GRUPPI E LORO AZIONI

1. Azioni e rappresentazioni

Siano G un gruppo e S un insieme. Si dice che G *agisce a sinistra su* S se vi è una applicazione

$$\sigma : G \times S \to S$$

dove, per semplicità si scriverà sempre

$$\sigma((g,x)) = g \cdot x\,,$$

o anche

$$\sigma((g,x)) = gx\,,$$

tale che

$$1x = x\,, \quad (gh)x = g(hx)\,, \quad \forall\, x \in S\,, \quad \text{and} \quad \forall\, g,h \in G\,.$$

Si dice invece che G *agisce a destra su* S se vi è una applicazione

$$\sigma : S \times G \to S$$

con

$$\sigma((g,x)) = xg\,,$$

tale che

$$x1 = x\,, \quad x(gh) = (xg)h\,, \quad \forall\, x \in S\,, \quad \text{and} \quad \forall\, g,h \in G\,.$$

In ogni caso, un insieme S su cui agisce un gruppo G si dice un G*-insieme.* Dato un insieme S indicheremo con il simbolo $\mathfrak{S}(S)$ il *gruppo delle permutazioni* di S, ovvero il gruppo delle applicazioni biunivoche di S in sé dotato del prodotto di composizione. Quando $S = \{1,2,\dots,n\}$, scriveremo, come d'uso:

$$\mathfrak{S}(\{1,2,\dots,n\}) = \mathfrak{S}_n$$

Esercizio 1.1. Mostrare che dare una azione sinistra di G su S equivale a dare un omomorfismo di gruppi $\varphi : G \to \mathfrak{S}(S)$.

Esercizio 1.2. Sia G un gruppo. Mostrare che il prodotto $G \times G \to G$ è un'azione sia destra che sinistra di G in sé.

Dati un gruppo G ed un insieme S, esiste una corrispondenza naturale tra azioni destre e sinistre di G su S. Infatti per ogni azione sinistra $G \times S \xrightarrow{\cdot} S$, l'applicazione

$$S \times G \to S, \qquad (s,g) \mapsto g^{-1} \cdot s,$$

è un'azione destra. Viceversa se $S \times G \xrightarrow{*} S$ è un'azione destra, allora l'applicazione

$$G \times S \to S, \qquad (g,s) \mapsto s * g^{-1},$$

è un'azione sinistra.

Quindi, dal punto di vista della teoria astratta, azioni destre e sinistre sono del tutto intercambiabili: nei casi concreti bisogna però fare attenzione a tale caratteristica, soprattutto se siamo in presenza di più azioni contemporaneamente.

Definizione 1.3. Siano G un gruppo e V uno spazio vettoriale. Una *rappresentazione* di G su V è un'azione sinistra $G \times V \to V$ tale che per ogni $g \in G$ l'applicazione

$$V \to V, \qquad v \mapsto gv,$$

è lineare.

Università di Roma 1: a.a. 2007-08, corso di Geometria Analitica, E.A., M.M. e A.F.

Esercizio 1.4. Sia $\mathbb{K}$ un campo. Mostrare che dare una rappresentazione di G su $\mathbb{K}^n$ equivale a dare un omomorfismo di gruppi $\varphi : G \to GL(n, \mathbb{K})$.

Esempio 1.5. $\mathbb{K}$ un campo, V uno $\mathbb{K}$-spazio vettoriale di dimensione finita. Allora il gruppo $G = GL(V)$ degli isomorfismi lineari di V agisce a sinistra su V, e l'azione è data da:

$$(T, v) \mapsto Tv, \qquad T \in GL(V),\ v \in V.$$

È inoltre tautologicamente vero che si tratta di una rappresentazione di $GL(V)$ su V.

Esempio 1.6. Siano $\mathbb{K}$ un campo e V uno $\mathbb{K}$-spazio vettoriale di dimensione finita e $PGL(V)$ il quoziente di $GL(V)$ per il sottogruppo dei multipli dell'identità. Allora $PGL(V)$ agisce a sinistra su $\mathbb{P}(V)$, con l'azione data da:

$$[T][v] = [Tv], \qquad T \in GL(V),\ [T] \in PGL(V),\ v \in V,$$

dove come al solito $[T]$ denota la proiezione di T al quoziente.

Esempio 1.7 (Coniugio)**.** Sia $G = GL(n, \mathbb{K})$ e sia $S = M_{n,n}(\mathbb{K})$, si definisce l'azione sinistra di coniugio: $(T, A) \mapsto TAT^{-1}$ e quella destra: $(A, T) \mapsto T^{-1}AT$. In modo più intrinseco si può dire che $GL(n, \mathbb{K})$ agisce su $M_{n,n}(\mathbb{K})$ a destra, e a sinistra, per coniugio.

Esempio 1.8 (Congruenza)**.** Sia $G = GL(n, \mathbb{K})$ e $S = M_{n,n}(\mathbb{K})$, allora si può definire una azione sinistra di G su S ponendo $(U, A) \mapsto UAU^T$ e una destra ponendo $(A, U) \mapsto U^TAU$. In modo più intrinseco si può dire che $GL(n, \mathbb{K})$ agisce su $M_{n,n}(\mathbb{K})$ a destra, e a sinistra, per congruenza.

Esempio 1.9. Il gruppo additivo $\mathbb{Z}$ agisce su $S = \mathbb{R}$ per traslazione: $(n, x) \mapsto x + n$.

Esempio 1.10. Il gruppo delle radici quarte dell'unità agisce per moltiplicazione sulle soluzioni complesse dell'equazione $z^{20} - 3 = 0$.

Esempio 1.11. Ogni gruppo G agisce per coniugio sull'insieme S i cui elementi sono i sottogruppi di G:

$$(g, H) \mapsto gHg^{-1}.$$

Esempio 1.12. Siano G un gruppo ed $H \subset G$ un sottogruppo. Allora G agisce a destra sull'insieme dei laterali destri $\{Hg \mid g \in G\}$ per moltiplicazione

$$(Hg, g') \mapsto Hgg'.$$

In maniera simile, G agisce a sinistra sull'insieme dei laterali sinistri $\{gH \mid g \in G\}$

$$(g, g'H) \mapsto gg'H.$$

2. Azioni indotte

Ogni azione induce in modo canonico e naturale altre azioni. Ad esempio, se G agisce su S, allora ogni sottogruppo di G agisce su S. Più in generale, se G agisce a sinistra su S, allora ogni omomorfismo di gruppi $\phi\colon H \to G$ induce un'azione

$$H \times S \to S, \qquad (h, s) \mapsto \phi(h) \cdot s.$$

Discorso del tutto simile se G agisce a destra. Se invece $\phi\colon H \to G$ è un *antiomomorfismo*, e cioè un'applicazione tale che $\phi(ab) = \phi(b)\phi(a)$, allora ogni azione sinistra di G induce un'azione destra di H e viceversa: i dettagli sono lasciati per esercizio.

Esempio 2.1. A volte, al posto di un gruppo G, si considera l'opposto di G e cioè il guppo G^o in cui la *nuova* moltiplicazione $a \cdot b$ è definita da $a \cdot b = ba$. Dunque l'identità su G è un antiomomorfismo di G^o su G, mentre l'applicazione $G^o \to G$, $g \mapsto g^{-1}$ è un isomorfismo. Abbiamo ritrovato il fatto che ad una azione sinistra di G^o corrisponde a una azione destra di G.

Esempio 2.2. Il gruppo $GL(n,\mathbb{R})$ agisce a sinistra su $\mathbb{R}^n$, di conseguenza anche i sottogruppi $O(n,\mathbb{R})$, e $SO(n,\mathbb{R})$ e $SL(n,\mathbb{R})$ agiscono su $\mathbb{R}^n$.

