq d^n$ .
2. (\*\*?) Il grado di  $v_d(\mathbb{P}^n)$  è  $= d^n$ .

**9.54 (\*\*).** Sia  $\mathbb{K} = \mathbb{C}$ ,  $X \subset \mathbb{P}^n$  un chiuso irriducibile di Zariski e  $U \subset X$  un aperto non vuoto di Zariski. Provare che la chiusura di  $U$  nella topologia classica è uguale a  $X$ . (Sugg.: provare l'esercizio dapprima nel caso  $X = \mathbb{P}^n$ , poi per le ipersuperfici utilizzando il teorema di preparazione di Weierstrass e infine il caso  $k = \dim X \leq n - 2$ ,  $Z = X - U$  e  $p \in Z$ . Bisogna dimostrare che  $p$  è il limite classico di una successione  $p_n$  in  $U$ . Sia  $\pi: X \rightarrow \mathbb{P}^{n-1}$  una proiezione tale che  $\pi^{-1}(\pi(p)) = \{p\}$  e lavorare su  $\pi(X)$  e  $\pi(X) - \pi(Z)$ . Per un'altra dimostrazione vedi [Mum1976, Th. 2.33].)

**9.55 (\*\*?).** Sia  $\mathbb{K} = \mathbb{C}$ ,  $X \subset \mathbb{C}^n$  un chiuso di Zariski dotato della topologia classica: allora ogni punto di  $X$  è un retratto per deformazione di un suo intorno.

## Varietà algebriche: nozioni base

Quando si parla di varietà si intende generalmente uno spazio topologico dotato di strutture accessorie. Lo scòpo principale di questo capitolo è quello di mostrare che ogni sottoinsieme localmente chiuso di  $\mathbb{P}^n$  possiede un cosiddetto “fascio strutturale” che gli fornisce la struttura di “varietà quasiproiettiva”. Per tutto il capitolo assumeremo che  $\mathbb{K}$  sia un campo fissato algebricamente chiuso.

**Avvertenza.** In questo capitolo, ed anche nei prossimi, il lettore troverà definizioni diverse di enti matematici chiamati con lo stesso nome: se ciò accade è per far familiarizzare il lettore con i nuovi concetti, inizialmente nei casi di migliore comprensione. Naturalmente prima o poi ci sarà un teorema che equiparerà le varie definizioni.

### 10.1 Varietà affini

**Definizione 10.1.1.** Sia  $X \subset \mathbb{A}^n$  un sottoinsieme chiuso di Zariski. Diremo che una funzione  $f: X \rightarrow \mathbb{K}$  è **regolare** su  $X$  se è la restrizione di una funzione polinomiale su  $\mathbb{A}^n$ : in altri termini  $f$  è regolare se esiste  $F \in \mathbb{K}[x_1, \dots, x_n]$  tale che  $F(x) = f(x)$  per ogni  $x \in X$ .

Le funzioni regolari su  $X$  formano una  $\mathbb{K}$ -algebra  $\mathbb{K}[X]$ , il morfismo naturale di restrizione  $\pi: \mathbb{K}[x_1, \dots, x_n] \rightarrow \mathbb{K}[X]$  è surgettivo per definizione ed ha come nucleo esattamente l'ideale  $I(X)$ .

*Esempio 10.1.2.* Sia  $X \subset \mathbb{A}^2$  la curva di equazione  $x_1^2 = x_2^3$ ; le proiezioni sugli assi coordinati  $x_i: X \rightarrow \mathbb{K}$ ,  $i = 1, 2$ , sono funzioni regolari. Per definizione la  $\mathbb{K}$ -algebra  $\mathbb{K}[X]$  è generata da  $x_1$  e  $x_2$ . L'applicazione  $\phi: \mathbb{K} \rightarrow X$ ,  $\phi(t) = (t^3, t^2)$  è un omeomorfismo (vedi Esercizio 9.34) ma  $\phi^{-1}: X \rightarrow \mathbb{K}$  non è regolare. Infatti, se esistesse  $P \in \mathbb{K}[x, y]$  tale che  $P(x) = \phi^{-1}(x)$  per ogni  $x \in X$ , si avrebbe  $P(t^3, t^2) = t$  per ogni  $t \in \mathbb{K}$ .

Se  $X$  è un chiuso affine, allora  $\mathbb{K}[X]$  è una  $\mathbb{K}$ -algebra finitamente generata senza nilpotenti ed è quindi Noetheriana. Viceversa se  $A$  è una  $\mathbb{K}$ -algebra finitamente generata senza nilpotenti, allora si può scrivere  $A = \mathbb{K}[x_1, \dots, x_n]/J$ , con  $J = \sqrt{J}$ , e quindi  $A = \mathbb{K}[X]$ , dove  $X = V(J) \subset \mathbb{A}^n$ .

Esiste una ovvia generalizzazione delle corrispondenze  $V, I$  definite nel Capitolo 4 ad ogni chiuso affine  $X \subset \mathbb{A}^n$ . Per ogni ideale  $J \subset \mathbb{K}[X]$  si definisce

$$V_X(J) = \{x \in X \mid f(x) = 0 \text{ per ogni } f \in J\}.$$

Denotando con  $\pi: \mathbb{K}[x_1, \dots, x_n] \rightarrow \mathbb{K}[X]$  la proiezione canonica, siccome  $V_X(J) = V(\pi^{-1}(J))$ , si ha che i sottoinsiemi chiusi di  $X$  sono tutti e soli i sottoinsiemi della forma  $V_X(J)$  al variare di  $J$  tra gli ideali di  $\mathbb{K}[X]$ .

Viceversa se  $Z \subset X$  è un sottoinsieme chiuso, si definisce  $I_X(Z) \subset \mathbb{K}[X]$  come l'ideale delle funzioni regolari su  $X$  che si annullano su  $Z$ . I seguenti fatti sono di semplice verifica:

1.  $V_X(J) = V(\pi^{-1}(J))$  per ogni ideale  $J \subset \mathbb{K}[X]$ .
2.  $\pi^{-1}(I_X(Z)) = I(Z)$  per ogni  $Z \subset X$ .
3.  $\pi^{-1}(\sqrt{J}) = \sqrt{\pi^{-1}(J)}$  per ogni ideale  $J \subset \mathbb{K}[X]$ .

Dalle precedenti proprietà 1) 2) e 3) segue che le corrispondenze  $V_X, I_X$  soddisfano proprietà analoghe a quelle di  $V$  e  $I$  definite sullo spazio affine. In particolare  $V_X(I_X(Z)) = Z$  per ogni  $Z \subset X$  chiuso.

**Teorema 10.1.3 (degli zeri).** *Sia  $X$  un chiuso affine e  $J \subset \mathbb{K}[X]$  un ideale: allora vale l'uguaglianza  $I_X(V_X(J)) = \sqrt{J}$ . Gli ideali massimali di  $\mathbb{K}[X]$  sono tutti e soli quelli della forma  $I_X(x)$ , con  $x \in X$ .*

*Dimostrazione.* La prima asserzione segue dalle uguaglianze

$$\pi^{-1}(\sqrt{J}) = \sqrt{\pi^{-1}(J)} = I(V(\pi^{-1}(J))) = I(V_X(J)) = \pi^{-1}(I_X(V_X(J))).$$

La seconda segue dalla bigezione naturale tra ideali massimali (risp.: primi) di  $\mathbb{K}[X]$  ed ideali massimali (risp.: primi) di  $\mathbb{K}[x_1, \dots, x_n]$  che contengono  $I(X)$ .  $\square$

Se  $f \in \mathbb{K}[X]$ , allora l'aperto  $X_f = \{x \in X \mid f(x) \neq 0\}$  si dice un **aperto principale** di  $X$ . Per ogni ideale  $J \subset \mathbb{K}[X]$  si ha  $X - V_X(J) = \cup_{f \in J} X_f$  e quindi gli aperti principali formano una base per la topologia di  $X$ .

**Definizione 10.1.4.** *Un'applicazione tra spazi affini  $\Phi: \mathbb{A}^n \rightarrow \mathbb{A}^m$  si dice **regolare** se è indotta da polinomi, cioè se in un sistema di coordinate affini si ha  $\Phi = (F_1, \dots, F_m)$ , con  $F_i \in \mathbb{K}[x_1, \dots, x_n]$  per ogni indice  $i$ . Se  $X \subset \mathbb{A}^n$  e  $Y \subset \mathbb{A}^m$  sono chiusi, un'applicazione  $\phi: X \rightarrow Y$  si dice **regolare** se è la restrizione di una applicazione regolare  $\Phi: \mathbb{A}^n \rightarrow \mathbb{A}^m$ .*

È tautologico osservare che un'applicazione  $\phi = (f_1, \dots, f_m): X \rightarrow Y \subset \mathbb{A}^m$  tra chiusi affini è regolare se e solo se  $f_i \in \mathbb{K}[X]$  per ogni  $i$ . Le identità sono regolari e la composizione di due applicazioni regolari è ancora regolare. Ci troviamo quindi di fronte ad una categoria che ha come oggetti i chiusi affini e come morfismi le applicazioni regolari. Useremo il termine **morfismo regolare** come sinonimo di applicazione regolare.

Per ogni insieme  $X$  denotiamo con  $\mathbb{K}^X$  la  $\mathbb{K}$ -algebra di tutte le funzioni su  $X$  a valori in  $\mathbb{K}$ . Ogni applicazione  $\phi: X \rightarrow Y$  definisce per composizione un morfismo di  $\mathbb{K}$ -algebre  $\phi^*: \mathbb{K}^Y \rightarrow \mathbb{K}^X$ .

**Lemma 10.1.5.** *Nelle notazioni precedenti, un'applicazione tra chiusi affini  $\phi: X \rightarrow Y$  è regolare se e solo se  $\phi^*\mathbb{K}[Y] \subset \mathbb{K}[X]$ . In particolare, poiché  $\phi^{-1}(Y_g) = X_{\phi^*g}$  per ogni  $g \in \mathbb{K}[Y]$ , ogni applicazione regolare è continua.*

*Dimostrazione.* Supponiamo  $Y$  un chiuso dello spazio affine  $\mathbb{A}^m$  e siano  $y_1, \dots, y_n \in \mathbb{K}[Y]$  le restrizioni a  $Y$  delle coordinate su  $\mathbb{A}^m$ ; se  $f_i = \phi^*y_i$ , allora si ha  $\phi = (f_1, \dots, f_m)$  e quindi  $\phi$  è regolare se e solo se  $\phi^*y_i \in \mathbb{K}[X]$  per ogni  $i$ . Basta adesso osservare che le  $y_i$  generano  $\mathbb{K}[Y]$  come  $\mathbb{K}$ -algebra.  $\square$

**Proposizione 10.1.6.** *Siano  $X$  e  $Y$  due chiusi affini. Allora esiste una bigezione naturale tra l'insieme dei morfismi regolari  $\phi: X \rightarrow Y$  e l'insieme dei morfismi di  $\mathbb{K}$ -algebre  $\phi^*: \mathbb{K}[Y] \rightarrow \mathbb{K}[X]$ .*

*Dimostrazione.* Si assuma  $Y \subset \mathbb{A}^m$ ,  $\pi: \mathbb{K}[\mathbb{A}^m] \rightarrow \mathbb{K}[Y]$  la proiezione naturale e siano  $y_1, \dots, y_m \in \mathbb{K}[\mathbb{A}^m]$  le coordinate affini. Dato un omomorfismo di  $\mathbb{K}$ -algebre  $h: \mathbb{K}[Y] \rightarrow \mathbb{K}[X]$  poniamo  $f_i = h(\pi(y_i))$ . L'applicazione  $\phi = (f_1, \dots, f_m): X \rightarrow \mathbb{A}^m$  è regolare e

$\phi^* = h\pi$ . Se  $g \in I(Y)$ , allora  $\phi^*g = 0$ ,  $\phi(X) \subset V(g)$ , e quindi l'immagine di  $\phi$  è contenuta in  $Y$ . Lasciamo per esercizio la semplice verifica che l'applicazione  $h \rightarrow \phi$  così definita è l'inversa dell'applicazione  $\phi \rightarrow \phi^*$ .  $\square$

**Definizione 10.1.7.** *Un morfismo regolare tra chiusi affini si dice un **isomorfismo regolare** se è bigettivo con inverso regolare.*

**Corollario 10.1.8.** *Un morfismo regolare  $\phi: X \rightarrow Y$  tra chiusi affini è un isomorfismo se e solo se  $\phi^*: \mathbb{K}[Y] \rightarrow \mathbb{K}[X]$  è un isomorfismo.*

*Dimostrazione.* Immediata conseguenza della Proposizione 10.1.6.  $\square$

*Esempio 10.1.9.* La retta  $\mathbb{A}^1$  e l'iperbole  $X = V(xy - 1) \subset \mathbb{A}^2$  non sono isomorfi. Infatti, se lo fossero esisterebbe un isomorfismo di  $\mathbb{K}$ -algebre

$$\mathbb{K}[t] = \mathbb{K}[\mathbb{A}^1] = \mathbb{K}[X] = \mathbb{K}[x, y]/(xy - 1)$$

e questo non è possibile dato che  $x$  è invertibile in  $\mathbb{K}[X]$ , mentre ogni invertibile di  $\mathbb{K}[\mathbb{A}^1]$  è costante.

*Esempio 10.1.10.* Sia  $X \subset \mathbb{A}^n$  un chiuso affine e  $\phi: X \rightarrow \mathbb{A}^m$  un'applicazione regolare. Siano  $Y = \{(x, \phi(x)) \in \mathbb{A}^{n+m} \mid x \in X\}$  il grafico di  $\phi$  e  $\pi: Y \rightarrow X$  la proiezione sul primo fattore. Allora  $Y$  è chiuso e  $\pi$  è un isomorfismo regolare. Infatti, se  $x_1, \dots, x_n$  sono le coordinate su  $\mathbb{A}^n$  e  $y_1, \dots, y_m$  sono le coordinate su  $\mathbb{A}^m$ , posto  $f_i = \phi^*y_i$  si ha che  $Y = V(J)$  dove  $J \subset \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$  è l'ideale generato da  $I(X)$  e  $y_i - f_i$ : quindi  $Y$  è un chiuso, la proiezione  $\pi$  è regolare, bigettiva e con inversa  $\pi^{-1} = (x_1, \dots, x_n, f_1, \dots, f_m)$  regolare.

*Esempio 10.1.11.* Sia  $X \subset \mathbb{A}^n$  un chiuso,  $f \in \mathbb{K}[X]$  una funzione regolare su  $X$  e consideriamo

$$Y = \{(x, t) \in \mathbb{A}^{n+1} \mid x \in X, tf(x) = 1\} = V(I(X), 1 - tf) \subset X \times \mathbb{A}^1.$$

L'insieme  $Y$  è un chiuso affine e la proiezione  $\pi: Y \rightarrow X$  è regolare ed induce una bigezione tra  $Y$  e l'aperto principale  $X_f$ . Il morfismo  $\pi^*: \mathbb{K}[X] \rightarrow \mathbb{K}[Y]$  ha le seguenti proprietà:

1. La funzione regolare  $\pi^*(f)$  è invertibile in  $\mathbb{K}[Y]$ .
2. Per ogni  $g \in \mathbb{K}[Y]$  esiste un intero  $s$  tale che  $\pi^*(f)^s g \in \pi^*\mathbb{K}[X]$ .
3.  $\pi^*(a) = 0$  se e solo se esiste un intero  $s \geq 0$  tale che  $f^s a = 0$ .

La verifica di 1) e 3) è immediata in quanto  $\pi^*(f)t = 1$  e  $\pi^*(a) = 0$  se e solo se  $a(x) = 0$  per ogni  $x \in X_f$ . Il morfismo  $\mathbb{K}[X][t] \rightarrow \mathbb{K}[Y]$  è surgettivo e quindi ogni  $g \in \mathbb{K}[Y]$  si può esprimere come un polinomio nella variabile  $t$  a coefficienti in  $\pi^*\mathbb{K}[X]$  ed il punto 2) segue dal fatto che  $\pi^*(f)t = 1$ . Possiamo decomporre il morfismo  $\pi^* = \beta\alpha$  con  $\alpha: \mathbb{K}[X] \rightarrow \mathbb{K}[X][t]/(1 - tf)$  morfismo naturale e  $\beta: \mathbb{K}[X][t]/(1 - tf) \rightarrow \mathbb{K}[Y]$ . Si osserva che il morfismo  $\alpha$  soddisfa le stesse proprietà 1), 2) e 3) di  $\pi^*$ . Le proprietà 1) e 2) sono banali, dimostriamo che vale 3). Se  $f^s a = 0$  per qualche  $s > 0$  allora  $a = (1 - tf)(\sum_{i \geq 0} t^i f^i a)$  e quindi  $\alpha(a) = 0$ . Viceversa se  $\alpha(a) = 0$  allora esistono  $b_0, \dots, b_s \in \mathbb{K}[X]$  tali che  $a = (1 - tf)(\sum b_i t^i)$  e quindi  $b_0 = a, b_1 = fa, \dots, b_s = f^s a, f^{s+1} a = 0$ . Dimostriamo adesso che  $\beta$  è un isomorfismo: infatti  $\pi^*$  soddisfa 2) e quindi  $\beta$  è surgettiva. Se  $\beta(g) = 0$  allora esiste  $s > 0$  tale che  $f^s g = \alpha(h)$  con  $\pi^*(h) = 0$  e quindi esiste  $r > 0$  tale che  $f^r h = 0$ . A maggior ragione  $f^{s+r} g = 0$  e dato che  $f$  è invertibile in  $\mathbb{K}[X][t]/(1 - tf)$  necessariamente  $g = 0$  e  $\beta$  risulta iniettiva.

L'Esempio 10.1.11 rende doveroso richiamare le nozioni di base sulla localizzazione degli anelli commutativi con unità; per ulteriori approfondimenti rimandiamo ai testi di algebra commutativa [AM1969], [Kapl1974], [Mat1986].

Sia  $A$  un anello commutativo con unità, un sottoinsieme  $S \subset A$  si dice una *parte moltiplicativa* se  $1 \in S$  e  $S$  è chiuso per il prodotto, cioè se  $st \in S$  ogniqualvolta  $t, s \in S$ .

Data una parte moltiplicativa  $S \subset A$  si definisce  $S^{-1}A$  come il quoziente di  $A \times S$  per la relazione:  $(a, s) \sim (b, t)$  se e solo se esiste  $r \in S$  tale che  $r(at - bs) = 0$ . Per comprensibili motivi si denota con  $\frac{a}{s} \in S^{-1}A$  la classe di equivalenza della coppia  $(a, s)$ . Lasciamo per esercizio al lettore la verifica che  $\sim$  è una relazione di equivalenza e che  $S^{-1}A$  è un anello commutativo con zero  $\frac{0}{1}$  e unità  $\frac{1}{1}$  rispetto alle operazioni

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}, \quad \frac{a}{s} \frac{b}{t} = \frac{ab}{st}$$

Si noti che  $S^{-1}A = 0$  se e solo se  $1 = 0$  in  $S^{-1}A$  se e solo se  $0 \in S$ . È consuetudine denotare con:

- $S^{-1}A = A_{\mathfrak{p}}$  se  $S = A - \mathfrak{p}$ , con  $\mathfrak{p}$  ideale primo.
- $S^{-1}A = A_f$  se  $S = \{f^s\}_{s \geq 0}$ , con  $f \in A$ .
- $S^{-1}A = \text{Fraz}(A)$  se  $S = A - \{\text{divisori di } 0\}$ .

L'anello  $\text{Fraz}(A)$  si dice anello delle frazioni globali di  $A$  e coincide con il campo delle frazioni quando  $A$  è un dominio di integrità. Esiste un omomorfismo naturale di anelli  $l: A \rightarrow S^{-1}A$  definito da  $l(a) = \frac{a}{1}$ . È immediato verificare che

1.  $l(s)$  è invertibile in  $S^{-1}A$  per ogni  $s \in S$ .
2. Per ogni  $g \in S^{-1}A$  esistono  $s \in S$  e  $a \in A$  tali che  $l(s)g = l(a)$ .
3.  $l(a) = 0$  se e solo se  $sa = 0$  per qualche  $s \in S$ .

**Teorema 10.1.12.** *Sia  $S \subset A$  una parte moltiplicativa,  $l: A \rightarrow S^{-1}A$  l'omomorfismo naturale e  $\phi: A \rightarrow B$  un omomorfismo di anelli tale che:*

1.  $\phi(s)$  è invertibile per ogni  $s \in S$ .

Allora esiste un unico omomorfismo  $\beta: S^{-1}A \rightarrow B$  tale che  $\phi = \beta l$ . Se inoltre vale:

2. Per ogni  $b \in B$  vale  $\phi(s)b = \phi(a)$  per qualche  $s \in S$ ,  $a \in A$ .
3.  $\phi(a) = 0$  se e solo se  $sa = 0$  per qualche  $s \in S$ .

Allora  $\beta$  è un isomorfismo.

*Dimostrazione.* Assumiamo 1). Se  $\beta$  esiste allora deve necessariamente soddisfare  $\beta\left(\frac{a}{s}\right) = \phi(a)\phi(s)^{-1}$  e quindi  $\beta$  è unico. Inoltre se  $(a, s) \sim (b, t)$  allora  $\phi(a)\phi(s)^{-1} = \phi(b)\phi(t)^{-1}$  e quindi la precedente relazione fornisce una buona definizione di  $\beta$ . Se valgono 1) e 2) è evidente che  $\beta$  è surgettiva. La condizione 3) equivale a dire che  $\phi$  e  $l$  hanno lo stesso nucleo, dunque se vale 1), 3) e  $\beta\left(\frac{a}{s}\right) = 0$  allora  $\phi(a) = 0$  e  $\frac{a}{s} = \frac{1}{s}l(a) = 0$ .  $\square$

La stesso argomento usato nell'Esempio 10.1.11 mostra che per ogni anello  $A$  e  $f \in A$  vale  $A_f = A[t]/(1 - tf)$ .

## Esercizi

**10.1.** Provare che una funzione regolare  $f: X \rightarrow \mathbb{K}$  è invertibile in  $\mathbb{K}[X]$  se e solo se  $f(x) \neq 0$  per ogni  $x \in X$ . (Sugg.: Teorema 10.1.3.)

**10.2.** Dati  $f, g \in \mathbb{K}[X]$ , dimostrare che  $X_f \subset X_g$  se e solo se  $g$  divide una potenza di  $f$ .

**10.3.** Nelle notazioni dell'Esempio 10.1.10, provare che  $J = I(Y)$ .

**10.4.** Sia  $\phi: X \rightarrow Y$  un'applicazione regolare tra chiusi affini. Provare che:

1.  $\phi(X)$  è denso in  $Y$  se e solo se  $\phi^*: \mathbb{K}[Y] \rightarrow \mathbb{K}[X]$  è iniettiva.
2.  $\phi(X) \subset V_Y(\text{Ker}(\phi^*))$ .
3. Se  $\phi^*$  è surgettiva allora  $\phi$  è una immersione topologica chiusa.

Mostrare inoltre con un esempio che il viceversa del punto 3 è generalmente falso.

**10.5.** Nelle notazioni precedenti, dimostrare che l'omomorfismo  $l: A \rightarrow S^{-1}A$  è iniettivo se e solo se  $S$  non contiene divisori di 0 e che  $l$  è un isomorfismo se e solo se ogni elemento di  $S$  è invertibile in  $A$ .

**10.6.** Sia  $I \subset S^{-1}A$  un ideale e sia  $E \subset A$  un insieme di generatori di  $l^{-1}(I)$ . Mostrare che  $l(E)$  genera  $I$ ; in particolare se  $A$  è Noetheriano allora anche  $S^{-1}A$  è Noetheriano.

## 10.2 Fasci strutturali

Obiettivo di questa sezione è quello di associare ad ogni sottoinsieme localmente chiuso di uno spazio affine multiproiettivo  $X \subset \mathbb{A}^m \times \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_k}$  un'applicazione

$$\mathcal{O}_X: \{\text{Aperti di } X\} \rightarrow \{\mathbb{K}\text{-algebre}\}$$

che chiameremo **fascio strutturale** di  $X$ . Consideriamo inizialmente tre casi particolari:

$$X = \mathbb{A}^n. \quad (10.1)$$

Per ogni  $U \subset \mathbb{A}^n$  aperto, definiamo  $\mathcal{O}_{\mathbb{A}^n}(U)$  come la sottoalgebra di  $U^{\mathbb{K}}$  formata dalle funzioni  $f: U \rightarrow \mathbb{K}$  che sono localmente un quoziente di polinomi. Più precisamente  $f \in \mathcal{O}_{\mathbb{A}^n}(U)$  se e solo se per ogni  $x \in U$  esiste un intorno aperto  $x \in V \subset U$  e polinomi  $F, G \in \mathbb{K}[\mathbb{A}^n] = \mathbb{K}[x_1, \dots, x_n]$  tali che  $G(y) \neq 0$  e  $f(y) = \frac{F(y)}{G(y)}$  per ogni  $y \in V$ .

$$X = \mathbb{P}^n. \quad (10.2)$$

Per ogni  $U \subset \mathbb{P}^n$  aperto, definiamo  $\mathcal{O}_{\mathbb{P}^n}(U)$  come la sottoalgebra di  $U^{\mathbb{K}}$  formata dalle funzioni  $f: U \rightarrow \mathbb{K}$  che sono localmente un quoziente di polinomi omogenei dello stesso grado. Cioè  $f \in \mathcal{O}_{\mathbb{P}^n}(U)$  se e solo se per ogni  $x \in U$  esiste un intorno aperto  $x \in V \subset U$  e polinomi  $F, G \in \mathbb{K}[x_0, x_1, \dots, x_n]$  omogenei dello stesso grado e tali che  $G(y) \neq 0$  e  $f(y) = \frac{F(y)}{G(y)}$  per ogni  $y \in V$ .

$$X = \mathbb{P}^n \times \mathbb{P}^m. \quad (10.3)$$

Per ogni  $U \subset \mathbb{P}^n \times \mathbb{P}^m$  aperto, definiamo  $\mathcal{O}_X(U)$  come la sottoalgebra di  $U^{\mathbb{K}}$  formata dalle funzioni  $f: U \rightarrow \mathbb{K}$  che sono localmente un quoziente di polinomi biomogenei dello stesso bigrado. Cioè  $f \in \mathcal{O}_X(U)$  se e solo se per ogni  $x \in U$  esiste un intorno aperto  $x \in V \subset U$  e polinomi  $F, G \in \mathbb{K}[x_0, x_1, \dots, x_n, y_0, \dots, y_m]$  biomogenei dello stesso bigrado e tali che  $G(y) \neq 0$  e  $f(y) = \frac{F(y)}{G(y)}$  per ogni  $y \in V$ .

*Lasciamo all'immaginazione del lettore il compito di formulare la definizione del fascio strutturale per il prodotto di un arbitrario numero di spazi affini e proiettivi.*

Se  $\mathbb{A}^n \subset \mathbb{P}^n$  indica un aperto affine, complementare di un iperpiano e  $U \subset \mathbb{A}^n$  è un aperto, allora  $U$  è pure aperto in  $\mathbb{P}^n$  e fortunatamente vale  $\mathcal{O}_{\mathbb{A}^n}(U) = \mathcal{O}_{\mathbb{P}^n}(U)$ . Infatti, se  $x_0, \dots, x_n$  sono coordinate omogenee su  $\mathbb{P}^n$  tali che  $\mathbb{A}^n = \{x_0 \neq 0\}$ , allora  $y_i = x_i x_0^{-1}$  sono coordinate affini su  $\mathbb{A}^n$ . Dati due polinomi  $f, g \in \mathbb{K}[y_1, \dots, y_n]$ , per  $d \gg 0$  vale

$$\frac{f(y_1, \dots, y_n)}{g(y_1, \dots, y_n)} = \frac{x_0^d f(x_1 x_0^{-1}, \dots, x_n x_0^{-1})}{x_0^d g(x_1 x_0^{-1}, \dots, x_n x_0^{-1})} = \frac{F(x_0, \dots, x_n)}{G(x_0, \dots, x_n)}$$

con  $F, G$  polinomi omogenei di grado  $d$ . Viceversa dati  $F, G \in \mathbb{K}[x_0, \dots, x_n]$  omogenei dello stesso grado si ha che

$$\frac{F(x_0, \dots, x_n)}{G(x_0, \dots, x_n)} = \frac{F(1, y_1, \dots, y_n)}{G(1, y_1, \dots, y_n)} = \frac{f(y_1, \dots, y_n)}{g(y_1, \dots, y_n)}.$$

Similmente se  $x_0, \dots, x_n$  sono coordinate omogenee su  $\mathbb{P}^n$  e  $y_0, \dots, y_m$  sono coordinate omogenee su  $\mathbb{P}^m$  allora  $u_i = x_i x_0^{-1}$ ,  $v_j = y_j y_0^{-1}$  sono coordinate affini su  $\mathbb{A}^{n+m} = \{x_0 y_0 \neq 0\} \subset \mathbb{P}^n \times \mathbb{P}^m$ . Dati due polinomi  $f, g \in \mathbb{K}[u_1, \dots, u_n, v_1, \dots, v_m]$ , per  $d, h \gg 0$  vale

$$\frac{f(u_1, \dots, v_m)}{g(u_1, \dots, v_m)} = \frac{x_0^d y_0^h f(x_1 x_0^{-1}, \dots, y_m y_0^{-1})}{x_0^d y_0^h g(x_1 x_0^{-1}, \dots, y_m y_0^{-1})} = \frac{F(x_0, \dots, y_m)}{G(x_0, \dots, y_m)}$$

con  $F, G$  polinomi biomogenei di bigrado  $(d, h)$ . Viceversa dati  $F, G \in \mathbb{K}[x_0, \dots, y_m]$  biomogenei dello stesso bigrado si ha che

$$\frac{F(x_0, \dots, y_m)}{G(x_0, \dots, y_m)} = \frac{F(1, u_1, \dots, u_n, 1, v_1, \dots, v_m)}{G(1, u_1, \dots, u_n, 1, v_1, \dots, v_m)}.$$

In particolare se  $U \subset \mathbb{A}^{n+m}$  è aperto vale  $\mathcal{O}_{\mathbb{A}^n \times \mathbb{P}^m}(U) = \mathcal{O}_{\mathbb{P}^n \times \mathbb{P}^m}(U)$ . Risultato analogo per aperti contenuti nelle parti affini degli spazi affino-multiproiettivi.

Denotiamo con  $M$  uno dei nostri “spazi modello”, cioè  $M = \mathbb{A}^n, \mathbb{P}^n, \mathbb{P}^n \times \mathbb{P}^m$  ecc. Se  $U \subset M$  è un aperto, chiameremo  $\mathcal{O}_M(U)$  **algebra delle funzioni regolari su  $U$** . Se invece  $U \subset M$  è localmente chiuso, allora diremo che una funzione  $f: U \rightarrow \mathbb{K}$  è regolare in  $U$  se è localmente la restrizione di funzioni regolari su aperti di  $M$ . Più in dettaglio,  $f: U \rightarrow \mathbb{K}$  è regolare se e solo se per ogni  $x \in U$  esiste un aperto  $x \in V \subset M$  ed una funzione regolare  $F \in \mathcal{O}_M(V)$  tale che  $F(y) = f(y)$  per ogni  $y \in U \cap V$ . Se  $X \subset M$  è localmente chiuso e  $U \subset X$  è un aperto, allora  $U$  è localmente chiuso in  $M$  e denotiamo con  $\mathcal{O}_X(U) \subset \mathbb{K}^U$  la sottoalgebra delle funzioni regolari su  $U$ . Se  $X$  è localmente chiuso in  $\mathbb{A}^n$  allora  $X$  è localmente chiuso anche in  $\mathbb{P}^n$ ,  $(\mathbb{P}^1)^n$  ecc. e possiamo considerare  $X$  come sottoinsieme localmente chiuso di vari “spazi modello”  $M$ . Le precedenti osservazioni su omogeneizzazione e disomogeneizzazione mostrano che  $\mathcal{O}_X$  non dipende dalla scelta di  $M$ .

**Definizione 10.2.1.** Se  $X \subset \mathbb{A}^m$  è un sottoinsieme localmente chiuso, chiameremo la coppia  $(X, \mathcal{O}_X)$  **varietà quasiffine**.

Se  $X \subset \mathbb{A}^m \times \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_k}$  è un sottoinsieme localmente chiuso, chiameremo la coppia  $(X, \mathcal{O}_X)$  **varietà quasiproiettiva**.

*Osservazione 10.2.2.* La definizione di varietà quasiproiettiva come coppia  $(X, \mathcal{O}_X)$  è pedante ma necessaria. Tuttavia nel seguito denoteremo per semplicità una varietà  $(X, \mathcal{O}_X)$  solamente con  $X$ , lasciando sottinteso il fascio strutturale  $\mathcal{O}_X$ .

**Lemma 10.2.3.** Sia  $X$  una varietà quasiproiettiva,  $U \subset X$  un aperto e  $f: U \rightarrow \mathbb{K}$  una funzione. Se  $U$  è unione di una famiglia di aperti  $\{U_i\}$ , allora  $f$  è regolare su  $U$  se e solo se la restrizione  $f: U_i \rightarrow \mathbb{K}$  è regolare su  $U_i$  per ogni indice  $i$ .



*Dimostrazione.* Immediata conseguenza della definizione di funzione regolare.  $\square$

**Lemma 10.2.4.** *Sia  $X$  una varietà quasiproiettiva,  $U \subset X$  un aperto e  $f \in \mathcal{O}_X(U)$ . Allora il sottoinsieme  $U_f = \{x \in U \mid f(x) \neq 0\}$  è aperto e la funzione  $1/f: U_f \rightarrow \mathbb{K}$  è regolare.*

*Dimostrazione.* Esercizio.  $\square$

Il fascio strutturale è caratterizzato dalle seguenti proprietà assiomatiche:

**F1** Per ogni coppia di aperti  $V \subset U$  della varietà  $X$ , è dato un morfismo di  $\mathbb{K}$ -algebre  $\rho_V^U: \mathcal{O}_X(U) \rightarrow \mathcal{O}_X(V)$ . Se  $W \subset V \subset U$  sono aperti allora  $\rho_W^U = \rho_W^V \rho_V^U$  e  $\rho_U^U = Id$ .

In concreto, il morfismo  $\rho_V^U$  è dato dalla restrizione a  $V$  delle funzioni regolari su  $U$ ; scriveremo spesso  $f|_V$  al posto di  $\rho_V^U(f)$ .

**F2** Se  $U = \cup\{U_i \mid i \in I\}$  è un ricoprimento aperto e  $f \in \mathcal{O}_X(U)$  è una funzione tale che  $f|_{U_i} = 0$  per ogni  $i \in I$ , allora  $f = 0$ .

**F3** Se  $U = \cup\{U_i \mid i \in I\}$  è un ricoprimento aperto e per ogni indice  $i \in I$  è data una funzione  $f_i \in \mathcal{O}_X(U_i)$  in modo tale che  $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$  per ogni  $i, j \in I$ , allora esiste  $f \in \mathcal{O}_X(U)$  tale che  $f|_{U_i} = f_i$  per ogni  $i$ .

Si noti che dalla proprietà **F2** è possibile dedurre che la funzione  $f$  come al punto **F3** è unica. Inoltre, considerando  $U = I = \emptyset$ , si deduce da **F2** che  $\mathcal{O}_X(\emptyset) = 0$ . La condizione **F1** esprime il fatto che, se pensiamo gli aperti di  $X$  come gli oggetti di una categoria i cui morfismi sono le inclusioni, allora  $\mathcal{O}_X$  è un funtore controvariante.

Le condizioni **F1**, **F2** e **F3** si dicono **assiomi di fascio**. Più in generale, se  $X$  è uno spazio topologico, un'applicazione  $\mathcal{F}: \{\text{Aperti di } X\} \rightarrow \{\text{Gruppi}\}$  che soddisfa, mutatis mutandis, i tre assiomi precedenti (con i morfismi di restrizione omomorfismi di gruppi) si dice un **fascio**. Infine, cosa importante, osserviamo che il Lemma 10.2.3 segue formalmente dagli assiomi di fascio.

Se  $X$  è una varietà quasiproiettiva e  $Y \subset X$  è un sottoinsieme localmente chiuso, allora anche  $Y$  è una varietà quasiproiettiva ed una funzione è regolare su di un aperto di  $Y$  se e solo se è localmente la restrizione di funzioni regolari su aperti di  $X$ .

Concentriamoci adesso nello studiare il fascio strutturale di chiusi affini  $X \subset \mathbb{A}^n$ . Notiamo immediatamente che è possibile definire le funzioni regolari su aperti di  $X$  come le funzioni che sono localmente quoziente di elementi di  $\mathbb{K}[X]$ .

**Teorema 10.2.5.** *Sia  $X$  un chiuso affine e  $f \in \mathbb{K}[X]$ . Allora*

$$\mathcal{O}_X(X_f) = \mathbb{K}[X]_f = \mathbb{K}[X][t]/(1 - tf).$$

*In particolare si ha (se  $f = 1$ )  $\mathcal{O}_X(X) = \mathbb{K}[X]$ .*

*Dimostrazione.* Basta verificare che il morfismo naturale  $\phi: \mathbb{K}[X] \rightarrow \mathcal{O}_X(X_f)$  soddisfa le condizioni 1), 2) e 3) del Teorema 10.1.12 rispetto alla parte moltiplicativa  $\{f^n\}_{n \geq 0}$ . La 1) e la 3) sono immediate in quanto  $f^s \in \mathcal{O}_X(X_f)$  per ogni  $s \in \mathbb{Z}$  e  $\phi(a) = 0$  se e solo se  $a(x) = 0$  per ogni  $x \in X_f$  e quindi se e solo se  $af^s = 0$  per qualche  $s \geq 0$ . Rimane da dimostrare che se  $g \in \mathcal{O}_X(X_f)$  allora  $f^s g \in \mathbb{K}[X]$  per  $s \gg 0$ . Per definizione di  $\mathcal{O}_X$  esiste un ricoprimento aperto  $X_f = \cup_{i \in I} U_i$  e funzioni regolari  $F_i, G_i \in \mathbb{K}[X]$  tali che, se  $x \in U_i$  allora  $G_i(x) \neq 0$  e  $gG_i(x) = F_i(x)$ . Non è restrittivo assumere gli aperti  $U_i$  principali, diciamo  $U_i = X_{u_i}$  e a meno di considerare  $F_i u_i$  e  $G_i u_i$  al posto di  $F_i, G_i$  possiamo assumere che  $gG_i = F_i$  su tutto  $X$ . Infine  $X_f$  è quasi compatto e possiamo sopprimere il ricoprimento finito e  $I = \{1, \dots, r\}$ . Dato che  $V(G_1, \dots, G_r) \subset V(f)$ , per il teorema degli zeri esiste  $s > 0$  ed una relazione  $f^s = \sum H_i G_i$ ,  $H_i \in \mathbb{K}[X]$ . Moltiplicando ambo i membri per  $g$  si ottiene  $f^s g = \sum H_i G_i g = \sum H_i F_i \in \mathbb{K}[X]$ .  $\square$

**Proposizione 10.2.6.** *Siano  $X$  e  $Y$  due chiusi affini e  $\phi: X \rightarrow Y$  un'applicazione. Se  $\phi$  è regolare, allora  $\phi^*\mathcal{O}_Y(U) \subset \mathcal{O}_X(\phi^{-1}(U))$  per ogni aperto  $U \subset Y$ .*

*Viceversa, se  $\phi$  è continua ed esiste un ricoprimento aperto  $Y = \cup\{U_i \mid i \in I\}$  tale che  $\phi^*\mathcal{O}_Y(U_i) \subset \mathcal{O}_X(\phi^{-1}(U_i))$  per ogni  $i \in I$ , allora  $\phi$  è regolare.*

*Dimostrazione.* Se  $\phi$  è regolare allora  $\phi^*$  trasforma funzioni localmente quoziente di elementi di  $\mathbb{K}[Y]$  in funzioni localmente quoziente di elementi di  $\phi^*\mathbb{K}[Y] \subset \mathbb{K}[X]$  e quindi  $\phi^*\mathcal{O}_Y(U) \subset \mathcal{O}_X(\phi^{-1}(U))$  per ogni aperto  $U \subset Y$ .

Viceversa sia  $g \in \mathbb{K}[Y]$ , allora  $(\phi^*g)|_{\phi^{-1}(U_i)} = \phi^*(g|_{U_i}) \in \mathcal{O}_X(\phi^{-1}(U_i))$  e, per il Lemma 10.2.3 (o equivalentemente per l'assioma **F3**), si ha  $\phi^*g \in \mathcal{O}_X(X) = \mathbb{K}[X]$ . Dunque  $\phi^*\mathbb{K}[Y] \subset \mathbb{K}[X]$  e  $\phi$  è regolare per 10.1.5.  $\square$

Dunque per ogni chiuso affine  $X$  si ha  $\mathbb{K}[X]_f = \mathcal{O}_X(X_f)$  per ogni  $f \in \mathbb{K}[X]$ . Sorge spontaneo chiedersi se per ogni ideale primo  $\mathfrak{p} \subset \mathbb{K}[X]$  esiste una descrizione geometrica dell'anello  $\mathbb{K}[X]_{\mathfrak{p}}$ . Daremo adesso una risposta affermativa fornendo una descrizione di  $\mathbb{K}[X]_{\mathfrak{p}}$  che utilizza il fascio strutturale  $\mathcal{O}_X$ . Siano  $X$  un chiuso affine e  $Z \subset X$  un chiuso irriducibile. Definiamo  $\mathcal{O}_{Z,X}$  come l'insieme delle coppie  $(U, f)$ , con  $U \subset X$  aperto tale che  $U \cap Z \neq \emptyset$  e  $f \in \mathcal{O}_X(U)$ , quozientato per la relazione di equivalenza  $(U, f) \sim (V, g)$  se e solo se esiste un aperto  $W \subset U \cap V$  tale che  $W \cap Z \neq \emptyset$  e  $f|_W = g|_W$ . L'irriducibilità di  $Z$  implica che su  $\mathcal{O}_{Z,X}$  è ben definita una struttura di anello con le operazioni

$$(U, f) + (V, g) = (U \cap V, f + g), \quad (U, f)(V, g) = (U \cap V, fg).$$

Definiamo inoltre  $\mathfrak{m}_{Z,X} = \{(U, f) \in \mathcal{O}_{Z,X} \mid f|_{Z \cap U} = 0\}$ : la verifica che si tratta di una buona definizione richiede di nuovo che  $Z$  sia irriducibile. L'insieme  $\mathfrak{m}_{Z,X}$  è chiaramente un ideale e se  $(U, f) \notin \mathfrak{m}_{Z,X}$ , allora  $U_f \cap Z \neq \emptyset$  e  $(U, f)$  è invertibile in  $\mathcal{O}_{Z,X}$  con inverso  $(U_f, f^{-1})$ . Questo implica che  $\mathcal{O}_{Z,X}$  è un anello locale con ideale massimale  $\mathfrak{m}_{Z,X}$ . Notiamo che se  $X$  è irriducibile, allora  $\mathfrak{m}_{X,X} = 0$  e quindi  $\mathcal{O}_{X,X}$  è un campo.

**Definizione 10.2.7.** *Se  $X$  è irriducibile si denota  $\mathbb{K}(X) = \mathcal{O}_{X,X}$ . Il campo  $\mathbb{K}(X)$  si chiama **campo delle funzioni razionali** su  $X$ . Se  $x \in X$  l'anello  $\mathcal{O}_{x,X}$  si dice anello dei **germi di funzioni regolari** nel punto  $x$ .*

Si faccia attenzione al fatto che le cosiddette funzioni razionali su  $X$  non sono delle vere funzioni su  $X$  ma sono funzioni definite su aperti densi di  $X$ . È consuetudine indicare graficamente le funzioni razionali con delle frecce a tratti medi<sup>1</sup>  $f: X \dashrightarrow \mathbb{K}$ . Ogni elemento di  $\mathcal{O}_{x,X}$  si rappresenta con una coppia del tipo  $(X_g, fg^{-1})$  con  $f, g \in \mathbb{K}[X]$  e  $g(x) \neq 0$ .

**Teorema 10.2.8.** *Sia  $X$  un chiuso affine. Allora per ogni chiuso irriducibile  $Z \subset X$  con ideale  $\mathfrak{p} = I_X(Z)$ , l'omomorfismo naturale  $\phi: \mathbb{K}[X] \rightarrow \mathcal{O}_{Z,X}$  induce un isomorfismo di  $\mathbb{K}$ -algebre  $\mathbb{K}[X]_{\mathfrak{p}} = \mathcal{O}_{Z,X}$ .*

*Dimostrazione.* Basta dimostrare che  $\phi$  soddisfa le condizioni 1), 2) e 3) del Teorema 10.1.12 rispetto alla parte moltiplicativa  $S = \mathbb{K}[X] - \mathfrak{p}$ . Se  $f \in S$  allora  $X_f \cap Z \neq \emptyset$  e quindi  $\phi(f) = (X, f)$  è invertibile con inverso  $(X_f, f^{-1})$ . Se  $\phi(a) = 0$  significa che esiste un aperto  $U$  tale che  $U \cap Z \neq \emptyset$  e  $a(x) = 0$  per ogni  $x \in U$ . Dato che  $U$  è unione di aperti principali non è restrittivo supporre  $U = X_f$  per qualche  $f \in S$  e quindi  $fa = 0$ . Viceversa se  $af = 0$  per qualche  $f \in S$  allora  $\phi(a) = (X_f, 0) = 0$ . Sia infine  $b \in \mathcal{O}_{Z,X}$ , possiamo rappresentare  $g$  con una coppia  $(X_f, g)$  per qualche  $f \in S$  e  $g \in \mathcal{O}_X(X_f) = \mathbb{K}[X]_f$ ; esiste quindi  $s > 0$  tale che  $gf^s \in \mathbb{K}[X]$  e quindi  $b = \phi(gf^s)\phi(f)^{-s}$ .  $\square$

<sup>1</sup> Disponibili in  $\text{T}_E\text{X}$  con il comando `\dashrightarrow`. Nel disegno tecnico, le linee a tratti medi sono quelle tratteggiate nelle quali la lunghezza dei tratti disegnati è costante ed all'incirca doppia della lunghezza degli spazi vuoti.

**Corollario 10.2.9.** *Per ogni chiuso irriducibile  $Z$  in un chiuso affine  $X$ , l'anello  $\mathcal{O}_{Z,X}$  è Noetheriano.*

*Dimostrazione.* Esercizio. □

### Esercizi

**10.7.** Sia  $U \subset (\mathbb{P}^1)^4$  l'aperto delle quaterne di punti distinti. Provare che il birapporto e (in caratteristica  $\neq 2, 3$ ) l'invariante  $j$  sono funzioni regolari.

**10.8.** Se  $n \geq 2$ , dimostrare che  $\mathcal{O}_{\mathbb{A}^n}(\mathbb{A}^n - \{0\}) = \mathbb{K}[\mathbb{A}^n]$ . (Sugg.:  $\mathbb{K}[\mathbb{A}^n]$  è un dominio a fattorizzazione unica.)

**10.9.** Sia  $\phi: X \rightarrow Y$  un morfismo regolare tra chiusi affini e  $Z \subset X$  un chiuso irriducibile. Provare che, se  $W = \overline{\phi(Z)}$ , allora è ben definito un morfismo di  $\mathbb{K}$ -algebre  $\phi^*: \mathcal{O}_{W,Y} \rightarrow \mathcal{O}_{Z,X}$ .

**10.10.** Sia  $X$  chiuso affine e  $U \subset X$  un aperto irriducibile. Provare che per ogni aperto non vuoto  $V \subset U$ , l'applicazione di restrizione  $\mathcal{O}_X(U) \rightarrow \mathcal{O}_X(V)$  è iniettiva.

**10.11.** Sia  $\pi: X \rightarrow Y$  un morfismo regolare di chiusi affini irriducibili. Dimostrare che se  $\pi(X)$  è denso in  $Y$ , allora  $\pi(X)$  contiene un aperto di  $Y$ . (Sugg.: ridursi al caso  $Y \subset \mathbb{A}^n$ ,  $X \subset \mathbb{A}^{n+s}$  chiusi e  $\pi$  indotta dalla proiezione sulle prime  $n$  coordinate. Usare induzione su  $s$ . Se  $s = 0$  o se  $X = \pi^{-1}(Y)$  non c'è nulla da dimostrare, altrimenti sia  $F \neq 0$  appartenente al nucleo di  $\mathbb{K}[Y][x_{n+1}, \dots, x_{n+s}] \rightarrow \mathbb{K}[X]$ ; se  $d$  è il grado di  $F$ , a meno di un cambio lineare di coordinate si ha  $F = f x_{n+s}^d +$  termini di grado minore in  $x_{n+s}$  con  $f \in \mathbb{K}[Y]$ . Se  $f$  è invertibile e  $p: \mathbb{A}^{n+s} \rightarrow \mathbb{A}^{n+s-1}$  è la proiezione sulle prime coordinate allora  $p(X)$  è chiuso. Se  $f$  non è invertibile si considerino i chiusi  $Y_f \subset \mathbb{A}^{n+1}$  e  $X_f \subset \mathbb{A}^{n+1+s}$ .)

## 10.3 Varietà quasiproiettive

**Definizione 10.3.1.** *Siano  $X$  e  $Y$  varietà quasiproiettive. Un'applicazione  $\phi: X \rightarrow Y$  si dice **regolare** se è continua e per ogni aperto  $U \subset Y$  vale  $\phi^* \mathcal{O}_Y(U) \subset \mathcal{O}_X(\phi^{-1}(U))$ .*

È importante osservare che:

1. (Categoricità) La composizione di applicazioni regolari è ancora regolare, l'identità è regolare e quindi le varietà quasiproiettive e le applicazioni regolari formano una categoria. Come nel caso affine, il termine **morfismo regolare** è sinonimo di applicazione regolare.
2. (Località) Una applicazione è regolare se e soltanto se è localmente regolare: cioè  $\phi: X \rightarrow Y$  è regolare se e solo se per ogni  $x \in X$  esistono aperti  $x \in V \subset X$  e  $\phi(x) \in U \subset Y$  tali che  $\phi(V) \subset U$  e  $\phi: V \rightarrow U$  è regolare.
3. (Ereditarietà) Sia  $\phi: X \rightarrow Y$  un morfismo regolare di varietà quasiproiettive e siano  $Z \subset X$ ,  $W \subset Y$  sottoinsiemi localmente chiusi tali che  $\phi(Z) \subset W$ . Allora  $\phi: Z \rightarrow W$  è un morfismo regolare di varietà quasiproiettive. In particolare per ogni varietà quasiproiettiva  $X$  e per ogni sottoinsieme localmente chiuso  $Y \subset X$ , l'inclusione  $Y \rightarrow X$  è regolare.

**Lemma 10.3.2.** *Sia  $X$  una varietà quasiproiettiva e  $\phi = (f_1, \dots, f_n): X \rightarrow \mathbb{A}^n$  una applicazione. Allora  $\phi$  è regolare se e solo se  $f_i \in \mathcal{O}_X(X)$  per ogni  $i$ .*

*Dimostrazione.* Siano  $y_i$  le coordinate affini su  $\mathbb{A}^n$ , allora  $\phi^*y_i = f_i$ . Poiché le  $y_i$  sono funzioni regolari su  $Y$ , se  $\phi$  è regolare, allora anche le  $f_i$  sono regolari.

Viceversa se ogni  $f_i$  è regolare, allora per ogni polinomio  $F \in \mathbb{K}[y_1, \dots, y_n]$  vale  $\phi^*F \in \mathcal{O}_X(X)$  e, per il Lemma 10.2.4,  $\phi^{-1}(\mathbb{A}_F^n) = X_{\phi^*F}$  è aperto. Dato che gli  $\mathbb{A}_F^n$  formano una base di aperti, l'applicazione  $\phi$  è continua. Inoltre  $\phi^*$  trasforma funzioni regolari su aperti dello spazio affine in funzioni che sono localmente quoziente di elementi di  $\mathcal{O}_X(X)$  e quindi, sempre per 10.2.4,  $\phi^*$  trasforma funzioni regolari in funzioni regolari.  $\square$

*Esempio 10.3.3.* La proiezione  $\pi: \mathbb{A}^{n+1} - \{0\} \rightarrow \mathbb{P}^n$  è regolare. Infatti, per ogni indice  $i = 0, \dots, n$ , la restrizione di  $\pi$  all'aperto  $\{x_i \neq 0\} \subset \mathbb{P}^n$  è

$$\pi: \{x \in \mathbb{A}^{n+1} \mid x_i \neq 0\} \rightarrow \mathbb{A}^n, \quad (x_0, \dots, x_n) \mapsto \left( \frac{x_0}{x_i}, \dots, \frac{x_n}{x_i} \right)$$

le cui coordinate sono le funzioni  $x_j/x_i$ , per  $j \neq i$ , che sono regolari sul dominio.

**Definizione 10.3.4.** *Un morfismo tra varietà quasiproiettive si dice un **isomorfismo regolare** se è regolare, bigettivo ed ha inverso regolare.*

Ad esempio le proiettività sono isomorfismi regolari di  $\mathbb{P}^n$ .

**Definizione 10.3.5.** *Una varietà quasiproiettiva si dice **affine** (risp.: **proiettiva**) se è isomorfa, nel senso di 10.3.4, ad un chiuso di uno spazio affine (risp.: proiettivo).*

*Esempio 10.3.6.* Nelle stesse notazioni dell'Esempio 10.1.11, la proiezione  $\pi: Y \rightarrow X_f$  è un isomorfismo di varietà quasiproiettive con inverso  $s: X_f \rightarrow Y$ ,  $s(x) = (x, f(x)^{-1})$ : in particolare  $X_f$  è una varietà affine. Infatti  $X_f \subset \mathbb{A}^n$  è localmente chiuso e la mappa composta  $Y \rightarrow \mathbb{A}^n$  è indotta dalla proiezione sulle prime coordinate ed è quindi continua. Similmente le coordinate di  $s$  sono funzioni regolari su  $X_f$  e quindi anche  $s$  è regolare per il Lemma 10.3.2.

**Lemma 10.3.7.** *Ogni varietà quasiproiettiva possiede una base di aperti affini.*

*Dimostrazione.* Precisiamo che con il termine aperto affine di  $X$  intendiamo un aperto di Zariski che, con la struttura di varietà indotta da  $X$ , è una varietà affine nel senso di 10.3.5. Sia  $X$  una varietà quasiproiettiva, per definizione  $X$  è un sottoinsieme di uno "spazio modello"  $M$  che è unione finita di spazi affini. Quindi esiste un ricoprimento aperto finito  $X = \cup X_i$  tale che ogni  $X_i$  è un sottoinsieme localmente chiuso in uno spazio affine. Non è quindi restrittivo assumere  $X \subset \mathbb{A}^n$  quasi-affine; sia  $\overline{X}$  la chiusura di  $X$  in  $\mathbb{A}^n$ ,  $Y = \overline{X} - X$ . Una base di  $X$  è allora data dagli aperti  $\overline{X}_f$ , con  $f \in V(Y) \subset \mathbb{K}[\overline{X}]$ . Tali aperti sono varietà affini per l'Esempio 10.3.6.  $\square$

Un utile criterio per stabilire la regolarità di una applicazione è il seguente:

**Corollario 10.3.8.** *Sia  $\phi: X \rightarrow Y$  un'applicazione tra varietà quasiproiettive e  $Y = \cup Y_i$  un ricoprimento di aperti affini. Allora  $\phi$  è regolare se e solo se per ogni indice  $i$  l'insieme  $V_i = \phi^{-1}(Y_i)$  è aperto in  $X$  e  $\phi^*\mathbb{K}[Y_i] \subset \mathcal{O}_X(V_i)$ .*

*Dimostrazione.* Immediata conseguenza di 10.2.6.  $\square$

*Esempio 10.3.9.* Siano  $F_0, \dots, F_m \in \mathbb{K}[x_0, \dots, x_n]$  omogenei dello stesso grado e sia  $U \subset \mathbb{P}^n$  un aperto tale che  $U \cap V(F_0, \dots, F_m) = \emptyset$ . Allora l'applicazione  $\phi: U \rightarrow \mathbb{P}^m$ ,  $\phi([x]) = [F_0(x), \dots, F_m(x)]$  è regolare. Infatti  $U_i := \phi^{-1}(\{y_i \neq 0\}) = \{[x] \in U \mid F_i(x) \neq 0\}$  è un aperto e la restrizione di  $\phi$  a  $U_i$  ha come coordinate le funzioni regolari  $F_j/F_i$ , per  $j \neq i$ .

**Teorema 10.3.10.** *Sia  $U \subset \mathbb{P}^n$  un aperto nonvuoto e sia  $\phi: U \rightarrow \mathbb{P}^m$  un morfismo regolare. Allora esistono, unici a meno di costante moltiplicativa,  $m+1$  polinomi  $F_0, \dots, F_m \in \mathbb{K}[x_0, \dots, x_n]$  omogenei dello stesso grado e senza fattori comuni tali che  $V(F_0, \dots, F_m) \cap U = \emptyset$  e  $\phi = [F_0, \dots, F_m]$  (vedi Esempio 10.3.9). In particolare il chiuso  $\mathbb{P}^n - U$  ha dimensione  $\geq (n-m-1)$  e ogni automorfismo regolare di  $\mathbb{P}^n$  è una proiettività.*

*Dimostrazione.* Dimostriamo per prima cosa che per ogni  $p \in U$  esiste un aperto  $p \in V \subset U$  tale che l'enunciato del teorema vale per la restrizione di  $\phi$  a  $V$ . Prendiamo coordinate omogenee  $x_i$  su  $\mathbb{P}^n$  e  $y_j$  su  $\mathbb{P}^m$  tali che  $p = [1, 0, \dots, 0]$  e  $\phi(p) = [1, 0, \dots, 0]$ , dunque  $p \in \mathbb{A}_0^n = \{x_0 \neq 0\}$  ed esiste  $f \in \mathbb{K}[\mathbb{A}_0^n] = \mathbb{K}[x_1, \dots, x_n]$  tale che  $f(p) \neq 0$ ,  $\mathbb{A}_f^n = \mathbb{A}_0^n - V(f) \subset U$  e  $\phi(\mathbb{A}_f^n) \subset \mathbb{A}_0^m$ . Esistono  $g_1, \dots, g_m \in \mathbb{K}[x_1, \dots, x_n]$  ed un intero  $s > 0$  tali che  $\phi^* y_i = \frac{g_i}{f^s}$  per ogni  $i$ , a meno di sostituire  $f^s$  con  $f$  non è restrittivo assumere  $s = 1$  e quindi  $\phi = [f, g_1, \dots, g_m]$  su  $\mathbb{A}_f^n$ . Basta adesso porre  $V = \mathbb{A}_f^n$  ed  $F_0, \dots, F_m$  gli omogeneizzati di  $f, g_1, \dots, g_m$  divisi per il loro massimo comune divisore. Siano adesso  $p, q \in U$  e  $F_0, \dots, F_m, G_0, \dots, G_m \in \mathbb{K}[x_0, \dots, x_n]$  omogenei tali che:

1.  $\deg F_i = \deg F_j, \deg G_i = \deg G_j$  per ogni  $i, j$ .
2.  $\text{GCD}(F_0, \dots, F_m) = \text{GCD}(G_0, \dots, G_m) = 1$ .
3.  $p \notin V(F_0, \dots, F_m), q \notin V(G_0, \dots, G_m)$ .
4.  $\phi = [F_0, \dots, F_m]$  in un intorno di  $p$  e  $\phi = [G_0, \dots, G_m]$  in un intorno di  $q$ .

Dato che  $U$  è uno spazio irriducibile esiste un aperto  $W \subset U$  dove vale  $[F_0, \dots, F_m] = [G_0, \dots, G_m]: W \rightarrow \mathbb{P}^m$  e quindi  $F_i G_j = F_j G_i$  per ogni  $i, j$ . Sia  $F_0 = \prod H_i^{t_i}$  la decomposizione in fattori irriducibili, esiste allora  $j > 0$  tale che  $H_1$  non divide  $F_j$  e dato che  $H_1^{t_1}$  divide  $G_0 F_j = F_0 G_j$  si ha che  $H_1^{t_1}$  divide  $G_0$ . Ripetendo per ogni fattore irriducibile di  $F_0$  si deduce che  $F_0$  divide  $G_0$  e per simmetria esiste una costante  $a$  tale che  $F_i = a G_i$  per ogni  $i$ . La disuguaglianza  $n-m-1 \leq \dim(\mathbb{P}^n - U)$  segue dal fatto che, detto  $Y = V(F_0, \dots, F_m)$  si ha  $Y \subset \mathbb{P}^n - U$  e  $\dim Y \geq n-m-1$  per il Teorema 9.6.7. Un'applicazione regolare  $[F_0, \dots, F_n]: \mathbb{P}^n \rightarrow \mathbb{P}^n$  può essere un isomorfismo solo se i polinomi  $F_i$  hanno grado 1.  $\square$

**Definizione 10.3.11.** *Un morfismo  $\phi: X \rightarrow Y$  tra varietà quasiproiettive si dice **dominante** se  $\phi(X)$  è denso in  $Y$ .*

La restrizione di un morfismo dominante ad ogni aperto denso è ancora dominante; nei prossimi capitoli avremo bisogno del seguente risultato.

**Lemma 10.3.12.** *Sia  $\phi: X \rightarrow Y$  un morfismo dominante tra varietà quasiproiettive. Allora  $\phi(X)$  contiene un aperto denso di  $Y$ .*

*Dimostrazione.* (Cfr. Esercizio 10.11) Consideriamo prima il caso in cui  $Y$  è una varietà affine irriducibile. Possiamo scrivere  $X$  come unione finita di aperti affini  $X_i$ ; siccome  $\phi(X) = \cup \phi(X_i)$ , almeno una delle restrizioni di  $\phi$  a  $X_i$  è dominante. Possiamo quindi assumere senza perdita di generalità anche  $X$  affine e, a meno di sostituire  $X$  con il grafico di  $\phi$ , possiamo supporre  $X$  sia un chiuso di  $Y \times \mathbb{A}^n$  e che  $\phi$  sia la proiezione sul primo fattore. Abbiamo già dimostrato nell'Esempio 9.7.3 che  $\phi(X)$  è un insieme costruibile, cioè  $\phi(X) = \cup_{i=1}^s (C_i \cap U_i)$  con ogni  $C_i$  chiuso irriducibile,  $U_i$  aperto e  $C_i \cap U_i \neq \emptyset$ . Siccome  $\phi(X)$  è denso deve esistere  $i$  tale che  $C_i = Y$  e quindi  $U_i \subset \phi(X)$ . Se  $Y$  è una varietà quasiproiettiva qualsiasi, allora avrà un insieme finito di componenti irriducibili  $Y_1, \dots, Y_r$ . Per ogni  $i$  scegliamo un aperto affine non vuoto  $U_i \subset Y_i - \cup \{Y_j \mid j \neq i\}$ . Poiché ogni  $U_i$  è irriducibile e  $U_i \cap \phi(X) \neq \emptyset$ , per ogni indice  $i$  esiste un aperto  $V_i$  non vuoto tale che  $V_i \subset U_i \cap \phi(X)$ . L'unione dei  $V_i$  è l'aperto denso cercato.  $\square$

**Esercizi**

**10.12.** Siano  $X, Y$  varietà quasiproiettive. Dimostrare che un'applicazione  $\phi: X \rightarrow Y$  è regolare se e solo se per ogni aperto  $U \subset Y$  e per ogni  $x \in \phi^{-1}(U)$  esiste un aperto  $V \subset X$  tale che  $\phi(V) \subset U$  e  $\phi|_V^* \mathcal{O}_Y(U) \subset \mathcal{O}_X(V)$ .

**10.13.** Dimostrare le proprietà di categoricità, località ed ereditarietà dei morfismi regolari.

**10.14.** Dimostrare che:

1. Ogni proiettività  $f: \mathbb{P}^n \rightarrow \mathbb{P}^n$  è regolare.
2. L'immersione diagonale  $\Delta: \mathbb{P}^n \rightarrow \mathbb{P}^n \times \mathbb{P}^n$  è regolare.
3. Le proiezioni sui fattori  $\mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^n, \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^m$  sono regolari.

**10.15.** Sia  $X$  una varietà quasiproiettiva e  $Y$  una varietà affine. Dimostrare che esiste una bigezione naturale tra l'insieme delle applicazioni regolari  $X \rightarrow Y$  e l'insieme degli omomorfismi di  $\mathbb{K}$ -algebre  $\mathbb{K}[Y] \rightarrow \mathcal{O}_X(X)$ .

**10.16.** Sia  $L \subset \mathbb{P}^n$  un sottospazio proiettivo di dimensione  $n - m - 1$ . Provare che la proiezione di centro  $L$  non può essere estesa ad una applicazione regolare su un aperto contenente strettamente  $\mathbb{P}^n - L$ .

**10.17.** (caratteristica  $\neq 2$ ) Quali delle seguenti varietà quasiproiettive sono isomorfe ad  $\mathbb{A}^1 - \{0\}$ .

$$\begin{aligned} X &= \{x^2 + y^2 = 1\} \subset \mathbb{A}^2, & Y &= \{xy = 1\} \subset \mathbb{A}^2, \\ Z &= \{x + y^2 = 0\} \subset \mathbb{A}^2, & W &= Z \cap \{x \neq 1\}. \end{aligned}$$

**10.4 Le immersioni di Segre**

Ricordiamo la definizione delle immersioni di Veronese (Definizione 9.2.1). Consideriamo due interi positivi  $n$  e  $d$ , sia  $x_0, \dots, x_n$  un sistema di coordinate omogenee su  $\mathbb{P}^n$  e denotiamo con  $e_0, \dots, e_n$  la base canonica di  $\mathbb{Z}^{n+1}$ . Sia  $N = \binom{n+d}{n} - 1$  e consideriamo un sistema di coordinate omogenee  $\{y_I\}$  su  $\mathbb{P}^N$  indicizzate dai multiindici

$$I = i_0 e_0 + \dots + i_n e_n \in \mathbb{N}^{n+1}, \quad \text{con} \quad i_0 + \dots + i_n = d.$$

La  $d$ -esima immersione di Veronese

$$v_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$$

è l'applicazione definita dalle relazioni

$$y_I = x^I, \quad \text{dove} \quad x^{\sum i_j e_j} = \prod x_j^{i_j}.$$

Abbiamo già dimostrato (Proposizione 9.2.2) che  $v_d$  è una immersione topologica chiusa, in particolare l'immagine  $V_d = v_d(\mathbb{P}^n)$ , detta **varietà di Veronese**, eredita da  $\mathbb{P}^N$  una struttura di varietà proiettiva.

**Proposizione 10.4.1.** *Le immersioni di Veronese sono isomorfismi sull'immagine.*

*Dimostrazione.* L'Esempio 10.3.9 mostra che  $v_d$  è un morfismo regolare. Bisogna mostrare che, per ogni  $i = 0, \dots, n$ , l'applicazione  $v_d^{-1}: v_d(\{x_i \neq 0\}) \rightarrow \{x_i \neq 0\}$  è regolare, e questo segue semplicemente osservando che per ogni  $i, j$  vale

$$v_d(\{x_i \neq 0\}) = V_d \cap \{y_{de_i} \neq 0\}, \quad (v_d^{-1})^* \left( \frac{x_j}{x_i} \right) = \frac{y_{e_j+(d-1)e_i}}{y_{de_i}}.$$

□

**Corollario 10.4.2.** *Il complementare di ogni ipersuperficie proiettiva è una varietà affine.*

*Dimostrazione.* Sia  $X \subset \mathbb{P}^n$  una ipersuperficie proiettiva, diciamo  $X = V(f)$ , con  $f$  polinomio omogeneo di grado  $d$ . Allora, se  $v_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$  è la  $d$ -esima immersione di Veronese, esiste un iperpiano  $H \subset \mathbb{P}^N$  tale che  $v_d^{-1}(H) = X$  e quindi  $\mathbb{P}^n - X$  è isomorfo al chiuso affine  $V_d - H$ . □

Passiamo adesso alle **immersioni di Segre**. La più semplice delle immersioni di Segre è l'applicazione

$$\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^3, \quad ([x_0, x_1], [y_0, y_1]) \mapsto [x_0y_0, x_0y_1, x_1y_0, x_1y_1].$$

È ben noto, e comunque facile da dimostrare, che tale applicazione è iniettiva ed ha come immagine la quadrica di equazione  $z_0z_3 = z_1z_2$ . Tale applicazione si generalizza senza problemi ad un qualsiasi prodotto di spazi proiettivi. Nel seguito siano  $n$  e  $m$  due interi positivi fissati.

**Definizione 10.4.3.** *L'immersione di Segre*

$$s: \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{nm+n+m}$$

è definita in coordinate omogenee come

$$([\dots, x_i, \dots], [\dots, y_j, \dots]) \mapsto [\dots, x_i y_j, \dots].$$

In altri termini, se consideriamo  $\mathbb{P}^{nm+n+m}$  come il proiettivizzato dello spazio vettoriale delle matrici di ordine  $(n+1) \times (m+1)$ , allora  $s([x], [y]) = [w]$ , dove  $w$  è la matrice di coefficienti  $w_{ij} = x_i y_j$ . È chiaro dalla definizione che l'immagine di  $s$  coincide con il proiettivizzato dell'insieme delle matrici di rango 1 ed è quindi uguale al chiuso definito dalle equazioni  $w_{ij}w_{hk} - w_{ik}w_{hj} = 0$ .

**Proposizione 10.4.4.** *L'immersione di Segre  $s: \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^{nm+n+m}$  è chiusa ed è un isomorfismo sull'immagine.*

*Dimostrazione.* Sia  $\{w_{ij}\}$ , per  $i = 0, \dots, n$  e  $j = 0, \dots, m$  il sistema di coordinate omogenee su  $\mathbb{P}^{nm+n+m}$  nel quale  $s$  è definita dalle relazioni  $w_{ij} = x_i y_j$  e denotiamo  $S$  l'immagine di  $s$ . Allora vale  $s^{-1}(S \cap \{w_{ij} \neq 0\}) = \{x_i y_j \neq 0\}$  e bisogna dimostrare che  $s: \mathbb{A}^{n+m} = \{x_i y_j \neq 0\} \rightarrow S \cap \{w_{ij} \neq 0\}$  è un isomorfismo di varietà affini per ogni  $i, j$ : per evidenti ragioni di simmetria basta verificare questo fatto per  $i = j = 0$ . Un sistema di coordinate affini su  $\{x_0 y_0 \neq 0\}$  è  $u_1, \dots, u_n, v_1, \dots, v_m$ , dove  $u_i = x_i/x_0$  e  $v_j = y_j/y_0$ . Un sistema di coordinate affini su  $\{w_{00} \neq 0\}$  è  $z_{ij}$ , dove  $i + j > 0$  e  $z_{ij} = w_{ij}/w_{00}$ . In tali sistemi di coordinate l'applicazione  $s$  e la sua inversa si scrivono come

$$s(u, v) = (u_1, \dots, u_n, v_1, \dots, v_m, u_1 v_1, \dots, u_n v_m)$$

$$s^{-1}(z) = (z_{10}, \dots, z_{n0}, z_{01}, \dots, z_{0m})$$

e quindi sono entrambe applicazioni regolari. □

Le immagini delle immersioni di Segre vengono dette **Varietà di Segre**. Al pari delle varietà di Veronese, la loro nozione ha senso solo se vengono considerate come sottovarietà di uno spazio proiettivo e non come classi di isomorfismo di varietà quasiproiettive.

È utile dare una descrizione astratta della mappa di Segre: se  $V, W$  sono spazi vettoriali di dimensione finita, la mappa di Segre  $s: \mathbb{P}(V) \times \mathbb{P}(W) \rightarrow \mathbb{P}(\text{Hom}(V^\vee, W))$  è data da  $s([a], [b]) = [a \otimes b]$ , dove per definizione  $(a \otimes b)h = h(a)b$  per ogni  $h \in V^\vee$ . Appare chiaro che la varietà di Segre corrisponde al proiettivizzato delle applicazioni lineari di rango  $\leq 1$  e che quindi è definita da equazioni quadratiche.

Una ulteriore generalizzazione della immersione di Segre consiste nel considerare il prodotto di un numero arbitrario di spazi proiettivi, in tal caso  $s$  è data da

$$s: \prod_{i=1}^r \mathbb{P}^{n_i} \rightarrow \mathbb{P}^N, \quad N = \prod_{i=1}^r (n_i + 1) - 1,$$

$$s([x^1], \dots, [x^r]) = [\dots, x_{i_1}^1 \cdots x_{i_r}^r, \dots].$$

Anche tali immersioni sono isomorfismi sull'immagine: si può verificare questo fatto ripetendo sostanzialmente la dimostrazione della Proposizione 10.4.4 oppure più semplicemente per induzione su  $r$ , osservando che tale applicazione è la composizione di

$$\mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \dots \times \mathbb{P}^{n_r} \xrightarrow{s \times Id} \mathbb{P}^{n_1 n_2 + n_1 + n_2} \times \mathbb{P}^{n_3} \times \dots \times \mathbb{P}^{n_r} \xrightarrow{s} \mathbb{P}^N.$$

La prima conseguenza dell'immersione di Segre è quindi che il *prodotto di spazi proiettivi è una varietà proiettiva*. Più in generale se  $X_i \subset \mathbb{P}^{n_i}$ , per  $i = 1, \dots, k$  sono sottovarietà chiuse, allora la sottovarietà

$$X_1 \times \dots \times X_k \subset \mathbb{P}^{n_1} \times \dots \times \mathbb{P}^{n_k}$$

è una varietà proiettiva.

**Corollario 10.4.5.** *Ogni varietà quasiproiettiva è isomorfa ad un sottoinsieme localmente chiuso di uno spazio proiettivo  $\mathbb{P}^n$ .*

*Dimostrazione.* Per definizione una varietà quasiproiettiva è un sottoinsieme localmente chiuso di uno spazio misto affine multiproiettivo. Considerando eventualmente una immersione della componente affine in uno spazio proiettivo non è restrittivo supporre che ogni varietà quasiproiettiva è un sottoinsieme localmente chiuso di un prodotto di spazi proiettivi. Basta adesso considerare l'immersione di Segre.  $\square$

## Esercizi

**10.18.** Mostrare che il gruppo delle proiettività di  $\mathbb{P}^n$  in sé ha una struttura di varietà affine.

**10.19.** Dimostrare che ogni varietà proiettiva è isomorfa ad una intersezione di quadriche in un opportuno spazio proiettivo.

**10.20.** Sia  $X$  una varietà quasiproiettiva e  $\phi: X \rightarrow \mathbb{P}^n$  un morfismo regolare. Provare che esiste una varietà proiettiva  $Y$  tale che  $X$  è isomorfa ad un aperto di  $Y$  e  $\phi$  si estende ad una applicazione regolare  $\psi: Y \rightarrow \mathbb{P}^n$ . (Sugg.: si assuma  $X$  localmente chiuso in  $\mathbb{P}^m$  e si consideri la chiusura del grafico di  $\phi$  in  $\mathbb{P}^m \times \mathbb{P}^n$ .)

**10.21.** Sia  $\mathbb{P}^2 = \bigcup_{i=1}^s U_i$  un ricoprimento aperto. Se ogni  $U_i$  è isomorfo, come varietà, ad un chiuso affine allora  $s \geq 3$ . Generalizzare a ricoprimenti aperti di  $\mathbb{P}^n$



## 10.5 Prodotti

Vogliamo adesso definire il prodotto di due varietà quasiproiettive. Iniziamo con il caso più semplice delle varietà affini. Consideriamo due varietà affini, cioè due varietà rispettivamente isomorfe a due chiusi affini  $X \subset \mathbb{A}^n$  e  $Y \subset \mathbb{A}^m$ . Il sottoinsieme  $X \times Y \subset \mathbb{A}^{n+m}$  è ancora un chiuso affine e quindi definisce una struttura di varietà affine sul prodotto cartesiano  $X \times Y$ . Per dimostrare che tale struttura non dipende dalla scelta delle immersioni di  $X$  e  $Y$  in spazi affini, basta tenere presente il Corollario 10.1.8 e osservare che l'algebra delle funzioni regolari  $\mathbb{K}[X \times Y]$  coincide con la sottoalgebra di  $\mathbb{K}^{X \times Y}$  generata da  $p_X^* \mathbb{K}[X]$  e  $p_Y^* \mathbb{K}[Y]$ , dove  $p_X$  e  $p_Y$  sono le proiezioni sui fattori.

**Lemma 10.5.1.** *Consideriamo i chiusi affini  $X \subset \mathbb{A}^n$ , con ideale  $I(X) \subset \mathbb{K}[x_1, \dots, x_n]$  e  $Y \subset \mathbb{A}^m$ , con ideale  $I(Y) \subset \mathbb{K}[y_1, \dots, y_m]$ . Denotiamo con  $p_X: X \times Y \rightarrow X$  la proiezione sul primo fattore. Allora:*

1.  $X \times Y \subset \mathbb{A}^{n+m}$  è un chiuso e  $I(X \times Y) \subset \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$  è uguale all'ideale generato da  $I(X)$  e  $I(Y)$ .
2. Se  $f(x, y) \in \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$  e scriviamo

$$f(x, y) = \sum_{i=1}^r f_i(x)g_i(y) + h(x, y),$$

con  $h \in I(X \times Y)$  e  $r \geq 0$  minimo intero possibile, allora vale

$$p_X(\{(x, y) \in X \times Y \mid f(x, y) \neq 0\}) = \bigcup_{i=1}^r \{x \in X \mid f_i(x) \neq 0\}.$$

3. L'applicazione  $p_X$  è aperta.

*Dimostrazione.* Denotiamo con  $J \subset \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$  l'ideale generato da  $I(X)$  e  $I(Y)$ . È immediato osservare che  $V(J) = X \times Y \subset \mathbb{A}^{n+m}$  e quindi  $X \times Y$  è un chiuso affine. Sia  $f(x, y) \in \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$  e consideriamo una espressione

$$f(x, y) = \sum_{i=1}^r f_i(x)g_i(y) + h(x, y) \tag{10.4}$$

con  $h \in J$  e  $r \geq 0$  minimo intero possibile. Notiamo che, essendo  $r$  minimo, per ogni  $i = 1, \dots, r$  vale  $f_i \notin I(X)$ . Vogliamo provare che vale

$$p_X(\{(x, y) \in X \times Y \mid f(x, y) \neq 0\}) = \bigcup_{i=1}^r \{x \in X \mid f_i(x) \neq 0\}.$$

L'inclusione  $\subset$  è ovvia. Per evidenti ragioni di simmetria, per dimostrare l'inclusione  $\supset$  basta dimostrare che

$$p_X(\{(x, y) \in X \times Y \mid f(x, y) \neq 0\}) \supset \{x \in X \mid f_r(x) \neq 0\}.$$

Sia  $p \in X$  un punto tale che  $f_r(p) \neq 0$ . Se per assurdo  $f(p, y) = 0$  per ogni  $y \in Y$ , allora  $\sum_{i=1}^r f_i(p)g_i(y) \in I(Y)$  e quindi

$$g_r(y) + \frac{1}{f_r(p)} \sum_{i=1}^{r-1} f_i(p)g_i(y) \in I(Y) \subset J.$$

Sostituendo in 10.4 e semplificando si ottiene

$$f(x, y) - \sum_{i=1}^{r-1} \left( f_i(x) - f_r(x) \frac{f_i(p)}{f_r(p)} \right) g_i(y) \in J.$$

Dato che  $r$  era il minimo possibile si ottiene una contraddizione. Se  $f \in I(X \times Y)$ , allora si ha  $\{(x, y) \in X \times Y \mid f(x, y) \neq 0\} = \emptyset$  e quindi necessariamente  $r = 0$  e  $f = h \in J$ . Adesso tutto segue facilmente.  $\square$

**Lemma 10.5.2.** *Siano  $X, Y$  due varietà affini e  $U \subset X, V \subset Y$  due aperti affini. Allora per ogni aperto  $W \subset U \times V$  vale*

$$\mathcal{O}_{U \times V}(W) = \mathcal{O}_{X \times Y}(W)$$

e quindi la struttura di varietà prodotto in  $U \times V$  coincide con la struttura di sottovarietà aperta di  $X \times Y$ .

*Dimostrazione.* Per evitare possibili ambiguità, se  $A \subset X$  e  $B \subset Y$  sono aperti affini, scriviamo temporaneamente  $\mathbb{K}[A] \otimes \mathbb{K}[B]$  per indicare l'algebra delle funzioni su  $A \times B$  generata da  $\mathbb{K}[A]$  e  $\mathbb{K}[B]$ , cioè  $\mathbb{K}[A] \otimes \mathbb{K}[B] = \mathbb{K}[A \times B]$ , dove su  $A \times B$  ha la struttura prodotto. L'inclusione  $\supset$  è chiara: infatti ogni  $f \in \mathbb{K}[X \times Y]$  si rappresenta con una espressione algebrica di elementi di  $\mathbb{K}[X]$  e  $\mathbb{K}[Y]$  e quindi la restrizione di  $f$  a  $U \times V$  appartiene a  $\mathbb{K}[U] \otimes \mathbb{K}[V]$ . Ogni funzione di  $\mathcal{O}_{X \times Y}(W)$  è per definizione localmente quoziente di elementi di  $\mathbb{K}[X \times Y]$  e quindi appartiene anche a  $\mathcal{O}_{U \times V}(W)$ .

Siano viceversa  $f \in \mathcal{O}_{U \times V}(W)$  e  $(x, y) \in W$ . Vogliamo dimostrare che in un intorno di  $(x, y)$  la funzione  $f$  si scrive come un quoziente di elementi di  $\mathbb{K}[X \times Y]$ . Scegliamo  $g \in \mathbb{K}[X]$  e  $h \in \mathbb{K}[Y]$  tali che  $x \in X_g \subset U$  e  $y \in Y_h \subset V$  e denotiamo  $W_{gh} = W \cap (X_g \times Y_h)$ . Abbiamo appena visto che la restrizione di  $f$  a  $W_{gh}$  appartiene a  $\mathcal{O}_{X_g \times Y_h}(W_{gh})$ . D'altra parte ogni elemento di  $\mathbb{K}[X_g] \otimes \mathbb{K}[Y_h]$  è il quoziente di un elemento di  $\mathbb{K}[X] \otimes \mathbb{K}[Y]$  per una potenza sufficientemente grande di  $gh$  e quindi  $f$  è, in un intorno di  $(x, y)$ , il quoziente di due elementi di  $\mathbb{K}[X \times Y]$ .  $\square$

**Definizione 10.5.3.** *Chiameremo **prodotto** di due varietà quasiproiettive  $X$  e  $Y$  una struttura di varietà quasiproiettiva sul prodotto cartesiano  $X \times Y$  tale che per ogni coppia di aperti affini  $U \subset X$  e  $V \subset Y$ , l'insieme  $U \times V$  è aperto in  $X \times Y$  e la struttura di varietà prodotto in  $U \times V$  coincide con la struttura di sottovarietà aperta di  $X \times Y$ .*

Vogliamo dimostrare esistenza ed unicità del prodotto. L'unicità è facile a vedersi: infatti se  $X = \cup X_i$  e  $Y = \cup Y_j$  sono due ricoprimenti in aperti affini, allora il fascio strutturale  $\mathcal{O}_{X \times Y}$  è univocamente determinato dalle restrizioni agli aperti  $X_i \times Y_j$ .

Proviamo l'esistenza: per il Corollario 10.4.5 possiamo limitarci a considerare il prodotto di sottoinsiemi localmente chiusi dello spazio proiettivo. Analizziamo prima il caso delle varietà quasiasfinitive. Notiamo a tal fine che se  $X \subset \mathbb{A}^n$  e  $Y \subset \mathbb{A}^m$  sono sottoinsiemi localmente chiusi, allora  $X \times Y$  è localmente chiuso in  $\mathbb{A}^{n+m}$ .

**Lemma 10.5.4.** *Siano  $X \subset \mathbb{A}^n$  e  $Y \subset \mathbb{A}^m$  due sottoinsiemi localmente chiusi. Allora la varietà quasiasfinitiva  $X \times Y \subset \mathbb{A}^{n+m}$  è il prodotto di  $X$  e  $Y$ .*

*Dimostrazione.* La varietà quasiasfinitiva  $X \times Y \subset \mathbb{A}^{n+m}$  è una sottovarietà aperta della varietà affine  $\bar{X} \times \bar{Y} \subset \mathbb{A}^{n+m}$  per la quale si applica il risultato del Lemma 10.5.2.  $\square$

**Teorema 10.5.5.** *Siano  $X \subset \mathbb{P}^n$  e  $Y \subset \mathbb{P}^m$  due sottoinsiemi localmente chiusi. Allora la varietà quasiproiettiva  $X \times Y \subset \mathbb{P}^n \times \mathbb{P}^m$  è il prodotto di  $X$  e  $Y$ ; in particolare il prodotto di due varietà proiettive è una varietà proiettiva. Inoltre, per ogni coppia di sottoinsiemi localmente chiusi  $X' \subset X$  e  $Y' \subset Y$  la struttura di varietà prodotto su  $X' \times Y'$  coincide con la struttura di sottovarietà di  $X \times Y$ .*

*Dimostrazione.* Siano  $U \subset X$  e  $V \subset Y$  due aperti affini e vogliamo dimostrare che la restrizione del fascio strutturale  $\mathcal{O}_{X \times Y}$  a  $U \times V$  coincide con il fascio del prodotto affine. Scegliamo  $U = \cup U_i$  e  $V = \cup V_j$  ricoprimenti in aperti affini tali che ogni  $U_i$  è contenuto nel complementare di un iperpiano di  $\mathbb{P}^n$  ed ogni  $V_j$  è contenuto nel complementare di un iperpiano di  $\mathbb{P}^m$ . Per il Lemma 10.5.4, per ogni  $i, j$  la struttura di sottovarietà aperta su  $U_i \times V_j \subset X \times Y$  coincide con la struttura prodotto. Basta adesso applicare il Lemma 10.5.2. Se  $X'$  è localmente chiuso in  $X$  allora lo è anche in  $\mathbb{P}^n$ ; similmente per  $Y'$  e quindi la struttura di varietà prodotto su  $X' \times Y'$  è uguale alla struttura di sottovarietà di  $\mathbb{P}^n \times \mathbb{P}^m$  che è coincide con la struttura di sottovarietà di  $X \times Y$ .  $\square$

Vediamo adesso alcune semplici conseguenze:

*Esempio 10.5.6.* Siano  $X, Y$  varietà quasiproiettive. Allora la proiezione  $X \times Y \rightarrow X$  è un morfismo regolare e aperto. Basta infatti ridursi al caso affine e applicare il Lemma 10.5.1.

*Esempio 10.5.7.* Siano  $X, Y, Z$  varietà quasiproiettive,  $f: Z \rightarrow X \times Y$  un'applicazione e  $f_X: Z \rightarrow X$ ,  $f_Y: Z \rightarrow Y$  le composizioni di  $f$  con le proiezioni sui fattori. Allora  $f$  è regolare se e solo se  $f_X$  e  $f_Y$  sono regolari. Infatti possiamo ridurre il problema al caso affine dove è facile a dimostrarsi.

*Esempio 10.5.8.* Dati due morfismi regolari di varietà  $f: X \rightarrow Z$  e  $g: Y \rightarrow W$ , il morfismo prodotto  $f \times g: X \times Y \rightarrow Z \times W$  è regolare. Questo segue immediatamente da 10.5.7.

*Esempio 10.5.9.* Sia  $X$  una varietà quasiproiettiva. Allora la diagonale  $\Delta_X \subset X \times X$  è chiusa nel prodotto. Questo si verifica direttamente per  $X = \mathbb{P}^n$  e quindi basta osservare che se  $X \subset \mathbb{P}^n$ , allora  $\Delta_X = \Delta_{\mathbb{P}^n} \cap X \times X$ .

*Esempio 10.5.10.* Siano dati due morfismi regolari  $f, g: X \rightarrow Y$  ed un sottoinsieme denso  $D \subset X$ . Se  $f(x) = g(x)$  per ogni  $x \in D$ , allora  $f = g$ . Infatti  $(f, g): X \rightarrow Y \times Y$  è regolare e  $(f, g)^{-1}(\Delta_Y)$  è un chiuso che contiene  $D$ .

*Esempio 10.5.11.* Il grafico  $G_f \subset X \times Y$  di un morfismo regolare  $f: X \rightarrow Y$  è chiuso e la proiezione  $G_f \rightarrow X$  è un isomorfismo. Infatti  $G_f$  è la controimmagine di  $\Delta_Y$  mediante il morfismo  $f \times Id_Y$  ed il morfismo  $(id, f): X \rightarrow G_f$  è l'inverso regolare della proiezione.

La proprietà 10.5.10 si esprime gerzialmente dicendo che le varietà quasiproiettive sono **separate**.

Una variante del prodotto è il prodotto fibrato; dati due morfismi regolari  $f: X \rightarrow Z$  e  $g: Y \rightarrow Z$  si definisce

$$X \times_Z Y = \{(x, y) \in X \times Y \mid f(x) = g(y)\} = (f \times g)^{-1}(\Delta_Z)$$

si tratta evidentemente di una sottovarietà chiusa del prodotto usuale.

