ISTITUZIONI DI GEOMETRIA SUPERIORE 2019-20 PER GLI INDIRIZZI DIDATTICO E APPLICATIVO

MARCO MANETTI A ROMA

Versione preliminare del **10 aprile 2020***:*
l'autore ringrazia tutti coloro che segnalano ed hanno segnalato errori ed imprecisioni

Indice

1. Preliminari di teoria dei gruppi

Inizia qui la prima parte delle dispense dedicata all'omologia simpliciale e persistente.

Salvo avviso contrario tutti i gruppi sono considerati abeliani e scritti in notazione additiva, con elemento neutro 0, inverso $-x$ e $nx = x + \cdots + x$ (n-volte) per $n \in \mathbb{Z}$.

Con $\mathbb{Q}^n$ intenderemo lo spazio vettoriale numerico sul campo $\mathbb{Q}$ dei vettori colonna ad n componenti e con $\mathbb{Z}^n \subset \mathbb{Q}^n$ il sottogruppo dei vettori a coordinate intere. Quando ciò non creerà problemi, per semplicità di scrittura in molte occasioni spianeremo le colonne, scrivendo

$$(a_1, \dots, a_n) \in \mathbb{Z}^n \text{ con lo stesso significato di } (a_1, \dots, a_n)^T = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{Z}^n .$$

Useremo i simboli $\subset$ e $\subseteq$ con lo stesso significato di inclusione non necessariamente propria.

Iniziamo con due semplicissimi risultati la cui evidenziatura è motivata dal fatto che entrano, mutatis mutandis[1], come assiomi in alcune teorie avanzate (non trattate in queste note) e molto astratte come ad esempio l'*omotopia algebrica*.

Lemma 1.1 (Regola del 2 su 3)**.** *Siano $A \xrightarrow{f} B \xrightarrow{g} C$ due omomorfismi di gruppi. Se due qualsiasi dei tre omomorfismi f, g, gf sono isomorfismi, allora lo è anche il terzo.*

Dimostrazione. Consideriamo il caso in cui f e gf sono isomorfismi, lasciando gli altri due per esercizio. Dato che gf è surgettivo, anche g è surgettivo. Se $g(b) = 0$ con $b \in B$, allora possiamo scrivere $b = f(a)$, dunque $gf(a) = 0$ e poiché gf è iniettivo ne consegue che $a = 0$ ed a maggior ragione $b = f(0) = 0$. □

Lemma 1.2 (Regola del 2 su 6)**.** *Dato un diagramma commutativo*

$$\begin{array}{ccc} A & \longrightarrow & B \\ {\scriptstyle f}\downarrow & \searrow & \downarrow{\scriptstyle g} \\ C & \longrightarrow & D \end{array}$$

di 4 gruppi e 6 omomorfismi, se f e g sono isomorfismi, allora sono isomorfismi pure i rimanenti quattro omomorfismi.

Dimostrazione. Per la regola del 2 su 3 è sufficiente dimostrare che la freccia diagonale da B a C è un isomorfismo. Diamo un nome anche ai rimanenti omomorfismi, trascurando per esigenze grafiche la freccia da A a D:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle f}\downarrow & \overset{\beta}{\swarrow} & \downarrow{\scriptstyle g} \\ C & \xrightarrow{\gamma} & D \end{array}$$

Si ha $f = \beta\alpha$ e $g = \gamma\beta$. Siccome f è surgettivo, anche β è surgettivo; siccome g è iniettivo, anche β è iniettivo. Dunque β è surgettivo e quindi un isomorfismo. □

[1] Mutatis mutandis = cambiando quel che c'è da cambiare.

Se A, B sono due sottogruppi di un gruppo abeliano G, allora anche $A \cap B$ e

$$A + B = \{a + b \mid a \in A,\ b \in B\}$$

sono sottogruppi di G. Se G, H sono due gruppi abeliani, allora anche la loro **somma diretta**

$$G \oplus H = \{(x, y) \mid x \in G,\ y \in H\}$$

è un gruppo abeliano, con somma $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ ed elemento neutro $(0, 0)$. Ad esempio $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$. Si noti che esistono due inclusioni naturali $G \subset G \oplus H$, $H \subset G \oplus H$, dove ciascun $x \in G$ viene identificato con $(x, 0)$ e ciascun $y \in H$ viene identificato con $(0, y)$.

L'insieme degli omomorfismi tra due gruppi abeliani è ancora un gruppo abeliano, dove per $f, g \colon G \to H$ omomorfismi si definisce $f + g \colon G \to H$, $(f + g)x = f(x) + g(x)$.

Siano G un gruppo abeliano, $H \subseteq G$ un sottogruppo e $\pi \colon G \to G/H$ la proiezione al quoziente.

1) Esiste una bigezione naturale tra i sottogruppi di G/H ed i sottogruppi di G che contegono H. Secondo tale bigezione, ad un sottogruppo $K \subseteq G/H$ si associa il sottogruppo

$$\pi^{-1}(K) = \{x \in G \mid \pi(x) \in K\}$$

mentre ad un sottogruppo $H \subseteq M \subseteq G$ si associa il quoziente $M/H \subset G/H$.

2) Se $f \colon G \to P$ è un omomorfismo di gruppi, allora f si fattorizza al quoziente, ossia esiste $\overline{f} \colon G/H \to P$ tale che $f = \overline{f}\pi$ se e solo se $H \subseteq \ker(f)$. In tal caso, l'immagine di $\overline{f}$ è uguale all'immagine di f ed il nucleo di $\overline{f}$ è uguale a $\ker(f)/H$. In particolare: $\overline{f}$ è surgettiva se e solo se f è surgettiva; $\overline{f}$ è iniettiva se e solo se $\ker(f) = H$.

3) Sia adesso $A \subseteq G$ un sottogruppo. Dati $x \in G$ e $y \in A$ si ha $\pi(x) = \pi(y)$ se e solo se $x - y \in H$, ossia se e solo se esiste $h \in H$ tale che $x = y + h$. Da ciò segue che

$$\pi^{-1}(\pi(A)) = A + H = \{y + h \mid y \in A,\ h \in H\}$$

e di conseguenza che $\pi(A) = \dfrac{A + H}{H}$. È chiaro che il nucleo della restrizione $\pi \colon A \to G/H$ è $A \cap H$. In conclusione si ha:

(1) $\pi \colon A \to G/H$ iniettiva se e solo se $A \cap H = 0$;
(2) $\pi \colon A \to G/H$ surgettiva se e solo se $A + H = G$.

Sono inoltre fatti ben noti:

(1) ogni gruppo abeliano finito G è somma diretta di gruppi ciclici:

$$G = \frac{\mathbb{Z}}{(n_1)} \oplus \cdots \oplus \frac{\mathbb{Z}}{(n_k)}\,.$$

(2) se un primo p divide l'ordine di un gruppo finito G, allora esiste un elemento $x \in G$ tale che $x \neq 0$, $px = 0$.

Sia G un gruppo abeliano. In analogia con il caso degli spazi vettoriali, diremo che un sottoinsieme $E \subset G$ **forma una base** di G se ogni $x \in G$ può essere scritto in modo unico come combinazione lineare finita a coefficienti interi di elementi di E. Più dettagliatamente, E forma una base di G se:

(1) per ogni $x \in G$ esistono $e_1, \ldots, e_n \in E$ e $a_1, \ldots, a_n \in \mathbb{Z}$ tali che $x = \sum a_i e_i$;
(2) se, per dati $e_1, \ldots, e_n \in E$ elementi distinti e $a_1, \ldots, a_n \in \mathbb{Z}$ interi vale $\sum a_i e_i = 0$, allora $a_i = 0$ per ogni i.

A differenza degli spazi vettoriali non tutti i gruppi abeliani possiedono una base. Ad esempio in un gruppo finito G di ordine $n > 0$, per ciascun elemento $e \in E$ vale $ne = 0$ e quindi la precedente condizione (2) è soddisfatta solo da $E = \emptyset$.

Definizione 1.3. Un gruppo abeliano che possiede una base viene detto **gruppo abeliano libero**.

Ad esempio, per ogni $n \geq 0$ il gruppo $\mathbb{Z}^n$ è abeliano libero in quanto ogni suo elemento si scrive in maniera unica come combinazione lineare a coefficienti interi della base canonica:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_1 \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_n \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Ovviamente esistono altre basi di $\mathbb{Z}^n$ oltre alla base canonica, completamente determinate dal seguente lemma.

Lemma 1.4. *Sia $B \in M_{n,n}(\mathbb{Z})$ una matrice $n \times n$ a coefficienti interi. Allora le colonne di B formano una base di $\mathbb{Z}^n$ se e solo se $\det(B) = \pm 1$.*

Dimostrazione. La condizione $\det(B) = \pm 1$ è del tutto equivalente a dire che B è invertibile con inversa B^{-1} a coefficienti interi. Infatti se $\det(B) = \pm 1$ allora

$$B^{-1} = \frac{\text{(aggiunta classica)}}{\det(B)} = \frac{\text{(matrice dei cofattori)}^T}{\det(B)} \in M_{n,n}(\mathbb{Z}),$$

mentre se $B^{-1} \in M_{n,n}(\mathbb{Z})$ allora $\det(B^{-1}) \in \mathbb{Z}$ e siccome $\det(B^{-1}) = \det(B)^{-1}$ deve essere $\det(B) = \det(B^{-1}) = \pm 1$.

Dunque l'omomorfismo

$$B \colon \mathbb{Z}^n \to \mathbb{Z}^n, \qquad a \mapsto Ba \text{ (solito prodotto righe per colonne)},$$

è un isomorfismo di gruppi se e solo se $\det(B) = \pm 1$. D'altra parte è chiaro che un omomorfismo di gruppi abeliani liberi è un isomorfismo se e solo se trasforma basi in basi. □

Lemma 1.5. *Siano G un gruppo abeliano ed $E \subset G$ un suo sottoinsieme. Allora E forma una base se e solo se per ogni gruppo abeliano H ed ogni applicazione (di insiemi) $F \colon E \to H$ vi è un unico omomorfismo di gruppi $f \colon G \to H$ tale che $F(e) = f(e)$ per ogni $e \in E$.*

Dimostrazione. Se E forma una base di G, allora ogni applicazione $F \colon E \to H$ a valori in un gruppo abeliano H si estende ad un omomorfismo $f \colon G \to H$ tramite la formula

$$f(a_1e_1 + \cdots + a_ne_n) = a_1F(e_1) + \cdots + a_nF(e_n), \qquad a_i \in \mathbb{Z}, \quad e_i \in E, \tag{1.1}$$

ed il fatto per E di essere una base implica che f è ben definito.

L'implicazione inversa, essendo meno rilevante ai fini di queste note, viene lasciata per esercizio al lettore. □

In particolare, se G_1, G_2 sono gruppi abeliani liberi con basi E_1, E_2, allora ogni applicazione $F \colon E_1 \to E_2$ si estende in maniera unica ad un omomorfismo di gruppi $f \colon G_1 \to G_2$, che quindi risulta determinato dalla formula di estensione lineare (1.1); è chiaro che F è iniettiva (risp.: surgettiva) se e solo se f è iniettiva (risp.: surgettiva).

In particolare, se E_1, E_2 hanno la stessa cardinalità allora i due gruppi G_1, G_2 sono isomorfi[2].

Definizione 1.6. Dato un qualunque insieme E denotiamo con $\mathbb{Z}^{(E)}$ il gruppo abeliano di tutte le combinazioni lineari formali finite a coefficienti interi di elementi di E.

Per le usuali regole distributive ogni elemento di $\mathbb{Z}^{(E)}$ si scrive in maniera unica in forma ridotta, ossia come $a_1e_1 + \cdots + a_ne_n$, con $a_i \in \mathbb{Z}$, $e_i \in E$, $a_i \neq 0$ ed $e_i \neq e_j$ per ogni $i \neq j$ (unica a meno di permutazioni degli addendi a_ie_i, ovviamente):

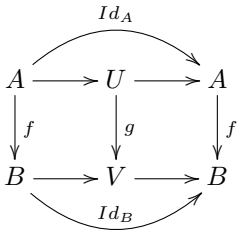
$$\mathbb{Z}^{(E)} = \{0\} \cup \{ae \mid a \in \mathbb{Z} - \{0\},\ e \in E\} \cup \{a_1e_1 + a_2e_2 \mid a_i \in \mathbb{Z} - \{0\},\ e_i \in E,\ e_1 \neq e_2\} \cup \cdots.$$

Identificando ciascun $e \in E$ con $1e \in \mathbb{Z}^{(E)}$ è chiaro per costruzione che E è una base di $\mathbb{Z}^{(E)}$. Chiameremo $\mathbb{Z}^{(E)}$ il **gruppo abeliano libero generato da** E. Ad esempio, il gruppo $\mathbb{Z}^n$ si identifica naturalmente con il gruppo abeliano libero generato dalla base canonica di $\mathbb{Q}^n$.

Esercizi:

[2] È vero anche il viceversa [13, Esercizio 14.8], ma la dimostrazione non è affatto banale in quanto non è detto che un ipotetico isomorfismo $G_1 \to G_2$ sia indotto da un'applicazione $E_1 \to E_2$.

Esercizio 1 (retrazioni)**.** Con il termine retrazione si intende un diagramma commutativo di omomorfismi di gruppi



ed in tal caso diremo che f è un retratto di g.

(1) Dimostrare che la relazione di retrazione gode della proprietà transitiva, ossia che se f è un retratto di g e se g è un retratto di h, allora f è un retratto di h.
(2) Sia f un retratto di g, dimostrare che se g è iniettiva (risp.: surgettiva), allora anche f è iniettiva (risp.: surgettiva).
(3) Sia $e\colon G \to G$ un'omomorfismo di gruppi tale che $e^2 = e$ e si denoti
$$H = \{x \in G \mid e(x) = x\}.$$
Dimostrare che:
   (a) H è un sottogruppo di G che coincide con l'immagine di e;
   (b) siano $i\colon H \to G$ il morfismo di inclusione e $p\colon G \to H$ l'unico omomorfismo tale che $ip = e$. Allora i e p sono entrambe dei retratti di e.

Esercizio 2. Siano A, B, C tre sottogruppi di un gruppo abeliano G, si assuma $C \subseteq A \cap B$ in modo tale che la composizione dell'inclusione $A \subset G$ con la proiezione al quoziente $G \to G/B$ si fattorizza ad un omomorfismo di gruppi quoziente $f\colon \dfrac{A}{C} \to \dfrac{G}{B}$. Provare che f è surgettivo se e solo se $A + B = G$ e che f è iniettivo se e solo se $C = A \cap B$.

Esercizio 3. Provare il gruppo $\mathbb{Q}$ non è abeliano libero. Più in generate provare che se G è un gruppo abeliano libero allora l'unico omomorfismo $\mathbb{Q} \to G$ è quello banale.

Esercizio 4. Provare che un gruppo finito T non è abeliano libero. Più in generate provare che se G è un gruppo abeliano libero allora l'unico omomorfismo $T \to G$ è quello banale.

Esercizio 5. Siano n un intero, p un numero primo e $f\colon \mathbb{Z}^n \to \mathbb{Z}/(p)$ un omomorfismo surgettivo. Provare che esistono due isomorfismi di gruppi $\alpha\colon \mathbb{Z}^n \to \mathbb{Z}^n$ e $\beta\colon \mathbb{Z}/(p) \to \mathbb{Z}/(p)$ tali che
$$\beta f \alpha(a_1, \ldots, a_n) \equiv a_1 \pmod{p},$$
e dedurre che $\ker(f) \cong \mathbb{Z}^n$. (Suggerimento: dimostrare preliminarmente che esistono due isomorfismi di gruppi $\gamma\colon \mathbb{Z}^n \to \mathbb{Z}^n$ e $\beta\colon \mathbb{Z}/(p) \to \mathbb{Z}/(p)$ tali che $\beta f \gamma(1, 0, \ldots, 0) \equiv 1 \pmod{p}$.)

2. Successioni esatte

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). Tra le nuove nozioni troviamo anche quelle di *complesso*, *successione esatta*, nonché una tecnica di dimostrazione nota come *caccia al diagramma*.

La caccia al diagramma, dove il termine caccia non è inteso in senso venatorio ma allo stesso modo di caccia al tesoro, è un utile metodo di dimostrazione usato specialmente in algebra omologica. Dato un diagramma commutativo, la caccia al diagramma sfrutta in maniera formale alcune proprietà del diagramma stesso come l'iniettività o la surgettività di alcune applicazioni o come l'esattezza di alcune successioni.

Sappiamo già cosa sono le applicazioni iniettive e surgettive; introduciamo adesso il concetto di successione esatta: fra i tanti possibili diagrammi di gruppi abeliani ed omomorfismi, particolarmente importanti sono quelli a forma di stringa, ossia i diagrammi con le applicazioni disposte in serie:

$$\cdots \to G_n \xrightarrow{f_n} G_{n-1} \xrightarrow{f_{n-1}} G_{n-2} \to \cdots \tag{2.1}$$

Definizione 2.1. Un diagramma di omomorfismi di gruppi abeliani disposti in serie come in (2.1) si dice un **complesso** se $f_{n-1}f_n = 0$ per ogni n, ossia se la composizione di omomorfismi contigui è sempre nulla.

Equivalentemente il diagramma (2.1) è un complesso se per ogni n l'immagine di f_n è contenuta nel nucleo di f_{n-1}. Un complesso si dice finito o limitato se contiene solo un numero finito di spazi vettoriali ed applicazioni lineari; tuttavia è utile, in vista di future applicazioni, considerare anche complessi infiniti o illimitati, nei quali gli indici n che compaiono nel diagramma sono tutti gli interi contenuti in un intervallo della retta reale.

Naturalmente la scelta degli indici a pedice in (2.1) è puramente decorativa e possiamo anche denotare complessi in altre forme, come ad esempio:

$$\cdots \to G^n \xrightarrow{f_n} G^{n+1} \xrightarrow{f_{n+1}} G^{n+2} \to \cdots, \qquad \cdots \to G_a \xrightarrow{f_a} G_b \xrightarrow{f_b} G_c \to \cdots,$$

$$0 \to G_{\text{Adamo}} \to G_{\text{Caino}} \to \cdots \to G_{\text{nonno}} \to G_{\text{babbo}} \to G_{\text{me}} \to 0\,.$$

Definizione 2.2. Un diagramma di omomorfismi di gruppi abeliani disposti in serie come in (2.1) si dice una **successione esatta** se per ogni n il nucleo di f_{n-1} è uguale all'immagine di f_n.

In particolare ogni successione esatta è anche un complesso, mentre il viceversa è generalmente falso: ad esempio, il diagramma

$$0 \to G \to 0$$

è un complesso qualunque sia il gruppo G, mentre è una successione esatta se e solo se $G = 0$.

Esempio 2.3. Supponiamo che

$$G_3 \xrightarrow{f_3} G_2 \xrightarrow{f_2} G_1 \xrightarrow{f_1} G_0$$

sia una successione esatta. Allora le seguenti condizioni sono equivalenti:

(1) f_3 è surgettiva;
(2) $f_2 = 0$;
(3) f_1 è iniettiva.

Infatti, per l'esattezza in G_1 il nucleo di f_1 è uguale all'immagine di f_2; in particolare f_2 è nulla se e solo se $\ker f_1 = 0$, ossia se e solo se f_1 è iniettiva. Similmente, per l'esattezza in G_2 il nucleo di f_2 è uguale all'immagine di f_3 ed in particolare $f_2 = 0$ se e solo se f_3 è surgettiva.

Esempio 2.4. Supponiamo che

$$G_0 \xrightarrow{f_0} G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \xrightarrow{f_3} G_4$$

sia una successione esatta. Allora le seguenti condizioni sono equivalenti:

(1) f_0 è surgettiva e f_3 è iniettiva;
(2) $f_1 = f_2 = 0$;
(3) $G_2 = 0$.

I ragionamenti da fare sono analoghi a quelli dell'esempio precedente e lasciati per esercizio al lettore.

Definizione 2.5. Una **successione esatta corta** è una successione esatta del tipo

$$0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0\,. \tag{2.2}$$

Dunque, la (2.2) è una successione esatta corta se e solo se f è iniettiva, g è surgettiva e $\ker g = f(U)$.

In particolare, se (2.2) è una successione esatta si ha $W = g(V)$ e $f\colon U \to \ker g$ è un isomorfismo.

Esempio 2.6. Consideriamo una successione esatta

$$0 \to V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} V_3 \xrightarrow{f_3} V_4 \to 0\,;$$

indichiamo con $U = \ker f_3 = f_2(V_2)$ e con $i\colon U \to V_3$ il morfismo di inclusione. Allora la precedente successione si *spezza* in due successioni esatte corte

$$0 \to V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} U \to 0, \qquad 0 \to U \xrightarrow{i} V_3 \xrightarrow{f_3} V_4 \to 0.$$

Teorema 2.7 (Lemma dei 5)**.** *Sia dato il seguente diagramma commutativo di gruppi abeliani:*

$$\begin{array}{ccccccccc} E_1 & \xrightarrow{d_1} & E_2 & \xrightarrow{d_2} & E_3 & \xrightarrow{d_3} & E_4 & \xrightarrow{d_4} & E_5 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \alpha_4} & & \downarrow{\scriptstyle \alpha_5} \\ H_1 & \xrightarrow{h_1} & H_2 & \xrightarrow{h_2} & H_3 & \xrightarrow{h_3} & H_4 & \xrightarrow{h_4} & H_5 \end{array}$$

con entrambe le righe esatte.

(1) *se α_1 è surgettiva e α_2, α_4 sono iniettive, allora β è iniettiva;*
(2) *se α_5 è iniettiva e α_2, α_4 sono surgettive, allora β è surgettiva;*
(3) *se $\alpha_1, \alpha_2, \alpha_4, \alpha_5$ sono bigettive, allora β è bigettiva.*

Dimostrazione. Dimostriamo solo il primo punto; la dimostrazione del secondo è del tutto simile ed è lasciata per esercizio. Il terzo punto segue banalmente dai primi due.

Sia $x \in E_3$ tale che $\beta(x) = 0$, allora $\alpha_4 d_3(x) = h_3\beta(x) = 0$ ed essendo per ipotesi α_4 iniettiva si ha $d_3(x) = 0$. La prima riga è esatta e quindi esiste $y \in E_2$ tale che $x = d_2(y)$; siccome $h_2\alpha_2(y) = \beta d_2(y) = \beta(x) = 0$ e la riga inferiore è esatta, esiste $z \in H_1$ tale che $h_1(z) = \alpha_2(y)$. Adesso usiamo la surgettività di α_1 per trovare $w \in E_1$ tale che $\alpha_1(w) = z$, quindi $\alpha_2 d_1(w) = h_1\alpha_1(w) = h_1(z) = \alpha_2(y)$. Per l'iniettività di α_2 si ha $y = d_1(w)$ e quindi $x = d_2(y) = d_2 d_1(w) = 0$. □

Data una successione esatta corta $0 \to A \to B \to C \to 0$ di gruppi abeliani, in generale i due gruppi B e $A \oplus C$ non sono isomorfi, come ad esempio nella successione esatta

$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{d} \mathbb{Z}/(2) \to 0\,.$$

Tuttavia, il lemma dei 5 permette di dimostrare in maniera rapidissima il seguente criterio standard

Corollario 2.8. *Sia $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ una successione esatta corta di gruppi abeliani. Se esiste un omomorfismo $h\colon C \to B$ tale che $gh = \mathrm{Id}_C$, allora esiste un isomorfismo $A \oplus C \cong B$.*

Dimostrazione. Sia $h\colon C \to B$ un omomorfismo tale che $gh = \mathrm{Id}_C$, allora l'applicazione $\beta\colon A \oplus C \to B$, $\beta(a, c) = f(a) + h(c)$, è un omomorfismo di gruppi che si innesta nel diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & A \oplus C & \xrightarrow{\pi} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Id}_A} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \mathrm{Id}_C} & & \\ 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \end{array}$$

dove π ed i sono la proiezione e l'inclusione naturale. Adesso il Teorema 2.7 implica che β è un isomorfismo. □

Corollario 2.9. *Sia $g\colon G \to \mathbb{Z}^n$ un omomomorfismo surgettivo di gruppi abeliani. Allora esiste un isomorfismo (non canonico) di gruppi abeliani $G \cong \ker(g) \oplus \mathbb{Z}^n$.*

Dimostrazione. Per ipotesi esiste una successione esatta corta $0 \to \ker(g) \xrightarrow{i} G \xrightarrow{g} \mathbb{Z}^n \to 0$ e per il Corollario 2.8 basta dimostrare che esiste un omomorfismo $h\colon \mathbb{Z}^n \to G$ tale che $gh = \mathrm{Id}_{\mathbb{Z}^n}$.

Siano $y_1, \ldots, y_m \in G$ le cui immagini tramite g siano la base canonica; questo equivale a dire che

$$g(a_1y_1 + \cdots + a_my_m) = (a_1, \ldots, a_m), \text{ per ogni } a_1, \ldots, a_m \in \mathbb{Z}$$

e quindi che la composizione di g con l'omomorfismo

$$h\colon \mathbb{Z}^m \to G, \qquad h(a_1, \ldots, a_m) = a_1y_1 + \cdots + a_my_m,$$

è l'identità su $\mathbb{Z}^n$. □

Esercizi:

Esercizio 6. Si consideri il diagramma commutativo di gruppi abeliani

$$\begin{array}{ccccccc}
 & & & & & & 0 \\
 & & & & & & \downarrow \\
 & & & & N_1 & \longrightarrow & M_1 & \longrightarrow & P_1 \\
 & & & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & N_2 & \longrightarrow & M_2 & \longrightarrow & P_2 \\
 & & \downarrow & & \downarrow & & \\
 & & N_3 & \xrightarrow{f} & M_3 & & \\
 & & \downarrow & & & & \\
 & & 0 & & & &
\end{array}$$

in cui tutte le righe e tutte le colonne sono successioni esatte. Provare che l'applicazione f è iniettiva.

Esercizio 7. Si consideri un diagramma commutativo di spazi vettoriali di dimensione finita e applicazioni lineari

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0\,. \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0
\end{array}$$

Dimostrare che il polinomio caratteristico di β è il prodotto dei polinomi caratteristici di α e γ.

3. Gruppi abeliani finitamente generati

Definizione 3.1. Sia G gruppo abeliano. Un elemento $x \in G$ è detto:

(1) **di torsione** se esiste un intero $n > 0$ tale che $nx = 0$;
(2) **divisibile** se per ogni intero $n > 0$ esiste $y \in G$ tale che $ny = x$;
(3) **primitivo** se $x \neq ny$ per ogni $y \in G$ ed ogni intero $n > 1$.

Il sottoinsieme degli elementi di torsione di G verrà indicato con $T(G)$. Il gruppo G si dice **senza torsione** se $T(G) = 0$. Il gruppo G si dice **di torsione** se $T(G) = G$.

Ad esempio, in un gruppo finito ogni elemento è di torsione. Il gruppo $\mathbb{Q}$ è senza torsione ed ogni suo elemento è divisibile. La torsione commuta con le somme dirette, ossia $T(G \oplus H) = T(G) \oplus T(H)$. Se $H \subseteq G$ è un sottogruppo si ha $T(H) = T(G) \cap H$. Si noti che un elemento non può essere contemporaneamente primitivo e di torsione, infatti se $nx = 0$ per qualche $n > 0$ allora $(n+1)x = x$ e quindi x non è primitivo.

Lemma 3.2. *Sia G un gruppo abeliano. Allora $T(G)$ è un sottogruppo di G ed il quoziente $G/T(G)$ è senza torsione.*

Dimostrazione. Chiaramente $0 \in T(G)$; se $x, y \in T(G)$ esistono due interi $n, m > 0$ tali che $nx = my = 0$ e quindi $nm(x \pm y) = 0$.

Dire che il quoziente $G/T(G)$ è senza torsione equivale a dire che se $x \in G$, $n > 0$ e $nx \in T(G)$, allora $x \in T(G)$. Ma se $m(nx) = 0$ per qualche $m > 0$ allora $(nm)x = 0$ e dunque $x \in T(G)$. □

Ogni omomorfismo di gruppi $f\colon G \to H$ si restringe ad un omomorfismo $f\colon T(G) \to T(H)$ tra i rispettivi sottogruppi di torsione. Infatti se $x \in T(G)$ e $nx = 0$ per qualche intero $n > 0$, allora $nf(x) = f(nx) = 0$ e quindi anche $f(x)$ è di torsione. In particolare se $G = T(G)$ e $T(H) = 0$ l'unico omomorfismo $f\colon G \to H$ è quello nullo: in altri termini, *non esistono omomorfismi non banali da un gruppo di torsione ad un gruppo senza torsione.*

Se S è un qualunque sottoinsieme di un gruppo abeliano G denoteremo con $\langle S \rangle \subset G$ il sottogruppo generato da S. Equivalentemente $\langle S \rangle$ è l'insieme di tutte le espressioni del tipo

$$n_1 s_1 + \cdots + n_k s_k, \qquad k \geq 0, \quad n_i \in \mathbb{Z}, \quad s_i \in S\,.$$

Per definizione, un elemento $x \in G$ non è di torsione se e solo se l'omomorfismo di gruppi

$$\mathbb{Z} \to G, \qquad n \mapsto nx$$

è iniettivo, e dato che l'immagine di tale omomorfismo è $\langle x \rangle$ si ha la seguente casistica:

(1) x è di torsione e $\langle x \rangle$ è un gruppo finito ciclico;
(2) x non è di torsione e $\langle x \rangle \simeq \mathbb{Z}$ è il gruppo ciclico infinito.

Lemma 3.3. *Siano G gruppo abeliano senza torsione e $x \in G$ primitivo. Allora il gruppo quoziente $G/\langle x \rangle$ è senza torsione.*

Dimostrazione. Per ogni $y \in G$ indichiamo con $\overline{y} \in G/\langle x \rangle$ la sua immagine al quoziente. Dire che $\overline{y}$ è di torsione vuol dire che esiste un intero $n > 0$ tale che $n\overline{y} = 0$, ossia $ny \in \langle x \rangle$. Sia $y \in G$ un elemento fissato tale che $ny \in \langle x \rangle$ per qualche $y \in G$ e qualche $n > 0$; vogliamo dimostrare che $y \in \langle x \rangle$. Sia n il più piccolo intero positivo tale che $ny \in \langle x \rangle$ e sia $m \in \mathbb{Z}$ tale che $ny = mx$. I due numeri n, m non hanno fattori comuni. Infatti se $p > 1$ divide sia n che m si avrebbe

$$p\left(\frac{n}{p}y - \frac{m}{p}x\right) = 0$$

e siccome G è senza torsione ne consegue $\frac{n}{p}y - \frac{m}{p}x = 0$ in contraddizione con la minimalità di n. Dunque esistono due interi a, b tali che $an + bm = 1$ e quindi

$$x = (an + bm)x = anx + bny = n(ax + by)$$

e poiché x è primitivo deve essere $n = 1$. □

Definizione 3.4. Diremo che un gruppo abeliano G è **finitamente generato** se è generato da un numero finito di elementi, ossia

$$G = \langle x_1, \ldots, x_n \rangle = \left\{ \sum_{i=1}^{n} a_i x_i \mid a_i \in \mathbb{Z} \right\}.$$

Ad esempio, ogni gruppo finito è finitamente generato (basta prendere come generatori tutti gli elementi). Il gruppo $\mathbb{Z}^n$ è senza torsione, è generato dalla "base canonica"

$$e_1 = (1, 0, \ldots, 0), \quad e_2 = (0, 1, \ldots, 0), \quad \ldots \quad , e_n = (0, 0, \ldots, 1),$$

ed è quindi finitamente generato. Se G è un gruppo finitamente generato e $f\colon G \to H$ è un omomorfismo surgettivo di gruppi, allora anche H è finitamente generato: se $x_1, \ldots, x_n$ generano G allora $f(x_1), \ldots, f(x_n)$ generano H. In particolare ogni quoziente di un gruppo finitamente generato è finitamente generato.

Lemma 3.5. *Un gruppo abeliano è finito se e solo se è finitamente generato e di torsione.*

Dimostrazione. Una implicazione è chiara, ogni gruppo finito è finitamente generato ed è di torsione. Viceversa, se un gruppo abeliano di torsione G è generato da $x_1, \ldots, x_n$ allora per ogni indice i esiste un intero $r_i > 0$ tale che $r_i x_i = 0$. Presa una qualunque combinazione lineare a coefficienti interi $y = a_1 x_1 + \cdots + a_n x_n$, sostituendo eventualmente ad ogni a_i il

resto della divisione per r_i non è restrittivo supporre $0 \leq a_i < r_i$. Ne segue che G possiede al più $r_1 r_2 \cdots r_n$ elementi distinti. □

Lemma 3.6. *Sia $f\colon G \to H$ un omomorfismo di gruppi abeliani con nucleo $K = \ker f$.*

(1) *Siano $A \subseteq B \subseteq G$ due sottogruppi. Se $f(A) = f(B)$ e $A \cap K = B \cap K$, allora $A = B$.*
(2) *Sia $B \subset G$ un sottogruppo. Se $B \cap K$ è generato da n elementi e $f(B)$ è generato da m elementi allora B è generato da $n + m$ elementi.*

Dimostrazione. (1) Sia $x \in B$, siccome $f(A) = f(B)$ esiste $y \in A$ tale che $f(x) = f(y)$. Quindi $f(x - y) = 0$ e $x - y \in K \cap B$. Per ipotesi $K \cap B \subset A$ e dunque $x = y + (x - y) \in A$.

(2) Siano $x_1, \ldots, x_n$ generatori di $B \cap K$ e $y_1, \ldots, y_m \in B$ tali che $f(y_1), \ldots, f(y_m)$ generano $f(B)$. Consideriamo il sottogruppo $A \subseteq B$ generato da $x_1, \ldots, x_n, y_1, \ldots, y_m$. Per costruzione A è generato da $n + m$ elementi, $A \subseteq B$, $A \cap K = B \cap K$ e $f(A) = f(B)$. Per il punto precedente $A = B$. □

Una delle differenze sostanziali tra il caso abeliano ed il caso generale è dato dal seguente risultato.

Teorema 3.7. *Sia G un gruppo abeliano generato da n elementi. Allora:*

(1) *ogni sottogruppo $A \subseteq G$ è generato da al più n elementi;*
(2) *ogni* catena ascendente *(= successione non decrescente infinita) di sottogruppi*

$$A_1 \subseteq A_2 \subseteq A_3 \subseteq A_4 \subseteq \cdots$$

è stazionaria, ossia esiste un intero N tale che $A_i = A_{i+1}$ per ogni $i \geq N$.

Dimostrazione. Dimostriamo il teorema per induzione su n. Il caso $n = 1$ è ben noto dal corso di Algebra 1. Infatti, per definizione i gruppi ciclici sono quelli generati da un solo elemento e sono:

(1) il gruppo ciclico infinito $\mathbb{Z}$, i cui sottogruppi sono 0 ed $(n) \simeq \mathbb{Z}$ con $n > 0$;
(2) i gruppi ciclici finiti $\mathbb{Z}/(n)$ i cui sottogruppi sono $\mathbb{Z}/(m)$ con m che divide n.

I gruppi ciclici finiti contengono un numero finito di sottogruppi e quindi ogni catena ascendente è ovviamente stazionaria. Ogni catena ascendente di sottogruppi di $\mathbb{Z}$ è del tipo

$$(n_1) \subseteq (n_2) \cdots, \qquad n_i \geq 0, \quad n_2 | n_1,\ n_3 | n_2, \ldots$$

Se $n_i = 0$ per ogni i non c'è nulla da dimostrare. Se $n_k > 0$ allora la successione non crescente $n_k \geq n_{k+1} \geq \cdots$ di interi positivi è stazionaria.

Supponiamo quindi $G = \langle x_1, \ldots, x_n \rangle$ con $n > 1$ ed il teorema vero per gruppi generati da $n - 1$ elementi. Consideriamo allora la proiezione al quoziente

$$f\colon G \to H = \frac{G}{\langle x_1 \rangle}.$$

Il gruppo H è generato dagli $n-1$ elementi $f(x_2), \ldots, f(x_n)$, mentre il nucleo di f è generato da x_1. Se $A \subset G$ è un sottogruppo, per l'ipotesi induttiva $f(A) \subseteq H$ è generato da al più $n - 1$ elementi e $A \cap \ker f \subseteq \ker f$ è un gruppo ciclico. La conclusione segue dal Lemma 3.6.

Se $A_1 \subseteq A_2 \subseteq \cdots$ è una successione crescente di sottogruppi, per l'ipotesi induttiva le due successioni

$$\ker f \cap A_1 \subseteq \ker f \cap A_2 \subseteq \cdots, \qquad f(A_1) \subseteq f(A_2) \subseteq \cdots$$

sono stazionarie e per il Lemma 3.6 anche $A_1 \subseteq A_2 \subseteq \cdots$ è stazionaria. □

Corollario 3.8. *Siano G un gruppo abeliano finitamente generato e $x \in G$. Se x non è di torsione, allora x è un multiplo intero di un elemento primitivo.*

Dimostrazione. Sia x non di torsione. Se x è primitivo abbiamo finito, altrimenti possiamo scrivere $x = n_1 x_1$ con $n_1 > 1$ e $x_1 \in G$. Se x_1 è primitivo abbiamo finito, altrimenti si ha $x_1 = n_2 x_2$ con $n_2 > 1$ e $x_2 \in G$. Se x_2 è primitivo allora $x = (n_1 n_2) x_2$, altrimenti si prosegue con una successione

$$x = n_1 x_1, \quad x_1 = n_2 x_2, \ \ldots, \quad x_{k-1} = n_k x_k, \ \ldots$$

Se x_k è primitivo per qualche k si ha $x = (n_1 \cdots n_k)x_k$, altrimenti la successione non termina; dimostriamo che questa ipotesi porta ad una contraddizione.

Si noti che siccome x non è di torsione, nessun x_k è di torsione. Per il Teorema 3.7 la catena ascendente di sottogruppi

$$\langle x_1 \rangle \subseteq \langle x_2 \rangle \cdots$$

è stazionaria. In particolare esiste k tale che $\langle x_{k-1} \rangle = \langle x_k \rangle$. Dunque $x_k = a x_{k-1}$ per qualche $a \in \mathbb{Z}$, e quindi $x_k = a n_k x_k$ che implica $(a n_k - 1)x_k = 0$. Siccome x_k non è di torsione deve essere $a n_k - 1 = 0$ in contraddizione con il fatto che $n_k > 1$. □

Dal Corollario 3.8 segue facilmente che un gruppo finitamente generato senza torsione non possiede elementi divisibili diversi da 0 (esercizio: perché?).

Teorema 3.9. *Ogni gruppo abeliano G finitamente generato senza torsione (ossia con $T(G) = 0$) è isomorfo a $\mathbb{Z}^n$ per qualche n.*

Dimostrazione. Induzione sul numero n di generatori. Per $n = 1$ già sappiamo che $\mathbb{Z}$ è l'unico gruppo ciclico senza torsione. Supponiamo $n > 1$ e G generato da $x_1, \ldots, x_n$. Se $x_1 = 0$ allora G è generato da $n-1$ elementi ed il teorema segue dall'ipotesi induttiva. Se $x_1 \neq 0$, allora x_1 non è di torsione e per il Corollario 3.8 possiamo scrivere $x_1 = ny$ con y primitivo. A meno di sostituire x_1 con y non è restrittivo supporre x_1 primitivo e quindi il gruppo quoziente $H = G/\langle x_1 \rangle$ senza torsione per il Lemma 3.3.

Siccome H è generato dalle classi di $x_2, \ldots, x_n$ si ha $H \simeq \mathbb{Z}^m$ per qualche m. Esiste quindi un omomorfismo surgettivo di gruppi $f\colon G \to \mathbb{Z}^m$ con nucleo $\langle x_1 \rangle \simeq \mathbb{Z}$. Per il Corollario 2.9 si ha $G \cong \mathbb{Z} \oplus \mathbb{Z}^m = \mathbb{Z}^{m+1}$.

□

Corollario 3.10. *Ogni sottogruppo $A \subseteq \mathbb{Z}^n$ è isomorfo a $\mathbb{Z}^m$ per qualche $m \leq n$. Inoltre vale $n = m$ se e solo se il quoziente $\mathbb{Z}^n/A$ è finito. In particolare $\mathbb{Z}^n \cong \mathbb{Z}^m$ se e solo se $n = m$.*

Dimostrazione. Siccome $\mathbb{Z}^n$ è finitamente generato e senza torsione, anche A è finitamente generato e senza torsione e quindi isomorfo a $\mathbb{Z}^m$ per qualche m. Componendo l'isomorfismo $A \simeq \mathbb{Z}^m$ con l'inclusione $A \subseteq \mathbb{Z}^n$ otteniamo un *omomorfismo iniettivo* di gruppi $f\colon \mathbb{Z}^m \to \mathbb{Z}^n$ che è descritto da una matrice $n \times m$ a coefficienti interi M (le colonne di M sono le immagini tramite f dei vettori della base canonica).

Se $m > n$ oppure se $n = m$ e $\det(M) = 0$, pensando M come una matrice a coefficienti razionali, esiste un vettore non nullo $v \in \mathbb{Q}^m$ tale che $Mv = 0$. A meno di moltiplicare v per un denominatore comune possiamo supporre $v \in \mathbb{Z}^m$, ma questo contraddice l'iniettività di f e quindi $m < n$, oppure $n = m$ e $\det(M) \neq 0$.

Se $m < n$ oppure se esiste un vettore $v \in \mathbb{Q}^n$ non nullo e tale che $v^T M = 0$, come prima non è restrittivo supporre $v \in \mathbb{Z}^m$. Ma allora l'immagine di f è contenuta nel sottogruppo

$$B = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n \mid \sum v_i a_i = 0\}.$$

Siccome $\sum_i v_i^2 > 0$, ne segue che $nv \notin B$ per ogni $n > 0$ e quindi l'immagine di v nel quoziente $\mathbb{Z}^n/A$ non è di torsione.

Rimane da dimostrare che se $n = m$ e $\det(M) \neq 0$, allora il quoziente $\mathbb{Z}^n/A$ è di torsione (essendo finitamente generato ne consegue che è finito), o equivalentemente che per ogni $x \in \mathbb{Z}^n$ esiste un intero $n > 0$ tale che $nx \in A$. Siccome M è invertibile su $\mathbb{Q}$ esiste un vettore $w \in \mathbb{Q}^n$ tale che $x = Mw$. Sia $n > 0$ un intero tale che $nw \in \mathbb{Z}^n$, allora $nx = Mnw \in A$.

Nota: è possibile dimostrare (ma non lo faremo qui) che per $n = m$ e $\det(M) \neq 0$, il valore assoluto $|\det(M)|$ è ben definito, ossia non dipende dalla scelta delle basi, e coincide con il numero di elementi del gruppo quoziente $\mathbb{Z}^n/A$. □

Teorema 3.11. *Sia G un gruppo abeliano finitamente generato. Allora esiste (non unico) un sottogruppo $A \subseteq G$ senza torsione tale che $G = A \oplus T(G)$. Se $A \simeq \mathbb{Z}^n$ (vedi Teorema 3.9) allora il numero n non dipende dalla scelta di A, viene detto **rango** di G e si scrive $n = \operatorname{rank}(G)$.*

Dimostrazione. Abbiamo visto che il quoziente $G/T(G)$ è finitamente generato senza torsione e quindi isomorfo a $\mathbb{Z}^n$ per un intero n che è ben definito per il Corollario 3.10. Esiste quindi un omomorfismo surgettivo di gruppi $f\colon G \to \mathbb{Z}^n$ il cui nucleo è esattamente $T(G)$. Per ogni vettore $e_1, \dots, e_n$ della base canonica di $\mathbb{Z}^n$ scegliamo un elemento $x_i \in G$ tale che $f(x_i) = e_i$ e definiamo A come il sottogruppo generato da $x_1, \dots, x_n$; equivalentemente A è l'immagine dell'omomorfismo di gruppi

$$g\colon \mathbb{Z}^n \to G, \qquad g(a_1, \dots, a_n) = \sum a_i x_i \,.$$

Siccome fg è uguale all'identità su $\mathbb{Z}^n$ per il Corollario 2.8 si ha $G \cong A \oplus T(G)$. □

Esercizi:

Esercizio 8. Dimostrare che in un gruppo abeliano finitamente generato non esistono elementi divisibili diversi da 0.

Esercizio 9. Sia $f\colon \mathbb{Z}^n \to \mathbb{Z}^n$ l'omomorfismo di gruppi descritto da una matrice $M \in M_{n,n}(\mathbb{Z})$. Dimostrare che f è un isomorfismo se e solo se $\det(M) = \pm 1$.

4. Additività del rango

Iniziamo con il richiamare la nozione di **conucleo** di un omomorfismo. Dato un omomorfismo di gruppi abeliani $f\colon G \to H$, l'immagine $f(G)$ è un sottogruppo (normale in quanto H abeliano) di H e si definisce il conucleo di f come il gruppo quoziente

$$\operatorname{coker}(f) = \frac{H}{f(G)} \,.$$

Se denotiamo con $\pi\colon H \to \operatorname{coker}(f)$ la proiezione al quoziente, per definizione si ha una successione esatta

$$G \xrightarrow{f} H \xrightarrow{\pi} \operatorname{coker}(f) \to 0 \,.$$

Viceversa, se $G \xrightarrow{f} H \xrightarrow{p} K \to 0$ è una successione esatta, per i classici teoremi di omomorfismo dei gruppi, essendo p surgettivo, si ha un isomorfismo di gruppi

$$K \cong \frac{H}{\ker p} = \frac{H}{f(G)} = \operatorname{coker}(f) \,.$$

Sempre dai classici teoremi di teoria dei gruppi segue la seguente proprietà universale del conucleo:

Sia $G \xrightarrow{f} H$ un omomorfismo di gruppi con proiezione sul conucleo $H \xrightarrow{\pi} \operatorname{coker}(f)$. Per ogni omomorfismo di gruppi $q\colon H \to K$ tale che $qf = 0$ esiste, ed è unico, un omomorfismo di gruppi $\overline{q}\colon \operatorname{coker}(f) \to K$ tale che $q = \overline{q}\pi$.

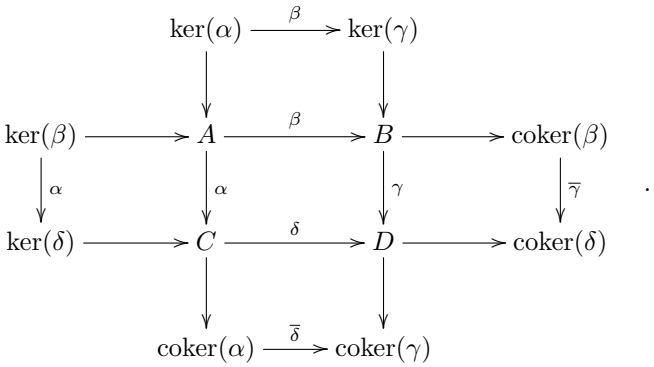
Infatti, dire che $qf = 0$ equivale a dire $f(G) \subseteq \ker q$ e questa è condizione necessaria e sufficiente affinché q si fattorizzi al quoziente $H/f(G)$. L'unicità segue dal fatto che π è surgettivo.

Consideriamo adesso un *quadrato commutativo* di gruppi abeliani, ossia un diagramma commutativo del tipo

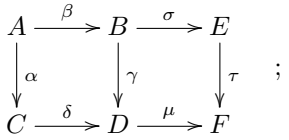
$$\begin{array}{ccc} A & \xrightarrow{\beta} & B \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \gamma} \\ C & \xrightarrow{\delta} & D \end{array}$$

Se $x \in \ker \alpha$, allora $\gamma\beta(x) = \delta\alpha(x) = 0$ e quindi $\beta(x) \in \ker \gamma$. Dunque il quadrato commutativo definisce per restrizione un omomorfismo $\beta\colon \ker(\alpha) \to \ker(\gamma)$. Si noti che se $\beta\colon A \to B$ è iniettivo, allora anche $\beta\colon \ker(\alpha) \to \ker(\gamma)$ è iniettivo.

Si consideri adesso la proiezione sul conucleo $\pi\colon D \to \operatorname{coker}(\gamma)$. Allora $\pi\delta\alpha = \pi\gamma\beta = 0$ poiché $\pi\gamma = 0$ e per la proprietà universale del conucleo, l'omomorfismo $\pi\delta$ si fattorizza ad un omomorfismo tra i conuclei $\overline{\delta}\colon \operatorname{coker}(\alpha) \to \operatorname{coker}(\gamma)$:



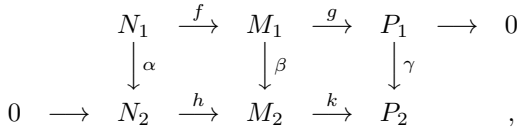
Consideriamo adesso due quadrati commutativi con un lato in comune



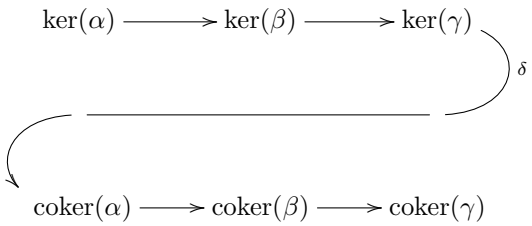
le precedenti osservazioni ci forniscono gli omomorfismi

$$\ker(\alpha) \xrightarrow{\beta} \ker(\gamma) \xrightarrow{\sigma} \ker(\tau), \qquad \operatorname{coker}(\alpha) \xrightarrow{\overline{\delta}} \operatorname{coker}(\gamma) \xrightarrow{\overline{\mu}} \operatorname{coker}(\tau)\,.$$

Lemma 4.1 (Lemma del serpente, prima versione)**.** *Sia dato un diagramma commutativo di gruppi abeliani*



con entrambe le righe successioni esatte. Allora esiste un morfismo (di bordo) $\delta\colon \ker(\gamma) \to \operatorname{coker}(\alpha)$ tale che la successione



è esatta.

Dimostrazione. (vedi anche https://www.youtube.com/watch?v=etbcKWEKnvg.) Sia $p \in \ker(\gamma)$, ossia un elemento $p \in P_1$ tale che $\gamma(p) = 0$, e sia $m \in M_1$ tale che $g(m) = p$; siccome il diagramma è commutativo, $k\beta(m) = 0$ in P_2 e quindi $\beta(m) = h(x)$ per un unico $x \in N_2$. Definiamo $\delta(p)$ come la classe di x nel conucleo di α.

Siccome l'elemento m non è unico, dobbiamo verificare che $\delta(p)$ non dipende dalla scelta di m: sia $m_1 \in M_1$ un altro elemento tale che $g(m_1) = p$ e sia $x_1 \in N_2$ tale che $h(x_1) = \beta(m_1)$: bisogna dimostrare che le immagini di x, x_1 in $\operatorname{coker}(\alpha)$ coincidono, ossia che $x_1 - x \in \alpha(N_1)$. Poiché $m_1 - m \in \ker(g)$ esiste $z \in N_1$ tale che $f(z) = m_1 - m$. Siccome $h\alpha(z) = \beta f(z) = \beta(m_1) - \beta(m) = h(x_1 - x)$. Dato che h è iniettiva deve essere $x_1 - x = \alpha(z) \in \alpha(N_1)$.

Lasciamo per esercizio al lettore la verifica che la successione dei nuclei e conuclei è esatta. □

Corollario 4.2 (Lemma del serpente, seconda versione)**.** *Sia dato un diagramma commutativo di gruppi abeliani*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_1 & \xrightarrow{f} & M_1 & \xrightarrow{g} & P_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & N_2 & \xrightarrow{h} & M_2 & \xrightarrow{k} & P_2 & \longrightarrow & 0, \end{array}$$

con entrambe le righe successioni esatte. Allora esiste un morfismo (di bordo) $\delta\colon \ker(\gamma) \to \operatorname{coker}(\alpha)$ *tale che la successione*

$$0 \longrightarrow \ker(\alpha) \longrightarrow \ker(\beta) \longrightarrow \ker(\gamma) \xrightarrow{\delta} \operatorname{coker}(\alpha) \longrightarrow \operatorname{coker}(\beta) \longrightarrow \operatorname{coker}(\gamma) \longrightarrow 0$$

è esatta.

Dimostrazione. Immediata conseguenza del Lemma 4.1 e del fatto che l'iniettività di f implica l'iniettività di $\ker(\alpha) \to \ker(\beta)$ e la surgettività di k implica la surgettività di $\operatorname{coker}(\beta) \to \operatorname{coker}(\gamma)$. □

Usando il linguaggio delle successioni esatte possiamo riscrivere il Corollario 3.10 nel modo seguente:

Lemma 4.3 (=Corollario 3.10)**.** *Sia* $0 \to \mathbb{Z}^n \to \mathbb{Z}^m \to G \to 0$ *una successione esatta corta di gruppi abeliani. Allora* $n \leq m$ *e vale* $n = m$ *se e solo se* G *è un gruppo di torsione. In particolare* $\mathbb{Z}^n \simeq \mathbb{Z}^m$ *se e solo se* $n = m$*.*

Va osservato che nel Lemma 4.3 essendo G un quoziente di un gruppo finitamente generato è anch'esso finitamente generato e quindi è di torsione se e solo se è finito.

Lemma 4.4. *Sia*

$$0 \to \mathbb{Z}^n \xrightarrow{f} \mathbb{Z}^m \xrightarrow{g} \mathbb{Z}^p \to 0$$

una successione esatta corta di gruppi abeliani. Allora $n + p = m$*.*

Dimostrazione. Per il Corollario 2.9 esiste un isomorfismo

$$\mathbb{Z}^m \cong \ker(g) \oplus \mathbb{Z}^p \cong \mathbb{Z}^n \oplus \mathbb{Z}^p = \mathbb{Z}^{n+p}$$

e quindi $m = n + p$. □

Siamo adesso in grado di applicare il lemma del serpente a due importanti risultati di teoria dei gruppi.

Definizione 4.5. Un gruppo G si dice **Hopfiano** se ogni omomorfismo surgettivo $G \to G$ è un isomorfismo.

Non tutti i gruppi sono Hopfiani: ad esempio l'omomorfismo

$$\prod_{i=1}^{\infty} \mathbb{Z} \to \prod_{i=1}^{\infty} \mathbb{Z}, \qquad (a_1, a_2, a_3, \ldots) \mapsto (a_2, a_3, \ldots),$$

è surgettivo ma non iniettivo.

Teorema 4.6. *Ogni gruppo abeliano finitamente generato è Hopfiano.*

Dimostrazione. Dimostriamo prima che i gruppi $\mathbb{Z}^n$ sono Hopfiani. Se $g\colon \mathbb{Z}^n \to \mathbb{Z}^n$ è surgettivo, allora il suo nucleo è finitamente generato e senza torsione, quindi isomorfo a $\mathbb{Z}^m$ per qualche m. Per il Lemma 4.4 si ha $n = n + m$ e quindi $\ker(g) = \mathbb{Z}^0$, ossia g è anche iniettivo.

I gruppi finiti sono Hopfiani per ovvii motivi di cardinalità.

Passiamo adesso al caso generale. Sia G un gruppo abeliano finitamente generato e sia $g\colon G \to G$ un omomorfismo surgettivo. Se $x \in T(G)$ è di torsione allora anche $g(x)$ è di

torsione e quindi g si restringe ad un omomorfismo $g_T\colon T(G) \to T(G)$ e si fattorizza ad un omomorfismo surgettivo $\overline{g}\colon G/T(G) \to G/T(G)$.

Si ha quindi un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T(G) & \longrightarrow & G & \longrightarrow & G/T(G) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g_T} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \overline{g}} & & \\ 0 & \longrightarrow & T(G) & \longrightarrow & G & \longrightarrow & G/T(G) & \longrightarrow & 0 \end{array}$$

Il gruppo $G/T(G)$ è Hopfiano in quanto senza torsione, quindi $\ker(\overline{g}) = 0$ e per il lemma del serpente anche g_T è surgettivo. Quindi g_T è anche iniettivo e sempre per il lemma del serpente $\ker(g) = 0$. □

Osservazione 4.7. È possibile dare una diversa dimostrazione del precedente teorema che utilizza la stazionarietà delle catene ascendenti di sottogruppi di un gruppo abeliano finitamente generato. Per ogni $n > 0$ denotiamo con K_n il nucleo di g^n (composizione di g con se stesso n volte). Allora $K_1 \subseteq K_2 \subset K_3 \cdots$ ed esiste un indice n tale che $K_n = K_{n+1}$. Sia $x \in \ker(g)$, siccome g^n è surgettivo si ha $x = g^n(y)$ per qualche $y \in G$. Ma allora $g^{n+1}(y) = 0$ e quindi $x = g^n(y) = 0$ poiché $K_n = K_{n+1}$.

Osservazione 4.8. La definizione di gruppo Hopfiano si applica anche ai gruppi non abeliani. In tal caso è però falso che ogni gruppo finitamente generato è Hopfiano.

Teorema 4.9 (Additività del rango)**.** *Sia*

$$0 \to G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \to 0$$

una successione esatta corta di gruppi abeliani finitamente generati. Allora

$$\operatorname{rank}(G_1) + \operatorname{rank}(G_3) = \operatorname{rank}(G_2)\,.$$

Dimostrazione. Per semplicità notazionale indichiamo $T_i = T(G_i)$. Abbiamo già dimostrato il teorema in due casi particolari, ossia quando $T_2 = T_3 = 0$ ($T_2 = 0$ implica che anche $T_1 = 0$) e quando $T_1 = T_2 = 0$, $T_3 = G_3$. In generale abbiamo un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_2 & \longrightarrow & G_2 & \longrightarrow & G_2/T_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g_T} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle \overline{g}} & & \\ 0 & \longrightarrow & T_3 & \longrightarrow & G_3 & \longrightarrow & G_3/T_3 & \longrightarrow & 0 \end{array}$$

Per definizione di rango si ha $\operatorname{rank}(G_i) = \operatorname{rank}(G_i/T_i)$ e se denotiamo con H il nucleo di $\overline{g}$ si ha

$$\operatorname{rank}(H) = \operatorname{rank}(G_2/T_2) - \operatorname{rank}(G_3/T_3) = \operatorname{rank}(G_2) - \operatorname{rank}(G_3)\,,$$

e rimane da dimostrare che G_1 ha lo stesso rango di H. Identificando G_1 con la sua immagine $f(G_1)$ si ha $G_1 = \ker(g)$, $T_1 = G_1 \cap T_2 = \ker(g) \cap T_2 = \ker(g_T)$ e per il lemma del serpente abbiamo una successione esatta

$$0 \to T_1 \to G_1 \to H \to \operatorname{coker}(g_T) \to 0$$

che si spezza in due successioni esatte corte

$$0 \to T_1 \to G_1 \to \frac{G_1}{T_1} \to 0, \qquad 0 \to \frac{G_1}{T_1} \to H \to \operatorname{coker}(g_T) \to 0\,.$$

Siccome $\dfrac{G_1}{T_1}, H$ sono senza torsione e $\operatorname{coker}(g_T)$ è di torsione si ha

$$\operatorname{rank}(G_1) = \operatorname{rank}(G_1/T_1) = \operatorname{rank}(H)\,.$$

Si noti che in generale $\operatorname{coker}(g_T) \neq 0$ che equivale a dire $G_1/T_1 \neq H$ che equivale a dire che

$$\frac{G_1}{T_1} \to \frac{G_2}{T_2} \to \frac{G_3}{T_3} \to 0$$

non è esatta. □

Corollario 4.10. *Sia $\mathbb{Z}^m \xrightarrow{M} \mathbb{Z}^n$ l'omomorfismo indotto da una matrice $M \in M_{n,m}(\mathbb{Z})$ e sia r il rango di M, pensata come matrice a coefficienti razionali. Allora* $\ker M \simeq \mathbb{Z}^{m-r}$ *e* $M(\mathbb{Z}^m) \simeq \mathbb{Z}^r$.

Dimostrazione. Indichiamo com $G = M(\mathbb{Z}^m)$ l'immagine di M. Siccome $G \subset \mathbb{Z}^n$ e $\ker M \subset \mathbb{Z}^m$, entrambi i gruppi sono finitamente generati e senza torsione, dunque $\ker M \simeq \mathbb{Z}^p$, $G \simeq \mathbb{Z}^q$ per opportuni interi p, q talei che $p + q = m$; ci basta quindi dimostrare che $q = r$.

Siano $e_1, \dots, e_m \in \mathbb{Z}^m \subset \mathbb{Q}^m$ i vettori della base canonica. A meno di permutazioni possiamo supporre che $Me_1, \dots, Me_r$ siano linearmente indipendenti in $\mathbb{Q}^n$. Siccome $r = \operatorname{rank}(M)$ si ha che $M(\mathbb{Q}^m) = \operatorname{Span}(Me_1, \dots, Me_r)$ e quindi per ogni $x \in G$ esistono $a_1, \dots, a_r \in \mathbb{Q}$ tali che $x = \sum_{i=1}^r a_i Me_i$. Equivalentemente, per ogni $x \in G$ esistono interi $d > 0$ (il denominatore comune degli a_i) e $b_1, \dots, b_r \in \mathbb{Z}$ tali che $nx = \sum_{i=1}^r b_i Me_i$.

Ne segue che l'applicazione

$$f \colon \mathbb{Z}^r \to G, \qquad f(b_1, \dots, b_r) = \sum b_i Me_i,$$

è iniettiva e per ogni $x \in G$ esiste un intero $n > 0$ tale che nx appartiene all'immagine di f. In conclusione il conucleo si f è di torsione e per l'additività del rango $q = r$. □

Esempio 4.11 (I mulini a vento)**.** Ad ogni omomorfismo di gruppi $f \colon A \to B$ possiamo associare in maniera canonica una successione esatta corta

$$0 \to A \xrightarrow{f_1} A \oplus B \xrightarrow{f_2} B \to 0, \qquad f_1(a) = (a, f(a)), \quad f_2(a, b) = b - f(a)\,,$$

mentre ad ogni coppia di omomorfismi in serie $A \xrightarrow{f} B \xrightarrow{g} C$ si può associare un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f_1} & A \oplus B & \xrightarrow{f_2} & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle -g} & & \\ 0 & \longrightarrow & B & \xrightarrow{g_1} & B \oplus C & \xrightarrow{g_2} & C & \longrightarrow & 0 \end{array} \qquad \varphi(a, b) = (b, gf(a))\,.$$

È importante osservare che φ è diversa dall'applicazione "canonica" $(a, b) \mapsto (f(a), g(b))$ che farebbe commutare il diagramma qualora la freccia verticale a destra fosse g invece di $-g$. Siccome g e $-g$ hanno gli stessi nucleo e conucleo ed è immediato osservare che l'inclusione $A \subset A \oplus B$ e la proiezione $B \oplus C \to C$ inducono isomorfismi $\ker(\varphi) = \ker(gf)$, $\operatorname{coker}(\varphi) = \operatorname{coker}(gf)$. Applicando il lemma del serpente si ottiene quindi la successione esatta lunga della Figura 1.

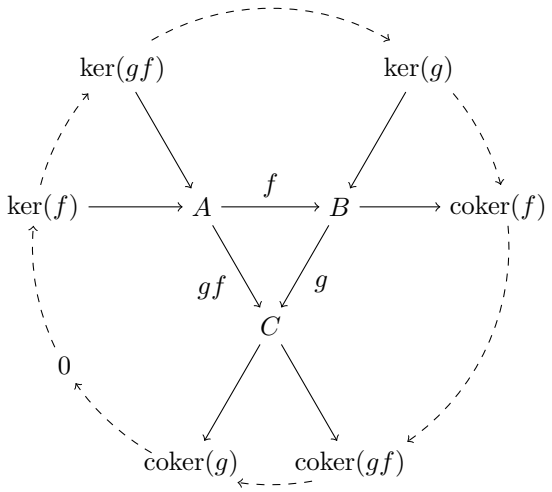


FIGURA 1. Il mulino vento, con la ruota esterna successione esatta.

Esercizi:

Esercizio 10. Si consideri il seguente diagramma commutativo di gruppi abeliani:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & M_1 & \longrightarrow & P_1 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_2 & \xrightarrow{f} & M_2 & \xrightarrow{g} & P_2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & N_3 & \longrightarrow & M_3 & \longrightarrow & P_3 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array} .$$

Si assuma che le colonne siano esatte e che $gf = 0$. Provare che ogni riga è un complesso e che se due righe sono esatte allora è esatta anche la terza.

Esercizio 11. Siano G un gruppo abeliano finitamente generato di rango r e con sottogruppo di torsione $T(G)$ di cardinalità N. Dato un numero primo $p > N$, calcolare la cardinalità del nucleo e del conucleo dell'omomorfismo $G \xrightarrow{p\cdot -} G$ di moltiplicazione per p. Usare questo fatto ed il lemma del serpente per una diversa dimostrazione del teorema di additività del rango.

Esercizio 12. Siano $\mathbb{Z}^l \xrightarrow{R} \mathbb{Z}^m \xrightarrow{S} \mathbb{Z}^n$ omomorfismi tali che $SR = 0$ e siano r, s i ranghi delle matrici R, S rispettivamente. Provare che

$$\operatorname{rank} \frac{\ker S}{R(\mathbb{Z}^l)} = m - r - s \,.$$

5. Complessi di catene e omologia

Figura 2. Guglielmo il dentone (esercizio: perché?).

Iniziamo con la definizione di complesso di catene di gruppi abeliani, dove il termine *catene* specifica una ben definita convenzione sugli indici.

Definizione 5.1. Un complesso di catene di gruppi abeliani è una successione $\{M_n\}_{n\in\mathbb{Z}}$ di gruppi abeliani insieme a degli omomorfismi $d=d_n\colon M_n\to M_{n-1}$ detti **differenziali**, tali che $d\circ d\colon M_n\to M_{n-2}$ risulti essere il morfismo nullo.

$$\cdots\ M_{n+1}\xrightarrow{d_{n+1}} M_n\xrightarrow{d_n} M_{n-1}\xrightarrow{d_{n-1}} M_{n-2}\ \cdots$$

Per semplicità parleremo semplicemente di complessi omettendo il termine catene. Si noti che nei complessi di catene il differenziale abbassa gli indici a pedice di 1.

Definizione 5.2. Un morfismo di complessi $f\colon C\to D$ è una successione di omomorfismi $\{f_n\colon C_n\to D_n\}_{n\in\mathbb{Z}}$ che commutano coi differenziali d, ossia per ogni intero n vale l'uguaglianza $f_{n-1}\circ d_n=d_n\circ f_n$ così da rendere commutativo il seguente diagramma:

$$\begin{array}{ccccccc}
\cdots & \longrightarrow & C_n & \xrightarrow{d_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\
\cdots & \longrightarrow & D_n & \xrightarrow{d_n} & D_{n-1} & \longrightarrow & \cdots
\end{array}$$

Diremo inoltre che un morfismo di complessi $f\colon C\to D$ è un isomorfismo (risp.: iniettivo, surgettivo) se $f_n\colon C_n\to D_n$ è un isomorfismo (risp.: iniettivo, surgettivo) per ogni n.

Definizione 5.3. Dato un complesso C possiamo definire:

- i **cicli** come gli elementi nei nuclei dei differenziali; per ogni n il nucleo $Z_n(C):=\ker(d_n)\subseteq C_n$ è detto gruppo degli n-cicli;
- i **bordi** come gli elementi immagine dei differenziali; per ogni n definiamo il gruppo degli n-bordi $B_n(C):=d_{n+1}(C_{n+1})\subseteq C_n$.

Osserviamo inoltre che la proprietà dei differenziali $d\circ d=0$ implica in particolar modo l'inclusione $B_n(C)\subseteq Z_n(C)$ ed è quindi possibile considerare il quoziente tra cicli e bordi.

Definizione 5.4. Definiamo l'*n-esimo gruppo di omologia* come il quoziente:

$$H_n(C):=\frac{Z_n(C)}{B_n(C)}\,.$$

Diremo che il complesso C è **aciclico** se per ogni n $H_n(C)=0$: ciò equivale a dire che il complesso C è una successione esatta.

