Corso di Algebra Superiore

Docente: Guido Pezzini

a.a. 2020/2021

Appunti

versione del 22.1.2021

1. Introduzione

Uno degli obiettivi principali del corso è quello di studiare dal punto di vista algebrico e geometrico quozienti del tipo X/G, dove X è uno spazio topologico e G è un gruppo che agisce su X. Doteremo X e G di strutture aggiuntive, es. varietà differenziabili o varietà algebriche, studieremo la possibilità di dotare il quoziente X/G (o spazi topologici ad esso legati) strutture simili a quelle date in partenza su X e G.

Vedremo che la teoria delle rappresentazioni di G avrà un ruolo centrale. Questo ci porterà ad approfondire aspetti più algebrici, come la teoria delle rappresentazioni delle algebre associative e la teoria classica degli invarianti.

1.1. **Azioni di gruppi su insiemi: terminologia.** Siano G un gruppo e X un insieme.

Definizione 1.1. Un'*azione* di G su X è un omomorfismo φ di gruppi da G nel gruppo delle biiezioni di X in se stesso. Spesso viene denotata anche come

$$\begin{array}{ccc} G \times X & \to & X \\ (g,x) & \mapsto & \varphi(g)(x) \end{array}$$

e, se non si dà luogo ad ambiguità, l'elemento $\varphi(g)(x)$ si scrive anche come $g \cdot x$ oppure gx.

Data un'azione di G su X, ricordiamo le seguenti definizioni.

Definizione 1.2. Dato un elemento $x \in X$, si definisce lo *stabilizzatore*

$$G_x = \{g \in G \mid gx = x\}$$

di x in G, e l'*orbita*

$$G \cdot x = \{gx \mid g \in G\}$$

di x. Si definisce inoltre il sottoinsieme X^G degli elementi di X *fissati* da G, cioè tali che la loro orbita contiene un solo punto. Infine, dati sottoinsiemi $Y \subseteq X$ e $H \subseteq G$, si dice che Y è *stabilizzato* da H se $h \cdot y \in Y$ per ogni $h \in H$ e $y \in Y$.

Ricordiamo che G_x come sopra è un sottogruppo di G, e il quoziente G/G_x è in biiezione con l'orbita $G \cdot x$ tramite $gG_x \mapsto gx$.

Definizione 1.3. Sia Z un insieme. L'azione di G su X induce un'azione sull'insieme Z^X delle applicazioni $X \to Z$, tramite la formula

$$(gf)(x) = f(g^{-1}x)$$

per $f \in X^Z$, $g \in G$, $x \in X$.

Definizione 1.4. Se X è uno spazio vettoriale, e $\varphi(g)$ è lineare per ogni $g \in G$, allora X si dice un G-*modulo*, e $\varphi\colon G \to \mathrm{GL}(X)$ si dice una *rappresentazione* di G.

1.2. **Esempi fondamentali: lo spazio proiettivo, le Graßmanniane.** Gli spazi proiettivi reali e complessi[1] hanno struttura naturale di varietà differenziabili. Sia $k = \mathbb{R}$ oppure $\mathbb{C}$, e sia n intero positivo. Le carte locali su $\mathbb{P}^n = \mathbb{P}^n_k$ sono date sugli aperti

$$U_i = \{[x_0, \ldots, x_i, \ldots, x_n] \mid x_i \neq 0\}$$

per $i \in \{0, \ldots, n\}$, tramite $[x_0, \ldots, x_{i-1}, x_i, x_{i-1}, \ldots, x_n] \mapsto (x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i)$.

[1] In quest'introduzione, considereremo $\mathbb{R}^n$ e $\mathbb{C}^n$ dotati della usuale topologia euclidea.

Questa struttura è fornita ad hoc, e non è legata all'usuale presentazione di $\mathbb{P}^n$ come quoziente di $k^n \smallsetminus \{0\}$ per il gruppo delle omotetie k^*. D'altronde è facile costruire esempi di azioni di $\mathbb{R}^*$ o $\mathbb{C}^*$ su varietà differenziabili, in modo che il quoziente non sia dotabile di una struttura di varietà differenziabile, ad esempio il quoziente può non essere uno spazio topologico di Hausdorff (esercizio!).

Analogamente si comporta la Graßmanniana $\mathrm{Gr}(d, n)$ dei sottospazi vettoriali d-dimensionali in k^n (con $1 \leq k \leq n$).

Un tale sottospazio $W \subseteq k^n$ si può pensare descritto da una sua base $(w_1, \ldots, w_d)$. Scriviamo le loro entrate in una matrice, con i vettori scritti in colonna, e scegliamo indici $i_1, \ldots, i_d$ in modo che il minore $d \times d$ con le righe $i_1, \ldots, i_d$ sia invertibile. A meno di cambiare base di W, possiamo supporre che questo minore sia la matrice identità. Ad esempio con $i_1 = 1, \ldots, i_d = d$:

$$\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \\ a_{d+1,1} & a_{d+1,2} & \cdots & a_{d+1,d} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,d} \end{pmatrix}$$

Le entrate delle righe rimanenti (qui, le entrate da $a_{d+1,1}$ fino a $a_{n,d}$) forniscono la carta locale, definita sull'aperto di tutti i sottospazi le cui basi hanno la proprietà "il minore delle righe $i_1, \ldots, i_d$ è invertibile".

Esercizio 1.5. Esprimere le carte locali come funzioni delle entrate di tutta la matrice, senza supporre di aver reso il blocco $d \times d$ uguale alla matrice identità. In altre parole, generalizzare alle Graßmanniane la formula data qui sopra per le carte locali dello spazio proiettivo.

Anche questa definizione è data ad hoc. Vedremo nel corso che si può dare la stessa struttura a $\mathbb{P}^n$ e $\mathrm{Gr}(d, n)$ usando invece l'azione naturale di $\mathrm{GL}(n)$ su questi due insiemi, con una costruzione del tutto generale. Questo sarà reso possibile dal fatto che $\mathrm{GL}(n)$ agisce **transitivamente** in entrambi i casi.

1.3. **Un altro esempio fondamentale.** Sia $X = \mathbb{R}^n$ e G il gruppo simmetrico S_n, che agisce su X permutando le entrate degli elementi.

Ad esempio per $n = 2$, l'azione di G identifica nel quoziente i punti di $\mathbb{R}^2$ simmetrici rispetto alla bisettrice del primo e del terzo quadrante. Quindi X/G non sembra dotato di struttura di varietà differenziabile, semmai di varietà con bordo: potremmo identificarlo con uno dei due semipiani chiusi definiti da questa bisettrice.

Definiamo

$$\begin{array}{cccc} \varphi\colon & \mathbb{R}^2 & \to & \mathbb{R}^2 \\ & (x, y) & \mapsto & (x + y, xy). \end{array}$$

L'immagine di questa applicazione è la regione di piano $Q \subset \mathbb{R}^2$ definita dalla condizione $y \leq x^2/4$, e le controimmagini dei punti di questa regione sono esattamente le orbite di G. Inoltre effettivamente Q è omeomorfa ad un semipiano chiuso, ed è omeomorfa al quoziente $\mathbb{R}^2/S_2$ (esercizio). Quindi φ si può considerare come una "realizzazione concreta" del quoziente

$$\pi\colon \quad \mathbb{R}^2 \quad \to \quad \mathbb{R}^2/S_2$$

tramite le funzioni **simmetriche** xy e $x + y$.

Avere usato funzioni simmetriche ovviamente non è un caso. Nelle prossime sezioni ci focalizzeremo su questo punto di vista e studieremo le funzioni simmetriche polinomiali. Questo permetterà inoltre di mostrare come il quoziente $\mathbb{C}^n/S_n$ abbia una struttura molto semplice.

1.4. **Le funzioni simmetriche elementari.** Fissiamo un anello commutativo R e un intero positivo n, e consideriamo l'anello dei polinomi $R[x_1, \ldots, x_n]$ in n variabili. Facciamo agire S_n su $R[x_1, \ldots, x_n]$ permutando le variabili. I polinomi simmetrici sono i polinomi lasciati fissi dall'azione di S_n, e formano un sottoanello che denotiamo con $R[x_1, \ldots, x_n]^{S_n}$ in accordo con la notazione ricordata prima.

Definizione 1.6. Sia n un intero positivo. Le *funzioni simmetriche elementari* in n variabili $x_1, \ldots, x_n$ sono definite come

$$\begin{aligned}
\sigma_1 &= x_1 + \ldots + x_n, \\
\sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n, \\
&\vdots \\
\sigma_k &= \sum_{1 \le i_1 < i_2 < \ldots < i_k \le n} x_{i_1}x_{i_2}\ldots x_{i_k}, \\
&\vdots \\
\sigma_n &= x_1x_2\ldots x_n.
\end{aligned}$$

Per sottolineare il fatto che consideriamo n variabili, useremo anche la notazione $\sigma_i^{(n)}$ invece che solo σ_i.

Teorema 1.7. *L'anello dei polinomi simmetrici $R[x_1, \ldots, x_n]^{S_n}$ è esso stesso un anello di polinomi, negli elementi $\sigma_1, \ldots, \sigma_n$.*

In altre parole, fissando variabili $y_1, \ldots, y_n$, l'omomorfismo di anelli $R[y_1, \ldots, y_n] \to R[x_1, \ldots, x_n]^{S_n}$ che manda y_i in σ_i per ogni i è un isomorfismo.

Dimostrazione. Procediamo per induzione su n. Il caso $n = 1$ è ovvio, visto che $\sigma_1^{(1)} = x_1$, e $R[x_1]^{S_1} = R[x_1]$. Dimostriamo il passo induttivo, supponendo $n > 1$ e dimostrando che ogni $f \in R[x_1, \ldots, x_n]^{S_n}$ si scrive in modo unico come polinomio in $\sigma_1^{(n)}, \ldots, \sigma_n^{(n)}$. Procediamo anche per induzione sul grado di f (il caso di grado 0 è banale).

Consideriamo l'omomorfismo $\rho\colon R[x_1, \ldots, x_n] \to R[x_1, \ldots, x_{n-1}]$ che pone x_n a zero, cioè manda $f(x_1, \ldots, x_n)$ in $f(x_1, \ldots, x_{n-1}, 0)$. Osserviamo che ρ manda $R[x_1, \ldots, x_n]^{S_n}$ in $R[x_1, \ldots, x_{n-1}]^{S_{n-1}}$, e che $\rho(\sigma_i^{(n)}) = \rho(\sigma_i^{(n-1)})$ per ogni $i < n$.

Sia $f \in R[x_1, \ldots, x_n]^{S_n}$, e consideriamo $\rho(f)$. Se $\rho(f) = 0$, allora ogni monomio di f contiene x_n, cioè f è divisibile per x_n, e per simmetria è divisibile per $\sigma_n^{(n)}$. Il quoziente $f/\sigma_n^{(n)}$ è un polinomio simmetrico di grado inferiore ad f, per cui si scrive in modo unico come polinomio in $\sigma_1^{(n)}, \ldots, \sigma_n^{(n)}$. Lo stesso segue per f.

Se invece $\rho(f) \neq 0$, allora per ipotesi induttiva (su n) esiste un unico polinomio p in $n-1$ variabili tale che

$$p\left(\sigma_1^{(n-1)}, \ldots, \sigma_{n-1}^{(n-1)}\right) = \rho(f).$$

Segue che

$$g = f - p\left(\sigma_1^{(n)}, \ldots, \sigma_{n-1}^{(n)}\right)$$

è un polinomio tale che $\rho(g) = 0$. Per la prima parte della dimostrazione, g si scrive in modo unico come polinomio in $\sigma_1^{(n)}, \ldots, \sigma_n^{(n)}$, e lo stesso segue per f. □

Questo teorema fornisce uno strumento per studiare il quoziente R^n/S_n, perché considerando i polinomi come funzioni su R^n, quelli simmetrici sono proprio quelli che "passano al quoziente".

Nel caso $R = \mathbb{C}$ (o un qualsiasi campo algebricamente chiuso), il fatto che $\mathbb{C}[x_1, \ldots, x_n]^{S_n}$ sia un anello di polinomi in n variabili, cioè l'anello dei polinomi su $\mathbb{C}^n$, è sufficiente a concludere che $\mathbb{C}^n/S_n$ è proprio identificabile con $\mathbb{C}^n$. Questo grazie a risultati di base di geometria algebrica, che ricorderemo più avanti. Nella prossima sezione diamo un'interpretazione alternativa di questo fatto.

1.5. **Funzioni simmetriche e radici dei polinomi.** Sia n un intero positivo e siano $p_1, \ldots, p_n \in \mathbb{C}$. Sono esattamente le radici del polinomio monico

$$f_{p_1,\ldots,p_n}(x) = \prod_{i=1}^{n}(x - p_i),$$

inoltre questo è l'unico polinomio monico che ha esattamente quelle radici, e per il teorema fondamentale dell'algebra ogni polinomio monico su $\mathbb{C}$ si ottiene in questo modo.

Visto che le radici di un polinomio non hanno un ordine prestabilito, considerare il polinomio $f_{p_1,\ldots,p_n}(x)$ invece dei numeri complessi $p_1, \ldots, p_n$ equivale effettivamente a prendere $p_1, \ldots, p_n$ *a meno di permutazioni.* D'altronde, l'insieme dei polinomi monici di grado n è in biiezione proprio con $\mathbb{C}^n$, prendendo i coefficienti dei polinomi.

Abbiamo dunque realizzato il quoziente nel modo seguente

$$\begin{array}{ccc} \mathbb{C}^n & \to & \mathbb{C}^n/S_n \cong \mathbb{C}^n \\ (p_1, \ldots, p_n) & \mapsto & f_{p_1,\ldots,p_n}(x). \end{array} \tag{1.1}$$

In realtà, in coordinate, stiamo facendo esattamente la stessa cosa della sezione precedente. Infatti, svolgendo il prodotto otteniamo

$$x^n - (p_1 + \ldots + p_n)x^{n-1} + (p_1p_2 + p_1p_3 + \ldots + p_{n-1}p_n)x^{n-2} \ldots + (-1)^n(p_1 \ldots p_n),$$

e si riconoscono le funzioni simmetriche elementari, calcolate nei valori $p_1, \ldots, p_n$ e cambiate di segno in modo alterno.

Vale la pena evidenziare che abbiamo dimostrato la seguente

Proposizione 1.8. *I coefficienti di un polinomio monico $f \in \mathbb{C}[x]$, presi a segni alterni, sono uguali alle funzioni simmetriche elementari calcolate nelle radici del polinomio.*

Possiamo dedurne un corollario molto utile.

Corollario 1.9. *Per ogni intero positivo n esiste un polinomio $D \in \mathbb{C}[x_1, \ldots, x_n]$ tale che, preso un qualsiasi polinomio monico $f \in \mathbb{C}[x]$ di grado n,*

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_n$$

si ha $D(a_1, \ldots, a_n) \neq 0$ se e solo se f ha tutte radici distinte.

Dimostrazione. Consideriamo il seguente polinomio simmetrico nelle variabili $y_1, \ldots, y_n$:

$$C(y_1, \ldots, y_n) = \prod_{1 \le i < j \le n} (y_i - y_j)^2$$

Osserviamo che C si annulla esattamente quando almeno una coppia di variabili y_i, y_j assume lo stesso valore. D'altronde C è simmetrico, quindi esiste un polinomio D in n variabili tale che

$$C(y_1, \ldots, y_n) = D(-\sigma_1(y_1, \ldots, y_n), \sigma_2(y_1, \ldots, y_n), \ldots, (-1)^n\sigma_n(y_1, \ldots, y_n)).$$

Da quanto visto sopra, abbiamo che

$$D(a_1, \ldots, a_n) = 0$$

se e solo se almeno due radici del polinomio f coincidono. $\square$

Nel corollario abbiamo considerato solo polinomi monici per comodità, ma è facile fare una costruzione analoga per polinomi qualsiasi; una costruzione classica di un tale D è quella del *discriminante*.

1.6. **Coniugio di matrici.** La sezione precedente si può usare per studiare un'altra azione: quella di $\mathrm{GL}(n) = \mathrm{GL}(n, \mathbb{C})$ che agisce per coniugio sullo spazio $M_n = M_n(\mathbb{C})$ di tutte le matrici $n \times n$. Cioè $g \in \mathrm{GL}(n)$ agisce su $A \in M_n$ come gAg^{-1}.

Il quoziente $M_n/\,\mathrm{GL}(n)$ non può avere struttura di varietà differenziabile o algebrica, perché non è uno spazio topologico di Hausdorff. Per questo basta considerare la matrice elementare A che ha tutte le entrate uguali a 0 tranne quella nell'angolo in alto a destra, uguale ad 1, e osservare che la chiusura dell'orbita $\mathrm{GL}(n) \cdot A$ contiene la matrice nulla. Nel quoziente quindi la classe di A è un punto non chiuso.

Tuttavia, la struttura dell'anello dei polinomi su M_n invarianti per coniugio è molto semplice. Denotiamo con $\mathbb{C}[M_n]$ l'anello dei polinomi nelle n^2 variabili $x_{1,1}, x_{1,2}, \ldots, x_{n,n}$, pensate come le funzioni su M_n che danno le entrate della matrice, e con $\mathbb{C}[M_n]^{\mathrm{GL}(n)}$ il sottoanello dei polinomi invarianti per coniugio.

Data $A \in M_n$, scriviamo il suo polinomio caratteristico come

$$\det(xI - A) = \sum_{i=0}^{n} (-1)^i a_i(A) x^{n-i}$$

I coefficienti $a_i(A)$ sono polinomi nelle entrate di A, cioè sono elementi di $\mathbb{C}[M_n]$, e sono invarianti per coniugio perchè lo è tutto il polinomio caratteristico. Inoltre le radici del polinomio sono gli autovalori di A, per cui i coefficienti $a_i(A)$ sono uguali alle funzioni simmetriche elementari calcolate negli autovalori di A.

Esempio 1.10. Sia $n = 2$ e

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

allora

$$\det(xI - A) = x^2 - (a+d)x + (ad - bc)$$

e abbiamo $a_1(A) = a + d$, $a_2(A) = ad - bc$.

Teorema 1.11. *Sia $f \in \mathbb{C}[M_n]^{GL(n)}$. Allora f è un polinomio in $a_1, \dots, a_n$.*

Dimostrazione. Sia $D \subseteq M_n$ il sottospazio delle matrici diagonali, e $K \cong S_n$ il sottogruppo di $\mathrm{GL}(n)$ delle matrici di permutazione. Osserviamo che D è stabile per l'azione di coniugio di K, che D è isomorfo a $\mathbb{C}^n$ prendendo le entrate sulla diagonale come coordinate, e che tramite questo isomorfismo l'azione di K corrisponde all'azione di S_n su $\mathbb{C}^n$ di permutazione delle entrate. Inoltre queste entrate sono proprio gli autovalori di D, e dalla Proposizione 1.8 segue che $f|_D$ è un polinomio in $a_1|_D, \dots, a_n|_D$. Cioè

$$f|_D = p(a_1|_D, \dots, a_n|_D)$$

dove p è un polinomio in n variabili.

Consideriamo

$$F = p(a_1, \dots, a_n).$$

Si tratta di un elemento di $\mathbb{C}[M_n]^{GL(n)}$, e coincide con f su D come funzione $M_n \to \mathbb{C}$. Per invarianza tramite coniugio, abbiamo che F ed f coincidono sull'insieme delle matrici diagonalizzabili. Tale insieme è denso in M_n, per cui $f = F$. $\square$

Esercizio 1.12. Dimostrare che l'insieme delle matrici diagonalizzabili è denso in $M_n(\mathbb{C})$. (*Suggerimento*: usare l'applicazione (1.1), il Corollario 1.9, e il fatto che se una matrice ha n autovalori distinti allora è diagonalizzabile.)

2. Gruppi algebrici lineari: fondamenti

In questa e nelle prossime sezioni prenderemo come campo $k = \mathbb{C}$. Scriveremo allora sistematicamente $\mathrm{GL}(n)$ invece di $\mathrm{GL}(n, \mathbb{C})$, ecc. Su $\mathbb{C}^n$ (e gli altri spazi vettoriali considerati) prenderemo la topologia di Zariski.

Definizione 2.1. Un *gruppo algebrico lineare* (su $\mathbb{C}$) è un sottogruppo $G \subseteq \mathrm{GL}(n)$ tale che esistono polinomi $f_1, \dots, f_m$ su M_n tali che

$$G = \{g \in \mathrm{GL}(n) \mid f_i(g) = 0 \ \forall i\}.$$

Esempio 2.2.
(1) I gruppi $\mathrm{GL}(n)$ ed $\mathrm{SL}(n)$ sono gruppi algebrici lineari, il secondo definito dal polinomio $f = \det - 1$.
(2) Sono gruppi algebrici lineari il il gruppo banale $\{I\} \subseteq \mathrm{GL}(n)$, il *gruppo ortogonale (complesso)*

$$\mathrm{O}(n, \mathbb{C}) = \{A \in \mathrm{GL}(n) \mid A \cdot {}^tA = I\},$$

il *gruppo simplettico (complesso)*

$$\mathrm{Sp}(2n, \mathbb{C}) = \{A \in \mathrm{GL}(2n) \mid AJ\,{}^tA = J\}$$

dove

$$J=\begin{pmatrix} 0 & 0 & \dots & 0 & 0 & \dots & 0 & 1\\ 0 & 0 & \dots & 0 & 0 & \dots & 1 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & \dots & 0 & 1 & \dots & 0 & 0\\ 0 & 0 & \dots & -1 & 0 & \dots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 0 & -1 & \dots & 0 & 0 & \dots & 0 & 0\\ -1 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \end{pmatrix},$$

il gruppo $H(n) \subseteq \mathrm{GL}(n)$ delle matrici diagonali, il gruppo $B(n) \subseteq \mathrm{GL}(n)$ delle matrici triangolari superiori, e il gruppo $U(n) \subseteq \mathrm{GL}(n)$ delle matrici triangolari superiori con solo entrate uguali a 1 sulla diagonale. Infatti sono tutti gruppi definiti da condizioni polinomiali nelle entrate della matrice.

(3) Il gruppo $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, con il prodotto di numeri complessi, è un gruppo algebrico lineare: si tratta semplicemente di $\mathrm{GL}(1)$.

(4) Si può considerare $\mathbb{C}$ con la somma come gruppo algebrico lineare, identificandolo col gruppo di matrici 2×2 della forma

$$\begin{pmatrix} 1 & a\\ 0 & 1 \end{pmatrix}.$$

(5) Ogni gruppo finito G è un gruppo algebrico lineare, basta immergerlo in S_n per qualche n, e poi identificare S_n come il sottogruppo di $\mathrm{GL}(n)$ delle matrici di permutazione (esercizio: come mai questo rende G un gruppo algebrico lineare?).

Dato uno spazio vettoriale V di dimensione finita, fissando una base si induce un isomorfismo naturale $\mathrm{GL}(V) \to \mathrm{GL}(n)$. Chiameremo anche un sottogruppo $G \subseteq \mathrm{GL}(V)$ *gruppo algebrico lineare* se la sua immagine in $\mathrm{GL}(n)$ lo è. Tutte le costruzioni che faremo nelle prossime sezioni lavorando in $\mathrm{GL}(n)$ si applicano in questo modo anche a qualsiasi $\mathrm{GL}(V)$. Osserviamo anche che M_n corrisponderà allora all'insieme degli endomorfismi lineari $\mathrm{End}(V)$.

Esercizio 2.3. Dimostrare che la definizione data qui sopra non dipende dalla scelta di una base di V.

3. Funzioni regolari su gruppi algebrici lineari

Ricordiamo che $\mathrm{GL}(n)$ è il luogo degli elementi di M_n dove il determinante non si annulla. Identifichiamo M_n con $\mathbb{C}^{(n^2)}$ tramite le funzioni $x_{1,1}, x_{1,2}, \dots, x_{n,n}$ che sono le entrate della matrice "generica" $x \in \mathrm{GL}(n)$, e il determinante come un polinomio $\det(x) \in \mathbb{C}[x_{1,1}, x_{1,2}, \dots, x_{n,n}]$. Allora $\mathrm{GL}(n)$ è un sottoinsieme aperto di M_n in topologia di Zariski.

Come ricordato nell'Appendice, il gruppo $\mathrm{GL}(n)$ è una varietà affine. Per la Proposizione A.10 e il Corollario A.11 l'anello delle funzioni regolari $\mathcal{O}(\mathrm{GL}(n))$ è generato da $x_{1,1}, x_{1,2}, \dots, x_{n,n}$ assieme al reciproco del determinante:

$$\mathcal{O}(\mathrm{GL}(n)) = \mathbb{C}[x_{1,1}, x_{1,2}, \dots, x_{n,n}, \det(x)^{-1}]$$

Quindi un gruppo algebrico lineare è in particolare una varietà affine; se chiamiamo $I_{GL(n)}(G) \subseteq \mathcal{O}(\mathrm{GL}(n))$ l'ideale delle funzioni regolari su $\mathrm{GL}(n)$ che svaniscono su tutto G, allora la restrizione da $\mathrm{GL}(n)$ a G induce il solito isomorfismo

$$\mathcal{O}(G) \cong \mathcal{O}(\mathrm{GL}(n))/I_{GL(n)}(G).$$

come nel Lemma A.7.

Proposizione 3.1. *Sia G un gruppo algebrico lineare. La moltiplicazione*

$$\begin{array}{rccc} \mu\colon & G \times G & \to & G\\ & (g,h) & \mapsto & gh \end{array}$$

e l'inversa

$$\begin{array}{rccc} \eta\colon & G & \to & G\\ & g & \mapsto & g^{-1} \end{array}$$

sono applicazioni regolari. Inoltre, dato $g \in G$, sono regolari l'applicazione $G \to G$ che manda h in gh, e l'applicazione $G \to G$ che manda h in hg. Infine, data $f \in \mathcal{O}(G)$, esistono funzioni regolari $a_1, b_1, \dots, a_p, b_p$ tali che

$$f(gh) = \sum_{i=1}^{p} a_i(g) b_i(h) \tag{3.1}$$

per ogni $g, h \in G$.

Dimostrazione. Possiamo considerare G come un chiuso di Zariski contenuto in $\mathbb{C}^{n^2+1}$ (con coordinate $x_{1,1}, x_{1,2}, \dots, x_{n,n}, y$), contenuto in $\mathrm{GL}(n)$ che identifichiamo con il sottoinsieme di $\mathbb{C}^{n^2+1}$ definito dall'equazione $y \cdot \det(x) = 1$. In questo modo la coordinata y su $\mathrm{GL}(n)$ coincide con $\det(x)^{-1}$. Le regole usuali della moltiplicazione e dell'inversione forniscono le entrate dei risultati tramite formule polinomiali nelle coordinate $x_{1,1}, \dots, x_{n,n}, y$, quindi tutte le applicazioni dell'enunciato sono regolari.

Infine, ricordiamo che ogni funzione regolare su $G \times G$ si scrive come somma di prodotti di funzioni su G, il che termina la dimostrazione. □

4. Rappresentazioni regolari

Definizione 4.1. Sia G un gruppo algebrico lineare. Una rappresentazione $\varphi\colon G \to \mathrm{GL}(V)$ si dice *regolare* se V ha dimensione finita e φ è un'applicazione regolare fra varietà algebriche affini. Se V ha dimensione qualsiasi, φ si dice *localmente regolare* (o *razionale*) se ogni sottospazio $E \subset V$ di dimensione finita è contenuto in un sottospazio $E' \subset V$ tale che E' è stabile sotto l'azione di G, e restringendo l'azione di G da V ad E' si ottiene una rappresentazione regolare.

L'anello delle funzioni regolari $\mathcal{O}(G)$ fornisce esempi fondamentali di rappresentazioni localmente regolari. Iniziamo defininendo le due seguenti azioni di G su se stesso:

(1) l'azione per *traslazione a sinistra* $g \cdot_L h = gh$,
(2) l'azione per *traslazione a destra* $g \cdot_R h = hg^{-1}$.

Queste azioni inducono azioni su $\mathcal{O}(G)$, denotate $L, R\colon G \to \mathrm{GL}(\mathcal{O}(G))$ e chiamate anch'esse rispettivamente *traslazione a sinistra* e *a destra*, nel modo solito: dati $g \in G$ e $f \in \mathcal{O}(G)$, la funzione $L(g)(f)$ manda h in $f(g^{-1}h)$, e la funzione $R(g)(f)$ manda h in $f(hg)$. Si verifica immediatamente usando la Proposizione 3.1 che $L(g)(f)$ e $R(g)(f)$ sono effettivamente elementi di $\mathcal{O}(G)$.

Proposizione 4.2. *Sia G gruppo algebrico lineare. Le rappresentazioni L ed R sono localmente regolari.*

Dimostrazione. Sia $f \in \mathcal{O}(G)$. La formula (3.1) fornisce funzioni $a_i, b_i \in \mathcal{O}(G)$ tali che

$$L(g)(f) = \sum_i a_i(g^{-1}) b_i, \qquad R(g)(f) = \sum_i a_i b_i(g).$$

Consideriamo i sottospazi G-stabili $V_L(f)$ e $V_R(f)$ generati rispettivamente dalle funzioni $L(g)(f)$ e $R(g)(f)$ per ogni $g \in G$. Questi spazi hanno dimensione finita, perché sono contenuti nei sottospazi di $\mathcal{O}(G)$ generati dalle funzioni b_i e a_i rispettivamente.

Dimostriamo che si tratta di rappresentazioni regolari di G. Lavoriamo con $V_L(f)$, il ragionamento con $V_R(f)$ è lo stesso. Prima di tutto, possiamo assumere che le funzioni b_i siano linearmente indipendenti (altrimenti, è immediato riscrivere l'espressione per $L(g)(f)$ scartando le b_i superflue e "riassorbendo" i loro coefficienti in quelli delle altre b_i). Quindi assumiamo che le funzioni b_i siano una base dello spazio vettoriale che generano. Osserviamo poi che possiamo cambiare base ottenendo una formula del tutto equivalente per $L(g)(f)$, basta esprimere le b_i in termini della nuova base. Quindi possiamo assumere che alcune delle b_i formino una base di $V_L(f)$. A questo punto quelle b_i sono le uniche coinvolte nella formula di $L(g)(f)$ con coefficienti non nulli, per cui possiamo semplicemente assumere che le b_i siano proprio una base di $V_L(f)$. Infine, una base di $V_L(f)$ è anche ottenibile scegliendo elementi opportuni $g_1, \dots, g_p$ e prendendo le funzioni $L(g_i)(f)$, per cui possiamo ancora assumere che $b_i = L(g_i)(f)$ per ogni i.

Calcoliamo allora la matrice dell'operazione di $g \in G$ su $V_L(f)$ in questa base:

$$L(g)(b_i) = L(g)(L(g_i)(f)) = L(gg_i)(f) = \sum_j a_j(g_i^{-1} g^{-1}) b_j,$$

cioè g agisce tramite la matrice $a_j(g_i^{-1}g^{-1})$, che è una funzione regolare (nella variabile g). Quindi $V_L(f)$ è un G-modulo regolare.

Sia ora $V \subseteq \mathcal{O}(G)$ un sottospazio vettoriale di dimensione finita, e si scelga una base $f_1, \dots, f_m$. La somma $V_L(f_1) + \dots + V_L(f_m)$ è G-stabile, contiene V, ed è un G-modulo regolare per la prima parte della dimostrazione. □

Esempio 4.3. Consideriamo $G = \mathbb{C}$, quindi $\mathcal{O}(G)$ è semplicemente l'anello dei polinomi $\mathbb{C}[x]$ in una variabile[2]. La traslazione (a destra o a sinistra) di G su $\mathcal{O}(G)$ è letteralmente la traslazione delle funzioni, cioè la "traslazione del loro grafico in orizzontale". Dato un elemento $f \in \mathbb{C}[x]$, esso è contenuto per esempio nel sottospazio $\mathbb{C}[x]_d$ dei polinomi di grado $d = \deg(f)$, sottospazio che è G-stabile.

5. Azioni di gruppi algebrici lineari

Definizione 5.1. Un'azione di un gruppo algebrico lineare G su una varietà algebrica affine X è *regolare* se l'applicazione corrispondente

$$\begin{array}{cccc} \varphi\colon & G \times X & \to & X \\ & (g, x) & \mapsto & g \cdot x \end{array}$$

è un'applicazione regolare fra varietà algebriche. In questo caso X si dice anche una *G-varietà* (affine). Un'applicazione regolare $\varphi\colon X \to Y$ si dice *G-equivariante* se $\varphi(g \cdot x) = g \cdot \varphi(x)$ per ogni $g \in G$ e $x \in X$. Due G-varietà X, Y si dicono *G-isomorfe* se esiste fra esse un isomorfismo (di varietà algebriche) che sia G-equivariante.

Proposizione 5.2. *Sia X una G-varietà affine. Allora $\mathcal{O}(X)$, con l'azione solita di G, è un G-modulo localmente regolare di G.*

Dimostrazione. Dati $f \in \mathcal{O}(X)$ e $g \in G$, la funzione $g \cdot f$ manda x in $f(g^{-1}x)$. Possiamo vedere questa funzione come la composizione $\psi^*(f) = f \circ \psi$, dove $\psi\colon G \times X \to X$ manda (g, x) in $g^{-1}x$. Visto che l'inversione su G e φ sono applicazioni regolari, anche ψ è regolare. Quindi anche $g \cdot f$ è una funzione regolare su X, cioè effettivamente $\mathcal{O}(G)$ è una rappresentazione di G.

Come per la formula 3.1, esistono funzioni regolari $a_i \in \mathcal{O}(G)$ e $b_i \in \mathcal{O}(X)$ tali che

$$(g \cdot f)(x) = \sum_{i=1}^{p} a_i(g) b_i(x),$$

e il resto della dimostrazione procede nello stesso modo che per la Proposizione 4.2. □

Siamo pronti per mostrare, nel prossimo teorema, un'applicazione fondamentale delle rappresentazioni localmente regolari considerate qui. Iniziamo con un'osservazione semplice.

Osservazione 5.3. Sia U un G-modulo. Allora il duale U^* ha struttura naturale di G-modulo, con l'azione usuale: dati $f \in U^*$ e $g \in G$, è ovvio che la solita traslata $(g \cdot f)\colon u \mapsto f(g^{-1} \cdot u)$ è ancora un elemento di U^*.