## Esercizi

**10.22.** Siano  $U, V$  aperti affini di una varietà quasiproiettiva. Dimostrare che  $U \cap V$  è affine.

## 10.6 Morfismi proiettivi

**Definizione 10.6.1.** Un morfismo regolare di varietà quasiproiettive  $f: X \rightarrow Y$  si dice una **immersione chiusa** se  $f(X)$  è chiuso in  $Y$  e se  $f: X \rightarrow f(X)$  è un isomorfismo.

*Esempio 10.6.2.* Per ogni morfismo regolare  $f: X \rightarrow Y$ , l'applicazione

$$g: X \rightarrow X \times Y, \quad g(x) = (x, f(x))$$

è una immersione chiusa. Infatti  $g(X)$  coincide con il grafico di  $f$  e basta applicare 10.5.11.

**Definizione 10.6.3.** Un morfismo regolare di varietà quasiproiettive  $f: X \rightarrow Y$  si dice un **morfismo proiettivo** se per ogni  $y \in Y$  esiste un aperto  $U \subset Y$ , un intero  $n \geq 0$  ed una immersione chiusa  $h: V = f^{-1}(U) \rightarrow U \times \mathbb{P}^n$  tale che  $f|_V$  è la composizione di  $h$  e della proiezione sul primo fattore.

Si noti che se  $X \subset \mathbb{P}^n$  è una varietà proiettiva, allora ogni applicazione regolare  $X \rightarrow Y$  è proiettiva. Infatti basta considerare  $U = Y$  e  $h: X \rightarrow Y \times \mathbb{P}^n$  l'immersione sul grafico di  $f$ .

**Proposizione 10.6.4.** Ogni morfismo proiettivo è chiuso.

*Dimostrazione.* Siccome la restrizione di un morfismo proiettivo  $f: X \rightarrow Y$  ad un chiuso di  $X$  è ancora proiettivo basta dimostrare che esiste un ricoprimento affine  $Y = \cup U_i$  tale che  $f(X) \cap U_i = f(f^{-1}(U_i))$  è chiuso in  $U_i$  per ogni indice  $i$ . Non è quindi restrittivo assumere  $Y \subset \mathbb{A}^m$  chiuso affine e  $X \subset Y \times \mathbb{P}^n$ ; la dimostrazione segue da 9.1.7 e dal fatto che  $Y \times \mathbb{P}^n$  è chiuso in  $\mathbb{A}^m \times \mathbb{P}^n$ .  $\square$

**Corollario 10.6.5.** Sia  $X$  una varietà proiettiva irriducibile, allora  $\mathcal{O}_X(X) = \mathbb{K}$ . Più in generale ogni morfismo da una varietà proiettiva irriducibile ad una varietà affine è costante.

*Dimostrazione.* Sia  $Y \subset \mathbb{A}^n$  una varietà affine e  $f: X \rightarrow Y$  regolare; componendo  $f$  con l'inclusione  $Y \subset \mathbb{P}^n$  otteniamo un morfismo proiettivo  $g: X \rightarrow \mathbb{P}^n$ . Per la Proposizione 10.6.4  $g(X)$  è un chiuso di  $\mathbb{P}^n$  che non interseca l'iperpiano all'infinito e quindi deve avere dimensione 0. Le funzioni regolari su  $X$  possono essere pensate come morfismi regolari a valori in  $\mathbb{A}^1$ .  $\square$

**Teorema 10.6.6.** Sia  $f: X \rightarrow Y$  un morfismo regolare di varietà quasiproiettive; per ogni  $y \in Y$  denotiamo  $X_y = f^{-1}(y)$ . Allora:

1. Per ogni  $y \in Y$  e  $x \in X_y$  vale  $\dim_x X \leq \dim_x X_y + \dim_y \overline{f(X)}$ .
2. Se  $X$  è irriducibile, allora esiste un aperto nonvuoto  $U \subset \overline{f(X)}$  tale che per ogni  $y \in U$  vale  $\dim X = \dim \overline{f(X)} + \dim X_y$ .

Se inoltre  $f$  è proiettivo, allora vale anche:

3. L'applicazione  $y \mapsto \dim X_y$  è semicontinua superiormente.
4. Se  $Y$  è irriducibile e le fibre  $X_y$  sono tutte irriducibili della stessa dimensione, allora  $X$  è irriducibile.

*Dimostrazione.* Possiamo tranquillamente assumere che  $f(X)$  sia denso in  $Y$ . Proviamo dapprima i 4 enunciati nel caso in cui  $f$  è proiettivo; dato che basta dimostrare il teorema per le restrizioni di  $f$  ad un ricoprimento aperto di  $Y$  non è restrittivo supporre  $Y$  affine e  $X$  chiuso in  $\mathbb{P}^n \times Y$ . Il teorema segue quindi da 9.7.1 e 9.7.2.

Se  $f$  non è proiettivo si consideri  $X \subset \overline{X}$  una chiusura proiettiva (ricordiamo che  $X$  è aperto in  $\overline{X}$ ) e sia  $Z$  la chiusura del grafico di  $f$  in  $\overline{X} \times Y$  e  $f: Z \rightarrow Y$  il morfismo indotto dalla proiezione. Dato che per ogni  $y \in Y$ , la fibra  $X_y$  è aperta (possibilmente vuota) in  $Z_y$ , il punto 1) segue immediatamente dal caso proiettivo. Se  $X$  è irriducibile, allora anche  $Z$  è irriducibile ed esiste un aperto  $U \subset Y$  tale che per ogni  $y \in U$  e per ogni  $z \in Z_y$  vale  $\dim_z Z_y = \dim Z - \dim Y = \dim X - \dim Y$ . Siccome  $f(X)$  è denso esso interseca  $U$  e questo prova il punto 2).  $\square$

**Corollario 10.6.7.** *Siano  $X, Y$  varietà quasiproiettive irriducibili, allora  $X \times Y$  è irriducibile e  $\dim X \times Y = \dim X + \dim Y$ .*

*Dimostrazione.* Le varietà  $X$  e  $Y$  sono aperte nelle loro chiusure proiettive, non è quindi restrittivo supporre  $X$  e  $Y$  proiettive. In questo caso basta applicare il Teorema 10.6.6 al morfismo di proiezione  $X \times Y \rightarrow Y$ .  $\square$

**Esercizi**

**10.23.** Dimostrare che la composizione di morfismi proiettivi è ancora un morfismo proiettivo.

**10.24.** Dimostrare che, se  $f: X \rightarrow Y$  è un morfismo proiettivo e  $g: Z \rightarrow Y$  è un morfismo regolare, allora  $X \times_Y Z \rightarrow Z$  è proiettivo.

**10.25.** Sia  $f: X \rightarrow Y$  un morfismo regolare di varietà quasiproiettive. Mostrare che per ogni sottoinsieme  $Z \subset X$  costruibile anche  $f(Z)$  è costruibile.

**10.26.** Sia  $X \subset \mathbb{P}^n$  chiuso di dimensione  $> 0$ . Provare che  $C(X) - \{0\}$  non è isomorfo a  $X \times (\mathbb{K} - \{0\})$ .

**10.27 (Teorema di Hopf).** Siano  $A, B, C$  spazi vettoriali di dimensione finita su di un campo algebricamente chiuso e  $\mu: A \otimes B \rightarrow C$  lineare e separatamente iniettiva, cioè tale che se  $a, b \neq 0$  allora  $\mu(a \otimes b) \neq 0$ . Provare che  $\dim C \geq \dim A + \dim B - 1$ . (Sugg.:  $\mathbb{P}(\text{Ker}(\mu))$  non interseca la varietà di Segre  $\mathbb{P}(A) \times \mathbb{P}(B) \subset \mathbb{P}(A \otimes B)$ .)

**10.28 (Lemma di Rigidità).** Sia  $f: X \rightarrow Y$  un morfismo proiettivo di varietà quasiproiettive irriducibili le cui fibre hanno tutte la stessa dimensione. Provare:

1. Se esiste una fattorizzazione  $f = pq$ , con  $q: X \rightarrow Z$  e  $p: Z \rightarrow Y$  morfismi proiettivi, allora le fibre di  $p: q(X) \rightarrow Y$  hanno tutte la stessa dimensione.
2. Se  $g: X \rightarrow \mathbb{P}^n$  è un morfismo regolare, allora la dimensione di  $g(f^{-1}(y))$  è costante al variare di  $y \in Y$ . (Sugg.: applicare il punto 1) alla fattorizzazione  $X \xrightarrow{(f,g)} Y \times \mathbb{P}^n \rightarrow Y$ .)

**10.7 Punti lisci e singolari, spazio tangente di Zariski**

Sia  $X \subset \mathbb{A}^n$  un chiuso affine e  $u \in X$  un suo punto. In analogia con il caso delle curve piane, diremo che un vettore  $v = (v_1, \dots, v_n) \in \mathbb{K}^n$  è **tangente** a  $X$  nel punto  $u$  se per ogni  $f \in I(X)$  il polinomio  $f_v(t) = f(u + tv)$  ha una radice multipla per  $t = 0$ . Derivando rispetto a  $t$  si ottiene che  $v$  è tangente a  $X$  in  $u$  se e solo se per ogni  $f \in I(X)$  il vettore  $v$  appartiene al nucleo dell'applicazione lineare

$$df(u): \mathbb{K}^n \rightarrow \mathbb{K}, \quad \langle df(u), v \rangle = \sum_{i=1}^n v_i \frac{\partial f}{\partial x_i}(u).$$

L'insieme, che denoteremo  $T_u X \subset \mathbb{K}^n$ , dei vettori tangenti a  $X$  in  $u$  è un sottospazio vettoriale detto **spazio tangente di Zariski (immerso)**. Facciamo alcune semplici osservazioni:

1. Se  $X \subset Y \subset \mathbb{A}^n$  sono chiusi, allora  $I(Y) \subset I(X)$  e quindi  $T_u X \subset T_u Y$  per ogni  $u \in X$ .
2. Se  $X, Y \subset \mathbb{A}^n$  sono chiusi, allora  $I(X) + I(Y) \subset I(X \cap Y)$  a quindi  $T_u(X \cap Y) \subset T_u X \cap T_u Y$  per ogni  $u \in X \cap Y$ .

3. Lo spazio vettoriale  $T_u X$  dipende solo dal germe di  $X \subset \mathbb{A}^n$  in  $u$ : più precisamente, se  $Y \subset \mathbb{A}^n$  è un altro chiuso ed esiste un aperto  $U \subset \mathbb{A}^n$  tale che  $X \cap U = Y \cap U$ , allora  $T_u X = T_u Y$  per ogni  $u \in X \cap U$ . Infatti non è restrittivo supporre  $X = \overline{Y \cap U}$ , dunque  $X \subset Y$  e quindi  $T_u X \subset T_u Y$ . Inoltre,  $Y = X \cup (Y - U)$  ed esiste  $g \in I(Y - U)$  tale che  $g(u) = 1$ . Per ogni  $v \in T_u Y$  e per ogni  $f \in I(X)$  si ha  $fg \in I(Y)$  e quindi  $fg(u + tv)$  ha una radice multipla per  $t = 0$ . Poiché  $g(u) \neq 0$ , anche  $f(u + tv)$  ha una radice multipla in  $t = 0$  e quindi che  $v \in T_u X$ .
4. Se l'ideale  $I(X)$  è generato da  $f_1, \dots, f_s$ , allora la regola di Leibniz implica che  $v \in T_u X$  se e solo se  $\langle v, df_i(u) \rangle = 0$  per ogni  $i = 1, \dots, s$  e quindi  $T_u X$  è il nucleo dell'applicazione lineare  $\mathbb{K}^n \rightarrow \mathbb{K}^s$  rappresentata dalla matrice jacobiana  $\left( \frac{\partial f_i}{\partial x_j}(u) \right)$ .
5. L'applicazione  $u \mapsto \dim T_u X$  è semicontinua superiormente in  $X$ . Infatti, se  $f_1, \dots, f_s$  sono generatori di  $I(X)$  e denotiamo con  $J_h \subset \mathbb{K}[X]$  l'ideale generato dai determinanti minori di ordine  $(n-h+1)$  della matrice Jacobiana di  $f_1, \dots, f_s$ , allora vale  $\dim T_u X \geq h$  se e solo se  $u \in V(J_h)$ .

**Proposizione 10.7.1.** *Siano  $X \subset \mathbb{A}^n$  e  $Y \subset \mathbb{A}^m$  chiusi affini. Allora per ogni  $(x, y) \in X \times Y$  vale*

$$T_{(x,y)} X \times Y = T_x X \times T_y Y.$$

*Dimostrazione.* Per il Lemma 10.5.1 l'ideale  $I(X \times Y)$  è generato da  $I(X)$  e  $I(Y)$ .  $\square$

Vogliamo adesso definire lo spazio tangente in maniera più astratta.

**Lemma 10.7.2.** *Siano  $x_1, \dots, x_n$  un sistema di coordinate affini su  $\mathbb{A}^n$ ,  $X \subset \mathbb{A}^n$  un chiuso,  $u = (u_1, \dots, u_n)$  un punto di  $X$  e  $\mathfrak{m}_u$  l'ideale massimale di  $\mathcal{O}_{u,X}$ . Allora l'applicazione lineare*

$$\text{Hom}_{\mathbb{K}} \left( \frac{\mathfrak{m}_u}{\mathfrak{m}_u^2}, \mathbb{K} \right) \rightarrow T_u X, \quad \xi \mapsto (\xi(x_1 - u_1), \dots, \xi(x_n - u_n))$$

*è ben definita ed è un isomorfismo di  $\mathbb{K}$ -spazi vettoriali.*

*Dimostrazione.* Convieni pensare l'anello  $\mathcal{O}_{u,X}$  come l'insieme delle classi di equivalenza delle frazioni  $f/g$ , con  $f, g \in \mathbb{K}[x_1, \dots, x_n]$  e  $g(u) \neq 0$ , e dove  $f/g \sim h/k$  se e solo se esiste  $q$  tale che  $q(u) \neq 0$  e  $q(fk - gh) \in I(X)$ . L'ideale  $\mathfrak{m}_u$  è formato dalle classi di frazioni  $f/g$  con  $f(u) = 0$  ed è generato dai germi delle funzioni regolari  $x_1 - u_1, \dots, x_n - u_n$ . Dato un vettore  $v = (v_1, \dots, v_n) \in T_u X$  ed  $f/g \in \mathfrak{m}_u$  si verifica facilmente che il loro accoppiamento

$$\langle v, d(f/g)(u) \rangle = \frac{1}{g(u)} \sum v_i \frac{\partial f}{\partial x_i}(u) \in \mathbb{K}$$

è ben definito, cioè dipende solo dalla classe di equivalenza di  $f/g$ . Inoltre se  $f/g \in \mathfrak{m}_u^2$ , allora per la regola di Leibniz  $\langle v, d(f/g)(u) \rangle = 0$  e risulta quindi definita un'applicazione bilineare

$$T_u X \times \frac{\mathfrak{m}_u}{\mathfrak{m}_u^2} \rightarrow \mathbb{K}, \quad (v, f/g) \mapsto \langle v, d(f/g)(u) \rangle$$

che vogliamo dimostrare essere non degenerare. Siccome  $\langle v, d(x_i)(u) \rangle = v_i$  per ogni  $i$ , l'applicazione è non degenerare su  $T_u X$ .

Viceversa, se  $f/g \in \mathfrak{m}_u$  e  $\langle v, d(f/g)(u) \rangle = 0$  per ogni  $v \in T_u X$ , allora anche  $\langle v, df(u) \rangle = 0$  per ogni  $v \in T_u X$  e segue dalla definizione di  $T_u X$  che esiste  $h \in I(X)$  tale  $df(u) = dh(u)$ , cioè  $d(f-h)(u) = 0$  che equivale a dire che  $f-h \in \mathfrak{m}_u^2$ .  $\square$

**Definizione 10.7.3.** Sia  $X$  una varietà quasiproiettiva e  $u \in X$ . Si definisce lo **spazio tangente di Zariski (astratto)** di  $X$  in  $u$  come

$$T_u X = \text{Hom}_{\mathbb{K}} \left( \frac{\mathfrak{m}_u}{\mathfrak{m}_u^2}, \mathbb{K} \right),$$

dove  $\mathfrak{m}_u$  è l'ideale massimale dell'anello  $\mathcal{O}_{u,X}$  dei germi delle funzioni regolari in  $u$ .

Ove non sussistano ambiguità, diremo spazio tangente intendendo lo spazio tangente di Zariski.

**Lemma 10.7.4.** Sia  $X$  una varietà quasiproiettiva e  $U \subset X$  un aperto. Allora, per ogni  $u \in U$ , l'inclusione  $U \subset X$  induce un isomorfismo di spazi tangenti  $T_u U = T_u X$ .

*Dimostrazione.* Basta osservare che  $\mathcal{O}_{u,U} = \mathcal{O}_{u,X}$ . □

**Lemma 10.7.5.** Sia  $X$  una varietà quasiproiettiva. Allora per ogni punto  $u \in X$  vale  $\dim_{\mathbb{K}} T_u X \geq \dim_u X$ .

*Dimostrazione.* Entrambe le dimensioni dipendono da un intorno di  $u$  e quindi non è restrittivo supporre  $X$  chiuso in uno spazio affine  $\mathbb{A}^n$ . Se  $\dim_u X = 0$  non c'è nulla da dimostrare. Supponiamo quindi  $\dim_u X > 0$ . In tal caso  $\mathcal{O}_{u,X}$  contiene funzioni non costanti e quindi  $\mathfrak{m}_u \neq 0$ ; per Nakayama  $\mathfrak{m}_u \neq \mathfrak{m}_u^2$  e dunque lo spazio tangente di Zariski è diverso da 0. Possiamo adesso ragionare per induzione su  $d = \dim T_u X$ . Se  $d = 0$  abbiamo visto che anche  $\dim_u X = 0$ , se  $d > 0$  consideriamo un iperpiano  $H \subset \mathbb{A}^n$  passante per  $u$  tale che  $T_u X$  non è contenuto in  $T_u H$ ; per il Corollario 9.6.8 vale  $\dim_u(X \cap H) \geq \dim_u X - 1$  e per l'ipotesi induttiva

$$\dim_{\mathbb{K}} T_u X > \dim_{\mathbb{K}} (T_u X \cap T_u H) \geq \dim_{\mathbb{K}} T_u(X \cap H) \geq \dim_u(X \cap H) \geq \dim_u X - 1.$$

□

**Definizione 10.7.6.** Sia  $X$  una varietà quasiproiettiva. Diremo che un punto  $u \in X$  è **singolare** se  $\dim_{\mathbb{K}} T_u X > \dim_u X$ , altrimenti si dice **liscio**.

Osserviamo che se  $X, Y$  sono varietà quasiproiettive, allora un punto  $(x, y) \in X \times Y$  è liscio se e solo se  $x$  e  $y$  sono punti lisci di  $X$  e  $Y$  rispettivamente.

*Esempio 10.7.7.* Si consideri una ipersuperficie  $X \subset \mathbb{A}^n$  con ideale  $I(X) = (F)$ . Sappiamo che  $X$  ha dimensione pura  $n - 1$  e quindi un punto  $x \in X$  è singolare se e solo se annulla tutte le derivate parziali di  $F$ . Dato che  $\mathbb{K}$  è perfetto,  $F$  è ridotto e non ha fattori in comune con le derivate parziali; per il teorema degli zeri ogni componente irriducibile di  $X$  contiene punti lisci. Similmente si prova che se  $F$  è un polinomio omogeneo senza fattori multipli, un punto della ipersuperficie proiettiva definita da  $F$  è singolare se e solo se tutte le derivate parziali di  $F$  si annullano in  $X$ .

Più avanti dimostreremo che l'insieme dei punti lisci di una varietà è un aperto denso. Per il momento dimostriamo un risultato leggermente più debole.

**Lemma 10.7.8.** Sia  $X$  una varietà quasiproiettiva. Allora l'insieme dei punti lisci contiene un aperto denso.

*Dimostrazione.* Non è restrittivo supporre  $X \subset \mathbb{A}^n$  chiuso irriducibile. Lavoriamo per induzione su  $n$  essendo il risultato banalmente vero se  $n = 0$  e se  $X = \mathbb{A}^n$ . Si assuma quindi  $n > 0$  e  $X$  chiuso proprio; prendiamo un polinomio  $f \in I(X) - \{0\}$  di grado minimo. Essendo  $I(X)$  un ideale primo necessariamente  $f$  è irriducibile e quindi con almeno una derivata parziale, diciamo  $\frac{\partial f}{\partial x_n}$ , non nulla. Si consideri adesso un generico cambio di coordinate del tipo  $x_n = y_n, x_i = y_i + a_i y_n$ , con  $a_i \in \mathbb{K}$ ; si ha

$$\frac{\partial f}{\partial y_n} = \sum_{i=1}^n \frac{\partial f}{\partial x_i} \frac{\partial x_i}{\partial y_n} = \frac{\partial f}{\partial x_n} + \sum_{i=1}^{n-1} a_i \frac{\partial f}{\partial x_i}.$$

Tutto questo mostra che, a meno di un cambio lineare di coordinate, possiamo supporre il polinomio  $f$  monico rispetto a  $x_n$  e  $\frac{\partial f}{\partial x_n} \neq 0$ . Per ragioni di grado  $\frac{\partial f}{\partial x_n} \notin I(X)$  e  $Z = X \cap V\left(\frac{\partial f}{\partial x_n}\right)$  è un chiuso proprio di  $X$ . Sia  $\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}$  la proiezione sulle prime coordinate, per i ben noti risultati sulle proiezioni normalizzate si ha che  $Y = \pi(X)$  è chiuso irriducibile di dimensione uguale a dimensione di  $X$  e  $\pi(Z)$  è un chiuso proprio di  $Y$ . Per l'ipotesi induttiva esiste  $y \in Y - \pi(Z)$  punto liscio, proviamo che se  $x \in X$ ,  $\pi(x) = y$  allora la proiezione  $\pi: T_x X \rightarrow T_y Y$  è iniettiva e quindi  $\dim T_x X \leq \dim T_y Y = \dim Y = \dim X$  che implica la lisciezza di  $x$ . Un vettore  $(v_1, \dots, v_n)$  appartiene al nucleo di  $\pi$  se e solo se  $v_1 = \dots = v_{n-1} = 0$  e, dato che  $\frac{\partial f}{\partial x_n}(x) \neq 0$ , un tale vettore può essere tangente a  $X$  solo se  $v_n = 0$ .  $\square$

**Definizione 10.7.9.** Sia  $X \subset \mathbb{P}^n$  una varietà proiettiva e  $[x] \in X$ . Lo **spazio tangente proiettivo** a  $X$  in  $[x]$  è definito come  $\mathbb{T}_{[x]}X = \mathbb{P}(T_x C(X)) \subset \mathbb{P}^n$ , dove  $C(X) \subset \mathbb{K}^{n+1}$  è il cono affine di  $X$ .

In altri termini

$$\mathbb{T}_{[x]}X = \{[v] \in \mathbb{P}^n \mid f(x + tv) \equiv 0 \pmod{t^2} \text{ per ogni } f \in I(X)\}.$$

Si noti che, se ad esempio  $x = (1, y)$  e  $v = (0, u)$ , con  $y, u \in \mathbb{K}^n$ , allora  $[x + tv] \in \mathbb{T}_{[x]}X$  se e solo se  $v \in T_y Y$ , dove  $Y$  è la varietà affine  $X \cap \{x_0 \neq 0\}$ . Questo semplicemente perché l'ideale di  $Y$  è generato dai polinomi  $f(1, x_1, \dots, x_n)$ , al variare di  $f \in I(X)$ . In particolare  $\dim \mathbb{T}_{[x]}X \geq \dim_{[x]}X$  e vale l'uguaglianza se e solo se  $[x]$  è un punto non singolare.

Sia  $\phi: X \rightarrow Y$  un morfismo regolare di varietà quasiproiettive e  $x \in X$ . Se  $y = \phi(x)$ , allora  $\phi$  induce un omomorfismo di  $\mathbb{K}$ -algebre  $\phi^*: \mathcal{O}_{y,Y} \rightarrow \mathcal{O}_{x,X}$ . L'omomorfismo  $\phi^*$  è locale, cioè, se  $\mathfrak{m}_x \subset \mathcal{O}_{x,X}$  e  $\mathfrak{m}_y \subset \mathcal{O}_{y,Y}$  denotano gli ideali massimali, allora  $\phi^*(\mathfrak{m}_y) \subset \mathfrak{m}_x$  e quindi induce per passaggio al quoziente un'applicazione lineare di  $\mathbb{K}$ -spazi vettoriali

$$\frac{\mathfrak{m}_y}{\mathfrak{m}_y^2} \longrightarrow \frac{\mathfrak{m}_x}{\mathfrak{m}_x^2}. \quad (10.5)$$

**Definizione 10.7.10.** Nelle notazioni precedenti, chiameremo **differenziale di  $\phi$  in  $x$**  l'applicazione lineare

$$d\phi(x): T_x X \rightarrow T_{\phi(x)} Y$$

trasposta dell'applicazione 10.5.

Siano  $X \subset \mathbb{A}^n$  e  $Y \subset \mathbb{A}^m$  due chiusi e  $\phi: X \rightarrow Y$  un'applicazione regolare; descriviamo il differenziale di  $\phi$  in termini degli spazi tangenti immersi. Denotiamo con  $x_1, \dots, x_n$  e  $y_1, \dots, y_m$  le coordinate su  $\mathbb{A}^n$  e  $\mathbb{A}^m$  rispettivamente. Per definizione,  $\phi$  è la restrizione ad



$X$  di un'applicazione regolare  $(F_1, \dots, F_m): \mathbb{A}^n \rightarrow \mathbb{A}^m$ , con i polinomi  $F_i \in \mathbb{K}[x_1, \dots, x_n]$  determinati da  $\phi$  modulo  $I(X)$ . Se  $x \in X$  e  $v = (v_1, \dots, v_n) \in T_x X$ , allora  $d\phi(x)v$  è il vettore di coordinate

$$(d\phi(x)v)_j = \langle dF_j(x), v \rangle = \sum_{i=1}^n v_i \frac{\partial F_j}{\partial x_i}(x).$$

In particolare se  $\phi$  è la restrizione di un'applicazione lineare, allora  $d\phi(x) = \phi$  per ogni  $x \in X$ . Supponiamo infatti per semplicità notazionale che  $x = 0$  e che  $\phi(x) = 0$ . Il vettore  $v$  corrisponde nello spazio tangente astratto al funzionale  $v: \mathfrak{m}/\mathfrak{m}^2 \rightarrow \mathbb{K}$  tale che  $v(x_i) = v_i$  e la coordinata  $(d\phi(x)v)_j$  è per definizione uguale a  $v(\phi^*y_j)$ . Siccome per ogni  $j = 1, \dots, m$  si ha  $\phi^*y_j = F_j$  e

$$F_j - \sum_{i=1}^n x_i \frac{\partial F_j}{\partial x_i}(0) \in (x_1, \dots, x_n)^2,$$

ne deduciamo che

$$(d\phi(x)v)_j = v(F_j) = \sum_{i=1}^n v(x_i) \frac{\partial F_j}{\partial x_i}(0) = \sum_{i=1}^n v_i \frac{\partial F_j}{\partial x_i}(0).$$

### Esercizi

**10.29.** Per ogni  $n, d > 0$  descrivere esplicitamente un polinomio irriducibile  $f \in \mathbb{K}[x_0, \dots, x_n]$  omogeneo di grado  $d$  tale che l'ipersuperficie proiettiva  $V(f) \subset \mathbb{P}^n$  è liscia. (Sugg.: se la caratteristica del campo divide  $d$  consultare l'Esercizio 3.21.)

**10.30.** Sia  $S \subset \mathbb{P}(\text{Hom}(V^\vee, W))$  la varietà di Segre,  $[f] \in S$ . Provare che  $\mathbb{T}_{[f]}S = \mathbb{P}(H_f)$ , dove  $H_f$  è il sottospazio vettoriale delle  $g \in \text{Hom}(V^\vee, W)$  tali che  $g(\text{Ker}(f)) \subset \text{Im}(f)$ . (Sugg.: mostrare prima che, se  $f = v \otimes w$ , allora  $H_f = \{v \otimes x + y \otimes w\}$ ,  $x \in W$ ,  $y \in V$ .)

**10.31 (Definizione intrinseca dello spazio tangente di Zariski).** 1) Sia  $A$  una  $\mathbb{K}$ -algebra locale con ideale massimale  $\mathfrak{m}$  e campo residuo  $\mathbb{K}$  e denotiamo con  $\text{Der}_{\mathbb{K}}(A, \mathbb{K})$  il  $\mathbb{K}$ -spazio vettoriale delle  $\mathbb{K}$ -derivazioni di  $A$  a valori in  $\mathbb{K}$ . Provare che esiste un isomorfismo naturale di spazi vettoriali  $\text{Der}_{\mathbb{K}}(A, \mathbb{K}) \rightarrow \text{Hom}_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2, \mathbb{K})$ .

2) Sia  $X \subset \mathbb{A}^n$  un chiuso affine; ogni punto  $x \in X$  induce un omomorfismo di anelli  $e_x: \mathbb{K}[X] \rightarrow \mathbb{K}$  dato da  $e_x(f) = f(x)$  e quindi una struttura di  $\mathbb{K}[X]$ -modulo su  $\mathbb{K}$ . Provare che il morfismo di localizzazione  $\mathbb{K}[X] \rightarrow \mathcal{O}_{x,X}$  induce un isomorfismo di spazi vettoriali  $\text{Der}_{\mathbb{K}}(\mathcal{O}_{x,X}, \mathbb{K}) \rightarrow \text{Der}_{\mathbb{K}}(\mathbb{K}[X], \mathbb{K})$ .

3) Provare che esiste un isomorfismo naturale  $T_x X \rightarrow \text{Der}_{\mathbb{K}}(\mathbb{K}[X], \mathbb{K})$  e utilizzare questo fatto per una dimostrazione alternativa del Lemma 10.7.2.

## 10.8 Irriducibilità locale delle varietà lisce

In questa sezione dimostreremo il fatto, intuitivamente ovvio ma per nulla banale, che i punti lisci di una varietà quasiproiettiva appartengono ad una sola componente irriducibile. Per motivi che riguarderanno future applicazioni, dedurremo questo fatto da un risultato più generale di natura algebrica.

Consideriamo un ideale  $I \subset \mathbb{K}[x_1, \dots, x_n]$  con luogo di zeri  $X = V(I)$  tale che  $0 \in X$ . Denotiamo con  $J = \oplus J_i \subset \mathbb{K}[x_1, \dots, x_n]$  l'ideale omogeneo generato dalle parti iniziali degli elementi di  $I$  (cfr. Esempio 9.6.12). Abbiamo visto che la dimensione di  $V(J)$  è uguale alla dimensione di  $X$  nel punto 0. Consideriamo gli anelli

$$A = \frac{\mathbb{K}[x_1, \dots, x_n]_0}{(I)}, \quad B = \frac{\mathbb{K}[x_1, \dots, x_n]}{J}$$

dove  $\mathbb{K}[x_1, \dots, x_n]_0 = \mathcal{O}_{0, \mathbb{A}^n}$  è il localizzato di  $\mathbb{K}[x_1, \dots, x_n]$  per la parte moltiplicativa  $S = \{g \mid g(0) \neq 0\}$  e  $(I)$  è l'ideale generato da  $I$ . L'anello  $A$  è un anello locale con ideale massimale  $\mathfrak{m} = \{f/g \mid f(0) = 0\}$  e, se  $I = \sqrt{I} = I(X)$ , allora  $A = \mathcal{O}_{0, X}$  (Definizione 10.2.7). Denotiamo con  $I_0$  il nucleo del morfismo naturale di anelli  $\mathbb{K}[x_1, \dots, x_n] \rightarrow A$ . Dalla definizione di localizzazione segue che  $I_0$  è l'ideale formato dai polinomi  $f$  tali che esiste  $g \in \mathbb{K}[x_1, \dots, x_n]$  con  $g(0) \neq 0$  e  $gf \in I$ . Notiamo che se  $g(0) = 1$  allora  $gf$  ed  $f$  hanno la stessa parte iniziale.

**Lemma 10.8.1.** *Nelle notazioni precedenti  $V(I_0)$  è l'unione delle componenti irriducibili di  $X$  che contengono il punto 0.*

*Dimostrazione.* Se  $fg \in I$ ,  $g(0) \neq 0$  e  $Z$  è una componente irriducibile di  $X$  che contiene 0, allora  $f \in I(Z)$ . Viceversa se  $X = X_0 \cup Y$ , dove  $X_0$  (risp.:  $Y$ ) è l'unione delle componenti irriducibili che (risp.: che non) contengono 0, allora per ogni  $q \in Y - X_0$  possiamo trovare  $f \in I(X_0)$  e  $g \in I(Y)$  tali che  $f(q) \neq 0$  e  $g(0) \neq 0$ . Per il teorema degli zeri si ha  $f^k g^k \in I$  per  $k \gg 0$  e quindi  $f^k \in I_0$ ,  $f^k(q) \neq 0$ .  $\square$

**Teorema 10.8.2.** *Nelle notazioni precedenti, se esistono  $f_1, \dots, f_h \in I$  tali che la matrice  $\left(\frac{\partial f_i}{\partial x_j}(0)\right)$  ha rango  $\geq n - \dim_0 X$ , allora  $B$  è isomorfo ad un anello di polinomi, l'anello  $A$  è un dominio di integrità e  $I_0$  è un ideale primo.*

*Dimostrazione.* Non è restrittivo supporre  $h = n - \dim_0 X$  e, a meno di un cambio lineare di coordinate che la parte iniziale di  $f_i$  sia uguale a  $x_i$ , per  $i = 1, \dots, h$ . Se  $H \subset J$  è l'ideale generato da  $x_1, \dots, x_h$ , allora si ha  $V(J) \subset V(H) = \mathbb{A}^{n-h}$ . Inoltre, siccome  $H$  è un ideale primo e  $\dim V(J) = \dim_0 X = n - h$  deve essere  $V(J) = V(H)$ ,  $H \subset J \subset \sqrt{H} = H$ . Dato che  $\mathfrak{m}$  è generato da  $x_1, \dots, x_n$ , se  $a \in \mathfrak{m}^h$ , allora esiste un polinomio omogeneo  $f$  di grado  $h$  tale che  $a - f(x_1, \dots, x_n) \in \mathfrak{m}^{h+1}$ : infatti  $a$  è una combinazione lineare  $\sum b_I x^I$  a coefficienti in  $A$  di monomi in  $x_1, \dots, x_n$  e basta prendere  $f$  come  $\sum \bar{b}_I x^I$  dove  $\bar{b} \in \mathbb{K}$  denota la proiezione sul campo residuo di  $b \in A$ . Notiamo inoltre che, se  $f$  è un polinomio omogeneo di grado  $h$  in  $x_1, \dots, x_n$ , allora vale  $f \in \mathfrak{m}^{h+1}$  se e solo se  $f$  è la parte iniziale di un elemento di  $I$ .

Supponiamo per assurdo che  $A$  non sia un dominio di integrità, e siano  $a, b \in A - \{0\}$  tali che  $ab = 0$ . Per il lemma di Artin-Rees vale  $\bigcap_n \mathfrak{m}^n = 0$  e quindi esistono due interi positivi  $h, k$  tali che  $a \in \mathfrak{m}^h - \mathfrak{m}^{h+1}$ ,  $b \in \mathfrak{m}^k - \mathfrak{m}^{k+1}$ . Siano  $f, g \in \mathbb{K}[x_1, \dots, x_n]$  polinomi omogenei di gradi  $h, k$  tali che  $a - f \in \mathfrak{m}^{h+1}$  e  $b - g \in \mathfrak{m}^{k+1}$ . Siccome  $ab = 0$  deve essere  $fg \in \mathfrak{m}^{h+k+1}$ , in contraddizione con l'integrità di  $B$ .  $\square$

**Corollario 10.8.3.** *Ogni punto liscio di una varietà quasiproiettiva appartiene ad una sola componente irriducibile.*

*Dimostrazione.* Non è restrittivo assumere la varietà affine. Basta applicare il Lemma 10.8.1 ed il Teorema 10.8.2.  $\square$

**Teorema 10.8.4.** *L'insieme dei punti lisci di una varietà quasiproiettiva è un aperto denso.*

*Dimostrazione.* Denotiamo con  $X$  la varietà quasiproiettiva e con  $U \subset X$  il luogo nonsingolare. Se  $X$  è irriducibile allora  $\dim_x X$  non dipende da  $x$  e quindi, dalla semicontinuità di  $\dim T_x X$  segue che  $U$  è un aperto. Se  $X = X_1 \cup \dots \cup X_s$  è la decomposizione in componenti irriducibili allora  $p \in U \cap X_i$  se e solo se  $p$  è un punto liscio per  $X_i$  e  $p \notin X_j$  per ogni  $j \neq i$ .  $\square$

**Corollario 10.8.5.** *Sia  $x$  un punto liscio di una varietà irriducibile  $X$  di dimensione 1. Allora l'anello locale  $\mathcal{O}_{x,X}$  è un dominio di integrità con ideale massimale principale.*

*Dimostrazione.* Per il Teorema 10.8.1 l'anello  $\mathcal{O}_{x,X}$  è un dominio di integrità ed esiste  $t \in \mathfrak{m}_x$  tale che  $(t) + \mathfrak{m}_x^2 = \mathfrak{m}_x$ . Per il lemma di Nakayama l'ideale massimale  $\mathfrak{m} \subset \mathcal{O}_{x,X}$  è generato da  $t$ .  $\square$

## 10.9 Esercizi complementari

### Esercizi su varietà affini e quasiproiettive

**10.32.** Sia  $M$  una varietà differenziabile compatta. Denotiamo con  $\mathcal{C}$  la famiglia dei chiusi di  $M$  e con  $\mathcal{I}$  la famiglia degli ideali di  $C^\infty(M, \mathbb{C})$ . Descrivere le applicazioni  $V: \mathcal{I} \rightarrow \mathcal{C}$  e  $I: \mathcal{C} \rightarrow \mathcal{I}$  analoghe al caso delle varietà affini e dimostrare la forma debole del teorema degli zeri, cioè che se  $J \neq (1)$  allora  $V(J) \neq \emptyset$ . Se  $J \in \mathcal{I}$  si definisce  $J'$  come l'ideale generato da tutte le funzioni  $h \circ f$ ,  $f \in J$ ,  $h \in C^\infty(\mathbb{C}, \mathbb{C})$ ,  $h(0) = 0$ . Provare che  $\sqrt{J'} \subset I(V(J))$  ma che in generale non vale l'inclusione opposta.

**10.33.** Sia  $A$  un anello,  $S \subset A$  una parte moltiplicativa e  $l: A \rightarrow S^{-1}A$  l'omomorfismo naturale. Dimostrare che  $T = 1 + \text{Ker}(l)$  è una parte moltiplicativa ed esiste un omomorfismo di anelli  $T^{-1}A \rightarrow S^{-1}A$ .

**10.34.** Sia  $E \subset A$  un insieme finito e  $S \subset A$  la più piccola parte moltiplicativa contenente  $E$ . Mostrare che  $S^{-1}A$  è finitamente generata come  $A$ -algebra.

**10.35.** Sia  $R \rightarrow B$  un morfismo di anelli e  $\{I_n \mid n \in \mathbb{Z}\}$  una successione di ideali di  $B$  tali che  $I_a I_b \subset I_{a+b}$  per ogni  $a, b \in \mathbb{Z}$  e  $I_n = B$  per ogni  $n \leq 0$ . Provare che  $A = \bigoplus_{n \in \mathbb{Z}} I_{-n} t^n$  è una  $R[t]$ -algebra e descrivere gli anelli  $A/(t)$  e  $A_t$ . Nel caso particolare di  $X \subset \mathbb{A}^n$  chiuso,  $x_1, \dots, x_n$  coordinate affini su  $\mathbb{A}^n$ ,  $R = \mathbb{K}$ ,  $B = \mathbb{K}[X]$  e  $I_a = (x_1^a)$  per ogni  $a \geq 0$ , dare una interpretazione geometrica di  $A$ ,  $A/(t)$  e  $A_t$ .

**10.36.** Sia  $A$  un dominio di integrità con campo delle frazioni globali  $F$ . Per ogni ideale massimale  $\mathfrak{m} \subset A$ , interpretare il localizzato  $A_{\mathfrak{m}}$  come un opportuno sottoanello di  $F$  e provare che  $\bigcap A_{\mathfrak{m}} = A$ , dove l'intersezione è presa su tutti gli ideali massimali.

**10.37.** Sia  $Z \subset \mathbb{A}^n$  una ipersuperficie irriducibile con ideale  $I(Z) = (f)$ . Dimostrare che l'anello  $\mathcal{O}_{Z,X}$  è locale e che il suo ideale massimale è principale e generato da  $f$ .

**10.38.** Sia  $X$  varietà quasiproiettiva e  $Z \subset X$  un chiuso irriducibile. Dimostrare che  $\mathcal{O}_{Z,X}/\mathfrak{m}_{Z,X} = \mathbb{K}(Z)$ .

**10.39 (\*\*).** Sia  $X$  una varietà quasiproiettiva ed  $A = \mathcal{O}_X(X)$ . Diremo che  $X$  soddisfa il teorema degli zeri se per ogni ideale  $J \subset A$  si ha che  $I(V(J)) = \sqrt{J}$ , dove lasciamo per esercizio al lettore di definire, in analogia al caso dei chiusi affini, gli operatori  $I$  e  $V$ . Provare che una varietà quasiffine  $X$  è affine se e solo se soddisfa il teorema degli zeri e la  $\mathbb{K}$ -algebra  $\mathcal{O}_X(X)$  è finitamente generata. (Sugg.: vedi Esercizio II.2.17 in [Hart1977].)

**10.40.** Sia  $F \in \mathbb{K}[x_0, \dots, x_n]$  omogeneo di grado  $d > 0$  e  $U = \mathbb{P}^n - V(F)$ . Provare che ogni funzione regolare su  $U$  si può scrivere nella forma  $GF^{-a}$ , con  $a \geq 0$  e  $G \in \mathbb{K}[x_0, \dots, x_n]$  omogeneo di grado  $ad$ .

**10.41 (\*).**  $\mathbb{K} = \mathbb{C}$ . Provare che ogni varietà quasiproiettiva irriducibile complessa dotata della topologia classica è uno spazio topologico connesso per archi, cfr. [Mum1976, 4.16]. (Sugg.: basta dimostrare che esiste un sottoinsieme aperto di Zariski che è connesso per archi.)

**10.42 (\*)**. (caratteristica  $\neq 2$ ) Si consideri l'anello  $A = \mathbb{K}[x, y, z]/(y^2 - p(x), z^2 - q(x))$  con  $p, q \in \mathbb{K}[x]$  tali che il prodotto  $pq$  sia un polinomio di grado dispari senza radici multiple. Provare che  $A$  non è generato ciclicamente su  $\mathbb{K}[x]$ , cioè che non esiste alcun  $f \in A$  tale che  $A = \mathbb{K}[x, f]$ . (Sugg.: sia per assurdo  $f = ay + bz + cyz$ ,  $a, b, c \in \mathbb{K}[x]$ , come sopra e sia  $\alpha$  una radice di  $a^2p - b^2q$ . Provare che la mappa naturale  $\mathbb{K}[x, f] \rightarrow B = \mathbb{K}[y, z]/(y^2 - p(\alpha), z^2 - q(\alpha))$ ,  $x \rightarrow \alpha$ , non è surgettiva. Può essere utile capire quale è la varietà affine  $X$  tale che  $\mathbb{K}[X] = B$  e interpretare  $f$  come una funzione regolare su  $X$ .)

**10.43**. Sia  $X = \left\{ [x] \in \mathbb{P}^5 \mid \text{rank} \begin{pmatrix} x_0 & x_1 & x_2 \\ x_3 & x_4 & x_5 \end{pmatrix} = 2 \right\}$ . Dimostrare:

1.  $X$  è una varietà quasiproiettiva irriducibile. Qual è la sua dimensione?
2.  $X$  contiene almeno una retta proiettiva  $L \subset \mathbb{P}^5$ .
3.  $X$  non è una varietà affine.

**10.44**. Siano  $x_0, \dots, x_4$  coordinate su  $\mathbb{A}^5$  e  $Y \subset \mathbb{A}^5$  l'immagine del morfismo regolare

$$v: \mathbb{A}^2 \rightarrow \mathbb{A}^5, \quad v(t_0, t_1) = (t_0^4, t_0^3 t_1, t_0^2 t_1^2, t_0 t_1^3, t_1^4).$$

Denotiamo con  $X \subset \mathbb{A}^5$  il chiuso definito dalle equazioni  $x_2 = 0$ ,  $x_0 x_4 = x_1 x_3$ ,  $x_0^2 x_3 = x_1^3$ ,  $x_1 x_4^2 = x_3^3$ ,  $x_1^2 x_4 = x_3^2 x_0$  e con  $f: Y \rightarrow X$  la proiezione  $x_2 \mapsto 0$ . Dimostrare:

1.  $Y$  è chiuso e le restrizioni  $f: Y \cap \{x_i \neq 0\} \rightarrow X \cap \{x_i \neq 0\}$ , per  $i = 0$  e  $i = 4$ , sono isomorfismi di varietà quasiproiettive.
2.  $f$  è bigettiva ma non è un isomorfismo di varietà.
3.  $f: Y - \{0\} \rightarrow X - \{0\}$  è un isomorfismo di varietà.

**10.45 (\*)**. Dimostrare che un aperto  $U \subset \mathbb{P}^n$  è una varietà affine se e solo se  $\mathbb{P}^n - U$  è una ipersuperficie.

**10.46**. Sia  $A$  un dominio a fattorizzazione unica ed  $S \subset A$  una parte moltiplicativa. Dimostrare che  $S^{-1}A$  è a fattorizzazione unica.

**10.47**. Sia  $n > 1$  ed  $U \subset \mathbb{P}^n$  il complementare di una ipersuperficie irriducibile di grado  $> 1$ . Provare che  $\mathcal{O}_{\mathbb{P}^n}(U)$  non è un dominio a fattorizzazione unica.

### Esercizi su prodotti e morfismi proiettivi

**10.48**. Sia  $S$  l'immagine della mappa di Segre  $s: \mathbb{P}^n \times \mathbb{P}^m \rightarrow S \subset \mathbb{P}^N$  e  $L \subset S$  una retta. Provare che  $s^{-1}(L)$  è contenuta in una fibra di una delle due proiezioni  $\mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^n$ ,  $\mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^m$ . Dedurre che l'insieme delle rette in  $S$  è un sottoinsieme sconnesso di  $G(2, N + 1)$ .

**10.49**. Un morfismo regolare  $f: X \rightarrow Y$  si dice **universalmente chiuso** se per ogni morfismo regolare  $g: Z \rightarrow Y$ , il morfismo di proiezione  $X \times_Y Z \rightarrow Z$  è chiuso. Dimostrare che ogni morfismo universalmente chiuso è chiuso, ma che il viceversa è falso in generale.

**10.50 (\*)**. Sia  $X \subset \mathbb{P}^n$  localmente chiuso. Dimostrare che un morfismo regolare  $X \rightarrow Y$  è proiettivo se e solo se il suo grafico è chiuso in  $Y \times \mathbb{P}^n$ . (Sugg.: provare che se  $f: X \rightarrow Y$  è proiettivo, allora anche  $(i, f): X \rightarrow \mathbb{P}^n \times Y$  è proiettivo.)

**10.51 (\*)**. Sia  $f: X \rightarrow Y$  un morfismo di varietà quasiproiettive. Provare che  $f$  è proiettivo se e solo se è universalmente chiuso. (Sugg.: sia  $\bar{X}$  la chiusura proiettiva di  $X$  e  $\bar{G} \subset \bar{X} \times Y$  la chiusura del grafo. Provare che  $\{((x, f(x)), x) \in \bar{G} \times_Y X \mid x \in X\}$  è un chiuso.)

**10.52.** Mostrare con un esempio che i punti 3) e 4) del Teorema 10.6.6 sono in generale falsi se il morfismo  $f$  non è proiettivo.

**10.53 (Superfici di Segre-Hirzebruch).** In tutto l'esercizio  $k \geq 0$  è un intero fissato.

a) Sia  $v_{k+1}: \mathbb{P}_x^1 \rightarrow \mathbb{P}_y^{k+1}$  la  $k+1$ -esima immersione di Veronese, definita da  $y_i = x_0^{k+1-i} x_1^i$ , con  $i = 0, \dots, k+1$ . Denotiamo con  $C_{k+1} \subset \mathbb{P}^{k+1}$  l'immagine di  $v_{k+1}$ . Provare direttamente che  $C_{k+1}$  è chiuso e trovare un insieme finito di equazioni che lo definiscono. (Sugg.: descrivere  $C_{k+1}$  come il luogo dove si abbassa il rango di una opportuna matrice a coefficienti forme lineari nelle coordinate  $y_i$ .)

b) Siano  $x_0, x_1, y_0, \dots, y_{k+1}$  coordinate omogenee su  $\mathbb{P}^{k+3}$  e consideriamo i sottospazi proiettivi  $\mathbb{P}^1 = \{y_0 = \dots = y_{k+1} = 0\}$  e  $\mathbb{P}^{k+1} = \{x_0 = x_1 = 0\}$ . Definiamo  $S_k \subset \mathbb{P}^{k+3}$  come l'unione, al variare di  $p \in \mathbb{P}^1$ , delle rette congiungenti  $p$  e  $v_{k+1}(p) \in C_{k+1} \subset \mathbb{P}^{k+1}$ . Provare che  $S_k$  è chiuso e determinare un insieme finito di equazioni che lo definiscono.

c) Definiamo astrattamente un spazio topologico quoziente

$$\mathbb{F}_k = (\mathbb{A}^2 - \{0\}) \times (\mathbb{A}^2 - \{0\}) / \sim$$

dove la relazione di equivalenza è indotta dall'azione del gruppo moltiplicativo  $(\mathbb{K} - \{0\})^2$  ed è definita da

$$(l_0, l_1, t_0, t_1) \sim (\lambda l_0, \lambda l_1, \mu t_0, \mu \lambda^k t_1), \quad \lambda, \mu \in \mathbb{K} - \{0\}.$$

Determinare un morfismo regolare  $(\mathbb{A}^2 - \{0\}) \times (\mathbb{A}^2 - \{0\}) \rightarrow \mathbb{P}^{k+3}$  che induce, per passaggio al quoziente, una bigezione  $s: \mathbb{F}_k \rightarrow S_k$  tale che, nella struttura di varietà proiettiva indotta su  $\mathbb{F}_k$ , gli aperti  $U_{ij} = \{l_i t_j \neq 0\}$  siano isomorfi a  $\mathbb{A}^2$ .

d) (\*\*). Dimostrare che se  $a > b \geq 0$ , allora  $S_a$  non è isomorfo a  $S_b$ . (Sugg.: studiare i gruppi degli automorfismi regolari delle varietà  $S_k$ .)

**10.54 (\*\*?).** Sia  $f: X \rightarrow Y$  un morfismo regolare aperto di varietà affini, provare che il morfismo  $f \times id: X \times \mathbb{A}^1 \rightarrow Y \times \mathbb{A}^1$  è ancora aperto.

**10.55.** Siano  $n > m$  due interi positivi. Dimostrare che non esistono chiusi di  $\mathbb{P}^m \times \mathbb{P}^m$  omeomorfi a  $\mathbb{P}^n$ .

**10.56.** Sia  $S_n \subset \mathbb{K}[x_0, x_1]$  lo spazio vettoriale dei polinomi omogenei di grado  $n$ . Per ogni  $d$ -upla non decrescente di numeri naturali  $\lambda = \{\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_d\}$  tali che  $\sum \lambda_i = n$ , denotiamo

$$X_\lambda = \mathbb{P} \left( \left( \prod_{i=1}^d (a_i x_0 + b_i x_1)^{\lambda_i} \mid [a_i, b_i] \in \mathbb{P}^1 \right) \right) \subset \mathbb{P}(S_n).$$

Provare che  $X_\lambda$  è una varietà proiettiva irriducibile di dimensione  $d$ .

**10.57 (\*).** Sia  $n \geq 3$  e  $X \subset \mathbb{P}^n$  una ipersuperficie irriducibile di grado  $d > 1$  e sia  $U$  l'insieme degli iperpiani  $H \subset \mathbb{P}^n$  tali che  $X \cap H$  è irriducibile di grado  $d$ . Dimostrare che  $U$  è un aperto non vuoto dello spazio proiettivo duale. (Sugg.: siano  $x_0, \dots, x_n$  coordinate omogenee e  $f(x_0, \dots, x_n)$  un polinomio irriducibile omogeneo di grado  $d$  tale che  $V(f) = X$ . Per ogni intero  $a$  denotiamo con  $S_a \subset \mathbb{K}[x_1, \dots, x_n]$  lo spazio vettoriale dei polinomi omogenei di grado  $a$  e, se  $0 < a < d$ , con  $R_a \subset \mathbb{P}(S_d)$  l'immagine del morfismo

$$\mathbb{P}(S_a) \times \mathbb{P}(S_{d-a}) \rightarrow \mathbb{P}(S_d), \quad ([h], [g]) \mapsto [hg].$$

Per mostrare che  $U$  è aperto basta mostrare che  $U \cap V$  è aperto per ogni aperto affine  $V \simeq \mathbb{A}^n$  di  $(\mathbb{P}^n)^\vee$ . Ad esempio, se  $V$  è lo spazio affine degli iperpiani di equazione  $x_0 = v_1 x_1 + \dots + v_n x_n$ ,  $v_1, \dots, v_n \in \mathbb{K}$ , ne segue che  $V - U = \cup_{1 < a < d} \phi^{-1}(R_a)$ , dove  $\phi: V \rightarrow \mathbb{P}(S_d)$  è definita da  $\phi(v_1, \dots, v_n) = [f(\sum v_i x_i, x_1, \dots, x_n)]$ . Mostrare che  $U \neq \emptyset$  è più

difficile. A meno di un cambio di coordinate omogenee non è restrittivo supporre che la retta  $L = \{x_0 = x_1 = \dots = x_{n-2} = 0\}$  intersechi  $X$  in  $d$  punti distinti, cioè che la forma binaria  $f(0, \dots, 0, x_{n-1}, x_n)$  non abbia fattori multipli. Sia  $D = \mathbb{K}^2 - \{0\}$ . Consideriamo il fascio di iperpiani  $H_{[a,b]} = \{ax_0 = bx_1\}$ ,  $(a, b) \in D$ . Notare che  $L$  è contenuta in ogni iperpiano del fascio. Considerare la mappa

$$\phi: D \rightarrow \mathbb{P}(S_d), \quad \phi((a, b)) = [f(bx_1, ax_1, x_2, \dots, x_n)].$$

Se, per assurdo, fosse  $\phi(D) \subset R_a$  per qualche  $0 < a < d$ , considerando il sottoinsieme  $T \subset D \times \mathbb{P}(S_a) \times \mathbb{P}(S_{d-a})$  formato dalle terne  $((a, b), [f_1], [f_2])$  tali che  $\phi((a, b)) = [f_1 f_2]$ , la proiezione  $T \rightarrow \mathbb{P}^1$  sul primo fattore sarebbe surgettiva. Per ogni sottoinsieme  $A \subset L \cap X$  di cardinalità  $a$  sia

$$T_A = \{((a, b), [f_1], [f_2]) \in T \mid A \subset V(f_1)\}.$$

Chiaramente  $T_A$  è chiuso in  $T$  e  $T$  è l'unione di tutti i  $T_A$  al variare di  $A$ . Esiste dunque un sottoinsieme  $A_0 \subset L \cap X$  di cardinalità  $a$  tale che la proiezione  $T_{A_0} \rightarrow D$  è surgettiva. Per  $i = 1, 2$  si considerino i sottoinsiemi  $T_i \subset D \times \mathbb{P}(S_a) \times \mathbb{P}(S_{d-a}) \times \mathbb{P}^n$  formati dalle quadruple  $((a, b), [f_1], [f_2], [x])$  tali che

$$((a, b), [f_1], [f_2]) \in T_{A_0}, \quad ax_0 = bx_1 \quad \text{e} \quad f_i(bx_1, ax_1, x_2, \dots, x_n) = 0.$$

Siano  $W_i \subset D \times \mathbb{P}^n$  le proiezioni dei  $T_i$ ; mostrare che se  $((a, b), [x]) \in W_i$  allora anche  $((ta, tb), [x]) \in W_i$  per ogni  $t \in \mathbb{K} - \{0\}$  e dedurre che, detta  $\pi: D \times \mathbb{P}(S_a) \times \mathbb{P}(S_{d-a}) \times \mathbb{P}^n \rightarrow \mathbb{P}^n$  la proiezione sul quarto fattore, le immagini  $\pi(T_i)$  sono chiuse,  $X = \pi(T_1) \cup \pi(T_2)$  e che,  $A_0 \subset \pi(T_1) - \pi(T_2)$ ,  $L \cap X - A_0 \subset \pi(T_2) - \pi(T_1)$ .

**10.58.** Sia  $X \subset \mathbb{A}^1 \times \mathbb{P}^1$  l'ipersuperficie di equazione  $u_0^2 = xu_1^2$ . Mostrare che per ogni applicazione regolare  $s: \mathbb{A}^1 \rightarrow \mathbb{P}^1$  esiste almeno un  $x \in \mathbb{A}^1$  tale che  $(x, s(x)) \in X$ .

### Esercizi sullo spazio tangente

**10.59.** Dato un anello locale Noetheriano  $A$  con ideale massimale  $\mathfrak{m}$  si definisce l'anello graduato associato

$$G(A) = \bigoplus_{n \geq 0} \frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}.$$

Provare che se  $G(A)$  è un dominio di integrità allora anche  $A$  è un dominio di integrità. Il viceversa è invece falso in generale. (Sugg.: vedi la dimostrazione di 10.8.2; per il viceversa suggeriamo  $A = \mathbb{K}[x, y]/(y^2 - x^2 - x^3)$  come controesempio.)

**10.60.** Se  $x$  è un punto liscio di una varietà  $X$ , provare che il completamento  $\mathfrak{m}$ -adico (cfr. [AM1969]) di  $\mathcal{O}_{x, X}$  è un'algebra di serie di potenze formali.

**10.61.** Siano  $X \subset \mathbb{P}^n$  una varietà proiettiva irriducibile di dimensione  $m$ ,  $H \subset \mathbb{P}^n$  un sottospazio proiettivo di dimensione  $n - m$  e  $p \in X \cap H$ . Provare che se  $p$  è l'unico punto di intersezione di  $X$  e  $H$  e se  $\mathbb{T}_p X \cap \mathbb{T}_p H$  ha dimensione 0, allora  $X$  è un sottospazio proiettivo. (Sugg.: sia  $Y \subset \mathbb{P}^{n-1}$  la chiusura dell'immagine della proiezione di centro  $p$ ,  $\pi: X - \{p\} \rightarrow \mathbb{P}^{n-1}$ . Provare che  $Y \cap \pi(H) = \emptyset$  e quindi che  $\dim Y < \dim X$ .)

**10.62.** Un **Gruppo Algebrico** è un gruppo  $G$  che possiede una struttura di varietà quasiproiettiva tale che l'applicazione

$$G \times G \rightarrow G, \quad (a, b) \mapsto ab^{-1},$$

è un morfismo regolare di varietà. Provare:

1.  $G$  non possiede punti singolari (Sugg.: il gruppo degli automorfismi regolari di  $G$  agisce transitivamente).
2. Ogni curva piana liscia di grado 3, con la struttura di gruppo definita nella Sezione 6.4, è un gruppo algebrico.
3. Se  $H \subset G$  è un sottogruppo allora anche la sua chiusura  $\overline{H}$  è un sottogruppo.
4. Se  $G$  è proiettivo irriducibile allora  $G$  è un gruppo abeliano. (Sugg.: esistono almeno due dimostrazioni alternative: nella prima provare che per ogni aperto affine  $1 \in V \subset G$  esiste un aperto  $U \subset G$  tale che  $aba^{-1} \in V$  per ogni  $a \in G, b \in U$ . Nella seconda applicare il Lemma di Rigidità, Esercizio 10.28, ai morfismi  $f, g: G \times G \rightarrow G$ ,  $f(a, b) = b, g(a, b) = aba^{-1}$ .)

*Osservazione 10.9.1.* Un gruppo algebrico proiettivo irriducibile si dice una **Varietà Abeliiana**. Sul campo dei numeri complessi ogni varietà abeliana è biolomorfa ad un toro complesso, ossia ad un quoziente  $\mathbb{C}^n/\Lambda$  per un opportuno reticolo  $\Lambda \simeq \mathbb{Z}^{2n}$ . Se  $n \geq 2$  non tutti i tori complessi sono varietà abeliane.

**10.63.** (caratteristica  $\neq 2$ ) Sia  $\mathbb{P}^5$  lo spazio delle coniche di  $\mathbb{P}^2$ ,  $\Delta \subset \mathbb{P}^5$  l'ipersuperficie cubica delle coniche singolari e  $V \subset \Delta$  la varietà (di Veronese) delle rette doppie. Provare che i punti di  $V$  sono tutti e soli i punti singolari di  $\Delta$ . (Sugg.: siccome  $\text{Aut}(\mathbb{P}^2)$  agisce transitivamente su  $V$  basta dimostrare che  $\emptyset \neq \text{Sing}(\Delta) \subset V$ .)

**10.64.** (caratteristica 0) Sia  $\mathbb{P}^n$  il proiettivizzato dello spazio delle forme binarie di grado  $n$ ,  $\Delta$  il discriminante e  $X = V(\Delta) \subset \mathbb{P}^n$  l'ipersuperficie delle forme aventi una radice multipla. Provare che  $X$  è irriducibile di grado  $2(n-1)$  e che i punti lisci di  $X$  corrispondono alle forme con una sola radice doppia.

**10.65.** (caratteristica 0) Sia  $X \subset \mathbb{P}(M(n, n))$  il luogo delle matrici che non hanno autovalori distinti. Provare che  $X$  è una ipersuperficie irriducibile di grado  $n(n-1)$ . (Sugg.: Sia  $B$  una matrice  $(n-2) \times (n-2)$  invertibile ad autovalori distinti,

$$C_s = \begin{pmatrix} 0 & s \\ 1 & 0 \end{pmatrix}, \quad A_s = \begin{pmatrix} C_s & 0 \\ 0 & B \end{pmatrix}, \quad s \in \mathbb{K}.$$

Il polinomio  $f(s) = \Delta(\det(tI - A_s))$  ha una radice semplice in 0.)





## Varietà algebriche: argomenti scelti

### 11.1 Le Grassmanniane

Sia  $V$  uno spazio vettoriale di dimensione  $n$  sul campo  $\mathbb{K}$  e sia  $0 \leq s \leq n$  un intero.

**Definizione 11.1.1.** *L'insieme  $G(s, V)$  dei sottospazi  $s$ -dimensionali di  $V$  viene detto **Grassmanniana**.*

Notiamo che  $G(1, V) = \mathbb{P}(V)$  e  $G(n-1, V) = \mathbb{P}(V^\vee)$ . Quindi per  $s = 1, n-1$  la Grassmanniana ha una naturale struttura di varietà proiettiva. Mostriamo in questa sezione che per ogni  $s$ , la Grassmanniana  $G(s, V)$  ha una struttura di varietà proiettiva irriducibile ricoperta da aperti isomorfi a  $\mathbb{A}^{s(n-s)}$  e di conseguenza che è una varietà liscia di dimensione  $s(n-s)$ .

**Definizione 11.1.2.** *Un vettore  $v \in \bigwedge^s V$  si dice **totalmente decomponibile** se esistono  $v_1, \dots, v_s \in V$  tali che  $v = v_1 \wedge v_2 \wedge \dots \wedge v_s$ . Indicheremo con  $\mathbb{G}(s, V) \subset \mathbb{P}(\bigwedge^s V)$  l'insieme delle classi di omotetia dei vettori totalmente decomponibili.*

Esiste una bigezione naturale  $P: G(s, V) \rightarrow \mathbb{G}(s, V)$  chiamata **immersione di Plücker** e definita nel modo seguente. Se  $W \in G(s, V)$ , allora  $P(W) = [w_1 \wedge \dots \wedge w_s]$ , dove  $w_1, \dots, w_s$  è una base di  $W$ . Se  $v_1, \dots, v_s$  è un'altra base di  $W$ , allora  $w_1 \wedge \dots \wedge w_s = \det(A) v_1 \wedge \dots \wedge v_s$ , dove  $A$  è la matrice di cambiamento di base; questo prova che l'applicazione  $P$  è ben definita. Lasciamo per esercizio al lettore la semplice verifica che  $P$  è bigettiva.

Da ora in poi identifichiamo  $G(s, V)$  e  $\mathbb{G}(s, V)$  tramite l'immersione di Plücker  $P$ , preferendo la notazione  $\mathbb{G}(s, V)$  quando risulterà più comodo pensare la Grassmanniana come il proiettivizzato del cono dei vettori totalmente decomponibili.

Sia  $e_1, \dots, e_n$  una base di  $V$ . Allora una base di  $\bigwedge^s V$  è data dai vettori totalmente decomponibili  $e_I = e_{i_1} \wedge \dots \wedge e_{i_s}$ , al variare dei sottoinsiemi ordinati

$$I = \{i_1 < i_2 < \dots < i_s\} \subset \{1, \dots, n\}$$

di cardinalità  $s$ . Ogni vettore di  $\bigwedge^s V$  si scrive in modo unico come  $\sum p_I e_I$ , con  $p_I \in \mathbb{K}$ . Le  $p_I$  sono pertanto un sistema di coordinate omogenee sullo spazio proiettivo  $\mathbb{P}(\bigwedge^s V) = \mathbb{P}^N$ , con  $N = \binom{n}{s} - 1$ , e sono dette **coordinate Plückeriane** su  $G(s, V)$  rispetto alla base  $e_1, \dots, e_n$ . Al fine di semplificare alcune equazioni, se  $I = \{i_1, \dots, i_s\}$  è una qualsiasi successione di  $s$  indici distinti, compresi tra 1 ed  $n$  si pone:

$$p_I = p_{i_1, \dots, i_s} = (-1)^\sigma p_{i_{\sigma(1)}, \dots, i_{\sigma(s)}},$$

dove  $\sigma$  è l'unica permutazione su  $s$  elementi tale che  $i_{\sigma(1)} < i_{\sigma(2)} < \dots < i_{\sigma(s)}$ . Se invece la  $s$ -upla  $I$  contiene elementi ripetuti, allora si pone  $p_I = 0$ .

Per ogni sottospazio  $H \subset V$  dimensione  $n - s$  denotiamo con

$$H^c = \{W \in G(s, V) \mid W \cap H = 0\}.$$

Vogliamo adesso dimostrare che  $H^c$  è un aperto di Zariski in  $G(s, V)$  e che è una varietà affine isomorfa a  $\mathbb{A}^{s(n-s)}$ ; l'isomorfismo tra  $H^c$  e  $\mathbb{A}^{s(n-s)}$  non è canonico ma dipende dalla scelta di una proiezione  $\pi: V \rightarrow H$ ,  $\pi^2 = \pi$ . Per semplificare i conti consideriamo le coordinate Plückeriane rispetto ad una base  $e_1, \dots, e_n$  di  $V$  scelta in modo tale che  $H$  sia generato da  $e_{s+1}, \dots, e_n$  e  $\text{Ker } \pi$  sia generato da  $e_1, \dots, e_s$ .

Se  $I_0 = \{1, 2, \dots, s\}$ , allora  $H^c = \{[p_I] \in \mathbb{G}(s, V) \mid p_{I_0} \neq 0\}$ : infatti se  $W \cap H = 0$  allora l'applicazione  $I - \pi: W \rightarrow \text{Ker } \pi$  è bigettiva ed esistono unici  $v_1, \dots, v_s \in H$  tali che  $W$  è generato da  $e_1 + v_1, \dots, e_s + v_s$ ; quindi  $p_{I_0}(W) \neq 0$  in quanto  $P(W)$  è la classe di omotetia di

$$(e_1 + v_1) \wedge \dots \wedge (e_s + v_s) = e_{I_0} + \sum_{I \neq I_0} \alpha_I e_I.$$

Viceversa se  $W \cap H \neq 0$  possiamo prendere una base  $w_1, \dots, w_s$  di  $W$  tale che  $w_1 \in H$  e quindi  $p_{I_0}(W) = 0$ . Dunque  $H^c$  è il complementare in  $\mathbb{G}(s, V)$  della sezione iperpiana  $p_{I_0} = 0$  ed è quindi aperto in  $\mathbb{G}(s, V)$ .

Mostriamo adesso che  $H^c$  è chiuso nello spazio affine  $\mathbb{A}_{I_0}^N = \{[p_I] \in \mathbb{P}(\wedge^s V) \mid p_{I_0} \neq 0\}$ . Siano  $y_{ij}$ , per  $i = 1, \dots, s$  e  $j = s + 1, \dots, n$ , coordinate affini su  $\mathbb{A}^{s(n-s)}$ . Allora esiste una morfismo regolare bigettivo  $f: \mathbb{A}^{s(n-s)} \rightarrow H^c \subset \mathbb{P}^N$  dato da

$$f(a_{1,s+1}, \dots, a_{s,n}) = \left[ \left( e_1 + \sum_{j=s+1}^n a_{1j} e_j \right) \wedge \dots \wedge \left( e_s + \sum_{j=s+1}^n a_{sj} e_j \right) \right].$$

L'applicazione inversa di  $f$  si scrive nelle coordinate affini  $y_{i,j}$  su  $\mathbb{A}^{s(n-s)}$  e nelle coordinate affini  $x_I = p_I p_{I_0}^{-1}$  su  $\mathbb{A}_{I_0}^N$  mediante la formula

$$y_{ij} = (-1)^{s-i} x_{\{1, \dots, i-1, i+1, \dots, s, j\}}$$

e quindi  $H^c$  è il grafico di una applicazione regolare  $\mathbb{A}^{s(n-s)} \rightarrow \mathbb{A}^{N-s(n-s)}$  che il lettore non troverà difficoltoso scrivere. Questo prova che  $H^c$  è chiuso in  $\mathbb{A}_{I_0}^N$  ed è isomorfo come varietà affine a  $\mathbb{A}^{s(n-s)}$ .

In conclusione si può quindi affermare che  $\mathbb{G}(s, V)$  è chiuso in  $\mathbb{P}^N$ , e dato che  $\mathbb{G}(s, V) = \cup H^c$ , con  $H \in G(n - s, V)$  e  $H^c \cap K^c \neq \emptyset$  per ogni  $H, K$ , ne segue che  $\mathbb{G}(s, V)$  è pure irriducibile. Chiameremo in seguito gli aperti  $H^c \subset G(s, V)$  gli **aperti fondamentali** della Grassmanniana.

È interessante, oltreché utile, poter descrivere in maniera algebrica l'inverso dell'immersione di Plücker. A tal fine definiamo, per ogni  $a \leq s$ , il prodotto detto di **contrazione** o di **convoluzione**  $\wedge^a V^\vee \times \wedge^s V \rightarrow \wedge^{s-a} V$ , dove  $V^\vee$  indica lo spazio vettoriale duale di  $V$ . È comodo definire tale prodotto ricorsivamente in  $a$ . Per  $a = 1$  il prodotto di contrazione è l'estensione bilineare di

$$\phi \lrcorner (v_1 \wedge \dots \wedge v_s) = \sum_{i=1}^s (-1)^{i-1} \langle \phi, v_i \rangle v_1 \wedge \dots \wedge \widehat{v}_i \wedge \dots \wedge v_s,$$

mentre per  $a > 1$  è l'estensione bilineare di

$$(\phi_1 \wedge \dots \wedge \phi_a) \lrcorner w = \phi_1 \lrcorner ((\phi_2 \wedge \dots \wedge \phi_a) \lrcorner w)$$

Notiamo che se  $a = s$ , allora il prodotto  $\lrcorner$  è non degenere e induce un isomorfismo naturale tra  $(\wedge^s V)^\vee = \wedge^s V^\vee$ . Se  $a > s$ , allora poniamo per convenzione  $\lrcorner = 0$ . Per ogni funzionale lineare fissato  $\phi \in V^\vee$ , vale  $\phi \lrcorner w = 0$  se e solo se  $w \in \wedge^s(\text{Ker}(\phi))$ .

**Lemma 11.1.3.** *Sia  $w \in \bigwedge^s V$  un vettore non nullo e sia  $H \subset V$  l'immagine dell'applicazione lineare  $\bigwedge^{s-1} V^\vee \xrightarrow{\lrcorner w} V$ . Allora  $w \in \bigwedge^s H$  e  $\dim H \geq s$ . Inoltre vale  $\dim H = s$  se e solo se  $w$  è totalmente decomponibile ed in tal caso si ha  $H = P^{-1}([w])$ .*

*Dimostrazione.* Sia  $r = \dim H$  e sia  $e_1, \dots, e_n$  una base di  $V$  tale che  $e_1, \dots, e_r \in H$ . Se per assurdo  $w \notin \bigwedge^s H$ , allora esiste un indice  $i > r$  tale che  $w = e_i \wedge z + u$  dove  $z \neq 0$  ed i vettori  $z, u$  appartengono alle potenze esterne dell'iperpiano  $L_i$  generato dagli  $e_j$  con  $j \neq i$ . Prendendo  $\psi \in \bigwedge^{s-1}(e_i^\perp)$  tale che  $\psi \lrcorner z \neq 0$  si trova  $\psi \lrcorner w \notin L_i$  in contraddizione con le ipotesi. Dunque  $r \geq s$  e se vale  $r = s$  allora  $w$  è totalmente decomponibile. Viceversa se  $w = w_1 \wedge \dots \wedge w_s$  allora è immediato osservare che  $H$  è contenuto nel sottospazio generato da  $w_1, \dots, w_s$ .  $\square$

Osserviamo che, fissata una base di  $V$ , l'applicazione lineare  $\lrcorner w$  si rappresenta con una matrice di ordine  $n \times \binom{n}{s-1}$  i cui coefficienti sono coordinate Plückeriane di  $w$  e, per il Lemma 11.1.3, il chiuso  $\mathbb{G}(s, V)$  è il luogo di zeri dei determinanti minori di ordine  $(s+1) \times (s+1)$ .

Vogliamo adesso mostrare che il chiuso  $\mathbb{G}(s, V)$  è intersezione di  $\binom{n}{s+1} \binom{n}{s-1}$  quadriche, le cui equazioni sono dette **relazioni quadratiche di Plücker** (cfr. [Harr1992], [GH1978], [KL1972]). Esistono vari modi di dimostrare ciò; noi seguiremo un approccio che permetterà di estendere facilmente le relazioni quadratiche anche alla cosiddetta Grassmanniana semi-infinita (Esercizio 11.23).

Ricordiamo come è definita la bigezione naturale  $\text{Hom}(V, V) = V \otimes V^\vee$ : fissata una base  $e_1, \dots, e_n$  di  $V$ , essa determina la base duale  $\epsilon_1, \dots, \epsilon_n$  di  $V^\vee$  e, in tale bigezione, un endomorfismo  $\phi \in \text{Hom}(V, V)$  corrisponde al tensore  $\sum_{i=1}^n \phi(e_i) \otimes \epsilon_i \in V \otimes V^\vee$ .

**Lemma 11.1.4.** *Siano  $V, V_1$  e  $V_2$  spazi vettoriali di dimensione finita,  $\alpha: V \rightarrow V_1$  e  $\beta: V^\vee \rightarrow V_2$  due applicazioni lineari. Denotiamo  $H = \text{Ker}(\alpha)$ ,  $L = \text{Ker}(\beta)$  e supponiamo che  $H, L$  siano ortogonali, cioè che  $\langle v, h \rangle = 0$  per ogni  $v \in H$  ed ogni  $h \in L$ . Allora vale  $H = L^\perp$  se e solo se  $\alpha \otimes \beta(\text{Id}_V) = 0$ , dove  $\text{Id}_V \in \text{Hom}(V, V) = V \otimes V^\vee$  denota l'identità.*

*Dimostrazione.* Sappiamo per ipotesi che  $H \subset L^\perp$ . Scegliamo una base  $e_1, \dots, e_n$  di  $V$  tale che  $H$  sia generato da  $e_1, \dots, e_h$  e  $L^\perp$  sia generato da  $e_1, \dots, e_l$ , con  $h \leq l$ . Detta  $\epsilon_1, \dots, \epsilon_n \in V^\vee$  la base duale, è sufficiente osservare che  $\text{Id}_V = \sum_i e_i \otimes \epsilon_i$  e che il nucleo di  $\alpha \otimes \beta$  è generato dai vettori  $e_i \otimes \epsilon_j$  con  $i \leq h$  oppure  $j > l$ .  $\square$

Sia  $w \in \bigwedge^s V - \{0\}$  un vettore fissato e si considerino le due applicazioni lineari

$$\begin{aligned} \alpha: V &\rightarrow \bigwedge^{s+1} V, & \alpha(v) &= v \wedge w, \\ \beta: V^\vee &\rightarrow \bigwedge^{s-1} V, & \beta(\phi) &= \phi \lrcorner w. \end{aligned}$$

Denotiamo  $H = \text{Ker}(\alpha)$ ,  $L = \text{Ker}(\beta)$ ,  $h = \dim H$  e  $n - l = \dim L$ .

**Lemma 11.1.5.** *Nelle notazioni precedenti si ha:*

1.  $H \subset L^\perp$ .
2.  $L^\perp$  è il più piccolo sottospazio tale che  $w \in \bigwedge^s L^\perp$ .
3. Si può scrivere  $w = p \wedge q$  con  $p \in \bigwedge^h H$ .
4. Il vettore  $w$  è totalmente decomponibile se e solo se  $H = L^\perp$ .

*Dimostrazione.* Il Punto 1 segue immediatamente dalla formula di Leibniz

$$\phi \lrcorner (v \wedge w) + v \wedge (\phi \lrcorner w) = \langle \phi, v \rangle w.$$

Per definizione  $\phi \in L$  se e solo se  $w \in \bigwedge^s(\text{Ker}(\phi))$  e quindi  $w \in \bigwedge^s L^\perp$ . Il Punto 3 segue dal fatto che  $v \wedge w = 0$  se e solo se  $w = v \wedge p$  per qualche  $p \in \bigwedge^{s-1} V$ . Se  $w$  è totalmente decomponibile si verifica che  $h = l = s$  e quindi  $H = L^\perp$ ; viceversa, dai Punti 2 e 3 segue che  $h \leq s \leq l$  e quindi se  $H = L^\perp$  allora  $h = s = l$  e quindi  $w$  è totalmente decomponibile.  $\square$

**Proposizione 11.1.6.** *Fissata una base  $e_1, \dots, e_n \in V$  con base duale  $\epsilon_1, \dots, \epsilon_n$ , un vettore  $w \in \bigwedge^s V$  è totalmente decomponibile se e solo se*

$$\sum_{i=1}^n (e_i \wedge w) \otimes (\epsilon_i \lrcorner w) = 0 \in \bigwedge^{s+1} V \otimes \bigwedge^{s-1} V.$$

*Dimostrazione.* Per i lemmi precedenti, il vettore  $w$  è totalmente decomponibile se e solo se  $\wedge w \otimes \lrcorner w (Id_V) = 0$ .  $\square$

Travasando la Proposizione 11.1.6 in termini delle coordinate Plückeriane otteniamo, per ogni elemento  $e_H \otimes e_K$  della base di  $\bigwedge^{s+1} V \otimes \bigwedge^{s-1} V$ ,  $H = \{h_0, \dots, h_{s+1}\}$ ,  $K = \{k_2, \dots, k_s\}$ , la relazione quadratica

$$R_{H,K} = \sum_{i=0}^s (-1)^i p_{h_0, \dots, h_{i-1}, h_{i+1}, \dots, h_s} \cdot p_{h_i, k_2, \dots, k_s} = 0.$$

Veniamo infine al calcolo dello spazio tangente proiettivo nel punto di  $\mathbb{G}(s, V) \subset \mathbb{P}(\bigwedge^s V)$  corrispondente ad un sottospazio vettoriale  $H \subset V$  di dimensione  $s$ . Per ogni applicazione lineare  $f: H \rightarrow V$  ed ogni  $s$ -upla di vettori  $h_1, \dots, h_s \in H$  poniamo

$$f \lrcorner (h_1 \wedge \dots \wedge h_s) = \sum_{i=1}^s h_1 \wedge \dots \wedge h_{i-1} \wedge f(h_i) \wedge h_{i+1} \wedge \dots \wedge h_s \in \bigwedge^s V.$$

Si noti che  $f \lrcorner (h_1 \wedge \dots \wedge h_s)$  è uguale al coefficiente di  $t$  in

$$(h_1 + tf(h_1)) \wedge \dots \wedge (h_s + tf(h_s))$$

e che risulta definita una applicazione lineare

$$\lrcorner: \text{Hom}(H, V) \rightarrow \text{Hom}\left(\bigwedge^s H, \bigwedge^s V\right).$$

**Proposizione 11.1.7.** *Sia  $\tilde{H} \subset \bigwedge^s V$  il sottospazio formato da tutti i vettori  $f \lrcorner h$  al variare di  $f \in \text{Hom}(H, V)$  e  $h \in \bigwedge^s H \cong \mathbb{K}$ . Allora il morfismo  $\lrcorner$  induce un isomorfismo di spazi vettoriali*

$$\text{Hom}\left(H, \frac{V}{H}\right) = \text{Hom}\left(\bigwedge^s H, \frac{\tilde{H}}{\bigwedge^s H}\right)$$

e vale  $\mathbb{T}_H \mathbb{G}(s, V) = \mathbb{P}(\tilde{H})$ .

*Dimostrazione.* La prima parte è un semplice conto di algebra lineare che lasciamo per esercizio al lettore. Se  $F \in I(\mathbb{G}(s, V))$  allora, per ogni  $f \in \text{Hom}(H, V)$ , per ogni  $h_1, \dots, h_s \in H$  ed ogni  $t \in K$  vale

$$0 = F((h_1 + tf(h_1)) \wedge \dots \wedge (h_s + tf(h_s))) = F(h + t(f \lrcorner h)) + O(t^2),$$

dove  $h = h_1 \wedge \dots \wedge h_s$ . Ne consegue che  $\mathbb{P}(\tilde{H}) \subset \mathbb{T}_H X$  e per ragioni di dimensione vale  $\mathbb{P}(\tilde{H}) = \mathbb{T}_H X$ .  $\square$

### Esercizi

**11.1.** Provare che in caratteristica 0 vale

$$\begin{aligned} (v_a \wedge \cdots \wedge v_1) \lrcorner (z_1 \wedge \cdots \wedge z_b) &= \\ &= \frac{1}{(b-a)!} \sum_{\sigma \in \Sigma_b} (-1)^\sigma \left( \prod_{i=1}^a \langle v_i, z_{\sigma(i)} \rangle \right) z_{\sigma(a+1)} \wedge \cdots \wedge z_{\sigma(b)} \end{aligned}$$

**11.2 (Formula di Leibniz).** Provare che per ogni  $\phi \in V^\vee$ ,  $u \in \wedge^a V$  e  $v \in \wedge^b V$ , con  $a, b > 0$ , vale la formula

$$\phi \lrcorner (u \wedge v) = (\phi \lrcorner u) \wedge v + (-1)^a u \wedge (\phi \lrcorner v).$$

**11.3.** Convincersi che ogni automorfismo lineare di  $V$  induce un automorfismo regolare di  $G(s, V)$ .

**11.4.** Sia  $H \subset V$  sottospazio e  $l \geq 0$  un intero. Provare che

$$\Omega_l(H) = \{W \in G(s, V) \mid \dim_{\mathbb{K}}(W \cap H) \geq l\}$$

è l'intersezione di  $G(s, V)$  con un sottospazio proiettivo di  $\mathbb{P}(\wedge^s V)$ . (Sugg.: sia  $e_1, \dots, e_m$  una base di  $H$  e si consideri l'insieme dei vettori  $v \in \wedge^s V$  tali che  $v \wedge h = 0$  per ogni  $h \in \wedge^{m-l+1} H$ .)

**11.5 (Varietà di Schubert).** Sia  $A_1 \subset A_2 \subset \cdots \subset A_s \subset V$  una catena di sottospazi vettoriali di  $V$  di dimensioni  $d_i = \dim_{\mathbb{K}} A_i$ . Supponiamo che  $0 < d_1 < d_2 < \cdots < d_s$ , che  $d_i \leq n - s + i$  per ogni  $i$  e definiamo la **varietà di Schubert**

$$\Omega(A_1, \dots, A_s) = \{W \in G(s, V) \mid \dim_{\mathbb{K}}(W \cap A_i) \geq i\}.$$

Notiamo che  $\Omega(A_1, \dots, A_s)$  dipende, a meno di automorfismi regolari di  $G(s, V)$  dalle dimensioni  $d_i$  dei sottospazi  $A_i$ . Provare che  $\Omega(A_1, \dots, A_s)$  è un chiuso irriducibile della Grassmanniana e se ne calcoli la dimensione in funzione di  $d_1, \dots, d_s$ .

**11.6.** Siano dati  $m$  sottospazi proiettivi  $L_1, \dots, L_m \subset \mathbb{P}^n$ , di dimensioni  $d_1, \dots, d_m \leq n-2$  e tali che  $\sum_{i=1}^m \binom{n-d_i}{2} \leq 2(n-1)$ . Dimostrare che esiste una retta in  $\mathbb{P}^n$  che interseca  $L_1, \dots, L_m$ .

## 11.2 Le varietà di incidenza

Sia  $V$  uno spazio vettoriale di dimensione  $n$  su  $\mathbb{K}$ . Si definisce il **fibrato tautologico lineare** sulla Grassmanniana  $G(s, V)$  come

$$S = \{(W, v) \in G(s, V) \times V \mid v \in W\}.$$

Denotiamo inoltre con  $p: S \rightarrow G(s, V)$  e  $q: S \rightarrow V$  le proiezioni sui fattori. Diremo che un morfismo  $\phi: X \rightarrow Y$  di varietà algebriche è localmente un prodotto con fibra  $Z$  se esiste un ricoprimento aperto  $Y = \cup U_i$  ed isomorfismi  $h_i: \phi^{-1}(U_i) \rightarrow U_i \times Z$  tali che  $p$  è localmente la composizione di  $h_i$  e della proiezione sul primo fattore. I morfismi localmente prodotto sono aperti e stabili per cambio di base.

**Lemma 11.2.1.**  $S$  è un chiuso di  $G(s, V) \times V$  e  $p: S \rightarrow G(s, V)$  è localmente un prodotto a fibra  $\mathbb{K}^s$ .

*Dimostrazione.* Se pensiamo la Grassmanniana immersa in  $\mathbb{P}(\bigwedge^s V)$  tramite la mappa di Plücker si ha che

$$S = \left\{ ([w], v) \in \mathbb{P} \left( \bigwedge^s V \right) \times V \mid v \wedge w = 0, [w] \in \mathbb{G}(s, V) \right\}$$

da cui segue che  $S$  è chiuso. Si consideri adesso una decomposizione  $V = W \oplus H$ , con  $W \in G(s, V)$ , siano  $U \subset G(s, V)$  l'aperto dei sottospazi che intersecano trasversalmente  $H$  e  $r: S \rightarrow W$  la composizione di  $q$  e della proiezione  $\pi: V \rightarrow W$ . Proviamo che il morfismo regolare  $p^{-1}(U) \xrightarrow{(p,r)} U \times W$  è un isomorfismo. Infatti basta ricordare che  $U$  è isomorfo al sottospazio di  $\text{Hom}(W, V)$  delle mappe  $\alpha$  tali che  $\pi\alpha = \text{Id}$ . L'inversa di  $(p, r)$  è quindi data da  $(\alpha, v) = (\alpha, \alpha(v))$ .  $\square$

Definiamo con  $G(s, \mathbb{P}(V))$  l'insieme dei sottospazi proiettivi di  $\mathbb{P}(V)$  di dimensione  $s$ . Esiste una ovvia identificazione  $G(s, \mathbb{P}(V)) = G(s+1, V)$  e si definisce il **fibrato tautologico proiettivo**

$$Z = \{(W, v) \in G(s, \mathbb{P}(V)) \times \mathbb{P}(V) \mid v \in W\}, \quad p: Z \rightarrow G(s, \mathbb{P}(V)).$$

**Lemma 11.2.2.** Nelle notazioni precedenti, a varietà  $Z$  è liscia proiettiva irriducibile di dimensione  $s + (s+1)(\dim V - s - 1)$  ed il morfismo  $p: Z \rightarrow G(s, \mathbb{P}(V))$  è localmente prodotto a fibra  $\mathbb{P}^s$ .

**Definizione 11.2.3.** Sia  $X \subset \mathbb{P}^n$  una varietà proiettiva. Si definisce la **varietà di incidenza**  $I_X^s$  come il sottoinsieme di  $G(s, \mathbb{P}^n)$  formato dagli  $s$ -piani che intersecano  $X$ .

Abbiamo già dimostrato che  $I_X^s$  è un sottoinsieme proprio della Grassmanniana se e solo se  $s + \dim(X) < n$ .