Osservazione 5.5. Dato un complesso C, la condizione $d^2=0$ (ossia $d_nd_{n+1}=0$ per ogni n) implica che per ogni n il differenziale $d_n\colon C_n\to C_{n-1}$ si fattorizza ad un morfismo

$$\frac{C_n}{B_n(C)}\xrightarrow{\overline{d_n}} Z_{n-1}(C)$$

e si verifica immediatamente che $\ker\overline{d_n}=H_n(C)$, $\operatorname{coker}\overline{d_n}=H_{n-1}(C)$.

Una verifica diretta mostra che un morfismo di complessi $f\colon A\to B$ porta cicli in cicli e bordi in bordi, di conseguenza risultano ben definite a livello di omologia gli omomorfismi $f\colon H_n(A)\to H_n(B)$.

Definizione 5.6. Un morfismo di complessi $f\colon A\to B$ è detto un *quasi-isomorfismo* se per ogni n le applicazioni $f_n\colon H_n(A)\to H_n(B)$ sono isomorfismi.

Ogni isomorfismo di complessi è anche un quasi-isomorfismo, mentre il viceversa è generalmente falso.

Definizione 5.7. Sia $C=\{\cdots C_n\xrightarrow{d}C_{n-1}\cdots\}$ un complesso, un **sottocomplesso** $D\subseteq C$ è il dato di una successione di sottogruppi $D_n\subseteq C_n$ tali che $d(D_n)\subseteq D_{n-1}$ per ogni n.

Se $D\subseteq C$ è un sottocomplesso, l'inclusione $D\to C$ è un morfismo iniettivo di complessi. Bisogna fare **attenzione** al fatto che in generale i morfismi indotti in omologia $H_n(D)\to H_n(C)$ **non sono** iniettivi in generale. Similmente se $D\to E$ è un morfismo surgettivo di complessi, allora non è detto che i morfismi $H_n(D)\to H_n(E)$ siano surgettivi (vedi Esempio 5.10).

Esempio 5.8. Sia D un sottocomplesso di un complesso di catene C. Se per qualche intero n si ha che $D_i = C_i$ per $i = n-1, n, n+1$, allora l'inclusione $D \subset C$ induce un isomorfismo $H_n(D) \to H_n(C)$: infatti $H_n(C)$ dipende solo dal segmento $C_{n+1} \xrightarrow{d} C_n \xrightarrow{d} C_{n-1}$ che coincide con il corrispondente segmento del sottocomplesso D.

Definizione 5.9. Un diagramma di morfismi di complessi

$$0 \to C \xrightarrow{f} D \xrightarrow{g} E \to 0$$

si dice una **successione esatta corta** di complessi se per ogni n si ha che

$$0 \to C_n \xrightarrow{f_n} D_n \xrightarrow{g_n} E_n \to 0$$

è una successione esatta corta di gruppi abeliani.

Esempio 5.10. Possiamo interpretare il diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\mathrm{Id}} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}} & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\mathrm{Id}} & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

come una successione esatta corta di complessi $0 \to C \xrightarrow{f} D \xrightarrow{g} E \to 0$ concentrati nei gradi $0, 1$, ossia $C_n = D_n = E_n = 0$ per ogni n eccetto $C_0 = D_0 = D_1 = E_1 = \mathbb{Z}$. Si noti che D è aciclico, mentre $H_0(C) = H_1(E) = \mathbb{Z}$; in particolare $H_0(C) \to H_0(D)$ non è iniettiva e $H_1(D) \to H_1(E)$ non è surgettiva.

Teorema 5.11. *Data una successione esatta corta di complessi*

$$0 \to C \xrightarrow{f} D \xrightarrow{g} E \to 0$$

sono canonicamente definiti *degli omomorfismi* $\partial_n \colon H_n(E) \to H_{n-1}(C)$ *tali che si ottenga la successione esatta (infinita):*

$$\cdots \to H_n(C) \xrightarrow{f} H_n(D) \xrightarrow{g} H_n(E) \xrightarrow{\partial_n} H_{n-1}(C) \xrightarrow{f} H_{n-1}(D) \to \cdots \tag{5.1}$$

detta in gergo successione esatta lunga di omologia.

Dimostrazione. La dimostrazione si ottiene mediante un uso ripetuto del lemma del serpente. Per semplicità notazionale indichiamo con il medesimo simbolo d i differenziali dei tre complessi. Per ogni intero n si ha un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C_n & \longrightarrow & D_n & \longrightarrow & E_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle d} & & \\ 0 & \longrightarrow & C_{n-1} & \longrightarrow & D_{n-1} & \longrightarrow & E_{n-1} & \longrightarrow & 0 \end{array}$$

che per il lemma del serpente ci fornisce, per ogni $n \in \mathbb{Z}$, una successione esatta

$$0 \to Z_n(C) \to Z_n(D) \to Z_n(E) \to \frac{C_{n-1}}{B_{n-1}(C)} \to \frac{D_{n-1}}{B_{n-1}(D)} \to \frac{E_{n-1}}{B_{n-1}(E)} \to 0\,.$$

Poiché il differenziale $d \colon C_n \to C_{n-1}$ si fattorizza ad un omomorfismo $\overline{d} \colon \dfrac{C_n}{B_n(C)} \to Z_{n-1}(C)$ i cui nucleo e conucleo sono rispettivamente $H_n(C)$ e $H_{n-1}(C)$ (idem per i complessi D, E), per ogni n si ha un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccccc} & & \dfrac{C_n}{B_n(C)} & \longrightarrow & \dfrac{D_n}{B_n(D)} & \longrightarrow & \dfrac{E_n}{B_n(E)} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \overline{d}} & & \downarrow{\scriptstyle \overline{d}} & & \downarrow{\scriptstyle \overline{d}} & & \\ 0 & \longrightarrow & Z_{n-1}(C) & \longrightarrow & Z_{n-1}(D) & \longrightarrow & Z_{n-1}(E) & & \end{array}$$

che per l'Osservazione 5.5 ed il lemma del serpente ci fornisce, per ogni n, una successione esatta

$$H_n(C) \to H_n(D) \to H_n(E) \to H_{n-1}(C) \to H_{n-1}(D) \to H_{n-1}(E)\,.$$

Mettendo assieme tutte queste successioni esatte si ottiene la successione esatta lunga di omologia. □

Corollario 5.12. *Sia*

$$0 \to C \xrightarrow{f} D \xrightarrow{g} E \to 0$$

una successione esatta corta di complessi. Allora f è un quasi-isomorfismo se e solo se E è aciclico.

Dimostrazione. Consideriamo la successione esatta lunga di omologia

$$\cdots \to H_{n+1}(E) \to H_n(C) \xrightarrow{f} H_n(D) \xrightarrow{g} H_n(E) \xrightarrow{\partial_n} H_{n-1}(C) \xrightarrow{f} H_{n-1}(D) \to \cdots$$

Se E è aciclico allora per ogni n si ha $H_{n+1}(E) = H_n(E) = 0$ e dall'esattezza della successione si deduce che $H_n(C) \xrightarrow{f} H_n(D)$ è iniettiva e surgettiva. Viceversa, se f è un quasi-isomorfismo allora per ogni n il morfismo $H_n(C) \xrightarrow{f} H_n(D)$ è surgettivo ed il morfismo $H_{n-1}(C) \xrightarrow{f} H_{n-1}(D)$ è iniettivo. L'esattezza della successione implica allora che $H_n(E) = 0$. □

Definizione 5.13. Una **omotopia** di complessi di catene, scritta $h\colon C \to D[1]$, è il dato di due complessi di catene C, D e di una successione $h = \{h_n\}$ di omomorfismi di gruppi

$$h_n\colon C_n \to D_{n+1}\,,$$

(non si richiede alcuna regola di commutazione con i differenziali).

Definizione 5.14. Una **contrazione** di un complesso di catene C è una omotopia $h\colon C \to C[1]$ tale che $dh + hd = \mathrm{Id}$: con ciò intendiamo che per ogni n vale

$$d_{n+1}h_n + h_{n-1}d_n = \mathrm{Id}\colon C_n \to C_n\,.$$

Un complesso che possiede una contrazione si dice **contraibile**.

Lemma 5.15. *Ogni complesso contraibile è aciclico.*

Dimostrazione. Sia C un complesso che possiede una contrazione $h\colon C \to C[1]$ e sia $x \in Z_n(C)$. Allora, siccome $d(x) = 0$ a maggior ragione $hd(x) = 0$ e quindi

$$x = \mathrm{Id}(x) = dh(x) + hd(x) = dh(x) \in B_n(C)\,.$$

□

È generalmente falso che i complessi aciclici sono contraibili: ad esempio il complesso

$$0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{d} \mathbb{Z}/(2) \to 0$$

è aciclico ma non è contraibile. Infatti $\mathbb{Z}/(2)$ è di torsione, mentre $\mathbb{Z}$ è senza torsione e poiché ogni omomorfismo manda elementi di torsione in elementi di torsione, non esiste alcun omomorfismo $h\colon \mathbb{Z}/(2) \to \mathbb{Z}$ tale che dh sia l'identità.

Definizione 5.16. Due morfismi di complessi $f, g\colon (C, d) \to (D, \delta)$ si dicono **omotopi** se esiste una successione di omomorfismi $h_n\colon C_n \to D_{n+1}$ tali che

$$f - g = \delta h + hd \iff f_n - g_n = \delta_{n+1}h_n + h_{n-1}d_n \quad \forall\, n\,.$$

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{d} & C_n & \xrightarrow{d} & C_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f-g} & \swarrow{\scriptstyle h} & \downarrow{\scriptstyle f-g} & \swarrow{\scriptstyle h} & \downarrow{\scriptstyle f} & & \\
\cdots & \longrightarrow & D_{n+1} & \xrightarrow{\delta} & D_n & \xrightarrow{\delta} & D_{n-1} & \longrightarrow & \cdots
\end{array}$$

In particolare un complesso C è contraibile se e solo se Id_C è omotopa all'applicazione nulla.

Osservazione 5.17. L'omotopia sopra definita è una relazione di equivalenza e per indicare che f,g sono omotope scriveremo $f \sim g$. Infatti, prendendo $h = 0$ si ottiene $f \sim f$; se $f - g = \delta h + hd$ allora ponendo $k_n = -h_n$ per ogni n si ha $g - f = \delta k + kd$; se $f - g = \delta h + hd$ e $g - l = \delta k + kd$, allora $f - l = \delta(h + k) + (h + k)d$.

Lemma 5.18. *Due morfismi di complessi $f, g\colon C \to D$ omotopi, $f \sim g$, inducono gli stessi morfismi in omologia $f = g\colon H_n(C) \to H_n(D)$, per ogni n.*

Dimostrazione. Bisogna dimostrare che se $f \sim g$ e $x \in Z_n(C)$, allora $f(x) - g(x) \in B_n(D)$. Siccome $dx = 0$ si ha

$$f(x) - g(x) = \delta h(x) + hd(x) = \delta h(x) \in \delta(D_{n+1}) = B_n(D)\,.$$

□

Definizione 5.19. Un morfismo di complessi $f\colon C \to D$ si dice un'**equivalenza omotopica** se esiste un morfismo di complessi $g\colon D \to C$ tale che la composizione $gf\colon C \to C$ è omotopa all'identità Id_C e $fg\colon D \to D$ è omotopa all'identità Id_D:

$$C \text{ omotopo a } D \iff fg \sim \mathrm{Id}_D, \quad gf \sim \mathrm{Id}_C\,.$$

Lemma 5.20. *Le equivalenze omotopiche sono quasi-isomorfismi.*

Dimostrazione. Sia $f\colon C \to D$ un'equivalenza omotopica. Per definizione esiste un morfismo di complessi $g\colon D \to C$ tale che $gf \sim \mathrm{Id}_C$ e $fg \sim \mathrm{Id}_D$. Per ogni n abbiamo un diagramma commutativo

$$\begin{array}{ccc} H_n(C) & \xrightarrow{f} & H_n(D) \\ {\scriptstyle gf}\downarrow & \swarrow{\scriptstyle g} & \downarrow{\scriptstyle fg} \\ H_n(C) & \xrightarrow{f} & H_n(D) \end{array}$$

e per il lemma precedente le due frecce verticali sono le identità. La conclusione segue dalla regola del 2 su 6. □

Un utile risultato che useremo spesso nel seguito è:

Corollario 5.21. *Siano C un complesso di catene e $D \subset C$ un sottocomplesso. Se esiste una omotopia $h\colon C \to C[1]$ tale che:*

(1) *$h(D) \subset D$;*
(2) *l'immagine di $f := \mathrm{Id}_C - dh - hd\colon C \to C$ è contenuta in D;*

allora l'inclusione $D \subset C$ è una equivalenza omotopica e quindi induce un isomorfismo in omologia: $H_n(D) = H_n(C)$ per ogni n.

Dimostrazione. Iniziamo dimostrando che $f\colon C \to D$ è un morfismo di complessi: siccome $d^2 = 0$ si ha

$$df = d(\mathrm{Id} - dh - hd) = d - d^2h - dhd = d - dhd = d - dhd - hd^2 = (\mathrm{Id} - dh - hd)d = fd\,.$$

Se denotiamo con $i\colon D \to C$ l'inclusione e con k la restrizione di h a D si ha

$$\mathrm{Id}_D - fi = kd + dk, \qquad \mathrm{Id}_C - if = hd + dh\,.$$

□

Esercizi:

Esercizio 13. Sia $f\colon C \to D$ è un quasi-isomorfismo di complessi con $f_n\colon C_n \to D_n$ surgettivo per ogni n. Dimostrare che $f_n\colon Z_n(C) \to Z_n(D)$ è surgettivo per ogni n.

Esercizio 14. Sia

$$0 \to C \xrightarrow{f} D \xrightarrow{g} E \to 0$$

una successione esatta corta di complessi. Provare che g è un quasi-isomorfismo se e solo se C è aciclico.

Esercizio 15. Sia $C = \{C_n\}$ un complesso di catene di gruppi abeliani finitamente generati. Si assuma che $2x = 0$ per ogni n ed ogni $x \in C_n$. Dimostrare che C è aciclico se e solo se è contraibile.

6. Complessi simpliciali astratti

Iniziamo con il fissare alcune notazioni: se I è un insieme scriveremo Δ^I per indicare la famiglia di tutti i sottoinsiemi **finiti e non vuoti** di I. Nel caso in cui $I = \{0, 1, \ldots, n\}$ scriveremo più semplicemente Δ^n in luogo di $\Delta^{\{0,1,\ldots,n\}}$. È chiaro che $\Delta^\emptyset = \emptyset$.

Definizione 6.1. Un **complesso simpliciale astratto** (CSA) è una coppia (K, I), dove I è un insieme, i cui elementi sono detti **vertici**, e K è un sottoinsieme di Δ^I per cui valgano le seguenti condizioni:

(1) $\{x\} \in K$ per ogni $x \in I$;
(2) se $s \in K$, $t \in \Delta^I$ e $t \subseteq s$, allora $t \in K$.

Giova osservare che la precedente condizione (2) equivale a dire che se $s \in K$, allora $\Delta^s \subseteq K$.

Se (K, I) è un CSA, chiameremo **simplessi** gli elementi di K. La dimensione di un simplesso $s \in K$ è definita come il numero di elementi di s diminuito di 1: ogni vertice ha dimensione 0. Chiameremo anche p-simplesso un simplesso di dimensione p. Se $s \in K$ e $t \subset s$ diremo che t è una faccia di s, se $t \subset s$ e $t \neq s$ diremo che t è una faccia propria di s. Un simplesso $s \in K$ si dice massimale se son è faccia propria di alcun simplesso in K.

Segue dalla definizione che esiste una bigezione tautologica tra l'insieme dei vertici di un CSA (K, I) e l'insieme degli 0-simplessi. Dunque K determina univocamente I e nel seguito useremo la notazione semplificata $K = (K, I)$ quando non è necessario esplicitare l'insieme dei vertici.

Esempio 6.2. Per ogni insieme I, la coppia (Δ^I, I) è un complesso simpliciale astratto che viene detto **completo**.

Definizione 6.3. Dato un complesso simpliciale astratto K, chiamiamo p-**scheletro** di K, denotato con $K^{(p)}$, la sottofamiglia di tutti i simplessi di K di dimensione minore o uguale a p, ossia la famiglia dei simplessi di K con al più $p + 1$ elementi.

Un complesso simpliciale astratto (K, I) si dice finito se I è un insieme finito ($\iff$ K è finito). La **dimensione** $\dim K$ di un complesso simpliciale astratto K è l'estremo superiore delle dimensioni dei suoi simplessi. In particolare: $K = K^{(p)}$ se e solo se $\dim K \leq p$, Δ^I ha dimensione $|I| - 1$ e, coerentemente, definiamo uguale a -1 la dimensione del complesso simpliciale vuoto $\emptyset = \Delta^\emptyset$.

Ogni complesso simpliciale astratto finito ha dimensione finita, mentre il viceversa è generalmente falso.

Prima di sviluppare la teoria dei complessi simpliciali astratti, illustriamo alcuni esempi significativi.

Esempio 6.4. Se K è un CSA, allora $K^{(p)}$ è un CSA per ogni $p \geq 0$ (con gli stessi vertici di K).

Esempio 6.5. Dati due complessi simpliciali astratti (K, I) e (H, J), la loro unione $(K \cup H, I \cup J)$ e la loro intersezione $(K \cap H, I \cap J)$ sono ancora complessi simpliciali astratti.

Esempio 6.6. Per ogni complesso simpliciale astratto K si ha $K = \bigcup_{s \in K} \Delta^s$. Se K ha dimensione finita ogni simplesso è contenuto in un simplesso massimale e quindi

$$K = \bigcup_{s \in K,\, s \text{ massimale}} \Delta^s \,.$$

Esempio 6.7. Dati due complessi simpliciali astratti (K, I) e (H, J) la loro **giunzione** è il complesso simpliciale astratto $(K * H, I \cup J)$, dove

$$K * H = K \cup H \cup \{s \cup t \mid s \in K,\ t \in H\} \,.$$

Ogni applicazione di insiemi $f \colon I \to J$ induce in modo naturale un'applicazione

$$f \colon \Delta^I \to \Delta^J, \qquad f(s) = \text{immagine del sottoinsieme } s \subseteq I \text{ tramite } f \,.$$

Definizione 6.8. Un morfismo $f\colon (K,I)\to(H,J)$ di complessi simpliciali astratti è un'applicazione $f\colon I\to J$ tale che $f(s)\in H$ per ogni $s\in K$. Un morfismo $f\colon (K,I)\to(H,J)$ si dice un isomorfismo se entrambe le applicazioni $f\colon I\to J$ e $f\colon K\to H$ sono bigettive.

Definizione 6.9. Dato un complesso simpliciale astratto K e un sottoinsieme $L\subseteq K$, diremo che L è un **sottocomplesso** di K se L è a sua volta un complesso simpliciale astratto (i cui vertici sono contenuti nei vertici di K).

Ad esempio, gli scheletri sono sottocomplessi. Ogni complesso simpliciale astratto (K,I) è un sottocomplesso di Δ^I e per ogni $s\in K$ si ha che Δ^s è un sottocomplesso di K. Se L è un sottocomplesso simpliciale astratto di K l'inclusione $L\hookrightarrow K$ è un morfismo di complessi simpliciali.

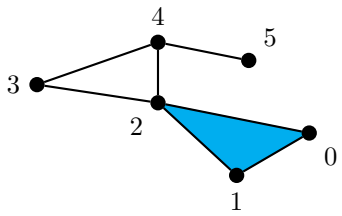
Esempio 6.10. Sia (K,I) un complesso simpliciale astratto finito con $I\subset\mathbb{R}^n$. Per ogni sottoinsieme finito $s\subset\mathbb{R}^n$ indichiamo con $\langle s\rangle\subset\mathbb{R}^n$ l'inviluppo convesso di s:

$$\langle\emptyset\rangle=\emptyset,\qquad \langle\{x_0,\dots,x_p\}\rangle=\left\{\sum t_ix_i\in\mathbb{R}^n\mid t_i\geq 0,\ \sum t_i=1\right\},\quad p\geq 0\,.$$

Se accade che per ogni $s,t\in K$ si ha $\langle s\rangle\cap\langle t\rangle=\langle s\cap t\rangle$, allora possiamo rappresentare K mediante la sua **realizzazione geometrica**

$$|K|:=\bigcup_{s\in K}\langle s\rangle=\bigcup_{s\in K,\ s\text{ massimale}}\langle s\rangle\subset\mathbb{R}^n\,.$$

Ad esempio la figura



rappresenta il complesso simpliciale astratto

$$K=\{\{0,1,2\},\{0,1\},\{1,2\},\{0,2\},\{2,3\},\{3,4\},\{2,4\},\{4,5\},\{0\},\{1\},\{2\},\{3\},\{4\},\{5\}\},$$

i cui scheletri sono:

$$K^{(0)}=\{\{0\},\{1\},\{2\},\{3\},\{4\},\{5\}\},$$
$$K^{(1)}=\{\{0,1\},\{1,2\},\{0,2\},\{2,3\},\{3,4\},\{2,4\},\{4,5\},\{0\},\{1\},\{2\},\{3\},\{4\},\{5\}\},$$
$$K^{(p)}=K\quad\text{per ogni } p\geq 2.$$

Tratteremo in maggiori dettagli le realizzazioni geometriche nella Sezione 7.

Esempio 6.11 (Catene ascendenti)**.** Sia $(I,\leq)$ un insieme (parzialmente) ordinato. Il complesso simpliciale astratto delle catene ascendenti di I è (K,I), dove:

$$K=\{\{x_0,\dots,x_p\}\in\Delta^I\mid x_0\leq x_1\leq\cdots\leq x_p\}.$$

È chiaro che ripetendo la stessa costruzione con le catene discendenti ritroviamo il medesimo complesso simpliciale astratto:

$$K=\{\{x_0,\dots,x_p\}\in\Delta^I\mid x_0\geq x_1\geq\cdots\geq x_p\}.$$

Esempio 6.12 (Suddivisione baricentrica)**.** Dato un qualunque complesso simpliciale astratto (K,I), l'insieme K è ordinato per inclusione e possiamo definire la sua **suddivisione baricentrica** $(b(K),K)$ come il complesso delle catene ascendenti di K:

$$b(K)=\{\{x_0,\dots,x_p\}\in\Delta^K\mid x_0\subset x_1\subset\cdots\subset x_p\}.$$

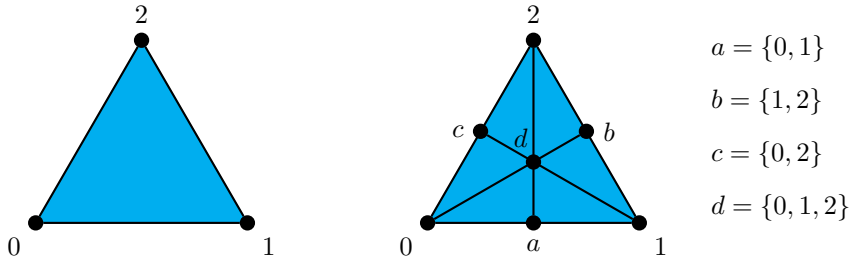


FIGURA 3. Il complesso simpliciale astratto Δ^2 e la sua suddivisione baricentrica $b(\Delta^2)$.

Esempio 6.13 (Il nervo)**.** Sia $\mathcal{U} = \{U_i\}$, $i \in I$, una famiglia di sottoinsiemi non vuoti di un insieme fissato. Possiamo definire un complesso simpliciale astratto $(N(\mathcal{U}), I)$ ponendo

$$N(\mathcal{U}) = \{\{i_0, \dots, i_p\} \in \Delta^I \mid U_{i_0} \cap \cdots \cap U_{i_p} \neq \emptyset\}.$$

È chiaro che la coppia $(N(\mathcal{U}), I)$ è un complesso simpliciale astratto. È utile osservare che se $U_i = U_j$ per ogni i, j allora il nervo coincide con il complesso simpliciale completo Δ^I.

Nel seguito, useremo i termini **nuvola di punti** e **point cloud** per indicare un sottoinsieme $I \subset \mathbb{R}^n$ con un numero finito ma molto grande di elementi, ossia $n << |I| < \infty$. Inoltre per ogni $x \in \mathbb{R}^n$ ed ogni numero reale r denotiamo la

$$U_x(r) = \{y \in \mathbb{R}^n \mid \|x - y\| \leq r\}.$$

Ciascun $U_x(r)$ è un chiuso limitato che, per ogni $r > 0$ coincide con la chiusura della sua parte interna (la palla aperta di raggio r). Chiameremo $U_x(r)$ il disco chiuso di centro x e raggio r.

Esempio 6.14 (Complesso di **Delaunay**)**.** Un caso particolare di nervo è dato dal **complesso di Delaunay** D_I di un insieme $I \subset \mathbb{R}^n$. Per ogni $s \in I$ definiamo la sua **regione di Voronoi**[3] $V_s \subseteq \mathbb{R}^n$ come:

$$V_s = \{x \in \mathbb{R}^n \mid \|x - s\| \leq \|x - t\|, \quad \forall\, t \in I\}.$$

Si noti che per una terna di punti x, s, t di $\mathbb{R}^n$ si ha (esercizio)

$$\|x - s\| \leq \|x - t\| \iff \left(x - \frac{s+t}{2}\right) \cdot (s - t) \geq 0,$$

(con $u \cdot v = \sum u_i v_i$ denotiamo il prodotto scalare canonico) e quindi V_s è intersezione di semispazi chiusi. In particolare V_s è un chiuso convesso. È chiaro che $V_s \neq \emptyset$ per ogni $s \in I$ e ha quindi perfettamente senso considerare il suo nervo $D_I := (N(\{V_s\}), I)$.

Equivalentemente un simplesso $\{s_0, \dots, s_p\} \in \Delta^I$ appartiene al complesso di Delaunay D_I se e solo se esiste $x \in \mathbb{R}^n$ tale che

$$\|x - s_0\| = \|x - s_1\| = \cdots = \|x - s_p\| \leq \|x - t\| \qquad \text{per ogni } t \in I\,.$$

In particolare, per ogni $\{s_0, \dots, s_p\} \in D_I$ i $p + 1$ punti $s_0, \dots, s_p$ sono contenuti in una sfera di dimensione $n - 1$ che non contiene al suo interno alcun punto di I. Dunque per un sottoinsieme finito I di $\mathbb{R}^n$ ed in *posizione generica* il complesso di Delaunay D_I ha al più dimensione n.

Esempio 6.15 (Complessi di **Čech** e **Vietoris-Rips**)**.** Dato un qualsiasi sottoinsieme $I \subset \mathbb{R}^n$, per ogni numero reale positivo $r \geq 0$ possiamo definire i complessi simpliciali astratti $(C(r), I)$ e $(V(r), I)$ nel modo seguente:

$$C(r) = \left\{\{x_0, \dots, x_p\} \in \Delta^I \;\middle|\; U_{x_0}(r) \cap \cdots \cap U_{x_p}(r) \neq \emptyset\right\}, \qquad \text{(Čech)},$$

$$V(r) = \left\{\{x_0, \dots, x_p\} \in \Delta^I \;\middle|\; \|x_i - x_j\| \leq 2r \text{ per ogni } i, j\right\}, \qquad \text{(Vietoris-Rips)}.$$

[3]Voronoi era un matematico russo, mentre Delaunay francese. Questo implica che il primo si pronuncia più o meno come si scrive, mentre il secondo richiede la pronuncia alla francese (all'incirca "delonaí ").

È evidente che se $r \leq t$ allora $V(r) \subseteq V(t)$ e $C(r) \subseteq C(t)$ (vedi Figura 4). Una semplice applicazione della disuguaglianza triangolare mostra che $C(r) \subseteq V(r) \subseteq C(2r)$.

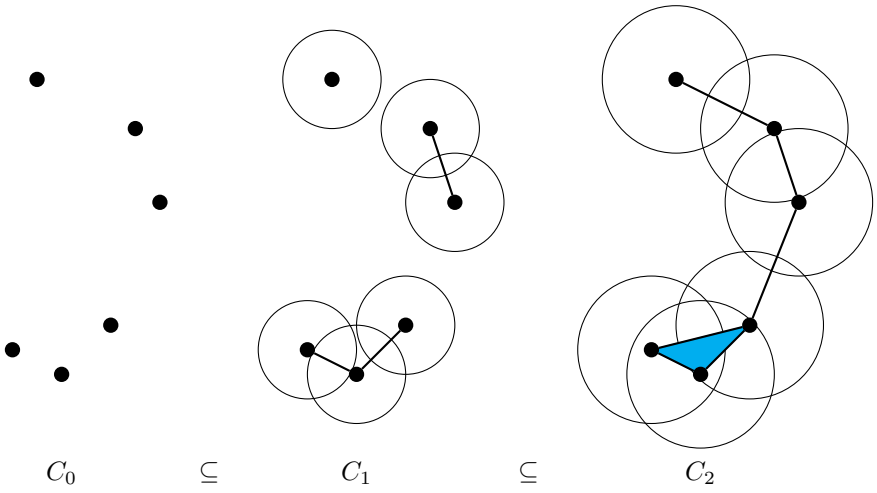


FIGURA 4. Filtrazione di Čech. Credits: la figura è tratta da [15].

Esempio 6.16 (Complessi **Alpha**)**.** Dato un qualsiasi sottoinsieme non vuoto $I \subset \mathbb{R}^n$, per ogni $u \in I$ ed ogni numero reale positivo $r > 0$ denotiamo $R_u(r) = U_u(r) \cap V_u$, dove $U_u(r))$ è il disco di centro u e raggio r, e V_u è la regione di Voronoi di u, definita nell'Esempio 6.13. Il complesso simpliciale Alpha(r) è definito come il nervo della famiglia $\{R_u(r)\}$, $u \in I$ (vedi Figura 5).

Equivalentemente un simplesso $\{s_0, \ldots, s_p\} \in \Delta^I$ appartiene al complesso Alpha(r) se e solo se esiste $x \in \mathbb{R}^n$ tale che:

$$\|x - s_0\| = \|x - s_1\| = \cdots = \|x - s_p\| \leq \min(r, \|x - t\|) \text{ per ogni } t \in I.$$

Possiamo riscrivere le due condizioni precedenti dicendo che un simplesso $\{s_0, \ldots, s_p\} \in \Delta^I$ appartiene al complesso Alpha(r) se e solo se esiste un disco di raggio r la cui parte interna non interseca I ma il cui bordo contiene $s_0, \ldots, s_p$.

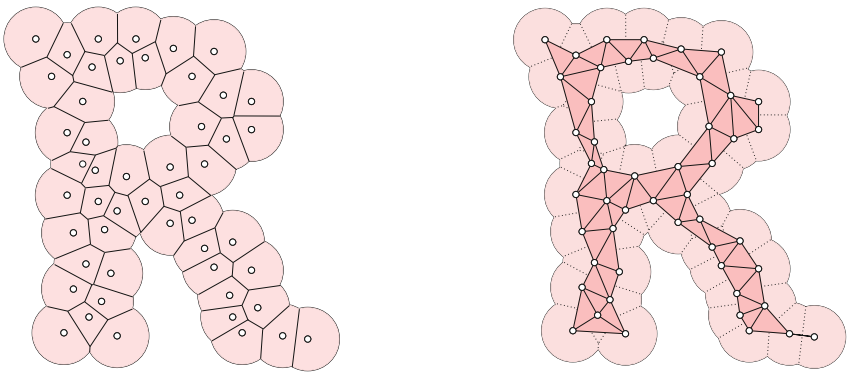


FIGURA 5. A sinistra una nuvola di punti in $\mathbb{R}^2$ (i pallini $\circ$) e le intesezioni $R_u(r)$ delle regioni di Voronoi V_u con le palle $B(u, r)$ (in rosa chiaro). A destra il complesso Alpha(r) (in rosa scuro). Credits: la figura è tratta da [5]

.

Esempio 6.17. Un complesso simpliciale astratto di dimensione ≤ 1 è detto un **grafo semplice**. Possiamo interpretare un grafo semplice come un insieme di vertici in cui alcune coppie di vertici distinti sono unite da un lato. Il termine semplice sta ad indicare che i lati non sono orientati e che per due vertici esiste al più un lato che li congiunge.

Definiamo ora due particolari sottoclassi di complessi simpliciali astratti: i coni e le cricche.

Definizione 6.18. Sia (K, I) un complesso simpliciale astratto. Diremo che K è un **cono** di vertice $v \in I$ se per ogni $s \in K$ si ha $s \cup \{v\} \in K$.

Ad esempio, il complesso vuoto $K = \emptyset$ non è un cono (non esiste alcun vertice), mentre per ogni $v \in I$, il complesso completo Δ^I è un cono di vertice v.

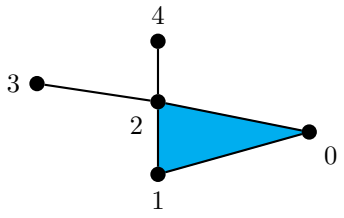


FIGURA 6. Un cono di vertice 2.

Definizione 6.19. Sia (K, I) un complesso simpliciale astratto. Diremo che K è un **complesso di cricche** se dato $s = \{x_0, \dots, x_p\} \in \Delta^I$ tale che $\{x_i, x_j\} \in K$ per ogni $0 \le i < j \le p$, si ha $s \in K$.

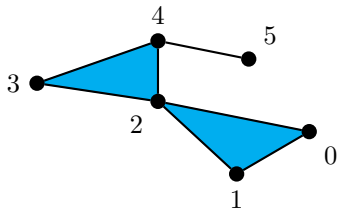
L'osservazione fondamentale è che ogni complesso di cricche K è univocamente determinato dal suo 1-scheletro $K^{(1)}$. Possiamo riscrivere la definizione precedente dicendo che (K, I) è di cricche se per ogni complesso simpliciale astratto (E, I) con gli stessi vertici e tale che $E^{(1)} = K^{(1)}$ si ha $E \subseteq K$; dunque i complessi di cricche sono elementi massimali nelle classi di CSA con 1-scheletro fissato.

Proponiamo alcuni esempi per chiarire meglio il concetto.

Esempio 6.20. Notiamo che il complesso simpliciale astratto descritto dalla figura nell'Esempio 6.10 non è un complesso di cricche. Questo perché si ha:

$$\{2,3\}, \{2,4\}, \{3,4\} \in K \text{ ma } \{2,3,4\} \notin K \ .$$

Aggiungendo $\{2,3,4\}$ a K otteniamo ancora un complesso simpliciale astratto



che, applicando la definizione, si verifica essere un complesso di cricche.

Proposizione 6.21. *La restrizione all'*1*-scheletro*

$$K \mapsto K^{(1)}$$

induce una bigezione tra le classi di isomorfismo di complessi di cricche e le classi di isomorfismo di grafi semplici.

Dimostrazione. Abbiamo visto che un complesso di cricche è univocamente determinato dal suo 1-scheletro e questo prova che $K \mapsto K^{(1)}$ è iniettiva sulle classi di isomorfismo. Viceversa, dato un grafo semplice $(E = E^{(1)}, I)$ possiamo definire un complesso di cricche (K, I) ponendo

$$K = \{\{x_0, \dots, x_p\} \in \Delta^I \mid \{x_i, x_j\} \in E \text{ per ogni } i, j\}.$$

□

Esercizi:

Esercizio 16. Denotiamo con $b(K)$ la suddivisione baricentrica del complesso simpliciale astratto K. Provare che:

(1) $b(\Delta^0) = \Delta^0$;
(2) $b(\Delta^n)$ è di tipo cono per ogni $n \geq 0$;
(3) se L è un sottocomplesso di K, allora $b(L)$ è un sottocomplesso di $b(K)$;
(4) se L, M sono sottocomplessi di K, allora $b(L \cap M) = b(L) \cap b(M)$ e $b(L \cup M) = b(L) \cup b(M)$.

Esercizio 17. Sia $I \subset \mathbb{R}^2$ l'insieme dei vertici di un esagono regolare di lato 1. Determinare il complesso di Vietoris-Rips (V_2, I).

Esercizio 18. Dato un $I \subset \mathbb{R}^n$ provare che $\mathrm{Alpha}(r) \subset D_I \cap C(r)$ e mostrare con un esempio che in generale $\mathrm{Alpha}(r) \neq D_I \cap C(r)$.

Esercizio 19. Sia $I \subset \mathbb{R}^n$ un chiuso non vuoto. Provare che le regioni di Voronoi V_s, $s \in I$, ricoprono $\mathbb{R}^n$, ossia $\mathbb{R}^n = \cup_{s \in I} V_s$.

7. Realizzazioni geometriche

In questa sezione studieremo esistenza ed unicità topologica delle realizzazioni geometriche dei complessi simpliciali astratti finiti. Per maggiori dettagli e per il caso dei complessi simpliciali infiniti rimandiamo a [17, Sezione 3.1].

Usando le stesse notazioni dell'Esempio 6.10, per ogni sottoinsieme finito $s \subset \mathbb{R}^n$ indichiamo con $\langle s \rangle \subset \mathbb{R}^n$ il suo *inviluppo convesso*

$$\langle \emptyset \rangle = \emptyset, \qquad \langle \{x_0, \ldots, x_p\} \rangle = \left\{ \sum t_i x_i \in \mathbb{R}^n \mid t_i \geq 0, \ \sum t_i = 1 \right\}, \quad p \geq 0\,,$$

e con $\langle\langle s \rangle\rangle \subset \mathbb{R}^n$ is suo *inviluppo affine*

$$\langle\langle \emptyset \rangle\rangle = \emptyset, \qquad \langle\langle \{x_0, \ldots, x_p\} \rangle\rangle = \left\{ \sum t_i x_i \in \mathbb{R}^n \mid t_i \in \mathbb{R}, \ \sum t_i = 1 \right\}, \quad p \geq 0\,.$$

Infine, denotiamo con $\Delta^n_{\mathbb{R}} \subset \mathbb{R}^{n+1}$ il simplesso topologico standard di dimensione n, definito come l'inviluppo convesso della base canonica, o equivalentemente come

$$\Delta^n_{\mathbb{R}} = \left\{ (t_0, \ldots, t_n) \in \mathbb{R}^{n+1} \mid t_i \geq 0, \ \sum t_i = 1 \right\}.$$

Lemma 7.1. *Sia $\{x_0, \ldots, x_p\} \subset \mathbb{R}^n$ un sottoinsieme di $p+1$ punti distinti con la proprietà che $\langle s \rangle \cap \langle t \rangle = \emptyset$ per ogni $s, t \subset \{x_0, \ldots, x_p\}$ tali che $s \cap t = \emptyset$. Allora:*

(1) *i p vettori $x_1 - x_0, \ldots, x_p - x_0$ sono linearmente indipendenti;*
(2) *l'applicazione*

$$f \colon \Delta^p_{\mathbb{R}} \to \langle \{x_0, \ldots, x_p\} \rangle, \qquad f(t_0, \ldots, t_n) = \sum_{i=0}^{p} t_i x_i,$$

è un omeomorfismo.

Dimostrazione. Supponiamo per assurdo che siano linearmente dipendenti, ossia

$$\sum_{i=1}^{p} a_i (x_i - x_0) = 0, \qquad a_i \in \mathbb{R} \text{ non tutti nulli.}$$

a meno di moltiplicare gli scalari a_i per -1 possiamo supporre $\sum_{i=0}^{p} a_i \geq 0$ ed a meno di permutare $x_1, \ldots, x_p$ possiamo supporre $a_1 > 0$ e che esista $1 \leq r \leq p$ tale che:

(1) $a_i > 0$ se $1 \leq i \leq r$,
(2) $a_i \leq 0$ se $r + 1 \leq i \leq p$.

Ponendo $b_i = -a_i$ si ha quindi

$$\sum_{i=1}^{r} a_i \geq \sum_{i=r+1}^{p} b_i, \qquad \sum_{i=1}^{r} a_i(x_i - x_0) = \sum_{i=r+1}^{p} b_i(x_i - x_0),$$

ed a meno di dividere per $\sum_{i=1}^{r} a_i > 0$ possiamo supporre

$$0 \leq \sum_{i=r+1}^{p} b_i \leq \sum_{i=1}^{r} a_i = 1\,.$$

Ma allora, sommando x_0 ad entrambi i membri di $\sum_{i=1}^{r} a_i(x_i - x_0) = \sum_{i=r+1}^{p} b_i(x_i - x_0)$ si ha

$$y := x_0 + \sum_{i=1}^{r} a_i(x_i - x_0) = \sum_{i=1}^{r} a_i x_i \in \langle x_1 \ldots, x_r \rangle\,,$$

$$= x_0 + \sum_{i=r+1}^{s} b_i(x_i - x_0) = \left(1 - \sum_{i=r+1}^{p} b_i\right) x_0 + \sum_{i=r+1}^{p} b_i x_i \in \langle x_0, x_{r+1} \ldots, x_p \rangle\,,$$

in contraddizione con il fatto che $\langle x_1 \ldots, x_r \rangle \cap \langle x_0, x_{r+1} \ldots, x_p \rangle = \emptyset$.

L'applicazione f è surgettiva per definizione di inviluppo convesso. Possiamo scrivere

$$f(t_0, \ldots, t_n) = \sum_{i=0}^{p} t_i x_i = x_0 + \sum_{i=1}^{p} t_i(x_i - x_0),$$

e dato che i vettori $x_i - x_0$ sono linearmente indipendenti ne segue che f è anche iniettiva. Dal punto di vista topologico, lo spazio $\Delta^p_{\mathbb{R}}$ è compatto di Hausdorff in quanto sottoinsieme chiuso dell'ipercubo $[0,1]^{p+1}$; dunque f è continua e bigettiva da un compatto in un Hausdorff e quindi un omeomorfismo. □

Proposizione 7.2. *Sia (K, I) un complesso simpliciale astratto con $I \subset \mathbb{R}^n$ e tale che $\langle s \rangle \cap \langle t \rangle = \emptyset$ per ogni $s, t \in K$ tali che $s \cap t = \emptyset$. Allora $\langle s \rangle \cap \langle t \rangle = \langle s \cap t \rangle$ per ogni $s, t \in K$.*

Dimostrazione. L'inclusione $\langle s \rangle \cap \langle t \rangle \supset \langle s \cap t \rangle$ è vera per ovvi motivi. Dimostriamo per induzione su $n = \dim(s \cap t)$ che vale l'inclusione opposta

$$\langle s \rangle \cap \langle t \rangle \subset \langle s \cap t \rangle\,. \tag{7.1}$$

Per $n = -1$, ossia se $s \cap t = \emptyset$, la (7.1) è vera per ipotesi. Supponiamo quindi $n \geq 0$, $s = \{s_0, \ldots, s_p\}$ e $t = \{t_0, \ldots, t_q\}$ con $s_i \neq s_j$ e $t_i \neq t_j$ per ogni $i \neq j$; a meno di permutazioni possiamo inoltre supporre $s_0 = t_0$.

Sia dunque $y \in \langle s \rangle \cap \langle t \rangle$. Si ha

$$y = \sum_{i=0}^{p} a_i s_i = \sum_{j=0}^{q} b_j t_j, \qquad 0 \leq a_i, b_j \leq 1, \sum a_i = \sum b_j = 1\,.$$

Supponiamo per fissare le idee che $a_0 \leq b_0$ (altrimenti sarà sufficiente scambiare s con t). Se $a_0 = 1$ allora $y = s_0 \in \langle s \cap t \rangle$. Se invece $a_0 < 1$, ponendo $r = \{s_1, \ldots, s_p\}$ si ha

$$z := \frac{1}{1 - a_0}(y - a_0 s_0) = \sum_{i=1}^{p} \frac{a_i}{1 - a_0} s_i \in \langle r \rangle\,.$$

D'altra parte, siccome $t_0 = s_0$

$$z = \frac{b_0 - a_0}{1 - a_0} t_0 + \sum_{j=1}^{q} \frac{b_j}{1 - a_0} t_j \in \langle t \rangle\,.$$

Per l'ipotesi induttiva $z \in \langle r \cap t \rangle$ e quindi $y = a_0 s_0 + (1 - a_0) z \in \langle s \cap t \rangle$. □

Definizione 7.3. Siano $K = (K, I)$ un complesso simpliciale astratto finito e $f \colon I \to \mathbb{R}^n$ un'applicazione tale che $\langle f(s) \rangle \cap \langle f(t) \rangle = \emptyset$ per ogni coppia di sottoinsiemi *disgiunti* $s, t \subset I$. Definiamo la **realizzazione geometrica** di K tramite f come

$$|f(K)| = \bigcup_{s \in K} \langle f(s) \rangle \subset \mathbb{R}^n\,,$$

dotato della topologia di sottospazio. Se f è il morfismo di inclusione di un sottoinsieme $I \subset \mathbb{R}^n$ scriveremo semplicemente $|K|$ in luogo di $|f(K)|$ (vedi Esempio 6.10).

Osserviamo che ogni $f\colon I \to \mathbb{R}^n$ come nella Definizione 7.3 è necessariamente iniettiva: se $u, v \in I$ sono due vertici distinti, allora $\{u\} \cap \{v\} = 0$ e quindi $f(u) \neq f(v)$. Ne segue che (K, I) è isomorfo come complesso simpliciale astratto a $(f(K), f(I))$, dove $f(K) = \{f(s) \mid s \in K\}$. Inoltre, per il Lemma 7.1 per ogni simplesso $\{x_0, \dots, x_p\} \in K$ di dimensione $p > 0$, i vettori $x_i - x_0$, $i = 1, \dots, p$ sono linearmente indipendenti, quindi $n \geq p$ da cui segue $n \geq \dim K$, mentre par la Proposizione 7.2 $\langle f(s)\rangle \cap \langle f(t)\rangle = \langle f(s) \cap f(t)\rangle$ per ogni $s, t \in K$.

Teorema 7.4. *Ogni complesso simpliciale astratto finito possiede realizzazioni geometriche, tra loro tutte topologicamente equivalenti.*

Dimostrazione. Sia (K, I) un complesso simpliciale astratto e sia V lo spazio vettoriale reale generato da I: ogni elemento di V è una combinazione lineare del tipo $\sum a_i x_i$, con $a_i \in \mathbb{R}$ e $x_i \in I$. Dato che gli elementi di I sono una base di V per ogni $s, t \in K$ tali che $s \cap t = \emptyset$ si ha $\langle s\rangle \cap \langle t\rangle = \emptyset$ e questo ci consente di definire la realizzazione geometrica canonica

$$|K|_{\text{can}} = \bigcup_{s \in K} \langle s\rangle \subset V\,.$$

Sia adesso $|f(K)|$ una realizzazione geometrica indotta da $f\colon I \to \mathbb{R}^n$. Siccome I è una base di V, l'applicazione f si estende in modo unico ad un'applicazione lineare

$$V \to \mathbb{R}^n, \qquad \sum a_i x_i \mapsto \sum a_i f(x_i)\,,$$

che per costruzione si restringe ad un'applicazione continua e surgettiva $F\colon |K|_{\text{can}} \to |f(K)|$. Siccome $|K|_{\text{can}}$ è compatto (unione finita di compatti) e $|f(K)|$ è compatto, basta dimostrare che F è anche iniettiva. Ma questo segue facilmente dal Lemma 7.1 e dalla Proposizione 7.2: i dettagli sono lasciati per esercizio. □

Non è difficile dimostrare che ogni complesso simpliciale astratto finito di dimensione k possiede una realizzazione geometrica in $\mathbb{R}^{2k+1}$. Per **triangolazione** di uno spazio topologico X si intende una coppia (K, f) con K complesso simpliciale astratto e $f\colon |K| \to X$ un omeomorfismo.

Data una realizzazione geometrica di un complesso simpliciale astratto (K, I) indotta da una inclusione $I \subset \mathbb{R}^n$ possiamo associare in maniera canonica una realizzazione geometrica della suddivisione baricentrica $(b(K), K)$ indotta dall'inclusione

$$f\colon K \to \mathbb{R}^n, \qquad f(\{x_0, \dots, x_p\}) = \frac{1}{p+1} \sum_{i=0}^{p} x_i\,.$$

Per future applicazioni è utile avere una stima dall'alto del diametro dei simplessi della realizzazione geometrica di $b(K)$. Due simplessi $a, b \in K$ appartengono ad un simplesso di $b(K)$ se e solo se uno è contenuto nell'altro. Diciamo

$$a = \{x_0, \dots, x_p\} \subset b = \{x_0, \dots, x_q\}, \qquad x_i \in I \subset \mathbb{R}^n, \quad p \leq q\,.$$

Vale allora la disuguaglianza

$$\|f(a) - f(b)\| \leq \frac{q}{q+1} \max_{0 \leq i,j \leq q} \|x_i - x_j\|\,.$$

Infatti, possiamo scrivere

$$\begin{aligned} f(a) - f(b) &= \sum_{i=0}^{p} \frac{x_i}{p+1} - \sum_{j=0}^{q} \frac{x_i}{q+1} = \sum_{i=0}^{p} \sum_{j=0}^{q} \frac{x_i - x_j}{(p+1)(q+1)} \\ &= \sum_{i=0}^{p} \sum_{j=0,\, j\neq i}^{q} \frac{x_i - x_j}{(p+1)(q+1)}\,. \end{aligned}$$

L'ultima sommatoria ha esattamente $(p+1)q$ addendi e se M denota il massimo delle norme $\|x_i - x_j\|$ al variare di $i = 0, \dots, p$ e $j = 0, \dots, q$, per la disuguaglianza triangolare si ha

$$\|f(a) - f(b)\| \leq \frac{(p+1)q}{(p+1)(q+1)} M = \frac{q}{q+1} M\,.$$

8. Omologia dei complessi simpliciali astratti

Definizione 8.1. Siano (K, I) un complesso simpliciale astratto e $p \geq 0$ un intero. Un **p-simplesso orientato** di K è un'applicazione di insiemi $x\colon \{0, 1, \ldots, p\} \to I$ la cui immagine appartiene a K. Denoteremo K_p l'insieme dei p-simplessi orientati di K.

Dato che ogni applicazione $x\colon \{0, 1, \ldots, p\} \to I$ la possiamo rappresentare mediante una $(p+1)$-upla $(x_0, \ldots, x_p)$ di elementi di I (dove x_i è l'immagine di i tramite x), possiamo scrivere

$$K_p = \{(x_0, \ldots, x_p) \in I^{p+1} \mid \{x_0, \ldots, x_p\} \in K\}.$$

Osserviamo che, poiché sono ammesse ripetizioni, K_p è non vuoto per ogni p, anche nel caso in cui K è un complesso finito. Ad esempio, per ogni $a \in I$ si ha $(a, \ldots, a) \in K_p$ per ogni p.

Se $f\colon \{0, \ldots, q\} \to \{0, \ldots, p\}$ è una qualunque applicazione, dato $x \in K_p$ possiamo considerare la sua composizione con f ed ottenere un nuovo simplesso orientato $f^*x \in K_q$:

$$f^*x := x \circ f\colon \{0, 1, \ldots, q\} \to I\,.$$

Poiché l'immagine di f^*x è contenuta nell'immagine di x, si ha che l'immagine di f^*x è un elemento di K. Equivalentemente possiamo definire f^* come

$$f^*(x_0, \ldots, x_p) = (x_{f(0)}, \ldots, x_{f(q)})\,.$$

Ad esempio, se consideriamo le applicazioni

$$\delta_i\colon \{0, \ldots, p-1\} \to \{0, \ldots, p\}, \quad 0 \leq i \leq p, \qquad \delta_i(j) = \begin{cases} j & \text{se } j < i, \\ j+1 & \text{se } j \geq i \end{cases},$$

allora

$$\delta_i^*(x_0, \ldots, x_p) = (x_0, \ldots, \widehat{x_i}, \ldots, x_p) = (x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_p).$$

Date due applicazioni $\{0, \ldots, r\} \xrightarrow{g} \{0, \ldots, q\} \xrightarrow{f} \{0, \ldots, p\}$, per l'associatività del prodotto di composizione si ha

$$g^*f^* = (fg)^*\colon K_p \to K_r\,.$$

Definizione 8.2. Dato un complesso simpliciale astratto K ed un intero p, definiamo il gruppo $C_p(K)$ delle **p-catene** in K come il gruppo abeliano libero generato da K_p. In altri termini, una p-catena in K è una combinazione lineare finita di p-simplessi orientati a coefficienti interi:

$$C_p(K) = \left\{ \sum_{\text{finita}} a_i\, s_i \;\middle|\; s_i \in K_p,\ a_i \in \mathbb{Z} \right\}.$$

Consideriamo adesso, per ogni $p > 0$, l'omomorfismo di gruppi $d_p\colon C_p(K) \to C_{p-1}(K)$ definito sui generatori del gruppo libero dalla formula $d_p x = \sum_{i=0}^{p} (-1)^i \delta_i^* x$, ossia

$$d_p(x_0, \ldots, x_p) = \sum_{i=0}^{p} (-1)^i (x_0, \ldots, \widehat{x_i}, \ldots, x_p), \qquad (x_0, \ldots, x_p) \in K_p\,.$$

In particolare, per $p = 1, 2$:

$$d_1(x_0, x_1) = x_1 - x_0, \qquad d_2(x_0, x_1, x_2) = (x_1, x_2) - (x_0, x_2) + (x_0, x_1)\,.$$

Lemma 8.3. *Nelle notazioni precedenti si ha $d_{p-1}d_p = 0$ per ogni p e quindi*

$$C(K) := \qquad \cdots \to C_4(K) \xrightarrow{d_4} C_3(K) \xrightarrow{d_3} C_2(K) \xrightarrow{d_2} C_1(K) \xrightarrow{d_1} C_0(K) \to 0$$

è un complesso di catene.

Dimostrazione. Non è restrittivo dimostrare $d_{p-1}d_p = 0$ per $p \geq 2$ e basta mostrare che per ogni generatore $(x_0, \dots, x_p) \in K_p$ vale $d_{p-1}d_p(x_0, \dots, x_p) = 0$. Qui bisogna fare un conto:

$$\begin{aligned} d_{p-1}d_p(x_0, \dots, x_p) &= d_{p-1} \sum_{i=0}^{p} (-1)^i (x_0, \dots, \widehat{x_i}, \dots, x_p) = \sum_{i=0}^{p} (-1)^i d_{p-1}(x_0, \dots, \widehat{x_i}, \dots, x_p) \\ &= \sum_{i=0}^{p} (-1)^i \left(\sum_{j=0}^{i-1} (-1)^j (\dots, \widehat{x_j}, \dots, \widehat{x_i}, \dots) + \sum_{j=i+1}^{p} (-1)^{j-1} (\dots, \widehat{x_i}, \dots, \widehat{x_j}, \dots) \right) \\ &= \sum_{j<i} (-1)^{i+j} (\dots, \widehat{x_j}, \dots, \widehat{x_i}, \dots) + \sum_{j>i} (-1)^{i+j-1} (\dots, \widehat{x_i}, \dots, \widehat{x_j}, \dots) \,. \end{aligned}$$

Scambiando i con j nella seconda sommatoria ci accorgiamo che tutti gli addendi si cancellano con quelli della prima sommatoria e quindi il totale ha somma nulla. □

Possiamo quindi definire l'**omologia** del complesso simpliciale astratto K come l'omologia del complesso di catene $C(K)$:

$$H_n(K) := H_n(C(K)) \,.$$

Esempio 8.4. Il complesso vuoto ha omologia banale. Infatti $K = \emptyset$ implica $K_p = \emptyset$ per ogni p e quindi $C_p(K) = 0$ per ogni p.

Ai fini del calcolo dell'omologia è utile introdurre un altro complesso di catene, detto **aumentato**. A tal fine si considera l'omomorfismo $d_0 \colon C_0(K) \to \mathbb{Z}$ che vale 1 su ciascun generatore $x \in K_0$. In altri termini

$$d_0(\sum_i a_i \, (x_i)) = \sum a_i, \qquad a_i \in \mathbb{Z}, \quad (x_i) \in K_0 \,.$$

Dato che per ogni $(x_0, x_1) \in K_1$ si ha $d_0 d_1(x_0, x_1) = d_0(x_1 - x_0) = 1 - 1 = 0$, ha senso definire il complesso di catene aumentato

$$\overline{C(K)} := \qquad \cdots \to C_4(K) \xrightarrow{d_4} C_3(K) \xrightarrow{d_3} C_2(K) \xrightarrow{d_2} C_1(K) \xrightarrow{d_1} C_0(K) \xrightarrow{d_0} \mathbb{Z} \to 0,$$

in cui $\mathbb{Z}$ è posizionato in grado -1. Si definisce poi l'omologia aumentata del complesso simpliciale K come

$$\overline{H}_n(K) := H_n(\overline{C(K)}) \,.$$

Lemma 8.5. *Per ogni complesso simpliciale astratto non vuoto K si ha $\overline{H}_n(K) = H_n(K)$ per ogni $n > 0$ ed esiste un isomorfismo (non canonico) di gruppi $H_0(K) \cong \overline{H}_0(K) \oplus \mathbb{Z}$.*

Dimostrazione. L'ipotesi che K sia non vuoto implica che d_0 è surgettivo e quindi $\overline{H}_{-1}(K) = 0$. Siccome $C(K)$ coincide con $\overline{C(K)}$ in tutti i gradi ≥ 0 si ha $H_n(K) = \overline{H}_n(K)$ per ogni $n \geq 1$ in quanto lo n-esimo gruppo di omologia di un complesso C dipende solo dal segmento $C_{n+1} \to C_n \to C_{n-1}$.

Dalla condizione $d_0 d_1 = 0$ segue che il morfismo d_0 si fattorizza ad un omomorfismo surgettivo $\beta \colon H_0(K) = C_0(K)/B_0(K) \to \mathbb{Z}$ il cui nucleo è $\ker(d_0)/B_0(K) = \overline{H}_0(K)$: in altri termini, si ha una successione esatta corta

$$0 \to \overline{H}_0(K) \xrightarrow{\alpha} H_0(K) \xrightarrow{\beta} \mathbb{Z} \to 0 \,.$$

Se $x \in H_0(K)$ è tale che $\beta(x) = 1$ si verifica facilmente che l'omomorfismo

$$\overline{H}_0(K) \oplus \mathbb{Z} \longrightarrow H_0(K), \qquad (y, a) \mapsto \alpha(y) + ax,$$

è un isomorfismo. Diverse scelte di x portano a diversi isomorfismi, il che mostra che l'isomorfismo $H_0(K) \cong \overline{H}_0(K) \oplus \mathbb{Z}$ esiste ma non è canonico. □

Teorema 8.6. *Il complesso di catene aumentato di un complesso simpliciale astratto K di tipo cono è contraibile. Di conseguenza $H_0(K) = \mathbb{Z}$ e $H_n(K) = 0$ per ogni $n > 0$.*

Dimostrazione. Per ipotesi esiste un vertice v di K tale che per ogni $s \in K$ si ha $s \cup \{v\} \in K$ e quindi per ogni $(x_0, \dots, x_p) \in K_p$ si ha $(v, x_0, \dots, x_p) \in K_{p+1}$. Consideriamo quindi gli omomorfismi di gruppi

$$h_{-1} \colon \mathbb{Z} \to C_0(K), \qquad h_p \colon C_p(K) \to C_{p+1}(K),$$

ponendo

$$h_{-1}(1) = (v), \qquad h_p(x_0, \dots, x_p) = (v, x_0, \dots, x_p)\,,$$

e dimostriamo che la famiglia $h = \{h_n\}$ è una contrazione, ossia che $dh + hd = \mathrm{Id}$. La verifica che $d_0 h_{-1} = \mathrm{Id}_{\mathbb{Z}}$ è immediata, mentre se (x) è uno 0-simplesso si ha

$$d_1 h_0(x) + h_{-1} d_0(x) = d_1(v, x) + h_{-1}(1) = (x - v) + v = x\,.$$

Consideriamo quindi un intero positivo $p > 0$ ed un simplesso orientato $(x_0, \dots, x_p) \in K_p$. Allora

$$\begin{aligned}(dh + hd)(x_0, \dots, x_p) &= d(v, x_0, \dots, x_p) + h\left(\sum_{i=0}^{p} (-1)^i (x_0, \dots, \widehat{x_i}, \dots, x_p)\right) \\ &= (x_0, \dots, x_p) + \sum_{i=0}^{p} (-1)^{i+1} (v, x_0, \dots, \widehat{x_i}, \dots, x_p) \\ &\qquad + \sum_{i=0}^{p} (-1)^i (v, x_0, \dots, \widehat{x_i}, \dots, x_p) \\ &= (x_0, \dots, x_p).\end{aligned}$$

□

Esempio 8.7. Per ogni insieme non vuoto I si ha $H_0(\Delta^I) = \mathbb{Z}$ e $H_n(\Delta^I) = 0$ per ogni $n \neq 0$. Questo si applica in particolare al caso Δ^0, ossia al caso in cui esiste un solo vertice.

I complessi di catene, e quindi anche i gruppi di omologia, si comportano bene (gli esperti direbbero in modo funtoriale) rispetto ai morfismi di complessi simpliciali astratti.

Sia $f \colon (K, I) \to (H, J)$ un morfismo di complessi simpliciali astratti. Allora per ogni simplesso orientato $(x_0, \dots, x_p) \in K_p$ si ha $(f(x_0), \dots, f(x_p)) \in H_p$. È dunque definito un morfismo di complessi di catene

$$f \colon C(K) \to C(H)$$

definito sui generatori dalla formula

$$f(x_0, \dots, x_p) = (f(x_0), \dots, f(x_p)), \qquad (x_0, \dots, x_p) \in K_p,\ p \geq 0\,.$$

Che si tratti di un morfismo di complessi è quasi ovvio in quanto

$$\begin{aligned}fd(x_0, \dots, x_p) &= f\left(\sum_{i=0}^{p} (-1)^i (x_0, \dots, \widehat{x_i}, \dots, x_p)\right) = \sum_{i=0}^{p} (-1)^i (f(x_0), \dots, \widehat{x_i}, \dots, f(x_p)) \\ &= \sum_{i=0}^{p} (-1)^i (f(x_0), \dots, \widehat{f(x_i)}, \dots, f(x_p)) = df(x_0, \dots, x_p).\end{aligned}$$

Abbiamo quindi che f definisce dei morfismi in omologia $f \colon H_n(K) \to H_n(H)$. Appare inoltre evidente che tale costruzione commuta con i prodotti di composizione: dati due morfismi di complessi simpliciali astratti $(K, I) \xrightarrow{f} (H, J) \xrightarrow{g} (S, T)$, il morfismo indotto $gf \colon H_n(K) \to H_n(S)$ è uguale alla composizione di $f \colon H_n(K) \to H_n(H)$ e $g \colon H_n(H) \to H_n(S)$.

Le stesse considerazioni valgono anche per i gruppi di omologia aumentata $\overline{H}_n$.

Corollario 8.8. *Sia K un complesso simpliciale astratto di tipo cono e sia $L \subseteq K$ un sottocomplesso di tipo cono. Allora il morfismo di inclusione $L \to K$ induce un isomorfismo in omologia.*

Dimostrazione. Siccome $H_n(K) = H_n(L) = 0$ per ogni $n \neq 0$ basta verificare che $H_0(L) \to H_0(K)$ è un isomorfismo. A tale fine basta osservare che i morfismi di aggiunzione $d_0 \colon C_0(L) \to \mathbb{Z}$ e $d_0 \colon C_0(K) \to \mathbb{Z}$ si fattorizzano a due isomorfismi $H_0(L) \simeq \mathbb{Z}$, $H_0(K) \simeq \mathbb{Z}$ e che $d_0 \colon C_0(L) \to \mathbb{Z}$ coincide con la restrizione di $d_0 \colon C_0(K) \to \mathbb{Z}$ a $C_0(L)$. □

Esercizi:

Esercizio 20. Siano K un complesso simpliciale astratto e $b(K)$ la sua suddivisione baricentrica. Per ogni p-simplesso orientato $x = (x_0, \dots, x_p) \in K_p$ ed ogni permutazione σ di $\{0, \dots, p\}$ definiamo il p-simplesso orientato $\sigma(x) \in b(K)_p$ come

$$\sigma(x) = (\{x_{\sigma(0)}, \dots, x_{\sigma(p)}\},\ \{x_{\sigma(1)}, \dots, x_{\sigma(p)}\},\ \dots,\ \{x_{\sigma(p-1)}, x_{\sigma(p)}\},\ \{x_{\sigma(p)}\})\,.$$

Dimostrare che esiste un morfismo di complessi di catene $f \colon C(K) \to C(b(K))$ tale che

$$f(x) = \sum_\sigma (-1)^\sigma \sigma(x), \qquad \text{per ogni } p \geq 0,\ x \in K_p\,,$$

dove la sommatoria è fatta su tutte le permutazioni di $\{0, \dots, p\}$ e $(-1)^\sigma$ indica ls segnatura. (Suggerimento: dimostrare che la composizione di f con gli omomorfismi $C_p(b(K)) \to C_{p-1}(b(K))$ indotti dalle applicazioni

$$\partial_i \colon b(K)_p \to b(K)_{p-1}, \qquad \partial_i(x_0, \dots, x_p) = (x_0, \dots, \widehat{x_i}, \dots, x_p),$$

si annulla per ogni $i > 0$.)

9. La successione esatta di Mayer-Vietoris

Dati due complessi di catene C, D possiamo considerare il complesso somma diretta

$$C \oplus D := \qquad \cdots \to C_n \oplus D_n \xrightarrow{(x,y)\mapsto(dx,dy)} C_{n-1} \oplus D_{n-1} \to \cdots\ .$$

Segue immediatamente dalla definizione del differenziale in $C \oplus D$ che per ogni n si ha

$$Z_n(C \oplus D) = Z_n(C) \oplus Z_n(D), \qquad B_n(C \oplus D) = B_n(C) \oplus B_n(D),$$

e quindi $H_n(C \oplus D) = H_n(C) \oplus H_n(D)$.

Ad un quadrato commutativo di morfismi di complessi di catene

$$\begin{array}{ccc} C & \xrightarrow{i} & D \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle p} \\ E & \xrightarrow{q} & F \end{array}$$

possiamo associare un diagramma in serie

$$0 \to C \xrightarrow{f} D \oplus E \xrightarrow{g} F \to 0, \qquad f(x) = (i(x), j(x)), \quad g(y, z) = p(y) - q(z), \tag{9.1}$$

con la proprietà che $gf = 0$.

Lemma 9.1. *Nelle notazioni precedenti, se* (9.1) *è una successione esatta corta di complessi di catene, allora esiste una successione esatta lunga di omologia*

$$\cdots \to H_n(C) \xrightarrow{f} H_n(D) \oplus H_n(E) \xrightarrow{g} H_n(F) \to H_{n-1}(C) \to \cdots\ .$$

Inoltre, se j è un quasi-isomorfismo, allora anche p è un quasi-isomorfismo. Se i è un quasi-isomorfismo, allora q è un quasi-isomorfismo

Dimostrazione. La prima parte è conseguenza immediata dalla successione esatta lunga di omologia e dagli isomorfismi naturali $H_n(D \oplus E) = H_n(D) \oplus H_n(E)$.

Supponiamo adesso che $j \colon H_n(C) \to H_n(E)$ sia bigettiva per ogni n, a maggior ragione $H_n(C) \xrightarrow{f=(i,j)} H_n(D) \oplus H_n(E)$ è iniettiva per ogni n e dalla successione esatta lunga di omologia segue che $H_n(D) \oplus H_n(E) \xrightarrow{g} H_n(F)$ è surgettiva per ogni n. D'altra parte per ogni $(y, z) \in H_n(D) \oplus H_n(E)$ si ha

$$p(y - ij^{-1}(z)) = p(y) - pij^{-1}(z) = p(y) - qjj^{-1}(z) = p(y) - q(z) = g(y, z)$$

e questo prova che $p\colon H_n(D) \to H_n(F)$ è surgettiva. Se $y \in H_n(D)$ e $p(y) = 0$, allora $(y, 0) \in \ker(g) = f(H_n(C))$ ed esiste $x \in H_n(C)$ tale che $i(x) = y$, $j(x) = 0$. Ma j è iniettiva, quindi $x = 0$ ed a maggior ragione $y = 0$.

Abbiamo quindi provato che se j è un quasi-isomorfismo allora anche p è un quasi-isomorfismo. Per ovvii motivi di simmetria, vale anche che se i è un quasi-isomorfismo allora anche q è un quasi-isomorfismo.