Esempio 2.3. Sia $S = Sym_{n,n}(\mathbb{R})$ lo spazio vettoriale delle matrici simmetriche a coefficienti reali, allora le azioni di congruenza e di coniugio di $GL(n,\mathbb{R})$ su $M_{n,n}(\mathbb{R})$ si restringono alle medesime azioni di $O(n,\mathbb{R}) \subset GL(n,\mathbb{R})$ su S. L'azione destra può scriversi nella forma

$$(T,A) \mapsto T^T AT = T^{-1}AT\,, \quad T \in O(n)\,, \quad A \in S\,.$$

In modo analogo, il gruppo unitario $U(n)$ agisce, per coniugio e congruenza, sull'insieme delle matrici hermitiane $H_{n,n}$.

Esempio 2.4. Sia $\mathbb{K} = \mathbb{R},\mathbb{C}$ e si consideri lo spazio proiettivo $\mathbb{P}^n_{\mathbb{K}}$; allora i punti dello spazio proiettivo

$$\mathbb{P}(Sym_{n+1,n+1}(\mathbb{K}\,)) \cong \mathbb{P}_{\mathbb{K}}^{\frac{(n+1)(n+2)}{2}-1}$$

sono (per definizione) in corrispondenza biunivoca con le quadriche in $\mathbb{P}^n_{\mathbb{K}}$. Se $[X_0,\dots,X_n]$ sono coordinate omogenee in $\mathbb{P}^n_K$, ad ogni punto $[A] \in \mathbb{P}(Sym_{n+1,n+1}(\mathbb{K}\,))$ si associa la quadrica:

$$Q_{[A]} : {}^tXAX = 0\,, \qquad X = (X_0,\dots,X_n)$$

e l'azione di $GL(n{+}1,\mathbb{K}\,)$ definisce, per passagio a quoziente, una azione di $\mathbb{P}GL(n{+}1,\mathbb{K}\,)$ su $\mathbb{P}_{\mathbb{K}}^{\frac{(n+1)(n+2)}{2}-1}$:

$$(Q_{[A]},[T]) \mapsto Q_{[{}^tTAT]}$$

Esempio 2.5. Se G agisce su S, allora agisce anche su tutti i prodotti cartesiani S^n, $n > 0$ come

$$g(s_1,\dots,s_n) = (gs_1,\dots,gs_n), \qquad g \in G, \quad s_1,\dots,s_n \in S.$$

Siccome per ogni $g \in G$ l'applicazione $g\colon S \to S$, $s \mapsto gs$, è iniettiva, il gruppo G agisce anche sul sottoinsieme

$$U = \{(s_1,\dots,s_n) \in S^n \mid s_i \neq s_j, \quad \forall\, i \neq j\}.$$

Esempio 2.6. Sia X un insieme fissato. Se G agisce a sinistra su un insieme S, allora G agisce a destra sull'insieme di tutte le applicazioni $f\colon S \to X$ tramite la formula

$$(f\sigma)(s) = f(\sigma s), \qquad s \in S, \quad f\colon S \to X.$$

Esempio 2.7. Sia X un insieme. Il gruppo simmetrico $\mathfrak{S}_n$ agisce a sinistra sull'insieme prodotto n-plo $X^n = X \times \cdots \times X$ (n-volte) ponendo

$$\sigma(x_1,x_2,\dots,x_n) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)},\dots,x_{\sigma^{-1}(n)})$$

Infatti, $\mathfrak{S}_n$ agisce tautologicamente a sinistra su $\{1,2,\dots,n\}$ e possiamo interpretare X^n come l'insieme di tutte le applicazioni $x\colon \{1,2,\dots,n\} \to X$. Per l'Esempio 2.6 esiste una naturale azione destra di $\mathfrak{S}_n$ su X^n,

$$(x_1,x_2,\dots,x_n)\sigma = (x_1,x_2,\dots,x_n) \circ \sigma = (x_{\sigma(1)}, x_{\sigma(2)},\dots,x_{\sigma(n)}).$$

Basta adesso trasformare nel modo standard tale azione destra in un'azione sinistra.

Esempio 2.8. Sia S un qualunque insieme, $\mathbb{K}$ un campo e V lo spazio vettoriale di tutte le applicazioni $v\colon S \to \mathbb{K}$. Esiste una rappresentazione naturale di $\mathfrak{S}(S)$ su V

$$\mathfrak{S}(S) \times V \to V, \qquad (\sigma,v) \mapsto= v \circ \sigma^{-1}.$$

Se $S = \{1,2,\dots,n\}$ allora $V = \{(x_1,\dots,x_n) \mid x_i \in \mathbb{K}\,\} = \mathbb{K}^{\,n}$ e la rappresentazione diventa

$$\mathfrak{S}_n \times \mathbb{K}^{\,n} \to \mathbb{K}^{\,n}, \qquad \sigma(x_1,\dots,x_n) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)},\dots,x_{\sigma^{-1}(n)}).$$

Esempio 2.9. I gruppi additivi $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ agiscono sull'insieme delle funzioni continue in $f\colon \mathbb{R} \to \mathbb{R}$ per traslazione

$$(r, f(x)) \mapsto f(x+r)$$

Esempio 2.10. Il gruppo simmetrico $\mathfrak{S}_n$ agisce a sinistra sull'anello $\mathbb{K}[x_1, \dots, x_n]$ mediante la formula:

$$\sigma \cdot p(x_1, x_2, \dots, x_n) \mapsto p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

Si noti che per i monomi di grado 1 vale $\sigma \cdot x_i = x_{\sigma(i)}$ e la relazione con l'azione destra naturale di $\mathfrak{S}_n$ su $\mathbb{K}^n$ (Esempio 2.6) è data dalla formula

$$(\sigma p)(a) = p(a \cdot \sigma), \qquad p \in \mathbb{K}[x_1, \dots, x_n], \quad a \in \mathbb{K}^n.$$

Esercizio 2.11. Sia A un insieme fissato. Se G agisce a destra su un insieme S, dimostrare che:

(1) G agisce a destra sull'insieme di tutte le applicazioni $f\colon A \to S$ tramite la formula
$$(f\sigma)(a) = f(a)\sigma, \qquad a \in A, \quad f\colon A \to S.$$
(2) G agisce a sinistra sull'insieme di tutte le applicazioni $f\colon S \to A$ tramite la formula
$$(\sigma f)(s) = f(s\sigma), \qquad s \in S, \quad f\colon S \to A.$$

3. Orbite e quozienti

Sia G un gruppo che agisce su di un insieme S. Si definisce allora *l'insieme quoziente di S per l'azione di G*, e lo si denota col simbolo S/G, ponendo

$$S/G = S/\sim$$

dove S è la relazione definita da:

$$\text{dati} \quad x\,, y \in S\,, \quad \text{allora} \quad x \sim y \quad \iff \quad \exists \quad g \in G\,, \quad \text{con} \quad y = gx\,.$$

Si verifica subito che $\sim$ è una relazione di equivalenza e che dunque ha buon senso parlare dell'insieme quoziente S/G. A volte si denota con il simbolo $[x]$, e altre volte con quello $\overline{x}$, la classe di equivalenza di x nel quoziente S/G. Dato $x \in S$, *l'orbita di x in S, per l'azione di G,* è il sottoinsieme

$$Gx = \{gx \in S \mid g \in G\} \subset S.$$

Dalla definizione segue subito che due orbite o coincidono o sono disgiunte. Non solo, è anche evidente che vi è una corrispondenza biunivoca tra l'insieme $O_G(S)$ delle orbite di S, per l'azione di G e l'insieme quoziente S/G:

$$O_G(S) \longrightarrow S/G$$
$$Gx \mapsto [x]$$

In definitiva, si ha dunque una decomposizione in unione disgiunta:

$$S = \bigcup_{[x] \in S/G} Gx$$

Esercizio 3.1. Trovare le orbite dell'azione di $GL(V)$ su V.

Esercizio 3.2. Trovare le orbite dell'azione del gruppo delle proiettività di $\mathbb{P}^2$ sul prodotto cartesiano $(\mathbb{P}^2)^3$.