**Proposizione 11.2.4.** Siano  $n > s \geq 0$  interi e  $X \subset \mathbb{P}^n$  una varietà irriducibile di codimensione  $d \geq s$ . Allora la varietà  $I_X^s$  degli  $s$ -piani che intersecano  $X$  è una sottovarietà chiusa irriducibile di codimensione  $d - s$  della Grassmanniana  $G(s, \mathbb{P}^n)$ .

*Dimostrazione.* Considerando il fibrato tautologico proiettivo sulla Grassmanniana

$$Z = \{(W, v) \in G(s, \mathbb{P}^n) \times \mathbb{P}^n \mid v \in W\}$$

notiamo che le fibre della proiezione  $p: Z \rightarrow G(s, \mathbb{P}^n)$  sono isomorfe a  $\mathbb{P}^s$ , mentre le fibre della proiezione  $q: Z \rightarrow \mathbb{P}^n$  sono isomorfe a  $G(s-1, \mathbb{P}^{n-1})$  e quindi sono varietà proiettive irriducibili di dimensione  $s(n-s)$ . In particolare  $q^{-1}(X)$  è una sottovarietà chiusa irriducibile di dimensione  $d + s(n-s)$ . Poiché  $d + s \leq n$ , abbiamo dimostrato (Proposizione 9.8.6) che esistono  $s$ -piani che intersecano  $X$  in un insieme finito e non vuoto di punti; ne consegue che  $I_X^s = p(q^{-1}(X))$  è un chiuso di dimensione  $d + s(n-s)$  e quindi di codimensione  $(s+1)(n-s) - d - s(n-s) = n - s - d$ .  $\square$

**Proposizione 11.2.5.** Sia  $T$  una varietà quasiproiettiva e  $X \subset \mathbb{P}^n \times T$  un chiuso; denotiamo con  $X_t$  la fibra di  $X$  sopra il punto  $t \in T$ . Allora il sottoinsieme

$$H = \{(W, t) \in G(s, \mathbb{P}^n) \times T \mid W \subset X_t\}$$

è chiuso in  $G(s, \mathbb{P}^n) \times T$ .

*Dimostrazione.* La proiezione  $p: Z \times T \rightarrow G(s, \mathbb{P}^n) \times T$  è localmente prodotto e quindi aperta ed  $H$  è il complementare di  $p(Z \times T - G(s, \mathbb{P}^n) \times X)$ .  $\square$

Siano  $x_0, \dots, x_n$  coordinate omogenee su  $\mathbb{P}^n$  e  $S_d \subset \mathbb{K}[x_0, \dots, x_n]$  il sottospazio vettoriale dei polinomi omogenei di grado  $d$ ; il proiettivizzato  $\mathbb{P}(S_d)$  può essere pensato come lo spazio delle ipersuperfici proiettive di grado  $d$  in  $\mathbb{P}^n$ . Esiste una famiglia universale di ipersuperfici

$$X_d = \{([F], [x_0, \dots, x_n]) \in \mathbb{P}(S_d) \times \mathbb{P}^n \mid F(x_0, \dots, x_n) = 0\}.$$

Il luogo  $X_d$  è chiaramente chiuso, lasciamo come esercizio di dimostrare che  $X_d$  è una ipersuperficie liscia irriducibile di bigrado  $(1, d)$ . Possiamo applicare la Proposizione 11.2.5 alla famiglia  $X_d \rightarrow \mathbb{P}(S_d)$  e otteniamo che

$$I_d(s, \mathbb{P}^n) = \{(W, [F]) \in G(s, \mathbb{P}^n) \times \mathbb{P}(S_d) \mid W \subset V(F)\}$$

è una varietà proiettiva.

**Lemma 11.2.6.** *La varietà  $I_d(s, \mathbb{P}^n)$  è irriducibile ed ha codimensione  $\binom{s+d}{d}$  nel prodotto  $G(s, \mathbb{P}^n) \times \mathbb{P}(S_d)$ .*

*Dimostrazione.* Si consideri la proiezione  $p: I_d(s, \mathbb{P}^n) \rightarrow G(s, \mathbb{P}^n)$ , la fibra  $p^{-1}(W)$  è composta dal sistema lineare di ipersuperfici che contengono  $W$  e quindi ha codimensione uguale alla dimensione dello spazio delle forme omogenee di grado  $d$  su  $W$  che è uguale a  $\binom{s+d}{d}$ . La irriducibilità di  $I_d(s, \mathbb{P}^n)$  segue allora dal Teorema 10.6.6.  $\square$

Consideriamo il caso  $s = 1, n = 3$ , e consideriamo la proiezione sul secondo fattore  $q: I_d(1, \mathbb{P}^3) \rightarrow \mathbb{P}(S_d)$ . Dato  $[F] \in \mathbb{P}(S_d)$ , la fibra  $q^{-1}([F])$  è l'insieme delle rette contenute in  $V(F)$ .

**Teorema 11.2.7.** *Nelle notazioni precedenti, se  $d \geq 3$ , allora  $q(I_d(1, \mathbb{P}^3)) \subset \mathbb{P}(S_d)$  è un chiuso di codimensione  $d - 3$ . Di conseguenza ogni superficie di grado 3 in  $\mathbb{P}^3$  contiene almeno una retta, mentre la generica superficie di grado  $d > 3$  non contiene rette.*

*Dimostrazione.* Siccome  $G(1, \mathbb{P}^3)$  ha dimensione 4 e  $I_d(1, \mathbb{P}^3)$  ha codimensione  $d + 1$ , la codimensione di  $q(I_d(1, \mathbb{P}^3))$  è  $\geq d + 1 - 4 = d - 3$  e vale = se e solo se esiste una fibra di  $q$  di dimensione 0. Preso  $F = x_0x_1x_2^{d-2} - x_3^d$  si vede facilmente (esercizio) che  $V(F)$  contiene esattamente tre rette  $L_0, L_1, L_2, L_i = \{x_i = x_3 = 0\}$ .  $\square$

**Esercizi**

**11.7.** Provare che  $p: I_d(s, \mathbb{P}^n) \rightarrow G(s, \mathbb{P}^n)$  è localmente un prodotto.

**11.8.** Siano  $S$  e  $T$  varietà quasiproiettive,  $X \subset \mathbb{P}^n \times T$  e  $Y \subset \mathbb{P}^n \times S$  chiusi. Denotiamo con  $X_t$  (risp.:  $Y_s$ ) la fibra di  $X$  (risp.:  $Y$ ) sopra il punto  $t \in T$  (risp.:  $s \in S$ ). Dimostrare che per ogni intero  $d$  l'insieme

$$K_d = \{(s, t) \in S \times T \mid \dim(X_t \cap Y_s) \geq d\}$$

è chiuso in  $S \times T$ .

**11.9.** Sia  $C$  una quartica piana liscia senza iperflessi. Dimostrare che  $C$  possiede almeno una bitangente. (Sugg.: sia  $L$  una retta fissata,  $\mathbb{P}^{14}$  lo spazio delle quartiche e  $B_L \subset \mathbb{P}^{14}$  l'insieme delle quartiche  $C$  tali che o  $L$  è bitangente a  $C$  oppure esiste  $p \in C$  tale che  $\nu_p(C, L) \geq 4$ . Provare che  $B_L$  è un chiuso irriducibile di dimensione 12.)

### 11.3 Il teorema delle 27 rette

In questa sezione dimostriamo, sotto l'ipotesi aggiuntiva che il campo  $\mathbb{K}$  abbia caratteristica  $\neq 2$ , il seguente celebre teorema.

**Teorema 11.3.1 (Cayley-Salmon, 1849).** *Sia  $S \subset \mathbb{P}^3$  una superficie liscia di grado 3. Allora  $S$  contiene esattamente 27 rette, ognuna delle quali ne interseca altre 10.*

Il Teorema 11.3.1 è vero anche in caratteristica 2, ma in tal caso è necessaria una diversa (e più difficile) dimostrazione. La dimostrazione di 11.3.1 è divisa in vari passi; il punto di partenza è il Teorema 11.2.7, in base al quale  $S$  contiene almeno una retta.

Introduciamo alcune notazioni: sia  $x_0, \dots, x_3$  un sistema di coordinate omogenee su  $\mathbb{P}^3$  e  $F(x_0, \dots, x_3)$  l'equazione di  $S$ , per ipotesi  $F$  è omogeneo di grado 3 e le derivate parziali  $\frac{\partial F}{\partial x_i}$ ,  $i = 0, \dots, 3$  non hanno zeri comuni su  $S$ . Se  $H \subset \mathbb{P}^3$  è un piano si denoterà con  $H \cdot S$  la cubica piana la cui equazione è la restrizione di  $F$  ad  $H$ . Per ogni  $p \in S$  denotiamo con  $\mathbb{T}_p S \subset \mathbb{P}^3$  il piano tangente proiettivo a  $S$  nel punto  $p$ , l'equazione di  $\mathbb{T}_p S$  è  $\sum x_i \frac{\partial F}{\partial x_i}(p) = 0$ .

**Lemma 11.3.2.** *Sia  $H \subset \mathbb{P}^3$  un piano e  $p \in H \cap S$ . Allora vale  $H = \mathbb{T}_p S$  se e solo se  $p$  è un punto singolare di  $H \cdot S$ .*

*Dimostrazione.* In opportune coordinate omogenee tali che  $p = [1, 0, 0, 0]$  e  $H = \{x_3 = 0\}$ , l'equazione di  $H \cdot S$  è data da  $F(x_0, x_1, x_2, 0)$  ed il punto  $p$  è singolare per  $H \cdot S$  se e solo se  $\frac{\partial F}{\partial x_i}(p) = 0$ ,  $i = 0, 1, 2$ .  $\square$

**Lemma 11.3.3.** *La cubica  $H \cdot S$  è ridotta per ogni piano  $H$ .*

*Dimostrazione.* Si assuma per assurdo che  $H \cdot S = 2L + M$  con  $L, M$  rette in  $H$ ; per il Lemma 11.3.2 vale  $H = \mathbb{T}_p S$  per ogni  $p \in L \subset S$ . Sia  $H'$  un qualsiasi piano contenente la retta  $L$ , si ha allora  $H' \cdot S = L + C$  per una opportuna conica  $C$ ; se  $q \in L \cap C$ , per il Lemma 11.3.2 si ha  $H' = \mathbb{T}_p S$ . Quindi  $H' = H$  che è alquanto assurdo.  $\square$

**Lemma 11.3.4.** *Sia  $Q(s, x_0, x_1, x_2)$  un polinomio a coefficienti in un campo algebricamente chiuso di caratteristica  $\neq 2$ , omogeneo di grado 2 nelle variabili  $x_i$  e sia  $\delta(s)$  il determinante della matrice Hessiana  $\left( \frac{\partial^2 Q}{\partial x_i \partial x_j} \right)$ . Fissato un punto  $p = (s_0, [v_0, v_1, v_2]) \in \mathbb{A}^1 \times \mathbb{P}^2$ , se la conica piana di equazione  $Q(s_0, x_0, x_1, x_2)$  è ridotta con un punto singolare in  $[v_0, v_1, v_2]$ , allora vale*

$$\frac{d\delta}{ds}(s_0) = 0 \quad \text{se e solo se} \quad \frac{\partial Q}{\partial s}(s_0, v_0, v_1, v_2) = 0.$$

*Dimostrazione.* (Cfr. [Shaf1972, II.6.4]) A meno di un cambio lineare di coordinate si può supporre  $p = (0, [0, 0, 1])$ , e  $Q(0, x_0, x_1, x_2) = x_0 x_1$ . Dunque  $\delta(0) = 0$  ed un semplice conto mostra che  $\frac{d\delta}{ds}(0) = -\frac{\partial^3 Q}{\partial s \partial x_2^2}(0)$ , mentre per la formula di Eulero, applicata a  $\frac{\partial Q}{\partial s}|_{s=0}$ , si ha  $\frac{\partial Q}{\partial s}(0, 0, 0, 1) = \frac{1}{2} \frac{\partial^3 Q}{\partial s \partial x_2^2}(0)$ .  $\square$

Si consideri adesso una retta fissata  $L \subset S$  e sia  $j$  il numero di rette  $M \neq L$  contenute in  $S$  che intersecano  $L$ . Grazie a 11.3.3 sappiamo che  $j$  è uguale al doppio del numero di piani  $H$  contenenti  $L$  e tali che, se  $H \cdot S = L + C$ , la conica  $C$  è singolare.



**Lemma 11.3.5.** *Nelle notazioni precedenti  $j = 10$ .*

*Dimostrazione.* Fissiamo un sistema di coordinate omogenee tali che  $L = \{x_0 = x_1 = 0\}$ . In tali coordinate l'equazione di  $S$  diventa

$$F = x_0A(x_2, x_3) + x_1B(x_2, x_3) + x_0^2m(x_2, x_3) + x_1^2n(x_2, x_3) + x_0x_1p(x_2, x_3) + G(x_0, x_1),$$

con  $m, n, p$  forme lineari,  $A, B$  forme quadratiche e  $G$  omogeneo di grado 3. Si noti che le derivate parziali  $\frac{\partial F}{\partial x_2}$  e  $\frac{\partial F}{\partial x_3}$  si annullano in tutti i punti di  $L$ , dato che  $S$  è liscia le due forme binarie  $\frac{\partial F}{\partial x_0}(0, 0, x_2, x_3) = A(x_2, x_3)$ ,  $\frac{\partial F}{\partial x_1}(0, 0, x_2, x_3) = B(x_2, x_3)$  non hanno zeri comuni. Per ogni  $a = (a_0, a_1) \in \mathbb{K}^2 - 0$  sia  $H_a$  il piano di equazione  $a_1x_0 = a_0x_1$  e sia  $\phi_a: \mathbb{P}^2 \rightarrow H_a$  la proiettività  $\phi_a([y_1, y_2, y_3]) = [a_0y_1, a_1y_1, y_2, y_3]$ . Si ha quindi  $\phi_a^{-1}(H_a \cap S) = L + C_a$  dove  $L$  è la retta di equazione  $\{y_1 = 0\}$  e  $C_a$  è la conica di equazione

$$Q = a_0A + a_1B + y_1(a_0^2m + a_1^2n + a_0a_1p) + y_1^2G(a_0, a_1),$$

con  $A, B$  (risp.:  $m, n, p$ ) forme quadratiche (risp.: lineari) in  $y_2, y_3$ . Denotando  $A_{ij} = \frac{\partial^2 A}{\partial y_i \partial y_j}$  e  $B_{ij} = \frac{\partial^2 B}{\partial y_i \partial y_j}$ , il discriminante  $\Delta(a_0, a_1)$  di  $C_a$  è il determinante della matrice Hessiana

$$\left| \frac{\partial^2 Q}{\partial y_i \partial y_j} \right| = \begin{vmatrix} 2G(a_0, a_1) & a_0^2m_2 + a_1^2n_2 + a_0a_1p_2 & a_0^2m_3 + a_1^2n_3 + a_0a_1p_3 \\ a_0^2m_2 + a_1^2n_2 + a_0a_1p_2 & a_0A_{22} + a_1B_{22} & a_0A_{23} + a_1B_{23} \\ a_0^2m_3 + a_1^2n_3 + a_0a_1p_3 & a_0A_{32} + a_1B_{32} & a_0A_{33} + a_1B_{33} \end{vmatrix}$$

Si vede subito che  $\Delta(a_0, a_1)$  è un polinomio omogeneo di grado 5 in  $a_0, a_1$ . Dato che i piani  $H_a$ , al variare di  $[a] \in \mathbb{P}^1$ , sono tutti e soli i piani contenenti  $L$ , è sufficiente dimostrare che  $\Delta$  non ha fattori multipli. Poniamo  $\delta(s) = \Delta(1, s)$  e proviamo che  $\delta$  non ha radici multiple, seguirà per simmetria che anche  $\Delta(s, 1)$  non ha radici multiple. Si osservi innanzitutto che l'ipersuperficie  $Z \subset \mathbb{A}^1 \times \mathbb{P}^2$  di equazione  $Q(1, s, y_1, y_2, y_3) = 0$  è liscia. Infatti, se esistesse un punto  $(1, s, v_1, v_2, v_3) \in Z$  che annulla tutte le derivate parziali di  $Q$ , siccome  $A$  e  $B$  non hanno zeri comuni deve necessariamente essere  $v_1 \neq 0$ , possiamo quindi restringerci all'aperto affine  $y_1 = 1$  dove  $Z$  ha equazione  $Q(1, s, y_2, y_3) = F(1, s, y_2, y_3)$  e tutto segue dalla liscchezza di  $S$ . Basta applicare adesso il Lemma 11.3.4.  $\square$

*Dimostrazione (del Teorema 11.3.1).* Abbiamo visto che esiste un piano  $H$  tale che  $H \cdot S = L_1 + L_2 + L_3$  con le  $L_i$  rette contenute in  $S$  e che  $H = \mathbb{T}_{p_{ij}}S$  dove  $p_{ij} = L_i \cap L_j$ . Ogni altra retta  $M$  contenuta in  $S$  interseca  $H$  e quindi almeno una delle rette  $L_i$ , d'altra parte se  $p \in L_i \cap M$  allora  $M \subset \mathbb{T}_pS$  e quindi  $M$  interseca al più una delle rette  $L_i$ . Tenendo presente che ogni retta  $L_i$  interseca altre 8 rette contenute in  $S$  ma non in  $H$ , ne consegue che il numero totale delle rette in  $S$  è uguale a  $3 + 3 \cdot 8 = 3 + 24 = 27$ .  $\square$

### Esercizi

**11.10.** (caratteristica  $\neq 2$ ) Sia  $S \subset \mathbb{P}^3$  una superficie cubica liscia,  $L \subset S$  una retta e  $\mathbb{P}^1$  il fascio di piani contenenti  $L$ . Provare che l'applicazione  $\phi_L: S \rightarrow \mathbb{P}^1$  definita da  $\phi_L(p) = L + p$  se  $p \notin L$  e  $\phi_L(p) = \mathbb{T}_pS$  se  $p \in L$  è un morfismo regolare.

**11.11.** (caratteristica  $\neq 2$ ) Siano  $L$  e  $M$  due rette sghembe contenute in una superficie cubica  $S \subset \mathbb{P}^3$ .

1. Provare che esistono esattamente 5 rette  $R_1, \dots, R_5$  contenute in  $S$  e che intersecano  $L$  e  $M$ .

2. Provare che l'applicazione (vedi Esercizio 11.10)  $\phi_L \times \phi_M: S \rightarrow \mathbb{P}^1 \times \mathbb{P}^1$  è surgettiva, contrae le rette  $R_1, \dots, R_5$  a dei punti  $p_1, \dots, p_5$  ed è iniettiva su  $S - (R_1 \cup \dots \cup R_5)$ .
3. Provare che i punti  $p_1, \dots, p_5$  sono in posizione generica, cioè ogni corrispondenza su  $\mathbb{P}^1 \times \mathbb{P}^1$  di tipo  $(1, 0), (0, 1), (1, 1)$  contiene rispettivamente al più 1, 1, 3 punti  $p_i$ .
4. Descrivere in funzione dei punti  $p_1, \dots, p_5$  le curve di  $\mathbb{P}^1 \times \mathbb{P}^1$  che sono immagine tramite  $\phi_L \times \phi_M$  delle 27 rette in  $S$ .

**11.12 (Le 28 bitangenti, \*\*).** (caratteristica  $\neq 2, 3$ ) Sia  $C \subset \mathbb{P}^2$  una quartica liscia senza iperflessi e sia  $L$  una retta bitangente a  $C$  (vedi Esercizio 11.9). Provare che esiste un sistema di coordinate omogenee  $x_0, x_1, x_2$  tali che le equazioni di  $L$  e  $C$  sono rispettivamente  $x_0 = 0$  e  $x_1^2 x_2^2 - 4x_0 g(x_0, x_1, x_2) = 0$ . Consideriamo  $\mathbb{P}^2$  come il piano di  $\mathbb{P}^3$  di equazione  $x_3 = 0$ , denotiamo  $o = [0, 0, 0, 1] \in \mathbb{P}^3$  e con  $\pi: \mathbb{P}^3 - \{o\} \rightarrow \mathbb{P}^2$  la proiezione di centro  $o$ . Sia  $S \subset \mathbb{P}^3$  la cubica di equazione  $x_0 x_3^2 + x_1 x_2 x_3 + g(x_0, x_1, x_2)$ . Dimostrare che la curva  $C$  coincide con l'insieme dei valori critici della proiezione  $\pi: S - \{o\} \rightarrow \mathbb{P}^2$ . Sia  $R = \pi^{-1}(C) \subset S - \{o\}$  l'insieme dei punti critici. Provare che  $S$  è liscia al di fuori di  $R$ . Sia  $p \in R$  tale che  $q := \pi(p) \notin L$  e sia  $H \subset \mathbb{P}^2$  una retta passante per  $q$ . Dimostrare che  $H$  è tangente a  $C$  in  $q$  se e solo se  $S \cdot \pi^{-1}(H)$  è singolare in  $p$  e dedurre che  $S$  è una cubica liscia (Sugg.: usare 6.3.2). Dimostrare che esiste una bigezione tra le rette contenute in  $S$  e le bitangenti a  $C$  diverse da  $L$ .

## 11.4 Il teorema di Bertini-Sard

**Definizione 11.4.1.** Sia  $\phi: X \rightarrow Y$  un morfismo regolare tra varietà quasiproiettive irriducibili, diremo che un punto  $x \in X$  è **critico** se il differenziale  $d\phi(x): T_x X \rightarrow T_{\phi(x)} Y$  non è surgettiva.

**Lemma 11.4.2.** Sia  $\phi: X \rightarrow Y$  un morfismo regolare di varietà quasiproiettive e per ogni  $x \in X$  denotiamo con  $V_x \subset T_x X$  il nucleo del differenziale di  $\phi$  nel punto  $x$ . Allora la funzione  $x \mapsto \dim_{\mathbb{K}} V_x$  è semicontinua superiormente su  $X$  e, se  $X$  è liscia, allora l'insieme dei punti critici è chiuso.

*Dimostrazione.* Possiamo assumere  $X, Y$  affini, a meno di comporre  $\phi$  con una immersione chiusa di  $Y$  in uno spazio affine possiamo supporre  $Y = \mathbb{A}^m$  ed a meno di sostituire  $X$  con il grafico di  $\phi$  si può assumere che  $X$  sia un chiuso di  $\mathbb{A}^{n+m}$  e che  $\phi$  sia la proiezione sulle ultime coordinate. Se  $f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m]$  è un insieme di generatori dell'ideale  $I(X)$ , un vettore  $v = (v_1, \dots, v_n, w_1, \dots, w_m)$  appartiene a  $V_x$  se e solo se  $w_i = 0$  per ogni  $i$  e

$$\sum_{i=1}^n v_i \frac{\partial f_j}{\partial x_i} = 0, \quad j = 1, \dots, r.$$

La semicontinuità è adesso chiara. Se  $X$  è liscia, un punto  $x$  è critico se e solo se  $\dim V_x + \dim T_{\phi(x)} > \dim X$ . Basta adesso osservare che le funzioni  $x \mapsto \dim V_x$ ,  $x \mapsto \dim T_{\phi(x)}$  sono entrambe semicontinue superiormente.  $\square$

**Teorema 11.4.3 (Bertini-Sard).** Sia  $\phi: X \rightarrow Y$  un morfismo regolare tra varietà quasiproiettive irriducibili definite su un campo  $\mathbb{K}$  algebricamente chiuso di caratteristica 0 e sia  $Z \subset X$  l'insieme dei suoi punti critici. Allora  $\phi(Z)$  è contenuto in un chiuso proprio di  $Y$ .

Prima di fornire la dimostrazione premettiamo alcune osservazioni ed un lemma.

*Osservazione 11.4.4.* Sul campo dei numeri complessi, i chiusi propri di Zariski di varietà irriducibili non hanno parte interna nella topologia euclidea (vedi Esercizio 9.54) ed hanno misura<sup>1</sup> nulla.

In caratteristica positiva il Teorema di Bertini-Sard è falso: si consideri ad esempio un campo di caratteristica  $p > 0$  ed il morfismo  $\phi: \mathbb{A}^1 \rightarrow \mathbb{A}^1, \phi(x) = x^p$ . Si tratta di un morfismo bigettivo ma tutti i punti del dominio sono critici.

In alcune applicazioni pratiche si riesce a dimostrare direttamente che  $\dim \bar{Z} < \dim Y$ , in questo caso il Teorema 11.4.2 è banalmente vero senza ipotesi sulla caratteristica del campo.

Se  $X$  è una varietà liscia, se il morfismo  $\phi$  è surgettiva e se  $y \notin \phi(Z)$ , allora la fibra  $V = \phi^{-1}(y)$  è una varietà liscia: infatti per ogni  $x \in V$  vale

$$\dim_{\mathbb{K}} T_x V \leq \dim_{\mathbb{K}} T_x X - \dim_{\mathbb{K}} T_y Y \leq \dim X - \dim Y \leq \dim_x V$$

da cui segue che  $y$  è un punto liscio di  $Y$  e  $x$  un punto liscio di  $V$ .

**Lemma 11.4.5.** *In caratteristica 0, se  $\phi: X \rightarrow Y$  è un morfismo dominante di varietà quasiproiettive irriducibili, allora i punti critici di  $\phi$  sono contenuti in un chiuso proprio di  $X$ .*

*Dimostrazione.* Riconduciamoci con opportune semplificazioni ad un caso particolare in cui dimostrare 11.4.5. A tal fine osserviamo che:

a) Siano  $U \subset X, V \subset Y$  aperti tali che  $\phi(U) \subset V$ . Se il risultato è vero per la restrizione  $\phi|_U$ , allora è vero anche per  $\phi$ ; non è quindi restrittivo assumere  $X$  e  $Y$  varietà affini nonsingolari.

b) Se  $\phi$  è la composizione di due morfismi dominanti  $\alpha: X \rightarrow Z$  e  $\beta: Z \rightarrow Y$  ( $Z$  è necessariamente irriducibile) e se il risultato è vero per  $\alpha$  e  $\beta$ , allora è vero anche per  $\phi$ .

A meno di cambiare  $X$  con il grafico di  $\phi$  si può assumere  $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$  chiusi,  $m \leq n$  e  $\phi$  la proiezione sulle prime  $m$ -coordinate. Se  $n = m$  allora  $X = Y$  e non c'è nulla da dimostrare; se  $m = n - 1$  sono possibili due casi: nel primo  $X = Y \times \mathbb{A}^1$  e non esistono punti critici.

Nel secondo caso  $X$  è un chiuso proprio di  $Y \times \mathbb{A}^1$ : si ha  $\dim X = \dim Y, I(Y) = I(X) \cap \mathbb{K}[x_1, \dots, x_m]$  e l'insieme dei polinomi  $f = \sum f_i(x_1, \dots, x_m)x_n^i \in I(X)$  tali che  $f_i \notin I(Y)$  per qualche  $i > 0$  è non vuoto; sia  $g$  un tale polinomio di grado in  $x_n$  minimo ed uguale a  $d > 0$ . Per ipotesi la caratteristica del campo è 0, quindi  $\frac{\partial g}{\partial x_n}$  non appartiene

a  $I(X)$  e  $Z = X \cap V\left(\frac{\partial g}{\partial x_n}\right)$  è un chiuso proprio di  $X$ . Ragionando come in 10.7.8, se  $x \in X - Z$  la proiezione  $T_x X \rightarrow T_{\phi(x)} Y$  è iniettiva e siccome  $X$  e  $Y$  sono varietà lisce della stessa dimensione il differenziale è anche surgettivo.

Infine se  $n > m + 1$  allora  $\phi$  è la composizione di  $\alpha$  e  $\beta$  dove  $\alpha: \mathbb{A}^n \rightarrow \mathbb{A}^{n-1}, \beta: \mathbb{A}^{n-1} \rightarrow \mathbb{A}^m$  sono le proiezioni sulle prime coordinate. Posto  $Z \subset \mathbb{A}^{n-1}$  la chiusura di  $\alpha(X)$ , chiaramente  $Z \subset \beta^{-1}(Y)$  ed i morfismi  $\alpha: X \rightarrow Z$  e  $\beta: Z \rightarrow Y$  sono dominanti. Per l'ipotesi induttiva il lemma è vero per  $\alpha$  e  $\beta$  e quindi anche per  $\phi$ .  $\square$

*Dimostrazione (Dimostrazione di 11.4.3).* Se  $\phi$  non è dominante non c'è nulla da dimostrare. Se  $\phi$  è dominante siano  $Z_1, \dots, Z_r$  le componenti irriducibili di  $Z$  e poniamo  $W_i \subset X$  la chiusura di  $Z_i$ . Per il Lemma 11.4.5  $W_i$  è un chiuso proprio e  $Z_i$  è denso in  $W_i$ , dato che per ogni  $x \in W_i$  vale  $T_x W_i \subset T_x X$ , i punti critici di  $\phi: W_i \rightarrow Y$  non sono contenuti in alcun chiuso proprio e per il Lemma 11.4.5  $\phi(W_i)$  è contenuto in un chiuso proprio di  $Y$ .  $\square$

<sup>1</sup> Rimandiamo a [GH1978, pp. 27-33] per i fondamentali di teoria della misura sulle varietà algebriche complesse.

**Corollario 11.4.6.** *Sia  $V$  un sistema lineare di curve piane di grado  $d$  e  $BS(V) \subset \mathbb{P}^2$  i punti base di  $V$ . Se il campo ha caratteristica 0, allora esiste un aperto non vuoto  $U \subset V$  i cui punti corrispondono a curve lisce su  $\mathbb{P}^2 - BS(V)$ .*

*Dimostrazione.* Sia  $d > 0$  la dimensione di  $V$  e siano  $F_0, \dots, F_d$  le equazioni di una base di  $V$ . Le combinazioni lineari di  $F_0, \dots, F_d$  sono tutte e sole le equazioni delle curve del sistema lineare e  $BS(V) = V(F_0, \dots, F_d)$ . Sia  $X \subset \mathbb{P}_y^d \times \mathbb{P}_x^2$  l'ipersuperficie definita da  $y_0 F_0(x_0, x_1, x_2) + \dots + y_d F_d(x_0, x_1, x_2) = 0$  e  $\phi: X \rightarrow \mathbb{P}^d$  la proiezione sul primo fattore. Se  $[C] \in \mathbb{P}^d \cong V$  è il punto corrispondente ad una curva  $C$  si ha  $\phi^{-1}([C]) = \{[C]\} \times C$ . I punti singolari di  $X$  sono contenuti in  $\mathbb{P}^d \times BS(V)$  e quindi la curva  $C$  è liscia al di fuori dei punti base se e solo se  $[C]$  non appartiene all'immagine dei punti critici di  $\phi: X - (\mathbb{P}^d \times BS(V)) \rightarrow \mathbb{P}^d$ .  $\square$

## Esercizi

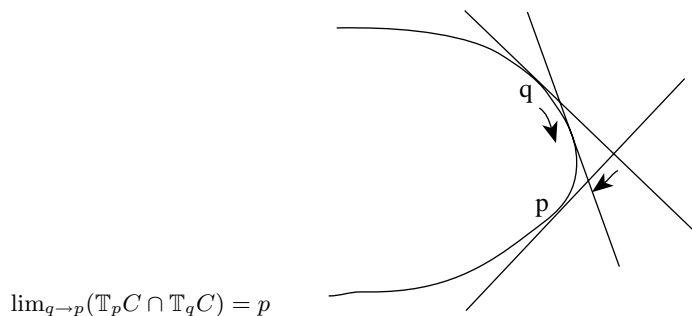
**11.13.** Trovare un esempio di morfismo regolare tra varietà irriducibili tale che i punti critici non siano un chiuso.

**11.14 (Teorema di Bertini delle sezioni iperpiane).** Sia  $X \subset \mathbb{P}^n$  una varietà proiettiva liscia di dimensione positiva; provare che la generica sezione iperpiana è una varietà liscia. Notare che questo risultato è valido in caratteristica arbitraria. (Sugg.: se  $X \neq \mathbb{P}^n$  si consideri  $Y \subset X \times (\mathbb{P}^n)^\vee$  l'insieme delle coppie  $(x, H)$  tali che  $x \in X \cap H$ ; provare che il luogo  $Z$  dei punti critici della proiezione  $Y \rightarrow (\mathbb{P}^n)^\vee$  è un chiuso irriducibile di dimensione  $n - 1$ .)

## 11.5 Varietà duali

In questa sezione considereremo esclusivamente varietà su di un campo  $\mathbb{K}$  algebricamente chiuso di caratteristica 0.

Una nozione classica di geometria proiettiva è quella di **inviluppo**, cioè del luogo delle intersezioni di elementi infinitamente vicini in una data famiglia di sottospazi proiettivi. Sembra risalire a Cartesio l'osservazione che ogni curva è l'inviluppo della famiglia delle sue tangenti, vedi Figura 11.1



**Figura 11.1.** Inviluppo delle rette tangenti ad una curva piana

Oggidì la nozione di inviluppo è stata quasi completamente soppiantata dal concetto di **varietà duale**. Sia  $V$  uno spazio vettoriale di dimensione  $N + 1$  e  $X \subset \mathbb{P}(V)$  una

varietà proiettiva irriducibile di dimensione  $n$ ; denotiamo con  $X_e \subset X$  l'aperto dei punti lisci e con

$$D_X = \{(x, [\alpha]) \in X_e \times \mathbb{P}(V^\vee) \mid \mathbb{T}_x X \subset \mathbb{P}(\text{Ker}(\alpha))\}.$$

**Lemma 11.5.1.**  $D_X$  è un chiuso irriducibile di dimensione  $N - 1$ .

*Dimostrazione.* Il fibrato tangente proiettivo

$$\mathbb{T}_{X_e} = \{(x, [v]) \in X_e \times \mathbb{P}(V) \mid [v] \in \mathbb{T}_x X\}$$

si dimostra facilmente essere chiuso; esso è infatti il luogo di zeri dei polinomi omogenei  $\sum v_i \frac{\partial f}{\partial x_i}$  al variare di  $f \in I(X)$ . In modo del tutto simile si prova che

$$Z = \{(x, [\alpha], [v]) \in X_e \times \mathbb{P}(V^\vee) \times \mathbb{P}(V) \mid [v] \in \mathbb{T}_x X, \langle v, \alpha \rangle = 0\}$$

è chiuso e quindi la proiezione sui primi due fattori  $q: Z \rightarrow X_e \times \mathbb{P}(V^\vee)$  è un morfismo proiettivo. Per definizione  $D_X$  è l'insieme dei punti  $(x, [\alpha])$  tali che la fibra  $q^{-1}(x, [\alpha])$  ha dimensione  $\geq n$  ed è quindi chiuso. Ogni fibra della proiezione  $p_1: D_X \rightarrow X_e$  è isomorfa ad un  $\mathbb{P}^{N-n-1}$  e quindi per il Teorema 10.6.5  $D_X$  è irriducibile di dimensione  $N - 1$ .  $\square$

**Definizione 11.5.2.** Nelle notazioni precedenti, la varietà duale di  $X$  è data da

$$X^\vee = p_2(\overline{D_X}) = \overline{p_2(D_X)} \subset \mathbb{P}(V^\vee)$$

dove  $p_2: \mathbb{P}(V) \times \mathbb{P}(V^\vee) \rightarrow \mathbb{P}(V^\vee)$  è la proiezione sul secondo fattore e  $\overline{D_X}$  è la chiusura di  $D_X$  in  $\mathbb{P}(V) \times \mathbb{P}(V^\vee)$ .

Chiaramente  $X^\vee$  è una varietà irriducibile di dimensione  $\leq N - 1$ . Il numero naturale  $\delta(X) = N - 1 - \dim X^\vee$  si dice **difetto** o **deficienza**. Per il principio di Plücker-Clebsch, vale  $\delta(X) \geq k$  se e solo se per ogni  $x \in X_e$  ed ogni iperpiano  $H \supset \mathbb{T}_x X$  si ha

$$\dim_x \{y \in X_e \mid \mathbb{T}_y X \subset H\} \geq k.$$

**Definizione 11.5.3.** La **Classe** di una varietà proiettiva  $X$  è uguale al grado di  $X^\vee$  se  $X^\vee$  è una ipersuperficie e 0 altrimenti.

*Esempio 11.5.4.* Sia  $X \subset \mathbb{P}^N$  la curva normale razionale di grado  $N$ , cioè l'immagine della  $N$ -esima immersione di Veronese

$$\phi: \mathbb{P}^1 \rightarrow \mathbb{P}^N, \quad [t_0, t_1] \mapsto [t_0^N, t_0^{N-1}t_1, \dots, t_1^N].$$

Un iperpiano di equazione  $\sum \alpha_i x_i = 0$  è tangente a  $X$  in  $\phi([a_0, a_1])$  se e solo se la forma binaria  $\sum \alpha_i t_0^i t_1^{N-i}$  ha una radice multipla in  $[a_0, a_1]$  e quindi  $X^\vee = V(\Delta)$ , dove  $\Delta(\alpha_0, \dots, \alpha_N)$  è il discriminante. Ne consegue che la classe di  $X$  è  $2N - 2$ .

**Teorema 11.5.5 (Teorema di dualità).** Per ogni varietà proiettiva  $X \subset \mathbb{P}(V)$  vale  $\overline{D_X} = \overline{D_{X^\vee}}$  e quindi  $X = X^{\vee\vee}$ .

*Dimostrazione.* Convien lavorare con i coni affini anziché con le varietà proiettive, sia dunque

$$V_X = \{(x, \alpha) \in (C(X_e) - 0) \times (V^\vee - 0) \mid \langle \alpha, T_x C(X) \rangle = 0\}$$

e dimostriamo che esiste un sottoinsieme non vuoto  $U \subset V_X \cap V_{X^\vee}$  che è aperto in  $V_X$ . Infatti la proiezione di  $U$  in  $D_X$  sarà ancora un aperto ed essendo  $D_X$  irriducibile si avrà  $\overline{D_X} = \overline{U} \subset \overline{D_{X^\vee}}$  e per ragioni di dimensione  $\overline{D_X} = \overline{D_{X^\vee}}$ . Per il Teorema di Bertini-Sard esiste un aperto non vuoto  $U \subset V_X \cap p_2^{-1}(C(X_e^\vee))$  tale che il differenziale della

proiezione  $p_2: V_X \rightarrow C(X_e^\vee)$  è surgettivo. Sia  $(x, \alpha) \in U$  e mostriamo che  $(x, \alpha) \in V_{X^\vee}$ , cioè che  $\langle x, T_\alpha C(X^\vee) \rangle = 0$ ; preso un qualsiasi vettore tangente  $\beta \in T_\alpha C(X^\vee)$  esiste un sollevamento  $(v, \beta) \in T_{(x, \alpha)} U$ . Dato che  $U \subset V_X$  vale  $\langle v, \alpha \rangle = 0$  e, siccome  $U$  è contenuto nel fibrato tautologico  $\{(y, \gamma) \mid \langle y, \gamma \rangle = 0\}$ , vale  $\langle x + tv, \alpha + t\beta \rangle = O(t^2)$  e quindi  $\langle x, \beta \rangle = 0$ .  $\square$

**Corollario 11.5.6.** *Sia  $C$  una curva piana irriducibile di grado  $> 1$ . Allora esiste un sottoinsieme finito  $S \subset C$  tale che ogni  $p \in C - S$  è liscio con tangente semplice, cioè  $\nu_p(C, \mathbb{T}_p C) = 2$  e  $\nu_q(C, \mathbb{T}_p C) \leq 1$  per ogni  $q \neq p$ . (vedi Esercizio 5.43).*

*Dimostrazione.* Siano  $\pi_1: \overline{D_C} = \overline{D_{C^\vee}} \rightarrow C$ ,  $\pi_2: \overline{D_C} = \overline{D_{C^\vee}} \rightarrow C^\vee$ . Sia  $U \subset C_e^\vee$  un aperto tale che  $\pi_2: \pi_2^{-1}(U) \rightarrow U$  è bigettiva e  $\pi_1: \pi_2^{-1}(U) \rightarrow C$  iniettiva. A meno di restringere  $U$  possiamo supporre che nessuna retta passante per i punti singolari di  $C$  appartenga ad  $U$ . Poniamo  $S$  come l'unione dei punti singolari di  $C$ , dei flessi di  $C$  (che sono finiti per l'Esercizio 6.17) e di  $\pi_1(\overline{D_C} - U)$ . Se  $p \in S$  allora  $\nu_p(C, \mathbb{T}_p C) = 2$ ; inoltre  $(p, \mathbb{T}_p C) \in U$  e quindi se  $q \in C$  è un punto liscio e  $\nu_q(C, \mathbb{T}_p C) \geq 2$  allora  $(q, \mathbb{T}_p C) \in U$  e dunque  $q = p$ .  $\square$

**Esercizi**

**11.15.** Mostrare che la classe è un attributo delle varietà proiettive  $X \subset \mathbb{P}^N$  invariante per proiezione generica su sottospazi  $\mathbb{P}^m \subset \mathbb{P}^N$ ,  $m > \dim X$ .

**11.16 (Varietà determinanti).** Sia  $M(n, m)$  lo spazio vettoriale delle matrici  $n \times m$  a coefficienti in un campo algebricamente chiuso  $\mathbb{K}$ . Per ogni intero positivo  $k$  denotiamo con  $M_k \subset M(n, m)$  il sottoinsieme delle matrici di rango  $\leq k$ . Assumiamo per fissare le idee che  $n \leq m$  (in caso contrario sarà sufficiente trasporre) e consideriamo esclusivamente interi  $0 < k < n$ . È ovvio che, essendo  $M_k$  definito dall'annullarsi di tutti i minori di ordine  $k + 1$ ,  $M_k$  è un chiuso affine.

1) Dimostrare che

$$Z = \{(H, A) \in G(k, \mathbb{K}^n) \times M(n, m) \mid \text{Im } A \subset H\}$$

è un chiuso irriducibile di dimensione  $k(n + m - k)$ .

2) La proiezione sul secondo fattore  $p: Z \rightarrow M(n, m)$  ha come immagine  $M_k$  e, se  $\text{rg}(A) = h \leq k$  esiste una bigezione naturale tra  $p^{-1}(A)$  e  $G(k - h, \mathbb{K}^{n-h})$ . Dedurre che  $M_k$  è una varietà irriducibile di dimensione  $k(n + m - k)$  (e quindi di codimensione  $(n - k)(m - k)$ ).

3) Sia  $U \subset M_k$  l'aperto dei punti lisci. Provare che  $M_k - M_{k-1} \subset U$ . (Sugg.:  $U$  non è vuoto ed esiste un'azione naturale di  $\text{GL}(n) \times \text{GL}(m)$  su  $M_k$ .)

4) Sia  $A \in M_k - M_{k-1}$  una matrice di rango  $k$  e sia  $B \in M(n, m)$  tale che  $B(\text{Ker}(A)) = 0$  oppure  $\text{Im}(B) \subset \text{Im } A$ . Dimostrare che  $A + tB \in M_k$  per ogni  $t \in \mathbb{K}$  e dedurne che

$$T_A M_k = \{B \in M(n, m) \mid B(\text{Ker}(A)) \subset \text{Im}(A)\}.$$

5) Se  $A \in M_{k-1}$ , provare che  $T_A M_k = M(n, m)$  e dedurne che  $M_k - M_{k-1}$  è aperto dei punti lisci di  $M_k$ .

6) L'accoppiamento di dualità  $\langle A, B \rangle = \text{trace}(A^T B) = \sum_{i,j} A_{ij} B_{ij}$  permette di identificare  $M(n, m)$  con il suo duale. Sia  $A \in M(n, m)$  una matrice di rango  $k$ . Dimostrare che  $T_A M_k^\perp \subset M_{n-k}$  e che esiste  $B \in M_{n-k}$  tale che  $A \in T_B M_{n-k}^\perp$ .

7) Dedurre dal punto 6) che  $\mathbb{P}(M_k)^\vee = \mathbb{P}(M_{n-k})$ .

8) Calcolare la classe delle varietà di Segre  $\mathbb{P}^{n-1} \times \mathbb{P}^{m-1} \subset \mathbb{P}^{nm-1}$ .

**11.17.** Mostrare che il teorema di dualità fallisce se la caratteristica del campo è positiva. (Sugg.: in caratteristica  $p > 0$  si consideri una ipersuperficie proiettiva di equazione  $x_0^p = F(x_1, \dots, x_N)$ .)

### 11.6 Esercizi complementari

**11.18.** Sia  $Y \subset M(n, s, \mathbb{K}) = \mathbb{A}^{sn}$ ,  $s \leq n$ , l'aperto delle matrici di rango massimo  $s$  e per ogni  $A \in Y$  sia  $f(A) \in G(s, \mathbb{K}^n) = X$  il sottospazio generato dai vettori colonna di  $A$ . Provare:

1. L'applicazione  $f: Y \rightarrow X$  è regolare ed aperta.
2.  $f(A) = f(B)$  se e solo se esiste  $C \in GL(s, \mathbb{K})$  tale che  $A = BC$ .
3. Sia  $U \subset X$  aperto, allora  $f^*: \mathcal{O}_X(U) \rightarrow \mathcal{O}_Y(f^{-1}(U))$  è iniettiva ed ha come immagine

$$\begin{aligned} \mathcal{O}_Y(f^{-1}(U))^{\text{GL}(s, \mathbb{K})} = \\ = \{g \in \mathcal{O}_Y(f^{-1}(U)) \mid g(AC) = g(A) \text{ per ogni } (A, C) \in f^{-1}(U) \times \text{GL}(s, \mathbb{K})\}. \end{aligned}$$

**11.19.** Siano  $V$  uno spazio vettoriale e  $H \subset V$  un sottospazio di dimensione  $l$ . Provare che il morfismo naturale  $G(s-l, V/H) \rightarrow G(s, V)$  è regolare.

**11.20.** In alcuni testi scolastici si trova la seguente definizione: dati due punti distinti  $(x, y, z)$ ,  $(x', y', z')$  di una retta  $L \subset \mathbb{A}^3$ , si dicono coordinate Plückeriane di  $L$  i sei numeri:

$$\begin{aligned} \alpha_1 = x' - x, \quad \alpha_2 = y' - y, \quad \alpha_3 = z' - z, \\ p_1 = y'z - z'y, \quad p_2 = z'x - x'z, \quad p_3 = x'y - y'x. \end{aligned}$$

Conciliare questa definizione con quella data nella Sezione 11.1.

**11.21.** (caratteristica  $\neq 2$ ) Provare che i vettori isotropi dell'applicazione quadratica  $\wedge^2 V \rightarrow \wedge^4 V$ ,  $v \mapsto v \wedge v$ , sono tutti e soli i vettori totalmente decomponibili di  $\wedge^2 V$ .

**11.22.** Sia  $X \subset G(s, \mathbb{P}^n) \times G(r, \mathbb{P}^n)$  l'insieme delle coppie  $(V, W)$  tali che  $\dim_{\mathbb{K}} V \cap W \geq h$ . Provare che  $X$  è un chiuso irriducibile e se ne calcoli la dimensione.

**11.23 (Grassmanniane semi-infinita).** Sia  $V = \bigoplus_i \mathbb{K} e_i$  uno spazio vettoriale di dimensione numerabile sul campo  $\mathbb{K}$  con base fissata  $\{e_i \mid i \in \mathbb{Z}\}$  e siano  $x_i: V \rightarrow \mathbb{K}$ , per  $i \in \mathbb{Z}$ , gli operatori lineari tali che  $x_i(e_j) = \delta_{ij}$ . Per ogni intero  $n$  denotiamo con  $V_n = \bigoplus_{i \geq n} \mathbb{K} e_i \subset V$ . Per ogni  $d \in \mathbb{Z}$  ed ogni  $n \geq |d|$  esiste un diagramma commutativo

$$\begin{array}{ccc} G\left(n+d, \frac{V_{-n}}{V_n}\right) & \xhookrightarrow{i} & G\left(n+d+1, \frac{V_{-n-1}}{V_{n+1}}\right) \\ \downarrow P & & \downarrow P \\ \mathbb{P}\left(\wedge^{n+d} \frac{V_{-n}}{V_n}\right) & \xrightarrow{[\wedge e_n]} & \mathbb{P}\left(\wedge^{n+d+1} \frac{V_{-n-1}}{V_{n+1}}\right) \end{array}$$

dove le frecce verticali sono le immersioni di Plücker ed  $i$  è la ovvia inclusione di Grassmanniane. Passando al limite diretto si ottiene

$$G\left(\frac{\infty}{2} + d, V\right) := \lim_n G\left(n+d, \frac{V_{-n}}{V_n}\right) \xrightarrow{P} \mathbb{P}\left(\wedge^{\frac{\infty}{2} + d} V\right) := \mathbb{P}\left(\lim_n \wedge^{n+d} \frac{V_{-n}}{V_n}\right).$$

Provare che:

1.  $P$  è iniettiva.
2.  $V_{-d} \in G\left(\frac{\infty}{2} + d, V\right)$ .
3.  $G\left(\frac{\infty}{2} + d, V\right)$  è in biezione naturale con l'insieme dei sottospazi vettoriali  $H \subset V$  tali che  $V_{-n} \subset H \subset V_n$  e  $\dim_{\mathbb{K}} H/V_n = n+d$  per  $n \gg 0$ .

4.  $\bigwedge^{\frac{\infty}{2}+d} V$  è lo spazio vettoriale che ha come base l'insieme dei “prodotti esterni semi-infiniti”

$$\{e_{i_0} \wedge e_{i_1} \wedge \cdots \wedge e_{i_n} \wedge \cdots \mid i_n < i_{n+1} \text{ e } i_n = n - d \text{ per } n \gg 0\}.$$

Definire in modo sensato gli operatori

$$e_i \wedge: \bigwedge^{\frac{\infty}{2}+d} V \rightarrow \bigwedge^{\frac{\infty}{2}+d+1} V, \quad x_i \lrcorner: \bigwedge^{\frac{\infty}{2}+d} V \rightarrow \bigwedge^{\frac{\infty}{2}+d-1} V$$

e provare che l'immagine di  $P$  è il proiettivizzato dell'insieme dei vettori  $w \in \bigwedge^{\frac{\infty}{2}+d} V$  tali che

$$\sum_{i \in \mathbb{Z}} (e_i \wedge w) \otimes (x_i \lrcorner w) = 0.$$

**11.24.** (caratteristica  $\neq 2, 3$ ) Verificare, anche con l'ausilio del calcolatore, che i 10 determinanti minori distinti di ordine 3 della matrice simmetrica

$$\begin{pmatrix} x & y & z & x \\ y & x & y & z \\ z & y & x & y \\ x & z & y & 0 \end{pmatrix}$$

formano una base dello spazio vettoriale dei polinomi omogenei di grado 3 nelle variabili  $x, y, z$ . (Ricchi premi a chi trova una dimostrazione semplice ed elegante di questo fatto: nel caso scrivetemi)

**11.25 (Hesse, 1853, \*\*).** In questo lungo esercizio esaminiamo un diverso approccio alle 28 bitangenti alla quartica generica piana che mette in risalto il fatto che  $28 = \binom{8}{2}$

anziché  $28 = 27 + 1$ . Si lavora su di un campo algebricamente chiuso di caratteristica  $\neq 2, 3$ . Sia  $V \cong \mathbb{P}^2$  una rete generica di quadriche di  $\mathbb{P}^3$  e denotiamo con  $C \subset V$  il luogo discriminante delle quadriche singolari. Provare:

- $V$  non contiene quadriche riducibili. (Sugg.: lo spazio delle quadriche di  $\mathbb{P}^3$  ha dimensione 9 mentre quello delle quadriche formate da due piani ha dimensione 6.)
- Si assuma come evidente che  $V$  ha esattamente 8 punti base  $p_1, \dots, p_8$  e che in ogni punto  $p_i$  non esistano vettori non nulli tangenti ad ogni quadrica della rete; provare che qualsivoglia quattro dei punti  $p_1, \dots, p_8$  non sono contenuti in alcun piano e quindi, a maggior ragione, qualsivoglia tre non sono allineati.
- Mostrare che ogni quadrica irriducibile singolare è un cono quadrico, cioè il cono proiettivo di una conica piana liscia.
- Sia  $Q \in V$  un cono quadrico e  $L \subset V$  una retta passante per  $Q$ . Provare che  $L$  è tangente a  $C$  in  $Q$  se e solo se il vertice di  $Q$  è un punto base del fascio di quadriche  $L$ . Dedurre che  $C$  è liscia e che, dati due coni quadrici  $Q_1, Q_2 \in V$ , la retta  $Q_1 + Q_2$  è bitangente a  $C$  se e solo se il vertice di  $Q_1$  appartiene a  $Q_2$  e viceversa.
- Dimostrare che la generica quartica piana si ottiene come discriminante di una generica rete di quadriche; in particolare  $C$  non contiene iperflessi (Sugg.: interpretare la matrice dell'Esercizio 11.24 come una rete di quadriche e provare la surgettività del differenziale).
- Sia  $L_{ij} \subset V$  l'insieme delle quadriche di  $V$  contenenti la retta  $p_i + p_j$ ; provare che  $L_{ij}$  è una retta bitangente a  $C$  e che  $L_{ij} = L_{hk}$  se e solo se  $p_i + p_j = p_h + p_k$ . (Sugg.: è facile dimostrare che  $L_{ij}$  è una retta, sia  $Q \in L_{ij}$  cono quadrico, necessariamente il vertice di  $Q$  è contenuto in  $p_i + p_j$  e quindi nel luogo base del fascio  $L_{ij}$ .)
- Viceversa sia  $L \subset V$  una retta bitangente a  $C$  in  $Q_1, Q_2$ , e  $H \subset \mathbb{P}^3$  la retta contenente i vertici di  $Q_1$  e  $Q_2$ ; provare che  $H$  è contenuta nel luogo base di  $L$  e che quindi  $H = p_i + p_j$



per qualche coppia  $i, j$ .

h) Utilizzare i punti f) e g) per dedurre che  $C$  contiene esattamente  $\binom{8}{2} = 28$  bitangenti.

*Osservazione 11.6.1.* Gli esercizi 11.12 e 11.25 non descrivono il metodo classico di determinazione del numero delle bitangenti ad una quartica liscia. Il metodo più frequentemente usato (in caratteristica 0) è descritto in [Walk1950, p.154] e fa uso del teorema di dualità e delle formule di Plücker.

**11.26 (\*)**. (caratteristica  $\neq 2, 3$ ) Siano  $Q_1, Q_2 \subset \mathbb{P}^3$  coni quadrici tali che il vertice dell'uno sia contenuto nell'altro e tali che la generica quadrica del fascio generato da  $Q_1, Q_2$  sia nonsingolare. Provare che esistono coordinate omogenee su  $\mathbb{P}^3$  nelle quali le equazioni di  $Q_1$  e  $Q_2$  sono rispettivamente  $x_0x_2 = x_1^2$ ,  $x_1x_3 = x_2^2$ . In particolare  $Q_1 \cap Q_2$  è l'unione di una retta e della curva razionale proiettivamente normale di grado 3. (Sugg.: siano  $v_1, v_2$  i vertici di  $Q_1, Q_2$ , provare per prima cosa che  $v_1 \neq v_2$  e che per un piano generico  $H \subset \mathbb{P}^3$  le coniche  $Q_1 \cap H$  e  $Q_2 \cap H$  sono lisce e si intersecano in quattro punti distinti  $p_0 = H \cap (v_1 + v_2)$ ,  $p_1, p_2, p_3$ . Fissato un piano  $H$  come sopra ed una radice terza di  $-1$   $\xi$ , si può prendere un sistema di coordinate omogenee tali che  $v_1 = [0, 0, 0, 1]$ ,  $v_2 = [1, 0, 0, 0]$ ,  $p_1 = [1, -1, 1, -1]$ ,  $p_2 = [1, \xi, \xi^2, -1]$ ,  $p_3 = [1, \xi^2, -\xi, -1]$ ; scrivere adesso le possibili equazioni dei due coni e giocare con cambi di coordinate dei seguenti tre tipi:

1.  $x_1 \mapsto x_2, x_2 \mapsto -x_1$ ,
2.  $x_0 \mapsto x_0 - ax_1 - bx_2$ ,
3.  $x_3 \mapsto x_3 - cx_1 - dx_2$ ,

fino a quando non si arriva alle equazioni cercate.)

**11.27.** (caratteristica 0) Sia  $S \subset \mathbb{P}^3$  una superficie cubica liscia e  $H \subset \mathbb{P}^3$  un piano tale che la cubica piana  $C = H \cdot S$  sia liscia. Sia  $o \in C$  un flesso e si consideri la legge di gruppo di  $C$  avente  $o$  come elemento neutro. Provare che la somma dei 27 punti di intersezione di  $C$  con le 27 rette in  $S$  è uguale a  $o$ .

**11.28 (\*)**. Sia  $f \in \mathbb{K}[x_1, \dots, x_n]$  un polinomio omogeneo non nullo di grado  $d \geq 2n - 3$ . Provare che esiste  $g \in \mathbb{K}[x_1, \dots, x_n]$  di grado  $< d$  tale che l'ipersuperficie affine  $V(f - g)$  contiene al più un numero finito di rette. (Sugg.: sia  $V \subset \mathbb{K}[x_1, \dots, x_n]$  lo spazio vettoriale dei polinomi di grado  $< d$  e, per ogni  $i = 1, \dots, n$  sia  $Y_i \subset V$  il sottoinsieme dei  $g$  tali che  $V(f - g)$  contiene infinite rette di equazione  $x_j = a_jx_i + b_j$ ,  $j \neq i$ . Provare che  $Y_i$  è costruibile e contenuto in un chiuso proprio.)

**11.29 (\*)**. Sia  $U \subset \mathbb{P}^{19}$  l'aperto delle ipersuperfici cubiche lisce di  $\mathbb{P}^3$  e sia  $X \subset U \times G(1, \mathbb{P}^3)$  l'insieme delle coppie  $(S, L)$  tali che  $L \subset S$ . Provare che  $X$  è una varietà liscia e che la proiezione  $X \rightarrow U$  ha il differenziale bigettivo in ogni punto. (Sugg.: sia  $L = \{x_2 = x_3 = 0\}$  e  $S = \{x_2F_2 + x_3F_3 = 0\}$ . Mostrare che  $S$  non ha punti singolari in  $L$  se e solo se ogni polinomio  $G \in \mathbb{K}[x_0, x_1]$  omogeneo di terzo grado appartiene all'ideale generato da  $F_2(x_0, x_1, 0, 0)$  e  $F_3(x_0, x_1, 0, 0)$ .)

**11.30.** Sia  $\mathbb{K}$  algebricamente chiuso di caratteristica  $\neq 3$ . Provare che la cubica piana  $\{x_0^3 + x_1^3 + x_2^3 = 0\}$  è liscia e possiede esattamente nove flessi, ottenuti intersecando con la cubica  $\{x_0x_1x_2 = 0\}$ . Trovare le rette contenute nella superficie cubica di equazione  $\{x_0^3 + x_1^3 + x_2^3 + x_3^3 = 0\}$  e verificare che sono 27 anche in caratteristica 2.

**11.31.** (caratteristica 0) Sia  $V$  un sistema lineare di curve piane di grado  $d$ . Dimostrare che l'insieme delle curve di  $V$  che hanno al più nodi come singolarità è un aperto di Zariski.

**11.32.** (caratteristica 0) Sia  $F \in \mathbb{K}[x_0, \dots, x_n]$  un polinomio omogeneo irriducibile di grado  $\geq 2$ . Provare che se  $V(F) \subset \mathbb{P}^n$  è una ipersuperficie liscia, allora il determinante Hessiano  $H(F) = |\partial^2 F / \partial x_i \partial x_j|$  non è identicamente nullo.

*Osservazione 11.6.2.* È quasi ovvio che, se a meno di un cambio lineare di coordinate, un polinomio omogeneo irriducibile  $F \in \mathbb{K}[x_0, \dots, x_n]$  non dipende da  $x_0$ , allora il suo determinante Hessiano è identicamente nullo. La validità del viceversa rappresenta una vecchia congettura di Hesse che si è dimostrata vera per  $n \leq 3$  e falsa per  $n \geq 4$ : il più semplice controesempio è dato da un polinomio irriducibile  $F \in \mathbb{K}[x_0, \dots, x_4]$  tale che  $V(F) \subset \mathbb{P}^4$  è una proiezione generica della varietà di Segre  $\mathbb{P}^2 \times \mathbb{P}^1 \subset \mathbb{P}^5$ .

**11.33.** Sia  $X \subset \mathbb{P}^n$  una varietà irriducibile non degenera (cioè non contenuta in alcun iperpiano) e sia  $C \subset (\mathbb{P}^n)^\vee$  una curva irriducibile. Provare che se per ogni  $x \in X$  l'iperpiano  $x^\vee$  interseca  $C$  in un unico punto, allora  $C$  è una retta oppure  $C \subset X^\vee$ .

**11.34.** Siano  $0 \leq d \leq n$  interi fissati e denotiamo con  $X_{d,n} \subset M(n, n)$  il sottoinsieme delle matrici il cui polinomio minimo ha grado al più  $d$ .

1. Provare che  $X_{d,n}$  è un chiuso affine.
2. Provare che  $X_{n-1,n}$  è irriducibile e se ne calcoli la dimensione (Sugg.:  $A \in X_{n-1,n}$  se e solo se  $A - tI$  ha rango  $\leq n - 2$  per qualche  $t \in \mathbb{K}$ ).
3. Mostrare che il numero di componenti irriducibili di  $X_{d,m}$  non è inferiore al coefficiente di  $t^{n-d}$  nello sviluppo in serie di

$$\prod_{i=1}^d \frac{1}{1-t^i}.$$

Dedurre che  $X_{d,n}$  è irriducibile se e solo se  $d = 0, 1, n - 1, n$ . (Sugg.: considerare per ogni multindice  $(i_1, \dots, i_d)$  di peso  $n - d$  il sottoinsieme delle matrici il cui polinomio caratteristico ha la forma  $(t - a_1)^{i_d+1} (t - a_2)^{i_d+i_{d-1}+1} \dots (t - a_d)^{i_d+\dots+i_1+1}$ .)

**11.35.** Siano  $V \subset X \subset \mathbb{K}^N$  due chiusi affini, con  $V$  sottospazio vettoriale di dimensione  $k$  e sia  $x \in V$  un punto tale che  $\dim_x X = \dim T_x X = n + k$ . Provare che per ogni iperpiano  $H \subset \mathbb{K}^N$  contenente  $T_x X$  vale

$$\dim_x \{y \in V \mid T_y X \subset H\} \geq k - n.$$

Dedurre che, se per una varietà proiettiva  $X \subset \mathbb{P}^N$  di dimensione  $n + k$  l'insieme

$$U = \bigcup_{H \subset X} H, \quad H \in G(k, \mathbb{P}^N)$$

è denso in  $X$ , allora  $\dim X^\vee \leq N - 1 + n - k$ .

## Piccolo bestiario di morfismi

Tutte le varietà algebriche saranno considerate su di un campo algebricamente chiuso fissato  $\mathbb{K}$ . Campi generici saranno denotati con le lettere  $K, F, L, E$  ecc. e, salvo avviso contrario, saranno supposti infiniti.

Obiettivo di questo capitolo è definire e studiare alcune classi interessanti di morfismi di varietà quasiproiettive. Nel Capitolo 10 abbiamo già incontrato la classe dei morfismi proiettivi, la cui importanza è risultata chiara dagli esempi visti. Qui introdurremo altre sottoclassi di morfismi regolari. Morfismi affini, finiti, quasifiniti, genericamente finiti, birazionali ecc. entreranno a far parte del bestiario. Fermo restando che sono gli esempi concreti a stabilire quali aggregati di morfismi sono interessanti e quali no, si può dire che, di norma, ogni famiglia “interessante” contiene gli isomorfismi, è chiusa per composizione e possiede la proprietà locale. Quello che intendiamo per proprietà locale lo spiegheremo nella Sezione 12.1.

### 12.1 Classi di morfismi e proprietà locale

Chiameremo *classe* di morfismi di varietà quasiproiettive una qualsiasi famiglia  $\mathcal{C}$  di morfismi regolari di varietà quasiproiettive che contiene tutti gli isomorfismi ed è chiusa per composizione con isomorfismi: ciò significa che per ogni diagramma commutativo di morfismi regolari di varietà quasiproiettive

$$\begin{array}{ccc} W & \xrightarrow{\alpha} & X \\ \downarrow g & & \downarrow f \\ Z & \xrightarrow{\beta} & Y \end{array}$$

con  $\alpha$  e  $\beta$  isomorfismi, vale  $f \in \mathcal{C}$  se e soltanto se  $g \in \mathcal{C}$ . Ad esempio, è una classe la famiglia di tutti i morfismi regolari iniettivi tra varietà quasiproiettive.

**Definizione 12.1.1.** Diremo che una classe  $\mathcal{C}$  di morfismi regolari di varietà quasiproiettive è chiusa per composizione se dati due morfismi  $X \xrightarrow{f} Y \xrightarrow{g} Z$  in  $\mathcal{C}$ , anche la loro composizione appartiene a  $\mathcal{C}$ .

**Definizione 12.1.2.** Diremo che una classe  $\mathcal{C}$  di morfismi regolari di varietà quasiproiettive ha la **proprietà locale** quando accade che:

1. Se  $f: X \rightarrow Y$  è un morfismo in  $\mathcal{C}$  e  $U \subset Y$  è un aperto, allora anche la restrizione  $f: f^{-1}(U) \rightarrow U$  appartiene a  $\mathcal{C}$ .

2. Se  $f: X \rightarrow Y$  è un morfismo regolare di varietà quasiproiettive e  $Y = \cup U_i$  è un ricoprimento aperto tale che  $f: f^{-1}(U_i) \rightarrow U_i$  appartiene a  $\mathcal{C}$  per ogni  $i$ , allora anche  $f: X \rightarrow Y$  appartiene a  $\mathcal{C}$ .

Ad esempio, sono chiuse per composizione e possiedono la proprietà locale le seguenti classi di morfismi:

1. I morfismi iniettivi ed i morfismi surgettivi.
2. I morfismi chiusi ed i morfismi aperti.
3. I morfismi proiettivi.
4. I morfismi dominanti.
5. Gli isomorfismi.
6. I morfismi non ramificati (vedi Definizione 12.1.3).

Ricordiamo (Definizione 10.3.11) che un morfismo si dice dominante se ha immagine densa nel codominio.

**Definizione 12.1.3.** *Un morfismo regolare  $\phi: X \rightarrow Y$  tra varietà quasiproiettive si dice **ramificato** in un punto  $x \in X$  se il differenziale  $d\phi: T_x X \rightarrow T_{\phi(x)} Y$  non è iniettivo; in tal caso  $x$  è detto punto di ramificazione e  $\phi(x)$  punto di diramazione. Un morfismo è non ramificato se non possiede punti di ramificazione.*

Osserviamo che, per il Lemma 11.4.2 l'insieme dei punti di ramificazione è un chiuso.

Se  $\mathcal{C}$  è una classe di morfismi e  $Y$  è una varietà quasiproiettiva, denotiamo con  $\mathcal{C}(Y) \subset \mathcal{C}$  la sottofamiglia dei morfismi della classe che hanno  $Y$  per codominio. Notiamo che, data una classe  $\mathcal{C}$ , le famiglie  $\mathcal{C}(Y)$  hanno le seguenti proprietà:

*Property 12.1.4.* L'identità su  $Y$  appartiene a  $\mathcal{C}(Y)$  e per ogni diagramma commutativo di morfismi regolari di varietà quasiproiettive

$$\begin{array}{ccc} W & \xrightarrow{\alpha} & X \\ \downarrow g & & \downarrow f \\ Z & \xrightarrow{\beta} & Y \end{array}$$

con  $\alpha$  e  $\beta$  isomorfismi, vale  $f \in \mathcal{C}(Y)$  se e soltanto se  $g \in \mathcal{C}(Z)$ .

Viceversa, dare una classe di morfismi  $\mathcal{C}$  equivale a dare, per ogni varietà quasiproiettiva  $Y$  una famiglia  $\mathcal{C}(Y)$  contenente l'identità e tale che la Proprietà 12.1.4 sia soddisfatta.

Dato che ogni varietà possiede una base di aperti affini, ogni classe  $\mathcal{C}$  di morfismi con la proprietà locale è determinata dei morfismi della classe che hanno come codominio varietà affini.

**Lemma 12.1.5.** *Sia data per ogni varietà affine  $Y$  una sottofamiglia  $C(Y)$  dei morfismi regolari di varietà quasiproiettive che hanno come codominio  $Y$  e che soddisfa la Proprietà 12.1.4 ogniqualevolta  $Y$  e  $Z$  sono varietà affini. Definiamo  $\mathcal{C}$  come la famiglia dei morfismi regolari di varietà proiettive  $f: X \rightarrow Y$  per i quali esiste un ricoprimento affine  $Y = \cup Y_i$  tale che la restrizione  $f: f^{-1}(Y_i) \rightarrow Y_i$  appartiene a  $C(Y_i)$  per ogni  $i$ . Allora  $\mathcal{C}$  è una classe e  $C(Y) \subset \mathcal{C}(Y)$  per ogni varietà affine  $Y$ .*

*Dimostrazione.* Banale. □

Diremo che le famiglie  $C(Y)$ , per  $Y$  affine, generano la classe  $\mathcal{C}$  se  $\mathcal{C}$  si costruisce come nel Lemma 12.1.5.

**Proposizione 12.1.6.** *Sia data per ogni varietà affine  $Y$  una sottofamiglia  $C(Y)$  dei morfismi regolari di varietà quasiproiettive che hanno come codominio  $Y$  e supponiamo che la Proprietà 12.1.4 sia soddisfatta ogniqualevolta  $Y$  e  $Z$  sono varietà affini. Se  $\phi \in C(Y)$  e  $U \subset Y$  è un aperto affine, scriveremo  $\phi \in C(U)$  se la restrizione  $\phi: \phi^{-1}(U) \rightarrow U$  appartiene a  $C(U)$ . Allora la classe  $\mathcal{C}$ , definita come nel Lemma 12.1.5, ha la proprietà locale se e solo se per ogni varietà affine  $Y$  le seguenti condizioni sono soddisfatte:*

1. *Se  $\phi: X \rightarrow Y$  appartiene a  $C(Y)$ , allora per ogni  $f \in \mathbb{K}[Y]$  vale  $\phi \in C(Y_f)$ .*
2. *Se  $\phi: X \rightarrow Y$  è regolare,  $Y = \cup_i Y_{f_i}$  per opportuni  $f_i \in \mathbb{K}[Y]$  e  $\phi \in C(Y_{f_i})$  per ogni  $i$ , allora anche  $\phi \in C(Y)$ .*

*Inoltre, se tali condizioni sono soddisfatte vale  $\mathcal{C}(Y) = C(Y)$  per ogni varietà affine  $Y$ .*

*Dimostrazione.* Sia  $\phi: X \rightarrow Y$  un morfismo regolare di varietà quasiproiettive. Siano  $V \subset U \subset Y$  aperti affini; assumiamo che  $\phi \in C(U)$  e mostriamo che  $\phi \in C(V)$ . Siano  $f_1, \dots, f_n \in \mathbb{K}[U]$  tali che  $V = \cup_i U_{f_i}$ ; per il punto 1)  $\phi \in C(U_{f_i})$  per ogni  $i$ . Dato che  $\mathbb{K}[U] \subset \mathbb{K}[V]$ , si ha  $U_{f_i} = V_{f_i}$  e dal punto 2) segue che  $\phi \in C(V)$ . Sia  $V \subset Y$  un aperto affine e sia  $V = \cup_i U_i$  un ricoprimento affine tale che  $\phi \in C(U_i)$  per ogni  $i$ . Possiamo trovare un ricoprimento affine  $V = \cup_i V_{f_i}$  tale che ogni  $V_{f_i}$  è contenuto in qualche  $U_j$ . Per il punto 2)  $\phi \in C(V)$ . Se  $A \subset Y$  è un aperto, scegliamo un ricoprimento affine  $A = \cup_i U_i$ , e stabiliamo che  $\phi: \phi^{-1}(A) \rightarrow A$  appartiene alla classe  $\mathcal{C}$  se e solo se  $\phi \in C(U_i)$  per ogni  $i$ . Se  $A = \cup_j V_j$  è un altro ricoprimento affine, possiamo trovare un raffinamento in aperti affini  $A = \cup_{ijk} W_{ijk}$  tale che  $W_{ijk} \subset U_i \cap V_j$  per ogni  $i, j, k$ ; questo prova che la classe  $\mathcal{C}$  è ben definita e che la definizione di  $\mathcal{C}$  coincide con quella data nel Lemma 12.1.5. Se  $A = \cup_i A_i$  è un ricoprimento aperto, basta considerare, per ogni  $i$ , un ricoprimento di  $A_i$  fatto con aperti affini per mostrare che la classe  $\mathcal{C}$  ha la proprietà locale.  $\square$

## 12.2 Morfismi affini e finiti

**Definizione 12.2.1.** *Siano  $Y$  una varietà affine e  $X$  una varietà quasiproiettiva. Un morfismo  $\phi: X \rightarrow Y$  si dice:*

1. **affine:** *se  $X$  è affine.*
2. **finito sull'immagine:** *se  $X$  è affine e  $\mathbb{K}[X]$  è finitamente generato come  $\mathbb{K}[Y]$ -modulo.*
3. **finito:** *se è surgettivo e finito sull'immagine.*

Il nostro prossimo obiettivo è quello di dimostrare che le classi di morfismi affini, finiti sull'immagine e finiti con codominio affine generano classi di morfismi chiuse per composizione e con la proprietà locale.

**Lemma 12.2.2.** *Sia  $A \rightarrow B$  un omomorfismo di anelli e siano  $f_1, \dots, f_n \in A$  tali che  $1 \in (f_1, \dots, f_n)$ . Allora  $B$  è finitamente generato come  $A$ -algebra (risp.: come  $A$ -modulo) se e solo se per ogni  $i = 1, \dots, n$ , l'anello  $B_{f_i}$  è finitamente generato come  $A_{f_i}$ -algebra (risp.: come  $A_{f_i}$ -modulo).*

*Dimostrazione.* Se  $b_1, \dots, b_s$  generano  $B$  come  $A$ -algebra (risp.: come  $A$ -modulo), allora  $b_1, \dots, b_s$  generano  $B_{f_i}$  come  $A_{f_i}$ -algebra (risp.: come  $A_{f_i}$ -modulo).

Viceversa, se ogni  $B_{f_i}$  è una  $A_{f_i}$ -algebra finitamente generata, possiamo trovare un sottoinsieme finito  $\{b_{ij}\} \subset B$ , tale che, per ogni  $i$ ,  $B_{f_i}$  è generato da  $b_{i1}, b_{i2}, \dots$ . Dunque per ogni  $b \in B$  esistono interi  $m_1, \dots, m_n$  e relazioni

$$f_i^{m_i} (b - \sum_h \hat{a}_{i,h} p_{i,h}(b_{i1}, b_{i2}, \dots)) = 0, \quad \hat{a}_{i,h} \in A_{f_i}, \quad p_{i,h} \in \mathbb{Z}[x_1, x_2, \dots].$$

Aumentando eventualmente  $m_i$  in modo tale che  $a_{i,h} = f_i^{m_i} \hat{a}_{i,h} \in A$  per ogni  $i, h$ , le relazioni precedenti diventano

$$f_i^{m_i} b = \sum_h a_{i,h} p_{i,h}(b_{i1}, b_{i2}, \dots), \quad a_{i,h} \in A, \quad p_{i,h} \in \mathbb{Z}[x_1, x_2, \dots].$$

Se  $\sum_i g_i f_i^{m_i} = 1$  è una partizione di 1, si ha

$$b = \sum_i g_i f_i^{m_i} b = \sum_{i,h} g_i a_{i,h} p_{i,h}(b_{i1}, b_{i2}, \dots)$$

e quindi i  $b_{ij}$  generano  $B$  come  $A$ -algebra. Se ogni  $B_{f_i}$  è un  $A_{f_i}$ -modulo finitamente generato, si ripete la dimostrazione considerando i polinomi  $p_{i,h}$  omogenei di grado 1.  $\square$

**Lemma 12.2.3.** *Sia  $X$  una varietà quasiproiettiva,  $f \in \mathcal{O}_X(X)$ . Allora il morfismo naturale  $\alpha: \mathcal{O}_X(X)_f \rightarrow \mathcal{O}_X(X_f) = \mathcal{O}_{X_f}(X_f)$  è un isomorfismo (per definizione  $X_f = \{x \in X \mid f(x) \neq 0\}$ ).*

*Dimostrazione.* Proviamo prima che  $\alpha$  è iniettivo. Se  $g/f^n$  è nullo in  $X_f$  allora la funzione  $g \in \mathcal{O}_X(X)$  si annulla su tutti i punti di  $X_f$  e quindi  $gf$  si annulla identicamente su  $X$  e  $g/f^n = gf/f^{n+1} = 0$ . Mostriamo adesso la surgettività. Sia  $g$  una funzione regolare su  $X_f$ . Dato che  $X$  è ricoperto da un numero finito di aperti affini basta dimostrare che per ogni aperto affine  $U \subset X$  esiste un intero  $n > 0$  tale che la funzione

$$h(x) = \begin{cases} 0 & \text{se } f(x) = 0 \\ gf^n(x) & \text{se } f(x) \neq 0 \end{cases}$$

è regolare su  $U$ . Se  $f$  è identicamente nulla su  $U$  l'asserzione è ovvia, altrimenti, siccome  $f$  è regolare su  $U$  si ha  $X_f \cap U = U_f$  e quindi la restrizione di  $g$  a  $U$  ha la forma  $h/f^{n-1}$  per qualche  $h \in \mathbb{K}[U]$ ,  $n > 0$ .  $\square$

**Teorema 12.2.4.** *Le classi dei morfismi affini, finiti sull'immagine e finiti soddisfano le condizioni della Proposizione 12.1.6 e quindi generano classi con la proprietà locale.*

*Dimostrazione.* Poiché la surgettività è chiaramente una proprietà locale, basta dimostrare che le classi dei morfismi affini e finiti sull'immagine soddisfano le due condizioni della Proposizione 12.1.6. Se  $\phi: X \rightarrow Y$  è un morfismo di varietà affini, allora per ogni  $f \in \mathbb{K}[Y]$  si ha  $\phi^{-1}(Y_f) = X_{\phi^* f}$  che è affine. Inoltre se  $\mathbb{K}[X]$  è finitamente generato come  $\mathbb{K}[Y]$  modulo, allora  $\mathbb{K}[X_{\phi^* f}] = \mathbb{K}[X]_{\phi^* f}$  è finitamente generato come  $\mathbb{K}[Y_f] = \mathbb{K}[Y]_f$ -modulo. Sia  $Y$  affine e  $Y = \cup_i Y_{f_i}$  è un ricoprimento affine, a meno di passare ad un sottoricoprimento finito possiamo supporre  $Y = Y_{f_1} \cup \dots \cup Y_{f_n}$  e quindi per il teorema degli zeri si ha  $1 \in (f_1, \dots, f_n)$ . Se ogni aperto  $X_{\phi^* f_i}$  è affine, allora  $\mathbb{K}[X_{\phi^* f_i}] = \mathcal{O}_X(X)_{\phi^* f_i}$  e per il Lemma 12.2.2, la  $\mathbb{K}[Y]$ -algebra  $\mathcal{O}_X(X)$  è finitamente generata, diciamo da  $g_1, \dots, g_m$ . Consideriamo il morfismo regolare

$$\alpha = (\phi, g_1, \dots, g_m): X \rightarrow Z \subset Y \times \mathbb{A}^m,$$

dove  $Z$  è il chiuso definito dal nucleo di

$$\mathbb{K}[Y][x_1, \dots, x_m] \rightarrow \mathcal{O}_X(X), \quad x_i \mapsto g_i.$$

La varietà  $Z$  è affine e  $\mathbb{K}[Z] = \mathcal{O}_X(X)$ , quindi per ogni indice  $i$  vale  $\mathbb{K}[Z_{f_i}] = \mathcal{O}_X(X)_{\phi^* f_i} = \mathcal{O}_X(X_{\phi^* f_i})$  ed il morfismo  $\alpha$  induce un isomorfismo  $X_{\phi^* f_i} = Z_{f_i}$ . Siccome  $\alpha$  commuta con  $\phi$  e con la proiezione su  $Y$ , si dimostra facilmente che è iniettivo. Dunque  $\alpha$  è bigettiva ed un isomorfismo locale e quindi è un isomorfismo. Per il Lemma 12.2.2, se ogni  $\mathbb{K}[X_{\phi^* f_i}]$  è un  $\mathbb{K}[Y_{f_i}]$ -modulo finitamente generato allora anche  $\mathbb{K}[X]$  è un  $\mathbb{K}[Y]$ -modulo finitamente generato.  $\square$

**Definizione 12.2.5.** *Un morfismo  $\phi: X \rightarrow Y$  tra varietà quasiproiettive si dice:*

1. **affine:** se  $\phi^{-1}(U)$  è affine per ogni aperto affine  $U \subset Y$ .
2. **finito sull'immagine:** se è affine e se per ogni aperto affine  $U \subset Y$ , l'anello  $\mathbb{K}[\phi^{-1}(U)]$  è finitamente generato come  $\mathbb{K}[U]$ -modulo.
3. **finito:** se è surgettivo e finito sull'immagine.

Segue dal Teorema 12.2.4 che le Definizioni 12.2.1 e 12.2.5 sono compatibili, cioè definiscono, per  $Y$  affine le stesse classi di morfismi

La Definizione 12.2.5 individua tre classi di morfismi che contengono l'identità e sono chiuse per composizione. L'unico fatto non banale richiesto è il seguente: se  $A \rightarrow B \rightarrow C$  sono morfismi di anelli,  $B$  è finitamente generato come  $A$ -modulo, e  $C$  è finitamente generato come  $B$ -modulo allora  $C$  è finitamente generato come  $A$ -modulo. Infatti se  $b_1, \dots, b_n$  generano  $B$  su  $A$  e  $c_1, \dots, c_m$  generano  $C$  su  $B$  allora gli  $nm$  prodotti  $b_i c_j$  generano  $C$  come  $A$ -modulo.

**Lemma 12.2.6.** *Siano  $Y$  una varietà affine e  $X \subset Y \times \mathbb{A}^n$  un chiuso. Allora  $\mathbb{K}[X]$  è un  $\mathbb{K}[Y]$ -modulo finitamente generato se e solo se  $X$  è chiuso in  $Y \times \mathbb{P}^n$ .*

*Dimostrazione.* Siano  $u_0, \dots, u_n$  coordinate omogenee su  $\mathbb{P}^n$  tali che  $\mathbb{A}^n$  corrisponda all'aperto  $u_0 \neq 0$  e denotiamo con  $x_i = u_i/u_0$  le coordinate affini su  $\mathbb{A}^n$ . Come  $\mathbb{K}[Y]$ -algebra,  $\mathbb{K}[X]$  è generato dalle funzioni  $x_i$ ; per ogni  $s \geq 0$  denotiamo con  $M_s \subset \mathbb{K}[X]$  il  $\mathbb{K}[Y]$ -sottomodulo generato dai monomi di grado  $\leq s$  in  $x_1, \dots, x_n$ . Se  $\mathbb{K}[X]$  è finitamente generato come  $\mathbb{K}[Y]$ -modulo, allora esiste un intero  $s > 0$  tale che  $M_{s-1} = M_s$  e quindi per ogni  $i = 1, \dots, n$  esiste un polinomio  $P_i \in \mathbb{K}[Y][x_1, \dots, x_n]$  di grado  $< s$  tale che  $x_i^s = P_i(x_1, \dots, x_s)$  in  $\mathbb{K}[X]$ . Se  $Z \subset Y \times \mathbb{P}^n$  è il chiuso definito dalle equazioni

$$u_i^s = u_0^s P_i \left( \frac{u_1}{u_0}, \dots, \frac{u_n}{u_0} \right), \quad i = 1, \dots, n,$$

allora  $Z \cap \{u_0 = 0\} = \emptyset$  e  $Z$  è contenuto in  $Y \times \mathbb{A}^n$ . Dunque  $X$  è chiuso in  $Z$  che a sua volta è chiuso in  $Y \times \mathbb{P}^n$ .

Viceversa, assumiamo  $X$  chiuso in  $Y \times \mathbb{P}^n$  e sia  $I \subset \mathbb{K}[Y][u_0, \dots, u_n]$  l'ideale delle forme omogenee nulle su  $X$ . Dato che  $X \cap \{u_0 = 0\} = \emptyset$ , per il teorema degli zeri esiste  $s > 0$  tale che  $u_i^s \in I + (u_0)$  per ogni  $i = 1, \dots, n$ . Dunque esistono polinomi omogenei  $P_i \in \mathbb{K}[Y][u_0, \dots, u_n]$  di grado  $s-1$  tali che  $u_i^s - u_0 P_i \in I$  per ogni  $i$ . Disomogeneizzando si ha  $x_i^s = P_i(x_1, \dots, x_n)$  in  $\mathbb{K}[X]$  ed un semplice argomento induttivo mostra che  $M_h = M_{h-1}$  per ogni  $h \geq ns$ . Quindi  $\mathbb{K}[X] = \cup M_h = M_{ns-1}$  è finitamente generato come  $\mathbb{K}[Y]$ -modulo.  $\square$

Un'altra classe di morfismi aventi la proprietà locale è quella dei morfismi quasifiniti.

**Definizione 12.2.7.** *Un morfismo di varietà quasiproiettive  $\phi: X \rightarrow Y$  si dice **quasifinito** se per ogni  $y \in Y$  la fibra  $\phi^{-1}(y)$  ha cardinalità finita.*

**Teorema 12.2.8.** *Per un morfismo di varietà quasiproiettive  $\phi: X \rightarrow Y$  le seguenti condizioni sono equivalenti:*

1.  $\phi$  è finito sull'immagine.
2.  $\phi$  è affine e proiettivo.
3.  $\phi$  è quasifinito e proiettivo.

*Dimostrazione.* [1  $\Rightarrow$  2]. Possiamo supporre  $X$  e  $Y$  affini; a meno di sostituire  $X$  con il grafico di  $\phi$  non è restrittivo assumere  $X \subset Y \times \mathbb{A}^n$  e  $\phi$  indotta dalla proiezione. Per il Lemma 12.2.6  $X$  è chiuso in  $\mathbb{P}^n$  e quindi  $\phi$  è proiettivo.

[2  $\Rightarrow$  3] Ogni fibra di  $\phi$  è una varietà che è contemporaneamente affine e proiettiva e quindi ogni sua componente irriducibile deve necessariamente essere un punto.

[3  $\Rightarrow$  1] Sia  $y \in Y$ . A meno di restringere  $Y$  ad un intorno affine di  $y$ , non è restrittivo assumere  $X \subset Y \times \mathbb{P}^n$  chiuso e  $\phi$  indotta dalla proiezione sul primo fattore. Sia  $X_y = \phi^{-1}(y)$  la fibra su  $y$  e siano  $u_0, \dots, u_n$  coordinate omogenee su  $\mathbb{P}^n$  tali che  $X_y \cap \{u_0 = 0\} = \emptyset$ . A meno di restringere  $Y$  ad un intorno ancora più piccolo di  $y$ , possiamo assumere  $X \cap \{u_0 = 0\} = \emptyset$  e quindi  $X$  chiuso in  $Y \times \mathbb{A}^n$ . Per il Lemma 12.2.6  $\mathbb{K}[X]$  è finitamente generato come  $\mathbb{K}[Y]$ -modulo.  $\square$

**Corollario 12.2.9.** *Ogni morfismo finito sull'immagine è chiuso. In particolare un morfismo è finito se e solo se è finito sull'immagine e dominante.*

*Dimostrazione.* I morfismi proiettivi sono chiusi.  $\square$

Siamo adesso in grado di enunciare e dimostrare il teorema di invertibilità locale.

