Istituzioni di Algebra e Geometria 2022-23
Parte II
Geometria proiettiva e curve piane

Marco Manetti

Versione preliminare del **20 dicembre 2022***:*
l'autore ringrazia tutti coloro che segnalano ed hanno segnalato errori ed imprecisioni

Avvertenza: Queste dispense sono ancora nella fase work in progress e contengono inevitabilmente molte lacune, imprecisioni ed errori di stmpa. Sono distribuite, senza alcuna garanzia, esclusivamente per gli usi relativi all'insegnamento di Istituzioni di Algebra e Geometria 2022-23, Corso di laurea Magistrale in Matematica Applicata, Sapienza Università di Roma.

Indice

CAPITOLO 1

Geometria affine e proiettiva

Indicheremo con $\mathbb{K}$ un campo fissato e non nullo, ossia con $1 \neq 0$. Le figure presentate si riferiscono al caso $\mathbb{K} = \mathbb{R}$ e sono un valido aiuto alla comprensione dei risultati, non solo su $\mathbb{R}$ ma anche su campi di caratteristica $\neq 2$. Occorre fare attenzione che in caratteristica 2 accadono alcuni fenomeni decisamente controintuitivi (vedi Esempio 1.6.4) e per i quali il disegno potrebbe essere fuorviante.

Per spazio vettoriale intenderemo sempre uno spazio vettoriale di *dimensione finita* su $\mathbb{K}$. Per ogni spazio vettoriale V indicheremo con $V^\vee$ il suo duale e con $\mathrm{GL}(V)$ il gruppo di tutti gli endomorfismi lineari di V invertibili, dotato del prodotto di composizione.

1.1. Il teorema di Menelao

Dati tre punti $p = (p_1, p_2)$, $q = (q_1, q_2)$ e $r = (r_1, r_2)$ del piano Cartesiano $\mathbb{R}^2$, è noto a tutti che si dicono allineati se appartengono ad una medesima retta, ossia se sono contenuti nel sottoinsieme di equazione $ax + by + c = 0$, con a, b, c costanti non tutte nulle.

Dunque, i suddetti p, q, r sono allineati se e solo se esistono a, b, c non tutti nulli tali che

$$a\begin{pmatrix} p_1 \\ q_1 \\ r_1 \end{pmatrix} + b\begin{pmatrix} p_2 \\ q_2 \\ r_2 \end{pmatrix} + c\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

ossia se il rango per righe[1] della matrice

$$\begin{pmatrix} p_1 & q_1 & r_1 \\ p_2 & q_2 & r_2 \\ 1 & 1 & 1 \end{pmatrix}$$

è al più 2. Siccome per ogni matrice il rango per righe è uguale al rango per colonne si ha che p, q, r sono allineati se e solo se se esistono scalari α, β, γ non tutti nulli tali che

$$\alpha\begin{pmatrix} p_1 \\ p_2 \\ 1 \end{pmatrix} + \beta\begin{pmatrix} q_1 \\ q_2 \\ 1 \end{pmatrix} + \gamma\begin{pmatrix} r_1 \\ r_2 \\ 1 \end{pmatrix} = 0$$

ossia se e solo se valgono le equazioni:

$$\alpha p + \beta q + \gamma r = 0, \qquad \alpha + \beta + \gamma = 0\,. \tag{1.1}$$

Notiamo che le equazioni (1.1) hanno perfettamente senso per un qualunque spazio vettoriale su qualunque campo.

Definizione 1.1.1. Sia V uno spazio vettoriale su di un campo $\mathbb{K}$. Diremo che tre punti $p, q, r \in V$ sono **allineati** se esistono $\alpha, \beta, \gamma \in \mathbb{K}$ non tutti nulli tali che

$$\alpha p + \beta q + \gamma r = 0, \qquad \alpha + \beta + \gamma = 0\,.$$

Osserviamo che se i tre punti p, q, r non sono distinti, allora sono allineati (se ad esempio $p = q$ basta prendere $\alpha = 1$, $\beta = -1$ e $\gamma = 0$).

Lemma 1.1.2. *Siano V spazio vettoriale e $p, q, r \in V$ con $p \neq q$. Allora p, q, r sono allineati se e solo se esiste $t \in \mathbb{K}$ tale che $r = (1-t)p + tq$; in tal caso t è unico.*

[1] Ricordiamo che il rango per righe (risp.: colonne) è il massimo numero di righe (risp.: colonne) linearmente indipendenti.

DIMOSTRAZIONE. Per ogni $p, q \in V$ ed ogni $t \in \mathbb{K}$ i tre punti $p, q, r = (1-t)p + tq$ sono allineati poiché $(1-t) + tq - r = 0$.

Viceversa, se p, q, r sono allineati e $p \neq 0$ esistono $\alpha, \beta, \gamma \in \mathbb{K}$ non tutti nulli tali che

$$\alpha p + \beta q + \gamma r = 0, \qquad \alpha + \beta + \gamma = 0\,.$$

Se fosse $\gamma = 0$ si avrebbe $\alpha = -\beta \neq 0$ da cui $\alpha(p-q) = 0$ in contraddizione con l'ipotesi $p \neq q$. Dunque $\gamma \neq 0$ e possiamo scrivere

$$r = \frac{-\alpha}{\gamma} p + \frac{-\beta}{\gamma} q\,.$$

Ponendo $t = \dfrac{-\beta}{\gamma}$ si ha

$$\frac{-\alpha}{\gamma} = \frac{\gamma + \beta}{\gamma} = 1 - t$$

e quindi $r = (1-t)p + tq$.

Per quanto riguarda l'uncità di t, se $r = (1-t)p + tq = (1-s)p + sq$ con $t, s \in \mathbb{K}$, facendo la differenza si ottiene

$$0 = (s-t)p + (t-s)q = (t-s)(q-p),$$

da cui $s = t$. □

Dunque, per ogni $p \neq q$ l'applicazione

$$f_{p,q} \colon \mathbb{K} \to V, \qquad f(t) = (1-t)p + tq, \tag{1.2}$$

induce una bigezione tra il campo $\mathbb{K}$ e l'insieme dei vettori allineati con p, q. Si noti che $f_{p,q}(0) = p$, $f_{p,q}(1) = q$ Chiameremo l'immagine di $f_{p,q}$ **retta affine** passante per p, q, che denoteremo $\overline{pq}$.

Per ogni $r \in \overline{pq}$ definiamo il **rapporto semplice**

$$(r, p, q) = f_{p,q}^{-1}(r)\,.$$

In altri termini, il rapporto semplice si ricava dalle seguenti equivalenze:

$$(r,p,q) = t \iff r = (1-t)p + tq \iff r - p = t(q-p)\,.$$

Il perché del nome rapporto semplice si capisce bene quando $V = \mathbb{K}^1 = \mathbb{K}$; in tal caso si può dividere per $q - p \in \mathbb{K}$ e quindi $(r,p,q) = (r-p)/(q-p)$.

Il rapporto semplice **non è** invariante per permutazioni: se p, q, r sono distinti e $(r,p,q) = t$ si ha

$$\begin{gathered}(r,p,q) = t, \qquad (p,q,r) = \frac{1}{1-t}, \qquad (q,r,p) = \frac{t-1}{t}\,, \\ (p,r,q) = \frac{t}{t-1}, \qquad (q,p,r) = \frac{1}{t}, \qquad (r,q,p) = 1-t,\end{gathered} \tag{1.3}$$

dove le precedenti formule (1.3) hanno senso poiché $t \neq 0$ ($r \neq p$) e $t \neq 1$ ($r \neq q$). Mostriamo solamente il calcolo di (p,q,r) lasciando le altre verifiche per esercizio. Se $(r,p,q) = t$ allora $r = (1-t)p + tq$ da cui

$$(r,p,q) = t \iff r = (1-t)p + tq \iff p = \frac{t}{t-1} q + \frac{1}{1-t} r \iff (p,q,r) = \frac{1}{1-t}\,.$$

TEOREMA 1.1.3 (Teorema di Menelao, prima versione). *Siano dati tre punti $a, b, c \in V$ non allineati e si considerino tre punti $c' \in \overline{ab}$, $a' \in \overline{bc}$, $b' \in \overline{ac}$. Se $a' \neq b, c$, $b' \neq a, c$ e $c' \neq a, b$ allora a', b', c' sono allineati se e solo se*

$$(a, c', b)(b, a', c)(c, b', a) = 1\,.$$

DIMOSTRAZIONE. Per semplicità notazionale indichiamo

$$(a, c', b) = r, \quad (b, a', c) = s, \quad (c, b', a) = t\,.$$

Dalle formule (1.3) si ricavano i valori

$$(a', b, c) = \frac{s}{s-1}, \qquad (b', a, c) = \frac{1}{1-t}, \qquad (c', a, b) = \frac{r}{r-1}\,,$$

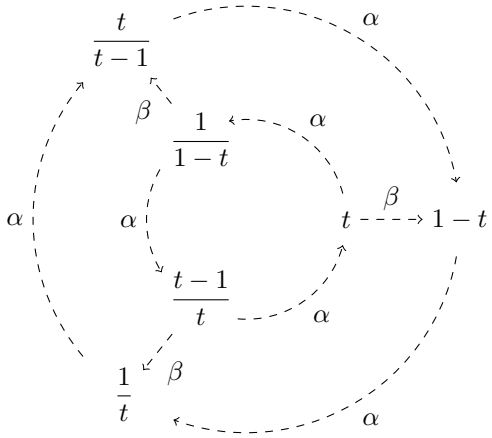


FIGURA 1. Le applicazioni

$$\alpha, \beta \colon \mathbb{K} - \{0,1\} \to \mathbb{K} - \{0,1\}, \qquad \alpha(t) = \frac{1}{1-t}, \quad \beta(t) = 1 - t,$$

soddisfano le relazioni $\alpha^3 = \beta^2 = \mathrm{Id}$, $\alpha\beta = \beta\alpha^2$ e definiscono la rappresentazione del gruppo simmetrico Σ_3 determinata dall'azione sui rapporti semplici.

che equivalgono alle uguaglianze

$$a' = \frac{1}{1-s}b + \frac{s}{s-1}c, \quad b' = \frac{t}{t-1}a + \frac{1}{1-t}c, \quad c' = \frac{1}{1-r}a + \frac{r}{r-1}b\,. \tag{1.4}$$

Si considerino i vettori di $\mathbb{K}^n \times \mathbb{K}$:

$$A = \begin{pmatrix} a \\ 1 \end{pmatrix}, \quad B = \begin{pmatrix} b \\ 1 \end{pmatrix}, \quad C = \begin{pmatrix} c \\ 1 \end{pmatrix}, \quad A' = \begin{pmatrix} a' \\ 1 \end{pmatrix}, \quad B' = \begin{pmatrix} b' \\ 1 \end{pmatrix}, \quad C' = \begin{pmatrix} c' \\ 1 \end{pmatrix}.$$

Allora i tre vettori A, B, C sono linearmente indipendenti e la matrice $(A, B, C) \in M_{n+1,3}(\mathbb{K})$ ha rango 3. Le uguaglianze in (1.4) forniscono immediatamente le uguaglianze

$$A' = \frac{1}{1-s}B + \frac{s}{s-1}C, \qquad B' = \frac{t}{t-1}A + \frac{1}{1-t}C, \qquad C' = \frac{1}{1-r}A + \frac{r}{r-1}B$$

che nel formalismo del prodotto righe x colonne si possono scrivere come

$$(A', B', C') = (A, B, C) \begin{pmatrix} 0 & \frac{t}{t-1} & \frac{1}{1-r} \\ \frac{1}{1-s} & 0 & \frac{r}{r-1} \\ \frac{s}{s-1} & \frac{1}{1-t} & 0 \end{pmatrix}.$$

Per il Lemma 1.2.2 i vettori A', B', C' sono allineati se e solo se la matrice (A', B', C') ha rango < 3 e questo vale se e solo se la matrice 3×3 nella formula precedente ha rango < 3. Adesso basta calcolare il determinante

$$\begin{vmatrix} 0 & \frac{t}{t-1} & \frac{1}{1-r} \\ \frac{1}{1-s} & 0 & \frac{r}{r-1} \\ \frac{s}{s-1} & \frac{1}{1-t} & 0 \end{vmatrix} = \frac{1 - srt}{(1-r)(1-s)(1-t)}\,,$$

che si annulla se e solo se $srt = 1$ e questo conclude la dimostrazione del teorema. □

Vediamo adesso l'interpretazione in geometria Euclidea del teorema di Menelao, con i punti a, b, c, a', b', c' considerati in $\mathbb{R}^2$. Per ogni $p, q \in \mathbb{R}^2$ denotiamo con $|pq| = \|p - q\|$ la

distanza Euclidea e osserviamo che se p, q, r sono allineati e distinti, allora

$$(p, r, q) = \pm \frac{|pr|}{|qr|}$$

dove il segno $-$ vale se e solo se r è compreso tra p e q, ossia se r appartiene al segmento di estremi p, q. Infatti $(p, r, q) = t \in \mathbb{R}$ se e solo se $p = (1-t)r + tq$ se e solo se $p - r = t(q - r)$ da cui $|t| = \dfrac{\|p - r\|}{\|q - r\|}$. Sempre dalla formula $p - r = t(q - r)$ segue che t è negativo se e solo se i vettori $p - r$ e $q - r$ hanno direzioni opposte, ossia se e solo se r è compreso tra p, q.