Teorema 5.4. *Sia G un gruppo algebrico lineare che agisce in modo regolare su una varietà affine X. Allora esiste un G-modulo regolare (finito-dimensionale) V di G che contiene una varietà algebrica Y, tali che Y è G-stabile e G-isomorfa ad X.*

Dimostrazione. Siano $f_1, \dots, f_m$ generatori di $\mathcal{O}(X)$ come algebra. Grazie alla Proposizione 5.2, possiamo assumere che lo *spazio vettoriale* $U \subseteq \mathcal{O}(X)$ generato da $f_1, \dots, f_m$ sia G-stabile. Poniamo $V = U^*$, con la struttura di G-modulo definita qui sopra.

Consideriamo l'applicazione regolare

$$\begin{array}{cccc} \varphi\colon & X & \to & V \\ & x & \mapsto & (u \mapsto u(x)). \end{array}$$

Cioè ad $x \in X$ associamo il "valutare una funzione regolare $u \in U \subseteq \mathcal{O}(X)$ in x", che è ovviamente lineare in u, quindi un elemento di U^*. Verifichiamo che φ è G-equivariante. Intanto $\varphi(g \cdot x)$ è il funzionale $u \mapsto u(g \cdot x)$.

---

[2]Per essere pedanti, abbiamo identificato G con un sottoinsieme di M_2 piuttosto che considerarlo semplicemente come $\mathbb{C}$, ma l'uguaglianza $\mathcal{O}(G) = \mathbb{C}[x]$ è ovvia lo stesso, basta prendere come x l'entrata $x_{1,2}$ delle matrici di G.

D'altronde
$$g \cdot (u \mapsto u(x)) = (u \mapsto (g^{-1} \cdot u)(x)) = (u \mapsto u(g \cdot x)),$$
quindi φ è effettivamente G-equivariante.

Dal Lemma A.17 segue che φ è anche un isomorfismo. □

Esempio 5.5. (1) Sia $G = \mathbb{C}^*$ che agisce su $V = \mathbb{C}^2$ tramite $g \cdot (a, b) = (ga, g^{-1}b)$. Alcuni chiusi G-stabili di V:
  (a) le iperboli di equazione $xy = \alpha$ dove $\alpha \in \mathbb{C}^*$ (sono singole orbite);
  (b) gli assi cartesiani $x = 0$ e $y = 0$ (contengono due orbite ciascuno);
  (c) l'origine $(0, 0)$.

(2) Sia $V = \mathbb{C}^n$ e $G = \mathrm{O}(n, \mathbb{C})$. Fissando $\alpha \in \mathbb{C}$ e ponendo
$$X_\alpha = \{v \in V \mid {}^t v \cdot v = \alpha\},$$
si ottiene un chiuso G-stabile (una *quadrica*, cioè un chiuso definito da una singola equazione di grado 2). Se $\alpha \neq 0$, la G-varietà X_α è costituita da una singola orbita. Infatti, preso un qualsiasi $v_1 \in X_\alpha$, si può completare ad una base $B = (v_1, v_2, \dots, v_n)$ tale che ${}^t v_i \cdot v_i \neq 0$ per ogni i. Poi, col procedimento di Gram-Schmidt, si può "ortonormalizzare" la base rispetto alla forma bilineare non degenere $(v, w) \mapsto {}^t v \cdot w$ di $\mathbb{C}^n$, ottenendo B'. Allora la matrice di passaggio dalla base canonica a B' è una matrice in $\mathrm{O}(n, \mathbb{C})$, e la sua inversa manda v_1 nel vettore
$$v_0 = \begin{pmatrix} \sqrt{\alpha} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$
Segue che $X_\alpha = \mathrm{O}(n, \mathbb{C}) \cdot v_0$.

(3) Sia $G = \mathrm{GL}(n)$ che agisce per coniugio su $X = M_n$. Fissato un intero non negativo r, il sottoinsieme $X_r \subseteq X$ delle matrici di rango *al più* r è un chiuso G-stabile, definito dallo svanire di tutti i minori $(r + 1) \times (r + 1)$.

(4) Sia $G = \mathrm{GL}(n)$ che agisce per moltiplicazione a sinistra, o a destra, su $X = M_n$. Anche qui i sottoinsiemi X_r sono chiusi G-stabili, è facile dare anche altri chiusi G-stabili: per esempio, con la moltiplicazione a sinistra, il chiuso Y_i delle matrici che hanno tutta la i-esima colonna uguale a zero.

(5) Sia $G = \mathrm{GL}(n) \times \mathrm{GL}(n)$ che agisce su $X = M_n$ per moltiplicazione a sinistra *e a destra*: $(g, h) \cdot A = gAh^{-1}$. Anche qui gli X_r sono chiusi G-stabili; questa volta le differenze $X_r \smallsetminus X_{r-1}$ con $r \in \{n, \dots, 1\}$ sono singole G-orbite (esercizio!).

(6) Sia $G = \mathrm{GL}(n)$ che agisce sull'insieme X delle matrici simmetriche $n \times n$, tramite l'azione
$$g \cdot A = g \cdot A \cdot {}^t g.$$
Anche in questo caso, imponendo che il rango sia al più un intero fissato r si ottiene un chiuso G-stabile.

(7) Sia $G = \mathbb{C}^*$, allora
$$\mathcal{O}(G) = \mathbb{C}[t, t^{-1}] = \bigoplus_{n \in \mathbb{Z}} \mathbb{C} t^n.$$
Se X è una G-varietà affine e $f \in \mathcal{O}(X)$, possiamo considerare la funzione $t \mapsto (t \cdot f)(x)$ con $t \in G$ e $x \in X$ come funzione di entrambe le variabili t, x. È una funzione regolare su $G \times X$, per cui si sviluppa come al solito come somma di prodotti di funzioni su G e su X. Raccogliendo le potenze di t, abbiamo
$$(t \cdot f)(x) = \sum_{n \in \mathbb{Z}} f_n(x) t^n,$$
con $f_n \in \mathcal{O}(X)$ per ogni n, e la somma è finita, cioè solo un numero finito di f_n è non zero. Vediamo alcune conseguenze della la formula $t' \cdot (t \cdot f) = (t't) \cdot f$:
$$((t't) \cdot f)(x) = \sum_{n \in \mathbb{Z}} f_n(x) (t')^n t^n,$$

D'altronde l'agire con t' su $\mathcal{O}(X)$ è lineare in f, per cui

$$(t' \cdot (t \cdot f))(x) = \sum_{n \in \mathbb{Z}} (t' \cdot f_n)(x) t^n$$

Confrontando addendo per addendo (si può fare, ricordando come è definito il prodotto $G \times X$), otteniamo

$$(t \cdot f_n)(x) = t^n \cdot (f_n(x))$$

dove il primo prodotto è l'azione di $t \in \mathbb{C}^*$ su $f_n \in \mathcal{O}(X)$, mentre il secondo è semplicemente il prodotto fra due funzioni, una su G e una su X.

Concludiamo che $\mathcal{O}(X)$ si decompone in somma diretta

$$\mathcal{O}(X) = \bigoplus_{n \in \mathbb{Z}} \mathcal{O}(X)_n$$

dove, per ogni $n \in \mathbb{Z}$, l'elemento $t \in G$ agisce su $f \in \mathcal{O}(X)_n$ moltiplicando f per t^n.

Osserviamo anche che allora la moltiplicazione di funzioni in $\mathcal{O}(X)$ soddisfa la proprietà

$$\mathcal{O}(X)_n \cdot \mathcal{O}(X)_m \subseteq \mathcal{O}(X)_{n+m},$$

per cui l'azione di G rende $\mathcal{O}(X)$ un anello $\mathbb{Z}$-*graduato*. La costruzione si può anche "invertire": data una varietà affine X, ogni $\mathbb{Z}$-gradazione di $\mathcal{O}(X)$ proviene da un'azione di $\mathbb{C}^*$ su X.

Corollario 5.6. *Sia G una varietà affine dotata di struttura di gruppo, tale che la moltiplicazione $G \times G \to G$ e l'inversione $G \to G$ sono applicazioni regolari. Allora G è isomorfo (come varietà e come gruppo) ad un sottogruppo chiuso di* $\mathrm{GL}(n)$ *per qualche n, cioè G è un gruppo algebrico lineare.*

Dimostrazione. Osserviamo prima di tutto che il Teorema 5.4 vale anche per G come in questo corollario, se abbiamo un'azione di G su una varietà affine X tale che l'applicazione $G \times X \to X$ è regolare. Infatti in realtà nella dimostrazione abbiamo usato soltanto questo, e non che il gruppo fosse in origine contenuto dentro un qualche $\mathrm{GL}(n)$.

Consideriamo allora $X = G$ come G-varietà, tramite la moltiplicazione a sinistra

$$\begin{array}{ccc} G \times X & \to & X \\ (g, x) & \mapsto & gx. \end{array}$$

Per il teorema, possiamo assumere che X sia un chiuso G-stabile di qualche G-modulo regolare V. Consideriamo le funzioni coordinate $y_1, \ldots, y_n$ su $V \cong \mathbb{C}^n$ rispetto a una base $(v_1, \ldots, v_n)$ di V.

L'azione di G, lineare su V, si rappresenta come un omomorfismo (di gruppi e di varietà algebriche) $\varphi\colon G \to \mathrm{GL}(n)$, chiamiamo $a_{i,j}(g)$ le entrate di $\varphi(g)$ per $g \in G$. Il prodotto usuale "matrice per vettore", dati $g \in G$ e $x \in V$, produce la formula

$$y_i(gx) = \sum_j a_{i,j}(g) y_j(x).$$

Nel caso particolare in cui prendiamo l'elemento neutro di X (scriviamolo come "e" per evitare confusione con $I \in \mathrm{GL}(n)$), abbiamo

$$y_i(g) = \sum_j a_{i,j}(g) y_j(e).$$

Ora: le funzioni $y_i|_G$ generano $\mathcal{O}(X)$, quindi le funzioni $a_{i,j}$ generano $\mathcal{O}(G)$ (che è lo stesso anello). Consideriamo allora di nuovo φ, ma come applicazione $G \to Y \subseteq M_n \cong \mathbb{C}^{n^2}$ dove Y è la chiusura dell'immagine di φ. Abbiamo che $\mathcal{O}(Y)$ è generato dalle restrizioni $x_{i,j}|_Y$ delle funzioni entrate delle matrici $x_{i,j}$. D'altronde $\varphi^*\colon \mathcal{O}(Y) \to \mathcal{O}(X)$ è iniettiva, infatti se due funzioni regolari su Y coincidono tirate indietro su G, allora coincidono sull'immagine di G, e allora coincidono anche sulla sua chiusura Y. D'altronde $\varphi^*(x_{i,j}|_Y)$ è la funzione $a_{i,j}$ per ogni i, j, quindi φ^* è anche suriettiva, cioè è un isomorfismo. Allora $\varphi\colon G \to Y$ è un isomorfismo. □

Esempio 5.7. Il corollario si può applicare a $\mathbb{C}$ con la somma, ritrovando in modo "astratto" che si tratta di un gruppo algebrico lineare, cosa che avevamo già osservato concretamente.

6. Gruppi linearmente riduttivi

Introduciamo una classe importantissima di gruppi algebrici lineari.

Definizione 6.1. Sia G un gruppo algebrico lineare, e V un G-modulo.

(1) Un sottospazio vettoriale G-stabile di V si dice *sottomodulo* (o G-sottomodulo);
(2) V si dice *irriducibile* (o *semplice*) se contiene esattamente due sottomoduli: $\{0\}$ e V stesso;
(3) V si dice *completamente riducibile* se è somma diretta di sottomoduli irriducibili;
(4) G si dice *linearmente riduttivo* se ogni G-modulo regolare è completamente riducibile.

La stessa terminologia "irriducibile", "semplice", "completamente riducibile" si usa anche per le corrispondenti rappresentazioni.

Osserviamo che il modulo nullo $V = \{0\}$ non è irriducibile, però è completamente riducibile: è la somma diretta di *nessun modulo*.

Esempio 6.2. (1) Il gruppo $G = \mathbb{C}$ non è linearmente riduttivo, perché la rappresentazione vista prima $\mathbb{C} \to \mathrm{GL}(2)$ (data dal mandare $a \in \mathbb{C}$ nella matrice $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$) non è completamente riducibile. Infatti il G-modulo $\mathbb{C}^2$ ha un solo sottomodulo diverso da $\{0\}$ e da $\mathbb{C}^2$, ed è il sottospazio generato dal primo vettore della base canonica. Quindi $\mathbb{C}^2$ non è irriducibile, e non esistono altri sottomoduli che permettono di ottenere $\mathbb{C}^2$ come somma diretta di sottomoduli propri.
(2) In modo analogo si dimostra che $B(n)$ ed $U(n)$ non sono linearmente riduttivi per $n \geq 2$.

Definizione 6.3. Un'applicazione lineare $\varphi \colon V \to W$ fra G-moduli si dice un *omomorfismo* (di G-moduli) se è un'applicazione G-equivariante.

Osservazione 6.4. È facile dimostrare che il nucleo e l'immagine di un omomorfismo di G-moduli sono entrambi sottomoduli.

Proposizione 6.5. *Un G-modulo V di dimensione finita è completamente riducibile se e solo se, per ogni G-sottomodulo $U \subseteq V$, esiste un G-sottomodulo $W \subseteq V$ tale che $V = U \oplus W$.*

Dimostrazione. Supponiamo che per ogni U esista W come nella proposizione, e dimostriamo che V è completamente riducibile. Procediamo per induzione su $\dim(V)$: la base dell'induzione è $\dim(V) = 0$, dove V è completamente riducibile. Dimostriamo il passo induttivo, supponendo $\dim(V) > 1$.

Se V non ha sottomoduli diversi da $\{0\}$ e da V, allora è irriducibile e abbiamo finito. Altrimenti esiste un sottomodulo U diverso dai due, possiamo assumere che U abbia dimensione minima possibile. Allora U è irriducibile, per minimalità della sua dimensione. Segue $V = U \oplus W$ con W sottomodulo di dimensione $< \dim(V)$.

Sia ora $W' \subseteq W$ sottomodulo, e consideriamo $U \oplus W'$: per ipotesi, questo sottomodulo ammette un complementare $Z \subseteq V$ tale che $Z \oplus (U \oplus W') = V$. Sia allora Z' la proiezione di Z su W lungo U: si dimostra facilmente che Z' è un sottomodulo di W e che $W = Z' \oplus W'$. Quindi per W vale la stessa proprietà che abbiamo supposto per V, e quindi W per induzione si decompone in somma di irriducibili. Segue lo stesso per V.

Viceversa, sia $V = V_1 \oplus \ldots \oplus V_m$ decomposizione in irriducibili, e $U \subseteq V$ sottomodulo. Scegliamo allora alcuni moduli V_i nel modo seguente: se U contiene V_1, allora "scartiamo V_1" definendo $V_1' = \{0\}$, altrimenti $U \cap V_1 = \{0\}$ (per irriducibilità di V_1), e definiamo $V_1' = V_1$. Andando avanti, per ogni $i > 1$ definiamo $V_i' = \{0\}$ se

$$U \oplus V_1' \oplus \ldots \oplus V_{i-1}'$$

contiene V_i, e definiamo $V_i' = V_i$ altrimenti (nel qual caso $U \oplus V_1' \oplus \ldots \oplus V_{i-1}'$ è in somma diretta con V_i'). Arriviamo ad una somma diretta di G-moduli

$$V = U \oplus \underbrace{V_1' \oplus \ldots \oplus V_n'}_{=W}$$

che conclude la dimostrazione. □

Corollario 6.6. *(della dimostrazione) Ogni sottomodulo di un modulo completamente riducibile di dimensione finita è completamente riducibile.*

Dimostrazione. Prendiamo come criterio di completa riducibilità la condizione espressa nella proposizione precedente. Nella sua dimostrazione, abbiamo visto che se V ha quella proprietà, allora anche un qualsiasi sottomodulo W ha la stessa proprietà. $\square$

Lemma 6.7. *(Schur) Sia V un G-modulo irriducibile di dimensione finita, e $A \in \operatorname{End}(V)$ che commuta con l'immagine di G in $\operatorname{GL}(V)$. Allora A è un multiplo scalare dell'identità.*

Dimostrazione. Visto che il campo su cui lavoriamo è algebricamente chiuso (e visto che V ha almeno dimensione 1), l'endomorfismo A ha un autovalore λ. L'autospazio corrispondente è un sottomodulo per l'azione di G, infatti dato $g \in G$ e v autovettore abbiamo

$$Agv = gAv = g\lambda v = \lambda gv.$$

Visto che l'autospazio non è nullo per definizione, coincide con tutto V, per cui $A = \lambda \cdot \mathrm{Id}_V$. $\square$

Lemma 6.8. *Sia $\varphi\colon V \to W$ un omomorfismo di G-moduli irriducibili. Allora è l'applicazione nulla oppure è un isomorfismo.*

Dimostrazione. Il lemma segue immediatamente dal fatto che il nucleo è un sottomodulo di V, e l'immagine un sottomodulo di W. $\square$

È utilissimo studiare il gruppo $\mathbb{C}$, non linearmente riduttivo. Il Lemma di Schur ha conseguenze notevoli su questo gruppo.

Lemma 6.9. *Sia V un $\mathbb{C}$-modulo regolare irriducibile. Allora V ha dimensione 1, e $\mathbb{C}$ vi agisce banalmente (cioè ogni $g \in \mathbb{C}$ agisce come l'identità).*

Dimostrazione. Visto che $\mathbb{C}$ è un gruppo commutativo, per il Lemma di Schur ogni $g \in \mathbb{C}$ agisce su V per moltiplicazione per uno scalare (invertibile, perché l'azione manda $\mathbb{C}$ in $\operatorname{GL}(V)$). Chiamiamo questo scalare $\chi(g) \in \mathbb{C}^*$. Fissiamo $v \in V \smallsetminus \{0\}$, e ricordiamo che $g \mapsto g \cdot v = \chi(g)v$ è un'applicazione regolare $\mathbb{C} \to V$. Prendendo una coordinata non nulla di v, essa varia con l'azione di $g \in \mathbb{C}$ come un multiplo di $\chi(g)$, per cui otteniamo che $\chi(g)$ è una funzione regolare nella variabile g, cioè χ è una funzione polinomiale $\mathbb{C} \to \mathbb{C}^*$.

Per il teorema fondamentale dell'algebra, la funzione χ è costante. Visto che $0 \in \mathbb{C}$ deve andare nell'identità $e \in \operatorname{GL}(V)$, abbiamo $\chi(g) = 1$ per ogni $g \in \mathbb{C}$, cioè $\mathbb{C}$ agisce banalmente. Inoltre allora ogni sottospazio è un sottomodulo, per cui V ha necessariamente dimensione 1. $\square$

Corollario 6.10. *Ogni $\mathbb{C}$-modulo regolare V non nullo ha un vettore $v \neq 0$ fissato da tutti gli elementi di $\mathbb{C}$.*

Dimostrazione. Sia U un sottomodulo non nullo di dimensione minima. Allora U è irriducibile, e $\mathbb{C}$ vi agisce banalmente per il lemma precedente. $\square$

Otteniamo un fondamentale criterio necessario per la lineare riduttività.

Teorema 6.11. *Sia G linearmente riduttivo. Allora G non contiene alcun sottogruppo chiuso normale isomorfo a $\mathbb{C}$.*

Dimostrazione. Sia per assurdo $H \cong \mathbb{C}$ sottogruppo chiuso normale di G. Per il Corollario 5.6, esiste un G-modulo regolare V tale che $G \to \operatorname{GL}(V)$ abbia nucleo banale. Per il Corollario 6.10, il sottospazio V^H dei vettori fissati da H è non banale; d'altronde è un G-sottomodulo perché

$$hgv = g \cdot \underbrace{g^{-1}hg}_{\in H} v = gv$$

per ogni $g \in G$, $h \in H$, $v \in V$. Quindi V si decompone in somma diretta di G-sottomoduli

$$V = V^H \oplus W.$$

Ma lo stesso ragionamento fatto su V si applica anche a W: quindi anche su W il gruppo H ha vettori fissati, e W^H ha un complemento G-stabile. Andando avanti, concludiamo che H agisce banalmente su tutto V, cioè H è nel nucleo della rappresentazione $G \to \operatorname{GL}(V)$: assurdo. $\square$

Osservazione 6.12. (1) Il Teorema 6.11 vale anche su campi algebricamente chiusi di caratteristica qualsiasi, con stessa dimostrazione (i risultati di geometria algebrica che abbiamo usato finora valgono in caratteristica qualsiasi).

(2) Su $\mathbb{C}$, è importante sapere che **vale anche il viceversa del teorema**. Si tratta di un risultato fondamentale per i gruppi algebrici, di cui non conosco però dimostrazioni semplici. Due strategie standard sono: ricorrere alla teoria delle algebre di Lie, e ridurre l'enunciato al Teorema di Weyl per algebre di Lie semisemplici, oppure ricorrere ai gruppi di Lie compatti, per i quali il viceversa del teorema si dimostra facilmente usando la misura di Haar. Il primo approccio vale su qualsiasi campo algebricamente chiuso di caratteristica 0.

(3) Invece, in caratteristica positiva il viceversa del teorema è falso, ad esempio per $V = S^2k^2$ e $G = \mathrm{SL}(2,k)$ dove k è un campo algebricamente chiuso di caratteristica 2. Il sottoinsieme dei vettori $v \cdot v$ con $v \in k^2$ è un sottospazio vettoriale, perché in caratteristica 2 vale $(a+b)^2 = a^2 + b^2$, ed è un sottomodulo che non ammette complementi G-stabili.

7. Alcuni gruppi linearmente riduttivi

Teorema 7.1. *Sia H un sottogruppo chiuso di indice finito di un gruppo algebrico lineare G. Se H è linearmente riduttivo, anche G è linearmente riduttivo.*

Dimostrazione. Sia V un G-modulo regolare, con rappresentazione $\varphi\colon G \to \mathrm{GL}(V)$, e sia U un sottomodulo. L'idea della dimostrazione è quella di partire da un H-sottomodulo Z tale che $V = U \oplus Z$, e renderlo G-stabile "facendo una media" fra la collezione finita di sottospazi $g \cdot Z$. Questa operazione ovviamente non ha senso in termini di sottospazi, ma lo ha in termini di proiezioni.

Sia allora Z siffatto, e consideriamo $P\colon V \to U$ la proiezione su U lungo Z. Si tratta di un endomorfismo idempotente (cioè $P^2 = P$), e vale

$$\varphi(h)P\varphi(h)^{-1} = P$$

per ogni $h \in G$, infatti decomponendo $v \in V$ come $v = u + z$ dove $u \in U$ e $z \in Z$ abbiamo

$$h \cdot P(h^{-1} \cdot v) = h \cdot P(\underbrace{h^{-1} \cdot u}_{\in U} + \underbrace{h^{-1} \cdot z}_{\in Z}) = h \cdot (h^{-1} \cdot u) = u = P(v.)$$

Allora, presa una classe laterale $gH \in G/H$, è ben definito l'endomorfismo $P_{gH} = \varphi(g)P\varphi(g^{-1})$. Definiamo

$$Q = \frac{1}{|G/H|} \sum_{gH \in G/H} P_{gH}.$$

Dato $u \in U$, visto che U è G-stabile, abbiamo $P_{gH}(u) = g \cdot P(g^{-1} \cdot u) = u$, quindi Q è l'identità su U. Inoltre per ogni $v \in V$ vale $Q(v) \in U$, quindi l'immagine di Q è U. Segue che $\ker(Q)$ è in somma diretta con U, cioè Q è la proiezione su U lungo il suo nucleo.

Infine Q commuta con $\varphi(G)$, infatti per ogni $a \in G$ abbiamo

$$\varphi(a)Q\varphi(a^{-1}) = \frac{1}{|G/H|} \sum_{gH \in G/H} \varphi(a)\varphi(g)P\varphi(g^{-1})\varphi(a^{-1}) = Q.$$

Segue facilmente che $W = \ker(Q)$ è G-stabile, quindi è un complemento G-stabile per U. $\square$

Corollario 7.2. *(Teorema di Maschke) Tutti i gruppi finiti sono linearmente riduttivi.*

Proposizione 7.3. *Il gruppo $\mathbb{C}^*$ è linearmente riduttivo. Inoltre, se V è un $\mathbb{C}^*$-modulo regolare irriducibile, allora V ha dimensione 1 ed esiste un intero n tale che $t \in \mathbb{C}^*$ agisce su V come la moltiplicazione per t^n.*

Dimostrazione. Sia V un $\mathbb{C}^*$-modulo regolare, e rifacciamo per $X = V^*$ le considerazioni dell'Esempio 5.5-(7). Otteniamo

$$\mathcal{O}(V^*) = \bigoplus_{n \in \mathbb{Z}} \mathcal{O}(V^*)_n$$

dove su $\mathcal{O}(V^*)_n$ l'elemento $t \in G$ agisce per moltiplicazione per t^n. Ora, il duale V di V^* è un sottospazio vettoriale di dimensione finita contenuto in $\mathcal{O}(V^*)$, quindi esiste un intero N tale che

$$V \subseteq \bigoplus_{n=-N}^{N} \mathcal{O}(V^*)_n.$$

Osserviamo che ciascun $\mathcal{O}(V^*)_n$ è completamente riducibile, perché ogni suo sottospazio vettoriale di dimensione 1 è un suo sottomodulo irriducibile. Dal Corollario 6.6 segue che V è completamente riducibile (attenzione: il corollario era enunciato solo per moduli di dimensione finita, mentre i moduli $\mathcal{O}(V^*)_n$ in generale possono avere dimensione infinita; lasciamo per esercizio di adattare questa dimostrazione in modo da poter effettivamente applicare il corollario al nostro caso).

Per dimostrare la seconda parte della proposizione, supponendo che V sia irriducibile, basta applicare il Lemma 6.8 alle proiezioni $V \to W$ dove W varia fra i sottomoduli 1-dimensionali irriducibili di $\mathcal{O}(V^*)_n$ citati prima, per tutti gli n, lungo la somma degli altri addendi di una decomposizione in irriducibili. Infatti almeno una di queste proiezioni deve essere non nulla, e quindi un isomorfismo. $\square$

Osservazione 7.4. La Proposizione 7.3 vale allo stesso modo per $(\mathbb{C}^*)^n$ con n intero positivo. Infatti l'Esempio 5.5-(7) si può riformulare in modo identico anche con questo gruppo, usando $\mathcal{O}(G) = \mathbb{C}[t_1, t_1^{-1}, \ldots, t_n, t_n^{-1}]$, e facendo vedere che ogni azione regolare di $(\mathbb{C}^*)^n$ su una varietà affine X rende $\mathcal{O}(X)$ un anello $\mathbb{Z}^n$-graduato. La dimostrazione della proposizione per $(\mathbb{C}^*)^n$ procede poi allo stesso modo. L'ultima affermazione assume la forma seguente: se V è un $(\mathbb{C}^*)^n$-modulo regolare irriducibile, allora V ha dimensione 1 ed esiste una n-upla $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ tale che $(t_1, \ldots, t_n) \in (\mathbb{C}^*)^n$ agisce su V come la moltiplicazione per $t_1^{a_1} \ldots t_n^{a_n}$.

Esempio 7.5. Sia N il sottogruppo di SL(2) dato dalle matrici con determinante 1 che siano diagonali oppure "antidiagonali", cioè della forma

$$\begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix}$$

con $a \in \mathbb{C}^*$. Osserviamo che H è un gruppo algebrico lineare, perché i due sottoinsiemi con cui l'abbiamo definito sono entrambi chiusi di Zariski. Inoltre N contiene come sottoguppo di indice 2 il gruppo $\mathrm{SL}(2) \cap H(2)$, che è isomorfo a $\mathbb{C}^*$. Quindi N è linearmente riduttivo. Osserviamo che N non ha un elemento di ordine 2 fuori da H (esercizio), quindi N non è un prodotto semidiretto di $\mathbb{Z}/2\mathbb{Z}$ con $\mathbb{C}^*$.

8. Quozienti categorici e teoria geometrica degli invarianti (Geometric Invariant Theory), versione affine

La lineare riduttività di un gruppo algebrico lineare G ci permette di studiare quozienti X/G, dove X è una varietà affine, in modo molto efficace. La geometria algebrica non può fornire strumenti per studiare questo quoziente vero e proprio in generale: come abbiamo visto, ci sono esempi in cui X/G ha punti non chiusi, cosa che non accade in topologia di Zariski.

Tuttavia possiamo "avvicinarci ad esso" per quanto possibile, nello spirito della seguente definizione.

Definizione 8.1. Sia X una G-varietà affine, dove G è un gruppo algebrico lineare. Una varietà affine Y assieme ad un'applicazione regolare $\pi \colon X \to Y$ si dice un *quoziente categorico* di X su G se π è costante sulle G-orbite, e ogni applicazione regolare $\varphi \colon X \to Z$ costante sulle G-orbite si fattorizza in modo unico come $X \to Y \to Z$, cioè esiste un'unica applicazione regolare $\psi \colon Y \to Z$ tale che $\varphi = \psi \circ \pi$.

Esempio 8.2. Se G ha un'orbita densa in X, allora ogni applicazione regolare $X \to Z$ costante sulle G-orbite dev'essere costante. Quindi prendendo Y che contiene un solo punto, l'applicazione $X \to Y$ è un quoziente categorico.

Se un quoziente categorico esiste è in un certo senso unico: dalla definizione segue immediatamente che dati due quozienti categorici $\pi \colon X \to Y$ e $\pi' \colon X \to Y'$ esiste un isomorfismo di varietà affini $\psi \colon Y \to Y'$ tale che $\pi' = \psi \circ \pi$. Ci riferiremo dunque semplicemente *al* quoziente categorico. Non sempre esiste[3] ; se esiste, si denota di solito con $\pi \colon X \to X//G$.

Il nostro obiettivo in questa sezione è dimostrare che il quoziente categorico esiste, se G è linearmente riduttivo. Per questo usiamo il sottoanello delle funzioni su X che sono G-invarianti: si tratta di un oggetto che ha un ruolo naturale in questo ambito.

Infatti, sia $\psi \colon X \to Z$ un'applicazione regolare in un'altra varietà affine Z, costante sulle G-orbite. Per ogni $f \in \mathcal{O}(Z)$, abbiamo $\psi^*(f) \in \mathcal{O}(X)^G$. In altre parole, ψ^* fattorizza tramite l'inclusione

[3]Dei controesempi sono stati trovati in tempi relativamente recenti, da A'Campo-Neuen e Hausen nel 2000 (Journal of Algebra).

$\iota\colon \mathcal{O}(X)^G \to \mathcal{O}(X)$:
$$\mathcal{O}(Z) \to \mathcal{O}(X)^G \to \mathcal{O}(X).$$
Questa sequenza di omomorfismi di anelli sembra ricalcare la proprietà universale richiesta dal quoziente categorico. Se $\mathcal{O}(X)^G$ fosse l'anello delle funzioni regolari di una varietà Y, avremmo in effetti per la Proposizione A.14 un'applicazione regolare $\varphi\colon X \to Y$ tale che $\varphi^* = \iota$, e ψ fattorizzerebbe in
$$X \to Y \to Z,$$
che è proprio la condizione voluta.

Osserviamo inoltre che $\mathcal{O}(X)^G$ è un'algebra senza nilpotenti, perchè $\mathcal{O}(X)$ non ne ha. Per applicare il Corollario A.5 e ottenere l'esistenza di Y, dobbiamo solo avere che $\mathcal{O}(X)^G$ sia un'algebra finitamente generata. Sfortunatamente, questo non è sempre vero: esistono controesempi, scoperti per primo da Nagata.

Esempio 8.3. Il fatto che $\mathcal{O}(X)^G$ sia *contenuto* nell'algebra finitamente generata $\mathcal{O}(X)$ non assicura la stessa proprietà per $\mathcal{O}(X)$, a differenza di quanto succede per gli spazi vettoriali finitamente generati. Infatti, ad esempio $\mathbb{C}[x,y]$ contiene la sottoalgebra A generata da 1, xy. x^2y, x^3y, x^4y, eccetera. Lasciamo per esercizio dimostrare che non è finitamente generata come algebra.

Il collegamento con la lineare riduttività di G avviene tramite l'*operatore di Reynolds.* Per introdurlo, è utile ricordare qualche altra nozione di base di teoria delle rappresentazioni.

Definizione 8.4. Sia G gruppo algebrico lineare, sia V un G-modulo, e U un G-modulo irriducibile. La *componente isotipica* di V di tipo U (o corrispondente a U) è la somma di tutti i sottomoduli di V isomorfi ad U.

Osservazione 8.5. Sia V completamente riducibile. Allora è somma diretta di sottomoduli irriducibili; raggruppando gli addendi isomorfi fra loro, otteniamo una somma diretta di componenti isotipiche. Infatti un qualsiasi sottomodulo irriducibile di V viene proiettato con immagine nulla sui sottomoduli della decomposizione che non sono a lui isomorfi. Segue che V è somma diretta delle sue componenti isotipiche.