Esempio 3.3. Abbiamo già osservato che per ogni insieme X il gruppo simmetrico $\mathfrak{S}_n$ agisce sul prodotto cartesiano X^n. Il quoziente di tale azione si denota $X^{(n)} = X^n/\mathfrak{S}_n$ e viene detto *prodotto simmetrico di X*.

Esercizio 3.4. Provare che esiste un'applicazione surgettiva $X^{(n)} \to F$, dove F è la famiglia di tutti i sottoinsiemi di X con d elementi, $1 \leq d \leq n$.

Esempio 3.5. Si consideri una permutazione $\sigma \in \mathfrak{S}_n$ e il sottogruppo $< \sigma > \subset \mathfrak{S}_n$ da essa generato:

$$< \sigma >= \{\sigma^i \mid i \in \mathbb{Z}\}$$

Allora i *cicli di* σ non sono altro che le orbite di $< \sigma >$ nella sua azione su $\{1, 2, \dots, n\}$.

Esempio 3.6. Siano V un $\mathbb{K}$-spazio vettoriale e F_k l'insieme delle k-ple di vettori linearmente indipendenti di V e si consideri l'azione

$$F_k \times GL(k, \mathbb{K}) \longrightarrow F_k$$
$$(\mathbf{e}, T) \mapsto \mathbf{e}T\,, \qquad \mathbf{e} = (e_1, \dots, e_k)$$

L'insieme quoziente $F_k/GL(k, \mathbb{K})$ si denota con il simbolo $Gr(k, V)$ e prende il nome di *Grassmanniana dei sottospazi k-dimensionali di V*. I suoi punti sono in corrispondenza biunivoca con i sottospazi k-dimensionali di V.

Definizione 3.7. Un gruppo G si dice agire *transitivamente* su di un insieme S se, in questa azione, vi è un'unica orbita, con il che S/G si riduce a un solo punto. In questo caso si dice che S è uno *spazio omogeneo* per l'azione di G.

Esempio 3.8. Sia V uno spazio vettoriale reale equipaggiato di prodotto scalare. Sia $n = \dim V$ e sia k un intero positivo minore o uguale a d. Allora il gruppo $O(n)$ agisce transitivamente sull'insieme FO_k delle k-ple di vettori ortonormali di V.

Sia S un G-insieme. I punti di S per cui $gs = s$ per ogni $g \in G$ si dicono i *punti fissi* o *punti invarianti* dell'azione di G su S.

Più in generale un sottoinsieme $A \subset S$ si dice un *sottospazio invariante* dell'azione di G se $ga \in A$ per ogni $g \in G$ ed ogni $a \in A$.

Esempio 3.9. Ogni multiplo dell'identità è un punto fisso per l'azione di coniugio di $GL(n, \mathbb{K})$ sull'insieme delle matrici $M_{n,n}(\mathbb{K})$. L'insieme delle matrici nilpotenti è un sottospazio invariante per la medesima azione.

Esempio 3.10. I polinomi simmetrici si definiscono come gli invarianti dell'azione di $\mathfrak{S}_n$ sull'anello dei polinomi $\mathbb{K}[x_1, \dots, x_n]$ descritta nell'Esempio 2.10.

Sia S un G-insieme. Abbiamo visto che per ogni insieme X il gruppo G agisce sull'insieme $\mathrm{Fun}(S, X)$, delle funzioni su S a valori in X, ponendo

$$(g \cdot f)(s) = f(g^{-1}s).$$

Gli invarianti di questa azione si chiamano *funzioni invarianti per l'azione di G su S*. Dunque, una funzione

$$f : S \longrightarrow X \tag{1}$$

è invariante se

$$f(g^{-1}s) = f(s)\,, \qquad \forall\, g \in G\,, \quad \forall\, s \in S$$

Naturalmente, una funzione invariante (1), induce un'applicazione

$$\overline{f} : S/G \to X$$

definita da $\overline{f}([s]) = f(s)$.

Esempio 3.11. Il determinante e la traccia sono funzioni invarianti

$$\det\,,\ \mathrm{Tr}\ :\ M_{n,n}(\mathbb{K}) \longrightarrow \mathbb{K}$$

per l'azione di coniugio di $GL(n, \mathbb{K})$ su $M_{n,n}(\mathbb{K})$.

Esercizio 3.12. Sia $f \in \mathbb{C}[x_1, \ldots, x_n]$ un polinomio simmetrico e denotiamo con

$$\sigma_f : M_{n,n}(\mathbb{C}) \longrightarrow \mathbb{C}$$

la funzione definita da

$$\sigma_f(A) = f(\lambda_1, \ldots, \lambda_n)$$

dove $\lambda_1, \ldots, \lambda_n$ sono gli autovalori di A. Dimostrare che $\sigma_f(A)$ è ben definita e che è una funzione invariante per l'azione di coniugio di $GL(n, \mathbb{C})$ su $M_{n,n}(\mathbb{C})$.

Definizione 3.13. Un insieme di funzioni invarianti $f_i : S \to X$, $i = 1, \ldots, N$, si dice un *sistema completo di invarianti per l'azione di G su S*, se:

$$s, t \quad \text{stanno nella stessa orbita} \qquad \Longleftrightarrow \qquad f_i(s) = f_i(t)\,,\ i = 1, \ldots, N\,.$$

Esempio 3.14 (L'invariante j)**.** In quanto segue $\mathbb{K}$ è un campo di caratteristica diversa da 2 e 3. Il gruppo simmetrico $\mathfrak{S}_3$ agisce su

$$U = \{(x_1, x_2, x_3) \in \mathbb{K}^3 \mid x_i \neq x_j \text{ per ogni } i \neq j\}$$

ed è un semplice esercizio dimostrare che, dati tre punti distinti $x_1, x_2, x_3 \in \mathbb{K}$, il rapporto

$$\frac{x_{\sigma(3)} - x_{\sigma(1)}}{x_{\sigma(2)} - x_{\sigma(1)}}$$

dipende solamente da σ e da

$$\lambda = \frac{x_3 - x_1}{x_2 - x_1} \in \mathbb{K} - \{0, 1\}.$$

Basta infatti osservare che

$$\frac{x_2 - x_1}{x_3 - x_1} = \frac{1}{\lambda}, \qquad \frac{x_3 - x_2}{x_1 - x_2} = 1 - \frac{x_3 - x_1}{x_2 - x_1} = 1 - \lambda,$$

e che le due trasposizioni $(1, 3, 2)$ e $(2, 1, 3)$ generano il gruppo delle permutazioni su tre elementi. Esiste quindi un'azione di $\mathfrak{S}_3$ su $\mathbb{K} - \{0, 1\}$ tale che

$$(1, 3, 2)\lambda = \lambda^{-1}, \qquad (2, 1, 3)\lambda = 1 - \lambda.$$

L'orbita di λ è data dall'insieme dei valori

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

Definiamo l'applicazione

$$j \colon \mathbb{K} - \{0, 1\} \to \mathbb{K}\,, \qquad j(\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

Un semplice conto, lasciato per esercizio, mostra che $j(\lambda) = j(\lambda^{-1}) = j(1 - \lambda)$ e quindi che è una funzione invariante.

Teorema 3.15. *La funzione j è un invariante completo per l'azione di $\mathfrak{S}_3$ su $\mathbb{K} - \{0, 1\}$.*

Dimostrazione. (solo idea: dettagli per esercizio) Sia $j \in \mathbb{K}$ fissato e sia λ una radice del polinomio di grado 6

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

Basta dimostrare che le radici di $f(x)$ sono tutte e sole

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

o equivalentemente che

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

Si tratta di un conto un po' laborioso ma che non presenta alcuna difficoltà. □

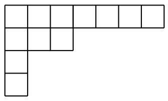


FIGURA 1. Diagramma di Young della partizione di 12 data da $(7, 3, 1, 1)$.