Se a', b', c' sono allineati, prendendo i valori assoluti dei rapporti semplici nella formula del Teorema 1.1.3 si ottiene

$$\frac{|ac'|}{|bc'|}\,\frac{|ba'|}{|ca'|}\,\frac{|cb'|}{|ab'|} = 1\,. \tag{1.5}$$

mentre dall'analisi dei segni segue che il numero dei punti a', b', c' appartenenti ai lati del triangolo è pari.

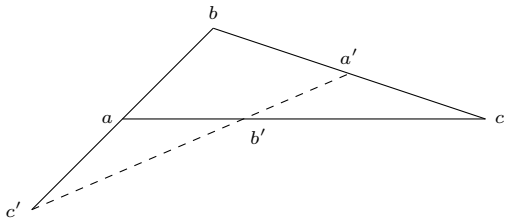


FIGURA 2. Il teorema di Menelao.

Viceversa, se vale (1.5) ed un numero pari di punti a', b', c' appartiene al perimetro del triangolo allora $(a, c', b)(b, a', c)(c, b', a) = 1$ e tali punti risultano allineati.

Esiste una versione alternativa del Teorema di Menelao, molto celebre nella grafica computerizzata, e nel cui enunciato intervengono alcune generalizzazioni delle funzioni $f_{p,q}(t) = (1-t)p + tq$ introdotte in (1.2).

TEOREMA 1.1.4 (Menelao, seconda versione). *Per ogni terna di punti $p, q, r \in V$ si consideri l'applicazione*

$$f_{p,q,r} \colon \mathbb{K}^2 \to V, \qquad f_{p,q,r}(t, s) = (1-s) f_{p,q}(t) + s f_{q,r}(t)\,.$$

Allora $f_{p,q,r}(t, s) = f_{p,q,r}(s, t)$ per ogni $s, t \in \mathbb{K}$.

La dimostrazione è banale, mentre tutt'altro che evidente è la relazione tra le due versioni del teorema di Menelao. Infatti, sviluppando i conti si ha

$$f_{p,q,r}(t, s) = (1-s)(1-t)p + (1-s)tq + s(1-t)q + str = (1-s)(1-t)p + (s + t - 2st)q + str$$

che risulta simmetrica nelle variabili s, t.

Qui mostriamo solamente come la seconda versione segue dalla prima. Si considerino tre punti non allineati p, q, r, due scalari $t, s \in \mathbb{K}$ e si guardi alla Figura 3

Il Teorema 1.1.3 applicato ai triangoli di vertici $f_{p,q}(s), q, f_{q,r}(s)$ e $f_{p,q}(t), q, f_{q,r}(t)$ rispettivamente ci dà le due uguaglianze:

$$(f_{p,q}(s), f_{p,q}(t), q)(q, f_{q,r}(t), f_{q,r}(s))(f_{q,r}(s), x, f_{p,q}(s)) = 1,$$
$$(f_{p,q}(t), f_{p,q}(s), q)(q, f_{q,r}(s), f_{q,r}(t))(f_{q,r}(t), x, f_{p,q}(t)) = 1.$$

I quattro rapporti semplici dove non compare x si calcolano facilmente in funzione di s, t:

$$(f_{p,q}(s), f_{p,q}(t), q) = \frac{s-t}{1-t}, \qquad (f_{p,q}(t), f_{p,q}(s), q) = \frac{t-s}{1-s},$$

$$(q, f_{q,r}(t), f_{q,r}(s)) = \frac{t}{t-s}, \qquad (q, f_{q,r}(s), f_{q,r}(t)) = \frac{s}{s-t}$$

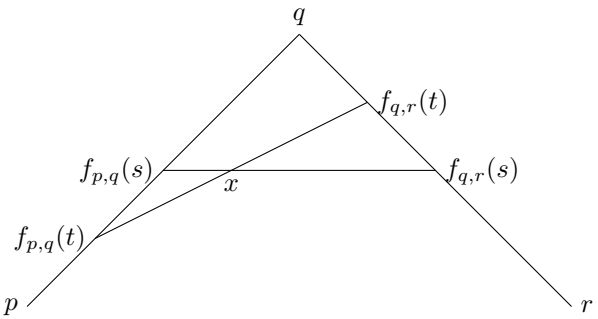


FIGURA 3. Il punto $x = f_{p,q,r}(t,s) = f_{p,q,r}(s,t)$ per $s \neq t$.

da cui segue

$$(f_{q,r}(s), x, f_{p,q}(s)) = \frac{(1-t)(t-s)}{(s-t)t} = \frac{t-1}{t} \iff (x, f_{p,q}(s), f_{q,r}(s)) = t \iff x = f_{p,q,r}(s,t),$$

$$(f_{q,r}(t), x, f_{p,q}(t)) = \frac{(1-s)(s-t)}{(t-s)s} = \frac{s-s}{t} \iff (x, f_{p,q}(t), f_{q,r}(t)) = s \iff x = f_{p,q,r}(t,s).$$

Esercizi

ESERCIZIO 1. Nella notazioni del Teorema 1.1.4, e per $\mathbb{K} = \mathbb{R}$, mostrare che $t \mapsto \gamma(t) = f_{p,q,r}(t,t)$ è una parametrizzazione della parabola passante per p, r e con derivate $\gamma'(p) = q - p$, $\gamma'(r) = r - q$.

1.2. Indipendenza affine e combinazioni baricentriche

Quando si passa da 3 a più punti in uno spazio vettoriale V, esistono due modi naturali di estendere la Definizione 1.1.1. Nel primo di questi, diremo che $p_0, \dots, p_n \in V$ sono allineati se appartengono tutti ad una medesima retta affine: equivalentemente, se ogni terna $p_{i_1}, p_{i_2}, p_{i_3}$ è allineata.

DEFINIZIONE 1.2.1. Sia V uno spazio vettoriale su $\mathbb{K}$. Dati $p+1$ vettori $v_0, \dots, v_p \in V$, si dicono **affinemente dipendenti** se esistono $a_0, \dots, a_p \in \mathbb{K}$, non tutti nulli, e tali che:

$$a_0 v_0 + \cdots + a_p v_p = 0, \qquad a_0 + \cdots + a_p = 0\,.$$

I medesimi vettori si dicono **affinemente indipendenti** se non sono affinemente dipendenti.

È chiaro che se $v_0, \dots, v_p$ sono affinemente dipendenti, allora sono anche linearmente dipendenti. Il viceversa non è vero in generale, as esempio tre vettori in $\mathbb{K}^2$ sono sempre linearmente dipendenti ma sono affinemente dipendenti se e solo se sono allineati.

LEMMA 1.2.2. *Sia V uno spazio vettoriale su $\mathbb{K}$. Dati $v_0, \dots, v_p \in V$ le seguenti condizioni sono equivalenti:*

1. *i $p+1$ vettori $v_0, \dots, v_p \in V$ sono affinemente dipendenti;*
2. *i $p+1$ vettori $(v_0, 1), \dots, (v_p, 1) \in V \times \mathbb{K}$ sono linearmente dipendenti;*
3. *esiste un indice $i = 0, \dots, p$ tale che i p vettori $v_j - v_i$, $j \neq i$, sono linearmente dipendenti;*
4. *per ogni $i = 0, \dots, p$ i p vettori $v_j - v_i$, $j \neq i$, sono linearmente dipendenti.*

DIMOSTRAZIONE. L'equivalenza tra le prime due condizioni, già osservata nel caso $p = 2$, si generalizza immediatamente al caso $p > 2$, dato che l'equazione

$$\sum_{i=0}^{p} a_i (v_i, 1) = 0, \qquad a_i \in \mathbb{K}\,,$$

è del tutto equivalente al sistema di due equazioni

$$\sum_{i=0}^{p} a_i v_i = 0, \quad \sum_{i=0}^{p} a_i = 0, \qquad a_i \in \mathbb{K}\,.$$

Mostriamo che (3) implica (1). Per semplicità supponiamo $i = 0$ (per $i \neq 0$ la dimostrazione è sostanzialmente identica). Siano $a_1, \ldots, a_p \in \mathbb{K}$ non tutti nulli e tali che $\sum_{j=1}^{p} a_j(v_j - v_0) = 0$. Se poniamo $a_0 = -\sum_{j=1}^{p} a_j$ si ha

$$\sum_{j=0}^{p} a_j v_j = \sum_{j=1}^{p} a_j v_j - \sum_{j=1}^{p} a_j v_0 = \sum_{j=1}^{p} a_j (v_j - v_0) = 0\,.$$

Mostriamo adesso che (1) implica (4). Sia i un indice fissato e siano $a_0, \ldots, a_p \in \mathbb{K}$ non tutti nulli e tali che $\sum a_j v_j = 0$. Siccome $a_i = -\sum_{j\neq i} a_j$ esiste almeno un indice $j \neq i$ tale che $a_j \neq 0$ e si ha la relazione di dipendenza lineare

$$\sum_{j\neq i} a_j (v_j - v_i) = \sum_{j\neq i} a_j v_j - (\sum_{j\neq i} a_j) v_i = \sum_{j=0}^{p} a_j v_j = 0\,.$$

□

Da notare che: il massimo numero di vettori affinemente indipendenti in $\mathbb{K}^n$ è $n+1$; ogni vettore (anche nullo) è affinemente indipendente; due vettori sono affinemente indipendenti se e solo se sono distinti.

Sia V uno spazio vettoriale sul campo $\mathbb{K}$. Una combinazione lineare $a_0 v_0 + \cdots + a_n v_n$ di vettori $v_i \in V$ e coefficienti $a_i \in \mathbb{K}$ si dice una **combinazione baricentrica**[2] se $\sum a_i = 1$.

LEMMA 1.2.3. *Finiti vettori in uno spazio vettoriale sono affinemente indipendenti se e solo se nessuno di essi può essere scritto come combinazione baricentrica dei rimanenti.*

DIMOSTRAZIONE. Siano $v_0, \ldots, v_n$ vettori nello spazio vettoriale V. Se sono affinemente dipendenti allora esistono $a_0, \ldots, a_n \in \mathbb{K}$ non tutti nulli tali che

$$\sum_i a_i v_i = 0, \qquad \sum_i a_i = 0\,.$$

Se j è un indice par cui $a_j \neq 0$ si ha

$$v_j = \sum_{i\neq j} \frac{-a_i}{a_j} v_j, \quad \sum_{i\neq j} \frac{-a_i}{a_j} = \frac{1}{a_j} \sum_{i\neq j} -a_i = \frac{a_j}{a_j} = 1\,,$$

e quindi v_i è combinazione baricentrica dei rimanenti vettori. Viceversa se per un qualche indice j si ha

$$v_j = \sum_{i\neq j} b_i v_i, \quad \sum_{j\neq i} b_i = 1,$$

ponendo $b_j = -1$ si ha

$$\sum_i b_i v_i = 0, \qquad \sum_i b_i = 0,$$

e quindi i vettori v_i sono affinemente dipendenti. □

Un sottoinsieme di V si dice un **sottospazio affine** se è chiuso per combinazioni baricentriche. In altri termini, un sottoinsieme $H \subset V$ è un sottospazio affine se per ogni successione finita $v_0, \ldots, v_n \in H$ ed ogni successione $a_0, \ldots, a_n \in \mathbb{K}$ tale che $\sum a_i = 1$ si ha $a_0 v_0 + \cdots + a_n v_n \in H$.