□

Consideriamo adesso un insieme I e due sottocomplessi simpliciali astratti $K, L \subseteq \Delta^I$ i cui rispettivi insiemi di vertici possono essere strettamente contenuti in I. Abbiamo visto che le loro unione $K \cup L$ ed intersezione $K \cap L$ sono ancora sottocomplessi simpliciali astratti.

Teorema 9.2 (Mayer-Vietoris)**.** *Nella notazioni precedenti esiste una successione esatta lunga di omologia*

$$\cdots \to H_n(K\cap L) \to H_n(K)\oplus H_n(L) \to H_n(K\cup L) \to H_{n-1}(K\cap L) \to \cdots \to H_0(K\cup L) \to 0\,.$$

Se l'inclusione $K \cap L \subseteq L$ induce un isomomorfismo in omologia, allora anche l'inclusione $K \subseteq K \cup L$ induce un isomorfismo in omologia.

Dimostrazione. Per un simplesso ordinato $(x_0, \ldots, x_p)$ le seguenti condizioni sono equivalenti:

(1) $(x_0, \ldots, x_p) \in (K \cup L)_p$;
(2) $\{x_0, \ldots, x_p\} \in K \cup L$;
(3) $\{x_0, \ldots, x_p\} \in K$ oppure $\{x_0, \ldots, x_p\} \in L$;
(4) $(x_0, \ldots, x_p) \in K_p$ oppure $(x_0, \ldots, x_p) \in L_p$;

e quindi $(K \cup L)_p = K_p \cup L_p$. Similmente $(K \cap L)_p = K_p \cap L_p$. Da ciò segue che esiste una successione esatta corta di complessi di catene

$$0 \to C(K \cap L) \xrightarrow{f} C(K) \oplus C(L) \xrightarrow{g} C(K \cup L) \to 0, \tag{9.2}$$

dove morfismi f e g sono definiti sui simplessi orientati come

$$f(x_0, \ldots, x_p) = ((x_0, \ldots, x_p), (x_0, \ldots, x_p)),$$
$$g((x_0, \ldots, x_p), (y_0, \ldots, y_p)) = (x_0, \ldots, x_p) - (y_0, \ldots, y_p)\,.$$

Basta adesso applicare il Lemma 9.1. □

Corollario 9.3. *Nelle ipotesi del Teorema 9.2, se $K \cap L = \emptyset$, allora $H_n(K \cup L) = H_n(K) \oplus H_n(L)$.*

Dimostrazione. $H_n(\emptyset) = 0$ per ogni n. □

Esempio 9.4. Se il complesso simpliciale astratto K è formato da n vertici senza alcun simplesso di dimensione positiva, allora $H_0(K) = \mathbb{Z}^n$ e $H_p(K) = 0$ per ogni $p \neq 0$.

10. Potature e baricentri aggiunti

Come prima applicazione della successione esatta di Mayer-Vietoris mostriamo che le operazioni di **potatura** di un complesso simpliciale astratto non cambiano l'omologia.

Siano M un complesso simpliciale astratto ed $s = (x_0, \ldots, x_p) \in M_p$ un simplesso orientato non degenere di dimensione positiva (ossia $x_i \neq x_j$ per ogni $i \neq j$ e $p > 0$). Si assuma che $\{x_0, \ldots, x_p\}$ sia un simplesso massimale (ossia non contenuto in alcun simplesso di dimensione maggiore) e che $\{x_0, \ldots, x_p\}$ sia l'unico simplesso di M che contiene strettamente $\{x_1, \ldots, x_p\}$.

Sia $K \subset P$ ottenuto togliendo i due simplessi $\{x_0, \ldots, x_p\}$ e $\{x_1, \ldots, x_p\}$; è chiaro per costruzione che K è un sottocomplesso simpliciale, che viene detto una **potatura** di s da P. Più in generale, parleremo di potatura (di una successione di simplessi orientati) per intedere una successione finita di operazioni come sopra, vedi Figura 7.

Consideriamo adesso il sottocomplesso $L = \Delta^{\{x_0,\ldots,x_p\}}$, allora $P = K \cup L$ ed i due sottocomplessi L, $K \cap L$ sono entrambi coni di vertice x_0.

Per il Corollario 8.8 l'inclusione $K \cap L \subset L$ induce un isomorfismo in omologia, e per il teorema di Mayer-Vietoris anche l'inclusione $K \subset P$ induce un isomorfismo in omologia.

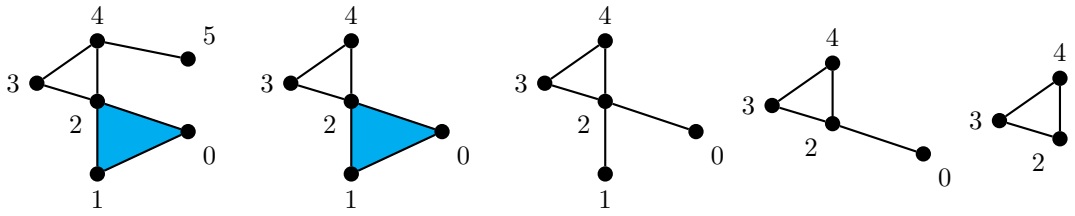


FIGURA 7. La potatura dei simplessi orientati $(4,5)$, $(2,1,0)$, $(2,1)$ e $(2,0)$.

Per transitività hanno la stessa omologia pure due complessi simpliciali astratti che si ottengono come potature (di simplessi distinti) di un medesimo complesso simpliciale astratto (vedi Figura 8).

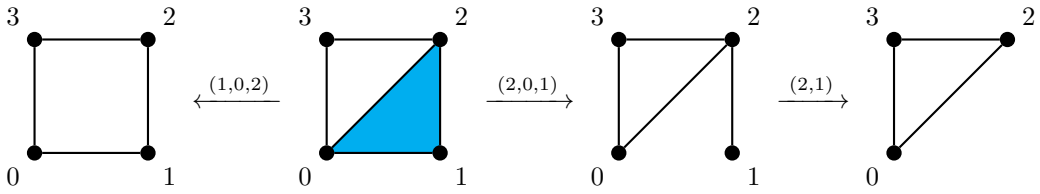


FIGURA 8. I bordi del quadrato e del triangolo si ottengono per potature da un medesimo complesso simpliciale astratto (il secondo da sinistra).

Possiamo formalizzare la procedura di Figura 8 nel modo seguente. Siano (K, I) un complesso simpliciale astratto $\{x_0, \dots, x_p\} \in K$ un simplesso massimale di dimensione p, $v \notin I$ e definiamo un nuovo complesso simpliciale

$$P = K \cup \Delta^{\{v, x_0, \dots, x_p\}} \subset \Delta^{I \cup \{v\}} .$$

È chiaro che $K \cap \Delta^{\{v, x_0, \dots, x_p\}} = \Delta^{\{x_0, \dots, x_p\}}$ e quindi, per Mayer-Vietoris si ha che l'inclusione $K \subset P$ è un isomorfismo in omologia. A questo punto possiamo eseguire su P la potatura del simplesso orientato $(v, x_0, \dots, x_p)$ ed ottenere un nuovo complesso simpliciale L che ha la stessa omologia di K.

Diremo che per passare da K ad L abbiamo **aggiunto il baricentro** al simplesso massimale $\{x_0, \dots, x_p\}$. In pratica, abbiamo prima eliminato da K il simplesso $\{x_0, \dots, x_p\}$ e poi abbiamo aggiunto tutti i $2^{p+1} - 1$ simplessi del tipo $\{v, x_{i_1}, \dots, x_{i_q}\}$, con $0 \le q \le p$ e $0 \le i_1 < \cdots < i_q \le p$ (Figura 9).

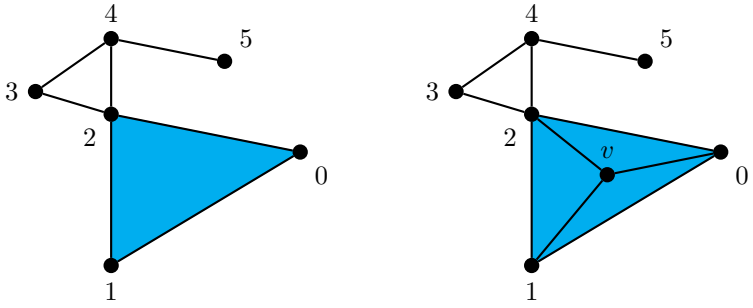
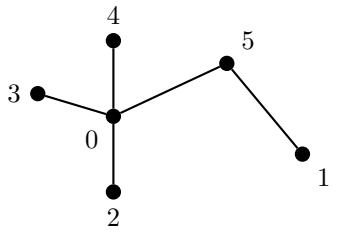


FIGURA 9. Aggiunta del baricentro al simplesso massimale $\{0, 1, 2\}$.

Esempio 10.1. Il grafo semplice



si può ricondurre per potatura al solo vertice 0 e pertanto ha la stessa omologia del punto. Un grafo riconducibile per potature ad un punto si dice un **albero**.

Definizione 10.2. Un complesso simpliciale astratto si dice **connesso** se non è unione di due sottocomplessi simpliciali non vuoti e disgiunti.

Lemma 10.3. *Un complesso simpliciale astratto K è connesso se e solo se ogni coppia di vertici v, w è collegata da una successione finita di 1-simplessi*

$$\{v, u_1\},\ \{u_1, u_2\},\ \ldots,\ \{u_n, w\} \in K^{(1)}\,.$$

In particolare K è connesso se e solo se $K^{(1)}$ è connesso.

Dimostrazione. Se $K = \emptyset$ non c'è nulla da dimostrare. Se K è sconnesso e $K = L \cup P$ con L, P complessi simpliciali astratti non vuoti e disgiunti, allora $\{l, p\} \notin K$ per ogni $l \in L^{(0)}$, $p \in P^{(0)}$: se per assurdo fosse $\{l, p\} \in K$ e, tanto per fissare le idee $\{l, p\} \in L$, allora $p \in L$ che è assurdo. In particolare nessun vertice di L è collegato ad un vertice di p.

Viceversa, sia (K, I) connesso e non vuoto, fissiamo un vertice $v \in I$ e scriviamo $I = J \cup (I - J)$ dove J è l'insieme dei vertici connessi a v mediante un numero finito di 1-simplessi; vogliamo dimostrare che $J = \emptyset$. Se fosse $J \neq \emptyset$ allora

$$L := \Delta^J \cap K \neq \emptyset, \qquad P := \Delta^{I-J} \cap K \neq \emptyset, \qquad L \cap P = \emptyset\,.$$

Se esistesse un simplesso $\{x_0, \ldots, x_p\} \in K - (L \cup P)$ allora esistono j, h tali che $x_j \in J$, $x_h \in I - J$ e quindi x_j, x_h sono collegati da un 1-simplesso. Siccome x_j è collegato a v mediante un numero finito di 1-simplessi, lo stesso vale anche per x_h. □

Teorema 10.4. *Se (K, I) è un complesso simpliciale astratto connesso e non vuoto. Allora $H_0(K) = \mathbb{Z}$.*

Dimostrazione. Abbiamo già dimostrato che $H_0(\Delta^I) = \mathbb{Z}$, basta quindi dimostrare che l'inclusione $K \subset \Delta^I$ induce un isomorfismo $H_0(K) = H_0(\Delta^I)$. Siccome $C_0(K) = C_0(\Delta^I) = \mathbb{Z}^{(I)}$ basta dimostrare che i due differenziali

$$d\colon C_1(K) \to C_0(K), \qquad d\colon C_1(\Delta^I) \to C_0(\Delta^I),$$

hanno la stessa immagine. Siccome $C_1(K) \subseteq C_1(\Delta^I)$ è chiaro che $d(C_1(K)) \subseteq d(C_1(\Delta^I))$. Siccome $d(C_1(\Delta^I))$ è il sottogruppo generato dagli elementi $d(v, w) = (w) - (v)$, $v, w \in I$, basta considerare una catena finita di 1-simplessi

$$\{v, u_1\},\ \{u_1, u_2\},\ \ldots,\ \{u_n, w\} \in K\,,$$

e scrivere

$$d(v, w) = d(v, u_1) + d(u_1, u_2) + \cdots + d(u_n, w) \in d(C_1(K))\,.$$

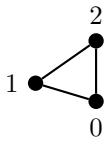
□

Esercizi:

Esercizio 21. Sia K un sottocomplesso proprio di Δ^n. Provare che se K è un complesso di cricche, allora K contiene al più due simplessi di dimensione $n - 1$.

11. Il sottocomplesso delle catene ordinate

Se vogliamo calcolare esplicitamente i gruppi di omologia di un complesso simpliciale astratto ci troviamo di fronte alla difficoltà di lavorare con insiemi di simplessi orientati K_p molto grandi e mai vuoti anche per p molto maggiore della dimensione del complesso simpliciale. Ad esempio, nel caso del triangolo vuoto



si ha che K_p contiene esattamente $3(2^{p+1}-1)$ elementi (esercizio: dimostrare).

Per ovviare a tale inconveniente si possono considerare i sottocomplessi di catene ordinate. Sia (K, I) un complesso simpliciale astratto e dotiamo I di una **relazione di ordine totale** $\leq$. Ricordiamo che per ordine totale si intende una relazione di ordine $\leq$ con la proprietà che per ogni x, y si ha $x \leq y$ oppure $y \leq x$. Le possibili relazioni di ordine totale su un insieme sono tante, almeno quanto le permutazioni, e per i nostri scopi ne va bene una qualunque.

A questo punto, per ogni intero $p \geq 0$ possiamo considerare il sottoinsieme dei **p-simplessi ordinati**

$$K_p^< = \{(x_0, \dots, x_p) \in K_p \mid x_0 < x_1 < \cdots < x_p\}.$$

Osserviamo con immenso piacere che se K ha dimensione n, allora $K_p^< = \emptyset$ per ogni $p > n$, e comunque che $K_p^<$ è notevolmente più piccolo di K_p: ad esempio, per il complesso simpliciale astratto Δ^n, l'insieme K_p contiene $(n+1)^{p+1}$ elementi, mentre $K_p^<$ ne contiene $\binom{n+1}{p+1}$.

Un'altra osservazione che ci riempie di gioia è che se $(x_0, \dots, x_p) \in K_p^<$ allora per ogni indice i si ha $(x_0, \dots, \widehat{x_i}, \dots, x_p) \in K_{p-1}^<$.

Indichiamo con $C_p(K, <) \subset C_p(K)$ il gruppo abeliano libero generato da $K_p^<$. Al variare di p questi gruppi definiscono un sottocomplesso di catene $C(K, <) \subseteq C(K)$ in quanto chiuso per il differenziale

$$d(x_0, \dots, x_p) = \sum_{i=0}^{p} (-1)^i (x_0, \dots, \widehat{x_i}, \dots, x_p)\,.$$

Vogliamo dimostrare il seguente risultato

Teorema 11.1. *Nelle notazioni precedenti l'inclusione di complessi di catene $C(K, <) \subseteq C(K)$ induce isomorfismi in omologia:*

$$H_n(C(K, <)) = H_n(C(K)) = H_n(K), \qquad \textit{per ogni } n\,.$$

La dimostrazione è abbastanza lunga e laboriosa e per chiarezza espositiva viene spezzata in una serie di lemmi. L'idea è la seguente: si introduce una successione di sottocomplessi

$$C(K, <) \subset C^0 \subset C^1 \subset \cdots \subset C(K)$$

tali che:

(1) le inclusioni $C(K, <) \subset C^0$ e $C^k \subset C^{k+1}$ inducono isomorfismi in omologia;
(2) $H_n(C^k) = H_n(C(K))$ per ogni $k > n$.

Per ogni coppia di interi non negativi $p, k \geq 0$ consideriamo il seguente insieme di simplessi ordinati:

$$K_p^k = \{(x_0, \dots, x_p) \in K_p \mid x_0 \leq x_1 \leq \cdots \leq x_{p-k}\}.$$

Osserviamo che:

(1) $K_p^k = K_p$ per ogni $k \geq p$;
(2) $K_p^0 = \{(x_0, \dots, x_p) \in K_p \mid x_0 \leq x_1 \leq \cdots \leq x_p\}$.
(3) se $(x_0, \dots, x_p) \in K_p^k$, allora $(x_0, \dots, \widehat{x_i}, \dots, x_p) \in K_{p-1}^k$ per ogni $i = 0, \dots, p$.

Definiamo quindi C^k come il sottocomplesso di $C(K)$ tale che $C_p^k \subset C_p(K)$ è il sottogruppo generato da K_p^k. Siccome $C_p^k = C_p(K)$ per ogni $k \geq p$ si ha che l'inclusione $C^k \subset C(K)$ induce un isomorfismo $H_p(C^k) = H_p(C(K))$ per ogni $k > p$.

Lemma 11.2. *L'inclusione $i\colon C(K,<) \to C^0$ è un'equivalenza omotopica e quindi un isomorfismo in omologia.*

Dimostrazione. Consideriamo la proiezione $\pi\colon C^0 \to C(K,<)$ definita per estensione lineare delle applicazioni $\pi\colon K_p^0 \to K_p^<$ definite come:

$$\pi(x_0,\dots,x_p) = \begin{cases} (x_0,\dots,x_p) & \text{se } (x_0,\dots,x_p) \in K_p^<, \\ 0 & \text{se } (x_0,\dots,x_p) \in K_p^0 - K_p^<. \end{cases}$$

È chiaro per definizione che $\pi i = \mathrm{Id}$ e vogliamo dimostrare che esiste un'omotopia $h\colon C^0 \to C^0[1]$ tale che $dh + hd = \mathrm{Id} - i\pi$. Dato $(x_0,\dots,x_p) \in K_p^<$ definiamo $h(x_0,\dots,x_p) = 0$; se invece $(x_0,\dots,x_p) \in K_p^0 - K_p^<$ e $0 \le k < p$ è il più piccolo indice tale che $x_k = x_{k+1}$ definiamo

$$h(x_0,\dots,x_p) = (-1)^k (x_0,\dots x_{k-1}, x_k, x_k, x_{k+1},\dots,x_p)\,.$$

Si noti che $(x_0,\dots x_{k-1}, x_k, x_k, x_{k+1},\dots,x_p)$ contiene, nelle posizioni $k, k+1, k+2$ tre vertici consecutivi uguali. Se proviamo che

$$(dh+hd)(x_0,\dots,x_p) = \begin{cases} 0 & \text{se } (x_0,\dots,x_p) \in K_p^<, \\ (x_0,\dots,x_p) & \text{se } (x_0,\dots,x_p) \in K_p^0 - K_p^<, \end{cases}$$

allora l'estensione lineare di h a tutto C^0 soddisfa la condizione $dh + hd = \mathrm{Id} - i\pi$.

Se $(x_0,\dots,x_p) \in K_p^<$, si ha banalmente che $(dh+hd)(x_0,\dots,x_p) = 0$. Esaminiamo quindi il caso $(x_0,\dots,x_p) \in K_p - K_p^<$ e sia $0 \le k < p$ il più piccolo indice tale che $x_k = x_{k+1}$. Per definizione

$$h(x_0,\dots,x_p) = (-1)^k (x_0,\dots,x_k,x_k,x_{k+1},\dots,x_p),$$

da cui

$$\begin{aligned} dh(x_0,\dots,x_p) &= (-1)^k \sum_{j=0}^{k-1} (-1)^j (x_0,\dots,\widehat{x_j},\dots,x_{k-1},x_k,x_k,x_{k+1},\dots,x_p) \\ &\quad + (-1)^{2k}(x_0,\dots,x_p) + (-1)^{2k+1}(x_0,\dots,x_p) + (-1)^{2(k+1)}(x_0,\dots,x_p) \\ &\quad + (-1)^k \sum_{j=k+2}^{p} (-1)^{j+1} (x_0,\dots,x_k,x_k,x_{k+1},x_{k+2},\dots,\widehat{x_j},\dots,x_p) \\ &= (-1)^k \sum_{j=0}^{k-1} (-1)^j (x_0,\dots,\widehat{x_j},\dots,x_{k-1},x_k,x_k,x_{k+1},\dots,x_p) \\ &\quad + (x_0,\dots,x_p) \\ &\quad + (-1)^k \sum_{j=k+2}^{p} (-1)^{j+1} (x_0,\dots,x_k,x_k,x_{k+1},x_{k+2},\dots,\widehat{x_j},\dots,x_p)\,. \end{aligned}$$

Usando il fatto che $x_k = x_{k+1}$ possiamo scrivere

$$d(x_0,\dots,x_p) = \sum_{j=0}^{k-1} (-1)^j (x_0,\dots,\widehat{x_j},\dots,x_p) + \sum_{j=k+2}^{p} (-1)^j (x_0,\dots,\widehat{x_j},\dots,x_p)\,,$$

$$\begin{aligned} hd(x_0,\dots,x_p) =& (-1)^{k-1} \sum_{j=0}^{k-1} (-1)^j (x_0,\dots,\widehat{x_j},\dots,x_{k-1},x_k,x_k,x_{k+1},\dots,x_p) \\ &+ (-1)^k \sum_{j=k+2}^{p} (-1)^j (x_0,\dots,x_k,x_k,x_{k+1},\dots,\widehat{x_j},\dots,x_p)\,. \end{aligned}$$

e sommando otteniamo

$$(dh+hd)(x_0,\dots,x_p) = (x_0,\dots,x_p)\,.$$

□

Lemma 11.3. *Per ogni $k \geq 0$ fissato l'inclusione di complessi di catene $C^k \subset C^{k+1}$ è un quasi-isomorfismo.*

Dimostrazione. Consideriamo l'omotopia $h\colon C^{k+1} \to C^{k+1}[1]$ definita sui generatoti, ossia sui simplessi $(x_0, \dots, x_p) \in K_p^{k+1}$ con $x_0 \leq \cdots \leq x_{p-k-1}$, come

$$h(x_0, \dots, x_p) = 0 \qquad \text{se} \quad k > p,$$

mentre se $k \leq p$ poniamo

$$h(x_0, \dots, x_p) = (-1)^j (x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p)$$

dove $0 \leq j \leq p-k$ è il più piccolo indice tale che $x_{p-k} \leq x_j$. L'omotopia h risulta ben definita in quanto

$$x_0 \leq \cdots \leq x_{j-1} \leq x_{p-k} \leq x_j \leq \cdots \leq x_{p-k-1}\,.$$

Si osserva che $h(C_p^k) \subset C_{p+1}^k$ e quindi, per il Corollario 5.21 basta dimostrare che

$$(dh + hd - \mathrm{Id})(C_p^{k+1}) \subseteq C_p^k \tag{11.1}$$

per ogni p.

Se $k \geq p$ l'inclusione (11.1) è ovvia in quanto $C_p^k = C_p^{k+1}$; supponiamo quindi $k < p$.

Fissiamo $(x_0, \dots, x_p) \in K_p^{k+1}$ (quindi $x_0 \leq \cdots \leq x_{p-k-1}$) e sia $0 \leq j \leq p-k$ è il più piccolo indice tale che $x_{p-k} \leq x_j$. Si ha

$$h(x_0, \dots, x_p) = (-1)^j (x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p),$$

$$(x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, \widehat{x_h}, \dots, x_p) \in K_p^k \quad \text{per ogni} \quad h \geq p-k,$$

e quindi

$$\begin{aligned} dh(x_0, \dots, x_p) &= (-1)^j d(x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p) \\ &= (-1)^j \sum_{l=0}^{j-1} (-1)^l (x_0, \dots, \widehat{x_l}, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p) + (-1)^{2j} (x_0, \dots, x_p) \\ &\quad + (-1)^j \sum_{l=j}^{p-k-1} (-1)^{l+1} (x_0, \dots, x_{j-1}, x_{p-k}, x_j, \dots, \widehat{x_l}, \dots, x_{p-k-1}, x_{p-k}, \dots, x_p) + y, \end{aligned}$$

per un opportuno elemento $y \in C_p^k$. Similmente:

$$\begin{aligned} d(x_0, \dots, x_p) &= \sum_{l=0}^{j-1} (-1)^l (x_0, \dots, \widehat{x_l}, \dots, x_{j-1}, \dots, x_p) \\ &\quad + \sum_{l=j}^{p-k-1} (-1)^l (x_0, \dots, x_j, \dots, \widehat{x_l}, \dots, x_{p-k-1}, \dots, x_p) + z, \end{aligned}$$

con $z \in C_{p-1}^k$, da cui

$$\begin{aligned} hd(x_0, \dots, x_p) &= (-1)^{j-1} \sum_{l=0}^{j-1} (-1)^l (x_0, \dots, \widehat{x_l}, \dots, x_{j-1}, x_{p-k}, x_j, \dots, x_p) \\ &\quad + (-1)^j \sum_{l=j}^{p-k-1} (-1)^l (x_0, \dots, x_j, x_{p-k}, x_j, \dots, \widehat{x_l}, \dots, x_{p-k-1}, \dots, x_p) + h(z)\,. \end{aligned}$$

Sommando si ottiene

$$(dh + hd)(x_0, \dots, x_p) = (x_0, \dots, x_p) + y + h(z)\,.$$

□

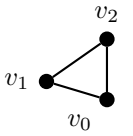
Adesso il Teorema 11.1 segue immediatamente dai due lemmi precedenti e dal fatto che $H_p(C^k) = H_p(C(K))$ per ogni $k > p$.

Corollario 11.4. *Per un complesso simpliciale astratto K si ha $H_n(K) = 0$ per ogni $n > \dim K$.*

Dimostrazione. Ordinando i vertici, per costruzione $C_n(K,<) = 0$ per ogni $n > \dim K$. □

Usando il complesso $C(K,<)$ delle catene ordinate possiamo calcolare direttamente, se necessario con l'aiuto del computer, l'omologia di alcuni complessi simpliciali astratti.

Esempio 11.5. Il complesso delle catene ordinate del triangolo vuoto



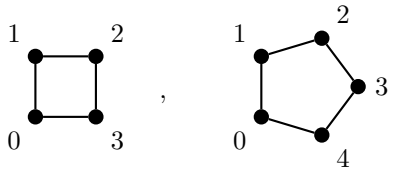
è $\oplus_{i<j}\mathbb{Z}(v_i,v_j) \xrightarrow{d} \oplus_i \mathbb{Z}(v_i)$, dove:

$$d(a(v_0,v_1)+b(v_0,v_2)+c(v_1,v_2)) = (-a-b)(v_0)+(a-c)(v_1)+(c+b)(v_2),$$

Per connessione $H_0 = \mathbb{Z}$, mentre

$$H_1 = \ker(d) = \{(a,b,c) \mid a = c = -b\} = \{(n,-n,n) \mid n \in \mathbb{Z}\} \cong \mathbb{Z}\,.$$

Aggiungendo baricentri a simplessi massimali si ottengono i grafi



eccetera,

che pertanto hanno la stessa omologia del triangolo.

Il precedente esempio è un caso particolare della seguente proposizione.

Proposizione 11.6. *Sia $K = \Delta^n - \{0,1,\dots,n\}$, $n \geq 2$. Allora*

$$H_0(K) = H_{n-1}(K) = \mathbb{Z}, \qquad H_i(K) = 0 \text{ per ogni } i \neq 0, n-1\,.$$

Dimostrazione. Il caso $n = 2$ è già stato analizzato nell'Esempio 11.5; possiamo quindi considerare il caso $n > 2$. Si osservi che $C_p(K,<) = C_p(\Delta^n,<)$ per ogni $p \neq n$ e $C_n(\Delta^n,<) = \mathbb{Z}(0,1,\dots,n) \cong \mathbb{Z}$. Sia E il complesso di catene che vale $E_n = C_n(\Delta^n,<)$ e $E_p = 0$ per ogni $p \neq n$, allora l'inclusione $C(K,<) \subset C(\Delta^n,<)$ si estende in maniera ovvia ad una successione esatta corta di complessi

$$0 \to C(K,<) \to C(\Delta^n,<) \to E \to 0$$

e la successione esatta lunga di omologia ci fornisce le successioni esatte

$$H_{p+1}(E) \to H_p(K) \to H_p(\Delta^n) \to H_p(E)$$

e siccome $H_{p+1}(E) = H_p(E) = 0$ per ogni $p \neq n-1, n$ si ha che $H_p(K) = H_p(\Delta^n)$ per ogni $p < n-1$. Si ha poi una successione esatta

$$0 = H_n(\Delta^n) \to H_n(E) = \mathbb{Z} \to H_{n-1}(K) \to H_{n-1}(\Delta^n) = 0$$

da cui segue $H_{n-1}(K) = \mathbb{Z}$. Infine se $p > n$ si ha $C_p(K,<) = 0$ ed a maggior ragione $H_p(K) = 0$. □

La **caratteristica di Eulero-Poincaré** di un complesso simpliciale astratto finito K si definisce mediante la formula

$$\chi(K) = \sum_{n=0}^{\dim K} (-1)^n k_n,$$

dove $k_n = |K^{(n)} - K^{(n-1)}|$ è il numero di simplessi in K di dimensione n.

Ad esempio, per il complesso simpliciale $K = \Delta^m$, per ogni $n = 0,\dots,m$ si ha $k_n = \binom{m+1}{n+1}$ e quindi

$$\chi(\Delta^m) = \sum_{n=0}^{m} (-1)^n \binom{m+1}{n+1} = 1 - \sum_{i=0}^{m+1} (-1)^i \binom{m+1}{i} = 1 - (1-1)^{m+1} = 1\,.$$

La caratteristica di Eulero-Poincaré è quindi una quantità di facile calcolo la cui importanza si deve al fatto che dipende solo dall'omologia di K. Per un complesso simpliciale astratto finito K i gruppi $C_p(K)$ sono tutti finitamente generati e quindi pure tutti i gruppi di omologia $H_n(K)$ sono finitamente generati. I loro ranghi vengono detti **numeri di Betti** e sono denotati $b_n(K) = \operatorname{rank} H_n(K)$.

Teorema 11.7 (di Eulero-Poincaré)**.** *Dato un complesso simpliciale astratto finito K si ha*

$$\chi(K) = \sum_{n=0}^{\dim K} (-1)^n b_n(K) = \sum_{n=0}^{\dim K} (-1)^n \operatorname{rank} H_n(K)\,.$$

Dimostrazione. Sia d la dimensione di K, possiamo allora fissare un ordinamento totale sui vertici e calcolare l'omologia usando il complesso delle catene ordinate:

$$0 \to C_d(K,<) \xrightarrow{d} \cdots C_1(K,<) \xrightarrow{d} C_0(K,<) \to 0\,.$$

Per costruzione ciascun $C_n(K,<)$ è un gruppo abeliano libero di rango k_n ed il complesso di catene ordinate si spezza in una serie di successioni esatte corte di gruppi abeliani finitamente generati:

$$0 \to Z_n \to C_n(K,<) \to B_{n-1} \to 0, \quad 0 \to B_n \to Z_n \to H_n(K) \to 0\,.$$

Per l'additività del rango si ha quindi per ogni n:

$$k_n = \operatorname{rank} C_n(K,<) = \operatorname{rank} Z_n + \operatorname{rank} B_{n-1}, \quad b_n(K) = \operatorname{rank} H_n(K) = \operatorname{rank} Z_n - \operatorname{rank} B_n$$

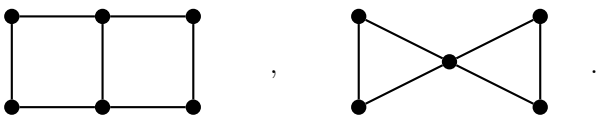
e quindi

$$\begin{aligned}\sum_n (-1)^n (k_n - b_n(K)) &= \sum_n (-1)^n (\operatorname{rank} B_{n-1} + \operatorname{rank} B_n) \\ &= \sum_n ((-1)^n + (-1)^{n-1}) \operatorname{rank} B_n = 0\,.\end{aligned}$$

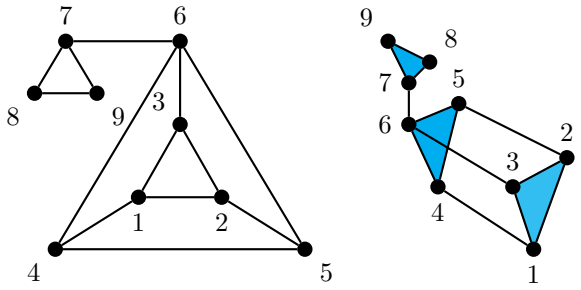
□

Esercizi:

Esercizio 22. Mediante potature, aggiunte di baricentri e loro operazioni inverse, trasformare l'uno nell'altro i seguenti grafi semplici:



Esercizio 23. Calcolare i gruppi di omologia del seguente grafo semplice (a sinistra) e del corrispondente complesso di cricche (a destra):



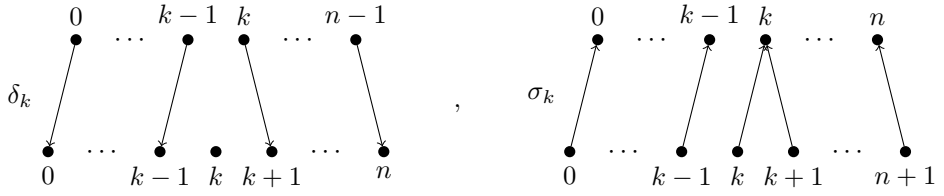


FIGURA 10. Facce e degenerazioni

12. Insiemi simpliciali

Se $n \geq 0$ è un intero non negativo denotiamo $[n] = \{0, \dots, n\}$ considerato come insieme *ordinato*, ossia dotato della usuale relazione di ordine $\leq$. Scriveremo inoltre $f\colon [n] \to [m]$ per indicare un'applicazione *monotona*

$$f\colon \{0,\dots,n\} \to \{0,\dots,m\}, \qquad f(0) \leq f(1) \leq \cdots \leq f(m)\,.$$

Lemma 12.1 (Fattorizzazione epi-moni)**.** *Ogni morfismo $f\colon [n] \to [m]$ si fattorizza in modo unico come $f = hg$ con $g\colon [n] \to [p]$ surgettiva e $h\colon [p] \to [m]$ iniettiva.*

Dimostrazione. Se l'immagine $f([n]) \subset [m]$ contiene $p+1$ elementi, esiste un'unica applicazione bigettiva e monotona $h\colon [p] \to f([n])$ e si definisce g come la composizione

$$g\colon [n] \xrightarrow{f} f([n]) \xrightarrow{h^{-1}} [p]\,.$$

□

Particolare importanza hanno i morfismi **faccia**:

$$\delta_k\colon [n-1] \to [n], \qquad \delta_k(p) = \begin{cases} p & \text{se } p < k \\ p+1 & \text{se } p \geq k \end{cases}, \qquad k = 0, \dots, n\,,$$

ed i morfismi **degenerazione**:

$$\sigma_k\colon [n+1] \to [n], \qquad \sigma_k(p) = \begin{cases} p & \text{se } p \leq k \\ p-1 & \text{se } p > k \end{cases}, \qquad k = 0, \dots, n\,.$$

Si noti che $\delta_k\colon [n-1] \to [n]$ è l'unica applicazione iniettiva monotona la cui immagine non contiene k e che $\sigma_k\colon [n+1] \to [n]$ è l'unica applicazione surgettiva monotona tale che il bersaglio k è colpito due volte (da k e $k+1$).

Le regole di commutazione di facce e degenerazioni sono regolate dal seguente lemma.

Lemma 12.2 (Identità cosimpliciali)**.** *Nelle notazioni precedenti si ha*

$$\delta_i\delta_j = \delta_{j+1}\delta_i \quad \textit{per ogni} \quad i \leq j;$$

$$\sigma_i\sigma_j = \sigma_j\sigma_{i+1} \quad \textit{per ogni} \quad i \geq j;$$

$$\sigma_i\delta_j = \begin{cases} \delta_{j-1}\sigma_i & \textit{per ogni } j > i+1 \\ \mathrm{Id} & \textit{per } j = i, i+1 \\ \delta_j\sigma_{i-1} & \textit{per ogni } j < i\,. \end{cases} \tag{12.1}$$

Dimostrazione. La dimostrazione è del tutto elementare ma decisamente noiosa. Pertanto ci fidiamo dei tanti di libri di testo dove le identità cosimpliciali sono riportate (e quasi sempre lasciate per esercizio). □

Osservazione 12.3. Possiamo raffinare ulteriormente la fattorizzazione epi-moni osservando che ogni $f\colon [n] \to [m]$ possiede un'unica decomposizione del tipo

$$f = \delta_{i_1} \cdots \delta_{i_k} \sigma_{j_1} \cdots \sigma_{j_h} \tag{12.2}$$

con

$$m \geq i_1 > i_2 > \cdots > i_k \geq 0, \qquad 0 \leq j_1 < \cdots < j_h < n\,.$$

La dimostrazione è lasciata per esercizio.

Definizione 12.4. Un **insieme simpliciale** $X_\bullet$ è una collezione di insiemi ed applicazioni cosí definita:

(1) per ogni intero $n \geq 0$ è dato un insieme X_n;
(2) per ogni applicazione monotona $f\colon [n] \to [m]$ è data un'applicazione $f^*\colon X_m \to X_n$.

Le applicazioni f^* devono soddisfare le seguenti *condizioni di controvarianza*:

(1) se $\mathrm{Id}\colon [n] \to [n]$ è l'identità allora anche $\mathrm{Id}^*\colon X_n \to X_n$ è l'identità;
(2) dati comunque $[n] \xrightarrow{f} [m] \xrightarrow{g} [p]$ si ha $(gf)^* = f^*g^*\colon X_p \to X_n$.

Dato un insieme simpliciale $X_\bullet$, per semplicità di notazione denotiamo

$$\partial_i = \delta_i^*\colon X_n \to X_{n-1}, \qquad i = 0, \dots, n\,.$$

$$s_i = \sigma_i^*\colon X_n \to X_{n+1}, \qquad i = 0, \dots, n\,.$$

Esempio 12.5. Ad ogni insieme U è associato in modo canonico un insieme simpliciale $X_\bullet$ ponendo $X_n = U$ per ogni n e $f^* = \mathrm{Id}_U$ per ogni $f\colon [n] \to [m]$.

Esempio 12.6. Se K è un complesso simpliciale astratto, la famiglia $K_\bullet$ degli insiemi K_p (p-simplessi orientati) ha una struttura di insieme simpliciale, dove per ogni $f\colon [n] \to [m]$ si definisce

$$f^*\colon K_m \to K_n, \qquad f^*(x_0, \dots, x_m) = (x_{f(0)}, \dots, x_{f(n)})\,.$$

Ad esempio se $f\colon [3] \to [2]$ è l'applicazione

$$f(0) = f(1) = 1, \quad f(2) = f(3) = 2,$$

e K è il complesso simpliciale astratto e completo dei supereroi si ha

$$f^*(\mathrm{Batman}, \mathrm{Superman}, \mathrm{Superciuk}) = (\mathrm{Superman}, \mathrm{Superman}, \mathrm{Superciuk}, \mathrm{Superciuk})\,.$$

Si osservi che

$$\partial_i(x_0, \dots, x_m) = \delta_i^*(x_0, \dots, x_m) = (x_0, \dots, \widehat{x_i}, \dots, x_m),$$

$$s_i(x_0, \dots, x_m) = \sigma_i^*(x_0, \dots, x_m) = (x_0, \dots, x_{i-1}, x_i, x_i, x_{i+1}, \dots, x_m).$$

Esempio 12.7. Per ogni intero $p \geq 0$ si definisce l'insieme simliciale $\Delta[p]$ ponendo

$$\Delta[p]_n = \{x\colon [n] \to [p] \text{ monotone }\}, \qquad n \geq 0,$$

$$x \in \Delta[p]_m, \quad f\colon [n] \to [m], \qquad f^*x = x \circ f\colon [n] \to [p]\,.$$

Esempio 12.8. Dati due insiemi simpliciali $X_\bullet$, $Y_\bullet$ la famiglia dei prodotti cartesiani $X_n \times Y_n$ possiede una naturale struttura simpliciale dove, per ogni $f\colon [n] \to [m]$ si definisce

$$f^*\colon X_m \times Y_m \to X_n \times Y_n, \qquad f^*(x, y) = (f^*x, f^*y)\,.$$

Il corrispondente insieme simpliciale viene detto il **prodotto** di $X_\bullet$, $Y_\bullet$ e si denota con il simbolo $X_\bullet \times Y_\bullet$.

Applicando le condizioni di controvarianza alle identità cosimpliciali otteniamo, per ogni insieme simpliciale le **identità simpliciali**:

$$\partial_j \partial_i = \partial_i \partial_{j+1} \quad \text{per ogni} \quad i \leq j;$$

$$s_j s_i = s_{i+1} s_j \quad \text{per ogni} \quad i \geq j;$$

$$\partial_j s_i = \begin{cases} s_i \partial_{j-1} & \text{per ogni } j > i+1 \\ \mathrm{Id} & \text{per } j = i, i+1 \\ s_{i-1} \partial_j & \text{per ogni } j < i\,. \end{cases} \tag{12.3}$$

Definizione 12.9. Un **morfismo di insiemi simpliciali** $\alpha\colon X_\bullet \to Y_\bullet$ è una successione di applicazioni $\alpha_n\colon X_n \to Y_n$ tali che per ogni $f\colon [n] \to [m]$ si ha $f^*\alpha_m = \alpha_n f^*$.

Ad esempio, ogni $\alpha\colon [n]\to[m]$ induce un morfismo di insiemi simpliciali

$$\alpha\colon \Delta[n]\to\Delta[m],\qquad \alpha_p(x)=\alpha\circ x,\quad x\colon [p]\to[n]\,.$$

Similmente ogni morfismo $\beta\colon K\to L$ di complessi simpliciali astratti induce un morfismo di insiemi simpliciali

$$\beta\colon K_\bullet\to L_\bullet,\qquad \beta_n(x_0,\ldots,x_n)=(\beta(x_0),\ldots,\beta(x_n))\,.$$

Ad esempio, dati due insiemi simpliciali $X_\bullet$ e $Y_\bullet$, le proiezioni naturali sui fattori

$$X_\bullet\times Y_\bullet\to X_\bullet,\qquad X_\bullet\times Y_\bullet\to Y_\bullet,$$

sono morfismi simpliciali.

13. Omologia degli insiemi simpliciali

Sia $X_\bullet$ insieme simpliciale fissato; per ogni n denotiamo con $C_n(X_\bullet)$ il gruppo abeliano libero generato da X_n. Per ogni $f\colon [n]\to[m]$, l'applicazione indotta $f^*\colon X_m\to X_n$ si estende per linearità ad un omomorfismo di gruppi $f^*\colon C_m(X_\bullet)\to C_n(X_\bullet)$. In particolare le facce e le degenerazioni inducono omomorfismi

$$\partial_i\colon C_n(X_\bullet)\to C_{n-1}(X_\bullet),\quad s_i\colon C_n(X_\bullet)\to C_{n+1}(X_\bullet),\qquad i=0,\ldots,n\,.$$

Lemma 13.1. *Nelle notazioni precedenti, gli omomorfismi*

$$\partial\colon C_n(X_\bullet)\to C_{n-1}(X_\bullet),\qquad \partial=\sum_{i=0}^n(-1)^i\partial_i,$$

$$s\colon C_n(X_\bullet)\to C_{n+1}(X_\bullet),\qquad s=\sum_{i=0}^n(-1)^i s_i,$$

soddisfano le seguenti identità:

$$\partial^2=0,\qquad s^2=0,\qquad \partial s+s\partial=0\,.$$

Dimostrazione. Sia $n\geq 0$ fissato e mostriamo le precedenti identità su $C_n(X_\bullet)$. Per quanto riguarda $\partial^2=0$ non è restrittivo supporre $n\geq 2$.

$$\partial^2=\sum_{j=0}^{n-1}\sum_{i=0}^n(-1)^{i+j}\partial_j\partial_i=\sum_{j=0}^{n-1}\sum_{i=0}^j(-1)^{i+j}\partial_j\partial_i+\sum_{j=0}^{n-1}\sum_{i=j+1}^n(-1)^{i+j}\partial_j\partial_i$$

Nella prima sommatoria usiamo le identità simpliciali e nella seconda scambiamo i con j

$$\partial^2=\sum_{j=0}^{n-1}\sum_{i=0}^j(-1)^{i+j}\partial_i\partial_{j+1}+\sum_{i=0}^{n-1}\sum_{j=i+1}^n(-1)^{i+j}\partial_i\partial_j$$

Nella prima sommatoria sostituiamo j con $j-1$ e nella seconda scambiamo i simboli di sommatoria

$$\partial^2=\sum_{j=1}^{n}\sum_{i=0}^{j-1}(-1)^{i+j-1}\partial_i\partial_j+\sum_{j=1}^{n}\sum_{i=0}^{j-1}(-1)^{i+j}\partial_i\partial_j=0.$$

Proviamo adesso che $s^2=0$.

$$s^2=\sum_{j=0}^{n+1}\sum_{i=0}^n(-1)^{i+j}s_js_i=\sum_{i=0}^{n}\sum_{j=0}^i(-1)^{i+j}s_js_i+\sum_{i=0}^{n}\sum_{j=i+1}^{n+1}(-1)^{i+j}s_js_i$$

Nella prima sommatoria usiamo le identità simpliciali e nella seconda scambiamo i con j

$$s^2=\sum_{i=0}^{n}\sum_{j=0}^i(-1)^{i+j}s_{i+1}s_j+\sum_{j=0}^{n}\sum_{i=j+1}^{n+1}(-1)^{i+j}s_is_j$$

Nella prima sommatoria sostituiamo i con $i-1$ e nella seconda scambiamo i simboli di sommatoria

$$s^2=\sum_{i=1}^{n+1}\sum_{j=0}^{i-1}(-1)^{i+j-1}s_is_j+\sum_{i=1}^{n+1}\sum_{j=0}^{i-1}(-1)^{i+j}s_is_j=0$$

Rimane da dimostrare che $\partial s = -s\partial$. Se $n = 0$ abbiamo $s\partial = 0$ e $\partial s = \partial_0 s_0 - \partial_1 s_0 = \mathrm{Id} - \mathrm{Id} = 0$ e quindi per l'uguaglianza $\partial s + s\partial = 0$ possiamo assumere $n \geq 1$.

$$\partial s = \sum_{j=0}^{n+1}\sum_{i=0}^{n}(-1)^{i+j}\partial_j s_i$$

Siccome $\partial_j s_i = \mathrm{Id}$ per $j = i, i+1$ possiamo scrivere

$$\partial s = \sum_{i=1}^{n}\sum_{j=0}^{i-1}(-1)^{i+j}\partial_j s_i + \sum_{i=0}^{n-1}\sum_{j=i+2}^{n+1}(-1)^{i+j}\partial_j s_i$$

E usando le identità simpliciali

$$\partial s = \sum_{i=1}^{n}\sum_{j=0}^{i-1}(-1)^{i+j} s_{i-1}\partial_j + \sum_{i=0}^{n-1}\sum_{j=i+2}^{n+1}(-1)^{i+j} s_i\partial_{j-1}$$

Scambiando i con $i+1$ nella prima e j con $j+1$ nella seconda si ottiene

$$\partial s = \sum_{i=0}^{n-1}\sum_{j=0}^{i}(-1)^{i+j+1} s_i\partial_j + \sum_{i=0}^{n-1}\sum_{j=i+1}^{n}(-1)^{i+j+1} s_i\partial_j$$

$$\partial s = -\sum_{i=0}^{n-1}\sum_{j=0}^{n}(-1)^{i+j} s_i\partial_j = -s\partial\,.$$

□

In particolare

$$C(X_\bullet): \qquad \cdots \xrightarrow{\partial} C_2(X_\bullet) \xrightarrow{\partial} C_1(X_\bullet) \xrightarrow{\partial} C_0(X_\bullet) \to 0$$

è un complesso di catene ed ha quindi senso considerare i gruppi di omologia $H_n(X_\bullet) = H_n(C(X_\bullet))$. Segue immediatamente dalla definizione che se $K_\bullet$ è l'insieme simpliciale dei simplessi orientati di un complesso simpliciale astratto K, allora $H_n(K) = H_n(K_\bullet)$ per ogni n.

Esempio 13.2. Siccome ogni elemento di $\Delta[n]_p$ può essere interpretato come una successione $(x_0, \ldots, x_p)$ con $0 \leq x_0 \leq x_1 \leq \cdots \leq x_p \leq n$ si ha che $C(\Delta[n]_\bullet)$ coincide con il complesso $C(\Delta^n, \leq)$ delle catene debolmente ordinate del complesso simpliciale astratto Δ^n e quindi $H_p(\Delta[n]_\bullet) = H_p(\Delta^n)$ per ogni p, ossia $H_0(\Delta[n]_\bullet) = \mathbb{Z}$ e $H_p(\Delta[n]_\bullet) = 0$ per ogni $p \neq 0$.

Sia $X_\bullet$ un insieme simpliciale; come nel caso dei complessi simpliciali astratti è possibile trovare dei sottocomplessi molto più piccoli di $C(X_\bullet)$ che calcolano la stessa omologia. A tal fine osserviamo che per ogni $0 \leq k \leq n$ l'operatore $\partial s_k \colon C_n(X_\bullet) \to C_n(X_\bullet)$ è uguale a

$$\begin{aligned}\partial s_k &= \sum_{i=0}^{n+1}(-1)^i\partial_i s_k = \sum_{i=0}^{k-1}(-1)^i\partial_i s_k + \sum_{i=k+2}^{n+1}(-1)^i\partial_i s_k \\ &= \sum_{i=0}^{k-1}(-1)^i s_{k-1}\partial_i + \sum_{i=k+2}^{n+1}(-1)^i s_k\partial_{i-1},\end{aligned} \tag{13.1}$$

e quindi se denotiamo con $D_n(X_\bullet) \subset C_n(X_\bullet)$ il sottogruppo abeliano libero generato dagli elementi del tipo $s_k x$, con $0 \leq k \leq n-1$ e $x \in X_{n-1}$, si ha $\partial(D_n(X_\bullet)) \subset D_{n-1}(X_\bullet)$ e quindi tali sottogruppi definiscono un sottocomplesso $D(X_\bullet) \subset C(X_\bullet)$, detto delle **catene degeneri** e che però non è quello che cerchiamo dato che:

Lemma 13.3. *Nelle notazioni precedenti il complesso $D(X_\bullet)$ è aciclico.*

Dimostrazione. La Formula (13.1) ci consente di definire una catena ascendente di sottocomplessi

$$0 = D^{-1} \subset D^0 \subset D^1 \subset \cdots\ D(X_\bullet),$$

dove D^k è il sottocomplesso generato da tutti gli elementi del tipo $s_k x$, con $0 \leq k \leq p$. Più precisamente, per ogni $n \geq 0$, $D_n^k \subset D_n(X_\bullet)$ è il sottogruppo abeliano libero generato dagli elementi del tipo $s_i x$, con $0 \leq i \leq \min(k, n-1)$ e $x \in X_{n-1}$. Siccome $D_n^k = D_n(X_\bullet)$ per

ogni $k \geq n-1$, per dimostrare che $D_n(X_\bullet)$ è aciclico basta dimostrare che per ogni $k \geq 0$ l'inclusione $D^{k-1} \subset D^k$ è un quasi-isomorfismo.

A tal fine considerando l'omotopia $h = (-1)^k s_k \colon D^k \to D^k[1]$; per un elemento del tipo $s_h x \in D_n^{k-1}$, $h < k$, si ha

$$(-1)^k h(s_h x) = s_k s_h x = s_h s_{k-1} x \in D_n^{k-1}\,.$$

Ponendo $\phi = \partial h + h\partial - \mathrm{Id}$, vogliamo dimostrare che per ogni generatore $s_h x \in D_n^k$, $n > 1$, $h \leq k$, $x \in X_{n-1}$, si ha $\phi(s_h x) \in D_n^{k-1}$. Se $h < k$ abbiamo già visto che $h(s_h x)$ appartiene al sottocomplesso D^{k-1} e a maggior ragione $\phi(s_h x) \in D^{k-1}$. Se $h = k$, usando la Formula (13.1) e le identità simpliciali si ha

$$\begin{aligned}
(-1)^k \phi(s_k x) &= \sum_{i=0}^{k-1} (-1)^i s_{k-1}\partial_i s_k x + \sum_{i=k+2}^{n+1} (-1)^i s_k \partial_{i-1} s_k x + \sum_{i=0}^{n} (-1)^i s_k \partial_i s_k x \; - (-1)^k s_k x \\
&= \sum_{i=0}^{k-1} (-1)^i s_{k-1}\partial_i s_k x - \sum_{i=k+1}^{n} (-1)^i s_k \partial_i s_k x + \sum_{i=0}^{n} (-1)^i s_k \partial_i s_k x \; - (-1)^k s_k x \\
&= \sum_{i=0}^{k-1} (-1)^i s_{k-1}\partial_i s_k x + \sum_{i=0}^{k} (-1)^i s_k \partial_i s_k x \; - (-1)^k s_k x \\
&= \sum_{i=0}^{k-1} (-1)^i s_{k-1}\partial_i s_k x + \sum_{i=0}^{k-1} (-1)^i s_k \partial_i s_k x \\
&= \sum_{i=0}^{k-1} (-1)^i s_{k-1}\partial_i s_k x + \sum_{i=0}^{k-1} (-1)^i s_k s_{k-1} \partial_i x \\
&= \sum_{i=0}^{k-1} (-1)^i s_{k-1}\partial_i s_k x + \sum_{i=0}^{k-1} (-1)^i s_{k-1} s_{k-1} \partial_i x \in D_n^{k-1}\,.
\end{aligned}$$

□

Sia $X_\bullet$ un insieme simpliciale, definiamo $N_0(X_\bullet) = C_0(X_\bullet)$ e per ogni $n > 0$

$$N_n(X_\bullet) = \{a \in C_n(X_\bullet) \mid \partial_i a = 0 \text{ per ogni } 0 < i \leq n\}.$$

Se $a \in N_n(X_\bullet)$ si ha $\partial a = \partial_0 a$ e per ogni $i \geq 0$ vale

$$\partial_i \partial a = \partial_i \partial_0 a = \partial_0 \partial_{i+1} a = 0,$$

e quindi $\partial a \in N_{n-1}(X_\bullet)$, ossia i sottogruppi $N_n(X_\bullet)$ definiscono un sottocomplesso $N(X_\bullet) \subset C(X_\bullet)$ detto **complesso di Moore** dell'insieme simpliciale.

Teorema 13.4. *Nella notazioni precedenti si ha $C(X_\bullet) = N(X_\bullet) \oplus D(X_\bullet)$ e l'inclusione di complessi di catene $N(X_\bullet) \subset C(X_\bullet)$ induce un isomorfismo in omologia.*

Dimostrazione. Dato che $D_0(X_\bullet) = 0$, $N_0(X_\bullet) = C_0(X_\bullet)$ basta provare che per ogni $n > 0$ si ha $C_n(X_\bullet) = N_n(X_\bullet) \oplus D_n(X_\bullet)$. Per provare che $N_n(X_\bullet) \cap D_n(X_\bullet) = 0$ supponiamo per assurdo che esista $0 \neq a \in N_n(X_\bullet) \cap D_n(X_\bullet)$ e sia $0 \leq p \leq n-1$ il più piccolo intero per cui è possibile scrivere $a = \sum_{i=0}^{p} s_i(a_i)$, con $a_i \in C_{n-1}(X_\bullet)$. Allora

$$0 = \partial_{p+1}(a) = \sum_{i=0}^{p-1} \partial_{p+1} s_i(a_i) + a_p = \sum_{i=0}^{p-1} s_i \partial_p(a_i) + a_p\,,$$

$$s_p(a_p) = -\sum_{i=0}^{p-1} s_p s_i \partial_p(a_i) = -\sum_{i=0}^{p-1} s_i s_{p-1} \partial_p(a_i),$$

da cui segue

$$y = \sum_{i=0}^{p-1} s_i(a_i - s_{p-1}\partial_p(a_i))\,,$$

in contraddizione con la definizione di p.

Per dimostrare che $C_n(X_\bullet) = N_n(X_\bullet) + D_n(X_\bullet)$ sia $a \in C_n(X_\bullet)$ e sia $-1 \leq p \leq n$ il più piccolo intero tale che $\partial_i a = 0$ per ogni $1 \leq i \leq n-p$. Se $p = -1$ allora $a \in N_n(X_\bullet)$. Se $p \geq 0$ consideriamo la catena $b = a - s_{n-p}\partial_{n-p}a$. Allora

$$\partial_{n-p}b = \partial_{n-p}a - \partial_{n-p}s_{n-p}\partial_{n-p}a = \partial_{n-p}a - \partial_{n-p}a = 0,$$

mentre se $1 \leq i < n-p$ si ha

$$\partial_i b = \partial_i a - \partial_i s_{n-p}\partial_{n-p}a = -s_{n-p-1}\partial_i\partial_{n-p}a = -s_{n-p-1}\partial_{n-p-1}\partial_i a = 0\,.$$

Per induzione su p si ha $b \in N_n(X_\bullet) + D_n(X_\bullet)$ e quindi

$$a = b + s_{n-p}\partial_{n-p}a \in N_n(X_\bullet) + D_n(X_\bullet)\,.$$

Per concludere, abbiamo dimostrato che il sottocomplesso $D(X_\bullet)$ delle catene degeneri è aciclico e quindi

$$H_n(C(X_\bullet)) = H_n(N(X_\bullet)) \oplus H_n(D(X_\bullet)) = H_n(N(X_\bullet))\,.$$

□

Osservazione 13.5. Per evitare un errore comune, se per ogni n definiamo $M_n \subset C_n(X_\bullet)$ come il sottogruppo abeliano libero generato dagli elementi di $X_n - \cup_i s_i(X_{n-1})$, è chiaro che $C_n(X_\bullet) = M_n \oplus D_n(X_\bullet)$ per ogni n, ma la successione degli M_n **non è** in generale un sottocomplesso. Consideriamo ad esempio l'insieme simpliciale $\Delta^1_\bullet$ dei simplessi orientati del complesso simpliciale astratto Δ^1. Allora $(0,1,0) \in M_2$ ma

$$\partial(0,1,0) = (1,0) - (0,0) + (0,1) = (1,0) - s_0(0) + (0,1) \notin M_1\,.$$

14. Omotopia simpliciale

Dato un morfismo di insiemi simpliciali $\alpha\colon X_\bullet \to Y_\bullet$, i morfismi $\alpha_n\colon X_n \to Y_n$ commutano con le facce ∂_i; lo stesso vale per le loro estensioni lineari $\alpha_n\colon C_n(X_\bullet) \to C_n(Y_\bullet)$ ed è quindi definito un morfismo di complessi di catene $\alpha\colon C(X_\bullet) \to C(Y_\bullet)$ che a sua volta induce omomorfismi in omologia.

Teorema 14.1. *Siano $X_\bullet$ un insieme simpliciale e $p \geq 0$ un intero fissato. Allora la proiezione*

$$X_\bullet \times \Delta[p]_\bullet \to X_\bullet$$

induce un isomorfismo in omologia.

Dimostrazione. Rappresentiamo gli elementi di $\Delta[p]_n$ come $n+1$-uple $(y_0, \ldots, y_n)$ tali che $0 \leq y_0 \leq \cdots \leq y_n \leq p$: la $n+1$-upla $(y_0, \ldots, y_n)$ corrisponde all'applicazione $[n] \to [p]$, $i \mapsto y_i$. Per ogni coppia di interi $n, k \geq 0$ definiamo

$$T^k_n = \{(y_0, \ldots, y_n) \in \Delta[p]_n \mid \text{ se } i \leq n-k \text{ allora } y_i = 0\},$$

osservando che T^0_n contiene solo l'elemento $(0, \ldots, 0)$, $T^k_n \subset T^{k+1}_n$, $T^k_n = \Delta[p]_n$ per ogni $k > n$ e $\partial_i T^k_n \subset T^k_{n-1}$ per ogni $n > 0$ ed ogni $0 \leq i \leq n$.

Definiamo T^k come l'unione dei T^k_n al variare di n e consideriamo l'applicazione

$$\tau\colon T^k \to T^k, \qquad \tau(y_0, \ldots, y_n) = (0, y_0, \ldots, y_n)\,.$$

Dato un qualunque elemento $y \in T^k_n$, sono di immediata verifica le relazioni:

(1) $\partial_0\tau(y) = y$;
(2) $\partial_{i+1}\tau(y) = y$ se $0 \leq i \leq n-k$;
(3) $\partial_{i+1}\tau(y) \in T^{k-1}_n$ se $i > n-k$ e $0 \leq i \leq n$;
(4) $\partial_{i+1}\tau(y) = \tau\partial_i(y)$ se $n > 0$ e $0 \leq i \leq n$.

Per ogni $k \geq 0$ consideriamo il sottocomplesso $C^k \subset C(X_\bullet \times \Delta[p]_\bullet)$ generato in grado n dagli elementi di $X_n \times T^k_n$. Siccome T^0_n contiene un solo elemento, il morfismo $C(X_\bullet \times \Delta[p]_\bullet) \to C(X_\bullet)$ indotto dalla proiezione stabilisce un isomorfismo $C^0 \simeq C(X_\bullet)$, quindi $H_n(C^0) = H_n(X_\bullet)$. D'altra parte $C^k_n = C_n(X_\bullet \times \Delta[p]_\bullet)$ per ogni $k > n$ e quindi $H_n(C^k) = H_n(X_\bullet \times \Delta[p]_\bullet)$ per ogni $k \geq n+2$.

Per dimostrare il teorema sarà quindi sufficiente provare che ogni inclusione $C^k \subset C^{k+1}$ è un quasi-isomorfismo. Per il Corollario 5.21 basta trovare, per ogni $k > 0$, un'omotopia $h\colon C^k \to C^k[1]$ tale che:

(1) $h(C^{k-1}) \subset C^{k-1}$;

(2) se $\phi = \partial h + h\partial - \mathrm{Id}$, allora $\phi(C^k) \subset C^{k-1}$.

Sia quindi $k > 0$ fissato e definiamo le applicazioni

$$h_n\colon C^k_n \to C^k_{n+1}, \qquad h_n(x,y) = \begin{cases} (-1)^{n-k+1}(s_{n-k+1}x, \tau y) & \text{se } n+1 \geq k, \\ 0 & \text{se } n+1 < k. \end{cases}$$

La condizione $h(C^{k-1}) \subset C^{k-1}$ è chiara; occupiamoci adesso di studiare, per ogni $n \geq 0$, l'immagine dell'operatore $\phi = \partial h + h\partial - \mathrm{Id}\colon C^k_n \to C^k_n$; trattiamo separatamente i tre casi $k > n+1$, $k = n+1$ e $k < n+1$.

1) Se $k > n+1$ allora $C^k_n = C^{k-1}_n$ e quindi l'immagine di ϕ è contenuta in C^{k-1}_n.

2) Se $k = n+1$ si ha $\phi = \partial h - \mathrm{Id}$ e per ogni $(x,y) \in X_n \times T^k_n$, siccome $\partial_0 s_0 = \mathrm{Id}$ si ha

$$\phi(x,y) = \sum_{i=0}^{n+1} (-1)^i (\partial_i s_0 x, \partial_i \tau y) - (x,y) = \sum_{i=1}^{n+1} (-1)^i (\partial_i s_0 x, \partial_i \tau y)$$

e ogni elemento nella sommatoria a destra appartiene a $T^{k-1}_n = T^n_n$. Quindi anche in questo caso l'immagine di ϕ è contenuta in C^{k-1}_n.

3) Se $k < n+1$ e $(x,y) \in X_n \times T^k_n$, usando le identità simpliciali e le uguaglianze $\partial_i \tau y = y$ per ogni $0 \leq i \leq n-k+1$, si ha:

$$\begin{aligned} \partial h(x,y) &= \sum_{i=0}^{n+1} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, \partial_i \tau y) \\ &= \sum_{i=0}^{n-k} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, y) + (x,y) + \sum_{i=n-k+2}^{n+1} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, \partial_i \tau y) \\ &= \sum_{i=0}^{n-k} (-1)^{n-k+1+i} (s_{n-k} \partial_i x, y) + (x,y) + \sum_{i=n-k+2}^{n+1} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, \partial_i \tau y)\,, \end{aligned}$$

$$h\partial(x,y) = \sum_{i=0}^{n-k} (-1)^{n-k+i} (s_{n-k} \partial_i x, y) + \sum_{i=n-k+1}^{n} (-1)^{n-k+i} (s_{n-k} \partial_i x, \tau \partial_i y)\,.$$

Dunque

$$\phi(x,y) = \sum_{i=n-k+2}^{n+1} (-1)^{n-k+1+i} (\partial_i s_{n-k+1} x, \partial_i \tau y) + \sum_{i=n-k+1}^{n} (-1)^{n-k+i} (s_{n-k} \partial_i x, \tau \partial_i y)$$

ed è chiaro che ogni addendo in ciascuna sommatoria appartiene a C^{k-1}_n. □

Per ogni insieme simpliciale $X_\bullet$ possiamo considerare i due morfismi di insiemi simpliciali

$$i_0, i_1\colon X_\bullet \to X_\bullet \times \Delta[1]_\bullet$$

$$i_0(x) = (x, (0,0,\dots,0)), \quad i_1(x) = (x, (1,1,\dots,1)).$$

La verifica che si tratta di morfismi di insiemi simpliciali è immediata in quanto per ogni $f\colon [n] \to [m]$ si ha

$$f^*(0,\dots,0) = (0,\dots,0), \qquad f^*(1,\dots,1) = (1,\dots,1)\,.$$

Corollario 14.2. *Nelle notazioni precedenti, per ogni insieme simpliciale $X_\bullet$ i due morfismi di insiemi simpliciali*

$$i_0, i_1 \colon X_\bullet \to X_\bullet \times \Delta[1]_\bullet :$$

inducono lo stesso isomorfismo in omologia

$$i_0 = i_1 \colon H_n(X_\bullet) \xrightarrow{\simeq} H_n(X_\bullet \times \Delta[1]_\bullet)\,.$$

Dimostrazione. Per il teorema precedente la proiezione $\pi \colon X_\bullet \times \Delta[1]_\bullet \to X_\bullet$ induce un isomorfismo in omologia e siccome $\pi i_0 = \pi i_1 = \mathrm{Id}$ si ha che

$$i_0, i_1 \colon H_n(X_\bullet) \to H_n(X_\bullet \times \Delta[1]_\bullet)$$

sono entrambi l'inverso dell'isomorfismo

$$\pi \colon H_n(X_\bullet \times \Delta[1]_\bullet) \xrightarrow{\simeq} H_n(X_\bullet)\,.$$

□

Definizione 14.3. Due morfismi di insiemi simpliciali $\alpha, \beta \colon X_\bullet \to Y_\bullet$ si dicono **omotopi** se esiste una successione finita di morfismi di insiemi simpliciali

$$\theta_i \colon X_\bullet \times \Delta[1]_\bullet \to Y_\bullet, \qquad i = 1, \dots, p$$

tali che

$$\alpha = \theta_1 i_0, \quad \theta_1 i_1 = \theta_2 i_0, \quad \dots, \quad \theta_{n-1} i_1 = \theta_n i_0, \quad \theta_n i_1 = \beta\,.$$

La definizione è analoga alla definizione di omotopia di applicazioni continue, dato che $\Delta[1]_\bullet$ è l'analogo simpliciale dell'intervallo $[0, 1]$; la necessità di prendere più morfismi : $X_\bullet \times \Delta[1]_\bullet \to Y_\bullet$ serve a garantire la proprietà transitiva dell'omotopia.