Esempio 3.16. Sia S la famiglia di tutti i sottoinsiemi di quattro punti distinti di $\mathbb{P}^1$. Il gruppo $\mathrm{Aut}(\mathbb{P}^1)$ delle proiettività di $\mathbb{P}^1$ agisce su S:

$$\phi \cdot \{a, b, c, d\} = \{\phi(a), \phi(b), \phi(c), \phi(d)\}, \qquad \phi \in \mathrm{Aut}(\mathbb{P}^1), \quad \{a, b, c, d\} \in S.$$

Definiamo

$$j(\{a, b, c, d\}) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}, \quad \text{dove} \quad \lambda = [a, b, c, d] \quad \text{birapporto.}$$

Scambiando l'ordine dei quattro punti a, b, c, d il birapporto assume i sei valori

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

e per quanto visto nell'Esempio 3.14 ne segue che $j(\{a, b, c, d\})$ è ben definito. Il Teorema 3.15 ci dice che due quaterne hanno lo stesso invariante j se a meno di permutazioni hanno lo stesso birapporto. Quindi j è un invariante completo per l'azione di $\mathrm{Aut}(\mathbb{P}^1)$ su S .

4. Forma canonica delle applicazioni nilpotenti

Definizione 4.1. Una *partizione* di un numero intero positivo n è una successione $a_0, a_1, \ldots, a_k, \ldots \in \mathbb{N}$ tale che $a_i \geq a_{i+1}$ per ogni $i \geq 0$ e $\sum_{i=0}^{\infty} a_i = n$ (si noti che necessariamente $a_i = 0$ per ogni $i \geq n$).

Per semplicità notazionale, spesso per scrivere una partizione si omettono i termini nulli: avremo quindi che (4), $(3, 1)$, $(2, 2)$, $(2, 1, 1)$ e $(1, 1, 1, 1)$ sono tutte e sole le partizioni di 4.

Il modo standard di visualizzare le partizioni è mediante i cosiddetti *diagrammi di Young*. Il diagramma di Young della partizione $(a_0, a_1, \ldots)$ è per definizione uno schema vuoto[1] di righe e colonne incrociate, a forma di scala, in cui la prima riga è costituita da a_0 quadretti, la seconda riga da a_1 quadretti, e così via, vedi Figura 1.

Scambiando righe e colonne di un diagramma di Young troviamo un'altra partizione, detta *partizione duale*. Ad esempio, la duale di $(7, 3, 1, 1)$ è (vedi Figura 1) $(4, 2, 2, 1, 1, 1, 1)$.

In altri termini, una partizione $(b_0, b_1, \ldots)$ è la duale di $(a_0, a_1, \ldots)$ se b_i è uguale al numero degli indici j tali che $a_j > i$.

Esercizio 4.2. Qual è la partizione duale di $(6, 4, 2, 1, 1)$? La risposta è a pagina 10.

Se V è uno spazio vettoriale di dimensione finita n ed $f \colon V \to V$ è un'applicazione lineare nilpotente, poniamo per convenzione $f^0 = Id$ e

$$a_0 = n - \mathrm{rank}(f), a_1 = \mathrm{rank}(f) - \mathrm{rank}(f^2), \ldots, a_i = \mathrm{rank}(f^i) - \mathrm{rank}(f^{i+1}), \ldots$$

Allora la successione $a_0, a_1, \ldots$ è è una partizione di n. Infatti per Cayley-Hamilton si ha $a_n = 0$ e segue immediatamente dalla definizione che $a_0 + a_1 + \cdots + a_{n-1} = n$. Per dimostrare che $a_i \geq a_{i+1}$ per ogni i osserviamo che l'applicazione

$$f \colon f^i(V) \to f^{i+1}(V)$$

[1] Qualora, per qualsivoglia motivo, tale schema venga riempito con numeri, lettere ecc. si ha un *tableau di Young*.

è surgettiva ed ha come nucleo $\ker f \cap f^i(V)$. Dunque $a_i = \dim(\ker f \cap f^i(V))$ per ogni i e, siccome $f^{i+1}(V) \subset f^i(V)$, a maggior ragione

$$\ker f \cap f^{i+1}(V) \subset \ker f \cap f^i(V)$$

e quindi $a_i \geq a_{i+1}$.

Sia V uno spazio vettoriale di dimensione n su di un campo $\mathbb{K}$ e sia $\mathcal{N}$ l'insieme di tutti le applicazioni nilpotenti $f\colon V \to V$. Il gruppo degli isomorfismi di V in sé agisce per coniugio su $\mathcal{N}$. Se $f_1, f_2 \in \mathcal{N}$ sono coniugate, allora anche f_1^k è coniugato a f_2^k per ogni $k \geq 0$ ed in particolare f_1^k ha lo stesso rango di f_2^k.

Abbiamo quindi dimostrato che due applicazioni nilpotenti coniugate danno luogo alla stessa partizione di n. Nel resto di questa sezione dimostreremo che vale anche il viceversa, ossia che se due applicazioni nilpotenti danno luogo alla stessa partizione di n, allora sono coniugate.

Definizione 4.3. Siano V uno spazio vettoriale e $f\colon V \to V$ nilpotente. Diremo che $v_1, \dots, v_k \in V$ sono *generatori ciclici* di V rispetto ad f se tutti i vettori non nulli della forma $f^i(v_j)$, con $i = 0, 1, 2, \dots$ e $j = 1, \dots, k$ formano una base di k.

Lemma 4.4. *Siano V uno spazio vettoriale, $f\colon V \to V$ nilpotente e $v_1, \dots, v_k \in V$ generatori ciclici di V rispetto ad f. Allora $k = \dim \ker(f)$.*

Dimostrazione. Denotiamo con b_i l'indice di nilpotenza di v_i, ossia il più piccolo intero tale che $f^{b_i}(v_i) = 0$, allora ogni elemento di $u \in V$ si scrive in modo unico come combinazione lineare

$$u = \sum_{j=1}^{k} \sum_{i=0}^{b_j - 1} a_{ij} f^i(v_j), \qquad a_{ij} \in \mathbb{K},$$

e dunque

$$f(u) = \sum_{j=1}^{k} \sum_{i=0}^{b_j - 2} a_{ij} f^{i+1}(v_j)$$

si annulla se e solo se $a_{ij} = 0$ per ogni $i \leq b_j - 2$. Dunque $f^{b_1 - 1}(v_1), \dots, f^{b_k - 1}(v_k)$ è una base di $\ker(f)$. $\square$

Teorema 4.5. *Siano V uno spazio vettoriale di dimensione n e $f\colon V \to V$ nilpotente. Allora esiste un insieme di generatori ciclici di V rispetto ad f.*

Dimostrazione. Il teorema è banalmente vero se $f = 0$: in tal caso ogni base di V è anche un sistema di generatori ciclici. Dimostriamo il teorema per induzione su n: se $n = 1$ allora $f = 0$.

Sia $k = \dim \ker(f)$. Per l'ipotesi induttiva esistono $u_1, \dots, u_s \in f(V)$ che sono generatori ciclici del sottospazio $f(V)$ rispetto ad f. Abbiamo già osservato che $s = \dim(\ker f \cap f(V))$. Siano dunque $v_1, \dots, v_s \in V$ tali che $f(v_i) = u_i$, scegliamo una decomposizione in somma diretta

$$\ker(f) = H \oplus (\ker f \cap f(V))$$

ed una base $v_{s+1}, \dots, v_k$ di H. Vogliamo dimostrare che $v_1, \dots, v_k$ sono generatori ciclici di V. Dato che $v_{s+1}, \dots, v_k \in \ker(f)$, e che gli elementi non nulli della forma $f^i(u_j)$ sono esattamente $n - k$, ne segue che gli elementi non nulli della forma $f^i(v_j)$ sono esattamente n. Basta dunque dimostrare che essi generano v.