Lemma 8.6. *Sia G un gruppo algebrico lineare; supponiamo che G sia linearmente riduttivo, e sia V un G-modulo localmente regolare di dimensione al più numerabile. Allora esiste un unico G-sottomodulo $V_G \subseteq V$ tale che*
$$V = V_G \oplus V^G.$$

Dimostrazione. Scegliamo una base $(v_i)_{i\in I}$ di V, con insieme di indici I fatto di interi positivi, che per comodità possiamo supporre contenga 1. Per ogni n intero positivo, il sottospazio generato da v_i con $i \in I$ e $i \leq n$ è contenuto in un sottomodulo regolare $W_n \subseteq V$. Ponendo U_n uguale alla somma dei W_i per $i \leq n$, otteniamo una filtrazione di V in sottomoduli regolari
$$V = \bigcup_{n=1}^{\infty} U_n.$$
Fissiamo infine $V_1 = U_1$, e per ogni $n > 1$ fissiamo un complemento G-stabile V_n a U_{n-1} in U_n, cioè $U_n = U_{n-1} \oplus V_n$. Otteniamo, per ogni n, la decomposizione
$$U_n = \underbrace{V_1 \oplus \ldots \oplus V_{n-1}}_{=U_{n-1}} \oplus V_n$$
facilmente per induzione, e concludiamo che V si decompone come
$$V = \bigoplus_{n=1}^{\infty} V_n,$$
in cui ogni addendo è regolare. Deduciamo che V è somma diretta, eventualmente infinita, di irriducibili. Quindi V ammette la decomposizone in componenti isotipiche, e V^G è una di esse. Infatti possiamo considerarla come la somma (in realtà, è perfino l'unione) di tutti i sottomoduli di dimensione 1 dove G agisce banalmente. Questi sono tutti irriducibili, d'altronde in generale tutti i G-moduli irriducibili dove G agisce banalmente hanno per forza dimensione 1, e sono tutti isomorfi fra loro. Quindi V^G è la componente isotipica di V di tipo "il G-modulo irriducibile dove G agisce

banalmente". Per cui V_G esiste ed è univocamente determinato come somma di tutte le componenti isotipiche diverse da V^G. $\square$

Definizione 8.7. Siano G e V come nel Lemma 8.6. La proiezione

$$R_V\colon \quad V \to V^G$$

lungo V_G è detto *operatore di Reynolds.*

Veniamo ora finalmente all'utilizzo dei gruppi linearmente riduttivi, grazie ad un teorema fondamentale ispirato da risultati di D. Hilbert.

Teorema 8.8. *Sia G gruppo algebrico lineare, che agisce su una varietà affine X. Se G è linearmente riduttivo, allora $\mathcal{O}(X)^G$ è un'algebra finitamente generata.*

Per la dimostrazione, abbiamo bisogno di qualche lemma preliminare.

Lemma 8.9. *Siano G e due moduli V, W come nella Definizione 8.7, sia $\varphi\colon V \to W$ un omomorfismo di G-moduli, e sia $\varphi^G = \varphi|_{V^G}$. Allora φ^G manda V^G in W^G, e vale*

$$\varphi^G \circ R_V = R_W \circ \varphi.$$

Dimostrazione. Visto che φ è G-equivariante, manda sottomoduli irriducibili in immagini a loro isomorfe, oppure in $\{0\}$. Questo implica che ogni componente isotipica di V viene mandata nella corrispondente componente isotipica di W, oppure in $\{0\}$. Segue che, dato $v \in V$ e scrivendo $v = v_G + v^G$ la decomposizione con $v_G \in V_G$ e $v^G \in V^G$, abbiamo

$$\varphi(v) = \underbrace{\varphi(v_G)}_{\in W_G} + \underbrace{\varphi(v^G)}_{\in W^G}.$$

Allora

$$\varphi^G(R_V(v)) = \varphi(v^G) = R_W(\varphi(v)).$$

$\square$

Lemma 8.10. *Siano G e X come nel Teorema 8.8, e denotiamo con $R_X\colon \mathcal{O}(X) \to \mathcal{O}(X)^G$ l'operatore di Reynolds. Allora per ogni $f \in \mathcal{O}(X)$ e ogni $a \in \mathcal{O}(X)^G$ vale*

$$R_X(af) = aR_X(f).$$

Dimostrazione. La moltiplicazione per a, cioè

$$\begin{array}{rccc} \mu_a\colon & \mathcal{O}(X) & \to & \mathcal{O}(X) \\ & f & \mapsto & af \end{array}$$

è un omomorfismo di G-moduli, infatti dato $g \in G$ abbiamo

$$\mu_a(g \cdot f) = a(g \cdot f) = (g \cdot a)(g \cdot f) = g \cdot (af) = g \cdot \mu_a(f)$$

poiché $g \cdot a = a$. Il lemma precedente, applicato a $\varphi = \mu_a$, implica che

$$R_X(af) = R_X(\mu_a(f)) = \mu_a(R_X(f)) = aR_X(f).$$

$\square$

Lemma 8.11. *Siano G e X come nel Teorema 8.8. Allora $\mathcal{O}(X)^G$ è un anello Noetheriano, cioè ogni suo ideale è finitamente generato (come ideale), o equivalentemente ogni catena ascendente di ideali si stabilizza.*

Dimostrazione. Sia $I \subseteq \mathcal{O}(X)^G$ un ideale. Ad esso è associato l'ideale $J = I\mathcal{O}(X)$ di $\mathcal{O}(X)$; visto che I è G-stabile, lo è anche J. Possiamo allora considerare i suoi elementi G-invarianti, e per il lemma precedente abbiamo

$$R_X(J) = R_X(I\mathcal{O}(X)) = IR_X(\mathcal{O}(X)) = I\mathcal{O}(X)^G = I.$$

Ricordiamo che $\mathcal{O}(X)$ è Noetheriano, perché è un quoziente di un anello di polinomi, quindi ogni catena ascendente di ideali di $\mathcal{O}(X)$ si stabilizza. Prendiamo una catena ascendente $I_1 \subseteq I_2 \subseteq \dots$ di ideali di $\mathcal{O}(X)^G$; abbiamo visto che $I_n = R_X(I_n\mathcal{O}(X))$, e la catena ascendente data dagli $I_n\mathcal{O}(X)$ si stabilizza, per cui si stabilizza anche la catena degli I_n. $\square$

Lemma 8.12. *Sia $A = \bigoplus_{n=0}^{\infty} A_n$ un'algebra commutativa unitaria, graduata sugli interi non negativi, tale che $A_0 = \mathbb{C} \cdot 1$, e tale che l'ideale $A_+ = \bigoplus_{n=1}^{\infty} A_n$ è finitamente generato. Allora A è un'algebra finitamente generata.*

Dimostrazione. Siano $f_1, \ldots, f_m$ generatori dell'ideale A_+. Possiamo assumere che siano omogenei, e dimostriamo che allora $1, f_1, \ldots, f_m$ generano A come algebra. Sia B l'algebra da essi generata, e dimostriamo per induzione su n che $A_n \subseteq B$. La base dell'induzione è vera perché $A_0 = \mathbb{C} \cdot 1$. Sia $f \in A_n$ con $n > 1$, e siano $c_1, \ldots, c_m \in A$ tali che

$$f = c_1 f_1 + \ldots + c_m f_m.$$

Possiamo assumere che c_i sia omogeneo per ogni i, da cui deduciamo che c_i è in A_{r_i} per qualche $r_i < n$. Per ipotesi induttiva $c_i \in B$ per ogni i, da cui segue che $f \in B$. $\square$

Dimostrazione del Teorema 8.8. Come primo passo, dimostriamo il teorema per $X = V$ un G-modulo regolare. Siano $x_1, \ldots, x_n$ coordinate su $V \cong \mathbb{C}^n$, allora

$$\mathcal{O}(V) = \bigoplus_{d=0}^{\infty} \underbrace{\mathbb{C}[x_1, \ldots, x_n]_d}_{=\mathcal{O}(V)_d}$$

è un'algebra graduata, i cui addendi omogenei sono G-stabili. Segue che anche $\mathcal{O}(V)^G$ è graduata:

$$\mathcal{O}(V)^G = \bigoplus_{d=0}^{\infty} (\mathcal{O}(V)_d)^G.$$

Per il Lemma 8.11, l'anello $\mathcal{O}(V)^G$ è Noetheriano, e per il Lemma 8.12 è un'algebra finitamente generata.

Sia ora X qualsiasi. Per il Teorema 5.4, esiste un G-modulo regolare V che contiene X (a meno di isomorfismo G-equivariante) come chiuso di Zariski. La restrizione $\varphi\colon \mathcal{O}(V) \to \mathcal{O}(X)$ è un omomorfismo suriettivo di G-moduli, e visto che gli operatori di Reynolds R_V e R_X sono suriettivi, per il Lemma 8.9 anche $\varphi^G\colon \mathcal{O}(V)^G \to \mathcal{O}(X)^G$ è suriettivo. Per la prima parte della dimostrazione, l'algebra $\mathcal{O}(V)^G$ è finitamente generata, per cui lo è anche $\mathcal{O}(X)^G$. $\square$

Corollario 8.13. *Siano G e X come nel Teorema 8.8. Allora il quoziente categorico $\pi\colon X \to X//G$ esiste, scegliendo come $X//G$ la varietà affine tale che $\mathcal{O}(X//G) = \mathcal{O}(X)^G$, e π l'applicazione regolare che corrisponde all'inclusione $\mathcal{O}(X)^G \to \mathcal{O}(X)$.*

Esempio 8.14.

(1) Ritroviamo grazie alla teoria svolta finora i risultati della Sezione 1.5. Possiamo infatti applicare i nostri risultati a $G = S_n$, che è linearmente riduttivo, e alla sua azione regolare su $X = \mathbb{C}^n$ per permutazione delle entrate. Abbiamo già osservato che $\mathcal{O}(X)^G$ è un'algebra finitamente generata, e che è un'algebra di polinomi nelle funzioni simmetriche elementari. Per cui il quoziente

$$\pi\colon X \to X//G$$

si può realizzare come l'applicazione regolare

$$\pi\colon \mathbb{C}^n \to \mathbb{C}^n$$

corrispondente all'omomorfismo di algebre $\mathbb{C}[y_1, \ldots, y_n] \to \mathbb{C}[x_1, \ldots, x_n]$ che manda y_i in $\sigma_i(x_1, \ldots, x_n)$. Osserviamo che in questo caso $X//G$ è proprio in biiezione col quoziente insiemistico X/G, cioè le fibre di π sono proprio le G-orbite.

(2) Sia $G = \mathbb{C}^*$ (che è linearmente riduttivo) che agisce su $X = \mathbb{C}^2$ come nell'Esempio 5.5-(1). L'anello $\mathcal{O}(X)^G \subseteq \mathbb{C}[x, y]$ è fatto dai polinomi che, in ogni monomio, hanno il grado in x uguale al grado in y. Cioè

$$\mathcal{O}(X)^G = \mathbb{C}[xy].$$

Concludiamo che $X//G$ è isomorfo a $\mathbb{C}$, e che il quoziente $\pi\colon X \to X//G$, in coordinate è l'applicazione regolare

$$\begin{array}{ccc} \mathbb{C}^2 & \to & \mathbb{C} \\ (x, y) & \mapsto & xy \end{array}$$

Le fibre di quest'applicazione non coincidono però con le G-orbite. La fibra su un punto $\alpha \in \mathbb{C}$ con $\alpha \neq 0$ effettivamente è la singola orbita (chiusa) data da $xy = \alpha$, mentre la fibra su $0 \in \mathbb{C}$ è l'unione di tre orbite: una chiusa, e due che la contengono nella loro chiusura.

(3) Ritroviamo anche in un certo senso i risultati della Sezione 1.6. Qui $G = \mathrm{GL}(n)$ agisce su $X = M_n$. Il gruppo $\mathrm{GL}(n)$ è effettivamente linearmente riduttivo, anche se non l'abbiamo ancora dimostrato. In ogni caso, abbiamo già dimostrato che $\mathcal{O}(X)^G$ è finitamente generato, ed è un anello di polinomi. Segue che anche qui $X//G$ è isomorfo a $\mathbb{C}^n$.

(4) Studiamo più in dettaglio il quoziente di $G = \mathrm{GL}(3)$ che agisce per coniugio su $X = M_3$, in particolare le sue fibre. Sappiamo che $\mathcal{O}(M_3)^{\mathrm{GL}(3)}$ è un anello di polinomi nelle funzioni simmetriche elementari degli autovalori di $A \in M_3$. Possiamo esprimere sinteticamente l'applicazione nel modo seguente

$$\begin{array}{rccc} \pi\colon & M_3 & \to & \mathbb{C}^3 \\ & A & \mapsto & (\operatorname{Tr} A, \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3, \det A) \end{array}$$

dove $\lambda_1, \lambda_2, \lambda_3$ sono gli autovalori di A. Osserviamo prima di tutto che $M_3 = \mathbb{C} \cdot I \oplus V$ dove V è il sottospazio delle matrici a traccia nulla. La traccia è anche la prima entrata di π, e induce una biiezione $\mathbb{C} \cdot I \to \mathbb{C}$. Per cui, una fibra $\pi^{-1}(a, b, c)$ con $a, b, c \in \mathbb{C}$ si può scrivere come

$$\pi^{-1}(a, b, c) = \left\{ \frac{a}{3} \cdot I \right\} \times \pi_0^{-1}(b, c)$$

dove abbiamo identificato M_3 con $\mathbb{C} \cdot I \times V$ e dove

$$\begin{array}{rccc} \pi_0\colon & V & \to & \mathbb{C}^2 \\ & A & \mapsto & (\lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3, \det A). \end{array}$$

Studiamo allora le fibre di π_0. Ricordiamo che in V abbiamo tre tipi di forme normali di Jordan:

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & -\lambda - \mu \end{pmatrix}, \qquad \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & -2\lambda \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Sia $A \in V$ coniugata ad una matrice del primo tipo, e supponiamo che i suoi tre autovalori siano distinti. Allora sappiamo che A è diagonalizzabile, e nella fibra di $\pi_0(A)$ ci sono esattamente le altre matrici con i suoi stessi autovalori, in qualsiasi ordine: cioè esattamente la classe di coniugio di A. Quindi le G-orbite delle matrici del primo tipo con autovalori distinti coincidono con alcune fibre di π_0, e per questo sono anche G-orbite chiuse.

Sia ora $B \in V$ con un autovalore λ di molteplicità algebrica 2. Allora è coniugata ad una matrice del primo tipo (con $\lambda = \mu \neq 0$) o del secondo tipo (con $\lambda \neq 0$), e vale

$$\pi'(A) = (-3\lambda^2, -2\lambda^3).$$

Deduciamo che $\pi_0(B)$ come elemento di $\mathbb{C}^2$ soddisfa l'equazione $4x^3 + 27y^2 = 0$. Chiamiamo $K \subset \mathbb{C}^2$ la curva di questa equazione. La fibra su un punto $(x, y) \in K$ con $x \neq 0$ contiene esattamente due classi di coniugio, basta scegliere una matrice del primo tipo con $\lambda = \mu = \frac{3y}{2x}$, oppure del secondo tipo con lo stesso λ. La seconda classe di coniugio contiene la prima (esercizio), mentre la prima classe di coniugio è chiusa (esercizio[4]).

Rimane solo il punto $(0, 0) \in K$, che come controimmagine ha tutte le matrici di singolo autovalore 0: formano tre classi di coniugio, quelle delle tre matrici

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Solo la terza classe di coniugio, che è un singolo punto, è chiusa.

Come visto negli esempi, anche laddove G è linearmente riduttivo non sempre il quoziente categorico coincide con quello insiemistico, cioè non sempre le fibre di $\pi\colon X \to X//G$ sono le G-orbite. È però possibile dare un risultato generale sulla struttura delle fibre di π, e in particolare vedremo poi una relazione precisa fra fibre e G-orbite *chiuse*. Iniziamo con il teorema seguente.

---

[4]Suggerimento: visto che gi autovalori sono fissati, si può esprimere in termini delle entrate della matrice la condizione che la molteplicità geometrica di λ sia almeno 2, e quella di -2λ sia almeno 1.

Teorema 8.15. *Sia G un gruppo algebrico lineare linearmente riduttivo e X una G-varietà affine.*

1. *Il quoziente categorico $\pi\colon X \to X//G$ è suriettivo.*
2. *Sia $Y \subseteq X$ un chiuso G-stabile, sia $\iota\colon Y \to X$ l'inclusione, e si consideri $\pi'\colon Y//G \to X//G$ data dal passaggio al quoziente $Y \to Y//G$ dell'applicazione $\pi \circ \iota\colon Y \to X//G$. Allora π' ha immagine chiusa ed è un isomorfismo di $Y//G$ con la sua immagine in $X//G$. In altre parole, il quoziente categorico $\pi_Y\colon Y \to Y//G$ si può identificare con $\pi|_Y$.*
3. *Dati $Y, Y' \subseteq X$ chiusi G-stabili, vale $\pi(Y \cap Y') = \pi(Y) \cap \pi(Y')$. In particolare, ogni fibra di π contiene* **al più** *una G-orbita chiusa.*

Dimostrazione. Per la parte (1), sia $I \subseteq \mathcal{O}(X//G)$ un ideale massimale corrispondente a un punto qualsiasi di $X//G$. La controimmagine del punto è definita in $\mathcal{O}(X)$ dalle stesse funzioni, considerate in $\mathcal{O}(X)$ tramite l'inclusione $\mathcal{O}(X//G) \to \mathcal{O}(X)$, cioè l'ideale J generato da I in $\mathcal{O}(X)$ ha per luogo degli zeri proprio questa controimmagine. Possiamo scrivere J nuovamente come $J = I\mathcal{O}(X)$, e ricordiamo che $J^G = I$ come abbiamo visto. Segue che $J \neq \mathcal{O}(X)$, quindi J è un ideale proprio, e per il Nullstellensatz il luogo degli zeri di J in X è non vuoto. Quindi π è suriettiva.

Per la parte (2) basta usare il Corollario A.15, osservando che l'omomorfismo suriettivo di algebre $\mathcal{O}(X) \to \mathcal{O}(Y)$ dato dalla restrizione di funzioni da X a Y si restringe a un omomorfismo suriettivo di algebre $\mathcal{O}(X)^G \to \mathcal{O}(Y)^G$, come nella dimostrazione del Teorema 8.8.

Infine, dimostriamo la parte (3). Siano I, I' gli ideali rispettivamente di Y e Y' in $\mathcal{O}(X)$. Allora $Y \cap Y'$ è il luogo degli zeri di $I + I'$. D'altronde $\pi(Y)$, $\pi(Y')$ e $\pi(Y \cap Y')$ in $\mathcal{O}(X//G)$ sono rispettivamente i luoghi degli zeri di I^G, $(I')^G$ e $(I + I')^G$. A questo punto basta osservare che

$$(I + I')^G = R_X(I + I') = R_X(I) + R_X(I') = I^G + (I')^G$$

e quest'ultimo ha per luogo degli zeri $\pi(Y) \cap \pi(Y')$. □

Questo teorema è molto efficace nel caso delle azioni dei gruppi finiti.

Corollario 8.16. *Siano G ed X come nel Teorema 8.15, e supponiamo che G sia finito. Allora $X//G$ è il quoziente insiemistico, cioè ogni fibra del quoziente categorico è esattamente una G-orbita.*

Dimostrazione. Basta osservare che ogni G-orbita contiene solo un numero finito di punti, per cui ogni G-orbita è chiusa in X. □

9. Sulla geometria dei gruppi e delle orbite

Vediamo in questa sezione qualche applicazione importante del Corollario A.31.

Proposizione 9.1. *Sia G gruppo algebrico lineare.*

1. *Esiste un'unica componente irriducibile G° contenente l'elemento neutro $e \in G$. Questa componente irriducibile è una componente connessa di G, ed è un sottogruppo normale e chiuso.*
2. *Le classi laterali di G° sono le componenti irriducibili e anche le componenti connesse di G, sono aperte in G e sono in numero finito.*
3. *Ogni sottogruppo chiuso di G di indice finito contiene G°.*

Dimostrazione. Sia $X = X_1 \cup \ldots \cup X_m$ l'unione delle componenti irriducibili di G contenenti e. Consideriamo l'immagine Y della moltiplicazione $X_1 \times \ldots \times X_m \to G$, è un sottoinsieme irriducibile di G contenente e, quindi è contenuto in X ed essendo irriducibile è contenuto in X_{i_0} per qualche i_0. D'altronde Y contiene evidentemente tutte le componenti X_j, quindi $X_j \subseteq X_{i_0}$ per ogni j, cioè $X_j = X_{i_0}$. Segue che $m = i_0 = 1$, e che X è una componente irriducibile di G. Allora poniamo $G^\circ = X$, e osserviamo che G° è chiuso essendo una componente irriducibile. È anche un sottogruppo, perché le immagini della moltiplicazione $G^\circ \times G^\circ \to G$ e dell'inversione $G^\circ \to G$ sono irriducibili.

Dimostriamo che G° è normale: sia $g \in G$, e consideriamo $gG^\circ g^{-1}$. Si tratta di un sottogruppo chiuso e isomorfo a G°, quindi è irriducibile e interseca G°, e segue $gG^\circ g^{-1} = G^\circ$.

Le classi laterali di G° sono chiuse, disgiunte e irriducibili, ricoprono G, quindi sono le sue componenti irriducibili e sono anche in numero finito. Da questo segue anche che sono aperte, infatti fissandone una allora l'unione delle altre è un chiuso. Quindi sono anche le componenti connesse di G.

Sia infine H un sottogruppo chiuso di G di indice finito. Come per G°, vale che H e le sue classi laterali sinistre in G sono aperte e chiuse, essendo in numero finito e ricoprendo tutto G. Intersecate con G° ne forniscono un ricoprimento di aperti disgiunti, quindi ce n'è solo uno di questi aperti, e dev'essere $H \cap G^\circ$ perché H e G° si intersecano. Cioè $H \supseteq G^\circ$. $\square$

Esempio 9.2. (1) I gruppi $\mathbb{C}$, $\mathbb{C}^n$, $\mathbb{C}^*$ e $(\mathbb{C}^*)^n$ sono irriducibili, quindi connessi per la proposizione precedente.

(2) Sia N il gruppo dell'Esempio 7.5. Allora $N^\circ \cong \mathbb{C}^*$ è il sottogruppo delle matrici diagonali di N.

(3) Ponendo $\mathrm{SO}(n,\mathbb{C}) = \mathrm{O}(n,\mathbb{C}) \cap \mathrm{SL}(n)$, è facile vedere che $\mathrm{SO}(n,\mathbb{C})$ è un sottogruppo normale di indice 2 in $\mathrm{O}(n,\mathbb{C})$. Esercizio: dimostrare che $\mathrm{SO}(n,\mathbb{C})$ è connesso, da cui deriva che è anche irriducibile, e che $\mathrm{SO}(n,\mathbb{C}) = \mathrm{O}(n,\mathbb{C})^\circ$.

Proposizione 9.3. *Sia $\varphi\colon G \to H$ un omomorfismo di gruppi e un'applicazione regolare fra gruppi algebrici lineari. Allora la sua immagine è chiusa*[5].

Dimostrazione. Per il Corollario A.31, l'immagine K di φ contiene un aperto denso U di $\overline{K}$. D'altronde K è un sottogruppo di H, ed è facile dimostrare che anche $\overline{K}$ è un sottogruppo. Dimostriamo ora che $\overline{K} = U \cdot U$: preso $h \in \overline{K}$, osserviamo che xU^{-1} è anch'esso un aperto denso di $\overline{K}$. Segue che U interseca xU^{-1}, da cui deduciamo che $x \in U \cdot U$. Cioè $\overline{K} = U \cdot U$.

Ora basta osservare che $U \cdot U \subseteq K$ per concludere la dimostrazione. $\square$

Proposizione 9.4. *Sia G gruppo algebrico lineare che agisce su una varietà affine X. Ogni G-orbita è aperta nella sua chiusura.*

Dimostrazione. Ogni orbita Y di G in X è immagine di un'applicazione regolare $\varphi\colon G \to X$. Per il Corollario A.31, l'immagine Y contiene un aperto U della sua chiusura Z. D'altronde Y è G-stabile, quindi

$$Y = \bigcup_{g \in G} g \cdot U,$$

e ogni $g \in G$ agisce come un isomorfismo di Z in se stesso, per cui $g \cdot U$ è aperto in Z per ogni g. Concludiamo che Y è aperta in Z. $\square$

Corollario 9.5. *Nelle ipotesi della proposizione precedente, ogni chiuso G-stabile non vuoto di X contiene almeno una G-orbita chiusa.*

Dimostrazione. Sia $Y_1 \subseteq X$ un chiuso G-stabile, allora è unione di G-orbite. Sia Z una sua G-orbita, e sia $Y_2 = Y_1 \setminus Z$. Per la proposizione precedente, Y_2 è un chiuso, ed è G-stabile. Se è vuoto, allora $Y_1 = Z$ era una singola G-orbita, altrimenti ripetiamo la procedura con Y_2 al posto di Y_1, e così via. Essa deve terminare, perché ogni catena discendente di chiusi $Y_1 \supseteq Y_2 \supseteq \dots$ si stabilizza. Per costruzione, il termine su cui si stabilizza la catena è l'insieme vuoto, e l'ultimo termine non vuoto è un'orbita chiusa contenuta in Y_1. $\square$

Con questa proposizione possiamo rendere più preciso il Teorema 8.15.

Corollario 9.6. *Siano G ed X come nel Teorema 8.15. Allora ogni fibra del quoziente $\pi\colon X \to X/\!/G$ contiene* **esattamente** *una G-orbita chiusa.*

Dimostrazione. Sia Y una fibra di π. Si tratta di un chiuso G-stabile non vuoto, quindi contiene almeno una G-orbita chiusa per il Corollario 9.5. $\square$

Concludiamo con un legame sorprendente fra G-orbite "grandi" e "piccole".

Corollario 9.7. *Siano G ed X come nel Teorema 8.15. Se X ha una G-orbita densa, allora ha esattamente una G-orbita chiusa.*

Dimostrazione. Nelle nostre ipotesi, le funzioni in $\mathcal{O}(X)^G$ sono solo le costanti, per cui $X/\!/G$ è un singolo punto. $\square$

Sottolineiamo che le proprietà viste finora del quoziente categorico valgono solo per G linearmente riduttivo.

---

[5] Questa è una particolarità utilissima degli omomorfismi regolari fra gruppi algebrici, e non vale ad esempio per omomorfismi differenziabili fra gruppi di Lie.

Esempio 9.8. Sia $X = \mathrm{GL}(n)$, e $G = B(n)$ che agisce per moltiplicazione a destra. Allora il quoziente insiemistico è l'insieme X/G delle classi laterali sinistre, e sono tutte G-orbite chiuse in X. Si può dimostrare che però le sole funzioni G-invarianti per traslazione a destra sono le costanti, cioè il quoziente categorico $X//G$ esiste ma è un singolo punto.

10. Altri gruppi linearmente riduttivi: i gruppi autoaggiunti

Avendo visto l'importanza della lineare riduttività, in questa sezione introduciamo un criterio sufficiente che assicura la lineare riduttività di diversi gruppi noti. È interessante anche perché è conseguenza di un legame molto importante e generale fra G-moduli regolari e il G-modulo $\mathcal{O}(G)$.

Lemma 10.1. *Sia $G \subseteq \mathrm{GL}(n)$ un gruppo algebrico lineare, e sia V un G-modulo regolare. Allora V è isomorfo ad un sottomodulo di $\mathcal{O}(G)^n$ per qualche intero positivo n, dove G agisce su $\mathcal{O}(G)$ per traslazione a destra.*

Dimostrazione. Se V ha dimensione 0 allora il lemma è ovvio semplicemente ponendo $n = 1$. Altrimenti sia $(u_1, \dots, u_n)$ una base di V^*, e si consideri l'applicazione

$$\begin{array}{rcc} V & \to & \mathcal{O}(G)^n \\ v & \mapsto & (g \mapsto (u_1(g \cdot v), \dots, u_n(g \cdot v)). \end{array}$$

Si tratta di un'applicazione G-equivariante: dato $h \in G$, il vettore $h \cdot v$ va nell'n-upla di funzioni

$$g \mapsto (u_1(g \cdot (h \cdot v)), \dots, u_n(g \cdot (h \cdot v))).$$

Consideriamo invece l'azione di h per traslazione a destra sull'entrata i-esima $g \mapsto u_i(g \cdot v)$: si tratta della funzione che a g associa il valore della vecchia funzione in gh, cioè si tratta della funzione

$$g \mapsto u_i((gh) \cdot v) = u_i(g \cdot (h \cdot v)).$$

Inoltre l'applicazione $V \to \mathcal{O}(G)^n$ che abbiamo costruito è iniettiva, basta porre la variabile g uguale all'elemento neutro del gruppo G. □

Lo stesso enunciato è vero anche se facciamo agire G su $\mathcal{O}(G)$ per traslazione a sinistra, con dimostrazione simile (esercizio).

Grazie al lemma possiamo collegare le rappresentazioni regolari di $G \subseteq \mathrm{GL}(V)$ col G-modulo V e le sue potenze tensoriali. Prima di procedere, osserviamo due fatti di carattere generale.

Osservazione 10.2.
(1) Siano U, V entrambi G-moduli regolari, dove G è un gruppo algebrico lineare. Allora il prodotto tensoriale $U \otimes V$ è dotato di struttura naturale di G-modulo regolare, definendo
$$g \cdot (u \otimes v) = (g \cdot u) \otimes (g \cdot v)$$
per ogni $g \in G$, $u \in U$ e $v \in V$.
(2) La stessa costruzione si applica alle potenze simmetriche S^dV e alle potenze esterne $\bigwedge^d V$.
(3) Dati un G-modulo regolare V e un sottomodulo U, lo spazio vettoriale quoziente V/U è dotato di struttura naturale di G-modulo regolare, definendo
$$g \cdot (v + U) = (g \cdot v) + U$$
per ogni $g \in G$ e $v \in V$. Lasciamo per esercizio il dimostrare che ogni quoziente di un G-modulo completamente riducibile è completamente riducibile.

Teorema 10.3. *Sia $G \subseteq \mathrm{GL}(V)$ un gruppo algebrico lineare, e sia U un G-modulo regolare. Esistono interi positivi d, s ed $m_1, \dots, m_s$ tali che $U \otimes \mathbb{C}_d$ è isomorfo ad un quoziente di un sottomodulo della somma diretta*

$$V^{\otimes m_1} \oplus \dots \oplus V^{\otimes m_s}.$$

Qui $\mathbb{C}_d$ è il G-modulo di dimensione 1 dove $g \in G$ agisce come moltiplicazione per $\det(g)^d$.

Dimostrazione. Sappiamo per il Lemma 10.1 che U è contenuto in $\mathcal{O}(G)^n$ (considerato come G-modulo con la traslazione a destra) per qualche intero positivo n. D'altronde, per la Proposizione A.10, esistono interi positivi d ed n tali che l'immagine di U è contenuta nel sottospazio $(A \cdot \det(x)^{-d}|_G)^n$ di $\mathcal{O}(G)^n$, dove A è l'anello delle funzioni su G che sono polinomiali nelle entrate delle matrici[6]. In altre parole A è l'immagine di $\mathcal{O}(\mathrm{End}(V))$ in $\mathcal{O}(G)$ tramite la restrizione da $\mathrm{End}(V)$ a G. Questa restrizione è anche un omomorfismo di G-moduli; qui stiamo considerando $\mathrm{End}(V)$ come G-modulo con la traslazione a destra, che estende la traslazione a destra di G su se stesso.

Ora, tensorizzare U con $\mathbb{C}_d$ vuol dire semplicemente moltiplicare per $\det(g)^d$ l'endomorfismo di U associato a $g \in G$. Ripercorrendo la dimostrazione del Lemma 10.1, questo implica che le funzioni su G che associamo agli elementi di U vengono tutte moltiplicate per la funzione $\det(x)^d|_G$. Allora $U \otimes \mathbb{C}_d$ è contenuto in A^n. Quest'ultimo, come osservato prima, è un quoziente di $\mathcal{O}(\mathrm{End}(V))^n$.

Come G-modulo, lo spazio vettoriale $\mathrm{End}(V)$ è isomorfo a $(V^*)^{\dim(V)}$. Infatti, stiamo moltiplicando righe per colonne due matrici: a sinistra un endomorfismo qualsiasi, a destra g^{-1} dove $g \in G$. Questo è come moltiplicare le singole righe della prima matrice ciascuna per g^{-1}. E questa è proprio l'azione di G sul duale V^* ripetuta $\dim(V)$ volte, basta interpretare gli elementi di V^* come vettori riga e il valore di un vettore riga (=funzionale) su un vettore colonna come il prodotto riga per colonna.

Quindi come G-modulo possiamo identificare $\mathcal{O}(\mathrm{End}(V))$ con $\mathcal{O}((V^*)^{\dim(V)})$. D'altronde le funzioni polinomiali su ciascuna singola copia di V^* non sono altro che la somma diretta

$$\mathcal{O}(V^*) = \bigoplus_{i=0}^{\infty} S^i V.$$

Visto che ogni S^iV è un quoziente di $V^{\otimes i}$, esiste una somma diretta (in generale infinita) di potenze tensoriali di V che ammette un omomorfismo di G-moduli suriettivo su $\mathcal{O}(\mathrm{End}(V))^n$.

Infine basta scegliere un numero finito di tali addendi, in modo che l'immagine della loro somma

$$\Sigma = V^{\otimes m_1} \oplus \ldots \oplus V^{\otimes m_s}$$

contenga il sottomodulo $U \otimes \mathbb{C}_d$ di $\mathcal{O}(\mathrm{End}(V))^n$. Allora $U \otimes \mathbb{C}_d$ è isomorfo alla sua controimmagine in Σ, quozientata per il nucleo dell'omomorfismo $\Sigma \to \mathcal{O}(\mathrm{End}(V))^n$. □

Vediamo come applicare questo teorema alla lineare riduttività. A differenza delle sezioni precedenti, qui è importante lavorare su $\mathbb{C}$ invece che su un qualsiasi campo algebricamente chiuso di caratteristica zero.

Definizione 10.4. Un gruppo algebrico lineare $G \subseteq \mathrm{GL}(n, \mathbb{C})$ si dice *autoaggiunto* se per ogni $g \in G$ anche ${}^t\overline{g}$ è in G.

Più in generale, se abbiamo V uno spazio di Hilbert complesso di dimensione finita, con prodotto Hermitiano $\langle -, - \rangle$, per ogni $A \in \mathrm{End}(V)$ è definita l'aggiunta A^* tale che $\langle Av, w \rangle = \langle v, A^*w \rangle$ per ogni $v, w \in V$. Allora $G \subseteq \mathrm{GL}(V)$ si dice *autoaggiunto* se $g^* \in G$ per ogni $g \in G$.