Corollario 14.4. *Due morfismi omotopi di insiemi simpliciali $\alpha, \beta \colon X_\bullet \to Y_\bullet$ inducono lo stesso morfismo in omologia.*

Dimostrazione. Siano $\theta_1, \dots, \theta_n$ come nella Definizione 14.3. Siccome i_0, i_1 inducono lo stesso morfismo in omologia, per ogni k pure i morfismi $\theta_k i_0$ e $\theta_k i_1$ inducono lo stesso morfismo in omologia. □

15. Brevi cenni di omologia singolare

Per ogni $n \geq 0$ consideriamo l'applicazione "base canonica" $e \colon [n] \to \mathbb{R}^{n+1}$:

$$e_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad e_1 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \qquad \cdots \qquad e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Definiamo poi il **simplesso topologico standard** di dimensione n, denotato $\Delta^n_{\mathbb{R}}$, come l'inviluppo convesso di $e([n])$:

$$\Delta^n_{\mathbb{R}} = \langle e([n]) \rangle = \left\{ \sum_{i=0}^n t_i e_i \mid t_i \geq 0,\ \sum t_i = 1 \right\} = \left\{ (t_0, \dots, t_n) \in \mathbb{R}^{n+1} \mid t_i \geq 0,\ \sum t_i = 1 \right\}$$

(per semplicità di scrittura intendiamo il vettore riga $(t_0, \dots, t_n)$ con lo stesso significato del corrispondente vettore colonna). Per ogni morfismo $f \colon [n] \to [m]$ abbiamo un diagramma commutativo

$$\begin{array}{ccc} [n] & \xrightarrow{f} & [m] \\ \downarrow{\scriptstyle e} & & \downarrow{\scriptstyle e} \\ \mathbb{R}^{n+1} & \xrightarrow{f_{\mathbb{R}}} & \mathbb{R}^{m+1} \end{array},$$

dove

$$f_{\mathbb{R}} \left(\sum_{i=0}^n t_i e_i \right) = \sum_{i=0}^n t_i e_{f(i)} \iff f_{\mathbb{R}}(t_0, \dots, t_n) = \left(\sum_{\{i \mid f(i)=0\}} t_i\,,\ \dots\ ,\ \sum_{\{i \mid f(i)=m\}} t_i \right).$$

In particolare:

$$(\delta_i)_{\mathbb{R}}(t_0,\dots,t_n) = (t_0,\dots,t_{i-1},0,t_i,\dots,t_n)\,,$$

$$(\sigma_i)_{\mathbb{R}}(t_0,\dots,t_n) = (t_0,\dots,t_{i-1},t_i+t_{i+1},t_{i+2},\dots,t_n)\,.$$

Sono evidenti sia la continuità di $f_{\mathbb{R}}$ sia le proprietà funtoriali della precedente costruzione, ossia $\mathrm{Id}_{\mathbb{R}} = \mathrm{Id}$ e $(fg)_{\mathbb{R}} = f_{\mathbb{R}}\, g_{\mathbb{R}}$. Per ogni applicazione faccia $\delta_i\colon [n] \to [n+1]$ si ha un omeomorfismo

$$(\delta_i)_{\mathbb{R}}\colon \Delta^n_{\mathbb{R}} \xrightarrow{\simeq} \{(t_0,\dots,t_{n+1}) \in \Delta^{n+1}_{\mathbb{R}} \mid t_i = 0\}\,.$$

Definizione 15.1. Un **n-simplesso singolare** di uno spazio topologico X è un'applicazione continua $\alpha\colon \Delta^n_{\mathbb{R}} \to X$. L'insieme degli n-simplessi singolari di X viene denotato $S_n(X)$.

Per ogni morfismo $f\colon [n] \to [m]$ possiamo definire

$$f^*\colon S_m(X) \to S_n(X), \qquad f^*\alpha = \alpha \circ f_{\mathbb{R}},$$

ed è immediato osservare che tutto ciò definisce un insieme simpliciale $S_\bullet(X)$.

Definizione 15.2. Il complesso $C(S_\bullet(X))$ viene detto complesso delle **catene singolari** di X ed i gruppi

$$H_n(X) \overset{\text{per definizione}}{=\!=} H_n(S_\bullet(X))$$

sono detti gruppi di **omologia singolare** dello spazio topologico X.

Lo studio dell'omologia singolare è uno degli argomenti principali dei corsi di topologia algebrica; in queste note ci limiteremo a dimostrare la loro invarianza omotopica ed a enunciare (senza dimostrazioni) alcuni teoremi fondamentali. Per approfondimenti e maggiori dettagli rimandiamo a [3, 4, 9, 10, 18].

Esempio 15.3. Se $X = \emptyset$, allora $S_n(X) = \emptyset$ per ogni $n \geq 0$ e quindi $H_n(\emptyset) = 0$ per ogni n.

Esempio 15.4. Se $X = *$ è formato da un solo punto, allora $S_n(X)$ contiene solo il simplesso singolare constante $c_n\colon \Delta^n_{\mathbb{R}} \to *$ e quindi $\partial_i c_n = c_{n-1}$ per ogni $n > 0$ $0 \leq i \leq n$. Per ogni $n > 0$ si ha

$$\partial c_n = \sum_{i=0}^{n} (-1)^i \partial_i c_n = \sum_{i=0}^{n} (-1)^i c_{n-1} = \begin{cases} c_{n-1} & \text{se } n \text{ pari},\\ 0 & \text{se } n \text{ dispari}. \end{cases}$$

Dunque il complesso delle catene singolari diventa

$$\cdots \to C_4 = \mathbb{Z} \xrightarrow{\mathrm{Id}} C_3 = \mathbb{Z} \xrightarrow{0} C_2 = \mathbb{Z} \xrightarrow{\mathrm{Id}} C_1 = \mathbb{Z} \xrightarrow{0} C_0 = \mathbb{Z} \to 0$$

che ha come omologia $H_0 = \mathbb{Z}$ e $H_n = 0$ per ogni $n > 0$.

Alternativamente, si può osservare che $S_\bullet(*)$ coincide con l'insieme simpliciale dei simplessi orientati di Δ^0, di cui abbiamo già calcolato l'omologia.

Alternativamente, siccome $\partial_n c_n \neq 0$ per ogni $n > 0$, il complesso di Moore $N(*)$ si annulla in tutti i gradi positivi.

Esempio 15.5. Sia X spazio topologico; per ogni cammino continuo $\alpha\colon [0,1] \to X$ consideriamo il simplesso singolare

$$\alpha'\colon \Delta^1_{\mathbb{R}} \to X, \qquad \alpha'(t_0,t_1) = \alpha(t_1)\,.$$

Se $\alpha\colon [0,1] \to X$ è un cammino chiuso, diciamo $\alpha(0) = \alpha(1) = x \in X$, allora il simplesso singolare α' è un ciclo in $C(S_\bullet(X))$: infatti

$$\partial\alpha' = \partial_0\alpha' - \partial_1\alpha' = \alpha'(\delta_0)_{\mathbb{R}} - \alpha'(\delta_1)_{\mathbb{R}} = \alpha'(0,1) - \alpha'(1,0) = \alpha(1) - \alpha(0) = x - x = 0\,.$$

Se $\alpha, \beta\colon [0,1] \to X$ sono due cammini chiusi omotopi, allora la differenza $\alpha' - \beta'$ è un bordo in $C(S_\bullet(X))$: sia $x = \alpha(0) = \alpha(1) = \beta(0) = \beta(1)$ il punto base dei due cammini chiusi α, β e denotiamo con $1_x\colon [0,1] \to X$ il cammino costante $1_x(t) = x$. Per ipotesi esiste un'omotopia di cammini $F\colon [0,1]^2 \to X$:

$$F(t,0) = \alpha(t), \quad F(t,1) = \beta(t), \quad F(0,s) = F(1,s) = x, \qquad s,t \in [0,1]\,.$$

Consideriamo adesso il cammino "diagonale" $\gamma\colon [0,1] \to X$, $\gamma(t) = F(t,t)$ ed i due simplessi singolari (vedi Figura 11)

$$\sigma, \tau\colon \Delta^2_{\mathbb{R}} \to X, \qquad \sigma(t_0,t_1,t_2) = F(t_1+t_2, t_2), \quad \tau(t_0,t_1,t_2) = F(t_2, t_1+t_2)\,,$$

le cui facce sono (ricordarsi che $t_0+t_1+t_2 = 1$):

$$\begin{aligned}
\partial_0\sigma(t_0,t_1) &= \sigma(0,t_0,t_1) = F(1,t_1) = 1_x(t_1) = 1'_x(t_0,t_1), \quad \Rightarrow \quad \partial_0\sigma = 1'_x\,,\\
\partial_1\sigma(t_0,t_1) &= \sigma(t_0,0,t_1) = F(t_1,t_1) = \gamma(t_1) = \gamma'(t_0,t_1), \quad \Rightarrow \quad \partial_1\sigma = \gamma'\,,\\
\partial_2\sigma(t_0,t_1) &= \sigma(t_0,t_1,0) = F(t_1,0) = \alpha(t_1) = \alpha'(t_0,t_1), \quad \Rightarrow \quad \partial_2\sigma = \alpha'\,,\\
\partial_0\tau(t_0,t_1) &= \tau(0,t_0,t_1) = F(t_1,1) = \beta(t_1) = \beta'(t_0,t_1), \quad \Rightarrow \quad \partial_0\tau = \beta'\,,\\
\partial_1\tau(t_0,t_1) &= \tau(t_0,0,t_1) = F(t_1,t_1) = \gamma(t_1) = \gamma'(t_0,t_1), \quad \Rightarrow \quad \partial_1\tau = \gamma'\,,\\
\partial_2\tau(t_0,t_1) &= \tau(t_0,t_1,0) = F(0,t_1) = 1_x(t_1) = 1'_x(t_0,t_1), \quad \Rightarrow \quad \partial_2\tau = 1'_x\,,
\end{aligned}$$

da cui segue

$$\partial(\sigma-\tau) = (\partial_0 - \partial_1 + \partial_2)(\sigma-\tau) = \alpha' - \beta'\,.$$

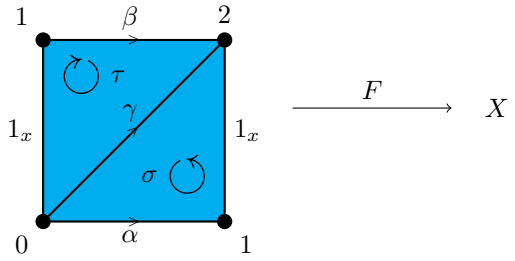


FIGURA 11. I cammini chiusi α e β sono omologhi.

La costruzione dei simplessi singolari commuta con i prodotti: infatti, per ogni coppia di spazi topologici X_1, X_2, dare un'applicazione continua $\alpha\colon \Delta^n_{\mathbb{R}} \to X_1 \times X_2$ è la stessa cosa che dare le due componenti $\alpha_i\colon \Delta^n_{\mathbb{R}} \to X_i$, $i = 1,2$. Ne segue che esiste un isomorfismo canonico

$$S_\bullet(X_1 \times X_2) = S_\bullet(X_1) \times S_\bullet(X_2)\,.$$

Ogni applicazione continua $\phi\colon X \to Y$ induce per composizione un morfismo di insiemi simpliciali $\phi_\bullet\colon S_\bullet(X) \to S_\bullet(Y)$:

$$\phi_n\colon S_n(X) \to S_n(Y), \qquad \phi_n\alpha = \phi \circ \alpha, \quad \alpha\colon \Delta^n_{\mathbb{R}} \to X\,.$$

Infatti, per ogni $f\colon [n] \to [m]$ ed ogni $\alpha \in S_m(X)$ si ha:

$$f^*(\phi_n\alpha) = (\phi_n\alpha) \circ f_{\mathbb{R}} = \phi \circ \alpha \circ f_{\mathbb{R}} = \phi \circ (f^*\alpha) = \phi_n(f^*\alpha)\,.$$

È chiaro che se ϕ è un omeomorfismo, allora $\phi_\bullet$ è un isomorfismo di insiemi simpliciali.

Di conseguenza ogni applicazione continua $\phi\colon X \to Y$ induce un morfismo di complessi di catene $\phi\colon C(S_\bullet(X)) \to C(S_\bullet(Y))$ e quindi dei morfismi tra gruppi di omologia singolare

$$\phi\colon H_n(X) \to H_n(Y)\,.$$

Esempio 15.6. Per ogni $p \geq 0$ è definito in maniera canonica un morfismo di insiemi simpliciali

$$(-)_{\mathbb{R}}\colon \Delta[p]_\bullet \to S_\bullet(\Delta^p_{\mathbb{R}}), \qquad f \mapsto f_{\mathbb{R}}\,.$$

Infatti, per ogni $\alpha \in \Delta[p]_m$ ed ogni $f\colon [n] \to [m]$ si ha

$$f^*(\alpha_{\mathbb{R}}) = \alpha_{\mathbb{R}} \circ f_{\mathbb{R}} = (\alpha \circ f)_{\mathbb{R}} = (f^*\alpha)_{\mathbb{R}}\,.$$

Per future applicazioni è utile esplicitare il morfismo di insiemi simpliciali $\psi_\bullet\colon \Delta[1]_\bullet \to S_\bullet([0,1])$ composizione di $(-)_{\mathbb{R}}\colon \Delta[1]_\bullet \to S_\bullet(\Delta^1_{\mathbb{R}})$ con l'isomofismo di insiemi simpliciali $\phi_\bullet\colon S_\bullet(\Delta^1_{\mathbb{R}}) \to S_\bullet([0,1])$ indotto dall'omeomorfismo

$$\phi\colon \Delta^1_{\mathbb{R}} \xrightarrow{\simeq} [0,1], \qquad \phi(t_0,t_1) = t_1 \quad (= 1-t_0)\,.$$

Dato un morfismo $f\colon [n]\to[1]$, si ha $f_{\mathbb{R}}(t_0,\dots,t_n)=\sum t_i e_{f(i)}$ e siccome $\phi(e_0)=0$, $\phi(e_1)=1$ si ottiene:

$$\psi_\bullet(f)(t_0,\dots,t_n)=\phi(f_{\mathbb{R}}(t_0,\dots,t_n))=\sum_{\{i|f(i)=1\}} t_i\,.$$

In particolare se f è costante, ossia se $f(i)=c$ per ogni i, allora $c=0$ oppure $c=1$ ed in entrambi i casi si ottiene $\psi_\bullet(f)(t_0,\dots,t_n)=c$ per ogni $(t_0,\dots,t_n)\in\Delta^n_{\mathbb{R}}$.

Lemma 15.7. *Per ogni spazio topologico X le due applicazioni continue*

$$j_0,j_1\colon X\to X\times[0,1],\qquad j_0(x)=(x,0),\quad j_1(x)=(x,1)\,,$$

inducono lo stesso morfismo in omologia singolare

$$j_0=j_1\colon H_*(X)\to H_*(X\times[0,1])\,.$$

(Nota: vedremo a posteriori che j_0,j_1 sono isomorfismi in omologia in quanto equivalenze omotopiche).

Dimostrazione. Nell'Esempio 15.6 abbiamo definito un morfismo di insiemi simpliciali $\psi\colon\Delta[1]_\bullet\to S_\bullet([0,1])$ tale che se $f\in\Delta[1]_\bullet$ è l'applicazione monotona costante $f\equiv c$ $(c=0,1)$, allora $\psi(f)$ è il simplesso singolare costante $\psi(f)\equiv c$. Definiamo il morfismo di insiemi simpliciali

$$H\colon S_\bullet(X)\times\Delta[1]_\bullet\to S_\bullet(X)\times S_\bullet([0,1])=S_\bullet(X\times[0,1]),\qquad H(x,y)=(x,\psi(y))\,.$$

Siano $i_0,i_1\colon S_\bullet(X)\to S_\bullet(X)\times\Delta[1]_\bullet$ i morfismi di insiemi simpliciali definiti nel Corollario 14.2. È chiaro dalle definizioni che per $a=0,1$ si ha

$$j_a=Hi_a\colon S_\bullet(X)\to S_\bullet(X)\times\Delta[1]_\bullet\to S_\bullet(X\times[0,1])$$

e siccome i_0,i_1 inducono lo stesso morfismo in omologia, a maggior ragione lo stesso vale per j_0,j_1. □

Ricordiamo che due applicazioni continue $f,g\colon X\to Y$ si dicono omotope se esiste un'applicazione continua $F\colon X\times[0,1]\to Y$ tale che $f=Fj_0$ e $g=Fj_1$, ossia

$$F(x,0)=f(x),\qquad F(x,1)=g(x),\qquad\text{per ogni}\quad x\in X\,.$$

Teorema 15.8. *Due applicazioni continue omotope $f,g\colon X\to Y$ inducono gli stessi morfismi in omologia $f=g\colon H_n(X)\to H_n(Y)$.*

Dimostrazione. Sia $F\colon X\times[0,1]\to Y$ continua tale che $f=Fj_0$ e $g=Fj_1$. Siccome le due immersioni $j_0,j_1\colon X\to X\times[0,1]$ inducono gli stessi morfismi in omologia, a maggior ragione lo stesso vale per le composizioni Fj_0 e Fj_1. □

In particolare se $f\colon X\to X$ è omotopa all'identità, allora f induce i morfismi identici in omologia.

Ricordiamo che un'applicazione continua $f\colon X\to Y$ si dice un'equivalenza omotopica se esiste $g\colon Y\to X$ continua e tale che entrambe le composizioni gf e fg sono omotope all'identità, su X e Y rispettivamente.

Corollario 15.9. *Ogni equivalenza omotopica induce isomorfismi in omologia.*

Dimostrazione. Siano $f\colon X\to Y$ e $g\colon Y\to X$ continue con entrambe le composizioni gf e fg omotope all'identità. Allora entrambe le composizioni

$$H_n(X)\xrightarrow{f}H_n(Y)\xrightarrow{g}H_n(X),\qquad H_n(Y)\xrightarrow{g}H_n(X)\xrightarrow{f}H_n(Y),$$

sono le applicazioni identiche e quindi g è l'inversa di f in omologia. □

In particolare tutti gli spazi topologici contraibili (ad esempio i sottoinsiemi convessi di $\mathbb{R}^n$) hanno la stessa omologia del punto.

Enunciamo adesso senza dimostrazione alcuni teoremi riguardanti l'omologia singolare.

Teorema 15.10. *Per ogni spazio topologico X il gruppo $H_0(X)$ è il gruppo abeliano libero generato da $\pi_0(X)$, l'insieme delle componenti connesse per archi di X.*

Teorema 15.11 (Omologia delle sfere)**.** *Sia $S^n = \{x \in \mathbb{R}^{n+1} \mid \|x\| = 1\}$ la sfera di dimensione n. Per ogni $n > 0$ si ha:*

$$H_0(S^n) = H_n(S^n) = \mathbb{Z}, \qquad H_i(S^n) = 0 \text{ per ogni } i \neq 0, n\,.$$

In particolare S^n è omotopicamente equivalente a S^m se e solo se $n = m$. Più in generale, se $X = S^{n_1} \times \cdots \times S^{n_k}$ è un prodotto di sfere, con $n_i > 0$ per ogni i, allora per ogni m il gruppo $H_m(X)$ è abeliano libero di rango uguale al numero di sottoinsiemi $A \subset \{1, \ldots, k\}$ tali che $m = \sum_{i \in A} n_i$.

Ad esempio, se $n_i = 1$ per ogni i, ossia $X = (S^1)^k$, allora il gruppo $H_m(X)$ è abeliano libero di rango $\binom{k}{m}$.

Teorema 15.12. *Per ogni spazio topologico connesso per archi X si ha*

$$H_1(X) \cong \frac{\pi_1(X)}{[\pi_1(X), \pi_1(X)]},$$

dove per ogni gruppo G si denota con $[G, G]$ il sottogruppo dei commutatori, definito come il sottogruppo generato da tutti gli elementi del tipo $aba^{-1}b^{-1}$, al variare di $a, b \in G$.

Lasciamo per esercizio la semplice dimostrazione che $[G, G]$ è un sottogruppo normale di G.

Teorema 15.13. *Se X è una varietà differenziabile compatta, i gruppi di omologia $H_i(X)$ sono finitamente generati.*

Teorema 15.14. *Sia $|K| \subset \mathbb{R}^n$ la realizzazione geometrica di un complesso simpliciale astratto K. Allora $H_n(|K|) = H_n(K)$ per ogni n.*

Teorema 15.15 (Successione esatta di Mayer-Vietoris)**.** *Siano $U, V \subset X$ due aperti tali che $X = U \cup V$. Allora esiste una successione esatta lunga*

$$\cdots \to H_n(U \cap V) \to H_n(U) \oplus H_n(V) \to H_n(X) \to H_{n-1}(U \cap V) \to \cdots \to H_0(X) \to 0\,.$$

Se l'inclusione $U \cap V \subseteq V$ induce un isomomorfismo in omologia, allora anche l'inclusione $U \subseteq X$ induce un isomorfismo in omologia.

16. Omologia con coefficienti

Sia $X_\bullet$ un insieme simpliciale. Abbiamo definito il gruppo delle p-catene $C_p(X_\bullet)$ come il gruppo abeliano libero generato da X_p. Dato che i gruppi abeliani liberi sono anche detti $\mathbb{Z}$-moduli liberi, spesso si usa la notazione $H_n(X_\bullet, \mathbb{Z})$ per indicare $H_n(X_\bullet)$. La stessa notazione si applica sia ai complessi simpliciali astratti, sia agli spazi topologici.

La stessa identica costruzione si può fare considerando un qualsiasi campo $\mathbb{K}$ e definire $C_p(X_\bullet, \mathbb{K})$ come lo spazio vettoriale su $\mathbb{K}$ generato da X_p. Tutta la teoria generale si comporta allo stesso modo (con spazi vettoriali al posto di gruppi abeliani ed applicazioni lineari al posto degli omomorfismi) ed otteniamo un complesso di catene $C(X_\bullet, \mathbb{K})$ i cui spazi vettoriali di omologia sono denotati $H_n(X_\bullet, \mathbb{K})$. Lo stesso si può fare per complessi simpliciali astratti e spazi topologici.

In linea teorica, lo studio dei gruppi $H_n(X, \mathbb{K})$ non ci fornisce alcuna ulteriore informazione su X dato che per un teorema generale di algebra omologica (lo studio dei complessi di catene) detto **teorema dei coefficienti universali**, i gruppi $H_n(X, \mathbb{Z}) = H_n(X)$ determinano univocamente i gruppi $H_n(X, \mathbb{K})$. Ad esempio è abbastanza facile dimostrare che se $\mathbb{K}$ è un campo di caratteristica 0, allora $H_n(X, \mathbb{K})$ è uno spazio vettoriale di dimensione uguale al rango di $H_n(X, \mathbb{Z})$. Se la caratteristica del campo è positiva allora la dimensione è maggiore od uguale al rango e la differenza dipende (in maniera ben definita ma di lunga e laboriosa descrizione) dal sottogruppo di torsione di $H_{n-1}(X, \mathbb{Z})$.

Tuttavia, lo studio dei gruppi di omologia con coefficienti è importante per almeno tre ordini di motivi:

(1) i gruppi $H_n(X, \mathbb{K})$ sono generalmente più semplici da calcolare rispetto ai gruppi $H_n(X)$. Ad esempio in *topologia computazionale*, dove si ha a che fare con complessi simpliciali astratti K con moltissimi vertici, il calcolo di $H_n(K, \mathbb{Z}/(2))$ richiede una potenza computazionale molto minore di quella necessaria per determinare $H_n(K, \mathbb{Z})$.

(2) alcuni teoremi generali forniscono strumenti per calcolare i gruppi $H_n(X, \mathbb{K})$ per opportuni campi $\mathbb{K}$ ma non i gruppi $H_n(X, \mathbb{Z})$. Ad esempio, per X varietà differenziabile, il *teorema di de Rham* fornisce una ricetta per il calcolo degli spazi vettoriali duali di $H_n(X, \mathbb{R})$ in termini di forme differenziali su X.

(3) i gruppi $H_n(X, \mathbb{K})$ intervengono naturalmente in svariate teorie matematiche. Ad esempio:
   (a) con $\mathbb{K} = \mathbb{Z}/(2)$ in *omologia persistente* e nella teoria delle *classi caratteristiche*;
   (b) con $\mathbb{K} = \mathbb{Q}$ in *omotopia razionale* e *teoria di Hodge*;
   (c) con $\mathbb{K} = \mathbb{R}, \mathbb{C}$ in *geometria algebrica* e *teoria di de Rham*.

17. L'incredibile ubiquità della topologia persistente

Riportiamo in questa breve sezione un estratto dall'articolo di Massimo Ferri (Università di Bologna) pubblicato su Maddmaths il 12 agosto 2015 e recuperabile per intero al sito *maddmaths.simai.eu/divulgazione/focus/lincredibile-ubiquita-della-topologia-persistente/*.

C'è una branca della matematica chiamata "Topologia persistente" che ha applicazioni spesso sorprendenti all'analisi della forma e ai problemi di classificazione e recupero dei dati. Cerchiamo di capire meglio di cosa si tratta.

La geometria offre ottimi strumenti alla visione artificiale e alla pattern recognition. I problemi di classificazione, riconoscimento, ricerca di difetti, recupero in database estesi si risolvono talvolta trovando una trasformazione (euclidea, affine o proiettiva) che sovrapponga un'immagine a un'altra; qui l'algebra matriciale risulta vincente. Soprattutto, però, questi problemi si affrontano associando ad ogni immagine una stringa di misure geometriche (descrittori di forma) compiute su di essa ed eseguendo classificazione, riconoscimento, ecc. sulle stringhe invece che sulle immagini. Questa prassi funziona benissimo su pezzi meccanici, veicoli, oggetti rigidi: per esempio Google riconosce un monumento anche se fotografato da un'angolazione insolita. Però le cose cambiano con immagini di origine naturale; la rigidità della geometria diventa un ostacolo: riconoscere la somiglianza fra un uomo seduto e uno in piedi è problematico.

È qui che la topologia, molto più "libera" della geometria, sembra essere la carta giusta da giocare. Invece che dalla sovrapponibilità mediante trasformazioni geometriche, l'equivalenza fra due spazi topologici X, Y è data dall'eventuale esistenza di un omeomorfismo $\varphi\colon X \to Y$, cioè una funzione continua con inversa continua. L'uomo seduto e l'uomo in piedi sono omeomorfi, cioè esiste fra loro un omeomorfismo, ma non una trasformazione geometrica. Allora basta sostituire la geometria con la topologia, l'algebra matriciale con l'omeomorfismo? Purtroppo ci sono due problemi.

In genere è difficile capire se due spazi sono omeomorfi o no. Allora interviene la topologia algebrica, che associa a uno spazio degli enti (invarianti) che risultano uguali per spazi omeomorfi. Perciò se due spazi X, Y hanno invarianti diversi sono sicuramente non omeomorfi (purtroppo il viceversa non vale).

Invarianti di questo tipo sono i numeri di Betti: $b_0(X)$ è il numero di componenti connesse (o 0-cicli), in pratica il numero di pezzi separati da cui è composto X; $b_1(X)$ conta i buchi fatti "a circonferenza" di X; 1-cicli; come quello di una ciambella; $b_2(X)$ conta i vuoti bidimensionali di X (come quelli di un pallone o di una camera d'aria; 2-cicli) e così via. Per capire davvero il significato di questi concetti occorrono definizioni formali; non sono male l'articolo di Wikipedia *Betti number* e il più generale *Omologia*.

C'è un secondo problema: la geometria è troppo rigida, ma la topologia è troppo libera. La battuta "per un topologo una tazza con manico e una ciambella sono la stessa cosa" è fondata: i due oggetti sono omeomorfi; i numeri di Betti naturalmente coincidono: $b_0 = 1$, $b_1 = 1$, $b_2 = 0$ eccetera per entrambi.

L'idea base della topologia persistente è di associare il concetto di forma non solo a uno spazio topologico X, ma ad una coppia (X, f) dove f una funzione continua (che chiameremo *funzione filtrante*) definita su X, a valori solitamente nei numeri reali. A questo punto la topologia algebrica (in particolare il suo settore omologia, di cui fanno parte i numeri di Betti) viene applicata ad ogni insieme di sottolivello $X(u)$, costituito dai punti $x \in X$ per cui $f(x) \leq u$. Per esempio possiamo appoggiare una tazza X e una ciambella Y di eguale altezza sul tavolo, e usare come funzione f la quota, ossia la distanza dal pavimento. Entrambi gli oggetti hanno quota minima a e massima c. Se $a - \epsilon$ è un numero appena sotto ad a, allora $X(a-\epsilon) = Y(a-\epsilon) = \emptyset$; invece $X(c) = X$, $Y(c) = Y$. Se applichiamo l'omologia agli insiemi di sottolivello intermedi, ecco che possiamo distinguere tazza e ciambella! In realtà la teoria è più complicata (e più informativa) e si avvale di suoi specifici descrittori di forma: numeri di Betti persistenti, diagrammi di persistenza, barcode.

18. Complessi filtrati

In queste note ci occuperemo solamente della parte "algebro-geometrica" dell'omologia persistente. Con riferimento alla Figura 12, studieremo nelle prossime sezioni con sufficiente dettaglio i passaggi (b) e (c), mentre studieremo in questa sezione il passaggio (a) in alcuni casi molto particolari. Per quanto riguarda l'interpretazione, che richiede strumenti di natura analitica e statistica, rimandiamo alla letteratura sull'argomento: un buon punto di partenza è dato dagli articoli [2, 6, 7, 19].

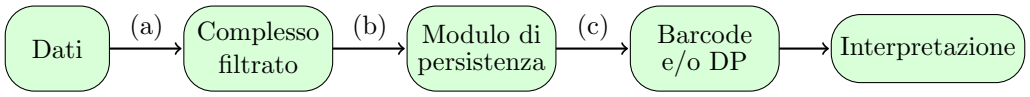


Figura 12. La catena di montaggio dell'omologia persistente.

Introduciamo l'analogo di funzione filtrante per i complessi simpliciali astratti.

Definizione 18.1. Sia K un complesso simpliciale astratto. Una **funzione filtrante** su K è un'applicazione $f\colon K \to \mathbb{R}$ limitata inferiormente e tale che se $s \in K$ e $r \subset s$ allora $f(r) \leq f(s)$.

Equivalentemente, un'applicazione $f\colon K \to \mathbb{R}$ è una funzione filtrante se per ogni $t \in \mathbb{R}$ il sottoinsieme **di livello**

$$K(t) = \{s \in K \mid f(s) \leq t\} = f^{-1}(]-\infty, t])$$

è un sottocomplesso simpliciale, che risulta vuoto per t tendente a $-\infty$.

Per semplicità notazionale, quando non ci saranno rischi di ambiguità, chiameremo semplicemente **complesso filtrato** una coppia (K, f) con K complesso simpliciale astratto e $f\colon K \to \mathbb{R}$ funzione filtrante.

Esempio 18.2. Dato un complesso simpliciale astratto (K, I), ogni applicazione $f\colon I \to [0, +\infty[$ si estende ad una funzione filtrante

$$f\colon K \to [0, +\infty[, \qquad f(\{x_0, \ldots, x_p\}) = \max_i f(x_i)\,.$$

Esempio 18.3. Dato un complesso simpliciale astratto (K, I) ed una applicazione $d\colon I \times I \to \mathbb{R}$ tale che $d(x, y) = d(y, x) \geq 0$ per ogni $x, y \in I$, possiamo definire una funzione filtrante

$$f\colon K \to [0, +\infty[, \qquad f(\{x_0, \ldots, x_p\}) = \max_{i,j} d(x_i, x_j)\,.$$

Esempio 18.4. Sia K un complesso simpliciale astratto e sia $K(0) \subset K(1) \subset K(2) \subset \cdots$ una catena ascendente di sottocomplessi simpliciali tali che $\cup_n K(n) = K$. Allora la funzione

$$f\colon K \to [0, +\infty[, \qquad f(x) = \min\{n \mid x \in K(n)\}$$

è una funzione filtrante tale che $K(n) = \{x \in K \mid f(x) \leq n\}$.

Dato un complesso filtrato (K,f), l'immagine $f(K)\subset\mathbb{R}$ viene detto **luogo dei valori critici** di f. Segue dalla definizione dei sottocomplessi di livello che un numero reale t è un valore critico se e solo se $K(s)\neq K(t)$ per ogni $s<t$.

Diremo che un complesso filtrato (K,f) è di **tipo finito** se K è un complesso simpliciale astratto finito. In particolare ogni complesso filtrato di tipo finito possiede un numero finito di valori critici.

Diremo che un complesso filtrato (K,f) è **localmente di tipo finito** se $K(t)$ è un sottocomplesso finito per ogni $t\in\mathbb{R}$. In tal caso per ogni $t\in\mathbb{R}$ i valori critici $\leq t$ coincidono con i valori critici della restrizione $f\colon K(t)\to\mathbb{R}$ e questo implica che il luogo dei valori critici è chiuso e discreto (ossia ogni intervallo limitato contiene un numero finito di punti critici).

I prossimi esempi descrivono alcuni casi del passaggio (a) di Figura 12.

Esempio 18.5. Si consideri un ben definito insieme I di matematici, ad esempio l'insieme dei docenti afferenti al Dipartimento di Matematica Guido Castelnuovo il 4 novembre 2019. Il complesso simpliciale astratto (K,I) delle collaborazioni scientifiche di I è definito dalla regola che un elemento $\{x_0,\dots,x_p\}\in\Delta^I$ appartiene a K se e solo se esiste (almeno) una pubblicazione in cui tra gli autori figurano $x_0,\dots,x_p$.

La funzione filtrante temporale $f\colon K\to\mathbb{R}$ è definita ponendo $f(s)$ come l'anno della prima pubblicazione avente s come sottoinsieme di autori.

Esempio 18.6 (Cf. [16])**.** Si consideri l'insieme I dei personaggi di un film e per ogni coppia $(x,y)\in I\times I$ sia $d(x,y)$ il numero di scene (o se preferite il numero fotogrammi) in cui x,y compaiono simultaneamente. Si consideri adesso il complesso di cricche (K,I), dove $\{x_0,\dots,x_p\}\in K$ se e solo se $d(x_i,x_j)>0$ per ogni i,j.

Una possibile funzione filtrante $f\colon K\to\mathbb{R}$ sensata in tale situazione è data da

$$f(\{x_0,\dots,x_p\})=\max_{i,j}\frac{1}{d(x_i,x_j)}\,.$$

Costruzioni analoghe hanno senso quando I è l'insieme dei cellulari agganciati ad un insieme di antenne in corrispondenza di un attentato terroristico e $d(x,y)$ il numero di telefonate/messaggini intercorsi tra x e y.

Esempio 18.7. Consideriamo un sottoinsieme finito e non vuoto $I\subset\mathbb{R}^n$ come dato iniziale. Allora i complessi di Vietoris-Rips, Čech ed Alpha possono essere descritti come sottocomplessi di livello per delle opportune funzioni filtranti, che denoteremo rispettivamente v,c,α.

1) Il caso più semplice è dato dai complessi di Vietoris-Rips. Sia $K=\Delta^I$ e si consideri la funzione filtrante

$$v\colon K\to[0,+\infty[,\qquad v(\{x_0,\dots,x_p\})=\frac{1}{2}\max_{i,j}\|x_i-x_j\|\,.$$

È chiaro per definizione che $K(t)=V(t)$ per ogni t.

2) Nel caso Čech si prende $K=\Delta^I$ assieme alla funzione filtrante

$$c\colon K\to[0,+\infty[,\qquad c(\{x_0,\dots,x_p\})=\min\{r\in\mathbb{R}\mid U_{x_0}(r)\cap\cdots\cap U_{x_p}(r)\neq\emptyset\},$$

ed è chiaro per definizione che $K(t)=C(t)$ per ogni t. Il fatto che c sia ben definita richiede un semplice ragionamento topologico: sia $\{x_0,\dots,x_p\}\in K$ fissato e scegliamo un numero reale $R>0$ sufficientemente grande e tale che $U_{x_0}(R)\cap\cdots\cap U_{x_p}(R)\neq\emptyset$. Adesso consideriamo il sottoinsieme chiuso e limitato (quindi compatto):

$$Z=\{(y,r)\in U_{x_0}(R)\times[0,R]\ \mid\|y-x_i\|\leq r,\ \forall i\}\,.$$

Per le ipotesi su R l'insieme Z è non vuoto ed esiste quindi

$$c(\{x_0,\dots,x_p\})=\min_{(y,r)\in Z}r\,.$$

3) Nel caso dei complessi Alpha si prende $K=D_I$ (complesso di Delaunay). Per definizione di D_I, dato un p-simplesso $s=\{x_0,\dots,x_p\}\in K$ il sottoinsieme

$$Z=\{(y,r)\in U_R(x_0)\times[0,R]\mid\|x_0-y\|=r\text{ per ogni }i\}$$

è un chiuso non vuoto per R sufficientemente grande (dipendente da s), e quindi e basta prendere come funzione filtrante

$$\alpha(s) = \min_{(y,r)\in Z} r\,.$$

In conclusione, ad ogni sottoinsieme finito e non vuoto $I \subset \mathbb{R}^n$ abbiamo associato tre diversi complessi filtrati: (Δ^I, v), (Δ^I, c) e (D_I, α), nell'ordine dal più semplice (ma meno informativo) al più complesso (ma anche con più informazioni).

19. Moduli di persistenza

Secondo alcuni la persistenza è "semplice, naturale ed intuitiva". Tuttavia per poterla raccontare correttamente e in modo monosemantico è necessario sviluppare un apposito linguaggio.

Definizione 19.1. Un **modulo di persistenza** è una successione di omomorfismi di gruppi abeliani

$$0 \to P(t_0) \xrightarrow{p_0} P(t_1) \xrightarrow{p_1} P(t_2) \xrightarrow{p_2} \cdots\,, \tag{19.1}$$

parametrizzati da una successione strettamente crescente di numeri reali $t_i \in \mathbb{R}$, $t_i < t_{i+1}$.

Attenzione: non si richiede che un modulo di persistenza sia un complesso, ossia le composizioni $p_s\, p_{s-1}$ possono anche essere $\neq 0$.

Dal punto di vista astratto non è restrittivo supporre $t_i = i \in \mathbb{N}$, tuttavia in previsione delle applicazioni alla cosiddetta *topologia computazionale* è opportuno considerare le etichette come numeri reali.

Esempio 19.2. Siano V uno spazio vettoriale ed $f\colon V \to V$ un endomorfismo nilpotente, diciamo $f^n = 0$ per qualche $n > 0$. Se poniamo $V(0) = V$ e $V(i) = f^i(V)$ per ogni $i > 0$, si ha un modulo di persistenza

$$0 \to V(0) \xrightarrow{f} V(1) \xrightarrow{f} V(2) \xrightarrow{f} \cdots \xrightarrow{f} V(n) = 0\,, \tag{19.2}$$

con le applicazioni $p_s = f$ surgettive per $s \geq 0$.

Esempio 19.3 (Freccia (b) della Figura 12)**.** Sia (K, f) un complesso filtrato localmente di tipo finito e sia $t_0 < t_1 < \cdots$ la successione dei suoi valori critici in ordine crescente (abbiamo già dimostrato che ogni intervallo limitato contiene un numero finito di valori critici). Per ogni $n \geq 0$ fissato, gli n-esimi gruppi di omologia della catena ascendente dei sottocomplessi di livello $K(t_0) \subset K(t_1) \subset \cdots$ determinano un diagramma di persistenza

$$0 \to H_n(K(t_0)) \xrightarrow{p_0} H_n(K(t_1)) \xrightarrow{p_1} H_n(K(t_2)) \xrightarrow{p_2} \cdots\,, \tag{19.3}$$

dove p_s è il morfismo indotto in omologia dall'inclusione $K(t_s) \subset K(t_{s+1})$. Osserviamo inoltre che, essendo per ipotesi $K(t)$ un complesso simpliciale astratto finito per ogni t, i gruppi di omologia $H_n(K(t_i))$ sono finitamente generati.

Il precedente esempio serve anche a motivare la seguente definizione:

Definizione 19.4. Un modulo di persistenza come in (19.1) si dice di **tipo finito**, o anche **tame**, se la successione dei t_i è finita e se ciascun gruppo $P(t_i)$ è finitamente generato. Si dice invece **localmente di tipo finito** se ogni $P(t_i)$ è finitamente generato e se ogni intervallo limitato di $\mathbb{R}$ contiene al più un numero finito di elementi t_i della successione.

Definizione 19.5. Dato un modulo di persistenza come in (19.1), diremo che un elemento $x \in P(t_i)$ è **primordiale** se non appartiene all'immagine di p_{i-1} (si intende che l'immagine di p_{-1} è nulla).

In particolare gli elementi primordiali non sono mai nulli. Per ogni $i \leq j$ denotiamo con $p_{i,j}\colon P(t_i) \to P(t_j)$ la composizione di $p_i, p_{i+1}, \ldots, p_{j-1}$: si ha $p_{i,i} = \mathrm{Id}$, $p_{i,i+1} = p_i$ eccetera.

Se $x \in P(t_i)$ è primordiale, diremo anche che x nasce, oppure che **è creato**, in t_i.

Definizione 19.6. Diremo che un elemento primordiale $x \in P(t_i)$ **muore**, od anche che viene distrutto, in t_j se:

$$j > i, \qquad p_{i,j}(x) = 0, \qquad p_{i,j-1}(x) \neq 0\,.$$

In tal caso chiameremo $[t_i, t_j[\subset \mathbb{R}$ l'**intervallo di vita** di x. Se x è immortale il suo intervallo di vita è $[t_i, +\infty[$.

È chiaro dalle definizioni che un elemento può nascere e morire solo su dei valori critici, pertanto gli estremi degli intervalli di vita sono sempre dei valori critici.

Dato il modulo di persistenza (19.1), per ogni coppia di interi non negativi $i \leq j$ definiamo

$$P^{i,j} = \frac{P(t_i)}{\ker(p_{i,j})}\,.$$

Dunque ciascun morfismo $p_{i,j}$ si fattorizza come composizione di un morfismo surgettivo $P(t_i) \to P^{i,j}$ ed un morfismo iniettivo $P^{i,j} \to P(t_j)$. Informalmente, il gruppo $P^{i,j}$ rappresenta gli elementi di $P(t_i)$ che sono ancora vivi in t_j. Osserviamo inoltre che:

(1) se $i \leq j \leq k$ allora $\ker(p_{i,j}) \subseteq \ker(p_{i,k})$ ed è quindi definito un morfismo *surgettivo* $P^{i,j} \to P^{i,k}$;
(2) se $i \leq h \leq j$, siccome $p_{i,j} = p_{h,j} \circ p_{i,h}$, per un elemento $x \in P(t_i)$ si ha

$$x \in \ker(p_{i,j}) \iff p_{i,h}(x) \in \ker(p_{h,j})$$

e quindi $p_{i,h}\colon P(t_i) \to P(t_h)$ si fattorizza ad un morfismo *iniettivo* $\overline{p_{i,h}}\colon P^{i,j} \to P^{h,j}$.

Dunque, per ogni quaterna $i \leq h \leq k \leq j$ di numeri naturali si ha un quadrato commutativo

$$\begin{array}{ccc} P^{i,k} & \longrightarrow & P^{h,k} \\ \downarrow & & \downarrow \\ P^{i,j} & \longrightarrow & P^{h,j} \end{array} \tag{19.4}$$

con le frecce orizzontali iniettive e le frecce verticali surgettive.

In particolare, per ogni $i < j$ si ha un diagramma commutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P^{i-1,j-1} & \xrightarrow{\sigma_{i,j}} & P^{i,j-1} & \longrightarrow & \operatorname{coker}(\sigma_{i,j}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \gamma_{i,j}} & & \\ 0 & \longrightarrow & P^{i-1,j} & \xrightarrow{\tau_{i,j}} & P^{i,j} & \longrightarrow & \operatorname{coker}(\tau_{i,j}) & \longrightarrow & 0 \end{array}$$

con le righe esatte e le frecce verticali surgettive. Informalmente, il conucleo di $\sigma_{i,j}$ (rispettivamente: di $\tau_{i,j}$) rappresenta le classi primordiali di $P(t_i)$ che sono ancora vive in $P(t_{j-1})$ (rispettivamente: di $P(t_j)$). Da ciò segue che il nucleo di $\gamma_{i,j}$ è il gruppo che rappresenta le classi primordiali di $P(t_i)$ che muoiono in $P(t_j)$.

Se il modulo di persistenza è localmente di tipo finito, per ipotesi i gruppi $P(t_i)$ sono tutti finitamente generati, e quindi lo sono anche i gruppi $P^{i,j}$: ed i loro ranghi

$$\beta^{i,j} = \operatorname{rank}(P^{i,j})$$

vengono detti **numeri di Betti persistenti**. Per le precedenti osservazioni, i numeri

$$\mu^{i,j} = \operatorname{rank}(\ker(\gamma_{i,j}))\,,$$

rappresentano la "misura dimensionale" degli elementi che nascono in t_i e muoiono in t_j; chiameremo $\mu^{i,j}$ la **molteplicità** dell'intervallo di vita $[t_i, t_j[$.

Lemma 19.7. *Se $i \leq h \leq k \leq j$, ossia se $[t_h, t_k[\subset [t_i, t_j[$, allora:*

(1) *$\beta^{h,k} \geq \beta^{i,j}$, e cioè i numeri di Betti persistenti sono una funzione decrescente sugli intervalli di vita;*
(2) *$(\beta^{h,k} - \beta^{h,j}) \geq (\beta^{i,k} - \beta^{i,j})$.*

Dimostrazione. Dal fatto che nel quadrato commutativo (19.4) le frecce orizzontali sono iniettive segue che $\beta^{i,k} \leq \beta^{h,k}$, mentre dal fatto le frecce verticali sono surgettive segue che $\beta^{i,j} \leq \beta^{i,k}$.

Ribaltando il quadrato (19.4) rispetto alla diagonale principale ed aggiungendo al diagramma i nuclei dei morfismi orizzontali (che prima del ribaltamento erano verticali) otteniamo un diagramma commutativo con le righe esatte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & P^{i,k} & \longrightarrow & P^{i,j} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \sigma} & & \downarrow & & \\ 0 & \longrightarrow & B & \longrightarrow & P^{h,k} & \longrightarrow & P^{h,j} & \longrightarrow & 0 \end{array}$$

e con il morfismo σ iniettivo. A maggior ragione la restrizione $\sigma_{|A} \colon A \to B$ è iniettiva e quindi per l'additività del rango

$$\beta^{h,k} - \beta^{h,j} = \operatorname{rank}(B) \geq \operatorname{rank}(A) = \beta^{i,k} - \beta^{i,j} \,.$$

□

Per l'additività del rango abbiamo:

$$\begin{aligned} \mu^{i,j} &= \operatorname{rank}(\ker(\gamma_{i,j})) = \operatorname{rank}(\operatorname{coker}(\sigma_{i,j})) - \operatorname{rank}(\operatorname{coker}(\tau_{i,j})) \\ &= \operatorname{rank}(P^{i,j-1}) - \operatorname{rank}(P^{i-1,j-1}) - \operatorname{rank}(P^{i,j}) + \operatorname{rank}(P^{i-1,j}) \\ &= \beta^{i,j-1} - \beta^{i-1,j-1} - \beta^{i,j} + \beta^{i-1,j} = (\beta^{i,j-1} - \beta^{i,j}) - (\beta^{i-1,j-1} - \beta^{i-1,j}) \,. \end{aligned}$$

Le molteplicità $\mu^{i,j}$ misurano solamente le classi mortali. Per "contare" le classi immortali si introducono:

$$P^{i,\infty} = \frac{P(t_i)}{\cup_{j>i} \ker(p_{i,j})}, \qquad \beta^{i,\infty} = \operatorname{rank}(P^{i,\infty}), \qquad \mu^{i,\infty} = \beta^{i,\infty} - \beta^{i-1,\infty} \,.$$

Il gruppo $P^{i,\infty}$ rappresenta le classi di $P(t_i)$ che non muoiono; dato che il morfismo $P(t_{i-1}) \to P(t_i)$ si fattorizza ad un morfismo iniettivo $P^{i-1,\infty} \xrightarrow{\sigma} P^{i,\infty}$ il cui conucleo (di rango $\mu^{i,\infty}$) rappresenta le classi di $P(t_i)$ che sono primordiali e immortali.

Quindi i numeri di Betti persistenti determinano le molteplicità; viceversa le molteplicià determinano i numeri di Betti persistenti in virtù del seguente risultato.

Lemma 19.8 (Lemma fondamentale dell'omologia persistente)**.** *Dato un modulo di persistenza localmente di tipo finito, per ogni i esiste un intero $n_i \geq i$ tale che $\mu^{i,j} = 0$ per ogni $j > n_i$, e valgolo la formule*

$$\beta^{h,k} = \sum_{i=0}^{h} \sum_{k<j\leq\infty} \mu^{i,j} = \sum_{i=0}^{h} \left(\mu^{i,\infty} + \sum_{j=k+1}^{\infty} \mu^{i,j} \right) \,.$$

Dimostrazione. Sia i fissato, allora si ha una catena ascendente di sottogruppi

$$0 \subset \ker(p_{i,i+1}) \subset \ker(p_{i,i+2}) \subset \cdots$$

che è stazionaria poiché per ipotesi $P(t_i)$ è finitamente generato. Dunque esiste un intero $N_i \geq i$ tale che $\ker(p_{i,j-1}) = \ker(p_{i,j})$ per ogni $j > N_i$. In particolare per ogni $j > n_i := \max(N_i, N_{i-1})$ si ha

$$\beta^{i,j-1} = \beta^{i,j} = \beta^{i,\infty}, \qquad \beta^{i-1,j-1} = \beta^{i-1,j} = \beta^{i-1,\infty}, \qquad \mu^{i,j} = 0 \,.$$

Le precedenti uguaglianze ci dicono inoltre che ha perfettamente senso scrivere

$$\begin{aligned} \mu^{i,\infty} + \sum_{j=k+1}^{\infty} \mu^{i,j} &= \beta^{i,\infty} - \beta^{i-1,\infty} + \sum_{j=k+1}^{\infty} (\beta^{i,j-1} - \beta^{i,j}) - \sum_{j=k+1}^{\infty} (\beta^{i-1,j-1} - \beta^{i-1,j}) \\ &= \beta^{i,k} - \beta^{i-1,k} \,. \end{aligned}$$

Dato che $\beta^{-1,k}=0$ si ottiene finalmente

$$\sum_{i=0}^{h}\sum_{k<j\leq\infty}\mu^{i,j}=\sum_{i=0}^{k}(\beta^{i,k}-\beta^{i-1,k})=\beta^{h,k}\,.$$

□

Quando il modulo di persistenza (19.1) è formato da spazi vettoriali di dimensione finita ed applicazioni lineari, possiamo rifare le stesse considerazioni con la dimensione al posto del rango ed abbiamo

$$\begin{aligned}\beta^{i,j}&=\dim P^{i,j}=\dim P(t_i)-\dim\ker(p_{i,j})=\operatorname{rank}(p_{i,j}),\\ \mu^{i,j}&=\operatorname{rank}(p_{i,j-1})-\operatorname{rank}(p_{i-1,j-1})-\operatorname{rank}(p_{i,j})+\operatorname{rank}(p_{i-1,j})\,.\end{aligned}\tag{19.5}$$

Esempio 19.9. Lo studio delle molteplicità numeri $\mu^{i,j}$ del modulo di persistenza dell'Esempio 19.2 ci restituisce quantità già studiate nei corsi di algebra lineare. Infatti, in tal caso per ogni $i\leq j$ si ha

$$\operatorname{rank}(p_{i,j})=\begin{cases}\operatorname{rank}(f^j) & \text{per } i\geq 0,\\ 0 & \text{per } i<0,\end{cases}$$

da cui segue che $\mu^{i,j}=0$ per ogni $0<i<j$, mentre

$$\mu^{0,j}=\operatorname{rank}(f^{j-1})-\operatorname{rank}(f^j)=\text{numero di blocchi di Jordan di ordine } \geq j\,.$$

Attenzione: la ben nota catena di disuguaglianze $\mu^{0,1}\geq\mu^{0,2}\geq\cdots$ che vale nel caso specifico dell'Esempio 19.2, non vale per un generico modulo di persistenza. In aggiunta, non è difficile dimostrare (esercizio per il lettore) che ogni successione $\mu^{i,j}\in\mathbb{N}$, $0\leq i<j$, appare come dato di molteplicità di un modulo di persistenza.

Esercizi:

Esercizio 24. Siano $g\colon V\to W$ un'applicazione lineare tra spazi vettoriali, $v\in V$ tale che $g(v)\neq 0$ e $H\subseteq W$ un sottospazio tale che $W=\operatorname{Span}(g(v))\oplus H$. Provare che

$$V=\operatorname{Span}(v)\oplus g^{-1}(H),\quad\text{dove}\quad g^{-1}(H)=\{u\in V\mid g(u)\in H\}.$$

Esercizio 25. Sia

$$P_0\xrightarrow{p_0}P_1\xrightarrow{p_1}\cdots\longrightarrow P_i\xrightarrow{p_i}\cdots\longrightarrow P_j\xrightarrow{p_j}\cdots\xrightarrow{p_{k-1}}P_k\,,\quad k\geq 1\,,$$

$$P_i\xrightarrow{p_{i,j}}P_j$$

un modulo di persistenza (di tipo finito) di spazi vettoriali di dimensione finita su di un campo $\mathbb{K}$ e sia $\mathcal{B}_i$ una base dello spazio vettoriale P_i per ogni indice i. L'unione $\mathcal{B}=\cup_i\mathcal{B}_i$ viene detta una **base di persistenza** se per ogni $i<k$ ed ogni $e\in\mathcal{B}_i$ si ha $p_i(e)=0$ oppure $p_i(e)\in\mathcal{B}_{i+1}$. Dimostrare che esistono basi di persistenza (Suggerimento: non è restrittivo supporre $P_0\neq 0$ e sia n il massimo intero tale che $p_{0,n}\neq 0$. Preso un qualunque vettore $e\in P_0$ tale che $p_{0,n}(e)\neq 0$, usare l'Esercizio 24 e induzione sulla somma delle dimensioni degli spazi P_i.)

Esercizio 26. Usare l'esistenza delle basi di persistenza per dimostrare che un modulo di persistenza di tipo finito a valori spazi vettoriali è determinato, a meno di isomorfismo, dalla successione delle molteplicità $\mu^{i,j}$.

20. Barcode e diagramma di persistenza (DP)

Fino agli inizi del XX secolo, i matematici parlavano senza imbarazzo di *funzioni polidrome*, ossia di funzioni che ad un punto del dominio associano più punti del codominio. Tale concetto, che sembrava scomparso, sta ritornando prepotentemente all'attenzione in teoria della persistenza (ma non solo).

In accordo con quanto affermato da Jacobson ([12, p. 5]) per le funzioni monodrome (quelle usuali), il miglior modo per formalizzare il concetto di funzione polidroma è definendo in maniera rigorosa quello che può essere considerato il suo grafo.

Definizione 20.1 (cf. [1, Defn. 2.2])**.** Siano S, X due insiemi. Una **rappresentazione polidroma**[4] di base S e indici X è un sottoinsieme $T \subset S \times X$. Per ogni $s \in S$, la **molteplicità** μ_s di s in T è per definizione la cardinalità di $p^{-1}(s)$, dove $p\colon T \to S$ è la restrizione a T della proiezione sul primo fattore. Equivalentemente

$$\mu_s = |\{x \in X \mid (s,x) \in T\}|\,.$$

Qualora $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ eccetera, diremo che la rappresentazione polidroma è naturale, intera, razionale, reale eccetera.

È chiaro come ad ogni funzione polidroma $f\colon S \rightsquigarrow X$, $s \mapsto f(s) \subset X$, corrisponde una rappresentazione polidroma $T = \cup_{s\in S}\{s\} \times f(s)$, e viceversa.

Definizione 20.2. Due rappresentazioni polidrome $T \subset S \times X$, $R \subset S \times Y$ sulla medesima base S si dicono **equivalenti per cambio di indici**, od anche per **reindicizzazione**, se esiste un'applicazione bigettiva $f\colon T \to R$ che commuta con le proiezioni sulla base, ossia se per ogni $(s,x) \in T$ vale $f(s,x) = (s,y)$ per qualche $y \in Y$.

Chiameremo **multi-insieme**[5], od anche **insieme con ripetizioni**, una classe di equivalenza di rappresentazioni polidrome per cambio di indici.

Ad esempio le due rappresentazioni polidrome di base $\mathbb{N}$:

$$T = \{(s,x) \in \mathbb{N} \times \mathbb{N} \mid s < x < 2s\}, \qquad R = \{(s,y) \in \mathbb{N} \times \mathbb{Z} \mid 3s < y < 4s\},$$

definiscono lo stesso multi-insieme: una possibile reindicizzazione è data dall'applicazione bigettiva $T \to R$, $(s,x) \mapsto (s, x+2s)$.

È chiaro che la molteplicità di un elemento della base è invariante per reindicizzazione, ossia per cambio di indici e segue dall'assioma della scelta che due rappresentazioni polidrome sulla medesima base S sono equivalenti per cambio di indici se e solo se hanno la stessa molteplicità in ogni $s \in S$. Quindi per ogni multi-insieme risultano bene definite sia la sua base S sia le sue molteplicità per ogni $s \in S$.

Definizione 20.3. Chiameremo **barcode**[6] un multi-insieme avente come base la famiglia di tutti gli intervalli di $\mathbb{R}$ del tipo $[a, b[$, con $a \leq b \leq +\infty$.

Per comprendere il motivo del nome barcode, supponiamo che la somma di tutte le molteplicià sia finita; allora esistono al più un numero finito di intervalli, diciamo $I_1, \ldots, I_n \subset R$ di molteplicià positiva: $\mu_{I_j} > 0$. In tale situazione il barcode si può rappresentare graficamente a foggia di *lasagna*, ossia come unione di barre orizzontali in $\mathbb{R}^2$ in numero uguale alla somma delle molteplicità: in buona sostanza, per ogni j l'intervallo $I_j \times \{0\}$ viene traslato in verticale per μ_{I_j} valori distinti (vedi Figura 13).

È adesso chiaro come ad ogni modulo di persistenza si associa un barcode (freccia (b) in Figura 12): per ogni coppia di interi $i < j$, l'intervallo $[t_i, t_j[$ viene contato con molteplicità $\mu^{i,j}$, mentre l'intervallo $[t_i, +\infty[$ viene contato con molteplicità $\mu^{i,\infty}$.

Esempio 20.4. Calcoliamo i barcode degli 0-cicli e 1-cicli del complesso filtrato di Vietoris-Rips della (micro)nuvola di punti $I = \{(0,0), (4,0), (0,4), (5,5)\} \subset \mathbb{R}^2$. I valori critici della

[4] In inglese multiset representation.
[5] In inglese multiset.
[6] Qui preferiamo mantenere il termine inglese (in attesa di traduzioni soddisfacenti).

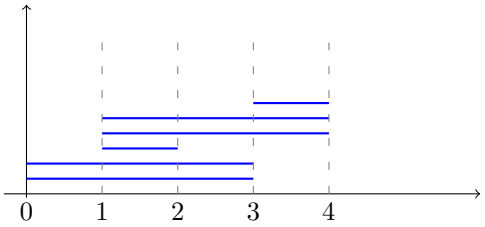


FIGURA 13. Un esempio di barcode, con gli intervalli $[0,3[$ e $[1,4[$ di molteplicità 2, gli intervalli $[1,2[$ e $[3,4[$ di molteplicità 1 (e tutti gli altri di molteplicità 0).

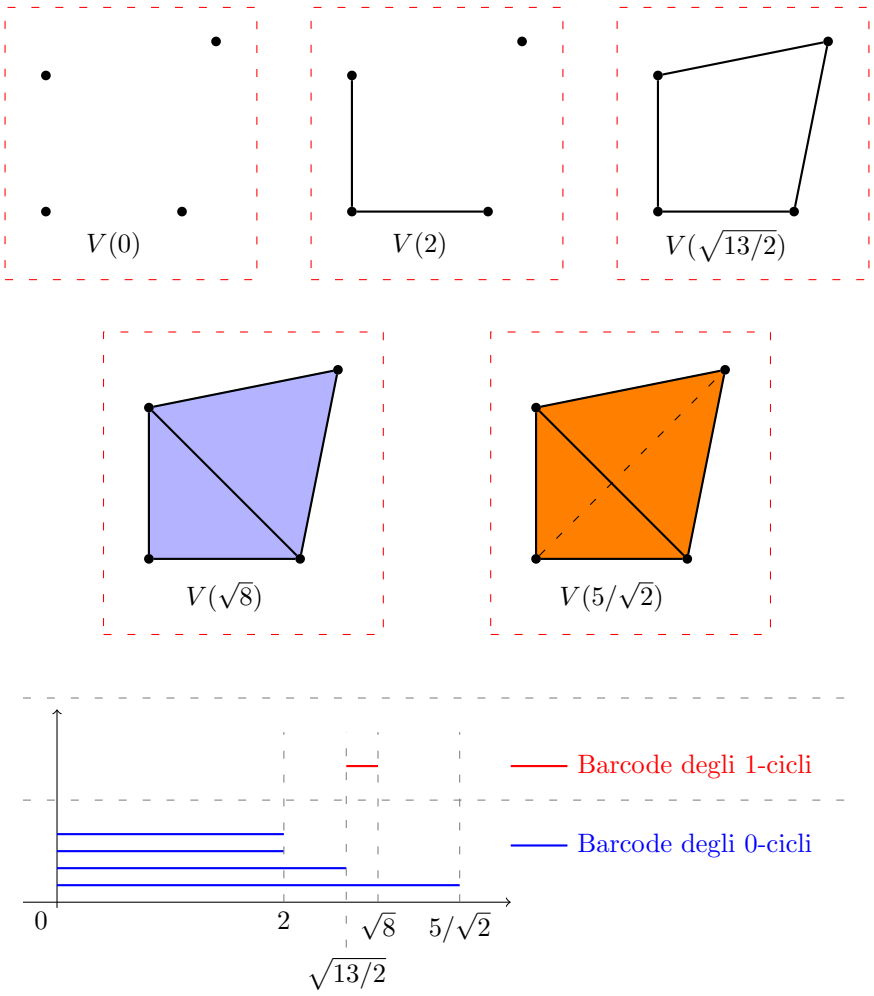


FIGURA 14. Descrizione nell'Esempio 20.4.

funzione filtrante $v\colon \Delta^I \to \mathbb{R}$ sono tutte e sole le semidistanze tra coppie di punti di I e sono quindi

$$0 < 2 < \sqrt{13/2} < \sqrt{8} < 5/\sqrt{2}\,.$$

La Figura 14 mostra i sottocomplessi di livello $V(t) = \{x \in \Delta^I \mid v(x) \le t\}$ per ciascuno dei 5 valori critici (in celeste i 2-simplessi massimali ed in arancio i 3-simplessi massimali). La stessa figura contiene i barcode degli 0-cicli (intervalli di vita delle componenti connesse) e degli 1-cicli (intervalli di vita dei buchi a circonferenza).

Un altro modo di rappresentare un intervallo del tipo $[a, b[$ con $a \leq b \leq \infty$ è mediante il punto nel piano esteso $(a, b) \in \overline{\mathbb{R}}^2 = (\mathbb{R} \cup \{+\infty\})^2$. Si noti che il punto (a, b) si colloca sempre nel semipiano (esteso) $\overline{S} = \{(a, b) \mid a \leq b \leq +\infty\}$ dei punti al di sopra della diagonale $\Delta = \{(t, t) \mid t \in \mathbb{R} \cup \{+\infty\}\}$.

Definizione 20.5. Sia κ un numero cardinale infinito. Un **diagramma di persitenza** di taglia κ è un multi-insieme con base il semipiano esteso $\overline{S}$ tale che:

(1) la molteplicità di ogni punto $(a, b) \in \overline{S}$ è $\leq \kappa$;
(2) la molteplicità di ogni punto (a, a) della diagonale è esattamente $= \kappa$.

Quando non viene fatto riferimento alla taglia si intende implicitamente che essa sia la più piccola possibile, $\kappa = \aleph_0$.

La richiesta di infilare nei diagrammi di persistenza tutti i punti della diagonale (corrispondenti ad intervalli vuoti), ciascuno con molteplicità infinita, è uno stratagemma utile (ma esteticamente orrendo!) per poter definire strutture metriche e topologiche sulla famiglia di tutti i diagrammi di persistenza. Se, con molta fantasia[7], pensiamo ad un modulo di persistenza come un'evoluzione temporale di un insieme di particelle, ed i tempi t_i come quelli in cui si crea o si distrugge una particella che abbia un tempo di vita positivo, stiamo formalmente ipotizzando che ad ogni istante vengano create ed immediatamente distrutte una infinità di particelle.

Esiste una ovvia bigezione tra barcode e diagrammi di persistenza, che per i moduli di persistenza di tipo finito ci porta alla seguente definizione.

Definizione 20.6. Dato un modulo di persistenza localmente di tipo finito, il suo **diagramma di persistenza** è il multi-insieme con base il semipiano esteso $\overline{S} = \{(a, b) \mid a \leq b \leq +\infty\}$ e con molteplicità:

(1) per ogni $i < j$ il punto (t_i, t_j) ha molteplicità $\mu^{i,j}$;
(2) per ogni i il punto $(t_i, +\infty)$ ha molteplicità $\mu^{i,\infty}$;
(3) ogni punto della diagonale ha molteplicità infinita numerabile;
(4) in tutti gli altri casi la molteplicità è uguale a 0.

21. Una molto vaga interpretazione

Come detto non ci addentriamo in questa parte, a mio avviso non molto chiara neppure a tanti che pubblicano lavori in omologia persistente (che la evitano accuratamente fornendo discorsi vaghi, fumosi, generici e scopiazzati).

Abbiamo visto che prendendo una nuvola di punti $I \subset \mathbb{R}^n$ possiamo ad essa associare il complesso filtrato di Vietoris-Rips (K, v), $K = \Delta^I$. Se spostiamo anche di pochissimo i punti di I, i valori critici di v cambiano e si ha una diversa filtrazione di sottocomplessi di livello.

Quello che succede nel barcode ci fa però ben sperare. Infatti, si può dimostrare che, a seguito di una piccola perturbazione:

(1) le classi di omologia persistente che si creano (per effetto della perturbazione) hanno una breve durata di vita;
(2) le classi di omologia persistente che si distruggono (per effetto della perturbazione) avevano una breve durata di vita;
(3) ogni classe con intervallo di vita $[a, b[$ sufficientemente lungo[8] si "trasforma" in una classe con intervallo di vita $[a', b'[$, con a vicino ad a' e b vicino ad b'.

Da ciò traiamo il seguente insegnamento:

1) ha senso interpretare come significativi solo gli intervalli di vita lunghi, mentre quelli corti devono essere considerati "rumore topologico" e quindi non significativi del dato che si vuole interpretare.

[7] In mancanza di fantasia va bene anche l'arroganza da effetto Dunning-Kruger.
[8] Ossia contenente un numero abbastanza alto, in senso statistico, di valori critici.

2) Esistono delle funzioni distanza che rendono l'insieme dei barcode uno spazio metrico. Nella filtrazione di Vietoris-Rips, piccole perturbazioni del point cloud inducono piccole perturbazioni (in senso metrico) del barcode. Questa proprietà viene detta **stabilità** ed è l'ingrediente senza il quale quello che abbiano sviluppato non sarebbe altro che un bell'esercizio intellettuale senza alcuna applicazione pratica. In generale ogni tipo di passaggio (a) dai dati ai complessi filtrati, per avere un qualche interesse applicativo, dovrà soddisfare la condizione di **stabilità**.

3) Recentemente si intravedono alcune applicazioni dell'omologia persistente anche in ambiti della matematica pura, come ad esempio la geometria algebrica [14]. In tale ambito, più che come spazio metrico, l'insieme dei barcode ci interessa maggiormente come insieme degli oggetti di una categoria tale che il passaggio da complessi filtrati a barcode sia un funtore [1].

Qui termina la prima parte delle dispense

22. Il teorema di Menelao

Inizia qui la seconda parte delle dispense dedicata a temi di geometria proiettiva classica.

Indicheremo con $\mathbb{K}$ un campo non nullo, ossia con $1 \neq 0$. Le figure si riferiscono alla geometria proiettiva su $\mathbb{R}$ e sono un valido aiuto alla comprensione dei risultati, non solo su $\mathbb{R}$ ma anche su campi di caratteristica $\neq 2$. Occorre fare attenzione che in caratteristica 2 accadono alcuni fenomeni decisamente controintuitivi (vedi Esempio 26.4) e per i quali il disegno potrebbe essere fuorviante.

Per spazio vettoriale intenderemo uno spazio vettoriale di dimensione finita su $\mathbb{K}$. Per ogni spazio vettoriale V indicheremo con $V^\vee$ il suo duale e con $\mathrm{GL}(V)$ il gruppo di tutti gli endomorfismi lineari di V invertibili, dotato del prodotto di composizione.

Iniziamo con il concetto di dipendenza affine di un insieme finito di vettori. In questa sezione la lettera V indicherà sempre uno spazio vettoriale su $\mathbb{K}$.