Sia dunque $v \in V$; possiamo scrivere

$$f(v) = \sum_{j=1}^{s} \sum_{i \geq 0} a_{ij} f^{i+1}(v_j), \qquad a_{ij} \in \mathbb{K},$$

e quindi
$$u = v - \sum_{j=1}^{s} \sum_{i \geq 0} a_{ij} f^i(v_j) \in \ker(f).$$
D'altra parte ogni elemento di $\ker(f)$ è la somma di una combinazione lineare di $v_{s+1}, \ldots, v_k$ e di un elemento dell'immagine di f, che per ipotesi si può scrivere come combinazione lineare dei $f^i(v_j)$. $\square$

È chiaro dalla dimostrazione che i generatori ciclici non sono univocamante determinati da f: tuttavia sono univocamente determinati i loro indici. Abbiamo infatti:

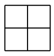
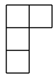
Proposizione 4.6. *Siano V uno spazio vettoriale, $f\colon V \to V$ nilpotente con partizione associata $(a_0, a_1, \ldots)$ e $v_1, \ldots, v_k \in V$ generatori ciclici di V rispetto ad f. Si assuma che $b_1 \geq b_2 \geq \cdots \geq b_k > 0$, dove b_i indica l'indice di nilpotenza di v_i:*
$$a_i = \dim f^i(V) - \dim f^{i+1}(V), \qquad b_i = \min\{m > 0 \mid f^m(v_i) = 0\}.$$
Allora $(b_1, b_2, \ldots, b_k)$ è la partizione duale di $(a_0, a_1, \ldots)$.

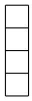
Dimostrazione. Costruiamo un diagramma di Young con k colonne di lunghezze $b_1, b_2, \ldots, b_k$ e facciamo corrispondere la casella (i, j) (riga $i \geq 0$, colonna j) al vettore $f^i(v_j)$. Per dimostrare che il numero di caselle della riga i è uguale alla differenza tra la dimensioni di $f^i(V)$ e $f^{i+1}(V)$ basta dimostrare che per ogni s il sottospazio $f^s(V)$ è generato dai vettori $f^i(v_j)$, con $i \geq s$. Sia $v \in f^s(V)$: possiamo allora scrivere $v = f^s(u)$, $u = \sum_{i \geq 0} a_{ij} f^i(v_j)$ e quindi
$$v = \sum_{i \geq s} a_{ij} f^i(v_j).$$
$\square$

Dato un insieme di generatori ciclici $v_1, \ldots, v_k$ di V rispetto ad f, con relativi indici di nilpotenza $b_1 \geq b_2 \geq \ldots b_k > 0$, la matrice che rappresenta f nella base
$$f^{b_k - 1}(v_k), \ldots, v_k, \ldots, f^{b_2 - 1}(v_2), \ldots, v_2, f^{b_1 - 1}(v_1), \ldots, v_1,$$
viene detta *forma canonica* di f e dipende solo dal diagramma di Young. Quindi *due endomosrfismi nilpotenti sono coniugati se e solo se hanno lo stesso diagramma di Young.*

Vediamo adesso tutte le forme canoniche delle applicazioni nilpotenti $\mathbb{K}^n \to \mathbb{K}^n$, per $n = 1, 2, 3, 4$.

$n = 1$
$$\ydiagram{1} \mapsto (0)$$
$n = 2$
$$\ydiagram{2} \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}; \qquad \ydiagram{1,1} \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
$n = 3$
$$\ydiagram{3} \mapsto \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \qquad \ydiagram{2,1} \mapsto \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$
$$\ydiagram{1,1,1} \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$
$n = 4$
$$\ydiagram{4} \mapsto \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \qquad \ydiagram{3,1} \mapsto \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

 $\mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$;  $\mapsto \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

 $\mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

Definizione 4.7. La matrice corrispondente al diagramma di Young con una sola colonna viene detta *blocco di Jordan nilpotente*. Geometricamente corrisponde ad un'applicazione nilpotente con un unico generatore ciclico.

È abbastanza evidente che la forma canonica di un'applicazione nilpotente è ottenuta mettendo blocchi di Jordan sulla diagonale principale.

Soluzione dell'Esercizio 4.2. $(5, 3, 2, 2, 1, 1)$.

5. Forma canonica di Jordan

Uno dei teoremi fondamentali dell'algebra lineare, il Teorema di Jordan, asserisce che ogni matrice $A \in M_{n,n}(\mathbb{C})$ è coniugata a una matrice della forma

$$J = \begin{pmatrix} J_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & J_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & J_3 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & J_{k+1} & 0 \\ 0 & 0 & 0 & \cdots & 0 & J_k \end{pmatrix}$$

dove ogni J_ν è un blocco di Jordan, e cioè una matrice $d_\nu \times d_\nu$ della forma

$$J_\nu = \begin{pmatrix} \lambda_\nu & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_\nu & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_\nu & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & \lambda_\nu & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_\nu \end{pmatrix}$$

dove, naturalmente, $n = \sum_{\nu=1}^{k} d_\nu$ e dove i numeri λ_ν sono gli autovalori di A (non necessariamente distinti). La matrice J prende il nome di *forma canonica di Jordan* della matrice A. Essa è completamente determinata da A, a meno di un eventuale riordino dei vari blocchi J_ν. Dunque le forme canoniche di Jordan, a meno di riordinamento dei loro blocchi, indicizzano le orbite dell'azione di coniugio di $GL(n, \mathbb{C})$ su $M_{n,n}(\mathbb{C})$. Si noti che $J + \lambda I$ è ancora una forma canonica di Jordan per ogni valore di $\lambda \in \mathbb{C}$.

Nella Sezione 4 abbiamo dimostrato che il Teorema di Jordan è vero per le applicazioni nilpotenti. Nel caso generale si ragiona per induzione su n. Se A possiede un solo autovalore, chiamiamolo λ, il polinomio caratteristico di A è $\pm(t - \lambda)^n$. Per Cayley-Hamilton, la matrice $B = A - \lambda I$ è nilpotente e quindi è coniugata ad una forma canonica di Jordan J. Dunque A è coniugata a $J + \lambda I$ che è ancora una forma canonica di Jordan.

Se A possiede almeno due autovalori distinti e $\lambda \in \mathbb{C}$ è uno di essi, allora l'applicazione $T = A - \lambda I$ non è invertibile e non è nilpotente. Siccome le immagini delle applicazioni T^m si stabilizzano per $m >> 0$, esiste un esponente $d > 0$ tale che $T^d \colon Im(T^d) \to Im(T^{2d})$ è iniettiva, ossia $\ker(T^d) \oplus Im(T^d) = 0$. Dalla Formula di Grassmann segue la decomposizione in somma diretta

$$\mathbb{C}^n = \ker(T^n) \oplus Im(T^n).$$

Siccome T commuta con A, i sottospazi $U = \ker(T^n)$ e $V = Im(T^n)$ sono entrambi A-invarianti, ossia $A(U) \subset U$ e $A(V) \subset V$. Per l'ipotesi induttiva le restrizioni di A ad U e V possiedono la forma canonica di Jordan.

Osservazione 5.1. Segue dalla dimostrazione che il teorema di Jordan vale su qualunque campo algebricamente chiuso, e più in generale che una matrice $A \in M_{n,n}(\mathbb{K})$ è coniugata ad una matrice di Jordan $J \in M_{n,n}(\mathbb{K})$ se e solo se il polinomio caratteristico di A possiede tutte le radici in $\mathbb{K}$.