ESEMPIO 1.2.4.
(1) il vuoto è un sottopazio affine;
(2) per ogni $v \in V$, il sottoinsieme $\{v\}$ è un sottospazio affine;
(3) ogni sottospazio vettoriale è anche un sottospazio affine;
(4) intersezione di una famiglia arbitaria di sottospazi affini è ancora un sottospazio affine;

[2]Qui purtroppo non esiste una terminologia standard in letteratura: le combinazioni baricentriche vengono chiamate *combinazioni affini* da alcuni autori e *centroidi* da altri.

(5) Il sottoinsieme di $\mathbb{K}^n$ formato dalle soluzioni $(x_1, \dots, x_n)^T$ di un sistema lineare
$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \quad \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases}$$
è un sottospazio affine;
(6) Se $H \subseteq V$ e $K \subseteq W$ sono sottospazi affini, il loro prodotto cartesiano $H \times K$ è un sottospazio affine di $V \times W$.

LEMMA 1.2.5. *Siano V uno spazio vettoriale e $H \subset V$ un sottospazio affine che non contiene il vettore nullo. Allora $n+1$ vettori $v_0, \dots, v_n \in H$ sono affinemente indipendenti se e solo se sono linearmente indipendenti in V.*

DIMOSTRAZIONE. Una implicazione è chiara: se $v_0, \dots, v_n$ sono linearmente indipendenti, a maggior ragione sono affinemente indipendenti.

Supponiamo viceversa che i vettori v_i siano linearmente dipendenti, ossia che si abbia una combinazione lineare $\sum_{i=0}^n a_i v_i = 0$, con gli $a_i \in \mathbb{K}$ non tutti nulli e denotiamo $a = \sum_{i=0}^n a_i$. Se $a \neq 0$ allora
$$\sum_{i=0}^n \frac{a_i}{a} = 1, \qquad \sum_{i=0}^n \frac{a_i}{a} v_i = 0,$$
in contraddizione con l'ipotesi $0 \notin H$. Dunque $a = 0$ e di conseguenza i vettori v_i sono affinemente dipendenti. □

DEFINIZIONE 1.2.6 (Inviluppo affine). Per ogni insieme finito di vettori $v_0, \dots, v_n$, l'insieme
$$\langle\langle v_0, \dots, v_n \rangle\rangle = \{a_0 v_0 + \cdots + a_n v_n \mid a_i \in \mathbb{K}, \sum a_i = 1\}$$
di tutte le combinazioni baricentriche viene detto **inviluppo affine** di $v_0, \dots, v_n$.

Ogni inviluppo affine è un sottospazio affine. Infatti dati $w_0, \dots, w_m \in \langle\langle v_0, \dots, v_n \rangle\rangle$ per definizione esiste una matrice a_{ij}, $i = 0, \dots, n$, $j = 0, \dots, m$ tale che
$$w_j = \sum_{i=0}^n a_{ij} v_i, \quad \sum_{i=0}^n a_{ij} = 1, \text{ per ogni } j = 0, \dots, m\,.$$
Allora per ogni $b_0, \dots, b_m \in \mathbb{K}$ tali che $\sum b_j = 1$ si ha
$$\sum_j b_j w_j = \sum_{i,j} a_{ij} b_j v_i = \sum_i c_i v_i, \qquad c_i = \sum_j b_j a_{ij},$$
e siccome
$$\sum_i c_i = \sum_i \sum_j b_j a_{ij} = \sum_j b_j \sum_i a_{ij} = \sum_j b_j \cdot 1 = 1$$
ne consegue che $\sum_j b_j w_j \in \langle\langle v_0, \dots, v_n \rangle\rangle$.

Segue immediatamente dalle definizioni che se H è un sottospazio affine di uno spazio vettoriale e $v_0, \dots, v_n \in H$, allora $\langle\langle v_0, \dots, v_n \rangle\rangle \subset H$. Ne segue che l'inviluppo affine $\langle\langle v_0, \dots, v_n \rangle\rangle$ coincide con l'intersezione dei sottospazi affini contenenti $v_0, \dots, v_n$.

LEMMA 1.2.7. *Siano $v_0, \dots, v_n$ vettori affinemente indipendenti in uno spazio vettoriale V. Per un vettore $w \in V$ le seguenti condizioni sono equivalenti:*
(1) *$w \in \langle\langle v_0, \dots, v_n \rangle\rangle$;*
(2) *$v_0, \dots, v_n, w$ sono affinemente dipendenti.*

DIMOSTRAZIONE. Una implicazione segue immediatamente dal Lemma 1.2.3: se $w \in \langle\langle v_0, \dots, v_n \rangle\rangle$ allora w è combinazione baricentrica di $v_0, \dots, v_n$ e quindi $v_0, \dots, v_n, w$ sono affinemente dipendenti.

Viceversa, se $v_0, \dots, v_n, w$ sono affinemente dipendenti si hanno due relazioni
$$aw + \sum_{i=0}^n a_i v_i = 0, \qquad a + \sum_{i=0}^n a_i = 0,$$

con i coefficienti $a, a_0, \dots, a_n$ non tutti nulli.

Se fosse $a = 0$ allora anche i vettori $v_0, \dots, v_n$ sarebbero affinemente dipendenti, quindi $a \neq 0$ ed allora

$$1 = \frac{a}{a} = -\sum_{i=0}^{n} \frac{a_i}{a}, \qquad w = -\sum_{i=0}^{n} \frac{a_i}{a} v_i \in \langle\langle v_0, \dots, v_n \rangle\rangle .$$

□

LEMMA 1.2.8. *Sia K un sottospazio affine di uno spazio vettoriale V. Allora per ogni vettore $u \in V$ il sottoinsieme*

$$u + K := \{u + x \mid x \in K\}$$

è ancora un sottospazio affine detto il ***traslato di*** *K* ***tramite*** *u.*

DIMOSTRAZIONE. Dati $v_0, \dots, v_n \in u + K$ e $a_0, \dots, a_n \in \mathbb{K}$ tali che $\sum a_i = 1$, per definizione $v_i = u + x_i$ con $x_i = v_i - u \in K$ e quindi

$$\sum a_i v_i = \sum a_i (u + x_i) = (\sum a_i) u + \sum a_i x_i = u + \sum a_i x_i \in u + K .$$

□

LEMMA 1.2.9. *Sia K un sottospazio affine non vuoto di uno spazio vettoriale V. Allora il sottoinsieme $W = \{u - v \mid u, v \in K\} \subset V$ è un sottospazio vettoriale ed è l'unico sottospazio vettoriale che risulta essere un traslato di K. In particolare K è un sottospazio vettoriale se e solo se $0 \in K$.*

DIMOSTRAZIONE. Siccome K è non vuoto, pure W è non vuoto. Dati $u, v, x, y \in K$ e $a, b \in \mathbb{K}$ si ha

$$a(u - v) + b(x - y) = u - ((1 - a)u + av - bx + by) \in W ,$$

poiché $(1 - a) + a - b + b = 1$ e quindi $(1 - a)u + av - bx + by \in K$. Abbiamo provato che W è chiuso per combinazioni lineari di due vettori e dunque che è un sottospazio vettoriale.

Proviamo adesso che K è un traslato di W. Sia $u \in K$ un elemento qualsiasi e mostriamo che $K = u + W$; se $v \in K$ allora $v - u \in W$ e quindi $v = u + (v - u) \in u + W$. Viceversa, se $w \in W$ allora $w = x - y$ con $x, y \in K$ e quindi $u + w = u + x - y \in K$ poiché $1 + 1 - 1 = 1$.

Per finire, mostriamo che se K è un traslato di un sottospazio vettoriale U, allora $U = W$. Se $U = v + W$ allora $0 \in v + W$, ossia $-v \in W$, quindi $v \in W$ e di conseguenza $v + W = W$. □

Secondo il Lemma 1.2.9, per ogni sottospazio affine non vuoto $K \subset V$ esiste un unico sottospazio vettoriale W che è un traslato di K. Chiameremo W **spazio tangente** di K in V e si definisce la **dimensione di** K come la dimensione di W come spazio vettoriale. Se $K = \emptyset$ allora si pone per convenzione $\dim K = -1$.

Esercizi

ESERCIZIO 2. Sia E un sottoinsieme di uno spazio vettoriale su di un campo diverso da $\mathbb{Z}/2$. Provare che E è un sottospazio affine se e solo se per ogni $u, v \in E$ e per ogni $a \in \mathbb{K}$ vale $au + (1 - a)v \in E$.

ESERCIZIO 3. Sia E un sottoinsieme di uno spazio vettoriale sul campo $\mathbb{Z}/2$. Provare che E è un sottospazio affine se e solo se per ogni $u, v, w \in E$ vale $u + v + w \in E$.

ESERCIZIO 4. Dedurre dagli esercizi precedenti che un sottoinsieme E di uno spazio vettoriale è un sottospazio affine se e solo se per ogni $u, v, w \in E$ ed ogni $a, b, c \in \mathbb{K}$ tali che $a + b + c = 1$ vale $au + bv + cw \in E$.

ESERCIZIO 5. Sia V uno spazio vettoriale su di un campo F. Provare che se F possiede almeno $n + 1$ elementi, allora V non può essere unione di n sottospazi affini propri. In particolare uno spazio vettoriale su di un campo infinito non può essere unione finita di sottospazi affini propri. (Sugg.: induzione su n; sia per assurdo $V = \cup_{i=1}^{n} V_i$, allora a meno di traslazioni possiamo supporre $0 \in V_n$. Se $V_n \subset V_i$ per qualche $i < n$ abbiamo finito, altrimenti scegliamo $v \in V_n - \cup_{i=1}^{n-1}(V_n \cap V_i)$, $h \in V - V_n$ e consideriamo la retta affine

$L = \{tv + (1-t)h \mid t \in F\}$. Esiste allora un indice i tale che L interseca V_i in almeno due punti.)

1.3. Spazi e applicazioni affini

Per **spazio affine** su di un campo $\mathbb{K}$ intenderemo un sottospazio affine di uno spazio vettoriale sul medesimo campo. Per semplicità espositiva consideriamo esclusivamente spazi affini di dimensione finita, definiti come sottospazi affini di spazi vettoriali di dimensione finita.

Per rimarcare la differenza chiameremo **punti** (anziché vettori) gli elementi di uno spazio affine; al di là della questione terminologica uno spazio affine può anche essere pensato come uno spazio vettoriale in cui il vettore nullo è un vettore come tutti gli altri ed in cui le uniche combinazioni lineari consentite sono quelle baricentriche.

I punti sono tutti e soli i sottospazi affini di dimensione 0: sottospazi affini di dimensione 1 e 2 sono detti rispettivamente rette e piani affini.

Per il Lemma 1.2.3 possiamo caratterizzare la dipendenza affine di punti in uno spazio affine H esclusivamente in termini di combinazioni baricentriche. In altri termini, la seguente definizione non porta a contraddizioni con le precedenti.

Definizione 1.3.1. Finiti punti in uno spazio affine si dicono **affinemente indipendenti** se nessuno di essi può essere scritto come combinazione baricentrica dei rimanenti.

Consequentemente, possiamo caratterizzare la dimensione di uno spazio affine usando esclusivamente le combinazioni baricentriche.

Teorema 1.3.2. *Sia n la dimensione di uno spazio affine H. Allora il massimo numero di punti di H affinemente indipendenti è uguale a $n+1$.*

Dimostrazione. Rappresentiamo H come un sottospazio affine dello spazio vettoriale V e sia $W \subset V$ il suo spazio tangente, ossia l'unico sottospazio vettoriale traslato di H. Per definizione di dimensione si ha $\dim W = n$.