Lemma 22.1. *Sia V uno spazio vettoriale su $\mathbb{K}$. Dati $v_0, \dots, v_p \in \mathbb{K}^n$ le seguenti condizioni sono equivalenti:*

1. *esiste un indice $i = 0, \dots, p$ tale che i p vettori $v_j - v_i$, $j \neq i$, sono linearmente dipendenti;*
2. *per ogni $i = 0, \dots, p$ i p vettori $v_j - v_i$, $j \neq i$, sono linearmente dipendenti;*
3. *i $p+1$ vettori $w_i = (v_i, 1) \in V \times \mathbb{K}$ sono linearmente dipendenti.*

Dimostrazione. Mostriamo che (1) implica (3). Per semplicità supponiamo $i = 0$ (per $i \neq 0$ la dimostrazione è sostanzialmente identica). Siano $a_1, \dots, a_p \in \mathbb{K}$ non tutti nulli e tali che $\sum_{j=1}^p a_j(v_j - v_i) = 0$. Se poniamo $a_0 = -\sum_{j=1}^p a_j$ si ha

$$\sum_{j=0}^p a_j(v_j, 1) = \left(\sum_{j=0}^p a_j v_j, \sum_{j=0}^p a_j\right) = \left(\sum_{j=1}^p a_j v_j - \sum_{j=1}^p a_j v_0, 0\right) = \left(\sum_{j=1}^p a_j(v_j - v_0), 0\right) = (0,0)\,.$$

Mostriamo adesso che (3) implica (2). Siano $a_0, \dots, a_p \in \mathbb{K}$ non tutti nulli e tali che $\sum a_j w_j = 0$. Siccome

$$\sum a_j w_j = (\sum a_j v_j, \sum a_j)$$

si ha che $\sum a_j = 0$ e quindi per ogni indice i si ha

$$a_i = -\sum_{j \neq i} a_j$$

e di conseguenza $a_j \neq 0$ per qualche $j \neq i$. Ma allora

$$\sum_{j \neq i} a_j(v_j - v_i) = \sum_{j \neq i} a_j v_j - (\sum_{j \neq i} a_j) v_i = \sum_{j=0}^p a_j v_j = 0\,.$$

□

Definizione 22.2. I vettori $v_0, \dots, v_p$ di uno spazio vettoriale si dicono **affinemente dipendenti** se soddisfano le condizioni del Lemma 22.1. Altrimenti si dicono **affinemente indipendenti**.

In particolare: il massimo numero di vettori affinemente indipendenti in $\mathbb{K}^n$ è $n+1$; ogni vettore (anche nullo) è affinemente indipendente; due vettori sono affinemente dipendenti se e solo se sono uguali.

Tre vettori si dicono **allineati** se sono affinemente dipendenti.

Lemma 22.3. *Siano V spazio vettoriale e $p, q, r \in V$ con $p \neq q$. Allora p, q, r sono allineati se e solo se esiste $t \in \mathbb{K}$ tale che $r = (1-t)p + tq$; in tal caso t è unico.*

Dimostrazione. Per definzione p, q, r sono allineati se e solo se esistono $a, b \in \mathbb{K}$ non entrambi nulli e tali che $a(r-p) + b(q-p) = 0$. Siccome $q - p \neq 0$ si ha $a \neq 0$ (se fosse $a = 0$ allora anche $b = 0$); dividendo per a si ottiene

$$r - p = -\frac{b}{a}(q-p) \iff r = (1-t)p + tq \quad \text{dove} \quad t = -\frac{b}{a}\,.$$

Se $r = (1-t)p + tq = (1-s)p + sq$ con $t, s \in \mathbb{K}$, facendo la differenza si ottiene

$$0 = (s-t)p + (t-s)q = (t-s)(q-p)$$

da cui $s = t$. □

Dunque, per ogni $p \neq q$ l'applicazione

$$f_{p,q} \colon \mathbb{K} \to V, \qquad f(t) = (1-t)p + tq, \tag{22.1}$$

induce una bigezione tra il campo $\mathbb{K}$ e l'insieme dei vettori allineati con p, q. Si noti che $f_{p,q}(0) = p$, $f_{p,q}(1) = q$ Chiameremo l'immagine di $f_{p,q}$ **retta affine** passante per p, q, che denoteremo $\overline{pq}$.

Per ogni $r \in \overline{pq}$ definiamo il **rapporto semplice**

$$(r, p, q) = f_{p,q}^{-1}(r)\,.$$

In altri termini

$$(r, p, q) = t \iff r = (1-t)p + tq \iff r - p = t(q-p)\,.$$

Il perché del nome rapporto semplice si capisce bene quando $V = \mathbb{K}^1$; in tal caso si può dividere per $q - p \in \mathbb{K}$ e quindi $(r, p, q) = (r-p)/(q-p)$.

Il rapporto semplice **non è** invariante per permutazioni: se p, q, r sono distinti e $(r, p, q) = t$ si ha

$$(r, p, q) = t, \qquad (p, q, r) = \frac{1}{1-t}, \qquad (q, r, p) = \frac{t-1}{t}\,,$$

$$(p, r, q) = \frac{t}{t-1}, \qquad (q, p, r) = \frac{1}{t}, \qquad (r, q, p) = 1 - t,$$

dove le precedenti formule hanno senso poiché $t \neq 0$ ($r \neq p$) e $t \neq 1$ ($r \neq q$). Mostriamo solamente il calcolo di (p, q, r) lasciando le altre verifiche per esercizio. Se $(r, p, q) = t$ allora $r = (1-t)p + tq$ da cui

$$(r, p, q) = t \iff r = (1-t)p + tq \iff p = \frac{t}{t-1}q + \frac{1}{1-t}r \iff (p, q, r) = \frac{1}{1-t}\,.$$

Lemma 22.4. *Siano dati tre punti $a, b, c \in \mathbb{K}^n$ non allineati e si considerino tre punti $c' \in \overline{ab}$, $a' \in \overline{bc}$, $b' \in \overline{ac}$. Presi i rapporti semplici*

$$(c', b, a) = t, \qquad (a', c, b) = s, \qquad (b', a, c) = r,$$

vale l'uguaglianza $tsr = (t-1)(s-1)(r-1)$ se e solo se a', b', c' sono allineati.

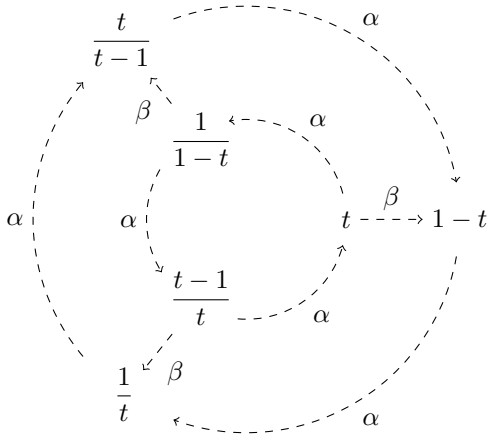


FIGURA 15. Le applicazioni $\alpha, \beta \colon \mathbb{K} - \{0,1\} \to \mathbb{K} - \{0,1\}$, $\alpha(t) = \dfrac{1}{1-t}$, $\beta(t) = 1-t$, soddisfano le relazioni $\alpha^3 = \beta^2 = \mathrm{Id}$, $\alpha\beta = \beta\alpha^2$ e definiscono la rappresentazione del gruppo simmetrico Σ_3 determinata dall'azione sui rapporti semplici.

Dimostrazione. Si considerino i vettori di $\mathbb{K}^n \times \mathbb{K}$:

$$A = \begin{pmatrix} a \\ 1 \end{pmatrix}, \quad B = \begin{pmatrix} b \\ 1 \end{pmatrix}, \quad C = \begin{pmatrix} c \\ 1 \end{pmatrix}, \quad A' = \begin{pmatrix} a' \\ 1 \end{pmatrix}, \quad B' = \begin{pmatrix} b' \\ 1 \end{pmatrix}, \quad C' = \begin{pmatrix} c' \\ 1 \end{pmatrix}.$$

Allora i tre vettori A, B, C sono linearmente indipendenti e la matrice $(A, B, C) \in M_{n+1,3}(\mathbb{K})$ ha rango 3. Dato che

$$A' = sB + (1-s)C, \qquad B' = (1-r)A + rC, \qquad C' = tA + (1-t)B,$$

si ha il prodotto righe per colonne

$$(A', B', C') = (A, B, C) \begin{pmatrix} 0 & 1-r & t \\ s & 0 & 1-t \\ 1-s & r & 0 \end{pmatrix}.$$

Per il Lemma 22.1 i vettori A', B', C' sono allineati se e solo se la matrice (A', B', C') ha rango < 3 e questo vale se e solo se la matrice 3×3 nella formula precedente ha rango < 3. Adesso basta calcolare il determinante:

$$\begin{vmatrix} 0 & 1-r & t \\ s & 0 & 1-t \\ 1-s & r & 0 \end{vmatrix} = (1-r)(1-s)(1-t) + rst\,.$$

□

Teorema 22.5 (Teorema di Menelao, prima versione)**.** *Siano dati tre punti $a, b, c \in V$ non allineati e si considerino tre punti $c' \in \overline{ab}$, $a' \in \overline{bc}$, $b' \in \overline{ac}$. Se $a' \neq b, c$, $b' \neq a, c$ e $c' \neq a, b$ allora a', b', c' sono allineati se e solo se*

$$(a, c', b)(b, a', c)(c, b', a) = 1\,.$$

Dimostrazione. Se

$$(c', b, a) = t, \qquad (a', c, b) = s, \qquad (b', a, c) = r,$$

allora

$$(a, c', b) = \frac{t-1}{t}, \qquad (b, a', c) = \frac{s-1}{s}, \qquad (c, b', a) = \frac{r-1}{r}\,.$$

La formula $(a, c', b)(b, a', c)(c, b', a) = 1$ è equivalente a $\dfrac{t-1}{t}\dfrac{s-1}{s}\dfrac{r-1}{r} = 1$ e la conclusione segue dal Lemma 22.4. □

Vediamo adesso l'interpretazione in geometria Euclidea del teorema di Menelao, con i punti a, b, c, a', b', c' considerati in $\mathbb{R}^2$. Per ogni $p, q \in \mathbb{R}^2$ denotiamo con $|pq| = \|p - q\|$ la distanza Euclidea e osserviamo che se p, q, r sono allineati e distinti, allora

$$(p, r, q) = \pm \frac{|pr|}{|qr|}$$

dove il segno $-$ vale se e solo se r è compreso tra p e q, ossia se r appartiene al segmento di estremi p, q. Infatti $(p, r, q) = t \in \mathbb{R}$ se e solo se $p = (1-t)r + tq$ se e solo se $p - r = t(q - r)$ da cui $|t| = \dfrac{\|p - r\|}{\|q - r\|}$. Sempre dalla formula $p - r = t(q - r)$ segue che t è negativo se e solo se i vettori $p - r$ e $q - r$ hanno direzioni opposte, ossia se e solo se r è compreso tra p, q.

Se a', b', c' sono allineati, siccome una retta non passante per i vertici del triangolo abc interseca i lati in 0 oppure 2 punti ne segue che

$$\frac{|ac'|}{|bc'|}\,\frac{|ba'|}{|ca'|}\,\frac{|cb'|}{|ab'|} = 1\,. \tag{22.2}$$

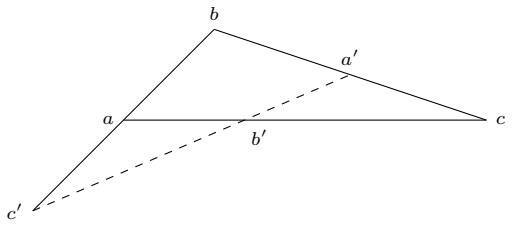


FIGURA 16. I teorema di Menelao.

Viceversa, se vale (22.2) ed un numero pari di punti a', b', c' appartiene al perimetro del triangolo allora $(a, c', b)(b, a', c)(c, b', a) = 1$ e tali punti risultano allineati.

Esiste una versione alternativa del Teorema di Menelao, molto celebre nella grafica computerizzata, e nel cui enunciato intervengono alcune generalizzazioni delle funzioni $f_{p,q}(t) = (1-t)p + tq$ introdotte in (22.1).

Teorema 22.6 (Menelao, seconda versione)**.** *Per ogni terna di punti $p, q, r \in V$ si consideri l'applicazione*

$$f_{p,q,r} \colon \mathbb{K}^2 \to V, \qquad f_{p,q,r}(t, s) = (1 - s) f_{p,q}(t) + s f_{q,r}(t)\,.$$

Allora $f_{p,q,r}(t, s) = f_{p,q,r}(s, t)$ per ogni $s, t \in \mathbb{K}$.

La dimostrazione è banale, mentre tutt'altro che evidente è la relazione tra le due versioni del teorema di Menalao. Infatti, sviluppando i conti si ha

$$f_{p,q,r}(t, s) = (1-s)(1-t)p + (1-s)tq + s(1-t)q + str = (1-s)(1-t)p + (s + t - 2st)q + str$$

che risulta simmetrica nelle variabili s, t.

Qui mostriamo solamente come la seconda versione segue dalla prima. Si considerino tre punti non allineati p, q, r, due scalari $t, s \in \mathbb{K}$ e si guardi alla Figura 17

Il Teorema 22.5 applicato ai triangoli di vertici $f_{p,q}(s), q, f_{q,r}(s)$ e $f_{p,q}(t), q, f_{q,r}(t)$ rispettivamente ci dà le due uguaglianze:

$$(f_{p,q}(s), f_{p,q}(t), q)(q, f_{q,r}(t), f_{q,r}(s))(f_{q,r}(s), x, f_{p,q}(s)) = 1,$$

$$(f_{p,q}(t), f_{p,q}(s), q)(q, f_{q,r}(s), f_{q,r}(t))(f_{q,r}(t), x, f_{p,q}(t)) = 1.$$

I quattro rapporti semplici dove non compare x si calcolano facilmente in funzione di s, t:

$$(f_{p,q}(s), f_{p,q}(t), q) = \frac{s - t}{1 - t}, \qquad (f_{p,q}(t), f_{p,q}(s), q) = \frac{t - s}{1 - s},$$

$$(q, f_{q,r}(t), f_{q,r}(s)) = \frac{t}{t - s}, \qquad (q, f_{q,r}(s), f_{q,r}(t)) = \frac{s}{s - t}$$

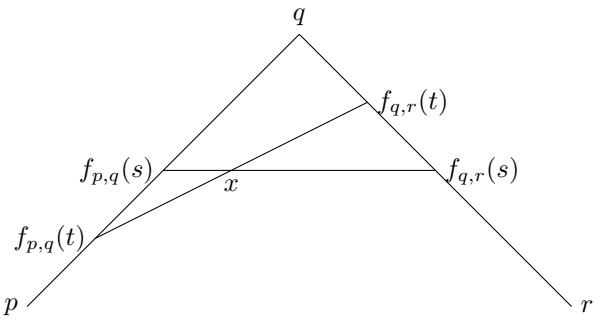


FIGURA 17. Il punto $x = f_{p,q,r}(t,s) = f_{p,q,r}(s,t)$ per $s \neq t$.

da cui segue

$$(f_{q,r}(s), x, f_{p,q}(s)) = \frac{(1-t)(t-s)}{(s-t)t} = \frac{t-1}{t} \iff (x, f_{p,q}(s), f_{q,r}(s)) = t \iff x = f_{p,q,r}(s,t),$$

$$(f_{q,r}(t), x, f_{p,q}(t)) = \frac{(1-s)(s-t)}{(t-s)s} = \frac{s-s}{t} \iff (x, f_{p,q}(t), f_{q,r}(t)) = s \iff x = f_{p,q,r}(t,s).$$

Esercizio 27. Nella notazioni precedenti, e per $\mathbb{K} = \mathbb{R}$, mostrare che $t \mapsto \gamma(t) = f_{p,q,r}(t,t)$ è una parametrizzazione della parabola passante per p, r e con derivate $\gamma'(p) = q - p$, $\gamma'(r) = r - q$.

23. Sottospazi e trasformazioni affini

Sia V uno spazio vettoriale. Una combinazione lineare $a_0v_0 + \cdots + a_nv_n$ 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. In altri termini, un sottoinsieme $H \subset V$ è un sottospazio affine se per ogni successione finita $v_0, \ldots, v_n \in H$ ed ogni successione $a_0, \ldots, a_n \in \mathbb{K}$ tale che $\sum a_i = 1$ si ha $a_0v_0 + \cdots + a_nv_n \in H$.

Esempio 23.1.
(1) il vuoto è un sottopazio affine;
(2) per ogni $v \in V$, il sottoinsieme $\{v\}$ è un sottospazio affine;
(3) ogni sottospazio vettoriale è anche un sottospazio affine;
(4) intersezione di una famiglia arbitaria di sottospazi affini è ancora un sottospazio affine;
(5) Il sottoinsieme di $\mathbb{K}^n$ formato dalle soluzioni $(x_1, \ldots, x_n)^T$ di un sistema lineare

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$

è un sottospazio affine;
(6) Se $H \subseteq V$ e $K \subseteq W$ sono sottospazi affini, il loro prodotto cartesiano $H \times K$ è un sottospazio affine di $V \times W$.

Lemma 23.2. *Siano V uno spazio vettoriale e $H \subset V - \{0\}$ un sottospazio affine che non contiene il vettore nullo. Allora $n+1$ vettori $v_0, \ldots, v_n \in H$ sono affinemente indipendenti se e solo se sono linearmente indipendenti in V.*

Dimostrazione. Una implicazione è chiara: se $v_0, \ldots, v_n$ sono linearmente indipendenti in V, a maggior ragione i vettori $(v_0, 1), \ldots, (v_n, 1)$ sono linearmente indipendenti in $V \times \mathbb{K}$.

Supponiamo viceversa che i vettori v_i siano linearmente dipendenti, ossia che si abbia una combinazione lineare $\sum_{i=0}^n a_iv_i = 0$, con gli $a_i \in \mathbb{K}$ non tutti nulli. Siccome $0 \notin H$ si

ha $v_0 \neq 0$ e quindi esiste almeno un indice $i > 0$ tale che $a_i \neq 0$. Denotiamo $b = \sum a_i$ e mostriamo che $b = 0$. Se per assurdo fosse $b \neq 0$ si avrebbe una combinazione baricentrica

$$0 = \frac{0}{b} = \sum_{i=0}^{n} \frac{a_i}{b} v_i$$

in contraddizione con l'ipotesi che $0 \notin H$. Dunque $\sum a_i = 0$,

$$0 = \sum_{i=0}^{n} a_i v_i = (\sum_{i=0}^{n} a_i) v_0 + \sum_{i=1}^{n} a_i (v_i - v_0) = \sum_{i=1}^{n} a_i (v_i - v_0)$$

e quindi i vettori $v_1 - v_0, \ldots, v_n - v_0$ sono linearmente dipendenti. □

Definizione 23.3 (Inviluppo affine)**.** Per ogni insieme finito di vettori $v_0, \ldots, v_n$, l'insieme

$$\langle\langle v_0, \ldots, v_n \rangle\rangle = \{a_0 v_0 + \cdots + a_n v_n \mid a_i \in \mathbb{K}, \sum a_i = 1\}$$

di tutte le combinazioni baricentriche viene detto **inviluppo affine** di $v_0, \ldots, v_n$.

L'inviluppo affine è un sottospazio affine. Infatti dati $w_0, \ldots, w_m \in \langle\langle v_0, \ldots, v_n \rangle\rangle$ per definizione esiste una matrice a_{ij}, $i = 0, \ldots, n$, $j = 0, \ldots, m$ tale che

$$w_j = \sum_{i=0}^{n} a_{ij} v_i, \quad \sum_{i=0}^{n} a_{ij} = 1, \text{ per ogni } j = 0, \ldots, m\,.$$

Allora per ogni $b_0, \ldots, b_m \in \mathbb{K}$ tali che $\sum b_j = 1$ si ha

$$\sum_j b_j w_j = \sum_{i,j} a_{ij} b_j v_i = \sum_i c_i v_i, \qquad c_i = \sum_j b_j a_{ij},$$

e siccome

$$\sum_i c_i = \sum_i \sum_j b_j a_{ij} = \sum_j b_j \sum_i a_{ij} = \sum_j b_j \cdot 1 = 1$$

ne consegue che $\sum_j b_j w_j \in \langle\langle v_0, \ldots, v_n \rangle\rangle$.

Segue immediatamente dalle definizioni che se un sottospazio affine contiene un numero finito di vettori, allora contiene anche il loro inviluppo affine; dunque l'inviluppo affine $\langle\langle v_0, \ldots, v_n \rangle\rangle$ coincide con l'intersezione dei sottospazi affini contenenti $v_0, \ldots, v_n$.

Lemma 23.4. *Sia K un sottospazio affine di uno spazio vettoriale V. Allora per ogni vettore $u \in V$ il sottoinsieme*

$$u + K := \{u + x \mid x \in K\}$$

*è ancora un sottospazio affine detto il **traslato di K tramite u**.*

Dimostrazione. Dati $v_0, \ldots, v_n \in u + K$ e $a_0, \ldots, a_n \in \mathbb{K}$ tali che $\sum a_i = 1$, per definizione $v_i = u + x_i$ con $x_i = v_i - u \in K$ e quindi

$$\sum a_i v_i = \sum a_i (u + x_i) = (\sum a_i) u + \sum a_i x_i = u + \sum a_i x_i \in u + K\,.$$

□

Dati due sottospazi affini H, K, scriveremo $H \sim K$ se H è un traslato di K: è immediato osservare che $\sim$ è una relazione di equivalenza.

Lemma 23.5. *Sia K un sottospazio affine non vuoto di uno spazio vettoriale V. Allora il sottoinsieme $W = \{u - v \mid u, v \in K\} \subset V$ è un sottospazio vettoriale ed è l'unico sottospazio vettoriale che risulta essere un traslato di K. In particolare K è un sottospazio vettoriale se e solo se $0 \in K$.*

Dimostrazione. Siccome K è non vuoto, pure W è non vuoto. Dati $u, v, x, y \in K$ e $a, b \in \mathbb{K}$ si ha

$$a(u - v) + b(x - y) = u - ((1 - a)u + av - bx + by) \in W\,,$$

poiché $(1-a)+a-b+b = 1$ e quindi $(1-a)u+av-bx+by \in K$; quindi W è un sottospazio vettoriale. Resta da provare che $K \sim W$, ossia che K è un traslato di W e che se $W \sim U$ con U sottospazio vettoriale, allora $U = W$. Sia $u \in K$ un elemento qualsiasi e mostriamo che $K = u + W$; se $v \in K$ allora $v - u \in W$ e quindi $v = u + (v - u) \in K$. Viceversa, se $w \in W$

allora $w = x - y$ con $x, y \in K$ e quindi $u + w = u + x - y \in K$ poiché $1 + 1 - 1 = 1$. Per finire, se $v + W$ è un sottospazio vettoriale allora $0 \in v + W$, ossia $-v \in W$, quindi $v \in W$ e di conseguenza $v + W = W$. □

Secondo il Lemma 23.5, per ogni sottospazio affine non vuoto $K \subset V$ esiste un unico sottospazio vettoriale W che è un traslato di K. Chiameremo W **spazio tangente** di K e si definisce la **dimensione di** K come la dimensione di W come spazio vettoriale. Se $K = \emptyset$ allora si pone per convenzione $\dim K = -1$.

Dunque i punti sono tutti e soli i sottospazi affini di dimensione 0: sottospazi affini di dimensione 1 e 2 sono detti rispettivamente rette e piani affini.

Diremo che due sottospazi affini H, K sono **paralleli** se i rispettivi spazi tangenti U, W soddisfano una relazione di inclusione, ossia $U \subset W$ oppure $W \subset U$. In particolare, due sottospazi affini della stessa dimensione sono paralleli se e solo se hanno lo stesso spazio tangente, ossia se e solo se sono uno il traslato dell'altro.

Per **spazio affine** su di un campo $\mathbb{K}$ intenderemo un sottospazio affine di uno spazio vettoriale. Per rimarcare la differenza chiameremo **punti** (anziché vettori) gli elementi di uno spazio affine; al di là della questione terminologica uno spazio affine può anche essere pensato come uno spazio vettoriale in cui il vettore nullo è un vettore come tutti gli altri ed in cui le uniche combinazioni lineari consentite sono quelle baricentriche.

Definizione 23.6. Un'applicazione $f\colon V \to W$ tra spazi affini 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 $f(\sum a_i v_i) = \sum a_i f(v_i)$. Le applicazioni affini invertibili (ossia bigettive) vengono dette **affinità**.

È chiaro che composizione di applicazioni affini è ancora affine.

Esempio 23.7. Ogni applicazione lineare tra spazi vettoriali è anche affine.

Esempio 23.8. Siano V uno spazio vettoriale e $v \in V$. Allora la **traslazione**

$$T_v\colon V \to V, \qquad T_v(x) = v + x,$$

è un'affinità con inversa T_{-v}. Infatti se $\sum a_i = 1$ si ha

$$T_v(\sum a_i x_i) = v + \sum a_i x_i = (\sum a_i)v + \sum a_i x_i = \sum a_i(v + x_i) = \sum a_i T_v(x_i)\,.$$

Lemma 23.9. *Sia $f\colon V \to W$ un'applicazione affine tra spazi vettoriali. Allora esiste un'applicazione lineare $g\colon V \to W$ tale che $f = T_{f(0)}g$. In particolare f è lineare se e solo se $f(0) = 0$.*

Dimostrazione. Già sappiamo che se f è lineare allora $f(0) = 0$. Viceversa, se $f(0) = 0$ allora per ogni $u, v \in V$ ed ogni $a, b \in \mathbb{K}$ si ha

$$f(au + bv) = f((1 - a - b)0 + au + bv) = (1 - a - b)f(0) + af(u) + bf(v) = +af(u) + bf(v)$$

e quindi f è lineare. Dunque l'applicazione affine $g = T_{-f(0)}f$ è lineare in quanto $g(0) = T_{-f(0)}(f(0)) = 0$. □

In generale, se $f\colon V \to W$ è un'applicazione affine tra spazi vettoriali non è detto che si possa scrivere $f = gT_v$ per opportuni $v \in V$ e g lineare. Una condizione necessaria è che $0 = gT_v(-v)$ appartenga all'immagine di f; tale condizione è anche sufficiente in quanto se esiste $v \in V$ tale che $f(-v) = 0$, allora l'applicazione $g = fT_{-v}$ risulta lineare in quanto $g(0) = 0$.

Teorema 23.10. *Siano $\mathbb{K}$ un campo con almeno tre elementi (ossia $\mathbb{K} \neq \mathbb{Z}/(2)$) e $f\colon H \to K$ un'applicazione tra due spazi affini definiti su$\mathbb{K}$. Allora f è affine se e solo se per ogni $p, q \in H$ ed ogni $t \in \mathbb{K}$ vale*

$$f((1 - t)p + tq) = (1 - t)f(p) + tf(q)\,.$$

In altri termini f è affine se e solo se preserva gli allineamenti ed i rapporti semplici.

Dimostrazione. La condizione è chiaramente necessaria. Per quanto riguarda la sufficienza dimostriamo per induzione su $n \geq 1$ che

$$f(\sum_{i=0}^{n} t_i p_i) = \sum_{i=0}^{n} t_i f(p_i), \qquad p_i \in H, \quad t_i \in \mathbb{K}\,, \quad \sum t_i = 1\,. \tag{23.1}$$

Per $n = 1$ la (23.1) è vera per ipotesi; supponiamo quindi $n > 1$ e scegliamo un $b \in \mathbb{K} - \{0, 1\}$. Si può scrivere

$$\sum_{i=0}^{n} t_i p_i = (1-b)\left(\frac{t_0}{1-b}p_0 + \frac{1-b-t_0}{1-b}p_1\right) + b\left(\frac{t_0+t_1+b-1}{b}p_1 + \sum_{i=2}^{n}\frac{t_i}{b}p_i\right)$$

e per l'ipotesi induttiva

$$\begin{aligned} f(\sum_{i=0}^{n} t_i p_i) &= (1-b) f\left(\frac{t_0}{1-b}p_0 + \frac{1-b-t_0}{1-b}p_1\right) + b f\left(\frac{t_0+t_1+b-1}{b}p_1 + \sum_{i=2}^{n}\frac{t_i}{b}p_i\right) \\ &= (1-b)\left(\frac{t_0}{1-b}f(p_0) + \frac{1-b-t_0}{1-b}f(p_1)\right) + b\left(\frac{t_0+t_1+b-1}{b}f(p_1) + \sum_{i=2}^{n}\frac{t_i}{b}f(p_i)\right) \\ &= \sum_{i=0}^{n} t_i f(p_i)\,. \end{aligned}$$

□

Sia V uno spazio affine, denotiamo con $\mathcal{L}$ l'insieme di tutte le rette affini in V e con $\sim$ la relazione di parallelismo in $\mathcal{L}$, ossia $L_1 \sim L_2$ se e solo se esiste $v \in V$ tale che $L_2 = v + L_1$. Notiamo che, fissato un punto $p \in V$, le rette affini passanti per p formano un insieme di rappresentanti per la relazione di equivalenza $\sim$, e cioè per ogni retta affine in $L \subset V$ esiste un'unica retta L' passante per p e parallela a L. Chiameremo il quoziente $\mathcal{L}/\sim$ **iperpiano all'infinito** e l'unione

$$\hat{V} = V \cup (\mathcal{L}/\sim)$$

completamento proiettivo di V.

Sia $t_1, \ldots, t_n$ un sistema di coordinate su V. Possiamo allora considerare l'applicazione affine iniettiva

$$h\colon V \to \mathbb{K}^{n+1}, \qquad f(t_1, \ldots, t_n) = (1, t_1, \ldots, t_n).$$

L'applicazione h preserva la relazione di parallelismo e la sua immagine è il sottospazio affine $\{x_0 = 1\}$. Possiamo quindi identificare il completamento proiettivo di V con il completamento proiettivo di $\{x_0 = 1\}$.

Ogni retta affine in $\{x_0 = 1\}$ è parallela ad un unico sottospazio vettoriale di dimensione 1 di $\{x_0 = 0\}$. Ogni punto di $\{x_0 = 1\}$ è contenuto in un unico sottospazio vettoriale di dimensione 1 di $\mathbb{K}^{n+1}$. Esiste dunque una bigezione tra il completamento proiettivo di $\{x_0 = 1\}$ e l'insieme di tutte le rette per l'origine in $\mathbb{K}^{n+1}$.

Esercizi

Esercizio 28. Sia E un sottoinsieme di uno spazio vettoriale su di un campo diverso da $\mathbb{Z}/2$. 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 $au + (1-a)v \in E$.

Esercizio 29. Sia V uno spazio vettoriale su di un campo F. Provare che se F possiede almeno $n+1$ elementi, allora V non può essere unione di n sottospazi affini propri. In particolare uno spazio vettoriale su di un campo infinito non può essere 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 $L = \{tv + (1-t)h \mid t \in F\}$. Esiste allora un indice i tale che L interseca V_i in almeno due punti.)

Esercizio 30. Sia $f\colon V \to W$ una applicazione affine. Dimostrare che:

(1) Se $E \subset V$ è un sottospazio affine, allora $f(E)$ è un sottospazio affine.

(2) Se $H, K \subset V$ sono sottospazi affini della stessa dimensione e paralleli, allora $f(H), f(K)$ sono paralleli.

Esercizio 31. Sia $f\colon \mathbb{K}^n \to \mathbb{K}^m$ 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 $\mathbb{K}^n$.

Esercizio 32. Sia $H \subset \mathbb{K}^n$ un sottospazio affine non contenente 0 e $f\colon H \to \mathbb{K}^m$ un'applicazione affine. Dimostrare che f è la restrizione ad H di un'applicazione lineare $g\colon \mathbb{K}^n \to \mathbb{K}^m$.

Esercizio 33. Siano $P_1 = (1,2)$, $P_2 = (3,1)$, $P_3 = (3,3)$, $Q_1 = (1,8)$, $Q_2 = (0,7)$ e $Q_3 = (7,3)$. Si determini l'affinità di $\mathbb{R}^2$ in sé che trasforma P_i in Q_i per $i = 1, 2, 3$.

24. 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

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

L'insieme $\mathbb{P}(V)$ è in bigezione naturale con l'insieme dei sottospazi vettoriali di dimensione 1 (rette per l'origine) di V.

Dato un vettore $v \in V - \{0\}$ si è soliti denotare con $[v] \in \mathbb{P}(V)$ la classe di equivalenza corrispondente.

Chiameremo $\mathbb{P}^n_{\mathbb{K}} = \mathbb{P}(\mathbb{K}^{n+1})$ **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 $\mathbb{P}^n_{\mathbb{K}}$. 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 e $S \subset \mathbb{P}(V)$ è un sottoinsieme, si definisce

$$\mathbb{P}(M) = \{[v] \mid v \in M - \{0\}\} \subset \mathbb{P}(V) \quad \text{ e } \quad C(S) = \{v \in V - \{0\} \mid [v] \in S\} \cup \{0\}.$$

Il sottoinsieme $C(S) \subset V$ viene detto **cono affine** di S; 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 vettoriale, chiameremo $\mathbb{P}(W)$ **sottospazio proiettivo** di $\mathbb{P}(V)$. Si noti che ogni punto di uno spazio proiettivo è un sottospazio: $[v] = \mathbb{P}(\mathbb{K}\, v)$.

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.

Definizione 24.1 (Inviluppo di sottospazi proiettivi)**.** Se $W_1, W_2, \dots, W_n \subset V$ sono sottospazi vettoriali scriveremo

$$\mathbb{P}(W_1) + \mathbb{P}(W_2) + \cdots + \mathbb{P}(W_n) = \mathbb{P}(W_1 + W_2 + \cdots + W_n).$$

In altri termini, se $H_1, \dots, H_n \subset \mathbb{P}(V)$ sono sottospazi proiettivi, allora $H_1 + \cdots + H_n$, è il più piccolo sottospazio proiettivo di $\mathbb{P}(V)$ che li contiene.

Dati due punti $p, q \in \mathbb{P}(V)$ scriveremo anche $\overline{pq}$ per indicare l'inviluppo proiettivo $p + q$.

Se vale $p_1 = [v_1]$, $p_2 = [v_2]$,..., $p_n = [v_n]$, con $v_1, \dots, v_n \in V - \{0\}$, allora

$$p_1 + p_2 + \cdots + p_n = \mathbb{P}(\text{Span}(v_1, \dots, v_n)).$$

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 l'insieme vuoto $\emptyset = \mathbb{P}(0)$ avrà dimensione -1 quando viene considerato come uno spazio proiettivo.

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**.

Si noti che due punti $p = [v]$ e $q = [w]$ in uno spazio proiettivo sono distinti se e solo se i vettori v, w sono linearmente indipendenti. Tre punti $p = [v]$, $q = [w]$ e $r = [u]$ sono allineati se e solo se in tre vettori u, v, w sono linearmente dipendenti, ossia se e solo se $\mathrm{Span}(u, v, w)$ ha dimensione ≤ 2.

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

$$\dim(H \cap K) + \dim(H + K) = \dim H + \dim K$$

e quindi H e K sono sghembi se e solo se $\dim(H + K) = \dim H + \dim K + 1$.

Sia $f\colon V \to W$ un isomorfismo lineare di spazi vettoriali. In particolare $f(v) = 0$ se e solo se $v = 0$ ed è ben definita la fattorizzazione al quoziente

$$[f]\colon \mathbb{P}(V) \to \mathbb{P}(W), \qquad [v] \mapsto [f(v)]\,.$$

È chiaro che $[f]$ è bigettiva, trasforma sottospazi proiettivi in sottospazi proiettivi della stessa dimensione e preserva le relazioni di incidenza, concorrenza, allineamento, complanarità ecc.

Definizione 24.2. Un'applicazione $\phi\colon \mathbb{P}(V) \to \mathbb{P}(W)$ si dice un **isomorfismo proiettivo** o **proiettività** se è indotta per passaggio al quoziente da una applicazione lineare invertibile $f\colon V \to W$ mediante la regola

$$\phi([v]) = [f(v)], \qquad v \in V - \{0\},$$

e scriveremo in tal caso $\phi = [f]$.

Ogni proiettività è bigettiva e la sua inversa è ancora una proiettività. Più precisamente, se $\phi = [f]$, allora $\phi^{-1} = [f^{-1}]$.

La geometria proiettiva si occupa di studiare i luoghi geometrici (configurazioni, chiusi di Zariski, varietà ecc.) contenuti in uno spazio proiettivo, a meno di isomorfismi proiettivi. Per il momento ci occuperemo solamente di configurazioni, ossia di famiglie finite di sottospazi proiettivi che soddisfano alcune relazioni di incidenza, allineamento eccetera.

Esempio 24.3. Siano V, W due spazi vettoriali della stessa dimensione e siano $H \subset V$ e $K \subset W$ due sottospazi della stessa dimensione. Allora esiste una proiettività $\psi\colon \mathbb{P}(V) \to \mathbb{P}(W)$ tale che $\psi(\mathbb{P}(H)) = \mathbb{P}(K)$. A tal fine basta considerare $\psi = [f]$, con $f\colon V \to W$ un qualunque isomorfismo lineare tale che $f(H) = K$.

In particolare, se V ha dimensione $n+1$, la scelta di una base di V, ossia di un isomorfismo $\mathbb{K}^{n+1} \to V$ induce un isomorfismo proiettivo $\mathbb{P}^n \simeq \mathbb{P}(V)$. Lo stesso accade per qualunque scelta di un sistema di coordinate, ossia di una base di $V^\vee$, ossia di un isomorfismo lineare $V \to \mathbb{K}^{n+1}$.

Esempio 24.4. Siano $H \subset \mathbb{P}(V)$ un iperpiano e $W \subset \mathbb{P}(V)$ un sottospazio proiettivo di dimensione m. Se W non è contenuto in H allora $H + W = \mathbb{P}(V)$ e per la formula di Grassmann $\dim H \cap W = m - 1$.

Per ogni punto $p \in W - H = \{q \in W \mid q \notin H\}$ si ha $p + (H \cap W) = W$. Infatti $p + (H \cap W) \subset W$ (i due sottospazi p e $W \cap H$ sono entrambi contenuti in W) e per Grassmann $\dim(p + (H \cap W)) = 1 + (m - 1) = \dim W$.

Sia $\mathbb{K}$ un campo finito con q elementi se V è uno spazio vettoriale di dimensione $n + 1$, allora $\mathbb{P}(V)$ è isomorfo a $\mathbb{P}^n$ e quindi il numero di punti di $\mathbb{P}(V)$, e più in generale il numero di sottospazi proiettivi di dimensione fissata, dipende solo da n e $\mathbb{K}$. La prossima proposizione fornisce un metodo di calcolo di tale quantità.

Proposizione 24.5. *Sia $\mathbb{K}$ un campo finito con q elementi e si consideri il polinomio*

$$\frac{1}{t}\left(\prod_{i=0}^{n}(1+tq^i)-1\right)=\sum_{p=0}^{n}a_p^n t^p\in\mathbb{Z}[t]\,.$$

Allora per ogni $0\leq p\leq n$ il numero s_p^n dei sottospazi proiettivi di dimensione p contenuti in $\mathbb{P}^n_{\mathbb{K}}$ è uguale a $s_p^n=\dfrac{a_p^n}{\prod_{i=0}^{p}q^i}$.

Dimostrazione. È istruttivo trattare prima il caso $p=0$, ossia calcolare quanti punti contiene lo spazio proiettivo di dimensione n. Siccome

$$\frac{1}{t}\left(\prod_{i=0}^{n}(1+tq^i)-1\right)=\sum_{i=0}^{n}q^i+t(\cdots)$$

dimostriamo per induzione su n che $\mathbb{P}^n_{\mathbb{K}}$ contiene $1+q+\cdots+q^n$ punti. Per l'ipotesi induttiva ogni iperpiano H di $\mathbb{P}^n_{\mathbb{K}}$ contiene $1+q+\cdots+q^{n-1}$ punti; basta adesso osservare che $\mathbb{P}^n_{\mathbb{K}}-H$ è lo spazio affine $\mathbb{K}^n$ che contiene q^n punti. Similmente la proposizione è vera per $p=n$: si verifica immediatamente che $a_n^n=\prod_{i=0}^{n}q^i$.

Consideriamo adesso il caso generale. Per ogni coppia di interi $-1\leq p\leq n$ indichiamo con s_p^n il numero di sottospazi proiettivi di $\mathbb{P}^n$ di dimensione p. Vale allora la formula ricorsiva

$$s_{-1}^n=s_n^n=1,\qquad s_p^n=s_p^{n-1}+q^{n-p}s_{p-1}^{n-1},\quad 0\leq p<n\,.$$

Infatti se $0\leq p\leq n-1$ e scriviamo $\mathbb{P}^n=\mathbb{K}^n\cup\mathbb{P}^{n-1}$ (parte affine unito iperpiano all'infinito), i sottospazi di dimensione p si dividono in due classi disgiunte: quelli contenuti nell'iperpiano all'infinito, che sono s_p^{n-1}, e quelli del tipo $a+H$, con $a\in\mathbb{K}^n$ e $H\subset\mathbb{P}^{n-1}$ di dimensione $p-1$. I punti $a\in\mathbb{K}^n$ sono q^n, ma $a+H=b+H$ se e solo se $b\in(a+H)\cap\mathbb{K}^n$. Basta adesso osservare che $(a+H)\cap\mathbb{K}^n$ è il complementare di un iperpiano in $\mathbb{P}^p$ e quindi contiene q^p punti.

D'altra parte, siccome

$$\frac{1}{t}\prod_{i=0}^{n}(1+tq^i)=\frac{1}{t}+\sum_{p=0}^{n}a_p^n t^p=\left(\frac{1}{t}+\sum_{p=0}^{n-1}a_p^{n-1}t^p\right)(1+tq^n)$$

si hanno le formule ricorsive

$$a_p^n=a_p^{n-1}+q^n a_{p-1}^{n-1},\qquad 0\leq p\,,$$

e dividendo per $\prod_{i=0}^{p}q^i$ si ottiene

$$\frac{a_p^n}{\prod_{i=0}^{p}q^i}=\frac{a_p^{n-1}}{\prod_{i=0}^{p}q^i}+q^{n-p}\frac{a_{p-1}^{n-1}}{\prod_{i=0}^{p-1}q^i}\,.$$

La conclusione segue dunque dal principio di definizione ricorsiva. □

Esercizi

Esercizio 34. Se H,K sono sottospazi non vuoti di uno spazio proiettivo allora

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

Esercizio 35. 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.

Esercizio 36. Nella situazione della Proposizione 24.5, provare che

$$s_p^n=\sum_{S}q^{\sum_{i=0}^{p}a_i},\quad\text{dove}\quad S=\left\{(a_0,\ldots,a_p)\in\mathbb{N}^{p+1}\mid a_0\leq a_1\leq\cdots\leq a_p\leq n-p\right\}\,,$$

ed in particolare che il numero di rette in $\mathbb{P}^n_{\mathbb{K}}$ è uguale a

$$s_1^n=\sum_{0\leq i\leq j\leq n-1}q^{i+j}\,.$$

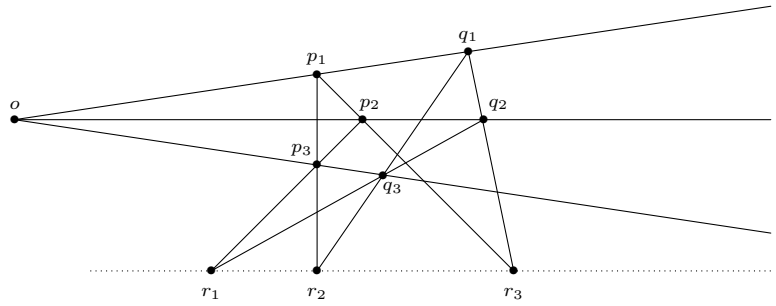


FIGURA 18. Il teorema di Desargues.

25. Il teorema di Desargues

Per la formula di Grassmann, due rette in $\mathbb{P}^2$ sono sempre incidenti. Se $p = [u] \neq q = [v]$, $r = [w] \neq s = [z]$ si ha

$$\overline{pq} \cap \overline{rs} = \mathbb{P}(\mathrm{Span}(u, v) \cap \mathrm{Span}(w, z)) \,,$$

e quindi bisogna trovare le soluzioni non banali del sistema lineare (3 equazioni e 4 incognite)

$$x_0 u + x_1 v = y_0 w + y_1 z \,.$$

Ad esempio, se $p = [1, 0, 0]$, $q = [0, 1, 0]$, $r = [0, 0, 1]$ e $s = [1, 1, 1]$, siccome

$$(1, 1, 0) = (1, 0, 0) + (0, 1, 0) = -(0, 0, 1) + (1, 1, 1)$$

si ha che $\overline{pq} \cap \overline{rs} = [1, 1, 0]$.

La comprensione del teorema di Pappo (III secolo D.C.) e di un teorema scoperto dal matematico francese Girard Desargues nel 1639 è stata una delle principali motivazioni dello sviluppo, nel XIX secolo, della geometria proiettiva.

Teorema 25.1 (Desargues)**.** *Siano dati 7 punti distinti $o, p_1, p_2, p_3, q_1, q_2, q_3 \in \mathbb{P}^2$ tali che ciascuna delle tre terne (o, p_1, q_1), (o, p_2, q_2) e (o, p_3, q_3) sia formata da tre punti allineati. Allora i tre punti*

$$r_1 = \overline{p_2 p_3} \cap \overline{q_2 q_3}, \quad r_2 = \overline{p_1 p_3} \cap \overline{q_1 q_3}, \quad r_3 = \overline{p_1 p_2} \cap \overline{q_1 q_2},$$

sono allineati (Figura 18).

Dimostrazione. Sia $\mathbb{P}^2 = \mathbb{P}(V)$, con V spazio vettoriale di dimensione 3 e scegliamo 7 vettori $u, v_1, v_2, v_3, w_1, w_2, w_3 \in V - \{0\}$ tali che

$$o = [u], \quad p_i = [v_i], \quad q_i = [w_i].$$

Per ipotesi o appartiene alla retta $\overline{p_1 q_1}$. Questo equivale a dire che u è una combinazione lineare di v_1 e w_1: diciamo $u = a_1 v_1 + b_1 w_1$. Similmente si ha

$$u = a_1 v_1 + b_1 w_1 = a_2 v_2 + b_2 w_2 = a_3 v_3 + b_3 w_3.$$

Da tali uguaglianze deduciamo che

$$a_1 v_1 - a_2 v_2 = b_2 w_2 - b_1 w_1, \quad a_2 v_2 - a_3 v_3 = b_3 w_3 - b_2 w_2, \quad a_1 v_1 - a_3 v_3 = b_3 w_3 - b_1 w_1.$$

da cui segue

$$r_3 = [a_1 v_1 - a_2 v_2], \quad r_1 = [a_2 v_2 - a_3 v_3], \quad r_2 = [a_1 v_1 - a_3 v_3].$$

I tre punti r_1, r_2 ed r_3 sono allineati poiché

$$(a_1 v_1 - a_2 v_2) + (a_2 v_2 - a_3 v_3) + (a_1 v_1 - a_3 v_3) = 0.$$

□

Osservazione 25.2. Il teorema di Desargues ha senso anche se esiste un indice i tale che $p_i = q_i$, ed in tal caso la sua validità è evidente perché se ad esempio $p_1 = q_1$ allora $r_2 = r_3 = p_1 = q_1$, mentre l'ennunciato perde di significato se $p_i = q_i$ per almeno due indici i.

26. Sistemi di riferimento e coordinate omogenee

Definizione 26.1. 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, due punti in $\mathbb{P}^1$ sono proiettivamente indipendenti se e solo se sono distinti; 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 26.2. 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 26.3. *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 $p_{n+1} = [e_0 + e_1 + \cdots + e_n]$.*

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 $p_{n+1} = [e_0 + e_1 + \cdots + e_n]$ sono 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 $e_{n+1} = a_0 v_0 + \cdots + a_n v_n$. Se fosse $a_i = 0$ per qualche indice i, allora gli $n+1$ vettori

$$v_0, \dots, v_{i-1}, e_{n+1}, v_{i+1}, \dots, v_n$$

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 $e_i = a_i v_i$, $i = 0, \dots, n$. □

Per quadrilatero completo in $\mathbb{P}^n$ si intende la configurazione di una quaterna di punti a, b, c, d (i vertici) e delle 6 rette $\overline{ab}, \overline{ac}, \overline{ad}, \overline{bc}, \overline{bd}, \overline{cd}$ (i lati). Il quadrilatero di dice **non degenere** se tra i 4 punti non ne esistono 3 allineati.

Se $n = 2$, un quadrilatero completo è non degenere se e solo se i vertici formano un sistema di riferimento proiettivo.

Esempio 26.4. Siano $a, b, c, d \in \mathbb{P}^2$ i vertici di un quadrilatero completo non degenere. Allora i tre punti di intersezione delle coppie di lati opposti

$$p = \overline{ab} \cap \overline{cd}, \qquad q = \overline{ac} \cap \overline{bd}, \qquad r = \overline{ad} \cap \overline{bc}$$

sono distinti. Inoltre p, q, r sono allineati se e solo se il campo $\mathbb{K}$ ha caratteristica 2.

Infatti possiamo trovare coordinate proiettive tali che

$$a = [1,0,0], \quad b = [0,1,0], \quad c = [0,0,1], \quad d = [1,1,1],$$

da cui segue

$$p = [1,1,0], \quad q = [1,0,1], \quad r = [0,1,1],$$

ed il determinante

$$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} = -2$$

si annulla se e solo se il campo è di caratteristica 2.

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 $[a_0,\dots,a_n]=[b_0,\dots,b_n]$ se e solo se esiste $\lambda\in\mathbb{K}-\{0\}$ tale che $b_i=\lambda a_i$ per ogni i.

Lemma 26.5. *Siano $f,g\colon V\to W$ due applicazioni lineari iniettive e consideriamo le applicazioni*

$$\phi,\psi\colon \mathbb{P}(V)\to\mathbb{P}(W),\qquad \phi([v])=[f(v)],\quad \psi([v])=[g(v)]\,.$$

Allora vale $\phi=\psi$ se e solo se esiste $\lambda\in\mathbb{K}-\{0\}$ tale che $f=\lambda g$.

Dimostrazione. L'unica implicazione non banale è il "solo se". Supponiamo quindi $\phi=\psi$ e fissiamo una base $v_0,\dots,v_n$ di V. L'iniettività di g implica allora che i vettori $g(v_0),\dots,g(v_n)$ sono linearmente indipendenti.

Dalle relazioni $[f(v_i)]=[g(v_i)]$ si ricava che esistono $n+1$ scalari invertibili λ_i tali che

$$f(v_i)=\lambda_i g(v_i),\qquad i=0,\dots,n\,.$$

Siccome f,g sono univocamente determinate dai valori che assumono sulla base $v_0,\dots,v_n$, per concludere basta dimostrare che $\lambda_i=\lambda_j$ per ogni i,j. Dalla relazione

$$[f(v_0+\cdots+v_n)]=[g(v_0+\cdots+v_n)]$$

deduciamo che esiste un $\lambda\in\mathbb{K}-\{0\}$ tale che

$$f(v_0+\cdots+v_n)=\lambda g(v_0+\cdots+v_n)=\sum_i \lambda g(v_i)\,.$$

D'altra parte

$$f(v_0+\cdots+v_n)=\sum_i f(v_i)=\sum_i \lambda_i g(v_i)$$

e l'indipendenza lineare dei vettori $g(v_0),\dots,g(v_n)$ implica che $\lambda_i=\lambda$ per ogni indice i. □

Si denota $\mathrm{PGL}(V)$ il gruppo delle proiettività di $\mathbb{P}(V)$ in sé. Per definizione esiste un omomorfismo surgettivo di gruppi $\mathrm{GL}(V)\to\mathrm{PGL}(V)$ che, per il lemma precedente ha come nucleo i multipli dell'identità. Si indica anche $\mathrm{PGL}_n(\mathbb{K})=\mathrm{PGL}(\mathbb{K}^n)$, e quindi $\mathrm{PGL}_{n+1}(\mathbb{K})$ è il gruppo degli automorfismi proiettivi di $\mathbb{P}^n_{\mathbb{K}}$.

Proposizione 26.6. *Dati due sistemi di riferimento $p_0,\dots,p_{n+1}$ e $q_0,\dots,q_{n+1}$ di $\mathbb{P}^n$, esiste un'unica proiettività $\varphi\in\mathrm{PGL}_{n+1}(\mathbb{K})$ tale che $\varphi(p_i)=q_i$ per ogni i.*

Dimostrazione. L'esistenza segue immediatamente dal Lemma 26.3, mentre per 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 $f\colon\mathbb{K}^{n+1}\to\mathbb{K}^{n+1}$ lineare invertibile tale che $[f]p_i=p_i$ per ogni i. Allora esistono costanti $a_0,\dots,a_{n+1}\in\mathbb{K}$ tali che $f(e_i)=a_ie_i$ 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. □

Per $n=1$ possiamo scrivere $\mathbb{P}^1=\mathbb{K}\cup\{\infty\}$, dove $\mathbb{K}=\{[1,t]\mid t\in\mathbb{K}\}$ e $\infty=[0,1]$ (intuitivamente $[0,1]$ è il limite per $t\to\infty$ di $[1/t,1]=[1,t]$). Ogni proiettività ϕ di $\mathbb{P}^1$ in sé è rappresentata da $\phi([x_0,x_1])=[ax_0+bx_1,cx_0+dx_1]$, $ad\neq bc$, che, nella coordinata affine $t=x_1/x_0$ diventa

$$\phi(t)=\frac{cx_0+dx_1}{ax_0+bx_1}=\frac{c+dt}{a+bt},\qquad \text{con } ad-bc\neq 0\,.$$

Teorema 26.7 (Pappo)**.** *Siano $p_1,\dots,p_6$ punti distinti e non allineati di $\mathbb{P}^2$, divisi in due terne allineate p_1,p_3,p_5 e p_2,p_4,p_6 (Figura 19).*

Allora i tre punti

$$\overline{p_1p_2}\cap\overline{p_4p_5},\quad \overline{p_2p_3}\cap\overline{p_5p_6},\quad \overline{p_3p_4}\cap\overline{p_6p_1},$$

sono allineati.

Dimostrazione. Vediamo una prima dimostrazione che utilizza conteggi elementari ma piuttosto grezzi con le coordinate omogenee. Altre dimostrazioni più concettuali saranno date in seguito.

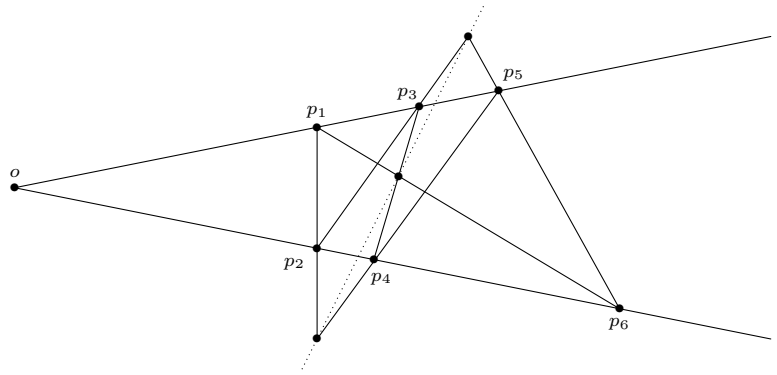


FIGURA 19. Il teorema di Pappo.

Siano L la retta contenente p_1, p_3, p_5 e M la retta contenente p_2, p_4, p_6. A meno di permutazioni cicliche degli indici non è restrittivo supporre che nessuno dei 4 punti $p_1, \dots, p_4$ sia uguale al punto o di intersezione di L e M.

Dunque $p_1, \dots, p_4$ sono un sistema di riferimento proiettivo ed esiste un sistema di coordinate omogenee tali che

$$p_1 = [1,0,0], \quad p_3 = [1,1,0], \quad p_2 = [0,0,1], \quad p_4 = [0,1,1]\,.$$

Dunque

$$o = [0,1,0], \quad p_5 = [a,1,0], \quad p_6 = [0,1,b], \qquad a,b \in \mathbb{K} - \{1\}\,,$$

e l'ipotesi $p_5 \neq p_6$ implica che a e b non possono essere contemporaneamente nulli. Si ha:

$$a(1,0,0) - (0,0,1) = -(0,1,1) + (a,1,0), \qquad \overline{p_1p_2} \cap \overline{p_4p_5} = [a,0,-1],$$
$$b(a-1)(0,0,1) + a(1,1,0) = (a,1,0) + (a-1)(0,1,b), \qquad \overline{p_2p_3} \cap \overline{p_5p_6} = [a,a,b(a-1)],$$
$$(1-b)(1,1,0) + b(0,1,1) = (0,1,b) + (1-b)(1,0,0), \qquad \overline{p_3p_4} \cap \overline{p_6p_1} = [1-b,1,b],$$

e l'allineamento dei tre punti segue, tenendo presente la commutatività del prodotto ($ab = ba$), dalla relazione:

$$(a,a,b(a-1)) = b(a,0,-1) + a(1-b,1,b)\,.$$

□

Esercizi

Esercizio 37. Determinare le proiettività di $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ in sé che preservano i seguenti sottoinsiemi di $\mathbb{C}$:

$$\mathbb{R} = \{x+iy \mid y = 0\}, \qquad H = \{x+iy \mid y > 0\}, \qquad \overline{H} = \{x+iy \mid y \geq 0\},$$
$$\Delta = \{x+iy \mid x^2+y^2 < 1\}, \qquad \overline{\Delta} = \{x+iy \mid x^2+y^2 \leq 1\}\,.$$

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

27. Proiezioni e prospettive

Iniziamo con l'osservare che per ogni proiettività $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ l'insieme dei suoi punti fissi si decompone nella forma

$$\operatorname{Fix}(\psi) = \{p \in \mathbb{P}^n \mid \psi(p) = p\} = H_1 \cup \cdots \cup H_h$$

dove gli H_i sono sottospazi proiettivi disgiunti e tali che $\sum_{i=1}^h (\dim H_i + 1) \leq n+1$. Infatti se ψ è indotta da un'applicazione lineare invertibile $f\colon \mathbb{K}^{n+1} \to \mathbb{K}^{n+1}$, allora i punti fissi di ψ corrispondono agli autovettori di f. Se $\lambda_1, \dots, \lambda_h \in \mathbb{K}$ sono gli autovalori di f, allora il luogo dei punti fissi di ψ coincide con l'unione dei sottospazi $H_i = \mathbb{P}(\ker(f - \lambda_i I))$. Tale unione è disgiunta in quanto ad ogni autovettore corrisponde un unico autovalore.

Lemma 27.1. *Sia $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ una proiettività e H, K due sottospazi proiettivi contenuti nel luogo dei punti fissi* $\mathrm{Fix}(\psi)$*. Se $H \cap K \neq \emptyset$, allora $H + K \subset \mathrm{Fix}(\psi)$.*

Dimostrazione. Siano $U, V \subset \mathbb{K}^{n+1}$ i due sottospazi vettoriali tali che $H = \mathbb{P}(U)$, $K = \mathbb{P}(V)$, e sia $f\colon \mathbb{K}^{n+1} \to \mathbb{K}^{n+1}$ un automorfismo lineare che induce ψ. Siccome $\psi_{|H}$ è l'identità esiste uno scalare non nullo $h \in \mathbb{K}$ tale che $f(u) = hu$ per ogni $u \in U$; similmente esiste $k \in \mathbb{K}$ tale che $f(v) = kv$ per ogni $v \in V$. Se $H \cap K \neq \emptyset$ allora $U \cap V$ contiene un vettore non nullo e questo implica $h = k$ ed allora $f(x) = hx = kx$ per ogni $x \in U + V$. □

Teorema 27.2. *Per una proiettività $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ le seguenti condizioni sono equivalenti:*

1. *i punti fissi di ψ contengono un iperpiano H;*
2. *esiste un punto $o \in \mathbb{P}^n$ tale che $\psi(o) = o$ e $\psi(p) \in \overline{op}$ per ogni $p \neq o$;*
3. *esiste un sistema di riferimento proiettivo $p_0, \dots, p_{n+1}$ tale che $\psi(p_0) = p_0$ e $\psi(p_i) \in \overline{p_0 p_i}$ per ogni $i = 1, \dots, n+1$.*

Inoltre, se $n > 1$ e $\psi \neq \mathrm{Id}$ soddisfa le precedenti condizioni, allora il punto o e l'iperpiano H sono unici e $\mathrm{Fix}(\psi) = H \cup \{o\}$.

Dimostrazione. Possiamo chiaramente supporre ψ diversa dall'identità.

[1 implica 2]: Osserviamo innanzitutto che la condizione 2) è del tutto equivalente a dire che $\psi(p) \in o + p$ per ogni $p \in \mathbb{P}^n$. Sia $\psi = [f]$ e fissiamo una base $v_0, \dots, v_n$ tale che $[v_i] \in H$ per ogni $i = 1, \dots, n$. La restrizione di ψ ad H è l'identità, quindi a meno di moltiplicare f per uno scalare possiamo supporre $f(v_i) = v_i$ per ogni $i > 0$. Se $f(v_0) = \sum_{i=0}^n a_i v_i$ consideriamo il punto $o = [f(v_0) - v_0]$. Allora per ogni vettore $w = \sum b_i v_i$ si ha

$$f(w) = b_0 f(v_0) + f(w - b_0 v_0) = b_0 f(v_0) + w - b_0 v_0 = b_0(f(v_0) - v_0) + w\,,$$

ed in particolare $f(w) \in \mathrm{Span}(f(v_0) - v_0, w)$.

[2 implica 3]: Basta estendere il punto o ad un sistema di riferimento proiettivo.

[3 implica 1]: Possiamo prendere una base $v_0, \dots, v_n$ di $\mathbb{K}^{n+1}$ tale che $p_i = [v_i]$ per ogni i e $p_{n+1} = [v_0 + \cdots + v_n]$. Siccome $\psi(p_0) = p_0$ esiste un unico isomorfismo lineare f che induce ψ e tale che $f(v_0) = v_0$. Per ipotesi esistono $a_i, b_i \in \mathbb{K}$, $i = 1, \dots, n+1$ tali che

$$f(v_i) = a_i v_0 + b_i v_i, \qquad i = 1, \dots, n$$

$$f(\sum v_i) = a_{n+1} v_0 + b_{n+1} \sum v_i\,.$$

Ponendo, per semplicità notazionale $b = b_{n+1}$ si ha

$$a_{n+1} v_0 + b \sum v_i = f(\sum v_i) = \sum f(v_i) = v_0 + \sum_{i=1}^n (a_i v_0 + b_i v_i)$$

e dato che $v_0, \dots, v_n$ sono linearmente indipendenti si ricava in particolare che $b_i = b \neq 0$ per ogni $i = 1, \dots, n$. In definitiva, ponendo $a_0 = 1 - b$ si ha:

$$f(v_i) = a_i v_0 + b v_i, \quad \text{per ogni} \quad i = 0, \dots, n\,,$$

e siccome abbiamo assunto ψ diversa dall'identità i coefficienti a_i non possono essere tutti nulli. Consideriamo adesso il seguente iperpiano $U = \ker(h) \subset \mathbb{K}^{n+1}$:

$$h\colon \mathbb{K}^{n+1} \to \mathbb{K}\,, \quad h(v_i) = a_i\,; \qquad U = \left\{ \sum x_i v_i \;\middle|\; \sum_{i=0}^n a_i x_i = 0 \right\}.$$

Allora per ogni $w = \sum x_i v_i \in U$ si ha

$$f(w) = \sum x_i (a_i v_0 + b v_i) = (\sum x_i a_i) v_0 + b \sum x_i v_i = bw\,,$$

ossia U è contenuto nell'autospazio dell'endomorfismo f relativo all'autovalore b e $H = \mathbb{P}(U)$ è un iperpiano contenuto in $\mathrm{Fix}(\psi)$.

Mostriamo adesso che se $n > 1$ e $\psi \neq \mathrm{Id}$ allora o ed H sono unici. L'unicità di H è facile: infatti se M è un altro iperpiano di punti fissi, siccome $n > 1$ si ha $H \cap M \neq \emptyset$ e quindi $\mathbb{P}^n = H + M \subset \mathrm{Fix}(\psi)$ per il Lemma 27.1.

Sia $q \neq o$ un punto tale che $\psi(q) = q$ e $\psi(p) \in \overline{pq}$ per ogni $p \neq q$. Allora possiamo completare o, q ad un sistema di riferimento proiettivo $o, q, p_1, \dots, p_n$. Siccome $n > 1$, per

ogni $i = 1, \dots, n$ i punti o, q, p_i non sono allineati e quindi le due rette $\overline{op_i}$ e $\overline{qp_i}$ si intersecano nell'unico punto p_i. Quindi

$$\psi(p_i) \in \overline{op_i} \cap \overline{qp_i} = \{p_i\}$$

da cui segue che ψ lascia fisso un sistema di riferimento proiettivo, ma questo è possibile solo se $\psi = \mathrm{Id}$.

Per finire, dimostriamo che se $n > 1$ e $\psi \neq \mathrm{Id}$ allora non esistono altri punti fissi oltre o ed H, ossia $\mathrm{Fix}(\psi) = H \cup \{o\}$. Sia q un punto fisso di ψ; se $q \notin H$ allora ogni retta L passante per q viene trasformata in se stessa da ψ. Infatti $L \not\subset H$ e quindi L interseca H in un unico punto, diciamo $r = L \cap H$, $r \neq q$. Allora $L = \overline{qr}$ e $\psi(L) = \overline{\psi(q)\psi(r)} = L$, in contraddizione con l'unicità del punto o. □

Definizione 27.3. Una proiettività $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ che soddisfa le tre condizioni equivalenti del Teorema 27.2 viene detta **prospettiva**.

Qualora $n > 2$ e ψ non sia l'identità, l'iperpiano H viene detto **asse di prospettiva** ed il punto o **centro di prospettiva**.

Osservando con un pizzico di attenzione la dimostrazione del Teorema 27.2 si osserva che entrambe le possibilità $o \notin H$ e $o \in H$ sono possibili. Più precisamente, se ψ è una prospettiva indotta da un endomorfismo lineare $f\colon V \to V$, allora vale $o \notin H$ se e solo se f è diagonalizzabile (1 autovalore di molteplicità geometrica n ed un altro di molteplicità geometrica 1), mentre vale $o \in H$ se e solo se f non è diagonalizzabile (1 autovalore di molteplicità algebrica $n+1$ e molteplicità geometrica n.)

Definizione 27.4. Una prospettiva di centro o ed asse H viene detta: **omologia**[9] se $o \notin H$; **trasvezione** od **omologia speciale** se $o \in H$.

Osservazione 27.5. Per quanto dimostrato in precedenza le nozioni di omologia e trasvezione sono ben definite per prospettive diverse dall'identità su spazi proiettivi di dimensione maggiore di 1. Tuttavia possiamo estendere in maniera ovvia tali nozioni anche a prospettive diverse dall'identità su $\mathbb{P}^1$: omologia se ha due punti fissi, trasvezione se ha un solo punto fisso. Siccome tre punti distinti di $\mathbb{P}^1$ formano un sistema di riferimento, l'unica proiettività con più di due punti fissi è l'identità.

Sia $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ una prospettiva di centro o e siano $L, M \subset \mathbb{P}^n$ due iperpiani tali che $o \notin M$ e $\psi(L) \subset M$. Allora la restrizione $\psi_{|L}\colon L \to M$ ha una evidente interpretazione geometrica. Osserviamo innanzitutto che $o \notin L$, altrimenti $o = \psi(o) \in M$, e quindi per ogni $p \in L$ abbiamo una retta $\overline{op}$ che interseca M in un unico punto. Possiamo quindi definire un'applicazione

$$\phi\colon L \to M, \qquad \phi(p) = \overline{op} \cap M\,,$$

detta **proiezione di centro** o (Figura 20). È quasi ovvio che $\phi = \psi_{|L}$, dato che per ogni $p \in L$ si ha $\psi(p) = \psi(L \cap \overline{op}) = M \cap \overline{op}$.