6. Coniche proiettive reali e complesse

Ritorniamo all'Esempio (2.4) e studiamo più in detaglio il caso in cui $K = \mathbb{R}, \mathbb{C}$ e $n = 2$. Scriviamo $\mathbb{P}^2_K = \mathbb{P}^2$. In $\mathbb{P}^2$ consideriamo coordinate $[X_0, X_1, X_2]$. Una conica C in $\mathbb{P}^2$ ha equazione:

$$C: \qquad a_{00}X_0^2 + a_{11}X_1^2 + a_{22}X_2^2 + 2a_{01}X_0X_1 + 2a_{02}X_0X_2 + 2a_{12}2X_1X_2 = 0$$

Più brevemente, si scrive:

$$C: \qquad {}^tXAX = 0\,, \quad \text{dove} \quad X = (X_0, X_1, X_2)\,, \quad A = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{01} & a_{11} & a_{12} \\ a_{02} & a_{12} & a_{22} \end{pmatrix}$$

Dunque ogni conica C individua ed è individuata dal punto

$$[A] = [a_{00}, a_{11}, a_{22}, a_{01}, a_{02}, a_{12}] \quad \in \quad \mathbb{P}^5$$

Per ricordarci di ciò, a volte scriveremo $C = C_{[A]}$. Come sappiamo il gruppo proiettivo $\mathbb{P}GL(3, K)$ agisce in modo transitivo su $\mathbb{P}^2$:

$$([B], [X]) \mapsto [BX]\,, \qquad B = \begin{pmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{pmatrix}\,, \qquad X = (X_0, X_1, X_2)$$

D'altro canto, quando si agisce su $\mathbb{P}^2$ con una proiettività $[B] \in \mathbb{P}GL(3, K)$, le coniche in $\mathbb{P}^2$ si trasformano in coniche. Precisamente la conica $C_{[A]}$ si trasforma nella conica $C_{{}^tBAB}$:

$$C_{[A]}: \quad {}^tXAX = 0, \quad \rightsquigarrow {}^t(BX)ABX = 0 \qquad \text{i.e.} \quad \rightsquigarrow \qquad C_{{}^tBAB}: \quad {}^tX({}^tBAB)X = 0$$

Stiamo quindi studiando l'azione di $\mathbb{P}GL(3, K)^o$ su $\mathbb{P}^5$ data da:

$$\mathbb{P}GL(3, K)^o \times \mathbb{P}^5 \longrightarrow \mathbb{P}^5$$

$$(2) \qquad ([B], [A]) \mapsto [{}^tBAB]\,, \qquad B = \begin{pmatrix} b_{00} & b_{01} & b_{02} \\ b_{10} & b_{11} & b_{12} \\ b_{20} & b_{21} & b_{22} \end{pmatrix}\,, \quad A = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{01} & a_{11} & a_{12} \\ a_{02} & a_{12} & a_{22} \end{pmatrix}.$$

Caso di $\mathbb{P}^2_{\mathbb{C}}$:

In questo caso il teorema di classificazione delle forme quadratiche ci dice che vi sono esattamente *tre* orbite per l'azione di data da (2). Le coniche rappresentative per ognuna di queste orbite sono:

$$X_0^2 + X_1^2 + X_2^2 = 0\,, \quad X_0^2 + X_1^2 = 0\,, \quad X_0^2 = 0\,.$$

Caso di $\mathbb{P}^2_{\mathbb{R}}$:

In questo caso il teorema di classificazione delle forme quadratiche ci dice che vi sono esattamente *cinque* orbite per l'azione di data da (2). Le coniche rappresentative per ognuna di queste orbite sono:

$$\begin{aligned} X_0^2 + X_1^2 + X_2^2 &= 0\,, \\ X_0^2 + X_1^2 - X_2^2 &= 0\,, \\ X_0^2 + X_1^2 &= 0\,, \\ X_0^2 - X_1^2 &= 0\,, \\ X_0^2 &= 0\,. \end{aligned}$$

7. Lo spazio affine e le coniche affini.

Lo *spazio affine* $\mathbb{A}^n = \mathbb{A}^n_K$ è, per definizione, l'insieme che si ottiene da $\mathbb{P}^n = \mathbb{P}^n_K$ togliendone una retta proiettiva. Per comodità introduciamo coordinate omogenee $[X_0, \ldots, X_n]$ in $\mathbb{P}^n$ e poniamo

$$\mathbb{A}^n = \mathbb{P}^n \setminus \{X_0 = 0\}$$

Dunque i punti di $\mathbb{A}^n$ sono in corrispondenza biunivoca con punti di K^n

$$\begin{aligned} \mathbb{A}^n &\longrightarrow K^n \\ [X_0, \ldots, X_n] &\mapsto \left(\tfrac{X_1}{X_0}, \ldots, \tfrac{X_n}{X_0}\right) \end{aligned}$$

Si pone $x_i = X_i/X_0$ per $i = 1, \ldots, n$, e si dice che $(x_1, \ldots, x_n)$ sono *coordinate affini per* $\mathbb{A}^n$. Il gruppo affine $\mathbb{A}\mathrm{ff}(n, K)$ è il sottogruppo delle proiettività di $\mathbb{P}^n$ che portano la retta $\{X_0 = 0\}$ in sé stessa. Gli elementi di $\mathbb{A}\mathrm{ff}(n, K)$ prendono il nome di *affinità.* Sia $[B] \in \mathbb{P}GL(n, K)$ e poniamo

$$B = (b_{ij}) \in GL(n+1, K)\,, \quad i, j = 0, \ldots, n$$

La condizione perchè

$$[B]\Big(\{X_0 = 0\}\Big) \;=\; \{X_0 = 0\}$$

è che $b_{0j} = 0$ per $j = 1, \ldots, n$. Dunque la matrice B, di un elemento $[B] \in \mathbb{A}\mathrm{ff}(n, K)$, ha la forma

$$B = \begin{pmatrix} b_{00} & 0 \\ \mathbf{b}' & B' \end{pmatrix}, \quad b_{00} \neq 0$$

Poiché ci interessa la proiettività $[B] \in \mathbb{P}GL(n, K)$, possiamo assumere che $b_{00} = 1$. Dunque possiamo scrivere gli elementi L di $\mathbb{A}\mathrm{ff}(n, K)$ in modo unico nella forma

$$L = \begin{pmatrix} 1 & 0 \\ \mathbf{a} & A \end{pmatrix}, \qquad A \in GL(n, K)\,, \quad \mathbf{a} \in K^n$$

Quindi, da un punto di vista *insiemistico,* si ha una identificazione

$$\begin{aligned} \mathbb{A}\mathrm{ff}(n, K) &\longleftrightarrow K^n \times GL(n, K) \\ L &\mapsto (\mathbf{a}, A) \end{aligned} \tag{3}$$

Bisogna però fare attenzione a come si legge in $GL(n, K) \times K^n$ la moltiplicazione di due elementi di $\mathbb{A}\mathrm{ff}(n, K)$. Se

$$M = \begin{pmatrix} 1 & 0 \\ \mathbf{b} & B \end{pmatrix},$$

Allora

$$LM = \begin{pmatrix} 1 & 0 \\ A\mathbf{b}+\mathbf{a} & AB \end{pmatrix},$$

Perciò, usando l'identificazione (3), si scriverà

$$(A, \mathbf{a})(B, \mathbf{b}) = (A\mathbf{b}+\mathbf{a}, AB) \tag{4}$$

Per calare tutto ciò nella realtà, consieriamo l'azione

$$\mathbb{A}\mathrm{ff}(n, K) \times \mathbb{A}^n \longrightarrow \mathbb{A}^n$$

indotta da quella di $\mathbb{P}GL(n+1, K)$ su $\mathbb{P}^n$. Per $x = (x_1, \ldots, x_n) \in \mathbb{A}^n$, si ha

$$Lx = M = \begin{pmatrix} 1 & 0 \\ \mathbf{a} & A \end{pmatrix} \begin{pmatrix} 1 \\ x \end{pmatrix} = \begin{pmatrix} 1 \\ Ax+\mathbf{a} \end{pmatrix}$$

o, più semplicemente

$$Lx = Ax + \mathbf{a}$$

Le affinità del tipo $T_{\mathbf{a}} = (\mathbf{a}, I)$ prendono il nome di *traslazioni.* Ovviamente, per $x \in \mathbb{A}^n$, si ha $T_{\mathbf{a}}(x) = x + \mathbf{a}$. Dunque ogni affinità si può scrivere come la composizione di un elemento $(0, A)$ con $A \in GL(n, K)$ e di una traslazione (si confronti con (4)):

$$L = AT_{\mathbf{a}} = (0, A)(\mathbf{a}, I) = (\mathbf{a}, A).$$

Naturalmente, la (4) può anche leggersi nel modo che segue:

$$AT_{\mathbf{a}}BT_{\mathbf{b}} = ABT_{A\mathbf{b}+\mathbf{a}}$$

Esercizio 7.1. Il gruppo delle affinità $\mathbb{A}\mathrm{ff}(n, K)$ agisce transitivamente su $\mathbb{A}^n$.