Lemma 10.5. *Sia V come sopra, e sia $G \subseteq \mathrm{GL}(V)$ un gruppo algebrico lineare autoaggiunto. Allora V è completamente riducibile.*

Dimostrazione. Dato U un sottomodulo di V, abbiamo $U \oplus U^\perp = V$, e inoltre dato $v \in U^\perp$ e $g \in G$ vale

$$\langle gv, u \rangle = \langle v, g^*u \rangle = 0$$

per ogni $u \in U$, visto che $g^* \in G$. Segue che $U^\perp$ è un complemento G-stabile di U in V. □

Corollario 10.6. *Siano G e V come nel lemma precedente. Allora $V^{\otimes m}$ è completamente riducibile per ogni intero positivo m.*

Dimostrazione. Basta osservare che $V^{\otimes m}$ è uno spazio di Hilbert complesso, con il prodotto Hermitiano

$$\langle v_1 \otimes \ldots \otimes v_n, w_1 \otimes \ldots \otimes w_n \rangle = \langle v_1, w_1 \rangle \cdots \langle v_n, w_n \rangle.$$

Inoltre, denotando con $g^{\otimes m}$ l'endomorfismo di $V^{\otimes m}$ indotto da g, si verifica facilmente che $(g^{\otimes m})^* = (g^*)^{\otimes m}$, per cui anche l'immagine di G in $\mathrm{GL}(V^{\otimes m})$ è un sottogruppo autoaggiunto. □

Arriviamo alla conclusione della sezione.

Corollario 10.7. *Sia $G \subseteq \mathrm{GL}(n, \mathbb{C})$ un guppo algebrico lineare autoaggiunto. Allora G è linearmente riduttivo.*

[6] Stiamo identificando come al solito gli endomorfismi di V con le matrici loro associate, fissata una base di V una volta per tutte.

Dimostrazione. Basta porre $V = \mathbb{C}^n$ e osservare che ogni somma diretta del tipo

$$V^{\otimes m_1} \oplus \ldots \oplus V^{\otimes m_s},$$

è completamente riducibile per il lemma precedente. Quindi anche ogni suo sottomodulo, e anche ogni quoziente di ogni suo sottomodulo. A questo punto il Teorema 10.3 conclude la dimostrazione. □

Esempio 10.8. Dal corollario deduciamo che i gruppi $\mathrm{GL}(n,\mathbb{C})$, $\mathrm{SL}(n,\mathbb{C})$, $\mathrm{O}(n,\mathbb{C})$, $\mathrm{Sp}(2n,\mathbb{C})$ sono linearmente riduttivi, e anche il gruppo $\mathrm{SO}(n,\mathbb{C}) = \mathrm{O}(n,\mathbb{C}) \cap \mathrm{SL}(n,\mathbb{C})$.

11. Spazi omogenei

Se il gruppo che agisce non è linearmente riduttivo, può essere estremamente difficile studiare i suoi quozienti categorici, anche quando esistono. Essenzialmente, l'unico caso che si riesce a studiare in generale è quello di un sottogruppo chiuso H di un gruppo algebrico lineare G, dove H agisce su G per traslazione a destra o a sinistra.

In questo caso il quoziente insiemistico, che è l'insieme delle classi laterali destre o sinistre, si può *sempre* dotare di struttura di varietà algebrica, però non sempre affine. Con essa, che vedremo in questa sezione, il quoziente si chiama uno *spazio omogeneo.* È anche un quoziente categorico, ma solo se prendiamo una definizione più generale della Definizione 8.1, come mostra l'Esempio 9.8.

Esempio 11.1. Sia $G = B(n)$ e $H = U(n)$, che agisce su G per moltiplicazione a destra. Ogni matrice $g \in G$ si scrive in modo unico come $t \cdot h$, dove $h \in H$ e t è una matrice diagonale, che ha sulla diagonale proprio le entrate sulla diagonale di g. Quindi, intanto il quoziente insiemistico $G \to G/H$ si può realizzare nel modo seguente

$$\begin{array}{ccc} G & \to & (\mathbb{C}^*)^n \\ \begin{pmatrix} a_{1,1} & \ldots & a_{1,n} \\ \vdots & \ddots & \vdots \\ 0 & \ldots & a_{n,n} \end{pmatrix} & \mapsto & (a_{1,1}, \ldots, a_{n,n}). \end{array}$$

D'altronde questo è anche il quoziente categorico. Intanto è un'applicazione regolare. Poi, ogni funzione $f \in \mathcal{O}(G)^H$ dipende solo da t, e preso un qualsiasi polinomio di Laurent nelle entrate sulla diagonale, esso si può considerare come funzione regolare su G (considerandolo come polinomio dove le altre entrate della matrice sono variabili che non compaiono). Cioè $\mathcal{O}(G)^H$ è isomorfo a $\mathcal{O}((\mathbb{C}^*)^n)$, e l'isomorfismo che abbiamo descritto è quello indotto da φ^*.

Quindi, anche se H non è linearmente riduttivo, il quoziente categorico $\pi\colon G \to G/\!/H$ esiste e coincide con quello insiemistico.

Il seguente è il teorema principale che ci permetterà di studiare gli spazi omogenei.

Teorema 11.2. *(Chevalley) Sia G gruppo algebrico lineare, e sia $H \subseteq G$ un sottogruppo chiuso. Allora esiste una rappresentazione regolare $G \to \mathrm{GL}(V)$ e un sottospazio $U \subseteq V$ di dimensione 1 che ha stabilizzatore esattamente H, cioè*

$$H = \{g \in G \mid g \cdot U = U\}.$$

Dimostrazione. Iniziamo col trovare V' e U', analoghi a V e U, ma con U' di dimensione non necessariamente 1. Consideriamo $I_G(H) \subseteq \mathcal{O}(G)$: si tratta di un ideale finitamente generato, quindi possiamo trovare un sottospazio $U' \subseteq I_G(H)$ di dimensione finita e che genera $I_G(H)$ come ideale. Per la Proposizione 5.2, possiamo assumere che U' sia stabile sotto l'azione di H per traslazione a destra. Per la Proposizione 4.2, il sottospazio $U' \subseteq \mathcal{O}(G)$ è contenuto in un G-sottomodulo regolare $V' \subseteq \mathcal{O}(G)$.

Dimostriamo che $H = \{g \in G \mid g \cdot U' = U'\}$. L'inclusione "⊆" è chiara, sia allora $g \in G$ tale che $g \cdot U' = U'$. Ricordiamo che la traslazione a destra per g è un automorfismo di algebre, da cui segue $g \cdot I_G(H) = I_G(H)$. Sia ora $f \in I_G(H)$: la funzione $g \cdot f$ svanisce su H, ma calcolata in $e \in H$ vale $0 = (g \cdot f)(e) = f(eg) = f(g)$, quindi f svanisce su g. Segue che $g \in H$.

Abbiamo dunque trovato V' e U'. Per trovare U e V, basta prendere $V = \bigwedge^d V'$ e $U = \bigwedge^d U'$, dove $d = \dim(U')$. Allora V è un G-modulo razionale, e U è un sottospazio H-stabile di dimensione 1. Va solo verificato che H è proprio il suo stabilizzatore.

Sia allora $g \in G$ tale che $g \cdot U = U$, e facciamo vedere che $g \cdot U' = U'$, da cui seguirà $g \in H$. Scegliamo una base $u_1, \ldots, u_n$ di V' tale che $u_1, \ldots, u_d$ generano U', e $u_{r+1}, \ldots, u_{r+d}$ generano $g \cdot U'$, per qualche intero non negativo r. Il vettore $u_1 \wedge \ldots \wedge u_d$ genera U per costruzione, e viene mandato da g in un suo multiplo scalare perché g stabilizza U; d'altronde g manda U' in $g \cdot U'$ quindi manda ogni u_i per $i \in \{1, \ldots, d\}$ in combinazioni lineari degli u_j con $j \in \{r+1, \ldots, r+d\}$. Segue che g manda $u_1 \wedge \ldots \wedge u_d$ in un multiplo scalare di $u_{r+1} \wedge \ldots \wedge u_{r+d}$. Da questo deduciamo che $r = 0$, cioè $g \cdot U' = U'$. □

Prendiamo allora il quoziente G/H, cioè l'insieme delle classi laterali sinistre. Il teorema ci assicura che G/H si può dotare di struttura di varietà quasi proiettiva, come osserva il corollario seguente.

Corollario 11.3. *Nelle ipotesi del Teorema 11.2, è possibile dotare G/H di struttura di varietà quasi proiettiva. Più precisamente, esiste una varietà quasi proiettiva Y e un'applicazione regolare suriettiva $\pi \colon G \to Y$ tali che le fibre di π sono esattamente le classi laterali sinistre di H in G.*

Dimostrazione. Siano V ed U come nel Teorema 11.2, consideriamo U come un punto p dello spazio proiettivo $\mathbb{P}(V)$. Possiamo anche considerarlo come classe d'equivalenza $p = [u]$ di un vettore $u \in U \setminus \{0\}$.

L'applicazione $\pi \colon G \to \mathbb{P}(V)$ che manda g in $[g \cdot u]$ è regolare, basta esprimerla in coordinate sul ricoprimento aperto usuale di $\mathbb{P}(V)$. Infatti, siano $y_0, \ldots, y_m$ coordinate su V, e siano $a_0, \ldots, a_m \in \mathcal{O}(G)$ tali che $g \mapsto g \cdot u$ si esprime in coordinate come $g \mapsto (a_0(g), \ldots, a_m(g))$. Definiamo $G_i = G \setminus V_G(a_i)$, osserviamo che π manda l'aperto affine G_i di G nell'aperto affine di $\mathbb{P}(V)$ definito da $y_i \neq 0$, e $\pi|_{G_i}$ in coordinate è l'applicazione

$$g \mapsto \left(\frac{a_0(g)}{a_i(g)}, \ldots, \frac{a_{i-1}(g)}{a_i(g)}, \frac{a_{i+1}(g)}{a_i(g)}, \ldots, \frac{a_m(g)}{a_i(g)} \right),$$

che è un'applicazione regolare su G_i.

Infine, l'immagine Y di π, cioè la G-orbita di p, è localmente chiusa in $\mathbb{P}(V)$. Infatti, l'immagine Y contiene un aperto denso della sua chiusura grazie al Corollario A.31 applicato a tutte le $\pi|_{G_i}$, e a questo punto lo stesso argomento della Proposizione 9.4 assicura che Y è aperto nella sua chiusura. Quindi per concludere la dimostrazione basta restringere il codominio di π da $\mathbb{P}(V)$ a Y. □

Esempio 11.4.
(1) Sia $G = \mathrm{GL}(2)$ e $H = B(2)$. Allora $\mathbb{C}^2$ con l'azione naturale di G si può prendere come V, e il sottospazio generato dal primo vettore della base canonica si può prendere come U. Quindi G/H è una G-orbita contenuta in $\mathbb{P}^1$. D'altronde, $\mathbb{P}^1$ contiene una sola G-orbita, per cui $G/H = \mathbb{P}^1$.
(2) Più in generale, il quoziente $\mathrm{GL}(n)/B(n)$ si identifica insiemisticamente con l'insieme $\mathcal{F}$ delle *bandiere* di $\mathbb{C}^n$, cioè l'insieme delle catene di sottospazi $\{0\} = V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_{n-1} \subsetneq V_n = \mathbb{C}^n$ dove V_i ha dimensione i per ogni i. Infatti G agisce in modo ovviamente transitivo su $\mathcal{F}$, e $B(n)$ è proprio lo stabilizzatore della bandiera dove V_i è generato dai primi i vettori della base canonica. Grazie ai risultati che abbiamo visto, $\mathcal{F}$ si dota di struttura naturale di varietà, e si può dimostrare che si tratta sempre di una varietà proiettiva.
(3) Ripetiamo la costruzione precedente, ma considerando *bandiere parziali.* Fissiamo cioè una sequenza strettamente crescente di interi non negativi $\underline{i} = (i_1, \ldots, i_m)$, con il loro numero m fissato e tutti $\leq n$. Definiamo $\mathcal{F}_{\underline{i}}$ come l'insieme delle bandiere $\{0\} \subsetneq V_{i_1} \subsetneq \ldots \subsetneq V_{i_m} \subsetneq \mathbb{C}^n$. Il gruppo $G = \mathrm{GL}(n)$ agisce transitivamente anche su $\mathcal{F}_{\underline{i}}$, e possiamo descrivere lo stabilizzatore H del punto che corrisponde alla bandiera in cui il sottospazio V_{i_r} è generato dai primi i_r vettori della base canonica. Si tratta di un sottogruppo contenente $B(n)$, ed è fatto dalle matrici che sulla diagonale hanno blocchi $i_1 \times i_1$, poi $(i_2 - i_1) \times (i_2 - i_1)$, fino a $(i_m - i_{m-1}) \times (i_m - i_{m-1})$, infine $(n - i_m) \times (n - i_m)$. In questi blocchi le entrate sono arbitrarie, e sono arbitrarie anche quelle al di sopra di questa sequenza di blocchi in diagonale. Sotto i blocchi invece tutte le entrate sono 0.
(4) Ponendo $m = 1$ e per semplicità $i_1 = d$, riotteniamo come $\mathcal{F}_{\underline{i}}$ la Graßmanniana $\mathrm{Gr}(d, n)$ dei sottospazi di dimensione d in $\mathbb{C}^n$. Le matrici in H qui hanno la forma

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

dove il blocco in alto a sinistra è $d \times d$. Si tratta di una varietà proiettiva, e si può realizzare facilmente nel modo indicato dalla dimostrazione del Teorema 11.2. Infatti possiamo prendere

$V' = \mathbb{C}^n$, e allora H è lo stabilizzatore del sottospazio U' generato dai primi d vettori della base canonica. Come in quella dimostrazione, prendiamo $V = \bigwedge^d \mathbb{C}^n$, e $U = \bigwedge^d U'$.

Vediamo quindi G/H come l'insieme dei punti del tipo $g \cdot U$, ed è tutta la Graßmanniana $\mathrm{Gr}(d, n)$ perché per ogni V_d come sopra esiste $g \in G$ tale che $g \cdot U' = V_d$. In $\mathbb{P}(\bigwedge^d \mathbb{C}^n)$ coincide con l'insieme dei punti di $\mathbb{P}(\bigwedge^d \mathbb{C}^n)$ del tipo $[v_1 \wedge \ldots \wedge v_d]$, dove i vettori $v_1, \ldots, v_d$ sono linearmente indipendenti (e quindi formano una base di V_d). Vediamo come realizzare questa inclusione di $\mathrm{Gr}(d, n)$ in $\mathbb{P}(\bigwedge^d \mathbb{C}^n)$ esplicitamente in coordinate.

Ricordiamo che una base di $\bigwedge^d \mathbb{C}^n$ è data dagli elementi del tipo $e_{i_1} \wedge \ldots \wedge e_{i_d}$, dove $e_1, \ldots, e_n$ sono i vettori della base canonica, per ogni scelta di indici tali che $1 \le i_1 < \ldots < i_d \le n$. Ad ogni tale scelta di indici, chiamiamola come prima $\underline{i}$, corrisponde una coordinata su $\bigwedge^d \mathbb{C}^n$, coordinata che chiamiamo $x_{\underline{i}}$.

Dato un sottospazio $V_d \in \mathrm{Gr}(d, n)$, prendiamo una sua base $(v_1, \ldots, v_d)$ e mettiamo i vettori come colonne di una matrice A, di entrate $a_{i,j}$. Facciamo corrispondere a ogni scelta di indici $1 \le i_1 < \ldots < i_d \le n$ la sottomatrice quadrata $d \times d$ che coinvolge quelle righe. Chiamiamo il suo determinante $q_{\underline{i}}$, è una funzione delle entrate $a_{i,j}$. È facile dimostrare usando le proprietà del prodotto esterno che $q_{\underline{i}}$ è precisamente il valore della variabile $x_{\underline{i}}$ sull'elemento $v_1 \wedge \ldots \wedge v_d$ di $\bigwedge^d \mathbb{C}^n$, basta esprimere ogni v_i in termini della base canonica e "svolgere" il prodotto $v_1 \wedge \ldots \wedge v_d$ esprimendolo in termini dei vettori $e_{j_1} \wedge \ldots \wedge e_{j_d}$ per tutte le scelte di indici $\underline{j}$.

Naturalmente il valore delle funzioni $q_{\underline{i}}$ non è univocamente determinato da V_d, ma dalla scelta della base che abbiamo fatto: se cambiamo base cambiano i valori. Tuttavia, ricordando come cambia il determinante se facciamo operazioni elementari sulle colonne, è chiaro che i rapporti $q_{\underline{i}}/q_{\underline{j}}$ sono ben definiti, nel senso che dipendono solo da V_d e non dalla base scelta.

Per questo motivo le funzioni $q_{\underline{i}}$ sono "coordinate omogenee" su $\mathrm{Gr}(d, n)$: sono infatti proprio le coordinate omogenee dello spazio ambiente $\mathbb{P}(\bigwedge^d \mathbb{C}^n)$ "ristrette" agli elementi del sottoinsieme $\mathrm{Gr}(d, n)$. Queste coordinate prendono il nome di *coordinate di Plücker*. È possibile descrivere esplicitamente delle relazioni soddisfatte dalle coordinate di Plücker, le cosiddette *relazioni di Plücker*, che descrivono $\mathrm{Gr}(d, n)$ come chiuso di Zariski di $\bigwedge^d \mathbb{C}^n$.

Non diamo queste relazioni, però dimostriamo che $\mathrm{Gr}(d, n)$ è chiuso in $\bigwedge^d \mathbb{C}^n$, vedendo che per ogni $\underline{i}$ l'intersezione $\mathrm{Gr}(d, n) \cap U_{\underline{i}}$ è chiusa in $U_{\underline{i}}$, dove quest'ultimo è l'aperto affine di $\bigwedge^d \mathbb{C}^n$ dove $x_{\underline{i}} \neq 0$. Quindi le coordinate su $U_{\underline{i}}$ sono i rapporti $x_{\underline{j}}/x_{\underline{i}}$ per ogni $\underline{j} \neq \underline{i}$.

Se $V_d \in \mathrm{Gr}(d, n) \cap U_{\underline{i}}$, allora su una qualsiasi base di V_d la funzione $q_{\underline{i}}$ è non nulla. Possiamo scegliere la base in modo che il minore corrispondente a $\underline{i}$ sia l'identità, e allora le altre coordinate di V_d in $U_{\underline{i}}$ sono proprio i valori $q_{\underline{j}}$ su quella base, invece che i rapporti $q_{\underline{j}}/q_{\underline{i}}$. Osserviamo che, fissato questo minore uguale all'identità, qualsiasi altra scelta nelle entrate rimanenti della matrice A corrisponde a un altro elemento di $\mathrm{Gr}(d, n) \cap U_{\underline{i}}$. Supponiamo per semplicità che $\underline{i} = (1, \ldots, d)$, e consideriamo l'applicazione che alla matrice A associa il sottospazio V_d, visto come punto in $\bigwedge^d \mathbb{C}^n$, in coordinate su $U_{\underline{i}}$. Si tratta dell'applicazione che manda

$$\begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \\ a_{d+1,1} & a_{d+1,2} & \ldots & a_{d+1,d} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1} & a_{n,2} & \ldots & a_{n,d} \end{pmatrix}$$

nella sequenza dei valori delle $q_{\underline{j}}$ su questa matrice, per ogni $\underline{j} \neq \underline{i}$.

L'osservazione cruciale ora è che le entrate $a_{i,j}$ "libere" della matrice qui sopra compaiono come *alcune* delle $q_{\underline{j}}$ a meno del segno. Basta osservare che ad es. $a_{d+1,d}$ è il valore di $q_{\underline{j}}$ dove $\underline{j} = (1, 2, \ldots, d-1, d+1)$. Lo stesso avviene con tutte le altre $a_{i,j}$, scegliendo opportunamente le righe da coinvolgere. Naturalmente tante altre $q_{\underline{j}}$ saranno invece polinomi più complicati nelle entrate di A. In ogni caso, allora $\mathrm{Gr}(d, n) \cap U_{\underline{i}}$ è un chiuso di $U_{\underline{i}}$ grazie al Lemma A.18.

(5) Sia $G = \mathrm{GL}(2)$ e $H = U(2)$. Allora possiamo vedere G/H come l'orbita del primo vettore e_1 della base canonica di $\mathbb{C}^2$. Osserviamo che quest'orbita è quasi affine, essendo $\mathbb{C}^2 \smallsetminus \{0\}$. Per vederla come orbita di un punto di $\mathbb{P}(V)$ come prima, basta prendere $V = \mathbb{C}^2 \oplus \mathbb{C}$ dove sul secondo addendo G agisce banalmente, e prendere il vettore $v = e_1 + 1$ dove $e_1 \in \mathbb{C}^2$ e $1 \in \mathbb{C}$.

(6) Sia $G = \mathrm{GL}(2)$ e $H = H(2)$. Qui possiamo prendere $V = \mathbb{C}^2 \otimes \mathbb{C}^2$ (prodotto tensoriale di due G-moduli isomorfi) e $v = e_1 \otimes e_2'$, dove e_1 è il primo vettore della base canonica della prima copia di $\mathbb{C}^2$, ed e_2' è il secondo vettore della base canonica della seconda copia di $\mathbb{C}^2$. Con questa scelta si dimostra facilmente che lo stabilizzatore della retta generata da v è proprio H, quindi G/H si realizza come orbita in $\mathbb{P}(V) = \mathbb{P}^3$.

Esercizio 11.5. Si consideri di nuovo $G = \mathrm{GL}(2)$, $H = H(2)$, V e v come nell'esempio precedente. Si dimostri che l'orbita $G \cdot [v]$ è nell'immagine dell'immersione di Segre $S\colon \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$, e che si tratta proprio di $\mathbb{P}^1 \times \mathbb{P}^1$ privato della diagonale. Si concluda che G/H in questo caso è una varietà affine.

Allo stesso modo potremmo trattare il quoziente $H \setminus G$, cioè l'insieme delle classi laterali destre, dotandolo di struttura di varietà quasi proiettiva.

Queste strutture di varietà su G/H e su $H \setminus G$ non dipendono dalle scelte fatte nelle dimostrazioni qui sopra, e sono dotate delle proprietà universali di quozienti categorici (se le estendiamo in modo ovvio alle varietà quasi proiettive).

Prendendo il caso di G/H, possiamo esprimere la sua proprietà universale nel teorema seguente. La dimostrazione in sé non è molto profonda, però si appoggia in modo essenziale al Teorema Principale di Zariski (Zariski's Main Theorem). Si tratta di un risultato difficile di geometria algebrica e ci porterebbe al di là degli scopi del corso, per cui diamo il nostro teorema senza dimostrazione.

Teorema 11.6. *(senza dimostrazione) Siano G un gruppo algebrico lineare e H un sottogruppo chiuso. Supponiamo che G/H sia dotato di struttura di varietà quasi proiettiva, in modo tale che il quoziente $\pi\colon G \to G/H$ sia un'applicazione regolare. Sia $\varphi\colon G \to Z$ un'applicazione regolare costante sulle classi laterali sinistre di H, dove Z è una varietà quasi proiettiva. Allora esiste un'applicazione regolare $\psi\colon G/H \to Z$ che fattorizza φ, cioè tale che $\varphi = \psi \circ \pi$.*

In realtà esiste una versione ancora più generale del teorema, espressa in termini di varietà algebriche più generali di quelle quasi proiettive. Anch'essa va oltre gli scopi del corso.

In alternativa al Teorema 11.6, dimostriamo il Teorema 11.8 qui sotto. Si tratta di un risultato più debole che si dimostra molto più facilmente, perché richiede che G agisca sulle varietà in questione, cosa che non avviene col Teorema 11.6. È comunque utilissimo nelle applicazioni e negli esempi.

Per enunciare il teorema, innanzitutto, va estesa la nozione di G-varietà.

Definizione 11.7. Sia X una varietà quasi proiettiva e G un gruppo algebrico lineare. Se G agisce su X in modo che l'applicazione corrispondente $G \times X \to X$ è regolare, allora l'azione è detta *regolare*, e X è detta *G-varietà.*

Le nozioni di G-equivarianza e isomorfismo fra G-varietà si estendono in modo ovvio al caso quasi proiettivo.

Teorema 11.8. *Siano G un gruppo algebrico lineare e H un sottogruppo chiuso. Supponiamo che G/H sia dotato di struttura di varietà quasi proiettiva, in modo tale che il quoziente $\pi\colon G \to G/H$ sia un'applicazione regolare. Sia poi Z una G-varietà quasi proiettiva con un punto $z \in Z$ fissato da H. Allora esiste un'unica applicazione regolare G-equivariante $\psi\colon G/H \to Z$ tale che $\psi(eH) = z$.*

Per la dimostrazione usiamo il lemma seguente.

Lemma 11.9. *Sia G un gruppo algebrico lineare, e siano X, Y G-varietà quasi proiettive costituite ciascuna da una singola G-orbita. Se esiste un'applicazione regolare G-equivariante biiettiva $\varphi\colon X \to Y$, allora φ è un isomorfismo.*

Dimostrazione. L'inversa $\varphi^{-1}\colon Y \to X$ è definita come applicazione fra insiemi, dobbiamo solo dimostrare che è regolare. Sia $Y' \subseteq Y$ un aperto non vuoto affine denso, sia $X' \subseteq X$ un aperto non vuoto affine denso contenuto in $\varphi^{-1}(Y')$, e consideriamo l'applicazione $\psi = \varphi|_{X'}\colon X' \to Y'$. L'immagine $\psi(X')$ contiene un aperto denso V di Y', e poniamo $U = \psi^{-1}(V)$. Visto che ψ è iniettiva, induce una biiezione fra U e V. Osserviamo che U e V sono anche aperti densi in X e Y rispettivamente.

Grazie al Corollario A.34 sappiamo che ψ (e quindi anche φ) è un isomorfismo, se ristretta ad aperti densi $U' \subseteq X$ e $V' \subseteq Y$. Grazie alla G-equivarianza di φ, concludiamo che φ è un isomorfismo anche se ristretta a $g \cdot U' \to g \cdot V'$ per $g \in G$. D'altronde al variare di $g \in G$ questi aperti ricoprono rispettivamente X e Y, per cui φ^{-1} è l'incollamento di applicazioni regolari definite su ricoprimenti aperti del dominio Y e del codominio X. Segue che φ^{-1} è regolare. $\square$

Esempio 11.10. Nel lemma, l'ipotesi che X e Y siano G-varietà è assolutamente necessaria. È facile infatti fare esempi di applicazioni regolari biiettive che non sono isomorfismi. Ad esempio si può prendere $X = \mathbb{C}$ e Y la curva in $\mathbb{C}^2$ di equazione $x^2 = y^3$, e $\varphi\colon X \to Y$ l'applicazione $t \mapsto (t^3, t^2)$. È ovviamente biiettiva, però $\varphi^*(\mathcal{O}(Y))$ è la sottoalgebra propria $\mathbb{C}[t^2, t^3]$ di $\mathcal{O}(X) = \mathbb{C}[t]$, quindi φ non può essere un isomorfismo.

Dimostrazione del Teorema 11.8. L'unicità è evidente dalla G-equivarianza, perché gH dev'essere per forza mandato in $g \cdot z$. Dimostriamo allora l'esistenza, cioè dimostriamo che $\psi\colon gH \mapsto g \cdot z$ è un'applicazione regolare.

Consideriamo l'applicazione $\varphi\colon G \to Z$ data da $g \mapsto g \cdot z$. La sua immagine W è una G-orbita, quindi è localmente chiusa in Z ed è una varietà quasi proiettiva. Sia ora $\Phi\colon G \to G/H \times W$ l'applicazione $\Phi = \pi \times \varphi$. Anche la sua immagine D è una G-orbita, e precisamente del punto (eH, z), che ovviamente ha stabilizzatore esattamente H.

La proiezione sul primo fattore $\eta\colon D \to G/H$ è un'applicazione regolare e G-equivariante fra due G-varietà quasi proiettive, ciascuna costituita da una singola G-orbita, ed è una biiezione perché lo stabilizzatore di $(eH, z) \in D$ è lo stesso di $eH \in G/H$. Dal Lemma 11.9 concludiamo che η è un isomorfismo. A questo punto basta osservare che ψ è data dalla composizione della seconda proiezione $D \to W$ con $\eta^{-1}\colon G/H \to D$. $\square$

Naturalmente i teoremi visti qui si applicano anche al caso in cui H è linearmente riduttivo, e agisce su G per traslazione a destra. Quanto visto nelle Sezioni 8 e 9 ci assicurano il risultato seguente.

Proposizione 11.11. *Siano G e H come nel Teorema 11.8, e supponiamo che H sia linearmente riduttivo. Allora G/H è una varietà affine.*

Dimostrazione. Per il Corollario 8.13, esiste il quoziente categorico nell'ambito delle varietà affini. Inoltre le fibre del quoziente $\pi\colon G \to G/\!/H$ sono esattamente le classi laterali di H, perché sono le H-orbite e sono tutte chiuse in G. Cioè $G/\!/H$ è a tutti gli effetti una struttura di varietà affine sull'insieme G/H.

Per non confonderci, continuiamo però ad usare la notazione $G/\!/H$ per questa varietà affine, e usiamo la notazione del quoziente G/H assumendo per esso una struttura di varietà quasi proiettiva come nell'enunciato del Teorema 11.8. Per il Teorema 11.8, esiste un'applicazione regolare G-equivariante $G/H \to G/\!/H$, ed è biiettiva, per cui è un isomorfismo per il Lemma 11.9. $\square$

Se H è un sottogruppo normale, allora G/H è naturalmente un gruppo, ed una varietà quasi proiettiva per il Teorema 11.6. Queste due strutture sono compatibili, cioè G/H è anche un gruppo algebrico lineare. In particolare, è una varietà affine.

Dimostrare questo fatto partendo dalla costruzione del Corollario 11.3 necessiterebbe degli stessi strumenti citati prima, quindi non lo faremo.

Diamo anche qui allora un enunciato più debole.

Teorema 11.12. *Sia G un gruppo algebrico lineare, e H un sottogruppo chiuso normale. Allora esiste un gruppo algebrico lineare K e un omomorfismo regolare suriettivo di gruppi $G \to K$ con nucleo H.*

Dimostrazione. Per il Teorema 11.2, esiste un G-modulo regolare V ed una rappresentazione $\varphi\colon G \to \mathrm{GL}(V)$ tale che H è lo stabilizzatore di una retta $U \subseteq V$. Cioè ogni $h \in H$ agisce su U come la moltiplicazione per uno scalare $\chi(h)$, e come nella dimostrazione del Lemma 6.9, abbiamo che $\chi\colon H \to \mathbb{C}$ è una funzione regolare. Inoltre non è mai nulla ed è moltiplicativa, semplicemente perché il prodotto in H si trasforma (essendo un'azione) nel prodotto dei valori di χ. Cioè $\chi\colon H \to \mathbb{C}^*$ è un omomorfismo regolare fra gruppi algebrici lineari, cosa che prende il nome di *carattere* di H.

Consideriamo ora un carattere qualsiasi $\mu\colon H \to \mathbb{C}^*$, e consideriamo l'autospazio simultaneo di tutti gli elementi di H che agiscono su V, di autovalore dato da μ, cioè il sottospazio vettoriale

$$V_\mu = \{v \in V \mid h \cdot v = \mu(h)v\}.$$

Usando che H è normale, si dimostra immediatamente che ogni elemento di $\varphi(G)$ manda ogni V_μ in un altro $V_{\mu'}$ (dove μ' dipende ovviamente dall'elemento di $\varphi(G)$), quindi la somma W di tutti i V_μ (che è diretta, come si vede facilmente) è un G-sottomodulo. Contiene U, per cui possiamo assumere direttamente che $V = W$, cioè che V è somma diretta dei V_μ per ogni μ. Osserviamo che in generale H può avere un numero infinito di caratteri diversi, e ovviamente i sottospazi V_μ saranno tutti lo spazio vettoriale nullo, tranne che per un numero finito di caratteri di H.

Facciamo ora agire G, invece che su V, su $E = \mathrm{End}(V)$, ponendo che $g \in G$ agisce su $A \in \mathrm{End}(V)$ per coniugio tramite $\varphi(g)$:

$$g \cdot A = \varphi(g)A\varphi(g)^{-1}.$$

È un'azione lineare, denotiamola con $\psi\colon G \to \mathrm{GL}(E)$. Sia $F \subseteq E$ il sottospazio vettoriale degli endomorfismi che stabilizzano ogni V_μ; se fissiamo una base di ogni V_μ e le mettiamo tutte insieme per formare una base di E, allora le matrici in F sono a blocchi sulla diagonale, ciascun blocco corrispondente a un V_μ.

Dimostriamo ora che G, agendo su E, stabilizza il sottospazio F. Sia $A \in F$, e controlliamo se $A' = g \cdot A$ è in F per ogni $g \in G$. Cioè dobbiamo controllare che $A'V_\mu \subseteq V_\mu$ per ogni carattere μ di H. Abbiamo

$$A'V_\mu = \varphi(g)A\underbrace{\varphi(g)^{-1}V_\mu}_{=V_{\mu'}} = \varphi(g)\underbrace{AV_{\mu'}}_{\subseteq V_{\mu'}} \subseteq \varphi(g)V_{\mu'} = V_\mu$$

quindi effettivamente G stabilizza F. Restringiamo allora l'azione da E ad F, ottenendo $\eta\colon G \to \mathrm{GL}(F)$. L'immagine K di η è un sottogruppo chiuso di $\mathrm{GL}(F)$: controlliamo che il nucleo di η sia proprio H.

Se $h \in H$, allora $\varphi(h)$ agisce come la moltiplicazione per uno scalare su ogni V_μ; d'altronde ogni endomorfismo in F è fatto a blocchi come spiegato prima, e coniugare ciascun blocco per la matrice scalare proveniente dall'azione di h su ciascun V_μ lascia fissato l'endomorfismo di partenza. Quindi H agisce banalmente su F.