Mostreremo tra poco che che ogni proiezione $\psi\colon L \to M$ di centro $o \notin L \cup M \subset \mathbb{P}^n$ (L, M iperpiani), può essere descritta come restrizione di una opportuna prospettiva di centro o. Questo ha come immediata conseguenza il fatto che $\psi\colon L \to M$ è un isomorfismo proiettivo.

Possiamo dimostrare direttamente e facilmente questo fatto usando le coordinate.

Infatti, a meno di un cambio di coordinate omogenee possiamo supporre $o = [1, 0, \dots, 0]$ e $M = \mathbb{P}(\{x_0 = 0\})$. Siccome $o \notin L$ l'equazione di L sarà del tipo $x_0 = \sum_{i=1}^n a_i x_i$ e possiamo considerare l'isomorfismo proiettivo

$$\phi\colon \mathbb{P}^{n-1} \to L, \qquad [y_1, \dots, y_n] \mapsto [\sum a_i y_i, y_1, \dots, y_n]\,.$$

Ma allora la composizione $\psi\phi$ coincide con l'isomorfismo proiettivo

$$\psi\phi\colon \mathbb{P}^{n-1} \to M, \qquad [y_1, \dots, y_n] \mapsto [0, y_1, \dots, y_n]\,.$$

Siano $L, M \subset \mathbb{P}^n$ due iperpiani, $p, q \notin L \cup M$ due punti e

$$\phi_p,\ \phi_q\colon L \to M$$

[9] Nulla a che vedere con l'analogo concetto in topologia algebrica.

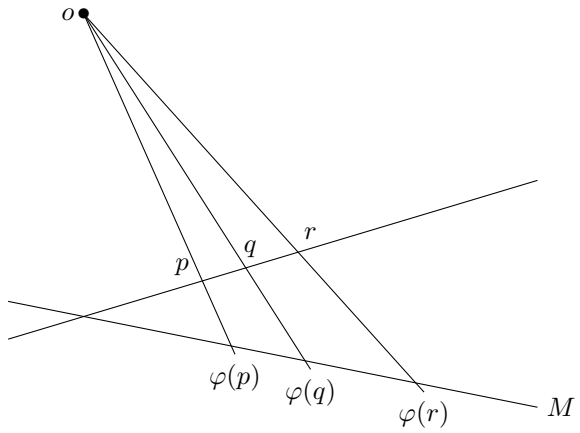


FIGURA 20. Proiezione $\varphi\colon L \to M$ di centro o.

le proiezioni di centro p e q rispettivamente. Allora l'applicazione

$$\psi = \phi_q \phi_p^{-1} \colon M \to M$$

è una prospettiva di centro $o = M \cap \overline{pq}$ ed asse $H = L \cap M$. Infatti H è un iperpiano di M di funti fissi di ψ e per ogni $r \in M$ il punto $\psi(r)$ appartiene all'intersezione di M con il piano $p + q + r$, ossia $\psi(r) \in \overline{or}$ (Figura 21).

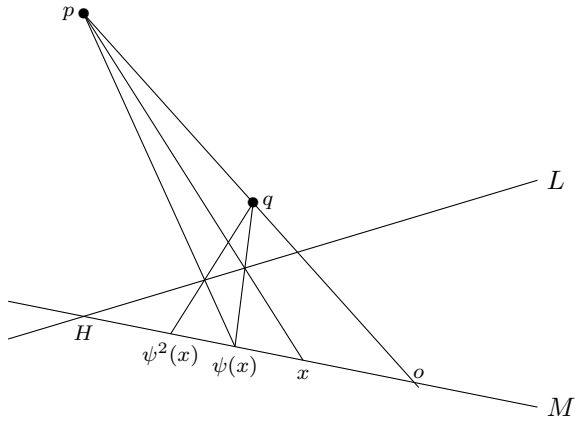


FIGURA 21. Una prospettiva $\psi\colon M \to M$ di centro o ed asse $H = L \cap M$, composizione della proiezione $M \to L$ di centro p e della proiezione $L \to M$ di centro q.

Lemma 27.6. *Siano $L, M \subset \mathbb{P}^n$ due iperpiani distinti ed $o \notin L \cup M$. Esiste allora una unica prospettiva $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ di centro o e tale che $\psi(L) = M$, $\psi(M) = L$. Inoltre:*

(1) *la prospettiva ψ è una involuzione, ossia $\psi^2 = Id$, ed è una omologia se e solo se il campo ha caratteristica $\neq 2$.*
(2) *le restrizioni $\psi\colon L \to M$ e $\psi\colon M \to L$ coincidono con le proiezioni di centro o.*

Dimostrazione. Fissiamo un sistema di coordinate omogenee $x_0, \dots, x_n$ tale che

$$o = [1, 0, \dots, 0], \qquad L \cap M = \{x_0 = x_1 = 0\}\,.$$

Le equazioni di L, M saranno allora del tipo

$$L = \{x_0 = l x_1\}, \qquad M = \{x_0 = m x_1\}, \qquad l, m \in \mathbb{K}\,,$$

mentre le prospettive di centro o sono tutte e sole le proiettività rappresentate da una matrice

$$f = \begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_n \\ 0 & b & 0 & \cdots & 0 \\ 0 & 0 & b & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b \end{pmatrix}, \qquad b \neq 0, \qquad a_1, \ldots, a_n \in \mathbb{K}\,.$$

Si considerino i due punti $p = [l, 1, 0, \ldots, 0] \in L$ e $q = [m, 1, 0, \ldots, 0] \in M$. Poiché

$$L = (L \cap M) + p, \qquad M = (L \cap M) + q,$$

le due condizioni $\psi(L) = M$, $\psi(M) = L$ sono equivalenti alle tre condizioni

$$\psi(L \cap M) \subset L \cap M, \qquad \psi(p) \in M, \qquad \psi(q) \in L\,.$$

La condizione $\psi(L \cap M) \subset L \cap M$ è equivalente all'annullamento $a_2 = \cdots = a_n = 0$, mentre le condizioni $\psi(p) \in M$ e $\psi(q) \in L$ equivalgono al sistema lineare nelle incognite a_1, b

$$l + a_1 = mb, \qquad m + a_1 = lb$$

che ha come unica soluzione $b = -1$ e $a_1 = -l - m$. La verifica che $f^2 = I$ è immediata. □

Corollario 27.7. *Dati tre punti distinti $o, p, q \in \mathbb{P}^1$ esiste una prospettiva ψ di centro o tale che $\psi(p) = q$ e $\psi(q) = p$.*

Lemma 27.8. *Sia $U \subset \mathbb{P}^n$ sottospazio proiettivo e $\psi\colon U \to U$ una prospettiva di centro o ed asse H. Allora ψ si estende ad una prospettiva $\phi\colon \mathbb{P}^n \to \mathbb{P}^n$ di centro o il cui asse contiene H.*

Dimostrazione. Se $U = \mathbb{P}(V)$ con $V \subset \mathbb{K}^{n+1}$, possiamo scegliere una base $v_0, \ldots, v_n$ tale che $v_0, \ldots, v_p$ sia una base di V e $v_1, \ldots, v_p$ base dell'asse di prospettiva. Possiamo allora rappresentare la prospettiva con $f\colon V \to V$ lineare e tale che $f(v_i) = v_i$ per $0 < i \leq p$. Basta allora estendere f ponendo $f(v_i) = v_i$ per ogni $i > 0$.

□

Teorema 27.9. *Sia ψ una proiettività di $\mathbb{P}^n$ e sia $H \subset \operatorname{Fix}(\psi)$ un sottospazio proiettivo di dimensione $r \leq n$. Allora ψ è composizione di $s \leq n - r$ prospettive i cui assi contengono H.*

Dimostrazione. Se $n - r \leq 1$ non c'è nulla da dimostrare, per induzione su r basta provare che esiste una prospettiva ϕ tale che $\phi^{-1}\psi$ contiene un sottospazio di punti fissi di dimensione $> r$. Scegliamo $p \notin \operatorname{Fix}(\psi)$ e denotiamo $q = \psi(p) \neq p$

Se $H = \emptyset$ per il Corollario 27.7 esiste una prospettiva ϕ della retta $\overline{pq}$ che tale che $\phi(p) = q$. Possiamo estendere ϕ ad una prospettiva di $\mathbb{P}^n$ e la proiettività $\phi^{-1}\psi$ possiede p come punto fisso.

Se $H \neq \emptyset$ denotiamo $L = H + p$, $\dim L = r + 1$. Se $q \in L$, allora $\psi(L) = L$ e la restrizione di ψ a L è una prospettiva che si può estendere ad una prospettiva ϕ di $\mathbb{P}^n$. Allora la proiettività $\phi^{-1}\psi$ contiene L come luogo di punti fissi.

Se $q \notin L$ allora $\overline{pq} \cap H = \emptyset$ scegliamo un qualunque punto $r \in H$, allora $q \notin \overline{rp}$, $\psi(\overline{rp}) = \overline{rq}$, le due rette $\overline{rp}$ e $\overline{rq}$ sono contenute nel piano P contenente i tre punti non allineati p, q, r. Poniamo $M = H + q$ e $K = H + P$. L ed M sono iperpiani di K che si intersecano in H.

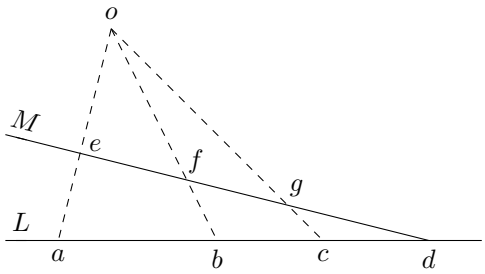
Scegliamo un punto $s \in \overline{rp}$ diverso da r, p e poniamo $t = \psi(s)$. Sia $o \in P$ il punto di intersezione delle rette $\overline{pq}$ e $\overline{st}$. Sia $\phi\colon K \to K$ una prospettiva di centro o e tale che $\phi(L) = M$ ed estendiamola ad una prospettiva su $\mathbb{P}^n$ di centro o ed asse contenente H. Necessariamente $\phi(p) = q$, $\phi(s) = t$ e quindi p, s, r sono punti fissi di $\phi^{-1}\psi$. Essendo p, s, r un sistema di riferimento in $\overline{pr}$, anche la retta $\overline{pr}$ è contenuta nel luogo fisso di $\phi^{-1}\psi$. Poiché $\overline{rp} \cap H \neq \emptyset$ ne segue che anche L è contenuto nel luogo fisso di $\phi^{-1}\psi$. □

Esempio 27.10. Siano a, b, c, d quattro punti distinti di una retta proiettiva L. Allora esiste una proiettività $\varphi\colon L \to L$ tale che

$$a\,b\,c\,d \xrightarrow{\varphi} b\,a\,d\,c\,,$$

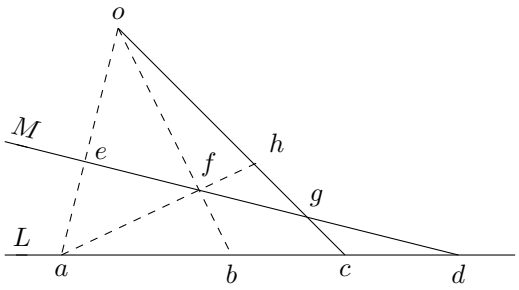
ossia $\varphi(a) = b$, $\varphi(b) = a$, $\varphi(c) = d$ e $\varphi(d) = c$. Siccome a, b, c a, b, d sono sistemi di riferimento proiettivi, ne segue che φ è unica e che φ^2 è uguale all'identità.

Un modo particolarmente carino di dimostrare tale fatto è quello di scrivere esplicitamente φ come composizione di 3 proiezioni. A tal fine consideriamo $L \subset \mathbb{P}^2$, sia $M \neq L$ una qualunque retta passante per d e sia $\alpha\colon L \to M$ una qualunque proiezione di centro $o \notin L \cup M$:



$$a\,b\,c\,d \xrightarrow{\alpha} e\,f\,g\,d\,,$$

Siano adesso $\beta\colon M \to \overline{oc}$ la proiezione di centro a e $\gamma\colon \overline{oc} \to L$ la proiezione di centro f. Allora



$$e\,f\,g\,d \xrightarrow{\beta} o\,h\,g\,c\,,$$

$$o\,h\,g\,c \xrightarrow{\gamma} b\,a\,d\,c\,.$$

In conclusione la proiettività $\varphi = \gamma\beta\alpha\colon L \to L$ scambia a con b e c con d. Per simmetria, esistono altresì due proiettività $\psi, \eta\colon L \to L$ tali che

$$a\,b\,c\,d \xrightarrow{\varphi} b\,a\,d\,c\,, \qquad a\,b\,c\,d \xrightarrow{\psi} c\,d\,a\,b\,, \qquad a\,b\,c\,d \xrightarrow{\eta} d\,c\,b\,a\,,$$

e vedremo più avanti che altre permutazioni di a, b, c, d sono ottenute per restrizione di una proiettività solamente in casi molto particolari.

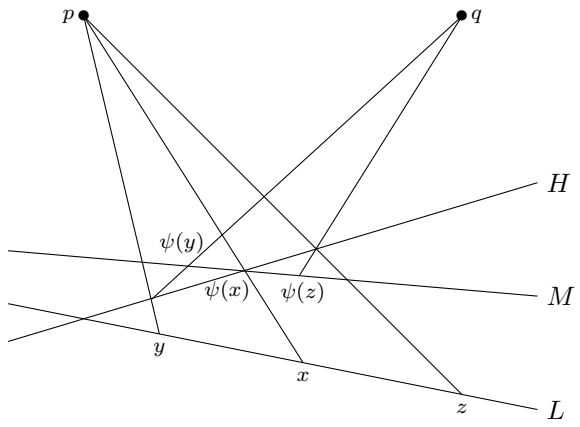
Teorema 27.11. *Sia $\psi\colon L \to M$ una proiettività tra due rette distinte di $\mathbb{P}^2$ e sia $o = L \cap M$ il loro punto di intersezione;*

(1) *se $\psi(o) = o$, allora ψ è una proiezione;*
(2) *se $\psi(o) \neq o$, allora ψ è composizione di due proiezioni.*

Dimostrazione. Se $\psi(o) = o$, estendiamo o ad un sistema di riferimento proiettivo $o, x, y \in L$ di L e sia p il punto di intersezione delle rette $\overline{x\psi(x)}$ e $\overline{y\psi(y)}$. Se $\varphi_p\colon L \to M$ è la proiezione di centro p, allora $\varphi_p(o) = o$, $\varphi_p(x) = \psi(x)$, $\varphi_p(y) = \psi(y)$ e questo implica che $\varphi_p = \psi$.

Se $\psi(o) \neq o$ fissiamo un sistema di riferimento proiettivo $x, y, z \in L$ tale che $\psi(x) \notin L \cap M$ e scegliamo una qualsiasi retta $H \subset \mathbb{P}^2$, diversa da M che contiene $\psi(x)$. Sia poi $p \notin L \cup H$ un punto allineato con $x, \psi(x)$ e consideriamo la proiezione $\varphi_p\colon L \to H$ di centro p. Allora $\varphi_p(x) = \psi(x)$ e per quanto visto prima esiste una proiezione $\varphi_q\colon H \to M$ tale che $\varphi_q\varphi_p(x) =$

$\psi(x)$, $\varphi_q\varphi_p(y) = \psi(y)$ e $\varphi_q\varphi_p(z) = \psi(z)$: quindi $\varphi_q\varphi_p = \psi$.



□

Corollario 27.12. *Sia $L \subset \mathbb{P}^2$ una retta proiettiva. Allora ogni proiettività $\psi\colon L \to L$ è composizione di al più tre proiezioni.*

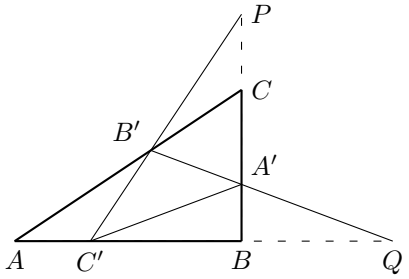
Dimostrazione. Sia $\varphi\colon M \to L$ una qualunque proiezione, con $M \neq L$. Per il teorema la proiettività $\varphi^{-1}\psi\colon L \to M$ è composizione di al più due proiezioni. □

Proposizione 27.13 (Steiner 1832)**.** *In $\mathbb{P}^2$ si consideri un triangolo non degenere ABC ed un triangolo (non degenere) $A'B'C'$ ad esso iscritto, ossia $A' \in \overline{BC}$, $B' \in \overline{CA}$, $C' \in \overline{AB}$. Siano:*

1. *$\varphi_A\colon \overline{C'A'} \to \overline{A'B'}$ la proiezione di centro A;*
2. *$\varphi_B\colon \overline{A'B'} \to \overline{B'C'}$ la proiezione di centro B;*
3. *$\varphi_C\colon \overline{B'C'} \to \overline{C'A'}$ la proiezione di centro C.*

Allora $\varphi_C\varphi_B\varphi_A = \mathrm{Id}$.

Dimostrazione. Basta dimostrare che $\psi := \varphi_C\varphi_B\colon \overline{A'B'} \to \overline{C'A'}$ è la proiezione di centro A. Siccome $A' = \overline{A'B'} \cap \overline{C'A'}$ e A', B, C sono allineati, ne segue che $\varphi_C\varphi_B(A') = \varphi_C(P) = A'$ e quindi $\varphi_C\varphi_B$ è una proiezione.



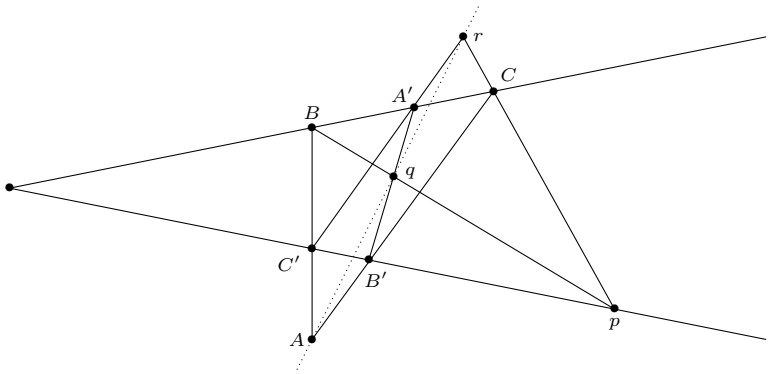
Inoltre se $Q = \overline{AB} \cap \overline{A'B'}$ si ha

$$\psi(B') = \varphi_C\varphi_B(B') = \varphi_C(B') \in \overline{B'C} = \overline{AB'},$$

$$\psi(Q) = \varphi_C\varphi_B(Q) = \varphi_C(C') = C' \in \overline{AB} = \overline{AQ}.$$

Ma le precedenti due relazioni impongono che il centro di prospettiva di ψ deve necessariamente essere A. □

Possiamo ridimostrare il teorema di Pappo come conseguenza della Proposizione 27.13. A tal fine riprendiamo la Figura 19 con i punti ridenominati nel modo seguente



Allora $\varphi_C\varphi_B(q) = \varphi_C(p) = r$, quindi $\varphi_A(q) = r$ ed in particolare A, q, r sono allineati.

Esercizi

Esercizio 38. Siano date n rette proiettive $L_1, \dots, L_n \subset \mathbb{P}^n$, nessuna delle quali contenuta nell'iperpiano $H_0 = \{x_0 = 0\}$. Scriviamo $\mathbb{P}^n = \mathbb{K}^n \cup H_0$, per ogni $i = 1, \dots, n$ esiste una rappresentazione parametrica della retta affine $L_i \cap \mathbb{K}^n$ 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 $\det(a_{ij}) \neq 0$.

Esercizio 39 $(*)$**.** Siano date quattro rette $L_1, \dots, L_4 \subset \mathbb{P}^3(\mathbb{C})$. 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 38.)

28. Il birapporto

Sia $\mathbb{P}(V)$ uno spazio proiettivo di dimensione 1. Abbiamo visto che per ogni terna di punti distinti p_2, p_3, p_4 di $\mathbb{P}(V)$ esiste un'unica proiettività $\phi\colon \mathbb{P}(V) \to \mathbb{P}^1$ tale che:

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

Nelle precedenti uguaglianze $[0, 1] = \infty$ e $[1, t] = t$, abbiamo identificato $\mathbb{P}^1$ con $\mathbb{K} \cup \{\infty\}$ nel modo standard, ossia tramite il processo di disomogeneizzazione $[x_0, x_1] \leftrightarrow x_1/x_0$.

È allora chiaro che dati quattro punti distinti $p_1, \dots, p_4 \in \mathbb{P}(V)$, esistono unici una proiettività $\phi\colon \mathbb{P}(V) \to \mathbb{P}^1$ ed un elemento $\lambda \in \mathbb{K} - \{0, 1\}$ tali che

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

Definizione 28.1. Nella situazione precedente, la quantità $\lambda = [p_1, p_2; p_3, p_4]$ si dice **birapporto**[10] della quaterna ordinata $p_1, \dots, p_4$.

È immediato osservare che per ogni $\lambda \in \mathbb{P}^1 = \mathbb{K} \cup \{\infty\}$, $\lambda \neq 0, 1, \infty$, allora $\lambda = [\lambda, 1; 0, \infty]$. In particolare, il birapporto può assumere qualsiasi valore in $\mathbb{K} - \{0, 1\}$.

Proposizione 28.2. *Siano $\mathbb{P}(V)$ e $\mathbb{P}(U)$ due rette proiettive e $p_1, \dots, p_4 \in \mathbb{P}(V)$, $q_1, \dots, q_4 \in \mathbb{P}(U)$ due quaterne di punti distinti. Allora esiste una proiettività $\phi\colon \mathbb{P}(V) \to \mathbb{P}(U)$ tale che $\phi(p_i) = q_i$ per ogni i se e solo se $[p_1, p_2; p_3, p_4] = [q_1, q_2; q_3, q_4]$.*

[10] In inglese *cross ratio*; in francese *rapport anharmonique*.

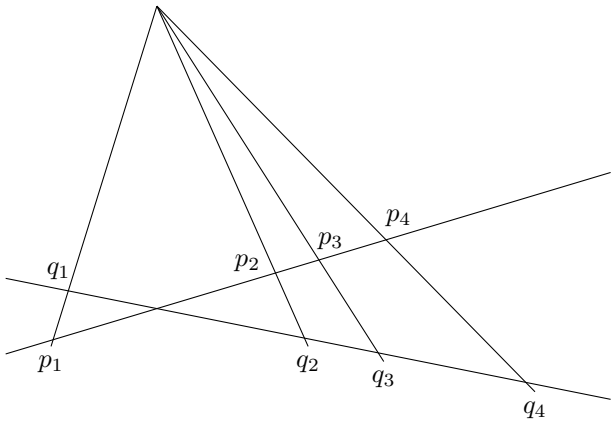


FIGURA 22. Le due quaterne p_1, p_2, p_3, p_4 e q_1, q_2, q_3, q_4 hanno lo stesso birapporto.

Dimostrazione. Siano $\eta\colon \mathbb{P}(V) \to \mathbb{P}^1$ e $\mu\colon \mathbb{P}(U) \to \mathbb{P}^1$ le uniche proiettività tali che

$$\eta(p_2) = \mu(q_2) = 1, \qquad \eta(p_3) = \mu(q_3) = 0, \qquad \eta(p_4) = \mu(q_4) = \infty\,.$$

Allora $\phi = \mu^{-1}\eta\colon \mathbb{P}(V) \to \mathbb{P}(U)$ coincide con l'unica proiettività tale che $\phi(p_i) = q_i$, $i = 2, 3, 4$.

Ma allora $\phi(p_1) = q_1$ se e solo se $\eta(p_1) = \mu(q_1)$, ossia se e solo se le due quaterne hanno lo stesso birapporto. □

Dunque il birapporto è invariante per proiettività e quindi è invariante per prospettive e proiezioni (Figura 22).

Il nome birapporto è motivato dalla formula

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

da interpretarsi come nella seguente proposizione.

Proposizione 28.3. *Siano $p_1 = [x_1, y_1], \ldots, p_4 = [x_4, y_4]$ punti distinti di $\mathbb{P}^1$. Allora vale la formula*

$$[p_1, p_2; p_3, p_4] = \frac{\begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}}{\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}} : \frac{\begin{vmatrix} x_1 & x_4 \\ y_1 & y_4 \end{vmatrix}}{\begin{vmatrix} x_2 & x_4 \\ y_2 & y_4 \end{vmatrix}} = \frac{x_1y_3 - x_3y_1}{x_2y_3 - x_3y_2} : \frac{x_1y_4 - x_4y_1}{x_2y_4 - x_4y_2}\,, \tag{28.1}$$

che nelle coordinate affini $t_i = \dfrac{y_i}{x_i} \in \mathbb{K} \cup \{\infty\}$, diventa

$$[p_1, p_2; p_3, p_4] = \frac{t_3 - t_1}{t_3 - t_2} : \frac{t_4 - t_1}{t_4 - t_2}\,. \tag{28.2}$$

Dimostrazione. Osserviamo preliminarmente che la Formula (28.1) è ben definita, ossia è invariante per moltiplicazione della coppia x_i, y_i per uno scalare non nullo, ed applicata alla quaterna

$$p_1 = [1, \lambda], \quad p_2 = [1, 1], \quad p_3 = [1, 0], \quad p_4 = [0, 1],$$

restituisce il valore $[p_1, p_2; p_3, p_4] = \lambda$. Basta quindi provare che la Formula (28.1) è invariante per proiettività.

Sia $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ una proiettività indotta da una matrice invertibile $A \in \mathrm{GL}_2(\mathbb{K})$. Per ogni indice i si ha

$$\phi(p_i) = [z_i, w_i], \qquad \text{con} \quad A \begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} z_i \\ w_i \end{pmatrix}\,.$$

Per il teorema di Binet, per ogni coppia di indici i, j si ha:

$$A\begin{pmatrix} x_i & x_j \\ y_i & y_j \end{pmatrix} = \begin{pmatrix} z_i & z_j \\ w_i & w_j \end{pmatrix}, \qquad \det(A)\begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} = \begin{vmatrix} z_i & z_j \\ w_i & w_j \end{vmatrix},$$

e di conseguenza

$$\frac{\begin{vmatrix} z_1 & z_3 \\ w_1 & w_3 \end{vmatrix}}{\begin{vmatrix} z_2 & z_3 \\ w_2 & w_3 \end{vmatrix}} : \frac{\begin{vmatrix} z_1 & z_4 \\ w_1 & w_4 \end{vmatrix}}{\begin{vmatrix} z_2 & z_4 \\ w_2 & w_4 \end{vmatrix}} = \frac{\begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}}{\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}} : \frac{\begin{vmatrix} x_1 & x_4 \\ y_1 & y_4 \end{vmatrix}}{\begin{vmatrix} x_2 & x_4 \\ y_2 & y_4 \end{vmatrix}}.$$

□

Definizione 28.4. Denotiamo con Σ_4 il gruppo delle permutazioni dell'insieme $\{1, 2, 3, 4\}$. Il **gruppo trirettangolo**[11] Γ_4 è il sottogruppo di Σ_4 formato dall'identità e dalle tre permutazioni[12] di ordine 2

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

Il birapporto di una quaterna dipende dall'ordine in cui vengono presi i punti. Tuttavia segue immediatamente dalle Formule (28.1) e (28.2) che per ogni quaterna di punti distinti $p_1, \dots, p_4$ si ha:

$$[p_1, p_2; p_3, p_4] = [p_2, p_1; p_4, p_3] = [p_3, p_4; p_1, p_2] = [p_4, p_3; p_2, p_1].$$

Possiamo esprimere questo fatto dicendo che *il birapporto è invariante per l'azione del gruppo trirettangolo.*

Più in generale è naturale chiedersi come agisce Σ_4 sul birapporto: in altri termini, data una permutazione $\sigma \in \Sigma_4$, siamo interessati alla relazione esistente tra i due birapporti $[p_1, p_2; p_3, p_4]$ e $[p_{\sigma(1)}, p_{\sigma(2)}; p_{\sigma(3)}, p_{\sigma(4)}]$.

Siccome ogni permutazione σ si scrive in modo unico nella forma $\gamma\tau$, con $\gamma \in \Gamma_4$, $\gamma(4) = \sigma(4)$ e $\tau(4) = 4$, basta vedere come cambia il birapporto per effetto delle 6 permutazioni che fissano il numero 4.

Lemma 28.5. *Sia $\lambda = [p_1, p_2; p_3, p_4]$ il birapporto di una quaterna di punti distinti sulla retta proiettiva. Allora si hanno le 6 uguaglianze:*

$$\begin{array}{lll} [p_1, p_2; p_3, p_4] = \lambda & [p_2, p_3; p_1, p_4] = \dfrac{\lambda - 1}{\lambda} & [p_3, p_1; p_2, p_4] = \dfrac{1}{1 - \lambda} \\ [p_2, p_1; p_3, p_4] = \dfrac{1}{\lambda} & [p_3, p_2; p_1, p_4] = \dfrac{\lambda}{\lambda - 1} & [p_1, p_3; p_2, p_4] = 1 - \lambda \end{array}.$$

Dimostrazione. La dimostrazione non presenta alcuna difficoltà, anche perché possiamo sempre trovare un sistema di coordinate affini tali che

$$p_1 = \lambda, \quad p_2 = 1, \quad p_3 = 0, \quad p_4 = \infty.$$

□

Possiamo riassumere le precedenti considerazioni nel seguente risultato:

Lemma 28.6. *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*

$$\lambda, \quad \frac{1}{\lambda}, \quad 1 - \lambda, \quad 1 - \frac{1}{\lambda}, \quad \frac{1}{1 - \lambda}, \quad \frac{\lambda}{\lambda - 1}. \tag{28.3}$$

Per un generico $\lambda \in \mathbb{K} - \{0, 1\}$ le sei espressioni in (28.3) 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**.

[11] In inglese *Klein fourgroup*.

[12] Con la notazione $\sigma = (a_1, \dots, a_n)$ si intende la permutazione tale che $\sigma(i) = a_i$.

(2) Caratteristica $\neq 3$, $\xi^2-\xi+1=0$ e $\lambda=\xi,\xi^{-1}$. In questo caso la quaterna è detta **equianarmonica**.

Lasciamo per esercizio la verifica delle seguenti affermazioni, la prima delle quali giustifica il termine di quaterna armonica:

(1) In caratteristica $\neq 2$, dati tre valori distinti $\lambda_1,\lambda_2,\lambda_3\in\mathbb{K}-\{0\}$ si ha $[0,\lambda_1;\lambda_2,\lambda_3]=-1$ se e solo se λ_1 è la media armonica di λ_2,λ_3, ossia se e solo se

$$\lambda_1=\frac{2}{\frac{1}{\lambda_2}+\frac{1}{\lambda_3}}=\frac{2\lambda_2\lambda_3}{\lambda_2+\lambda_3}\,.$$

In particolare per ogni $x\in\mathbb{K}$ si ha

$$\left[0,\frac{1}{x};\frac{1}{x-1},\frac{1}{x+1}\right]=\left[\frac{1}{x+1},\frac{1}{x-1};\frac{1}{x},0\right]=\left[\frac{1}{x+1},\frac{1}{x-1};0,\frac{1}{x}\right]=-1\,.$$

(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.

Teorema 28.7 (Quadrilatero armonico)**.** *Sia $\mathbb{P}^2$ il piano proiettivo su di un campo di caratteristica $\neq 2$, e siano $a,b,c,d\in\mathbb{P}^2$ i vertici di un quadrilatero completo non degenere, ossia con nessuna terna allineata. Allora i seguenti 4 punti allineati (Figura 23):*

$$p_1=\overline{ab}\cap\overline{cd},\quad p_2=\overline{ac}\cap\overline{bd},\quad p_3=\overline{p_1p_2}\cap\overline{bc},\quad p_4=\overline{p_1p_2}\cap\overline{ad}\,.$$

formano una quaterna armonica, e più precisamente $[p_1,p_2;p_3,p_4]=-1$.

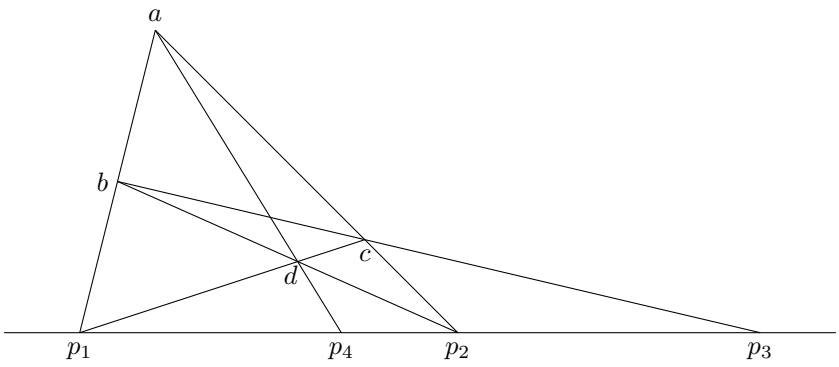


FIGURA 23. Il quadrilatero "armonico".

Dimostrazione. Sia $[p_1,p_2;p_3,p_4]=\lambda\neq 1,0$ e di conseguenza $[p_2,p_1;p_3,p_4]=\lambda^{-1}$. Si considerino adesso le due prospettive $\overline{p_1p_2}\to\overline{ad}$ di centro b e $\overline{ad}\to\overline{p_1p_2}$ di centro c. Se indichiamo con o il punto di intersezione di $\overline{ad}$ e $\overline{bc}$, dalla prima prospettiva ricaviamo che $[p_1,p_2;p_3,p_4]=[a,d;o,p_4]$ e dalla seconda che $[a,d;o,p_4]=[p_2,p_1;p_3,p_4]$. Quindi $[p_1,p_2;p_3,p_4]=[p_2,p_1;p_3,p_4]$ e dunque $\lambda=\lambda^{-1}$ che ha come unica soluzione $\lambda=-1$. □

Dati tre punti distinti p_1,p_2,p_3 di $\mathbb{P}^1$, possiamo applicare il il Teorema 28.7 per costruire "con la sola riga" l'unico punto p_4 tale che $[p_1,p_2;p_3,p_4]=-1$. Si consideri infatti $\mathbb{P}^1$ come una retta proiettiva $M\subset\mathbb{P}^2$ e per ogni $i=1,2,3$ si prenda una qualunque retta proiettiva

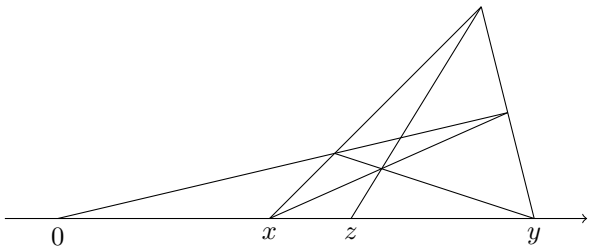
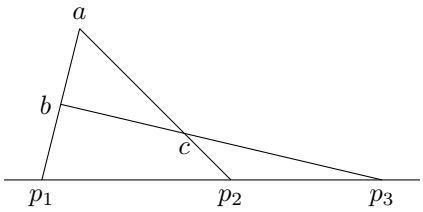
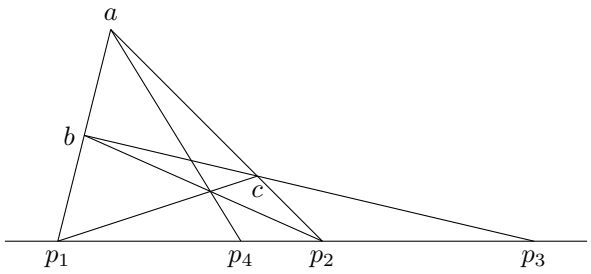


FIGURA 24. Il punto z è uguale alla media armonica di x e y.

L_i tale che $L_i \cap M = p_i$. Denotiamo $a = L_1 \cap L_2$, $b = L_1 \cap L_3$ e $c = L_2 \cap L_3$:

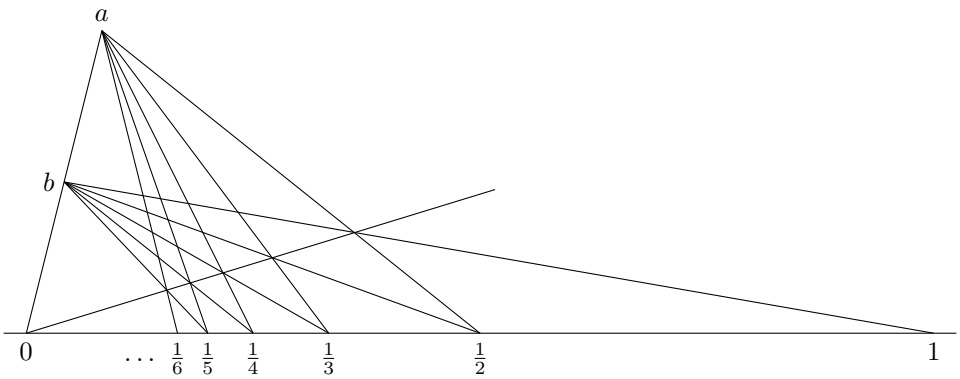


Adesso si definisca d come il punto di intersezione delle rette $\overline{p_1 c}$ e $\overline{p_2 b}$, allora il punto cercato p_4 è dato dall'intersezione di M con $\overline{ad}$:



La precedente costruzione si applica anche per calcolare graficamente la media armonica $z = \dfrac{2xy}{x+y}$ ossia l'unico numero tal che $[x, y; 0, z] = -1$ (Figura 24).

Siccome $\left[0, \frac{1}{n}; \frac{1}{n-1}, \frac{1}{n+1}\right] = -1$ per ogni intero positivo n, la precedente costruzione dà un metodo "con sola riga" per costruire la serie armonica partendo da $0, 1, \frac{1}{2}$, e ben raffigurato dal seguente disegnino,



nel quale, ribadiamo, la scelta delle tre rette $\overline{0a}$, $\overline{\frac{1}{2}a}$ e $\overline{1b}$ è arbitraria, dopo di che tutte le altre rette seguono in maniera univoca. Inoltre il disegno illustra la proiettività $\phi(x) = x/(x+1)$ di $\mathbb{P}^1$ (x=coordinata affine) come composizione di due proiezioni di centri b ed a rispettivamente.

Esercizi

Esercizio 40. 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 $\phi \in \mathrm{Aut}(\mathbb{P}^1)$ e $\phi(S) \subset S$, allora $\phi = Id$.

Esercizio 41. Sia $p \in \mathbb{P}^n$ e $G \subset \mathrm{Aut}(\mathbb{P}^n)$ il sottogruppo delle proiettività ϕ 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.

Esercizio 42. Sia $\lambda \in \mathbb{K} - \{0, 1\}$ fissato, $L \subset \mathbb{P}^2$ una retta e $\pi\colon \mathbb{P}^2 - \{o\} \to L$ la proiezione di centro $o \notin L$. Definiamo un'applicazione $\phi\colon \mathbb{P}^2 \to \mathbb{P}^2$ 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 $q \in o + p$ è l'unico punto tale che $[o, r; p, q] = \lambda$.
Provare che ϕ è una proiettività. Provare inoltre ϕ è un involuzione (cioè $\phi^2 = Id$) se e solo se $\lambda = -1$.

Esercizio 43. (Rapporti plurisezionali)
Sia $n \geq 2$ un intero e $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{P}^1$ tali che $b_i \neq a_{i+1}$; si definisce il rapporto n-sezionale come

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

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 $[a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n] = [a_1, a_2, \ldots, a_{n-1}; b_1, b_2, \ldots, b_{n-1}]$.

Se invece $a_1, \ldots, a_n \in \mathbb{P}^2$ e $b_i \in \overline{a_i a_{i+1}}$, con $b_i \neq a_{i+1}$ per ogni $i = 1, \ldots, n$, allora, fissato un punto $p \in \mathbb{P}^2$ non appartenente all'unione delle rette $\overline{a_i a_{i+1}}$ si definisce $[a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n]$ 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 $[a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n]$ come un prodotto di rapporti semplici.)

Esercizio 44 (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 $\overline{b_1 b_2}$ come retta all'infinito).

Esercizio 45 (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 $\overline{a_1 a_2}$).

Esercizio 46. Sia $\mathbb{K}$ algebricamente chiuso e $\phi \in \mathrm{Aut}(\mathbb{P}^1)$ una proiettività di ordine finito e non divisibile per la caratteristica di $\mathbb{K}$. Provare che ϕ ha esattamente due punti fissi.

Esercizio 47. (caratteristica $\neq 2$) Una quaterna ordinata $p_1, \ldots, p_4$ di punti distinti di $\mathbb{P}^1$ definisce un omomorfismo iniettivo di gruppi $h\colon \Gamma_4 \to \mathrm{PGL}(2, \mathbb{K}) = \mathrm{Aut}(\mathbb{P}^1)$ 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 $\Gamma_4 \to \mathrm{GL}(2, \mathbb{K})$. (Sugg.: non è restrittivo assumere $\mathbb{K}$ algebricamente chiuso; si prenda una coordinata affine tale che la quaterna sia $1, -1, a, -a$ con $a \neq \pm 1$.)

Esercizio 48. Trovare una elemento di ordine 2 di $\mathrm{PGL}(2, \mathbb{Q})$ che non si rappresenta con elementi di ordine finito di $\mathrm{GL}(2, \mathbb{Q})$.

Esercizio 49. 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 $\Gamma \subset \mathrm{PGL}(n, \mathbb{K})$ di ordine m esiste un sottogruppo finito $\Gamma' \subset \mathrm{GL}(n, \mathbb{K})$ di ordine $\leq hdm$ che si mappa surgettivamente su Γ tramite la proiezione naturale $\mathrm{GL}(n, \mathbb{K}) \to \mathrm{PGL}(n, \mathbb{K})$.

Esercizio 50. (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 $[p_1, \dots, p_4]$ è invariante per l'azione di un sottogruppo di ordine 8 di Σ_4. Dedurre che il gruppo simmetrico Σ_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 $[p_1, \dots, p_4]$ è invariante per l'azione del gruppo alterno A_4.

Esercizio 51. Si consideri l'applicazione $v_n \colon \mathbb{P}^1 \to \mathbb{P}^n$, 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*.

Esercizio 52. Si consideri il piano $\mathbb{R}^2$ con la metrica euclidea usuale, per ogni $p \in \mathbb{R}^2$ sia $F_p \cong \mathbb{P}^1_{\mathbb{R}}$ il fascio di rette passanti per il punto p. Verificare che l'applicazione $F_p \to F_p$ che manda ogni retta nella sua perpendicolare è una proiettività. Tale proiettività è chiamata *involuzione degli angoli retti*.

Esercizio 53. 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.

Esercizio 54 (∗)**.** Con l'utilizzo della sola riga dividere un rettangolo del piano euclideo in n parti uguali, per ogni $n \geq 2$. (Sugg.: quadrilatero armonico.)

Esercizio 55. Sia $p \in \mathbb{P}^2$, siano L, H, T tre rette distinte di $\mathbb{P}^2$ passanti per il punto p e $q, r \in T$ punti distinti da p. Si consideri le proiettività $\phi \colon L \to H$ e $\psi \colon H \to L$ ottenute per proiezione di centro q ed r rispettivamente. Detta $\eta \colon L \to L$ la composizione di ϕ e ψ calcolare il valore del birapporto $[p, s; \eta(s), \eta^2(s)]$ al variare di s in $L - \{p\}$.

29. Dualità

Definiamo lo spazio proiettivo duale $\mathbb{P}(V)^*$ 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 $V \to \mathbb{K}$. Esiste quindi una bigezione naturale $\mathbb{P}(V)^* = \mathbb{P}(V^*)$.

I sottospazi proiettivi di $\mathbb{P}(V)^*$ 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 $H^\perp \subset \mathbb{P}(V)^*$ 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 si hanno degli isomorfismo naturali

$$\mathbb{P}(V)^{**} = \mathbb{P}(V^*)^* = \mathbb{P}(V^{**}) = \mathbb{P}(V)$$

tramite i quali si ha $H^{\perp\perp} = H$ per ogni sottospazio proiettivo H.

Esercizio 56. Siano H, K sottospazi di uno spazio proiettivo di dimensione n. Definiamo il *difetto incidente* di H e K tramite la formula

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

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

Esercizio 57. Siano H,K sottospazi di uno spazio proiettivo di dimensione n. Definiamo il *difetto secante* di H e K come

$$\mathrm{DS}(H,K)=\dim H+\dim K+1-\dim(HK)$$

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

Qui finisce la seconda parte delle dispense

30. Polinomi numerici

Inizia la terza ed ultima parte delle dispense dedicata ad alcuni concetti base di geometria algebrica.

Per evitare eccessivi tecnicismi, non tutti i risultati sono dimostrati completamente: alcune dimostrazioni sono omesse, altre fatte sotto ipotesi aggiuntive ed altre ancora sostituite con argomenti euristici.

Sempre per semplicità espositiva, da questo momento in poi e salvo avviso contrario, con il simbolo $\mathbb{K}$ denoteremo sempre un campo *algebricamente chiuso*, sebbene alcuni molti risultati esposti siano validi per una classe di campi più estesa; in alcuni casi metteremo delle condizioni sulla caratteristica di $\mathbb{K}$.

Giova ricordare che ogni campo algebricamente chiuso $\mathbb{K}$ è infinito: infatti se contenesse un numero finito di elementi $a_1,\ldots,a_n$, allora il polinomio

$$p(t)=1+\prod_{i=1}^{n}(t-a_i)$$

non avrebbe radici in $\mathbb{K}$, contraddicendo la chiusura algebrica.

Supporremo che il lettore abbia conoscenza delle nozioni e delle principali proprietà dei campi e degli spazi proiettivi. Il simbolo $\mathbb{N}=\{0,1,\ldots\}$ denota l'insieme degli interi non negativi, mentre indicheremo con $\mathbb{Q},\mathbb{R},\mathbb{C}$ i campi dei numeri razionali, reali e complessi, rispettivamente. Infine, se X è un insieme finito, indichiamo con $|X|\in\mathbb{N}$ il suo numero di elementi.

Dati due interi non negativi $n,d\in\mathbb{N}$, il coefficiente binomiale

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

può essere definito come il numero dei sottoinsiemi di cardinalità d contenuti in un insieme di n elementi e sono ben note le formule:

$$\binom{n}{0}=\binom{n}{n}=1,\qquad \binom{n}{d}=\frac{1}{d!}\prod_{i=0}^{d-1}(n-i),\qquad d>0\,,$$

$$\binom{n}{d}=\binom{n-1}{d-1}+\binom{n-1}{d},\qquad d,n>0\,.$$

$$(x+y)^n=\sum_{d=0}^{n}\binom{n}{d}x^dy^{n-d}.$$

Osserviamo anche che $\binom{n}{d}=0$ se $d>n$ e che per $0\leq d\leq n$ vale $\binom{n}{d}=\dfrac{n!}{d!(n-d)!}$.

Più in generale, se t è una indeterminata, $n\in\mathbb{Z}$, $d\in\mathbb{N}$ e consideriamo i polinomi

$$\binom{t+n}{0}=1,\qquad \binom{t+n}{d}=\frac{1}{d!}\prod_{i=0}^{d-1}(t+n-i)\in\mathbb{Q}[t],\qquad d>0\,,$$

allora continua a valere la formula

$$\binom{t+n}{d}=\binom{n+t-1}{d-1}+\binom{n+t-1}{d}.$$

Basta infatti osservare che

$$\binom{n+t-1}{d-1} = \binom{t+n}{d}\frac{d}{n+t}, \qquad \binom{n+t-1}{d} = \binom{t+n}{d}\frac{n+t-d}{n+t}.$$

Definizione 30.1. Un polinomio $p(t) \in \mathbb{Q}[t]$ si dice un **polinomio numerico** se esiste un intero N tale che $p(n) \in \mathbb{Z}$ per ogni intero $n \geq N$.

Ogni polinomio a coefficienti interi è numerico, ma esistono anche polinomi numerici a coefficienti razionali: ad esempio il polinomio $\binom{t+n}{d}$ è numerico in quanto uguale ad un coefficiente binomiale per ogni t intero e $t \geq d-n$.

Lemma 30.2. *Se $p(t) \in \mathbb{Q}[t]$ è un polinomio numerico, allora $p(n) \in \mathbb{Z}$ per ogni $n \in \mathbb{Z}$.*

Dimostrazione. Induzione sul grado di $p(t)$. Se $p(t)$ è una costante, allora tale costante deve essere intera. Se $p(t)$ ha grado $n > 0$, allora il polinomio $q(t) = p(t) - p(t-1)$ è numerico di grado $n-1$ e per l'ipotesi induttiva $q(n) \in \mathbb{Z}$ per ogni intero n. Ne consegue inevitabilmente che anche $p(n) \in \mathbb{Z}$ per ogni $n \in \mathbb{Z}$. □

Notiamo che dal lemma precedente segue che il prodotto di d interi consecutivi è sempre divisibile per $d!$. Infatti il polinomio $p(t) = \binom{t+d}{d}$ è numerico e per ogni $n \in \mathbb{Z}$ si ha

$$\frac{1}{d!}\prod_{i=0}^{d-1}(n+i) = p(n-1) \in \mathbb{Z}.$$

Osserviamo che per ogni $a \in \mathbb{Z}$ ed ogni $n > 0$ il polinomio numerico $\binom{t+a+n}{n}$ ha grado n, e più precisamente:

$$\binom{t+a+n}{n} = \frac{t^n}{n!} + \left(a + \frac{n+1}{2}\right)\frac{t^{n-1}}{(n-1)!} + \cdots \tag{30.1}$$

Teorema 30.3. *Sia $p(t)$ un polinomio numerico di grado n. Allora esiste un'unica successione di interi $a_0, \ldots, a_n$ tale che*

$$p(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i}.$$

Dimostrazione. Sia $V \subset \mathbb{Q}[t]$ il $\mathbb{Q}$-sottospazio vettoriale dei polinomi di grado $\leq n$. Per ogni $i = 0, \ldots, n$ il polinomio $\binom{t+i}{i}$ ha grado i, i polinomi

$$\binom{t+0}{0}, \ldots, \binom{t+n}{n},$$

sono linearmente indipendenti e siccome V ha dimensione $n+1$ sono anche generatori. Abbiamo provato quindi che esistono unici $a_0, \ldots, a_n \in \mathbb{Q}$ tali che

$$p(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i}.$$

Dimostriamo per induzione su n che ogni a_i è intero; a tal fine basta provare che $a_n \in \mathbb{Z}$. Infatti se $a_n \in \mathbb{Z}$ allora il polinomio

$$p(t) - a_n\binom{t+n}{n} = \sum_{i=0}^{n-1} a_i \binom{t+i}{i}$$

è numerico di grado $< n$ e per l'ipotesi induttiva $a_i \in \mathbb{Z}$ per ogni i. Consideriamo adesso il polinomio numerico $q(t) = p(t+1) - p(t)$. I coefficienti direttori di $p(t)$ e $q(t)$ si calcolano facilmente:

$$p(t) = \frac{a_n}{n!}t^n + \cdots, \qquad q(t) = p(t+1) - p(t) = \frac{a_n}{n!}(nt^{n-1}) + \cdots$$

Per l'ipotesi induttiva esistono n interi $b_0, \dots, b_{n-1}$ tali che

$$q(t) = \sum_{i=0}^{n-1} b_i \binom{t+i}{i} = \frac{b_{n-1}}{(n-1)!} t^{n-1} + \cdots$$

da cui segue $a_n = b_{n-1} \in \mathbb{Z}$. □

Per uso futuro diamo un'altra interpretazione combinatoria dei coefficienti binomiali $\binom{d+n}{n}$ per $d \geq 0$.

Lemma 30.4. *Siano $x_0, \dots, x_n$ indeterminate. Il numero di monomi*

$$x_0^{a_0} x_1^{a_1} \cdots x_n^{a_n}$$

di grado $a_0 + \cdots + a_n = d$ è uguale al coefficiente binomiale $\binom{d+n}{n}$.

Dimostrazione. Dobbiamo calcolare la cardinalità dell'insieme

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

A tal fine consideriamo gli insiemi

$$A' = \{(a_1, \dots, a_n) \in \mathbb{N}^n \mid a_1 + \cdots + a_n \leq d\},$$
$$B = \{(b_1, \dots, b_n) \in \mathbb{N}^n \mid 1 \leq b_1 < b_2 < \cdots < b_n \leq d+n\},$$

osservando che B è in bigezione con i sottoinsiemi di cardinalità n di $\{1, \dots, d+n\}$ e pertanto $|B| = \binom{d+n}{n}$. Osserviamo poi che le applicazioni $A \xrightarrow{f} A' \xrightarrow{g} B$:

$$f(a_0, \dots, a_n) = (a_1, \dots, a_n), \quad g(a_1, \dots, a_n) = (a_1 + 1, a_1 + a_2 + 2, \dots, a_1 + \cdots + a_n + n),$$

sono bigettive con inverse

$$f^{-1}(a_1, \dots, a_n) = (d - \sum a_i, a_1, \dots, a_n),$$
$$g^{-1}(b_1, \dots, b_n) = (b_1 - 1, b_2 - b_1 - 1, \dots, b_n - b_{n-1} - 1).$$

Si noti che A' è in bigezione con l'insieme dei monomi $x_1^{a_1} \cdots x_n^{a_n}$ di grado $\leq d$. □

Esercizi

Esercizio 1. Provare che per ogni $n, d \geq 0$ vale la formula

$$\binom{d+n}{n} = \sum_{k \geq 0}^{n} \binom{n}{k}\binom{d}{k} = \sum_{k \geq 0}^{n} \binom{n}{n-k}\binom{d}{k}$$

considerando un insieme X formato da d palline bianche, n palline nere ed i sottoinsiemi di X formati da k palline bianche e $n-k$ palline nere.

Esercizio 2. Per ogni coppia di interi positivi n, m, denotiamo con $M(n, m)$ l'insieme di tutte e applicazioni

$$f \colon \{1, 2, \dots, n\} \to \{1, 2, \dots, m\}$$

non decrescenti, ossia tali che $f(i+1) \geq f(i)$ per ogni $i < n$. Calcolare le cardinalità di $M(n, m)$, del suo sottoinsieme delle applicazioni iniettive quando $n \leq m$ e del suo sottoinsieme delle applicazioni surgettive quando $n \geq m$.

Esercizio 3. 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

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

Esercizio 4. 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 $A_{i_1}\cap\cdots\cap A_{i_a}$. Dimostrare che la cardinalità di $A_1\cup\cdots\cup A_n$ 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.)

Esercizio 5. 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 $(1-t)^{-s}$.)

Esercizio 6. Provare che con la relazione di ordine, $p\geq q$ se e solo se $p(n)\geq q(n)$ per $n>>0$, i polinomi numerici sono un insieme totalmente ordinato.

31. Polinomi omogenei

Denotiamo con $\mathbb{K}[x_0,\dots,x_n]$ l'anello dei polinomi a coefficienti in $\mathbb{K}$ nelle indeterminate $x_0,\dots,x_n$: ogni polinomio in $\mathbb{K}[x_0,\dots,x_n]$ è una combinazione lineare finita a coefficienti in $\mathbb{K}$ di monomi $x_0^{a_0}\cdots x_n^{a_n}$, il grado $\deg(p)$ di un polinomio non nullo p è uguale al massimo grado dei monomi che vi compaiono con coefficiente diverso da 0. Con la convenzione che il grado del polinomio nullo è uguale a $-\infty$ le seguenti formule sono di immediata verifica:

$$\deg(fg)=\deg(f)+\deg(g),\quad \deg(f+g)\leq\max(\deg(f),\deg(g)),\quad f,g\in\mathbb{K}[x_0,\dots,x_n].$$

In particolare $fg=0$ se e solo se $f=0$ oppure $g=0$, ossia $\mathbb{K}[x_0,\dots,x_n]$ è un dominio di integrità: il suo campo delle frazioni globali è detto **campo delle funzioni razionali** e viene denotato $\mathbb{K}(x_0,\dots,x_n)$:

$$\mathbb{K}(x_0,\dots,x_n)=\left\{\frac{f}{g}\;\middle|\; f,g\in\mathbb{K}[x_0,\dots,x_n],\ g\neq 0\right\}.$$

Ad ogni polinomio $f\in\mathbb{K}[x_0,\dots,x_n]$ è associata la corrispondente funzione polinomiale $f\colon\mathbb{K}^{n+1}\to\mathbb{K}$ ottenuta sostituendo gli elementi di $\mathbb{K}$ al posto delle indeterminate ed eseguendo le necessarie operazioni di somma e prodotto. Come nel caso di polinomi in una variabile, siccome il campo $\mathbb{K}$ è infinito, il polinomio è univocamente determinato dalla corrispondente funzione polinomiale: ciò segue immediatamente dal seguente lemma.

Lemma 31.1. *Per ogni polinomio non nullo $0\neq f\in\mathbb{K}[x_0,\dots,x_n]$ esistono $a_0,\dots,a_n$ tali che $f(a_0,\dots,a_n)\neq 0$.*

Dimostrazione. Sia d il grado di f e dimostriamo il lemma per induzione su n: se $n=0$ il polinomio $f(x_0)$ ha al più d radici distinte e quindi esiste $a_0\in\mathbb{K}$ tale che $f(a_0)\neq 0$. Se $n>0$, raccogliendo a fattor comune le potenze di x_0 possiamo scrivere

$$f=f_0+f_1x_0+f_2x_0^2+\cdots+f_dx_0^d,$$

con i polinomi $f_i\in\mathbb{K}[x_1,\dots,x_n]$ non tutti nulli. Per induzione possiamo trovare $a_1,\dots,a_n\in\mathbb{K}$ tali che i valori $f_i(a_1,\dots,a_n)\in\mathbb{K}$ non sono tutti nulli e quindi tali che il polinomio

$$g(x_0)=f(x_0,a_1,\dots,a_n)$$

è non nullo. Come nel caso $n=0$ esiste $a_0\in\mathbb{K}$ tale che $g(a_0)\neq 0$. □

Un polinomio $f \in \mathbb{K}[x_0, \dots, x_n]$ si dice **omogeneo** di grado d se è combinazione lineare a coefficienti in $\mathbb{K}$ di monomi di grado d. Con questa definizione cadiamo nella contraddizione che il polinomio nullo è contemporaneamente di grado $-\infty$ ed omogeneo dei grado d per ogni $d \in \mathbb{N}$: si tratta tuttavia di una contraddizione del tutto innocua che semplifica l'esposizione rispetto ad una trattazione più formale e rigorosa.

Equivalentemente, un polinomio $f(x_0, \dots, x_n)$ è omogeneo di grado d se, nel campo delle funzioni razionali, vale l'uguaglianza

$$f(x_0, x_1, \dots, x_n) = x_0^d f\left(1, \frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

Notiamo infine che ogni polinomio f di grado $n \geq 0$ si scrive in modo unico come

$$f = f_0 + f_1 + \cdots + f_n,$$

con f_i polinomio omogeneo di grado i e $f_n \neq 0$.

Lemma 31.2. *Siano $f, g \in \mathbb{K}[x_0, \dots, x_n]$ con f che divide g e $g \neq 0$. Se g è omogeneo, allora anche f è omogeneo.*

Dimostrazione. Per ipotesi esiste un polinomio h tale che $fh = g$ e siccome $g \neq 0$ anche $f, h \neq 0$. Se f ha grado n e h ha grado m possiamo scrivere

$$f = f_0 + f_1 + \cdots + f_n, \qquad h = h_0 + h_1 + \cdots + h_m, \qquad n, m \geq 0,$$

con f_i, h_i omogenei di grado i e f_n, h_m non nulli. Siano

$$r = \min\{i \mid f_i \neq 0\}, \qquad s = \min\{i \mid h_i \neq 0\},$$

e supponiamo per assurdo $r < n$; allora

$$g = \sum_{d=r+s}^{n+m} \sum_{i+j=d} f_i h_j = f_r h_s + \sum_{i+j=r+s+1}^{n+m-1} f_i h_j + f_n h_m,$$

e siccome $f_r h_s \neq 0$, $f_n h_m \neq 0$ il polinomio g contiene sia monomi di grado $r+s$ che monomi di grado $n+m$, contraddicendo l'ipotesi di omogeneità. □

Lemma 31.3. *Sia $\mathbb{K}$ algebricamente chiuso. Allora ogni polinomio omogeneo $f \in \mathbb{K}[x_0, x_1]$ non nullo di grado d è il prodotto di d polinomi omogenei di grado 1.*

Dimostrazione. Sia $h \leq d$ il grado del polinomio $f(1, t) \in \mathbb{K}[t]$. Siccome $\mathbb{K}$ è algebricamente chiuso si ha

$$f(1, t) = c(t - a_1)(t - a_2) \cdots (t - a_h), \qquad c, a_1, \dots, a_h \in \mathbb{K},$$

e quindi

$$f(x_0, x_1) = x_0^d f\left(1, \frac{x_1}{x_0}\right) = c x_0^{d-h} \prod_{i=1}^{h} (x_1 - a_i x_0).$$

□

Un'altra fondamentale proprietà di $\mathbb{K}[x_0, \dots, x_n]$, ben nota dai corsi di Algebra, è quella di essere un dominio a fattorizzazione unica: un polinomio f si dice **irriducibile** se ha grado positivo e se non è il prodotto di polinomi di grado strettamente inferiore. Ogni polinomio non nullo si scrive in maniera essenzialmente unica come prodotto di polinomi irriducibili. Più precisamente, se

$$f = p_1 \cdots p_n = q_1 \cdots q_m$$

con $p_1, \dots, p_n, q_1, \dots, q_m$ polinomi irriducibli, allora $n = m$ e, a meno dell'ordine, per ogni indice i vale $p_i = c_i q_i$ per qualche $c_i \in \mathbb{K}$.

Due polinomi f, g si dicono senza fattori comuni, o relativamente primi, se non esiste alcun polinomio irriducibile che li divide entrambi.

Ricordiamo che un diagramma in serie di spazi vettoriali ed applicazioni lineari

$$\cdots \to V_i \xrightarrow{f_i} V_{i+1} \xrightarrow{f_{i+1}} V_{i+2} \to \cdots$$

si dice una **successione esatta** se $\ker f_i$ è uguale all'immagine di f_{i-1}, beninteso ogni volta che f_i ed f_{i-1} fanno parte del diagramma.

Ad esempio la successione $0 \to V \xrightarrow{f} W$ è esatta se e solo se f è iniettiva, mentre $V \xrightarrow{f} W \to 0$ è una successione esatta se e solo se f è surgettiva. Segue dal teorema del rango che se $0 \to V \to W \to U \to 0$ è una successione esatta di spazi vettoriali di dimensione finita, allora $\dim W = \dim V + \dim U$.

Il conucleo di un'applicazione lineare $f\colon V \to W$ è definito come lo spazio vettoriale quoziente $\operatorname{coker}(f) = \dfrac{W}{f(V)}$: si ha dunque una successione esatta

$$0 \to \ker(f) \xrightarrow{i} V \xrightarrow{f} W \xrightarrow{p} \operatorname{coker}(f) \to 0$$

dove i e p sono le applicazioni di inclusione e proiezione al quoziente, rispettivamente. Similmente, ogni quadrato commutativo

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} \\ A & \xrightarrow{g} & B \end{array}$$

si estende ad un diagramma commutativo con le righe esatte:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(f) & \longrightarrow & V & \xrightarrow{f} & W & \longrightarrow & \operatorname{coker}(f) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\beta} & & \\ 0 & \longrightarrow & \ker(g) & \longrightarrow & A & \xrightarrow{g} & B & \longrightarrow & \operatorname{coker}(g) & \longrightarrow & 0. \end{array}$$

Il seguente risultato è un caso particolare del lemma del serpente in algebra omologica e sarà utilizzato nelle prossime sezioni nello studio delle curve algebriche piane.

Lemma 31.4. *Si consideri un diagramma commutativo di spazi vettoriali con le righe esatte*

$$\begin{array}{ccccccc} & & U & \xrightarrow{f} & V & \xrightarrow{g} & W & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \\ 0 & \longrightarrow & A & \xrightarrow{h} & B & \xrightarrow{k} & C & & \end{array}$$

Allora l'applicazione indotta $\ker(\beta) \to \ker(\gamma)$ *è surgettiva se e solo se l'applicazione indotta* $\operatorname{coker}(\alpha) \to \operatorname{coker}(\beta)$ *è iniettiva.*

Dimostrazione. Dal fatto che $\beta f = h\alpha$ segue immediatamente che $\beta f(U) \subseteq h(A) \cap \beta(V)$ e, siccome h è iniettiva, l'iniettività di $\operatorname{coker}(\alpha) \to \operatorname{coker}(\beta)$ equivale alla relazione

$$h(A) \cap \beta(V) = \beta f(U)\,. \tag{31.1}$$

Supponiamo che $g\colon \ker(\beta) \to \ker(\gamma)$ sia surgettiva e consideriamo un elemento $x \in h(A) \cap \beta(V)$ e scriviamo $x = \beta(v_1)$ per qualche $v_1 \in V$. Siccome $x \in h(A)$ si ha $k(x) = 0$ e quindi $g(v_1) \in \ker(\gamma)$. Possiamo quindi trovare un elemento $v_2 \in \ker\beta$ tale che $g(v_2) = g(v_1)$. Ponendo $v = v_1 - v_2$ si ha $\beta(v) = x$ e $g(v) = 0$, quindi $v = f(u)$ per qualche $u \in U$ e $x = \beta f(u) \in \beta f(U)$.

Viceversa, supponiamo che valga (31.1) e sia $w \in \ker(\gamma)$. Siccome g è surgettiva esiste $v \in V$ tale che $g(v) = w$. Siccome $k\beta(v) = \gamma g(v) = 0$ esiste $a \in A$ tale che $\beta(v) = h(a)$ e quindi esiste un vettore $u \in U$ tale che $\beta(v) = h(a) = \beta f(u)$. Basta adesso osservare che $\beta(v - f(u)) = 0$, ossia $v - f(u) \in \ker(\beta)$ e $g(v - f(u)) = w$. □

In analogia con la teoria delle derivate parziali delle funzioni di variabile reale, per ogni indice $i = 0, \dots, n$ indichiamo con

$$\frac{\partial}{\partial x_i}\colon \mathbb{K}[x_0, \dots, x_n] \to \mathbb{K}[x_0, \dots, x_n]$$

l'applicazione lineare definita sui monomi mediante la formula

$$\frac{\partial}{\partial x_i} x_0^{a_0} \cdots x_n^{a_n} = \frac{a_i}{x_i} x_0^{a_0} \cdots x_n^{a_n}\,.$$

Lasciamo per esercizio che continua a valere la **formula di Leibniz**:

$$\frac{\partial fg}{\partial x_i} = \frac{\partial f}{\partial x_i} g + f \frac{\partial g}{\partial x_i}\,.$$

Lemma 31.5. *Se $\mathbb{K}$ è algebricamente chiuso e $f \in \mathbb{K}[x_0, \ldots, x_n]$ è un polinomio, allora vale $\dfrac{\partial f}{\partial x_i} = 0$ per ogni $i = 0, \ldots, n$ se e solo se vale una delle seguenti condizioni.*

1. *il campo $\mathbb{K}$ ha caratteristica 0 ed $f \in \mathbb{K}$ è una costante;*
2. *il campo $\mathbb{K}$ ha caratteristica positiva $p > 0$ ed esiste $g \in \mathbb{K}[x_0, \ldots, x_n]$ tale che $f = g^p$.*

In particolare se f è irriducibile, allora esiste sempre un indice i tale che $\dfrac{\partial f}{\partial x_i} \neq 0$.

Dimostrazione. Segue dalla formula di Leibniz che se una delle due condizioni è soddisfatta allora tutte le derivate parziali di f si annullano. Dimostriamo le implicazioni inverse per induzione su n, osservando preliminarmente che per ogni $a \in \mathbb{K}$ ed ogni numero primo p esiste b tale che $b^p = a$: infatti siccome $\mathbb{K}$ è algebricamente chiuso il polinomio $t^p - a$ possiede radici.