Coniche in $\mathbb{A}^2_{\mathbb{C}}$

Consideriamo ora il caso in cui $K = \mathbb{C}$ e $n = 2$. Una *conica affine complessa,* si rappresenta in coordinate affini nella forma

$$C_{[A]}: \qquad a_{11}x_1^2 + a_{22}x_2^2 + 2a_{12}x_1x_2 + 2a_{01}x_1 + 2a_{02}x_2 + a_{00} = 0, \qquad a_{ij} \in \mathbb{C} \tag{5}$$

dove, si fa la richiesta (ulteriore rispetto al caso proiettivo) che la matrice

$$A_1 = \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}$$

sia non nulla. Dunque, se nello spazio proiettivo complesso $\mathbb{P}^5_{\mathbb{C}}$ con coordinate omogenee

$$(a_{11}, a_{22}, a_{12}, a_{01}, a_{02}, a_{00}),$$

si considera il piano $\pi \cong \mathbb{P}^2_{\mathbb{C}}$ di equazioni $a_{11} = a_{22} = a_{12} = 0$, le coniche affini corrispondono ai punti di $\mathbb{P}^5_{\mathbb{C}} \setminus \pi$. Per accertarci che l'azione di $\mathbb{P}GL(3, \mathbb{C})$ sul $\mathbb{P}^5_{\mathbb{C}}$, i cui punti rappresentano le coniche proiettive, induce una azione

$$\mathbb{A}\mathrm{ff}(2, \mathbb{C}) \times (\mathbb{P}^5_{\mathbb{C}} \setminus \pi) \longrightarrow (\mathbb{P}^5_{\mathbb{C}} \setminus \pi) \tag{6}$$

del suo sottogruppo $\mathbb{A}\mathrm{ff}(2, \mathbb{C})$, sul sottoisinsieme $\mathbb{P}^5_{\mathbb{C}} \setminus \pi$, i cui punti rappresentano le coniche affini, facciamo un semplice conto. Sia

$$A = \begin{pmatrix} a_{00} & {}^t\mathbf{a} \\ \mathbf{a} & A_1 \end{pmatrix}, \qquad \mathbf{a} = \begin{pmatrix} a_{01} \\ a_{02} \end{pmatrix}, \qquad [A] \in \mathbb{P}^5_{\mathbb{C}} \setminus \pi$$

e sia

$$B = \begin{pmatrix} 1 & 0 \\ \mathbf{b} & B_1 \end{pmatrix} \in \mathbb{A}\mathrm{ff}(2, \mathbb{C}), \qquad \mathbf{b} \in \mathbb{C}^2, \quad B_1 \in GL(2, \mathbb{C})$$

L'azione di $\mathbb{A}\mathrm{ff}(2, \mathbb{C})$ su $[A]$ è data da:

$$A \rightsquigarrow {}^tBAB = \begin{pmatrix} 1 & {}^t\mathbf{b} \\ 0 & {}^tB_1 \end{pmatrix} \begin{pmatrix} a_{00} & {}^ta \\ a & A_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \mathbf{b} & B_1 \end{pmatrix} =$$
$$\begin{pmatrix} a_{00} + {}^t\mathbf{ab} + {}^t\mathbf{ba} + {}^t\mathbf{b}A_1\mathbf{b} & {}^ta{}^tB_1 + {}^t\mathbf{b}A_1B_1 \\ {}^tB_1a + {}^tB_1A_1\mathbf{b} & {}^tB_1A_1B_1 \end{pmatrix}$$

Essendo $B_1 \in GL(2, \mathbb{C})$ si ha che, in effetti, $[{}^tBAB]$ è un punto di $\mathbb{P}^5_{\mathbb{C}} \setminus \pi$. Troviamo le orbite dell'azione di $\mathbb{A}\mathrm{ff}(2, \mathbb{C})$ su questo $\mathbb{P}^5_{\mathbb{C}} \setminus \pi$. Possiamo innanzi tutto scegliere la matrice B_1 in modo che ${}^tB_1A_1B_1$ abbia una delle due seguenti forme, a seconda che $rg(A)$ sia uguale a 1, o a 2:

$${}^tB_1A_1B_1 = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}, \quad \text{oppure:} \quad {}^tB_1A_1B_1 = \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}, \quad \alpha \neq 0$$

Nel primo caso si sceglie $\mathbf{b} = -A^{-1}\mathbf{a}$, nel secondo caso si sceglie $\mathbf{b}$ in modo che ${}^tB_1a + {}^tB_1A_1\mathbf{b} = (0, c_{02})$. Dunque, agendo con $\mathbb{A}\mathrm{ff}(2, \mathbb{C})$, la conica originaria si trasforma in una delle seguenti:

$$\alpha x_1^2 + \alpha x_2^2 + c_{00} = 0, \quad \text{oppure}$$
$$\alpha x_1^2 + 2c_{02}x_2 + c_{00} = 0, \qquad \alpha \neq 0$$

Vi sono ora da esaminare vari casi. Consideriamo la prima equazione. Se $c_{00} \neq 0$, si pone $\alpha = c_{00}$ e si divide per α. Se $c_{00} = 0$, si divide semplicemente per α. Consideriamo ora la seconda equazione. Se $c_{02} \neq 0$, si opera con l'affinità

$$x'_1 = x_1, \qquad x'_2 = \frac{1}{\alpha}(2c_{02}x_2 + c_{00}),$$

e si divide per α. Se $c_{00} \neq 0$ e $c_{02} = 0$, si pone $\alpha = c_{00}$ e si divide per α. In definitiva si ottengono le coniche seguenti:

$$\begin{aligned} x_1^2 + x_2^2 + 1 &= 0, && \text{conica irriducibile con due punti all'infinito.} \\ x_1^2 + x_2^2 &= 0, && \text{coppia di rette.} \\ x_1^2 + x_2 &= 0, && \text{conica irriducibile con un punto all'infinito.} \\ x_1^2 &= 0, && \text{retta doppia..} \end{aligned}$$

Il termine *irriducibile* indica che la conica in questione non si spezza nell'unione di due rette. Si osserva infine che le quattro coniche ottenute appartengono a orbite distinte per l'azione di $\mathbb{A}\mathrm{ff}(2, \mathbb{C})$. Infatti, il rango di A_1 e il numero di intersezioni con la retta all'infinito sono invarianti per l'azione di $\mathbb{A}\mathrm{ff}(2, \mathbb{C})$. In definitiva, le quattro coniche affini sopra scritte rappresentano le orbite distinte dell'azione di $\mathbb{A}\mathrm{ff}(2, \mathbb{C})$ sull'insieme $\mathbb{P}^5_{\mathbb{C}} \setminus \pi$ delle coniche affini complesse.

Coniche in $\mathbb{A}^n_{\mathbb{R}}$

Consideriamo ora le coniche affini reali. In questo caso avremo l'azione di $\mathbb{A}\mathrm{ff}(2, \mathbb{R})$ sull'insieme $\mathbb{P}^5_{\mathbb{R}} \setminus \pi$ delle coniche affini reali. Descriviamo le orbite di questa azione. Mantenendo le stesse notazioni usate nel caso complesso, dovremo ora considerare, non solo il rango, ma anche la segnatura della matrice A_1. Si ottengono quindi 9 orbite distinte i cui rappresenti sono le seguenti coniche:

$x_1^2 + x_2^2 + 1 = 0\,,$ conica irriducibile, puramente immaginaria, con due punti, complessi coniugati, all'infinito.