Se $v_0, \dots, v_m \in H$ sono affinemente indipendenti, allora i vettori $v_i - v_0 \in W$, $i = 1, \dots, m$, sono linearmente indipendenti e quindi $m \leq n$. Viceversa se $w_1, \dots, w_n \in W$ sono una base, allora per un qualunque elemento $v_0 \in K$ i vettori $v_0, v_0 + w_1, \dots, v_0 + w_n$ sono affinemente indipendenti. □

Definizione 1.3.3. Un'applicazione $f\colon H \to K$ tra spazi affini si dice **affine** se commuta con le combinazioni baricentriche, cioè se per ogni $v_0, \dots, v_n \in H$ e per ogni $a_0, \dots, a_n \in \mathbb{K}$ tali che $\sum a_i = 1$ vale $f(\sum a_i v_i) = \sum a_i f(v_i)$. Le applicazioni affini invertibili (ossia bigettive) vengono dette **isomorfismi affini** .

È chiaro che composizione di applicazioni affini è ancora affine. Segue dal Teorema 1.3.2 che la dimensione di uno spazio affine è invariante per isomorfismi affini.

Esempio 1.3.4. Ogni applicazione lineare tra spazi vettoriali è anche affine.

Esempio 1.3.5. Siano V uno spazio vettoriale e $v \in V$. Allora la **traslazione**

$$T_v\colon V \to V, \qquad T_v(x) = v + x,$$

è un'affinità con inversa T_{-v}. Infatti se $\sum a_i = 1$ si ha

$$T_v(\sum a_i x_i) = v + \sum a_i x_i = (\sum a_i)v + \sum a_i x_i = \sum a_i (v + x_i) = \sum a_i T_v(x_i)\,.$$

Lemma 1.3.6. *Sia $f\colon V \to W$ un'applicazione affine tra spazi vettoriali. Allora esiste un'applicazione lineare $g\colon V \to W$ tale che $f = T_{f(0)}g$. In particolare f è lineare se e solo se $f(0) = 0$.*

Dimostrazione. Già sappiamo che se f è lineare allora $f(0) = 0$. Viceversa, se $f(0) = 0$ allora per ogni $u, v \in V$ ed ogni $a, b \in \mathbb{K}$ si ha

$$f(au + bv) = f((1-a-b)0 + au + bv) = (1-a-b)f(0) + af(u) + bf(v) = +af(u) + bf(v)$$

e quindi f è lineare. Dunque l'applicazione affine $g = T_{-f(0)}f$ è lineare in quanto $g(0) = T_{-f(0)}(f(0)) = 0$. □

In generale, se $f\colon V \to W$ è un'applicazione affine tra spazi vettoriali non è detto che si possa scrivere $f = gT_v$ per opportuni $v \in V$ e g lineare. Una condizione necessaria è che $0 = gT_v(-v)$ appartenga all'immagine di f; tale condizione è anche sufficiente in quanto se esiste $v \in V$ tale che $f(-v) = 0$, allora l'applicazione $g = fT_{-v}$ risulta lineare in quanto $g(0) = 0$.

TEOREMA 1.3.7. *Siano $\mathbb{K}$ un campo con almeno tre elementi (ossia $\mathbb{K} \neq \mathbb{Z}/(2)$) e $f\colon H \to K$ un'applicazione tra due spazi affini definiti su $\mathbb{K}$. Allora f è affine se e solo se per ogni $p, q \in H$ ed ogni $t \in \mathbb{K}$ vale*

$$f((1-t)p + tq) = (1-t)f(p) + tf(q)\,.$$

In altri termini f è affine se e solo se preserva gli allineamenti ed i rapporti semplici.

DIMOSTRAZIONE. La condizione è chiaramente necessaria. Per quanto riguarda la sufficienza dimostriamo per induzione su $n \geq 1$ che

$$f(\sum_{i=0}^{n} t_i p_i) = \sum_{i=0}^{n} t_i f(p_i), \qquad p_i \in H, \quad t_i \in \mathbb{K}\,, \quad \sum t_i = 1\,. \tag{1.6}$$

Per $n = 1$ la (1.6) è vera per ipotesi; supponiamo quindi $n > 1$ e scegliamo un $b \in \mathbb{K} - \{0, 1\}$. Si può scrivere

$$\sum_{i=0}^{n} t_i p_i = (1-b)\left(\frac{t_0}{1-b}p_0 + \frac{1-b-t_0}{1-b}p_1\right) + b\left(\frac{t_0+t_1+b-1}{b}p_1 + \sum_{i=2}^{n}\frac{t_i}{b}p_i\right)$$

e per l'ipotesi induttiva

$$\begin{aligned} f(\sum_{i=0}^{n} t_i p_i) &= (1-b)f\left(\frac{t_0}{1-b}p_0 + \frac{1-b-t_0}{1-b}p_1\right) + bf\left(\frac{t_0+t_1+b-1}{b}p_1 + \sum_{i=2}^{n}\frac{t_i}{b}p_i\right) \\ &= (1-b)\left(\frac{t_0}{1-b}f(p_0) + \frac{1-b-t_0}{1-b}f(p_1)\right) + b\left(\frac{t_0+t_1+b-1}{b}f(p_1) + \sum_{i=2}^{n}\frac{t_i}{b}f(p_i)\right) \\ &= \sum_{i=0}^{n} t_i f(p_i)\,. \end{aligned}$$

□

PROPOSIZIONE 1.3.8. *Siano V uno spazio vettoriale di dimensione $n+1$ e $H \subset V$ un sottospazio affine di dimensione n che non contiene il vettore nullo. Allora per ogni applicazione affine $f\colon H \to H$ esiste unica un'applicazione lineare $g\colon V \to V$ tale che $g_{|H} = f$.*

DIMOSTRAZIONE. Sia $W \subset V$ lo spazio tangente di H. Scegliamo un vettore $v_0 \in H$, allora $H = v_0 + W$ e $v_0 \notin W$, altrimenti si avrebbe $-v_0 \in W$ e quindi $0 = v_0 - v_0 \in H$ contrariamente alle ipotesi. Sia $v_1, \ldots, v_n$ una base di W, allora $v_0, v_1, \ldots, v_n$ è una base di V e $v_0, v_0 + v_1, \ldots, v_0 + v_n \in H$.

Se $g\colon V \to V$ è lineare che estende f, allora

$$g(v_0) = f(v_0), \qquad g(v_i) = g(v_0 + v_i) - g(v_0) = f(v_0 + v_i) - f(v_0) \tag{1.7}$$

da cui segue che g è unica. Per mostrare l'esistenza sia $g\colon V \to V$ l'applicazione lineare definita sulla base $v_0, \ldots, v_n$ dalle precedenti formule (1.7). Allora per ogni $x \in H$ si ha $x - v_0 \in W$ ed esistono $a_1, \ldots, a_n \in \mathbb{K}$ tali che

$$x = v_0 + \sum a_i v_i = (1 - \sum a_i)v_0 + \sum a_i(v_0 + v_i)\,.$$

Dunque

$$\begin{aligned} f(x) &= f((1 - \sum a_i)v_0 + \sum a_i(v_0 + v_i)) = (1 - \sum a_i)f(v_0) + \sum a_i f(v_0 + v_i) \\ &= (1 - \sum a_i)g(v_0) + \sum a_i g(v_0 + v_i) = g(v_0) + \sum a_i g(v_i) = g(x)\,. \end{aligned}$$

Si noti che $g(v_0) \in H$, mentre $g(v_i) = f(v_i + v_0) - f(v_0) \in W$ per ogni $i > 0$.

□

La precedente proposizione permette di descrivere in forma matriciale le applicazioni affini $f\colon \mathbb{K}^n \to \mathbb{K}^n$. Infatti l'applicazione

$$\mathbb{K}^n \to \mathbb{K}^{n+1}, \qquad (x_1, \dots, x_n) \mapsto (1, x_1, \dots, x_n),$$

è un isomorfismo affine con il sottospazio affine $H = \{x_0 = 1\}$. Le applicazioni lineari $g\colon \mathbb{K}^{n+1} \to \mathbb{K}^{n+1}$ tali che $g(H) \subset H$ sono tutte e sole quelle che si rappresentano con una matrice a blocchi del tipo

$$\begin{pmatrix} 1 & 0 \\ A & B \end{pmatrix}, \qquad A \in M_{n,1}(\mathbb{K}),\ B \in M_{n,n}(\mathbb{K})\,.$$

Osservazione 1.3.9. La definizione di spazio affine come sottoinsieme di uno spazio vettoriale chiuso per combinazioni baricentriche è semplice e funzionale alla stragrande maggioranza delle situazioni. Tuttavia in certi casi può essere utile introdurre la nozione di **spazio affine astratto**, ad esempio nel modo seguente (che ricalca la definizione di varietà astratta).

Per ogni insieme X indichiamo con $\mathcal{A}(X)$ la collezione delle applicazioni bigettive $\phi\colon X \to H$, con H sottospazio affine di uno spazio vettoriale. Su $\mathcal{A}(X)$ consideriamo la relazione di equivalenza

$$(\phi\colon X \to H) \sim (\psi\colon X \to K) \text{ se } \psi\phi^{-1}\colon H \to K \text{ è un isomorfismo affine.}$$

Chiameremo struttura affine su X una classe di equivalenza in $\mathcal{A}(X)$. Uno spazio affine astratto è un insieme dotato di struttura affine.

È possibile definire le traslazioni in uno spazio affine non vuoto H usando esclusivamente le combinazioni baricentriche, rendendo quindi tale definizione indipendente dalla scelta dell'inclusione di H in uno spazio vettoriale. Infatti, dato due punti $p, q \in H$ possiamo definire l'applicazione

$$T_{\overrightarrow{pq}}\colon H \to H, \qquad T_{\overrightarrow{pq}}(x) = x + q - p$$

che chiaramente coincide con T_{q-p} qualora si consideri H contenuto in uno spazio vettoriale.

È utile osservare che due traslazioni $T_{\overrightarrow{pq}}, T_{\overrightarrow{rs}}\colon H \to H$ concidono ovunque se e solo se coincidono in almeno un punto. Infatti se esiste $x \in H$ tale che $T_{\overrightarrow{pq}}(x) = T_{\overrightarrow{rs}}(x)$, allora per ogni $y \in H$ vale

$$T_{\overrightarrow{pq}}(y) = y + q - p = y + q - p + x - x = y + s - r + x - x = y + s - r = T_{\overrightarrow{rs}}(y)\,.$$

Siccome $T_{\overrightarrow{pq}}(p) = q$ si ha quindi

$$T_{\overrightarrow{pq}} = T_{\overrightarrow{rs}} \iff q = T_{\overrightarrow{rs}}(p) = s - r + p \iff q - p = s - r,$$

dove l'uguaglianza più a destra va intesa in uno spazio vettoriale contenente H come sottospazio affine.

Lemma 1.3.10. *Sia $f\colon H \to K$ un'applicazione affine. Per ogni $p, q \in H$ vale*

$$f \circ T_{\overrightarrow{pq}} = T_{\overrightarrow{f(p)f(q)}} \circ f\,.$$

Dimostrazione. Per ogni $x \in H$ si ha

$$f(T_{\overrightarrow{pq}}(x)) = f(x + q - p) = f(x) + f(q) - f(p) = T_{\overrightarrow{f(p)f(q)}}(f(x))\,.$$

□

Dato uno spazio affine H, chiameremo **affinità di** H un qualunque isomorfismo affine $H \to H$. L'insieme $\mathrm{Aff}(H)$ delle affinità di H, dotato del prodotto di composizione è un gruppo, con l'identità come elemento neutro.

Teorema 1.3.11. *L'insieme di tutte le traslazioni in uno spazio affine H è un sottogruppo normale abeliano del gruppo delle affinità* $\mathrm{Aff}(H)$.

Dimostrazione. Sia $T(H) \subset \mathrm{Aff}(H)$ il sottoinsieme delle traslazioni. $T(H)$ contiene l'identità ed è chiuso rispetto all'inverso, poiché $T_{\overrightarrow{pq}} = T^{-1}_{\overrightarrow{qp}}$ per ogni $p, q \in H$.