Sia $n \geq 0$ e supponiamo il lemma vero in $\mathbb{K}[x_0, \ldots, x_{n-1}]$. Dato $f \in \mathbb{K}[x_0, \ldots, x_n]$ con $\dfrac{\partial f}{\partial x_i} = 0$ per ogni i, possiamo scrivere

$$f(x_0, \ldots, x_n) = \sum_{j=0}^{d} f_j(x_0, \ldots, x_{n-1}) x_n^j, \qquad \frac{\partial f}{\partial x_n}(x_0, \ldots, x_n) = \sum_{j=1}^{d} j f_j(x_0, \ldots, x_{n-1}) x_n^{j-1}\,,$$

e quindi $\dfrac{\partial f}{\partial x_n} = 0$ se e solo se $jf_j = 0$ per ogni j.

Se $\mathbb{K}$ ha caratteristica 0, e $jf_j = 0$ per ogni j, allora $f_j = 0$ per ogni $j > 0$, ossia $f = f_0$ è un polinomio in $x_0, \ldots, x_{n-1}$ e la tesi segue dall'ipotesi induttiva.

Se $\mathbb{K}$ ha caratteristica $p > 0$, e $jf_j = 0$ per ogni j, allora $f_j = 0$ per ogni j non divisibile per p e quindi possiamo scrivere

$$f(x_0, \ldots, x_n) = \sum_{j=0}^{h} g_j(x_0, \ldots, x_{n-1}) x_n^{jp}, \qquad g_j = f_{pj}\,.$$

Siccome, per ogni $i < n$ si ha $\dfrac{\partial f}{\partial x_i} = \sum_j \dfrac{\partial g_j}{\partial x_i} x_n^{jp}$ ne consegue che $\dfrac{\partial g_j}{\partial x_i} = 0$ per ogni i, j e per l'ipotesi induttiva si può scrivere

$$g_j = h_j^p, \qquad f = \sum_j h_j^p (x_n^j)^p\,.$$

Per concludere basta osservare che, poiché $(a+b)^p = a^p + b^p$ (p divide i coefficienti binomiali $\binom{p}{i}$ per $0 < i < p$), si ha

$$\left(\sum_j h_j x_n^j \right)^p = \sum_j h_j^p (x_n^j)^p = f\,.$$

□

Lemma 31.6. *Siano $\mathbb{K}$ un campo algebricamente chiuso e $f \in \mathbb{K}[x_0, \ldots, x_n]$ un polinomio omogeneo di grado positivo e senza fattori multipli. Allora esiste almeno una "derivata parziale" $\dfrac{\partial f}{\partial x_i}$ non nulla e senza fattori in comune con f.*

Dimostrazione. Supponiamo per assurdo che $f = f_1 f_2 \cdots f_r$ con i polinomi f_i irriducibili e senza fattori in comune e che f_1 abbia grado positivo e divida tutte le derivate parziali di f. Segue allora dalla formula di Leibniz

$$\frac{\partial f}{\partial x_i} = \frac{\partial f_1}{\partial x_i} f_2 \cdots f_r + f_1 \frac{\partial f_2 \cdots f_r}{\partial x_i},$$

che f_1 divide $\dfrac{\partial f_1}{\partial x_i}$ per ogni i e quindi, siccome il grado della derivata è strettamente inferiore, deve essere necessariamente $\dfrac{\partial f_1}{\partial x_i} = 0$ per ogni i.

Basta quindi dimostrare che se f è irriducibile di grado positivo, allora possiede almeno una derivata parziale non nulla e questo segue dal Lemma 31.5. □

È immediato verificare la validità della seguente formula, detta **Formula di Eulero**: per ogni polinomio omogeneo $f \in \mathbb{K}[x_0, \dots, x_n]$ di grado d vale

$$\sum_{i=0}^{n} x_i \frac{\partial f}{\partial x_i} = d\, f\,. \tag{31.2}$$

Concludiamo le sezione precisando cosa si intende quando diciamo che **i polinomi irriducibili sono invarianti per cambio di coordinate**. Sia $A = (a_{ij}) \in M_{n+1,m+1}(\mathbb{K})$ una matrice e denotiamo con lo stesso simbolo $A\colon \mathbb{K}^{m+1} \to \mathbb{K}^{n+1}$ l'applicazione lineare associata, ossia l'applicazione che manda il punto y di coordinate $y_0, \dots, y_m$ nel punto $x = Ay$ di coordinate $x_i = \sum_j a_{ij} y_j$, $i = 0, \dots, n$.

Dato un polinomio $f(x_0, \dots, x_n)$ possiamo considerare il polinomio $A^*f \in \mathbb{K}[y_0, \dots, y_m]$ ottenuto sostituendo alla variabile x_i l'espressione $\sum_j a_{ij} y_j$:

$$A^*f(y_0, \dots, y_n) = f(\sum_j a_{0j} y_j, \dots, \sum_j a_{nj} y_j)\,.$$

Ad esempio, se $f(x_0, x_1) = x_0^2 - x_1^2$ e l'applicazione lineare A è data dalle relazioni

$$x_0 = y_0 + y_1, \qquad x_1 = y_0 - y_1$$

si ha:

$$A^*f(y_0, y_1) = (y_0 + y_1)^2 - (y_0 - y_1)^2 = 4y_0y_1\,.$$

Lasciamo per esercizio la verifica che l'applicazione $A^*\colon \mathbb{K}[x_0, \dots, x_n] \to \mathbb{K}[y_0, \dots, y_m]$ commuta con somme e prodotti e che il grado di A^*f è minore od uguale al grado di f. La funzione polinomiale $A^*f\colon \mathbb{K}^{m+1} \to \mathbb{K}$ è uguale alla composizione $\mathbb{K}^{m+1} \xrightarrow{A} \mathbb{K}^{n+1} \xrightarrow{f} \mathbb{K}$.

Se A è invertibile, allora $(A^{-1})^* = (A^*)^{-1}$. In particolare A^* è un isomorfismo di anelli e di spazi vettoriali ed il grado di A^*f è uguale al grado di f. Se f è irriducibile, allora anche A^*f è irriducibile: infatti se fosse $A^*f = gh$ con g, h polinomi di grado positivo, allora si avrebbe $f = ((A^{-1})^*g)((A^{-1})^*h)$ ed i due polinomi $(A^{-1})^*g$, $(A^{-1})^*h$ hanno grado positivo.

32. Ipersuperfici proiettive

In questa sezione n è un intero positivo fissato. Per ogni intero d denotiamo con $S_d \subset \mathbb{K}[x_0, \dots, x_n]$ il sottospazio vettoriale dei polinomi omogenei di grado d; in particolare $S_d = 0$ per ogni $d < 0$. Segue immediatamente dal Lemma 30.4 che per ogni $d \geq -n$ la dimensione di S_d è uguale a

$$\dim S_d = \binom{d+n}{n} = \frac{1}{n!}d^n + \frac{n+1}{2(n-1)!}d^{n-1} + \cdots\,.$$

Una dimostrazione alternativa si ottiene per induzione su $d + n$ ed osservando che per ogni $d > 0$ si ha una successione esatta

$$0 \to S_{d-1} \xrightarrow{\cdot x_0} S_d \xrightarrow{x_0 \mapsto 0} S_d \cap \mathbb{K}[x_1, \dots, x_n] \to 0,$$

da cui segue

$$\dim S_d = \binom{d+n-1}{n} + \binom{d+n-1}{n-1}.$$

Lemma 32.1. *Siano $f, g \in \mathbb{K}[x_0, \dots, x_n]$ polinomi omogenei di grado $a, b > 0$ rispettivamente. Allora f, g non hanno fattori comuni se e solo se per ogni intero d la successione*

$$0 \to S_{d-a-b} \xrightarrow{\alpha} S_{d-a} \oplus S_{d-b} \xrightarrow{\beta} S_d, \qquad \alpha(p) = (gp, fp), \quad \beta(q, r) = fq - gr,$$

è esatta.

Dimostrazione. È chiaro che $\beta\alpha = 0$. Inoltre, per ipotesi f, g sono entrambi non nulli quindi α è iniettiva poiché $\mathbb{K}[x_0, \dots, x_n]$ è un dominio di integrità. Dunque basterà provare che f, g non hanno fattori comuni se e solo se $\ker\beta \subseteq \operatorname{Im}\alpha$.

Supponiamo quindi f, g senza fattori comuni, d qualsiasi e sia $(q, r) \in \ker\beta$, ossia $fq = gr$. Vale $r = 0$ se e solo se $q = 0$ ed in tal caso la coppia $(q, r) = (0, 0)$ appartiene all'immagine di α. Se $r \neq 0$, siccome nessun fattore di f divide g si ha $r = fp$ con $p \in S_{d-a-b}$. Dunque $gfp = fq$ da cui segue $q = gp$ e di conseguenza $(q, r) = \alpha(p)$. Viceversa, se f, g hanno un fattore comune p di grado $0 < c \leq \min(a, b)$, allora la coppia $(g/p, f/p)$ appartiene al nucleo di $\beta\colon S_{b-c} \oplus S_{a-c} \to S_{a+b-c}$ ma non può appartenere all'immagine di $\alpha\colon S_{-c} \to S_{b-c} \oplus S_{a-c}$ per l'ovvio motivo che $S_{-c} = 0$. □

Lemma 32.2. *Siano $f, g \in \mathbb{K}[x_0, \dots, x_n]$ polinomi senza fattori comuni ed omogenei di gradi $a, b > 0$ rispettivamente. Per ogni intero d si consideri il sottospazio vettoriale*

$$(f, g)_d = \{hf + kg \mid h \in S_{d-a},\ k \in S_{d-b}\} \subset S_d\,.$$

Allora esiste un polinomio numerico $p(t) \in \mathbb{Q}[t]$ di grado $\deg(p(t)) \leq n - 2$ tale che

$$\dim S_d - \dim (f, g)_d = p(d) \quad \text{per ogni} \quad d \geq a + b - n\,.$$

Dimostrazione. Sia $d \geq a + b - n$ un intero fissato. Per il Lemma 32.1 la successione

$$0 \to S_{d-a-b} \xrightarrow{\alpha} S_{d-a} \oplus S_{d-b} \xrightarrow{\beta} S_d, \qquad \alpha(p) = (gp, fp), \quad \beta(q, r) = fq - gr,$$

è esatta e per definizione $(f, g)_d$ è l'immagine di β. Dal teorema del rango segue che

$$\begin{aligned}\dim S_d - \dim (f, g)_d &= \dim S_d - \dim S_{d-a} - \dim S_{d-b} + \dim S_{d-a-b} \\ &= \binom{d+n}{n} - \binom{d-a+n}{n} - \binom{d-b+n}{n} + \binom{d-a-b+n}{n}\end{aligned}$$

e per concludere basta osservare che, per (30.1), il polinomio numerico

$$p(t) = \binom{t+n}{n} - \binom{t-a+n}{n} - \binom{t-b+n}{n} + \binom{t-a-b+n}{n}$$

ha grado $\leq n - 2$. □

Teorema 32.3 (Eliminazione semplice)**.** *Siano $f, g \in \mathbb{K}[x_0, \dots, x_n]$ polinomi senza fattori comuni ed omogenei di gradi $a, b > 0$, rispettivamente. Allora esistono un intero d e due polinomi omogenei $h, k \in \mathbb{K}[x_0, \dots, x_n]$ di gradi $d - a, d - b$ rispettivamente tali che*

$$0 \neq hf + kg \in \mathbb{K}[x_1, \dots, x_n]\,.$$

È chiaro l'uso del termine eliminazione nel Teorema 32.3 in quanto la variabile x_0 viene "eliminata" mediante la combinazione $hf + kg$.

Dimostrazione. Sicomme $a, b > 0$, l'ipotesi che f, g non abbiano fattori comuni implica necessariamente $n > 0$. Per il Lemma 30.4 lo spazio vettoriale $R_d = S_d \cap \mathbb{K}[x_1, \dots, x_n]$ ha dimensione uguale a

$$\binom{d+n-1}{n-1} = \frac{d^{n-1}}{(n-1)!} + \cdots$$

ed il Lemma 32.2 implica che per d sufficientemente grande si ha

$$\dim R_d > \dim S_d - \dim (f, g)_d\,.$$

Per la formula di Grassmann l'intersezione $R_d \cap (f, g)_d$ ha dimensione strettamente positiva e contiene polinomi non nulli. □

Osservazione 32.4. Nei prossimi capitoli, usando tecniche più raffinate, ma sempre riconducibili all'algebra lineare, daremo una versione più forte del Teorema 32.3 in cui proveremo, tra le altre cose, che l'intero d può essere preso uguale al prodotto ab.

Indicheremo con $\mathbb{K}$ un campo algebricamente chiuso. Se $f \in \mathbb{K}[x_0, \dots, x_n]$ è omogeneo di grado $d \geq 0$, $(a_0, \dots, a_n) \in \mathbb{K}^{n+1}$ e $t \in \mathbb{K} - \{0\}$, allora

$$f(ta_0, \dots, ta_n) = t^d f(a_0, \dots, a_n)$$

e quindi $f(a_0, \dots, a_n)$ se e solo se $f(ta_0, \dots, ta_n)$. Tali considerazioni permettono di dare senso alle seguente definizione.

Definizione 32.5. Il luogo di zeri proiettivo $Z(f)$ di un polinomio omogeneo $f \in \mathbb{K}[x_0, \dots, x_n]$ è il sottoinsieme di $\mathbb{P}^n$ dato da:

$$Z(f) = \{p \in \mathbb{P}^n \mid f(p) = 0\} = \{[a_0, \dots, a_n] \in \mathbb{P}^n \mid f(a_0, \dots, a_n) = 0\}.$$

Quando il contesto lo consente si può scrivere, con un leggero abuso di notazione, anche $f(x) = 0$ per indicare il luogo di zeri proiettivo $Z(f)$ di un polinomio omogeneo. Il lettore tenga sempre presente che un polinomio omogeneo $f \in \mathbb{K}[x_0, \dots, x_n]$ non definisce alcuna funzione $\mathbb{P}^n \to \mathbb{K}$ ma solamente il suo luogo di zeri $Z(f)$.

In alcuni casi, motivi di chiarezza notazionale suggeriranno di usare lettere maiuscole per denotare polinomi omogenei $F \in \mathbb{K}[x_0, \dots, x_n]$.

Lemma 32.6. *Se $f \in \mathbb{K}[x_0, \dots, x_n]$ è omogeneo e non nullo, allora $Z(f)$ è un sottoinsieme proprio di $\mathbb{P}^n$.*

Dimostrazione. Se f ha grado 0, ossia f è una costante non nulla, allora $f(x) = 0$ è l'insieme vuoto. Se il grado di f è positivo allora $f(0, \dots, 0) = 0$, mentre per il Lemma 31.1 esistono $a_0, \dots, a_n \in \mathbb{K}$ tali che $f(a_0, \dots, a_n) \neq 0$. Dunque gli a_i non sono tutti nulli ed il punto $[a_0, \dots, a_n]$ non appartiene a $Z(f)$. □

Definizione 32.7. Chiemeremo **ipersuperfice proiettiva** ciascun sottoinsieme del tipo $Z(f) \subset \mathbb{P}^n$, con f polinomio omogeneo *di grado positivo.*

Ogni ipersuperfice in $\mathbb{P}^1$ è un insieme finito e non vuoto di punti. Infatti, se $f \in \mathbb{K}[x_0, x_1]$ è omogeneo di grado $d > 0$ per il Lemma 31.3 esiste una scomposizione in fattori lineari

$$f(x_0, x_1) = \prod_{i=1}^{d} (a_i x_0 + b_i x_1)$$

e quindi $Z(f) = \{[b_i, -a_i] \mid i = 1, \dots d\}$. Lo stesso argomento prova che ogni sottoinsieme finito di $\mathbb{P}^1$ è una ipersuperfice.

Lemma 32.8. *Le ipersuperfici proiettive intersecano ogni retta, ossia per ogni $X \subset \mathbb{P}^n$ ipersuperfice ed ogni retta proiettiva $L \subset \mathbb{P}^n$ vale $L \cap X \neq \emptyset$. In particolare X è infinito se $n \geq 2$.*

Dimostrazione. Fissiamo un sistema di coordinate omogenee tali che $L = \{x_2 = x_3 = \cdots = x_n = 0\}$, sia f polinomio omogeneo tale che $X = Z(f)$ e consideriamo il polinomio $g(x_0, x_1) = f(x_0, x_1, 0, \dots, 0)$. Il polinomio g è nullo se e solo se $L \subset X$; se L non è contenuta in X allora g è omogeneo dello stesso grado di f ed i punti di $L \cap X$ corrispondono allora ai fattori lineari di g. Se $n \geq 2$ e $o \in \mathbb{P}^n$ non appartiene ad X, allora esistono infinite rette passanti per o e ciascuna di esse interseca X. □

Si osserva immediatamente che più polinomi omogenei possono definire la medesima ipersuperfice, ad esempio per ogni costante $c \neq 0$ e per ogni polinomio omogeneo f si ha $Z(cf) = Z(f)$, ed anche $Z(f) = Z(f^2) = Z(f^3) = \cdots$. Per ogni coppia di polinomi omogenei f, g, vale la regola $Z(fg) = Z(f) \cup Z(g)$, mentre l'intersezione $Z(f) \cap Z(g)$ può essere scritta convenientemente nella forma $f(x) = g(x) = 0$.

Fortunatamente, almeno nel caso in cui f è irriducibile, il seguente teorema permette di ricostruire f (a meno di costanti moltiplicative) dalla ipersuperfice $f(x) = 0$.

Teorema 32.9 (degli zeri per ipersuperfici)**.** *Siano $\mathbb{K}$ algebricamente chiuso e $f, g \in \mathbb{K}[x_0, \dots, x_n]$ polinomi omogenei con f irriducibile. Allora $Z(f) \subseteq Z(g)$ se e solo se f divide g.*

Dimostrazione. Abbiamo già visto che se f divide g allora $Z(f) \subseteq Z(g)$. Viceversa se f è irriducibile, allora ha grado positivo e per il Lemma 32.6 esiste un punto $o \notin Z(f)$. A meno di un cambio lineare di coordinate, possiamo supporre che $o = [1, 0, \dots, 0]$.

Siano a il grado di f e b il grado di g. Se f non divide g, allora f e g non hanno fattori comuni ed abbiamo visto nel Teorema 32.3 che esiste un intero $d > 0$ e due polinomi omogenei h, di grado $d-a$, e k, di grado $d-b$, tali che

$$0 \neq r = hf + kg \in \mathbb{K}[x_1, \dots, x_n].$$

La ipersuperfice $Z(r)$ è una unione di rette passanti per il punto o: se $p \neq o$ e $p \in Z(r)$, allora $p = [a_0, \dots, a_n]$ con $a_1, \dots, a_n$ non tutti nulli e tali che $r(a_1, \dots, a_n) = 0$. Dunque $Z(r)$ contiene tutti i punti della retta op, i cui punti, in aggiunta a o sono tutti e soli quelli di coordinate omogenee $[a_0 + t, \dots, a_n]$, $t \in \mathbb{K}$.

È chiaro che $Z(f) \cap Z(g) \subseteq Z(r)$ e quindi se $Z(f) \subset Z(g)$, allora $Z(f) \subset Z(r)$. D'altra parte ogni retta passante per o interseca $Z(f)$, quindi interseca $Z(r)$ in un punto diverso da o e quindi è interamente contenuta in $Z(r)$. Ma questo implicherebbe $Z(r) = \mathbb{P}^n$ che è assurdo. □

Corollario 32.10. *Siano $f, g \in \mathbb{K}[x_0, \dots, x_n]$ polinomi omogenei irriducibili. Allora $Z(f) = Z(g)$ se e solo se f e g differiscono per una costante moltiplicativa. In particolare f e g hanno lo stesso grado.*

Dimostrazione. Per il teorema, siccome $Z(f) = Z(g)$ ne consegue che f divide g e g divide f. □

Definizione 32.11. Se il campo $\mathbb{K}$ è algebricamente chiuso, chiemeremo **ipersuperfice proiettiva irriducibile di grado** d ciascun sottoinsieme del tipo $Z(f)$, con f polinomio omogeneo irriducibile di grado d.

Ogni ipersuperfice proiettiva è unione finita di ipersuperfici irriducibili. Infatti se f è omogeneo e $f = f_1^{a_1} \cdots f_r^{a_r}$ è la sua decomposizione in fattori irriducibili, allora ciascun f_i è omogeneo e

$$Z(f) = Z(f_1^{a_1}) \cup \cdots \cup Z(f_r^{a_r}) = Z(f_1) \cup \cdots \cup Z(f_r).$$

Esercizi

Esercizio 7. Provare che l'applicazione

$$\mathbb{P}^1 \to \mathbb{P}^n, \qquad [t_0, t_1] \mapsto [t_0^n, t_0^{n-1}t_1, \dots, t_0 t_1^{n-1}, t_1^n],$$

è ben definita, iniettiva ed ha come immagine il sottoinsieme

$$X = \left\{ [x_0, \dots, x_n] \in \mathbb{P}^n \;\middle|\; \operatorname{rank} \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & x_2 & \cdots & x_n \end{pmatrix} = 1 \right\}.$$

Scrivere inoltre X come intersezione finita di ipersuperfici.

33. Curve piane

Da questo punto, e fino alla fine del capitolo restringeremo la nostra attenzione alle ipersuperfici di $\mathbb{P}^2$, altrimenti dette curve piane. Salvo avviso contrario indicheremo con $S_d \subset \mathbb{K}[x_0, x_1, x_2]$ il sottospazio vettoriale dei polinomi omogenei di grado d. Abbiamo già provato che per ogni $d \geq -2$ la dimensione di S_d è uguale a

$$\binom{d+2}{2} = \frac{(d+2)(d+1)}{2}.$$

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 delle 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 33.1. 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 $C = Z(f)$, 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

$$f(y_0, y_1, y_2) = 0 \quad \text{ se e solo se } \quad [y_0, y_1, y_2] \in C.$$

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 32.9, f divide g e se g è irriducibile allora $g = af$ per qualche $a \in \mathbb{K}$.

Definizione 33.2. Una curva algebrica piana è una combinazione lineare formale $C = m_1 C_1 + m_2 C_2 + \cdots + m_r C_r$ dove, per ogni indice i, C_i è una curva irriducibile e m_i è un intero positivo.

- Le curve C_i si dicono le **componenti irriducibili** di C.
- Per ogni $i = 1, \ldots, r$, il numero m_i viene detto la **molteplicità** della componente C_i.
- Il sottoinsieme $\mathrm{Supp}(C) = \cup C_i \subset \mathbb{P}^2$ 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 $p \in \mathrm{Supp}(C)$. Similmente se C, D sono due curve scriveremo $C \cap D$ per indicare l'intersezione dei supporti $\mathrm{Supp}(C) \cap \mathrm{Supp}(D)$.
- Se $n_1, \ldots, n_r$ sono i gradi delle componenti irriducibili $C_1, \ldots, C_r$, allora il numero $\deg(C) = n_1 m_1 + \cdots + n_r m_r$ 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 $f = f_1^{m_1} \cdots f_r^{m_r}$: possiamo quindi associare ad f la curva le cui componenti irriducibili $C_i = Z(f_i)$ sono i luoghi di zeri dei polinomi f_i aventi molteplicità m_i. Per l'unicità della fattorizzazione, la curva $C = m_1 C_1 + \cdots + m_r C_r$ risulta ben definita e la denoteremo spesso come la curva di equazione $f(x) = 0$.

Sia data viceversa una curva $C = \sum m_i C_i$; per definizione di curva irriducibile possiamo scrivere $C_i = Z(f_i)$, 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.

Si noti che in tale corrispondenza biunivoca vale la relazione $\mathrm{Supp}(C) = Z(f)$.

Iniziamo il nostro studio delle curve piane con una versione più raffinata del lemma di eliminazione semplice.

Lemma 33.3. *Siano $f, g \in \mathbb{K}[x_0, x_1, x_2]$ polinomi senza fattori comuni ed omogenei di gradi $a, b > 0$, rispettivamente. Allora per ogni intero $d \geq ab$ esistono due polinomi omogenei*

$h, k \in \mathbb{K}[x_0, x_1, x_2]$ di gradi $d-a, d-b$ rispettivamente tali che

$$0 \neq hf + kg \in \mathbb{K}[x_1, x_2].$$

Dimostrazione. Sia $d \geq ab$ intero fissato. Lo spazio vettoriale $R_d = S_d \cap \mathbb{K}[x_1, x_2]$ ha dimensione $d+1$. Si ha una successione esatta

$$0 \to S_{d-a-b} \xrightarrow{\alpha} S_{d-a} \oplus S_{d-b} \xrightarrow{\beta} S_d,$$

$$\alpha(h) = (gh, fh), \qquad \beta(p, q) = pf - qg,$$

e vogliamo provare che $R_d \cap \operatorname{Im}(\beta) \neq 0$. Per la formula di Grassmann basta provare che $\dim R_d = d+1 > \dim S_d - \operatorname{rank}\beta$. Basta quindi osservare che $d \geq ab \geq a+b-1$ e quindi

$$\begin{aligned}\dim S_d - \operatorname{rank}\beta &= \binom{d+2}{2} - \binom{d-a+2}{2} - \binom{d-b+2}{2} + \binom{d-a-b+2}{2} \\ &= \frac{1}{2}\left((d+2)(d+1) - (d-a+2)(d-a+1) - (d-b+2)(d-b+1)\right. \\ &\quad \left. +(d-a-b+2)(d-a-b+1)\right) \\ &= ab.\end{aligned}$$

□

Ogni coppia di curve piane $Z(f)$ e $Z(g)$ ha intersezione non vuota: se f e g hanno un fattore comune $f = hf'$, $g = hg'$, allora $Z(f) = Z(h) \cup Z(f')$, $Z(g) = Z(h) \cup Z(g')$ e di conseguenza

$$\emptyset \neq Z(h) \subseteq Z(f) \cap Z(g).$$

Se f e g non hanno fattori comuni, l'intersezione delle due curve segue dal seguente risultato.

Lemma 33.4. *Sia $\mathbb{K}$ algebricamente chiuso. Siano $f, g \in \mathbb{K}[x_0, x_1, x_2]$ polinomi senza fattori comuni ed omogenei di gradi $a, b > 0$, rispettivamente, allora $Z(f) \cap Z(g) \neq \emptyset$. Più precisamente, se è d il minimo intero per cui esiste una relazione del tipo*

$$0 \neq pf - gq = l_1 l_2 \cdots l_d \tag{33.1}$$

per opportuni $l_1, \ldots, l_d \in S_1$, $p \in S_{d-a}$, $q \in S_{d-b}$. Allora $Z(f) \cap Z(g) \cap Z(l_i) \neq \emptyset$ per ogni i.

Dimostrazione. Osserviamo preliminarmente che l'enunciato del lemma ha senso in virtù del lemma di eliminazione semplice e dal fatto che ogni polinomio omogeneo in due variabili è un prodotto di fattori lineari.

Per la minimalità di d abbiamo che per ogni i ed ogni coppia di polinomi omogenei p', q' tale che $p'f - gq' = l_1 l_2 \cdots l_d$, i polinomi l_i, p', q' non hanno fattori comuni. Fissiamo un indice i, a meno di un cambio di coordinate possiamo supporre $l_i = x_2$, e supponiamo per assurdo che $Z(f) \cap Z(g) \cap Z(l_i) = \emptyset$, o equivalentemente che i polinomi $f(x_0, x_1, 0)$ e $g(x_0, x_1, 0)$ non hanno fattori comuni. Denotando con $R_n \subset \mathbb{K}[x_0, x_1]$ il sottospazio vettoriale dei polinomi omogenei di grado n, per il Lemma 32.1 si ha un diagramma commutativo con righe e colonne esatte:

$$\begin{array}{lccccccc}
\gamma(r) = (gr, fr), & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \\
\beta(h,k) = hf - kg, & & S_{d-a-b} & \longrightarrow & R_{d-a-b} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \gamma} & & \downarrow & & \\
0 \longrightarrow & x_2 S_{d-a-1} \oplus x_2 S_{d-b-1} & \longrightarrow & S_{d-a} \oplus S_{d-b} & \longrightarrow & R_{d-a} \oplus R_{d-b} & \longrightarrow & 0 \\
 & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow & & \\
0 \longrightarrow & x_2 S_{d-1} & \longrightarrow & S_d & \longrightarrow & R_d & \longrightarrow & 0
\end{array}$$

Per costruzione, il polinomio $pf - gq$, appartiene all'intersezione $x_2 S_{d-1}$ con l'immagine di β ma non appartiene all'immagine di α, in contraddizione con il Lemma 31.4. □

Osservazione 33.5. Nella situazione del Lemma 33.4, le rette $L_i = Z(l_i)$ non sono univocamente determinate da f, g, anche nel caso in cui l'intero d è il minimo possibile.

Il caso limite è quando f, g hanno entrambi grado 1 ed al variare di $(p, q) \in \mathbb{K}^2 - \{0\}$ le rette $Z(pf - qg)$ sono tutte e sole le rette passanti per il punto $f(x) = g(x) = 0$.

Come ulteriore esempio si considerino i polinomi di secondo grado $f = x_0x_1$, $g = x_2(x_0 + x_1 + x_2)$. Allora, oltre alle ovvie scomposizioni in fattori lineari $1f + 0g = x_0x_1$ e $0f + 1g = x_2(x_0 + x_1 + x_2)$ si ha:

$$f + g = (x_0 + x_2)(x_1 + x_2)\,.$$

Lemma 33.6. *Siano $X \subset \mathbb{P}^2$ e d un intero positivo. Se per ogni punto $q \in \mathbb{P}^2$ l'insieme X è contenuto nell'unione di d rette passanti per q, allora X contiene al più d punti distinti.*

Dimostrazione. Supponiamo per assurdo che esistano $p_0, \dots, p_d \in X$ punti distinti; siccome il campo $\mathbb{K}$ è infinito possiamo trovare un punto $p \in \mathbb{P}^2$ non appartenente all'unione delle $d(d+1)/2$ rette p_ip_j, $0 \le i < j \le d$. Ogni retta per q contiene al più un punto p_i e quindi X non è contenuto in d rette passanti per q. □

Teorema 33.7 (Bézout debole)**.** *Siano $f, g \in \mathbb{K}[x_0, x_1, x_2]$ polinomi omogenei senza fattori comuni di gradi $a, b > 0$. Allora l'intersezione $f(x) = g(x) = 0$ delle corrispondenti ipersuperfici proiettive è non vuota e contiene al più ab punti distinti.*

Dimostrazione. Abbiamo già dimostrato che $Z(f) \cap Z(g) \neq \emptyset$. Per il lemma precedente basta dimostrare che per ogni punto $o \in \mathbb{P}^2$, l'intersezione è contenuta nell'unione di ab rette passanti per o. A meno di un cambio di coordinate omogenee possiamo supporre $o = [1, 0, 0]$ e per il Lemma 33.3 esistono due polinomi omogenei h, k tali che $hf + kg$ è un polinomio omogeneo non nullo di grado ab in x_1, x_2. Dunque

$$0 \neq hf + kg = \prod_{i=1}^{ab}(a_ix_1 + b_ix_2)$$

per opportune costanti $a_i, b_i \in \mathbb{K}$ e $Z(f) \cap Z(g)$ è contenuto nell'unione delle rette di equazione $a_ix_1 + b_ix_2 = 0$, $i = 1, \dots, ab$. □

Esempio 33.8. Su $\mathbb{K} = \mathbb{C}$, per ogni $n > 0$ consideriamo i tre polinomi omogenei di grado n:

$$f_n = \prod_{i=1}^{n}(x_0 - ix_1), \quad g_n = \prod_{j=1}^{n}(x_2 - jx_1), \quad h_n = \prod_{i=1}^{n}(x_0 + ix_1)\,.$$

Allora per ogni $a, b > 0$ l'intersezione $Z(f_a) \cap Z(h_b)$ contiene solo il punto $[0, 0, 1]$, mentre $Z(f_a) \cap Z(g_b)$ è formata dagli ab punti distinti $[i, 1, j]$, $i = 1, \dots, a$, $j = 1, \dots, b$.

Corollario 33.9. *Sia f polinomio omogeneo di grado n e sia $L \subset \mathbb{P}^2$ una retta. Se $L \cap Z(f)$ contiene almeno $n + 1$ punti distinti, allora l'equazione di L divide f.*

Dimostrazione. L'equazione di L è un polinomio omogeneo irriducibile l di grado 1. Per il teorema di Bézout se l non divide f l'intersezione $L \cap Z(f)$ contiene al più n punti distinti. □

Teorema 33.10. (Forma debole del teorema di Bézout) *Siano C e D due curve algebriche di gradi n e m rispettivamente. Allora:*

(1) *$C \cap D \neq \emptyset$.*
(2) *Se $C \cap D$ contiene più di nm punti, allora C e D hanno una componente irriducibile in comune.*

Dimostrazione. Conseguenza immediata del Lemma 33.4 e del Teorema 33.7. □

Corollario 33.11. *Due curve irriducibili distinte di gradi n, m hanno al più nm punti in comune.*

Dimostrazione. Immediata. □

Sia $f(x_0,x_1,x_2)=0$ l'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

$$\frac{\partial g}{\partial y_i}=a\sum_{j=0}^{2}\frac{\partial g}{\partial x_j}\frac{\partial x_j}{\partial y_i}$$

2) Se il campo $\mathbb{K}$ ha caratteristica 0, dalla formula di Eulero 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 $f(x)=0$ allora, essendo $\mathbb{K}$ algebricamente chiuso e quindi perfetto, esiste una derivata parziale non nulla e quindi per Bézout debole (Teorema 33.10) C ha al più $n(n-1)$ 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 33.12. *Siano $C_1,\dots,C_r$ curve algebriche (non necessariamente irriducibili) e sia $C=C_1+\cdots+C_r$. 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 $\dfrac{\partial f}{\partial x_h}(p)=0$ se e solo se $\dfrac{\partial f_i}{\partial x_h}(p)=0$. Siccome una curva $C=C_1+\cdots+C_r$, 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. □

Dunque ogni curva piana liscia è irriducibile, mentre il viceversa è falso. Ad esempio sono irriducibili e singolari nel punto $[1,0,0]$ tutte le cubiche di equazione

$$x_0x_2^2=x_1^3+\lambda x_0x_1^2\,,\qquad \lambda\in\mathbb{K}\,.$$

Osserviamo che a meno di proiettività la precedente famiglia di cubiche si riduce all'insieme delle due equazioni $x_0x_2^2=x_1^3$ e $x_0x_2^2=x_1^3+x_0x_1^2$. Infatti se $\lambda\neq 0$ e $\xi\in\mathbb{K}$ è una radice quadrata di λ, la proiettività

$$[x_0,x_1,x_2]\mapsto[\xi x_0,\xi^3x_1,\xi^4x_2]$$

trasforma la cubica di equazione $x_0x_2^2=x_1^3+\lambda x_0x_1^2$ in quella di equazione $x_0x_2^2=x_1^3+x_0x_1^2$.

Esempio 33.13. Per ciascuna cubica $C\subset\mathbb{P}^2$ di equazione

$$x_0x_2^2=x_1^3+px_0^2x_1+qx_0^3,\qquad p,q\in\mathbb{K}\,,$$

definiamo il suo *discriminante* come $\Delta=4p^3+27q^2$. Se il campo ha caratteristica diversa da 2, allora C è singolare se e solo se $\Delta=0$.

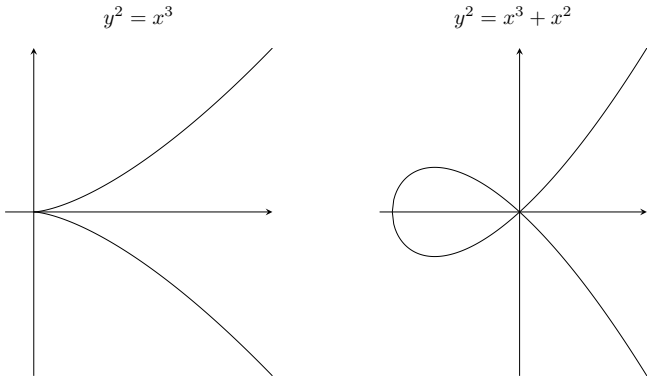


FIGURA 25. Due esempi di cubiche irriducibili singolari

Per definizione i punti singolari di C sono le soluzioni in $\mathbb{P}^2$ del sistema di equazioni omogeneee

$$\begin{cases} x_0x_2^2 = x_1^3 + px_0^2x_1 + qx_0^3 \\ x_2^2 = 2px_0x_1 + 3qx_0^2 \\ 0 = 3x_1^2 + px_0^2 \\ 2x_0x_2 = 0 \end{cases}$$

Osserviamo preliminarmente che non esistono punti singolari sulla retta di equazione $x_0 = 0$. Infatti se $x_0 = 0$ dalla prima equazione segue $x_1^3 = 0$ e dalla seconda $x_2^2 = 0$, da cui $x_0 = x_1 = x_2 = 0$ che non definisce alcun punto del piano proiettivo. Quindi ogni eventuale punto singolare sarà del tipo $[1, x, y]$ con $x, y \in \mathbb{K}$ soluzioni del sistema di equazioni

$$\begin{cases} y^2 = x^3 + px + q \\ y^2 = 2px + 3q \\ 0 = 3x^2 + p \\ 2y = 0 \end{cases}$$

Si noti che in caratteristica 2 tale sistema ammette l'unica soluzione $x = \sqrt{p}$, $y = \sqrt{q}$, mentre in caratteristica $\neq 2$ segue dall'ultima equazione che $y = 0$ e $x \in \mathbb{K}$ è una soluzione del sistema

$$\begin{cases} 0 = x^3 + px + q \\ 0 = 2px + 3q \\ 0 = 3x^2 + p \end{cases}$$

Consideriamo separatamente i due casi $p = 0$ e $p \neq 0$. Se $p = 0$ si ha $\Delta = -27q^2$, $q\Delta = (-3q)^3$ e quindi $\Delta = 0$ se e solo se $3q = 0$. Il sistema di equazioni diventa

$$0 = x^3 + q = 3q = 3x^2$$

che ammette soluzioni se e solo se $3q = 0$: infatti se $3q = 0$ e x è una soluzione di $x^3 + q = 0$, si ha $(3x^2)^3 = 27x^6 = 27q^2 = 0$.

Se $p \neq 0$, dalla seconda equazione segue $x = -\dfrac{3q}{2p}$ ed il sistema si riduce a

$$0 = -\frac{27q^3}{8p^3} - \frac{3q}{2} + q = \frac{27q^2}{4p^2} + p \iff 0 = -q(27q^2 + 4p^3) = 27q^2 + 4p^3 \,.$$

Esercizi

Esercizio 8. Provare che per ogni curva algebrica C, il supporto $\mathrm{Supp}(C)$ è un sottoinsieme proprio e infinito di $\mathbb{P}^2$.

Esercizio 9. Mostrare che in caratteristica 0, per ogni intero positivo n la curva di equazione $x_0^n + x_1^n + x_2^n = 0$ è liscia.

Esercizio 10. In caratteristica $\neq 2,3$, determinare per quali valori del parametro $\lambda \in \mathbb{K}$ risultano singolari le cubiche di equazioni

$$x_0x_2^2 = x_1(x_1+x_0)(x_1+\lambda x_0), \qquad x_0^3+x_1^3+x_2^3-3\lambda x_0x_1x_2 = 0.$$

Esercizio 11. Siano $C_1,\dots,C_r$ curve piane di gradi $n_1 \geq n_2 \geq \cdots \geq n_r$ e sia $V = C_1 \cap \cdots \cap C_r$. Dimostrare che se V è finito, allora contiene al più n_1n_r punti.

Esercizio 12. Determinare e descrivere i punti singolari (su $\mathbb{C}$) delle curve di equazioni

$$y^3(4z-y)^3 - 4x^4(x+3z)^2 = 0, \quad (8y-x-z)^3 = 216xyz, \quad (x^2-z^2)^2y = (y^2-z^2)^2x.$$

Esercizio 13. Sia $f \in \mathbb{K}[x_0,x_1]$ omogeneo di grado n senza fattori multipli. Provare che la curva di equazione $f(x_0,x_1)+x_2^n = 0$ è liscia, anche nel caso in cui n è divisibile per la caratteristica del campo.

34. Retta tangente e punti di flesso

Sia C una curva algebrica piana di grado n ed equazione $f(x)=0$ 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.

Se il punto p appartiene all'intersezione $L \cap C$, il calcolo della molteplicità di intersezione di L con C in p è molto semplice. Basta infatti calcolare la molteplicità di $t=0$ come radice del polinomio (non omogeneo)

$$F(1,t) = f(p_0+tq_0, p_1+tq_1, p_2+tq_2)\,.$$

Esempio 34.1. Il punto $p=[0,0,1]$ appartiene all'intersezione della cubica C di equazione $f = x_0x_2^2 - x_1^3 - x_0^3$ con la retta L di equazione $x_0+x_1=0$. Calcoliamo la molteplicità di intersezione di L con C in p. Siccome il punto $q=[1,-1,0] \neq p$ appartiene a L basta calcolare la molteplicità in $t=0$ del polinomio $f(t,-t,1)$. Dato che $f(t,-t,1)=t$ la molteplicità è 1. Notiamo inoltre che anche $q \in L \cap C$ e dato che $f(1,-1,t)=t^2$ la molteplicità di intersezione in q è uguale a 2.

Definizione 34.2. Siano L una retta, C una curva e $p \in L \cap C$. Diremo che L è **tangente** a C nel punto p se la molteplicità di intersezione di L con C in p è strettamente maggiore di 1.

Diremo che L è tangente a C se lo è in qualche punto di $C \cap L$; 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.

Proposizione 34.3. *Siano dati una curva C di equazione f e due punti distinti $p=[p_0,p_1,p_2]$ e $q=[q_0,q_1,q_2]$, con $p \in C$. Allora la retta $L=\overline{pq}$ è tangente a C in p se e solo se*

$$\sum_{i=0}^{2} q_i \frac{\partial f}{\partial x_i}(p_0,p_1,p_2) = 0\,.$$

Dimostrazione. La retta L è tangente a C in p se e solo se $t=0$ è una radice multipla del polinomio $g(t) = f(x_0+ty_0, x_1+ty_1, x_2+ty_2)$, cioè se e solo se $g'(0)=0$, dove g' denota la derivata di f rispetto a t. Basta adesso applicare la regola di derivazione della funzione composta. □

Corollario 34.4. *Sia $p=[p_0,p_0,p_1]$ un punto di una curva C di equazione f:*

(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 la cui equazione è*

$$\sum_{i=0}^{2} x_i \frac{\partial f}{\partial x_i}(p_0, p_1, p_2) = 0\,.$$

Dimostrazione. Conseguenza immediata della Proposizione 34.3. □

Le precedenti considerazioni forniscono un metodo per il calcolo delle rette tangenti ad una curva C passanti per un punto $q \in \mathbb{P}^2$. Se $f(x) = 0$ è l'equazione di f e $q = [q_0, q_1, q_2]$ abbiamo visto che, dato un punto $p \in C$, $p \neq q$, la retta $\overline{pq}$ è tangente a C in p se e solo se $\sum_i q_i f_i(p) = 0$. Quindi se $q \notin C$ le rette tangenti a C passanti per q sono tutte e sole quelle del tipo $\overline{pq}$ al variare di p tra le soluzioni dell'equazione

$$f(p) = \sum_i q_i f_i(p) = 0,\,. \tag{34.1}$$

Se invece $q \in C$ è un punto liscio, oltre a considerare le rette $\overline{pq}$ con $p \neq q$ che soddisfa (34.1) bisogna ovviamente aggiungere le retta tangente a C in q. Infine, se $q \in C$ è singolare, ogni retta passante per q è tangente a C.

Definizione 34.5. 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 la molteplicità di intersezione di $\mathbb{T}_p C$ con C nel punto p è maggiore od uguale a 3

Ad esempio, in una retta tutti i punti sono di flesso. Più in generale se la curva C è unione di rette allora ogni punto liscio di C è un flesso. Per il teorema di Bezout una conica possiede punti di flesso se e solo se è unione di rette.

Dato un polinomio omogeneo $f \in \mathbb{K}[x_0, x_1, x_2]$, per semplicità notazionale indichiamo

$$f_i = \frac{\partial f}{\partial x_i}, \qquad f_{ij} = f_{ji} = \frac{\partial^2 f}{\partial x_i \partial x_j}\,.$$

Si definisce la matrice Hessiana di f come:

$$H(x) = \begin{pmatrix} f_{00} & f_{01} & f_{02} \\ f_{10} & f_{11} & f_{12} \\ f_{20} & f_{21} & f_{22} \end{pmatrix}.$$

Se f ha grado $d \geq 2$ i coefficienti di $H(x)$ sono polinomi di grado $d-2$ ed il suo determinante $\det(H(x))$ è un polinomio omogeneo di grado $3(d-2)$.

Lemma 34.6. *Siano $\mathbb{K}$ un campo algebricamente chiuso e $H \in M_{3,3}(\mathbb{K})$ una matrice 3×3 simmetrica. Denotando con $\mathbb{K}^3$ lo spazio vettoriale numerico dei vettori colonna, le seguenti condizioni sono equivalenti:*

(1) $\det(H) = 0$*;*
(2) *per ogni vettore non nullo $v \in \mathbb{K}^3$ tale che $v^T H v = 0$ esiste un vettore $u \in \mathbb{K}^3$ linearmente indipendente da v tale che $u^T H v = u^T H u = 0$.*
(3) *esistono due vettori linearmente indipendenti $v_1, v_2 \subset \mathbb{K}^3$ tali che $v_i^T H v_j = 0$ per ogni i, j;*

Dimostrazione. 1 implica 2. Trattiamo separatamente i due casi $Hv = 0$ e $Hv \neq 0$. Se $Hv = 0$ completiamo v ad una base $v_1, v_2, v_3 = v$ di $\mathbb{K}^3$ e consideriamo il polimonio omogeneo di secondo grado

$$f(t_1, t_2) = (t_1 v_1 + t_2 v_2)^T H (t_1 v_1 + t_2 v_2)\,.$$

Per ipotesi il campo $\mathbb{K}$ è algebricamente chiuso e quindi esiste una coppia (t_1, t_2) non nulla tale che $f(t_1, t_2) = 0$. Allora il vettore $u = t_1 v_1 + t_2 v_2$ è quello cercato.

Se $Hv \neq 0$ è sufficiente prendere u un qualsiasi vettore non nullo tale che $Hu = 0$.

2 implica 3. Basta provare che esiste un vettore non nullo $v \in \mathbb{K}^3$ tale che $v^T H v = 0$. Questo si prova esattamente come sopra, considerando due vettori linearmente indipendenti v_1, v_2 ed il polinomio omogeneo $f(t_1, t_2) = (t_1 v_1 + t_2 v_2)^T H (t_1 v_1 + t_2 v_2)$.

3 implica 1. Supponiamo per assurdo che H sia invertibile, allora i vettori Hv_1, Hv_2 sono linearmente indipendenti e la matrice $A = (Hv_1, Hv_2) \in M_{3,2}(\mathbb{K})$ ha rango massimo. D'altra parte, il nucleo dell'applicazione lineare

$$A^T \colon \mathbb{K}^3 \to \mathbb{K}^2$$

coincide con l'insieme dei vettori u tali che $u^T Hv_1 = u^T Hv_2 = 0$ e quindi contiene v_1, v_2, in contraddizione con il fatto che A^T ha rango 2.

Notiamo che quest'ultima implicazione non richiede che il campo sia algebricamente chiuso. D'altra parte se $\mathbb{K} = \mathbb{R}$, la coppia

$$H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad v = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

soddisfa la condizione 1 ma non le condizioni 2 e 3. Sempre su $\mathbb{R}$, la matrice identità soddisfa la condizione 2 ma non soddisfa 3 ed 1.

□

Teorema 34.7. *(caratteristica 0) Sia C la curva piana di grado d ed equazione $f(x) = 0$ e sia $h(x)$ il determinate della matrice Hessiana $H(x)$ di f. Un punto liscio $p \in C$ è un flesso di C se e solo se $h(p) = 0$.*

Dimostrazione. Il teorema è banalmente verificato per le rette, non è quindi restrittivo supporre $d \geq 2$. Fissiamo $v \in \mathbb{K}^3 - \{0\}$ tale che $p = [v]$. Supponiamo che la matrice $A = H(v)$ non sia invertibile, per la formula di Eulero

$$0 = d(d-1)f(v) = (d-1)\sum_i v_i f_i(v) = \sum_{i,j} v_i v_j f_{ij}(v) = v^T Av\,.$$

Per il Lemma 34.6 esiste un punto $q = [u] \neq p$ tale che $u^T Av = u^T Au = 0$. Proviamo che la retta pq è la retta tangente a C in p e che p è un punto di flesso, ossia che $t = 0$ è una radice di molteplicià > 2 del polinomio

$$g(t) = f(v + tu) = t\sum_i f_i(v)u_i + \frac{t^2}{2}\sum_{ij} f_{ij}(v)u_i u_j + t^3(\cdots)\,. \tag{34.2}$$

Adesso basta osservare che

$$\sum_{ij} f_{ij}(v)u_i u_j = u^T Au = 0$$

e che per la formula di Eulero

$$(d-1)\sum_i f_i(v)u_i = \sum_{ij} f_{ij}(v)v_j u_i = v^T Au = 0\,.$$

Viceversa, supponiamo che p sia un punto di flesso e che pq sia la retta tangente a C in p, con $p \neq q = [u]$. Per (34.2) questo implica che

$$(d-1)\sum_i f_i(v)u_i = \sum_{ij} f_{ij}(v)v_i u_j = v^T Au = 0, \qquad \sum_{ij} f_{ij}(v)u_i u_j = u^T Au = 0$$

e per il Lemma 34.6 la matrice A non è invertibile.

□

Corollario 34.8. *In un campo algebricamente chiuso di caratteristica 0 ogni curva piana liscia di grado ≥ 3 possiede punti di flesso.*

Dimostrazione. Il determinante della matrice Hessiana definisce una curva di grado $3(d-2) > 0$ che quindi interseca C. □

Esercizi

Esercizio 14. Sul campo dei numeri complessi, si determini il numero di rette passanti per il punto $[1, 1, 0]$ e tangenti alla curva di Fermat $x_0^n + x_1^n + x_2^n = 0$.

Esercizio 15. 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.

35. 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

$$H = \begin{pmatrix} f_{00} & f_{01} & f_{02} \\ f_{10} & f_{11} & f_{12} \\ f_{20} & f_{21} & f_{22} \end{pmatrix} \in M_{3,3}(\mathbb{K}), \qquad f_{ij} = \frac{\partial^2 f}{\partial x_i \partial x_j}.$$

Il rango di una conica non dipende dalla scelta del sistema di coordinate omogenee.

Teorema 35.1. *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. Dato un punto $p = [v_0, v_1, v_2] = [v] \in \mathbb{P}^2$ per la formula di Eulero vale

$$v^T H = (f_0(v), f_1(v), f_2(v)), \qquad 2f(v) = v^T H v,$$

e quindi p è un punto singolare di C se e solo se $v^T H = (Hv)^T = 0$.

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 $\mathbb{P}^2$, possiamo quindi supporre a meno di proiettività che

$$p = [1, 0, 0], \qquad q = [0, 0, 1], \qquad r = [1, 1, 1], \qquad o = [0, 1, 0]\,.$$

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 $a = b$. □

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 35.2. *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 $x_0 x_2 = x_1^2$.*

Dimostrazione. Basta osservare che, nella dimostrazione del Teorema 35.1, la scelta dei punti p, q e r è arbitraria. □

Teorema 35.3 (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 $F_p \to F_q$ 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. Per il Corollario 35.2 possiamo supporre che C sia la conica di equazione $x_0 x_2 = x_1^2$ e che $p = [1, 0, 0]$, $q = [0, 0, 1]$.

Si consideri adesso l'applicazione $v\colon \mathbb{P}^1 \to C$ descritta in coordinate omogenee da $v([t_0, t_1]) = [t_0^2, t_0 t_1, t_1^2]$; si vede facilmente che v è biiettiva.

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 $v([a,b]) = [a^2, ab, b^2]$, mentre la retta di equazione $ax_1 - bx_0$ interseca C nei punti $q = [0,0,1]$ e $v([a,b]) = [a^2, ab, b^2]$.

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 $q = [0,0,1]$. L'applicazione descritta nel teorema è la composizione della seconda proiettività con l'inversa della prima. □

Il Teorema di Steiner 35.3 permette di definire sulla conica liscia C una struttura di retta proiettiva mediante l'applicazione v introdotta nella dimostrazione. In particolare è ben definito il birapporto di una quaterna ordinata di punti su C: basta fissare un punto $p \in C$ e considerare il birapporto delle 4 rette passanti per p ed i punti della quaterna.

Esercizi

Esercizio 16. Provare che il Corollario 35.2 è vero anche in caratteristica 2.

Esercizio 17. Trovare le componenti irriducibili della conica di equazione

$$3x_0^2 + 5x_0x_1 + 2x_0x_2 + 2x_1^2 + x_1x_2 - x_2^2 = 0.$$

36. Sistemi lineari

Abbiamo già osservato che le curve piane di grado n sono in corrispondenza biunivoca con il proiettivizzato $\mathbb{P}(S_n)$ dello spazio vettoriale $S_n \subset \mathbb{K}[x_0,x_1,x_2]$ dei polinomi omogenei di grado n. Abbiamo già visto che S_n ha dimensione $\binom{n+2}{2}$ e quindi, prendendo i monomi come base canonica di S_n si ottiene un isomorfismo di spazi proiettivi

$$\mathbb{P}(S_n) \simeq \mathbb{P}^N, \qquad N = \binom{n+2}{2} - 1 = \frac{n(n+3)}{2}.$$

Alla curva di equazione $\sum_{ijk} a_{ijk} x_0^i x_1^j x_2^k = 0$ corrisponde il punto di $\mathbb{P}^N$ di coordinate omogenee $[a_{ijk}]$.

Definizione 36.1. Un sottospazio proiettivo di $\mathbb{P}(S_n)$ si dice un **sistema lineare** di curve di grado n. Lo stesso spazio $\mathbb{P}(S_n)$ è un sistema lineare che viene detto **completo**.

Se $D_0, \dots, D_r$ sono curve di grado n denotiamo con $\langle D_0, \dots, D_r \rangle \subset \mathbb{P}(S_n)$ il sistema lineare da esse generato: se $f_i \in S_n$ è l'equazione di D_i, allora le curve del sistema lineare $\langle D_0, \dots, D_r \rangle$ sono esattamente quelle di equazione

$$a_0 f_0(x) + \cdots + a_r f_r(x) = 0$$

dove $a_0, \dots, a_r \in \mathbb{K}$ sono coefficienti tali che il polinomio $a_0f_0 + \cdots + a_rf_r$ sia non nullo.

Se V è un sistema lineare, indicheremo con $\dim V$ la sua dimensione. Ad esempio se D_0, D_1 sono curve distinte, allora $\dim\langle D_0 \rangle = \dim\langle D_1 \rangle = 0$, $\dim\langle D_0, D_1 \rangle = 1$: un sistema lineare di dimensione 1 si dice un **fascio** od anche **pennello**[13] o **schiera**.

Sia V un sistema lineare di curve, un punto $p \in \mathbb{P}^2$ si dice un **punto base** di V se per ogni curva $D \in V$ vale $p \in D$. 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 $\sum \lambda_i f_i$ e quindi i punti base di V sono quelli determinati dal sistema di equazioni

$$f_0(x) = \cdots = f_r(x) = 0.$$

L'equazione di un iperpiano in $\mathbb{P}(S_n)$ si dice una **condizione lineare** sulle curve di grado n.

Esempio 36.2. Sia $p \in \mathbb{P}^2$ un punto fissato. La relazione $p \in D$, con D curva di grado n, viene detta **condizione di passaggio per** p **su** $\mathbb{P}(S_n)$. Essa impone una condizione lineare sul sistema lineare completo: 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 $\mathbb{P}(S_n)$.

[13] In inglese **pencil**, in francese **pinceau**.

Più in generale, sia $\mathcal{P}$ una proprietà definita sulle curve di grado n e $V \subset \mathbb{P}(S_n)$ 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 V di codimensione r. Ad esempio la condizione 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 $\mathbb{P}^2$) induce una condizione lineare su un sistema V se e solo se p non è un punto base di V.

Lemma 36.3. *Sia V un sistema lineare di curve e siano $p_1, \dots, p_s$ punti di $\mathbb{P}^2$. Allora il passaggio per $p_1, \dots, p_s$ induce r condizioni lineari su V, con $0 \leq r \leq s$.*

In altri termini, l'insieme W delle curve $D \in V$ tali che $p_1, \dots, p_s \in D$ è un sistema lineare di dimensione $\dim W \geq \dim V - s$.

Dimostrazione. Sia n il grado delle curve del sistema lineare V. Abbiamo visto che per ogni $i = 1, \dots, s$ l'insieme $W_i = \{D \in \mathbb{P}(S_n) \mid p_i \in D\}$ è un iperpiano e quindi

$$W = V \cap W_1 \cap \cdots \cap W_s$$

è un sottospazio proiettivo. La formula $\dim W \geq \dim V - s$ segue immediatamente dalla formula di Grassmann. □

Definizione 36.4. Diremo che un insieme di punti $p_1, \dots, p_s$ induce **condizioni di passaggio indipendenti** su un sistema lineare V di curve se il passaggio per $p_1, \dots, p_s$ induce s condizioni lineari su V.

Ricordiamo che l'insieme vuoto, quando considerato come spazio proiettivo, ossia $\emptyset = \mathbb{P}(0)$ ha dimensione -1. Per il Lemma 36.3, affinché s punti inducano condizioni di passaggio indipendenti su un sistema lineare V è necessario che $s \leq \dim V + 1$.

Lemma 36.5. *Sia V un sistema lineare di curve e siano $p_1, \dots, p_s$ punti di $\mathbb{P}^2$. Allora $p_1, \dots, p_s$ inducono condizioni di passaggio indipendenti su V se e solo se per ogni $i = 1, \dots, s$ esiste una curva $D_i \in V$ tale che*

$$p_i \notin D_i, \qquad p_j \in D_i \quad \text{per ogni } j < i\,.$$

Dimostrazione. Sia n il grado delle curve del sistema lineare V e per ogni $i = 1, \dots, s$ consideriamo l'iperpiano $W_i = \{D \in \mathbb{P}(S_n) \mid p_i \in D\}$. Per la formula di Grassmann si ha che $\dim(V \cap W_1 \cap \cdots \cap W_s) = \dim V - s$ se e solo se per ogni indice $i = 1, \dots, s$ vale

$$V \cap W_1 \cap \cdots \cap W_i \neq V \cap W_1 \cap \cdots \cap W_{i-1}$$

Gli elementi di $V \cap W_1 \cap \cdots \cap W_{i-1} - V \cap W_1 \cap \cdots \cap W_i$ sono esattamente le curve D del sistema lineare tali che $p_i \notin D_i$ e $p_j \in D_i$ per ogni $j < i$. □

È utile osservare che se $p_1, \dots, p_s$ inducono condizioni di passaggio indipendenti su V lo stesso vale per ogni sottoinsieme di $p_1, \dots, p_s$.

Esempio 36.6. Un punto p induce una condizione di passaggio indipendente, ossia non nulla, su un sistema lineare se e solo se p non è un punto base del sistema lineare. In particolare se V è un fascio di curve e p non è un punto base, allora esiste ed è unica una curva $C \in V$ tale che $p \in C$.

Esempio 36.7. Tre punti inducono condizioni indipendenti sulle rette, ossia sul sistema lineare completo delle curve di grado 1, se e solo se non sono allineati.

Esempio 36.8. Quattro punti distinti inducono condizioni di passaggio indipendenti sulle coniche, ossia sul sistema lineare completo di dimensione 5 delle curve di grado 2, se e solo se non sono allineati.

Se i quattro punti appartengono ad una retta L, le coniche del tipo $L + M$, con M retta, formano un sistema lineare di dimensione 2 che passa per i quattro punti che pertanto non inducono condizioni di passaggio indipendenti. Viceversa se p è uno qualunque di 4 punti non allineati, allora p è allineato al più con una coppia dei rimanenti 3 e possiamo numerarli $p_1, \dots, p_4$ in modo tale che $p = p_4$ e $p \notin \overline{p_1p_2} \cup \overline{p_1p_3}$. Ma allora la conica $\overline{p_1p_2} + \overline{p_1p_3}$ passa per p_1, p_2, p_3 ma non per p_4.

Esempio 36.9. Cinque punti distinti inducono condizioni di passaggio indipendenti sulle coniche se e solo se non ve ne sono quattro allineati.

Abbiamo già visto che 4 punti allineati inducono condizioni dipendenti sulle coniche; a maggior ragione 5 punti di cui 4 allineati inducono condizioni di passaggio dipendenti.

Viceversa se 5 punti non inducono condizioni dipendenti, esistono almeno due coniche distinte C_1, C_2 che li contengono. Per Bézout le due coniche devono avere una retta L in comune, ossia $C_1 = L + M_1$ e $C_2 = L + M_2$ con M_1, M_2 rette distinte. Siccome M_1, M_2 hanno un solo punto in comune, almeno 4 dei 5 punti devono appartenere alla retta L.

Prima di proseguire con lo studio dell'indipendenza delle condizioni di passaggio vediamo alcune interessanti applicazioni dei sistemi lineari.

Teorema 36.10 (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 $p_1, \ldots, p_{n^2}$ i punti di intersezione di C e D, dal teorema di Bézout segue che necessariamente C, D, E sono curve ridotte.

Infatti C e D non hanno componenti in comune e se $C = \sum a_i C_i$ con le C_i irriducibili, allora $C \cap D = \cup_i C_i \cap D$,

$$n^2 = n(\sum a_i \deg(C_i)) = |C \cap D| \leq \sum |C_i \cap D| \leq \sum n \deg(C_i)$$

e questo prova che $a_i = 1$ per ogni i, ossia che C è ridotta. Per simmetria anche D è una curva ridotta.

Per mostrare che anche E è ridotta, scriviamo $E = \sum a_i E_i$; allora con E_i irriducibile per ogni i. Siccome C, D non hanno componenti in comune si ha $E_1 \not\subset C$ oppure $E_1 \not\subset D$; supponiamo per fissare le idee che $E_1 \not\subset C$, allora

$$|E_1 \cap C \cap D| \leq |E_1 \cap C| \leq n \deg(E_1).$$

Similmente $|E_i \cap C \cap D| \leq n \deg(E_i)$ per ogni i e quindi

$$nm = n(\sum_i a_i \deg(E_i)) = |E \cap C \cap D| \leq \sum_i |E_i \cap C \cap D| \leq \sum_i n \deg(E_i)$$

da cui segue $a_i = 1$ per ogni i, $|E_i \cap E_j \cap C \cap D| = \emptyset$ per ogni $i \neq j$ e $E_i \cap C \cap D$ contiene esattamente $n \deg(E_i)$ punti.

Siano C_t, con $t \in \mathbb{P}^1$, le curve del fascio V generato da C e D; notiamo che i punti base del fascio generato da C, D sono esattamente $C \cap D$. Sia $E = E_1 + \cdots + E_r$ la decomposizione in componenti irriducibili e denotiamo con m_i il grado di E_i. Siccome $E_i \cap C \cap D \subset E_i \cap C_t$ per ogni t, dal teorema di Bezout segue che per ogni $t \in \mathbb{P}^1$ vale una, ed una soltanto delle seguenti alternative:

(1) $E_i \cap C_t = E_i \cap C \cap D$;
(2) E_i è una componente di C_t.

Per ogni $i = 1, \ldots, r$, sia $q_i \in E_i - (C \cap D)$ un punto fissato, allora esiste un unico $t_i \in \mathbb{P}^1$ tale che $q_i \in C_{t_i}$; 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 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 $H = C_t - E$. □

Corollario 36.11. (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) Siano $L_1, L_2, \ldots, L_6$ i lati successivi di un esagono inscritto in una conica E. In virtù del teorema di Gergonne 36.10, 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. □

È facile dimostrare che ogni fascio di coniche contiene almeno una conica riducibile. Infatti siano C_1, C_2 coniche di equazioni f_1, f_2 e matrici Hessiane H_1, H_2 rispettivamente. Sappiamo

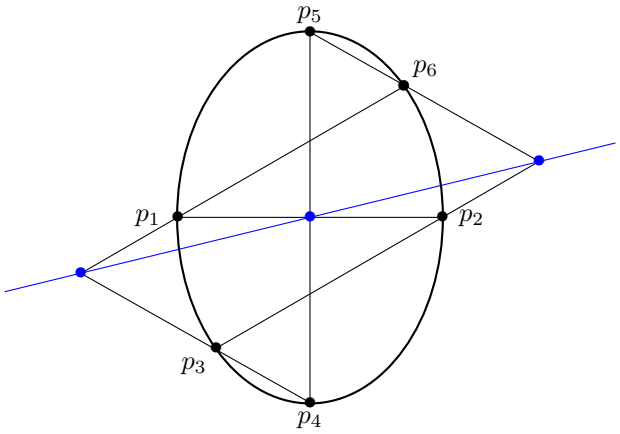


FIGURA 26. Il teorema di Pascal

che la conica di equazione $af_0 + bf_1$ è riducibile se e solo se (a, b) è una radice del polinomio omogeneo $p(t_1, t_2) = \det(t_1 H_1 + t_2 H_2)$. Se vogliamo determinare i punti di intersezione di due coniche C_1, C_2 si può procedere nel modo seguente.

Se C_2 è riducibile, si determinano le sue componenti (sono due rette) e per ciascuna di esse si calcola l'intersezione con C_1: il procedimento richiede la soluzione di alcune equazioni di secondo grado. Se invece C_2 è irriducibile si determina (risolvendo un'equazione di terzo grado) una conica riducibile $C_0 \neq C_2$ appartenente al fascio generato da C_1 e C_2 e quindi ricondursi al caso precedente osservando che $C_1 \cap C_2 = C_0 \cap C_2$.

Lemma 36.12. *Sia X un insieme finito con $2d$ elementi e sia $\sim$ una relazione di equivalenza su X tale che ciascuna classe di equivalenza contenga al più d elementi. Allora possiamo scrivere $X = \{a_1, b_1, \ldots, a_d, b_d\}$ con $a_i \not\sim b_i$ per ogni $i = 1, \ldots, d$.*

Dimostrazione. Induzione su d, essendo il risultato evidente per $d = 1$. Sia dunque $d > 1$ e scriviamo X come unione disgiunta delle sue classi di equivalenza, ordinate per cardinalità decrescente.

$$X = S_1 \cup S_2 \cup \cdots , \qquad d \geq |S_1| \geq |S_2| \geq \cdots .$$

Siccome S_1, S_2 non sono vuote e $d - 1 \geq |S_3|$ possiamo scegliere $a_1 \in S_1$, $b_1 \in S_2$ ed applicare l'ipotesi induttiva all'insieme $Y = X - \{a_1, b_1\}$. □

Lemma 36.13. *Siano $n > 0$, $V = \mathbb{P}(S_n)$ il sistema lineare completo delle curve di grado n e $k \leq 2n + 1$ un intero. Allora k punti distinti di $\mathbb{P}^2$ inducono condizioni di passaggio indipendenti su V se e solo se non ve ne sono $n + 2$ allineati. In particolare:*

(1) *$n + 1$ punti distinti inducono condizioni di passaggio indipendenti su V;*
(2) *$n + 2$ punti distinti inducono condizioni di passaggio indipendenti su V se e solo se non sono allineati.*

Dimostrazione. Consideriamo k punti distinti $p_1, \ldots, p_k$ e supponiamo che ne esistano $n + 2$ contenuti in una retta L: supponiamo per fissare le idee che $p_1, \ldots, p_{n+2} \in L$, allora per Bezout ogni curva di grado n che contiene $p_1, \ldots, p_{n+1}$ contiene L e di conseguenza contiene anche p_{n+2}.

Supponiamo adesso che in un insieme $S \subset \mathbb{P}^2$ di k punti non ne esistano $n + 2$ allineati: vogliamo dimostrare che per ogni $s \in S$ esiste una curva C di grado n che contiene $S - \{s\}$ ma non contiene s. A meno di aggiungere ad S un numero opportuno di punti in posizione generica non è restrittivo supporre $k = 2n + 1$.