$-x_1^2 - x_2^2 + 1 = 0\,,$ conica irriducibile reale con due punti, complessi coniugati, all'infinito.

$x_1^2 - x_2^2 - 1 = 0\,,$ conica irriducibile reale con due punti reali all'infinito.

$x_1^2 - x_2^2 = 0\,,$ due rette reali che si intersecano in un punto, i.e. con due punti reali all'infinito.

$x_1^2 + x_2^2 = 0\,,$ due rette complesse coniugate con due punti complessi coniugati all'infinito.

$x_1^2 + x_2 = 0\,,$ conica irriducibile reale con un punto all'infinito.

$x_1^2 - 1 = 0\,,$ coppia di rette reali parallele, i.e. con un punto all'infinito.

$x_1^2 + 1 = 0\,,$ coppia di rette complesse coniugate con un punto all'infinito.

$x_1^2 = 0\,,$ retta doppia.

Le prime cinque coniche sono quelle per cui $rg(A_1) = 2$, per le rimanenti, $rg(A_1) = 1$.

8. Stabilizzatori

Si consideri l'azione di un gruppo G su di un insieme S. Dato un punto $s \in S$, lo *stabilizzatore di s in G* è il sottogruppo

$$G_s = \{g \in G \mid gs = s\}$$

Che G_s sia un sottogruppo è chiaro. Prima di procedere introduciamo un altro concetto. Supponiamo di avere due azioni di G: una su di un insieme S ed una su di un insieme T che, con abuso di notazione denotiamo con lo stesso simbolo " $\cdot$ " Diremo che le due azioni sono *isomorfe,* se vi è una corrispondenza biunivoca

$$\tau : S \longrightarrow T$$

tale che

$$\tau(g \cdot x) = g \cdot \tau(x), \quad \forall x \in S.$$

Ora vediamo che l'azione di G sull'insieme delle classi laterali G/G_s è isomorfa all'azione di G sull'orbita Gs. Infatti basta porre:

$$\begin{aligned} \tau : Gs &\longrightarrow G/G_s \\ gs &\mapsto gG_s \end{aligned}$$

e osservare che

$$\tau(gs) = \tau(hs) \iff gG_s = hG_s \iff h^{-1}gG_s = G_s \iff h^{-1}g \in G_s \iff gs = hs$$

e che dunque τ, oltre ad essere ovviamente suriettiva, è anche iniettiva. Mentre, d'altro canto,

$$\tau(h \cdot gs) = \tau(hgs) = hgG_s = h \cdot gG_s\,.$$

È da osservare che, dati due elementi s e s' di una stessa orbita, gli stabilizzatori G_s e $G_{s'}$ sono coniugati in G. Infatti se $hs = s'$, si ha

$$G_{s'} = hG_sh^{-1}$$

Esempio 8.1. Dato un insieme finito X, si denoti con $|X|$ la sua cardinalità. Sia G un gruppo finito che agisce su un insieme finito S. Allora

$$\frac{|S|}{|G|} = \sum_{[s] \in S/G} \frac{1}{|G_s|}$$

Infatti:

$$|S| = \sum_{[s]\in S/G} |sG| = \sum_{[s]\in S/G} |G/G_s| = \sum_{[s]\in S/G} \frac{|G|}{|G_s|}$$

Esempio 8.2. L'esempio precedente si può subito usare nello studio della azione di G su sé stesso per coniugio. Sia Z il centro di G. Ogni elemento di Z è un'orbita. Siano $Gx_1G^{-1}, \dots, Gx_nG^{-1}$ le altre orbite e siano $G_{x_1}, \dots, G_{x_n}$ gli stabilizzatori di $x_1, \dots, x_n$. Allora si ha:

$$|G| = |Z| + \sum_{i=1,\dots,n} \frac{|G|}{|G_{x_i}|} \tag{7}$$

Esercizio 8.3. Si consideri la grasmanniana $Gr(k,d)$ dei sottospazi k-dimensionali di $\mathbb{R}^d$, definita nell' Esempio (3.6), e si ricordi l'azione dell'Esempio (3.8). Dimostrare che

$$Gr(k,d) \cong \frac{O(d)}{O(k)\times O(d-k)}$$

Esempio 8.4. Sia G un gruppo finito e sia p un numero primo. Un sottogruppo H di G si dice *p-Sylow* se il suo ordine è p^n e se p^n è la più grande potenza di p che divide l'ordine di G.

Teorema 8.5. *(di Sylow). Sia G un gruppo finito.*

a) Esistono sottogruppi di p-Sylow

b) Ogni sottogruppo H di G con ordine p^h è contenuto in un sottogruppo p-Sylow

c) I sottogruppi p-Sylow di G sono tutti coniugati.

d) Il numero dei sottogruppi p-Sylow è congruo a $1 \mod p$.

Dimostrazione. a) Si procede per induzione su $|G|$. Se l'ordine è primo non c'è nulla da dimostrare. Sia $|G| = n$ e assumiamo il risultato per gruppi Γ con $|\Gamma| < n$. Se esiste un sottogruppo $H \subset G$ il cui indice $[G : H]$ è primo con p, si procede ancora per induzione perchè un p-Sylow di G è automaticamente un p-Sylow per G. Possiamo quindi assumere che qualsiasi sia il sottogruppo H, il primo p divide $[G : H]$. Facciamo agire G su sé stesso per coniugio. Usando la formula (7) si deduce che p divide $|Z|$e in particolare $Z \neq \{e\}$, dove e denota l'identità. Sia a un elemento di Z di ordine p e si consideri il sottogruppo ciclico $< a >\subset G$ generato da a. Poiché $< a >\subset Z$ il sottogruppo $< a >$ è normale. Sia p^n la massima potenza di p che divide $|G|$. Allora p^{n-1} è la massima potenza di p che divide $|G/ < a > |$. Si $\pi : G \to G/ < a >$ l'omomorfismo canonico. Per induzione esiste un p-Sylow in $G/ < a >$, sia esso H'. Sia $H = \pi^{-1}(H')$. Evidentemente $H \supset< a >$. Dunque $H/ < a >\cong H'$ e perciò $|H| = |H'|| < a > | = p^n$.

b) Sia S l'insieme dei p-sottogruppi di Sylow di G. Il gruppo G opera su S per coniugio. Sia P un fissato p-sottogruppo di Sylow. Sia G_P lo stabilizzatore di P. Naturalmente $G_P \supset P$ e quindi l'ordine q dell'orbita T di P è primo con p. Sia H un sottogruppo di G con ordine p^h. Il sottogruppo H opera per coniugio su T. Dunque T si decompone nell'unione disgiunta di orbite sotto l'azione di H. Poiché l'ordine di H è p^h, anche gli stabilizzatori di questa azione devono avere ordine uguale a una potenza di p. In definitiva

$$q = \sum_{i=s,\dots,\nu} \frac{|H|}{|H_s|} = p^{i_1} + \cdots + p^{i_\nu}.$$

Essendo p primo con q, ciò può accadere solo se, per qualche s, si ha $i_s = 1$. Ma questo vuol dire che $H_s = H$, e cioè che l'H-orbita di un p-Sylow Q è costituita da un solo elemento:

$$HQH^{-1} = Q$$

Se ne deduce che HQ è un sottogruppo di G e Q è normale in HQ. Poiché

$$HQ/Q \cong H/H\cap Q\,,$$

l'ordine di HQ/Q è una potenza di p e così dunque lo è anche $|HQ|$. Essendo Q un p-Sylow, si deve avere $Q = HQ$ e dunque $H \supset Q$.

c) Continuando il ragionamento appena fatto, si ha in particolare che, se anche H è un p-Sylow allora $H = Q$ e quindi H è nell'orbita di P. Essendo H un arbitrario p-Sylow, la c) segue.

d) Sia ora $H = P$. Allora un'orbita (quella di P) è costituita da un solo elemento (P stesso), mentre le altre hanno ordine maggiore di 1 e divisibile per p, il che dimostra d). $\square$