Date due traslazioni $T_{\overrightarrow{pq}}$ e $T_{\overrightarrow{rs}}$ per ogni $x \in H$ si ha

$$T_{\overrightarrow{pq}} T_{\overrightarrow{rs}}(x) = x + s - r + q - p$$

da cui segue

$$T_{\overrightarrow{pq}} T_{\overrightarrow{rs}} = T_{\overrightarrow{rs}} T_{\overrightarrow{pq}} = T_{\overrightarrow{pt}}, \qquad t = s + q - r.$$

In particolare $T(H)$ è un sottogruppo abeliano di $\mathrm{Aff}(H)$. Data una traslazione $T_{\overrightarrow{pq}}$ ed una affinità $f\colon H \to H$, per il Lemma 1.3.10 vale $f \circ T_{\overrightarrow{pq}} = T_{\overrightarrow{f(p)f(q)}} \circ f$. Dato che f è invertibile si ha

$$f \circ T_{\overrightarrow{pq}} \circ f^{-1} = T_{\overrightarrow{f(p)f(q)}}$$

e questo implica che $T(H)$ è un sottogruppo normale. □

Sia H uno spazio affine, diremo che due sottospazi affini $A, B \subset H$ della stessa dimensione sono **paralleli**, e scriveremo $A \sim B$, se sono uno il traslato dell'altro, ossia se esistono $p, q \in H$ tali che $T_{\overrightarrow{pq}}(A) = B$; si tratta evidentemente di una relazione di equivalenza nell'insieme dei sottospazi affini di dimensione fissata.

PROPOSIZIONE 1.3.12. *Siano $f\colon H \to K$ un'applicazione affine e $A, B \subset H$ sottospazi paralleli. Allora i sottospazi affini $f(A), f(B)$ sono paralleli, ed in particolare della stessa dimensione.*

DIMOSTRAZIONE. Siano $p, q \in H$ tali che $T_{\overrightarrow{pq}}(A) = B$. Per il Lemma 1.3.10 vale $f \circ T_{\overrightarrow{pq}} = T_{\overrightarrow{f(p)f(q)}} \circ f$ e quindi

$$f(B) = f(T_{\overrightarrow{pq}}(A)) = T_{\overrightarrow{f(p)f(q)}}(f(A)).$$

□

Denotiamo con $\mathcal{L}$ l'insieme di tutte le rette affini (sottospazi affini di dimensione 1) in H e con $\sim$ la relazione di parallelismo in $\mathcal{L}$. Notiamo che, fissato un punto $p \in H$, le rette affini passanti per p formano un insieme di rappresentanti per la relazione di equivalenza $\sim$, e cioè per ogni retta affine in $L \subset H$ esiste un'unica retta L' passante per p e parallela a L. Chiameremo il quoziente $\mathcal{L}/\sim$ **iperpiano all'infinito** e l'unione

$$\hat{H} = H \cup (\mathcal{L}/\sim)$$

completamento proiettivo di H.

OSSERVAZIONE 1.3.13. Nello spazio $\mathbb{K}^n$ con coordinate $t_1, \dots, t_n$, possiamo allora considerare l'applicazione affine iniettiva

$$h\colon \mathbb{K}^n \to \mathbb{K}^{n+1}, \qquad h(t_1, \dots, t_n) = (1, t_1, \dots, t_n).$$

L'applicazione h preserva la relazione di parallelismo e la sua immagine è il sottospazio affine $H = \{x_0 = 1\}$. Possiamo quindi identificare il completamento proiettivo di $\mathbb{K}^n$ con il completamento proiettivo di H.

Ogni retta affine in $H = \{x_0 = 1\}$ è parallela ad un unico sottospazio vettoriale di dimensione 1 di $\{x_0 = 0\}$. Ogni punto di $\{x_0 = 1\}$ è contenuto in un unico sottospazio vettoriale di dimensione 1 di $\mathbb{K}^{n+1}$. *Esiste dunque una bigezione tra il completamento proiettivo di $\{x_0 = 1\} \simeq \mathbb{K}^n$ e l'insieme di tutte le rette per l'origine in $\mathbb{K}^{n+1}$.*

Esercizi

ESERCIZIO 6. Sia $f\colon \mathbb{K}^n \to \mathbb{K}^m$ un'applicazione affine e siano $f(0) = (b_1, \dots, b_m)$, $f(\delta^i) - f(0) = (a_{1i}, \dots, a_{mi})$, dove $\delta^1, \dots, \delta^n$ indica la base canonica di $\mathbb{K}^n$. Provare che f manda il punto $(x_1, \dots, x_n)$ nel punto $(y_1, \dots, y_m)$ che soddisfa la relazione

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

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

ESERCIZIO 7. Sia $H \subset \mathbb{K}^n$ un sottospazio affine non contenente 0 e $f\colon H \to \mathbb{K}^m$ un'applicazione affine. Dimostrare che f è la restrizione ad H di un'applicazione lineare $g\colon \mathbb{K}^n \to \mathbb{K}^m$.

ESERCIZIO 8. Siano $P_1 = (1,2)$, $P_2 = (3,1)$, $P_3 = (3,3)$, $Q_1 = (1,8)$, $Q_2 = (0,7)$ e $Q_3 = (7,3)$. Si determini l'affinità di $\mathbb{R}^2$ in sé che trasforma P_i in Q_i per $i = 1,2,3$.

1.4. Curve di Bezier

In alcuni algoritmi usati in grafica computerizzata giocano un ruolo fondamentale i **polinomi di Bernstein** $B_i^n(t)$, $n \geq 0$, $i \in \mathbb{Z}$, definiti dalla formula:

$$B_i^n(t) = \binom{n}{i} t^i (1-t)^{n-i}\,, \qquad \text{per} \quad 0 \leq i \leq n, \tag{1.8}$$

e $B_i^n(t) = 0$ per $i < 0$ e $i > n$. Per semplicità espositiva consideriamo i polinomi di Bernstein a coefficienti reali, sebbene gran parte delle considerazioni che seguiranno sono valide su qualsiasi campo di caratteristica 0.

Sia $V_n \subset \mathbb{R}[t]$ il sottospazio vettoriale dei polinomi di grado $\leq n$; una base naturale di V_n è data dagli $n+1$ monomi $t^0, t^1, \ldots, t^n$. Siccome

$$B_{n-i}^n(t) = \binom{n}{i} t^{n-i}(1-t)^i = \sum_{h=0}^{i} (-1)^h \binom{i}{h}\binom{n}{i} t^{n-i}t^h = \sum_{j=0}^{i} (-1)^{i-j}\binom{i}{j}\binom{n}{i} t^{n-j}$$

è immediato osservare che $B_n^n(t), \ldots, B_0^n(t)$ sono linearmente indipendenti e quindi sono una base di V_n. La matrice di cambio di base è uguale a

$$(B_n^n(t), \ldots, B_0^n(t)) = (t^n, \ldots, t^0)(m_{ji}), \qquad m_{ji} = (-1)^{i-j}\binom{i}{j}\binom{n}{i}\,.$$

Dunque la matrice di cambio base (m_{ji}) è triangolare superiore con elementi sulla diagonale uguali a $m_{jj} = \binom{n}{j}$. Ad esempio per $n = 2$ e $n = 3$ si ha:

$$(B_2^2(t), B_1^2(t), B_0^2(t)) = (t^2, 2t - 2t^2, 1 - 2t + t^2) = (t^2, t, 1)\begin{pmatrix} 1 & -2 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & 1 \end{pmatrix},$$

$$(B_3^3(t), \ldots, B_0^3(t)) = (t^3, \ldots, t^0)\begin{pmatrix} 1 & -3 & 3 & -1 \\ 0 & 3 & -6 & 3 \\ 0 & 0 & 3 & -3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Vediamo adesso alcune proprietà dei polinomi di Bernstein (le dimostrazioni sono lasciate per esercizio):

(1) (Simmetria) Vale $B_i^n(t) = B_{n-i}^n(1-t)$ per ogni n, i.
(2) (Relazioni ricorsive) Si ha $B_0^0 = 1$ e $B_i^0 = 0$ per $i \neq 0$. Per ogni $n > 0$ ed ogni i si ha
$$B_i^n(t) = tB_{i-1}^{n-1}(t) + (1-t)B_i^{n-1}(t).$$
(3) (Partizione dell'unità, vedi Figura 4) Per ogni $n \geq 0$ vale
$$\sum_{i=0}^{n} B_i^n(t) = (t + (1-t))^n = 1\,.$$
(4) (Derivate) Le derivate dei polinomi di Bernstein soddisfano la formula:
$$B_i^n(t)' = n(\, B_{i-1}^{n-1}(t) - B_i^{n-1}(t)\,)\,.$$

La proprietà $\sum_{i=0}^{n} B_i^n(t) = 1$ permette di usare i polinomi di Bernstein per definire curve parametriche nello spazio affine.

DEFINIZIONE 1.4.1. Sia $p_0, p_1, \ldots, p_n$ una successione di n punti in uno spazio affine H sul campo $\mathbb{R}$. Chiameremo **curva di Bézier** controllata da $p_0, p_1, \ldots, p_n$ l'applicazione

$$\mathbf{b}\colon [0,1] \to H, \qquad \mathbf{b}(t) = \sum_{i=0}^{n} B_i^n(t) p_i\,.$$

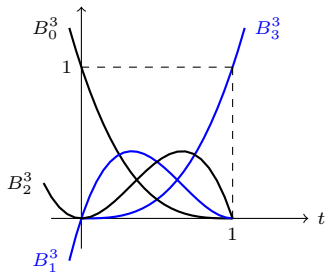


FIGURA 4. Grafici dei polinomi di Bernstein $B_i^3(t)$ per $0 \le t \le 1$ e $0 \le i \le 3$.

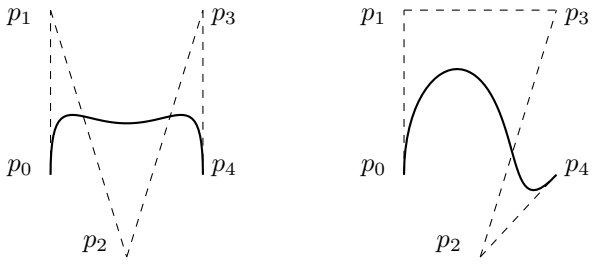


FIGURA 5. Due curve di Bézier del quarto grado; la prima controllata da p_0, p_1, p_2, p_3, p_4, la seconda da p_0, p_1, p_3, p_2, p_4.

Notiamo subito che gli estremi della curva di Bézier sono

$$\mathbf{b}(0) = p_0, \qquad \mathbf{b}(1) = p_n \ .$$

La costruzione delle curve di Bézier commuta con le applicazioni affini: nella situazione della Definizione 1.4.1, per ogni applicazione affine $f\colon H \to K$, la curva $f \circ \mathbf{b}$ è la curva di Bézier controllata da $f(p_0), f(p_1), \ldots, f(p_n)$. Infatti se $\mathbf{b}(t) = \sum_{i=0}^n B_i^n(t) p_i$ allora, siccome $\sum_{i=0}^n B_i^n(t) = 1$ si ha

$$f(\mathbf{b}(t)) = \sum_{i=0}^{n} B_i^n(t) f(p_i)\,.$$

La proprietà di simmetria dei polinomi di Bernstein implica che se $\mathbf{b}(t)$ è la curva di Bézier controllata da $p_0, p_1, \ldots, p_n$, allora $\mathbf{b}(1-t)$ è la curva di Bézier controllata da $p_n, p_{n-1}, \ldots, p_0$. Appare invece chiaro che l'insieme $\{\mathbf{b}(t) \mid t \in [0,1]\}$ non è invariante per permutazioni dei punti p_i (vedi Figura 5).

Nella sostanza, la curva di Bézier controllata da una successione di punti $p_0, \ldots, p_n$ è una approssimazione algebrica della poligonale di vertici $p_0, \ldots, p_n$. Spesso, ma non sempre, la curva di Bézier assume un aspetto "morbido".

PROPOSIZIONE 1.4.2 (Algoritmo di de Casteljau). *Sia $p_0, p_1, \ldots, p_n$ una successione di n punti in uno spazio affine H sul campo $\mathbb{R}$. Definiamo in maniera ricorsiva delle applicazioni*

$$\mathbf{b}_i^r\colon [0,1] \to H, \qquad 0 \le i, r; \quad i + r \le n;$$

ponendo $\mathbf{b}_i^0(t) = p_i$ per ogni t e

$$\mathbf{b}_i^r(t) = (1-t)\mathbf{b}_i^{r-1}(t) + t\mathbf{b}_{i+1}^{r-1}(t).$$

Allora $\mathbf{b}_0^n = \mathbf{b}$ è la curva di Bézier controllata da $p_0, p_1, \ldots, p_n$.