Considerando su $S - \{s\}$ la relazione di equivalenza $p \sim q$ se e solo se i punti s, p, q sono allineati, abbiamo una partizione in classi di equivalenza

$$S - \{s\} = S_1 \amalg S_2 \amalg \cdots \amalg S_h .$$

Per ipotesi ciascuna classe di equivalenza contiene al massimo n punti, quindi $h \geq 2$ e per il Lemma 36.12 possiamo ordinare i punti $S - \{s\} = \{p_1, \ldots, p_{2n}\}$ in modo tale che p_{2i} non sia equivalente a p_{2i-1} per ogni $i = 1, \ldots, n$. (vedi Esercizio).

Ma allora l'unione delle n rette $C = \overline{p_1p_2} + \cdots + \overline{p_{2n-1}p_{2n}}$ è una curva di grado n con le proprietà richieste. □

Il passo successivo al Lemma 36.13, ossia determinare sotto quali condizioni $2n + 2$ punti distinti inducono condizioni indipendenti sulle curve di grado n, inizia ad essere geometricamente non banale e precursore di importanti teoremi.

Senza entrare in dettaglio, se studiamo le condizioni di passaggio delle coniche per 6 punti distinti, osserviamo che il teorema di Steiner 35.3 può essere interpretato come una condizione necessaria e sufficiente sulle sestuple di punti distinti affinché siano contenute in una conica.

Anche il caso delle condizioni imposte da 8 punti sulle cubiche rimane tutto sommato abbordabile.

Lemma 36.14. *Otto punti distinti $p_1, \ldots, p_8$ inducono condizioni indipendenti sulle cubiche piane se e solo se non sono contenuti in una conica e non ve ne sono 5 allineati.*

Dimostrazione. Dire che $p_1, \ldots, p_8$ inducono condizioni indipendenti vuol dire che le cubiche passanti per tali punti sono un sistema lineare di dimensione 1. Questo esclude immediatamente che gli 8 punti possano appartenere ad una conica Q, altrimenti tutte le cubiche del tipo $Q + L$, con L retta, passano per $p_1, \ldots, p_8$ e formano un sistema lineare di dimensione 2. Che non vi possano essere 5 punti allineati è stato dimostrato nel Lemma 36.13.

Viceversa, supponiamo gli $p_1, \ldots, p_8$ non contenuti in una conica e che non ve ne sono 5 allineati: bisogna dimostrare che esiste una cubica che contiene $p_1, \ldots, p_7$ ma non p_8.

Per ogni $i = 1, \ldots, 7$ indichiamo con l_i il numero dei punti $p_1, \ldots, p_7$ che appartengono alla retta $\overline{p_ip_8}$. Per ipotesi ciascun l_i è minore od uguale a 3 e quindi l'insieme delle rette $\overline{p_ip_8}$, $i = 1, \ldots, 7$ contiene almeno tre elementi. A meno di di permutazioni sull'insieme $p_1, \ldots, p_7$ possiamo supporre che $\overline{p_1p_8}$, $\overline{p_2p_8}$ e $\overline{p_3p_8}$ sia una terna di rette distinte che massimizza la somma $l_1 + l_2 + l_3$. In particolare:

(1) le rette $\overline{p_1p_2}$, $\overline{p_1p_3}$ e $\overline{p_2p_3}$ non contengono p_8;
(2) per ogni $i = 4, \ldots, 7$ se p_i non appartiene a $\overline{p_1p_8} \cup \overline{p_2p_8} \cup \overline{p_3p_8}$, allora la retta $\overline{p_ip_8}$ non contiene alcun punto del tipo p_j con $j \neq i, 8$.

Se i punti p_4, p_5, p_6, p_7 appartengono ad una retta L, la cubica $L + \overline{p_1p_2} + \overline{p_1p_3}$ contiene $p_1, \ldots, p_7$ ma non p_8.

Se p_4, p_5, p_6, p_7 non sono allineati, per ogni $i = 1, 2, 3$ sia Q_i una conica passante per i cinque punti p_i, p_4, p_5, p_6, p_7 e mostriamo che l'ipotesi $p_8 \in Q_1 \cap Q_2 \cap Q_3$ conduce ad una contraddizione. Se $Q_1 = Q_2 = Q_3$ allora gli 8 punti sarebbero contenuti in una conica; se invece i punti p_4, p_5, p_6, p_7, p_8 sono contenuti in due coniche distinte allora 4 di essi sono contenuti in una retta M. Dato che i punti p_4, p_5, p_6, p_7 non sono allineati la retta M contiene p_8 e tre dei 4 punti p_4, p_5, p_6, p_7. Siccome abbiamo ordinato i punti in modo tale cha la somma $l_1 + l_2 + l_3$ sia massima deve necessariamente essere $M = \overline{p_hp_8}$ per qualche $h = 1, 2, 3$, ma questo implicherebbe che in $p_h, p_4, p_5, p_6, p_7, p_8$ vi sono 5 punti allineati.

Quindi p_8 non appartiene ad almeno una delle tre coniche Q_1, Q_2, Q_3: se per fissare le idee $p_8 \notin Q_1$, allora la cubica $Q_1 + \overline{p_2, p_3}$ contiene $p_1, \ldots, p_7$ ma non p_8. □

Esercizi

Esercizio 18. Sia dato un fascio di coniche generato da due rette doppie. Provare che ogni conica di tal fascio è singolare.

Esercizio 19. Calcolare i punti di intersezione delle coniche di equazioni

$$x_0^2 + x_1^2 + x_2^2 = 0, \qquad x_1^2 + x_2^2 - x_0x_1 - x_0x_2 = 0.$$

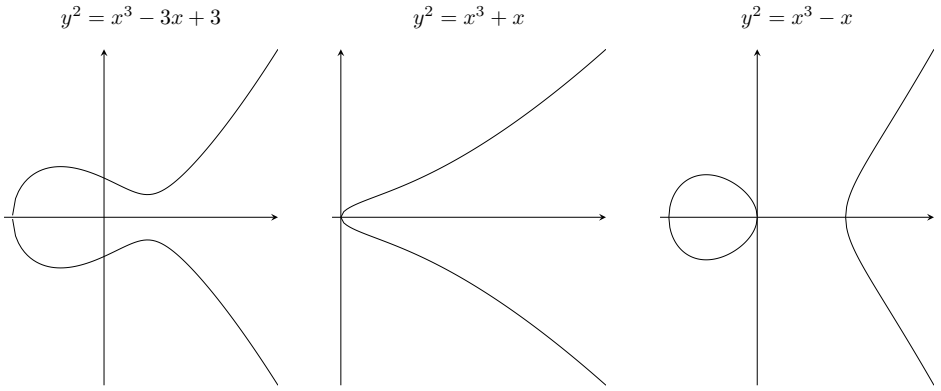


FIGURA 27. Tre esempi di cubiche lisce.

37. Curve ellittiche

Continuiamo con la convenzione che $\mathbb{K}$ sia un campo algebricamente chiuso di caratteristica 0.

Le curve piane di grado 3 sono dette cubiche piane. Siccome $3 = 2+1 = 1+2$ sono gli unici modi in cui possiamo scrivere 3 come somma di due interi positivi, una cubica è riducibile se e solo se contiene una retta. Ogni cubica riducibile è singolare mentre, a differenza di quanto accade per le coniche, esistono cubiche singolari irriducibili.

Abbiamo visto che ogni cubica liscia possiede punti di flesso: è possibile dimostrare che esistono esattamente 9 punti di flesso distinti, ma la dimostrazione di questo fatto va oltre gli obiettivi di questo capitolo.

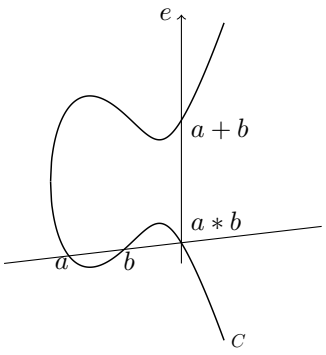
Se C è una cubica liscia ed $e \in C$ è un suo punto di flesso, allora la retta tangente a C in e non interseca C al di fuori di e. Infatti tale retta interseca C in esattamente 3 punti contati con molteplicità e, per definizione di flesso, la molteplicità di intersezione nel punto e è almeno 3.

Chiameremo (provvisoriamente) **curva ellittica** una coppia (C, e) dove C è una cubica liscia ed $e \in C$ è un punto di flesso. Data una curva ellittica (C, e) possiamo definire due operazioni

$$C \times C \xrightarrow{*} C, \qquad C \times C \xrightarrow{+} C,$$

nel modo seguente:

(1) $a * b =$ terzo punto di intersezione, oltre a e b, della retta $\overline{ab}$ con la cubica C, con la convenzione che se $a = b$ per retta $\overline{ab}$ si intende la tangente a C nel punto $a = b$.
(2) $a + b = (a * b) * e$.



$C: \; x_0 x_2^2 = x_1^3 - 4x_0^2 x_1 + 5x_0^3$

$e = [0, 0, 1]$

È chiaro dalla definizione che $a * b = b * a$, $a + b = b + a$ e $a * (a * b) = b$ per ogni coppia $a, b \in C$, e poichè e è un flesso si ha $e * e = e$. Inoltre per ogni punto $a \in C$ vale

$$a + e = e * (e * a) = a, \qquad a + (a * e) = e * (a * (a * e)) = e * e = e\,.$$

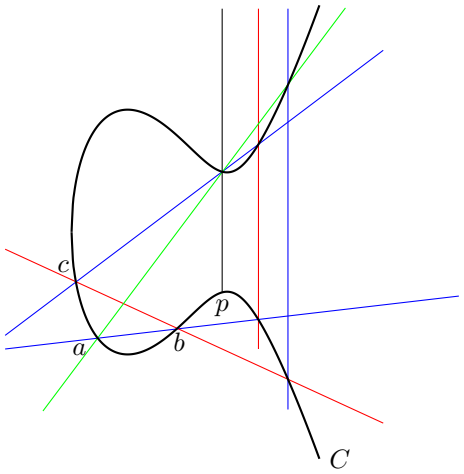


FIGURA 28. Legge associativa sulla cubica C, e cioè $p = (a+b)+c = a+(b+c)$. Nelle notazioni della dimostrazione le tre rette blu sono la cubica B, le due rette rosse sono la conica Q e la retta L è disegnata in verde. L'elemento neutro è il punto all'infinito corrispondente alla direzione verticale.

Teorema 37.1. *Sia (C,e) una curva ellittica. Allora l'operazione binaria $+$ induce su C una struttura di gruppo abeliano con elemento neutro e ed inverso $-a = a*e$.*

Dimostrazione. Tra i vari assiomi di gruppo rimane solo da verificare la proprietà associativa della somma $a+(b+c) = (a+b)+c$. La dimostrazione completa di questo fatto richiede strumenti non ancora sviluppati. Tuttavia, possiamo utilizzare il teorema di Gergonne per dare una dimostrazione per triple a,b,c in posizione generica e più precisamente sotto l'ipotesi aggiuntiva che i $9 = 3\times 3$ punti della tabella

$$\begin{array}{ccc} a & b+c & (a+b)*c \\ b & b*c & c \\ a*b & e & a+b \end{array} \tag{37.1}$$

siano tutti distinti (Figura 28).

Dalla definizione delle operazioni $*$ e $+$ segue che ciascuna colonna della Tabella (37.1) è formata da tre punti allineati e quindi i nove punti coincidono con l'intersezione di C con una cubica B unione di tre rette. Similmente la seconda e terza riga della tabella sono formate da terne allineate di punti; in particolare i 6 punti delle ultime due righe coincidono con l'intersezione di C con una conica Q unione di due rette.

Per il teorema di Gergonne 36.10 i tre punti della prima riga appartengono ad una retta L, ossia i tre punti a, $b+c$ e $(a+b)*c$ sono allineati, e questo è possible se e solo se $(a+b)*c = a*(b+c)$. Quindi

$$(a+b)+c = e*((a+b)*c) = e*(a*(b+c)) = a+(b+c)\,.$$

□

Osserviamo che un punto a in una curva ellittica (C,e) è un punto di flesso se e solo se $a*a = a$, o equivalentemente se e solo se $3a = a+a+a = e$. L'equivalenza tra flessi e punti a tali che $a*a = a$ segue immediatamente dalle definizioni. Se $a*a = a$, allora

$$2a = a+a = e*(a*a) = e*a, \qquad 3a = a+2a = e*(a*(e*a)) = e*e = e\,.$$

Viceversa, se $3a = e$ allora $e*(a*a) = 2a = -a = e*a$ e quindi $a = a*a$.

Analogamente si osserva che tre punti $a,b,c \in C$ sono allineati se e solo se $a+b+c = e$: la condizione $a+b+c = e$ è equivalente a dire che $e*(a*b) = a+b = -c = e*c$ che a sua volta equivale a dire che $a*b = c$.

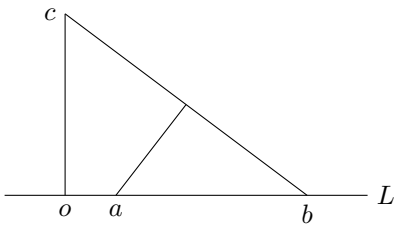


FIGURA 29. La distanza tra il punto a e la retta $\overline{bc}$ è strettamente minore della distanza del punto c dalla retta L.

Corollario 37.2. *Dati due punti di flesso distinti $a, b \in C$, il terzo punto c di intersezione di C con la retta $\overline{ab}$ è ancora un flesso.*

Dimostrazione. Fissiamo un flesso $e \in C$ (non necessariamente uguale ad a o b), abbiamo visto che rispetto alla struttura di gruppo sulla curva ellittica (C, e) si ha $a+b+c = e$, ossia $c = -a - b$. Allora $3c = -3a - 3b = -e - e = e$ e quindi anche c è un flesso. □

Esempio 37.3. Sia $\xi \in \mathbb{K} = \mathbb{C}$ una radice cubica primitiva di 1, ossia una radice del polinomio $\xi^2 + \xi + 1$. Allora i flessi della cubica di Fermat $x_0^3 + x_1^3 + x_2^3$ sono le intersezioni con la Hessiana $6^3 x_0 x_1 x_2 = 0$ e sono rappresentati nella tabella

$$\begin{array}{lll} [0,-1,1] & [0,-1,\xi] & [0,-1,\xi^2] \\ [-1,0,1] & [-1,0,\xi^2] & [-1,0,\xi] \\ [-1,1,0] & [-1,\xi,0] & [-1,\xi^2,0] \end{array} .$$

Senza usare il precedente corollario si verifica direttamente e facilmente che dati due punti della tabella ne esiste un terzo allineato.

Nel precedente esempio i flessi a coordinate reali sono esattamente i tre della prima colonna. Più in generale ogni cubica liscia complessa può avere al massimo tre flessi reali, come segue immediatamente dal Corollario 37.2 e dal seguente classico risultato di geometria proiettiva reale.

Teorema 37.4. *Sia $S \subset \mathbb{P}^n_{\mathbb{R}}$ un insieme* finito *di punti che soddisfa la seguente proprietà:*

(P): *per ogni coppia di punti distinti $p, q \in S$ esiste un punto $r \in S$, diverso da p, q e appartenente alla retta $\overline{pq}$.*

Allora i punti di S sono tutti allineati.

Dimostrazione. Supponiamo per assurdo che esistano tre punti $p, q, r \in S$ non allineati e sia $H \subset \mathbb{P}^n_{\mathbb{R}}$ il piano che li contiene. A meno di sostituire $\mathbb{P}^n_{\mathbb{R}}$ con H e S con $S \cap H$ non è restrittivo supporre $n = 2$. Infine, prendendo come retta all'infinito una qualsiasi retta che non interseca S possiamo ridurci al caso in cui $S \subset \mathbb{R}^2$ è un sottoinsieme finito che soddisfa la proprietà (P). Abbiamo supposto per assurdo che l'insieme T formato dalle terne ordinate $(p, q, r) \in S^3$ di punti non allineati sia non vuoto. Scegliamo un elemento $(u, v, c) \in T$ tale che la distanza di c dalla retta $L = \overline{uv}$ sia la minore possibile. Detta M la retta perpendicolare ad L passante per c, la distanza di c da L è uguale alla distanza di c dal punto o di intersezione di L con M. Il punto o divide la retta L in due semirette, ed L contiene almeno tre punti di S. Possiamo quindi trovare $a \neq b \in S \cap L$ tali che a è contenuto nel segmento di estremi o, b. Ma allora la distanza di a dalla retta $\overline{cb}$ è strettamente minore della distanza tra o e c (Figura 29), in contraddizione con le ipotesi. □

38. Operazioni sugli ideali

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

integrità, di campo e di caratteristica di un campo. Assumeremo inoltre che il lettore abbia familiarità con la nozione di insieme ordinato e con il lemma di Zorn.

Dato un anello A ed un suo sottoinsieme E, denotiamo con $(E) \subset A$ l'ideale generato da E, ossia 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:

$$(E) = \left\{ \sum_{\text{finita}} a_i e_i \;\middle|\; a_i \in A,\ e_i \in E \right\}.$$

Si noti che $(E) = E$ se e solo se E è un ideale. 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.

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: equivalentemente

$$I + J = \{x + y \mid x \in I,\ y \in J\}$$

così che, ad esempio, $I + (x) = \{a + bx \mid a \in I,\ b \in A\}$. Più in generale se I_α 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**[14] 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

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

Il radicale di un ideale è ancora un ideale: infatti se $a, b \in \sqrt{I}$ e n, m sono due interi positivi tali che $a^n, b^m \in I$ si ha $(-a)^n = \pm a^n \in I$,

$$\begin{aligned}(a+b)^{n+m} &= \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i} \\ &= b^m \sum_{i=0}^{n} \binom{n+m}{i} a^i b^{n-i} + a^n \sum_{i=n+1}^{n+m} \binom{n+m}{i} a^{i-n} b^{n+m-i} \in I,\end{aligned}$$

mentre per ogni $c \in A$ vale $(ac)^n = a^n c^n \in I$. Si noti che per ogni ideale I vale $I \subset \sqrt{I}$ e $\sqrt{\sqrt{I}} = \sqrt{I}$: infatti se $a \in \sqrt{\sqrt{I}}$, per definizione esistono due interi positivi n, m tali che $a^n \in \sqrt{I}$, $(a^n)^m \in I$ e quindi $a^{nm} \in I$.

Un **ideale radicale** è un ideale I tale che $I = \sqrt{I}$. Non tutti gli ideali sono radicali, ad esempio l'ideale $(4) \subset \mathbb{Z}$ non è radicale in quanto $\sqrt{(4)} = (2)$. Ogni ideale primo è radicale (esercizio).

Un ideale **massimale** è un ideale proprio che è massimale rispetto all'ordinamento 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 per definizione.

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

Lemma 38.1. *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 α, ne segue che $1 \notin J$, cioè che J è un ideale proprio. Per il lemma di Zorn $\mathcal{A}$ possiede elementi massimali. □

Lemma 38.2. *Sia $I \subset A$ un ideale. Allora $\sqrt{I}$ è l'intersezione di tutti gli ideali primi che contengono I.*

[14] In queste note, non è richiesto agli ideali primi di essere propri.

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_α 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 $\mathcal{A}$. □

Definizione 38.3. Il **nilradicale** di un anello commutativo è l'intersezione di tutti gli ideali primi.

Per il Lemma 38.2 il nilradicale coincide con l'insieme degli elementi nilpotenti $\sqrt{0}$.

Definizione 38.4. Un anello si dice **locale** se contiene un solo ideale massimale. L'unico campo quoziente di un anello locale si dice **campo residuo**.

Se $f\colon A \to B$ 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 $\mathbb{Z} \to \mathbb{Q}$ 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 38.5. *Sia $f\colon A \to B$ 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 bigezione 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 $b \equiv c \pmod{a}$.

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

Un elemento x di un anello A si dice un **nilpotente** se esiste un intero positivo n tale che $x^n = 0$. Un anello si dice **ridotto** se non contiene elementi nilpotenti diversi da 0; un anello è ridotto se e solo se l'ideale 0 è radicale; è chiaro che ogni dominio di integrità è ridotto, mentre il viceversa è generalmente falso (Esempio: $\mathbb{Z}/(6)$).

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"

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

La caratteristica di un domino di integrità è, per definizione, la caratteristica del suo campo delle frazioni; 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 38.6. Un dominio di integrità si dice **perfetto** se ha caratteristica 0 oppure se ha caratteristica $p > 0$ ed il morfismo di Frobenius è surgettivo.

Esercizi

Esercizio 20. Dimostrare che ogni ideale primo è irriducibile. Verificare che l'ideale 0 nell'anello $\dfrac{\mathbb{R}[x]}{(x^2)}$ è irriducibile ma non è primo.

Esercizio 21. 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 $a \in \mathfrak{m}$.

Esercizio 22. Sia $\mathfrak{rad}$ l'intersezione di tutti gli ideali massimali di un anello commutativo A. Dimostrare che $a \in \mathfrak{rad}$ se e solo se $1+ab$ è invertibile in A per ogni $b \in A$.

Esercizio 23. 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**.

Esercizio 24. Siano $I_1, \ldots, I_n$ 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.

Esercizio 25. 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 [8]; 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 $+, \cdot \colon E \times E \to E$ 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.

Esercizio 26. Sia A un anello commutativo con unità e siano

$$\mathfrak{rad} = \{x \in A \mid 1+xy \text{ è invertibile per ogni } y \in A\} \quad \text{(vedi Esercizio 22)},$$

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

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

Esercizio 27. 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.

39. 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 46).

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 l'anello $\mathbb{K}[t]$ e più in generale i domini di integrità a ideali principali sono domini a fattorizzazione unica (cfr. Esercizio 39).

Se A è un anello, indicheremo con $A[x_1, \ldots, x_n]$ l'anello dei polinomi a coefficienti in A nelle indeterminate $x_1, \ldots, x_n$. La proprietà caratterizzante di $A[x_1, \ldots, x_n]$ è che *per ogni omomorfismo di anelli* $\phi \colon A \to B$ *e per ogni n-upla* $b_1, \ldots, b_n \in B$ *esiste unica una*

estensione di ϕ ad un omomorfismo, detto di ***specializzazione***, $\hat{\phi}\colon A[x_1,\dots,x_n] \to B$ *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

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

Lemma 39.1. *Siano A un anello commutativo e $a \in A$. Allora il polinomio $1 - ta \in A[t]$ è invertibile in $A[t]$ se e solo se a è nilpotente in A.*

Dimostrazione. Se a è nilpotente, diciamo $a^{n+1} = 0$, allora

$$(1-ta)(1+ta+t^2a^2+\cdots+t^na^n) = 1\,,$$

e quindi $1 - ta$ è invertibile. Viceversa, se $1 - ta$ è invertibile si ha una relazione del tipo

$$(1-ta)(b_0+tb_1+t^2b_2+\cdots+t^nb_n) = 1, \qquad b_i \in A\,,$$

che equivale al sistema di equazioni

$$b_0 = 1, \quad tb_1 = tab_0, \quad t^2b_2 = t^2ab_1, \dots, t^{n+1}ab_n = 0\,,$$

ed una semplice induzione su i mostra che $b_i = a^i$ per ogni $i = 0,\dots,n$, da cui segue $a^{n+1} = 0$. □

Rimandiamo all'Esercizio 28 per una estensione del Lemma 39.1.

Definizione 39.2. 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 39.3 (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. 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 $r \le n$ e $s \le m$ due interi tali che $c | a_i$ per $i < r$, $c \not| a_r$, $c | b_j$ per $j < s$ e $c \not| b_s$. 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 $h = \dfrac{ag}{b}$ è un polinomio primitivo in $A[t]$. Dunque $fh = \dfrac{agf}{b}$ 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. □

Lemma 39.4 (Divisione Euclidea)**.** *Sia A un dominio di integrità e $p \in A[x]$ un polinomio monico di grado $d \ge 0$. Allora per ogni $f \in A[x]$ esistono unici $g, r \in A[x]$, con r di grado minore di d, tali che $f = gp + r$.*

Dimostrazione. Esistenza: sia $\mathcal{F} \subset A[t]$ la famiglia dei polinomi f per i quali non si può scrivere $f = gp + r$ con r di grado $< d$. Se per assurdo $\mathcal{F} \neq \emptyset$ si scelga $h \in \mathcal{F}$ di grado minimo s. Si ha $s \ge d$ altrimenti $h = 0g + h$, dunque $s > d$ e $h = a_0 t^s + \cdots$. Basta adesso osservare che $h - a_0 t^{s-d} p$ ha grado $< s$ e non appartiene a $\mathcal{F}$. Si può quindi scrivere $h - a_0 t^{s-d} p = gp + r$, da cui $h = (a_0 t^{s-d} + g)p + r \notin \mathcal{F}$.

Unicità: se $f = g_1p + r_1 = g_2p + r_2$ allora $r_1 - r_2 = (g_2 - g_1)p$; se fosse $g_1 \neq g_2$ allora il polinomio $(g_2 - g_1)p$ ha grado $\geq d$, mentre $r_1 - r_2$ ha grado $< d$. Dunque $g_1 = g_2$ e quindi $r_2 = f - g_2p = f - g_1p = r_1$. □

Lemma 39.5 (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. Per la divisione Eucliea si può scrivere $f(x) = g(x)(x - a) + f(a)$. □

Lemma 39.6. *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. □

Dal Lemma 39.5 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 $i = 1, \ldots, s$ esiste unica un'applicazione

$$\frac{\partial}{\partial x_i} \colon A[x_1, \ldots, x_s] \to A[x_1, \ldots, x_s]$$

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 $b_1, b_2 \in A[x_1, \ldots, x_s]$.
(3) (Leibniz) $\frac{\partial}{\partial x_i}(b_1b_2) = b_1\frac{\partial}{\partial x_i}(b_2) + b_2\frac{\partial}{\partial x_i}(b_1)$ per ogni $b_1, b_2 \in A[x_1, \ldots, x_s]$.
(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 $A \to B$, un'applicazione $d \colon B \to B$ 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 39.7. *Sia A un dominio perfetto a fattorizzazione unica e $f \in A[x_1, \ldots, x_s]$. Allora f possiede un fattore multiplo di grado positivo se e solo se $f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_s}$ 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 $f = f_1f_2 \cdots f_n$ 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 $f \in A[x_1^p, \ldots, x_s^p]$. Siccome A è perfetto, si ha che f appartiene all'immagine del morfismo di Frobenius $A[x_1, \ldots, x_s] \to A[x_1, \ldots, x_s]$ e quindi esiste $h \in B$ tale che $f = h^p$. □

Esercizi

Esercizio 28. Sia A un anello commutativo e $f = a_0 x^n + \cdots + a_n \in A[x]$ 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 $a_0, \ldots, a_{n-1}$ sono nilpotenti.

Esercizio 29. Siano A un anello, $0 \leq r < n$ interi e $a_{r+1}, \ldots, a_n \in A$. Mostrare che l'applicazione

$$\phi\colon A[x_1, \ldots, x_n] \to A[x_1, \ldots, x_r], \qquad \phi(f(x_1, \ldots, x_n)) = f(x_1, \ldots, x_r, a_{r+1}, \ldots, a_n)$$

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

Esercizio 30. 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 39.6 non vale in $A[x]$.

Esercizio 31. Siano $d_1, d_2\colon A[x_1, \ldots, x_s] \to A[x_1, \ldots, x_s]$ due A-derivazioni. Dimostrare che $d_1 = d_2$ se e solo se $d_1(x_i) = d_2(x_i)$ per ogni $i = 1, \ldots, s$.

Esercizio 32. La **derivazione di Eulero** è l'unica A-derivazione

$$E\colon A[x_1, \ldots, x_s] \to A[x_1, \ldots, x_s]$$

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

Esercizio 33. Siano $f \in A[x_1, \ldots, x_s]$ e $g_1, \ldots, g_s \in A[t]$, provare che

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

Esercizio 34. Provare che in $A[x_1, \ldots, x_s]$ gli operatori $\dfrac{\partial}{\partial x_i}$ commutano tra loro.

Esercizio 35. Sia $A \to B$ un morfismo di anelli e siano $f, g, h\colon B \to B$ 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) $[f \circ g, h] = f \circ [g, h] + [f, h] \circ g$.

Esercizio 36. 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 $a, p_1, \ldots, p_n \in R$ tali che $\mathrm{GCD}(p_1, \ldots, p_n) = 1$ e $A^{ij} = a p_i p_j$.

Esercizio 37. 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 $A(t)$.

Esercizio 38 (∗)**.** 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.

Esercizio 39. Dedurre dall'Esercizio 38 che ogni dominio ad ideali principali è a fattorizzazione unica.

Esercizio 40. Dimostrare che ogni dominio di integrità finito è un campo.

Esercizio 41. 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.

Esercizio 42. Provare che il polinomio $x^3+2x^2+2x-88$ non ha radici razionali positive.

40. 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 $A_nA_m\subset A_{n+m}$ 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 $f=f_n+f_{n+1}+\cdots+f_N$ e $g=g_r+g_{r+1}+\cdots+g_R$ sono le decomposizioni in componenti omogenee, con $f_n,f_N,g_r,g_R\neq 0$, allora $fg=f_Ng_R+f_ng_r+C$, dove C è una combinazione lineare di elementi omogenei di gradi strettamente compresi fra $n+r$ e $N+R$. Siccome f è omogeneo deve necessariamente essere $n+r=N+R$ e quindi $n=N,r=R$.

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

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

dove A_d è l'insieme dei polinomi omogenei di grado d, ossia l'insieme delle combinazioni lineari a coefficienti in A di monomi $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ con $i_1+\cdots+i_n=d$. 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 $x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ con $i_1w(x_1)+\cdots+i_nw(x_n)=m$.

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

Nello studio degli anelli graduati si utilizza con una certa frequenza il determinante di Vendermonde, che richiamiamo velocemente per completezza. Dati $n+1$ elementi $x_0,\ldots,x_n$ in un campo vale la formula

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

Possiamo dimostrare tale formula per induzione su n, considerando il polinomio

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

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

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

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

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

Lemma 40.1. *Sia A un dominio di integrità infinito e sia $f \in A[x_1, \ldots, x_s]$. Allora f è omogeneo di grado n se e solo se*

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

per ogni $t \in A$.

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

Lemma 40.2. *Sia $\mathbb{K}$ un campo infinito. Un ideale $I \subset \mathbb{K}[x_1, \ldots, x_n]$ è omogeneo se e solo se per ogni $f \in I$ e per ogni $t \in \mathbb{K}$, il polinomio $f_t(x_1, \ldots, x_n) := f(tx_1, \ldots, tx_n)$ appartiene all'ideale I.*

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

Scriviamo $f = f_0 + f_1 + \cdots + f_s$, dove f_i è omogeneo di grado i. Per ogni scelta di $t_0, t_1, \ldots, t_s \in \mathbb{K}$ vale $f_{t_i} = \sum_j t_i^j f_j$. Siccome $\mathbb{K}$ è infinito, possiamo scegliere gli scalari $t_0, t_1, \ldots, t_s$ 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 $j = 0, \ldots, s$, vale $f_j = \sum_i a_j^i f_{t_i} \in I$. □

Lemma 40.3 (Formula di Eulero)**.** *Se $f \in A[x_1, \ldots, x_s]$ 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 $j = 1, \ldots, s$ e f' omogeneo di grado $n-1$. Quindi per induzione

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

□

Esercizi

Esercizio 43. Sia $B = (b_{ij})$ una matrice le cui colonne sono linearmente dipendenti su A, provare che $\det(B)$ è un divisore di 0.

Esercizio 44. 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.)

Esercizio 45. 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).

Esercizio 46. 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).

Esercizio 47. 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.)

Esercizio 48. 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

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

Esercizio 49. (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 dedurne che p^{n-1} divide $qr' - rq'$.)

Esercizio 50. 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.

Esercizio 51. 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.

Esercizio 52. Provare che un dominio a fattorizzazione unica A è perfetto se e solo se per ogni $f \in A[t]$ irriducibile vale $\dfrac{df}{dt} \neq 0$.

Esercizio 53. Sia $A \to B$ un morfismo di anelli, $a, b \in B$ e siano $D, D' \colon B \to B$ due A-derivazioni; allora vale

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

Esercizio 54. Sia $\mathbb{Q} \to A$ un morfismo di anelli, $D \colon A \to A$ una $\mathbb{Q}$-derivazione e sia $x \in A$ tale che $Dx = 1$ e $\cap_{i=1}^{\infty}(x^i) = 0$. Provare che x non è un divisore di 0.

Esercizio 55. Enunciare e provare l'analogo della formula di Eulero (Lemma 40.3) per i polinomi isobari.

Esercizio 56. Sia $\mathbb{K}$ un campo di caratteristica 0 e $S = \mathbb{K}[x_1, \dots, x_n] = \oplus S_d$, dove S_d denota lo spazio vettoriale dei polinomi omogenei di grado d. Denotiamo $\partial_i = \dfrac{\partial}{\partial x_i} \colon S \to S$, per $i = 1, \dots, n$, le derivate parziali e $T = \mathbb{K}[\partial_1, \dots, \partial_n] = \oplus T_d$, 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 $S_d \times T_d \to \mathbb{K}$ 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.)

Esercizio 57 (Teorema di Macaulay)**.** (caratteristica 0) Nelle notazioni dell'Esercizio 56, 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) $f^\perp = \oplus I_d$. Sia $A = T/f^\perp = \oplus A_d$ dove $A_d = T_d/I_d$. Provare:

(3) $A_n = \mathbb{K}$ e $A_d = 0$ per ogni $d > n$.
(4) 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).

41. 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.

Lemma 41.1. *Per un insieme parzialmente ordinato $(S, \leq)$ le seguenti condizioni sono equivalenti.*

(1) *ogni sottoinsieme non vuoto di S possiede elementi massimali;*
(2) *ogni successione monotona non decrescente $x_0 \leq x_1 \leq \cdots$ in S è stazionaria, ossia esiste $m \in \mathbb{N}$ tale che $x_n = x_m$ per ogni $n \geq m$.*

Dimostrazione. Data una successione monotona non decrescente $x_0 \leq x_1 \leq \cdots$, se ogni sottoinsieme di S possiede elementi massimali, allora anche l'insieme $\{x_0, x_1, \ldots\}$ possiede un elemento massimale, diciamo x_m. Allora necessariamente $x_n = x_m$ per ogni $n \geq m$ e la successione è stazionaria.

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 $f\colon H \to H$ tale che $f(x) \in H_x$ per ogni $x \in H$. Preso comunque $x_0 \in H$, la successione $x_n = f^n(x_0)$ è monotona e non è stazionaria. □

Ricordiamo che una catena in un insieme parzialmente ordinato $(S, \leq)$ è un sottoinsieme che, con la relazione di ordine indotta, risulta essere un insieme totalmente ordinato. Una catena è detta **stazionaria** se possiede massimo.

Le nozioni di catena e catena stazionaria si applicano in particolare all'insieme degli ideali di un anello, ordinato per inclusione.

Definizione 41.2. Un anello in cui ogni ideale è finitamente generato si dice **Noetheriano**.

È chiaro dalla definizione che i campi e gli anelli ad ideali principali sono tutti Noetheriani.

Proposizione 41.3. *Sia A un anello Noetheriano e I un ideale. Allora l'anello quoziente A/I è Noetheriano.*

Dimostrazione. Siano $\pi\colon A \to A/I$ la proiezione al quoziente e $J \subset A/I$ un ideale. Allora l'ideale $\pi^{-1}(J)$ è finitamemte generato, diciamo $\pi^{-1}(J) = (a_1, \ldots, a_n)$. Ma allora, essendo $\pi^{-1}(J) \to J$ surgettiva si ha $J = (\pi(a_1), \ldots, \pi(a_n))$. □

È invece falso in generale che un sottoanello di un anello Noetheriano è ancora Noetheriano: ogni dominio di integrità non Noetheriano (Esempio 41.5) è un sottoanello del suo campo delle frazioni che è Noetheriano.

Lemma 41.4. *Per un anello A le seguenti condizioni sono equivalenti:*

(1) *A è Noetheriano;*
(2) *Ogni catena non vuota di ideali in A è stazionaria, ossia possiede massimo;*
(3) *Ogni successione non decrescente di ideali in A è stazionaria.*
(4) *Ogni famiglia non vuota di ideali di A contiene un elemento massimale.*

Dimostrazione. [1 $\Rightarrow$ 2] Sia $\{I_v \mid v \in V\}$ una catena di ideali e sia $I = \cup\{I_v \mid v \in V\}$. Allora I è un ideale che risulta finitamente generato, diciamo da $a_1, \ldots, a_n$. 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 I_w è il massimo della catena.

$[2 \Rightarrow 3]$ è ovvio e $[3 \Rightarrow 4]$ è una immediata applicazione del Lemma 41.1.

$[4 \Rightarrow 1]$ 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 $a \in J$. □

Esempio 41.5. L'anello delle funzioni olomorfe intere, ossia definite su tutto $\mathbb{C}$ è un dominio di integrità che non è Noetheriano. Il fatto che sia un dominio di integrità segue immediatamente dal fatto che le funzioni olomorfe sono sviluppabili in serie di potenze, mentre la prova che esiste un ideale che non è finitamente generato è una conseguenza del teorema di estensione di Riemann. La funzione $e^{2\pi iz} - 1$ è olomorfa e ha uno zero semplice in ciascun punto di $\mathbb{Z} \subset \mathbb{C}$, pertanto per ogni intero n la funzione

$$f_n(z) = \frac{e^{2\pi iz} - 1}{2\pi i(z - n)}$$

è olomorfa, $f_n(n) = 1$ e $f_n(m) = 0$ per ogni intero $m \neq n$. Per ogni intero positivo n, la funzione f_n non appartiene all'ideale generato da $f_1, \dots, f_{n-1}$ per il semplice fatto che $f_i(n) = 0$ per ogni $i < n$ mentre $f_n(n) \neq 0$. In particolare la catena di ideali

$$(f_1) \subset (f_1, f_2) \subset (f_1, f_2, f_3) \subset \cdots$$

non è stazionaria.

Teorema 41.6 (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 $g - (a_1 f_1^r + \cdots + a_j f_j^r)x^s$ ha grado minore del grado di g. Dato che $\sum a_i f_i^r \in H$ l'assurdo è servito. □

Corollario 41.7. *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 41.3. □

Teorema 41.8 (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 $f\colon A[t_1, \dots, t_r] \to A$ 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 $J_0 \subset J_1 \subset \cdots$ 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. □

Corollario 41.9. *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 $J = \cap_{n \geq 0} M^n$; per il lemma di Artin-Rees 41.8 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 $J = 0$. □

Corollario 41.10. *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 41.9 all'anello quoziente A/I ed al suo ideale massimale. □

Esercizi

Esercizio 58. Provare che l'anello delle funzioni continue $f\colon [0,1] \to \mathbb{R}$ non è Noetheriano.

Esercizio 59. Siano A un anello Noetheriano ed $E \subset A$ un sottoinsieme. Provare che esiste un sottoinsieme finito $E_0 \subset E$ tale che $(E) = (E_0)$.

Esercizio 60. Siano A un anello Noetheriano e $f\colon A \to A$ un endomorfismo surgettivo di anelli. Provare che f è un isomorfismo.

Esercizio 61. Sia A un anello e denotiamo con $\mathcal{D}$ la famiglia degli ideali di A che non sono finitamente generati. Provare che se $\mathcal{D} \neq \emptyset$, cioè se A non è Noetheriano, allora $\mathcal{D}$ contiene elementi massimali rispetto all'inclusione. Dimostrare inoltre gli elementi massimali di $\mathcal{D}$ 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 $(I : x) = \{y \in A \mid xy \in I\}$.)

Esercizio 62. Dimostrare che la famiglia degli ideali primi di un anello commutativo possiede elementi minimali rispetto all'inclusione.

42. Il risultante

Siano A un anello commutativo. L'obiettivo di questa sezione è quello di definire esplicitamente, per ogni polinomio *monico* $f \in A[x]$, un'applicazione

$$A[x] \to A, \qquad g \mapsto R(f,g),$$

che gode di alcune buone proprietà che saranno elencate a breve. L'elemento $R(f,g)$ verrà detto **risultante** di f e g e sarà definito come il determinante di una opportuna matrice a coefficienti in A.

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 Σ_n è il gruppo simmetrico delle permutazioni di $\{1, \dots, n\}$ e $(-1)^\sigma$ è la segnatura di σ. 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

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

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

(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 $\det(AB)=\det(A)\det(B)$.

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.

Consideriamo un polinomio $f(x)=x^d+a_1x^{d-1}+\cdots+a_d\in A[x]$ monico di grado $d\geq 0$.

Grazie al Lemma 39.4, per ogni $g\in A[x]$ esistono e sono unici dei polinomi $h_1,\dots,h_d\in A[x]$ ed una matrice $(r_{ij})\in M_{d,d}(A)$ a coefficienti in A tali che

$$x^{i-1}g=h_if+\sum_{j=1}^{d}r_{ij}x^{j-1},\qquad i=1,\dots,d\,. \tag{42.1}$$

Definiamo il **risultante** di f e g mediante la formula

$$R(f,g)=\det(r_{ij})\in A\,.$$

Lemma 42.1. *Per ogni $a\in A$ vale $R(f,a)=a^d$.*

Dimostrazione. Nelle notazioni di (42.1) si ha $h_i=0$ per ogni i e $(r_{ij})=aI$. □

Lemma 42.2. *Esistono due polinomi $\alpha,\beta\in A[x]$, con β di grado $<d$ tali che $R(f,g)=\alpha f+\beta g$. In particolare $R(f,g)$ appartiene all'intersezione di A con l'ideale (f,g) generato da f e g.*

Dimostrazione. Denotiamo con $(R^{ij})\in M_{n,n}(A)$ l'aggiunta classica della matrice (r_{ij}), allora si ha $(R^{ij})(r_{ij})=\det(r_{ij})I$ e quindi in particolare

$$\sum_{i=1}^{d}R^{1i}r_{i1}=R(p,q),\qquad \sum_{i=1}^{d}R^{1i}r_{ih}=0,\quad 2\leq h\leq d\,.$$

Ma allora

$$\sum_{i=1}^{d}R^{1i}(x^{i-1}g-h_if)=\sum_{i=1}^{d}\sum_{j=1}^{d}R^{1i}r_{ij}x^{j-1}=R(f,g)\,,$$

e basta considerare $\alpha=-\sum_{i=1}^{d}R^{1i}h_i$ e $\beta=\sum_{i=1}^{d}R^{1i}x^{i-1}$. □

Lemma 42.3. *Se esiste un polinomio $h\in A[x]$ di grado positivo che divide f e g, allora $R(f,g)=0$.*

Dimostrazione. Siccome h divide f il suo coefficiente direttore divide 1 in A ed è quindi invertibile. In particolare ogni elemento non nullo dell'ideale principale $(h)\subset A[x]$ è un polinomio di grado positivo e siccome $R(f,g)\in(f,g)\subset(h)$ ne consegue che $R(f,g)=0$. □

Lemma 42.4. *Se A è un dominio a fattorizzazione unica (ad esempio un campo) e $R(f,g)=0$, allora f e g possiedono un fattore comune di grado positivo.*

Dimostrazione. Se $R(f,g)=0$, allora esistono due polinomi $\alpha,\beta\in A[x]$, con β di grado $<d$ tali che $\alpha f+\beta g=0$. Siccome $\deg(\beta)<\deg(f)$ deve esistere un fattore irriducibile di f che divide g. □

Lemma 42.5. *Sia $\varphi\colon A\to B$ un omomorfismo di anelli ed estendiamolo nel modo naturale ad un omomorfismo di anelli*

$$\varphi\colon A[x]\to B[x],\qquad \varphi(\sum a_i x^i)=\sum \varphi(a_i)x^i\,.$$

Allora $R(\varphi(f),\varphi(g))=\varphi(R(f,g))$.

Dimostrazione. Basta osservare che ogni omomorfismo preserva le relazioni (42.1) e commuta con i determinanti. □

I lemmi precedenti descrivono solo una piccola parte delle ben proprietà del risultante, e sono tuttavia sufficienti per caratterizzare gli ideali primi dell'anello dei polinomi a coefficienti in un campo.

Proposizione 42.6. *Sia $\mathbb{K}$ un campo. Per un ideale proprio e non nullo $0\neq I\subset\mathbb{K}[x]$ le seguenti condizioni sono equivalenti:*

(1) *I è massimale,*
(2) *I è primo,*
(3) *I è generato da un polinomio irriducibile di grado positivo.*

Dimostrazione. Che ogni massimale è primo è una proprietà generale degli ideali. Siccome $\mathbb{K}[x]$ è un anello ad ideali principali, si ha $I=(f)$ per qualche polinomio f non nullo (poiché $I\neq 0$) e di grado positivo (poiché $I\neq\mathbb{K}[x]$). Se $f=gh$ con h,g di grado positivo, allora $h,g\notin I$, mentre $hg\in I$ e questo prova che I non è primo.

Per concludere, supponiamo f polinomio irriducibile di grado positivo e sia J un ideale proprio che contiene (f). Siccome ogni elemento non nullo di J ha grado >0, per ogni $g\in J$ si ha $R(f,g)\in\mathbb{K}\cap(f,g)\subset\mathbb{K}\cap J=0$ da cui segue che f divide g, ossia $g\in(f)$.

□

Siamo inoltre in grado di dimostrare alcuni risultati algebrici a prima vista alquanto tecnici ma dei quali faremo largo uso nei prossimi capitoli.

Lemma 42.7. *Siano 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 $\mathfrak{p}^e=\left\{\dfrac{p}{a}\;\middle|\; p\in\mathfrak{p},\ a\in A-\{0\}\right\}$. Sia $\dfrac{p_1}{a_1}\dfrac{p_2}{a_2}\in\mathfrak{p}^e$ 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 $q\in\mathfrak{p}$. □

Teorema 42.8. *Sia A un dominio di integrita e siano $0\neq\mathfrak{p}\subset\mathfrak{q}\subset A[x]$ ideali primi non nulli e tali che $\mathfrak{q}\cap A=0$. Allora $\mathfrak{p}=\mathfrak{q}$.*

Dimostrazione. Se $\mathbb{K}$ è il campo delle frazioni di A, per il Lemma 42.7 è sufficiente dimostrare che gli ideali primi $\mathfrak{p}^e\subset\mathfrak{q}^e\subset\mathbb{K}[x]$ coincidono. Ma questo segue immediatamente dal fatto che $0\neq\mathfrak{p}^e$ e quindi $\mathfrak{p}^e$, $\mathfrak{q}^e$ sono ideali massimali per la Proposizione 42.6. □

Corollario 42.9. *Sia A un anello commutativo e siano $\mathfrak{p}\subset\mathfrak{q}\subset A[x]$ ideali primi tali che $\mathfrak{p}$ contenga un polinomio monico. Allora $\mathfrak{p}\cap A=\mathfrak{q}\cap A$ se e solo se $\mathfrak{p}=\mathfrak{q}$.*

Dimostrazione. Basta chiaramente dimostrare che se $\mathfrak{p}\cap A=\mathfrak{q}\cap A$, allora $\mathfrak{p}=\mathfrak{q}$. Se $A\subset\mathfrak{p}$ allora $\mathfrak{p}=\mathfrak{q}=A[x]$ e quindi non è restrittivo supporre che $\mathfrak{r}=\mathfrak{p}\cap A$ sia un ideale primo proprio di A. Osserviamo che per ipotesi $\mathfrak{p}$ contiene un polinomio monico e quindi $\mathfrak{r}[x]\neq\mathfrak{p}$, dove con $\mathfrak{r}[x]$ si intende l'ideale dei polinomi a coefficienti in $\mathfrak{r}$.

Dimostriamo che non è restrittivo supporre A dominio di integrità e $\mathfrak{p}\cap A=\mathfrak{q}\cap A=0$. Sia infatti $\mathfrak{r}=\mathfrak{p}\cap A$, allora $\mathfrak{r}[x]\subset\mathfrak{p}\subset\mathfrak{q}$ e quindi $\mathfrak{p}=\mathfrak{q}$ se e solo se $\mathfrak{p}/\mathfrak{r}[x]=\mathfrak{q}/\mathfrak{r}[x]$.

Basta allora dimostrare il teorema per le proiezioni dei due ideali primi nell'anello quoziente $A[x]/\mathfrak{r}[x] = (A/\mathfrak{r})[x]$, e questo segue dal Teorema 42.8.

□

Lemma 42.10. *Siano A, $\mathfrak{p} \subset A[x]$ come nel Lemma 42.7. Allora esiste $f \in \mathfrak{p}$ tale che $R(f,g) \neq 0$ per ogni $g \notin \mathfrak{p}$.*

Dimostrazione. Per il Lemma 42.7 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 $R(f,g) \neq 0$. □

Teorema 42.11. *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 42.10. □

Corollario 42.12. *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 42.11 esisterebbe $f \in \mathfrak{p}_1$ tale che $R(f,g) \notin \mathfrak{q}$ in contraddizione con il fatto che $R(f,g) \in (f,g) \subset \mathfrak{p}_2$. □

43. Il teorema degli zeri di Hilbert

Sia $\mathbb{K}$ un campo (infinito) fissato e $\mathbb{A}^n \cong \mathbb{K}^n$ lo spazio affine su $\mathbb{K}$ di dimensione n.
Il **luogo di zeri** di un sottoinsieme $E \subset \mathbb{K}[x_1, \dots, x_n]$ è definito come

$$Z(E) = \{(a_1, \dots, a_n) \in \mathbb{A}^n \mid f(a_1, \dots, a_n) = 0 \text{ per ogni } f \in E\}.$$

È chiaro dalla definizione che se $E \subset F$ allora $Z(F) \subset Z(E)$. Osserviamo inoltre che se (E) è l'ideale generato da E, allora E ed (E) hanno lo stesso luogo di zeri, cioè $Z(E) = Z((E))$. Infatti $E \subset (E)$ e quindi $Z((E)) \subset Z(E)$; viceversa se $p \in Z(E)$ e $g \in (E)$ si può scrivere $g = a_1 f_1 + \cdots + a_n f_n$ con $a_i \in \mathbb{K}[x_1, \dots, x_n]$ e $f_i \in E$ e quindi

$$f_i(p) = 0 \quad \text{per ogni } i \;\Rightarrow\; g(p) = \sum_i a_i(p) f_i(p) = 0\,.$$

Ne segue che non è restrittivo considerare esclusivamente luoghi di zeri di ideali di $\mathbb{K}[x_1, \dots, x_n]$.

Definizione 43.1. Un sottoinsieme $X \subset \mathbb{K}^n$ si dice **algebrico** se è $X = Z(I)$ per qualche ideale $I \subset \mathbb{K}[x_1, \dots, x_n]$.

L'immagine inversa di un insieme algebrico per un'applicazione lineare è ancora algebrico: sia $A\colon \mathbb{K}^n \to \mathbb{K}^m$ un'applicazione lineare, definita da una matrice (a_{ij}) e sia $f \in \mathbb{K}[y_1, \dots, y_m]$. Un punto $p \in \mathbb{K}^n$ appartiene a $A^{-1}(Z(f))$ se e solo se $f(Ap) = 0$ ossia se e solo se $p \in Z(fA)$ e basta osservare che fA è la funzione polinimiale associata al polinomio

$$g(x_1, \dots x_n) = f(\sum_i a_{1i} x_i, \dots, \sum_i a_{mi} x_i)\,.$$

Invece, gli insiemi algebrici non sono preservati dalle immagini dirette per applicazioni lineari. Si consideri ad esempio l'iperbole $X \subset \mathbb{K}^2$ di equazione $x_1 x_2 - 1 = 0$ e la proiezione $\pi\colon \mathbb{K}^2 \to \mathbb{K}$ sulla prima coordinata; allora $\pi(X) = \{x_1 \neq 0\}$ che non è un sottoinsieme algebrico (l'unico polinomio che si annulla su $\mathbb{K} - \{0\}$ è quello nullo e quindi $Z(f) \supset \mathbb{K} - \{0\}$ se e solo se $f = 0$). Come illustrato nel prossimo Teorema 43.2 il motivo di ciò consiste nel fatto che l'ideale generato da $x_1 x_2 - 1$ non contiene polinomi monici rispetto a x_2.

Teorema 43.2 (di proiezione generica)**.** *Siano $\mathbb{K}$ un campo* algebricamente chiuso *e $I \subset \mathbb{K}[x_1, \dots, x_n]$ un ideale che contiene un polinomio monico di grado positivo rispetto alla variabile x_n. Siano $J = I \cap \mathbb{K}[x_1, \dots, x_{n-1}]$ e $\pi\colon \mathbb{K}^n \to \mathbb{K}^{n-1}$ la proiezione sulle prime $n-1$ coordinate. Allora l'applicazione $\pi\colon Z(I) \to Z(J)$ è surgettiva.*

Dimostrazione. È chiaro dalle definizioni che $\pi(Z(I)) \subset Z(J)$ e pertanto l'applicazione $\pi\colon Z(I) \to Z(J)$ è ben definita. Sia $(a_1, \dots, a_{n-1}) \in Z(J)$ e consideriamo l'omomorfismo surgettivo di anelli

$$\epsilon\colon \mathbb{K}[x_1, \dots, x_n] \to \mathbb{K}[x], \qquad \epsilon(p) = p(a_1, \dots, a_{n-1}, x)\,.$$

Dato che ϵ è surgettivo l'immagine $\epsilon(I)$ è un ideale; dato che $\mathbb{K}[x]$ è un dominio ad ideali principali si ha $\epsilon(I) = (h)$ con $h = 0$ oppure polinomio monico di grado $d \geq 0$.

Mostriamo che l'ipotesi h monico di grado 0, ossia $h = 1$ conduce ad una contraddizione. Se così fosse esisterebbe $g \in I$ tale che $\epsilon(g) = 1$. Usiamo adesso l'ipotesi che I contiene un polinomio f monico di grado positivo rispetto a x_n e consideriamo il risultante $R(f, g)$ (a tal fine si considera $\mathbb{K}[x_1, \dots, x_n] = A[x_n]$ dove $A = \mathbb{K}[x_1, \dots, x_{n-1}]$). Per le proprietà del risultante $R(f, g) \in (f, g) \cap A \subset J$ e quindi, siccome $(a_1, \dots, a_{n-1}) \in Z(J)$ si ha $\epsilon(R(f, g)) = 0$. D'altra parte $\epsilon(R(f, g)) = R(\epsilon(f), \epsilon(g)) = R(\epsilon(f), 1) = 1$ dato che anche $\epsilon(f)$ è monico.

Dunque $h = 0$ oppure h ha grado positivo: in entrambi i casi esiste $a_n \in \mathbb{K}$ tale che $h(a_n) = 0$, da cui $\epsilon(q)(a_n) = q(a_1, \dots, a_n) = 0$ per ogni $q \in I$, ossia $(a_1, \dots, a_n) \in Z(I)$. □

Lemma 43.3 (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'insieme $\mathbb{K}^n - Z(f) = \{a \in \mathbb{K}^n \mid f(a) \neq 0\}$ 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.*

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 $a \in \mathbb{K}^{n-1}$ 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 $a \in \mathbb{K}^n$ 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 si ha $f_d(0, \dots, 0, y_n) = f_d(a) y_n^d$, dunque il polinomio $f(0, \dots, 0, y_n)$ ha grado d e basta quindi prendere come costante $c = 1/f_d(a)$. □

Corollario 43.4 (Forma debole del Teorema degli zeri di Hilbert)**.** *Siano $\mathbb{K}$ un campo* algebricamente chiuso *e $I \subset \mathbb{K}[x_1, \dots, x_n]$ un ideale* proprio*. Allora $Z(I) \neq \emptyset$.*

Dimostrazione. Prima di procedere alla dimostrazione mostriamo che entrambe le ipotesi sul campo e sull'ideale sono necessarie. Se l'ideale I non è proprio, allora $1 \in I$ e di conseguenza $Z(I) \subset Z(1) = \emptyset$. Se il campo $\mathbb{K}$ non è algebricamente chiuso esiste un polinomio di grado positivo $f \in \mathbb{K}[x]$ tale che $Z(f) = \emptyset$, mentre l'ideale (f) è proprio.

Dimostriamo il teorema per induzione su n, essendo il caso $n = 0$ banalmente verificato. Supponiamo quindi vero il teorema per polinomi in $n - 1$ variabili.
L'enunciato è inoltre ovvio se $I = 0$; assumiamo quindi $I \neq 0$, allora per il lemma di preparazione, a meno di automorfismi lineari di $\mathbb{K}^n$, possiamo supporre che esista $f \in I$ polinomio monico rispetto alla variabile x_n. Consideriamo l'intersezione $J = I \cap \mathbb{K}[x_1, \dots, x_{n-1}]$, siccome $1 \notin J$ per l'ipotesi induttiva $\emptyset \neq Z(J) \subset \mathbb{K}^{n-1}$ mentre per il teorema di proiezione generica esiste un'applicazione surgettiva $Z(I) \to Z(J)$. □

Riepilogando, abbiamo definito un'applicazione

$$Z\colon \{\text{ideali di } \mathbb{K}[x_1, \dots, x_n]\} \to \{\text{sottoinsiemi algebrici di } \mathbb{K}^n\}$$

che è surgettiva per definizione ma si guarda bene dall'essere iniettiva per ogni $n > 0$. Ad esempio gli ideali (x_1) ed (x_1^2) sono distinti ma definiscono lo stesso luogo di zeri.

Vogliamo adesso andare nella direzione opposta e definire un'applicazione iniettiva

$$I\colon \{\text{sottoinsiemi algebrici di } \mathbb{K}^n\} \to \{\text{ideali di } \mathbb{K}[x_1, \dots, x_n]\}$$

con l'ulteriore proprietà di essere un'inversa destra di Z, ossia $ZI = Id$.

Più in generale, dato un qualsiasi sottoinsieme $X \subset \mathbb{K}^n$, si definisce

$$I(X) = \{f \in \mathbb{K}[x_1, \dots, x_n] \mid f(a) = 0 \quad \text{per ogni } a \in X\}.$$

Segue immediatamente dalle definizioni di I e Z che per ogni sottoinsieme $X \subset \mathbb{K}^n$ si ha $X \subset Z(I(X))$ e che per ogni ideale $J \subset \mathbb{K}[x_1, \ldots, x_n]$ vale $J \subset I(Z(J))$.

Lemma 43.5. *Nelle notazioni precedenti, per ogni ideale $J \subset \mathbb{K}[x_1, \ldots, x_n]$ vale $Z(J) = Z(I(Z(J)))$; equivalentemente la composizione ZI è l'identità sull'insieme dei chiusi algebrici.*

Dimostrazione. La relazione $X \subset Z(I(X))$ applicata a $X = Z(J)$ dà $Z(J) \subset Z(I(Z(J)))$, mentre l'inclusione $J \subset I(Z(J))$ implica $Z(J) \supset Z(I(Z(J)))$. □

L'applicazione I soddisfa inoltre le seguenti proprieà:

(1) $I(\emptyset) = \mathbb{K}[x_1, \ldots, x_n]$ e $I(\mathbb{K}^n) = 0$;
(2) Se $X \subset Y$, allora $I(Y) \subset I(X)$;
(3) Per ogni sottoinsieme $X \subset \mathbb{K}^n$ l'ideale $I(X)$ è radicale, ossia $I(X) = \sqrt{I(X)}$;
(4) Per ogni ideale $J \subset \mathbb{K}[x_1, \ldots, x_n]$, vale $\sqrt{J} \subset I(Z(J))$.

L'inclusione del punto 4) è in generale propria: ad esempio, se $\mathbb{K} = \mathbb{R}$, $n = 1$ e $J = (x^2+1)$, allora $Z(J) = \emptyset$ e $I(Z(J)) = \mathbb{R}[x] \neq \sqrt{J}$.

Corollario 43.6. *Sia $\mathbb{K}$ un campo algebricamente chiuso, allora gli ideali massimali di $\mathbb{K}[x_1, \ldots, x_n]$ sono tutti e soli gli ideali del tipo $I(p)$, al variare di $p \in \mathbb{K}^n$. Esiste dunque una bigezione naturale fra $\mathbb{K}^n$ e l'insieme degli ideali massimali di $\mathbb{K}[x_1, \ldots, x_n]$.*

Dimostrazione. Sia $\mathfrak{m} \subset \mathbb{K}[x_1, \ldots, x_n]$ massimale, per la forma debole del teorema degli zeri di Hilbert $Z(\mathfrak{m}) \neq \emptyset$. Dato un qualunque punto $p \in Z(\mathfrak{m})$ vale allora $\mathfrak{m} \subset I(p)$ da cui segue $\mathfrak{m} = I(p)$ e quindi $Z(\mathfrak{m}) = ZI(p) = \{p\}$.

Viceversa se $p \in \mathbb{K}^n$ e $I(p) \subset \mathfrak{m}$, con $\mathfrak{m}$ massimale, allora esiste $q \in \mathbb{K}^n$ tale che $I(p) \subset \mathfrak{m} = I(q)$, da cui $\{q\} \subset \{p\}$ e quindi $p = q$. □

Teorema 43.7 (degli zeri di Hilbert (1892))**.** *Se il campo $\mathbb{K}$ è algebricamente chiuso, allora per ogni ideale $J \subset \mathbb{K}[x_1, \ldots, x_n]$ vale $\sqrt{J} = I(Z(J))$.*

Dimostrazione. Segue immediatamente dalle definizioni che $\sqrt{J} \subset I(Z(J))$. Sia quindi $f \in I(Z(J))$ e denotiamo con F la classe di f nell'anello quoziente $A = \mathbb{K}[x_1, \ldots, x_n]/J$. Vogliamo dimostrare che $f^n \in J$,o equivalentemente che $F^n = 0$, per qualche $n > 0$. Per il Lemma 39.1 tale condizione è equivalente all'invertibilità di $1-tF$ nell'anello $A[t]$. Denotiamo con $\pi\colon \mathbb{K}[x_1, \ldots, x_n, t] \to A[t]$ l'omomorfismo surgettivo tale che $\pi(t) = t$ e $\pi\colon \mathbb{K}[x_1, \ldots, x_n] \to A$ è la proiezione al quoziente.

Si consideri adesso l'ideale $H \subset \mathbb{K}[x_1, \ldots, x_n, t]$ generato da J e $1 - tf$ e si osservi che $Z(H) = \emptyset$. Infatti se per assurdo esiste $(a_1, \ldots, a_n, b) \in Z(H)$, allora $g(a_1, \ldots, a_n) = 0$ per ogni $g \in J$ e quindi $(a_1, \ldots, a_n) \in Z(J)$; dato che $f \in I(Z(J))$ si ha dunque $f(a_1, \ldots, a_n) = 0$ e quindi $1 - bf(a_1, \ldots, a_n) = 1$ in contraddizione con $1 - tf \in H$.

Dunque per la forma debole del teorema degli zeri l'ideale H non è proprio; a maggior ragione l'ideale $\pi(H)$ nell'anello quoziente $A[t]$ contiene 1. Siccome $\pi(J) = 0$ si ha $A[t] = \pi(H) = (1 - tF)$ e quindi $1 - tF$ è invertibile. □

Il teorema degli zeri per le ipersuperfici 32.9 segue immediatamente dal Teorema 43.7.

Corollario 43.8. *Supponiamo $\mathbb{K}$ algebricamente chiuso e siano $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ con f irriducibile. Se $Z(f) \subset Z(g)$, allora f divide g.*

Dimostrazione. Per il teorema degli zeri vale $g \in I(Z(f)) = \sqrt{(f)} = (f)$. □

Ricordiamo che un ideale $J \subset \mathbb{K}[x_1, \ldots, x_n]$ si dice omogeneo se è generato da polinomi omogenei; se $S_d \subset \mathbb{K}[x_1, \ldots, x_n]$ denota il sottospazio vettoriale dei polinomi omogenei di grado d si verifica facilmente che J è omogeneo se e solo se $J = \oplus(J \cap S_d)$. Sia infine $0 = (0, \ldots, 0) \in \mathbb{K}^n$; notiamo che se J è omogeneo e $Z(J) \neq \emptyset$, allora $0 \in Z(J)$.

Corollario 43.9 (Teorema degli zeri omogeneo)**.** *Se il campo $\mathbb{K}$ è algebricamente chiuso e $J \subset \mathbb{K}[x_1, \ldots, x_n]$ è un ideale omogeneo proprio, allora $Z(J) = \{0\}$ se e solo se esiste $d > 0$ tale che $S_d \subset I$.*

Dimostrazione. Se $S_d \subset J$, allora per ogni i si ha $x_i^d \in J$, quindi $x_i \in \sqrt{J}$ e perciò $Z(J) = Z(\sqrt{J}) = \{0\}$.

Viceversa, se $Z(J) = \{0\}$, allora per il teorema degli zeri $\sqrt{J} = I(\{0\}) = (x_1, \ldots, x_n)$. Esiste dunque $d > 0$ tale che $x_i^d \in J$ per ogni i e quindi $S_{dn-n+1} \subset J$. □

Esercizi

Esercizio 63. 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 $f(x, y, z) - f(0, y, z) - f(x, 0, z) - f(x, y, 0)$.)

Esercizio 64. Dimostrare che ogni ideale primo di $\mathbb{C}[x_1, \ldots, x_n]$ è intersezione di ideali massimali.

Esercizio 65. Sia $F \subset L$ una estensione di campi e siano $f_1, \ldots, f_n \in F[x_1, \ldots, x_n]$. Usare il teorema di Rouché-Capelli per dimostrare che $f_1, \ldots, f_n$ generano un ideale proprio di $F[x_1, \ldots, x_n]$ se e solo se generano un ideale proprio di $L[x_1, \ldots, x_n]$.

Esercizio 66. Sia $\mathbb{K} = \overline{F}$ una chiusura algebrica di un campo F e sia $J \subset F[x_1, \ldots, x_n]$ un ideale proprio e si denoti $L = F[x_1, \ldots, x_n]/J$. Dimostrare che se l'anello L è un campo, allora L è isomorfo ad un sottocampo di $\mathbb{K}$, ossia L è una estensione algebrica di F.(Sugg.: applicare l'Esercizio 65 alla coppia $F \subset \mathbb{K}$ ed usare la caratterizzazione degli ideali massimali di $\mathbb{K}[x_1, \ldots, x_n]$.)

Riferimenti bibliografici

[1] Bauer, U., Lesnick, M.: Persistence Diagrams as Diagrams: A Categorification of the Stability Theorem. arxiv:1610.10085.
[2] Carlsson, G.: Topology and data. Bull. AMS Volume **46**, Number 2, 255-308 (2009).
[3] Deo, S.: Algebraic Topology, a Primer. Springer (2018).
[4] Dold, A.: Lectures on algebraic topology. Second edition, Springer, Berlin Heidelberg New York (1980).
[5] Edelsbrunner, H.: A short course in computational geometry and topology.
[6] Edelsbrunner, H., Harer, J.: Persistent Homology - a survey. Contemporary Mathematics **453**, pp. 257-282 (2008).
[7] Edelsbrunner, H., Morozov, D.: Persistent Homology: Theory and Practice. Proceedings of the European Congress of Mathematics, 2012, pp. 31-50.
[8] P.R. Halmos: Naive set theory. D. Van Nostrand Co. Princeton, N.J. (1960).
[9] Greenberg, M., Harper, J.: Algebraic Topology: A First Course. Addison-Wesley (1981).
[10] Hatcher, A.: Algebraic Topology. (2001).
[11] Hilton P.J., Stammbach U.: A Course in Homological Algebra. Second Edition, Springer (1997).
[12] Nathan Jacobson: Basic Algebra, I. San Francisco (1974).
[13] Manetti, M.: Topologia, seconda edizione, Springer (2014)
[14] Yuri I. Manin, Matilde Marcolli: Nori diagrams and persistent homology. arXiv:1901.10301.
[15] Paparozzi, V.: Omologia persistente applicata allo studio del connettoma. Tesi di Laurea in Matematica, Roma (2018).
[16] Ashley Suh, Mustafa Hajij, Bei Wang, Carlos Scheidegger, and Paul Rosen: Persistent Homology Guided Force-Directed Graph Layouts. arXiv:1712.05548
[17] Spanier, E.H.: Algebraic topology. McGraw-Hill (1966).
[18] Vick, J.W.: Homology theory. Springer, Berlin Heidelberg New York (1994).
[19] Weinberger, S.: What is Persistent Homology? Notices of the AMS, Volume **58**, Number 1, 36–39 (2011)