Sia ora $g \in \mathrm{Ker}(\eta)$, cioè supponiamo che g agisca banalmente su F, cioè $\varphi(g)$ commuta con tutti gli endomorfismi in F. Allora intanto dimostriamo che $\varphi(g)$ stabilizza ciascun V_μ. Scegliamo un carattere qualsiasi μ di H, e definiamo un elemento $A \in F$ che è l'identità su V_μ, ed è l'endomorfismo nullo su tutti gli altri $V_{\mu'}$. Allora

$$V_\mu = AV_\mu = (g \cdot A)V_\mu = \varphi(g)A\varphi(g)^{-1}V_\mu = \varphi(g)AV_{\mu'} \subseteq \begin{cases} V_\mu & \text{se } \varphi(g)^{-1}V_\mu = V_\mu = \varphi(g)V_\mu \\ 0 & \text{altrimenti.} \end{cases}$$

Quindi effettivamente $\varphi(g)$ stabilizza ogni V_μ. D'altronde $\varphi(g)$ deve commutare con tutti gli endomorfismi di ciascun V_μ (i "blocchi" di prima), ma solo i multipli dell'identità di V_μ hanno questa proprietà. Segue che $\varphi(g)$ agisce come la moltiplicazione per uno scalare su ciascun V_μ.

Infine, osserviamo che V_χ, dove χ è come all'inizio della dimostrazione, contiene il sottospazio U. Ne consegue che $\varphi(g)$ agisce come la moltiplicazione per uno scalare su U, cioè stabilizza U. E allora $g \in H$, per le proprietà di U. Abbiamo dimostrato dunque che il nucleo di η è proprio H. $\square$

Il teorema permette dunque di considerare G/H come un gruppo algebrico lineare, identificandolo con K. Come abbiamo detto, non dimostriamo che questo è davvero "l'unico modo" di dotare G/H di struttura di gruppo algebrico lineare. Tuttavia il nostro teorema si può usare insieme al Teorema 11.8 in moltissime applicazioni.

Osservazione 11.13. Se assumiamo che anche G sia linearmente riduttivo, vale anche il viceversa della Proposizione 11.11 (cioè: se G è linearmente riduttivo e G/H è affine, allora anche H è linearmente riduttivo), cosa che non dimostriamo. L'equivalenza prende il nome di *Criterio di Matsushima*. Mettendo insieme questo e il Teorema 11.12, si conclude che ogni sottogruppo normale di un gruppo linearmente riduttivo è linearmente riduttivo.

Esempio 11.14. Grazie al teorema, possiamo concludere che $\mathrm{PGL}(n)$ è un gruppo algebrico lineare, dove $\mathrm{PGL}(n)$ è il quoziente di $\mathrm{GL}(n)$ per il suo centro $Z(\mathrm{GL}(n))$, cioè le matrici scalari invertibili. Si può realizzare $\mathrm{PGL}(n)$ in modo semplice, come immagine in $\mathrm{GL}(M_n) = \mathrm{GL}(n^2)$ della rappresentazione di $\mathrm{GL}(n)$ su M_n per coniugio. Infatti, intanto l'immagine è un sottogruppo chiuso di $\mathrm{GL}(n^2)$ per la Proposizione 9.3. Inoltre il nucleo della rappresentazione è fatto dalle matrici di $\mathrm{GL}(n)$ che commutano con tutte le matrici $n \times n$, quindi è proprio $Z(\mathrm{GL}(n))$. Lo stesso si applica ai gruppi $\mathrm{PSO}(n, \mathbb{C})$, $\mathrm{PSp}(n, \mathbb{C})$, definiti analogamente come il quoziente dei rispettivi $\mathrm{SO}(n, \mathbb{C})$, $\mathrm{Sp}(n, \mathbb{C})$ per la loro intersezione con $Z(\mathrm{GL}(n))$ (si può dimostrare che queste intersezioni sono proprio il centro dei rispettivi gruppi).

12. Algebre associative

In questa sezione ci spostiamo su un argomento di teoria delle rappresentazioni, di natura più algebrica: le rappresentazioni di algebre associative. Si tratta di un argomento fondamentale, e ne vedremo anche qualche applicazione ai gruppi algebrici.

Per comodità considereremo algebre unitarie, e come al solito tutti gli spazi vettoriali sono definiti su $\mathbb{C}$, tuttavia la teoria che vedremo si può sviluppare in modo simile in generalità molto più grande.

Definizione 12.1. Sia A un'algebra associativa unitaria (non necessariamente commutativa). Una *rappresentazione* di A è un omomorfismo di algebre $\varphi\colon A \to \mathrm{End}(V)$ tale che l'unità di A viene mandata in Id_V. Qui V è uno spazio vettoriale, che si dice in questo caso un *A-modulo*. Anche qui si usa la notazione $a \cdot v$ per $\varphi(a)(v)$, dove $a \in A$ e $v \in V$. Le nozioni di omomorfismo di A-moduli, sottomodulo, modulo irriducibile e completamente irriducibile si definiscono in modo simile a quanto visto nelle sezioni precedenti.

Osservazione 12.2.
(1) Dato un qualsiasi sottoinsieme X di un A-modulo V, l'insieme $A \cdot X = \{a \cdot x \mid a \in A, x \in X\}$ è un sottospazio vettoriale e anche un A-sottomodulo.
(2) Dato un A-modulo irriducibile V, allora ogni vettore non nullo v è *ciclico*, cioè $A \cdot v = V$. Viceversa, se $V \neq \{0\}$ e ogni vettore non nullo è ciclico, allora V è ovviamente irriducibile.

Esempio 12.3. Sia V uno spazio vettoriale, e $A = \mathrm{End}(V)$. Allora ovviamente V è un A-modulo in modo naturale, prendendo $\varphi = \mathrm{Id}_A$. Anche la somma diretta $V \oplus \ldots \oplus V$ di n copie di V è un A-modulo, con l'azione "diagonale"

$$a \cdot (v_1, \ldots, v_n) = (a \cdot v_1, \ldots, a \cdot v_n).$$

Il legame con la teoria delle rappresentazioni dei gruppi avviene tramite la costruzione seguente.

Definizione 12.4. Sia G un gruppo. Definiamo l'*algebra gruppo* $\mathbb{C}[G]$ di G come lo spazio vettoriale che ha per base G, e come prodotto la *convoluzione*, definito nel modo seguente. Dati $a, b \in \mathbb{C}[G]$, si esprimono come combinazioni lineari

$$a = \sum_{g \in G} a_g g, \qquad b = \sum_{g \in G} b_g g$$

dove i coefficienti $a_g, b_g \in \mathbb{C}$ sono tutti nulli tranne che per un numero finito di elementi $g \in G$. Allora il prodotto $ab \in \mathbb{C}[G]$ è definito come

$$ab = \sum_{g,h \in G} a_g b_h gh.$$

Osservazione 12.5.
(1) Sottolineiamo il nostro uso della notazione $\mathbb{C}[G]$ per quest'algebra, e non per l'anello delle funzioni regolari su G, laddove G è un gruppo algebrico lineare. Come nelle sezioni precedenti, quest'ultimo anello sarà denotato con $\mathcal{O}(G)$.
(2) Si dimostra immediatamente che $\mathbb{C}[G]$ così definita è un'algebra associativa unitaria, e contiene G naturalmente come sottoinsieme chiuso per moltiplicazione, vedendo ogni elemento di G come la combinazione lineare che ha 1 come coefficiente di quell'elemento, e 0 di ogni altro elemento di G.
(3) Identificando G con questo sottoinsieme di $\mathbb{C}[G]$, ogni rappresentazione di $\mathbb{C}[G]$ si restringe ad una rappresentazione di G, e viceversa ogni rappresentazione di G si estende ad una rappresentazione di $\mathbb{C}[G]$ per linearità. In questa corrispondenza, ovviamente i G-sottomoduli e i $\mathbb{C}[G]$-sottomoduli coincidono, quindi anche le nozioni di irriducibilità e di completa riducibilità coincidono.

(4) Per le rappresentazioni di qualsiasi algebra associativa unitaria valgono la Proposizione 6.5, il Corollario 6.6 e i Lemmi 6.7 e 6.8, con dimostrazioni identiche.

Lo strumento principale che useremo nelle rappresentazioni di algebre associative unitarie è il seguente.

Teorema 12.6. *(di densità di Jacobson) Sia A un'algebra associativa unitaria, e V un A-modulo irriducibile. Se $v_1, \dots, v_n \in V$ sono linearmente indipendenti, allora $A \cdot (v_1, \dots, v_n) = V \oplus \dots \oplus V$ (dove la somma ha n addendi).*

Dimostrazione. Usiamo la notazione V^n per la somma $V \oplus \dots \oplus V$ di n copie di V. Procediamo per induzione su n. Il caso $n = 1$ è ovvio, perché se v_1 è linearmente indipendente, cioè $v_1 \neq 0$, allora $A \cdot v_1$ è un sottomodulo non nullo, quindi è tutto V.

Siano allora $n \geq 1$ e $v_1, \dots, v_{n+1} \in V$ linearmente indipendenti. Dati $x_1, \dots, x_{n+1}$ elementi arbitrari di V, dobbiamo dimostrare che esiste un elemento $a \in A$ tale che $a \cdot v_i = x_i$ per ogni i. Per ipotesi induttiva, esiste $a_0 \in A$ tale che $a_0 \cdot v_i = x_i$ per ogni $i \in \{1, \dots, n\}$.

Definiamo $B = \{b \in A \mid b \cdot v_i = 0 \ \forall i \in \{1, \dots, n\}\}$. Allora l'insieme $B \cdot v_{n+1}$ è un sottospazio vettoriale di V, ed è A-stabile, perché dati $a \in A$ e $b \cdot v_{n+1}$ con $b \in B$, per ogni $i \in \{1, \dots, n\}$ abbiamo

$$(ab) \cdot v_i = a \cdot (b \cdot v_i) = a \cdot 0 = 0$$

e quindi $ab \in B$, per cui

$$a \cdot (b \cdot v_{n+1}) = (ab) \cdot v_{n+1} \in B \cdot v_{n+1}.$$

Per l'irriducibilità di V, allora $B \cdot v_{n+1} = \{0\}$ oppure V. Nel secondo caso abbiamo $x_{n+1} - a_0 \cdot v_{n+1} \in B \cdot v_{n+1}$, cioè esiste $b_0 \in B$ tale che $b_0 \cdot v_{n+1} = x_{n+1} - a_0 \cdot v_{n+1}$. Allora l'elemento $a = a_0 + b_0$ soddisfa

$$a \cdot v_i = (a_0 + b_0) \cdot v_i = a_0 \cdot v_i = x_i$$

per ogni $i \in \{1, \dots, n\}$, e

$$a \cdot v_{n+1} = (a_0 + b_0) \cdot v_{n+1} = a_0 \cdot v_{n+1} + x_{n+1} - a_0 \cdot v_{n+1} = x_{n+1}$$

quindi la dimostrazione è conclusa. Questo appunto se $B \cdot v_{n+1} = V$.

Supponiamo allora $B \cdot v_{n+1} = \{0\}$, e dimostriamo che questo porta ad un assurdo. Poniamo

$$W = A \cdot (v_1, \dots, v_{n+1})$$

e

$$U = \{(\underbrace{0, \dots, 0}_{n}, v) \mid v \in V\}.$$

Osserviamo che $(v_1, \dots, v_{n+1}) \in W$ perché l'immagine di A in $\mathrm{End}(V)$ contiene Id_V, e per ipotesi induttiva abbiamo

$$V^{n+1} = W + U.$$

Dimostriamo che la somma è diretta. Se $w \in W \cap U$, allora w è della forma $w = c \cdot (v_1, \dots, v_n, v_{n+1})$ per qualche $c \in A$, ma anche della forma $(0, \dots, 0, v)$ per qualche $v \in V$. Allora $c \cdot v_i = 0$ per ogni $i \in \{1, \dots, n\}$, e quindi $c \in B$, da cui segue $c \cdot v_{n+1} = 0$, cioè $w = 0$ e la somma $U + W$ è diretta.

Possiamo allora considerare la proiezione $P \colon V^{n+1} \to W$ lungo U. Visto che W e U sono A-sottomoduli, la proiezione P è A-equivariante. Siano $P_1, \dots, P_{n+1} \colon V^{n+1} \to V$ le sue componenti, cioè

$$P(r_1, \dots, r_{n+1}) = (P_1(r_1, \dots, r_{n+1}), \dots, P_{n+1}(r_1, \dots, r_{n+1})).$$

Visto che ciascuna P_i è lineare, possiamo scriverla a sua volta come somma delle applicazioni $P_{i,j} \colon V \to V$, che sono le restrizioni di P_i ai sottospazi di V^{n+1} del tipo $\{0\} \oplus \dots \oplus \{0\} \oplus V \oplus \{0\} \dots \oplus \{0\}$. Cioè

$$P(r_1, \dots, r_{n+1}) = \left(\sum_j P_{1,j}(r_j), \dots, \sum_j P_{n+1,j}(r_j) \right).$$

Visto che P è A-equivariante, le $P_{i,j}$ sono A-equivarianti, cioè come endomorfismi di V commutano con gli endomorfismi indotti da A. Per il Lemma di Schur, le $P_{i,j}$ sono tutti multipli scalari dell'identità: $P_{i,j} = q_{i,j} \mathrm{Id}_V$ per numeri $q_{i,j} \in \mathbb{C}$. Questo implica in particolare che, dato un qualsiasi sottospazio $Z \subseteq V$, abbiamo $P(Z^{n+1}) \subseteq Z^{n+1}$.

Siamo pronti a concludere la dimostrazione. Poniamo $Z = \mathrm{Span}\{v_1, \dots, v_{n+1}\}$, e consideriamo elementi arbitrari $w_1, \dots, w_{n+1}$ di V. Visto che $v_1, \dots, v_{n+1}$ sono linearmente indipendenti, esiste $T \in \mathrm{End}(V)$ tale che $Tv_i = w_i$ per ogni i. Denotiamo con T anche l'endomorfismo di V^n indotto da T, e calcoliamo

$$T(P(v_1, \dots, v_{n+1})) = T\left(\sum_j P_{1,j}(v_j), \dots, \sum_j P_{n+1,j}(v_j)\right) = \left(\sum_j q_{1,j}Tv_j, \dots, \sum_j q_{n+1,j}Tv_j\right) =$$

$$= \left(\sum_j q_{1,j}w_j, \dots, \sum_j q_{n+1,j}w_j\right) = P(w_1, \dots, w_{n+1}).$$

Inoltre $P(v_1, \dots, v_{n+1}) = (v_1, \dots, v_{n+1})$ e $T(v_1, \dots, v_{n+1}) = (w_1, \dots, w_{n+1})$, quindi otteniamo

$$P(w_1, \dots, w_{n+1}) = (w_1, \dots, w_{n+1})$$

cioè $(w_1, \dots, w_{n+1}) \in W$. Ma $(w_1, \dots, w_{n+1})$ è un elemento arbitrario di V^{n+1}, per cui otteniamo $W = V^{n+1}$, contraddicendo $V^{n+1} = W \oplus U$. □

Corollario 12.7. *(Teorema di Wedderburn) Sia A algebra associativa unitaria e $A \to \mathrm{End}(V)$ una rappresentazione, con V non nullo di dimensione finita. Allora φ è irriducibile se e solo se è suriettiva.*

Dimostrazione. Se φ è suriettiva è ovviamente irriducibile, dimostriamo il viceversa, quindi supponiamo che φ sia irriducibile. Sia $L \in \mathrm{End}(V)$, e si scelga una base $(v_1, \dots, v_n)$ di V. Per il teorema precedente, esiste $a \in A$ tale che $\varphi(a)v_i = Lv_i$ per ogni i, e questo implica che $\varphi(a) = L$. □

Esercizio 12.8. Dimostrare che se $n \geq 1$ allora $\mathbb{C}^n$ è una rappresentazione irriducibile di $\mathrm{O}(n)$, e $\mathbb{C}^{2n}$ è irriducibile per $\mathrm{Sp}(2n)$. Dedurre che questi due sottogruppi, rispettivamente di $\mathrm{GL}(n)$ e di $\mathrm{GL}(2n)$, generano, come algebra, tutto lo spazio delle matrici (M_n o M_{2n} a seconda dei casi).

Osservazione 12.9.
(1) Date due algebre associative unitarie A e B di dimensione finita, il loro prodotto tensoriale $A \otimes B$ ha struttura naturale di algebra associativa unitaria, con moltiplicazione definita da $(a \otimes b)(c \otimes d) = (ac) \otimes (bd)$ e unità $1_A \otimes 1_B$.
(2) Inoltre, se V è un A-modulo e W è un B-modulo, allora $V \otimes W$ ha una struttura naturale di $A \otimes B$-modulo ponendo
$$(a \otimes b) \cdot (v \otimes w) = (a \cdot v) \otimes (v \otimes w).$$
In particolare, questo definisce un omomorfismo naturale di algebre $\mathrm{End}(V) \otimes \mathrm{End}(W) \to \mathrm{End}(V \otimes W)$.
(3) Siano G e H due gruppi algebrici lineari, sia V un G-modulo, e sia W un H-modulo. Allora $G \times H$ ha la struttura naturale di gruppo algebrico lineare, e $V \otimes W$ ha una struttura naturale di $G \times H$-modulo ponendo
$$(g, h) \cdot v \otimes w = (g \cdot v) \otimes (h \cdot w).$$
È facile dimostrare che se V e W sono regolari, allora $V \otimes W$ è regolare.

Lemma 12.10. *Siano V e W spazi vettoriali di dimensione finita. Allora $\mathrm{End}(V \otimes W)$ è isomorfa a $\mathrm{End}(V) \otimes \mathrm{End}(W)$ tramite l'omomorfismo dell'Osservazione 12.9.*

Dimostrazione. Possiamo supporre che V e W siano non nulli. Grazie al Teorema 12.6, basta dimostrare che $V \otimes W$ è irriducibile come $C = \mathrm{End}(V) \otimes \mathrm{End}(W)$-modulo, infatti da questo seguirà la suriettività dell'omomorfismo, e l'iniettività allora è ovvia confrontando le dimensioni dei due spazi vettoriali. Consideriamo un qualsiasi vettore non nullo di $V \otimes W$

$$u = \sum_i v_i \otimes w_i$$

con $v_i \in V$ e $w_i \in W$ per ogni i, e dimostriamo che $C \cdot u = V \otimes W$.

Per bilinearità, possiamo assumere che i w_i siano linearmente indipendenti, e che tutti i v_i siano non nulli. Scegliamo un endomorfismo $b \in \mathrm{End}(W)$ tale che $bw_i = 0$ per ogni $i \neq 1$, e tale che $bw_1 = w_1$. Allora $c = \mathrm{Id}_V \otimes b$ manda u nel vettore

$$c \cdot u = v_1 \otimes w_1.$$

Da qui possiamo ottenere facilmente che $C \cdot u$ contiene tutti i vettori decomponibili, cioè i singoli prodotti $v \otimes w$ dove $v \in V$ e $w \in W$. Da questo segue immediatamente che $C \cdot u = V \otimes W$. $\square$

Possiamo applicare questi risultati sulle algebre associative unitare ai gruppi algebrici lineari.

Teorema 12.11. *Siano G e H gruppi algebrici lineari linearmente riduttivi. Se V e W sono rispettivamente un G-modulo e un H-modulo, entrambi irriducibili regolari, allora $V \otimes W$ è un $G \times H$-modulo irriducibile regolare, e ogni $G \times H$-modulo irriducibile regolare è di questo tipo a meno di isomorfismo.*

Dimostrazione. Se V e W sono irriducibili regolari, l'algebra gruppo $A = \mathbb{C}[G]$ (ricordiamo: non si tratta dell'anello delle funzioni regolari) viene mandata suriettivamente in $\operatorname{End}(V)$, e $B = \mathbb{C}[H]$ suriettivamente in $\operatorname{End}(W)$. Quindi l'immagine di $G \times H$ in $\operatorname{End}(V \otimes W)$ genera l'immagine di $\operatorname{End}(A) \otimes \operatorname{End}(B)$, che è tutta $\operatorname{End}(V \otimes W)$ per il lemma precedente. Questo dimostra che $V \otimes W$ è irriducibile come $G \times H$-modulo.

Viceversa, sia U un $G \times H$-modulo irriducibile. Allora è contemporaneamente un G-modulo e un H-modulo entrambi regolari, in modo naturale, identificando G col sottogruppo $G \times \{e_H\}$ di $G \times H$, e H col sottogruppo $\{e_G\} \times H$. Osserviamo che, visti in questo modo, gli elementi di G commutano con gli elementi di H nell'azione su U.

Essendo G linearmente riduttivo, U si scompone in somma diretta di G-sottomoduli irriducibili $U = \bigoplus_i V_i$. Possiamo interpretare questa decomposizione anche in modo diverso. Scegliamo $V = V_1$, e consideriamo l'insieme Z delle applicazioni lineari G-equivarianti[7] $\varphi \colon V \to U$. Si tratta di uno spazio vettoriale, ed è dotato naturalmente di una struttura di H-modulo: dati $\varphi \colon V \to U$, $h \in H$ e $v \in V$, possiamo definire $(h \cdot \varphi)(v) = h \cdot \varphi(v)$. Si verifica immediatamente che anche $h \cdot \varphi$, definita in questo modo, è un'applicazione lineare G-equivariante. Inoltre, esprimendo tutto in coordinate relativamente ad una base di $V = V_1$, una base di U, e alla base corrispondente dello spazio delle applicazioni lineari $V \to U$, si vede che Z è un H-modulo regolare, perché sia φ sia l'operazione di H su U sono espresse tramite funzioni regolari. Inoltre Z non è nullo, perché contiene almeno l'inclusione di $V = V_1$ in U, per cui possiamo scegliere un H-sottomodulo irriducibile W di Z.

Consideriamo allora $V \otimes W$ con struttura naturale di $G \times H$-modulo, e definiamo un'applicazione lineare $V \otimes W \to U$, data da $v \otimes \varphi \mapsto \varphi(v)$. Anche qui si verifica immediatamente che è ben definita ed è $G \times H$-equivariante. Inoltre la sua immagine contiene l'immagine di V tramite un qualche elemento non nullo di W, cioè contiene l'immagine di un omomorfismo non nullo $V \to U$.

Deduciamo che l'immagine di φ è tutto U, per irriducibilità. La dimostrazione è conclusa, perché φ è suriettiva e non nulla, V e W sono irriducibili per cui $V \otimes W$ è irriducibile per la prima parte della dimostrazione, e quindi φ è anche iniettiva. $\square$

Corollario 12.12. *("versione algebrica" del Teorema di Peter-Weyl) Sia G un gruppo algebrico lineare, linearmente riduttivo. Consideriamo $\mathcal{O}(G)$ come un $G \times G$-modulo, dove il primo fattore agisce per traslazione a sinistra, e il secondo per traslazione a destra. Allora esiste un isomorfismo di $G \times G$-moduli*

$$\mathcal{O}(G) \cong \bigoplus_V V^* \otimes V$$

dove V varia in un insieme di G-moduli irriducibili che contiene esattamente un elemento di ciascuna classe di isomorfismo di G-moduli irriducibili, la prima copia di G agisce solo sui fattori V^* e la seconda agisce solo sui fattori V. Ciascun addendo $V^* \otimes V$ è la componente isotipica di V per traslazione a destra, e la componente isotipica di V^* per traslazione a sinistra.

Dimostrazione. Iniziamo col definire un omomorfismo iniettivo $\iota_V \colon V^* \otimes V \to \mathcal{O}(G)$: dati $\eta \in V^*$ e $v \in V$, poniamo $\iota_V(\eta \otimes v)$ uguale alla funzione $g \mapsto \eta(g \cdot v)$. Come nella dimostrazione del Lemma 10.1, si verifica che ι_V è $G \times G$-equivariante e iniettiva. Per il teorema precedente il prodotto $V^* \otimes V$ è un $G \times G$-modulo irriducibile. Per questo va solo verificato che V^* è un G-modulo irriducibile, ma questo è ovvio perché dato un sottomodulo proprio non nullo di V^* allora l'intersezione in V dei nuclei dei suoi elementi è un sottomodulo proprio non nullo.

[7] Questo insieme si denota con $\operatorname{Hom}^G(V, U)$, o con $\operatorname{Hom}_G(V, U)$. Io preferisco $\operatorname{Hom}^G(V, U)$, perché si può interpretare come il sottospazio dei punti fissati da G che agisce sullo spazio vettoriale $\operatorname{Hom}(V, U)$ delle applicazioni lineari $V \to U$.

Grazie alla dimostrazione del Lemma 8.6, sappiamo che $\mathcal{O}(G)$ è somma diretta di irriducibili per entrambe le azioni di G considerate, quindi rimane solo da dimostrare l'ultima affermazione del corollario; essa implicherà anche la decomposizione voluta in somma diretta di $\mathcal{O}(G)$.

Dimostriamo l'ultima affermazione per l'azione di traslazione a destra, per l'altra l'argomento è lo stesso. Prima di tutto osserviamo che, se esiste un isomorfismo di G-moduli irriducibili $\varphi\colon V \to U$, allora l'immagine di ι_V è uguale all'immagine di ι_U. Infatti φ induce l'isomorfismo di spazi vettoriali $\varphi^*\colon U^* \to V^*$ dato da $\varphi^*(\eta)(v) = \eta(\varphi(v))$ per ogni $v \in V$. Allora

$$\varphi^*(\eta)(g \cdot v) = \eta(\varphi(g \cdot v)) = \eta(g \cdot \varphi(v))$$

e basta osservare che $\varphi(v)$ varia in tutto U se v varia in tutto V, e che $\varphi^*(\eta)$ varia in tutto V^* se η varia in tutto U^*. Sia dunque U un sottomodulo irriducibile di $\mathcal{O}(G)$, e mostriamo che U è nell'immagine di ι_U. Basta definire l'elemento $\eta \in U^*$ dato da

$$u \mapsto \eta(u) = u(e_G)$$

e osservare che l'elemento $\iota(\eta \otimes u)$ è la funzione

$$g \mapsto \eta(g \cdot u) = g \cdot u(e_G) = u(e_G g) = u(g)$$

cioè $\iota(\eta \otimes u)$ coincide con l'elemento u di $\mathcal{O}(G)$. $\square$

Esempio 12.13. Sia $G = \mathbb{C}^*$, allora la decomposizione

$$\mathcal{O}(G) = \mathbb{C}[t, t^{-1}] = \bigoplus_{n \in \mathbb{Z}} \mathbb{C}t^n$$

è la stessa del teorema. Dato $n \in \mathbb{Z}$, un elemento $z \in G$ agisce infatti per moltiplicazione a sinistra su $\mathbb{C}t^n$ come il prodotto per z^{-n}, e per moltiplicazione a destra come il prodotto per z^n. Possiamo allora considerare l'addendo $\mathbb{C}t^n$ come $\mathbb{C}_n^* \otimes \mathbb{C}_n$, dove $\mathbb{C}_n$ è il G-modulo di dimensione 1 dove $z \in G$ agisce come il prodotto per z^n.

Osservazione 12.14. Il teorema implica anche che l'insieme delle classi di isomorfismo di G-moduli è un insieme al più numerabile, se G è linearmente riduttivo, e che questo insieme è finito, se G è finito.

Anche se il teorema vale solo per G linearmente riduttivo, l'omomorfismo iniettivo di $G \times G$-moduli $\iota_V\colon V^* \otimes V \to \mathcal{O}(G)$ è definito per ogni gruppo algebrico lineare G e ogni G-modulo regolare V. Se $G \subseteq \mathrm{GL}(n)$ e $V = \mathbb{C}^n$ con l'azione usuale, allora l'immagine di ι_V contiene tutte le entrate della matrice $g \in G$, considerate come funzioni su G (in realtà, contiene le entrate di g anche come matrice rispetto a qualsiasi altra base di V). Questo motiva la seguente definizione.

Definizione 12.15. Dato G gruppo algebrico lineare e V un G-modulo regolare, gli elementi nell'immagine di ι_V si chiamano *coefficienti matriciali.*

Corollario 12.16. *Siano G ed H due gruppi algebrici lineari, linearmente riduttivi. Allora $G \times H$ è un gruppo algebrico linearmente riduttivo.*

Dimostrazione. Il corollario deriva dal corollario precedente, basta osservare che, come $G \times H$-moduli per traslazione a destra, abbiamo gli isomorfismi

$$\mathcal{O}(G \times H) \cong \mathcal{O}(G) \otimes \mathcal{O}(H) \cong \bigoplus_{V,U} (V^* \otimes V) \otimes (U^* \otimes V) \cong$$

$$\cong \bigoplus_{V,U} (V^* \otimes U^*) \otimes (U \otimes V)$$

dove V varia fra i G-moduli irriducibili (uno per ogni classe di isomorfismo) e U varia fra gli H-moduli irriducibili (uno per ogni classe di isomorfismo), e dove $G \times H$ agisce solo sui fattori $U \otimes V$ di ogni addendo. Quindi $\mathcal{O}(G \times H)$ è un $G \times H$-modulo completamente riducibile, e allora ogni $G \times H$-modulo regolare è completamente riducibile grazie al Lemma 10.1. $\square$

13. Doppio centralizzatore

In questa sezione riportiamo un teorema utilissimo nella teoria classica degli invarianti, ma non lo vedremo a lezione e non farà parte del programma.

Sia V uno spazio vettoriale, e $A \subseteq \mathrm{End}(V)$ un sottoinsieme. Definiamo

$$\mathrm{Comm}(A) = \{x \in \mathrm{End}(V) \mid xa = ax \ \forall a \in A\}.$$

Teorema 13.1. *(Teorema del doppio centralizzatore) Sia V uno spazio vettoriale di dimensione finita, sia A una sottoalgebra associativa unitaria di* $\mathrm{End}(V)$ *(con identità* Id_V*), e poniamo $B = \mathrm{Comm}(A)$. Se V è completamente riducibile come A-modulo, allora* $\mathrm{Comm}(B) = A$.

Dimostrazione. Per costruzione vale $A \subseteq \mathrm{Comm}(B)$, dimostriamo l'altra inclusione. Sia $(v_1, \ldots, v_n)$ una base di V, e sia $T \in \mathrm{Comm}(B)$ qualsiasi. Il teorema seguirà se troviamo $a \in A$ tale che $a(v_i) = T(v_i)$ per ogni i. Consideriamo $w = (v_1, \ldots, v_n)$ nella somma diretta $W = V \oplus \ldots \oplus$ di n copie di V. Anche W è completamente riducibile, quindi l'A-sottomodulo $M = A \cdot w$ ha un complemento A-stabile, e possiamo considerare la proiezione $P \colon W \to M$ lungo questo complemento.

Visto che P è lineare, possiamo scriverla come

$$P(u_1, \ldots, u_n) = \sum_{i,j=1}^{n} P_{i,j}(u_j)$$

dove $P_{i,j} \colon V \to V$ è definita come nel Teorema 12.6, cioè $P_{i,j}(v)$ è la i-esima componente dell'elemento $P(0, \ldots, 0, v, 0, \ldots, 0) \in V \oplus \ldots \oplus V$, dove v compare al j-esimo posto.

Visto che P è A-equivariante, abbiamo che ogni $P_{i,j}$ commuta con A, cioè ogni $P_{i,j}$ è in B. Segue anche che T commuta con ogni $P_{i,j}$. Chiamiamo di nuovo T l'endomorfismo "diagonale" di W indotto da T: visto che $T \in \mathrm{End}(V)$ commuta con $P_{i,j}$, allora $T \in \mathrm{End}(W)$ commuta con P. Inoltre $w \in M$, perché $\mathrm{Id}_V \in A$. Segue

$$P(T(v_1), \ldots, T(v_n)) = T(P(v_1, \ldots, v_n)) = T(P(w)) = T(w) = (T(v_1), \ldots, T(v_n)).$$

Ma l'immagine di P è contenuta in M, quindi $(T(v_1), \ldots, T(v_n)) \in M$. Per definizione di M, esiste $a \in A$ tale che

$$(a(v_1), \ldots, a(v_n)) = (T(v_1), \ldots, T(v_n))$$

cioè $T = a$, e la dimostrazione è conclusa. □

14. L'algebra di Lie di un gruppo algebrico lineare

Sia $G \subseteq \mathrm{GL}(n)$ un gruppo algebrico lineare. Facciamo qualche considerazione sulla geometria di G, non essenziali per il seguito ma utili intuitivamente.

Consideriamo come sottoinsieme dello spazio vettoriale *reale* $M_n(\mathbb{C})$, di dimensione $2n^2$ su $\mathbb{R}$. Visto che è definito da equazioni polinomiali, mettiamo $f_1 = \ldots = f_m = 0$ (sono equazioni globali, ma le consideriamo solo sulle matrici a determinante non nullo), prendendo separatamente la parte reale e la parte immaginaria di ogni equazione vediamo che G è definito da equazioni polinomiali *reali* in $M_n(\mathbb{C}) \cong \mathbb{R}^{2n^2}$. Dal teorema della funzione implicita, esiste un aperto U di G *in topologia euclidea* tale che U è una sottovarietà differenziabile (localmente chiusa) di $\mathbb{R}^{2n^2}$.

Un tale aperto è dato ad esempio guardando la matrice Jacobiana corrispondente alle equazioni di G, e prendendo come U l'insieme dei punti $g \in G$ dove questa matrice ha rango massimo (fra i ranghi assunti per ogni $g \in G$).

D'altronde G agisce su se stesso in modo transitivo con la moltiplicazione (ad es. a sinistra), e ogni $g \in G$ induce la biiezione $G \to G$ data appunto da $x \mapsto gx$. Questa biiezione si estende a un isomorfismo lineare $\mathbb{R}^{2n^2} \to \mathbb{R}^{2n^2}$, dato dalla stessa formula $x \mapsto gx$ se interpretato come isomorfismo $M_n(\mathbb{C}) \to M_n(\mathbb{C})$. Dal punto di vista della geometria differenziale si tratta di un diffeomorfismo $\mathbb{R}^{2n^2} \to \mathbb{R}^{2n^2}$ che stabilizza G.

Da questo segue che le proprietà topologiche locali di G come sottoinsieme di $\mathbb{R}^{2n^2}$ sono le stesse in tutti i punti di G, e quindi in realtà tutto G è una sottovarietà differenziabile localmente chiusa di $\mathbb{R}^{2n^2}$.

Lo stesso argomento, usando il teorema della funzione implicita per funzioni olomorfe di più variabili complesse, assicura che G è una sottovarietà complessa di $M_n(\mathbb{C}) \cong \mathbb{C}^{n^2}$. Si dice allora che

G è una varietà algebrica *liscia*, in contrapposizione ad esempi quali l'insieme di equazione $xy = 0$ in $\mathbb{C}^2$, insieme che è una varietà affine ma non è una sottovarietà differenziabile di $\mathbb{C}^2 \cong \mathbb{R}^4$.