DIMOSTRAZIONE. Segue dalla formula $B_i^r(t) = tB_{i-1}^{r-1}(t) + (1-t)B_i^{r-1}(t)$ e da una semplice induzione che per ogni coppia i, r tale che $i + r \le n$, si ha

$$\mathbf{b}_i^r(t) = \sum_{j=0}^{r} B_j^r(t) p_{i+j}\,.$$

□

OSSERVAZIONE 1.4.3. Il primo utilizzo delle curve di Bézier è avvenuto nell'industria automobilistica attorno[3] al 1960. Infatti sia P. Bézier che P. de Casteljau lavoravano al reparto carrozzeria della Renault e della Citröen, rispettivamente.

Esercizi.

ESERCIZIO 1. Dimostrare le seguenti proprietà dei polinomi di Bernstein:

$$\sum_{j=0}^{n} \frac{j}{n} B_j^n(t) = t, \qquad B_i^n(st) = \sum_{j=i}^{n} B_i^j(s) B_j^n(t),$$

$$t^i = \sum_{j=i}^{n} \frac{\binom{j}{i}}{\binom{n}{j}} B_j^n(t), \qquad B_i^n(t) B_j^m(t) = \frac{\binom{n}{i}\binom{m}{j}}{\binom{n+m}{i+j}} B_{i+j}^{n+m}(t),$$

$$\int_0^x B_i^n(t)dt = \frac{1}{n+1} \sum_{j=i+1}^{n+1} B_j^{n+1}(x),$$

$$tB_i^n(t) = \frac{i+1}{n+1} B_{i+1}^{n+1}(t), \quad (1-t)B_i^n(t) = \frac{n-i+1}{n+1} B_i^{n+1}(t),$$

$$B_i^n(t) = \frac{i+1}{n+1} B_{i+1}^{n+1}(t) + \frac{n-i+1}{n+1} B_i^{n+1}(t)\ .$$

ESERCIZIO 2. Calcolare il massimo assoluto delle funzioni di variabile reale $B_i^n \colon [0,1] \to \mathbb{R}$.

ESERCIZIO 3. Sia $\mathbf{b}$ la curva di Bézier controllata da $p_0, p_1, \ldots, p_n \in \mathbb{R}^k$ e provare che

$$\mathbf{b}(t) = p_0 + tn(p_1 - p_0) + t^2(\cdots)$$

Mostrare inoltre che se gli n vettori $p_i - p_0$, $i = 1, \ldots, n$ sono linearmente indipendenti allora la derivata di $\mathbf{b}(t)$ è sempre diversa da 0.

ESERCIZIO 4. Sia Sia $\mathbf{b} \colon [0,1] \to \mathbb{R}^2$ la curva di Bézier di terzo grado controllata dalla poligonale $(1,0), (-1,1), (1,1), (-1,0)$. Mostrare che tale curva possiede una cuspide semplice per $t = 1/2$, ossia che

$$\mathbf{b}\left(\frac{1}{2} + s\right) = \mathbf{b}\left(\frac{1}{2}\right) + As^2 + Bs^3,$$

con A, B vettori linearmente indipendenti.

1.5. Spazi proiettivi

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

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

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

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

L'insieme $\mathbb{P}(V)$ è in bigezione naturale con l'insieme dei sottospazi vettoriali di dimensione 1 (rette per l'origine) di V.

Dato un vettore $v \in V - \{0\}$ si è soliti denotare con $[v] \in \mathbb{P}(V)$ la classe di equivalenza corrispondente.

Chiameremo $\mathbb{P}^n_{\mathbb{K}} = \mathbb{P}(\mathbb{K}^{n+1})$ **spazio proiettivo** di dimensione n sul campo $\mathbb{K}$. In assenza di ambiguità sul campo $\mathbb{K}$ scriveremo più semplicemente $\mathbb{P}^n$ in luogo di $\mathbb{P}^n_{\mathbb{K}}$.

Siccome $\mathbb{P}^n$ può essere interpretato come l'insieme delle rette per l'origine in $\mathbb{K}^{n+1}$, per l'Osservazione 1.3.13 si ha una bigezione tra $\mathbb{P}^n$ ed il completamento proiettivo dello spazio affine $\mathbb{K}^n$.

[3] Il segreto industriale che per anni ha coperto tali tecniche di progettazione non consente di dare una datazione precisa.

Diremo che un sottoinsieme $M \subset V$ è un **cono** se $0 \in M$ e se $v \in M$ implica che $\lambda v \in M$ per ogni $\lambda \in \mathbb{K}$. Se $M \subset V$ è un cono e $S \subset \mathbb{P}(V)$ è un sottoinsieme, si definisce

$$\mathbb{P}(M) = \{[v] \mid v \in M - \{0\}\} \subset \mathbb{P}(V) \quad \text{e} \quad C(S) = \{v \in V - \{0\} \mid [v] \in S\} \cup \{0\}.$$

Il sottoinsieme $C(S) \subset V$ viene detto **cono affine** di S; è immediato osservare che le applicazioni

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

sono bigettive ed una l'inversa dell'altra.

Se $W \subset V$ è un sottospazio vettoriale, chiameremo $\mathbb{P}(W)$ **sottospazio proiettivo** di $\mathbb{P}(V)$. Si noti che ogni punto di uno spazio proiettivo è un sottospazio: $[v] = \mathbb{P}(\mathbb{K}\, v)$.

Se $W \subset V$ è un iperpiano diremo che $\mathbb{P}(W)$ è un **iperpiano** di $\mathbb{P}(V)$. Poiché $\mathbb{P}(\cap_i M_i) = \cap_i \mathbb{P}(M_i)$ per ogni famiglia di coni $\{M_i\}$, si ha in particolare che intersezione di sottospazi proiettivi è ancora un sottospazio proiettivo.

Esempio 1.5.1. Siano $L \subset \mathbb{P}(V)$ un sottospazio proiettivo e $p, q \in \mathbb{P}(V)$ non appartenenti ad L. Allora esiste un iperpiano $H \subset \mathbb{P}(V)$ tale che $L \subset H$ e $p, q \notin H$.

Infatti, sia $n = \dim V$ e $p = [u]$, $q = [v]$ e $L = \mathbb{P}(W)$ con $W \subset V$ sottospazio vettoriale di dimensione $m < n$. Se $m = n - 1$ basta prendere $H = L$. Se $m < n - 1$ si consideri una base $v_1, \dots, v_n$ di V tale che $v_1, \dots, v_m$ sia base di W e scriviamo

$$u = \sum_i a_i v_i, \qquad v = \sum_i b_i v_i$$

L'ipotesi che $p, q \notin L$ equivale a dire che esistono indici $m < i, j \leq n$ tali che $a_i, b_j \neq 0$. Se esiste un indice $i > m$ per cui $a_i b_i \neq 0$ basta considerare $H = \mathbb{P}(U)$ dove U è l'iperpiano generato da $v_1, \dots, \widehat{v_i}, \dots, v_n$.

Se invece per ogni $i > m$ vale $a_i b_i = 0$ allora esistono due indici $m < i, j \leq n$ tali che $a_i \neq 0$, $b_i = 0$, $a_j = 0$ e $b_j \neq 0$. In tal caso possiamo prendere $H = \mathbb{P}(U)$, dove U è l'iperpiano generato da $v_1, \dots, \widehat{v_i}, \dots, \widehat{v_j}, \dots, v_n, v_i + v_j$.

Definizione 1.5.2 (Inviluppo di sottospazi proiettivi). Se $W_1, W_2, \dots, W_n \subset V$ sono sottospazi vettoriali scriveremo

$$\mathbb{P}(W_1) + \mathbb{P}(W_2) + \cdots + \mathbb{P}(W_n) = \mathbb{P}(W_1 + W_2 + \cdots + W_n).$$

In altri termini, se $H_1, \dots, H_n \subset \mathbb{P}(V)$ sono sottospazi proiettivi, allora $H_1 + \cdots + H_n$, è il più piccolo sottospazio proiettivo di $\mathbb{P}(V)$ che li contiene.

Dati due punti $p, q \in \mathbb{P}(V)$ scriveremo anche $\overline{pq}$ per indicare l'inviluppo proiettivo $p + q$.

Se vale $p_1 = [v_1]$, $p_2 = [v_2]$,..., $p_n = [v_n]$, con $v_1, \dots, v_n \in V - \{0\}$, allora

$$p_1 + p_2 + \cdots + p_n = \mathbb{P}(\mathrm{Span}(v_1, \dots, v_n)).$$

Se lo spazio vettoriale V ha dimensione finita, definiamo la dimensione di $\mathbb{P}(V)$ mediante la formula $\dim \mathbb{P}(V) = \dim V - 1$: in particolare l'insieme vuoto $\emptyset = \mathbb{P}(0)$ avrà dimensione -1 quando viene considerato come uno spazio proiettivo.

Spazi proiettivi di dimensione 1 e 2 si dicono rispettivamente **rette** e **piani** proiettivi. Punti contenuti in una medesima retta vengono detti **allineati**, punti (o rette) contenuti in un medesimo piano si dicono **complanari**, rette passanti per un medesimo punto si dicono **concorrenti**.

Si noti che due punti $p = [v]$ e $q = [w]$ in uno spazio proiettivo sono distinti se e solo se i vettori v, w sono linearmente indipendenti. Tre punti $p = [v]$, $q = [w]$ e $r = [u]$ sono allineati se e solo se in tre vettori u, v, w sono linearmente dipendenti, ossia se e solo se $\mathrm{Span}(u, v, w)$ ha dimensione ≤ 2.

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

$$\dim(H \cap K) + \dim(H + K) = \dim H + \dim K$$

e quindi H e K sono sghembi se e solo se $\dim(H + K) = \dim H + \dim K + 1$.

Sia $f\colon V \to W$ un isomorfismo lineare di spazi vettoriali. In particolare $f(v) = 0$ se e solo se $v = 0$ ed è ben definita la fattorizzazione al quoziente

$$[f]\colon \mathbb{P}(V) \to \mathbb{P}(W), \qquad [v] \mapsto [f(v)]\,.$$

È chiaro che $[f]$ è bigettiva, trasforma sottospazi proiettivi in sottospazi proiettivi della stessa dimensione e preserva le relazioni di incidenza, concorrenza, allineamento, complanarità ecc.

Definizione 1.5.3. Un'applicazione $\phi\colon \mathbb{P}(V) \to \mathbb{P}(W)$ si dice un **isomorfismo proiettivo** o **proiettività** se è indotta per passaggio al quoziente da una applicazione lineare invertibile $f\colon V \to W$ mediante la regola

$$\phi([v]) = [f(v)], \qquad v \in V - \{0\},$$

e scriveremo in tal caso $\phi = [f]$.

Ogni proiettività è bigettiva e la sua inversa è ancora una proiettività. Più precisamente, se $\phi = [f]$, allora $\phi^{-1} = [f^{-1}]$.

La geometria proiettiva si occupa di studiare i luoghi geometrici (configurazioni, chiusi di Zariski, varietà ecc.) contenuti in uno spazio proiettivo, a meno di isomorfismi proiettivi. Per il momento ci occuperemo solamente di configurazioni, ossia di famiglie finite di sottospazi proiettivi che soddisfano alcune relazioni di incidenza, allineamento eccetera.

Esempio 1.5.4. Siano V, W due spazi vettoriali della stessa dimensione e siano $H \subset V$ e $K \subset W$ due sottospazi della stessa dimensione. Allora esiste una proiettività $\psi\colon \mathbb{P}(V) \to \mathbb{P}(W)$ tale che $\psi(\mathbb{P}(H)) = \mathbb{P}(K)$. A tal fine basta considerare $\psi = [f]$, con $f\colon V \to W$ un qualunque isomorfismo lineare tale che $f(H) = K$.