**Teorema 12.2.10.** *Sia  $\phi: X \rightarrow Y$  un morfismo finito e bigettivo di varietà quasiproiettive, e sia  $x \in X$  un punto di non ramificazione. Allora esiste un intorno aperto  $\phi(y) \in U \subset Y$  tale che  $\phi: \phi^{-1}(U) \rightarrow U$  è un isomorfismo. In particolare un morfismo regolare di varietà quasiproiettive è un isomorfismo se e solo se è finito, bigettivo e non ramificato.*

*Dimostrazione.* Non è restrittivo supporre  $X, Y$  affini; denotiamo  $y = \phi(x)$  e con  $\mathfrak{m} \subset \mathbb{K}[Y]$ ,  $\mathfrak{n} \subset \mathbb{K}[X]$  gli ideali massimali delle funzioni regolari nulle in  $y$  e  $x$  rispettivamente. Siccome  $\phi$  è surgettivo  $\phi^*: \mathbb{K}[Y] \rightarrow \mathbb{K}[X]$  è iniettivo e possiamo identificare  $\mathbb{K}[Y]$  con un sottoanello di  $\mathbb{K}[X]$ . Per ipotesi  $\phi$  è finito, quindi  $\mathbb{K}[X]$  è finitamente generato come  $\mathbb{K}[Y]$ -modulo. Inoltre  $\phi$ , essendo chiuso, continuo e bigettivo, è un omeomorfismo. L'ipotesi che  $x$  non sia un punto di ramificazione equivale a dire che l'applicazione

$$\frac{\mathfrak{m}}{\mathfrak{m}^2} \rightarrow \frac{\mathfrak{n}}{\mathfrak{n}^2}$$

è surgettiva, ovvero che  $\mathfrak{m}\mathbb{K}[X] + \mathfrak{n}^2 = \mathfrak{n}$ . Per il lemma di Nakayama 1.7.2 esiste  $f \in \mathfrak{n}$  tale che  $(1 - f)\mathfrak{n} = \mathfrak{m}\mathbb{K}[X]$ . A meno di restringere  $Y$  ad un aperto affine contenente  $y$  e contenuto in  $\phi(X_{1-f})$  possiamo supporre  $1 - f$  invertibile in  $X$  e quindi  $\mathfrak{m}\mathbb{K}[X] = \mathfrak{n}$ . Chiaramente  $\mathbb{K}[Y] + \mathfrak{n} = \mathbb{K}[X]$ , quindi  $\mathbb{K}[Y] + \mathfrak{m}\mathbb{K}[X] = \mathbb{K}[X]$  e per il lemma di Nakayama esiste  $g \in \mathfrak{m}$  tale che  $(1 - g)\mathbb{K}[X] = \mathbb{K}[Y]$ . A meno di sostituire  $Y$  con l'aperto affine  $Y_{1-g}$  possiamo supporre  $1 - g$  invertibile e quindi  $\mathbb{K}[X] = \mathbb{K}[Y]$ .  $\square$

**Definizione 12.2.11.** *Un morfismo di varietà quasiproiettive  $\phi: X \rightarrow Y$  si dice **genericamente finito** se esiste un aperto denso  $U \subset Y$  tale che la restrizione  $\phi: \phi^{-1}(U) \rightarrow U$  è un morfismo finito.*

## Esercizi

**12.1.** Dimostrare che un morfismo di varietà affini  $X \rightarrow Y$  è finito se e solo se il morfismo  $\mathbb{K}[Y] \rightarrow \mathbb{K}[X]$  è iniettivo e  $\mathbb{K}[X]$  è finitamente generato come  $\mathbb{K}[Y]$ -modulo.

**12.2.** Sia  $X \subset \mathbb{A}^3$  l'unione dei tre assi coordinati e  $Y = \{xy(x - y) = 0\} \subset \mathbb{A}^2$ . Mostrare che il morfismo

$$\phi: X \rightarrow Y, \quad \phi(x, y, z) = (x + z, y + z)$$

è finito, bigettivo e ramificato in 0.

**12.3.** Siano  $X = \mathbb{A}^1 - \{1\}$  e  $Y \subset \mathbb{A}^2$  la curva di equazione  $y^2 = x^2(x + 1)$ . Mostrare che il morfismo  $\phi: X \rightarrow Y$ ,  $\phi(t) = (t^2 - 1, t^3 - t)$ , è bigettivo e non ramificato ma non è finito.



**12.4.** In caratteristica 0 si consideri una ipersuperficie proiettiva  $X \subset \mathbb{P}^n$  di equazione  $x_0^d = F(x_1, \dots, x_n)$  e sia  $\pi: X \rightarrow \mathbb{P}^{n-1}$  la proiezione di centro  $[1, 0, \dots, 0]$ . Dimostrare che  $\pi$  è un morfismo finito e determinare il luoghi di ramificazione e diramazione.

**12.5.** Dimostrare che:

1. Ogni morfismo quasifinito dominante è genericamente finito.
2. La classe dei morfismi genericamente finiti è chiusa per composizione e ha la proprietà locale.
3. Ogni morfismo dominante tra varietà irriducibili della stessa dimensione è genericamente finito.

**12.6.** Sia  $X \subset \mathbb{P}^n$  una varietà proiettiva e sia  $\pi: X \rightarrow \mathbb{P}^{n-1}$  la proiezione di centro  $o \notin X$ . Dimostrare che  $\pi$  è un morfismo finito sull'immagine.

## 12.3 Funzioni razionali

La definizione degli anelli locali  $\mathcal{O}_{Z,X}$  data nella Sezione 10.1 per le varietà affini si estende senza variazioni sostanziali alle varietà quasiproiettive; in particolare se  $X$  è una varietà quasiproiettiva irriducibile, il campo  $\mathbb{K}(X)$  delle funzioni razionali su  $X$  si definisce come l'insieme delle classi di equivalenza di coppie  $(U, f)$ , con  $U \subset X$  aperto non vuoto e  $f \in \mathcal{O}_X(U)$ , e dove  $(U, f) \sim (V, g)$  se e solo se  $f$  e  $g$  coincidono su  $U \cap V$ . Si noti che, essendo  $X$  irriducibile, per ogni aperto non vuoto  $U$  esiste una naturale inclusione  $\mathcal{O}_X(U) \subset \mathbb{K}(U) = \mathbb{K}(X)$ : in particolare per ogni aperto affine  $U \subset X$ , il campo  $\mathbb{K}(X)$  è naturalmente isomorfo al campo delle frazioni globali del dominio di integrità  $\mathbb{K}[U]$  e quindi che l'estensione di campi  $\mathbb{K} \subset \mathbb{K}(X)$  è finitamente generata. Ricordiamo che, data una estensione di campi  $F \subset L$  ed un sottoinsieme  $\mathcal{A} \subset L$ , si denota con  $F(\mathcal{A}) \subset L$  il più piccolo sottocampo di  $L$  contenente  $F$  e  $\mathcal{A}$ . Se  $F(\mathcal{A}) = L$  diremo che  $\mathcal{A}$  è un **insieme di generatori** dell'estensione  $F \subset L$ . Se esiste  $\mathcal{A}$  di cardinalità finita e tale che  $L = F(\mathcal{A})$ , diremo che  $F \subset L$  è una estensione finitamente generata.

**Lemma 12.3.1.** *Ogni estensione finitamente generata di  $\mathbb{K}$  è isomorfa al campo delle funzioni razionali di una varietà affine irriducibile.*

*Dimostrazione.* Sia  $\mathbb{K} \subset \mathbb{K}(l_1, \dots, l_n) = L$  una estensione finitamente generata e si consideri il morfismo di  $\mathbb{K}$ -algebre

$$\phi: \mathbb{K}[x_1, \dots, x_n] \rightarrow L, \quad \phi(x_i) = l_i.$$

Se  $X = V(\text{Ker}(\phi)) \subset \mathbb{A}^n$ , allora l'immagine di  $\phi$  è isomorfa all'algebra delle funzioni regolari  $\mathbb{K}[X]$  e quindi  $\mathbb{K}(l_1, \dots, l_n) = \mathbb{K}(X)$ .  $\square$

Diremo che una funzione razionale  $f \in \mathbb{K}(X)$  è **definita in un punto**  $x \in X$  se è possibile rappresentarla con una coppia  $(U, f)$  con  $x \in U$ . È ovvio che l'insieme dei punti dove una funzione razionale è definita è un aperto detto **aperto di definizione** ed è facile vedere che, se  $U$  è l'aperto di definizione di una funzione razionale  $f$ , allora  $f$  è rappresentata da una coppia  $(U, f)$ .

Se  $X$  è irriducibile e  $x \in X$ , allora esiste un isomorfismo naturale tra l'anello  $\mathcal{O}_{x,X}$  dei germi di funzioni regolari in  $x$  ed il sottoanello di  $\mathbb{K}(X)$  delle funzioni razionali che sono definite in  $x$ . Infatti gli elementi di  $\mathcal{O}_{x,X}$  sono rappresentati da coppie  $(U, f)$  con  $U$  intorno aperto di  $x$  e  $f$  funzione regolare su  $U$  modulo la relazione  $(U, f) \sim (V, g)$  se esiste un aperto  $x \in W \subset U \cap V$  tale che  $f|_W = g|_W$ . Dato che  $X$  è irriducibile, anche  $U \cap V$  è irriducibile e quindi, se due funzioni coincidono in un aperto non vuoto  $W \subset U \cap V$ , allora coincidono anche in  $U \cap V$ .

Sia  $\phi: X \rightarrow Y$  un morfismo dominante di varietà irriducibili e sia  $f \in \mathbb{K}(Y)$  rappresentata da una coppia  $(U, f)$ ; l'aperto  $\phi^{-1}(U)$  è non vuoto e si definisce  $\phi^*f \in \mathbb{K}(X)$  come la funzione razionale definita dalla coppia  $(\phi^{-1}(U), \phi^*f)$ . Lasciamo per esercizio la semplice verifica che  $\phi^*: \mathbb{K}(Y) \rightarrow \mathbb{K}(X)$  è un omomorfismo di campi ben definito che estende l'identità su  $\mathbb{K}$ .

Sia  $F \subset L$  è una estensione di campi. Un sottoinsieme  $\{l_i \mid i \in I\} \subset L$  si dice **algebricamente indipendente** su  $F$  se il morfismo naturale di  $F$ -algebre

$$\phi: F[\{t_i\}] \rightarrow L, \quad t_i \mapsto l_i,$$

è iniettivo (e quindi induce un isomorfismo tra  $F(\{l_i\})$  ed il campo delle funzioni razionali  $F(\{t_i\})$  a coefficienti in  $F$  nelle indeterminate  $t_i$ , con  $i \in I$ .) Una **base di trascendenza** di una estensione  $F \subset L$  è un sottoinsieme di  $L$  che è algebricamente indipendente su  $F$  e massimale rispetto all'inclusione. Una estensione  $F \subset L$  si dice **trascendente** se non è algebrica; si dice **trascendente pura** se  $L$  è generato da una base di trascendenza.

**Lemma 12.3.2.** *Sia  $X$  una varietà quasiproiettiva irriducibile e siano  $f_1, \dots, f_d \in \mathbb{K}(X)$  funzioni razionali algebricamente indipendenti su  $\mathbb{K}$ . Allora  $d \leq \dim(X)$  e vale  $d = \dim(X)$  se e solo se  $f_1, \dots, f_d$  formano una base di trascendenza dell'estensione  $\mathbb{K} \subset \mathbb{K}(X)$ .*

*Dimostrazione.* A meno di restringere  $X$  non è restrittivo supporre  $X$  affine e  $f_1, \dots, f_d$  funzioni regolari su  $X$ . Siccome l'omomorfismo  $\mathbb{K}[x_1, \dots, x_d] \rightarrow \mathbb{K}[X]$ ,  $x_i \mapsto f_i$ , è iniettivo, il morfismo  $\phi = (f_1, \dots, f_d): X \rightarrow \mathbb{A}^d$  è dominante e quindi  $\dim(X) \geq d$ . In particolare se  $d = \dim(X)$  allora necessariamente  $f_1, \dots, f_d$  è una base di trascendenza. Supponiamo che  $\dim(X) > d$ , allora non è restrittivo supporre  $X$  sottoinsieme chiuso di  $\mathbb{A}^n$ , con  $n > d$  e  $\phi$  la proiezione sulle prime  $d$  coordinate. Sia  $p \in X$  un punto tale che  $\dim_p \phi^{-1}(\phi(p)) = \dim(X) - d$ , a meno di permutare gli indici possiamo supporre che la proiezione di  $X$  sulla coordinata  $d+1$ -esima non sia costante su  $\phi^{-1}(\phi(p))$  in un intorno di  $p$ . Dunque, detta  $\psi: X \rightarrow \mathbb{A}^{d+1}$  la proiezione sulle prime  $d+1$  coordinate vale  $\dim_p \psi^{-1}(\psi(p)) < \dim(X) - d$  e quindi  $\psi$  deve essere necessariamente dominante.  $\square$

Il Lemma 12.3.2 ha come conseguenza che due basi di trascendenza di  $\mathbb{K}(X)$  hanno la stessa cardinalità; questo segue anche da un risultato più generale che riportiamo senza dimostrazione:

**Teorema 12.3.3.** *Sia  $K \subset L$  una estensione di campi; allora tutte le basi di trascendenza hanno la stessa cardinalità.*

*Dimostrazione.* Una dimostrazione può essere trovata in [Lang1984].  $\square$

**Definizione 12.3.4.** *La cardinalità di una base di trascendenza di una estensione di campi si dice **grado di trascendenza** dell'estensione.*

**Corollario 12.3.5.** *La dimensione di una varietà quasiproiettiva  $X$  è uguale al grado di trascendenza dell'estensione  $\mathbb{K} \subset \mathbb{K}(X)$ .*

## Esercizi

- 12.7.** 1. Usare il Lemma di Zorn per dimostrare che ogni estensione di campi  $F \subset L$  ammette una base di trascendenza.  
 2. Sia  $\mathcal{B} = \{t_i\}$  un insieme di indeterminate. Provare che  $\mathcal{B}$  è una base di trascendenza su  $F$  del campo delle funzioni razionali  $F(\{t_i\})$ .  
 3. Provare che un sottoinsieme  $\mathcal{B} \subset L$  algebricamente indipendente su  $F$  è una base di trascendenza se e solo se l'estensione  $F(\mathcal{B}) \subset L$  è algebrica.

## 12.4 Morfismi birazionali

**Definizione 12.4.1.** *Un morfismo dominante tra varietà quasiproiettive irriducibili si dice **birazionale** se induce un isomorfismo tra i campi delle funzioni razionali.*

**Teorema 12.4.2.** *Un morfismo regolare tra varietà quasiproiettive irriducibili è birazionale se e soltanto se induce un isomorfismo tra due aperti non vuoti.*

*Dimostrazione.* Siccome il campo delle funzioni razionali è invariante per restrizione ad un aperto, se  $\psi$  induce un isomorfismo tra aperti non vuoti allora  $\psi$  è birazionale.

Viceversa supponiamo che  $\psi: X \rightarrow Y$  sia un morfismo birazionale di varietà quasiproiettive irriducibili. Vogliamo dimostrare che esistono aperti non vuoti  $U \subset X$  e  $V \subset Y$  tali che  $\psi: U \rightarrow V$  è un isomorfismo. Possiamo supporre senza perdita di generalità che  $X, Y$  siano varietà affini. Siccome  $\psi$  è dominante, l'omomorfismo  $\psi^*: \mathbb{K}[Y] \rightarrow \mathbb{K}[X]$  è iniettivo e possiamo identificare  $\mathbb{K}[Y]$  con la sua immagine in  $\psi^*\mathbb{K}[Y] \subset \mathbb{K}[X]$ . La condizione di birazionalità equivale allora a dire che i due domini di integrità  $\mathbb{K}[X]$  e  $\mathbb{K}[Y]$  hanno lo stesso campo delle frazioni. Sia  $u_1, \dots, u_n \in \mathbb{K}[X]$  un insieme di generatori come  $\mathbb{K}$ -algebra: allora possiamo considerare  $u_1, \dots, u_n$  come funzioni razionali su  $Y$  e sia  $V \subset Y$  un aperto affine dove le  $u_i$  sono regolari. Esistono dunque delle ovvie inclusioni

$$\mathbb{K}[Y] \subset \mathbb{K}[X] \subset \mathbb{K}[V] \subset \mathbb{K}(Y) = \mathbb{K}(X).$$

Poniamo  $U = \psi^{-1}(V)$  e dimostriamo che  $\psi: U \rightarrow V$  è un isomorfismo di varietà. Siccome  $X, V$  sono affini, esiste un morfismo dominante  $\gamma: V \rightarrow X$  che induce l'inclusione  $\mathbb{K}[X] \subset \mathbb{K}[V]$  e siccome anche  $Y$  è affine la composizione  $\psi \circ \gamma: V \rightarrow Y$  induce l'inclusione  $\mathbb{K}[Y] \subset \mathbb{K}[V]$  e quindi deve essere  $\psi \circ \gamma = Id_V$ . Chiaramente  $\gamma(V) \subset U$  e quindi per concludere la dimostrazione è sufficiente dimostrare che il morfismo  $\gamma \circ \psi: U \rightarrow U$  è l'identità sul sottoinsieme denso  $\gamma(V) \subset U$ . Se  $x = \gamma(y)$  allora  $\gamma \circ \psi(x) = \gamma \circ \psi \circ \gamma(y) = \gamma(y) = x$ .  $\square$

**Teorema 12.4.3.** *Un morfismo dominante  $\psi: X \rightarrow Y$  tra varietà quasiproiettive irriducibili è birazionale se e soltanto se esiste un aperto  $U \subset X$  tale che la restrizione  $\psi: U \rightarrow Y$  è iniettiva e non ramificata.*

*Dimostrazione.* Il “soltanto se” segue immediatamente dal Teorema 12.4.2. Supponiamo viceversa che la restrizione di  $\psi$  ad un aperto  $U$  sia iniettiva e non ramificata e dimostriamo che  $\psi$  è birazionale. A meno di restringere  $X$  e  $Y$  non è restrittivo supporre  $X, Y$  affini e  $U = X$ . Possiamo inoltre assumere  $X \subset Y \times \mathbb{A}^m$  e  $\psi$  indotta dalla proiezione; chiaramente  $X$  e  $Y$  hanno la stessa dimensione. Sia  $\overline{X} \subset Y \times \mathbb{P}^m$  la chiusura di  $X$ ; la proiezione  $\psi: \overline{X} \rightarrow Y$  è un morfismo proiettivo e dominante, quindi surgettivo. Il chiuso  $Z = \psi(\overline{X} - X) \subset Y$  ha dimensione strettamente minore della dimensione di  $Y$ , a meno di sostituire  $Y$  con  $Y - Z$  e  $X$  con  $X - \psi^{-1}(Z)$  possiamo supporre  $\psi: X \rightarrow Y$  proiettivo, bigettivo e non ramificato. Basta adesso applicare i Teoremi 12.2.8 e 12.2.10 per dimostrare che  $\psi: X \rightarrow Y$  è un isomorfismo.  $\square$

**Corollario 12.4.4.** *Siano  $X$  e  $Y$  varietà quasiproiettive irriducibili definite su di un campo di caratteristica 0 e sia  $\psi: X \rightarrow Y$  un morfismo dominante iniettivo. Allora  $\psi$  è birazionale.*

*Dimostrazione.* Non è restrittivo supporre  $X$  liscia. Siccome  $\psi$  è dominante iniettivo  $X$  e  $Y$  hanno la stessa dimensione, e per il teorema di Bertini-Sard esiste un aperto non vuoto  $U \subset X$  che non contiene punti di ramificazione. Il morfismo  $\psi: U \rightarrow Y$  è iniettivo, dominante e non ramificato.  $\square$

**Corollario 12.4.5.** *Sia  $X \subset \mathbb{P}^n$  una varietà proiettiva irriducibile di codimensione  $\geq 2$ . Allora la generica proiezione  $X \rightarrow \mathbb{P}^{n-1}$  è birazionale sull'immagine. In particolare per ogni varietà quasiproiettiva irriducibile  $X$  esiste un morfismo birazionale  $X \rightarrow H$  con  $H$  ipersuperficie proiettiva.*

*Dimostrazione.* Sia  $x \in X$  un punto liscio. Se  $o \notin \mathbb{T}_x X$ , allora la proiezione di centro  $o$  è non ramificata in  $x$  e questo prova che per la generica proiezione i punti di non ramificazione formano un aperto non vuoto. Mostriamo adesso che esiste un aperto non vuoto  $O \subset \mathbb{P}^n - X$  tale che, se  $o \in O$ , allora la proiezione di centro  $o$  è iniettiva in un aperto  $U \subset X$ . Sia  $h \leq n - 2$  la dimensione di  $X$  e consideriamo il sottoinsieme  $S \subset \mathbb{P}^n \times X \times X$  delle triple  $(z, x, y)$  tali che  $x \neq y$  e  $z, x, y$  sono allineati. È chiaro che  $S$  è un sottoinsieme localmente chiuso, le fibre della proiezione su  $X \times X - \Delta$  sono delle rette proiettive e quindi  $S$  è una varietà quasiproiettiva irriducibile di dimensione  $2h + 1$ . Sia  $\bar{S}$  la chiusura di  $S$ ,  $p: \bar{S} \rightarrow \mathbb{P}^n$  e  $q: \bar{S} \rightarrow X \times X$  le proiezioni sul primo e sul secondo fattore. Sia  $Z \subset \mathbb{P}^n$  il sottoinsieme dei punti  $z$  tali che la dimensione di  $p^{-1}(z)$  sia almeno  $h$ ; per il Teorema 9.7.1,  $Z$  è un chiuso di dimensione  $\leq h + 1 < n$ . Basta adesso osservare che se  $o \notin Z \cup X$  allora  $U = X - q(p^{-1}(o))$  è un aperto non vuoto di  $X$  e la proiezione di centro  $o$  è iniettiva su  $U$ .  $\square$

**Corollario 12.4.6.** *Ogni estensione finitamente generata di  $\mathbb{K}$  con grado di trascendenza  $d$  è isomorfa a  $\mathbb{K}(x_0, \dots, x_d)$  con  $x_1, \dots, x_d$  base di trascendenza e  $x_0$  algebrico su  $\mathbb{K}(x_1, \dots, x_d)$ .*

*Dimostrazione.* Abbiamo visto, come conseguenza di 12.3.1 e 12.4.5 che ogni estensione finitamente generata con grado di trascendenza  $d$  è isomorfa a  $\mathbb{K}(X)$  per qualche ipersuperficie affine irriducibile  $X \subset \mathbb{A}^{d+1}$ . Siano  $x_0, \dots, x_d$  coordinate su  $\mathbb{A}^{d+1}$  tali che  $X$  è definita da un polinomio monico in  $x_0$ . La proiezione  $X \rightarrow \mathbb{A}^d$  sulle coordinate  $x_1, \dots, x_d$  è surgettiva e quindi  $x_1, \dots, x_d$  sono algebricamente indipendenti su  $\mathbb{K}$ .  $\square$

**Definizione 12.4.7.** *Siano  $X, Y$  varietà quasiproiettive; una **applicazione razionale**  $\phi$  da  $X$  in  $Y$  è una classe di equivalenza di coppie  $(U, \phi)$  con  $U \subset X$  aperto denso e  $\phi: U \rightarrow Y$  morfismo regolare, modulo la relazione  $(U, \phi) \sim (V, \psi)$  se  $\phi = \psi$  in  $U \cap V$ .*

Un'applicazione razionale si denota graficamente con una freccia a tratti medi  $\dashrightarrow$ . Diremo che una applicazione razionale  $\phi: X \dashrightarrow Y$  è dominante se i suoi rappresentanti  $\phi: U \rightarrow Y$  sono dominanti. Se  $\phi: X \dashrightarrow Y$  e  $\psi: Y \dashrightarrow Z$  sono applicazioni razionali, con  $\phi$  dominante, ha senso considerare la composizione  $\psi\phi: X \dashrightarrow Z$ . Come sopra una applicazione razionale dominante  $\phi: X \dashrightarrow Y$  tra varietà irriducibili induce un omomorfismo di campi  $\phi^*: \mathbb{K}(Y) \rightarrow \mathbb{K}(X)$ . Un'applicazione razionale si dice **birazionale** se è dominante e induce un isomorfismo tra i campi di funzioni razionali. Segue immediatamente dal Teorema 12.4.2 che un'applicazione razionale dominante è birazionale se e solo se possiede un'inversa razionale.

*Esempio 12.4.8.* L'applicazione  $t \mapsto (t^2, t^3)$  è un morfismo birazionale tra la retta affine  $\mathbb{A}^1$  e la curva piana  $X \subset \mathbb{A}^2$  di equazione  $x^3 = y^2$ .

**Definizione 12.4.9.** *Una varietà irriducibile  $X$  di dimensione  $n$  si dice **razionale** se esiste una applicazione birazionale  $\phi: \mathbb{P}^n \dashrightarrow X$ .*

*Esempio 12.4.10.* I prodotti di spazi proiettivi, le Grassmanniane e più in generale tutte le varietà irriducibili che contengono un aperto isomorfo allo spazio affine sono razionali.

**Proposizione 12.4.11.** *La dimensione di una varietà quasiproiettiva irriducibile è il massimo intero  $n$  tale che esiste una applicazione razionale dominante  $\phi: X \dashrightarrow \mathbb{A}^n$ .*

*Dimostrazione.* Non è restrittivo assumere  $X$  affine, abbiamo già dimostrato che se  $\dim X = n$  esiste un morfismo chiuso e surgettivo  $X \rightarrow \mathbb{A}^n$ .

Viceversa sia  $\phi: X \dashrightarrow \mathbb{A}^n$  dominante, a meno di restringere  $X$  ad un aperto possiamo supporre  $\phi$  regolare; segue dunque dal Teorema 10.6.6 che  $\dim X \geq n$ .  $\square$

*Esempio 12.4.12.* Dati comunque  $m + 1$  polinomi omogenei  $F_0, \dots, F_m \in \mathbb{K}[x_0, \dots, x_n]$  dello stesso grado senza fattori comuni possiamo associare una applicazione razionale

$$\phi: \mathbb{P}^n \dashrightarrow \mathbb{P}^m, \quad \phi([x]) = [F_0(x), \dots, F_m(x)].$$

Per il Teorema 10.3.10 l'aperto di definizione di  $\phi$  è  $\mathbb{P}^n - V(F_0, \dots, F_m)$  ed ogni applicazione razionale  $\mathbb{P}^n \dashrightarrow \mathbb{P}^m$  si ottiene in questo modo. Il prossimo Esempio 12.4.13 mostra che l'applicazione può essere birazionale anche se i polinomi  $F_i$  hanno grado maggiore di 1.

*Esempio 12.4.13 (Trasformazioni Cremoniane).* La trasformazione Cremoniana associata ad un sistema di coordinate omogenee  $x_0, x_1, x_2$  su  $\mathbb{P}^2$  è l'applicazione razionale

$$\sigma: \mathbb{P}^2 \dashrightarrow \mathbb{P}^2, \quad \sigma([x_0, x_1, x_2]) = [x_1x_2, x_2x_0, x_0x_1].$$

La restrizione di  $\sigma$  all'aperto  $U = \{x_0x_1x_2 \neq 0\}$  è una involuzione regolare che si può esprimere come

$$\sigma([x_0, x_1, x_2]) = \left[ \frac{1}{x_0}, \frac{1}{x_1}, \frac{1}{x_2} \right].$$

Quindi  $\sigma$  è birazionale.

*Esempio 12.4.14.* In caratteristica 0 ogni curva piana proiettiva irriducibile è birazionale alla sua curva duale. Infatti se  $C \subset \mathbb{P}^2$ , allora, nelle notazioni della Sezione 11.5, le proiezioni  $D_C \rightarrow C$ ,  $D_{C^\vee} \rightarrow C^\vee$  sono birazionali e per il teorema di dualità  $D_C$  è birazionale a  $D_{C^\vee}$ .

**Teorema 12.4.15.** *Siano  $X$  e  $Y$  varietà quasiproiettive irriducibili. Allora esiste una bigezione naturale tra l'insieme delle applicazioni razionali dominanti  $X \dashrightarrow Y$  e l'insieme degli omomorfismi di campi  $\mathbb{K}(Y) \rightarrow \mathbb{K}(X)$  che fissano  $\mathbb{K}$ .*

*Dimostrazione.* Esercizio.  $\square$

**Definizione 12.4.16.** *Il **grado** di una applicazione razionale dominante  $\phi: X \dashrightarrow Y$  tra varietà irriducibili della stessa dimensione è uguale al grado dell'estensione algebrica finita di campi  $\phi^*\mathbb{K}(Y) \subset \mathbb{K}(X)$ .*

**Teorema 12.4.17.** *Il grado di una varietà proiettiva irriducibile  $X \subset \mathbb{P}^n$  di dimensione  $h$  è uguale al grado di una generica proiezione  $X \rightarrow \mathbb{P}^h$ .*

*Dimostrazione.* Denotiamo con  $d$  il grado di  $X$  e consideriamo prima il caso  $h = n - 1$ , cioè  $X$  ipersuperficie irriducibile. Abbiamo visto che  $X$  è il luogo di zeri di un polinomio irriducibile omogeneo  $F$  di grado  $d$ . Sia  $\pi: X \rightarrow \mathbb{P}^{n-1}$  la proiezione di centro  $o \notin X$  e fissiamo un sistema di coordinate omogenee  $u_0, \dots, u_n$  tali che  $o = [1, 0, \dots, 0]$ . Se  $Y = X \cap \{u_n \neq 0\}$  allora il grado di  $\pi$  è uguale al grado della restrizione

$$Y \rightarrow \mathbb{A}^{n-1}, \quad [x_0, \dots, x_n] \mapsto [x_1, \dots, x_{n-1}], \quad x_i = \frac{u_i}{u_n}.$$

Il disomogeneizzato di  $F$  è un polinomio di grado  $d$  monico in  $x_0$  che, per il lemma di Gauss, è irriducibile in  $\mathbb{K}(x_1, \dots, x_{n-1})[x_0]$ . Dunque  $\mathbb{K}(Y) = \mathbb{K}(x_1, \dots, x_{n-1})[x_0]/(F)$  è una estensione di grado  $d$  di  $\mathbb{K}(\mathbb{A}^{n-1})$ .

Supponiamo adesso che  $h \leq n - 2$ , abbiamo visto che per il generico sottospazio proiettivo  $K \subset \mathbb{P}^n - X$  di codimensione  $h + 1$ , la proiezione  $\pi: X \rightarrow \mathbb{P}^h$  di centro  $K$  soddisfa le condizioni:

1. Il differenziale di  $\pi$  è bigettivo in un aperto denso.
2. L'insieme

$$U = \{p \in \mathbb{P}^h \mid \#\pi^{-1}(p) = d\}$$

è un aperto non vuoto di Zariski.

Sia  $H \supset K$  un sottospazio di codimensione  $h$  che interseca  $X$  in  $d$  punti distinti  $p_1, \dots, p_d$ ; allora il generico sottospazio  $Z \subset K$  di codimensione  $h + 2$  non interseca l'unione delle rette  $\overline{p_i p_j}$ . Denotiamo con  $\rho: X \rightarrow \mathbb{P}^{h+1}$  la proiezione di centro  $Z$  e con  $Y = \rho(X)$ . Per quanto dimostrato nel caso  $h = n - 1$  basta dimostrare che  $Y$  è una ipersuperficie di grado  $d$  e che  $\rho: X \rightarrow Y$  è birazionale. Siccome  $\rho$  è surgettiva  $\deg(Y) \leq \deg(X) = d$  e siccome  $Y$  interseca  $\rho(H)$  in  $d$  punti distinti deve essere  $\deg(Y) = d$ . Dunque necessariamente  $\rho$  deve essere iniettiva in  $\pi^{-1}(U)$  e deve avere differenziale iniettivo dove  $d\pi$  è iniettivo. Per il Teorema 12.4.3  $\rho$  è birazionale.  $\square$

Nonostante le applicazioni razionali non siano delle applicazioni in senso insiemistico, ha ancora senso parlare dei concetti di grafico e di immagine.

**Definizione 12.4.18.** Sia  $\phi: X \dashrightarrow Y$  una applicazione razionale, rappresentata da  $\phi: U \rightarrow Y$ ; il grafico  $\Gamma_\phi \subset X \times Y$  di  $\phi$  è la chiusura in  $X \times Y$  del grafico di  $\phi: U \rightarrow Y$ . L'immagine  $\phi(X) \subset Y$  è la proiezione sul secondo fattore del grafico di  $\phi$ .

**Teorema 12.4.19 (Teorema del grafico chiuso).** Siano  $X, Y$  varietà quasiproiettive irriducibili. Un chiuso irriducibile  $\Gamma \subset X \times Y$  è il grafico di una applicazione razionale se e solo se esiste un aperto denso  $U \subset \Gamma$  tale che la proiezione  $U \rightarrow X$  è iniettiva, dominante e non ramificata. Se la caratteristica di  $\mathbb{K}$  è uguale a 0, l'ipotesi di non ramificazione può essere omessa.

*Dimostrazione.* Per il Teorema 12.4.3 la proiezione  $\Gamma \rightarrow X$  è birazionale ed ogni morfismo birazionale è invertibile nella classe delle applicazioni razionali dominanti.  $\square$

## Esercizi

**12.8.** In caratteristica 0, per ogni  $n \geq 3$  la curva piana di Fermat  $x_0^n + x_1^n + x_2^n = 0$  non è razionale. (Sugg.: Esercizio 1.50.)

**12.9 (L'applicazione di Cayley, 1846).** (caratteristica  $\neq 2$ ) Sia  $M(n, n, \mathbb{K})$  lo spazio affine delle matrici  $n \times n$  e si noti che se  $A \in M(n, n, \mathbb{K})$  e  $\det(I + A) \neq 0$ , allora  $(I + A)^{-1}(I - A) = (I - A)(I + A)^{-1}$ . Provare che l'applicazione razionale

$$\phi: M(n, n, \mathbb{K}) \dashrightarrow M(n, n, \mathbb{K}), \quad \phi(A) = \frac{I - A}{I + A},$$

è una involuzione (cioè  $\phi^2 = Id$ ) ed induce per restrizione un'applicazione birazionale tra il sottospazio lineare delle matrici antisimmetriche ed il gruppo delle matrici ortogonali di determinante 1. (Sugg.: mostrare che se  $A$  è antisimmetrica, allora  $\det(I + A) = \det(I - A)$ , mentre se  $B$  è ortogonale e  $\det(I + B) \neq 0$ , allora  $\det(B) = 1$ .)

**12.10.** Sia  $X$  una varietà irriducibile di dimensione  $n$ . Si dice che  $X$  è **unirazionale** se esiste un'applicazione razionale dominante  $\mathbb{P}^n \dashrightarrow X$ . Dimostrare:

1.  $X$  è unirazionale se e solo se  $\mathbb{K}(X)$  è isomorfo ad un sottocampo di  $\mathbb{K}(x_1, \dots, x_n)$ .
2. Se  $Y$  è una varietà unirazionale di dimensione  $\geq n$  ed esiste un'applicazione razionale dominante  $Y \dashrightarrow X$ , allora anche  $X$  è unirazionale.

## 12.5 Estensioni separabili

Nel seguito indicheremo con  $\overline{K}$  la chiusura algebrica di un campo  $K$ . Ricordiamo che essa è unica a meno di isomorfismo e che ogni estensione algebrica di  $K$  è isomorfa ad un sottocampo di  $\overline{K}$ .

**Definizione 12.5.1.** 1. Sia  $\overline{K}$  la chiusura algebrica di un campo  $K$ . Un elemento  $a \in \overline{K}$  si dice **separabile su  $K$**  se esiste un polinomio  $q(t) \in K[t]$  tale che  $q(a) = 0$  e  $q'(a) = \frac{dq}{dt}(a) \neq 0$ .

2. Una estensione algebrica di campi  $K \subset E$  si dice **separabile** se ogni  $a \in E$  è separabile su  $K$ .

Segue immediatamente dalla definizione che, se  $K \subset L \subset E$  sono estensioni algebriche e  $K \subset E$  è separabile, allora anche le estensioni  $K \subset L$  e  $L \subset E$  sono separabili.

**Lemma 12.5.2.** Sia  $\mu_a \in K[t]$  il polinomio minimo su  $K$  di un elemento  $a \in \overline{K}$ . Allora sono condizioni equivalenti:

1.  $a$  è separabile su  $K$ .
2.  $\mu'_a(a) \neq 0$ .
3.  $\mu'_a \neq 0$ .
4.  $\mu_a$  non ha radici multiple in  $\overline{K}$ .

In particolare se  $K$  ha caratteristica 0, allora ogni  $a \in \overline{K}$  è separabile su  $K$ .

*Dimostrazione.* [1  $\Leftrightarrow$  2] Se  $a$  è separabile su  $K$  e  $q \in K[t]$  è un polinomio tale che  $q(a) = 0$  e  $q'(a) \neq 0$ , allora  $q = \mu_a h$ ,  $q'(a) = \mu'_a(a)h(a)$  e quindi  $\mu'_a(a) \neq 0$ .

[2  $\Leftrightarrow$  3] Se  $\mu'_a(a) = 0$  allora  $\mu_a$  divide la sua derivata e questo è possibile solo se  $\mu'_a = 0$ .

[4  $\Rightarrow$  2] Se fosse  $\mu'_a(a) = 0$ , allora  $a$  sarebbe una radice multipla di  $\mu_a$ .

[3  $\Rightarrow$  4] Supponiamo per assurdo che esista  $b \in \overline{K}$  tale che  $\mu_a(b) = \mu'_a(b) = 0$ . Siccome  $\mu_a$  è irriducibile in  $K[t]$  e vale  $\mu_a(b) = 0$  si ha  $\mu_a = \mu_b$ . L'equivalenza [2  $\Leftrightarrow$  3] mostra quindi che  $\mu'_b = 0$  e di conseguenza  $\mu'_a = 0$ .  $\square$

**Lemma 12.5.3.** Sia  $K \subset L \subset \overline{K}$  una estensione algebrica di campi. Allora ogni omomorfismo di campi  $\sigma: L \rightarrow \overline{K}$  tale che  $\sigma(K) = K$  si estende (in modo non unico) ad un isomorfismo di campi  $\overline{\sigma}: \overline{K} \rightarrow \overline{K}$ .

*Dimostrazione.* Mostriamo per prima cosa che  $\sigma$  si estende ad un omomorfismo di campi  $\overline{\sigma}: \overline{K} \rightarrow \overline{K}$ . La dimostrazione di questo fatto è una delle più classiche applicazioni del lemma di Zorn. Consideriamo l'insieme  $\mathcal{A}$  formato dalle coppie  $(F, f)$ , dove  $L \subset F \subset \overline{K}$  è una estensione algebrica di campi e  $f: F \rightarrow \overline{K}$  è un omomorfismo che estende  $\sigma$ . Poniamo su  $\mathcal{A}$  l'ordinamento  $(F, f) \leq (G, g)$  se  $F \subset G$  e  $g$  estende  $f$ . L'insieme  $\mathcal{A}$  contiene la coppia  $(L, \sigma)$ , ogni catena  $\{(F_i, f_i)\}$  possiede un maggiorante  $(F = \cup F_i, \lim f_i)$  e dunque, per il Lemma di Zorn, esiste un elemento massimale  $(E, \overline{\sigma})$ . Se fosse  $E \neq \overline{K}$ , allora consideriamo un elemento  $a \in \overline{K} - E$  con polinomio minimo  $\mu = \sum_i a_i t^i \in E[t]$ . Basta allora considerare l'estensione  $f: E(a) \rightarrow \overline{K}$  di  $\overline{\sigma}$  data da  $f(a) = \alpha$ , dove  $\alpha$  è una radice di  $\sum_i \overline{\sigma}(a_i) t^i$ . Ricordiamo che ogni omomorfismo di campi non nullo è iniettivo; poiché  $\overline{\sigma}(K) = K$  si ha che  $\overline{\sigma}(\overline{K})$  è una chiusura algebrica di  $\sigma(K) = K$  e quindi  $\overline{\sigma}$  è anche surgettivo.  $\square$

**Definizione 12.5.4.** Se  $K \subset L \subset E \subset \overline{K}$  sono campi, denotiamo con  $G(E/L)$  l'insieme degli omomorfismi di campi  $f: E \rightarrow \overline{K}$  tali che  $f(l) = l$  per ogni  $l \in L$ . La cardinalità di  $G(E/L)$  viene detta **grado separabile** dell'estensione  $L \subset E$  e denotata con  $[E : L]_s$ .

*Esempio 12.5.5.* Se  $E = L(a)$  è una estensione semplice di  $L$ , allora il grado  $[E : L]$  è uguale al grado del polinomio minimo  $\mu_a$  di  $a$  in  $L$ , mentre il grado separabile  $[E : L]_s$  è uguale al numero di radici distinte di  $\mu_a$  in  $\bar{K} = \bar{L}$ . In particolare  $[L(a) : L]_s \leq [L(a) : L]$  e vale  $=$  se e solo se  $a$  è separabile su  $L$ .

**Lemma 12.5.6.** *Date due estensioni di campi  $K \subset L \subset E \subset \bar{K}$  esiste una bigezione (non canonica)*

$$G(L/K) \times G(E/L) \simeq G(E/K).$$

*Dimostrazione.* Siano  $G(L/K) = \{\sigma_i\}$ ,  $G(E/L) = \{\tau_j\}$  e, per ogni  $i$ , sia  $\bar{\sigma}_i \in G(\bar{K}/K)$  una estensione di  $\sigma_i$  come nel Lemma 12.5.3. Consideriamo l'applicazione

$$G(L/K) \times G(E/L) \rightarrow G(E/K), \quad (\sigma_i, \tau_j) \mapsto \bar{\sigma}_i \tau_j.$$

Siccome  $\bar{\sigma}_i \tau_j(l) = \sigma_i(l)$  per ogni  $l \in L$ , se vale  $\bar{\sigma}_i \tau_j = \bar{\sigma}_h \tau_k$ , allora deve essere  $h = i$  e, essendo  $\bar{\sigma}_i$  iniettiva, deve anche essere  $j = k$ . Se  $f \in G(E/K)$ , allora esiste un indice  $i$  tale che  $f(l) = \bar{\sigma}_i(l)$  per ogni  $l \in L$  e quindi  $\bar{\sigma}_i^{-1} f \in G(E/L)$ .  $\square$

**Teorema 12.5.7.** *Siano  $K \subset L \subset E$  estensioni finite di campi. Allora si ha*

$$[E : K]_s \leq [E : K], \quad [E : K]_s = [E : L]_s [L : K]_s.$$

*Dimostrazione.* Abbiamo già visto nell'Esempio 12.5.5 che la disuguaglianza  $[E : K]_s \leq [E : K]$  è vera per le estensioni semplici mentre, per il Lemma 12.5.6, l'uguaglianza  $[E : K]_s = [E : L]_s [L : K]_s$  è verificata ogniqualvolta uno dei due membri è  $< +\infty$ . Se  $E = K(a_1, \dots, a_n)$ , allora è sufficiente considerare la catena di estensioni semplici

$$K \subset K(a_1) \subset \dots \subset K(a_1, \dots, a_{n-1}) \subset E.$$

$\square$

**Corollario 12.5.8.** *Per una estensione algebrica finita di campi  $K \subset E$  le seguenti condizioni sono equivalenti:*

1.  $K \subset E$  è separabile.
2.  $E = K(a_1, \dots, a_n)$ , con ogni  $a_i$  separabile su  $K$ .
3.  $[E : K]_s = [E : K]$ .

*Dimostrazione.*  $[1 \Rightarrow 2]$  è ovvio.  $[2 \Rightarrow 3]$  segue dal Teorema 12.5.7 e dall'Esempio 12.5.5 applicato alla catena di estensioni semplici

$$K \subset K(a_1) \subset \dots \subset K(a_1, \dots, a_{n-1}) \subset E.$$

$[3 \Rightarrow 1]$  Sia  $a \in E$ . Per dimostrare che  $a$  è separabile su  $K$  basta applicare il Teorema 12.5.7 e l'Esempio 12.5.5 alla catena di estensioni semplici

$$K \subset K(a) \subset E.$$

$\square$

**Corollario 12.5.9.** *Se  $K \subset L$  e  $L \subset E$  sono estensioni algebriche separabili, allora anche l'estensione  $K \subset E$  è separabile e viceversa.*

*Dimostrazione.* Il viceversa è facile e lo abbiamo già visto. Se  $E$  è finito su  $K$  il risultato segue immediatamente dal Corollario 12.5.8. In generale ogni  $a \in E$  separabile su  $L$  è anche separabile su di un sottocampo  $F \subset L$  finito su  $K$  (basta ad esempio considerare il campo  $F$  generato dai coefficienti del polinomio minimo di  $a$  in  $L$ ) e si applica il caso finito alle estensioni  $K \subset F \subset K(a)$ .  $\square$



**Definizione 12.5.10.** Una estensione algebrica  $K \subset E$  si dice **inseparabile** se non è separabile. Si dice **puramente inseparabile** se ogni  $a \in E - K$  non è separabile su  $K$ .

**Teorema 12.5.11.** Una estensione algebrica  $K \subset E \subset \bar{K}$  è puramente inseparabile se e solo se  $[E : K]_s = 1$ .

*Dimostrazione.* In caratteristica 0 il risultato è evidente; non è quindi restrittivo supporre di essere in caratteristica  $p > 0$ . Se  $[E : K]_s = 1$ , allora per ogni  $a \in E - K$  si ha

$$1 \leq [K(a) : K]_s \leq [E : K]_s = 1$$

e quindi  $a$  non è separabile su  $K$ . Se  $[E : K]_s > 1$ , allora esistono un omomorfismo  $f: E \rightarrow \bar{K}$  che fissa  $K$  ed un elemento  $a \in E$  tale che  $f(a) \neq a$ . Dato che l'omomorfismo di Frobenius è iniettivo, si ha che  $f(a^p) = f(a)^p \neq a^p$  e quindi  $a^p \notin K$ . La successione di  $K$ -spazi vettoriali di dimensione finita  $K(a) \supset K(a^p) \supset K(a^{p^2}) \supset \dots$  è stazionaria; a meno di sostituire  $a$  con una sua potenza non è restrittivo assumere  $K(a) = K(a^p)$  e quindi esiste  $h \in K[t]$  tale che  $a = h(a^p)$ ; ponendo  $q(t) = t - h(t^p)$  si ha  $q(a) = 0$ ,  $q' = 1$  e perciò  $a$  è separabile.  $\square$

**Corollario 12.5.12.** Il grado di una estensione finita puramente inseparabile è una potenza della caratteristica del campo.

*Dimostrazione.* Denotiamo con  $p > 0$  la caratteristica e sia  $K \subset E$  una estensione puramente inseparabile. Se  $E = K$  non c'è nulla da dimostrare. Sia quindi  $a \in E - K$  e consideriamo la catena di estensioni

$$K \subset K(a^p) \subset K(a) \subset E.$$

Per il Teorema 12.5.7, tali estensioni sono tutte puramente inseparabili e  $[K(a) : K(a^p)] = p$ ; ragionando per induzione sul grado dell'estensione si arriva facilmente alla tesi.  $\square$

**Corollario 12.5.13.** Sia  $K \subset E$  una estensione algebrica e sia  $E_s \subset E$  il sottoinsieme degli elementi separabili su  $K$ . Allora  $E_s$  è un sottocampo di  $E$ , l'estensione  $E_s \subset E$  è puramente inseparabile e, se  $[E : K]_s < +\infty$ , allora vale

$$[E : K]_s = [E_s : K]_s = [E_s : K].$$

*Dimostrazione.* Se  $a, b \in E$  sono separabili su  $K$ , allora l'estensione  $K \subset K(a, b)$  è separabile e quindi  $K(a, b) \subset E_s$ . Per la seconda parte del corollario basta osservare che l'estensione  $E_s \subset E$  è puramente inseparabile e applicare il Lemma 12.5.6.  $\square$

**Definizione 12.5.14.** Il **grado inseparabile**  $[E : K]_i$  di una estensione finita di campi  $K \subset E$  è uguale a

$$[E : K]_i = \frac{[E : K]}{[E : K]_s}.$$

Per il Corollario 12.5.13  $[E : K]_i$  è uguale al grado dell'estensione puramente inseparabile  $E_s \subset E$  ed è quindi uguale ad una potenza della caratteristica del campo.

Sia  $K \subset E$  una estensione di campi di grado  $n$  e, per ogni  $a \in E$ , denotiamo con  $\text{trace}_{E/K}(a) \in K$  la traccia della moltiplicazione  $a: E \rightarrow E$ , ovvero il coefficiente di  $t^{n-1}$  del polinomio caratteristico di  $a$ . Ricordiamo che, se  $E = K(a)$ , allora il polinomio minimo di  $a$  coincide con il polinomio caratteristico della moltiplicazione per  $a$ . Osserviamo infine che, se  $K \subset L \subset E$  e  $a \in L$ , allora  $\text{trace}_{E/K}(a) = [E : L] \text{trace}_{L/K}(a)$ .

**Proposizione 12.5.15.** Sia  $K \subset E$  una estensione finita di campi. Allora:

1. Per ogni  $a \in E$  vale

$$\text{trace}_{E/K}(a) = [E : K]_i \sum_{f \in G(E/K)} f(a).$$

2. L'estensione è inseparabile se e solo se  $\text{trace}_{E/K}(a) = 0$  per ogni  $a$ .  
 3. L'estensione è separabile se e solo se l'applicazione bilineare

$$T: E \times E \rightarrow K, \quad T(a, b) = \text{trace}_{E/K}(ab)$$

è non degenere.

*Dimostrazione.* [1] Se  $a$  è separabile di grado  $[K(a) : K] = [K(a) : K]_s$ , allora  $\text{trace}_{K(a)/K}(a)$  è uguale alla somma delle radici del polinomio minimo di  $a$  e quindi

$$\text{Tr}_{K(a)/K}(a) = \sum_{f \in G(K(a)/K)} f(a),$$

$$\text{Tr}_{E/K}(a) = [E : E_s][E_s : K(a)] \sum_{f \in G(K(a)/K)} f(a) = [E : E_s] \sum_{g \in G(E_s/K(a))} \sum_{f \in G(K(a)/K)} fg(a).$$

Basta adesso ricordare la definizione di grado di inseparabilità e la bigezione  $G(E/K) = G(E_s/K) = G(E/K(a)) \times G(K(a)/K)$ .

Se  $a$  è inseparabile su  $K$ , il polinomio minimo di  $a$  su  $K$  contiene solo monomi di grado multiplo di della caratteristica del campo, quindi  $\text{trace}_{K(a)/K}(a) = 0$  ed a maggior ragione  $\text{trace}_{E/K}(a) = 0$ .

[2] Se l'estensione è inseparabile  $[E : K]_i = p^n$  con  $n > 0$  e quindi la traccia è identicamente nulla.

[3] Se l'estensione è separabile allora  $[E : K]_i = 1$ . Essendo  $K$  infinito e  $G(E/K)$  finito, esiste  $a \in E$  tale che  $f(a) \neq g(a)$  per ogni  $f, g \in G(E/K)$  con  $f \neq g$ . Assumiamo per assurdo che  $\sum_{f \in G(E/K)} f(a) = 0$  per ogni  $a \in E$ , allora per ogni  $n > 0$  vale anche

$$\sum_{f \in G(E/K)} f(a)^n = \sum_{f \in G(E/K)} f(a^n) = 0.$$

e dalle proprietà della matrice di Vandermonde si ricava una contraddizione. Esiste quindi  $a \in E$  tale che  $\text{Tr}_{E/K}(a) \neq 0$  e quindi per ogni  $b \in E$ ,  $b \neq 0$ , vale  $T(b, ab^{-1}) \neq 0$ .  $\square$

**Proposizione 12.5.16.** *Sia  $K$  un campo perfetto di caratteristica  $p > 0$ ,  $K \subset E$  una estensione finitamente generata con grado di trascendenza  $d$  e denotiamo con  $E^p \subset E$  il sottocampo delle potenze  $p$ -esime di  $E$ . Allora per una base di trascendenza  $t_1, \dots, t_d \in E$  le seguenti condizioni sono equivalenti:*

1.  $E^p(t_1, \dots, t_d) = E$ .
2.  $t_i \notin E^p(t_1, \dots, t_{i-1})$  per ogni  $i = 1, \dots, d$ .
3. L'estensione  $K(t_1, \dots, t_d) \subset E$  è separabile.

*Dimostrazione.* L'omomorfismo di Frobenius induce un isomorfismo tra l'estensione  $K(t_1, \dots, t_d) \subset E$  e  $K(t_1, \dots, t_d)^p \subset E^p$ ; in particolare le due estensioni hanno lo stesso grado e quindi

$$[E : E^p] = \frac{[E : K(t_1, \dots, t_d)^p]}{[E^p : K(t_1, \dots, t_d)^p]} = \frac{[E : K(t_1, \dots, t_d)^p]}{[E : K(t_1, \dots, t_d)]} =$$

$$[E : E^p] = [K(t_1, \dots, t_d) : K(t_1, \dots, t_d)^p] = p^d,$$

dove nell'ultima uguaglianza abbiamo usato il fatto che  $K = K^p$  e quindi  $K(t_1, \dots, t_d)^p = K(t_1^p, \dots, t_d^p)$ .

[1  $\Leftrightarrow$  2] Basta osservare che per ogni  $i = 1, \dots, d$  si ha  $t_i^p \in E^p(t_1, \dots, t_{i-1})$  e quindi l'estensione  $E^p(t_1, \dots, t_{i-1}) \subset E^p(t_1, \dots, t_i)$  ha grado  $p$  se  $t_i \notin E^p(t_1, \dots, t_{i-1})$  e grado 1 altrimenti.

[1 + 2  $\Rightarrow$  3] Sia  $a \in E$  e denotiamo  $F = K(t_1, \dots, t_d, a)$ ; l'argomento precedente, applicato all'estensione  $K \subset F$  con grado di trascendenza  $d$ , mostra che  $[F : F^p] = p^d$ . D'altra parte la condizione 2 implica che  $t_i \notin F^p(t_1, \dots, t_{i-1})$  per ogni  $i$  e quindi  $F = F^p(t_1, \dots, t_d)$  ed in particolare  $a \in F^p(t_1, \dots, t_d) = K(t_1, \dots, t_d)(a^p)$ , diciamo  $a = q(a^p)$  con  $q$  polinomio a coefficienti in  $K(t_1, \dots, t_d)$ . Lo stesso ragionamento fatto nella dimostrazione di 12.5.11 mostra che  $a$  è radice di  $t - q(t^p)$  ed è quindi separabile su  $K(t_1, \dots, t_d)$ .

[3  $\Rightarrow$  1] Per ipotesi  $K(t_1, \dots, t_d) \subset E$  è separabile mentre  $E^p \subset E$  è puramente inseparabile. Ne segue che, poiché  $K(t_1, \dots, t_d) \subset E^p(t_1, \dots, t_d)$  e  $E^p \subset E^p(t_1, \dots, t_d)$ , l'estensione  $E^p(t_1, \dots, t_d) \subset E$  è al tempo stesso separabile e puramente inseparabile.  $\square$

### Esercizi

**12.11.** Sia  $K \subset E$  una estensione finita di campi di caratteristica positiva e sia  $F: E \rightarrow E$  l'omomorfismo di Frobenius. Provare che l'estensione è puramente inseparabile se e solo se  $F^n(E) \subset K$  per  $n \gg 0$ .

**12.12.** Sia  $K \subset E$  un'estensione algebrica di campi infiniti. Dimostrare che gli elementi di  $G(E/K)$  sono linearmente indipendenti sul  $\overline{K}$ -spazio vettoriale  $\text{Hom}_K(E, \overline{K})$ . (Sugg.: usare il Vandermonde come nella dimostrazione di 12.5.15. Vedi anche [Her1982, 5.6.1].)

**12.13.** Un polinomio irriducibile  $q \in K[t]$  di grado positivo si dice **separabile** su  $K$  se non possiede radici multiple nella chiusura algebrica  $\overline{K}$ . Dimostrare che per un campo  $K$  le seguenti condizioni sono equivalenti:

1.  $K$  è perfetto.
2. Ogni polinomio irriducibile  $q \in K[t]$  di grado positivo è separabile.
3. Ogni estensione algebrica  $K \subset E$  è separabile.

## 12.6 Morfismi separabili

**Definizione 12.6.1.** Un morfismo di varietà quasiproiettive  $\phi: X \rightarrow Y$  si dice **separabile** se esiste un aperto denso  $U \subset X$  tale che la restrizione  $\phi: U \rightarrow Y$  non ha punti critici.

È un facile esercizio mostrare che la classe dei morfismi separabili è chiusa per composizione (sugg.: se  $\phi: X \rightarrow Y$  è separabile e  $U \subset X$  è un aperto non vuoto allora  $\phi(U)$  contiene un aperto di  $Y$ ) e che ha la proprietà locale.

Mostreremo in questa sezione che se  $\phi: X \rightarrow Y$  è un morfismo dominante tra varietà irriducibili della stessa dimensione, la separabilità di  $\phi$  è equivalente alla separabilità dell'estensione dei rispettivi campi delle funzioni razionali.

**Teorema 12.6.2.** Sia  $\phi: X \rightarrow Y$  un morfismo regolare dominante di varietà quasiproiettive irriducibili della stessa dimensione definite su di un campo  $\mathbb{K}$  algebricamente chiuso. Denotiamo con  $\phi^*: \mathbb{K}(Y) \rightarrow \mathbb{K}(X)$  l'omomorfismo iniettivo indotto tra i rispettivi campi delle funzioni razionali. Allora l'estensione  $\phi^*\mathbb{K}(Y) \subset \mathbb{K}(X)$  è algebrica finita ed è separabile se e solo se esiste un aperto non vuoto  $U \subset X$  tale che il differenziale  $d\phi: T_x X \rightarrow T_y Y$  è bigettivo per ogni  $x \in U$ .

*Dimostrazione.* Dato che  $X, Y$  hanno la stessa dimensione, per il Corollario 12.3.5 le estensioni  $\mathbb{K} \subset \mathbb{K}(Y) = \phi^*\mathbb{K}(Y)$ ,  $\mathbb{K} \subset \mathbb{K}(X)$  hanno lo stesso grado di trascendenza e quindi  $\phi^*\mathbb{K}(Y) \subset \mathbb{K}(X)$  è una estensione algebrica; inoltre per il Lemma 12.3.1  $\mathbb{K}(X)$  è finitamente generato su  $\mathbb{K}$  e quindi a maggior ragione è finitamente generato su  $\phi^*\mathbb{K}(Y)$ . Se  $\mathbb{K}$  ha caratteristica 0, allora la seconda parte dell'enunciato è un caso particolare del teorema di Bertini-Sard 11.4.3: assumiamo quindi che  $\mathbb{K}$  abbia caratteristica  $p > 0$ . Non è restrittivo supporre  $X, Y$  affini e lisce di dimensione  $n$ ; inoltre, se  $Y \subset \mathbb{A}^m$ , allora la generica proiezione lineare  $Y \rightarrow \mathbb{A}^n$  ha differenziale bigettivo in un aperto denso di  $Y$  e quindi, per il Corollario 12.5.9, non è restrittivo assumere  $Y = \mathbb{A}^n$ ,  $X \subset \mathbb{A}^{m+n}$ ,  $m > 0$ , e  $\phi$  indotta dalla proiezione sulle ultime coordinate, cioè  $\phi(x_1, \dots, x_m, y_1, \dots, y_n) = (y_1, \dots, y_n)$ . In particolare  $\mathbb{K}(X)$  è generato su  $\mathbb{K}(Y) = \mathbb{K}(y_1, \dots, y_n)$  dalle coordinate  $x_1, \dots, x_m$ . Sia  $X_i \subset \mathbb{A}^1 \times \mathbb{A}^n$  la chiusura dell'immagine del morfismo

$$\phi_i: X \rightarrow \mathbb{A}^1 \times \mathbb{A}^n, \quad \phi_i(x_1, \dots, x_m, y_1, \dots, y_n) = (x_i, y_1, \dots, y_n).$$

La varietà  $X_i$  è una ipersuperficie affine irriducibile, denotiamo con  $F_i \in \mathbb{K}[x_i, y_1, \dots, y_n]$  un polinomio irriducibile che definisce  $X_i$ . Per il lemma di Gauss  $F_i$  è il prodotto di una funzione razionale su  $Y$  ed il polinomio minimo di  $x_i$  su  $\mathbb{K}(Y) = \mathbb{K}(y_1, \dots, y_n)$ . Il vettore  $(1, 0, \dots, 0)$  è tangente a  $X_i$  in ogni suo punto se e solo se  $F_i$  divide  $\frac{\partial F_i}{\partial x_i}$  e quindi se e solo se  $\frac{\partial F_i}{\partial x_i} = 0$ . Ne segue che  $x_i$  è separabile su  $\mathbb{K}(Y)$  se e solo se la proiezione  $X_i \rightarrow Y$  ha differenziale genericamente bigettivo. Se il differenziale di  $\phi$  è genericamente bigettivo, allora per ogni  $i$  anche il differenziale della proiezione  $X_i \rightarrow Y$  è genericamente bigettivo e quindi ogni  $x_i$  è separabile su  $\mathbb{K}(Y)$ . Per ogni  $x \in X$  sia  $\delta_x$  la dimensione del nucleo di  $d\phi: T_x X \rightarrow T_{\phi(x)} Y$ . Ricordiamo che  $x \mapsto \delta_x$  è semicontinua superiormente. Sia  $x$  un punto tale che  $\delta_x$  sia minima; se  $\delta_x > 0$  esiste un indice  $i$  tale che il nucleo del differenziale  $d\phi_i: T_x X \rightarrow T_{(x_i, \phi(x))} X_i$  ha dimensione minore di  $\delta_x$ . Questo implica che il differenziale della proiezione  $X_i \rightarrow Y$  è genericamente non iniettivo e quindi  $x_i$  non è separabile su  $\mathbb{K}(Y)$ .  $\square$

**Corollario 12.6.3.** *Per ogni varietà irriducibile  $X$  di dimensione  $n$  esiste una base di trascendenza  $t_1, \dots, t_n \in \mathbb{K}(X)$  su  $\mathbb{K}$  tale che l'estensione  $\mathbb{K}(t_1, \dots, t_n) \subset \mathbb{K}(X)$  è finita e separabile.*

*Dimostrazione.* Non è restrittivo supporre  $X \subset \mathbb{A}^m$  affine; siano  $t_1, \dots, t_m$  le coordinate affini su  $\mathbb{A}^m$ . Fissato un punto liscio  $x \in X$ , a meno di trasformazioni lineari possiamo assumere  $T_x X = \{t_{n+1} = \dots = t_m = 0\}$  e di conseguenza il differenziale della proiezione sulle prime  $n$  coordinate genericamente bigettivo. Per il Teorema 12.6.2 l'estensione  $\mathbb{K}(t_1, \dots, t_n) \subset \mathbb{K}(X)$  è algebrica separabile.  $\square$

## Esercizi

**12.14.** Sia  $\mathbb{K}$  un campo algebricamente chiuso e  $\mathbb{K} \subset L$  una estensione finitamente generata di campi. Dimostrare che esistono  $x_1, \dots, x_n \in L$  tali che  $\mathbb{K}(x_1, \dots, x_n) = L$ , dove  $x_1, \dots, x_{n-1}$  sono algebricamente indipendenti su  $\mathbb{K}$  e  $x_n$  è algebrico separabile su  $\mathbb{K}(x_1, \dots, x_{n-1})$ . (Sugg.: un tale campo  $L$  è il campo delle funzioni razionali di una ipersuperficie affine irriducibile.)

*Osservazione 12.6.4.* Il risultato dell'Esercizio 12.14 è vero anche se  $\mathbb{K}$  è perfetto (vedi Esercizi 12.27, 12.27 ed anche [Hart1977, p. 27]).

## 12.7 Esercizi complementari

**12.15.** Sia  $f: X \rightarrow Y$  un morfismo finito di varietà quasiproiettive e sia  $Z \subset Y$  un sottoinsieme localmente chiuso. Mostrare che  $f: f^{-1}(Z) \rightarrow Z$  è un morfismo finito.

**12.16.** Dare un esempio di morfismo quasifinito surgettivo che non è finito.

**12.17.** Dimostrare che per ogni scelta di  $p_1, \dots, p_n \in \mathbb{K}[t]$  non tutti costanti, il morfismo

$$\mathbb{A}^1 \rightarrow \mathbb{A}^n, \quad t \mapsto (p_1(t), \dots, p_n(t)),$$

è finito sull'immagine.

**12.18.** Siano  $f, g \in \mathbb{K}[x, y]$  omogenei. Provare che il morfismo  $(f, g): \mathbb{A}^2 \rightarrow \mathbb{A}^2$  è finito se e solo se  $f$  e  $g$  non hanno fattori comuni.

**12.19.** Se  $f: X_1 \rightarrow Y_1$  e  $g: X_2 \rightarrow Y_2$  sono due morfismi affini (resp.: finiti sull'immagine, finiti) allora anche  $f \times g: X_1 \times X_2 \rightarrow Y_1 \times Y_2$  è affine (resp.: finito sull'immagine, finito).

**12.20.** Sia  $X \subset \mathbb{A}^n$  un chiuso proprio e per ogni retta  $L \subset \mathbb{A}^n$  passante per l'origine indichiamo con  $\phi_L: X \rightarrow \mathbb{A}^n/L \simeq \mathbb{A}^{n-1}$  la restrizione ad  $X$  della proiezione lineare di nucleo  $L$ . Provare che l'insieme delle rette  $L$  tali che  $\phi_L$  è finito sull'immagine, contiene un aperto denso di  $\mathbb{P}^{n-1}$ . (Sugg.: considerare l'intersezione di  $\overline{X} \subset \mathbb{P}^n$  con l'iperpiano all'infinito.)

**12.21.** Siano  $\sigma_1, \dots, \sigma_n \in \mathbb{K}[x_1, \dots, x_n]$  le funzioni simmetriche elementari. Dimostrare che il morfismo regolare

$$\sigma = (\sigma_1, \dots, \sigma_n): \mathbb{A}^n \rightarrow \mathbb{A}^n$$

è finito. (Sugg.: estendere  $\sigma$  ad un morfismo  $(\mathbb{P}^1)^n \rightarrow \mathbb{P}^n$ .)

**12.22.** Sia  $X$  una varietà irriducibile di dimensione positiva su di un campo  $\mathbb{K}$  di caratteristica positiva. Mostrare che il campo  $\mathbb{K}(X)$  non è perfetto.

**12.23.** Siano  $h, g \in \mathbb{K}[x_1, \dots, x_n]$  polinomi omogenei non nulli, di gradi  $m, m+1$  rispettivamente e senza fattori comuni. Provare che l'ipersuperficie  $V(h+g) \subset \mathbb{A}^n$  è irriducibile e razionale. Dedurre che ogni quadrica affine irriducibile è razionale. (Sugg.: eseguire lo scoppimento  $x_1 = y_1, x_2 = y_1 y_2, \dots, x_n = y_1 y_n$ .)

**12.24.** (caratteristica 0) Dimostrare che ogni superficie cubica irriducibile  $X \subset \mathbb{P}^3$  è razionale. (Sugg.: se  $X$  è singolare usare l'Esercizio 12.23, se è liscia usare l'Esercizio 11.11.)

**12.25.** (caratteristica  $\neq 2, 3$ ) Mostrare che le curve affini

$$X = \{x^3 + y^3 = 1\} \subset \mathbb{A}^2, \quad Y = \{4x^3 - 12y^2 + 1 = 0\} \subset \mathbb{A}^2$$

sono birazionali. (Sugg.: considerare la chiusura  $\overline{X} \subset \mathbb{P}^2$ .)

**12.26 (Il discriminante di una estensione algebrica).** Sia  $K \subset L$  una estensione algebrica finita di campi di grado  $n$ . Dati  $a_1, \dots, a_n \in L$  definiamo il discriminante  $\Delta(a_1, \dots, a_n) = \det(\text{trace}_{L/K}(a_i a_j))$ . Provare che:

1. Se l'estensione è separabile e  $G(L/K) = \{\sigma_1, \dots, \sigma_n\}$ , allora vale  $\Delta(a_1, \dots, a_n) = \det(\sigma_i(a_j))^2$ .
2.  $\Delta(1, a, \dots, a^{n-1})$  è uguale al discriminante del polinomio caratteristico della moltiplicazione  $a: L \rightarrow L$ .

**12.27.** Siano  $K$  un campo perfetto di caratteristica  $p > 0$  e  $K \subset E$  una estensione finitamente generata con grado di trascendenza  $d$ . Dimostrare che esiste una base di trascendenza  $t_1, \dots, t_d \in E$  tale che l'estensione  $K(t_1, \dots, t_d) \subset E$  è separabile. (Sugg.: procedere nell'ordine:

1) in una estensione non algebrica di campi  $F \subset L$  gli elementi di  $L$  trascendenti su  $F$  generano  $L$  come  $K$ -spazio vettoriale.

2) per ogni  $t_1, \dots, t_s \in E$  il grado dell'estensione  $E^p(t_1, \dots, t_s) \subset E$  è maggiore o uguale di  $p^{d-s}$ .

3) costruire in modo ricorsivo elementi  $t_1, \dots, t_d$  tali che per ogni indice  $i$ :

- $t_i$  è trascendente su  $K(t_1, \dots, t_{i-1})$ .
- $t_i \notin E^p(t_1, \dots, t_s)$ .

4) applicare la Proposizione 12.5.16.)

**12.28 (Teorema dell'elemento primitivo).** Sia  $K \subset E$  una estensione finita separabile di campi. Dimostrare che:

1. Per ogni  $a \in E$  il grado dell'estensione  $K \subset K(a)$  è uguale alla cardinalità dell'insieme  $\{g(a) \mid g \in G(E/K)\} \subset \bar{K}$ .
2. Esiste  $a \in E$  tale che  $E = K(a)$ . (Sugg.: per ogni coppia  $g, h \in G(E/K)$ , l'insieme  $\{a \in E \mid g(a) = h(a)\}$  è un sottocampo e quindi un  $K$ -sottospazio vettoriale.)

**12.29.** Sia  $E$  un campo e  $G$  un gruppo finito di automorfismi di  $E$ . Sia  $n$  la cardinalità di  $G$  e denotiamo

$$E^G = \{a \in E \mid g(a) = a \text{ per ogni } g \in G\}.$$

Dimostrare che l'estensione  $E^G \subset E$  è finita separabile di grado  $n$ . (Sugg.: per ogni  $a \in E$ , l'insieme  $S_a = \{g \in G \mid g(a) = a\}$  è un sottogruppo di  $G$  e  $g(a)$  dipende solo dalla classe laterale  $gS_a \subset G$ . Osservare che  $a$  è radice del polinomio  $G$ -invariante  $\prod_{g \in G/S_a} (x - g(a)) \in E^G[x]$  e dedurre che  $a$  è separabile su  $E^G$  di grado  $\leq n$ . Usare la relazione  $n \leq [E : E^G]_s = [E : E^G]$  ed il teorema dell'elemento primitivo.)

**12.30.** Sia  $A$  un anello,  $G$  un gruppo finito di automorfismi di  $A$  e denotiamo con

$$A^G = \{a \in A \mid g(a) = a \text{ per ogni } g \in G\}$$

il sottoanello degli invarianti. Se la cardinalità di  $G$  è invertibile in  $A$  si definisce l'operatore di media

$$r: A \rightarrow A^G, \quad r(a) = \frac{1}{|G|} \sum_{g \in G} g(a).$$

Provare:

1. Se  $|G|$  è invertibile in  $A$  e  $A$  è Noetheriano, allora anche  $A^G$  è Noetheriano.
2. Se  $A$  è un dominio di integrità con campo delle frazioni  $F$ , allora il campo delle frazioni di  $A^G$  è isomorfo a  $F^G$ .
3. Sia  $K$  un campo,  $\sigma_1, \dots, \sigma_n \in K[x_1, \dots, x_n]$  le funzioni simmetriche elementari e  $G = \Sigma_n$  il gruppo simmetrico. Allora  $K(\sigma_1, \dots, \sigma_n) = K(x_1, \dots, x_n)^G$ , le funzioni  $\sigma_1, \dots, \sigma_n$  sono algebricamente indipendenti su  $K$  e l'estensione  $K(\sigma_1, \dots, \sigma_n) \subset K(x_1, \dots, x_n)$  è finita separabile di grado  $n!$ .

## Il polinomio di Hilbert

A partire da questo capitolo adotteremo un approccio più algebrico allo studio delle varietà, nella convinzione che il lettore abbia già sviluppato un sufficiente intuito geometrico. L'approccio algebrico, sebbene inizialmente più oscuro, consentirà una maggiore potenza di fuoco per risolvere i problemi. Il polinomio di Hilbert è un attributo algebrico delle varietà proiettive con il quale è possibile caratterizzarne in modo altamente algebrico il grado e la dimensione.

Come al solito, indicheremo con  $\mathbb{K}$  un campo algebricamente chiuso. Le strutture nelle quali si ambienta il polinomio di Hilbert sono le  $\mathbb{K}$ -algebre graduate e finitamente generate  $A = \bigoplus_{i \geq 0} A_i$ , con i gradi numeri naturali. Indicheremo sempre con  $A_+ \subset A$  l'ideale  $A_+ = \bigoplus_{i \geq 1} A_i$ .

### 13.1 Decomposizioni irriducibili

**Definizione 13.1.1.** Sia  $A = \bigoplus_{i \in \mathbb{N}} A_i$  un anello graduato. Diremo che un ideale omogeneo  $I \subset A$  è **irriducibile omogeneo** se ogniqualvolta  $I = J \cap H$ , con  $J, H$  ideali omogenei, vale  $I = J$  oppure  $I = H$ .

**Lemma 13.1.2.** Sia  $A = \bigoplus A_i$  un anello graduato Noetheriano ed  $I \subset A$  un ideale proprio irriducibile omogeneo. Allora la moltiplicazione

$$\frac{A}{I} \xrightarrow{\cdot x} \frac{A}{I}$$

per un elemento omogeneo  $x \in A$  è iniettiva se e solo se  $x \notin \sqrt{I}$ . In particolare  $\sqrt{I}$  è un ideale primo.

*Dimostrazione.* Considerando possibilmente l'anello quoziente  $A/I$  non è restrittivo supporre  $I = 0$  e di conseguenza  $\sqrt{I} = \sqrt{0}$  è l'ideale dei nilpotenti. È ovvio che la moltiplicazione per elementi di  $\sqrt{0}$  non è iniettiva. Viceversa siano  $x, y \in A$  omogenei, con  $x \notin \sqrt{0}$  e tali che  $xy = 0$ . L'anello  $A$  è Noetheriano e quindi la catena di ideali annullatori  $\dots \text{Ann}(x^n) \subset \text{Ann}(x^{n+1}) \dots$  è stazionaria: fissiamo un intero  $n$  tale che  $\text{Ann}(x^n) = \text{Ann}(x^{n+1})$  e consideriamo un elemento

$$a = bx^n = cy \in (x^n) \cap (y).$$

Siccome  $bx^{n+1} = cxy = 0$  si ha  $b \in \text{Ann}(x^{n+1})$  e quindi  $b \in \text{Ann}(x^n)$ ,  $a = 0$ ; questo prova che  $(x^n) \cap (y) = 0$  e siccome, l'ideale  $0$  è per ipotesi irriducibile e  $x^n \neq 0$ , allora deve essere  $y = 0$ . Se  $x \notin \sqrt{0}$  e  $xy \in \sqrt{0}$ , allora  $x^n y^n = 0$  e quindi  $y^n = 0$  per  $n \gg 0$ .  $\square$

Una **decomposizione irriducibile** di un ideale omogeneo  $I \subset A$  è una relazione di intersezione finita  $I = I_1 \cap \dots \cap I_k$ , con gli ideali  $I_j$  irriducibili omogenei. La decomposizione si dice **minimale** se nessuno degli ideali  $I_j$  può essere omesso, cioè se per ogni  $j = 1, \dots, k$  vale  $I \neq \bigcap_{i \neq j} I_i$ ; è evidente che da ogni decomposizione irriducibile se ne può estrarre una minimale (generalmente in modo non unico).

**Lemma 13.1.3.** *Sia  $A = \bigoplus A_i$  un anello graduato Noetheriano. Allora ogni ideale proprio omogeneo  $I \subset A$  possiede una decomposizione irriducibile*

$$I = I_1 \cap I_2 \cap \dots \cap I_s.$$

Inoltre, il nucleo della moltiplicazione  $\frac{A}{I} \xrightarrow{\cdot x} \frac{A}{I}$  per un elemento omogeneo  $x \in A$  è contenuto in

$$\bigcap \{I_h \mid h = 1, \dots, s \text{ e } x \notin \sqrt{I_h}\}$$

e quindi il suo annullatore  $\text{Ann}(\text{Ker}(x))$  contiene l'intersezione degli ideali  $I_k$  tali che  $x \in \sqrt{I_k}$ .

*Dimostrazione.* Denotiamo con  $\mathcal{A}$  la famiglia degli ideali omogenei di  $A$  che non sono intersezione finita di ideali irriducibili omogenei. Se  $\mathcal{A}$  fosse  $\neq \emptyset$ , allora scelto un elemento massimale  $I \in \mathcal{A}$ , si avrebbe che  $I$  non è irriducibile ed esistono due ideali omogenei  $J, H \notin \mathcal{A}$  tali che  $I = J \cap H$ . Sia  $J$  che  $H$  sono intersezione finita di ideali irriducibili omogenei e quindi anche  $I$  lo è. A meno di permutare gli indici possiamo supporre  $x \notin \sqrt{I_h}$  per  $h \leq r$  e  $x \in \sqrt{I_k}$  per  $k > r$ . Se  $xy \in I$ , allora per il Lemma 13.1.2 deve essere  $y \in I_h$  per ogni  $h \leq r$  e quindi se  $z \in I_{r+1} \cap \dots \cap I_s$  vale  $zy \in I$ .  $\square$

Riepilogando, se  $I = I_1 \cap I_2 \cap \dots \cap I_s$  è una decomposizione irriducibile, allora per ogni elemento omogeneo  $x \in A$  vale

$$(I : x) := \{a \in A \mid ax \in I\} \subset \bigcap_{x \notin \sqrt{I_j}} I_j, \quad \bigcap_{x \in \sqrt{I_j}} I_j \subset \{a \in A \mid a(I : x) \subset I\}.$$

L'Esercizio 13.1 mostra che un ideale può avere infinite decomposizioni irriducibili minimali.

**Lemma 13.1.4.** *Siano  $A = \bigoplus_{n \geq 0} A_n$  un anello graduato Noetheriano e  $M = \bigoplus_{n \geq 0} M_n$  un  $A$ -modulo graduato finitamente generato. Allora vale  $M_n = 0$  per  $n \gg 0$  se e solo se esiste un ideale omogeneo  $H = \bigoplus H_n \subset A_+$  tale che  $HM = 0$  e  $H_n = A_n$  per  $n \gg 0$ .*

*Dimostrazione.* Se  $M_n = 0$  per ogni  $n \geq s$ , allora basta considerare l'ideale  $H = \bigoplus_{n > s} A_n$ . Viceversa se esiste un ideale omogeneo  $H$  tale che  $H_n = A_n$  per  $n \gg 0$  e  $HM = 0$ , allora anche  $A_n M = 0$  per  $n \gg 0$  ed essendo  $M$  finitamente generato ne consegue che  $M_n = 0$  per  $n \gg 0$ .  $\square$

**Lemma 13.1.5.** *Sia  $A_0$  una  $\mathbb{K}$ -algebra Noetheriana ed  $I \subset A_0[x_0, \dots, x_m] = \bigoplus_{n \geq 0} A_n$  un ideale omogeneo. Allora per il generico polinomio omogeneo  $f \in \mathbb{K}[x_0, \dots, x_m]$  di grado  $d$  esiste un intero positivo  $n_0$  tale che la moltiplicazione*

$$\frac{A_{n-d}}{I_{n-d}} \xrightarrow{\cdot f} \frac{A_n}{I_n}$$

è iniettiva per ogni  $n \geq n_0$ .



*Dimostrazione.* Denotiamo con  $R_d \subset \mathbb{K}[x_0, \dots, x_m]$  il sottospazio vettoriale dei polinomi omogenei di grado  $d$ . L'anello graduato  $A_0[x_0, \dots, x_m] = A_0 \oplus A_+$  è Noetheriano e quindi esiste una decomposizione irriducibile minimale dell'ideale  $I$ , diciamo

$$I = J_1 \cap \dots \cap J_r \cap H_1 \cap \dots \cap H_s,$$

dove  $A_+ \not\subset \sqrt{J_h}$  e  $A_+ \subset \sqrt{H_k}$  per ogni  $h, k$ . Se  $r = 0$  oppure  $d = 0$ , allora il risultato è banale: nel primo caso perché  $A_n = I_n$  per  $n \gg 0$ , nel secondo perché il generico polinomio di grado 0 è invertibile. Possiamo quindi supporre  $d, j > 0$  e quindi che  $R_d \cap \sqrt{J_h}$  è un  $\mathbb{K}$ -sottospazio vettoriale proprio per ogni  $h = 1, \dots, r$ . Dunque il generico polinomio  $f \in R_d$  non appartiene a  $\cup_h \sqrt{J_h}$  e quindi, per il Lemma 13.1.3, il nucleo  $K = \oplus K_n$  della moltiplicazione per  $f$  è annullato da  $H = H_1 \cap \dots \cap H_s$ . Siccome  $A_+ \subset \cap \sqrt{H_k} = \sqrt{H}$  ne segue, per il Lemma 13.1.4 che esiste  $n_0$  tale che  $K_n = 0$  per  $n \geq n_0$ .  $\square$

**Esercizi**

**13.1.** Verificare che  $(x^2, xy) = (x) \cap (x^2, y+ax)$  è una decomposizione irriducibile minimale in  $\mathbb{C}[x, y]$  per ogni  $a \in \mathbb{C}$  e dedurre che la decomposizione irriducibile di un ideale non è, in generale, sostanzialmente unica.

**13.2.** Quali dei seguenti ideali sono irriducibili?

1.  $\mathfrak{q} = (x, y^2) \subset \mathbb{C}[x, y]$ .
2.  $\mathfrak{q} = (x, z) \subset \frac{\mathbb{C}[x, y, z]}{(xy - z^2)}$
3.  $\mathfrak{q} = (x, z)^2 \subset \frac{\mathbb{C}[x, y, z]}{(xy - z^2)}$

**13.3.** Trovare esempi di ideali irriducibili che non sono primi e di ideali non irriducibili il cui radicale è un ideale primo.

**13.2 Il polinomio di Hilbert**

Consideriamo come anello graduato  $A = \oplus A_n = \mathbb{K}[x_0, \dots, x_m]$ , dove  $A_n$  indica il  $\mathbb{K}$ -spazio vettoriale, di dimensione  $\binom{n+m}{m}$ , dei polinomi omogenei di grado  $n$ .

**Definizione 13.2.1.** La *Serie di Poincaré* di un ideale omogeneo  $I = \oplus I_n \subset A$  è

$$P(I, t) = \sum_{n=0}^{+\infty} \dim_{\mathbb{K}} \left( \frac{A_n}{I_n} \right) t^n \in \mathbb{Z}[[t]].$$

Ad esempio la serie di Poincaré dell'ideale nullo in  $\mathbb{K}[x_0, \dots, x_m]$  è

$$P(0, t) = \sum_{n=0}^{+\infty} \binom{n+m}{m} t^n.$$

**Lemma 13.2.2.** Sia  $I \subset \mathbb{K}[x_0, \dots, x_m]$  un ideale omogeneo e  $f \in \mathbb{K}[x_0, \dots, x_m]$  un polinomio omogeneo di grado  $d > 0$ . Se:

- $f$  è generico, oppure
- $I$  è un ideale primo e  $f \notin I$ ,

allora  $(1 - t^d)P(I, t) - P(I + (f), t)$  è un polinomio in  $t$ .

*Dimostrazione.* Denotiamo con  $K$  il nucleo della moltiplicazione per  $f$ . Si hanno le successioni esatte

$$\begin{aligned} 0 \longrightarrow K \longrightarrow \frac{A}{I} \xrightarrow{f} \frac{A}{I} \longrightarrow \frac{A}{I + (f)} \longrightarrow 0, \\ 0 \longrightarrow K_{n-d} \longrightarrow \frac{A_{n-d}}{I_{n-d}} \xrightarrow{f} \frac{A_n}{I_n} \longrightarrow \frac{A_n}{I_n + fA_{n-d}} \longrightarrow 0. \end{aligned}$$

Nel secondo caso  $K = 0$ , mentre nel primo caso, in base al Lemma 13.1.5, esiste  $n_0 \in \mathbb{N}$  tale che  $K_n = 0$  per ogni  $n \geq n_0$ . In ogni caso vale

$$\begin{aligned} (1 - t^d)P(I, t) &= P(I, t) - t^d P(I, t) = \sum_{n=0}^{+\infty} \left( \dim_{\mathbb{K}} \frac{A_n}{I_n} - \dim_{\mathbb{K}} \frac{A_{n-d}}{I_{n-d}} \right) t^n \\ &= \sum_{n=0}^{+\infty} \left( \dim_{\mathbb{K}} \frac{A_n}{I_n + fA_{n-d}} - \dim_{\mathbb{K}} K_{n-d} \right) t^n = P(I + (f), t) - \sum_{n=1}^{n_0} \dim_{\mathbb{K}} K_{n-d} t^n. \end{aligned}$$

□

**Teorema 13.2.3.** Per ogni ideale omogeneo  $I \subset A_+ \subset \mathbb{K}[x_0, \dots, x_m]$  è possibile scrivere la serie di Poincaré nella forma

$$P(I, t) = \frac{f(t)}{(1-t)^{d+1}},$$

dove  $f(t) \in \mathbb{Z}[t]$  è un polinomio tale che  $f(1) > 0$  e  $d$  è un numero intero  $\geq -1$ .

*Dimostrazione.* Se  $P(I, t)$  è un polinomio, allora basta porre  $d = -1$  e  $f(t) = P(I, t)$ . In tal caso  $f(1)$  è uguale alla dimensione di  $A/I = \mathbb{K} \oplus A_+/I$  come  $\mathbb{K}$ -spazio vettoriale e quindi  $f(1) > 0$ . Assumiamo quindi che  $P(I, t)$  non sia un polinomio e dimostriamo il teorema per induzione sulla dimensione  $h$  del  $\mathbb{K}$ -spazio vettoriale  $A_1/(\sqrt{I} \cap A_1)$ . Se  $h = 0$ , allora  $A_1 \subset \sqrt{I}$  e la serie di Poincaré è un polinomio. Se  $h > 0$ , allora consideriamo un generico elemento  $x \in A_1 - \sqrt{I}$ . Per il Lemma 13.2.2, la differenza  $h(t) := P(I + (x), t) - (1-t)P(I, t) \in \mathbb{Z}[t]$  è un polinomio. Per l'ipotesi induttiva possiamo scrivere

$$P(I + (x), t) = \frac{g(t)}{(1-t)^d},$$

con  $g(t) \in \mathbb{Z}[t]$ ,  $d \geq 0$  e  $g(1) > 0$ . Dunque

$$P(I, t) = \frac{g(t) - (1-t)^d h(t)}{(1-t)^{d+1}} = \frac{f(t)}{(1-t)^{d+1}}.$$

Se  $d > 0$ , allora  $f(1) = g(1) > 0$ . Se invece  $d = 0$ , allora  $P(I, t) - f(1)(1-t)^{-1} \in \mathbb{Z}[t]$  e quindi  $f(1)$  è uguale alla dimensione di  $A_n/I_n$  per  $n \gg 0$ . Poiché per ipotesi  $x \notin \sqrt{I}$  si ha  $x^n \notin I$  per ogni  $n$  e quindi  $f(1) > 0$ . □

*Esempio 13.2.4.* È facile dimostrare (vedi Esercizio 1.4) che per ogni  $s \geq 0$  si ha

$$\frac{1}{(1-t)^{s+1}} = \sum_{n=0}^{+\infty} \binom{s+n}{s} t^n.$$

e quindi la serie di Poincaré dell'ideale nullo in  $\mathbb{K}[x_0, \dots, x_m]$  è uguale a

$$P(0, t) = \frac{1}{(1-t)^{m+1}}.$$

**Definizione 13.2.5.** *Sull'insieme degli ideali omogenei contenuti in  $\mathbb{K}[x_0, \dots, x_m]$  consideriamo la relazione di equivalenza  $I = \oplus I_n \sim J = \oplus J_n$  se esiste  $n_0 \in \mathbb{N}$  tale che  $I_n = J_n$  per ogni  $n > n_0$ , e denotiamo con  $Z(I)$  la classe di equivalenza di un ideale  $I$ . Chiameremo  $Z(I)$  **sottoschema chiuso**<sup>1</sup> di  $\mathbb{P}^m$ .*

Per assegnare un vago sapore geometrico ai sottoschemi, scriveremo con un po' di ambiguità  $\mathbb{P}^m = Z(0)$ . Poniamo inoltre  $Z(I) \subset Z(J)$  se  $J_n \subset I_n$  per ogni  $n$  sufficientemente grande. In particolare la notazione  $Z(I) \subset \mathbb{P}^m$  indicherà che  $Z(I)$  è un sottoschema chiuso di  $\mathbb{P}^m$ .

Vogliamo adesso indagare quali sono i parametri della serie di Poincaré invarianti per la relazione di equivalenza  $\sim$ , ovvero che dipendono solamente da  $Z(I)$ . Per fare questo occorre analizzare il comportamento asintotico di  $P(I, t)$ .

Sia  $P(I, t) = \frac{f(t)}{(1-t)^{1+d}}$ , con  $f(1) > 0$ , la serie di Poincaré di un ideale omogeneo  $I$ : considerando lo sviluppo di Taylor di  $f$  nel punto  $t = 1$  possiamo scrivere

$$P(I, t) = \frac{1}{(1-t)^{d+1}} \sum_{i=0}^{+\infty} \frac{d^i f}{dt^i}(1) \frac{(t-1)^i}{i!} = \sum_{i=0}^{\deg(f)} \frac{(-1)^i}{i!} \frac{d^i f}{dt^i}(1) \frac{1}{(1-t)^{d+1-i}}.$$

Quindi per ogni  $n \geq \deg(f) - d$  il coefficiente di  $t^n$  in  $P(I, t)$  è uguale al coefficiente di  $t^n$  nella serie

$$\sum_{i=0}^d \frac{(-1)^i}{i!} \frac{d^i f}{dt^i}(1) \sum_{n=0}^{+\infty} \binom{d-i+n}{d-i} t^n.$$

Ne deduciamo che il polinomio

$$\begin{aligned} p_{Z(I)}(x) &= \sum_{i=0}^d \frac{(-1)^i}{i!} \frac{d^i f}{dt^i}(1) \binom{x+d-i}{d-i} \\ &= \sum_{i=0}^d \frac{(-1)^i}{i!(d-i)!} \frac{d^i f}{dt^i}(1) \prod_{j=0}^{d-i-1} (x+d-i-j) \in \mathbb{Q}[x]. \end{aligned}$$

è tale che  $\dim_{\mathbb{K}}(A_n/I_n) = p_{Z(I)}(n)$  per ogni  $n \geq \deg(f) - d$ . In particolare  $p_{Z(I)}(t)$  non dipende dalla scelta di  $I$  all'interno della classe di equivalenza  $Z(I)$ . Se  $d = -1$  si pone convenzionalmente  $p_{Z(I)} = 0$ .