Vedremo ora costruzioni che coinvolgono gli spazi tangenti a G nei suoi punti. Le considerazioni fatte finora assicurano che tutto funziona anche intuitivamente come in geometria differenziale, visto che G è appunto una varietà differenziabile (sia reale sia complessa). In realtà formalmente quello che faremo vale anche se non avessimo osservato questo fatto: si potrebbe semplicemente prendere alla lettera le definizioni date e dimenticarsi che corrispondono intuitivamente a vettori tangenti, campi vettoriali, e così via.

Sia $\mathsf{x} \in M_n(\mathbb{C})$. Possiamo interpretare x come un vettore nello spazio tangente $T_{I_n}\,\mathrm{GL}(n)$ a $\mathrm{GL}(n)$ nell'identità I_n, identificandolo con l'applicazione "derivata direzionale" $\frac{\partial}{\partial \mathsf{x}}(I_n)$, cioè

$$\begin{array}{rccc} \frac{\partial}{\partial \mathsf{x}}(I_n)\colon & \mathcal{O}(\mathrm{GL}(n)) & \to & \mathbb{C} \\ & f & \mapsto & \frac{\partial f}{\partial \mathsf{x}}(I_n) \end{array}$$

Come in geometria differenziale, è facile dimostrare che al variare di $\mathsf{x} \in M_n(\mathbb{C})$ si ottengono in questo modo tutte le derivazioni $\mathcal{O}(\mathrm{GL}(n)) \to \mathbb{C}$ "nell'identità I_n", cioè tutte le applicazioni lineari $\delta\colon \mathcal{O}(\mathrm{GL}(n)) \to \mathbb{C}$ tali che $\delta(f_1 f_2) = \delta(f_1) f_2(I_n) + f_1(I_n)\delta(f_2)$. Infatti, da una tale δ si risale al vettore x calcolando δ sulle funzioni coordinate $x_{i,j}$, e mettendo questi valori come le coordinate di x. Con questa scelta è immediato poi verificare che $\delta = \frac{\partial}{\partial \mathsf{x}}(I_n)$, osservando che queste due derivazioni coincidono sulle funzioni coordinate, e quindi su tutti i polinomi e le funzioni razionali in esse.

Dato un gruppo algebrico lineare $G \subseteq \mathrm{GL}(n)$, si possono interpretare allo stesso modo le applicazioni $\mathcal{O}(G) \to \mathbb{C}$ con le stesse proprietà di prima come i vettori tangenti a G nell'identità I_n. È in modo naturale un sottospazio di M_n, dato dai vettori $\mathsf{x} \in M_n$ tali che $\frac{\partial f}{\partial \mathsf{x}}(I_n) = 0$ per ogni $f \in I = I_{\mathrm{GL}(n)}(G)$.

Infatti, dato un tale vettore, la derivata direzionale $\frac{\partial}{\partial \mathsf{x}}(I_n)$ passa al quoziente per I, inducendo una derivazione $\mathcal{O}(G) \to \mathbb{C}$. Viceversa, data una derivazione $\delta\colon \mathcal{O}(G) \to \mathbb{C}$, la possiamo sollevare ad una derivazione $\widetilde{\delta}\colon \mathcal{O}(\mathrm{GL}(n)) \to \mathbb{C}$ imponendo che $\widetilde{\delta}(f) = \delta(f + I)$.

La stessa costruzione si applica anche in qualsiasi punto $g \in G$; ad un vettore x nello spazio tangente a G in g corrisponde la derivazione $\frac{\partial}{\partial \mathsf{x}}(g)$.

Sempre come in geometria differenziale, esiste una versione globale di questa costruzione. Si considerano derivazioni $\mathcal{O}(G) \to \mathcal{O}(G)$, cioè applicazioni lineari che soddisfano $\delta(f_1 f_2) = \delta(f_1) f_2 + f_1 \delta(f_2)$ per ogni $f_1, f_2 \in \mathcal{O}(G)$. Queste corrispondono ai campi di vettori tangenti su G: ad una tale δ si associa il campo vettoriale che su $g \in G$ è dato dal vettore tangente la cui derivazione $\mathcal{O}(G) \to \mathbb{C}$ è $f \mapsto \delta(f)(g)$.

Definizione 14.1. Sia $G \subseteq \mathrm{GL}(n)$ un gruppo algebrico lineare. Si definisce l'*algebra di Lie* di G, in simboli $\mathrm{Lie}(G)$ oppure $\mathfrak{g}$, come lo spazio vettoriale delle derivazioni dell'algebra $\mathcal{O}(G)$ invarianti per traslazione a sinistra, cioè l'insieme delle applicazioni lineari $\delta\colon \mathcal{O}(G) \to \mathcal{O}(G)$ tali che $\delta(f_1 f_2) = \delta(f_1) f_2 + f_1 \delta(f_2)$ per ogni $f_1, f_2 \in \mathcal{O}(G)$, e tali che $\delta(g \cdot f) = g \cdot (\delta(f))$ per ogni $g \in G$ e ogni $f \in \mathcal{O}(G)$ (dove G agisce su $\mathcal{O}(G)$ per traslazione a sinistra).

Osservazione 14.2. Siano $\delta_1, \delta_2 \in \mathrm{Lie}(G)$. Allora $[\delta_1, \delta_2] = \delta_1 \circ \delta_2 - \delta_2 \circ \delta_1$, che in linea di principio è semplicemente un'applicazione lineare $\mathcal{O}(G) \to \mathcal{O}(G)$, è anche un elemento di $\mathrm{Lie}(G)$, come si ottiene facilmente con una verifica diretta. Questo rende $\mathrm{Lie}(G)$ un'*algebra di Lie* in senso astratto, che è definita in generale come uno spazio vettoriale L dotato di un'applicazione bilineare antisimmetrica $[-,-]\colon L \times L \to L$ chiamata *bracket (di Lie)* che soddisfa l'*identità di Jacobi* $[\mathsf{x}, [\mathsf{y}, \mathsf{z}]] + [\mathsf{y}, [\mathsf{z}, \mathsf{x}]] + [\mathsf{z}, [\mathsf{x}, \mathsf{y}]] = 0$ per ogni $\mathsf{x}, \mathsf{y}, \mathsf{z} \in L$. Anche se un'algebra di Lie in generale non è un'algebra associativa (rispetto al bracket), le definizioni di *sottoalgebra di Lie* e di *omomorfismo di algebre di Lie* si possono dare in modo ovvio.

Sia $\delta \in \mathrm{Lie}(G)$, e consideriamo l'applicazione lineare $\mathcal{O}(G) \to \mathbb{C}$ data da $f \mapsto \delta(f)(I_n)$, cioè prendiamo il vettore, fra quelli del campo vettoriale, che è tangente a I_n. Questo definisce un'applicazione lineare $\varepsilon\colon \mathrm{Lie}(G) \to T_{I_n}(G)$. Interpretiamo di nuovo gli elementi di $T_{I_n}(G)$ come vettori in M_n, vedendo $\mathsf{x} \in M_n$ come $\frac{\partial}{\partial \mathsf{x}}(I_n)$. Osserviamo che M_n ha una struttura naturale di algebra di Lie, data da $[\mathsf{x}, \mathsf{y}] = \mathsf{xy} - \mathsf{yx}$ per ogni $\mathsf{x}, \mathsf{y} \in M_n$.

Proposizione 14.3. *L'applicazione lineare* $\varepsilon\colon \mathrm{Lie}(G) \to T_{I_n}(G)$ *è un isomorfismo di spazi vettoriali, e vale* $\varepsilon([\delta_1, \delta_2]) = [\varepsilon(\delta_1), \varepsilon(\delta_2)]$ *per ogni* $\delta_1, \delta_2 \in \mathrm{Lie}(G)$. *Di conseguenza,* $T_{I_n}(G)$ *è una sottoalgebra di Lie di* M_n, *ed* ε *è un isomorfismo di algebre di Lie.*

Dimostrazione. Dimostriamo prima di tutto che ε è un isomorfismo di spazi vettoriali, definendo esplicitamente l'inversa $\mathsf{x} \mapsto *\mathsf{x}$, dove $*\mathsf{x}\colon \mathcal{O}(G) \mapsto \mathcal{O}(G)$ manda $f \in \mathcal{O}(G)$ nella funzione $f * \mathsf{x}$, che è definita da

$$(f * \mathsf{x})\colon g \mapsto \frac{\partial(g^{-1} \cdot f)}{\partial \mathsf{x}}(I_n)$$

dove l'azione di g^{-1} su f è per traslazione a sinistra. Si verifica facilmente che $*\mathsf{x}$ è ben definita, è una derivazione invariante a sinistra[8], e che $\mathsf{x} \mapsto *\mathsf{x}$ è l'inversa di ε. Ad esempio, data $\delta \in \mathrm{Lie}(G)$, calcoliamo $*\varepsilon(\delta)$ su una funzione $f \in \mathcal{O}(G)$: è la funzione $f * \varepsilon(\delta)$ che su $g \in G$ vale

$$\frac{\partial(g^{-1} \cdot f)}{\partial \mathsf{x}}(I_n) = \dots$$

dove x è il vettore tale che $\frac{\partial F}{\partial \mathsf{x}} = \delta(F)(I_n)$ per ogni $F \in \mathcal{O}(G)$. Quindi

$$\dots = \delta(g^{-1} \cdot f)(I_n) = (g^{-1} \cdot \delta(f))(I_n) = \delta(f)(g).$$

In altre parole, $f * \varepsilon(\delta)$ è la funzione $g \mapsto \delta(f)(g)$, cioè la funzione $\delta(f)$, come richiesto. Le altre verifiche sono simili.

Dimostriamo ora che $\varepsilon([\delta_1, \delta_2]) = [\varepsilon(\delta_1), \varepsilon(\delta_2)]$ per ogni $\delta_1, \delta_2 \in \mathrm{Lie}(G)$. È equivalente dimostrare che $[*\mathsf{x}, *\mathsf{y}] = *[\mathsf{x}, \mathsf{y}]$ per ogni $\mathsf{x}, \mathsf{y} \in T_{I_n}(G)$, però perché questo abbia senso bisogna anche verificare che $[\mathsf{x}, \mathsf{y}] \in T_{I_n}(G)$. Data una funzione f, calcoliamo intanto $[*\mathsf{x}, *\mathsf{y}] = (*\mathsf{x}) \circ (*\mathsf{y}) - (*\mathsf{y}) \circ (*\mathsf{x})$ su f, cioè $(f * \mathsf{y}) * \mathsf{x} - (f * \mathsf{x}) * \mathsf{y}$.

Per questo è conveniente considerare per un po' funzioni in $\mathcal{O}(\mathrm{GL}(n))$ invece che in $\mathcal{O}(G)$: la formula data per $*\mathsf{x}$ vale anche in questo ambito e fornisce una derivazione $\mathcal{O}(\mathrm{GL}(n)) \to \mathcal{O}(\mathrm{GL}(n))$. Inoltre prendiamo prima di tutto f uguale alla funzione $x_{i,j}$ che è l'entrata al posto (i,j) delle matrici. Allora abbiamo

$$(g^{-1} \cdot x_{i,j})(h) = x_{i,j}(gh) = \sum_k x_{i,k}(g) x_{k,j}(h)$$

per ogni $g, h \in \mathrm{GL}(n)$. Considerando nell'espressione qui sopra g come fissato e h come la variabile, segue

$$x_{i,j} * \mathsf{y}\colon g \mapsto \sum_k x_{i,k}(g) \frac{\partial x_{k,j}}{\partial \mathsf{y}}(I_n) = \dots$$

Scriviamo $\mathsf{y}_{i,j}$ le componenti di y, ed esplicitiamo la derivata direzionale qui sopra:

$$\frac{\partial x_{k,j}}{\partial \mathsf{y}} = \sum_{r,s} \frac{\partial x_{k,j}}{\partial x_{r,s}} \mathsf{y}_{r,s} = \mathsf{y}_{k,j},$$

da cui deduciamo

$$\dots = \sum_k x_{i,k}(g) \mathsf{y}_{k,j}.$$

Possiamo riscrivere quanto ottenuto come

$$x_{i,j} * \mathsf{y} = \sum_k x_{i,k} \mathsf{y}_{k,j}.$$

Usando ripetutamente questa formula otteniamo

$$(x_{i,j} * \mathsf{y}) * \mathsf{x} = \sum_k \left(\sum_r x_{i,r} \mathsf{x}_{r,k} \right) \mathsf{y}_{k,j} = \sum_r x_{i,r} \left(\sum_k \mathsf{x}_{r,k} \mathsf{y}_{k,j} \right)$$

e anche

$$(x_{i,j} * \mathsf{y}) * \mathsf{x} - (x_{i,j} * \mathsf{x}) * \mathsf{y} = \sum_r x_{i,r} \left(\sum_k \mathsf{x}_{r,k} \mathsf{y}_{k,j} - \mathsf{y}_{r,k} \mathsf{x}_{k,j} \right) = x_{i,j} * [\mathsf{x}, \mathsf{y}].$$

Da questo deduciamo che $[*\mathsf{x}, *\mathsf{y}]$ e $*[\mathsf{x}, \mathsf{y}]$ coincidono su ogni $f \in \mathcal{O}(\mathrm{GL}(n))$.

Visto che x e y sono nello spazio tangente a G, segue che $*\mathsf{x}$ e $*\mathsf{y}$ stabilizzano l'ideale di G in $\mathcal{O}(\mathrm{GL}(n))$. Quindi anche $*[\mathsf{x}, \mathsf{y}]$ ha questa proprietà, e applicando ε a questa derivazione si deduce immediatamente che $[\mathsf{x}, \mathsf{y}]$ appartiene allo spazio tangente a G.

Finalmente possiamo rileggere tutti i conti qui sopra considerando stavolta le funzioni in $\mathcal{O}(G)$ invece che in $\mathcal{O}(\mathrm{GL}(n))$, e deduciamo che effettivamente $[*\mathsf{x}, *\mathsf{y}] = *[\mathsf{x}, \mathsf{y}]$ come elementi di $\mathrm{Lie}(G)$. $\square$

[8] Verifica: $((h \cdot f) * \mathsf{x})(g) = \frac{\partial(g^{-1} \cdot (h \cdot f))}{\partial \mathsf{x}}(I_n) = \frac{\partial((h^{-1}g)^{-1} \cdot f)}{\partial \mathsf{x}}(I_n) = (f * \mathsf{x})(h^{-1}g) = (h \cdot (f * \mathsf{x}))(g)$.

Esempio 14.4. (1) L'algebra di Lie di $\mathrm{GL}(n)$ è ovviamente M_n, che si denota anche con $\mathfrak{gl}(n)$.

(2) L'algebra di Lie di $\mathbb{C}^*$ è $\mathbb{C}$, l'unica (a meno di isomorfismo) algebra di Lie di dimensione 1; ha necessariamente bracket nullo: $[\mathsf{x},\mathsf{y}] = 0$ per ogni x,y. Anche l'algebra di Lie del gruppo $\mathbb{C}$, ad esempio visto in $\mathrm{GL}(2)$ nel modo solito, ha dimensione 1 con bracket nullo. Segue che gruppi non isomorfi possono avere algebre di Lie isomorfe.

(3) Per calcolare l'algebra di Lie di $\mathrm{SL}(n)$ basta trovare lo spazio tangente all'identità. Consideriamo un vettore qualsiasi $\mathsf{x} \in M_n$, visto come un vettore tangente a $\mathrm{GL}(n)$ nell'identità e quindi identificato con la derivata direzionale $\frac{\partial}{\partial \mathsf{x}}(I_n)\colon \mathcal{O}(\mathrm{GL}(n)) \to \mathbb{C}$. Adesso, il vettore x è tangente a $\mathrm{SL}(n)$ se e solo se induce una derivazione $\mathcal{O}(\mathrm{SL}(n)) \to \mathbb{C}$, cioè se e solo se $\frac{\partial}{\partial \mathsf{x}}(I_n)$ si annulla sull'ideale $I_{\mathrm{GL}(n)}(\mathrm{SL}(n))$, e questo avviene se e solo se si annulla sulla funzione $g \mapsto \det(g) - 1$.

Cambiamo ora variabile: scriviamo $g = I_n + \mathsf{x}$ dove $\mathsf{x} \in M_n$, e osserviamo che $\det(g) = \det(I_n + \mathsf{x})$ è un polinomio nelle entrate di x, il cui termine di primo grado è $\mathrm{Tr}(\mathsf{x})$. Qui $g \in \mathrm{GL}(n)$ sarebbe la nostra variabile, ma possiamo considerare anche x come la variabile, bisogna solo ricordarsi che g deve variare nell'insieme $\mathrm{GL}(n)$, e allora x deve variare in un apposito intorno aperto di 0 in M_n (ad esempio l'aperto ottenuto traslando $\mathrm{GL}(n)$ per $-I_n$).

Concludiamo che x appartiene allo spazio tangente di $\mathrm{SL}(n)$ se e solo se $\mathrm{Tr}(\mathsf{x}) = 0$. Cioè l'algebra di Lie di $\mathrm{SL}(n)$ è

$$\mathfrak{sl}(n) = \{\mathsf{x} \in M_n \mid \mathrm{Tr}(\mathsf{x}) = 0\}.$$

(4) Con considerazioni analoghe al caso di $\mathrm{SL}(n)$ si ottengono l'algebra di Lie di $\mathrm{O}(n,\mathbb{C})$, che è la stessa di $\mathrm{SO}(n,\mathbb{C})$:

$$\mathfrak{so}(n,\mathbb{C}) = \{\mathsf{x} \in M_n \mid \mathsf{x} + {}^t\mathsf{x} = 0\},$$

e l'algebra di Lie di $\mathrm{Sp}(2n,\mathbb{C})$:

$$\mathfrak{sp}(2n,\mathbb{C}) = \{\mathsf{x} \in M_n \mid \mathsf{x} \cdot J + J \cdot {}^t\mathsf{x} = 0\}.$$

La costruzione delle algebre di Lie dei gruppi algebrici lineari è compatibile con gli omomorfismi fra i gruppi, e con la teoria delle rappresentazioni. Vediamo qualche risultato in questo senso.

Sia $\varphi\colon G \to H$ un omomorfismo regolare fra gruppi algebrici lineari. Allora è definito il differenziale $d\varphi\colon T_{e_G}G \to T_{e_H}H$: dato $\mathsf{x} \in T_{e_G}$, cioè una derivazione $\mathsf{x}\colon \mathcal{O}(G) \to \mathbb{C}$, si definisce $d\varphi(\mathsf{x})$ come la derivazione $\mathcal{O}(H) \to \mathbb{C}$ che a una funzione $f \in \mathcal{O}(H)$ associa $\mathsf{x}(\varphi^*(f))$, cioè $\mathsf{x}(f \circ \varphi)$.

Grazie alla Proposizione 14.3, possiamo interpretare $d\varphi$ come un'applicazione lineare $\mathrm{Lie}(G) \to \mathrm{Lie}(H)$.

Proposizione 14.5. *Sia $\varphi\colon G \to H$ un omomorfismo regolare fra gruppi algebrici lineari. L'applicazione $d\varphi\colon \mathrm{Lie}(G) \to \mathrm{Lie}(H)$ è un omomorfismo di algebre di Lie, cioè vale $d\varphi([\mathsf{x},\mathsf{y}]) = [d\varphi(\mathsf{x}), d\varphi(\mathsf{y})]$ per ogni $\mathsf{x},\mathsf{y} \in \mathrm{Lie}(G)$.*

Dimostrazione. Usando conti analoghi alla dimostrazione della Proposizione 14.3, questa proposizione segue immediatamente dal fatto che per definizione $\mathsf{x}(f) = (f * \mathsf{x})(e)$, e dall'uguaglianza $f * \mathsf{x} = \varphi^*(f' * \mathsf{x}')$. Qui stiamo considerando un qualsiasi vettore $\mathsf{x} \in T_{e_G}G$, abbiamo posto $\mathsf{x}' = d\varphi(\mathsf{x})$ e $f = \varphi^*(f')$ per una qualsiasi $f' \in \mathcal{O}(H)$, e la seconda uguaglianza si verifica facilmente calcolando il valore di entrambi i membri, che sono funzioni su G, su un qualsiasi $g \in G$. $\square$

In particolare, dalla proposizione precedente segue che data una rappresentazione regolare $\varphi\colon G \to \mathrm{GL}(V)$ di un gruppo algebrico lineare, allora il suo differenziale $d\varphi\colon \mathrm{Lie}(G) \to \mathrm{End}(V)$ è un omomorfismo di algebre di Lie. Una tale applicazione si dice anche una *rappresentazione* dell'algebra di Lie $\mathrm{Lie}(G)$, e V si dice anche un $\mathrm{Lie}(G)$-*modulo*. Di nuovo, anche se $\mathrm{Lie}(G)$ non è in generale associativa[9], i concetti di sottomodulo, modulo irriducibile e completamente riducibile si estendono in modo ovvio anche alle rappresentazioni delle algebre di Lie.

I legami fra le rappresentazioni di un gruppo algebrico lineare connesso G e della sua algebra di Lie sono molto stretti. Non si comportano esattamente allo stesso modo, tuttavia le uniche eccezioni sono essenzialmente riconducibili al seguente esempio.

[9]Una differenza banale ma importante con le rapresentazioni delle algebre associative, o dei gruppi, è che in un certo senso non si possono "applicare a ripetizione" ai vettori gli endomorfismi dati dall'algebra, o quantomeno non è immediato controllare cosa succede se lo si fa. Ad esempio, dato un vettore $v \in V$, l'insieme dei vettori $\mathrm{Lie}(G).v$, dato dall'applicare a v ogni endomorfismo indotto da $\mathrm{Lie}(G)$, non è in generale un sottomodulo.

Esempio 14.6. Sia $G = \mathbb{C}^*$, allora $\mathrm{Lie}(G) = \mathbb{C}$ con $[\mathsf{x}, \mathsf{y}] = 0$ per ogni $\mathsf{x}, \mathsf{y} \in \mathrm{Lie}(G)$. Sappiamo che ogni G-modulo è completamente riducibile, tuttavia esistono $\mathrm{Lie}(G)$-moduli non completamente riducibili. Infatti l'applicazione

$$\begin{array}{ccc} \mathbb{C} & \to & M_2(\mathbb{C}) \\ a & \mapsto & \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \end{array}$$

è lineare e preserva il bracket, quindi è una rappresentazione di $\mathbb{C} = \mathrm{Lie}(G)$ su $\mathbb{C}^2$. Però non è completamente riducibile: il sottospazio generato dal primo vettore della base canonica non ha un complemento $\mathrm{Lie}(G)$-stabile[10].

Proposizione 14.7. *Sia $\varphi\colon G \to \mathrm{GL}(V)$ una rappresentazione regolare di un gruppo algebrico lineare connesso G. Se un sottospazio vettoriale $W \subseteq V$ è un G-sottomodulo allora è anche un* $\mathrm{Lie}(G)$*-sottomodulo, per la rappresentazione data da $d\varphi$. Segue che V è irriducibile come G-modulo se lo è come* $\mathrm{Lie}(G)$*-modulo.*

Dimostrazione. Fissiamo una base di V tale che i primi vettori formano una base di W. Con essa identifichiamo $\mathrm{GL}(V)$ con $\mathrm{GL}(n)$ dove $n = \dim(V)$. Se W è G-stabile, allora l'immagine di G in $\mathrm{GL}(V)$ è contenuta nel sottoinsieme delle matrici della forma a blocchi

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

dove il primo blocco è $m \times m$ e $m = \dim(W)$. Segue facilmente che anche l'algebra di Lie di $\varphi(G)$ è contenuta in questo insieme di matrici, e inoltre ovviamente contiene l'immagine di $\mathrm{Lie}(G)$. $\square$

Vale anche il viceversa della proposizione precedente; la dimostrazione non è complicata ma sarebbe abbastanza lunga, e richiederebbe qualche risultato aggiuntivo di geometria algebrica che non abbiamo visto (in particolare, la dimensione delle varietà algebriche, e la dimensione delle fibre di un'applicazione regolare).

15. Altri esempi ed esercizi

Esempio 15.1. Consideriamo $G = \mathrm{SL}(n)$ con $n \geq 2$, e definiamo alcune rappresentazioni irriducibili. Sia $V_m = \bigwedge^m \mathbb{C}^n$, con $m \in \{1, \ldots, n-1\}$. Allora V_m ha dimensione non nulla, ed è un G-modulo irriducibile. Dimostriamolo facendo vedere che per ogni $v \in V_m$ non nullo, l'insieme $G \cdot v$ genera tutto V_m come spazio vettoriale. Possiamo scrivere v come una somma

$$v = \sum_{1 \leq i_1 < \ldots < i_m \leq n} a_{i_1,\ldots,i_m} e_{i_1} \wedge \ldots \wedge e_{i_m}$$

dove $a_{i_1,\ldots,i_m} \in \mathbb{C}$ per ogni scelta degli indici. A meno di rinominare gli indici e riscalando tutto v, possiamo assumere che $a_{1,\ldots,m} = 1$. Se allora $v = e_1 \wedge \ldots \wedge e_m$, possiamo moltiplicare v con matrici di permutazione (eventualmente con qualche -1 al posto di 1 per avere determinante $= 1$) per far vedere che qualsiasi vettore del tipo $e_{i_1} \wedge \ldots \wedge e_{i_m}$ (o l'opposto) è in $G \cdot v$. Questi formano una base di V_m, quindi in questo caso abbiamo finito.

Altrimenti, esistono $j_1, \ldots, j_m$ tali che $a = a_{j_1,\ldots,j_m} \neq 0$ e $j_m > m$. Per questi indici per forza esiste $s \in \{1, \ldots, m\}$ che non compare fra di essi. Consideriamo allora la matrice diagonale g, che sulla diagonale ha entrate uguali ad 1, eccetto che l'entrata s-esima uguale a 2 e la j_m-esima uguale a $\frac{1}{2}$. Allora $g \in \mathrm{SL}(n)$, e

$$v = e_1 \wedge \ldots \wedge e_m + a e_{j_1} \wedge \ldots \wedge e_{j_m} + (\text{altri addendi}),$$
$$gv = 2e_1 \wedge \ldots \wedge e_m + \frac{a}{2} e_{j_1} \wedge \ldots \wedge e_{j_m} + (\text{altri addendi}).$$

Prendiamo $v' = \frac{1}{3}(-v + 2gv)$, che è in $\mathrm{Span}(G \cdot v)$, e abbiamo

$$v' = e_1 \wedge \ldots \wedge e_m + 0 e_{j_1} \wedge \ldots \wedge e_{j_m} + (\text{altri addendi}).$$

[10] Questa rappresentazione di $\mathrm{Lie}(G)$ non è ottenibile differenziando una rappresentazione di G, cioè non si *integra* ad alcuna rappresentazione di G. Tuttavia questo non è l'unico motivo della "patologicità" di questo esempio, perché può succedere anche con algebre di Lie "linearmente riduttive", cioè per cui tutte le rappresentazioni di dimensione finita sono completamente riducibili. Ad esempio l'algebra di Lie di $\mathrm{PGL}(n)$ è isomorfa a $\mathfrak{sl}(n)$, che ha questa proprietà, ma se $n \geq 2$ la rappresentazione "standard" di $\mathfrak{sl}(n)$ su $\mathbb{C}^n$ non si integra ad una rappresentazione di $\mathrm{PGL}(n)$.

dove fra gli “altri addendi” compaiono solo termini che comparivano fra gli “altri addendi” di v (magari con coefficienti diversi). Ripetendo il procedimento arriviamo al vettore $e_1 \wedge \ldots \wedge e_m$, che quindi è in $\mathrm{Span}(G \cdot v)$. Questo ci riporta al caso precedente e conclude l’argomentazione.

L’importanza di questi $\mathrm{SL}(n)$ moduli è la seguente. Poniamo $\underline{v}_m = e_1 \wedge \ldots \wedge e_m$, e scegliamo interi non negativi $c_1, \ldots, c_{n-1}$. Consideriamo l’$\mathrm{SL}(n)$-modulo

$$U = V_1^{\otimes c_1} \otimes \ldots \otimes V_{n-1}^{\otimes c_{n-1}}$$

dove $V_i^{\otimes c_i} = V_i \otimes \ldots \otimes V_i$ con c_i fattori. Infine, consideriamo il G-modulo $\underline{V} = \mathrm{Span}(\mathrm{SL}(n) \cdot \underline{v})$ dentro U, dove

$$\underline{v} = \underline{v}_1^{\otimes c_1} \otimes \ldots \otimes \underline{v}_{n-1}^{\otimes c_{n-1}}.$$

Allora $\underline{V}$ è irriducibile (non è affatto ovvio), tutti gli $\mathrm{SL}(n)$-moduli irriducibili compaiono in questo modo a meno di isomorfismo, e scelte diverse dei coefficienti $c_1, \ldots, c_{n-1}$ portano a $\mathrm{SL}(n)$-moduli irriducibili non isomorfi (entrambe le cose sono ancora meno ovvie).

Esercizio 15.2. La fine dell’esempio precedente si generalizza a tutti i gruppi G linearmente riduttivi *connessi*. Cioè esistono un numero finito di G-moduli irriducibili $V_1, V_2, \ldots$, ciascuno con un vettore particolare $\underline{v}_1, \underline{v}_2, \ldots$ scelto dentro, tali che tutti i G-moduli irriducibili compaiono a meno di isomorfismi come moduli del tipo $\mathrm{Span}(G \cdot \underline{v})$ come sopra, per qualche scelta di coefficienti $c_1, c_2, \ldots$. Piccola osservazione aggiuntiva: diverse scelte di questi coefficienti possono portare a G-moduli irriducibili isomorfi, cioè non c’è sempre l’unicità che abbiamo citato per $\mathrm{SL}(n)$. Per certi gruppi esistono anche diverse scelte possibili dei moduli $V_1, V_2, \ldots$. L’esercizio consiste nel trovare una scelta di questi moduli e questi vettori per il gruppo $G = (\mathbb{C}^*)^n$.

Esempio 15.3. Svolgiamo l’Esercizio 12.8 per $\mathrm{O}(n, \mathbb{C})$. Osserviamo che se $n = 1$ allora $\mathbb{C}$ è ovviamente irriducibile. Sia $n \geq 2$, e consideriamo un vettore colonna $v \in \mathbb{C}^n$ non nullo. Se ${}^t v \cdot v \neq 0$ (cioè se v è *non isotropo*), allora possiamo completare $v = v_1$ ad una base $(v_1, \ldots, v_n)$ di $\mathbb{C}^n$, con vettori che hanno la stessa proprietà, basta prendere vettori della base canonica $(e_1, \ldots, e_n)$. Usando il procedimento di Gram-Schmidt con la forma bilineare simmetrica non degenere $(u, w) \mapsto {}^t u \cdot w$, si ortogonalizza la base, ottenendo $(v_1, v_2', \ldots, v_n')$. Ognuno di questi vettori è non isotropo, altrimenti la forma bilineare di prima sarebbe degenere. Quindi la nuova base si può ortonormalizzare: mettiamo i vettori ottenuti come colonne di una matrice g. Allora $g \in \mathrm{O}(n, \mathbb{C})$, e il vettore ge_1 è un multiplo scalare di v. Quindi, a meno di riscalaggio, due vettori non isotropi qualsiasi possono essere collegati con e_1 tramite matrici di $\mathrm{O}(n, \mathbb{C})$.

Concludiamo che se $W \subseteq \mathbb{C}^n$ è un $\mathrm{O}(n, \mathbb{C})$-sottomodulo e contiene un vettore non isotropo, allora W contiene tutti i vettori non isotropi, in particolare contiene tutti i vettori della base canonica, per cui $W = \mathbb{C}^n$.

Supponiamo invece che v sia isotropo e sia dentro un sottomodulo $W \subseteq \mathbb{C}^n$, e scegliamo fra i vettori della base canonica un vettore w tale che ${}^t vw \neq 0$. Allora è facile trovare un $a \neq 0$ tale che w e $w' = w + av$ siano entrambi non isotropi. Completando w, w' ad una base e usando il procedimento di prima, troviamo una matrice $g \in \mathrm{O}(n, \mathbb{C})$ tale che $g^{-1} v$ è in $\mathrm{Span}\{e_1, e_2\}$.

Assumiamo allora per semplicità che v sia un vettore isotropo in $\mathrm{Span}\{e_1, e_2\}$, cioè $v = ae_1 + be_2$ con $a^2 + b^2 = 0 = (a + ib)(a - ib)$ dove $i = \sqrt{-1}$. Allora $b = ia$ oppure $b = -ia$. Consideriamo $v' = e_1 + ie_2$ e $v'' = ie_1 + e_2$: uno dei due è un multiplo scalare di v perché a seconda dei due casi abbiamo $v/a = e_1 + ie_2$ oppure $v/b = ie_1 + e_2$. Inoltre v' e v'' formano una base di $\mathrm{Span}\{e_1, e_2\}$, e sono scambiati dalla matrice di permutazione che scambia e_1 ed e_2, che è una matrice di $\mathrm{O}(n, \mathbb{C})$.

Segue che entrambi v' e v'' sono in $\mathrm{Span}\, G \cdot v$ che è contenuto in W, quindi anche e_1 ed e_2, e allora $W = \mathbb{C}^n$ per la prima parte, concludendo l’esercizio.

Lo spazio $\mathbb{C}^n$ è irriducibile anche per il gruppo $\mathrm{SO}(n, \mathbb{C})$, ma solo per $n \geq 3$. Infatti $\mathrm{SO}(2) \cong \mathbb{C}^*$, e non ha moduli regolari irriducibili di dimensione 2. Sotto l’azione di $\mathrm{SO}(2)$, lo spazio $\mathbb{C}^2$ si decompone come $\mathbb{C}v' \oplus \mathbb{C}v''$, e gli addendi sono entrambi sottomoduli irriducibili.