In particolare, se V ha dimensione $n+1$, la scelta di una base di V, ossia di un isomorfismo $\mathbb{K}^{n+1} \to V$ induce un isomorfismo proiettivo $\mathbb{P}^n \simeq \mathbb{P}(V)$. Lo stesso accade per qualunque scelta di un sistema di coordinate, ossia di una base di $V^\vee$, ossia di un isomorfismo lineare $V \to \mathbb{K}^{n+1}$.

Esempio 1.5.5. Siano $H \subset \mathbb{P}(V)$ un iperpiano e $W \subset \mathbb{P}(V)$ un sottospazio proiettivo di dimensione m. Se W non è contenuto in H allora $H + W = \mathbb{P}(V)$ e per la formula di Grassmann $\dim H \cap W = m - 1$.

Per ogni punto $p \in W - H = \{q \in W \mid q \notin H\}$ si ha $p + (H \cap W) = W$. Infatti $p + (H \cap W) \subset W$ (i due sottospazi p e $W \cap H$ sono entrambi contenuti in W) e per Grassmann $\dim(p + (H \cap W)) = 1 + (m-1) = \dim W$.

Siano $\mathbb{K}$ un campo finito con q elementi e V è uno spazio vettoriale di dimensione $n+1$ su $\mathbb{K}$, allora $\mathbb{P}(V)$ è isomorfo a $\mathbb{P}^n_{\mathbb{K}}$ e quindi il numero di punti di $\mathbb{P}(V)$, e più in generale il numero di sottospazi proiettivi di dimensione fissata, dipende solo da n e $\mathbb{K}$. La prossima proposizione fornisce un metodo di calcolo di tale quantità.

Proposizione 1.5.6. *Siano $\mathbb{K}$ un campo finito con q elementi, n un intero positivo e si consideri il polinomio*

$$\frac{1}{t}\left(\prod_{i=0}^{n}(1+tq^i) - 1\right) = \sum_{p=0}^{n} a_p^n t^p \in \mathbb{Z}[t]\,.$$

Allora per ogni $0 \le p \le n$ il numero s_p^n dei sottospazi proiettivi di dimensione p contenuti in $\mathbb{P}^n_{\mathbb{K}}$ è uguale a $s_p^n = \dfrac{a_p^n}{\prod_{i=0}^{p} q^i}$.

Dimostrazione. È istruttivo trattare prima il caso $p = 0$, ossia calcolare quanti punti contiene lo spazio proiettivo di dimensione n. Siccome

$$\frac{1}{t}\left(\prod_{i=0}^{n}(1+tq^i) - 1\right) = \sum_{i=0}^{n} q^i + t(\cdots)$$

dimostriamo per induzione su n che $\mathbb{P}^n_{\mathbb{K}}$ contiene $1 + q + \cdots + q^n$ punti. Per l'ipotesi induttiva ogni iperpiano H di $\mathbb{P}^n_{\mathbb{K}}$ contiene $1 + q + \cdots + q^{n-1}$ punti; basta adesso osservare che $\mathbb{P}^n_{\mathbb{K}} - H$

è lo spazio affine $\mathbb{K}^n$ che contiene q^n punti. Similmente la proposizione è vera per $p = n$: si verifica immediatamente che $a_n^n = \prod_{i=0}^n q^i$.

Consideriamo adesso il caso generale. Per ogni coppia di interi $-1 \le p \le n$ indichiamo con s_p^n il numero di sottospazi proiettivi di $\mathbb{P}^n$ di dimensione p. Vale allora la formula ricorsiva

$$s_{-1}^n = s_n^n = 1, \qquad s_p^n = s_p^{n-1} + q^{n-p} s_{p-1}^{n-1}, \quad 0 \le p < n\,.$$

Infatti se $0 \le p \le n-1$ e scriviamo $\mathbb{P}^n = \mathbb{K}^n \cup \mathbb{P}^{n-1}$ (parte affine unito iperpiano all'infinito), i sottospazi di dimensione p si dividono in due classi disgiunte: quelli contenuti nell'iperpiano all'infinito, che sono s_p^{n-1}, e quelli del tipo $a + H$, con $a \in \mathbb{K}^n$ e $H \subset \mathbb{P}^{n-1}$ di dimensione $p-1$. I punti $a \in \mathbb{K}^n$ sono q^n, ma $a + H = b + H$ se e solo se $b \in (a+H) \cap \mathbb{K}^n$. Basta adesso osservare che $(a + H) \cap \mathbb{K}^n$ è il complementare di un iperpiano in $\mathbb{P}^p$ e quindi contiene q^p punti.

D'altra parte, siccome

$$\frac{1}{t}\prod_{i=0}^n (1 + tq^i) = \frac{1}{t} + \sum_{p=0}^n a_p^n t^p = \left(\frac{1}{t} + \sum_{p=0}^{n-1} a_p^{n-1} t^p\right)(1 + tq^n)$$

si hanno le formule ricorsive

$$a_p^n = a_p^{n-1} + q^n a_{p-1}^{n-1}, \qquad 0 \le p\,,$$

e dividendo per $\prod_{i=0}^p q^i$ si ottiene

$$\frac{a_p^n}{\prod_{i=0}^p q^i} = \frac{a_p^{n-1}}{\prod_{i=0}^p q^i} + q^{n-p}\frac{a_{p-1}^{n-1}}{\prod_{i=0}^{p-1} q^i}\,.$$

La conclusione segue dunque dal principio di definizione ricorsiva. □

Per la formula di Grassmann, due rette in $\mathbb{P}^2$ sono sempre incidenti. Se $p = [u] \ne q = [v]$, $r = [w] \ne s = [z]$ si ha

$$\overline{pq} \cap \overline{rs} = \mathbb{P}(\mathrm{Span}(u, v) \cap \mathrm{Span}(w, z))\,,$$

e quindi bisogna trovare le soluzioni non banali del sistema lineare (3 equazioni e 4 incognite)

$$x_0 u + x_1 v = y_0 w + y_1 z\,.$$

Ad esempio, se $p = [1, 0, 0]$, $q = [0, 1, 0]$, $r = [0, 0, 1]$ e $s = [1, 1, 1]$, siccome

$$(1, 1, 0) = (1, 0, 0) + (0, 1, 0) = -(0, 0, 1) + (1, 1, 1)$$

si ha che $\overline{pq} \cap \overline{rs} = [1, 1, 0]$.

Esempio 1.5.7. Sia p un punto di $\mathbb{P}^2$. L'insieme di tutte le rette $L \subset \mathbb{P}^2$ che contengono p viene detto **fascio di rette** passanti per p. Più raramente il termine fascio viene chiamato *pennello* o *schiera*.

Se $H \subset \mathbb{P}^2$ è una retta che non contiene p vi è una ovvia applicazione

$$H \to \{\text{fascio di rette per } p\}, \qquad q \mapsto \overline{pq},$$

che è iniettiva in quanto $p \notin H$ ed è surgettiva in quanto due rette in $\mathbb{P}^2$ si intersecano sempre.

La comprensione del teorema di Pappo (III secolo D.C.) e di un teorema scoperto dal matematico francese Girard Desargues nel 1639 è stata una delle principali motivazioni dello sviluppo, nel XIX secolo, della geometria proiettiva.

Teorema 1.5.8 (Desargues). *Siano dati 7 punti distinti $o, p_1, p_2, p_3, q_1, q_2, q_3 \in \mathbb{P}^2$ tali che ciascuna delle tre terne (o, p_1, q_1), (o, p_2, q_2) e (o, p_3, q_3) sia formata da tre punti allineati. Allora i tre punti*

$$r_1 = \overline{p_2 p_3} \cap \overline{q_2 q_3}, \quad r_2 = \overline{p_1 p_3} \cap \overline{q_1 q_3}, \quad r_3 = \overline{p_1 p_2} \cap \overline{q_1 q_2},$$

sono allineati (Figura 6).

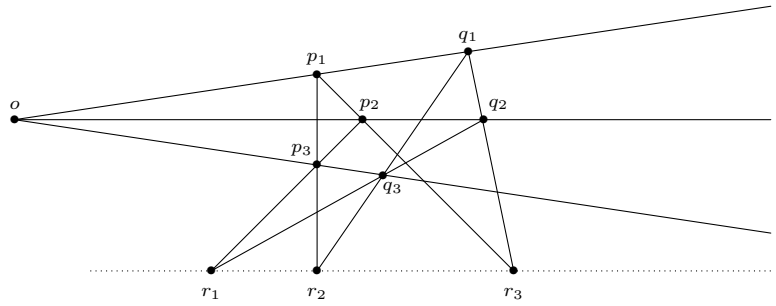


FIGURA 6. Il teorema di Desargues.

DIMOSTRAZIONE. Sia $\mathbb{P}^2 = \mathbb{P}(V)$, con V spazio vettoriale di dimensione 3 e scegliamo 7 vettori $u, v_1, v_2, v_3, w_1, w_2, w_3 \in V - \{0\}$ tali che

$$o = [u], \quad p_i = [v_i], \quad q_i = [w_i].$$

Per ipotesi o appartiene alla retta $\overline{p_1 q_1}$. Questo equivale a dire che u è una combinazione lineare di v_1 e w_1: diciamo $u = a_1 v_1 + b_1 w_1$. Similmente si ha

$$u = a_1 v_1 + b_1 w_1 = a_2 v_2 + b_2 w_2 = a_3 v_3 + b_3 w_3.$$

Da tali uguaglianze deduciamo che

$$a_1 v_1 - a_2 v_2 = b_2 w_2 - b_1 w_1, \quad a_2 v_2 - a_3 v_3 = b_3 w_3 - b_2 w_2, \quad a_1 v_1 - a_3 v_3 = b_3 w_3 - b_1 w_1.$$

da cui segue

$$r_3 = [a_1 v_1 - a_2 v_2], \quad r_1 = [a_2 v_2 - a_3 v_3], \quad r_2 = [a_1 v_1 - a_3 v_3].$$

I tre punti r_1, r_2 ed r_3 sono allineati poiché

$$(a_1 v_1 - a_2 v_2) + (a_2 v_2 - a_3 v_3) + (a_1 v_1 - a_3 v_3) = 0.$$

□

OSSERVAZIONE 1.5.9. Il teorema di Desargues ha senso anche se esiste un indice i tale che $p_i = q_i$, ed in tal caso la sua validità è evidente perché se ad esempio $p_1 = q_1$ allora $r_2 = r_3 = p_1 = q_1$, mentre l'enunciato perde di significato se $p_i = q_i$ per almeno due indici i.

Esercizi

ESERCIZIO 9. Se H, K sono sottospazi non vuoti di uno spazio proiettivo allora

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

ESERCIZIO 10. Siano $p = [1, 0, \ldots, 0]$ e $q = [a_0, a_1, \ldots, a_n]$ punti distinti di $\mathbb{P}^n$. Provare che i punti della retta $\overline{pq}$ diversi da p sono tutti e soli quelli di coordinate

$$[a_0 + t, a_1, \ldots, a_n], \qquad t \in \mathbb{K}\ .$$

ESERCIZIO 11. Sia V uno spazio vettoriale di dimensione $n+1$. Provare che ogni sottospazio proiettivo di $\mathbb{P}(V)$ di dimensione k è intersezione di $n-k$ iperpiani proiettivi.

ESERCIZIO 12. Nella situazione della Proposizione 1.5.6, provare che

$$s_p^n = \sum_S q^{\sum_{i=0}^p a_i}, \quad \text{dove} \quad S = \left\{(a_0, \ldots, a_p) \in \mathbb{N}^{p+1} \mid a_0 \le a_1 \le \cdots \le a_p \le n - p\right\}\ ,$$

ed in particolare che il numero di rette in $\mathbb{P}^n_{\mathbb{K}}$ è uguale a

$$s_1^n = \sum_{0 \le i \le j \le n-1} q^{i+j}\ .$$

1.6. Sistemi di riferimento e coordinate omogenee

DEFINIZIONE 1.6.1. Diremo che $s+1$ punti $p_0, \dots, p_s \in \mathbb{P}(V)$ sono **proiettivamente indipendenti** se il sottospazio $\langle p_0, \dots, p_s \rangle$ da essi generato ha dimensione esattamente s.