**Definizione 13.2.6.** *Il polinomio  $p_{Z(I)}(x)$  si dice **Polinomio di Hilbert** di  $Z(I)$ .*

**Lemma 13.2.7.** *Sia  $P(I, t) = \frac{f(t)}{(1-t)^{1+d}}$ , con  $f(1) > 0$ , la serie di Poincaré di un ideale omogeneo  $I$ . Allora il grado di  $p_{Z(I)}(x)$  è uguale a  $d$  ed il suo coefficiente direttore è uguale  $f(1)/d!$ .*

*Dimostrazione.* Il polinomio  $\binom{x+d-i}{d-i} \in \mathbb{Q}[x]$  ha grado  $d-i$  e quindi

$$p_{Z(I)}(x) = f(1) \binom{x+d}{d} + \sum \{\text{polinomi di grado } < d\} = \frac{f(1)}{d!} x^d + \dots$$

□

<sup>1</sup> Si indica con  $\text{Hilb}(\mathbb{P}^m)$  la famiglia dei sottoschemi chiusi di  $\mathbb{P}^m$ . Si deve a Grothendieck una descrizione geometrica degli  $Z(I)$  come spazi topologici dotati di fascio strutturale, e la dimostrazione che  $\text{Hilb}(\mathbb{P}^m)$  è a sua volta unione numerabile di sottoschemi chiusi detti in gergo *Schemi di Hilbert*.

**Definizione 13.2.8.** *Sia*

$$P(I, t) = \frac{f(t)}{(1-t)^{1+d}}, \quad f(1) > 0$$

la serie si Poincaré di un ideale omogeneo  $I \subset A_+$ . Il numero  $d = \dim Z(I)$  si dice la **dimensione** di  $Z(I)$ . Se  $d \geq 0$ , si definisce il **grado** di  $Z(I)$  come  $\deg(Z(I)) = f(1) > 0$ . Se  $d = -1$  si pone per convenzione  $\deg(Z(I)) = 0$ .

Ad esempio la dimensione di  $Z(0) = \mathbb{P}^m$  è uguale ad  $m$ , mentre il grado di  $Z(0)$  è uguale ad 1.

Segue dal Lemma 13.2.7 che la dimensione ed il grado possono essere dedotti dal polinomio di Hilbert e che quindi non dipendono dalla scelta di  $I$  nella sua classe di equivalenza. Infatti, se  $p_{Z(I)} = 0$  allora  $\dim Z(I) = -1$  e  $\deg(Z(I)) = 0$ , mentre se  $p_{Z(I)} \neq 0$ , allora  $\dim Z(I) = \deg p_{Z(I)}$  e  $\frac{\deg(Z(I))}{d!}$  è il coefficiente direttore di  $p_{Z(I)}$ . Osserviamo inoltre che se  $\dim Z(I) = 0$ , allora  $\deg(Z(I))$  è uguale alla dimensione dello spazio vettoriale  $A_n/I_n$  per  $n \gg 0$ .

**Lemma 13.2.9.** *Siano  $Z(I) \subset Z(J) \subset \mathbb{P}^m$  due sottoschemi chiusi. Allora vale  $\dim Z(I) \leq \dim Z(J)$  e, se vale  $\dim Z(I) = \dim Z(J)$ , allora  $\deg(Z(I)) \leq \deg(Z(J))$ .*

*Dimostrazione.* Per definizione  $Z(I) \subset Z(J)$  se e solo se  $J_n \subset I_n$  per  $n \gg 0$  e quindi  $p_{Z(I)}(n) \leq p_{Z(J)}(n)$  per ogni intero  $n$  sufficientemente grande.  $\square$

**Corollario 13.2.10.** *Se  $I$  è un ideale primo, allora  $\deg(Z(I, f)) = \deg(f) \deg(Z(I))$  per ogni  $f \notin I$  omogeneo.*

*Dimostrazione.* Immediata conseguenza del Lemma 13.2.2.  $\square$

**Corollario 13.2.11.** *Sia  $I \subset \mathbb{K}[x_0, \dots, x_m]$  un ideale omogeneo e sia  $x$  una generica combinazione lineare di  $x_0, \dots, x_m$  a coefficienti in  $\mathbb{K}$ .*

1. *Se  $\dim Z(I) \geq 0$ , allora  $\dim Z(I + (x)) = \dim Z(I) - 1$ .*
2. *Se  $\dim Z(I) > 0$ , allora  $\deg(Z(I + (x))) = \deg(Z(I))$ .*

*Dimostrazione.* Per il Lemma 13.2.2 le due serie  $P(I + (x), t)$  e  $(1-t)P(I, t)$  differiscono per un polinomio.  $\square$

**Lemma 13.2.12.** *Per ogni coppia di ideali omogenei  $I, J \subset A = \mathbb{K}[x_0, \dots, x_m]$  vale*

$$P(I \cap J, t) = P(I, t) + P(J, t) - P(I + J, t),$$

$$p_{Z(I \cap J)} = p_{Z(I)} + p_{Z(J)} - p_{Z(I+J)}.$$

*Dimostrazione.* Immediata conseguenza della successione esatta

$$0 \longrightarrow \frac{A}{I \cap J} \longrightarrow \frac{A}{I} \oplus \frac{A}{J} \longrightarrow \frac{A}{I + J} \longrightarrow 0.$$

$\square$

**Esercizi**

**13.4.** Un polinomio  $p(x) \in \mathbb{Q}[x]$  si dice un **polinomio numerico** se  $p(n) \in \mathbb{Z}$  per ogni intero  $n \gg 0$ . Provare che:

1. Se  $p(x)$  è un polinomio numerico, allora  $p(n) \in \mathbb{Z}$  per ogni  $n \in \mathbb{Z}$  (Sugg.: il polinomio  $q(x) = p(x+1) - p(x)$  è numerico.)
2. Lo  $\mathbb{Z}$ -modulo dei polinomi numerici è libero ed una sua base è data dai polinomi

$$\binom{x}{d} = \frac{1}{d!} \prod_{j=0}^{d-1} (x-j), \quad d \in \mathbb{N}.$$

3. Con la relazione di ordine,  $p \geq q$  se e solo se  $p(n) \geq q(n)$  per  $n \gg 0$ , i polinomi numerici sono un insieme totalmente ordinato.

**13.5.** Se  $\dim Z(I) > 0$ , provare che per il generico elemento  $x \in A$  omogeneo di grado  $s$  vale  $\deg(Z(I+(x))) = s \deg(Z(I))$ .

**13.6.** Provare che se  $\sqrt{I} = \sqrt{J}$ , allora  $\dim Z(I) = \dim Z(J)$ . (Sugg.: provare prima che  $\dim Z(I) = -1$  se e solo se  $\dim Z(J) = -1$ , poi mostrare che  $\sqrt{I+(x)} = \sqrt{J+(x)}$  per ogni  $x \in A$ .)

**13.7.** Sia  $I \subset A_+$  un ideale omogeneo ed  $f \in A$  un polinomio omogeneo. Dimostrare che  $\dim Z(I) \geq \dim Z(I+(f)) \geq \dim Z(I) - 1$ . (Sugg.: utilizzare le successioni esatte

$$\frac{A_{n-d}}{I_{n-d}} \xrightarrow{f} \frac{A_n}{I_n} \rightarrow \frac{A_n}{(I+(f))_n} \rightarrow 0, \quad d = \deg f,$$

per mostrare che per  $n \gg 0$  vale  $p_{Z(I)}(n) \geq p_{Z(I+(f))}(n) \geq p_{Z(I)}(n) - p_{Z(I)}(n-d)$ .)

**13.3 Varietà proiettive come sottoschemi**

Continuiamo adesso il lavoro delle sezioni precedenti, sempre assumendo che  $\mathbb{K} = \overline{\mathbb{K}}$  sia un campo algebricamente chiuso. Tra i vari risultati, più o meno tecnici, mostreremo che ad ogni varietà proiettiva  $X \subset \mathbb{P}^n$  è associato in modo canonico un sottoschema chiuso  $Z(I(X)) \subset \mathbb{P}^n$  per il quale le nozioni di dimensione e grado definite per via algebrica in questo capitolo corrispondono alle stesse nozioni definite geometricamente nel Capitolo 9.

Per ogni ideale omogeneo  $J \subset \mathbb{K}[x_0, \dots, x_m]$  denotiamo con  $V(J) \subset \mathbb{P}^m$  il chiuso dei punti  $p$  che annullano tutti i polinomi omogenei di  $J$  e per ogni chiuso  $X \subset \mathbb{P}^m$  denotiamo con  $I(X) \subset A_+$  l'ideale generato dai polinomi omogenei di grado positivo che si annullano su  $X$ . Per il teorema degli zeri omogeneo  $I(V(J)) = \sqrt{J}$  per ogni  $J \subset A_+$ . Se  $I \sim J$ , allora  $\sqrt{I} = \sqrt{J}$  e dunque  $V(I) = V(J)$ . Infine scriveremo  $X \subset Z(J)$  se  $Z(I(X)) \subset Z(J)$ , o equivalentemente se  $X \subset V(J)$ . In particolare per un punto  $p \in \mathbb{P}^m$  la condizione  $p \in Z(I)$  è perfettamente equivalente a  $p \in V(I)$ .

**Lemma 13.3.1.** Per ogni ideale omogeneo  $I \subset A_+$  vale

$$\dim Z(I) = \dim V(I).$$

*Dimostrazione.* Procediamo per induzione sulla dimensione di  $V(I)$ : per il teorema degli zeri vale  $V(I) = \emptyset$  se e solo se  $\sqrt{I} = A_+$  ed abbiamo già convenuto che tale condizione è equivalente a  $\dim Z(I) = -1$ . Se  $V(I) \neq \emptyset$  e  $\dim Z(I) \geq 0$ , allora segue dal Teorema 9.6.5 e dal Corollario 13.2.11 che per il generico iperpiano  $H = \{x = 0\}$ , con  $x \in A_1$ , vale  $\dim V(I+(x)) = \dim(V(I) \cap H) = \dim V(I) - 1$  e  $\dim Z(I+(x)) = \dim Z(I) - 1$ .  $\square$

**Definizione 13.3.2.** Sia  $I$  un ideale omogeneo tale che  $V(I) \neq \emptyset$ ; per ogni  $p \in V(I)$  denotiamo con  $I_p$  l'ideale formato dai polinomi  $f \in A_+$  tali che  $fg \in I$  per qualche polinomio omogeneo  $g \in A_+$  con  $g(p) \neq 0$ .

Dato che, nella Definizione 13.3.2, il polinomio  $g$  ha grado positivo, ne segue facilmente che se  $I \sim J$  allora  $I_p = J_p$ . La stessa dimostrazione del Lemma 10.8.1 mostra che  $V(I_p)$  è l'unione delle componenti irriducibili di  $V(I)$  che contengono il punto  $p$ .

**Lemma 13.3.3.** Nelle notazioni della Definizione 13.3.2, se  $I = J_1 \cap \dots \cap J_s$  è una decomposizione irriducibile minimale e  $p \in V(I)$ , allora

$$I_p = \bigcap_{p \in V(J_i)} J_i$$

è una decomposizione irriducibile minimale.

*Dimostrazione.* Se  $f \in I_p$ , allora esiste  $g$  omogeneo tale che  $g(p) \neq 0$  e  $gf \in I$ ; per il Lemma 13.1.3 si ha che  $f \in J_i$  per ogni  $i$  tale che  $g \notin \sqrt{J_i}$  e quindi a maggior ragione  $f \in J_i$  per ogni  $i$  tale che  $p \in V(J_i)$ . Viceversa se  $f$  appartiene all'intersezione dei  $J_i$  tali che  $p \in V(J_i)$ , allora per ogni  $h$  con  $p \notin V(J_h)$  possiamo trovare  $a_h \in J_h$  tale che  $a_h(p) \neq 0$ . Il prodotto di  $f$  con tutti gli  $a_h$  appartiene ad  $I$  e quindi  $f \in I_p$ .  $\square$

**Definizione 13.3.4.** Sia  $I \subset A_+ \subset \mathbb{K}[x_0, \dots, x_m]$  un ideale omogeneo e sia  $p \in Z(I)$  un punto di  $\mathbb{P}^m$ :

1.  $p$  si dice un **punto singolare** di  $Z(I)$  se, per ogni scelta di  $f_1, \dots, f_s \in I$  polinomi omogenei, il rango della matrice  $\left( \frac{\partial f_i}{\partial x_j}(p) \right)$  è strettamente minore di  $m - \dim_p V(I)$ .
2.  $p$  si dice un **punto immerso** di  $Z(I)$  se esiste un divisore di 0 in  $A/I_p$  che è omogeneo e non si annulla in alcuna componente irriducibile di  $V(I_p)$ .

Denoteremo con  $\text{Sing}(Z(I)), \text{Imm}(Z(I)) \subset V(I)$  gli insiemi dei punti singolari e immersi di  $Z(I)$ , rispettivamente.

Si noti che se  $g_1, \dots, g_r$  è un insieme di generatori omogenei dell'ideale  $I$ , un punto  $p \in Z(I)$  è singolare se e solo se il rango della matrice  $\left( \frac{\partial g_i}{\partial x_j}(p) \right)$  è minore di  $m - \dim_p V(I)$ . In completa analogia con il caso delle varietà possiamo definire lo spazio tangente proiettivo. Se  $I \subset A_+ \subset \mathbb{K}[x_0, \dots, x_m]$  è un ideale omogeneo e  $p \in V(I)$  si definisce

$$\mathbb{T}_p(Z(I)) = \left\{ [v_0, \dots, v_n] \in \mathbb{P}^n \mid \sum_{j=0}^n v_j \frac{\partial f}{\partial x_j}(p) = 0 \text{ per ogni } f \in I \right\}.$$

È chiaro che  $\mathbb{T}_p(V(I)) \subset \mathbb{T}_p(Z(I))$  e che  $p$  è un punto singolare di  $Z(I)$  se e solo se  $\dim \mathbb{T}_p(Z(I)) > \dim_p V(I)$ .

Notiamo che  $p \in \text{Sing}(Z(I))$  se e solo se  $p \in \text{Sing}(Z(I_p))$  e quindi  $\text{Sing}(Z(I))$  dipende solo dalla classe di equivalenza di  $I$ . Dalla semicontinuità del rango segue che, se  $V(I)$  è irriducibile, e quindi equidimensionale, allora  $\text{Sing}(Z(I))$  è un sottoinsieme chiuso di  $V(I)$ .

Se  $V(I)$  non è irriducibile, poiché i punti singolari di  $V(I)$  sono contenuti in  $\text{Sing}(Z(I))$ , i punti appartenenti a più di una componente irriducibile sono punti singolari di  $Z(I)$  e ragionando come in 10.8.4 si deduce che  $\text{Sing}(Z(I))$  è un sottoinsieme chiuso di  $V(I)$ . Se  $I = I(X)$  è l'ideale di una varietà proiettiva, allora  $\text{Sing}(Z(I))$  coincide con il chiuso dei punti singolari di  $X$ . Notiamo che, se  $I$  non è un ideale radicale, può succedere che

$\text{Sing}(Z(I)) = V(I)$ . I punti immersi hanno invece un comportamento più ragionevole: dimostreremo tra breve che i punti non immersi formano sempre un aperto denso. Ovviamente se  $p$  è un punto immerso, allora  $A/I_p$  non è un dominio di integrità, quindi  $I_p$  non è un ideale primo e, per il Teorema 10.8.2,  $p$  è un punto singolare. Si deduce quindi che  $\text{Imm}(Z(I)) \subset \text{Sing}(Z(I)) \subset V(I)$ .

**Definizione 13.3.5.** Sia  $I = J_1 \cap \cdots \cap J_s$  una decomposizione irriducibile di un ideale omogeneo  $I \subset \mathbb{K}[x_0, \dots, x_m]$ . Diremo che un ideale  $J_i$  è un elemento **isolato** della decomposizione se  $V(J_i)$  è una componente irriducibile di  $V(I)$ . Diremo invece che  $J_i$  è un elemento **immerso** se  $V(J_i)$  non è una componente irriducibile di  $V(I)$ .

La Definizione 13.3.5 è sensata in quanto  $V(I) = \cup_i V(J_i)$  ed abbiamo già dimostrato che  $\sqrt{J_i}$  è un ideale primo e quindi  $V(J_i) = V(\sqrt{J_i})$  è un chiuso irriducibile.

**Lemma 13.3.6.** Sia  $I$  ideale omogeneo e sia  $I = J_1 \cap \cdots \cap J_s$  una decomposizione irriducibile omogenea minimale. Allora vale

$$\text{Imm}(Z(I)) = \cup \{V(J_i) \mid J_i \text{ è un ideale immerso} \}.$$

In particolare  $\text{Imm}(Z(I))$  è un chiuso proprio di  $V(I)$ .

*Dimostrazione.* A meno di permutazioni degli indici possiamo assumere che esista un intero  $r \leq s$  tale che  $J_i$  è immerso se e solo se  $i > r$  e quindi  $V(J_1), \dots, V(J_r)$  sono tutte e sole le componenti irriducibili di  $V(I)$ . Per il Lemma 13.3.3, per ogni  $p \in V(I)$  esiste almeno un indice  $j \leq r$  tale che  $p \in V(J_j)$  ed una decomposizione irriducibile minimale

$$I_p = \bigcap_{p \in V(J_i)} J_i.$$

Sia  $h > r$  e  $p \in V(J_h)$ ; vogliamo dimostrare che  $p$  è immerso. Possiamo scrivere  $I_p = J_h \cap H_p$ , dove  $H_p$  è l'intersezione degli ideali  $J_i$  tali che  $i \neq h$  e  $p \in V(J_i)$ . Siccome la decomposizione è assunta minimale, esiste  $h \in H_p - I_p$  ed anche un  $f \in J_h - I_p$  che non si annulla in alcuna componente irriducibile di  $V(I)$ ; chiaramente  $fh \in I_p$  e quindi  $p \in \text{Imm}(Z(I))$ .

Viceversa se  $p \in \text{Imm}(Z(I))$  allora esistono  $h, f \notin I_p$  tali che  $f \notin \sqrt{J_i}$  per ogni  $i = 1, \dots, r$  e  $fh \in I_p$ . Per il Lemma 13.1.3, applicato alla decomposizione irriducibile di  $I_p$ , deve esistere  $i > r$  tale che  $p \in V(J_i)$ .  $\square$

Il prossimo teorema è una versione effettiva del Corollario 13.2.11.

**Teorema 13.3.7.** Sia  $I \subset A_+$  ideale omogeneo con  $V(I)$  di dimensione pura  $d > 0$  e sia  $f \in A_n$  un polinomio omogeneo di grado  $n$  tale che  $\dim V(I, f) = d - 1$ . Allora  $\deg Z(I, f) \geq n \deg Z(I)$  e vale l'uguaglianza se  $\dim(\text{Imm}(Z(I)) \cap V(f)) < d - 1$ .

*Dimostrazione.* La disuguaglianza segue immediatamente dalla successione esatta

$$\frac{A}{I} \xrightarrow{f} \frac{A}{I} \longrightarrow \frac{A}{(I, f)} \longrightarrow 0$$

che induce la disuguaglianza tra polinomi di Hilbert  $p_{Z(I, f)}(l) \geq p_{Z(I)}(l) - p_{Z(I)}(l - d)$  per  $l \gg 0$ . Prendiamo una decomposizione irriducibile omogenea minimale

$$I = J_1 \cap \cdots \cap J_r \cap H_1 \cap \cdots \cap H_s \cap K_1 \cap \cdots \cap K_t = J \cap H \cap K$$

con  $\dim V(J_i) = d$ ,  $\dim V(H_i) = d - 1$  e  $\dim V(K_i) < d - 1$ . Dalla condizione  $\dim V(I, f) = d - 1$  segue che  $f \notin \sqrt{J_i}$  per ogni  $i$ , mentre dalla condizione  $\dim(\text{Imm}(Z(I)) \cap V(f)) <$

$d - 1$  e dal Lemma 13.3.6 segue che  $f \notin \sqrt{H_j}$  per ogni  $j$ . Quindi se  $fa \in I$  deve essere  $a \in J \cap H$  e quindi  $Ka \subset I$ . L'anello  $A/I$  è Noetheriano e quindi il nucleo della mappa di moltiplicazione per  $f$  è generato da un numero finito di elementi omogenei  $v_1, \dots, v_k$  di gradi  $d_1, \dots, d_k$ . Esiste allora una successione esatta

$$\bigoplus_1^k \frac{A}{K} \xrightarrow{(v_1, \dots, v_k)} \frac{A}{I} \xrightarrow{f} \frac{A}{I} \longrightarrow \frac{A}{(I, f)} \longrightarrow 0$$

che induce la disuguaglianza tra polinomi di Hilbert, per  $l \gg 0$

$$p_{Z(I, f)}(l) \leq p_{Z(I)}(l) - p_{Z(I)}(l - d) + \sum_{i=1}^k p_{Z(K)}(l - d - d_i).$$

Basta adesso osservare che  $p_{Z(K)}$  è un polinomio di grado  $< d - 1$ . □

È facile mostrare con degli esempi che, in generale, non vi sono relazioni di inclusione tra  $\text{Imm}(Z(I)) \cap V(f)$  e  $\text{Imm}(Z(I, f))$ ; occorre pertanto fare molta attenzione nell'applicare ricorsivamente il risultato del Teorema 13.3.7 (vedi in proposito l'Esempio 13.5.7).

Vediamo adesso come calcolare il grado di  $Z(I)$  quando  $\dim Z(I) = 0$ .

**Definizione 13.3.8.** *Se  $\dim Z(I) = 0$  definiamo il grado locale di  $Z(I)$  in un punto  $p \in V(I)$  come*

$$\deg_p Z(I) = \deg Z(I_p).$$

**Lemma 13.3.9.** *Se  $\dim Z(I) = 0$  e  $p \in Z(I)$ , allora vale  $\deg_p Z(I) > 1$  se e solo se  $p$  è un punto singolare di  $Z(I)$ .*

*Dimostrazione.* Prendiamo un sistema di coordinate omogenee  $x_0, \dots, x_m$  tali che  $p = [1, 0, \dots, 0]$ . Il punto  $p$  è una componente irriducibile di  $V(I)$  e pertanto si ha  $\sqrt{I_p} = I(p)$ . Se  $p$  non è un punto singolare di  $Z(I)$  allora, per il Teorema 10.8.2 vale  $I_p = I(p)$  e di conseguenza  $\deg_p(Z(I)) = 1$ . Viceversa se  $\deg(Z(I_p)) = 1$ , allora esiste  $n \in \mathbb{N}$  tale che il sottospazio  $I_p \cap A_n$  ha codimensione 1 in  $A_n$  e quindi per ogni  $i = 1, \dots, m$  esiste  $a_i \in \mathbb{K}$  tale che  $f_i := x_i x_0^{n-1} - a_i x_0^n \in I_p$ . Il rango della matrice  $\left( \frac{\partial f_i}{\partial x_j}(p) \right)$  è uguale a  $m$  e quindi  $p$  è non singolare. □

**Proposizione 13.3.10.** *Se  $V(I) = \{p_1, \dots, p_n\}$ , allora  $\deg Z(I) = \sum_i \deg_{p_i} Z(I)$ .*

*Dimostrazione.* Denotiamo  $I_j = I_{p_j}$ ,  $P_j = I(p_j) = \sqrt{I_j}$ ,  $P_0 = A_+$ . Per il teorema degli zeri di Hilbert,  $P_0, \dots, P_n$  sono tutti e soli gli ideali primi che contengono  $I$ . Se

$$I = \bigcap_{i=0}^n \bigcap_h J_{ih}$$

è una decomposizione irriducibile minimale, indicizzata in modo tale che  $\sqrt{J_{ih}} = P_i$  per ogni  $i, h$ , segue dal Lemma 13.3.3 che per ogni  $i = 1, \dots, n$  vale  $I_i = \bigcap_h J_{ih}$ . Possiamo dunque scrivere

$$I = I_0 \cap I_1 \cap \dots \cap I_n$$

dove  $I_0$  è un ideale tale che  $\sqrt{I_0} = P_0$ . Per ogni  $s = 1, \dots, n$  vale

$$P(I_0 \cap \dots \cap I_s, t) = P(I_0 \cap \dots \cap I_{s-1}, t) + P(I_s, t) - P((I_0 \cap \dots \cap I_{s-1}) + I_s, t)$$



e, siccome  $V((I_0 \cap \dots \cap I_{s-1}) + I_s) = \emptyset$ , la serie di Poincaré di  $(I_0 \cap \dots \cap I_{s-1}) + I_s$  è un polinomio. Quindi

$$\deg(Z(I_0 \cap I_1 \cap \dots \cap I_s)) = \deg_{p_s} Z(I) + \deg(Z(I_0 \cap I_1 \cap \dots \cap I_{s-1}))$$

e tutto segue per induzione su  $s$ . □

**Proposizione 13.3.11.** *Sia  $I \subset \mathbb{K}[x_0, \dots, x_m]$  un ideale omogeneo tale che  $\dim V(I) = 0$  e sia  $p \in V(I) \subset \mathbb{P}^m$ . Allora vale la formula*

$$\deg_p(Z(I)) = \dim_{\mathbb{K}} \frac{\mathcal{O}_{p, \mathbb{P}^m}}{I_{(p)}}$$

dove  $I_{(p)}$  è l'ideale di  $\mathcal{O}_{p, \mathbb{P}^m}$  generato dai quozienti  $f/g$ , con  $f \in I$ ,  $g(p) \neq 0$  ed i polinomi  $f, g$  omogenei dello stesso grado.

*Dimostrazione.* Denotiamo  $J = I_p$  e  $d = \deg_p(Z(I)) = \deg(Z(J))$ . Sia  $p = [v_0, \dots, v_m]$  e supponiamo, tanto per fissare le idee, che  $v_0 \neq 0$ . Proviamo che ogni  $d+1$ -upla  $\phi_0, \dots, \phi_d \in \mathcal{O}_{p, \mathbb{P}^m}/I_{(p)}$  è linearmente dipendente. Per ogni  $i = 0, \dots, d$ , scriviamo  $\phi_i = f_i/g_i$ , dove  $\deg f_i = \deg g_i$  e sia  $s = \sum_i \deg f_i$ . Per  $n \gg 0$  i polinomi omogenei

$$F_i = x_0^{n-s} f_i \prod_{j \neq i} g_j, \quad i = 0, \dots, d$$

sono linearmente dipendenti in  $A_n/J_n$  ed esistono  $a_0, \dots, a_d \in \mathbb{K}$  non tutti nulli e tali che  $\sum a_i F_i \in J_n$ . Per definizione di  $J$  esiste un polinomio omogeneo  $G$  tale che  $G(p) \neq 0$  e tale che  $\sum a_i F_i G \in J_{n+\deg G}$ ; dividendo per  $x_0^{n-s} G \prod_j g_j$  otteniamo una relazione di dipendenza lineare in  $\mathcal{O}_{p, \mathbb{P}^m}/I_{(p)}$ . Sia dunque  $\delta = \dim_{\mathbb{K}} \mathcal{O}_{p, \mathbb{P}^m}/I_{(p)} \leq d$  e dimostriamo che  $\delta \geq d$ . Sia  $n \gg 0$  e siano  $f_1, \dots, f_d \in A_n$  polinomi omogenei che inducono una base di  $A_n/I_n$ : è sufficiente dimostrare che i quozienti  $f_1/x_0^n, \dots, f_d/x_0^n \in \mathcal{O}_{p, \mathbb{P}^m}$  sono linearmente indipendenti in  $\mathcal{O}_{p, \mathbb{P}^m}/I_{(p)}$ . Se  $(\sum a_i f_i)/x_0^n \in I_{(p)}$ , allora esistono  $h \in I$  e  $g \in A$  omogenei dello stesso grado e tali che  $g(p) \neq 0$  e  $g(\sum a_i f_i) = hx_0^n$ . Siccome  $hx_0^n \in I$  ne segue che  $\sum a_i f_i \in J$  e quindi che  $a_1 = \dots = a_d = 0$ . □

**Esercizi**

**13.8.** Dimostrare che per due ideali omogenei  $I, J \subset \mathbb{K}[x_0, \dots, x_m]$  vale  $Z(J) \subset Z(I)$  se e solo se  $I_p \subset J_p$  per ogni  $p \in \mathbb{P}^m$ .

**13.9.** Sia  $I = (x_1^2, x_1 x_2) \subset \mathbb{K}[x_0, x_1, x_2]$ . Determinare i punti immersi ed i punti singolari di  $Z(I)$ .

**13.10.** Sia  $I = (x^2, xy) \subset \mathbb{K}[x, y, z]$ . Determinare il grado di  $Z(I)$  e quello di  $Z(I + (y - ax - bz))$  al variare di  $a, b \in \mathbb{K}$ .

**13.11.** Nelle notazioni della Proposizione 13.3.11, dimostrare che per due ideali omogenei  $I, J \subset \mathbb{K}[x_0, \dots, x_m]$  vale  $Z(J) \subset Z(I)$  se e solo se  $I_{(p)} \subset J_{(p)}$  per ogni  $p \in \mathbb{P}^m$ . (Sugg.: Esercizio 13.8.)

### 13.4 Successioni regolari ed intersezioni complete

**Definizione 13.4.1.** Una successione  $f_1, \dots, f_n \in A$  di elementi di un anello  $A$  si dice una **successione regolare** se  $(f_1, \dots, f_n) \neq A$  e se, per ogni  $i = 1, \dots, n$ , la moltiplicazione

$$\frac{A}{(f_1, \dots, f_{i-1})} \xrightarrow{f_i} \frac{A}{(f_1, \dots, f_{i-1})}$$

è iniettiva.

È chiaro che se  $f_1, \dots, f_n$  è una successione regolare allora anche  $f_1, \dots, f_r$  è una successione regolare per ogni  $r \leq n$ . È invece generalmente falso che  $f_r, \dots, f_n$  è una successione regolare, in particolare la proprietà di essere una successione regolare non è invariante per permutazioni degli indici.

Una proprietà sulle successioni più debole della regolarità ma invariante per permutazioni è data dalla seguente definizione.

**Definizione 13.4.2.** Diremo che una successione  $f_1, \dots, f_n \in A$  è **di Koszul** se per ogni successione  $a_1, \dots, a_n \in A$  tale che  $a_1 f_1 + \dots + a_n f_n = 0$  esiste una matrice quadrata  $(b_{ij})$  di ordine  $n$ , alternante (ossia antisimmetrica con gli elementi della diagonale principale nulli) a coefficienti in  $A$ , tale che  $a_i = \sum_j b_{ij} f_j$  per ogni  $i = 1, \dots, n$ .

**Lemma 13.4.3.** Ogni successione regolare è di Koszul.

*Dimostrazione.* Sia  $f_1, \dots, f_n \in A$  una successione regolare; allora  $f_1$  non è un divisore di 0, vale  $a_1 f_1 = 0$  se e solo se  $a_1 = 0$  e quindi  $f_1$  è di Koszul. Per induzione su  $n$  possiamo assumere  $f_1, \dots, f_{n-1}$  di Koszul e si abbia  $a_1 f_1 + \dots + a_n f_n = 0$ . Dalla regolarità della successione segue che  $a_n \in (f_1, \dots, f_{n-1})$ , diciamo  $a_n = c_1 f_1 + \dots + c_{n-1} f_{n-1}$ . Sostituendo eventualmente  $a_n$  con  $a_n - \sum c_i f_i$  ed  $a_i$  con  $a_i + c_i f_n$ , non è restrittivo supporre  $a_n = 0$ ; basta adesso ricordarsi che  $f_1, \dots, f_{n-1}$  è di Koszul.  $\square$

In alcuni casi fortunati vale anche il viceversa del Lemma 13.4.3; i più rilevanti sono trattati nel Lemma 13.4.4 e negli Esercizi 13.17 e 13.18.

**Lemma 13.4.4.** Sia  $A = \bigoplus_{i=0}^{+\infty} A_i$  un anello graduato. Una successione di elementi omogenei di grado positivo  $f_1, \dots, f_n \in A$  è regolare se e solo se è di Koszul.

*Dimostrazione.* Siano  $f_1, \dots, f_n$  elementi omogenei tali che  $\deg(f_i) > 0$  per ogni  $i$ ; bisogna dimostrare che se una tale successione è di Koszul allora è regolare. Per induzione su  $n$ , basta dimostrare che se  $f_1, \dots, f_n$  è di Koszul allora:

1. La successione  $f_1, \dots, f_{n-1}$  è di Koszul.
2. L'applicazione di moltiplicazione  $\frac{A}{(f_1, \dots, f_{n-1})} \xrightarrow{f_n} \frac{A}{(f_1, \dots, f_{n-1})}$  è iniettiva.

[1] Consideriamo una relazione  $a_1 f_1 + \dots + a_{n-1} f_{n-1} = 0$ ; separando le varie componenti omogenee in tale relazione non è restrittivo supporre che  $a_i$  sia omogeneo di grado  $d - \deg(f_i)$  per qualche  $d \in \mathbb{N}$  ed ogni  $i$ . Dimostriamo per induzione su  $d$  che esiste una matrice alternante  $b_{ij}$ , con  $i, j = 1, \dots, n-1$ , tale che  $a_i = \sum_{j < n} b_{ij} f_j$  per ogni  $i = 1, \dots, n-1$ . Per ipotesi la successione  $f_1, \dots, f_n$  è di Koszul e quindi esiste una matrice alternante  $c_{ij}$ , con  $i, j = 1, \dots, n$ , tale che

$$0 = \sum_{j=1}^{n-1} c_{nj} f_j \quad \text{e} \quad a_i = \sum_{j=1}^n c_{ij} f_j \quad \text{per ogni } i = 1, \dots, n-1.$$

Non è restrittivo supporre  $c_{ij}$  omogeneo di grado  $\deg(a_i) - \deg(f_j) = d - \deg(f_i f_j)$ : per l'ipotesi induttiva esiste una matrice alternante  $d_{jk}$ , con  $j, k = 1, \dots, n-1$ , tale che  $c_{nj} = \sum d_{jk} f_k$  per ogni  $j$ . Dunque

$$a_j = c_{jn} f_n + \sum_{k=1}^{n-1} c_{jk} f_k = \sum_{k=1}^{n-1} (c_{jk} - d_{jk} f_n) f_k$$

e possiamo prendere  $b_{ij} = c_{ij} - d_{ij} f_n$ .

[2] La condizione di Koszul implica in particolare che se  $f_n a_n \in (f_1, \dots, f_{n-1})$ , allora anche  $a_n \in (f_1, \dots, f_{n-1})$ , ovvero l'iniettività della moltiplicazione per  $f_n$ .  $\square$

Diamo adesso una interpretazione geometrica delle successioni regolari di polinomi omogenei in  $\mathbb{K}[x_0, \dots, x_m]$ .

*Esempio 13.4.5.* Una successione  $f_0, \dots, f_n \in \mathbb{K}[x_0, \dots, x_m]$  di polinomi omogenei di grado 1 è regolare se e solo se gli  $f_i$  sono linearmente indipendenti su  $\mathbb{K}$ . Una implicazione è ovvia, viceversa se  $f_1, \dots, f_n$  sono linearmente indipendenti, allora a meno di cambi lineari di coordinate possiamo supporre  $f_i = x_i$ , per  $i = 0, \dots, n$ , e quindi  $\mathbb{K}[x_0, \dots, x_m]/(f_0, \dots, f_i) = \mathbb{K}[x_{i+1}, \dots, x_m]$  per ogni  $i$ .

**Teorema 13.4.6.** *Siano  $f_0, \dots, f_h \in \mathbb{K}[x_0, \dots, x_m]$  polinomi omogenei di gradi  $d_0 \geq d_1 \geq \dots \geq d_h > 0$  e denotiamo con  $I = (f_0, \dots, f_h)$  l'ideale da essi generato. Allora sono condizioni equivalenti:*

1.  $f_0, \dots, f_h$  è una successione regolare.
2.  $P(I, t) = \frac{\prod_{i=0}^h (1 - t^{d_i})}{(1 - t)^{m+1}}$ .
3.  $h \leq m$  e  $\dim Z(I) = m - h - 1$ .

*Dimostrazione.* [1  $\Rightarrow$  2] Se  $h = -1$  allora  $I = 0$  e  $P(0, t) = (1 - t)^{-1-m}$ . Se  $h \geq 0$ , denotando con  $J = (f_0, \dots, f_{h-1})$  si ha una successione esatta

$$0 \longrightarrow \frac{A}{J} \xrightarrow{f_h} \frac{A}{J} \longrightarrow \frac{A}{I} \longrightarrow 0$$

dalla quale si deduce l'uguaglianza

$$P(I, t) = P(J, t)(1 - t^{d_h}).$$

Basta adesso utilizzare induzione su  $h$ .

[2  $\Rightarrow$  3] La dimensione di  $Z(I)$  è per definizione l'ordine di polo in  $t = 1$  della serie di Poincaré meno 1 ed è quindi uguale a  $m - h - 1$ .

[3  $\Rightarrow$  1] Aggiungendo alla successione generici polinomi omogenei di grado 1  $f_{h+1}, \dots, f_m$  non è restrittivo supporre  $h = m$ ,  $\dim Z(I) = 0$  e quindi  $\sqrt{I} = A_+$ . Dimostriamo per induzione sul prodotto  $d = d_0 d_1 \dots d_m$  che  $f_0, \dots, f_m$  è una successione regolare. Se  $d = 1$  basta applicare l'Esempio 13.4.5. Assumiamo quindi  $d \geq d_0 > 1$  e denotiamo  $J = (f_1, \dots, f_m)$ . Dato che  $0 = \dim Z(I) + 1 \geq \dim Z(J) \geq m - m = 0$  vale  $\dim Z(J) = 0$  e per il generico  $u \in A_1$  la dimensione di  $Z(J + (u))$  è uguale a  $-1$ . Per l'ipotesi induttiva  $u, f_1, \dots, f_m$  è una successione regolare, quindi  $f_1, \dots, f_m$  è una successione regolare e  $u$  non è un divisore di 0 in  $A/J$ . Siccome  $\sqrt{I} = A_+$ , esiste  $k > 0$  tale che  $u^k \in I$ , cioè  $u^k \equiv a f_0 \pmod{J}$  e se  $f_0$  fosse un divisore di 0 in  $A/J$  allora anche  $u^k$  sarebbe un divisore di 0: contraddizione.  $\square$

**Teorema 13.4.7.** *Siano  $f_1, \dots, f_m \in \mathbb{K}[x_0, \dots, x_m]$  polinomi omogenei. Se  $V(f_1) \cap \dots \cap V(f_m) = \{p_1, \dots, p_n\}$  ha dimensione 0, allora*

$$\sum_{i=1}^n \deg_{p_i}(Z(f_1, \dots, f_m)) = \prod_{j=1}^m \deg(f_j).$$

*Dimostrazione.* Per il Teorema 13.4.6 la successione  $f_1, \dots, f_m$  è regolare e quindi

$$P((f_1, \dots, f_m), t) = \frac{1}{(1-t)} \prod_{j=1}^m \frac{(1-t)^{\deg(f_j)}}{(1-t)} = \frac{1}{(1-t)} \prod_{j=1}^m \sum_{h=1}^{\deg(f_j)} t^{h-1}.$$

Basta adesso osservare che il grado di  $Z(f_1, \dots, f_m)$  è uguale al valore che assume il polinomio  $(1-t)P((f_1, \dots, f_m), t)$  per  $t = 1$ .  $\square$

**Definizione 13.4.8.** Una sottovarietà  $X \subset \mathbb{P}^m$  di codimensione  $d$  si dice una **intersezione completa** se l'ideale  $I(X)$  è generato da  $d$  polinomi omogenei.

Per il Teorema 13.4.6, una varietà  $X$  è intersezione completa se  $I(X)$  è generato da una successione regolare di polinomi omogenei.

**Teorema 13.4.9.** Sia  $X \subset \mathbb{P}^m$  una sottovarietà di codimensione  $d \leq m$  e sia  $I(X) \subset A = \mathbb{K}[x_0, \dots, x_m]$  l'ideale dei polinomi nulli su  $X$ . Se esistono  $f_1, \dots, f_d \in I(X)$  omogenei tali che  $X = Z(f_1, \dots, f_d)$ , allora  $I(X) = (f_1, \dots, f_d)$ , e quindi  $X$  è intersezione completa.

*Dimostrazione.* Denotiamo con  $I = I(X)$  e con  $J = (f_1, \dots, f_d)$ . Per ipotesi  $V(J) = X$ ,  $J \subset I$  e  $J \sim I$ ; vogliamo dimostrare che  $J = I$ . Inoltre vale  $I = \cap \{I_p \mid p \in X\}$  e  $I_p = J_p$  per ogni  $p \in X$ . Sia  $J = H_1 \cap \dots \cap H_s$  una decomposizione irriducibile minimale di  $J$ . Per il Lemma 13.3.3 vale  $J_p = \cap \{H_i \mid p \in V(H_i)\}$  e quindi si ha

$$I = \cap_{p \in X} I_p = \cap_{p \in X} J_p = \cap \{H_i \mid V(H_i) \neq \emptyset\}$$

Basta quindi dimostrare che  $V(H_i) \neq \emptyset$  per ogni  $i$ . Supponiamo che accada il contrario, possiamo allora scrivere  $J = I \cap K$ , con  $J \neq I$  e dove  $K$  è un ideale omogeneo tale che  $V(K) = \emptyset$ . Per il teorema degli zeri esiste un intero  $n$  tale che  $K_n = A_n$ . Possiamo quindi trovare  $g \in K_n$  tale che  $\dim(X \cap V(g)) < \dim X$  e quindi la successione  $f_1, \dots, f_d, g$  è regolare, in contraddizione con il fatto che  $gI \subset J$  e quindi che  $g$  è un divisore di 0 in  $A/J$ .  $\square$

## Esercizi

**13.12.** Si consideri l'anello  $A = \mathbb{K}[x, y, z]$  e la successione  $f_1 = y$ ,  $f_2 = x(y-1)$ ,  $f_3 = z(y-1)$ . Provare che la successione  $f_1, f_2, f_3$  è regolare e che la successione  $f_2, f_3$  non è regolare.

**13.13.** Dimostrare il Teorema 4.5.6.

**13.14.** Nelle notazioni del Corollario 9.1.5, dimostrare che se  $V(f_0, \dots, f_r) = \emptyset$ , allora  $r \geq n$  e  $\phi_d$  è surgettiva per  $d \geq d_0 + d_1 + \dots + d_n - n$ . (Sugg.: esiste una successione regolare  $u_0, \dots, u_n$  tale che  $u_i \equiv f_i \pmod{f_{i+1}, \dots, f_r}$ , cfr. [Ko1996, I.7.4].)

## 13.5 Intersezioni trasverse e teorema di Bézout

**Definizione 13.5.1.** Diremo che due varietà proiettive irriducibili  $X, Y \subset \mathbb{P}^m$  si **intersecano trasversalmente in un punto**  $p \in X \cap Y$  se vale

$$\dim(\mathbb{T}_p X \cap \mathbb{T}_p Y) = \dim X + \dim Y - m.$$

Diremo che si **intersecano trasversalmente** se tale condizione è soddisfatta in per ogni  $p \in X \cap Y$ .

Vediamo alcune conseguenze della nozione di trasversalità; si assuma  $X, Y \subset \mathbb{P}^m$  due chiusi che si intersecano trasversalmente:

1. Se  $X \cap Y \neq \emptyset$ , allora  $\dim X + \dim Y \geq m$ . Infatti se  $p \in X \cap Y$ , allora  $p \in \mathbb{T}_p X \cap \mathbb{T}_p Y$  e quindi  $\dim X + \dim Y - m = \dim(\mathbb{T}_p X \cap \mathbb{T}_p Y) \geq 0$ .
2. Se  $p \in X \cap Y$ , allora  $p$  è un punto liscio di  $X$ ,  $Y$  e  $X \cap Y$ . Abbiamo infatti dimostrato che  $\dim_p(X \cap Y) \geq \dim X + \dim Y - m$  e che  $\mathbb{T}_p(X \cap Y) \subset \mathbb{T}_p X \cap \mathbb{T}_p Y$ ; segue quindi che  $p$  è un punto liscio di  $X \cap Y$ . Inoltre dalla formula di Grassmann si ha  $\dim \mathbb{T}_p X + \dim \mathbb{T}_p Y \leq m + \dim(\mathbb{T}_p X \cap \mathbb{T}_p Y) \leq \dim X + \dim Y$  e quindi  $p$  è liscio sia per  $X$  che per  $Y$ .

Per la comprensione del prossimo teorema e della sua dimostrazione è richiesta la lettura preliminare del Capitolo 11. Se non lo avete ancora fatto, potete passare direttamente al Lemma 13.5.3.

**Teorema 13.5.2.** *Sia  $X \subset \mathbb{P}^m$  una varietà proiettiva irriducibile di codimensione  $d$  e sia  $E(X)$  il sottoinsieme della Grassmanniana  $G(d, \mathbb{P}^m)$  formato dai sottospazi di dimensione  $d$  che intersecano trasversalmente  $X$ . Allora  $E(X)$  è un aperto non vuoto.*

*Dimostrazione.* In base alla Proposizione 11.2.4, per ogni varietà proiettiva irriducibile  $Y \subset \mathbb{P}^m$  di codimensione  $s$  e per ogni  $d \leq s$ , la varietà di incidenza

$$I_Y^d = \{H \in G(d, \mathbb{P}^m) \mid H \cap Y \neq \emptyset\}$$

è una sottovarietà chiusa e irriducibile di  $G(d, \mathbb{P}^m)$  di codimensione  $s - d$ . Sia  $Z \subset X$  il chiuso dei punti singolari di  $X$ , sia  $U = X - Z$  l'aperto dei punti lisci e definiamo

$$D = \{(p, H) \in X \times G(d, \mathbb{P}^m) \mid p \in U \cap H, \dim(\mathbb{T}_p(X) \cap H) > 0\}.$$

$D$  è un chiuso di  $U \times G(d, \mathbb{P}^m)$  e ogni fibra del morfismo di proiezione  $D \rightarrow U$  è isomorfa ad una varietà irriducibile di dimensione  $d(m - d) - 1$ . Infatti, fissato  $p \in U$  si consideri un iperpiano  $\mathbb{P}^{m-1} \subset \mathbb{P}^m$  non contenente il punto  $p$  e sia  $Y = \mathbb{T}_p(X) \cap \mathbb{P}^{m-1}$ . La fibra sopra  $p$  è dunque la varietà di incidenza  $I_Y^{d-1} \subset G(d-1, \mathbb{P}^{m-1})$  che è irriducibile di codimensione  $d - (d - 1) = 1$ . Quindi la chiusura  $\overline{D} \subset X \times G(d, \mathbb{P}^m)$  è irriducibile di dimensione  $d(m - d) - 1 + (m - d) = (d + 1)(m - d) - 1$ . Se  $I(U) \subset G(d, \mathbb{P}^m)$  denota la proiezione di  $\overline{D}$  sul secondo fattore, allora  $I(U)$  è un chiuso irriducibile di codimensione  $\geq 1$ . Infine

$$I_Z^d = \{H \in G(d, \mathbb{P}^m) \mid H \cap Z \neq \emptyset\}$$

è unione finita di chiusi irriducibili di codimensione  $\geq 1$ . In conclusione  $E(X) = G(d, \mathbb{P}^m) - I(U) - I_Z^d$  è un aperto non vuoto.  $\square$

La nozione di trasversalità si estende in modo naturale all'intersezione di due sottoschemi chiusi. Osserviamo che in tale situazione vale il

**Lemma 13.5.3.** *Dati due sottoschemi  $Z(I), Z(J)$  di  $\mathbb{P}^m$  ed un punto  $p \in V(I) \cap V(J)$  le seguenti condizioni sono equivalenti:*

1.  $\dim(\mathbb{T}_p Z(I) \cap \mathbb{T}_p Z(J)) = \dim_p V(I) + \dim_p V(J) - m$
2.  $Z(I + J)$  è liscio in  $p$  e  $\dim_p(V(I) \cap V(J)) = \dim_p V(I) + \dim_p V(J) - m$

*Se tali condizioni sono soddisfatte allora  $p$  è un punto liscio di  $Z(I)$  e  $Z(J)$ .*

*Dimostrazione.* Basta osservare che  $\mathbb{T}_p Z(I + J) = \mathbb{T}_p Z(I) \cap \mathbb{T}_p Z(J)$  e ricordare che  $\mathbb{T}_p Z(I + J) \geq \dim_p(V(I) \cap V(J)) \geq \dim_p V(I) + \dim_p V(J) - m$ .  $\square$

**Teorema 13.5.4.** *Sia  $X \subset \mathbb{P}^m$  una varietà proiettiva di dimensione pura  $h$  ed  $H \subset \mathbb{P}^m$  un sottospazio proiettivo di dimensione  $m - h$  che interseca trasversalmente  $X$ . Allora il grado di  $Z(I(X))$  è uguale alla cardinalità  $\sharp(X \cap H)$  dell'intersezione di  $X$  con  $H$ .*

*Dimostrazione.* Sia  $I_0 = I(X)$  e  $H = V(f_1, \dots, f_h)$ , con  $f_1, \dots, f_h \in A_1$ . Per semplicità notazionale denotiamo  $I_j = (I_0, f_1, \dots, f_j)$  per ogni  $j = 0, \dots, h$ . Per l'ipotesi di trasversalità  $\text{Sing}(Z(I_h)) = \emptyset$  e quindi  $\text{deg } Z(I_h) = \sharp(X \cap H)$ . Dato che  $\dim Z(I_{i-1}) > \dim Z(I_i)$ , vale anche  $\text{Sing}(Z(I_{i-1})) \cap V(f_i) \subset \text{Sing}(Z(I_i))$  per ogni  $i$ ; deve dunque necessariamente valere

$$\begin{aligned} \dim(\text{Imm}(Z(I_{i-1})) \cap V(f_i)) &\leq \dim(\text{Sing}(Z(I_{i-1})) \cap V(f_i)) \leq \\ &\leq \dim \text{Sing}(Z(I_i)) < h - i = \dim V(I_i). \end{aligned}$$

Per il Teorema 13.3.7 si ha dunque  $\text{deg}(Z(I_h)) = \text{deg}(Z(I_0)) = \text{deg}(Z(I(X)))$ . □

**Corollario 13.5.5.** *Il grado  $\text{deg}(X)$  di una varietà proiettiva  $X \subset \mathbb{P}^m$  è uguale al grado del sottoschema chiuso associato  $Z(I(X))$ . Se  $H \subset \mathbb{P}^m$  è un sottospazio di codimensione uguale alla dimensione di  $X$  tale che  $\text{deg}(X) = \sharp(X \cap H)$ , allora  $H$  interseca trasversalmente  $X$ .*

*Dimostrazione.* Dai Teoremi 13.5.2 e 13.5.4 segue immediatamente la prima parte. La seconda parte segue dal Lemma 13.5.3 e dal Lemma 13.3.9. □

**Corollario 13.5.6.** *Sia  $X \subset \mathbb{P}^m$  una varietà proiettiva di dimensione  $h$ . Allora il grado di  $X$  è uguale alla somma dei gradi delle sue componenti irriducibili di dimensione  $h$ .*

*Dimostrazione.* Presi  $f_1, \dots, f_h$  elementi generici di  $A_1$ , il chiuso  $Y = V(I(X), f_1, \dots, f_h)$  ha dimensione 0 ed ogni suo punto  $p$  è contenuto in una sola componente irriducibile  $X_p \subset X$ , la quale ha dimensione  $h$ . Siccome

$$\text{deg } X = \text{deg } Z(I(X), f_1, \dots, f_h) = \sum_{p \in Y} \text{deg}_p Z(I(X), f_1, \dots, f_h)$$

e  $I_p = I(X_p) \subset (I, f_1, \dots, f_h)_p$  vale  $(I, f_1, \dots, f_h)_p = (I_p, f_1, \dots, f_h)_p$ . □

*Esempio 13.5.7.* (Caratteristica  $\neq 2, 3$ ) Sia  $X$  l'immagine del morfismo proiettivo

$$f: \mathbb{P}^2 \rightarrow \mathbb{P}^4, \quad f([t_0, t_1, t_2]) = [t_0^4, t_1^4, t_1^3 t_2, t_1 t_2^3, t_2^4],$$

e denotiamo  $I = I(X) \subset \mathbb{K}[x_0, \dots, x_4]$ . È facile vedere (guardando ad esempio le restrizioni di  $X$  agli aperti affini  $x_1 = 1$  e  $x_4 = 1$ ) che

$$I = (x_1 x_4 - x_2 x_3, x_1^2 x_3 - x_2^3, x_2 x_4^2 - x_3^3, x_2^2 x_4 - x_3^2 x_1).$$

Per il Teorema 13.3.7 il grado di  $X$  è uguale a  $\text{deg } Z(I, x_0) = \text{deg } Z(I, x_1)$ . Il sottoschema  $Z(I, x_0)$  non ha punti singolari e la cardinalità di  $V(I, x_0, x_1 + ax_2 + bx_3 + cx_4)$  è uguale al numero di radici del polinomio  $t^4 + at^3 + bt + c$ , che per generici  $a, b, c$  è uguale a 4. Dunque  $\text{deg } X = \text{deg } Z(I, x_1) = 4$ ; tuttavia il punto  $[1, 0, 0, 0, 0]$  è un punto immerso di  $Z(I, x_1)$ , ed infatti il grado di  $Z(I, x_1, x_4)$  è uguale alla dimensione di  $\mathbb{K}[x_2, x_3]/(x_2 x_3, x_2^3, x_3^3)$  (esercizio) che è uguale a 5.

*Esempio 13.5.8.* Siano  $I \subset A = \mathbb{K}[x_0, \dots, x_m]$  e  $J \subset B = \mathbb{K}[y_0, \dots, y_l]$  ideali omogenei. Denotiamo con  $H \subset C = \mathbb{K}[x_0, \dots, x_m, y_0, \dots, y_l]$  l'ideale biomogeneo generato da  $I$  e  $J$ . Siano  $f_1, \dots, f_r \in A_a, g_1, \dots, g_s \in B_b$  basi di  $A_a$  e  $B_b$  con  $f_1, \dots, f_r'$  base di  $I_a$  e  $g_1, \dots, g_s'$

base di  $J_b$ . Un polinomio biomogeneo  $h \in C_{a,b}$  appartiene ad  $H$  se e solo se   combinazione lineare dei prodotti  $f_i g_j$  con  $i \leq r'$  o  $j \leq s'$ . Dunque la dimensione di  $C_{a,b}/H_{a,b}$    uguale al prodotto delle dimensioni di  $A_a/I_a$  e  $B_b/J_b$  e quindi vale

$$P(H, t) = P(I, t)P(J, t).$$

Terminiamo la sezione con il Teorema di B zout per le intersezioni trasverse in  $\mathbb{P}^m$ . Trattasi di un caso particolare di un teorema pi  generale che fa parte della teoria dell'intersezione (vedi [Ful1984]).

**Teorema 13.5.9.** *Siano  $X, Y \subset \mathbb{P}^m$  variet  irriducibili con  $\dim X + \dim Y = m$  che si intersecano trasversalmente. Allora l'intersezione  $X \cap Y$    formata da  $\deg X \deg Y$  punti distinti.*

*Dimostrazione.* Siano  $I = I(X)$ ,  $J = I(Y)$ , e  $H \subset \mathbb{K}[x_0, \dots, x_m, y_0, \dots, y_m]$  l'ideale generato da  $I$  e  $J$ . Abbiamo visto nell'Esempio 13.5.8 che la serie di Poincar  di  $H$    uguale al prodotto delle serie di Poincar  di  $I$  e  $J$ , in particolare  $\deg Z(H) = \deg X \deg Y$ . Per il Lemma 10.5.1  $H$    un ideale primo e quindi la variet  proiettiva  $S = V(H) \subset \mathbb{P}^{2m+1}$  ha grado uguale al prodotto dei gradi di  $X$  e  $Y$ . L'ipotesi di trasversalit  equivale a dire che il sottospazio  $T = \{x_0 - y_0 = \dots = x_m - y_m = 0\}$  interseca trasversalmente  $S$ . Basta adesso osservare che esiste una ovvia bigezione tra  $S \cap T$  ed  $X \cap Y$ .  $\square$

### 13.6 Semicontinuit  del polinomio di Hilbert

Obiiettivo primario di questa sezione   generalizzare il Teorema 9.7.1. Sia  $B$    un anello,  $S \subset B$  una parte moltiplicativa e  $M$  un  $B$  modulo. La **localizzazione** di  $M$  su  $S$  si denota con  $S^{-1}M$  e si definisce come l'insieme delle classi di equivalenza di coppie  $\frac{m}{s}$ , con  $m \in M$ ,  $s \in S$  e dove  $\frac{m}{s} \sim \frac{n}{r}$  se e solo se esiste  $t \in S$  tale che  $t(mr - ns) = 0$ . Notiamo che se  $G \subset M$    un insieme di generatori di  $M$  come  $B$ -modulo, allora  $\left\{ \frac{m}{1} \mid m \in G \right\}$  genera  $S^{-1}M$  come  $S^{-1}B$ -modulo. Per ogni  $f \in B$  denotiamo con  $M_f$  il localizzato di  $M$  rispetto alla parte moltiplicativa  $\{f^n\}_{n \geq 0}$ . Lasciamo al lettore il facile esercizio di dimostrare che, se

$$M \xrightarrow{\alpha} N \xrightarrow{\beta} P$$

  una successione esatta di  $B$ -moduli, allora

$$S^{-1}M \xrightarrow{\alpha} S^{-1}N \xrightarrow{\beta} S^{-1}P, \quad \text{dove } \alpha\left(\frac{m}{s}\right) = \frac{\alpha(m)}{s} \text{ e } \beta\left(\frac{n}{t}\right) = \frac{\beta(n)}{t},$$

  una successione esatta di  $S^{-1}B$  moduli.

Supponiamo adesso che  $F$  sia un dominio di integrit  con campo delle frazioni  $\mathcal{K}$ , ossia  $\mathcal{K} = S^{-1}F$  dove  $S = F - \{0\}$ . Per ogni  $F$ -modulo finitamente generato  $M$  si definisce il suo **rango** come

$$\text{rank}_F(M) = \dim_{\mathcal{K}}(S^{-1}M).$$

Notiamo che per ogni parte moltiplicativa  $T \subset S$ , vale  $\text{rank}_{T^{-1}F} T^{-1}M = \text{rank}_F M$ . Se

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

  una successione esatta di  $F$ -moduli finitamente generati, allora

$$0 \longrightarrow S^{-1}M \longrightarrow S^{-1}N \longrightarrow S^{-1}P \longrightarrow 0$$

  una successione esatta di  $\mathcal{K}$ -spazi vettoriali di dimensione finita e quindi vale la formula  $\text{rank}_F M = \text{rank}_F N + \text{rank}_F P$ .

**Lemma 13.6.1.** *Sia  $F$  un dominio di integrità e  $M$  un  $F$ -modulo finitamente generato. Allora esiste  $f \in F$  tale che  $M_f$  è un  $F_f$ -modulo libero di rango  $\text{rank}_F M$ .*

*Dimostrazione.* Consideriamo prima il caso in cui  $\text{rank}_F M = 0$ ; questo vuol dire che  $(F-0)^{-1}M = 0$  e quindi per ogni  $m \in M$  esiste  $f \in F-0$  tale che  $fm = 0$ . Se  $M$  è generato da  $s$  elementi  $m_1, \dots, m_s$ , allora possiamo trovare  $f_1, \dots, f_s \in F-0$  tali che  $f_i m_i = 0$  per ogni  $i$ . Dunque  $f_1 f_2 \cdots f_s m = 0$  per ogni  $m \in M$  e, denotando  $f = f_1 f_2 \cdots f_s$ , vale  $M_f = 0$ . In generale, siano  $m_1, \dots, m_r \in M$  che inducono una base di  $(F-0)^{-1}M$  come spazio vettoriale su  $\mathcal{K}$  e consideriamo il morfismo di  $F$ -moduli

$$\alpha: \bigoplus_1^r F \rightarrow M, \quad \alpha(f_1, \dots, f_r) = \sum f_i m_i.$$

Dato che la localizzazione rispetta le successioni esatte, il nucleo ed il conucleo sono moduli finitamente generati di rango 0. Esistono quindi  $f, g \in F-0$  tali che  $(\text{Ker}(\alpha))_f = 0$ ,  $(\text{Coker}(\alpha))_g = 0$  e quindi  $\alpha$  induce un isomorfismo tra lo  $F$ -modulo libero  $\bigoplus_{i=1}^r F_{fg}$  e  $M_{fg}$ .  $\square$

Da ora in poi supponiamo che  $F = \mathbb{K}[X]$  sia l'anello delle funzioni regolari di una varietà affine irriducibile  $X$  su di un campo  $\mathbb{K}$  algebricamente chiuso; di conseguenza  $\mathcal{K} = \mathbb{K}(X)$  è uguale al campo delle funzioni razionali su  $X$ . Denotiamo con

$$A = \bigoplus A_n = F[x_0, \dots, x_m], \quad R = \bigoplus R_n = \mathbb{K}[x_0, \dots, x_m].$$

Per ogni  $x \in X$ , definiamo il morfismo di valutazione in  $x$  come

$$\text{ev}_x: F = \mathbb{K}[X] \rightarrow \mathbb{K}, \quad \text{ev}_x(f) = f(x).$$

Denoteremo inoltre con  $\text{ev}_x: A \rightarrow R$  l'unica estensione del morfismo di valutazione tale che  $\text{ev}_x(x_i) = x_i$  per ogni  $i = 0, \dots, m$ . Sia  $I \subset A_+$  un ideale omogeneo fissato. Per ogni  $x \in X$  denotiamo  $I_x = \text{ev}_x(I) \subset R_+$  e con  $p_x(t) \in \mathbb{Q}[t]$  il polinomio di Hilbert di  $Z(I_x)$ .

Siccome  $V(I_x) \subset \mathbb{P}^m$  è la fibra di  $V(I) \subset X \times \mathbb{P}^m$  sopra il punto  $x$ , sappiamo che il grado di  $p_x(t)$ , essendo uguale alla dimensione di  $V(I_x)$ , è semicontinuo superiormente in  $X$ .

In questa sezione generalizzeremo questo risultato mostrando che l'applicazione  $x \mapsto p_x(t)$  è semicontinua superiormente rispetto alla relazione di ordine sull'insieme dei polinomi numerici data da  $p(t) \geq q(t)$  se  $p(n) \geq q(n)$  per  $n \gg 0$ . In parole povere, dimostreremo che per ogni polinomio numerico  $q(t)$ , l'insieme dei punti  $x \in X$  tali che  $p_x(t) \geq q(t)$  è un sottoinsieme chiuso di Zariski.

**Lemma 13.6.2.** *Nelle notazioni precedenti, per ogni intero  $n \in \mathbb{N}$  fissato, la funzione*

$$h(n): X \rightarrow \mathbb{N}, \quad h_x(n) = \dim_{\mathbb{K}}(R/I_x)_n$$

*è semicontinua superiormente.*

*Dimostrazione.* Se l'ideale  $I$  è generato dai polinomi  $g_1, \dots, g_s \in A_+$  omogenei di gradi  $d_1, \dots, d_s$ , allora  $h_x(n)$  è la dimensione del conucleo dell'applicazione lineare

$$\bigoplus_{i=1}^s R_{n-d_i} \rightarrow R_n, \quad (a_1, \dots, a_s) \mapsto \sum a_i g_i(x)$$

che, nella base standard formata dai monomi in  $x_0, \dots, x_m$ , è rappresentata da una matrice i cui coefficienti sono funzioni regolari su  $X$ .  $\square$



**Lemma 13.6.3.** *Nelle notazioni precedenti, esiste  $f \in F - 0$  ed un intero  $n_0$  tale che,  $(A_n/I_n)_f$  è un  $F_f$ -modulo libero per ogni  $n \geq n_0$ .*

*Dimostrazione.* Proviamo il lemma per induzione sulla codimensione di  $I \cap R_1$  in  $R_1 = \bigoplus_i \mathbb{K} x_i$ . Se  $R_1 \subset I$  allora  $A_n/I_n = 0$  per ogni  $n > 0$ . Se invece  $R_1$  non è contenuto in  $I$ , per Lemma 13.1.5, esiste  $x \in R_1 - I$  ed un intero  $n_0$  tale che la successione

$$0 \longrightarrow \frac{A_{n-1}}{I_{n-1}} \xrightarrow{\cdot x} \frac{A_n}{I_n} \longrightarrow \frac{A_n}{(I, x)_n} \longrightarrow 0$$

è esatta per ogni  $n \geq n_0$ . A meno di aumentare  $n_0$ , per l'ipotesi induttiva esiste  $g \in F - 0$  tale che  $(A_n/(I, x)_n)_g$  è  $F_g$  libero per ogni  $n \geq n_0$ , mentre per il Lemma 13.6.1 esiste  $h \in F - 0$  tale che  $(A_{n_0}/I_{n_0})_h$  è  $F_h$  libero. Basta quindi porre  $f = gh$  e mostrare per induzione su  $n$  che  $(A_n/I_n)_f$  è  $F_f$ -libero per ogni  $n \geq n_0$ .  $\square$

Per meglio apprezzare il Lemma 13.6.3 osserviamo che, se  $f \in F$  e  $f(x) \neq 0$ , allora  $I_f$  è un ideale omogeneo di  $A_f = F_f[x_0, \dots, x_m]$  e vale  $I_x = \text{ev}_x(I_f)$ , dove  $\text{ev}_x: F_f = \mathbb{K}[X_f] \rightarrow \mathbb{K}$  è il morfismo di valutazione nel punto  $x \in X_f$ .

**Lemma 13.6.4.** *Nelle notazioni precedenti esiste un aperto  $U \subset X$  tale che  $p_x$  è costante per  $x \in U$  e  $p_y \geq p_x$  per ogni  $y \in X$ ,  $x \in U$ .*

*Dimostrazione.* Per il Lemma 13.6.3 esiste un aperto  $U = X_f$  ed un intero  $n_0$  tale che le funzioni  $h_x(n)$  sono costanti su  $U$  per ogni  $n \geq n_0$ . Questo prova che  $p_x$  è costante su  $U$  e che esiste un intero  $n_1 \geq n_0$  tale che  $p_x(n) = h_x(n)$  per ogni  $x \in U$ ,  $n \geq n_1$ . Se  $y \in X$  e  $p_y(n) = h_y(n)$  per ogni  $n \geq n_2$ , allora, per la semicontinuità di  $h_x$  vale  $h_y(n) \geq h_x(n)$  per ogni  $n \geq n_0$  e quindi  $p_y(n) \geq p_x(n)$  per ogni  $n \geq \max(n_1, n_2)$ .  $\square$

Siamo finalmente in grado di dimostrare quello che volevamo.

**Teorema 13.6.5.** *Nelle notazioni precedenti esiste una filtrazione di  $X$  in sottoinsiemi chiusi di Zariski  $X = X_0 \supset X_1 \supset \dots \supset X_s = \emptyset$  e polinomi numerici  $p_0 \leq p_1 \leq \dots \leq p_{s-1}$  tali che  $p_x = p_i$  per ogni  $x \in X_i - X_{i+1}$ .*

*Dimostrazione.* Per il Lemma 13.6.4 esiste un aperto  $U$  ed un polinomio numerico  $p_0$  tale che  $p_0 \leq p_x$  per ogni  $x$  e vale  $p_0 = p_x$  se  $x \in U$ . Poniamo  $X_1 = X - U$ , scegliamo una componente irriducibile  $Y$  di  $X_1$  e ripetiamo il procedimento considerando l'immagine di  $I$  nell'anello quoziente  $\mathbb{K}[Y][x_0, \dots, x_m]$ . Così facendo, dato che  $X$  è uno spazio topologico Noetheriano, si arriva in un numero finito di passi ad un chiuso  $X_s = \emptyset$ .  $\square$

## 13.7 Esercizi complementari

**13.15 (Ideali primari).** Un ideale  $\mathfrak{q} \subset A$  si dice **primario** se ogni divisore di 0 in  $A/\mathfrak{q}$  è nilpotente. Provare:

1. Se  $\mathfrak{q}$  è primario e  $\mathfrak{q} \subset \mathfrak{a} \subset \sqrt{\mathfrak{q}}$ , allora anche  $\mathfrak{a}$  è primario.
2. Se  $\mathfrak{q}$  è primario, allora  $\sqrt{\mathfrak{q}}$  è primo.
3. Se  $\sqrt{\mathfrak{q}}$  è massimale, allora  $\mathfrak{q}$  è primario.
4. Se  $A$  è Noetheriano, allora ogni irriducibile è primario; mostrare con un esempio che esistono ideali primari non irriducibili.

**13.16.** Sia  $A$  un anello ed  $M$  un  $A$ -modulo. Un sottomodulo  $N \subset M$  si dice *irriducibile* se ogni volta che  $N = N_1 \cap N_2$  vale  $N = N_1$  oppure  $N = N_2$ . Siano

$$N = \bigcap_{i=1}^r N_i = \bigcap_{j=1}^s P_j$$

due decomposizioni irriducibili di un sottomodulo con  $r$  minimo possibile (in particolare la decomposizione  $N = \bigcap N_i$  è minimale).

Provare che esiste una permutazione degli indici  $j$  tale per ogni  $n \leq r$  vale

$$N = P_1 \cap \cdots \cap P_n \cap N_{n+1} \cap \cdots \cap N_r.$$

In particolare ogni decomposizione irriducibile minimale di  $N$  è composta da  $r$  sottomoduli irriducibili. (Sugg.: non è restrittivo supporre  $N = 0$ ; per ogni  $i, j$  sia

$$Q_{ij} = N_1 \cap \cdots \cap N_{i-1} \cap P_j \cap N_{i+1} \cap \cdots \cap N_r.$$

Ogni  $Q_{ij}$  è naturalmente isomorfo ad un sottomodulo di  $M/N_i$  e  $\bigcap_j Q_{ij} = 0$ .)

**13.17.** Sia  $A$  un anello Noetheriano e  $f_1, \dots, f_n \in A$  una successione di Koszul. Provare che se  $f_1$  appartiene al radicale di Jacobson  $\mathfrak{R}$  (intersezione di tutti gli ideali massimali), allora  $f_2, \dots, f_n$  è ancora di Koszul. Usare questo fatto per dimostrare che se in aggiunta  $f_1, \dots, f_n \in \mathfrak{R}$ , allora la successione è regolare. (Sugg.: sia

$$M = \{(a_2, \dots, a_n) \in A^{n-1} \mid \sum a_i f_i = 0\}$$

e denotiamo con  $N \subset M$  il sottomodulo delle relazioni  $a_i = \sum b_{ij} f_j$  al variare di  $b_{ij}$  tra le matrici alternanti. Mostrare che  $f_1 M + N = M$  e applicare il lemma di Nakayama.)

**13.18.** Dimostrare che in un anello locale Noetheriano, la regolarità di una successione è una proprietà invariante per permutazioni degli indici.

**13.19 (Teorema della purezza di Macaulay, 1916).** Sia  $\mathbb{K}$  un campo algebricamente chiuso e  $I \subset \mathbb{K}[x_0, \dots, x_m]$  un ideale generato da  $d$  polinomi omogenei. Dimostrare che se  $V(I)$  ha codimensione  $d$ , allora  $Z(I)$  non possiede punti immersi.

*Osservazione 13.7.1.* Il teorema della purezza di Macaulay, in un enunciato algebrico equivalente, è stato esteso da Cohen nel 1946 ad altre classi di anelli. Analogamente a quanto successo con il teorema della base, dimostrato da Hilbert per l'anello dei polinomi e poi preso come assioma per definire la classe importantissima degli anelli Noetheriani, il teorema della purezza è l'assioma che definisce una classe altrettanto importante di anelli, quelli detti di **Cohen-Macaulay** (vedi [Kap1974], [Mat1986]).

**13.20 (Anelli catenari).** Una catena strettamente ascendente e finita di ideali primi in un anello  $A$  si dice saturata se non esistono ideali primi in  $A$  strettamente contenuti tra due ideali consecutivi della catena. Un anello  $A$  si dice **catenario** se per ogni coppia  $\mathfrak{p} \subset \mathfrak{p}'$  di ideali primi esistono catene saturate con estremi  $\mathfrak{p}$  e  $\mathfrak{p}'$  e se hanno tutte la stessa lunghezza. Provare che gli anelli di polinomi in un campo algebricamente chiuso sono catenari.

**13.21.** Sia  $v_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$  la  $d$ -esima immersione di Veronese. Provare che per ogni sottovarietà  $X \subset \mathbb{P}^n$  irriducibile di dimensione  $h$  vale

$$p_{v_d(X)}(l) = p_X(dl), \quad \deg(v_d(X)) = d^h \deg(X).$$

**13.22.** Sia  $I \subset A_+ \subset \mathbb{K}[x_0, \dots, x_m]$  un ideale omogeneo. Dimostrare che:

1. Le seguenti condizioni sono equivalenti:
  - a)  $A/I \cong \mathbb{K}[y_0, \dots, y_d]$ .

- b)  $P(I, t) = (1 - t)^{-1-d}$ .  
 c)  $\dim Z(I) = \dim_{\mathbb{K}}(A_1/I_1) - 1$ .  
 2. Se  $\dim Z(I) \geq 0$  e  $\deg(Z(I)) = 1$ , allora  $I$  è equivalente ad un ideale che soddisfa le condizioni (a), (b) e (c) del punto 1).

**13.23 (Teorema di Bertini delle sezioni iperpiane, cfr. Teorema 13.5.2).** Sia  $X \subset \mathbb{P}^n$  una varietà proiettiva irriducibile e sia  $Z \subset X$  il chiuso dei suoi punti singolari. Denotiamo con  $E(X, d)$  il sottoinsieme della Grassmanniana  $G(d, \mathbb{P}^n)$  formato dai sottospazi di dimensione  $d$  che intersecano trasversalmente  $X$ . Allora  $E(X, d)$  è un aperto ed è vuoto se e solo se  $d + \dim Z \leq n - 1$ .

**13.24.** Sia  $I \subset \mathbb{K}[x_0, \dots, x_m]$  un ideale omogeneo tale che  $\dim V(I) = 0$  e  $p := [1, 0, \dots, 0] \in V(I)$ . Dimostrare che vale la formula

$$\deg_p Z(I) = \dim_{\mathbb{K}} \frac{\mathbb{K}\{x_1, \dots, x_m\}}{(I)}$$

dove  $(I)$  è l'ideale generato dai polinomi  $f(1, x_1, \dots, x_m)$  al variare di  $f \in I$ . (Sugg.: i polinomi che non si annullano in  $p$  sono invertibili come serie di potenze e quindi  $I, I_p$  generano lo stesso ideale in  $\mathbb{K}\{x_1, \dots, x_m\}$ . Inoltre per il teorema degli zeri, l'ideale  $(I_{(p)})$  (vedi Proposizione 13.3.11) contiene una potenza dell'ideale massimale.

**13.25.** Siano  $p_1, \dots, p_d \subset \mathbb{P}^2$  punti distinti ed allineati. Dimostrare che la serie di Poincaré dell'ideale di  $\{p_1, \dots, p_d\}$  è uguale a

$$\frac{\sum_{h=0}^{d-1} t^h}{1-t} = \sum_{k=0}^{+\infty} \min(k+1, d) t^k.$$

**13.26.** Siano  $p_1, \dots, p_d \subset \mathbb{P}^2$  punti distinti contenuti in una conica liscia. Dimostrare che la serie di Poincaré dell'ideale di  $\{p_1, \dots, p_d\}$  è uguale a

$$\sum_{k=0}^{+\infty} \min(2k+1, d) t^k.$$

**13.27.** Siano  $f, g \in \mathbb{K}[x_0, x_1, x_2, x_3]$  omogenei di gradi  $n, m$  senza fattori comuni. Dimostrare che il polinomio di Hilbert di  $Z(f, g)$  è uguale a

$$p(t) = nmt + nm - \binom{n}{2}m - \binom{m}{2}n = nmt - \frac{nm(n+m-4)}{2}.$$

(Sugg.: per il Teorema 13.4.6 la serie di Poincaré è uguale a

$$\frac{(1-t^n)(1-t^m)}{(1-t)^4} = \left( \frac{\sum_{h=0}^{n-1} t^h}{1-t} \right) \left( \frac{\sum_{l=0}^{m-1} t^l}{1-t} \right).$$

Calcolare il valore per  $t = 1$  del polinomio  $(\sum_{h=0}^{n-1} t^h)(\sum_{l=0}^{m-1} t^l)$  e della sua derivata.)

### Esercizi sulle sottovarietà di Hilbert-Burch

Detto alla buona, una sottovarietà di uno spazio affine o proiettivo si dice di Hilbert-Burch se il suo ideale di definizione è generato dai determinanti minori di ordine  $n - 1$  di una matrice  $n \times (n - 1)$  a coefficienti polinomi. Nei prossimi esercizi mostreremo alcuni esempi e ricaveremo la serie di Poincaré di tali sottovarietà (nel caso proiettivo).

**13.28 (Lemma di Gauss rivisitato).** Sia  $S$  un dominio a fattorizzazione unica e  $M \in M(n, m, S)$  una matrice a coefficienti in  $S$ . Diremo che  $M$  è **primitiva** se i determinanti minori di ordine massimo non hanno fattori comuni (in particolare non sono tutti nulli). Diremo che un vettore  $a \in S^n = M(n, 1, S)$  è primitivo se è primitivo come matrice. Provare:

1. Una matrice  $M \in M(n, m, S)$  è primitiva se e solo se per ogni irriducibile  $f \in S$ , detto  $F$  il campo delle frazioni di  $S/(f)$ , l'immagine di  $M$  in  $M(n, m, F)$  ha rango massimo.
2. Se una matrice  $M \in M(n, m, S)$  è primitiva e  $m \leq n$ , allora l'applicazione  $M: S^m \rightarrow S^n$  è iniettiva e trasforma vettori primitivi in vettori primitivi. È vero il viceversa?
3. Sia  $m > 0$  un intero fissato. Allora un polinomio  $\sum_{i=0}^n a_i t^i \in S[t]$  è primitivo se e solo se la matrice

$$M = (M_{ij} = a_{i-j}) = \begin{pmatrix} a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ 0 & a_0 & \dots & \cdot & a_n & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \end{pmatrix} \in M(m, n+m, S)$$

è primitiva.

4. Dedurre il lemma di Gauss 1.5.2 dai punti precedenti.

**13.29.** Siano  $S$  un dominio a fattorizzazione unica ed  $(a_{ij}) \in M(n, n-1, S)$  una matrice primitiva. Denotiamo  $m_h = (-1)^{h-1} \det((a_{ij})_{i \neq h})$ . Per la regola di Laplace vale  $\sum_i m_i a_{ij} = 0$  per ogni  $j = 1, \dots, n-1$  e quindi esiste un complesso di morfismi di  $S$ -moduli liberi

$$0 \longrightarrow S^{n-1} \xrightarrow{a_{ij}} S^n \xrightarrow{m_h} S. \tag{13.1}$$

Dimostrare che 13.1 è una successione esatta.

**13.30.** Siano  $S = \mathbb{K}[x, y, z, u_1, \dots, u_s]$  e  $I = (xy, yz, xz) \subset S$ . Provare che

$$P(I, t) = \frac{1 + 2t}{(1-t)^{s+1}}.$$

(Sugg.: l'ideale  $I$  è generato dai determinanti minori di  $\begin{pmatrix} x & 0 & z \\ 0 & y & z \end{pmatrix}$ .)

**13.31.** Sia  $S = \mathbb{K}[x_0, \dots, x_m]$ , siano  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_{n-1}$  interi fissati e, per ogni  $1 = 1, \dots, n, j = 1, \dots, n-1$ , sia  $a_{ij} \in S$  un polinomio omogeneo di grado  $\alpha_i - \beta_j$ . Denotando  $m_h = (-1)^{h-1} \det((a_{ij})_{i \neq h})$  e  $d = \sum_i \alpha_i - \sum_j \beta_j$ , dimostrare che  $m_h$  è omogeneo di grado  $d - \alpha_h$  e quindi che l'ideale  $I = (m_1, \dots, m_n)$  è omogeneo. Provare inoltre che, se la matrice  $(a_{ij})$  è primitiva, allora

$$P(I, t) = \frac{1 - \sum_i t^{d-\alpha_i} + \sum_j t^{d-\beta_j}}{(1-t)^{m+1}}$$

ed il sottoschema  $Z(I)$  ha dimensione  $m-2$ .

**13.32.** Determinare il polinomio di Hilbert delle seguenti sottovarietà di  $\mathbb{P}^3$ .

1. Due rette sghembe.
2. Due rette complanari.
3. Tre rette complanari.
4. Tre rette non complanari passanti per un punto  $p$ .

## Curve gobbe

In questo capitolo tutte le varietà si intendono definite su di un campo algebricamente chiuso  $\mathbb{K}$ . Con il termine curva intenderemo una varietà quasiproiettiva irriducibile di dimensione 1. Classicamente per curva gobba si intendeva una curva proiettiva in  $\mathbb{P}^3$  non contenuta in alcun piano. Noi useremo il termine in un senso più esteso, chiamando curva gobba una qualsiasi curva proiettiva irriducibile.

Manteniamo le notazioni introdotte nel Capitolo 12; in particolare se  $x$  è un punto di una varietà quasiproiettiva  $X$ , denotiamo con  $\mathcal{O}_{x,X}$  l'anello locale dei germi di funzioni regolari in  $x$  e con  $\mathfrak{m}_x \subset \mathcal{O}_{x,X}$  il suo ideale massimale. Se inoltre  $X$  è irriducibile, denotiamo con  $\mathbb{K}(X)$  il campo delle funzioni razionali su  $X$  e, per ogni punto  $x \in X$ , identificheremo liberamente  $\mathcal{O}_{x,X}$  con il sottoanello di  $\mathbb{K}(X)$  formato dalle funzioni razionali che sono definite in  $x$ .

### 14.1 Anelli di valutazione discreta

**Definizione 14.1.1.** *Un anello  $A$  si dice **anello di valutazione discreta** se è un dominio di integrità e se esiste un elemento non invertibile  $t \in A$ , detto **parametro locale**, tale che ogni ideale proprio e non nullo di  $A$  è generato da  $t^s$ , per qualche  $s > 0$ .*

*Esempio 14.1.2.* - I campi sono, in modo banale, anelli di valutazione discreta con parametro locale  $t = 0$ .

- L'anello  $\mathbb{K}\{t\}$  è un anello di valutazione discreta con parametro locale  $t$ .
- Se  $p \in \mathbb{N}$  è un numero primo, allora

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \text{ non divide } b \right\}$$

è un anello di valutazione discreta con parametro locale  $p \in \mathbb{Z}_{(p)}$ .

In un anello di valutazione discreta  $A$  con parametro locale  $t$  vale  $(t^s) \subset (t)$  per ogni  $s > 0$ . Ne segue che  $(t)$  è l'unico ideale massimale di  $A$ , che gli ideali  $(t)$  e  $0$  sono gli unici ideali primi e che il parametro locale è unico a meno di moltiplicazione per invertibili.

**Proposizione 14.1.3.** *Sia  $A$  un anello locale Noetheriano con ideale massimale  $\mathfrak{m}$ . Se  $\mathfrak{m}$  è principale e  $\mathfrak{m}^n \neq 0$  per ogni  $n > 0$ , allora  $A$  è un anello di valutazione discreta.*

*Dimostrazione.* Sia  $t \in \mathfrak{m}$  un generatore dell'ideale massimale. Poiché  $\mathfrak{m}^n = (t^n) \neq 0$  per ogni  $n > 0$ , l'elemento  $t$  non è nilpotente. Per il lemma di Artin-Rees 4.3.8 vale  $\bigcap_{n>0} (t^n) = 0$  e quindi  $t^n \notin (t^{n+1})$  per ogni  $n$ . Sia  $I \subset (t)$  un ideale non nullo e sia  $s$  il più grande intero tale che  $I \subset (t^s)$ . Dato che  $(t^s)/(t^{s+1})$  ha dimensione 1 come spazio vettoriale

sul campo residuo  $A/(t)$ , ne segue che  $I + (t^{s+1}) = (t^s)$  e quindi  $t^s - at^{s+1} = t^s(1 - at) \in I$  per qualche  $a \in A$ . Siccome  $1 - at$  è invertibile, si ha che  $t^s \in I$  e  $I = (t^s)$ . In particolare per ogni elemento non nullo  $a \in A$  esiste  $s \geq 0$  tale che  $(a) = (t^s)$  e quindi  $a$  è il prodotto di un invertibile e di una potenza di  $t$ ; dato che  $t$  non è nilpotente, ne segue che  $A$  è un dominio di integrità.  $\square$

**Corollario 14.1.4.** *Sia  $A$  un dominio di integrità locale Noetheriano con ideale massimale  $\mathfrak{m}$ . Allora  $A$  è di valutazione discreta se e solo se  $\mathfrak{m}/\mathfrak{m}^2$  ha dimensione 1 come spazio vettoriale su  $A/\mathfrak{m}$ .*

*Dimostrazione.* L'anello  $A$  non è un campo perché  $\mathfrak{m} \neq 0$ . Sia  $t$  un elemento di  $\mathfrak{m}$  la cui immagine in  $\mathfrak{m}/\mathfrak{m}^2$  non è nulla; allora vale  $\mathfrak{m} = (t) + \mathfrak{m}^2$  e per il lemma di Nakayama  $\mathfrak{m} = (t)$ . Adesso la dimostrazione segue immediatamente dalla Proposizione 14.1.3.  $\square$

Per ogni anello di valutazione discreta  $A$  con parametro locale  $t$ , si pone per convenzione  $(t^0) = A$  e si definisce un'applicazione (detta appunto valutazione discreta)

$$\nu: A \rightarrow \mathbb{N} \cup \{+\infty\}, \quad \nu(a) = \sup\{s \mid a \in (t^s)\}.$$

**Lemma 14.1.5.** *Sia  $A$  un anello con valutazione discreta  $\nu$ . Se  $a, b \in A$ , allora:*

1.  $\nu(a + b) \geq \min(\nu(a), \nu(b))$ .
2.  $\nu(ab) = \nu(a) + \nu(b)$ .
3. Vale  $\nu(a) = +\infty$  se e solo se  $a = 0$  e vale  $\nu(a) = 0$  se e solo se  $a$  è invertibile.
4. Vale  $\nu(a) \leq \nu(b)$  se e solo se  $a$  divide  $b$ : in particolare  $A$  è un anello Euclideo (vedi Sezione 8.1) con funzione grado  $\nu$ .

*Dimostrazione.* Facile esercizio.  $\square$

## Esercizi

**14.1.** Sia  $K$  il campo delle frazioni di un anello di valutazione discreta  $A$  e sia  $a \in K - \{0\}$ . Provare che  $a \in A$  oppure che  $a^{-1} \in A$ .

**14.2.** Sia  $A$  un dominio di integrità locale con ideale massimale  $\mathfrak{m}$ . Provare che se  $\mathfrak{m}$  è principale e  $\bigcap_{n>0} \mathfrak{m}^n = 0$ , allora  $A$  è un anello di valutazione discreta.

## 14.2 Parametri locali su curve lisce

Per il Corollario 10.8.5, se  $x$  è un punto liscio di una curva  $X$ , allora l'anello locale  $\mathcal{O}_{x,X}$  è un dominio di integrità con ideale massimale principale e quindi è un anello di valutazione discreta.

**Lemma 14.2.1.** *Sia  $x$  un punto liscio di curva affine  $X$ . Allora esiste una funzione regolare  $t \in \mathbb{K}[X]$  la cui immagine in  $\mathcal{O}_{x,X}$  genera l'ideale massimale  $\mathfrak{m}_x$ .*

*Dimostrazione.* Supponiamo che  $X \subset \mathbb{A}^n$  e che  $x$  sia il punto di coordinate affini  $x_1 = \dots = x_n = 0$ . Allora l'ideale  $\mathfrak{m}_x$  è generato dalle coordinate  $x_1, \dots, x_n$  e quindi esiste un indice  $i$  tale che  $x_i \notin \mathfrak{m}_x^2$ ; per il lemma di Nakayama  $x_i$  genera l'ideale massimale.  $\square$

**Definizione 14.2.2.** *Sia  $X$  una curva e  $x$  un suo punto liscio: una funzione razionale  $t \in \mathbb{K}(X)$  si dice un **parametro locale in  $x$**  se è regolare in  $x$  e se  $\mathfrak{m}_x = t\mathcal{O}_{x,X}$ .*

Segue dal Lemma 14.2.1 che qualsiasi curva ammette parametro locale in ogni suo punto liscio.