Esercizio 15.4.
(1) Sia G un gruppo algebrico lineare e V un G-modulo regolare. Dimostrare che non si può usare in generale il Lemma di Schur per dimostrare che V è irriducibile, cioè non vale il Lemma di Schur col “se e solo se”. Per questo, trovare G e V tali che V non è irriducibile, ma gli scalari sono gli unici endomorfismi di V che commutano con tutti gli elementi dell’immagine di G.

(2) Invece se V è completamente riducibile (ad es. se G è linearmente riduttivo), allora vale il Lemma di Schur col "se e solo se": dimostrarlo.

Esempio 15.5. Se G è un gruppo finito, allora $\mathcal{O}(G)$ è naturalmente isomorfa a $\mathbb{C}[G]$, associando ad ogni elemento $f \in \mathcal{O}(G)$ la combinazione lineare

$$\sum_{g \in G} f(g)g.$$

Sia ad esempio $G = S_3$. Allora è facile dare almeno tre G-moduli:

(1) quello banale V_1;
(2) il modulo V_2 di dimensione 1 dove ogni permutazione $\sigma \in S_3$ agisce per moltiplicazione per il suo segno;
(3) il modulo V_3 di dimensione 2, definito come il sottospazio vettoriale di $\mathbb{C}^3$ di equazione $x + y + z = 0$. Qui G agisce su $\mathbb{C}^3$ nel solito modo, permutando le entrate dei vettori.

Si verifica facilmente che V_1, V_2 e V_3 sono irriducibili, e non isomorfi fra loro. Quindi a meno di isomorfismi abbiamo

$$\mathcal{O}(G) \supseteq (V_1^* \otimes V_1) \oplus (V_2^* \otimes V_2) \oplus (V_3^* \otimes V_3).$$

D'altronde $\mathcal{O}(G) \cong \mathbb{C}[G]$ ha dimensione 6, e questi addendi hanno dimensione rispettivamente 1, 1, 4. Allora l'inclusione qui sopra è un'uguaglianza. Segue anche che ogni G-modulo irriducibile è isomorfo a V_i per qualche $i \in \{1, 2, 3\}$.

Appendice A. Richiami di geometria algebrica

A.1. **Definizioni di base, Basissatz e Nullstellensatz.** In questa appendice consideriamo $\mathbb{C}^n$ dotato della topologia di Zariski. Ricordiamo che, per definizione, i chiusi di questa topologia sono i sottoinsiemi che sono zeri comuni di un insieme di polinomi.

Nel corso useremo diversi risultati di geometria algebrica, e in questa appendice faremo dei richiami su questo argomento, adattandoli al procedere del corso e alle conoscenze degli studenti.

Ricordiamo, per un ideale $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$, la notazione $V(I)$ per il luogo degli zeri comuni di tutti gli elementi di I in $\mathbb{C}^n$. Usiamo la stessa notazione $V(f_1, \ldots, f_m)$ per denotare gli zeri comuni di una famiglia finita $f_1, \ldots, f_m$ di polinomi.

Per un sottoinsieme $X \subseteq \mathbb{C}^n$ ricordiamo la notazione $I(X)$ per l'ideale dei polinomi che si annullano su tutto X, e dato un polinomio $f \in \mathbb{C}[x_1, \ldots, x_n]$, ricordiamo la notazione X_f per il luogo degli elementi di X dove f non si annulla.

Ricordiamo qualche formula elementare: $V(I) \cap V(J) = V(I + J)$, $V(I) \cup V(J) = V(I \cdot J)$ per I, J ideali di $\mathbb{C}[x_1, \ldots, x_n]$.

Teorema A.1. *(Basissatz) Ogni ideale di $\mathbb{C}[x_1, \ldots, x_n]$ è finitamente generato.*

Dimostrazione. Procediamo per induzione su n. Il caso $n = 0$ è ovvio, perché $\mathbb{C}$ ha solo due ideali, generati da 0 e da 1 rispettivamente.

Consideriamo allora $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ ideale, e costruiamo una sequenza di elementi $f_1, f_2, \ldots$ come segue. Sia f_1 un elemento di I il cui grado in x_n sia minimo. Per ogni intero $i \geq 1$, consideriamo $(f_1, \ldots, f_i)$: se è diverso da I, scegliamo f_{i+1} in $I \smallsetminus (f_1, \ldots, f_i)$ di grado minimo in x_n.

Se invece $I = (f_1, \ldots, f_i)$ allora ci fermiamo: avendo trovato un numero finito di generatori, il teorema vale per I. Dobbiamo discutere allora la possibilità che $(f_1, \ldots, f_i)$ possa essere diverso da I per ogni i. Si noti che per costruzione, per ogni i, il grado in x_n di f_{i+1} è uguale o maggiore di quello di f_i.

Scriviamo ogni f_i come polinomio in x_n, a coefficienti in $\mathbb{C}[x_1, \ldots, x_{n-1}]$, e sia $a_i \in \mathbb{C}[x_1, \ldots, x_{n-1}]$ il coefficiente direttore. Per induzione, l'ideale $J = (a_1, a_2, \ldots)$ generato dagli a_i in $\mathbb{C}[x_1, \ldots, x_{n-1}]$ è finitamente generato, quindi esiste un intero positivo m tale che $J = (a_1, \ldots, a_m)$.

Dimostriamo che allora $I = (f_1, \ldots, f_m)$. Per assurdo, se così non fosse, avremmo costruito f_{m+1}. D'altronde $a_{m+1} \in J$, quindi possiamo scrivere

$$a_{m+1} = a_1 u_1 + \ldots + a_m u_m$$

con u_i polinomi in $x_1, \ldots, x_{n-1}$. Consideriamo

$$g = \sum_{i=1}^{m} f_i u_i x_n^{\deg_{x_n} f_{m+1} - \deg_{x_n} f_i}.$$

Si tratta di un polinomio dell'ideale $(f_1, \ldots, f_m)$, e come polinomio in x_n ha lo stesso grado e lo stesso coefficiente direttore di f_{m+1}. Quindi $f_{m+1} - g$ ha grado in x_n minore di quello di f_{m+1}. D'altronde stiamo supponendo di aver costruito f_{m+1}, che per costruzione non appartiene a $(f_1, \ldots, f_m)$. Segue che neppure $f_{m+1} - g$ appartiene a $(f_1, \ldots, f_m)$, contraddicendo la minimalità del grado in x_n di f_{m+1}. □

Corollario A.2. *Ogni sottoinsieme di $\mathbb{C}^n$ è compatto*[11] *(in topologia di Zariski).*

Dimostrazione. Basta dimostrare il corollario per sottoinsiemi aperti di $\mathbb{C}^n$, il caso generale segue facilmente. Sia dunque A aperto di Zariski di $\mathbb{C}^n$, e sia

$$A = \bigcup_i U_i$$

un ricoprimento aperto. Dalla definizione della topologia di Zariski, una base è data dagli aperti del tipo $\mathbb{C}^n_f$ dove $f \in \mathbb{C}[x_1, \ldots, x_n]$. Possiamo assumere di avere $U_i = \mathbb{C}^n_{f_i}$ per ogni i, dove $f_i \in \mathbb{C}[x_1, \ldots, x_n]$: se un ricoprimento siffatto ammette sempre un sottoricoprimento finito, allora la compattezza di A segue immediatamente.

Con una facile generalizzazione della formula $V(I) \cap V(J) = V(I + J)$, otteniamo

$$\mathbb{C}^n \smallsetminus A = \bigcap_i V(f_i) = V(I)$$

dove I è l'ideale generato da tutti i polinomi f_i. Per il Basissatz, esistono $f_{i_1}, \ldots, f_{i_m}$ generatori di I. Quindi

$$\mathbb{C}^n \smallsetminus A = \bigcap_{j=1}^{m} V(f_{i_j})$$

cioè A è ricoperto da $\mathbb{C}^n_{f_{i_1}}, \ldots, \mathbb{C}^n_{f_{i_m}}$. □

Teorema A.3. *Sia I un ideale di $\mathbb{C}[x_1, \ldots, x_n]$ tale che $V(I) = \varnothing$. Allora $1 \in I$, cioè $I = \mathbb{C}[x_1, \ldots, x_n]$.*

Dimostrazione. Sia per assurdo I ideale proprio. Possiamo assumere che sia un ideale massimale, e troviamo uno zero comune a tutti i suoi elementi. Sia $R = \mathbb{C}[x_1, \ldots, x_n]/I$: si tratta di una $\mathbb{C}$-algebra finitamente generata, di dimensione al più numerabile come spazio vettoriale su $\mathbb{C}$. Visto che I è un ideale massimale, R è un campo che contiene $\mathbb{C}$. Dimostriamo che R è algebrico su $\mathbb{C}$: sia $\alpha \in R \smallsetminus \mathbb{C}$, e consideriamo gli elementi

$$\frac{1}{\alpha - z}$$

al variare di $z \in \mathbb{C}$. Visto che questi elementi sono in quantità più che numerabile, non possono essere linearmente indipendenti su $\mathbb{C}$, quindi esiste una combinazione lineare di essi a coefficienti $\lambda_i \in \mathbb{C}$ non tutti nulli tali che

$$\frac{\lambda_1}{\alpha - z_1} + \ldots + \frac{\lambda_m}{\alpha - z_m} = 0.$$

Moltiplicando per il prodotto $(\alpha - z_1) \cdots (\alpha - z_m)$ otteniamo un polinomio a coefficienti complessi che si annulla in α, cioè α è algebrico su $\mathbb{C}$. Visto che $\mathbb{C}$ è algebricamente chiuso, deduciamo $\mathbb{C} = R$.

D'altronde R^n contiene banalmente un elemento che è zero comune di tutti gli elementi di I: si tratta semplicemente di[12] $(x_1 + I, \ldots, x_n + I)$. □

Corollario A.4. *(Nullstellensatz) Se $f \in \mathbb{C}[x_1, \ldots, x_n]$ si annulla su tutto $V(I)$ per I un ideale di $\mathbb{C}[x_1, \ldots, x_n]$, allora esiste un intero positivo d tale che $f^d \in I$.*

[11] Ci riferiamo qui alla compattezza usuale come in topologia moderna. In geometria algebrica è rimasto tuttavia in uso chiamare "compatto" uno spazio topologico *di Hausdorff*, tale che ogni ricomprimento aperto abbia un sottoricoprimento finito. Ci si riferisce alla seconda condizione, cioè per noi la usuale compattezza, col termine di "quasi compattezza".

[12] È una tautologia: dato $f(x_1, \ldots, x_n) \in I$, valutarlo nel punto $(x_1 + I, \ldots, x_n + I)$ di R^n vuol dire prendere l'elemento $f(x_1 + I, \ldots, x_n + I)$ di R, che è uguale a $f(x_1, \ldots, x_n) + I$, che è zero in R perché $f \in I$.

Dimostrazione. Per il Basissatz, l'ideale I è finitamente generato: $I = (f_1, \ldots, f_m)$. Consideriamo l'ideale $J \subseteq \mathbb{C}[x_1, \ldots, x_n, x_{n+1}]$ generato da $f_1, \ldots, f_m$ (sono polinomi solo nelle prime n variabili), e dal polinomio $g = x_{n+1}f - 1$. In $\mathbb{C}^{n+1}$ abbiamo $V(J) = \varnothing$, perché dove si annullano simultaneamente $f_1, \ldots, f_n$ si annulla anche f e quindi non si annulla il polinomio g.

Quindi $J = (1)$, cioè 1 è ottenibile come combinazione lineare dei nostri generatori di J a coefficienti polinomi:

$$a_1 f_1 + \ldots + a_m f_m + a_{m+1}(x_{n+1}f - 1) = 1.$$

Sostituiamo $1/f$ al posto di x_{n+1}, e otteniamo la seguente uguaglianza nel campo $\mathbb{C}(x_1, \ldots, x_n)$:

$$a_1(x_1, \ldots, x_n, 1/f)f_1 + \ldots + a_m(x_1, \ldots, x_n, 1/f)f_m = 1.$$

Moltiplicando per un'opportuna potenza positiva f^d di f, eliminiamo i denominatori presenti al primo membro, e troviamo un'espressione in $\mathbb{C}[x_1, \ldots, x_n]$ di f^d in termini dei generatori di I. Conclusione: $f^d \in I$. $\square$

Il Nullstellensatz ci permette di caratterizzare gli anelli delle funzioni regolari delle varietà affini.

Corollario A.5. *Sia R una $\mathbb{C}$-algebra associativa commutativa unitaria finitamente generata e senza elementi nilpotenti. Allora esiste una varietà affine X tale che $\mathcal{O}(X) \cong R$.*

Dimostrazione. Siano $a_1, \ldots, a_n \in R$ generatori di R, e consideriamo l'omomorfismo di algebre $\mathbb{C}[x_1, \ldots, x_n] \to R$ che manda x_i in a_i per ogni i. È suriettivo, quindi chiamando I il suo nucleo abbiamo

$$R \cong \mathbb{C}[x_1, \ldots, x_n]/I.$$

Definiamo ora $X \subseteq \mathbb{C}^n$ come $X = V(I)$, e dimostriamo che $I = I(X)$. Abbiamo sicuramente $I \subseteq I(X)$, visto che per definizione di X ogni polinomio di I vi si annulla. Sia ora $f \in I(X)$, cioè f si annulla su $V(I)$. Per il Nullstellensatz, una potenza positiva f^d è in I. Allora nell'anello R, a meno dell'isomorfismo qui sopra, la classe $f + I$ è tale che una sua potenza $f^d + I$ è zero. Ma R non ha nilpotenti, per cui $f + I$ è già la classe nulla, cioè $f \in I$. Segue $I = I(X)$. Otteniamo che R è isomorfo a $\mathcal{O}(X)$. $\square$

Ricordiamo ora la seguente terminologia standard.

Definizione A.6. Una *varietà affine* è un sottoinsieme chiuso di $\mathbb{C}^n$ per qualche n intero positivo. Data una varietà affine $X \subseteq \mathbb{C}^n$, si definisce l'*anello delle funzioni regolari* su X, denotato $\mathcal{O}(X)$ (o $\mathbb{C}[X]$), l'insieme delle funzioni $f\colon X \to \mathbb{C}$ date dalla restrizione a X di polinomi nelle n variabili di $\mathbb{C}^n$.

Ricordiamo anche che, visto che $I(X)$ è l'ideale delle funzioni polinomiali su $\mathbb{C}^n$ che svaniscono su tutta una varietà affine $X \subseteq \mathbb{C}^n$, la restrizione di funzioni da $\mathbb{C}^n$ a X induce l'isomorfismo usuale

$$\mathcal{O}(X) \cong \mathbb{C}[x_1, \ldots, x_n]/I(X).$$

Lemma A.7. *Siano $X \subseteq Z \subseteq \mathbb{C}^n$ chiusi. Allora la restrizione $\mathcal{O}(Z) \to \mathcal{O}(X)$ è suriettiva, e induce un isomorfismo naturale*

$$\mathcal{O}(X) \cong \mathcal{O}(Z)/I_Z(X)$$

dove $I_Z(X)$ è l'ideale di $\mathcal{O}(Z)$ delle funzioni regolari su Z che svaniscono su X.

Corollario A.8. *Dato x elemento di una varietà algebrica affine X, l'ideale $I(\{x\})$ di $\mathcal{O}(X)$ è massimale, e tutti gli ideali massimali di $\mathcal{O}(X)$ si ottengono in questo modo.*

Dimostrazione. La prima affermazione è ovvia dal Lemma A.7, e dal fatto che $\mathcal{O}(\{x\}) = \mathbb{C}$, quindi è un campo. La seconda affermazione deriva dal Teorema A.3: se $X \subseteq \mathbb{C}^n$ e un ideale $I \subseteq \mathcal{O}(X)$ non svanisce in alcun punto di X, allora consideriamo la sua immagine inversa J in $\mathbb{C}[x_1, \ldots, x_n]$. L'ideale J contiene $I(X)$, per cui $V(J)$ è contenuto in X. Ma visto che I non svanisce in alcun punto di X, otteniamo che $V(I) = \varnothing$, quindi J contiene la funzione $1 \in \mathbb{C}[x_1, \ldots, x_n]$. Ma allora I contiene l'immagine in $\mathcal{O}(X)$ della funzione 1, cioè I non è un ideale proprio. $\square$

Ricordiamo anche che il prodotto cartesiano $X \times Y$ di due varietà affini $X \subseteq \mathbb{C}^n$ e $Y \subseteq \mathbb{C}^m$ è definito come la varietà affine in $\mathbb{C}^{n+m}$ definita dal prodotto dell'ideale $I(X)$, i cui elementi sono espressi nelle prime n coordinate $x_1, \ldots, x_n$ di $\mathbb{C}^{n+m}$, e dell'ideale $I(Y)$, i cui elementi però sono espressi nelle rimanenti m coordinate $y_1, \ldots, y_m$ di $\mathbb{C}^{n+m}$. Segue facilmente un isomorfismo naturale $\mathcal{O}(X \times Y) \cong \mathcal{O}(X) \otimes \mathcal{O}(Y)$.

Per comodità, riportiamo il seguente ovvio lemma.

A.2. **Varietà quasi affini.** Si generalizza l'anello delle funzioni regolari ai sottoinsiemi localmente chiusi di $\mathbb{C}^n$, nel modo seguente.

Definizione A.9. Sia $X \subseteq \mathbb{C}^n$ un insieme localmente chiuso. Si definisce l'*anello delle funzioni regolari* su X, denotato $\mathcal{O}(X)$ (o $\mathbb{C}[X]$), l'insieme delle funzioni $f\colon X \to \mathbb{C}$ tali che esiste un ricoprimento aperto $\{U_i\}$ di X e polinomi $a_i, b_i \in \mathbb{C}[x_1, \ldots, x_n]$ tali che per ogni indice i il polinomio b_i non abbia zeri su U_i, e

$$f|_{U_i} = \frac{a_i|_{U_i}}{b_i|_{U_i}}.$$

Visto che tutti i sottoinsiemi in topologia di Zariski sono compatti, nella definizione qui sopra possiamo sempre assumere che i varia in un insieme finito (per semplicità, di numeri naturali).

Grazie alla seguente proposizione, le due definizioni di $\mathcal{O}(X)$ coincidono per varietà affini.

Proposizione A.10. *Sia $Z \subseteq \mathbb{C}^n$ chiuso non vuoto, sia $h \in \mathbb{C}[x_1, \ldots, x_n]$ non costantemente nullo su Z, e sia $X = Z_h$. Allora per ogni elemento $f \in \mathcal{O}(X)$ esistono $a \in \mathbb{C}[x_1, \ldots, x_n]$ e un intero non negativo n tali che f coincide su X con la frazione*

$$\frac{a}{h^d}.$$

Dimostrazione. [13] Una base della topologia di Zariski su Z è data dagli insiemi Z_r dove r è un polinomio. Possiamo allora supporre che per ogni i abbiamo $U_i = Z_{r_i}$ per qualche r_i.

Osserviamo che $U_i = Z_{r_i} \subseteq Z_{b_i}$ per ogni i, quindi $V(r_i) \cap Z \supseteq V(b_i) \cap Z$. D'altronde abbiamo $V(r_i) \cap Z = V((r_i) + I(Z))$ e $V(b_i) \cap Z = V((b_i) + I(Z))$, e dal Nullstellensatz segue che una potenza positiva $r_i^{m_i}$ è in $(b_i) + I(Z)$. In altre parole $r_i^{m_i}$ coincide con $b_i c_i$ su Z, per un $c_i \in \mathbb{C}[x_1, \ldots, x_n]$ che non si annulla mai su U_i. Allora a_i/b_i coincide con $a_i c_i / r_i^{m_i}$ su Z. Possiamo rimpiazzare quindi r_i con $r_i^{m_i}$ e a_i con $a_i c_i$, e supporre che f coincida con a_i/r_i su U_i.

Osserviamo ora che, dati due indici i, j, la frazione a_i/r_i coincide con a_j/r_j su $U_i \cap U_j$, quindi $a_i r_j - a_j r_i$ è zero su $U_i \cap U_j$, che è uguale a $Z_{r_i r_j}$. Segue che $r_i r_j (a_i r_j - a_j r_i)$ si annulla su tutto Z, cioè $r_j^2(a_i r_i)$ coincide con $r_i^2(a_j r_j)$ su Z. Rimpiazzando ogni r_i con r_i^2 e ogni a_i con $a_i r_i$, possiamo assumere che $a_i r_j$ coincide con $a_j r_i$ su Z.

Infine, ricordiamo che Z_h è contenuto nell'unione degli Z_{r_i}, cioè

$$V(h) \cap Z \supseteq Z \cap \bigcap_i V(r_i) = Z \cap V(r_1, r_2, \ldots).$$

Di nuovo per il Nullstellensatz, abbiamo che una potenza positiva h^d coincide su Z con un elemento dell'ideale $(r_1, r_2, \ldots)$:

$$h^d + I(Z) = (s_1 r_1 + s_2 r_2 + \ldots) + I(Z).$$

Poniamo $a = s_1 a_1 + s_2 a_2 + \ldots$. Allora per ogni indice i abbiamo che su Z valgono le uguaglianze

$$r_i a = s_1 a_1 r_i + s_2 a_2 r_i + \ldots = s_1 a_i r_1 + s_2 a_i r_2 + \ldots = a_i h^d.$$

In altre parole su ogni U_i la frazione a_i/r_i, che coincide con f, coincide anche con a/h^d. Quindi f e a/h^d coincidono su tutto X. □

Corollario A.11. *Siano X, Z e h come nella Proposizione A.10, e sia $X' \subseteq \mathbb{C}^{n+1}$ definito da $I(X)$ nelle prime n coordinate $x_1, \ldots, x_n$ di $\mathbb{C}^{n+1}$, insieme al polinomio $h(x_1, \ldots, x_n)x_{n+1} = 1$. Allora l'applicazione*

$$\begin{array}{rccc} f\colon & X & \to & X' \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_n, 1/h(x_1, \ldots, x_n)) \end{array}$$

è una biiezione che soddisfa $f^*(\mathcal{O}(X')) = \mathcal{O}(X)$.

[13] Questa dimostrazione è essenzialmente un'applicazione diretta del Nullstellensatz. È interessante però osservare che usa in modo cruciale anche il seguente fatto banale: se $\frac{a}{b}$ è uguale a $\frac{c}{d}$, e se $b + d \neq 0$, allora $\frac{a}{b}$ è anche uguale a $\frac{a+c}{b+d}$. Detto meglio: nel campo dei quozienti di un dominio d'integrità, l'insieme dei denominatori possibili di una stessa frazione è un ideale (tolto lo zero).

In seguito al corollario qui sopra, chiameremo *varietà affine* anche un X come nella Proposizione A.10. Infine, diamo anche la seguente definizione standard.

Definizione A.12. Una *varietà quasi affine* è un aperto di Zariski di una varietà affine.

A.3. **Applicazioni regolari.**

Definizione A.13. Siano $X \subseteq \mathbb{C}^n$ e $Y \subseteq \mathbb{C}^m$ varietà affini. Un'applicazione $\varphi\colon X \to Y$ si dice *regolare* se $\varphi^*(\mathcal{O}(Y)) \subseteq \mathcal{O}(X)$, dove φ^* è la composizione con φ, cioè $\varphi^*(f) = f \circ \varphi$ per ogni $f \in \mathcal{O}(Y)$.

Equivalentemente, $\varphi\colon X \to Y$ è regolare se, come applicazione $X \to \mathbb{C}^m$, è data da m polinomi nelle coordinate di $\mathbb{C}^n$ (per dimostrare l'equivalenza, basta considerare φ^* applicata alle funzioni coordinate di $\mathbb{C}^m$). Inoltre φ si dice un *isomorfismo* se è una biiezione con inversa regolare.

Proposizione A.14. *Siano X e Y varietà affini. Data $\varphi\colon X \to Y$ applicazione regolare, l'applicazione $\varphi^*\colon \mathcal{O}(Y) \to \mathcal{O}(X)$ è un omomorfismo di algebre. Viceversa, dato un omomorfismo di algebre $\Phi\colon \mathcal{O}(Y) \to \mathcal{O}(X)$, esiste un'unica applicazione regolare $\varphi\colon X \to Y$ tale che $\varphi^* = \Phi$. Infine, φ è un isomorfismo di varietà affini se e solo se φ^* è un isomorfismo di algebre.*

Dimostrazione. La prima affermazione è ovvia dalla definizione di φ^*. Consideriamo allora Φ come sopra, l'inclusione $Y \subseteq \mathbb{C}^m$, e le coordinate $y_1, \ldots, y_m$ su $\mathbb{C}^m$ e le restrizioni $y_1|_Y, \ldots, y_m|_Y$ ad Y. Definiamo

$$\begin{array}{rccc} \varphi\colon & X & \to & \mathbb{C}^m \\ & x & \mapsto & (\Phi(y_1|_Y)(x), \ldots, \Phi(y_m|_Y)(x)). \end{array}$$

Si tratta evidentemente di un'applicazione regolare, verifichiamo che $\varphi(X) \subseteq Y$. Sia $p(y_1, \ldots, y_m) \in I(Y)$; visto che Φ è un omomorfismo di algebre, abbiamo

$$p(\Phi(y_1|_Y)(x), \ldots, \Phi(y_m|_Y)(x)) = \Phi(p(y_1|_Y, \ldots, y_m|_Y))(x) = \Phi(\underbrace{p(y_1, \ldots, y_m)|_Y}_{=0})(x) = 0.$$

Quindi $\varphi(X)$ svanisce su $V(I(Y))$, che è uguale ad Y perché Y è chiusa in $\mathbb{C}^m$. Per costruzione abbiamo inoltre $\varphi^*(y_i|_Y) = \Phi(y_i|_Y)$ per ogni i, e ovviamente questa φ è l'unica applicazione $X \to Y$ per cui valgono queste uguaglianze. Seguono l'uguaglianza $\varphi^* = \Phi$ e l'unicità di φ. L'ultima affermazione segue dalle precedenti. $\square$

Corollario A.15. *Siano X, Y, φ come nella Proposizione A.14. Allora φ^* è suriettiva se e solo se φ ha immagine chiusa e induce un isomorfismo fra X e $\varphi(X)$.*

Dimostrazione. L'omomorfismo φ^* è suriettivo se e solo se induce un isomorfismo fra $\mathcal{O}(X)$ e $\mathcal{O}(Y)/\ker(\varphi^*)$, e in generale $\ker(\varphi^*)$ è proprio l'ideale in $\mathcal{O}(Y)$ della chiusura di $\varphi(X)$. $\square$

Lemma A.16. *Sia $\varphi\colon X \to Y$ applicazione regolare fra varietà affini. Allora φ^* è iniettiva se e solo se $\varphi(X)$ è denso in Y.*

Dimostrazione. Supponiamo che $\varphi(X)$ sia denso in Y, e sia $f \in \mathcal{O}(Y)$. Se $\varphi^*(f)$ è la funzione nulla su X, allora f è la funzione nulla su $\varphi(X)$. Segue che f è la funzione nulla su tutto Y, cioè φ è iniettiva. Viceversa, supponiamo che φ^* sia iniettiva, e sia f nell'ideale $I_Y(\overline{\varphi(X)})$. Visto che $\varphi^*(f)$ è la funzione nulla, abbiamo che f è nulla come funzione su Y, cioè $I_Y(\overline{\varphi(X)})$ coincide con tutto Y. $\square$

Lemma A.17. *Sia X una varietà affine, e $U \subseteq \mathcal{O}(X)$ un sottospazio vettoriale di dimensione finita, tale che U genera $\mathcal{O}(X)$ come algebra. Sia $V = U^*$. Allora l'applicazione*

$$\begin{array}{rccc} \varphi\colon & X & \to & V \\ & x & \mapsto & (u \mapsto u(x)) \end{array}$$

è un isomorfismo di X con la sua immagine, che è un chiuso di Zariski di V.

Dimostrazione. Il lemma segue dal Corollario A.15, riformuliamo l'argomentazione in modo da essere sicuri che l'applicazione φ che segue da quel corollario è proprio quella di questo lemma.

Scegliamo una base $f_1, \ldots, f_m$ di U, allora essi sono generatori di $\mathcal{O}(X)$ come algebra. Segue che $\mathcal{O}(X)$ è isomorfa ad un quoziente del tipo

$$A = \mathbb{C}[y_1, \ldots, y_m]/J$$

dove J è un ideale, tramite un isomorfismo $\Psi\colon A \to \mathcal{O}(X)$ che manda la classe $y_i + J$ in f_i per ogni i. Poniamo $Y = V(J) \subseteq \mathbb{C}^m$, abbiamo allora il solito isomorfismo $A \cong \mathcal{O}(Y)$, e possiamo considerare Ψ come un isomorfismo di algebre $\mathcal{O}(Y) \to \mathcal{O}(X)$. La Proposizione A.14 fornisce un isomorfismo di varietà $\psi\colon X \to Y$ corrispondente a questa Ψ. Ripercorrendo la definizione di ψ data nella dimostrazione di quella proposizione, e ponendo la u dell'enunciato di questo lemma uguale alle funzioni f_i, otteniamo immediatamente $\psi = \varphi$. $\square$

Concludiamo con un lemma utile nello studio delle Graßmanniane.

Lemma A.18. *Sia $\varphi\colon \mathbb{C}^n \to \mathbb{C}^{n+m}$ un'applicazione regolare, data in coordinate come*

$$\begin{array}{cccc} \varphi\colon & \mathbb{C}^n & \to & \mathbb{C}^{n+m} \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_n, p_1, \ldots, p_m) \end{array}$$

dove i p_i sono polinomi in $x_1, \ldots, x_n$. Allora φ ha immagine chiusa, ed è un isomorfismo di $\mathbb{C}^n$ con la sua immagine.

Dimostrazione. Siano $y_1, \ldots, y_n, y_{n+1}, \ldots, y_m$ le coordinate su $\mathbb{C}^{n+m}$. L'immagine di φ è contenuta nel chiuso $W \subseteq \mathbb{C}^{n+m}$ definito dalle equazioni

$$y_{n+i} = p_i(y_1, \ldots, y_n)$$

per ogni $i \in \{1, \ldots, m\}$. Ora però l'inversa di φ è definita su tutto W, tramite la proiezione

$$(y_1, \ldots, y_n, y_{n+1}, \ldots, y_m) \mapsto (y_1, \ldots, y_n).$$

$\square$

A.4. **Varietà irriducibili.**

Definizione A.19. Uno spazio topologico X si dice *irriducibile* se per ogni Y, Z chiusi tali che $Y \cup Z = X$ vale $Y = X$ oppure $Z = X$. Una *componente irriducibile* di X è un sottospazio topologico irriducibile massimale di X.

Per l'irriduciblità valgono alcune proprietà simili alla connessione: la chiusura di un irriducibile (in uno spazio topologico più grande) è irriducibile, e l'immagine di un irriducibile tramite un'applicazione continua è irriducibile. Vale anche il seguente

Lemma A.20. *Siano X, Y varietà affini irriducibili. Allora $X \times Y$ è irriducibile.*

Dimostrazione. Siano Z_1, Z_2 chiusi di $X \times Y$ tali che $X \times Y = Z_1 \cup Z_2$. Per ogni $x \in X$, l'insieme $\{x\} \times Y$ è un chiuso di $X \times Y$ isomorfo a Y come varietà , per cui è irriducibile. Inoltre è contenuta nell'unione di Z_1 e di Z_2, quindi è immediato concludere che è contenuta interamente in Z_1 oppure in Z_2. Allora $X = X_1 \cup X_2$, dove

$$X_i = \{p \in X \mid \{p\} \times Y \subseteq Z_i\}.$$

Dimostriamo che si tratta di chiusi di Zariski, osservando che

$$X_i = \bigcap_{y \in Y} \{x \in X \mid (x, y) \in Z_i\}$$

e che $\{x \in X \mid (x, y) \in Z_i\}$ è la proiezione su X del sottoinsieme $W_i = (X \times \{y\}) \cap Z_i$ di $X \times Y$. Ora, $X \times \{y\}$ è un chiuso di Zariski di $X \times Y$, isomorfo ad X tramite la proiezione. Dato che W_i è chiuso in $X \times \{y\}$, la sua proiezione è chiusa in X. Allora X_i è chiuso in X essendo intersezione di chiusi. $\square$

Proposizione A.21. *Sia X una varietà affine. Allora X è irriducibile se e solo se $\mathcal{O}(X)$ è un dominio d'integrità.*

Dimostrazione. Supponiamo X sia irriducibile, e siano $f_1, f_2 \in \mathcal{O}(X)$ tali che $f_1 f_2 = 0$. Sia Z_i il luogo degli zeri di f_i su X. Abbiamo $Z_1 \cup Z_2 = X$, quindi $Z_i = X$ per qualche i, cioè f_i è la funzione nulla per qualche i. Segue che $\mathcal{O}(X)$ è un dominio d'integrità.

Viceversa, supponiamo che $\mathcal{O}(X)$ sia un dominio d'integrità, e siano Z_1, Z_2 sottoinsiemi chiusi tali che $Z_1 \cup Z_2 = X$. Supponiamo per assurdo che $Z_i \neq X$ per ogni i, quindi $I_X(Z_1) \cap I_X(Z_2) = (0)$ ma nessuno dei due ideali è nullo. Allora esistono $f_1 \in I_X(Z_2) \smallsetminus I_X(Z_1)$ e $f_2 \in I_X(Z_1) \smallsetminus I_X(Z_2)$. Segue che $f_1 f_2$ è la funzione nulla, ma allora f_i è nulla per qualche i: assurdo. $\square$

Osservazione A.22. Dalla proposizione precedente segue che X è irriducibile se e solo se $I(X)$ è un ideale primo.

Proposizione A.23. *Ogni varietà affine è unione finita di chiusi irriducibili.*

Dimostrazione. Possiamo supporre che X non sia irriducibile, e sia $X = X_1 \cup X_2$ una decomposizione di X in unione di chiusi propri. Se sono irriducibili abbiamo finito, altrimenti almeno uno di essi si decompone stesso modo, es. $X_1 = X_{1,1} \cup X_{1,2}$, eccetera. Il procedimento deve terminare dopo un numero finito di passi: ogni catena discendente di chiusi, es. $X \supseteq X_1 \supseteq X_{1,1} \supseteq \dots$ si stabilizza, perché ogni catena ascendente di ideali di $\mathcal{O}(X)$ si stabilizza. $\square$

Se X è una varietà algebrica affine irriducibile, allora è definito il campo dei quozienti di $\mathcal{O}(X)$. La notazione usuale è $\mathbb{C}(X)$, che si usa di solito assieme alla notazione $\mathbb{C}[X]$.