*Esempio 14.2.3.* La retta affine  $\mathbb{A}^1$  è una curva liscia; se  $t$  è una coordinata affine allora  $t - a$  è un parametro locale nel punto  $a$ .

Sia  $t$  un parametro locale in un punto liscio  $x$  di una curva  $X$ . Per definizione di parametro locale e anello di valutazione discreta, sappiamo che ogni  $f \in \mathcal{O}_{x,X} - \{0\}$  si scrive in modo unico come  $f = at^s$ , con  $s \geq 0$  e  $a$  invertibile. Siccome ogni funzione razionale è il quoziente di due elementi di  $\mathcal{O}_{x,X}$  possiamo dare la seguente definizione.

**Definizione 14.2.4.** *Sia  $t$  un parametro locale in un punto liscio  $x$  di una curva  $X$ . Per ogni funzione razionale non nulla  $f \in \mathbb{K}(X)^*$  si definisce **l'ordine di  $f$  nel punto  $x$**  come*

$$\text{ord}_x(f) = \sup\{n \in \mathbb{Z} \mid t^{-n}f \in \mathcal{O}_{x,X}\} \in \mathbb{Z}$$

Poiché ogni parametro locale in  $x$  è definito a meno di moltiplicazione per elementi invertibili di  $\mathcal{O}_{x,X}$ , si osserva immediatamente che l'ordine di una funzione razionale è ben definito. Notiamo inoltre che

$$\text{ord}_x(f) = n \quad \text{se e solo se} \quad t^{-n}f \in \mathcal{O}_{x,X} - \mathfrak{m}_x.$$

In altri termini ogni funzione razionale non nulla si scrive in modo unico come  $f = at^{\text{ord}_x(f)}$ , con  $a \in \mathcal{O}_{x,X}$  invertibile.

**Lemma 14.2.5.** *Sia  $x$  un punto liscio di una curva  $X$  ed  $n$  un numero intero. Allora l'insieme  $\{0\} \cup \{f \in \mathbb{K}(X)^* \mid \text{ord}_x(f) \geq n\}$  è un  $\mathcal{O}_{x,X}$ -sottomodulo di  $\mathbb{K}(X)$  ed è quindi a maggior ragione un  $\mathbb{K}$ -sottospazio vettoriale.*

*Dimostrazione.* Sia  $t$  un parametro locale in  $x$ . Basta osservare che  $\text{ord}_x(f) \geq n$  se e solo se  $t^{-n}f \in \mathcal{O}_{x,X}$ . □

Se  $\text{ord}_x(f) = n > 0$ , allora diremo che la funzione  $f$  ha uno **zero di ordine  $n$**  in  $x$ . Se  $\text{ord}_x(f) = -n < 0$ , allora diremo che  $f$  ha un **polo di ordine  $n$**  in  $x$ . Dato che  $\text{ord}_x(fg) = \text{ord}_x(f) + \text{ord}_x(g)$  e  $\text{ord}_x(f^{-1}) = -\text{ord}_x(f)$ , l'applicazione

$$\text{ord}_x: \mathbb{K}(X)^* \rightarrow \mathbb{Z}$$

è un omomorfismo di gruppi abeliani.

L'aperto di definizione di una funzione razionale  $f \in \mathbb{K}(X)$  è uguale all'insieme dei punti  $x$  tali che  $\text{ord}_x(f) \geq 0$ . In particolare se  $f$  e  $h$  sono funzioni razionali su di una curva liscia  $X$ , allora  $f^{-1}h$  è regolare in  $X$  se e solo se  $\text{ord}_x(h) \geq \text{ord}_x(f)$  per ogni  $x \in X$ .

**Lemma 14.2.6.** *Siano  $X$  una curva affine liscia e  $f: X \rightarrow \mathbb{K}$  una funzione regolare non costante. Se  $f^{-1}(0) = \{x_1, \dots, x_n\}$ , allora vale la formula*

$$\dim_{\mathbb{K}} \frac{\mathbb{K}[X]}{(f)} = \sum_i \text{ord}_{x_i}(f).$$

*Dimostrazione.* Per ogni  $i = 1, \dots, n$  denotiamo  $s_i = \text{ord}_{x_i}(f)$ . Osserviamo che una funzione  $g \in \mathbb{K}[X]$  appartiene all'ideale  $(f)$  se e solo se  $\text{ord}_{x_i}(g) \geq s_i$  per ogni  $i = 1, \dots, n$ . Scegliamo delle funzioni regolari  $t_i, g_i \in \mathbb{K}[X]$  tali che  $t_i$  è un parametro locale in  $x_i$ ,  $g_i(x_i) = 1$  e  $g_i(x_j) = 0$  se  $i \neq j$ . A meno di elevare le funzioni  $g_i$  a potenze di grado sufficientemente elevato, possiamo assumere  $\text{ord}_{x_i}(g_j) \geq s_i$  per ogni  $i \neq j$ . Vogliamo dimostrare che l'omomorfismo naturale di anelli

$$\alpha: \frac{\mathbb{K}[X]}{(f)} \rightarrow \prod_{i=1}^n \frac{\mathcal{O}_{x_i, X}}{\mathfrak{m}_{x_i}^{s_i}}$$

è un isomorfismo.

*Inieltività:* Vale  $\alpha(h) = 0$  se e solo se  $h \in \mathfrak{m}_{x_i}^{s_i}$  per ogni  $i$  e quindi  $\alpha(h) = 0$  se e solo se  $\text{ord}_{x_i}(h) \geq s_i$  per ogni  $i$ .

*Surgettività:* Per ogni  $i = 1, \dots, n$  la funzione  $g_i$  è invertibile in  $\mathcal{O}_{x_i, X}$  e quindi ogni elemento del codominio è rappresentato dalla  $n$ -upla  $(g_1 P_1(t_1), \dots, g_n P_n(t_n))$ , dove  $P_i$  è un opportuno polinomio di grado  $< s_i$ . Basta adesso osservare che tale  $n$ -upla è uguale a  $\alpha(\sum_i g_i P_i(t_i))$ .  $\square$

**Lemma 14.2.7.** *Sia  $\phi: X \rightarrow Y$  un morfismo dominante di curve affini, con  $X$  liscia. Allora per ogni  $f \in \mathbb{K}(X)$  esiste una funzione regolare non nulla  $g \in \mathbb{K}[Y]$  tale che  $\phi^*(g)f$  è regolare in  $X$ .*

*Dimostrazione.* Non è restrittivo supporre  $f = 1/h$  con  $h \in \mathbb{K}[X]$ . L'insieme  $D = \phi(h^{-1}(0))$  è un chiuso proprio di  $Y$  e, per il teorema degli zeri, esiste una funzione  $g \neq 0$ , regolare su  $Y$  e nulla su  $D$ . Ponendo  $s = \max\{\text{ord}_p(h) \mid p \in h^{-1}(0)\}$  vale  $\text{ord}_p(f\phi^*(g)^s) \geq 0$  per ogni  $p \in X$  e quindi  $f\phi^*(g^s)$  è regolare in  $X$ .  $\square$

**Teorema 14.2.8.** *Sia  $X$  una curva liscia,  $U \subset X$  un aperto denso e  $\phi: U \rightarrow \mathbb{P}^n$  un morfismo regolare. Allora  $\phi$  si estende ad un unico morfismo regolare  $\phi: X \rightarrow \mathbb{P}^n$ .*

*Dimostrazione.* Il problema è locale, possiamo quindi supporre  $X, U$  affini e che  $\phi(U)$  sia contenuto nel complementare di un iperpiano, diciamo  $x_0 = 0$ . Esistono allora  $f_1, \dots, f_n \in \mathbb{K}[U] \subset \mathbb{K}(X)$  tali che per ogni  $x \in U$  si ha  $\phi(x) = [1, f_1(x), \dots, f_n(x)]$ . Sia  $x \in X$  e sia  $t$  un parametro locale in  $x$ ; denotiamo  $a_i = \text{ord}_x(f_i)$ : se  $a_i \geq 0$  per ogni  $i$ , allora le funzioni  $f_i$  sono regolari in un intorno di  $x$  e quindi  $\phi$  si estende ad  $x$ . Se invece  $a = -\min(a_1, \dots, a_n) > 0$ , allora esiste un intorno  $V$  di  $x$  dove le funzioni razionali  $t^a f_i$  sono regolari, e l'applicazione

$$\phi: V \rightarrow \mathbb{P}^n, \quad \phi(x) = [t^a, t^a f_1(x), \dots, t^a f_n(x)]$$

è regolare e ben definita.  $\square$

Si osservi che se  $\phi(U)$  è contenuto in una varietà proiettiva  $Y \subset \mathbb{P}^n$  allora  $\phi(X) = \phi(\overline{U}) \subset \overline{Y} = Y$ .

**Corollario 14.2.9.** *Ogni morfismo birazionale tra due curve lisce proiettive è un isomorfismo.*

*Dimostrazione.* Ogni morfismo birazionale è invertibile su un aperto denso dell'immagine.  $\square$

Tra le conseguenze del Corollario 14.2.9 citiamo il fatto che una curva liscia e proiettiva è razionale (Definizione 12.4.9) se e solo se è isomorfa a  $\mathbb{P}^1$ .

**Corollario 14.2.10.** *Sia  $X$  una curva liscia. Fissato un sistema di coordinate omogenee su  $\mathbb{P}^1$ , esiste una bigezione naturale tra l'insieme delle funzioni razionali non costanti su  $X$  e l'insieme dei morfismi regolari dominanti  $X \rightarrow \mathbb{P}^1$ .*

*Dimostrazione.* Sia  $x_0, x_1$  un sistema di coordinate omogenee su  $\mathbb{P}^1$  e consideriamo l'inclusione  $\mathbb{K} \rightarrow \mathbb{P}^1, t \rightarrow [1, t]$ . Ad ogni  $f: X \rightarrow \mathbb{P}^1$  regolare dominante associamo la funzione razionale  $f^*(x_1/x_0)$ . Viceversa ad ogni funzione razionale  $g: U \rightarrow \mathbb{K} \subset \mathbb{P}^1, U \subset X$  aperto, associamo l'estensione a morfismo regolare  $X \rightarrow \mathbb{P}^1$ .  $\square$



### Esercizi

**14.3.** Sia  $X$  una curva e  $t \in \mathbb{K}(X)$  un parametro locale in un punto liscio  $x \in X$ . Provare che per ogni funzione razionale  $f \in \mathbb{K}(X)$  esiste unico un polinomio  $P$  a coefficienti in  $\mathbb{K}$  tale che  $f - P(t^{-1}) \in \mathfrak{m}_x$ .

## 14.3 Grado di morfismi di curve

Ogni morfismo dominante tra curve irriducibili  $\phi: X \rightarrow Y$  induce un'estensione di campi  $\mathbb{K}(Y) \cong \phi^*\mathbb{K}(Y) \subset \mathbb{K}(X)$ . I due campi  $\mathbb{K}(Y)$  e  $\mathbb{K}(X)$  sono finitamente generati e con grado di trascendenza 1 su  $\mathbb{K}$ , di conseguenza  $\mathbb{K}(X)$  è una estensione algebrica finita di  $\phi^*\mathbb{K}(Y)$ .

**Definizione 14.3.1.** (cfr. Definizione 12.4.16) Nelle notazioni precedenti, chiameremo **grado di  $\phi$**  la dimensione  $\deg(\phi) = [\mathbb{K}(X) : \phi^*\mathbb{K}(Y)]$  di  $\mathbb{K}(X)$  come  $\phi^*\mathbb{K}(Y)$  spazio vettoriale.

Sia  $\phi: X \rightarrow Y$  un morfismo di curve e sia  $x$  un punto liscio di  $X$  tale che  $y = \phi(x)$  sia liscio in  $Y$ . Definiamo la **molteplicità di  $\phi$  in  $x$**  come il numero

$$\text{mult}_x(\phi) = \dim_{\mathbb{K}} \frac{\mathcal{O}_{x,X}}{(\phi^*\mathfrak{m}_y)}.$$

È importante notare che se  $t$  è un parametro locale in  $y$ , allora  $\text{mult}_x(\phi) = \text{ord}_x(\phi^*t)$ : infatti  $t$  genera l'ideale  $\mathfrak{m}_y$  e quindi  $\phi^*t$  genera l'ideale  $(\phi^*\mathfrak{m}_y)$ .

*Esempio 14.3.2.* Sia  $X$  una curva e  $f: X \rightarrow \mathbb{K}$  un morfismo regolare. Se  $x \in f^{-1}(0)$  è un punto liscio di  $X$ , allora  $\text{mult}_x(f) = \text{ord}_x(f)$ .

**Teorema 14.3.3.** Sia  $\phi: X \rightarrow Y$  un morfismo finito di curve lisce. Allora per ogni  $y \in Y$  vale

$$\deg(\phi) = \sum_{x \in \phi^{-1}(y)} \text{mult}_x(\phi).$$

*Dimostrazione.* Sia  $y \in Y$  un punto fissato,  $\phi^{-1}(y) = \{x_1, \dots, x_n\}$ ,  $t$  un parametro locale in  $y$  e  $y \in U \subset Y$  un aperto affine tale che  $t$  sia regolare in  $U$  ed invertibile in  $U - y$ . Il morfismo  $\phi$  è finito e quindi  $V = \phi^{-1}(U)$  è affine e  $\mathbb{K}[V]$  è un  $\mathbb{K}[U]$ -modulo finitamente generato. Si consideri l'anello  $B = \mathbb{K}[V]/(\phi^*t)$ , per il Lemma 14.2.6 vale  $\dim_{\mathbb{K}} B = \sum_i \text{mult}_{x_i}(\phi)$ . Basta quindi dimostrare l'uguaglianza  $\dim_{\mathbb{K}} B = \deg \phi = [\mathbb{K}(V) : \phi^*\mathbb{K}(U)]$ . Siano  $u_1, \dots, u_d$  elementi di  $\mathbb{K}[V]$  che inducono una  $\mathbb{K}$ -base di  $B$  e dimostriamo che sono una  $\mathbb{K}(U)$ -base di  $\mathbb{K}(V)$ . Per semplicità di notazione identifichiamo  $\mathbb{K}(U)$  con la sua immagine  $\phi^*\mathbb{K}(U) \subset \mathbb{K}(V)$ .

1)  $u_1, \dots, u_d$  sono linearmente indipendenti. Sia per assurdo  $\sum f_i u_i = 0$  con  $f_i \in \mathbb{K}(U)$  non tutti nulli, moltiplicando per un denominatore comune possiamo supporre  $f_i \in \mathbb{K}[U]$  e dividendo per una opportuna potenza di  $t$  possiamo supporre che i numeri  $f_i(y)$  non siano tutti nulli. La riduzione modulo  $t$  è allora una relazione di equivalenza lineare in  $B$ .  
2)  $u_1, \dots, u_s$  generano  $\mathbb{K}(V)$ . Sia  $S = \mathbb{K}[U] - I(y)$ ;  $S$  è una parte moltiplicativa e  $S^{-1}\mathbb{K}[V]$  è un  $\mathcal{O}_{y,U} = S^{-1}\mathbb{K}[U]$  modulo finito. Osserviamo che

$$S^{-1}B = \frac{S^{-1}\mathbb{K}[V]}{(t)} = \frac{S^{-1}\mathbb{K}[V]}{(\phi^*\mathfrak{m}_y)}$$

e per il lemma di Nakayama  $u_1, \dots, u_d$  generano  $S^{-1}\mathbb{K}[V]$  come  $S^{-1}\mathbb{K}[U]$ -modulo. Se  $f$  è una funzione razionale su  $V$ , esiste  $h \in \mathbb{K}[U]$  tale che  $hf \in \mathbb{K}[V] \subset S^{-1}\mathbb{K}[V]$ .  $\square$

**Corollario 14.3.4.** *Sia  $\phi: X \rightarrow Y$  un morfismo surgettivo di curve lisce proiettive. Allora per ogni  $y \in Y$  vale*

$$\deg(\phi) = \sum_{x \in \phi^{-1}(y)} \text{mult}_x(\phi).$$

*Dimostrazione.* Siccome  $X$  è proiettiva ed irriducibile e  $\phi(X) = Y$ , per ragioni dimensionali le fibre di  $\phi$  devono avere dimensione 0, ovvero il morfismo  $\phi$  è quasifinito. Per il Teorema 12.2.8 il morfismo  $\phi$  è finito e si applica il Teorema 14.3.3.  $\square$

### Esercizi

**14.4.** Sia  $\phi: X \rightarrow Y$  un morfismo dominante di curve lisce. Dimostrare che  $\phi$  è ramificato in  $x \in X$  (Definizione 12.1.3) se e solo se  $\text{mult}_x(\phi) > 1$ .

**14.5.** In caratteristica  $p > 0$ , dimostrare che la molteplicità del morfismo di Frobenius

$$F: \mathbb{P}^1 \rightarrow \mathbb{P}^1, \quad [x_0, x_1] \mapsto [x_0^p, x_1^p]$$

è uguale a  $p$  in ogni punto.

**14.6.** Siano  $\phi: X \rightarrow Y$  e  $\psi: Y \rightarrow Z$  morfismi dominanti di curve lisce. Provare che per ogni  $x \in X$  vale  $\text{mult}_x(\psi\phi) = \text{mult}_x(\phi) \text{mult}_{\phi(x)}(\psi)$ .

## 14.4 Divisori

Un **divisore**<sup>1</sup>  $D$  su una curva liscia  $X$  è dato da una combinazione lineare formale finita di punti della curva  $X$  a coefficienti interi; ossia

$$D = \sum_{i=1}^s n_i x_i, \quad \text{con } n_i \in \mathbb{Z} \text{ e } x_i \in X.$$

Diremo poi che due combinazioni lineari definiscono lo stesso divisore se hanno le stesse molteplicità in ogni punto di  $X$ , dove la molteplicità in  $x \in X$  è data da

$$\text{mult}_x \left( \sum_{i=1}^s n_i x_i \right) = \begin{cases} 0 & \text{se } x \neq x_i \text{ per ogni } i, \\ \sum \{n_i \mid x_i = x\} & \text{altrimenti.} \end{cases}$$

I divisori formano un gruppo che viene indicato con  $\text{Div}(X)$ . Ogni divisore possiede una unica rappresentazione non ridondante  $\sum_i n_i x_i$ , dove  $n_i \neq 0$  per ogni  $i$  e  $x_i \neq x_j$  per ogni  $i \neq j$ . Lavorando con le combinazioni non ridondanti scriveremo quindi ad esempio  $(p + q - r) + (p - q + s) = 2p + s - r$ . L'elemento neutro di  $\text{Div}(X)$  è il **divisore nullo** corrispondente alla combinazione lineare nulla. Se  $D = \sum n_i x_i$  è la rappresentazione non ridondante di un divisore, allora  $\text{mult}_{x_i}(D) = n_i$  e  $\text{mult}_x(D) = 0$  se  $x \neq x_i$  per ogni  $i$ . Il **supporto** di un divisore è il sottoinsieme finito di  $X$  formato dai punti di molteplicità diversa da 0: ad esempio il supporto del divisore  $2p - q$  è uguale a  $\{p, q\}$ . Il **grado** di un divisore è la somma di tutte le molteplicità:

$$\deg(D) = \sum_{x \in X} \text{mult}_x(D), \quad \text{ossia} \quad \deg\left(\sum n_i x_i\right) = \sum n_i, \quad \text{dove } n_i \in \mathbb{Z}, x_i \in X.$$

<sup>1</sup> Il nome divisore è abbastanza recente ed è stato copiato da una nozione analoga in teoria algebrica dei numeri. Il termine precedente era *ciclo* (vedi [Walk1950]) che a sua volta aveva sostituito *gruppo di punti* (vedi [EC1915]).

Si indica con  $\text{Div}^0(X)$  il sottogruppo dei divisori di grado 0. Su  $\text{Div}(X)$  esiste un ordinamento naturale, dove  $D_1 \leq D_2$  se e soltanto se  $\text{mult}_x(D_1) \leq \text{mult}_x(D_2)$  per ogni  $x \in X$ . Un divisore si dice **effettivo** se è maggiore od uguale al divisore nullo; equivalentemente un divisore è effettivo se e soltanto se ha molteplicità non negativa in ogni punto. Si consideri adesso un morfismo surgettivo  $\phi: X \rightarrow Y$  di curve lisce proiettive, per ogni  $x \in X$  sia  $\text{mult}_x(\phi)$  la molteplicità di  $\phi$  in  $x$ . È possibile definire un omomorfismo di gruppi abeliani

$$\phi^*: \text{Div}(Y) \rightarrow \text{Div}(X)$$

ponendo

$$\phi^*y = \sum_{x \in \phi^{-1}(y)} \text{mult}_x(\phi)x$$

per ogni  $y \in Y$  ed estendendo per linearità.

**Teorema 14.4.1.** *Per ogni morfismo surgettivo di curve lisce proiettive  $\phi: X \rightarrow Y$  e per ogni divisore  $D \in \text{Div}(Y)$  vale*

$$\deg(\phi^*(D)) = \deg(D) \deg(\phi).$$

*Dimostrazione.* Immediata conseguenza del Teorema 14.3.3. □

**Definizione 14.4.2.** *Sia  $f$  una funzione razionale non nulla su una curva liscia  $X$ . Il **divisore di  $f$**  è il divisore che ha per molteplicità gli ordini di  $f$ , cioè<sup>2</sup>*

$$\text{div}(f) = \sum_{x \in X} \text{ord}_x(f)x.$$

*Se separiamo gli zeri dai poli, possiamo scrivere  $\text{div}(f) = \text{div}(f)_0 - \text{div}(f)_\infty$ , dove i divisori*

$$\text{div}(f)_0 = \sum \{\text{ord}_x(f)x \mid x \text{ zero di } f\}, \quad \text{div}(f)_\infty = - \sum \{\text{ord}_x(f)x \mid x \text{ polo di } f\},$$

*sono effettivi ed univocamente definiti. Più in generale ogni divisore si scrive in modo unico come differenza di due divisori effettivi a supporti disgiunti.*

*L'applicazione*

$$\mathbb{K}(X)^* \rightarrow \text{Div}(X), \quad f \mapsto \text{div}(f),$$

*è un omomorfismo di gruppi la cui immagine  $P(X) := \text{div}(\mathbb{K}(X)^*)$  viene detta **sottogruppo dei divisori principali**.*

**Corollario 14.4.3.** *Ogni divisore principale in una curva liscia proiettiva ha grado 0.*

*Dimostrazione.* Bisogna dimostrare che, se  $X$  è liscia e proiettiva e  $f \in \mathbb{K}(X)$  è una funzione razionale non nulla, allora  $\text{div}(f)$  ha grado 0. Se  $f$  è costante è tutto banale, altrimenti possiamo considerare  $f$  come un morfismo surgettivo  $f: X \rightarrow \mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ . Adesso basta osservare che  $\text{div}(f) = f^*(\{0\} - \{\infty\})$  ed applicare il Teorema 14.4.1. □

Dunque i divisori principali su una curva liscia proiettiva formano un sottogruppo  $P(X) \subset \text{Div}^0(X)$ .

**Definizione 14.4.4.** *Diremo che due divisori  $D_1$  e  $D_2$  sono **linearmente equivalenti**, e scriveremo  $D_1 \sim D_2$ , se la loro differenza è un divisore principale. Il **gruppo delle classi di una curva liscia proiettiva  $X$**  è definito come  $\text{Cl}(X) = \text{Div}(X)/P(X) = \text{Div}(X)/\sim$ .*

<sup>2</sup> Alcuni autori utilizzano il simbolo  $(f)$  per indicare il divisore di una funzione razionale  $f$

Dato che due divisori linearmente equivalenti hanno sempre lo stesso grado possiamo scrivere  $\text{Cl}(X) = \bigoplus_{n \in \mathbb{Z}} \text{Cl}^n(X)$ , dove  $\text{Cl}^n(X)$  indica l'insieme delle classi di equivalenza lineare dei divisori di grado  $n$ .

**Proposizione 14.4.5 (Teorema di Clebsch, 1863).** *Sia  $X$  una curva liscia proiettiva. Allora  $X$  è isomorfa a  $\mathbb{P}^1$  se e solo se  $\text{Cl}^0(X) = 0$ .*

*Dimostrazione.* Se  $X = \mathbb{P}^1$  e  $t$  è una coordinata affine, allora il divisore della funzione razionale  $t - a$  è  $\{a\} - \{\infty\}$ . Dunque tutti i punti sono linearmente equivalenti a  $\{\infty\}$  e ogni divisore di grado  $d$  è linearmente equivalente a  $d\{\infty\}$ .

Viceversa, se  $\text{Cl}^0(X) = 0$ , allora scelti due punti  $q \neq p$  in  $X$ , esiste una funzione razionale non costante  $f$  tale che  $\text{div}(f) = p - q$ . Se pensiamo  $f$  come un morfismo  $f: X \rightarrow \mathbb{P}^1$ , allora  $f^*(\{0\} - \{\infty\}) = p - q$  e l'unica possibilità è che  $f^*\{0\} = p$ . In particolare  $\text{deg}(f) = 1$  ed  $f$  è un morfismo birazionale, quindi un isomorfismo.  $\square$

**Definizione 14.4.6.** *Sia  $X$  una curva liscia proiettiva fissata. Per ogni divisore  $D$  su  $X$  si definisce*

$$H^0(X, D) = \{f \in \mathbb{K}(X)^* \mid \text{div}(f) + D \geq 0\} \cup \{0\}.$$

Quando è chiaro dal contesto quale sia la curva  $X$  scriveremo semplicemente  $H^0(D)$  al posto di  $H^0(X, D)$ . Notiamo che  $H^0(X, D)$  è un  $\mathbb{K}$ -sottospazio vettoriale di  $\mathbb{K}(X)$  e che, se  $\text{deg}(D) < 0$ , allora  $H^0(X, D) = 0$ .

**Teorema 14.4.7.** *Sia  $D$  un divisore su una curva liscia proiettiva  $X$ . Allora:*

1. *Lo spazio vettoriale  $H^0(X, D)$  ha dimensione finita su  $\mathbb{K}$  e vale*

$$\dim_{\mathbb{K}} H^0(X, D) \leq \max(0, \text{deg}(D) + 1).$$

2. *Per ogni divisore effettivo  $E$  su  $X$  vale*

$$\dim_{\mathbb{K}} H^0(X, D + E) \leq \dim_{\mathbb{K}} H^0(X, D) + \text{deg}(E).$$

*Dimostrazione.* Poiché  $E$  è un divisore effettivo si ha  $H^0(X, D) \subset H^0(X, D + E)$ . Dimostriamo come prima cosa che la codimensione di  $H^0(X, D)$  in  $H^0(X, D + E)$  è minore od uguale a  $\text{deg}(E)$ . Ragionando per induzione sul grado di  $E$ , è sufficiente dimostrare il teorema nel caso in cui il divisore  $E$  ha grado 1. Sia dunque  $E = x$ , per qualche  $x \in X$ , e sia  $\text{mult}_x(D) = a$ . Se  $t$  è un parametro locale in  $x$ , allora tutte le funzioni razionali appartenenti a  $H^0(X, D + x)$  si possono scrivere nella forma  $t^{-a-1}g$ , con  $g \in \mathcal{O}_{x, X}$ . Notiamo che  $H^0(D) \subset H^0(D + x)$  è esattamente il nucleo dell'applicazione lineare  $H^0(D + x) \rightarrow \mathbb{K}$  data da  $t^{-a-1}g \mapsto g(x)$  e quindi ha codimensione al più 1. Le funzioni razionali in  $H^0(X, 0)$  non hanno poli e quindi sono regolari su  $X$ . Per ipotesi  $X$  è proiettiva e quindi  $H^0(X, 0) \subset \mathbb{K}(X)$  è il sottospazio delle funzioni costanti. Ne segue che per ogni divisore effettivo  $E$  vale la formula

$$\dim_{\mathbb{K}} H^0(X, E) \leq \dim_{\mathbb{K}} H^0(X, 0) + \text{deg}(E) = \text{deg}(E) + 1.$$

Siamo adesso in grado di dimostrare il punto 1. Se  $H^0(X, D) = 0$ , allora il risultato è certamente vero. Se invece esiste una funzione razionale non nulla  $f \in H^0(X, D)$ , allora il divisore  $E = D + \text{div}(f)$  è effettivo e quindi si ha  $\dim_{\mathbb{K}} H^0(X, E) \leq \text{deg}(E) + 1$ . Basta adesso osservare che i divisori  $D$  ed  $E$  hanno lo stesso grado e che  $fH^0(X, E) = H^0(X, D) \subset \mathbb{K}(X)$ .  $\square$

**Definizione 14.4.8.** *Per ogni divisore  $D$  su di una curva liscia proiettiva  $X$  denotiamo  $h^0(X, D) = \dim_{\mathbb{K}} H^0(X, D)$ .*

Come sopra, se non ci sono ambiguità su  $X$ , scriveremo  $h^0(D)$  al posto di  $h^0(X, D)$ .

**Corollario 14.4.9.** *Se  $D$  ed  $E$  sono divisori linearmente equivalenti su di una curva liscia proiettiva, allora  $h^0(D) = h^0(E)$ .*

*Dimostrazione.* Sia  $X$  la curva. Se  $E = D + \text{div}(f)$ , allora la moltiplicazione per  $f$  induce un isomorfismo di spazi vettoriali  $fH^0(X, E) = H^0(X, D) \subset \mathbb{K}(X)$ .  $\square$

*Esempio 14.4.10.* Sia  $D$  un divisore di grado  $d > 0$  sulla retta proiettiva  $\mathbb{P}^1$ ; allora  $h^0(\mathbb{P}^1, D) = d + 1$ . Infatti, su  $\mathbb{P}^1$  i divisori dello stesso grado sono linearmente equivalenti e quindi, per il Corollario 14.4.7, è sufficiente dimostrare che  $h^0(\mathbb{P}^1, d\{\infty\}) = d + 1$ . Lo spazio vettoriale  $H^0(\mathbb{P}^1, d\{\infty\})$  può essere interpretato come lo spazio delle funzioni regolari su  $\mathbb{A}^1$  che hanno un polo di ordine al più  $d$  all'infinito. Tali funzioni sono tutti e soli i polinomi di grado  $\leq d$  nella coordinata affine.

Abbiamo visto che ogni insieme finito di divisori su una curva  $X$  possiede estremo inferiore ed estremo superiore. Notiamo che per ogni coppia di divisori  $D, E$  vale

$$\inf(D, E) = \sum_{x \in X} \min(\text{mult}_x(D), \text{mult}_x(E)),$$

$$\sup(D, E) = \sum_{x \in X} \max(\text{mult}_x(D), \text{mult}_x(E)),$$

e quindi  $D + E = \inf(D, E) + \sup(D, E)$ . Inoltre  $H^0(X, D)$  e  $H^0(X, E)$  sono sottospazi vettoriali di  $H^0(X, \sup(D, E))$  e la loro intersezione è esattamente  $H^0(X, \inf(D, E))$ .

**Lemma 14.4.11 (Formula di Grassmann).** *Siano  $D, E$  divisori su una curva liscia proiettiva  $X$ . Allora vale*

$$h^0(X, D) + h^0(X, E) \leq h^0(X, \inf(D, E)) + h^0(X, \sup(D, E)).$$

*Dimostrazione.* Lo spazio vettoriale  $H^0(X, \sup(D, E))$  ha dimensione finita e quindi basta applicare la classica formula di Grassmann che si studia nei corsi di algebra lineare.  $\square$

## Esercizi

**14.7.** Provare che ogni insieme finito di divisori su di una curva liscia possiede estremo inferiore e che, se  $f_1, \dots, f_n$  sono funzioni razionali, allora

$$\text{div}(c_1 f_1 + \dots + c_n f_n) \geq \inf\{\text{div}(f_i) \mid i = 1, \dots, n\}$$

per ogni scelta di costanti  $c_1, \dots, c_n$  tali che  $\sum c_i f_i \neq 0$ .

## 14.5 Sistemi lineari

**Definizione 14.5.1.** *Sia  $D$  un divisore su di una curva liscia proiettiva  $X$ . L'insieme dei divisori effettivi linearmente equivalenti a  $D$ , che denoteremo  $|D|$ , si dice un **sistema lineare completo** su  $X$ .*

Se il grado di un divisore  $D$  è negativo, allora  $|D| = \emptyset$ . La transitività dell'equivalenza lineare implica che se  $D \sim E$ , allora  $|D| = |E|$ . Viceversa se  $|D| = |E| \neq \emptyset$ , allora  $D \sim E$ .

Vogliamo adesso dimostrare che su ogni sistema lineare completo  $|D|$  esiste una struttura naturale di spazio proiettivo di dimensione finita, che non dipende dalla scelta di  $D$  all'interno della sua classe di equivalenza lineare. Esiste una bigezione tra il proiettivizzato  $\mathbb{P}(H^0(X, D))$  ed il sistema lineare completo  $|D|$ . Si consideri infatti l'applicazione

$$\gamma_D: (H^0(X, D) - \{0\}) \rightarrow |D|, \quad \gamma_D(f) = D + \operatorname{div}(f),$$

che alla funzione razionale  $f$  associa il divisore  $D + \operatorname{div}(f)$ . Per definizione  $f \in H^0(X, D) - \{0\}$  se e solo se  $D + \operatorname{div}(f)$  è effettivo e quindi  $\gamma_D$  è surgettiva. Viceversa se  $\gamma_D(f) = \gamma_D(g)$ , allora  $D + \operatorname{div}(f) = D + \operatorname{div}(g)$  da cui segue che  $\operatorname{div}(fg^{-1}) = 0$  e  $fg^{-1}$  è una funzione regolare su  $X$  e quindi costante. Poniamo su  $|D|$  la struttura di spazio proiettivo indotta dalla bigezione  $\gamma_D: \mathbb{P}(H^0(X, D)) \rightarrow |D|$  e consideriamo un divisore  $E$  linearmente equivalente a  $D$ : indichiamo con  $g$  una funzione razionale non nulla tale che  $D + \operatorname{div}(g) = E$ . Abbiamo già osservato che la moltiplicazione per  $g$  induce un isomorfismo di spazi vettoriali  $g: H^0(X, E) \rightarrow H^0(X, D)$  e dunque segue immediatamente dalle definizioni che  $\gamma_E = \gamma_D \circ [g]$ , dove  $[g]$  denota la proiettività indotta da  $g$ .

**Definizione 14.5.2.** *Un sistema lineare di divisori su una curva liscia proiettiva è un sottospazio proiettivo di  $|D|$ , per qualche divisore  $D$ .*

Anticamente i sistemi lineari venivano chiamati *serie lineari*. Una serie lineare  $L \subset |D|$  veniva chiamata una  $g_d^l$  se  $\deg(D) = d$  e  $\dim(L) = l$ . Ad esempio, la prima parte del Teorema 14.4.7 veniva enunciata dicendo che su una curva liscia proiettiva non esistono serie  $g_d^l$  con  $l > d \geq 0$ .

*Esempio 14.5.3.* Per il Teorema del Resto 6.5.2, i divisori aggiunti di grado fissato su di una curva piana liscia formano un sistema lineare completo.

**Lemma 14.5.4.** *Siano  $D, E$  divisori effettivi su una curva liscia proiettiva. Allora vale*

$$\dim |D + E| \geq \dim |D| + \dim |E|$$

*e vale l'uguaglianza se e solo se ogni divisore di  $|D + E|$  è la somma di un divisore di  $|D|$  e di uno di  $|E|$ .*

*Dimostrazione.* L'applicazione

$$s: |D| \times |E| \rightarrow |D + E|, \quad s(D', E') = D' + E'$$

è un morfismo regolare di varietà proiettive irriducibili. Poiché ogni divisore di  $|D + E|$  può essere scritto in al più un numero finito di modi come la somma di un divisore di  $|D|$  e di un divisore di  $|E|$ , le fibre di  $s$  hanno dimensione  $\leq 0$ : ne segue che  $\dim |D| \times |E| \leq \dim |D + E|$  e l'uguaglianza vale se e solo se  $s$  è surgettiva.  $\square$

**Definizione 14.5.5.** *Sia  $L$  un sistema lineare di divisori ed  $E$  un divisore effettivo su una curva liscia proiettiva. Si definisce*

$$L(-E) = \{D \in L \mid D - E \geq 0\},$$

*ovvero  $L(-E)$  è l'insieme dei divisori di  $L$  che si possono scrivere nella forma  $E + F$ , per qualche divisore effettivo  $F$ .*

**Lemma 14.5.6.** *Sia  $L$  un sistema lineare di divisori ed  $E$  un divisore effettivo su una curva liscia proiettiva. Allora  $L(-E)$  è un sottospazio proiettivo di  $L$  di codimensione al più  $\deg(E)$ . In particolare  $L(-E)$  è a sua volta un sistema lineare di divisori.*

*Dimostrazione.* Se  $L = \emptyset$  non c'è nulla da dimostrare, possiamo quindi supporre  $L$  non vuoto. Indichiamo con  $X$  la curva e con  $D$  un divisore tale che  $L \subset |D|$ . Esiste allora un sottospazio vettoriale  $V \subset H^0(X, D) \subset \mathbb{K}(X)$  tale che  $L = \mathbb{P}(V)$ . Data una funzione razionale  $f \in V - \{0\}$ , vale  $\text{div}(f) + D \in L(-E)$  se e solo se  $\text{div}(f) + D - E \geq 0$  e quindi  $L(-E)$  corrisponde al proiettivizzato di  $V \cap H^0(X, D - E)$ . Poiché  $E$  è effettivo, per il Teorema 14.4.7, il sottospazio  $H^0(X, D - E)$  ha codimensione al più  $\text{deg}(E)$  in  $H^0(X, D)$  e quindi  $V \cap H^0(X, D - E)$  ha codimensione al più  $\text{deg}(E)$  in  $V$ .  $\square$

Analizziamo più attentamente il Lemma 14.5.6 nel caso in cui  $E = p$  è un punto della curva. Sono possibili due alternative: nella prima  $L(-p) = L$ , questo significa che  $D - p$  è effettivo per ogni  $D \in L$  o, equivalentemente, che  $p$  è contenuto nel supporto di ogni divisore di  $L$ . Nel secondo caso  $L(-p)$  è un iperpiano in  $L$  ed esiste un divisore  $D \in L$  che non contiene  $p$  nel proprio supporto.

**Proposizione 14.5.7.** *Sia  $D$  un divisore di grado positivo su una curva liscia proiettiva  $X$ . Allora vale  $\dim |D| = \text{deg}(D)$  se e solo se  $X = \mathbb{P}^1$ .*

*Dimostrazione.* Abbiamo osservato nell'Esempio 14.4.10 che se  $X = \mathbb{P}^1$ , allora  $\dim |D| = \text{deg}(D)$  per ogni divisore effettivo  $D$ . Viceversa, dimostriamo per induzione su  $\text{deg}(D)$  che se  $\dim |D| = \text{deg}(D)$ , allora  $X = \mathbb{P}^1$ . Se  $\dim |D| = \text{deg}(D) = 1$  allora esistono due punti distinti  $p, q \in |D|$  e quindi una funzione razionale  $f$  tale che  $\text{div}(f) = p - q$ . L'applicazione  $f: X \rightarrow \mathbb{P}^1$  ha grado 1 ed è quindi un isomorfismo. Supponiamo  $\dim |D| = \text{deg}(D) = d > 1$  e sia  $p \in X$  un punto fissato. Il divisore  $D - p$  ha grado  $d - 1$ , per il Teorema 14.4.7 vale  $\dim |D - p| \leq d - 1$ , mentre per il Lemma 14.5.6 vale  $\dim |D - p| \geq d - 1$ .  $\square$

**Definizione 14.5.8.** *L'insieme dei **punti base** di un sistema lineare  $L$  di divisori su una curva  $X$  è*

$$BS(L) = \{p \in X \mid D - p \geq 0 \text{ per ogni } D \in L\} = \{p \in X \mid L(-p) = L\},$$

ovvero  $BS(L)$  è l'intersezione dei supporti dei divisori in  $L$ . Un sistema lineare  $L$  si dice **senza punti base** se  $BS(L) = \emptyset$ .

*Esempio 14.5.9.* Siano  $X$  una curva liscia proiettiva e  $\phi: X \rightarrow \mathbb{P}^n$  un morfismo regolare non costante. Vogliamo definire, per ogni ipersuperficie  $H \subset \mathbb{P}^n$  tale che  $\phi(X) \not\subset H$ , un divisore  $\phi^*(H)$  sulla curva  $X$ . Fissiamo un sistema di coordinate omogenee  $x_0, \dots, x_n$  su  $\mathbb{P}^n$  e siano  $f_0, \dots, f_n$  funzioni razionali su  $X$  tali che  $\phi = [f_0, \dots, f_n]$ . Scegliamo un iperpiano  $H_\infty$  tale che  $H \cap H_\infty \cap \phi(X) = \emptyset$ . Se  $F(x_0, \dots, x_n) = 0$  e  $\sum b_i x_i = 0$  sono le equazioni di  $H$  e  $H_\infty$  rispettivamente, si definisce  $\phi^*(H)$  come il divisore degli zeri  $\text{div}(g)_0$  della funzione razionale  $g = \phi^*(F / (\sum b_i f_i)^d)$ , dove  $d$  è il grado di  $F$ . Lasciamo per esercizio la necessaria verifica che  $\phi^*(H)$  è ben definito. L'insieme dei divisori  $\phi^*(H)$ , al variare di  $H$  tra le ipersuperfici in  $\mathbb{P}^n$  di grado  $d$  che non contengono  $\phi(X)$ , forma un sistema lineare senza punti base che denoteremo  $L_\phi(d)$ . Infatti i divisori di  $L_\phi(d)$  sono tutti e soli quelli della forma  $\phi^*(H) + \text{div}(\phi^*(G/F))$ , dove  $G$  varia tra i polinomi omogenei di grado  $d$ .

Per ogni sistema lineare di divisori  $L$  senza punti base su una curva liscia proiettiva  $X$ , possiamo definire il morfismo

$$\phi_L: X \rightarrow L^\vee, \quad \phi_L(p) = L(-p).$$

In altri termini  $\phi_L(p)$  è l'iperpiano in  $L$  formato dai divisori che hanno molteplicità positiva in  $p$ .

**Proposizione 14.5.10.** *Sia  $L$  un sistema lineare di divisori senza punti base su una curva liscia proiettiva  $X$ , allora:*

1. Il morfismo  $\phi_L: X \rightarrow L^\vee$  è regolare.
2. Per ogni divisore  $E \in L$  denotiamo con  $E^\perp \subset L^\vee$  l'iperpiano ad esso ortogonale. Allora, nelle notazioni dell'Esempio 14.5.9, vale  $\phi_L^* E^\perp = E$ . In particolare l'immagine  $\phi_L(X)$  non è contenuta in alcun iperpiano.
3. Il morfismo  $\phi_L: X \rightarrow L^\vee$  è un isomorfismo sull'immagine se e solo se per ogni coppia di punti  $p, q \in X$ , possibilmente coincidenti, vale  $\dim L(-p - q) = \dim L - 2$ .

*Dimostrazione.* [1] Per ogni divisore  $D \in L$  denotiamo  $X_D = X - \text{Supp}(D)$ ; poiché  $L$  non ha punti base gli aperti  $X_D$  ricoprono  $X$  ed è quindi sufficiente dimostrare che  $\phi_L$  è regolare in  $X_D$ , per ogni  $D$ . Sia  $n$  la dimensione di  $L$  e sia  $V \subset H^0(X, D)$  il sottospazio vettoriale di dimensione  $n + 1$  tale che

$$L = \{\text{div}(f) + D \mid f \in V - \{0\}\}.$$

Siano  $f_0, \dots, f_n$  funzioni razionali su  $X$  che formano una base di  $V$ . Poiché  $\text{div}(f) + D \geq 0$  per ogni  $f \in V - \{0\}$ , le funzioni  $f_0, \dots, f_n$  sono regolari in  $X_D$ . Inoltre, poiché  $L$  non ha punti base, le funzioni  $f_0, \dots, f_n$  non hanno zeri comuni in  $X_D$ : è quindi ben definita un'applicazione regolare

$$F: X_D \rightarrow \mathbb{P}^n, \quad F(p) = [f_0(p), \dots, f_n(p)].$$

La stessa base di  $V$  induce un isomorfismo di spazi proiettivi

$$\gamma: \mathbb{P}^n \rightarrow L, \quad \gamma([a_0, \dots, a_n]) = \text{div} \left( \sum_{i=0}^n a_i f_i \right) + D.$$

Dimostriamo adesso che  $F$  è la composizione di  $\phi_L$  e del trasposto di  $\gamma$ : per il principio di dualità è sufficiente dimostrare che, per ogni  $p \in X_D$ , vale  $\gamma(F(p)^\perp) \subset \phi_L^\perp$ , ovvero che

$$\gamma(\{[a_0, \dots, a_n] \mid \sum_i a_i f_i(p) = 0\}) \subset L(-p).$$

Dalla definizione di  $\gamma$  segue immediatamente la validità di quest'ultima inclusione.

[2] Dato che  $\phi_L(p) \in E^\perp$  se e solo se  $E \in L(-p)$ , ne segue che  $\phi_L(p) \in E^\perp$  se e solo se  $p$  appartiene al supporto di  $E$ . Utilizziamo la costruzione del punto [1] scegliendo il divisore  $D$  in modo tale che  $\text{Supp}(D) \cap \text{Supp}(E) = \emptyset$ , cioè in modo tale che il supporto di  $E$  sia contenuto in  $X_D$ . Possiamo inoltre scegliere le funzioni razionali  $f_i$  in modo tale che  $f_0 = 1$  e quindi che  $\gamma^{-1}(D) = [1, 0, \dots, 0]$ . Dire che  $\gamma^{-1}(E) = [a_0, \dots, a_n]$  significa dire che  $\text{div}(\sum_i a_i f_i) = E - D$  e che  $\gamma^t(E^\perp) = \{[x_0, \dots, x_n] \mid \sum a_i x_i = 0\}$ . In definitiva si ha che  $\phi_L^*(E^\perp)$  coincide con il divisore degli zeri della funzione razionale  $F^*((\sum_i a_i x_i)/x_0) = \sum a_i f_i$  ed è quindi uguale ad  $E$ .

[3] Se  $p, q \in X$  sono punti distinti, allora vale  $\phi_L(p) = \phi_L(q)$  se e solo se  $L(-p) = L(-q)$ , ovvero se e solo se  $L(-p - q) = L(-p) \cap L(-q)$  ha codimensione 1. Questo prova che  $\phi_L$  è iniettivo se e solo se per ogni coppia di punti distinti  $p, q \in X$  vale  $\dim L(-p - q) = \dim L - 2$ . Sia  $p \in X$  un punto fissato; vogliamo dimostrare che  $\phi_L$  è ramificato in  $p$  se e solo se  $L(-2p) = L(-p)$ . Infatti, poiché lo spazio tangente ad  $X$  in  $p$  ha dimensione 1,  $\phi_L$  è ramificato in  $p$  se e solo se  $\phi_L^* \mathfrak{m}_{q, L^\vee} \subset \mathfrak{m}_{p, X}^2$ , dove  $q = \phi_L(p)$ . Fissiamo un sistema di coordinate omogenee  $x_0, \dots, x_n$  in  $L^\vee$  tali che  $q = [1, 0, \dots, 0]$ ; allora  $\mathfrak{m}_{q, L^\vee}$  è generato dai germi in  $q$  delle funzioni razionali  $x_1/x_0, \dots, x_n/x_0$ . Dire che  $\phi_L$  è ramificato in  $p$  significa dire che  $\phi_L^*(\sum_{i=1}^n a_i x_i/x_0) \in \mathfrak{m}_{p, X}^2$  per ogni scelta delle costanti  $a_1, \dots, a_n$  e questo è, per il punto [2], equivalente a dire che ogni divisore di  $L$  passante per  $p$  ha in tal punto molteplicità almeno 2, cioè  $L(-p) = L(-2p)$ . Abbiamo quindi dimostrato che  $\phi_L$  è non ramificato se e solo se per ogni  $p \in X$  vale  $\dim L(-2p) = \dim L - 2$ . Osserviamo adesso che, per il Teorema 12.2.10, un morfismo regolare di varietà proiettive è un isomorfismo sull'immagine se e solo se è iniettivo e non ramificato.  $\square$



*Osservazione 14.5.11.* Sia  $L$  è un sistema lineare senza punti base su una curva liscia  $X$ ; alcuni autori dicono che:

1. Il sistema lineare  $L$  **separa i punti** se per ogni coppia di punti distinti  $p, q \in X$  vale  $\dim L(-p - q) = \dim L - 2$ .
2. Il sistema lineare  $L$  **separa i vettori tangenti** se per ogni punto  $p \in X$  vale  $\dim L(-2p) = \dim L - 2$ .

A questo punto la domanda sorge spontanea:

*Domanda 14.5.12.* Data una curva liscia proiettiva  $X$  ed un morfismo regolare non costante  $\phi: X \rightarrow \mathbb{P}^n$ , abbiamo un sistema lineare senza punti base  $L = L_\phi(1)$  (Esempio 14.5.9) e di conseguenza abbiamo un morfismo regolare  $\phi_L: X \rightarrow L^\vee$ . Che relazione c'è tra in due morfismi  $\phi$  e  $\phi_L$ ?

**Teorema 14.5.13.** *In risposta alla Domanda 14.5.12, esiste un'unica proiettività  $\eta: L^\vee \rightarrow \mathbb{P}^n$  tale che  $\phi = \eta \circ \phi_L$ .*

*Dimostrazione.* A meno di sostituire  $\mathbb{P}^n$  con il sottospazio proiettivo generato dall'immagine di  $\phi$ , possiamo supporre che  $\phi(X)$  non sia contenuta in alcun iperpiano. Siano  $x_0, \dots, x_n$  coordinate omogenee su  $\mathbb{P}^n$  e sia  $D = \phi^*\{x_0 = 0\}$ . Ne segue che  $L \subset |D|$  e che il morfismo

$$\phi: X_D = (X - \text{Supp}(D)) \rightarrow \mathbb{A}^n = \mathbb{P}^n - \{x_0 = 0\}$$

è regolare ed è quindi data da una  $n$ -upla di funzioni regolari su  $X_D$ , diciamo

$$\phi: X_D \rightarrow \mathbb{A}^n, \quad \phi = (f_1, \dots, f_n)$$

e quindi

$$\phi: X \rightarrow \mathbb{P}^n, \quad \phi = [f_0, f_1, \dots, f_n],$$

dove  $f_0 = 1$  e  $f_0, \dots, f_n$  sono considerate funzioni razionali su  $X$ . Basta adesso ripetere la stessa dimostrazione del punto [1] della Proposizione 14.5.10 per provare che  $\phi$  è la composizione di  $\phi_L$  e del trasposto di

$$\mathbb{P}^n \rightarrow L, \quad [a_0, \dots, a_n] \mapsto \text{div}(a_0 f_0 + \dots + a_n f_n) + D.$$

□

## Esercizi

**14.8.** State viaggiando nel tempo: aiutate il giovane Enriques a dimostrare che una curva liscia proiettiva è razionale se e soltanto se possiede una serie  $g_1^1$ .

**14.9.** Provare che ogni insieme di divisori effettivi possiede estremo inferiore. Se  $L$  è un sistema lineare, l'estremo inferiore  $\text{inf}(L)$  viene detto **parte fissa** di  $L$ . Dimostrare che  $BS(L)$  è uguale a supporto di  $\text{inf}(L)$  e che esiste un sistema lineare  $M$ , detto **parte mobile** di  $L$  tale che  $D \in M$  se e solo se  $D + \text{inf}(L) \in L$ .

**14.10.** Nelle notazioni dell'Esempio 14.5.9, se  $v_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$  indica la  $d$ -esima immersione di Veronese, dimostrare che  $L_\phi(d) = L_{v_d \phi}(1)$  e che la dimensione del sistema lineare  $L_\phi(d)$  è uguale alla dimensione del sottospazio proiettivo generato da  $v_d \phi(X)$ .

## 14.6 Il teorema del resto

Per le curve gobbe non è sempre vero che un divisore linearmente equivalente ad un divisore aggiunto è ancora aggiunto: tuttavia dimostreremo che per divisori di grado sufficientemente alto continua a valere il teorema del resto. Come nel caso delle curve piane, il teorema del resto segue dal Teorema  $Af + B\phi$  che, per varietà proiettive qualsiasi, assume la seguente forma.

**Teorema 14.6.1 (Teorema  $Af + B\phi$ ).** *Sia  $X \subset \mathbb{P}^m$  una varietà proiettiva irriducibile e siano  $H, \Phi \in \mathbb{K}[x_0, \dots, x_m]$  polinomi omogenei tali che  $\deg(H) - \deg(\Phi) = d \geq 0$  e  $\Phi \notin I(X)$ , dove con  $I(X) \subset \mathbb{K}[x_0, \dots, x_m]$  si intende l'ideale omogeneo dei polinomi nulli su  $X$ . Allora esiste un intero  $d_0$ , dipendente solo da  $X$ , tale che se  $d \geq d_0$  e, per ogni  $i = 0, \dots, m$ , la funzione razionale  $\frac{H}{x_i^d \Phi}$  è regolare sulla varietà affine  $X \cap \{x_i \neq 0\}$ , allora esiste un polinomio omogeneo  $B \in \mathbb{K}[x_0, \dots, x_m]$  di grado  $d$  tale che  $H - B\Phi \in I(X)$ .*

*Dimostrazione.* Dire che  $\frac{H}{x_0^d \Phi}$  è regolare su  $X \cap \{x_0 \neq 0\}$  equivale a dire che esiste un polinomio  $b_0(y_1, \dots, y_n)$  tale che

$$H(1, y_1, \dots, y_n) - b_0(y_1, \dots, y_n)\Phi(1, y_1, \dots, y_n)$$

si annulla su  $X \cap \{x_0 \neq 0\}$ . Sostituendo  $y_i$  con  $x_i/x_0$  e moltiplicando per una potenza sufficientemente alta di  $x_0$  si ottiene un polinomio omogeneo  $B_0 \in \mathbb{K}[x_0, \dots, x_m]$  ed un intero positivo  $l$  tali che  $x_0^l H - B_0 \Phi \in I(X)$ . Possiamo ripetere il ragionamento per ogni aperto affine  $X \cap \{x_i \neq 0\}$ , con  $i = 0, \dots, m$ , e quindi il teorema è del tutto equivalente al seguente Teorema 14.6.2.  $\square$

**Teorema 14.6.2.** *Sia  $X \subset \mathbb{P}^m$  una varietà proiettiva irriducibile e denotiamo con  $I(X) \subset \mathbb{K}[x_0, \dots, x_m]$  l'ideale omogeneo dei polinomi nulli su  $X$ . Allora esiste un intero  $d_0 \geq 0$ , dipendente da  $X$ , con la seguente proprietà. Se  $H$  e  $\Phi$  sono due polinomi omogenei tali che  $\deg(H) - \deg(\Phi) \geq d_0$  e se esistono un intero  $s > 0$  e  $m + 1$  polinomi  $B_0, \dots, B_m$  tali che  $x_i^s H - B_i \Phi \in I(X)$  per ogni  $i = 0, \dots, m$ , allora esiste un polinomio omogeneo  $B$  tale che  $H - B\Phi \in I(X)$ .*

Prima di passare alla dimostrazione, osserviamo che l'enunciato di 14.6.2 è indipendente dalla scelta del sistema di coordinate omogeneo. Infatti se  $y_i = \sum a_{ij}x_j$  è un altro sistema, ogni potenza  $y_i^{sm+s}$  appartiene all'ideale generato da  $x_0^s, \dots, x_m^s$ . Per il teorema degli zeri, il Teorema 14.6.2 continua a valere se al posto di  $x_0^s, \dots, x_m^s$  consideriamo  $k$  polinomi omogenei  $F_1, \dots, F_k$  tali che  $V(F_1, \dots, F_k) = \emptyset$ . Sia  $n \leq m$  la dimensione di  $X$  e sia  $\pi: X \rightarrow \mathbb{P}^n$  una proiezione generica. A meno di un cambio di coordinate omogenee possiamo supporre che il centro della proiezione sia il sottospazio  $\{x_{n+1} = \dots = x_m = 0\}$  e quindi che  $x_0, \dots, x_n$  sia un sistema di coordinate omogenee su  $\mathbb{P}^n$ . Dato che il morfismo  $\pi: X \rightarrow \mathbb{P}^n$  è regolare, finito e surgettivo, si ha un morfismo iniettivo di anelli graduati

$$Q := \mathbb{K}[x_0, \dots, x_n] \longrightarrow R := \frac{\mathbb{K}[x_0, \dots, x_m]}{I(X)}.$$

Notiamo che  $Q$  e  $R$  sono domini di integrità e che  $Q$  è anche a fattorizzazione unica.

**Lemma 14.6.3.** *Nelle notazioni precedenti, l'anello  $R$  è finitamente generato come  $Q$ -modulo.*

*Dimostrazione.* La dimostrazione è sostanzialmente equivalente a quella del Lemma 12.2.6 ed è lasciata per esercizio.  $\square$

*Dimostrazione (Dimostrazione del Teorema 14.6.2).* Denotiamo con  $S \subset Q$  la parte moltiplicativa  $S = Q - \{0\}$  e con  $r_1, \dots, r_k \in R$  generatori omogenei di  $R$  come  $Q$ -modulo. Siccome  $R$  è un dominio di integrità si ha  $R \subset S^{-1}R$  e  $r_1, \dots, r_k$  generano  $S^{-1}R$  come  $S^{-1}Q$ -spazio vettoriale; a meno di permutazioni degli indici possiamo supporre che  $r_1, \dots, r_h$ , con  $h \leq k$ , sia una base di  $S^{-1}R$ . Per ogni  $i = h + 1, \dots, k$  si può scrivere  $r_i = \sum_{j=1}^h a_{ij}r_j$  con gli  $a_{ij} \in S^{-1}Q$  univocamente determinati. Siccome  $\mathbb{K}$  è infinito e gli  $a_{ij}$  nono unici, allora essi devono necessariamente essere omogenei, cioè  $a_{ij} = b_{ij}/f_{ij}$  con  $b_{ij}, f_{ij} \in Q$  omogenei e  $\deg(b_{ij}) - \deg(f_{ij}) = \deg(r_i) - \deg(r_j)$ . Denotando con  $f_j = \prod_i f_{ij}$  e con  $m_j = r_j/f_j$  si ha che  $R$  è contenuto nel  $Q$ -sottomodulo di  $M \subset S^{-1}R$  generato da  $m_1, \dots, m_h$ . Inoltre il  $Q$ -modulo  $M$  è libero con base  $m_1, \dots, m_h$ . Riepilogando abbiamo la catena di inclusioni

$$Q \subset R \subset M = \bigoplus_{i=1}^h Qm_i \subset S^{-1}R \subset \mathcal{K},$$

dove  $\mathcal{K}$  è il campo delle frazioni di  $R$ . Gli elementi  $m_i$  sono omogenei, possibilmente di grado negativo, e quindi  $M$  è un  $Q$ -modulo graduato, cioè  $M = \bigoplus_{d \geq u} M_d$ , con  $u \in \mathbb{Z}$ . Consideriamo adesso  $H$  e  $\Phi$  come nell'enunciato di 14.6.2: se  $\Phi \in I(X)$  allora, poiché  $I(X)$  è un ideale primo che non contiene  $\{x_0, \dots, x_m\}$ , si ha che  $H \in I(X)$ . Non è quindi restrittivo supporre  $\Phi \notin I(X)$ ; denotiamo con  $h, \phi \in R$  le loro classi modulo  $I(X)$ . Bisogna dimostrare che se:

1. esiste  $s > 0$  tale che se  $x_i^s \frac{h}{\phi} \in R$  per ogni  $i = 0, \dots, m$ , e
2. il grado di  $\frac{h}{\phi}$  è maggiore od uguale ad un numero  $d_0$  dipendente solo da  $X$ ,

allora  $\frac{h}{\phi} \in R$ . Dimostriamo prima che se vale (1), allora  $\frac{h}{\phi} \in M$ . Infatti, poiché  $x_0^s \frac{h}{\phi} \in R$  e  $x_0 \in S$  si ha  $\frac{h}{\phi} \in S^{-1}R$  e quindi esistono uniche  $h$  frazioni omogenee  $a_1, \dots, a_h \in S^{-1}Q$  tali che

$$\frac{h}{\phi} = \sum_{i=1}^h a_i m_i.$$

Siccome  $x_i^s \frac{h}{\phi} \in R \subset M$  per ogni  $i$  si ha che  $x_i^s a_j \in Q$  per ogni  $i, j$  e poiché  $Q$  è un dominio a fattorizzazione unica segue che  $a_j \in Q$  per ogni  $j$ . Definiamo adesso il numero  $d_0$ : a tal fine consideriamo il  $Q$ -modulo graduato

$$N = \{m \in M \mid \text{esiste } s > 0 \text{ tale che } x_i^s m \in R \text{ per ogni } i = 0, \dots, n\}.$$

L'anello  $Q$  è Noetheriano e quindi  $N$  è finitamente generato, siano  $n_1, \dots, n_l \in N$  generatori omogenei e sia  $s_0$  un intero tale che  $qn_j \in R$  per ogni  $j$  e per ogni polinomio  $q \in Q$  omogeneo di grado  $s_0$ . Allora  $N_d = \sum_i Q_{d-\deg(n_i)} n_i \subset R_d$  per ogni  $d \geq s_0 + \max(\deg(n_1), \dots, \deg(n_s))$  e, siccome  $R_d \subset N_d$  per ogni  $d$ , possiamo definire  $d_0 = s_0 + \max(\deg(n_1), \dots, \deg(n_s))$ .  $\square$

Prima di procedere alle applicazioni, vediamo più in dettaglio il caso delle ipersuperfici.

*Esempio 14.6.4.* Nelle notazioni del Teorema 14.6.2, se  $X$  è una ipersuperficie irriducibile, allora il teorema vale con  $d_0 = 0$ . Sia  $F$  omogeneo e irriducibile tale che  $I(X) = (F)$ . Se  $F$  divide  $\Phi$  il risultato è praticamente banale. Possiamo quindi assumere che  $F$  non divide  $\Phi$ . Vediamo prima il caso in cui  $\Phi$  ha grado 1. Fissiamo le coordinate omogenee in modo tale che  $\Phi = x_0$  e scriviamo  $F = x_0 F_0 + F_1$ , con  $F_1 \in \mathbb{K}[x_1, \dots, x_m]$ . Siccome  $\Phi$  non ha fattori in comune con  $F$ , si ha  $F_1 \neq 0$ : scriviamo  $H = x_0 H_0 + H_1$ , con  $H_1 \in \mathbb{K}[x_1, \dots, x_m]$ . Sia  $Q \in \mathbb{K}[x_1, \dots, x_m]$  omogeneo di grado sufficientemente alto e senza

fattori in comune con  $F_1$ , per ipotesi vale  $QH \in (F, x_0)$  e quindi, specializzando a  $x_0 = 0$  si ricava  $QH_1 \in (F_1)$ . Per come abbiamo scelto  $Q$  si ha  $H_1 \in (F_1)$  e quindi  $H_1 = AF_1$ ,  $H = x_0H_0 + A(F - x_0F_0) = AF + (H_0 - F_0)\Phi$ .

Mostriamo adesso che se il teorema vale con  $d_0 = d > 0$ , allora vale anche con  $d_0 = d - 1$ . Prendiamo  $H, \Phi$  omogenei con  $\deg H = \deg(\Phi) + d - 1$  e tali che  $x_i^l H - B_i \Phi = A_i F$  per ogni  $i$ . Sia  $L$  un generico polinomio di grado 1, allora vale  $x_i^l HL - B_i L \Phi = A_i LF$  ed il teorema implica che  $HL = \tilde{A}F + \tilde{B}\Phi$ . D'altra parte  $x_i^l LH - LB_i \Phi, x_i^l LH - x_i^l \tilde{B}\Phi \in (F)$ , quindi anche  $(LB_i - x_i^l \tilde{B})\Phi \in (F)$  e  $(LB_i - x_i^l \tilde{B}) \in (F)$ . Siccome  $L$  ha grado 1, per il caso particolare visto sopra esiste  $C$  tale che  $\tilde{B} - CL \in (F)$  e quindi  $L(H - C\Phi) \equiv HL - \tilde{B}\Phi \equiv 0 \pmod{F}$ . Non ci sono fattori comuni in  $L$  e  $F$  e quindi  $H - C\Phi \in (F)$ .

Come nel caso delle curve piane, possiamo introdurre la nozione di divisore aggiunto su una curva liscia proiettiva  $X \subset \mathbb{P}^n$ . Sia  $H \subset \mathbb{P}^n$  una ipersuperficie definita da un polinomio  $F$  omogeneo di grado  $d$ . Se  $X$  non è contenuta in  $H$ , scegliamo un polinomio  $G$ , omogeneo di grado  $d$ , tale che  $X \cap H \cap V(G) = \emptyset$  e definiamo il divisore  $H|_X$  come il divisore degli zeri della funzione razionale  $F/G \in \mathbb{K}(X)$ . Se  $E$  è un altro polinomio omogeneo di grado  $d$  tale che  $X \cap H \cap V(E) = \emptyset$ , allora la funzione razionale  $E/G$  è invertibile in ogni punto di  $X \cap H$  e quindi le funzioni  $F/G$  e  $F/E$  hanno lo stesso divisore degli zeri: questo prova che il **divisore aggiunto**  $H|_X$  è ben definito. In particolare possiamo scegliere come  $G$  la potenza  $d$ -esima di un iperpiano generico: quindi il divisore dei poli di  $F/G$  ha grado uguale a  $d \deg(X)$  e, per il Corollario 14.4.3, anche il grado di  $H|_X$  è uguale al prodotto  $\deg(X) \deg(H)$ .

**Teorema 14.6.5.** *Sia  $X \subset \mathbb{P}^n$  una curva liscia proiettiva e, per ogni  $d \geq 1$ , denotiamo con  $L_X(d) \subset \text{Div}(X)$  l'insieme dei divisori aggiunti del tipo  $H|_X$ , con  $H$  ipersuperficie di grado  $d$  non contenente  $X$ . Allora:*

1.  $L_X(d)$  è un sistema lineare.
2. (Teorema del resto) *Esiste  $d_0 \in \mathbb{N}$  tale che il sistema lineare  $L_X(d)$  è completo per ogni  $d \geq d_0$ .*

*Dimostrazione.* [1] Sia  $L$  un iperpiano generico in  $\mathbb{P}^n$ , dobbiamo dimostrare che  $L_X(d)$  è un sottospazio proiettivo del sistema lineare completo  $|dL|_X$ . Fissiamo un sistema di coordinate omogenee  $x_0, \dots, x_n$  tali che  $L = \{x_0 = 0\}$ , allora l'insieme delle funzioni razionali

$$\left\{ \frac{F}{x_0^d} \mid F \in \mathbb{K}[x_0, \dots, x_n] \text{ omogeneo di grado } d \right\} \subset \mathbb{K}(X)$$

è un sottospazio vettoriale di  $H^0(X, dL|_X)$  e ogni divisore in  $L_X(d)$  è del tipo  $F|_X = \text{div}(F/x_0^d) + dL|_X$ .

[2] Prendiamo come  $d_0$  lo stesso che compare nell'enunciato del Teorema 14.6.1 e dimostriamo che  $L_X(d)$  è completo per ogni  $d \geq d_0$ . Non è restrittivo supporre che  $X$  non sia contenuto in alcun iperpiano; per ogni  $i = 0, \dots, n$  denotiamo con  $L_i \in L_X(1) \subset \text{Div}(X)$  il divisore della sezione iperiana di equazione  $x_i = 0$ . Siano  $d \geq d_0$  e  $D$  un divisore effettivo su  $X$  linearmente equivalente a  $dL_0$ ; dobbiamo dimostrare che  $D \in L_X(d)$ . Per definizione di equivalenza lineare, esiste una funzione razionale  $f_0 \in \mathbb{K}(X)$  tale che  $D - dL_0 = \text{div}(f_0)$ ; denotando  $f_i = f_0 x_0^d / x_i^d$  si ha  $D - dL_i = \text{div}(f_i)$  per ogni  $i$ . Siano  $H, \Phi$  due polinomi omogenei tali che  $\deg(H) - \deg(\Phi) = d$  e tali che su  $X$  valga  $f_i x_i^d \Phi = H$  per ogni  $i$ . Sull'aperto affine  $X_i = X \cap \{x_i = 1\}$  la funzione razionale  $f_i$  è regolare e quindi, per il Teorema 14.6.1, esiste un polinomio omogeneo  $B$  di grado  $d$  tale che  $H - B\Phi \in I(X)$  e quindi tale che  $B|_X = H|_X - \Phi|_X = D$ .  $\square$

**Esercizi**

**14.11.** Sia  $X \subset \mathbb{P}^n$  una curva liscia proiettiva. Dimostrare che per ogni  $d > 0$  vale  $L_X(d) = L_{v_d}(1)$  (vedi Esempio 14.5.9), dove  $v_d$  è la restrizione ad  $X$  della  $d$ -esima immersione di Veronese  $v_d: \mathbb{P}^n \rightarrow \mathbb{P}^N$ .

**14.7 Esercizi complementari**

**14.12.** Sia  $A$  un anello di valutazione discreta e denotiamo con  $K$  il campo delle frazioni su  $A$ . Dimostrare che la valutazione  $\nu: A \rightarrow \mathbb{N} \cup \{+\infty\}$  si estende in modo unico ad un'applicazione  $\nu: K \rightarrow \mathbb{Z} \cup \{+\infty\}$  tale che:

1. Vale  $\nu(a) = +\infty$  se e solo se  $a = 0$ .
2. Per ogni  $a, b \in K$  vale  $\nu(a + b) \geq \min(\nu(a), \nu(b))$ .
3. Per ogni  $a, b \in K$  vale  $\nu(ab) = \nu(a) + \nu(b)$ .

Dimostrare viceversa che se  $K$  è un campo e  $\nu: K \rightarrow \mathbb{Z} \cup \{+\infty\}$  è un'applicazione che soddisfa le precedenti tre condizioni, allora il subanello  $A = \{a \in K \mid \nu(a) \geq 0\}$  è un dominio di valutazione discreta con ideale massimale  $\mathfrak{m} = \{a \in K \mid \nu(a) > 0\}$  e campo delle frazioni  $K$ .

**Definizione 14.7.1.** Chiameremo **valutazione discreta** su di un campo  $K$  una qualsiasi applicazione  $\nu: K \rightarrow \mathbb{Z} \cup \{+\infty\}$  che soddisfa le tre condizioni dell'Esercizio 14.12. La valutazione nulla è quella che vale 0 su  $K - \{0\}$ . Denotiamo con  $C_K$  l'insieme delle valutazioni discrete surgettive su  $K$ .

Notiamo che per ogni valutazione discreta  $\nu$ , l'applicazione  $\nu: K - \{0\} \rightarrow \mathbb{Z}$  è un omomorfismo di gruppi. In particolare una valutazione discreta è surgettiva se e solo se la sua immagine contiene 1.

**14.13.** Sia  $\nu$  una valutazione discreta non nulla su un campo  $K$ . Dimostrare che:

1.  $\nu(1) = \nu(-1) = 0$ .
2. Se  $\nu(a) < \nu(b)$ , allora vale  $\nu(a \pm b) = \nu(a)$ .
3. Esiste un intero positivo  $m$  ed una valutazione discreta surgettiva  $\eta$  tali che  $\nu = m\eta$ .
4. Se  $F \subset K$  è un sottocampo algebricamente chiuso, allora  $\nu(a) = 0$  per ogni  $a \in F - \{0\}$ .

**14.14.** Provare che se  $x$  è un punto liscio di una curva irriducibile  $X$  allora l'applicazione

$$\nu: \mathbb{K}(X) \rightarrow \mathbb{Z} \cup \{+\infty\}, \quad \nu(f) = \text{ord}_x(f)$$

è una valutazione discreta surgettiva.

Quindi, per l'Esercizio 14.14 per ogni curva liscia  $X$  è definita un'applicazione iniettiva

$$\text{ord}: X \rightarrow C_{\mathbb{K}(X)}, \quad x \mapsto \text{ord}_x.$$

I prossimi esercizi mostreranno che se  $X$  è proiettiva, allora  $\text{ord}$  è bigettiva.

**14.15.** Sia  $X$  una curva irriducibile e  $\nu: \mathbb{K}(X) \rightarrow \mathbb{Z} \cup \{+\infty\}$  una valutazione discreta surgettiva. Scegliamo  $\xi \in \mathbb{K}(X)$  tale che  $\nu(\xi) = 1$ . Dimostrare:

1. Se  $f \in \mathbb{K}(X)$  è costante e non nulla, allora  $\nu(f) = 0$ .
2. Se  $f \in \mathbb{K}(X)$  non è costante, allora esiste  $g \in \mathbb{K}(f) \subset \mathbb{K}(X)$  tale che  $\nu(g) \neq 0$ . (Sugg.: la funzione  $\xi$  è algebrica sul campo  $\mathbb{K}(f)$ .)

3. Se  $f \in \mathbb{K}(X)$  non è costante e  $\nu(f) \geq 0$ , allora esiste un unico  $a \in \mathbb{K}$  tale che  $\nu(f - a) > 0$ .
4. Se  $f \in \mathbb{K}(X)$  non è costante e  $\nu(f) \geq 0$ , allora per ogni  $n$  esiste un unico polinomio  $p(t)$  di grado  $< n$  tale che  $\nu(f - p(\xi)) \geq n$ .

**14.16 (\*).** Sia  $X \subset \mathbb{P}^n$  una curva liscia proiettiva e  $\nu: \mathbb{K}(X) \rightarrow \mathbb{Z} \cup \{+\infty\}$  una valutazione discreta surgettiva. Dimostrare che esiste un unico punto  $p \in X$  tale che  $\nu = \text{ord}_p$ . (Sugg.: usare l'Esercizio 14.15 per provare che esiste un sistema di coordinate omogenee  $x_0, \dots, x_n$  tale che  $\nu(x_i/x_0) > 0$  per ogni  $i = 1, \dots, n$ . Mostrare poi che  $p = [1, 0, \dots, 0] \in X$  e che se  $f \in \mathcal{O}_{p,X}$ , allora  $\nu(f) > 0$  se e solo se  $f \in \mathfrak{m}_p$ .)

**14.17.** Determinare tutte le valutazioni discrete sul campo  $\mathbb{Q}$ . (Sugg.: vedi Esempio 7.1.3 ed Esercizio 7.26.)

**14.18.** Sia  $A$  un anello di valutazione discreta con parametro locale  $t$  e campo residuo  $\mathbb{K} = A/(t)$ . Per ogni  $A$ -modulo  $M$  se ne definisce la lunghezza come

$$l(M) = \sum_{i=0}^{+\infty} \dim_{\mathbb{K}} \frac{t^i M}{t^{i+1} M}.$$

Provare che, con tale definizione, il Teorema 8.1.6 continua a valere.

**14.19.** Siano  $X$  una curva liscia affine e  $p \in X$  un suo punto. Dimostrare che esiste una funzione razionale  $f \in \mathbb{K}(X)$  tale che  $\text{ord}_p(f) = -1$  e  $\text{ord}_q(f) \geq 0$  per ogni  $q \neq p$ .

**14.20.** Sia  $\phi: X \rightarrow Y$  un morfismo finito di curve lisce. Dimostrare che per ogni  $y \in Y$  esiste un aperto affine  $V \subset Y$  tale che  $y \in V$  e  $\mathbb{K}[\phi^{-1}(V)]$  è un  $\mathbb{K}[V]$ -modulo libero di rango  $\deg(\phi)$ . (Sugg.: guardare alla dimostrazione del Teorema 14.3.3.)

**14.21.** Sia  $X \subset \mathbb{P}^n$  una curva liscia di grado  $n$  non contenuta in alcun iperpiano. Dimostrare che:

1.  $X$  è isomorfa a  $\mathbb{P}^1$ . (Sugg.: Considerare il sistema lineare tagliato dal fascio di iperpiani passanti per  $n - 1$  punti generici di  $X$ .)
2. In un opportuno sistema di coordinate omogenee,  $X$  è l'immagine della  $n$ -esima immersione di Veronese  $v_n: \mathbb{P}^1 \rightarrow \mathbb{P}^n$ .

**14.22.** Sia  $X \subset \mathbb{P}^n$  una curva liscia non degenera, ossia non contenuta in alcun iperpiano. Dimostrare che il sistema lineare  $L_X(1)$  non è completo se e solo se  $X$  è la proiezione di una curva non degenera in  $\mathbb{P}^{n+1}$ .

**14.23.** Sia  $L$  un sistema lineare di dimensione  $\geq 1$  di divisori di grado  $d$  su una curva liscia proiettiva  $X$  e sia  $U \subset X$  un aperto non vuoto che non contiene punti base di  $L$ . Dimostrare che, se  $h$  è il massimo grado della restrizione di un divisore di  $L$  ad  $U$ , allora la parte fissa di  $L$  ha grado  $d - h$ .

## Differenziali

### 15.1 (Alcune) Costruzioni universali in algebra e geometria

La nozione di oggetto universale è una delle più importanti della matematica astratta. In questa sezione non vogliamo dare una definizione estensiva di universalità, che richiede il linguaggio delle categorie, ma solo presentare le proprietà “universali” di alcune costruzioni algebro-geometriche viste nei capitoli precedenti e di altre che saranno qui introdotte. Ad esempio, se  $A$  è un anello commutativo con unità e  $S$  è un insieme, lo  $A$ -modulo

$$F_S = \bigoplus_{s \in S} As$$

è detto  $A$ -modulo libero generato da  $S$ . Gli elementi di  $F_S$  sono le combinazioni lineari finite di elementi  $s \in S$ , pensati come simboli formali, a coefficienti in  $A$ . Considerando  $S$  come un sottoinsieme di  $F_S$  tramite l'inclusione  $s \mapsto 1s$ , vale la seguente proprietà universale. *Per ogni  $A$ -modulo  $M$  e per ogni applicazione di insiemi  $u: S \rightarrow M$  esiste un unico omomorfismo di  $A$ -moduli  $\phi: F_S \rightarrow M$  tale che  $\phi(s) = u(s)$  per ogni  $s \in S$ .* Infatti la legge  $\phi(\sum a_i s_i) = \sum a_i u(s_i) \in M$  definisce l'unico omomorfismo di  $A$ -moduli che estende  $u$ . Notiamo che l'immagine di  $\phi$  è uguale al sottomodulo di  $M$  generato da  $u(S)$ .

A volte la proprietà universale viene utilizzata per definire un oggetto matematico; è tipico il caso del prodotto tensoriale. Sia  $A$  un anello commutativo con unità e siano  $M, N, P$  tre  $A$ -moduli. Un'applicazione  $u: M \times N \rightarrow P$  si dice  $A$ -bilineare se per ogni  $m, m' \in M$ ,  $n, n' \in N$  ed  $a, b \in A$  vale:

- $u(am + bm', n) = au(m, n) + bu(m', n)$
- $u(m, an + bn') = au(m, n) + bu(m, n')$

In modo analogo si definisce, per ogni  $(n+1)$ -upla di  $A$ -moduli  $M_1, \dots, M_n, P$ , la nozione di applicazione  $A$ -multilineare  $u: M_1 \times \dots \times M_n \rightarrow P$ . L'insieme delle applicazioni  $A$ -multilineari  $M_1 \times \dots \times M_n \rightarrow P$  ha una ovvia struttura di  $A$ -modulo e verrà indicato con  $\text{Hom}_A(M_1 \otimes_A M_2 \otimes_A \dots \otimes_A M_n, P)$  (più avanti daremo vita ad un  $A$ -modulo  $M_1 \otimes_A \dots \otimes_A M_n$  in modo tale che il precedente Hom sia un “Hom reale” e non solamente una notazione grafica).

Supponiamo adesso che  $M_1 = M_2 = \dots = M_n = M$ . Un'applicazione  $A$ -multilineare  $u: M \times \dots \times M \rightarrow P$  si dice:

- **Simmetrica:** se per ogni permutazione  $\sigma \in \Sigma_n$  vale

$$u(m_{\sigma(1)}, \dots, m_{\sigma(n)}) = u(m_1, \dots, m_n).$$

- **Antisimmetrica:** se per ogni permutazione  $\sigma \in \Sigma_n$  vale

$$u(m_{\sigma(1)}, \dots, m_{\sigma(n)}) = (-1)^\sigma u(m_1, \dots, m_n),$$

dove  $(-1)^\sigma$  indica la segnatura di  $\sigma$ .

- **Alternante:** se  $u(m_1, \dots, m_n) = 0$  ogniqualvolta  $m_i = m_j$  per qualche coppia di indici  $1 \leq i < j \leq n$ .

Siano  $M_1, \dots, M_n$   $A$ -moduli fissati e denotiamo con  $F = F_{M_1 \times \dots \times M_n}$  lo  $A$ -modulo libero generato dal prodotto cartesiano  $M_1 \times \dots \times M_n$ . Denotiamo con  $\mathcal{A}$  la famiglia degli  $A$ -sottomoduli  $H \subset F$  tali che la mappa  $M_1 \times \dots \times M_n \rightarrow F/H$ , composizione dell'inclusione naturale  $M_1 \times \dots \times M_n \subset F$  e della proiezione al quoziente  $F \rightarrow F/H$ , è  $A$ -multilineare. Chiaramente  $\mathcal{A}$  non è vuota poiché contiene  $F$ . Poniamo

$$R = \bigcap_{H \in \mathcal{A}} H, \quad M_1 \otimes_A M_2 \otimes_A \dots \otimes_A M_n = F/R$$

e denotiamo  $u(m_1, m_2, \dots, m_n) = m_1 \otimes \dots \otimes m_n$ , dove

$$u: M_1 \times \dots \times M_n \rightarrow M_1 \otimes_A \dots \otimes_A M_n$$

è la composizione dell'inclusione  $M_1 \times \dots \times M_n \subset F$  e della proiezione al quoziente.

**Definizione 15.1.1.** Lo  $A$ -modulo  $M_1 \otimes_A \dots \otimes_A M_n$  viene detto **prodotto tensoriale su  $A$  di  $M_1, \dots, M_n$** .

Se  $M_1 = M_2 = \dots = M_n = M$  si scrive talvolta  $\bigotimes_A^n M$  in luogo di  $M_1 \otimes_A \dots \otimes_A M_n$ .

**Proposizione 15.1.2.** Nelle notazioni precedenti, l'applicazione  $u$  è  $A$ -multilineare e, per ogni applicazione  $A$ -multilineare  $\phi: M_1 \times \dots \times M_n \rightarrow P$  esiste un unico omomorfismo di  $A$ -moduli  $\psi: M_1 \otimes_A \dots \otimes_A M_n \rightarrow P$  tale che  $\phi = \psi u$ .

*Dimostrazione.* Siano  $m_i \in M_i, i = 2, \dots, n$ , elementi fissati e proviamo che l'applicazione  $u(-, m_2, \dots, m_n): M_1 \rightarrow F/R$  è  $A$ -lineare: questo equivale, per simmetria, a dimostrare la multilinearità di  $u$ . Dati  $m, m' \in M_1, a, b \in A$ , l'elemento di  $F$

$$(am + bm', m_2, \dots, m_n) - a(m, m_2, \dots, m_n) - b(m', m_2, \dots, m_n)$$

appartiene ad ogni sottospazio della famiglia  $\mathcal{A}$  e quindi appartiene anche ad  $R$ . Ne segue che

$$(am + bm') \otimes m_2 \otimes \dots \otimes m_n = a(m \otimes m_2 \otimes \dots \otimes m_n) + b(m' \otimes m_2 \otimes \dots \otimes m_n).$$

Ogni applicazione insiemistica  $\phi: M_1 \times \dots \times M_n \rightarrow P$  induce un unico omomorfismo di  $A$ -moduli  $\psi: F \rightarrow P$  e  $\text{Ker}(\psi) \in \mathcal{A}$  se e solo se  $\phi$  è  $A$ -multilineare. In particolare se  $\phi$  è  $A$ -multilineare allora  $\psi$  si fattorizza ad una applicazione  $\psi: F/R \rightarrow P$ ; siccome  $F/R$  è generato dall'immagine di  $u$ ,  $\psi$  è necessariamente unica.  $\square$

*Esempio 15.1.3.* Il prodotto tensoriale di moduli liberi è ancora libero, più precisamente se  $S$  e  $T$  sono insiemi allora l'applicazione

$$F_{S \times T} \rightarrow F_S \otimes_A F_T, \quad (s, t) \mapsto s \otimes t$$

si estende ad un isomorfismo di  $A$ -moduli.



Il rigore matematico imporrebbe adesso alcune pedanti e noiose verifiche come la seguente: *per ogni terna  $M, N, P$  di  $A$ -moduli esiste un isomorfismo canonico  $(M \otimes_A N) \otimes_A P \rightarrow M \otimes_A N \otimes_A P$ . Infatti, per ogni  $p \in P$  fissato, il morfismo*

$$M \times N \rightarrow M \otimes_A N \otimes_A P, \quad (m, n) \mapsto m \otimes n \otimes p$$

è bilineare e quindi induce, al variare di  $p$ , un morfismo

$$(M \otimes_A N) \times P \rightarrow M \otimes_A N \otimes_A P, \quad (m \otimes n, p) \mapsto m \otimes n \otimes p$$

che, essendo ancora bilineare induce un morfismo di  $A$ -moduli

$$(M \otimes_A N) \otimes_A P \rightarrow M \otimes_A N \otimes_A P, \quad (m \otimes n) \otimes p \mapsto m \otimes n \otimes p.$$

Viceversa l'applicazione

$$M \times N \times P \rightarrow (M \otimes_A N) \otimes_A P, \quad (m, n, p) \mapsto (m \otimes n) \otimes p$$

è multilineare e quindi induce un morfismo di  $A$ -moduli

$$M \otimes_A N \otimes_A P \rightarrow (M \otimes_A N) \otimes_A P, \quad m \otimes n \otimes p \mapsto (m \otimes n) \otimes p.$$

Il volenteroso lettore può dimostrare, in modo del tutto simile che esistono isomorfismi  $M \otimes_A N \otimes_A P \cong M \otimes_A (N \otimes_A P)$ ,  $N \otimes_A M \cong M \otimes_A N$  eccetera.

La costruzione del prodotto tensoriale si presta a molte varianti: ad esempio, se  $M_1 = M_2 = \dots = M_n = M$  ed  $F$  denota lo  $A$ -modulo libero generato dal prodotto cartesiano  $\prod_{i=1}^n M$ , allora possiamo considerare le famiglie  $\mathcal{B}$  e  $\mathcal{C}$  di sottomoduli di  $F$  definite nel modo seguente. Un sottomodulo  $H \subset F$  appartiene alla famiglia:

- $\mathcal{B}$  se l'applicazione  $\prod_{i=1}^n M \rightarrow F/H$  è  $A$ -multilineare simmetrica.
- $\mathcal{C}$  se l'applicazione  $\prod_{i=1}^n M \rightarrow F/H$  è  $A$ -multilineare alternante.

Denotiamo poi

$$R_1 = \bigcap_{H \in \mathcal{B}} H, \quad \bigodot_A^n M = F/R_1.$$

$$R_2 = \bigcap_{H \in \mathcal{C}} H, \quad \bigwedge_A^n M = F/R_2.$$

Lo  $A$ -modulo  $\bigodot_A^n M$  (in alcuni testi denotato con  $Sym_A^n(M)$  oppure con  $S_A^n(M)$ ) viene detto  **$n$ -esima potenza simmetrica su  $A$**  di  $M$ , mentre  $\bigwedge_A^n M$  si chiama  **$n$ -esima potenza esterna su  $A$**  di  $M$ .

Si pone per convenzione  $\bigotimes_A^0 M = \bigodot_A^0 M = \bigwedge_A^0 M = A$ ; si noti che esistono epimorfismi naturali di  $A$ -moduli  $\bigotimes_A^n M \rightarrow \bigodot_A^n M$ ,  $\bigotimes_A^n M \rightarrow \bigwedge_A^n M$ . In linea di principio si possono fare anche le potenze antisimmetriche di  $A$ -moduli che però sono scarsamente usate in matematica ed alle quali si preferiscono quasi sempre le potenze esterne. Lasciamo per esercizio al lettore enunciare e dimostrare i risultati analoghi alla Proposizione 15.1.2 per i prodotti esterni e simmetrici.

Le proprietà universali permettono di dimostrare facilmente l'esistenza di isomorfismi canonici; per fare questo serve il seguente lemma.

**Lemma 15.1.4.** *Un omomorfismo di  $A$ -moduli  $\phi: M \rightarrow N$  è un isomorfismo se e solo se per ogni  $A$ -modulo  $P$ , il morfismo di composizione  $\circ\phi: \text{Hom}_A(N, P) \rightarrow \text{Hom}_A(M, P)$  è bigettivo.*

*Dimostrazione.* Una implicazione è ovvia. Viceversa supponiamo che  $\circ\phi$  sia bigettiva per ogni  $A$ -modulo  $P$ . Scegliendo  $P = M$  possiamo trovare  $s: N \rightarrow M$  tale che  $s \circ \phi = Id_M$  e questo prova che  $\phi$  è iniettiva. Scegliendo invece  $P = N/\phi(M)$  allora, detta  $p: N \rightarrow P$  la proiezione al quoziente, si ha  $p \circ \phi = 0$  e, essendo  $\circ\phi$  iniettiva ne segue che  $p = 0$  e quindi che  $\phi(M) = N$ .  $\square$

Il Lemma 15.1.4 è un caso particolare di un risultato più generale la cui dimostrazione viene tradizionalmente lasciata per esercizio al lettore (Esercizio 15.6).

Se  $A \rightarrow B$  è un morfismo di anelli commutativi con unità e  $M$  è un  $A$ -modulo, il prodotto tensoriale  $M \otimes_A B$  possiede una struttura naturale di  $B$ -modulo, il cui prodotto per scalare è ottenuto estendendo per bilinearità la formula  $b(m \otimes b') = m \otimes bb'$ ,  $m \in M$ ,  $b, b' \in B$ . Tale struttura è detta di **estensione degli scalari**. Se  $N$  è un  $B$ -modulo, lasciamo per esercizio al lettore la dimostrazione della formula del **cambio di base**

$$\text{Hom}_A(M, N) = \text{Hom}_B(M \otimes_A B, N).$$

La proprietà universale del prodotto viene spesso usata in luogo della sua costruzione esplicita per la dimostrazione dell'esistenza di isomorfismi naturali; un esempio è dato dal seguente lemma.

**Lemma 15.1.5.** *Sia  $M$  un  $A$ -modulo,  $I \subset A$  un ideale e  $S \subset A$  una parte moltiplicativa. Allora esistono isomorfismi canonici*

$$M \otimes_A \frac{A}{I} = \frac{M}{IM}, \quad M \otimes_A S^{-1}A = S^{-1}M.$$

*In particolare, considerando  $S = \{1\}$  oppure  $I = 0$ , vale  $M \otimes_A A = M$ .*

*Dimostrazione.* Dimostriamo solamente la seconda uguaglianza  $M \otimes_A S^{-1}A = S^{-1}M$ : la dimostrazione della prima è sostanzialmente analoga ed è lasciata per esercizio. Esiste una ovvia applicazione  $A$ -bilinare

$$M \times_A S^{-1}A \rightarrow S^{-1}M, \quad \left(m, \frac{a}{s}\right) \mapsto \frac{am}{s}$$

che, per la proprietà universale, induce un omomorfismo di  $A$ -moduli

$$\phi: M \otimes_A S^{-1}A \rightarrow S^{-1}M, \quad \phi\left(m \otimes \frac{a}{s}\right) = \frac{am}{s}.$$

Notiamo che, considerando sia  $M \otimes_A S^{-1}A$  che  $S^{-1}M$  come  $S^{-1}A$ -moduli, il morfismo  $\phi$  è un morfismo  $S^{-1}A$ -lineare. La surgettività di  $\phi$  è evidente; sia quindi  $x = \sum_i m_i \otimes \frac{a_i}{s_i} \in \text{Ker}(\phi)$ . Se indichiamo con  $s \in S$  il prodotto degli  $s_i$  possiamo scrivere

$$x = \sum_i m_i \otimes \frac{b_i}{s} = m \otimes \frac{1}{s}, \quad b_i = \frac{a_i s}{s_i}, \quad m = \sum b_i m_i.$$

Quindi  $m/s = \phi(x) = 0$  in  $S^{-1}M$  ed esiste  $t \in S$  tale che  $tm = 0$ ; ne segue che  $x = m \otimes (1/s) = m \otimes (t/ts) = tm \otimes (1/ts) = 0$ .  $\square$

Consideriamo adesso due morfismi di anelli  $A \rightarrow B$ ,  $A \rightarrow C$ ; possiamo considerare  $B$  e  $C$  come  $A$ -moduli e farne il prodotto tensoriale  $B \otimes_A C$ . In aggiunta esiste su  $B \otimes_A C$  un prodotto dato dalla formula

$$\left(\sum_i b_i \otimes c_i\right) \left(\sum_j b_j \otimes c_j\right) = \sum_{i,j} b_i b_j \otimes c_i c_j.$$

Tale prodotto è l'unico che induce una struttura di anello sul prodotto tensoriale tale che

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \beta \\ C & \xrightarrow{\gamma} & B \otimes_A C \end{array}, \quad \beta(b) = b \otimes 1, \quad \gamma(c) = 1 \otimes c$$

è un diagramma commutativo di omomorfismi di anelli. La proprietà universale è in questo caso espressa nella seguente proposizione.

**Proposizione 15.1.6.** *Per ogni diagramma commutativo di omomorfismi di anelli commutativi con unità*

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow f \\ C & \xrightarrow{g} & D \end{array}$$

esiste un unico omomorfismo di anelli  $\phi: B \otimes_A C \rightarrow D$  tale che, nelle notazioni precedenti,  $f = \phi\beta$  e  $g = \phi\gamma$ .

*Dimostrazione.* Le condizioni  $f = \phi\beta$  e  $g = \phi\gamma$  equivalgono a dire che, per ogni  $b \in B$ ,  $c \in C$ , vale  $\phi(b \otimes 1) = f(b)$ ,  $\phi(1 \otimes c) = g(c)$ ; dato che gli elementi  $1 \otimes c$  e  $b \otimes 1$  generano  $B \otimes_A C$  come anello, l'omomorfismo  $\phi$  è necessariamente unico. La proprietà universale del prodotto tensoriale, applicata al morfismo  $A$ -bilineare  $B \times C \rightarrow D$ ,  $(b, c) \mapsto f(b)g(c)$ , fornisce un omomorfismo di  $A$ -moduli  $\phi: B \otimes_A C \rightarrow D$  tale che  $\phi(b \otimes c) = f(b)g(c)$  ed una semplice verifica mostra che  $\phi$  è un omomorfismo di anelli.  $\square$

*Esempio 15.1.7.* Per ogni anello commutativo con unità  $A$  esiste un isomorfismo naturale di  $A$ -algebre

$$A[x_1, \dots, x_n] \otimes_A A[y_1, \dots, y_n] = A[x_1, \dots, x_n, y_1, \dots, y_n].$$

Infatti il morfismo  $f(x) \otimes g(y) \mapsto f(x)g(y)$  è un omomorfismo di  $A$ -algebre e, per l'Esempio 15.1.3, è un isomorfismo di  $A$ -moduli liberi.

**Proposizione 15.1.8.** *Se  $X, Y$  sono varietà affini su  $\mathbb{K} = \overline{\mathbb{K}}$ , allora esiste un isomorfismo naturale  $\mathbb{K}[X \times Y] = \mathbb{K}[X] \otimes_{\mathbb{K}} \mathbb{K}[Y]$ .*

*Dimostrazione.* Le proiezioni sui due fattori inducono due omomorfismi di algebre di funzioni regolari  $\mathbb{K}[X] \rightarrow \mathbb{K}[X \times Y]$ ,  $\mathbb{K}[Y] \rightarrow \mathbb{K}[X \times Y]$ , che inducono un omomorfismo  $\mathbb{K}[X] \otimes_{\mathbb{K}} \mathbb{K}[Y] \rightarrow \mathbb{K}[X \times Y]$ . Se  $X \subset \mathbb{A}^n$  ha come ideale  $I = I(X) \subset \mathbb{K}[x_1, \dots, x_n]$  e  $Y \subset \mathbb{A}^m$  ha come ideale  $J = I(Y) \subset \mathbb{K}[y_1, \dots, y_m]$ , allora esiste un diagramma commutativo con le frecce verticali surgettive

$$\begin{array}{ccc} \mathbb{K}[x_1, \dots, x_n] \otimes_{\mathbb{K}} \mathbb{K}[y_1, \dots, y_m] & \xrightarrow{\phi} & \mathbb{K}[x_1, \dots, x_n, y_1, \dots, y_m] \\ \downarrow \alpha & & \downarrow \beta \\ \mathbb{K}[X] \otimes_{\mathbb{K}} \mathbb{K}[Y] & \xrightarrow{\psi} & \mathbb{K}[X \times Y] \end{array}$$

e quindi  $\phi(\text{Ker}(\alpha)) \subset \text{Ker}(\beta)$ . Per il Lemma 10.5.1, l'ideale di  $X \times Y$  è generato dall'ideale di  $X$  e dall'ideale di  $Y$  e quindi, a maggior ragione dal nucleo di  $\alpha$ . Di conseguenza  $\phi(\text{Ker}(\alpha)) = \text{Ker}(\beta)$  ed anche  $\psi$  è un isomorfismo.  $\square$

**Esercizi**

**15.1.** Provare che per ogni intero  $1 \leq i < n$ , esiste un isomorfismo naturale di  $A$ -moduli  $\text{Hom}_A(M_1 \otimes_A \cdots \otimes_A M_n, P) = \text{Hom}_A(M_1 \otimes_A \cdots \otimes_A M_i, \text{Hom}_A(M_{i+1} \otimes_A \cdots \otimes_A M_n, P))$ .

**15.2.** Sia  $u: M \times \cdots \times M \rightarrow P$  un'applicazione  $A$ -multilineare tale che  $u(m_1, \dots, m_n) = 0$  ogniqualvolta  $m_i = m_{i+1}$  per qualche indice  $1 \leq i < n$ . Provare che  $u$  è antisimmetrica ed alternante.

**15.3.** Sia  $A$  un anello fissato. Provare che:

1. Se  $2 = 1 + 1$  è invertibile in  $A$ , allora ogni applicazione  $A$ -multilineare antisimmetrica è anche alternante.
2. Se  $2 = 1 + 1$  non è invertibile in  $A$ , allora esistono applicazioni  $A$ -bilineari antisimmetriche che non sono alternanti.

**15.4.** Dimostrare che se  $M$  e  $N$  sono  $A$ -moduli finitamente generati, allora anche  $M \otimes_A N$  è finitamente generato.

**15.5.** Nelle notazioni della Proposizione 15.1.2, e per  $n = 2$ , trovare un insieme di generatori del sottomodulo  $R$ .

**15.6.** Provare che una successione  $L \rightarrow M \rightarrow N \rightarrow 0$  di omomorfismi di  $A$ -moduli è esatta se e solo se per ogni  $A$ -modulo  $P$  la successione

$$0 \rightarrow \text{Hom}_A(N, P) \rightarrow \text{Hom}_A(M, P) \rightarrow \text{Hom}_A(L, P)$$

è esatta.

**15.7.** Mostrare che esistono omomorfismi iniettivi di  $A$ -moduli  $M \rightarrow N$  tali che  $\text{Hom}_A(N, A) \rightarrow \text{Hom}_A(M, A)$  non è surgettiva.

**15.8.** Siano  $A \rightarrow B$  un morfismo di anelli ed  $M, N$  due  $B$ -moduli. Dimostrare che  $M \otimes_B N$  è isomorfo al quoziente di  $M \otimes_A N$  per il sottomodulo generato dagli elementi  $mb \otimes n - m \otimes bn$ , al variare di  $m \in M$ ,  $n \in N$  e  $b \in B$ .

**15.9.** Siano  $I, J$  ideali di un anello  $A$ . Provare che

$$\frac{A}{I} \otimes_A \frac{A}{J} = \frac{A}{I+J}.$$

**15.2 Derivazioni universali e differenziali razionali**

Siano  $A \rightarrow B$  un morfismo di anelli commutativi con unità e sia  $M$  un  $B$ -modulo. Un'applicazione  $\partial: B \rightarrow M$  si dice una  **$A$ -derivazione** se:

1.  $\partial$  è  $A$ -lineare (rispetto alle strutture di  $A$ -modulo su  $B, M$  indotte dal morfismo  $A \rightarrow B$ ).
2.  $\partial(b_1 b_2) = b_1 \partial(b_2) + b_2 \partial(b_1)$  per ogni  $b_1, b_2 \in B$  (regola di Leibniz).

Si noti che la regola di Leibniz implica  $\partial(1) = \partial(1) + \partial(1) = 0$  e di conseguenza  $\partial(a) = 0$  per ogni  $a \in A$ . Se  $\partial_1, \partial_2: B \rightarrow M$  sono  $A$ -derivazioni e  $b_1, b_2 \in B$ , allora anche  $b_1 \partial_1 + b_2 \partial_2$  è una  $A$ -derivazione; dunque l'insieme delle  $A$ -derivazioni da  $B$  in  $M$  ha una struttura naturale di  $B$  modulo che indicheremo con  $\text{Der}_A(B, M)$ . Per ogni  $A$ -derivazione  $\partial: B \rightarrow M$  e per ogni morfismo di  $B$ -moduli  $\phi: M \rightarrow N$ , la composizione  $\phi \circ \partial$  è ancora una  $A$ -derivazione ed il morfismo di composizione

$$\phi \circ : \text{Der}_A(B, M) \rightarrow \text{Der}_A(B, N)$$

è un omomorfismo di  $B$ -moduli.

**Teorema 15.2.1.** *Esiste una derivazione  $B \xrightarrow{d} \Omega_{B/A}$ , unica a meno di isomorfismo, con la seguente proprietà universale. Per ogni  $A$ -derivazione  $\partial: B \rightarrow M$  esiste un unico morfismo di  $B$ -moduli  $\phi: \Omega_{B/A} \rightarrow M$  tale che  $\partial = \phi \circ d$ .*

*Dimostrazione.* Esistono vari modi di costruire  $\Omega_{B/A}$ ; qui ne mostriamo solamente uno, rimandando agli esercizi per gli altri.

Consideriamo la struttura di  $B$ -modulo su  $B \otimes_A B$  indotta dalla moltiplicazione a sinistra (ossia  $b(c \otimes d) = bc \otimes d$ ) e definiamo

$$\Omega_{B/A} = \frac{B \otimes_A B}{R},$$

dove  $R$  è il  $B$ -sottomodulo generato dalle relazioni

$$1 \otimes b_1 b_2 - b_1 \otimes b_2 - b_2 \otimes b_1, \quad b_1, b_2 \in B.$$

Tali relazioni assicurano che l'applicazione

$$d: B \rightarrow \Omega_{B/A}, \quad db = 1 \otimes b,$$

è una  $A$ -derivazione. Notiamo che gli elementi  $db$ , con  $b \in B$ , generano  $\Omega_{B/A}$  come  $B$ -modulo. Se  $\partial: B \rightarrow M$  è una  $A$ -derivazione, allora l'applicazione  $B \times B \rightarrow M$ ,  $(b_1, b_2) \mapsto b_1 \partial(b_2)$ , è  $A$ -bilineare e quindi induce un morfismo di  $A$ -moduli  $\phi: B \otimes_A B \rightarrow M$ . Si verifica immediatamente che  $\phi$  è un omomorfismo di  $B$ -moduli che si annulla su  $R$  e che quindi definisce per passaggio al quoziente un omomorfismo  $\phi: \Omega_{B/A} \rightarrow M$  tale che  $\phi(db) = \phi(1 \otimes b) = \partial(b)$ . Dato che i  $db$  generano  $\Omega_{B/A}$ ,  $\phi$  è necessariamente unica. Se  $\delta: B \rightarrow P$  è un'altra derivazione con la medesima proprietà universale, esistono unici due omomorfismi di  $B$ -moduli  $P \rightarrow \Omega_{B/A}$ ,  $\Omega_{B/A} \rightarrow P$  che sono l'uno l'inverso dell'altro.  $\square$

**Definizione 15.2.2.** *Se  $A \rightarrow B$  è un omomorfismo di anelli, il  $B$ -modulo  $\Omega_{B/A}$  è detto modulo delle **forme differenziali relative** di  $B$  su  $A$  oppure modulo dei **differenziali di Kähler** di  $B$  su  $A$ . La derivazione  $d: B \rightarrow \Omega_{B/A}$  viene detta **derivazione universale**.*

Si noti che, per la regola di Leibniz applicata alla derivazione universale  $d: B \rightarrow \Omega_{B/A}$ , se  $B$  è una  $A$ -algebra finitamente generata, diciamo da  $b_1, \dots, b_s$ , allora  $\Omega_{B/A}$  è un  $B$ -modulo finitamente generato da  $db_1, \dots, db_s$ .

La proprietà universale implica che, per ogni  $B$ -modulo  $M$ , esiste un isomorfismo naturale

$$\text{Der}_A(B, M) = \text{Hom}_B(\Omega_{B/A}, M)$$

e di conseguenza esiste un accoppiamento  $B$ -bilineare

$$\langle \cdot, \cdot \rangle: \Omega_{B/A} \times \text{Der}_A(B, M) \rightarrow M$$

tale che  $\langle db, \partial \rangle = \partial(b)$  per ogni  $b \in B$ .

*Esempio 15.2.3.* Se  $B = A[t_1, \dots, t_n]$ , allora  $\Omega_{B/A}$  è il  $B$ -modulo libero generato da  $dt_1, \dots, dt_n$ . Abbiamo già visto che  $dt_1, \dots, dt_n$  generano  $\Omega_{B/A}$  come  $B$ -modulo. Considerando le derivate parziali  $\frac{\partial}{\partial t_i}: B \rightarrow B$ , si osserva che  $\left\langle \sum b_i dt_i, \frac{\partial}{\partial t_j} \right\rangle = b_j$  e quindi i  $dt_i$  sono linearmente indipendenti.

*Esempio 15.2.4.* Se  $\mathbb{K} \subset \mathbb{K}(t_1, \dots, t_d) = K$  è una estensione puramente trascendente di campi, allora  $dt_1, \dots, dt_n$  sono una  $K$ -base di  $\Omega_{K/\mathbb{K}}$ . Infatti una  $\mathbb{K}$ -derivazione  $\partial: K \rightarrow V$  è unicamente determinata dai  $\partial t_i$  e quindi  $dt_1, \dots, dt_n$  sono un sistema di generatori. D'altra parte le derivate parziali rispetto alle variabili  $t_i$  sono  $\mathbb{K}$ -derivazioni, si ha  $\left\langle dt_i, \frac{\partial}{\partial t_j} \right\rangle = \delta_{ij}$  e quindi  $dt_1, \dots, dt_n$  sono linearmente indipendenti.

Ogni morfismo di  $A$ -algebre  $\phi: B \rightarrow C$ , composto con la derivazione universale di  $C$  definisce una  $A$ -derivazione  $B \rightarrow \Omega_{C/A}$  e, per la proprietà universale di  $\Omega_{B/A}$ , esiste un unico morfismo di  $B$ -moduli  $\phi_*: \Omega_{B/A} \rightarrow \Omega_{C/A}$  che a sua volta induce, per cambio di base, un unico morfismo di  $C$ -moduli  $\phi_*: C \otimes_B \Omega_{B/A} \rightarrow \Omega_{C/A}$  tale che  $\phi_*(c \otimes db) = cd(\phi b)$  per ogni  $b \in B$ .

**Lemma 15.2.5.** *Siano  $\mathbb{K} \subset K \subset L$  estensioni di campi con  $L$  algebrico separabile su  $K$ . Allora esiste un isomorfismo naturale  $\Omega_{L/\mathbb{K}} = L \otimes_K \Omega_{K/\mathbb{K}}$ .*

*Dimostrazione.* Denotiamo con  $\alpha: L \otimes_K \Omega_{K/\mathbb{K}} \rightarrow \Omega_{L/\mathbb{K}}$  il morfismo indotto dall'inclusione  $K \subset L$ . Proviamo che  $\alpha$  è surgettiva, ossia dimostriamo che per ogni  $l \in L$  il differenziale  $dl$  è una combinazione lineare a coefficienti in  $L$  di elementi  $df$ ,  $f \in K$ . Sia  $l \in L$  e sia  $\mu_l = \sum f_i x^i$  il suo polinomio minimo su  $K$ , allora  $0 = d\mu_l(l) = \sum df_i l^i + \mu'_l(l)dl$  ed essendo  $l$  separabile vale  $\mu'_l(l) \neq 0$ .

Proviamo adesso che  $\alpha$  è iniettiva: a tal fine basta trovare una  $\mathbb{K}$ -derivazione  $\partial: L \rightarrow L \otimes_K \Omega_{K/\mathbb{K}}$  che estende  $1 \otimes d: K \rightarrow L \otimes_K \Omega_{K/\mathbb{K}}$ . Tale derivazione indurrà un morfismo  $L$ -lineare  $\beta: \Omega_{L/\mathbb{K}} \rightarrow L \otimes_K \Omega_{K/\mathbb{K}}$  che sarà l'inverso a sinistra di  $\alpha$ . Per il lemma di Zorn esiste un sottocampo  $K \subset E \subset L$  ed una derivazione  $\partial: E \rightarrow L \otimes_K \Omega_{K/\mathbb{K}}$  che estende  $1 \otimes d$  e tale che  $(E, \partial)$  è massimale tra le coppie aventi la stessa proprietà. Assumiamo per assurdo  $E \neq L$ ; prendiamo  $l \notin E$  e sia  $\mu_l = \sum e_i x^i \in E[x]$  il suo polinomio minimo su  $E$ . Consideriamo la struttura di  $E[x]$  modulo su  $L \otimes_K \Omega_{K/\mathbb{K}}$  indotta dal morfismo  $E[x] \rightarrow E[l] \subset L$ . Scelto un qualsiasi elemento  $y \in L \otimes_K \Omega_{K/\mathbb{K}}$  possiamo estendere  $\partial$  ad una derivazione  $\delta: E[x] \rightarrow L \otimes_K \Omega_{K/\mathbb{K}}$  tale che  $\delta(x) = y$ . Se  $y$  è scelto in modo tale che  $\delta(\mu_l) = 0$ , allora  $\delta$  si fattorizza ad una derivazione su  $E[l]$  in contraddizione alla massimalità. Essendo  $l$  separabile su  $E$ , una tale scelta di  $y$  è certamente possibile perché  $\mu'_l(l) \neq 0$  e  $\delta(\mu_l) = \sum \partial(e_i)l^i + \mu'_l(l)y$ .  $\square$

*Esempio 15.2.6.* Il risultato del Lemma 15.2.5 è falso se l'estensione  $K \subset L$  non è separabile. Consideriamo ad esempio un campo  $\mathbb{K}$  di caratteristica  $p > 0$  e  $\mathbb{K} \subset \mathbb{K}(t) = K$  una estensione trascendente pura. Sia  $\phi: K \rightarrow K$  l'omomorfismo di  $\mathbb{K}$ -algebre tale che  $\phi(t) = t^p$ , allora il morfismo indotto  $\phi_*: \Omega_{K/\mathbb{K}} \rightarrow \Omega_{K/\mathbb{K}}$  è nullo. Infatti  $dt$  genera il modulo dei differenziali e  $\phi_*(dt) = dt^p = 0$ .

## Esercizi

**15.10.** Siano  $A, B, M$  come sopra: provare che una  $\mathbb{Z}$ -derivazione  $\partial: B \rightarrow M$  è una  $A$ -derivazione se e solo se  $\partial(a) = 0$  per ogni  $a \in A$ .

**15.11.** Sia  $A \rightarrow B$  un omomorfismo di anelli e sia  $S \subset B$  una parte moltiplicativa. Dimostrare che  $\Omega_{S^{-1}B/A} = S^{-1}\Omega_{B/A}$ .

## 15.3 Residui astratti (secondo Tate)

Sia  $V$  uno spazio vettoriale su un campo  $\mathbb{K}$ ; un endomorfismo lineare  $f: V \rightarrow V$  si dice **di potenza finita** se  $f^n$  ha rango finito per  $n \gg 0$ . Se  $f$  è di potenza finita possiamo definire la sua **traccia**  $\text{trace}_V(f)$  come la traccia della restrizione di  $f$  al sottospazio di dimensione finita  $\cap_{n>0} f^n(V)$ . Se  $F \subset V$  è un sottospazio di dimensione finita tale che  $f(F) \subset F$  e  $f^n(V) \subset F$  per  $n \gg 0$ , allora è facile verificare che  $\text{trace}_V(f)$  è uguale alla traccia della restrizione di  $f$  a  $F$ .

**Lemma 15.3.1.** *Siano  $f: V \rightarrow V$  un'applicazione lineare ed  $A \subset V$  un sottospazio tale che  $f(A) \subset A$ . Denotiamo con*

$$f_1: A \rightarrow A, \quad f_2: \frac{V}{A} \rightarrow \frac{V}{A}$$

le applicazioni indotte. Allora:

1.  $f$  è di potenza finita se e solo se  $f_1$  e  $f_2$  sono di potenza finita.
2. Se  $f$  è di potenza finita, allora  $\text{trace}_V(f) = \text{trace}_A(f_1) + \text{trace}_{V/A}(f_2)$ .

*Dimostrazione.* [1] Per ogni  $n > 0$  vale  $f_1^n(A) \subset f^n(V)$ ,  $f_2^n(V/A) = (f^n(V) + A)/A$  e quindi se  $f$  è di potenza finita anche  $f_1, f_2$  lo sono. Viceversa, supponiamo  $f_1, f_2$  di potenza finita; esistono allora interi  $n, m > 0$  ed un sottospazio  $F \subset V$  di dimensione finita tali che  $\dim f^n(A) < +\infty$ ,  $f^m(V) \subset A + F$  e quindi  $f^{n+m}(V) \subset f^n(A) + f^n(F)$ .

[2] Sia  $n_0 \in \mathbb{N}$  tale che  $f^n(V) = f^{n_0}(V)$  per ogni  $n \geq n_0$ . Denotando  $F = f^{n_0}(V)$ , esiste un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccc} 0 & \longrightarrow & F \cap A & \longrightarrow & F & \longrightarrow & \frac{F+A}{A} \longrightarrow 0 \\ & & \downarrow f_1 & & \downarrow f & & \downarrow f_2 \\ 0 & \longrightarrow & F \cap A & \longrightarrow & F & \longrightarrow & \frac{F+A}{A} \longrightarrow 0 \end{array}$$

e, poiché  $F$  ha dimensione finita, la formula  $\text{trace}_V(f) = \text{trace}_A(f_1) + \text{trace}_{V/A}(f_2)$  segue dalle tradizionali proprietà della traccia, cfr. Esercizio 8.3. □

**Lemma 15.3.2.** *Siano  $f, g: V \rightarrow V$  due endomorfismi lineari. Se  $fg$  e  $gf$  hanno potenza finita, allora  $\text{trace}_V(fg) = \text{trace}_V(gf)$ .*

*Dimostrazione.* Sia  $n$  un intero sufficientemente grande e tale che gli spazi  $(fg)^n(V)$ ,  $(gf)^n(V)$  abbiano dimensione finita. Allora esistono e sono ben definiti i due morfismi

$$(fg)^n(V) \begin{array}{c} \xleftarrow{f} \\ \xrightarrow{g} \end{array} (gf)^n(V),$$

e si usano le ben note proprietà della traccia in dimensione finita. □

Siano  $A, B \subset V$  sottospazi vettoriali. Diremo che  $A$  non è molto più grande di  $B$ , e scriveremo  $A \prec B$ , se esiste un sottospazio  $F$  di dimensione finita tale che  $A \subset B + F$ . Notiamo che  $A \prec B$  se e solo se lo spazio vettoriale  $\frac{A}{A \cap B} = \frac{A+B}{B}$  ha dimensione finita. È palese che  $\prec$  è una relazione di ordine e quindi la relazione  $\sim$  data da

$$A \sim B \quad \text{se e solo se} \quad A \prec B, \quad B \prec A$$

è una relazione di equivalenza.

**Lemma 15.3.3.** *Se vale  $A \prec B$ , allora  $f(A) \prec f(B)$  per ogni applicazione lineare  $f$ .*

*Dimostrazione.* Evidente. □

**Definizione 15.3.4.** *Sia  $V$  uno spazio vettoriale. Per ogni sottospazio  $A \subset V$  definiamo*

$$\begin{aligned} E(A) &= \{f \in \text{Hom}_{\mathbb{K}}(V, V) \mid f(A) \prec A\}, \\ E_1(A) &= \{f \in E(A) \mid f(V) \prec A\}, \quad E_2(A) = \{f \in E(A) \mid f(A) \prec 0\}, \\ E_0(A) &= E_1(A) \cap E_2(A). \end{aligned}$$

Si osserva facilmente che  $E(A), E_0(A), E_1(A), E_2(A)$  sono sottospazi vettoriali di  $\text{Hom}_{\mathbb{K}}(V, V)$  che dipendono solo dalla classe di equivalenza di  $A$ . Ogni applicazione lineare  $f: V \rightarrow V$  induce un isomorfismo di spazi vettoriali

$$\frac{A}{A \cap f^{-1}(A)} \xrightarrow{f} \frac{A + f(A)}{A}$$

e quindi  $f \in E(A)$  se e soltanto se  $A \cap f^{-1}(A)$  ha codimensione finita in  $A$ .

*Esempio 15.3.5.* Nelle notazioni precedenti, vale  $A \prec B$  se e solo se  $E_1(A) \subset E_1(B)$ : infatti se  $E_1(A) \subset E_1(B)$ , allora la proiezione di  $V$  su  $A$  appartiene a  $E_1(B)$ . Dunque  $E_1(A)$  determina univocamente la classe di equivalenza di  $A$ .

**Lemma 15.3.6.** *Lo spazio  $E(A)$  è una  $\mathbb{K}$ -sottoalgebra unitaria di  $\text{Hom}_{\mathbb{K}}(V, V)$ , i sottospazi  $E_0(A), E_1(A), E_2(A)$  sono ideali bilateri di  $E(A)$  e vale  $E_1(A) + E_2(A) = E(A)$ .*

*Dimostrazione.* Per ogni  $a \in \mathbb{K}$ , la moltiplicazione per  $a$  appartiene a  $E(A)$ . Se  $f, g \in E(A)$  allora  $f(A) \prec A$ , per il Lemma 15.3.3  $gf(A) \prec g(A) \prec A$  e quindi  $gf(A) \prec A$ ,  $gf \in E(A)$ . Se  $f(A) \subset A+F, g(A) \subset A+G$ , con  $F, G$  sottospazi di dimensione finita, allora  $(f+g)(A) \subset A+F+G$  e  $f+g \in E(A)$ . La verifica che gli  $E_i(A)$ , per  $i = 0, 1, 2$ , sono ideali bilateri di  $E(A)$  è banale ed è lasciata per esercizio al lettore. Ne segue che  $E_1(A) + E_2(A)$  è un ideale bilatero ed è quindi sufficiente dimostrare che  $1 \in E_1(A) + E_2(A)$ . Se  $p_A: V \rightarrow A$  è la proiezione su  $A$ , allora  $p_A \in E_1(A), 1 - p_A \in E_2(A)$  e  $1 = p_A + (1 - p_A)$ .  $\square$

Se  $f \in E_0(A)$ , allora  $f^2(V) \prec 0$  e quindi  $f$  è di potenza finita ed è definita la traccia  $\text{trace}_V(f)$ .

**Lemma 15.3.7.** *L'applicazione  $\text{trace}_V: E_0(A) \rightarrow \mathbb{K}$  è lineare. Inoltre se  $f \in E_1(A)$  e  $g \in E_2(A)$ , allora  $\text{trace}_V(fg) = \text{trace}_V(gf)$  e quindi  $\text{trace}_V([f, g]) = 0$ .*

*Dimostrazione.* Per ogni coppia  $f, g \in E_0(A)$  possiamo trovare due sottospazi  $C \subset B$  tali che  $\dim_{\mathbb{K}} B/C < +\infty$ ,  $f(V) + g(V) \subset B$ ,  $f(C) = g(C) = 0$  (ad esempio  $C = A \cap \text{Ker}(f) \cap \text{Ker}(g)$ ,  $B = A + f(V) + g(V)$ ). Per il Lemma 15.3.1 vale la relazione

$$\text{trace}_V(af + bg) = \text{trace}_{B/C}(af + bg) = a \text{trace}_{B/C}(f) + b \text{trace}_{B/C}(g).$$

Se  $f \in E_1(A), g \in E_2(A)$  allora  $fg, gf \in E_0(A)$  e la formula  $\text{trace}_V(fg) = \text{trace}_V(gf)$  segue dal Lemma 15.3.2. Infine, il bracket  $[f, g]$  è per definizione uguale a  $fg - gf$ .  $\square$

Sia  $K \subset E(A)$  una  $\mathbb{K}$ -sottoalgebra *commutativa*, possiamo pensare quindi  $V$  come un  $K$ -modulo ed  $A$  un  $\mathbb{K}$ -sottospazio tale che  $fA \prec A$  per ogni  $f \in K$ . Il nostro prossimo obiettivo è quello di associare ad  $A$  un'applicazione  $\mathbb{K}$ -lineare

$$\text{res}_A^V: \Omega_{K/\mathbb{K}} \longrightarrow \mathbb{K}$$

che chiameremo **residuo**.

Siano  $f, g \in K$ , per il Lemma 15.3.6 è possibile scrivere (in modo non unico)  $f = f_1 + f_2$  e  $g = g_1 + g_2$ , con  $f_1, g_1 \in E_1(A)$  e  $f_2, g_2 \in E_2(A)$ . Si noti che  $[f_1, g_1] \in E_1(A)$  e che  $[f_1, g_1] \equiv [f, g] = 0 \pmod{E_2(A)}$ , dunque  $[f_1, g_1] \in E_0(A)$  ed è ben definito  $\text{trace}_V[f_1, g_1]$ . Per il Lemma 15.3.7 la traccia di  $[f_1, g_1]$  non dipende dalla particolare scelta di  $f_1, g_1$ . L'applicazione  $(f, g) \mapsto \text{trace}_V[f_1, g_1]$  è chiaramente  $\mathbb{K}$ -bilinare in  $f$  e  $g$ . Poniamo per definizione

$$\text{res}_A^V(fdg) = \text{Tr}_V[f_1, g_1].$$

Occorre verificare che si tratta di una buona definizione, bisogna cioè dimostrare che l'applicazione lineare



$$\text{trace}_V[-1, -1]: K \otimes_{\mathbb{K}} K \rightarrow \mathbb{K}$$

si annulla sul  $\mathbb{K}$ -sottospazio vettoriale generato dalle espressioni  $f \otimes hg - fh \otimes g - gf \otimes h$ . Fissati  $f_1, g_1, h_1$  possiamo scegliere  $(hg)_1 = h_1g_1$ ,  $(fh)_1 = f_1h_1$ ,  $(gf)_1 = g_1f_1$  e l'annullamento segue dalla relazione

$$[f_1, h_1g_1] - [f_1h_1, g_1] - [g_1f_1, h_1] = 0.$$

È chiaro dalle definizioni che  $\text{res}_A^V$  dipende solo dai sottospazi  $E_1(A), E_2(A)$  e che quindi dipende solo dalla classe di equivalenza di  $A$ . Segue immediatamente dalla definizione che  $\text{res}_A^V(fdg) + \text{res}_A^V(gdf) = 0$  per ogni  $f, g \in K$ ; in particolare per  $g = 1$  si ottiene  $\text{res}_A^V(df) = 0$ .

**Lemma 15.3.8.** *Nelle notazioni precedenti, se  $\pi: V \rightarrow A$  è una proiezione, allora vale*

$$\text{res}_A^V(fdg) = \text{trace}_{A/C}[\pi f, \pi g],$$

dove  $C = \{x \in A \mid f(x), g(x) \in A\} \sim A$ . In particolare, se  $V \subset V'$  è una inclusione di  $K$ -moduli, allora  $\text{res}_A^V = \text{res}_A^{V'}$ .

*Dimostrazione.* Nella definizione di  $\text{res}_A^V$  possiamo prendere  $f_1 = \pi f$  e  $g_1 = \pi g$ . Osserviamo inoltre che  $[\pi f, \pi g](V) \subset A$  e che, se  $x \in C$ , allora  $[\pi f, \pi g]x = \pi[f, g]x = 0$ .  $\square$

**Proposizione 15.3.9.** *Nelle notazioni precedenti:*

1. Se  $f, g \in K$ ,  $f(A) \subset A$  e  $g(A) \subset A$ , allora  $\text{res}_A^V(fdg) = 0$ . In particolare se  $A$  è un  $K$ -sottomodulo di  $V$ , allora il residuo è identicamente nullo.
2. Per ogni  $g \in K$  ed ogni  $n \geq 0$  vale  $\text{res}_A^V(g^n dg) = 0$ .
3. Se  $g \in K$  è invertibile e  $n \leq -2$ , allora  $\text{res}_A^V(g^n dg) = 0$ .
4. Se  $g \in K$  è invertibile e  $g(A) \subset A$ , allora  $\text{res}_A^V(g^{-1}dg)$  è uguale alla traccia dell'identità in  $A/g(A)$ .

*Dimostrazione.* [1] Sia  $\pi: V \rightarrow A$  una proiezione fissata, se  $f(A) \subset A$  allora  $\pi f = f$  e basta applicare il Lemma 15.3.8.

[2] Fissata una decomposizione  $g = g_1 + g_2$ , si può prendere  $(g^n)_1 = g_1^n$  e quindi  $[g_1^n, g_1] = 0$ .

[3] Se si pone  $h = g^{-1}$ , allora  $g^n dg = -h^{-2-n} dh$  e la tesi segue dal punto 2).

[4] Si applica il Lemma 15.3.8 osservando che  $C = g(A)$  e che per ogni  $x \in A$  vale

$$[\pi g^{-1}, \pi g]x = x - g(\pi g^{-1}x) \equiv x \pmod{g(A)}.$$

$\square$

*Esempio 15.3.10.* Sia  $U \subset \mathbb{C}$  un aperto contenente il punto  $z = 0$ . Denotiamo con  $K = V$  la  $\mathbb{C}$ -algebra delle funzioni meromorfe su  $U$  (ovvero localmente esprimibili in serie di Laurent) e con  $A \subset V$  la sottoalgebra delle funzioni che sono regolari in 0. Se  $f \in K$  ha un polo di ordine  $h$  in 0, allora

$$fA \subset A + \mathbb{C} \frac{1}{z^h} + \mathbb{C} \frac{1}{z^{h-1}} + \cdots + \mathbb{C} \frac{1}{z^{-1}} \prec A$$

e quindi siamo nelle condizioni di poter definire un residuo  $\text{res}_A^K: \Omega_{K/\mathbb{C}} \rightarrow \mathbb{C}$ . Se  $fdz$  è un differenziale meromorfo su  $U$ , allora il Lemma 15.3.9 implica che  $\text{res}_A^K(fdz) = 0$  se  $f$  è regolare in 0. Siccome  $A/zA = \mathbb{C}1$ , si ha  $\text{res}_A^K(z^{-1}dz) = 1$  e  $\text{res}_A^K(z^n dz) = 0$  per ogni  $n \neq -1$ . Abbiamo quindi ritrovato il residuo usuale.

Vediamo infine come si comportano i residui con le successioni esatte.

**Proposizione 15.3.11.** *Sia  $0 \rightarrow U \rightarrow V \xrightarrow{p} W \rightarrow 0$  una successione esatta di  $K$ -moduli e sia  $A \subset V$  un  $\mathbb{K}$ -sottospazio tale che  $f(A) \prec A$  per ogni  $f \in K$ . Indichiamo  $A_1 = A \cap U$  e  $A_2 = p(A)$ . Allora vale  $f(A_1) \prec A_1$ ,  $f(A_2) \prec A_2$  per ogni  $f \in K$  e*

$$\text{res}_A^V = \text{res}_{A_1}^U + \text{res}_{A_2}^W$$

*Dimostrazione.* Sia  $F \subset V$  un sottospazio di dimensione finita tale che  $f(A) \subset A + F$ ; allora è chiaro che  $f(A_2) \subset A_2 + p(F)$  e  $f(A_1) \subset U \cap (A + F)$ . Un semplice conto di algebra lineare che lasciamo per esercizio mostra che

$$\dim_{\mathbb{K}} \frac{U \cap (A + F)}{A_1} \leq \dim_{\mathbb{K}} F$$

e quindi  $f(A_1) \prec A_1$ . Fissiamo delle proiezioni  $\pi, \pi_1, \pi_2$  tali che il seguente diagramma sia commutativo

$$\begin{array}{ccccccc} 0 & \longrightarrow & U & \longrightarrow & V & \xrightarrow{p} & W & \longrightarrow & 0 \\ & & \downarrow \pi_1 & & \downarrow \pi & & \downarrow \pi_2 & & \\ 0 & \longrightarrow & A_1 & \longrightarrow & A & \xrightarrow{p} & A_2 & \longrightarrow & 0. \end{array}$$

Allora, per ogni  $f, g \in K$ , anche il diagramma

$$\begin{array}{ccccccc} 0 & \longrightarrow & U & \longrightarrow & V & \xrightarrow{p} & W & \longrightarrow & 0 \\ & & \downarrow [\pi_1 f, \pi_1 g] & & \downarrow [\pi f, \pi g] & & \downarrow [\pi_2 f, \pi_2 g] & & \\ 0 & \longrightarrow & U & \longrightarrow & V & \xrightarrow{p} & W & \longrightarrow & 0 \end{array}$$

è commutativo e la tesi segue dai Lemmi 15.3.1 e 15.3.8.  $\square$

**Corollario 15.3.12.** *Siano  $A, B \subset V$  due sottospazi tali che  $f(A) \prec A$  e  $f(B) \prec B$  per ogni  $f \in K$ . Allora vale  $f(A \cap B) \prec A \cap B$  e  $f(A + B) \prec A + B$  per ogni  $f \in K$  e*

$$\text{res}_A^V + \text{res}_B^V = \text{res}_{A \cap B}^V + \text{res}_{A+B}^V.$$

*Dimostrazione.* Si consideri  $A \oplus B \subset V \oplus V$ , è chiaro che  $f(A \oplus B) \prec A \oplus B$  per ogni  $f \in K$  e per la Proposizione 15.3.11,  $\text{res}_{A \oplus B}^{V \oplus V} = \text{res}_A^V + \text{res}_B^V$ . Considerando invece la successione esatta

$$0 \longrightarrow V \longrightarrow V \oplus V \xrightarrow{p} V \longrightarrow 0, \quad p(x, y) = x - y$$

si ottiene  $p(A \oplus B) = A + B$ ,  $V \cap (A \oplus B) = A \cap B$  e quindi  $\text{res}_{A \oplus B}^{V \oplus V} = \text{res}_{A+B}^V + \text{res}_{A \cap B}^V$ .  $\square$

## Esercizi

**15.12.** Nelle notazioni del Lemma 15.3.3, provare che se vale  $A \prec C$  e  $B \prec D$ , allora vale  $A \cap B \prec C \cap D$ .

## 15.4 Esercizi complementari

**15.13.** Siano  $X \rightarrow Z, Y \rightarrow Z$  morfismi regolari di varietà affini; mostrare:

1. Esiste un omomorfismo naturale  $\psi: \mathbb{K}[X] \otimes_{\mathbb{K}[Z]} \mathbb{K}[Y] \rightarrow \mathbb{K}[X \times_Z Y]$
2.  $\psi$  è surgettivo ed il suo nucleo contiene il nilradicale  $\sqrt{0}$ .

3. Trovare un esempio in cui  $\psi$  non è iniettivo (Sugg.:  $X, Y$  curve nel piano affine  $\mathbb{A}^2 = Z$ ).
4. (\*) Il nucleo di  $\psi$  è uguale al nilradicale  $\sqrt{0}$ .

**15.14.** Siano  $A \rightarrow B, A \rightarrow C$  omomorfismi di anelli Noetheriani. Dimostrare che  $B \otimes_A C$  è un anello Noetheriano.

**15.15.** Siano  $\{M_i \mid i \in I\}$  e  $\{N_j \mid j \in J\}$  due famiglie di  $A$ -moduli. Esiste un isomorfismo naturale

$$\text{Hom}_A \left( \bigoplus_i M_i, \prod_j N_j \right) = \prod_{i,j} \text{Hom}_A(M_i, N_j).$$

**15.16.** Siano  $M_i, i \in I,$  e  $N_j, j \in J,$  due famiglie di  $A$ -moduli. Dimostrare che esiste un'applicazione naturale

$$\left( \bigoplus_{i \in I} M_i \right) \times \left( \bigoplus_{j \in J} N_j \right) \rightarrow \bigoplus_{i,j} M_i \otimes_A N_j$$

che induce un isomorfismo

$$\left( \bigoplus_{i \in I} M_i \right) \otimes_A \left( \bigoplus_{j \in J} N_j \right) = \bigoplus_{i,j} M_i \otimes_A N_j.$$

(Sugg.: Lemma 15.1.4 ed Esercizi 15.1, 15.15.)

**15.17.** Sia  $L \rightarrow M \rightarrow N \rightarrow 0$  una successione esatta di  $A$ -moduli. Dimostrare che per ogni  $A$ -modulo  $P$  la successione

$$L \otimes_A P \rightarrow M \otimes_A P \rightarrow N \otimes_A P \rightarrow 0$$

è esatta. (Sugg.: Esercizio 15.6.)

**15.18.** Siano  $A \rightarrow B$  un morfismo di anelli unitari,  $S$  un insieme e  $F$  lo  $A$ -modulo libero generato da  $S$ . Provare che  $F \otimes_A B$  è isomorfo al  $B$ -modulo libero generato da  $S$ .

**15.19 (Lemma di Artin-Rees).** Siano  $A$  un anello noetheriano,  $M$  un  $A$ -modulo finitamente generato,  $N \subset M$  un sottomodulo ed  $I \subset A$  un ideale. Provare che esiste un intero  $k \geq 0$  tale che  $I^{n+k}M \cap N = I^n(I^kM \cap N)$  per ogni  $n \geq 0$ . (Sugg.: siano  $a_1, \dots, a_s$  generatori dell'ideale  $I$ : si considerino l'anello noetheriano  $T = A[t_1, \dots, t_s]$ , il  $T$ -modulo finitamente generato  $P = T \otimes_A M$ , l'applicazione

$$f: P \rightarrow M, \quad f(p(t_1, \dots, t_s) \otimes m) = p(a_1, \dots, a_s)m$$

e si ragioni come nella dimostrazione del Teorema 4.3.6.)

**15.20.** Siano  $A$  un anello locale noetheriano con ideale massimale  $\mathfrak{m}$  ed  $M$  un  $A$ -modulo finitamente generato. Dimostrare che  $\bigcap_{n>0} \mathfrak{m}^n M = 0$ .

**15.21.** Sia  $A \rightarrow B$  un morfismo di anelli unitari e sia  $F_{dB}$  il  $B$ -modulo libero generato dall'insieme dei simboli formali  $db$ , al variare di  $b \in B$ . Provare che  $\Omega_{B/A} = F_{dB}/R$ , dove  $R$  è il sottomodulo generato dai  $da$ , con  $a \in A$ , e dai  $d(bc) - bd(c) - cd(b)$ , con  $b, c \in B$ .

**15.22.** Siano  $A \rightarrow B \rightarrow C$  omomorfismi di anelli. Provare che per ogni  $C$ -modulo  $M$  la successione

$$0 \longrightarrow \text{Der}_B(C, M) \longrightarrow \text{Der}_A(C, M) \longrightarrow \text{Der}_A(B, M)$$

è esatta. Utilizzare l'Esercizio 15.6 per dimostrare l'esattezza della successione

$$C \otimes_B \Omega_{B/A} \longrightarrow \Omega_{C/A} \longrightarrow \Omega_{C/B} \longrightarrow 0.$$

**15.23.** Siano  $A \rightarrow B$  un morfismo di anelli,  $I \subset B$  un ideale e  $C = B/I$ . Provare che per ogni  $C$ -modulo  $M$  la successione

$$0 \longrightarrow \text{Der}_A(C, M) \longrightarrow \text{Der}_B(C, M) \longrightarrow \text{Hom}_B(I, M) = \text{Hom}_C(I/I^2, M)$$

è esatta. Utilizzare l'Esercizio 15.6 per dimostrare l'esattezza della successione di  $C$ -moduli

$$I/I^2 = C \otimes_B I \xrightarrow{1 \otimes d} C \otimes_B \Omega_{B/A} \longrightarrow \Omega_{C/A} \longrightarrow 0.$$

**15.24.** Nelle stesse notazioni della Proposizione 15.3.11, è vero o falso che se  $fA_1 \prec A_1$  e  $fA_2 \prec A_2$ , allora  $fA \prec A$ ?

**15.25.** Provare che  $\sum_{i=1}^n A_i \prec \cap_{j=1}^m B_j$  se e soltanto se  $A_i \prec B_j$  per ogni  $i, j$ .

## 15.5 Un lungo esercizio: il teorema di Krull

**Definizione 15.5.1.** Un ideale  $I \subset \mathbb{K}[x_1, \dots, x_m]$  si dice saturato in 0 se ogni volta che  $fg \in I$  e  $g(0) \neq 0$ , ne consegue che  $f \in I$ .

Se consideriamo la parte moltiplicativa  $S = \{g \in \mathbb{K}[x_1, \dots, x_m] \mid g(0) \neq 0\}$ , dire che un ideale  $I$  è saturato in 0 equivale a dire che

$$I = IS^{-1}\mathbb{K}[x_1, \dots, x_m] \cap \mathbb{K}[x_1, \dots, x_m].$$

Gli esercizi di questa sezione permetteranno di dimostrare il seguente risultato.

**Teorema 15.5.2 (Krull).** Sia  $\mathbb{K}$  un campo normato ed  $I \subset \mathbb{K}[x_1, \dots, x_m]$  un ideale saturato in 0. Allora vale

$$I = I\mathbb{K}\{x_1, \dots, x_m\} \cap \mathbb{K}[x_1, \dots, x_m].$$

Per semplificare le notazioni, denoteremo  $B = \mathbb{K}\{x_1, \dots, x_n\}$  ed  $A = S^{-1}\mathbb{K}[x_1, \dots, x_m]$ , dove  $S = \{g \in \mathbb{K}[x_1, \dots, x_m] \mid g(0) \neq 0\}$ .

### Esercizi

**15.26.** Provare che esistono inclusioni di anelli  $\mathbb{K}[x_1, \dots, x_m] \subset A \subset B$  e che un ideale  $I \subset \mathbb{K}[x_1, \dots, x_m]$  è saturato in 0 se e solo se  $IA \cap \mathbb{K}[x_1, \dots, x_m] = I$ .

**15.27.** Provare che gli anelli  $A, B$  sono locali e Noetheriani. Indicando con  $\mathfrak{m} \subset A, \mathfrak{n} \subset B$  i rispettivi ideali massimali e, per ogni  $n > 0$ , con  $A_n = A/\mathfrak{m}^n$  e  $B_n = B/\mathfrak{n}^n$ , si dimostri che valgono le uguaglianze  $\mathfrak{m}B = \mathfrak{n}$  e  $A_n = B_n$  per ogni  $n > 0$ .

**15.28.** Siano  $I \subset J$  ideali di  $A$ . Provare che  $I = J$  se e solo se il morfismo naturale  $I \otimes_A B \rightarrow J \otimes_A B$  è surgettivo. (Sugg.: se  $H = J/I$  e  $H \otimes_A B_1 = 0$ , allora applicare il Lemma di Nakayama per dimostrare che  $H = 0$ .)

**15.29 (\*)**. Dimostrare che per ogni ideale  $I \subset A$ , il morfismo naturale

$$\mu: I \otimes_A B \rightarrow B, \quad f(a \otimes b) = ab,$$

è iniettivo. (Sugg.: per Artin-Rees basta dimostrare che  $\text{Ker}(\mu) \subset \mathfrak{n}^n(I \otimes_A B)$  per ogni  $n$  sufficientemente grande. Sia dunque  $n > 0$  fissato, consideriamo un intero  $k$  tale che  $\mathfrak{m}^k \cap I \subset \mathfrak{m}^n I$  ed i due morfismi

$$I \otimes_A B \xrightarrow{f} \frac{I}{\mathfrak{m}^k \cap I} \otimes_A B \xrightarrow{g} \frac{I}{\mathfrak{m}^n I} \otimes_A B = \frac{I \otimes B}{\mathfrak{n}^n(I \otimes_A B)}.$$

D'altra parte  $\frac{I}{\mathfrak{m}^k \cap I}$  è un  $A_k = B_k$ -modulo e quindi  $\frac{I}{\mathfrak{m}^k \cap I} \otimes_A B = \frac{I}{\mathfrak{m}^k \cap I} \otimes_{A_k} B_k = \frac{I}{\mathfrak{m}^k \cap I}$ . In particolare il morfismo naturale  $\frac{I}{\mathfrak{m}^k \cap I} \otimes_A B \rightarrow B_k$  è iniettivo e quindi il nucleo di  $f$  coincide con il nucleo del morfismo naturale  $\mu_k: I \otimes_A B \rightarrow B_k$ . Basta adesso osservare che  $\text{Ker}(\mu) \subset \text{Ker}(f) \subset \text{Ker}(g)$ .

*Osservazione 15.5.3.* Per alcuni risultati di carattere generale sulla piatezza (vedi [AM1969]) il risultato dell'Esercizio 15.29 equivale a dire che  $B$  è piatto come  $A$ -modulo.

**15.30.** Sia  $I \subset A$  un ideale e  $K = \text{Ker}(A \rightarrow B/IB)$ . Provare che  $I = K$ . (Sugg.: si ha

$$I \otimes_A B \xrightarrow{f} K \otimes_A B \xrightarrow{\mu} IB.$$

Per l'Esercizio 15.29  $\mu$  è iniettiva mentre la composizione  $\mu f$  è surgettiva. Applicare l'Esercizio 15.28.)



## Il teorema di Riemann-Roch per curve lisce proiettive

Sia  $X$  è una curva liscia proiettiva; nella Sezione 14.4 abbiamo introdotto le nozioni di divisore su  $X$  e di gruppo delle classi  $\text{Cl}(X) = \bigoplus_{s \geq 0} \text{Cl}^s(X)$ . Per ogni intero  $s > 0$  si denota con  $\mu_s$  l'applicazione

$$\mu_s: X^s \rightarrow \text{Cl}^s(X), \quad \mu_s(p_1, \dots, p_s) = p_1 + \dots + p_s.$$

Per  $s = 0$  si pone per convenzione  $X^0 = 0$  e  $\mu_0(0) \in \text{Cl}^0(X)$  la classe di equivalenza lineare del divisore nullo. L'immagine della mappa  $\mu_s$  è l'insieme delle classi di equivalenza lineare dei divisori  $D$  di grado  $s$  tali che  $h^0(X, D) > 0$ : ne segue che  $\mu_s$  è surgettiva se e solo se  $h^0(X, D) > 0$  per ogni divisore di grado  $s$ . Dimosteremo tra poco che  $\mu_s$  è surgettiva per  $s \gg 0$ .

**Definizione 16.0.1 (Weierstrass).** *Il minimo intero  $g = g(X)$  per il quale l'applicazione  $\mu_g$  è surgettiva si dice **genere** della curva liscia proiettiva  $X$ .*

In altri termini, il genere di una curva liscia  $X$  è il più piccolo intero  $g$  tale che  $h^0(X, D) > 0$  per ogni divisore  $D$  di grado  $g$ .

### 16.1 Il teorema di Riemann-Roch, prima parte

Sia  $X$  una curva liscia proiettiva fissata. Abbiamo dimostrato nel Teorema 14.4.7 che per ogni coppia di divisori  $D, E$  su  $X$ , con  $E$  effettivo, vale la disuguaglianza

$$h^0(X, D + E) \leq h^0(X, D) + \deg(E).$$

**Definizione 16.1.1.** *Sia  $D$  un divisore su una curva liscia proiettiva. Diremo che  $D$  è **quasispeciale** se esiste un divisore effettivo  $E$  tale che  $h^0(D + E) < h^0(D) + \deg(E)$ . Diremo che un divisore è **speciale** se è quasispeciale ed effettivo.*

**Definizione 16.1.2 (provvisoria).** *Da questo momento, fino alla Definizione 16.5.5, chiameremo **canonico** un divisore quasispeciale massimale (rispetto all'ordinamento naturale di  $\text{Div}(X)$ ).*

Si noti che un divisore linearmente equivalente ad un divisore quasispeciale (canonico) è ancora quasispeciale (canonico).

Ogni divisore di grado  $\leq -2$  è quasispeciale; se  $X = \mathbb{P}^1$  è vero anche il viceversa. Questa sezione è interamente dedicata alla dimostrazione del seguente Teorema.

**Teorema 16.1.3 (Riemann-Roch, prima parte).** *Sia  $X$  una curva liscia proiettiva irriducibile definita su un campo  $\mathbb{K}$  algebricamente chiuso. Allora:*

1. Il genere  $g(X)$  è ben definito, cioè  $\mu_s$  è surgettiva per  $s \gg 0$ .
2. Esiste un divisore canonico, che indicheremo con  $K \in \text{Div}(X)$ . Esso è unico a meno di equivalenza lineare e vale  $h^0(X, K) = g(X)$ ,  $\deg(K) = 2g(X) - 2$ .
3. Per ogni divisore  $D$  su  $X$  vale

$$h^0(X, D) - h^0(X, K - D) = \deg(D) + 1 - g(X).$$

Premettiamo alla dimostrazione alcuni risultati preliminari.

**Lemma 16.1.4.** *Ogni curva liscia proiettiva possiede divisori effettivi non speciali.*

*Dimostrazione.* Assumiamo per assurdo che  $X$  sia una curva liscia proiettiva in cui ogni divisore effettivo è speciale; possiamo allora trovare una catena infinita  $0 < D_1 < D_2 < \dots < D_n < \dots$  di divisori effettivi tali che  $h^0(X, D_n) \leq \deg(D_n) - n$  per ogni  $n$ . Prendiamo un qualsiasi morfismo regolare surgettivo  $\phi: X \rightarrow \mathbb{P}^1$  e per ogni divisore  $D = \sum n_i x_i$  su  $X$  denotiamo  $\phi_*(D) = \sum n_i \phi(x_i) \in \text{Div}(\mathbb{P}^1)$ . Definiamo per ogni  $n > 0$  il divisore  $Q_n = \phi^* \phi_* D_n$ . Se  $d$  è il grado del morfismo  $\phi$  e  $d_n$  il grado del divisore  $D_n$ , allora  $Q_n - D_n$  è un divisore effettivo di grado  $(d-1)d_n$  e quindi per il Teorema 14.4.7 vale  $h^0(X, Q_n) \leq h^0(X, D_n) + (d-1)d_n \leq dd_n - n$ . Sia  $g_1, \dots, g_d$  una base di  $\mathbb{K}(X)$  come  $\mathbb{K}(\phi) = \mathbb{K}(\mathbb{P}^1)$ -spazio vettoriale e sia  $G$  un divisore effettivo tale che  $g_1, \dots, g_d \in H^0(X, G)$  (ad esempio prendiamo  $G$  uguale alla somma dei divisori di polo delle  $g_i$ ). Di nuovo per il Teorema 14.4.7 si ha  $h^0(X, Q_n + G) \leq dd_n - n + \deg(G)$  per ogni  $n > 0$ . D'altra parte per ogni  $i$  vale  $g_i H^0(X, \phi_* D_n) \subset H^0(X, Q_n + G)$  e, siccome le  $g_i$  sono linearmente indipendenti, vale  $h^0(X, Q_n + G) \geq dh^0(X, \phi_* D_n) = d(d_n + 1)$ , che non è possibile per  $n \geq \deg(G)$ .  $\square$

Esiste un criterio di specialità basato sulle classi di ripartizione (cfr. [Ser1959],[Weil1982]).

**Definizione 16.1.5.** *Una **ripartizione** su una curva liscia irriducibile  $X$  è una applicazione di insiemi  $r: X \rightarrow \mathbb{K}(X)$  tale che  $\text{ord}_x(r(x)) \geq 0$  eccetto per al più un numero finito di punti  $x \in X$ .*

Denotiamo con  $R(X)$  il  $\mathbb{K}(X)$ -spazio vettoriale delle ripartizioni su  $X$  e identifichiamo  $\mathbb{K}(X)$  con il sottospazio delle ripartizioni costanti. Per ogni divisore  $D$  su  $X$  si definisce

$$R(X, D) = \{r \in R(X) \mid \text{mult}_x(D) + \text{ord}_x(r(x)) \geq 0 \text{ per ogni } x \in X\}.$$

Per ogni  $f \in \mathbb{K}(X)$  vale  $fR(X, D) = R(X, D - \text{div}(f))$  e quindi  $R(X, D)$  è uno spazio vettoriale su  $\mathbb{K}$  ma non su  $\mathbb{K}(X)$ ; notiamo infine che  $R(X, D) \cap \mathbb{K}(X) = H^0(X, D)$ .

Una classe di ripartizione è un elemento del  $\mathbb{K}$ -spazio vettoriale

$$H^1(X, D) = \frac{R(X)}{R(X, D) + \mathbb{K}(X)}.$$

In altri termini,  $H^0(X, D)$  e  $H^1(X, D)$  sono rispettivamente il nucleo ed il conucleo del morfismo di  $\mathbb{K}$ -spazi vettoriali  $R(X, D) \oplus \mathbb{K}(X) \xrightarrow{\delta} R(X)$  dato da  $\delta(r, f) = r - f^1$ .

**Lemma 16.1.6.** *Sia  $X$  una curva liscia proiettiva e  $D$  un divisore tale che  $H^1(X, D) \neq 0$ . Allora  $D$  è **quasispeciale**.*

*Dimostrazione.* Basta dimostrare che esiste un punto  $p \in X$  ed un intero positivo  $h$  tale che  $H^0(X, D + hp) = H^0(X, D + (h-1)p)$ . Per ogni  $r \in R(X)$  definiamo il numero naturale

<sup>1</sup> Osservazione per gli esperti: la fascificazione di  $\delta$  è una risoluzione fiacca del fascio invertibile  $\mathcal{O}(D)$ .



$$n(r, D) = - \sum_{p \in X} \min(0, \text{ord}_p(r(p)) + \text{mult}_p(D)),$$

osservando che  $r \in R(X, D)$  se e soltanto se  $n(r, D) = 0$ . Sia  $r \notin R(X, D) + \mathbb{K}(X)$  una ripartizione che minimizza  $n(r, D)$  e scegliamo un punto  $p \in X$  tale che l'intero  $h = -(\text{ord}_p(r(p)) + \text{mult}_p(D))$  sia positivo. Supponiamo per assurdo  $H^0(X, D + hp) \neq H^0(X, D + (h-1)p)$  e scegliamo una funzione razionale  $f \in H^0(X, D + hp) - H^0(X, D + (h-1)p)$ . Allora vale  $\text{ord}_p(f) = -\text{mult}_p(D) - h = \text{ord}_p(r(p))$  ed esiste un'unica costante  $\alpha \in \mathbb{K}$  tale che  $\text{ord}_p(r(p) - \alpha f) > \text{ord}_p(r(p))$  e quindi

$$\min(0, \text{ord}_p(r(p) - \alpha f) + \text{mult}_p(D)) > \min(0, \text{ord}_p(r(p)) + \text{mult}_p(D)).$$

Se  $q \neq p$ , allora  $\text{ord}_q(f) + \text{mult}_q(D) \geq 0$  e quindi valgono le due disuguaglianze

$$\text{ord}_q(r(q) - \alpha f) \geq \min(\text{ord}_q(r(q)), -\text{mult}_q(D)) \quad e$$

$$\min(0, \text{ord}_q(r(q) - \alpha f) + \text{mult}_q(D)) \geq \min(0, \text{ord}_q(r(q)) + \text{mult}_q(D)).$$

Sommando si ottiene  $n(r - \alpha f, D) < n(r, D)$ , in contraddizione con la scelta di  $r$ .  $\square$

Se  $D_1 \leq D_2$  sono divisori su una curva  $X$ , allora  $R(X, D_1) + \mathbb{K}(X) \subset R(X, D_2) + \mathbb{K}(X)$  ed esiste una proiezione naturale  $H^1(X, D_1) \rightarrow H^1(X, D_2)$ . Il prossimo lemma mostrerà che la dimensione del nucleo è finita e non supera  $\text{deg}(D_2 - D_1)$ .

**Lemma 16.1.7.** *Per ogni divisore  $D$  e per ogni punto  $p \in X$  esiste una successione esatta di  $\mathbb{K}$ -spazi vettoriali*

$$0 \longrightarrow H^0(X, D) \longrightarrow H^0(X, D + p) \xrightarrow{\alpha} \mathbb{K} \xrightarrow{\bar{\beta}} H^1(X, D) \longrightarrow H^1(X, D + p) \longrightarrow 0.$$

*Dimostrazione.* Denotiamo  $h = \text{mult}_p(D)$  e sia  $t$  un parametro locale in  $p$ . Per ogni  $f \in H^0(X, D + p)$  si pone  $\alpha(f) = a$ , dove  $a$  è l'unica costante tale che  $\text{ord}_p(f - at^{-(h+1)}) \geq -h$ . Se  $a \in \mathbb{K}$ , allora si definisce  $\bar{\beta}(a)$  come la classe della ripartizione  $\beta(a): X \rightarrow \mathbb{K}(X)$  che vale 0 per  $q \neq p$  e  $at^{-(h+1)}$  nel punto  $p$ . L'esattezza della successione in  $H^0(X, D)$ ,  $H^0(X, D + p)$  e  $H^1(X, D + p)$  è banale. Se  $f \in H^0(X, D + p)$ , allora  $\beta(\alpha(f)) - f \in R(X, D)$  e questo implica che  $\beta(\alpha(f)) \in R(X, D) + \mathbb{K}(X)$  e quindi che  $\bar{\beta} \circ \alpha = 0$ . Osserviamo che il  $\mathbb{K}$ -spazio vettoriale  $R(X, D + p)/R(X, D)$  ha dimensione 1 ed è generato da  $\beta(1)$ : quindi  $\bar{\beta}$  induce un'applicazione surgettiva fra  $\mathbb{K}$  e il nucleo della proiezione  $H^1(X, D) \rightarrow H^1(X, D + p)$  che è isomorfo a  $(R(X, D + p) + \mathbb{K}(X))/(R(X, D) + \mathbb{K}(X))$ . Rimane da dimostrare che, se  $\bar{\beta}(1) = 0$ , allora  $\alpha$  è surgettiva: ma se  $\beta(a) = r + f$ , con  $f \in \mathbb{K}(X)$  e  $r \in R(X, D)$ , allora necessariamente  $f \in H^0(X, D + p)$  e  $\alpha(f) = a$ .  $\square$

**Teorema 16.1.8.** *Per ogni divisore  $D$  su una curva liscia proiettiva  $X$  lo spazio vettoriale  $H^1(X, D)$  ha dimensione finita e vale*

$$h^0(X, D) - h^1(X, D) = \text{deg}(D) + 1 - h^1(X, 0),$$

dove  $h^1(X, D) = \dim_{\mathbb{K}} H^1(X, D)$ .

*Dimostrazione.* Sia  $E$  è un divisore effettivo non speciale; abbiamo già allora dimostrato che  $h^1(E + F) = 0$  per ogni divisore effettivo  $F$ . Per la successione esatta del Lemma 16.1.7, per ogni punto  $p$  il nucleo di  $H^1(X, E + F - p) \rightarrow H^1(X, E + F)$  ha dimensione al più 1 e quindi per induzione sul grado si ottiene  $h^1(X, E + F - H) \leq \text{deg}(H)$  per ogni coppia di divisori effettivi  $F, H$ . In particolare  $h^1(0) \leq \text{deg}(E)$  e quindi il teorema è vero per  $D = 0$ . Possiamo raggiungere ogni divisore da 0 in un numero finito di passi, ogni volta aggiungendo o togliendo un punto. Per la successione esatta, ad ogni passo la quantità  $h^0(X, D) - h^1(X, D) - \text{deg}(D)$  resta costante.  $\square$

**Corollario 16.1.9.** *Un divisore  $D$  su una curva liscia proiettiva  $X$  è quasispeciale se e soltanto se  $H^1(X, D) \neq 0$ .*

*Dimostrazione.* Per il Lemma 16.1.6, se  $H^1(X, D) \neq 0$ , allora  $D$  è quasispeciale. Se invece  $H^1(X, D) = 0$ , allora per ogni divisore effettivo  $E$  vale  $H^1(X, D + E) = 0$  e dal Teorema 16.1.8 segue che  $h^0(X, D + E) - h^0(X, D) = \deg(E)$ .  $\square$

**Corollario 16.1.10.** *Ogni curva liscia proiettiva  $X$  possiede divisori canonici. Se  $K$  è un divisore canonico su  $X$ , allora  $h^1(X, K) = 1$ .*

*Dimostrazione.* Per dimostrare l'esistenza è sufficiente provare che esiste un intero  $N$  tale che ogni divisore quasispeciale ha grado minore o uguale a  $N$ . Scegliamo un divisore effettivo non speciale  $E$  e poniamo  $N = \deg(E) + h^1(0)$ . Se un divisore  $D$  ha grado maggiore o uguale ad  $N$ , allora per il Teorema 16.1.8 si ha  $h^0(X, D - E) \geq 1 + \deg(D) - \deg(E) - h^1(X, 0) > 0$  e quindi esiste un divisore effettivo  $D_0$  linearmente equivalente a  $D - E$ . Ne consegue che  $D$  è linearmente equivalente al divisore non speciale  $E + D_0$ . Proviamo adesso che per ogni divisore canonico  $K$  vale  $h^1(X, K) = 1$ . Per il Corollario 16.1.9 si ha  $h^1(X, K) > 0$  e se fosse  $h^1(X, K) > 1$ , allora per ogni punto  $p \in X$  si avrebbe  $h^1(X, K + p) \neq 0$ , in contraddizione con la massimalità di  $K$ .  $\square$

Dal Teorema 16.1.8 segue in particolare che la dimensione  $h^1(X, D)$  è invariante per equivalenza lineare. Questo poteva essere dimostrato più semplicemente osservando che per ogni funzione razionale non nulla  $f \in \mathbb{K}(X)$ , la moltiplicazione  $f: R(X) \rightarrow R(X)$  è tale che  $fR(X, D) = R(X, D - \text{div}(f))$  e quindi induce un isomorfismo  $f: H^1(X, D) \rightarrow H^1(X, D - \text{div}(f))$ . Su tale circostanza si basa la possibilità di definire, per ogni coppia di divisori  $D_1, D_2$  il **prodotto cup**

$$H^0(X, D_1) \times H^1(X, D_2 - D_1) \xrightarrow{\cup} H^1(X, D_2).$$

Infatti se  $f \in H^0(X, D_1)$  e  $r \in H^1(X, D_2 - D_1)$ , allora  $fr \in H^1(X, D_2 - D_1 - \text{div}(f))$  e, poiché  $-D_1 - \text{div}(f) \leq 0$  possiamo definire  $f \cup r$  come l'immagine di  $fr$  mediante la proiezione  $H^1(X, D_2 - D_1 - \text{div}(f)) \rightarrow H^1(X, D_2)$ . Denotando con  $V^\vee = \text{Hom}(V, \mathbb{K})$  il duale di uno spazio vettoriale  $V$  su  $\mathbb{K}$ , ed identificando  $H^1(X, D)^\vee$  con lo spazio delle applicazioni  $\mathbb{K}$ -lineari  $\omega: R(X) \rightarrow \mathbb{K}$  tali che  $R(X, D) + \mathbb{K}(X) \subset \text{Ker}(\omega)$ , il prodotto cup è il duale del prodotto

$$H^0(X, D_1) \times H^1(X, D_2)^\vee \longrightarrow H^1(X, D_2 - D_1)^\vee, \quad (f, \omega) \mapsto f\omega,$$

dove  $f\omega: R(X) \rightarrow \mathbb{K}$  è definito come  $f\omega(r) = \omega(fr)$ . Notiamo che  $\text{Ker}(\omega) = f \text{Ker}(f\omega)$  e che  $H^0(X, D_1) \cdot R(X, D_2 - D_1) \subset R(X, D_2)$ .

**Definizione 16.1.11.** *Sia  $X$  una curva liscia. Definiamo  $J_X \subset R(X)^\vee$  come l'insieme delle applicazioni  $\mathbb{K}$ -lineari  $\phi: R(X) \rightarrow \mathbb{K}$  tali che  $\phi = 0$  su  $R(X, D) + \mathbb{K}(X)$  per qualche divisore  $D$ , dipendente da  $\phi$ .*

Equivalentemente, siccome  $H^1(X, D)^\vee \subset R(X)^\vee$ , l'insieme  $J_X$  è l'unione di tutti gli  $H^1(X, D)^\vee$  al variare di  $D \in \text{Div}(X)$ . Notiamo che  $J_X$  ha una struttura di  $\mathbb{K}(X)$ -spazio vettoriale compatibile con il duale del prodotto cup: la moltiplicazione per scalare è definita dalla formula

$$f\phi(r) = \phi(fr), \quad \phi \in J_X, \quad f \in \mathbb{K}(X), \quad r \in R(X).$$

**Lemma 16.1.12.** *Nelle notazioni precedenti,  $J_X$  è uno spazio vettoriale di dimensione 1 su  $\mathbb{K}(X)$ .*

*Dimostrazione.* Per ogni divisore  $D$  di grado  $\leq -2$  vale  $H^1(X, D) \neq 0$  e quindi  $J_X \neq 0$ . Supponiamo per assurdo che esistano  $\phi_1, \phi_2 \in J_X$  linearmente indipendenti su  $\mathbb{K}(X)$  e sia  $D$  un divisore tale che  $\phi_1, \phi_2 \in H^1(X, D)^\vee$ . Allora per ogni divisore  $E$  e per ogni coppia  $f_1, f_2 \in H^0(X, E) \subset \mathbb{K}(X)$  vale  $f_1\phi_1 + f_2\phi_2 \in H^1(X, D - E)^\vee$  e, siccome  $\phi_1, \phi_2$  sono indipendenti, ne consegue che  $2h^0(X, E) \leq h^1(X, D - E) \leq h^1(X, D) + \deg(E)$ . Facendo tendere il grado di  $E$  all'infinito otteniamo una contraddizione al Teorema 16.1.8.  $\square$

**Teorema 16.1.13 (Dualità di Serre).** *Sia  $K$  un divisore canonico su una curva liscia proiettiva  $X$ . Allora, per ogni divisore  $D$  su  $X$ , il prodotto cup*

$$H^0(X, D) \times H^1(X, K - D) \xrightarrow{\cup} H^1(X, K) \cong \mathbb{K}$$

*è una dualità di spazi vettoriali e quindi  $h^0(X, D) = h^1(X, K - D)$ .*

*Dimostrazione.* Sia  $\pi$  un generatore di  $H^1(X, K)^\vee \cong \mathbb{K}$ . Per il Lemma 16.1.12,  $\pi$  è un generatore di  $J_X$  come spazio vettoriale su  $\mathbb{K}(X)$  e quindi l'applicazione

$$\mathbb{K}(X) \rightarrow J_X, \quad f \mapsto f\pi,$$

è un isomorfismo di  $\mathbb{K}(X)$ -spazi vettoriali. Dovendo dimostrare che

$$H^0(X, D) \rightarrow H^1(X, K - D)^\vee, \quad f \mapsto f\pi,$$

è un isomorfismo, basta dimostrare che  $f\pi \in H^1(X, K - D)^\vee$  soltanto se  $f \in H^0(X, D)$ . Supponiamo che  $f\pi(r) = 0$  per ogni  $r \in R(X, K - D) + \mathbb{K}(X)$ ; per definizione  $f\pi(r) = \pi(fr)$  e quindi la condizione  $f\pi(r) = 0$  equivale a  $fr \in R(X, K) + \mathbb{K}(X)$ . Supponiamo per assurdo che  $\text{ord}_p(f) + \text{mult}_p(D) < 0$  per qualche punto  $p \in X$  e denotiamo  $a = \text{ord}_p(f)$ ,  $b = \text{mult}_p(D)$  e  $c = \text{mult}_p(K)$ . Siccome  $H^1(X, K + p) = 0$ , la successione esatta del Lemma 16.1.7 implica che, se  $t$  è un parametro locale in  $p$ , allora la ripartizione  $r$  definita da  $r(p) = t^{-(c+1)}$  e  $r(q) = 0$  se  $q \neq p$ , non appartiene a  $R(X, K) + \mathbb{K}(X)$  e quindi  $f\pi(r) \neq 0$ . Osserviamo però che  $-a - c - 1 \geq b - c$  e quindi la ripartizione  $f^{-1}r$  appartiene a  $R(X, K - D)$ , in contraddizione con le ipotesi.  $\square$

**Lemma 16.1.14.** *Sia  $X$  una curva liscia proiettiva. Allora l'applicazione*

$$\mu_s: X^s \rightarrow \text{Cl}^s(X), \quad \mu_s(p_1, \dots, p_s) = p_1 + \dots + p_s$$

*è surgettiva se e solo se  $s \geq h^1(X, 0)$  e quindi il genere  $g(X)$  è ben definito ed è uguale a  $h^0(X, K) = h^1(X, 0)$ .*

*Dimostrazione.* Per definizione  $\mu_s$  è surgettiva se e solo se  $h^0(X, D) > 0$  per ogni divisore  $D$  di grado  $s$ . Se  $\deg(D) \geq h^1(X, 0)$ , allora per 16.1.8 si ha  $h^0(X, D) \geq \deg(D) + 1 - h^1(X, 0) > 0$ . Supponiamo adesso  $s = h^1(X, 0) - 1$  e sia  $D_1$  un divisore non speciale di grado  $\geq s$ . Per il Teorema 16.1.8 vale  $h^0(X, D) = \deg(D) + 1 - h^1(X, 0) = \deg(D) - s$ . Se  $D_2$  è un generico divisore effettivo di grado  $\deg(D) - s$ , allora  $h^0(X, D_1 - D_2) = h^0(X, D_1) - \deg(D_2) = 0$ .  $\square$

*Dimostrazione (del Teorema 16.1.3).* Osserviamo innanzitutto che se  $K$  è un divisore canonico, per il Teorema 16.1.8 e per il Teorema 16.1.13, vale

$$\deg(K) = h^0(X, K) - h^0(X, 0) + g(X) - 1 = 2g(X) - 2.$$

Se  $K_1$  e  $K_2$  sono due divisori canonici, allora per la dualità di Serre vale  $h^0(X, K_1 - K_2) = h^1(X, K_2) = 1$  e perciò  $K_1 - K_2$  è linearmente equivalente ad un divisore effettivo di grado  $= \deg(K_1) - \deg(K_2) = 0$ . L'unico divisore effettivo di grado 0 è il divisore nullo e questo prova che  $K_1$  e  $K_2$  sono linearmente equivalenti. Sempre per il Teorema 16.1.13 si ha  $h^0(X, K) = h^1(X, 0)$  e basta applicare 16.1.8 e 16.1.14.  $\square$

**Esercizi**

**16.1.** Dimostrare che se  $X$  è una curva liscia e affine, allora  $H^1(X, D) = 0$  per ogni divisore  $D$ . (Sugg.: Esercizio 14.19.)

**16.2 Prime applicazioni di Riemann-Roch**

**Corollario 16.2.1 (Teorema di Riemann, 1857).** *Sia  $D$  un divisore effettivo non speciale su una curva liscia proiettiva di genere  $g$ . Allora vale  $\dim |D| = \deg(D) - g$ .*

*Dimostrazione.* Banale conseguenza del Teorema 16.1.3. □

**Corollario 16.2.2.** *Ogni curva liscia proiettiva di genere  $g$  è isomorfa ad una curva nondegenere in  $\mathbb{P}^{g+1}$  di grado  $2g + 1$ .*

*Dimostrazione.* Sia  $X$  la curva, prendiamo un qualsiasi divisore  $D$  di grado  $2g + 1$  e sia  $L = |D|$  il sistema lineare associato. Per Riemann-Roch vale  $\dim L = \deg(D) - g = g + 1$  e per ogni coppia di punti  $p, q$  vale  $\dim L(-p - q) = g - 1$ . Per la Proposizione 14.5.10 il morfismo associato  $\phi_L: X \rightarrow L^\vee$  è un isomorfismo sull'immagine. □

Ad esempio ogni curva di genere 2 si immerge in  $\mathbb{P}^3$  come una curva di grado 5. Mostriamo nell'Esercizio 16.9 che nessuna curva liscia in  $\mathbb{P}^3$  di grado  $\leq 4$  ha genere 2.

**Esercizi**

**16.2.** Provare che in una curva liscia proiettiva di genere  $g$  ogni divisore effettivo di grado  $d \leq g - 1$  è speciale, ogni divisore di grado  $d \geq 2g - 1$  non è speciale, mentre se il grado  $d$  è compreso tra  $g$  e  $2g - 2$ , allora l'applicazione  $\mu_d: X^d \rightarrow \text{Cl}^d(X)$  è surgettiva ed il sottoinsieme di  $\text{Cl}^d(X)$  corrispondente alle classi di equivalenza lineare di divisori speciali è un sottoinsieme proprio e non vuoto. (Osservazione: dello studio di tali sottoinsiemi si occupa la *teoria di Brill-Noether*, vedi [ACGH1984, Ch. IV]).

**16.3.** Sia  $X$  una curva liscia proiettiva di genere 1. Dimostrare che l'applicazione  $\mu_1: X \rightarrow \text{Cl}^1(X)$  è bigettiva e dedurre che per ogni punto  $o \in X$  esiste una struttura di gruppo abeliano su  $X$  che ha  $o$  come elemento neutro.

**16.3 Profilassi per caratteristiche positive**

In caratteristica 0 possiamo derivare, differenziare ed applicare Bertini-Sard senza paura. In caratteristica positiva questi sono comportamenti a rischio e bisogna prendere le necessarie precauzioni.

Per iniziare, diremo che un morfismo dominante di curve irriducibili  $\phi: X \rightarrow Y$  è *separabile*, oppure *inseparabile*, oppure *puramente inseparabile*, se l'estensione di campi  $\phi^*\mathbb{K}(Y) \subset \mathbb{K}(X)$  ha la medesima proprietà.

Ad esempio, in caratteristica  $p > 0$ , il **morfismo di Frobenius**  $F: \mathbb{P}^1 \rightarrow \mathbb{P}^1$ , definito in coordinate omogenee da  $[x_0, x_1] \mapsto [x_0^p, x_1^p]$ , è puramente inseparabile di grado  $p$ . Infatti, se  $t = x_1/x_0$  è la coordinata affine, allora  $\mathbb{K}(\mathbb{P}^1) = \mathbb{K}(t)$ ,  $F^*\mathbb{K}(t) = \mathbb{K}(t^p) = \mathbb{K}(t)^p$  e quindi l'estensione  $F^*\mathbb{K}(t) \subset \mathbb{K}(t)$  è puramente inseparabile.

**Proposizione 16.3.1.** *Sia  $\phi: X \rightarrow Y$  un morfismo regolare dominante di curve irriducibili definite su un campo di caratteristica  $p > 0$ . Allora l'estensione  $\phi^*\mathbb{K}(Y) \subset \mathbb{K}(X)$  è inseparabile se e solo se  $\phi^*\mathbb{K}(Y) \subset \mathbb{K}(X)^p$ .*

*Dimostrazione.* Abbiamo dimostrato (Proposizione 12.5.16) che l'estensione  $\mathbb{K}(X)^p \subset \mathbb{K}(X)$  è puramente inseparabile di grado  $p^{\dim X} = p$  e quindi, se  $\phi^*\mathbb{K}(Y) \subset \mathbb{K}(X)^p$ , allora  $\phi$  è inseparabile. Viceversa se esiste  $g \in \phi^*\mathbb{K}(Y) - \mathbb{K}(X)^p$ , allora, sempre per la Proposizione 12.5.16, l'estensione  $\mathbb{K}(g) \subset \mathbb{K}(X)$  è separabile e quindi sono separabili anche le estensioni  $\mathbb{K}(g) \subset \phi^*\mathbb{K}(Y)$  e  $\mathbb{K}(Y) \subset \mathbb{K}(X)$ .  $\square$

**Corollario 16.3.2.** *Sia  $X$  una curva liscia su un campo algebricamente chiuso  $\mathbb{K}$  di caratteristica  $p > 0$  e sia  $f \in \mathbb{K}(X)$  tale che  $\text{div}(f)$  non è divisibile per  $p$  nel gruppo  $\text{Div}(X)$ . Allora l'estensione  $\mathbb{K}(f) \subset \mathbb{K}(X)$  è separabile. In particolare se  $t \in \mathbb{K}(X)$  è un parametro locale in un punto, allora l'estensione  $\mathbb{K}(t) \subset \mathbb{K}(X)$  è separabile.*

*Dimostrazione.* Se  $f \in \mathbb{K}(X)^p$  allora  $\text{div}(f)$  è divisibile per  $p$  in  $\text{Div}(X)$ . Basta applicare la Proposizione 16.3.1.  $\square$

Possiamo generalizzare il morfismo di Frobenius  $F: \mathbb{P}^1 \rightarrow \mathbb{P}^1$  ad ogni curva liscia proiettiva  $X$ . Abbiamo infatti un'estensione di campi  $\mathbb{K}(X) \subset \mathbb{K}(X)^{\frac{1}{p}}$ , dove  $\mathbb{K}(X)^{\frac{1}{p}}$  è il campo delle radici  $p$ -esime di elementi di  $\mathbb{K}(X)$ . Siccome  $\mathbb{K}(X)$  è una estensione finitamente generata con grado di trascendenza 1 sul campo perfetto  $\mathbb{K}$ , il grado dell'estensione  $\mathbb{K}(X) \subset \mathbb{K}(X)^{\frac{1}{p}}$  è esattamente  $p$ . Per il Corollario 17.2.3 esiste una curva liscia proiettiva  $X_p$  tale che  $\mathbb{K}(X_p) = \mathbb{K}(X)^{\frac{1}{p}}$ . L'inclusione  $\mathbb{K}(X) \subset \mathbb{K}(X)^{\frac{1}{p}}$  induce un'applicazione razionale da  $X_p$  in  $X$  che, essendo  $X_p$  liscia e  $X$  proiettiva, si estende ad un morfismo regolare  $F: X_p \rightarrow X$ ; notiamo che per costruzione  $F^*\mathbb{K}(X) = \mathbb{K}(X_p)^p$  e quindi il morfismo di Frobenius è puramente inseparabile di grado  $p$ . Osserviamo infine che  $F: X_p \rightarrow X$  è bigettivo: infatti è surgettivo per motivi di dimensione, mentre  $F(x) = F(y)$  se e solo se  $f(x) = f(y)$  per ogni  $f \in F^*\mathbb{K}(X)$ . D'altra parte se  $x, y$  sono punti distinti di  $X_p$  possiamo sempre trovare una funzione razionale  $g \in \mathbb{K}(X_p)$  tale che  $g(x) = 0$ ,  $g(y) = \infty$  e quindi  $g^p(x) = 0$ ,  $g^p(y) = \infty$ .

*Osservazione 16.3.3.* In generale  $X$  e  $X_p$  non sono isomorfe come curve su  $\mathbb{K}$ . Dimostriamo però (Esercizio 16.20) che hanno lo stesso genere.

**Corollario 16.3.4.** *In caratteristica  $p > 0$ , un morfismo dominante di curve lisce proiettive  $\phi: Y \rightarrow X$  è inseparabile se e solo se esiste una fattorizzazione*

$$\phi: Y \xrightarrow{\psi} X_p \xrightarrow{F} X,$$

dove  $F$  è il morfismo di Frobenius.

*Dimostrazione.* Immediata conseguenza della Proposizione 16.3.1.  $\square$

Ricordiamo che il grado di un morfismo dominante di curve irriducibili  $\phi: X \rightarrow Y$  è per definizione uguale al grado della corrispondente estensione di campi di funzioni razionali, ossia  $\text{deg}(\phi) = [\mathbb{K}(X) : \phi^*\mathbb{K}(Y)]$ .

**Definizione 16.3.5.** *Il **grado separabile** ed il **grado inseparabile** di un morfismo dominante  $\phi: X \rightarrow Y$  di curve irriducibili sono definiti rispettivamente come*

$$\text{deg}_s(\phi) = [\mathbb{K}(X) : \phi^*\mathbb{K}(Y)]_s, \quad \text{deg}_i(\phi) = [\mathbb{K}(X) : \phi^*\mathbb{K}(Y)]_i.$$

## 16.4 Differenziali razionali su curve lisce

**Definizione 16.4.1.** *Sia  $X$  una varietà quasiproiettiva irriducibile su un campo algebricamente chiuso  $\mathbb{K}$ . Un **differenziale razionale** su  $X$  è un elemento di  $\Omega_X = \Omega_{\mathbb{K}(X)/\mathbb{K}}$ .*

Il Corollario 12.6.3 implica che, per ogni varietà irriducibile di dimensione  $d$ , esiste una base di trascendenza  $t_1, \dots, t_d$  tale che l'estensione  $\mathbb{K}(t_1, \dots, t_d) \subset \mathbb{K}(X)$  è algebrica separabile e quindi, per il Lemma 15.2.5,  $dt_1, \dots, dt_d$  è una base di  $\Omega_X$  come  $\mathbb{K}(X)$ -spazio vettoriale.

**Definizione 16.4.2.** Sia  $\omega \in \Omega_X$  un differenziale razionale su  $X$  e sia  $p \in X$ . Diremo che  $\omega$  è **regolare** in  $p$  se esistono  $f_1, \dots, f_n, g_1, \dots, g_n \in \mathcal{O}_{p,X} \subset \mathbb{K}(X)$  tali che  $\omega = \sum f_i dg_i$ . In altre parole  $\omega$  è regolare in  $p$  se appartiene all'immagine dell'applicazione naturale  $\Omega_{\mathcal{O}_{p,X}/\mathbb{K}} \rightarrow \Omega_X$ . Per ogni aperto  $U$  indicheremo con  $\Omega_X(U)$  lo  $\mathcal{O}_X(U)$ -modulo dei differenziali regolari in ogni punto di  $U$ .