Osservazione A.24. Si dimostra facilmente che la decomposizione di una varietà affine come unione delle sue componenti irriducibili è unica, come per le componenti connesse di uno spazio topologico.

Proposizione A.25. *Sia $\varphi\colon X \to Y$ un'applicazione regolare fra varietà algebriche affini irriducibili. Supponiamo φ^* induca un isomorfismo fra $\mathbb{C}(Y)$ e $\mathbb{C}(X)$. Allora esiste un aperto denso $V' \subseteq Y$ tale che, ponendo $U' = \varphi^{-1}(V')$, allora $\varphi|_{U'}$ è un isomorfismo $U' \to V'$.*

Dimostrazione. Siano $f_1, \dots, f_m$ generatori di $\mathcal{O}(X)$ come algebra. In particolare sono elementi di $\mathbb{C}(X)$, quindi si possono scrivere come
$$f_i = \frac{\varphi^*(a_i)}{\varphi^*(b_i)}$$
dove $a_i, b_i \in \mathcal{O}(Y)$ e $b_i \neq 0$ per ogni i. Poniamo $b = b_1 \cdots b_m$ e $B = \varphi^*(b)$, e consideriamo $\varphi|_{X_B}\colon X_B \to Y_b$. Osserviamo che $X_B = \varphi^{-1}(Y_b)$.

Da una parte, l'algebra $\mathcal{O}(X_B)$ è generata dalle restrizioni delle funzioni $f_1, \dots, f_m$ a X_B, e dall'inverso della restrizione di B. D'altra parte vale
$$f_i|_{X_B} = (\varphi|_{X_B})^* \left(\frac{a_i|_{Y_b}}{b_i|_{Y_b}}\right)$$
per ogni i, e
$$\frac{1}{B|_{X_B}} = (\varphi|_{X_B})^* \left(\frac{1}{b|_{Y_b}}\right),$$
dove tutte le funzioni fra parentesi sono in $\mathcal{O}(Y_b)$. Segue che $(\varphi|_{X_B})^*$ è un isomorfismo fra $\mathcal{O}(X_B)$ e $\mathcal{O}(Y_b)$, per cui basta porre $U' = X_B$ e $V' = Y_b$. $\square$

A.5. **Applicazioni regolari finite.** Sia $\varphi\colon X \to Y$ un'applicazione regolare fra varietà affini. L'immagine di φ non è necessariamente un sottoinsieme localmente chiuso di Y, come mostra l'esempio seguente.

Esempio A.26. Sia $\varphi\colon \mathbb{C}^2 \to \mathbb{C}^2$ l'applicazione regolare $\varphi(x, y) = (x, xy)$. La sua immagine è costituita da $(0, 0) = \varphi(0, *)$, e tutti i punti del tipo $(a, b) = \varphi(a, b/a)$ con $a \neq 0$. Non si tratta di un sottoinsieme localmente chiuso.

Introduciamo una classe importante di applicazioni regolari, che si comportano bene sotto questo punto di vista.

Definizione A.27. Sia $\varphi\colon X \to Y$ un'applicazione regolare, e si consideri l'applicazione $\varphi^*\colon \mathcal{O}(Y) \to \mathcal{O}(X)$. Se esistono elementi $f_1, \dots, f_m \in \mathcal{O}(X)$ tali che
$$\mathcal{O}(X) = \sum_{i=1}^{m} \varphi^*(\mathcal{O}(Y)) \cdot f_i,$$
allora φ si dice *finita*.

Un altro modo di formulare la stessa condizione è dire che $\mathcal{O}(X)$ è un $\varphi^*(\mathcal{O}(Y))$*-modulo finito.*

Esempio A.28. L'applicazione $\mathbb{C} \to \mathbb{C}$ che manda x in x^2 è finita, infatti $\varphi^*(\mathcal{O}(\mathbb{C}))$ è $\mathbb{C}[x^2]$ dentro $\mathcal{O}(\mathbb{C}) = \mathbb{C}[x]$, e abbiamo
$$\mathcal{O}(X) = \mathbb{C}[x] = \mathbb{C}[x^2] \cdot 1 + \mathbb{C}[x^2] \cdot x.$$

Teorema A.29. *Sia $\varphi\colon X \to Y$ applicazione regolare finita fra varietà affini. Allora φ è chiusa.*

Per la dimostrazione abbiamo bisogno di un risultato preliminare, di natura puramente algebrica. È una conseguenza del *Lemma di Nakayama*, e di fatto semplicemente un'applicazione della matrice dei cofattori di una matrice.

Lemma A.30. *Siano $B = \mathcal{O}(X)$ e $A = \varphi^*(\mathcal{O}(Y))$ come nel Teorema A.29. Sia $I \subsetneq A$ un ideale proprio di A. Allora IB è un ideale proprio di B.*

Dimostrazione. Supponiamo per assurdo che $IB = B$, e siano $f_1, \ldots, f_m \in \mathcal{O}(X)$ come nella Definizione A.27. Allora esistono elementi $a_{i,j} \in I$ tali che

$$f_i = \sum_{j=1}^{m} a_{i,j} f_j$$

per ogni i, cioè

$$\sum_{j=1}^{m} (a_{i,j} - \delta_{i,j}) f_j = 0,$$

che possiamo anche scrivere come

$$R \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} = 0$$

dove R è la matrice $(a_{i,j} - \delta_{i,j})_{i,j \in \{1,\ldots,m\}}$. Sia ora $K = (c_{i,j})_{i,j\in\{1,\ldots,m\}}$ la matrice dei cofattori di R. Moltiplicando K a sinistra nell'espressione qui sopra, otteniamo $\det(R) \cdot f_i = 0$ per ogni i, da cui otteniamo $\det(R) \cdot B = 0$.

Per come è fatta la matrice R, abbiamo che $\det(R)$ si può scrivere come[14] $\det(R) = 1 + a$ dove $a \in I$. Segue che $(1 + a)B = 0$, cioè $b = -ab$ per ogni $b \in B$. Applicata a $1 \in B$, otteniamo $1 \in I$, cioè I non è un ideale proprio di A. Assurdo. □

Dimostrazione del Teorema A.29. Sia $Z \subseteq X$ un chiuso, e consideriamo la restrizione $\psi = \varphi|_Z : Z \to Y' = \overline{\varphi(Z)}$. Allora $\psi^*\colon \mathcal{O}(Y') \to \mathcal{O}(Z)$ è iniettiva, ed è indotta da $\varphi^*\colon \mathcal{O}(Y) \to \mathcal{O}(X)$ sui due quozienti $\mathcal{O}(Y') = \mathcal{O}(Y)/I_Y(Y')$ e $\mathcal{O}(Z) = \mathcal{O}(X)/I_X(Z)$. Segue che ψ è finita.

Sia ora $y \in Y'$, sia $I = I_{Y'}(\{y\})$ l'ideale massimale corrispondente, e consideriamo $J = \psi^*(I)$, che è un ideale massimale di $\psi^*(\mathcal{O}(Y'))$. Le funzioni su Z che svaniscono su $\psi^{-1}(y)$ costituiscono l'ideale $J \cdot \mathcal{O}(Z)$ generato in $\mathcal{O}(Z)$ da Z. Per il Teorema A.29, l'ideale J è un ideale proprio, per cui $\psi^{-1}(y)$ è non vuota per il Nullstellensatz. □

Corollario A.31. *Sia $\varphi\colon X \to Y$ un'applicazione regolare fra varietà affini. Allora $\varphi(X)$ contiene un aperto denso della sua chiusura.*

Dimostrazione. Grazie alla Proposizione A.23, possiamo supporre che X sia irriducibile e non vuota. Allora si dimostra facilmente che $\varphi(X)$ e la sua chiusura $\overline{\varphi(X)}$ sono irriducibili. Possiamo quindi supporre che X e Y siano irriducibili, e che $Y = \overline{\varphi(X)}$. Identifichiamo allora anche $\mathcal{O}(Y)$ col sottoanello $\varphi^*(\mathcal{O}(Y))$ di $\mathcal{O}(X)$.

Visto che $\mathcal{O}(X)$ e $\mathcal{O}(Y)$ sono domini d'integrità, come abbiamo visto sono definiti i rispettivi campi delle frazioni $L = \mathbb{C}(X), K = \mathbb{C}(Y)$, ed L è un'estensione di K. Sia r il suo grado di trascendenza, e scegliamo $u_1, \ldots, u_r \in \mathcal{O}(X)$ elementi algebricamente indipendenti [15] su K. Cioè L contiene il campo $K(u_1, \ldots, u_r)$ delle funzioni razionali in r variabili a coefficienti in K. Consideriamo allora i seguenti anelli:

$$\mathcal{O}(X) \supseteq \mathcal{O}(Y)[u_1, \ldots, u_r] \supseteq \mathcal{O}(Y).$$

[14] Qui "1" vuol dire la funzione $X \to \mathbb{C}$ costante, con immagine $\{1\}$. Va fatta però una precisazione: questo ha senso solo se X è non vuota. Se invece X è vuota, allora l'anello $\mathcal{O}(X)$ è sempre ben definito ma contiene un solo elemento, l'applicazione vuota $\varnothing \to \mathbb{C}$. In questo caso consideriamo $\mathcal{O}(X)$ sempre come una $\mathbb{C}$-algebra: come spazio vettoriale è lo spazio vettoriale nullo, e come anello è l'anello con un solo elemento, che è un anello unitario ponendo $1 = 0$.

[15] Tali elementi esistono. Diamo un'idea della dimostrazione, lasciando i dettagli per esercizio. Primo passo: se ogni elemento di $\mathcal{O}(X)$ è algebrico su K, allora $\mathcal{O}(X)$ è un campo (perché?), quindi $L = \mathcal{O}(X)$ è algebrico su K, cioè $r = 0$. Per cui, se $r > 0$, allora esiste un elemento trascendente $u_1 \in \mathcal{O}(X)$ su K. Si prosegue allo stesso modo per trovare u_2 usando il campo $K(u_1)$ al posto di K, e così via.

L'anello $\mathcal{O}(Y)[u_1,\dots,u_r]$ è isomorfo all'anello dei polinomi in r variabili a coefficienti in $\mathcal{O}(Y)$, quindi è isomorfo all'anello $\mathcal{O}(Y\times\mathbb{C}^r)$. Le inclusioni qui sopra quindi corrispondono a fattorizzare φ come

$$X \stackrel{\psi}{\to} Y\times\mathbb{C}^r \stackrel{\rho}{\to} Y$$

dove la seconda applicazione è la proiezione sul primo fattore. Poniamo $Z = Y\times\mathbb{C}^r$.

Osserviamo che ogni elemento $f\in\mathcal{O}(X)$ è algebrico su $K(u_1,\dots,u_r)$, e si vede facilmente che allora esiste un $a\in\mathcal{O}(Y)[u_1,\dots,u_r]$ tale che af è integrale[16] su $\mathcal{O}(Y)[u_1,\dots,u_r]$.

Scegliamo ora $f_1,\dots,f_m$ generatori di $\mathcal{O}(X)$ come algebra, e scegliamo elementi $a_1,\dots,a_m\in\mathcal{O}(Y)[u_1,\dots,u_r]$ tali che a_if_i è integrale su $\mathcal{O}(Y)[u_1,\dots,u_r]$ per ogni i. Poniamo $F = a_1\dots a_m$, consideriamo l'aperto $Z' = (Y\times\mathbb{C}^r)_F$, l'aperto $X' = X_{\psi^*(F)}$, e la restrizione $\psi' = \psi|_{X'}\colon X'\to Z'$. Ricordiamo che abbiamo identificato K con un sottocampo di L, per cui possiamo identificare F con $\psi^*(F)$ e scrivere semplicemente $X' = X_F$ considerando le funzioni su uno spazio o su un altro a seconda del contesto.

Osserviamo che le funzioni a_i sono invertibili su Z' e su X', e questo implica che le funzioni $f_i|_{X'}$ sono integrali su $\mathcal{O}(Z')$. Inoltre entrambi gli anelli $\mathcal{O}(X')$ e $\mathcal{O}(Z')$ sono ottenuti rispettivamente da $\mathcal{O}(X)$ e $\mathcal{O}(Z)$ "invertendo" F. Mettendo insieme questi due fatti, concludiamo che ogni elemento di $\mathcal{O}(X')$ è integrale su $\mathcal{O}(Z')$. È facile allora concludere che ψ' è un'applicazione finita, per cui è chiusa. Essendo $\psi'(X')$ denso in Z', l'applicazione ψ' è suriettiva.

Quindi $\psi(X)$ contiene l'aperto $Z' = Z_F$ di Z, e rimane da dimostrare che $\rho(Z_F)$ contiene un aperto[17] denso di Y. Scriviamo

$$F = \sum F_{i_1,\dots,i_r} u_1^{i_1}\cdots u_r^{i_r}$$

dove $u_1,\dots,u_r$ sono le coordinate su $\mathbb{C}^r$, la somma è su $(i_1,\dots,i_r)\in(\mathbb{Z}_{\geq 0})^r$ e i coefficienti $F_{i_1,\dots,i_r}$ sono in $\mathcal{O}(Y)$. Allora vale

$$\rho(Z_F)\supseteq\bigcup Y_{F_{i_1,\dots,i_r}}$$

perché basta che in $y_0\in Y$ una delle funzioni $F_{i_1,\dots,i_r}$ sia non nulla, perché esistano valori $\tau_1,\dots,\tau_r\in\mathbb{C}$ tali che $F(y_0,\tau_1,\dots,\tau_r)\neq 0$ (esercizio).

Quindi abbiamo dimostrato che $\varphi(X)$ contiene un aperto non vuoto di Y. Infine, visto che Y è irriducibile, ogni aperto non vuoto è denso. □

A.6. **Applicazioni regolari genericamente biiettive.** Grazie al Corollario A.31 possiamo dimostrare alcuni risultati utili riguardo ad applicazioni regolari che sono biiettive se ristrette ad aperti densi.

Lemma A.32. *Sia Y una varietà affine irriducibile, e sia $p(z)$ un polinomio monico a coefficienti in $\mathcal{O}(Y)$, irriducibile come elemento di $\mathbb{C}(Y)[z]$. Sia inoltre $W\subseteq Y\times\mathbb{C}$ definito dall'equazione $p(z)=0$. Allora W è irriducibile, e il suo ideale in $\mathcal{O}(Y\times\mathbb{C})$ è generato da $p(z)$.*

Dimostrazione. Dimostriamo che l'ideale $I = I_{Y\times\mathbb{C}}(W)$ in $\mathcal{O}(Y\times\mathbb{C}) = \mathcal{O}(Y)[z]$ è primo. Siano $f_1(z), f_2(z)$ elementi di $\mathcal{O}(Y)[z]$ tali che $f_1(z)f_2(z)$ si annulla su W. Per il Nullstellensatz, una potenza positiva $f_1(z)^df_2(z)^d$ è divisibile per $p(z)$ in $\mathcal{O}(Y)[z]$. Visto che $p(z)$ è monico, possiamo eseguire la divisione con resto di $f_i(z)$ per $p(z)$ in $\mathcal{O}(Y)[z]$, ottenendo $f_i(z) = p(z)q_i(z) + r_i(z)$ con $r_i(z)$ un polinomio in z di grado minore di $p(z)$. Esprimendo f_i in questo modo e svolgendo il prodotto $f_1(z)^df_2(z)^d$, si vede subito che $r_1(z)^dr_2(z)^d$ è divisibile per $p(z)$ in $\mathcal{O}(Y)[z]$. Lo stesso allora vale in $\mathbb{C}(Y)[z]$, in cui però $p(z)$ è un elemento primo, quindi divide $r_1(z)$ o $r_2(z)$. Ma hanno entrambi grado strettamente minore di $p(z)$, per cui almeno uno fra $r_1(z)$ e $r_2(z)$ è il polinomio nullo, quindi almeno uno fra $f_1(z)$ e $f_2(z)$ è divisibile per $p(z)$ in $\mathcal{O}(Y)[z]$.

Abbiamo dimostrato che I è un ideale primo, per cui $\mathcal{O}(W) = \mathcal{O}(Y\times\mathbb{C})/I$ è un dominio d'integrità, e W è irriducibile. Lo stesso ragionamento di prima, applicato al caso in cui f_1 è la funzione costante 1 e invece $f_2(z)$ si annulla su tutto W, dimostra che I è generato da $p(z)$. □

Proposizione A.33. *Sia $\varphi\colon X\to Y$ un'applicazione regolare fra varietà algebriche affini irriducibili. Supponiamo esistano aperti densi $U\subseteq X$ e $V\subseteq Y$ tali che $U = \varphi^{-1}(V)$ e tali che φ induce una*

[16] Cioè esiste un polinomio *monico* a coefficienti in $\mathcal{O}(Y)[u_1,\dots,u_r]$ che si annulla in af.

[17] La topologia di Zariski sul prodotto $Y\times\mathbb{C}^r$ in generale *non* è la topologia che otterremmo come topologia prodotto da quella di Zariski su Y e quella di Zariski su $\mathbb{C}^r$, quindi non possiamo concludere automaticamente che la proiezione è aperta.

biiezione $U \to V$. Allora φ^* induce un isomorfismo $\mathbb{C}(Y) \to \mathbb{C}(X)$ fra il campo dei quozienti di $\mathcal{O}(Y)$ e quello di $\mathcal{O}(X)$.

Dimostrazione. Osserviamo che φ^* è iniettiva nelle nostre ipotesi, per cui possiamo identificare $\mathcal{O}(Y)$ col sottoanello $\varphi^*(\mathcal{O}(Y))$ di $\mathcal{O}(X)$.

Procediamo per assurdo e supponiamo esista $f \in \mathbb{C}(X) \setminus \mathbb{C}(Y)$. Ragionando separatamente su numeratore e denominatore di f espressa come quoziente di elementi di $\mathcal{O}(X)$, possiamo anche assumere $f \in \mathcal{O}(X)$.

Consideriamo gli omomorfismi di anelli

$$\mathcal{O}(Y) \to \mathcal{O}(Y)[z] \to \mathcal{O}(X)$$

dove z è una variabile, il primo omomorfismo è l'inclusione naturale, e il secondo è dato da φ^* su $\mathcal{O}(Y)$, e manda la variabile z in f. Essi corrispondono a fattorizzare φ in

$$X \xrightarrow{\eta} Y \times \mathbb{C} \xrightarrow{\mu} Y$$

dove $\eta = \varphi \times f$, e μ è la proiezione sul primo fattore.

Se f è trascendente su $\mathbb{C}(Y)$, allora l'immagine di X in $Y \times \mathbb{C}$ è densa. Infatti, se soddisfacesse un'equazione del tipo $p(z) = 0$ dove $p(z)$ è un polinomio a coefficienti in $\mathcal{O}(Y)$, allora varrebbe $p(f) = 0$ in $\mathbb{C}(X)$, che contraddirebbe la trascendenza di f.

Dunque l'immagine di X in $Y \times \mathbb{C}$ contiene un aperto denso del codominio, e anche l'immagine di U ha la stessa proprietà. Ma questo è assurdo: se un aperto denso di $Y \times \mathbb{C}$ interseca una fibra della proiezione μ, la interseca in un numero infinito di punti, perché l'intersezione è un aperto non vuoto di una varietà del tipo $\{y\} \times \mathbb{C}$ dove $y \in Y$, e questa varietà è isomorfa a $\mathbb{C}$. Quindi $\varphi|_U$ non potrebbe essere iniettiva: assurdo.

Applicando questo ragionamento ad ogni $f \in \mathcal{O}(X)$, possiamo già concludere che l'estensione di campi $\mathbb{C}(X) \supseteq \mathbb{C}(Y)$ è algebrica. Ripercorrendo la dimostrazione del Corollario A.31, possiamo rimpiazzare Y con un aperto affine denso e X con la sua controimmagine (che per costruzione era a sua volta un aperto affine denso in X), e assumere che φ sia un'applicazione regolare finita. A meno di prendere l'aperto di Y ancora più piccolo e contenuto in V, possiamo assumere che φ sia anche iniettiva.

Ora riconsideriamo l'estensione $\mathbb{C}(X) \supseteq \mathbb{C}(Y)$. Visto che $\mathbb{C}(X)$ è finitamente generato come campo (ad esempio da un insieme finito di generatori di $\mathcal{O}(X)$ come algebra) l'estensione è finita. Possiamo supporre che questa estensione sia generata da un singolo elemento f, e possiamo anche assumere che $f \in \mathcal{O}(X)$ (esercizio). Cioè assumiamo che $\mathbb{C}(X)$ è isomorfo al campo $\mathbb{C}(Y)[z]/(p(z))$ dove $p(z)$ è il polinomio minimo di f. Ricordiamo che $p(z)$ è monico.

Sia F il prodotto dei denominatori dei coefficienti di $p(z)$, dove questi coefficienti sono espressi come frazioni di elementi di $\mathcal{O}(Y)$. Rimpiazzando Y con Y_F e X con X_F, possiamo assumere che $p(z)$ sia un polinomio a coefficienti in $\mathcal{O}(Y)$. Anche con questo cambiamento, l'applicazione φ rimane iniettiva e finita.

Consideriamo di nuovo le inclusioni di anelli di prima rispetto a questa scelta di f, e la corrispondente fattorizzazione di φ in $\mu \circ \eta$. Questa volta l'immagine di η non è densa in $Y \times \mathbb{C}$, bensì contenuta nel chiuso $W \subseteq Y \times \mathbb{C}$ di equazione $p(z) = 0$, dove z è la coordinata su $\mathbb{C}$. Per il lemma precedente, la varietà affine W è irriducibile, e il campo $\mathbb{C}(W)$ è isomorfo a $\mathbb{C}(Y)[z]/(p(z))$. Ma quindi η induce un isomorfismo fra $\mathbb{C}(X)$ e $\mathbb{C}(W)$, e dalla Proposizione A.25 deriva che $\eta(X)$ è denso in W.

D'altra parte anche $\eta \colon X \to W$ è un'applicazione finita, basta osservare che $\eta^*(\mathcal{O}(W))$ contiene $\varphi^*(\mathcal{O}(Y))$. Quindi $\eta \colon X \to W$ è suriettiva, e visto che φ è iniettiva ora su tutto X, allora $\mu|_W$ è iniettiva.

A questo punto possiamo concludere in modo simile al caso in cui f era trascendente, se dimostriamo il fatto seguente: Y contiene un aperto non vuoto tale che su di esso $\mu|_W$ ha tutte fibre che contengono esattamente d punti, dove $d > 0$ è il grado di $p(z)$. Dimostriamo questo fatto usando il polinomio D del Corollario 1.9.

Possiamo farlo perché il Teorema 1.7 vale anche per $R = \mathbb{Z}$, e il polinomio C della dimostrazione del Corollario 1.9 ha coefficienti in $\mathbb{Z}$, quindi il polinomio D ha effettivamente coefficienti in $\mathbb{Z}$. Allora si può usare lo stesso polinomio D ottenuto lì con qualsiasi campo di caratteristica zero. Il Corollario 1.9 assicura che D distingue se un polinomio ha radici multiple nella chiusura algebrica K di $\mathbb{C}(Y)$. Scriviamo

$$p(z) = z^d + a_1 z^{d-1} + \ldots + a_d$$

dove $a_i \in \mathcal{O}(Y)$ per ogni i. Visto che $p(z)$ è irriducibile in $\mathbb{C}(Y)[z]$, non ha zeri multipli[18] e quindi $D(a_1, \ldots, a_d)$ non è l'elemento nullo di K. Ma $D(a_1, \ldots, a_d)$ è un elemento di $\mathcal{O}(Y)$, quindi come funzione su Y non è costantemente nulla. Cioè la condizione $D(a_1, \ldots, a_d) \neq 0$ definisce un aperto non vuoto di Y, e si tratta dell'aperto non vuoto cercato. $\square$

Corollario A.34. *Sia $\varphi\colon X \to Y$ un'applicazione regolare fra varietà algebriche affini. Supponiamo siano dati aperti densi $U \subseteq X$ e $V \subseteq Y$, tali che $U = \varphi^{-1}(V)$ e tali che che $\varphi|_U$ è una biiezione $U \to V$. Allora esistono aperti densi $U' \subseteq X$ e $V' \subseteq Y$, tali che $\varphi|_{U'}$ è un isomorfismo $U' \to V'$.*

Dimostrazione. Riduciamo il corollario al caso in cui X e Y sono irriducibili. Per ogni componente irriducibile Y_i di Y esiste almeno una componente irriducibile X_i di X la cui immagine è densa in Y_i. Le intersezioni $V \cap Y_i$ e $U \cap X_i$ sono non vuote, e l'immagine di $U \cap X_i$ contiene un aperto denso V_i di $V \cap Y_i$. Prendiamo $U_i = \varphi^{-1}(V_i) \cap X_i$. Allora $\varphi(U_i) = V_i$, e visto che $U_i \subseteq U$ e $V_i \subseteq V$, allora $\varphi|_{U_i}\colon U_i \to V_i$ è biiettiva. Cioè X_i, Y_i, $\varphi|_{X_i}\colon X_i \to Y_i$, U_i (che è uguale a $(\varphi|_{X_i})^{-1}(V_i)$) e V_i soddisfano le nostre ipotesi.

Concludiamo che basta dimostrare il corollario per tutte le componenti irriducibili singolarmente; poi a meno di restringere gli aperti U_i' e V_i' trovati per ogni componente irriducibile, possiamo supporre che gli U_i' siano disgiunti, e basta porre U' uguale alla loro unione.

Supponiamo allora che X e Y siano irriducibili. Il corollario precedente assicura che φ^* induce un isomorfismo fra $\mathbb{C}(Y)$ e $\mathbb{C}(X)$, e a questo punto il corollario segue dalla Proposizione A.25. $\square$

Osservazione A.35. Le ipotesi $U = \varphi^{-1}(V)$ in entrambi gli ultimi due corollari sono superflue. Però senza quest'ipotesi la dimostrazione del Corollario A.33 sembrerebbe richiedere alcuni risultati sulla dimensione delle varietà irriducibili, non richiamati in queste note.

A.7. **Geometria algebrica proiettiva.** Lo *spazio proiettivo* $\mathbb{P}^n = \mathbb{P}^n_{\mathbb{C}}$ è dotato di topologia di Zariski, in cui i chiusi sono definiti dall'annullarsi di una famiglia di polinomi *omogenei* nelle variabili $x_0, \ldots, x_n$. Sono definiti in modo ovvio, e analogo al caso della geometria algebrica affine, i simboli $V_{\mathbb{P}^n}(I)$ dove $I \subseteq \mathbb{C}[x_0, \ldots, x_n]$ è un ideale omogeneo, $I_{\mathbb{P}^n}(X)$ dove $X \subseteq \mathbb{P}^n$ è un sottoinsieme, e X_f dove $X \subseteq \mathbb{P}^n$ è un sottoinsieme e $f \in \mathbb{C}[x_0, \ldots, x_n]$ è *omogeneo.*

Osservazione A.36. Il Nullstellensatz vale anche in $\mathbb{P}^n$, ma con una modifica essenziale. Infatti l'ideale I_1 generato da $x_1, \ldots, x_n \in \mathbb{C}[x_1, \ldots, x_n]$ è un ideale proprio, però in $\mathbb{C}^{n+1}$ ha solo l'origine come luogo degli zeri, per cui $V_{\mathbb{P}^n}(I_1) = \varnothing$.

La stessa osservazione vale per gli ideali I_d per ogni $d \geq 1$, definiti come

$$I_d = \bigoplus_{i=d}^{\infty} \mathbb{C}[x_0, \ldots, x_n]_d.$$

Teorema A.37. *Sia $I \subseteq \mathbb{C}[x_0, \ldots, x_n]$ un ideale omogeneo tale che $V_{\mathbb{P}^n}(I) = \varnothing$. Allora I contiene I_d per qualche $d \geq 1$.*

Dimostrazione. Il luogo degli zeri $V(I)$ di I in $\mathbb{C}^{n+1}$ è vuoto, oppure è $\{0\}$, altrimenti ci sarebbero punti di $\mathbb{P}^n$ che sono zeri comuni degli elementi di I. Se $V(I) = \varnothing$ allora $I = (1)$, quindi supponiamo che $V(I) = \{0\}$. Per il Nullstellensatz, per ogni i esiste un intero positivo d_i tale che $x_i^{d_i}$ è in I. Poniamo $D = \max\{d_i\}$, e consideriamo un monomio qualsiasi

$$x_0^{a_0} x_1^{a_1} \cdots x_n^{a_n}.$$

Se $a_0 + \ldots + a_n \geq (n+1)D$, allora almeno un a_i dev'essere $\geq D$, quindi dev'essere $\geq a_i$, e in questo caso il monomio è in I. Concludiamo che I contiene I_d con $d = (n+1)D$. $\square$

Definizione A.38. Una *varietà proiettiva* è un sottoinsieme chiuso di un qualche $\mathbb{P}^n$. Una *varietà quasi proiettiva* è un sottoinsieme localmente chiuso di un qualche $\mathbb{P}^n$.

---

[18]Ricordiamo perché. Se $p(z)$ avesse zeri multipli in K allora, lavorando in $K[z]$, avrebbe fattori in comune con la derivata $p'(z)$. Quindi $MCD(p(z), p'(z))$ non sarebbe 1. D'altronde il MCD fra due polinomi non dipende dal campo in cui lo calcoliamo, a patto che il campo contenga tutti i coefficienti. Cioè $MCD(p(z), p'(z))$ è lo stesso se lo calcoliamo in $\mathbb{C}(Y)[z]$ oppure in $K[z]$, quindi nel nostro caso $p(z)$ non potrebbe essere irriducibile in $\mathbb{C}(Y)[z]$.

Le funzioni regolari su un localmente chiuso $X \subseteq \mathbb{P}^n$ si definiscono in modo simile al caso quasi affine. Osserviamo che un polinomio nelle variabili $x_0, \dots, x_n$ non definisce una funzione su X, ma una funzione razionale omogenea di grado 0 invece sì, a patto che si possa esprimere come quoziente di due polinomi omogenei dove il denominatore non svanisce mai su X (questo è ben definito).

Definizione A.39. Sia $X \subseteq \mathbb{P}^n$ una varietà quasi proiettiva. L'anello $\mathcal{O}(X)$ delle *funzioni regolari* su X è definito come l'insieme delle funzioni $f\colon X \to \mathbb{C}$ tali che esiste un ricoprimento aperto $\{U_i\}$ di X e polinomi $a_i, b_i \in \mathbb{C}[x_0, \dots, x_n]$ omogenei dello stesso grado tali che per ogni indice i il polinomio b_i non abbia zeri su U_i, e

$$f|_{U_i} = \left.\frac{a_i}{b_i}\right|_{U_i}.$$

Osservazione A.40.
(1) Lo spazio proiettivo $\mathbb{P}^n$ contiene diverse "copie" di $\mathbb{C}^n$, basta porre una coordinata omogenea uguale ad 1. Si dimostra facilmente che, per una varietà quasi affine X dentro uno di questi $\mathbb{C}^n$, la Definizione A.39 per $\mathcal{O}(X)$ coincide con la Definizione A.9: in un verso, basta passare da un polinomio omogeneo in $x_0, \dots, x_n$ ad uno in n variabili ponendo una di esse uguale ad 1, nell'altro verso basta passare da un polinomio in n variabili ad uno omogeneo in $n+1$ variabili moltiplicando ogni monomio per una potenza opportuna della variabile mancante.
(2) Unendo il punto precedente con il Corollario A.11 (e la definizione generale che abbiamo dato di varietà affine), otteniamo che ogni varietà quasi proiettiva ammette un ricoprimento aperto fatto di varietà affini.

Definizione A.41. Siano X, Y varietà quasi proiettive. Un'applicazione $\varphi\colon X \to Y$ è *regolare* se esistono ricoprimenti aperti $\{U_i\}$ di X e $\{V_j\}$ di Y, fatti di varietà affini, tali che per ogni i l'immagine $\varphi(U_i)$ è contenuta in qualche V_j in modo che la restrizione $\varphi|_{U_i}\colon U_i \to V_j$ è un'applicazione regolare.

Il prodotto cartesiano di due varietà (quasi) proiettive è dotato naturalmente di struttura di varietà (quasi) proiettiva. Non è però così ovvio come per le varietà affini, e il punto fondamentale è costruire il prodotto $\mathbb{P}^n \times \mathbb{P}^m$ identificandolo con una sottovarietà proiettiva di $\mathbb{P}^{nm}$.

Proposizione A.42. *Siano m, n interi positivi. L'applicazione*

$$\begin{array}{cccc} S\colon & \mathbb{P}^n \times \mathbb{P}^m & \to & \mathbb{P}^{(n+1)(m+1)-1} \\ & ([x_0, \dots, x_n], [y_0, \dots, y_m]) & \mapsto & [x_0y_0, x_1y_0, \dots, x_ny_0, x_0y_1, \dots, x_ny_1, \dots, x_ny_m] \end{array}$$

è una biiezione con la sua immagine, che è un chiuso di Zariski.

Dimostrazione. Denotiamo le coordinate omogenee su $\mathbb{P}^{(n+1)(m+1)-1}$ come $z_{i,j}$, con $i \in \{0, \dots, n\}$ e $j \in \{0, \dots, m\}$. Allora è facile dimostrare che l'immagine di S è il chiuso definito dalle equazioni $z_{i,j}z_{r,s} = z_{i,s}z_{r,j}$ per ogni i, j, r, s. □

L'applicazione S della proposizione prende il nome di *immersione di Segre*.

Esercizio A.43.
(1) Completare i dettagli della dimostrazione della proposizione precedente.
(2) Siano $X \subseteq \mathbb{P}^n$ e $Y \subseteq \mathbb{P}^m$ sottoinsiemi localmente chiusi (quindi varietà quasi proiettive). Dimostrare che $S(X \times Y)$ è localmente chiuso in $\mathbb{P}^{(n+1)(m+1)-1}$, quindi è una varietà quasi proiettiva.