Notiamo che per ogni differenziale razionale  $\omega$ , l'insieme dei punti dove  $\omega$  è regolare è un aperto denso di  $X$ .

Siano  $X$  una curva liscia e  $t$  un parametro locale in un suo punto. Per il Corollario 16.3.2 l'estensione  $\mathbb{K}(t) \subset \mathbb{K}(X)$  è separabile e quindi il differenziale  $dt$  genera  $\Omega_X$  come  $\mathbb{K}(X)$ -spazio vettoriale. In particolare per ogni  $f \in \mathbb{K}(X)$  esiste un'unica funzione razionale  $\frac{df}{dt}$  tale che  $df = \frac{df}{dt} dt$ . Segue dalla regola di Leibniz che se  $f = P(t)$  è un polinomio in  $t$ , allora  $\frac{df}{dt} = P'(t)$ .

**Lemma 16.4.3.** Sia  $X$  una curva liscia e sia  $t$  un parametro locale in  $x \in X$ . Allora per ogni  $f \in \mathcal{O}_{x,X}$  vale  $\frac{df}{dt} \in \mathcal{O}_{x,X}$ . In particolare se  $s$  è un altro parametro locale in  $x$ , allora  $\frac{ds}{dt}$  è invertibile in  $\mathcal{O}_{x,X}$ .

*Dimostrazione.* (vedi anche [Hart1977, II.8.8]) Sia  $U$  un intorno affine di  $x$  e siano  $x_1, \dots, x_n$  generatori di  $\mathcal{O}_X(U)$  come  $\mathbb{K}$ -algebra. Per ogni  $g \in \mathcal{O}_{x,X}$  esistono polinomi  $P, Q$  nelle  $x_i$  tali che  $Q(x) \neq 0$  e  $g = PQ^{-1}$ . Differenziando si ottiene  $dg = Q^{-2} \sum G_i dx_i$ , dove ogni  $G_i$  è un polinomio nelle variabili  $x_1, \dots, x_n$ . Denotando con  $a = \min_i \left\{ \text{ord}_x \left( \frac{dx_i}{dt} \right) \right\}$ ,

allora per ogni  $g \in \mathcal{O}_{x,X}$  vale  $\text{ord}_x \left( \frac{dg}{dt} \right) \geq a$ . Siano ora  $f \in \mathcal{O}_{x,X}$  e  $b$  un intero positivo tale che  $b+a > 0$ , esiste allora un polinomio  $P(t)$  ed una  $g \in \mathcal{O}_{x,X}$  tale che  $f = P(t) + t^b g$ ; basta adesso osservare che la derivata rispetto a  $t$  di  $P(t) + t^b g$  è regolare in  $x$ . Se  $s$  è un altro parametro locale, allora  $dt = \frac{dt}{ds} ds$  e quindi  $\frac{dt}{ds} = \left( \frac{ds}{dt} \right)^{-1}$ .  $\square$

**Lemma 16.4.4.** Siano  $X$  una curva liscia,  $t$  un parametro locale in un suo punto  $x$  e  $f$  una funzione razionale su  $X$ . Allora il differenziale  $f dt$  è regolare in  $x$  se e soltanto se  $f$  è regolare in  $x$ .

*Dimostrazione.* Se  $f$  è regolare allora  $f dt$  è regolare per definizione. Viceversa se  $f dt = \sum f_i dg_i$ , con  $f_i, g_i \in \mathcal{O}_{x,X}$ , allora  $f = \sum f_i \frac{dg_i}{dt}$  e la tesi segue dal Lemma 16.4.3.  $\square$

Se  $\omega \in \Omega_X$  e  $t$  è un parametro locale in un punto  $x \in X$ , allora esiste un'unica funzione razionale  $f$  tale che  $\omega = f dt$ . Si definisce **l'ordine di  $\omega$  in  $x$**  mediante la formula  $\text{ord}_x(\omega) = \text{ord}_x(f)$ . Una semplice applicazione dei lemmi precedenti mostra che tale definizione non dipende dalla scelta del parametro locale e che  $\text{ord}_x(\omega) \geq 0$  se e soltanto se  $\omega$  è regolare in  $x$ .

**Lemma 16.4.5.** Sia  $\omega$  un differenziale razionale non nullo su una curva liscia irriducibile. Allora  $\text{ord}_x(\omega) = 0$  eccetto al più un numero finito di punti.

*Dimostrazione.* Basta chiaramente dimostrare il lemma per il differenziale  $dt$  di un parametro locale  $t$ . Sia  $U$  un aperto affine di  $X$  nel quale  $t$  è regolare: siccome  $X - U$  è finito basta dimostrare che  $dt$  possiede un numero finito di zeri in  $U$ . Se  $U \subset \mathbb{A}^n$  chiuso irriducibile con  $x_1, \dots, x_n$  coordinate affini. A meno di permutazioni negli indici possiamo supporre che esista  $s \leq n$  tale che  $dx_i = 0$  se e soltanto se  $i > s$ . Se  $p = (a_1, \dots, a_n) \in U$ , le funzioni  $x_i - a_i$ , per  $i = 1, \dots, n$ , generano l'ideale massimale e quindi, essendo  $d(x_i - a_i) = dx_i = \frac{dx_i}{dt} dt$ , esiste un intero  $j \leq s$  tale che  $x_j - a_j$  è un parametro locale in  $p$ . Dunque gli zeri di  $dt$  in  $U$  sono contenuti nell'unione dei poli delle funzioni razionali  $\frac{dx_i}{dt}$ , con  $i = 1, \dots, s$ , e tali poli sono in numero finito.  $\square$

Ad ogni differenziale razionale  $\omega$  su di una curva liscia  $X$  possiamo associare un divisore

$$\operatorname{div}(\omega) = \sum \operatorname{ord}_p(\omega)p.$$

Se  $f \in \mathbb{K}(X)$ , allora  $\operatorname{div}(f\omega) = \operatorname{div}(f) + \operatorname{div}(\omega)$  e quindi i divisori dei differenziali razionali sono tutti linearmente equivalenti tra loro. Ogni morfismo  $\phi: X \rightarrow Y$  regolare e dominante di curve lisce induce un morfismo  $\phi^*: \Omega_Y \rightarrow \Omega_X$  che è  $\mathbb{K}(Y)$ -lineare e tale che, per ogni  $f \in \mathbb{K}(Y)$  vale  $\phi^*(df) = d\phi^*(f)$ . Per il Lemma 15.2.5 se  $\phi$  è separabile, allora  $\phi^*$  è iniettivo. Sia ora  $\omega \in \Omega_Y$  e  $x \in X$  un punto fissato; vogliamo determinare  $\operatorname{ord}_x(\phi^*\omega)$ . Indichiamo con  $e = \operatorname{mult}_x(\phi)$ ,  $y = \phi(x)$ ,  $a = \operatorname{ord}_y(\omega)$  e siano  $t$  un parametro locale in  $x$  ed  $s$  parametro locale in  $y$ . Questo implica che si ha  $\omega = gs^a ds$ , con  $g(y) \neq 0$  e  $\phi^*(s) = ht^e$ , con  $h(x) \neq 0$ . Di conseguenza, identificando per semplicità notazionale  $\mathbb{K}(Y)$  con  $\phi^*\mathbb{K}(Y)$ , si ha

$$\phi^*(\omega) = gs^a \phi^*(ds) = gh^a t^{ae} d(ht^e) = gh^a t^{ae} \left( et^{e-1} h + t^e \frac{dh}{dt} \right) dt$$

e quindi  $\operatorname{ord}_p(\phi^*\omega) \geq ae + e - 1$  e vale = se e soltanto se  $e$  non è divisibile per la caratteristica del campo. Per il Lemma 16.4.5, se  $\omega \neq 0$ , allora  $\phi^*\omega \neq 0$  se e soltanto se la molteplicità di  $\phi$  è uguale a 1 eccetto un numero finito di punti.

**Proposizione 16.4.6.** *Sia  $i$  il grado di inseparabilità di un morfismo regolare dominante  $\phi$  di curve lisce proiettive. Allora  $\operatorname{mult}_x(\phi) \geq i$  per ogni  $x \in X$  e vale = eccetto un numero finito di punti.*

*Dimostrazione.* Se  $i = 1$  allora  $\phi$  è separabile allora  $\phi^*$  è iniettiva e la tesi segue dalle osservazioni precedenti. Supponiamo quindi che  $\phi: X \rightarrow Y$  abbia grado di inseparabilità  $i > 1$  e sia  $p > 0$  la caratteristica del campo. In generale se  $\psi: Y \rightarrow Z$  è un morfismo dominante di curve lisce, allora vale la formula  $\operatorname{mult}_x(\psi\phi) = \operatorname{mult}_x(\phi) \operatorname{mult}_{\phi(x)}(\psi)$ . Per il Corollario 16.3.4 esiste una fattorizzazione

$$\phi: X \xrightarrow{\psi} Y_p \xrightarrow{F} Y,$$

dove  $F$  è il morfismo di Frobenius e, per induzione sul grado possiamo supporre che la proposizione sia vera per il morfismo  $\psi$ . Basta adesso ricordare che  $F$  è puramente inseparabile di grado  $p$  ed ha molteplicità uguale a  $p$  in ogni punto.  $\square$

## Esercizi

**16.4.** Sia  $L$  un sistema lineare di divisori di grado  $d$  su una curva liscia proiettiva definita su un campo di caratteristica 0 oppure  $> d$ . Si assuma  $L$  di dimensione positiva e senza punti base. Dimostrare che il generico divisore in  $L$  non ha punti di molteplicità  $\geq 2$ .

### 16.5 Il teorema dei residui e seconda parte del teorema di Riemann-Roch

Sia  $X$  una curva liscia proiettiva irriducibile su un campo  $\mathbb{K}$  algebricamente chiuso e denotiamo con  $K = \mathbb{K}(X)$  il campo delle funzioni razionali su  $X$ . Se  $S \subset X$  è un qualsiasi sottoinsieme, allora definiamo  $\mathcal{O}_X(S) = \cap_{x \in S} \mathcal{O}_{x,X} \subset \mathbb{K}(X)$ : per meglio dire,  $\mathcal{O}_X(S)$  è la sottoalgebra delle funzioni razionali che sono regolari in ogni punto di  $S$ . Notiamo che se  $S = X$ , allora  $\mathcal{O}_X(X) = \mathbb{K}$ .

**Lemma 16.5.1.** *Nelle notazioni della Sezione 15.3, per ogni funzione razionale  $f \in K$  ed ogni sottoinsieme  $S \subset X$  vale  $f\mathcal{O}_X(S) \prec \mathcal{O}_X(S)$  ed è quindi possibile definire il residuo*

$$\text{res}_S: \Omega_X \rightarrow \mathbb{K} \quad \text{res}_S := \text{res}_{\mathcal{O}_X(S)}^K.$$

*Dimostrazione.* Osserviamo prima che per ogni  $f \in K, x \in X$  vale  $f\mathcal{O}_{x,X} \prec \mathcal{O}_{x,X}$ . Infatti se  $f$  è regolare in  $x$  allora  $f\mathcal{O}_{x,X} \subset \mathcal{O}_{x,X}$ , mentre se  $f$  ha un polo di ordine  $h > 0$  in  $X$  e  $t$  è un parametro locale in  $x$ , allora  $f\mathcal{O}_{x,X} \subset \mathcal{O}_{x,X} + \mathbb{K}t^{-1} + \dots + \mathbb{K}t^{-h}$ . Se  $s_1, \dots, s_n \in S$  sono i punti dove  $f$  non è regolare e  $T = S - \{s_1, \dots, s_n\}$ , allora  $f\mathcal{O}_X(T) \subset \mathcal{O}_X(T)$  e  $f\mathcal{O}_{s_i,X} \prec \mathcal{O}_{s_i,X}$  per ogni  $i$ . Vale quindi

$$f\mathcal{O}_X(S) \subset \mathcal{O}_X(T) \cap_i f\mathcal{O}_{s_i,X} \prec \mathcal{O}_X(T) \cap_i \mathcal{O}_{s_i,X} = \mathcal{O}_X(S).$$

□

Se  $S = \{x\}$  è un punto, scriveremo  $\text{res}_x = \text{res}_S$ . Siccome  $f\mathcal{O}_{x,X} \subset \mathcal{O}_{x,X}$  se e soltanto se  $f$  è regolare in  $x$ , dal Lemma 16.4.4 e dalla Proposizione 15.3.9 segue immediatamente che se  $\omega$  è un differenziale razionale che è regolare in  $x$ , allora  $\text{res}_x(\omega) = 0$ . Sempre per la Proposizione 15.3.9, se  $t$  è un parametro locale in  $x$ , allora vale

$$\text{res}_x(t^n dt) = \begin{cases} 1 & \text{se } n = -1 \\ 0 & \text{altrimenti} \end{cases}$$

All'estremo opposto, se  $S = X$ , allora  $\mathcal{O}_X(X) = \mathbb{K} \sim 0$  e vale  $\text{res}_X = \text{res}_{\mathbb{K}}^K = \text{res}_0^K \equiv 0$ .

**Teorema 16.5.2.** *Per ogni differenziale  $\omega \in \Omega_X$  ed ogni sottoinsieme non vuoto  $S \subset X$  vale*

$$\text{res}_S(\omega) = \sum_{x \in S} \text{res}_x(\omega).$$

*Dimostrazione.* Notiamo, prima di proseguire, che  $\omega$  è regolare in tutti i punti di  $S$  eccetto al più un numero finito e quindi la formula dell'enunciato ha perfettamente senso. Sia  $R(S) \subset R(X)$  il  $K$ -sottospazio vettoriale delle ripartizioni  $r \in R(X)$  su  $X$  tali che  $r(x) = 0$  se  $x \notin S$ . L'inclusione  $S \subset X$  induce una proiezione naturale  $R(X) \xrightarrow{p} R(S)$ . Identifichiamo  $K$  con il sottospazio di  $R(S)$  delle ripartizioni costanti su  $S$ , per il Lemma 15.3.8 si ha  $\text{res}_S = \text{res}_{\mathcal{O}_X(S)}^{R(S)}$ . Per ogni divisore  $D \in \text{Div}(X)$  si pone  $R(S, D) = p(R(X, D)) \subset R(S)$ ; si noti che  $\mathcal{O}_X(S) = K \cap R(S, 0)$  e quindi per il Corollario 15.3.12

$$\text{res}_S = \text{res}_K^{R(S)} + \text{res}_{R(S,0)}^{R(S)} - \text{res}_{R(S,0)+K}^{R(S)}.$$

Inoltre  $K \subset R_S$  è un  $K$ -sottomodulo e quindi  $\text{res}_K^{R(S)} \equiv 0$ . La proiezione  $p$  induce una applicazione surgettiva  $R(X)/(R(X, 0) + K) \rightarrow R(S)/(R(S, 0) + K)$  dalla quale si deduce che  $R(S, 0) + K$  ha codimensione finita in  $R(S)$  e quindi  $\text{res}_{R(S,0)+K}^{R(S)} = \text{res}_{R(S)}^{R(S)} \equiv 0$ . Resta quindi da dimostrare la formula



$$\operatorname{res}_{R(S,0)}^{R(S)}(\omega) = \sum_{x \in S} \operatorname{res}_{\mathcal{O}_{x,X}}^{R(S)}(\omega) = \sum_{x \in S} \operatorname{res}_x(\omega).$$

Siano  $f, g \in K$  tali che  $\omega = fdg$  e sia  $T \subset S$  il sottoinsieme dei punti dove  $f$  e  $g$  sono regolari. Allora  $S - T$  è un insieme finito di punti e vale  $R(S, 0) = R(T, 0) \oplus \bigoplus_{x \in S-T} \mathcal{O}_{x,X}$ . Per il Corollario 15.3.12

$$\operatorname{res}_{R(S,0)}^{R(S)}(fdg) = \operatorname{res}_{R(T,0)}^{R(S)}(fdg) + \sum_{x \in S-T} \operatorname{res}_{\mathcal{O}_{x,X}}^{R(S)}(fdg)$$

e siccome  $fR(T, 0) + gR(T, 0) \subset R(T, 0)$ , per la Proposizione 15.3.9, il primo termine della sommatoria è nullo e la dimostrazione è conclusa.  $\square$

**Corollario 16.5.3 (Teorema dei residui).** *Sia  $\omega$  un differenziale razionale su curva liscia proiettiva  $X$ . Allora  $\sum_{x \in X} \operatorname{res}_x(\omega) = 0$ .*

*Dimostrazione.* Per il Teorema 16.5.2 tale somma è uguale a  $\operatorname{res}_X(\omega) = 0$ .  $\square$

**Teorema 16.5.4.** *Su una curva liscia proiettiva, un divisore è canonico se e soltanto se è il divisore di un differenziale razionale.*

*Dimostrazione.* Per ogni differenziale  $\omega \in \Omega_X$  definiamo una applicazione  $\mathbb{K}$ -lineare

$$\hat{\omega}: R(X) \rightarrow \mathbb{K}, \quad \hat{\omega}(r) = \sum_{x \in X} \operatorname{res}_x(r(x)\omega).$$

Osserviamo che  $\hat{\omega}(r)$  è ben definita poiché  $r(x)\omega$  è regolare in  $x$  eccetto al più per un numero finito di punti  $x \in X$ . Per il teorema dei residui, il morfismo  $\hat{\omega}: R(X) \rightarrow \mathbb{K}$  si annulla sul sottospazio  $\mathbb{K}(X) \subset R(X)$ . Per definizione, una ripartizione  $r$  appartiene al sottospazio  $R(X, \operatorname{div}(\omega))$  se e solo se per ogni punto  $x \in X$  il differenziale  $r(x)\omega$  è regolare in  $x$ . Ne segue che  $\hat{\omega}$  si annulla su  $R(X, \operatorname{div}(\omega)) + \mathbb{K}(X)$  e quindi, nelle notazioni della Sezione 16.1, si ha  $\omega \in H^1(X, \operatorname{div}(\omega))^\vee \subset J_X$ . Abbiamo quindi definito un'applicazione

$$\Omega_X \rightarrow J_X, \quad \omega \mapsto \hat{\omega},$$

che risulta tautologicamente un omomorfismo iniettivo di  $\mathbb{K}(X)$ -spazi vettoriali. Siccome  $\Omega_X$  e  $J_X$  hanno dimensione 1, tale applicazione è un isomorfismo. Sia  $K$  un divisore canonico e sia  $\omega$  un differenziale non nullo tale che  $\hat{\omega} \in H^1(X, K)^\vee$ . Allora, siccome  $R(X, K) + \mathbb{K}(X)$  ha codimensione 1 deve necessariamente essere  $R(X, K) + \mathbb{K}(X) = \operatorname{Ker}(\hat{\omega})$ . Vogliamo dimostrare che  $K = \operatorname{div}(\omega)$ . Siano  $x \in X$  e  $t$  un parametro locale in  $x$ . Se  $h = \operatorname{mult}_x(K)$ , allora  $H^1(X, K + x) = 0$  e quindi la classe della ripartizione

$$r: \quad r(x) = t^{-h-1}, \quad r(y) = 0 \text{ se } y \neq x,$$

è una base di  $H^1(X, K)$ . Dunque  $\hat{\omega}(r_s) = \operatorname{res}_x(t^{-h-1}\omega) \neq 0$  e quindi necessariamente  $\operatorname{ord}_x(\omega) = h$ .  $\square$

Da questo momento ci dimenticheremo della Definizione 16.1.2 e, in virtù del Teorema 16.5.4, adatteremo la seguente Definizione 16.5.5.

**Definizione 16.5.5 (definitiva).** *Un divisore su una curva liscia proiettiva si dice canonico se è il divisore di un differenziale razionale.*

**Corollario 16.5.6.** *Sia  $X$  una curva liscia proiettiva e sia data per ogni  $x \in X$  un'applicazione  $\mathbb{K}$ -lineare  $s_x: \Omega_X \rightarrow \mathbb{K}$  con le seguenti proprietà:*

1.  $s_x(\omega) = 0$  se  $\omega$  è regolare in  $x$ .
2.  $\sum_{x \in X} s_x(\omega) = 0$  per ogni  $\omega \in \Omega_X$ .

Allora esiste una costante  $a \in \mathbb{K}$  tale che per ogni punto  $x$  vale  $s_x = a \operatorname{res}_x$ .

*Dimostrazione.* Ripetendo il ragionamento fatto nella dimostrazione del Teorema 16.5.4, si dimostra che le funzioni  $s_x$  possono essere utilizzate per costruire un isomorfismo  $\Omega_X \rightarrow J_X \subset R(X)^\vee$  e, siccome  $J_X$  ha dimensione 1 su  $\mathbb{K}(X)$ , esiste una funzione razionale  $f$  tale che per ogni  $x \in X$ , ogni  $\omega \in \Omega_X$  ed ogni  $r \in \mathbb{K}(X)$  vale  $s_x(r\omega) = \operatorname{res}_x(fr\omega)$ . Dalla proprietà 1) segue immediatamente che  $f$  non possiede poli e quindi è una funzione costante.  $\square$

**Corollario 16.5.7.** *Sia  $X$  una curva liscia proiettiva di genere  $g$ . Allora:*

1. Il divisore di un differenziale razionale su  $X$  ha grado  $2g - 2$ .
2. Il  $\mathbb{K}$ -spazio vettoriale dei differenziali razionali su  $X$  che sono regolari in ogni punto ha dimensione  $g$ .

*Dimostrazione.* Per il Teorema 16.5.4 il divisore di un differenziale è canonico. Sia  $\omega \neq 0$  un differenziale razionale fissato e  $f \in \mathbb{K}(X)$ , allora  $f\omega$  è regolare in ogni punto di  $X$  se e soltanto se  $f \in H^0(X, \operatorname{div}(\omega))$ .  $\square$

**Definizione 16.5.8.** *Un morfismo di curve lisce  $\phi: X \rightarrow Y$  si dice **docilmente ramificato** se per ogni  $x \in X$  la caratteristica del campo non divide  $\operatorname{mult}_x(\phi)$ .*

**Corollario 16.5.9 (Formula di Hurwitz).** *Sia  $\phi: X \rightarrow Y$  un morfismo separabile docilmente ramificato tra curve lisce proiettive, allora*

$$2g(X) - 2 = \deg(\phi)(2g(Y) - 2) + \sum_{x \in X} (\operatorname{mult}_x(\phi) - 1).$$

*Dimostrazione.* Se  $\omega \in \Omega_Y$  è un differenziale non nullo, allora  $\phi^*\omega \neq 0$  e vale

$$\operatorname{div}(\phi^*\omega) = \phi^* \operatorname{div}(\omega) + \sum_{x \in X} (\operatorname{mult}_x(\phi) - 1)x.$$

$\square$

Si noti che se  $\phi$  è separabile ma non docilmente ramificato vale comunque la relazione

$$\operatorname{div}(\phi^*\omega) = \phi^* \operatorname{div}(\omega) + \sum_{x \in X} e_x(\phi)x,$$

dove  $e_x(\phi)$  è detto **indice di ramificazione** di  $\phi$  in  $x$  ed è definito come  $e_x(\phi) = \operatorname{ord}_x(\phi^*(dt))$ , dove  $t$  è un parametro locale in  $\phi(x)$ . Notiamo che  $e_x(\phi) \geq \operatorname{mult}_x(\phi) - 1$  e vale  $>$  se e solo se la caratteristica del campo divide  $\operatorname{mult}_x(\phi)$ .

## Esercizi

**16.5 (Teorema di Lüroth).** Sia  $f: X \rightarrow Y$  un morfismo surgettivo di curve lisce proiettive. Dimostrare che  $g(X) \geq g(Y)$ . (Sugg.: se  $f$  non è separabile fattorizzare con il Frobenius.)

**16.6 (Teorema di Weber, 1878).** Dimostrare che in caratteristica 0 ogni applicazione razionale dominante tra due curve lisce proiettive dello stesso genere  $g > 1$  è un isomorfismo.

## 16.6 Curve iperellittiche ed applicazione canonica

In questa sezione  $X$  denoterà una curva liscia proiettiva di genere positivo e con  $|K|$  il sistema lineare completo dei divisori canonici. In questa sezione risulterà utile la versione di Riemann-Roch dove compaiono le dimensioni dei sistemi lineari completi, e cioè

$$\dim |D| - \dim |K - D| = \deg(D) + 1 - g,$$

dove si intende che  $\dim \emptyset = -1$ .

**Lemma 16.6.1.** *Sia  $X$  curva liscia proiettiva di genere  $g > 0$ . Allora il sistema lineare  $|K|$  non ha punti base.*

*Dimostrazione.* Bisogna dimostrare che  $\dim |K - p| = g - 2$  per ogni punto  $p \in X$ . Abbiamo dimostrato nella Proposizione 14.5.7 che per ogni divisore effettivo  $D$  vale  $\dim |D| < \deg(D)$  e quindi per Riemann-Roch vale  $\dim |K - p| = \dim |p| + g - 2 \leq g - 2$ .  $\square$

Quindi il sistema lineare  $|K|$  definisce un'applicazione regolare  $\phi_K: X \rightarrow \mathbb{P}^{g-1}$ . Se  $g \geq 2$ , allora l'immagine  $\phi_K(X)$  è una curva non degenere e quindi di grado  $d \geq g - 1$ . Inoltre il prodotto di  $d$  per il grado di  $\phi_K: X \rightarrow \phi_K(X)$  è uguale al grado del divisore canonico che è  $2g - 2$ .

**Definizione 16.6.2.** *Nelle notazioni precedenti, il morfismo  $\phi_K: X \rightarrow \mathbb{P}^{g-1}$  viene detto **applicazione canonica**. La curva  $X$  si dice **ellittica** se  $g = 1$  ed **iperellittica** se  $g > 1$  e l'applicazione canonica non è un isomorfismo sull'immagine.*

Ad esempio ogni curva di genere 2 è iperellittica: infatti in tal caso l'applicazione canonica  $\phi_K: X \rightarrow \mathbb{P}^1$  non può essere un isomorfismo. È possibile mostrare che per ogni genere  $> 2$  esistono sia curve iperellittiche che curve non iperellittiche.

**Lemma 16.6.3.** *Una curva liscia di genere  $\geq 2$  è iperellittica se e solo se contiene un divisore  $D$  di grado 2 tale che  $\dim |D| = 1$ .*

*Dimostrazione.* Per la Proposizione 14.5.10, l'applicazione canonica non è un isomorfismo sull'immagine se e solo se esistono  $p, q \in X$  tali che  $\dim |K - p - q| \geq g - 2$ . Per Riemann-Roch questa disuguaglianza è equivalente alla  $\dim |p + q| \geq 1$ .  $\square$

**Teorema 16.6.4 (Teorema di Clifford, prima parte).** *Sia  $D$  è un divisore speciale su una curva liscia proiettiva. Allora vale*

$$\dim |D| \leq \frac{1}{2} \deg(D).$$

*Dimostrazione.* Speciale significa che i sistemi lineari  $|D|$  e  $|K - D|$  sono non vuoti. Per il Lemma 14.5.4 e per il teorema di Riemann-Roch si ha

$$\dim |D| - \dim |K - D| = \deg(D) + 1 - g, \quad \dim |D| + \dim |K - D| \leq \dim |K| = g - 1.$$

Sommando membro a membro si ottiene  $2 \dim |D| \leq \deg(D)$ .  $\square$

**Lemma 16.6.5.** *Sia  $X$  una curva iperellittica di genere  $g$  e sia  $D$  un divisore su  $X$  di grado 2 tale che  $\dim |D| = 1$ . Allora ogni divisore speciale  $E$  tale che  $\deg(E) = 2 \dim |E|$  è somma di divisori di  $|D|$ . In particolare  $D$  è unico a meno di equivalenza lineare ed ogni divisore canonico è la somma di  $g - 1$  divisori del sistema lineare  $|D|$ .*

*Dimostrazione.* Denotiamo con  $d = \dim |E|$ , osservando che la specialità di  $E$  implica che  $0 \leq d \leq g - 1$ . Se  $d = 0$ , allora  $E = 0$  e non c'è nulla da dimostrare; supponiamo quindi  $d > 0$ . Per Riemann-Roch vale  $\dim |K - E| = g - 1 - \dim |E| = g - 1 - d$ . Sia  $p \in X$  un punto tale che  $\text{mult}_p(E) > 0$ ; dato che  $\dim |D - p| \geq 0$  esiste un punto  $q \in X$  tale che  $p + q \sim D$ : vogliamo dimostrare che il divisore  $E' = E - p - q$  è speciale e che  $\deg(E') = 2 \dim |E'|$ . Supponiamo per assurdo che  $E'$  non sia effettivo, allora  $q$  non è contenuto nel supporto di  $E - p$  e valgono le uguaglianze  $\sup(p + q, E) = E + q$ ,  $\inf(p + q, E) = p$ . Per la formula di Grassmann 14.4.11 si ha  $\dim |E + q| \geq \dim |E| + \dim |D| - \dim |p| = d + 1$ . Se  $d = g - 1$ , allora  $\deg(E + q) = 2g - 1$  e per Riemann-Roch vale  $\dim |E + q| = 2g - 1 + 1 - g - 1 = g - 1$ . Se invece  $d < g - 1$ , allora  $\dim |K - E| > 0$ ,  $|K - E - q| \neq \emptyset$ , il divisore  $E + q$  è speciale a per il Teorema di Clifford  $2 \dim |E + q| \leq 2d + 1$ . In entrambi i casi abbiamo provato che  $\dim |E + q| \leq d$ . Dunque  $E'$  è effettivo ed è anche speciale in quanto minore del divisore speciale  $E$ . Per il Teorema di Clifford si ha  $\dim |K - E'| \leq g - d$ , mentre per il Lemma 14.5.4 si ha  $\dim |K - E'| \geq \dim |K - E| + \dim |p + q| = g - d$ . Dunque  $\dim |K - E'| = g - d$  e per Riemann-Roch  $\dim |E'| = d - 1$ .  $\square$

La seconda parte del Lemma 16.6.5 ha una interessante interpretazione geometrica. Sia  $X$  una curva iperellittica e  $D$  un divisore tale che  $\deg(D) = 2$  e  $\dim |D| = 1$ . Denotiamo con  $\phi: X \rightarrow \mathbb{P}^1$  il morfismo di grado 2 indotto dal sistema lineare  $|D|$ . Per costruzione ogni divisore di  $|D|$  è della forma  $\phi^*(p)$  per qualche  $p \in \mathbb{P}^1$  e quindi  $|K| = L_\phi(g - 1)$ , cioè ogni divisore di  $|K|$  è della forma  $\phi^*(E)$ , con  $E$  divisore effettivo di grado  $g - 1$  in  $\mathbb{P}^1$ . Se  $v_{g-1}: \mathbb{P}^1 \rightarrow \mathbb{P}^{g-1}$  è la  $(g - 1)$ -esima immersione di Veronese, si ha che  $|K| = L_{v_{g-1}\phi}(1)$  e di conseguenza l'applicazione canonica è la composizione di  $\phi$  e  $v_{g-1}$ .

Un'altra conseguenza è che su ogni curva iperellittica esiste un unico sistema lineare  $g_2^1$  di dimensione 1 e tale che  $\deg(D) = 2$  per ogni  $D \in g_2^1$ . Chiameremo **pennello iperellittico** un tale sistema lineare.

**Teorema 16.6.6 (Teorema di Clifford, seconda parte).** *Sia  $D$  un divisore speciale su una curva liscia proiettiva tale che*

$$\dim |D| = \frac{1}{2} \deg(D).$$

*Allora  $D = 0$ , oppure  $D$  è un divisore canonico, oppure la curva è iperellittica e  $D$  è una somma di divisori del pennello iperellittico.*

*Dimostrazione.* Denotiamo con  $g$  il genere della curva. Se  $D$  ha grado 0, allora  $D = 0$ , mentre ogni divisore speciale di grado  $2g - 2$  è canonico. Per il Lemma 16.6.5 basta quindi dimostrare che se  $0 < \dim |D| < g - 1$ , allora la curva è iperellittica; dimostriamo questo fatto per induzione sul grado di  $D$ . Se  $\deg(D) = 2$  allora  $\dim |D| = 1$  è la curva è iperellittica. Supponiamo quindi  $\deg(D) \geq 4$ ; per ipotesi esiste un divisore effettivo  $E$  di grado positivo tale che  $D + E$  è canonico e per Riemann-Roch vale  $2 \dim |E| = \deg(E)$ . Scegliamo due punti  $p, q$  tali che  $\text{mult}_p(E) > 0$  e  $\text{mult}_q(E) = 0$ . Il sistema lineare  $|D - p - q|$  non è vuoto e quindi, a meno di sostituire  $D$  con un divisore linearmente equivalente, possiamo supporre  $D \geq p + q$ . Denotiamo con  $F = \inf(D, E)$ , allora  $\text{mult}_p(F) = 1$ ,  $\text{mult}_q(F) = 0$  e  $0 < F < D$ . I divisori  $F$  e  $D + E - F$  sono speciali e quindi, per l'ipotesi induttiva, basta dimostrare che  $\deg(F) \geq 2 \dim |F|$ . Per la formula di Grassmann 14.4.11 vale

$$g - 1 = \dim |D| + \dim |E| \leq \dim |F| + \dim |D + E - F|,$$

mentre per la prima parte del Teorema di Clifford si ha

$$\dim |F| + \dim |D + E - F| \leq \frac{1}{2} (\deg(F) + \deg(D + E - F)) = g - 1.$$

Mettendo insieme i pezzi si ricava  $2 \dim |F| = \deg(F)$ .  $\square$

**Esercizi**

**16.7.** Sia  $X \subset \mathbb{P}^2$  una curva liscia di grado  $d \geq 4$ . Provare che  $X$  non è iperellittica. (Sugg.: sia  $D \in L_X(d-3)$ , provare che  $\deg(D) = 2g - 2$ . Per il teorema del resto vale  $|D| = L_X(d-3)$  e quindi  $\dim |D| = g - 1$ . Dedurre che  $|K| = L_X(d-3)$ .)

**16.8.** Sia  $X$  una curva liscia di genere  $\geq 2$ . Provare che  $X$  è iperellittica se e solo se esiste un morfismo  $X \rightarrow \mathbb{P}^1$  di grado 2.

**16.9.** Dimostrare, senza l'aiuto della disuguaglianza di Castelnuovo, che se  $X \subset \mathbb{P}^n$  è una curva liscia nondegenere di grado  $d$  e  $d < 2n$ , allora  $g(X) \leq d - n$ . (Sugg.: il divisore della sezione iperpiana non è speciale.)

**16.7 Esercizi complementari**

**16.10.** Sia  $\phi: X \rightarrow X$  un automorfismo regolare di una curva liscia proiettiva di genere  $g$ . Dimostrare che  $\phi$  ha al più  $2g + 2$  punti fissi. (Sugg.: sia  $D$  un generico divisore effettivo di grado  $g + 1$ . Allora  $D \cap \phi(D) = \emptyset$  ed esiste una funzione razionale non costante  $f$  tale che  $\text{div}(f) + D \geq 0$ ; ogni punto fisso di  $\phi$  è uno zero della funzione razionale  $f - \phi^*f$ .)

**16.11 (\*)**. Sia  $X \subset \mathbb{P}^3$  una curva liscia irriducibile nondegenere di grado 4 e genere 1. Dimostrare che  $X$  è intersezione completa di due quadriche. (Sugg.: valutare la dimensione del sistema lineare  $L_X(2)$  per dedurre che esistono due polinomi  $F, G \in \mathbb{K}[x_0, \dots, x_3]$  omogenei di grado 2 e linearmente indipendenti tali che  $X \subset V(F, G)$ . Mostrare che  $V(F, G)$  ha dimensione 1 e poi confrontare il polinomio di Hilbert di  $X$  con quello di  $Z(F, G)$ . Infine applicare il Teorema 13.4.9)

**16.12.** Sia  $X \subset \mathbb{P}^3$  una curva liscia irriducibile nondegenere di grado 4 e genere 1. Dimostrare che per ogni  $n > 0$  il sistema lineare  $L_X(n)$  è completo. (Sugg.: è facile se si usa il risultato di uno degli Esercizi 16.11, 17.17 o 17.13. Per una dimostrazione più elementare, provare preliminarmente che un insieme di sei punti in posizione generale in  $\mathbb{P}^3$  è intersezione di quadriche, da questo dedurre che non tutti i divisori di  $L_X(2)$  sono somma di due sezioni iperpiane. Mostrare che, se  $H \in \text{Div}^4(X)$  è una sezione iperpiana, allora  $\dim L_X(n) - (n-2)H \geq 7$  e usare Riemann-Roch per provare la completezza.)

**16.13.** Sia  $U$  un aperto affine di una varietà quasiproiettiva irriducibile  $X$ . Dimostrare che  $\Omega_X(U)$  è un  $\mathcal{O}_X(U)$ -modulo Noetheriano isomorfo a  $\Omega_{\mathcal{O}_X(U)/\mathbb{K}}/\text{torsione}$ . (Sugg: se  $U \subset \mathbb{A}^n$  e  $x_1, \dots, x_n$  sono coordinate affini, mostrare utilizzando la partizione dell'unità che  $dx_1, \dots, dx_n$  sono generatori).

**16.14.** Trovare una varietà affine irriducibile  $X$  tale che  $\Omega_{\mathcal{O}_X(X)/\mathbb{K}}$  possiede torsione come  $\mathcal{O}_X(X)$ -modulo. (Sugg: provare con  $X \subset \mathbb{A}^2$  curva singolare).

**Definizione 16.7.1.** Una curva liscia  $X$  si dice **trigonale** se possiede un divisore  $D$  di grado 3 tale che  $\dim |D| > 0$ .

**16.15.** Dimostrare che ogni curva di genere  $\leq 4$  è trigonale. (Sugg.: gli unici casi non banali sono  $g = 3, 4$  e  $X$  non iperellittica. Considerare allora l'applicazione canonica  $\phi_K$  e se  $g = 4$ , e mostrare che la proiezione di  $\phi_K(X)$  di centro un suo punto è una curva piana singolare di grado 5.)

**16.16.** (caratteristica  $\neq 3$ ) Sia  $X$  una curva non iperellittica di genere  $g$  e  $\phi_K$  la sua applicazione canonica. Mostrare che  $X$  è trigonale se e solo se  $\phi_K(X)$  possiede poliscanti. (Sugg.: siano  $p_1, \dots, p_n \in X$  punti distinti; valutare la dimensione del sistema lineare  $|p_1 + \dots + p_n|$  in funzione della dimensione del sottospazio proiettivo generato da  $\phi_K(p_1), \dots, \phi_K(p_n)$ .)

**16.17.** (caratteristica  $\neq 3$ ) Sia  $X \subset \mathbb{P}^4$  una curva liscia intersezione completa di 3 quadriche. Mostrare che  $g(X) = 5$ , che il divisore della sezione iperpiana è il divisore canonico e che  $X$  non è trigonale. (Sugg.: mostrare che ogni polisecante di  $X$  è contenuta in ogni quadrica che contiene  $X$ .)

### Esercizi sull'invarianza algebrica del genere

Siano  $X$  e  $Y$  due curve lisce proiettive irriducibili. Abbiamo visto che se esiste un isomorfismo di  $\mathbb{K}$ -algebre  $\mathbb{K}(X) \cong \mathbb{K}(Y)$ , allora  $X$  e  $Y$  sono birazionali e quindi isomorfe. Se invece esiste solamente un isomorfismo di campi  $\mathbb{K}(X) \cong \mathbb{K}(Y)$ , allora proveremo che  $g(X) = g(Y)$  (Esercizio 16.18), ma che in generale  $X$  non è isomorfo ad  $Y$  (Esercizio 16.18).

**16.18.** Per ogni  $\lambda \in \mathbb{C}$ , la coniugazione complessa induce un isomorfismo tra i campi delle funzioni razionali delle due curve piane di equazioni affini  $y^2 = 4x(x-1)(x-\lambda)$  e  $y^2 = 4x(x-1)(x-\bar{\lambda})$ . Dedurre dal teorema di Salmon che per il generico  $\lambda$  tali curve non sono tra loro birazionali.

**16.19.** Sia  $X$  una curva liscia proiettiva irriducibile definita su un campo algebricamente chiuso  $\mathbb{K}$ . Denotiamo  $K = \mathbb{K}(X)$  e con  $C_K$  l'insieme delle valutazioni discrete surgettive  $\nu: K \rightarrow \mathbb{Z} \cup \{+\infty\}$ : abbiamo già dimostrato (Esercizio 14.16) che l'applicazione  $\text{ord}: X \rightarrow C_K$ ,  $x \mapsto \text{ord}_x$ , è bigettiva. Dimostrare che:

1.  $H_K^0(0) := \{f \in K \mid \nu(f) = 0 \text{ per ogni } \nu \in C_K\}$  è un campo (Sugg.: mostrare direttamente che è uguale a  $\mathbb{K}$ ).
2. Per ogni  $\nu \in C_K$  e per ogni  $n \in \mathbb{N}$ , l'insieme

$$H_K^0(n\nu) := \{f \in K \mid \nu(f) + n \geq 0 \text{ e } \eta(f) \geq 0 \text{ per ogni } \eta \in C_K - \{\nu\}\}$$

è un  $H_K^0(0)$ -spazio vettoriale.

3. Per ogni  $\nu \in C_K$  esiste  $n_0 \in \mathbb{N}$  tale che la dimensione di  $H_K^0(n\nu)$  è uguale a  $n+1-g(X)$  per ogni  $n \geq n_0$ .
4. Dedurre dai punti precedenti che il genere di  $X$  dipende solamente dalla classe di isomorfismo del campo  $\mathbb{K}(X)$ .

**16.20.** Sia  $X$  una curva liscia proiettiva definita su un campo algebricamente chiuso di caratteristica  $p > 0$  e sia  $F: X_p \rightarrow X$  il morfismo di Frobenius. Dimostrare che  $X$  e  $X_p$  hanno lo stesso genere.

## Genere aritmetico e disuguaglianza di Castelnuovo

Capitolo incompleto

In questo capitolo continuiamo lo studio delle curve proiettive mediante un utilizzo più raffinato della nozione di grado e del polinomio di Hilbert. Salvo avviso contrario, per curva intenderemo una varietà irriducibile di dimensione 1 possibilmente singolare.

**Definizione 17.0.1.** Sia  $p_X$  il polinomio di Hilbert di una curva proiettiva irriducibile  $X \subset \mathbb{P}^n$ . Il numero intero  $p_a(X) = 1 - p_X(0)$  viene detto **genere aritmetico** di  $X$ .

Segue quindi dai risultati del Capitolo 13 che il polinomio di Hilbert di una curva proiettiva irriducibile  $X \subset \mathbb{P}^n$  è uguale a

$$p_X(t) = \deg(X)t + 1 - p_a(X).$$

### 17.1 Il grado delle proiezioni

Sia  $X \subset \mathbb{P}^n$  una curva irriducibile proiettiva. Ricordiamo (Teorema 13.5.4 e Corollario 13.5.5) che un iperpiano  $H \subset \mathbb{P}^n$  interseca trasversalmente  $X$  se e solo se  $H \cap X$  ha cardinalità  $\deg(X)$ ; inoltre, per il Teorema 13.5.2, l'insieme degli iperpiani con tale proprietà è un aperto denso dello spazio proiettivo duale. Osserviamo inoltre che, se  $x_0, \dots, x_n$  è un sistema di coordinate omogenee tali che l'iperpiano  $H = \{x_1 = 0\}$  interseca trasversalmente  $X$  e  $X \cap \{x_0 = x_1 = 0\} = \emptyset$ , allora la funzione razionale  $x_1/x_0 \in \mathbb{K}(X)$  è un parametro locale in ogni punto di  $X \cap H$ .

**Teorema 17.1.1.** Siano  $X \subset \mathbb{P}^n$  una curva proiettiva irriducibile di grado  $> 1$  ed  $o \in \overline{\mathbb{P}^n}$  un punto. Denotiamo con  $\pi: X \dashrightarrow \mathbb{P}^{n-1}$  la proiezione di centro  $o$  e con  $Y = \overline{\pi(X - \{o\})} \subset \mathbb{P}^{n-1}$  l'immagine di  $\pi$ .

1. Se  $o \notin X$ , allora vale  $\deg(X) = \deg(\pi) \deg(Y)$ .
2. Se  $o$  è un punto liscio di  $X$ , allora vale  $\deg(X) = \deg(\pi) \deg(Y) + 1$ .
3. Se  $o$  è un punto singolare di  $X$ , allora vale  $\deg(X) \geq \deg(\pi) \deg(Y) + 2$ .

*Dimostrazione.* Per il morfismo  $\pi: X - \{o\} \rightarrow Y$  è regolare e dominante. Sia  $H \subset \mathbb{P}^n$  un iperpiano che contiene  $o$  e che interseca  $Y$  trasversalmente in  $\deg(Y)$  punti lisci e distinti. Fissiamo un sistema di coordinate omogenee  $x_0, \dots, x_n$  e siano  $I = I(X) \subset \mathbb{K}[x_0, \dots, x_n]$  l'ideale dei polinomi omogenei nulli su  $X$  e  $f \in \mathbb{K}[x_0, \dots, x_n]$  l'equazione di  $H$ . Per il Corollario 13.2.10 e la Proposizione 13.3.10 vale

$$\deg(X) = \sum_{p \in X \cap H} \deg_p(Z(I + (f))).$$

Per la Proposizione 13.3.11, per ogni  $p \in X \cap H$  vale

$$\deg_p(Z(I + (f))) = \dim_{\mathbb{K}} \frac{\mathcal{O}_{p,X}}{(f/g)},$$

dove  $g$  è una qualsiasi forma lineare che non si annulla in  $p$ . Se  $p \in X \cap H$  è un punto singolare di  $X$ , allora è singolare anche per  $Z(I + (f))$  e quindi  $\deg_p(Z(I + (f))) \geq 2$ . Se  $p \in X \cap H$  è un punto liscio di  $X$  diverso da  $o$ , allora  $\deg_p(Z(I + (f))) = \text{mult}_p(\pi)$ : infatti possiamo scegliere  $g$  in modo tale che  $g(o) = 0$  e quindi  $f/g$  è la composizione di  $\pi$  con un parametro locale della curva  $Y$  nel punto  $\pi(p)$ . Il morfismo  $\pi: X - \{o\} \rightarrow Y$  è quasifinito e dominante, esistono quindi due aperti non vuoti  $U \subset X$  e  $V \subset Y$  tali che  $\pi(U) = V$  e  $\pi: U \rightarrow V$  è un morfismo proiettivo e quindi finito. Non è restrittivo assumere che  $U$  e  $V$  non contengano punti singolari di  $X$  e  $Y$  rispettivamente. Dato che il grado di  $\pi$  è uguale al grado della sua restrizione  $\pi: U \rightarrow V$ , se  $q \in V$ , allora il Teorema 14.3.3 implica che

$$\deg(\pi) = \sum_{p \in U, \pi(p)=q} \text{mult}_p(\pi).$$

Se  $H = \{f = 0\}$  è un generico iperpiano passante per il punto  $o$ , allora  $H \cap (Y - V) = \emptyset$  e vale

$$\begin{aligned} \deg(X) &= \deg_o(Z(I + (f))) + \sum_{p \in H \cap U} \text{mult}_p(\pi) \\ &= \deg_o(Z(I + (f))) + \sum_{q \in H \cap Y} \sum_{p \in U, \pi(p)=q} \text{mult}_p(\pi) \\ &= \deg_o(Z(I + (f))) + \deg(Y) \deg(\pi). \end{aligned}$$

□

## Esercizi

**17.1.** In caratteristica  $p > 0$ , dimostrare che la molteplicità del morfismo di Frobenius

$$F: \mathbb{P}^1 \rightarrow \mathbb{P}^1, \quad [x_0, x_1] \mapsto [x_0^p, x_1^p]$$

è uguale a  $p$  in ogni punto.

**17.2.** Siano  $\phi: X \rightarrow Y$  e  $\psi: Y \rightarrow Z$  morfismi dominanti di curve lisce. Provare che per ogni  $x \in X$  vale  $\text{mult}_x(\psi\phi) = \text{mult}_x(\phi) \text{mult}_{\phi(x)}(\psi)$ .

## 17.2 Modelli nonsingolari

Abbiamo già osservato che ogni morfismo birazionale di curve lisce proiettive è di fatto un isomorfismo regolare e che curve lisce possono essere birazionalmente equivalenti a curve singolari.

Ricordiamo che una curva proiettiva irriducibile  $X \subset \mathbb{P}^n$  si dice *nondegenere* se non è contenuta in alcun iperpiano. Per il Lemma 9.8.5, se  $X \subset \mathbb{P}^n$  è non degenere, allora  $\deg(X) \geq n$ .

**Lemma 17.2.1.** *Ogni curva proiettiva irriducibile è isomorfa ad una curva nondegenere in  $\mathbb{P}^n$  di grado  $< 2n - 2$ , per qualche  $n > 0$ .*



*Dimostrazione.* Sia  $d$  il grado di una curva  $X \subset \mathbb{P}^m$ , allora il polinomio di Hilbert di  $X$  è  $p_X(t) = dt + e$  per qualche  $e \in \mathbb{Z}$ . Ne segue che per  $m$  sufficientemente grande, lo spazio dei polinomi omogenei di grado  $m$  che si annullano su  $X$  ha codimensione  $dm + e$  e quindi che il sottospazio proiettivo generato da  $v_m(X)$  ha dimensione  $n = dm + e - 1$ , dove  $v_m: \mathbb{P}^m \rightarrow \mathbb{P}^n$  è la  $m$ -esima immersione di Veronese. Poiché il grado di  $v_m(X)$  è uguale a  $dm$ , per  $m$  abbastanza grande la curva  $v_m(X)$  è isomorfa ad  $X$  e soddisfa le condizioni richieste.  $\square$

**Teorema 17.2.2 (Noether-Kronecker, 1871).** *Ogni curva irriducibile è birazionale ad una curva liscia proiettiva.*

*Dimostrazione.* (Albanese<sup>1</sup>, [Al1924]) Sia  $X$  una curva irriducibile; vogliamo costruire una successione finita di applicazioni birazionali

$$X \dashrightarrow X_1 \dashrightarrow X_2 \dashrightarrow \cdots \dashrightarrow X_k$$

in modo tale che  $X_k$  sia una curva liscia proiettiva. A meno di considerare una chiusura proiettiva di  $X$  non è restrittivo supporre che  $X$  sia proiettiva e nondegenere in  $\mathbb{P}^n$  e, per il Lemma 17.2.1, che  $n \leq \deg(X) < 2n - 2$ . Se  $X$  è liscia abbiamo finito, altrimenti scegliamo un suo punto singolare  $o \in X$  e definiamo  $X_1 = \overline{\pi_o(X - \{o\})}$ , dove  $\pi_o: \mathbb{P}^n - \{o\} \rightarrow \mathbb{P}^{n-1}$  è la proiezione di centro  $o$ . Per il Teorema 17.1.1 si ha  $\deg(X) \geq \deg(\pi_o) \deg(X_1) + 2$ . La curva  $X_1$  è non degenere e quindi per il Lemma 9.8.5 vale  $\deg(X_1) \geq n - 1$ . Dato che  $\deg(X) < 2n - 2$  si ha  $\deg(\pi_o) = 1$ , quindi  $\pi_o: X \dashrightarrow X_1$  è birazionale e  $\deg(X_1) \leq \deg(X) - 2 < 2(n - 1) - 2$ . Qualora  $X_1$  fosse singolare si ripete la procedura con  $X_1$  al posto di  $X$  e si ottiene  $X_2 \subset \mathbb{P}^{n-2}$  nondegenere di grado  $< 2(n - 2) - 2$  ecc. Un tal bel gioco dura poco e si ferma prima di arrivare a curve in  $\mathbb{P}^2$ ; in altri termini la curva  $X_k$  deve essere necessariamente liscia per qualche  $k < n - 2$ .  $\square$

**Corollario 17.2.3.** *Sia  $\mathbb{K} \subset F$  una estensione di campi finitamente generata con grado di trascendenza uguale a 1. Allora esiste una curva liscia proiettiva irriducibile  $X$  tale che  $\mathbb{K}(X) = F$ .*

*Dimostrazione.* Per il Lemma 12.3.1 ed il Corollario 12.3.5 esiste una curva affine irriducibile  $Y$  tale che  $\mathbb{K}(Y) = F$ , mentre per il Teorema 17.2.2 la curva  $Y$  è birazionale ad una curva liscia proiettiva.  $\square$

## 17.3 Il teorema di posizione generale

Da questo momento, e fino alla fine del capitolo supporremo, salvo avviso contrario, che le varietà siano tutte definite su di un campo algebricamente chiuso  $\mathbb{K}$  di **caratteristica 0**. Per alcuni risultati tale ipotesi sulla caratteristica è essenziale, mentre per altri è di convenienza. Per chi fosse interessato alla caratteristica positiva rimandiamo alla Sezione VI.3 del libro di Hartshorne [Hart1977].

**Definizione 17.3.1.** *Un insieme finito di punti  $S \subset \mathbb{P}^n$  si dice in **posizione generale** se ogni sottoinsieme di  $S$  di cardinalità  $\leq n + 1$  è proiettivamente indipendente.*

Ad esempio,  $n + 2$  punti in  $\mathbb{P}^n$  sono in posizione generale se e solo se sono un sistema di riferimento proiettivo.

Consideriamo una curva proiettiva irriducibile  $X \subset \mathbb{P}^n$  di grado  $d$ . Supponiamo inoltre che  $X$  sia **non degenere**, ossia non contenuta in alcun iperpiano; questa condizione implica in particolare, per il Lemma 9.8.5, che  $d \geq n$ .

Obiettivo di questa sezione è dimostrare il seguente risultato.

<sup>1</sup> Giacomo Albanese: Geraci Siculo 1890-San Paolo del Brasile 1948.

**Teorema 17.3.2 (Teorema di posizione generale).** *Sia  $X \subset \mathbb{P}^n$  una curva proiettiva irriducibile e non degenera definita su un campo algebricamente chiuso di caratteristica 0. Allora il generico iperpiano  $H \subset \mathbb{P}^n$  interseca trasversalmente  $X$  e l'insieme  $H \cap X$  è in posizione generale in  $H$ .*

Prima di affrontare la dimostrazione del teorema di posizione generale, dimostriamo alcuni lemmi. Ricordiamo che per il Teorema 13.5.2, l'insieme degli iperpiani che intersecano trasversalmente  $X$  è un aperto denso dello spazio proiettivo duale. Basta quindi dimostrare che per il generico iperpiano  $H$  l'insieme  $H \cap X$  è in posizione generale in  $H$ ; possiamo supporre senza perdita di generalità  $n \geq 3$ .

Per ogni intero positivo  $k$  indichiamo con  $X[k] \subset X^k$  l'aperto formato dalle  $k$ -uple di punti distinti di  $X$  e con  $L[k] \subset X[k]$  l'insieme delle  $k$ -uple di punti distinti che sono contenute in un sottospazio di dimensione  $k - 2$ . È facile dimostrare che  $L[k]$  è chiuso in  $X[k]$ .

**Lemma 17.3.3.** *Nelle notazioni precedenti,  $L[3]$  ha dimensione minore od uguale a 1.*

*Dimostrazione.* Osserviamo che

$$L[3] = \{(p, q, r) \in X[3] \mid p, q, r \text{ sono allineati}\}.$$

A meno di proiettare da un punto esterno alla varietà secante di  $X$  non è restrittivo supporre  $n = 3$ , ossia  $X \subset \mathbb{P}^3$  irriducibile e non degenera. Supponiamo per assurdo che  $L[3]$  abbia una componente irriducibile  $Z$  di dimensione  $> 1$  e consideriamo le due proiezioni

$$\begin{aligned} \pi_1: Z &\rightarrow X, & \pi_1(p, q, r) &= p, \\ \pi_{23}: Z &\rightarrow X[2], & \pi_{23}(p, q, r) &= (q, r). \end{aligned}$$

Le fibre di  $\pi_{23}$  hanno cardinalità finita e per motivi di dimensione  $\pi_{23}$  deve quindi essere un morfismo dominante. A maggior ragione il morfismo  $(p, q, r) \mapsto r$  è dominante e per simmetria anche  $\pi_1$  è dominante. Consideriamo adesso il chiuso  $B \subset X[2]$  definito come

$$B = \{(p, q) \in X[2] \mid \mathbb{T}_p X \cap \mathbb{T}_q X \neq \emptyset\}.$$

Vogliamo dimostrare che  $\dim B \leq 1$ : a tal fine dimostriamo che per ogni punto liscio  $p \in X$ , l'insieme  $\{q \in X \mid (p, q) \in B\}$  è finito. Siano  $Y \subset X$  il complementare di  $X \cap \mathbb{T}_p X$  e  $p: Y \rightarrow \mathbb{P}^1$  la proiezione di centro  $\mathbb{T}_p X$ . Siccome siamo in caratteristica 0, per il teorema di Bertini-Sard il morfismo  $p$  possiede un numero finito di punti di ramificazione. Basta adesso osservare che un punto  $q \in Y$  è di ramificazione se e solo se  $\mathbb{T}_q X \cap \mathbb{T}_p X \neq \emptyset$ . Dunque  $B$  ha dimensione 1 e quindi  $U = Z - \pi_{23}^{-1}(B)$  è un aperto denso di  $Z$ . Le due proiezioni  $\pi_1: U \rightarrow X$  e  $\pi_{23}: U \rightarrow X[2]$  continuano ad essere dominanti. Scegliamo un punto liscio  $o \in X$  tale che la fibra  $\pi_1^{-1}(o) \cap U$  sia infinita e indichiamo con  $Y = \pi_o(X) \subset \mathbb{P}^2$  l'immagine della proiezione di centro  $o$ . Scegliamo inoltre  $(o, p, q) \in U$  tale che il punto  $\pi_o(p) = \pi_o(q)$  sia liscio in  $Y$ ; questo implica che le rette tangenti  $\mathbb{T}_q X$  e  $\mathbb{T}_p X$  sono contenute in uno stesso piano passante per  $o$  e di conseguenza  $\mathbb{T}_q X \cap \mathbb{T}_p X \neq \emptyset$ , in contraddizione con la definizione di  $U$ .  $\square$

**Lemma 17.3.4.** *Nelle notazioni precedenti, per ogni  $3 \leq k \leq n$ , la dimensione di  $L[k]$  è minore od uguale a  $k - 2$ .*

*Dimostrazione.* **(IDEA)** Bisogna escludere che  $L[k]$  abbia componenti irriducibili di dimensione  $k - 1$ . Induzione su  $k$ : se  $k = 3$  applicare il Lemma 17.3.3, mentre se  $k > 3$  proiettare  $X$  da un suo punto generico.  $\square$

**Lemma 17.3.5.** (*caratteristica 0*) Sia  $(\mathbb{P}^n)^\vee$  lo spazio proiettivo duale. Nelle notazioni precedenti consideriamo

$$Y = \{(H, p_1, \dots, p_n) \in (\mathbb{P}^n)^\vee \times X[n] \mid p_1, \dots, p_n \in H\}$$

e siano  $q_1: Y \rightarrow (\mathbb{P}^n)^\vee$ ,  $q_2: Y \rightarrow X[n]$  le due proiezioni. Allora che per ogni chiuso proprio  $Z \subset X[n]$  il chiuso  $q_1(q_2^{-1}(Z))$  ha dimensione  $< n$ .

*Dimostrazione.* (**IDEA**) Sia  $M_k \subset X[n]$  l'insieme delle  $n$ -uple che generano un sottospazio proiettivo di dimensione  $\leq k$ . Sia  $K$  una componente irriducibile di  $q_2^{-1}(Z)$ , dato che le fibre di  $q_1$  sono finite basta dimostrare che  $\dim K < n$ . Se  $x \in X[n] - M_k$ , allora  $\dim q_2^{-1}(x) < n - k$ . Mostrare che per ogni  $k = 1, \dots, n - 2$  la dimensione di  $M_k$  è  $\leq k$ .  $\square$

*Dimostrazione (del Teorema 17.3.2).* **IDEA** Usare il Lemma 17.3.5, con  $Z = L[n]$ .  $\square$

*Osservazione 17.3.6.* Su  $\mathbb{K} = \mathbb{C}$  esiste una bella dimostrazione del teorema di posizione generale che si basa su argomenti di monodromia dei rivestimenti e che potete trovare in [ACGH1984, pag. 109]. Da tale dimostrazione segue inoltre che l'insieme  $Y$  definito nel Lemma 17.3.5 è irriducibile di dimensione  $n$ . Rimandiamo invece a [GH1978, pag. 249] per una dimostrazione semplice ma sbagliata del Teorema 17.3.2.

Sia  $X \subset \mathbb{P}^n$  una varietà proiettiva irriducibile e non degenera. Chiameremo **poliseccanti** le rette di  $\mathbb{P}^n$  che intersecano  $X$  in almeno tre punti distinti.

**Teorema 17.3.7.** Sia  $X \subset \mathbb{P}^n$ ,  $n \geq 3$ , una curva proiettiva irriducibile e non degenera definita su di un campo algebricamente chiuso di caratteristica 0. Allora esiste un aperto non vuoto  $U \subset X$  tale che ogni punto  $x \in U$  appartiene al più ad un numero finito di poliseccanti di  $X$ .

*Dimostrazione.* Consideriamo la proiezione  $\pi: L[3] \rightarrow X$  data da  $\pi(p, q, r) = p$ . Segue dalla definizione di  $L[3]$  che  $\pi^{-1}(p)$  è infinito se e solo se il punto  $p$  appartiene a infinite poliseccanti. Per il Lemma 17.3.3 esiste un aperto  $U$  tale che  $\pi^{-1}(x)$  è vuoto o finito per ogni  $x \in U$ .  $\square$

*Osservazione 17.3.8.* Il Teorema 17.3.7 è falso in caratteristica positiva: vedi Esercizio 17.5.

## Esercizi

**17.3.** Sia  $X \subset \mathbb{P}^n$  una curva di grado  $n$  non contenuta in alcun iperpiano. Dimostrare che  $X$  è liscia.

**17.4 (\*)**. Sia  $p_X$  il polinomio di Hilbert di una curva proiettiva irriducibile  $X \subset \mathbb{P}^n$ . Dimostrare che  $p_X(0) \leq 1$ . (Sugg.: applicare il Lemma 9.8.5 alla  $d$ -esima immersione di Veronese di  $X$ , per  $d \gg 0$ .) Dimostrare inoltre che se  $p_X(0) = 1$ , allora  $X$  è liscia ed isomorfa a  $\mathbb{P}^1$ . (Sugg.: Esercizi 17.3 e 14.21.)

**17.5.** In caratteristica  $p > 0$ , consideriamo la curva  $Z \subset \mathbb{P}^3$  di parametrizzazione  $t \mapsto \phi(t) = [1, t, t^p, t^{p^2}]$ . Provare che  $Z$  è non degenera di grado  $p^2$ , che ogni retta tangente in un suo punto liscio passa per il punto  $[0, 1, 0, 0]$  e che per ogni  $t, s \in \mathbb{K}$ , con  $s \neq t$ , la retta  $\phi(s) + \phi(t)$  interseca  $Z$  in almeno  $p$  punti distinti.

**17.6.** Sia  $X$  una curva piana liscia di grado  $d$ . Provare che

$$p_a(X) = \frac{(d-1)(d-2)}{2}.$$

(Sugg.: si può usare il Teorema di Riemann (Esercizio 6.60) per mostrare che  $p_a(X) = g(X)$ ; oppure si può usare il Teorema 13.4.6 ed i trucchi contabili dell'Esercizio 13.27 per mostrare che il polinomio di Hilbert di  $X$  è  $p_X(n) = d(n+1) - \binom{d}{2}$ .)

**17.7.** Provare che se l'ideale di una curva liscia  $X \subset \mathbb{P}^3$  è generato da due polinomi omogenei di gradi  $n$  e  $m$ , allora vale  $p_a(X) = \frac{mn(n+m-4)}{2} + 1$ . (Sugg.: Esercizio 13.27.)

**17.8.** Sia  $X \subset \mathbb{P}^n$  una curva liscia proiettiva irriducibile. Dimostrare che per  $d \gg 0$  il sistema lineare  $L_X(d)$  ha dimensione  $d \deg(X) - p_a(X)$  e dedurre che  $p_a(X) \geq 0$ . (Sugg.: Teoremi 14.4.7 e 14.6.5.)

**17.9 (Disuguaglianza di Riemann).** Sia  $X$  una curva liscia proiettiva e  $D \in \text{Div}(X)$  un divisore effettivo. Dimostrare che  $\dim |D| \geq \deg(D) - p_a(X)$ . Dedurre che  $p_a(X)$  è il più piccolo intero  $q$  per il quale vale  $\dim |D| \geq \deg(D) - q$  e quindi dipende solo dalla classe di isomorfismo di  $X$  e non dalla particolare immersione in uno spazio proiettivo.

**17.10.** Utilizzare la disuguaglianza di Riemann ed il risultato dell'Esercizio 14.8 per dimostrare che una curva liscia proiettiva è isomorfa a  $\mathbb{P}^1$  se e solo se il suo genere aritmetico è uguale a 0.

## 17.4 La disuguaglianza di Castelnuovo

In questa sezione consideriamo una curva non degenere  $X \subset \mathbb{P}^n$  di grado  $d$  e denotiamo con  $m \in \mathbb{N}$  la parte intera di  $\frac{d-1}{n-1}$ .

Il nostro obiettivo è trovare, mediante la soluzione degli esercizi proposti, un limite superiore al genere aritmetico di  $X$  quando  $n \geq 3$ . La **disuguaglianza di Castelnuovo** è ottenuta mettendo assieme i Teoremi 17.3.2 e 17.4.1.

**Teorema 17.4.1.** *Sia  $X \subset \mathbb{P}^n$  una curva liscia nondegenere di grado  $d$ . Se per il generico iperpiano  $H \subset \mathbb{P}^n$  l'intersezione  $H \cap X$  è in posizione generale in  $H$ , allora*

$$p_a(X) \leq m(d-1) - \binom{m+1}{2}(n-1), \quad \text{dove } m = \left\lfloor \frac{d-1}{n-1} \right\rfloor.$$

*Nota storica.* La disuguaglianza 17.4.1 è stata dimostrata per  $n = 3$  da Halphen nel 1882 ed è stata poi estesa da Guido Castelnuovo nel 1889. In tale epoca, l'esistenza della sezione iperpiana in posizione generale veniva considerata da tutti come un principio evidente e quindi senza necessità alcuna di dimostrazione.

*Osservazione 17.4.2.* Gli Esercizi 17.6 e 17.7 mostrano che se  $X$  è una curva piana oppure una intersezione completa di una quadrica e di una superficie di grado  $d/2$  in  $\mathbb{P}^3$ , allora vale l'uguaglianza nel Teorema 17.4.1.

**Esercizi**

**17.11.** Sia  $\sum a_k t^k$  la serie di Poincaré dell'ideale di  $d$  punti in posizione generale in  $\mathbb{P}^{n-1}$ . Dimostrare che:

1. Per ogni  $k \in \mathbb{N}$  vale  $a_k \geq \min(k(n-1) + 1, d)$ . (Sugg.: siano  $p_1, \dots, p_d$  i punti in questione. Fissiamo un intero  $k \geq 0$  e denotiamo  $l = \min(k(n-1) + 1, d)$ ; provare che per ogni indice  $i = 1, \dots, l$  esistono  $k$  iperpiani  $H_{i1}, \dots, H_{ik} \subset \mathbb{P}^{n-1}$  tali che  $p_j \in \cup_k H_{ik}$  se e solo se  $j < i$ .)
2. Sia  $m$  la parte intera di  $(d-1)/(n-1)$ . Allora per ogni  $N \geq m$  vale

$$\sum_{k=1}^N a_k \geq dN + \binom{m+1}{2}(n-1) - m(d-1).$$

**17.12.** Sia  $X \subset \mathbb{P}^n$  una curva irriducibile nondegenere di grado  $d$ . Se per il generico iperpiano  $H \subset \mathbb{P}^n$  l'intersezione  $H \cap X$  è in posizione generale in  $H$ , dimostrare che

$$p_X(0) - 1 \geq \binom{m+1}{2}(n-1) - m(d-1), \quad \text{dove } m = \left\lfloor \frac{d-1}{n-1} \right\rfloor,$$

e dedurne il Teorema 17.4.1. (Sugg.: sappiamo che  $p_X(N) = Nd + p_X(0)$  e quindi basta dimostrare che  $p_X(N) - 1 \geq dN + \binom{m+1}{2}(n-1) - m(d-1)$  per  $N \gg 0$ . Usare il Lemma 13.2.2 e l'Esercizio 17.11.)

**17.13.** (caratteristica 0) Per usi futuri, diamo una versione più forte dell'Esercizio 17.12 assumendo che  $X \subset \mathbb{P}^n$  sia una curva liscia proiettiva nondegenere di grado  $d$ . Dimostrare che per ogni  $N > 0$  vale

$$\dim L_X(N) \geq \sum_{k=1}^N \min(k(n-1) + 1, d).$$

(Sugg.: sia  $N > 0$  un intero fissato e scegliamo  $N$  iperpiani  $H_1, \dots, H_N$  tali che  $X \cap H_i \cap H_j = \emptyset$  per ogni  $i \neq j$  e  $H_i \cap X$  è in posizione generale in  $H_i$  per ogni  $i$ . Denotiamo  $s = \sum_{k=1}^N \min(k(n-1) + 1, d)$  e prendiamo  $s$  punti distinti  $p_1, \dots, p_s \in \cup\{X \cap H_i \mid i = 1, \dots, N\}$  in modo tale che  $p_j \in H_{i+1}$  se e solo se

$$\sum_{k=N-i+1}^N \min(k(n-1) + 1, d) < j \leq \sum_{k=N-i}^N \min(k(n-1) + 1, d).$$

Bisogna provare che i punti  $p_i$  inducono condizioni lineari indipendenti sul sistema lineare  $L_X(N)$ , e cioè che per ogni  $j = 1, \dots, s$  esiste una ipersuperficie  $F_j$  di grado  $N$  in  $\mathbb{P}^n$  che contiene  $p_1, \dots, p_{j-1}$  ma non contiene  $p_j$ . Se  $p_j \in H_{i+1}$  usare lo stesso trucco dell'Esercizio 17.11 per trovare una ipersuperficie  $G$  di grado  $N-i$  tale che  $F_j = H_1 \cup \dots \cup H_i \cup G$  è adatta allo scopo.)

**17.5 Il teorema di Max Noether**

In questa sezione si richiede il teorema di Riemann-Roch.

**Lemma 17.5.1.** *Il genere  $g(X)$  di una curva liscia proiettiva è uguale al genere aritmetico  $p_a(X)$ .*

*Dimostrazione.* Se  $X \subset \mathbb{P}^n$  ha grado  $d$  e  $H \in \text{Div}^d(X)$  è il divisore di una sezione iperpiana, allora per il teorema del resto 14.6.5 vale  $h^0(lH) = ld + 1 - p_a(X)$  per  $l \gg 0$  e questo implica che  $p_a(X) = g(X)$ .  $\square$

**Teorema 17.5.2 (Max Noether).** (caratteristica 0) Sia  $K$  il divisore canonico di una curva non iperellittica  $X$ . Allora per ogni  $n > 0$  l'immagine dell'applicazione multilineare

$$H^0(X, K) \times \cdots \times H^0(X, K) \rightarrow H^0(X, nK), \quad (f_1, \dots, f_n) \mapsto f_1 \cdots f_n,$$

non è contenuta in alcun iperpiano.

*Dimostrazione.* Esercizio 17.15.  $\square$

### Esercizi

**17.14.** (caratteristica 0) Sia  $X \subset \mathbb{P}^n$  una curva liscia non degenera di grado  $2n$  e sia  $H \in L_X(1)$  il divisore di una sezione iperpiana. Per la disuguaglianza di Castelnuovo (Teorema 17.4.1) vale

$$g(X) \leq 2(2n - 1) - \binom{3}{2}(n - 1) = n + 1.$$

Dimostrare che se  $g(X) = n + 1$  ed il sistema lineare  $L_X(1)$  è completo, allora  $H$  è un divisore canonico e  $L_X(k)$  è completo per ogni  $k > 0$ . (Sugg.: se  $K$  è canonico, allora  $\deg(K) = \deg(H)$  e per Riemann-Roch vale  $h^0(X, K - H) = 1$ . Se  $N > 1$  vale  $h^0(NH) = 2nN - n$  ed il sistema lineare  $L_X(N)$  è completo se e solo se  $\dim L_X(N) = h^0(NH) - 1$ . Usare l'Esercizio 17.13.)

**17.15.** Dimostrare il Teorema 17.5.2. (Sugg.: immersione canonica ed Esercizio 17.14.)

**17.16.** (caratteristica 0) Siano  $X \subset \mathbb{P}^n$  una curva liscia non degenera e  $L$  un sistema lineare su  $X$  di dimensione  $r < n$ . Dimostrare che il generico iperpiano  $H$  ha la seguente proprietà: presi comunque  $r + 1$  punti distinti  $p_0, \dots, p_r \in H \cap X$ , essi inducono condizioni lineari indipendenti su  $L$ , cioè  $L(-(p_0 + \cdots + p_r)) = \emptyset$ . (Sugg.: applicare 17.3.5, con  $Z$  uguale al chiuso delle  $n$ -uple di punti che contengono un sottoinsieme  $E$  di cardinalità  $r + 1$  tale che  $\dim L(-E) \geq 0$ .)

**17.17.** (caratteristica 0) Sia  $E \subset \mathbb{P}^d$  una curva liscia nondegenera di grado  $d + 1$  e genere 1. Dimostrare che il sistema lineare  $L_E(n)$  è completo per ogni  $n$ . (Sugg.: induzione su  $n$ , essendo  $n = 1$  conseguenza di Riemann-Roch. Supponiamo  $L_E(n - 1)$  completo, allora la sua dimensione è  $(n - 1)(d + 1) - 1$  e, essendo  $\dim L_E(n) \geq \dim L_E(1) + \dim L_E(n - 1)$ , basta dimostrare che esiste  $D \in L_E(n)$  che non contiene sezioni iperpiane. Se  $v_n: \mathbb{P}^d \rightarrow \mathbb{P}^?$  è la  $n$ -esima immersione di Veronese, applicare l'Esercizio 17.16 alla curva  $X = v_n(E)$  ed al sistema lineare  $L = L_E(1)$ .)

## Miscellanea di esercizi

### Capitolo 4

**18.1 (\*)**. Nelle stesse notazioni dell'Esercizio 3.41, provare che se il campo  $\mathbb{K}$  è algebricamente chiuso,  $s = 1$  e  $V$  è generato dal vettore  $(1, 1, \dots, 1)$ , allora  $S^V$  è la sottoalgebra generata da  $x_1, \dots, x_n$  e dalle forme quadratiche  $A_{ij} = x_i y_j - x_j y_i$ , per  $i < j$ . (Sugg.: se  $n = 1$  è ovvio; se  $n > 1$  e  $f \in S_{d_1, \dots, d_n, d}^V$  svolgere nell'ordine:

1. Se  $f$  si annulla su  $X = \{A_{12} = 0\} \subset \mathbb{A}^{2n}$ , allora  $f = (x_1 y_2 - x_2 y_1)g$ , con  $g \in S^V$ .
2.  $d_1 + d_2 + \dots + d_n \geq 2d$ : supponiamo per fissare le idee che  $d_2 > 0$ ; se  $f$  non soddisfa la condizione 1) allora esistono  $a_1, a_2, b_1, b_2 \in \mathbb{K}$  tali che  $a_1 b_2 = a_2 b_1$  ed il polinomio  $f(a_1, a_2, x_3, \dots, x_n, b_1, b_2, \dots, y_n)$  non è identicamente nullo. I valori  $a_2$  e  $b_2$  non possono essere entrambi nulli e quindi esiste  $\alpha \in \mathbb{K}$  tale che  $f(\alpha x_2, x_2, \dots, x_n, \alpha y_2, y_2, \dots, y_n) \neq 0$ ; induzione su  $n$ .
3. Assumiamo per fissare le idee  $d_1 > 0$ . Se  $x_1$  divide  $f$ , allora  $f = x_1 g$  con  $g \in S^V$ ; viceversa si ha  $f(0, x_2, \dots, y_n) = y_1^{d_1} g$  con  $g \in \mathbb{K}[x_2, \dots, x_n, y_2, \dots, y_n]^V$  ed il grado in  $x$  di  $g$  è maggiore o uguale al grado in  $y$  aumentato di  $d_1$ . Dedurre che esiste un polinomio  $p \in S_{d_1, \dots, d_n, d}^V$  nelle variabili  $x_i, A_{ij}$  tale che  $f - p$  è divisibile per  $x_1$ . Induzione su  $\sum d_i$ .)

### Capitolo 6

**18.2**. Provare che le coniche tangenti ad una retta data sono una quadrica non degenera di  $|\mathcal{O}(2)|$ .

### Capitolo 7

**18.3**. Sia  $(\mathbb{K}, |\cdot|)$  un campo normato e sia  $n > 0$  un intero positivo fissato; denotiamo con  $\sigma_1, \dots, \sigma_n: \mathbb{K}^n \rightarrow \mathbb{K}$  le funzioni simmetriche elementari. Provare che:

1. Rispetto alla topologia prodotto su  $\mathbb{K}^n$ , le funzioni  $\sigma_i$  sono continue.
2. Per ogni  $\epsilon > 0$  esiste  $\delta > 0$  tale che se  $|\sigma_i(a_1, \dots, a_n)| < \delta$  per ogni  $i$ , allora  $|a_i| < \epsilon$  per ogni  $i$ . (Sugg.: non è restrittivo assumere  $\max |\sigma_i(a)| = \delta < 1/n$ ; sia  $j$  indice fissato e sia  $t = |a_j|$  dalle relazioni  $\sum \pm \sigma_i(a) a_j^{n-i} = 0$  si ottiene  $t^n \leq \delta(1 + t + \dots + t^{n-1})$ . Basta osservare che  $t^n \geq \min(t^n, 1)(1 + t + \dots + t^{n-1})/n$ .)

3. Per ogni  $\epsilon, M > 0$  esiste  $\delta > 0$  con la seguente proprietà: se  $a = (a_1, \dots, a_n)$  e  $b = (b_1, \dots, b_n) \in \mathbb{K}^n$  sono tali che  $|a_1| < M$  e  $|\sigma_i(a) - \sigma_i(b)| < \delta$  per ogni  $i$ , allora si ha  $|a_1 - b_j| < \epsilon$  per qualche  $j = 1, \dots, n$ . (Sugg.: sia  $g(x) = \prod(x - b_i)$ ,  $f(x) = \prod(x - a_i)$ , allora  $|g(a_1)| = |g(a_1) - f(a_1)| \leq \delta(M^{n-1} + \dots + 1)$ .)

**18.4.** Sia  $(\mathbb{K}, |\cdot|)$  un campo normato algebricamente chiuso. Provare che il suo completamento metrico è ancora un campo algebricamente chiuso.

**18.5.** Sia  $(\mathbb{K}, |\cdot|)$  un campo normato. Provare che se  $\mathbb{K} - \{0\}$  è connesso, allora  $\mathbb{K}^n - V$  è un aperto denso e connesso per ogni sottospazio vettoriale proprio  $V \subset \mathbb{K}^n$ .

**18.6.** Sia  $(\mathbb{K}, |\cdot|)$  un campo normato. Dimostrare che se  $\mathbb{K}$  è completo e  $\mathbb{K} - \{0\}$  è connesso, allora  $\mathbb{K}$  è algebricamente chiuso. (Sugg.: ripetere la dimostrazione fatta nel caso  $\mathbb{K} = \mathbb{C}$  utilizzando gli Esercizi 18.3, 18.4, 18.5.)

## Capitolo 9

**18.7.** Siano  $\mathbb{P}^{14}$  lo spazio proiettivo delle quartiche piane e  $U \subset \mathbb{P}^{14}$  l'insieme delle quartiche lisce  $C$  tali che  $\nu_p(C, L) \leq 3$  per ogni  $p \in C$  e per ogni retta  $L \subset \mathbb{P}^2$ . Dimostrare che  $U$  è un aperto non vuoto.

## Capitolo 10

**18.8.** (caratteristica  $\neq 2$ ) Sia  $X \cong \mathbb{P}^5$  il sistema lineare completo delle coniche di  $\mathbb{P}^2$  e  $Y \cong \mathbb{P}^5$  il sistema lineare completo delle coniche di  $(\mathbb{P}^2)^\vee$ . Siano inoltre  $U \subset X$  e  $V \subset Y$  gli aperti delle coniche lisce. Provare che  $U$  e  $V$  sono varietà affini e che l'applicazione  $\phi: U \rightarrow V$ ,  $\phi(C) = C^\vee$ , è un isomorfismo regolare di varietà.

**18.9.** (caratteristica  $\neq 2, 3$ ) Sia  $C \subset \mathbb{P}^2$  una cubica piana liscia e denotiamo con  $j: C \rightarrow \mathbb{K}$  l'applicazione che al punto  $p \in C$  associa l'invariante  $j$  della quaterna di Salmon di  $(C, p)$ . Provare che  $j$  è una funzione regolare e si usi questo fatto per una dimostrazione alternativa del teorema di Salmon 6.3.6.

## Capitolo 16

**18.10.** Usare la disuguaglianza di Riemann (Esercizio 17.9) per dare una dimostrazione alternativa del Lemma 16.1.4.

## Capitolo 17

**18.11.** Sia  $C \subset \mathbb{P}^2$  una curva piana irriducibile di grado  $d \geq 2$  e siano  $p_1, \dots, p_r \in C$  i suoi punti singolari. Dimostrare che se

$$\sum_{i=1}^r \text{mult}_{p_i}(C)(\text{mult}_{p_i}(C) - 1) = (d - 1)(d - 2),$$

allora  $C$  è una curva razionale. (Sugg.: esiste una curva liscia  $X$  ed un morfismo birazionale  $\phi: X \rightarrow C \subset \mathbb{P}^2$ ; i divisori del sistema lineare  $L_\phi(d - 1)$  hanno grado  $d(d - 1)$ . Siano  $q_1, \dots, q_{2d-3} \in C$  punti lisci e distinti; mostrare che l'insieme dei divisori  $\phi^*(H)$ , al variare di  $H$  tra le curve piane di grado  $d - 1$  che passano per  $q_1, \dots, q_{2d-3}$  e tali che  $\text{mult}_{p_i}(H) \geq \text{mult}_{p_i}(C) - 1$ , è un sistema lineare di dimensione  $\geq 1$ . Usare il Teorema di Bézout e l'Esercizio 14.23 per provare che la parte fissa ha grado  $d(d - 1) - 1$ .)



---

## Riferimenti bibliografici

*Bibliografia non esaustiva*

- Al1924. G. Albanese: *Trasformazione birazionale di una curva algebrica qualunque in un'altra priva di punti multipli*. Rend. R. Acc. Naz. Lincei (V) **33-I** (1924) 13-14.
- An1977. A. Andreotti: *Note su un corso di geometria algebrica*. Scuola Normale Superiore a.a. 1977/78.
- ACGH1984. E. Arbarello, M. Cornalba, P. Griffiths, J. Harris: *Geometry of algebraic curves, I*. Springer (1984).
- Art1968. M. Artin: *On the solutions of analytic equations*. Invent Math. **5** (1968) 277-291.
- AM1969. M.F. Atiyah, I.G. Macdonald: *Introduction to commutative algebra*. Addison-Wesley, Reading, Mass. (1969).
- BK1986. E. Brieskorn, H. Knörrer: *Plane algebraic curves*. Birkhäuser, Basel (1986).
- Cay1871. A. Cayley: *On the porism of the in-and-circumscribed polygon and the (2,2) correspondence of points on a conic*. Quart. Math. Jour. t. XI (1871) 83-91.
- Cia1919. E. Ciani: *Lezioni di geometria proiettiva ed analitica*. Pisa (1919).
- Cre1862. L. Cremona: *Introduzione ad una teoria geometrica delle curve piane*. Bologna (1862).
- Cool1931. J. Coolidge: *A treatise on Algebraic Plane Curves*. Oxford University press (1931).
- Die1974. J. Dieudonné: *Cours de géométrie algébrique*. Presses Universitaires de France (1974).
- EGH1996. D. Eisenbud, M. Green, J. Harris: *Cayley-Bacharach theorems and conjectures*. Bulletin AMS **33** (1996).
- Enr1898. F. Enriques: *Lezioni di geometria proiettiva*. Zanichelli (1898).
- EC1915. F. Enriques, O. Chisini: *Lezioni sulla teoria geometrica delle equazioni e delle funzioni algebriche*. I,II,III,IV, Zanichelli Bologna (1915),(1918),(1924),(1934).
- Ful1969. W. Fulton: *Algebraic Curves: an introduction to algebraic geometry*. Benjamin (1969).
- Ful1984. W. Fulton: *Intersection theory*. Springer-Verlag Ergebnisse der Mathematik **2** (1984).
- GKZ1994. I. Gelfand, M. Kapranov, A. Zelevinsky: *Discriminants, resultants and multidimensional determinants*. Birkhäuser Boston (1994).
- GRT1980. F. Gherardelli, L.A. Rosati, G. Tomassini: *Lezioni di Geometria*. (2 volumi) Cedam Padova (1980).
- GH1978. P. Griffiths, J. Harris: *Principles of Algebraic Geometry*. Wiley-Interscience publication (1978).
- GR1965. R. Gunning, H. Rossi: *Analytic functions of several complex variables*. Prentice-Hall (1965).
- Halm1960. P.R. Halmos: *Naive set theory*. D. Van Nostrand Co. Princeton, N.J. (1960).
- Harr1992. J. Harris: *Algebraic Geometry: a first course*. Springer Verlag GTM **133** (1992).
- Hart1977. R. Hartshorne: *Algebraic geometry*. Springer-Verlag GTM **52** (1977).
- Her1982. I.N. Herstein: *Algebra*. Editori Riuniti (1982).
- Hilb1890. D. Hilbert: *Ueber die Theorie der algebraischen Formen*. Math. Ann. **36** (1890) 473-534.
- Hilb1893. D. Hilbert: *Ueber die vollen Invariantensysteme*. Math. Ann. **42** (1893) 313-373.

- Hilb1993. D. Hilbert: *Theory of algebraic invariants*. Cambridge Univ. Press (1993).
- Hilt1932. H. Hilton: *Plane algebraic curves*. Oxford University Press (1932).
- Hum1973. J. Humphreys: *Introduction to Lie algebras and representation theory*. Springer-Verlag GTM **9** (1973).
- Kapl1974. I. Kaplansky: *Commutative rings*. The University of Chicago Press (1974).
- Kemp1993. G.R. Kempf: *Algebraic Varieties*. Cambridge Univ. Press (1993).
- KL1972. S.L. Kleiman, D. Laksov: *Schubert calculus*. Amer. Math. Monthly **79** (1972) 1061-1082.
- Ko1996. J. Kollár: *Rational curves on algebraic varieties*. Springer-Verlag Ergeb. **32** (1996).
- KR1984. J. Kung, G. Rota. *The invariant theory of binary forms*. Bull. A.M.S. **10** (1984) 27-85.
- Lang1984. S. Lang: *Algebra*. Addison-Wesley, second edition (1984).
- Man2004. M. Manetti: *Nullstellensatz per tutti*. Ricordando Franco Conti, Pubbl. Cent. Ric. Mat. Ennio Giorgi, Scuola Norm. Sup., Pisa (2004) 235-244.
- Man2008. M. Manetti: *Topologia* Springer-Verlag Italia, Milano (2008).
- Mat1986. H. Matsumura: *Commutative Ring Theory*. Cambridge University Press (1986).
- Mum1976. D. Mumford: *Algebraic geometry I: Complex Projective Varieties*. Springer-Verlag GMW **221** (1976).
- Reid1988. M. Reid: *Undergraduate algebraic geometry*. Cambridge Univ. Press (1988).
- Ser1956. J.P. Serre: *Géométrie algébrique et géométrie analytique*. Ann. Inst. Fourier **6** (1956) 1-42.
- Ser1959. J.P. Serre: *Groupes algébriques et corps de classes*. Hermann Paris (1959).
- Sev1906. F. Severi: *Complementi di geometria proiettiva*. Zanichelli (1906).
- Shaf1972. I.R. Shafarevich: *Basic algebraic geometry*. Springer-Verlag (1972).
- Sil1986. J.H. Silverman: *The arithmetic of elliptic curves*. Springer-Verlag New York (1986).
- Stu1998. B. Sturmfels: *Introduction to resultants*. Proc. Symp. Appl. Math. **53** (1998) 25-39.
- Walk1950. R.J. Walker: *Algebraic curves*. Princeton (1950).
- Weil1982. A. Weil: *Adeles and algebraic groups*. Lectures at I.A.S. Princeton 1959-60. Ristampato da Birkhäuser Progress in Math. **23** (1982).
- Zar1962. O. Zariski: *The theorem of Riemann-Roch for high multiples of an effective divisor on an algebraic surface*. Ann. of Math. **76** (1962).