Ad esempio, due punti in $\mathbb{P}^1$ sono proiettivamente indipendenti se e solo se sono distinti; tre punti in $\mathbb{P}^2$ sono proiettivamente indipendenti se e solo se non sono allineati.
È fondamentale osservare che, se $v_0, \dots, v_s \in V - \{0\}$, allora i punti $[v_0], \dots, [v_s]$ sono proiettivamente indipendenti se e solo se i vettori $v_0, \dots, v_s$ sono linearmente indipendenti.

DEFINIZIONE 1.6.2. Diremo che $n+2$ punti $p_0, \dots, p_{n+1} \in \mathbb{P}(V)$ sono un **sistema di riferimento** se $\dim V = n+1$ e se per ogni indice i fissato, i punti p_j, per $j \neq i$, sono proiettivamente indipendenti.

Sono esempi di sistemi di riferimento:

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

LEMMA 1.6.3. *Sia V uno spazio vettoriale di dimensione $n+1$. Allora $n+2$ punti $p_0, \dots, p_{n+1} \in \mathbb{P}(V)$ sono un sistema di riferimento se e solo se esiste una base $e_0, \dots, e_n \in V$ tale che $p_i = [e_i]$ per $i = 0, \dots, n$ e $p_{n+1} = [e_0 + e_1 + \cdots + e_n]$.*

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

Sia viceversa $p_0, \dots, p_{n+1}$ un sistema di riferimento e scegliamo vettori $v_0, \dots, v_n \in V$ tali che $p_i = [v_i]$ per ogni $i = 0, \dots, n$. Siccome $p_0, \dots, p_n$ sono indipendenti, ne segue che $v_0, \dots, v_n$ è una base di V e quindi esistono $a_0, \dots, a_n \in \mathbb{K}$ tali che $p_{n+1} = [e_{n+1}]$, dove $e_{n+1} = a_0 v_0 + \cdots + a_n v_n$. Se fosse $a_i = 0$ per qualche indice i, allora gli $n+1$ vettori

$$v_0, \dots, v_{i-1}, e_{n+1}, v_{i+1}, \dots, v_n$$

sarebbero linearmente dipendenti e quindi $p_0, \dots, p_{n+1}$ non potrebbe essere un sistema di riferimento. Quindi $a_i \neq 0$ per ogni i ed è sufficiente considerare la base $e_i = a_i v_i$, $i = 0, \dots, n$. □

Per quadrilatero completo in $\mathbb{P}^n$ si intende la configurazione di una quaterna di punti a, b, c, d (i vertici) e delle 6 rette $\overline{ab}, \overline{ac}, \overline{ad}, \overline{bc}, \overline{bd}, \overline{cd}$ (i lati). Il quadrilatero si dice **non degenere** se tra i 4 punti non ne esistono 3 allineati.

Se $n = 2$, un quadrilatero completo è non degenere se e solo se i vertici formano un sistema di riferimento proiettivo.

ESEMPIO 1.6.4. Siano $a, b, c, d \in \mathbb{P}^2$ i vertici di un quadrilatero completo non degenere. Allora i tre punti di intersezione delle coppie di lati opposti

$$p = \overline{ab} \cap \overline{cd}, \qquad q = \overline{ac} \cap \overline{bd}, \qquad r = \overline{ad} \cap \overline{bc}$$

sono distinti. Inoltre p, q, r sono allineati se e solo se il campo $\mathbb{K}$ ha caratteristica 2.

Infatti possiamo trovare coordinate proiettive tali che

$$a = [1,0,0], \quad b = [0,1,0], \quad c = [0,0,1], \quad d = [1,1,1],$$

da cui segue

$$p = [1,1,0], \quad q = [1,0,1], \quad r = [0,1,1],$$

ed il determinante

$$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} = -2$$

si annulla se e solo se il campo è di caratteristica 2.

Chiameremo **sistema di coordinate omogenee** su $\mathbb{P}(V)$ un qualsiasi sistema di coordinate lineari su V. Se $\mathbb{P}(V)$ ha dimensione finita n, la scelta di un sistema di coordinate omogenee definisce un isomorfismo proiettivo $\mathbb{P}(V) = \mathbb{P}^n$ e quindi permette di rappresentare ogni punto $p \in \mathbb{P}(V)$ nella forma $p = [a_0, \dots, a_n]$, con i numeri $a_i \in \mathbb{K}$ non tutti nulli.

Tale rappresentazione non è unica: infatti vale $[a_0,\dots,a_n]=[b_0,\dots,b_n]$ se e solo se esiste $\lambda\in\mathbb{K}-\{0\}$ tale che $b_i=\lambda a_i$ per ogni i.

Le seguenti quaterne di punti di $\mathbb{P}^2$, descritte in coordinate omogenee, sono sistemi di riferimento:

(1) $[1,0,0],[0,1,0],[0,0,1],[1,1,1]$;

(2) $[1,0,0],[1,1,0],[0,0,1],[0,1,1]$.

La prima non è altro che la rappresentazione del Lemma 1.6.3 per la base canonica; la seconda quaterna è invece riferita alla base $e_0=(-1,0,0), e_1=(1,1,0), e_2=(0,0,1)$, poiché $[1,0,0]=[-1,0,0]$.

LEMMA 1.6.5. *Siano $f,g\colon V\to W$ due applicazioni lineari iniettive e consideriamo le applicazioni*

$$\phi,\psi\colon \mathbb{P}(V)\to\mathbb{P}(W),\qquad \phi([v])=[f(v)],\quad \psi([v])=[g(v)]\,.$$

Allora vale $\phi=\psi$ se e solo se esiste $\lambda\in\mathbb{K}-\{0\}$ tale che $f=\lambda g$.

DIMOSTRAZIONE. L'unica implicazione non banale è il "solo se". Supponiamo quindi $\phi=\psi$ e fissiamo una base $v_0,\dots,v_n$ di V. L'iniettività di g implica allora che i vettori $g(v_0),\dots,g(v_n)$ sono linearmente indipendenti.

Dalle relazioni $[f(v_i)]=[g(v_i)]$ si ricava che esistono $n+1$ scalari invertibili λ_i tali che

$$f(v_i)=\lambda_i g(v_i),\qquad i=0,\dots,n\,.$$

Siccome f,g sono univocamente determinate dai valori che assumono sulla base $v_0,\dots,v_n$, per concludere basta dimostrare che $\lambda_i=\lambda_j$ per ogni i,j. Dalla relazione

$$[f(v_0+\cdots+v_n)]=[g(v_0+\cdots+v_n)]$$

deduciamo che esiste un $\lambda\in\mathbb{K}-\{0\}$ tale che

$$f(v_0+\cdots+v_n)=\lambda g(v_0+\cdots+v_n)=\sum_i \lambda g(v_i)\,.$$

D'altra parte

$$f(v_0+\cdots+v_n)=\sum_i f(v_i)=\sum_i \lambda_i g(v_i)$$

e l'indipendenza lineare dei vettori $g(v_0),\dots,g(v_n)$ implica che $\lambda_i=\lambda$ per ogni indice i. □

Si denota $\mathrm{PGL}(V)$ il gruppo delle proiettività di $\mathbb{P}(V)$ in sé. Per definizione esiste un omomorfismo surgettivo di gruppi $\mathrm{GL}(V)\to\mathrm{PGL}(V)$ che, per il lemma precedente ha come nucleo i multipli dell'identità. Si indica anche $\mathrm{PGL}_n(\mathbb{K})=\mathrm{PGL}(\mathbb{K}^n)$, e quindi $\mathrm{PGL}_{n+1}(\mathbb{K})$ è il gruppo degli automorfismi proiettivi di $\mathbb{P}^n_{\mathbb{K}}$.

PROPOSIZIONE 1.6.6. *Dati due sistemi di riferimento $p_0,\dots,p_{n+1}$ e $q_0,\dots,q_{n+1}$ di $\mathbb{P}^n$, esiste un'unica proiettività $\varphi\in\mathrm{PGL}_{n+1}(\mathbb{K})$ tale che $\varphi(p_i)=q_i$ per ogni i.*

DIMOSTRAZIONE. L'esistenza segue immediatamente dal Lemma 1.6.3, mentre per l'unicità non è restrittivo supporre $p_i=q_i$ per ogni i. Sia $e_0,\dots,e_n$ una base di $\mathbb{K}^{n+1}$ tale che $p_i=[e_i]$ con $e_{n+1}=\sum e_i$ e $f\colon\mathbb{K}^{n+1}\to\mathbb{K}^{n+1}$ lineare invertibile tale che $[f]p_i=p_i$ per ogni i. Allora esistono costanti $a_0,\dots,a_{n+1}\in\mathbb{K}$ tali che $f(e_i)=a_ie_i$ per ogni i. Poiché $e_0,\dots,e_n$ sono una base segue necessariamente che $a_i=a_{n+1}$ per ogni $i=0,\dots,n$ e quindi f è un multiplo dell'identità. □

Per $n=1$ possiamo scrivere $\mathbb{P}^1=\mathbb{K}\cup\{\infty\}$, dove $\mathbb{K}=\{[1,t]\mid t\in\mathbb{K}\}$ e $\infty=[0,1]$ (intuitivamente $[0,1]$ è il limite per $t\to\infty$ di $[1/t,1]=[1,t]$). Ogni proiettività ϕ di $\mathbb{P}^1$ in sé è rappresentata da $\phi([x_0,x_1])=[ax_0+bx_1,cx_0+dx_1]$, $ad\neq bc$, che, nella coordinata affine $t=x_1/x_0$ diventa

$$\phi(t)=\frac{cx_0+dx_1}{ax_0+bx_1}=\frac{c+dt}{a+bt},\qquad \text{con } ad-bc\neq 0\,.$$

TEOREMA 1.6.7 (Pappo). *Siano $p_1, \dots, p_6$ punti distinti e non allineati di $\mathbb{P}^2$, divisi in due terne allineate p_1, p_3, p_5 e p_2, p_4, p_6 (Figura 7).*

Allora i tre punti

$$\overline{p_1p_2} \cap \overline{p_4p_5}, \quad \overline{p_2p_3} \cap \overline{p_5p_6}, \quad \overline{p_3p_4} \cap \overline{p_6p_1},$$

sono allineati.

DIMOSTRAZIONE. Vediamo una prima dimostrazione che utilizza conteggi elementari ma piuttosto grezzi con le coordinate omogenee. Altre dimostrazioni più concettuali saranno date in seguito.

Siano L la retta contenente p_1, p_3, p_5 e M la retta contenente p_2, p_4, p_6. A meno di permutazioni cicliche degli indici non è restrittivo supporre che nessuno dei 4 punti $p_1, \dots, p_4$ sia uguale al punto o di intersezione di L e M.

Dunque $p_1, \dots, p_4$ sono un sistema di riferimento proiettivo ed esiste un sistema di coordinate omogenee tali che

$$p_1 = [1,0,0], \quad p_3 = [1,1,0], \quad p_2 = [0,0,1], \quad p_4 = [0,1,1]\,.$$

La retta passante per p_1, p_3 è dunque formata dai punti di coordinate omogenee $[x+y, y, 0]$. Siccome $p_5 \neq p_1, p_3$ si ha $p_5 = [x+y, y, 0]$ con x, y entrambi non nulli; ponendo $a = (x+y)/y$ si può scrivere $p_5 = [a, 1, 0]$.

Con analogo ragionamento applicato ai punti p_6, o si ha

$$o = [0,1,0], \quad p_5 = [a,1,0], \quad p_6 = [0,1,b], \qquad a, b \in \mathbb{K} - \{1\}\,,$$

e l'ipotesi $p_5 \neq p_6$ implica che a e b non possono essere contemporaneamente nulli. Siccome:

$$a(1,0,0) - (0,0,1) = -(0,1,1) + (a,1,0),$$
$$b(a-1)(0,0,1) + a(1,1,0) = (a,1,0) + (a-1)(0,1,b),$$
$$(1-b)(1,1,0) + b(0,1,1) = (0,1,b) + (1-b)(1,0,0),$$

si hanno le intersezioni

$$\overline{p_1p_2} \cap \overline{p_4p_5} = [a,0,-1], \qquad \overline{p_2p_3} \cap \overline{p_5p_6} = [a, a, b(a-1)], \qquad \overline{p_3p_4} \cap \overline{p_6p_1} = [1-b, 1, b],$$

e l'allineamento dei tre punti segue, *tenendo presente la commutatività del prodotto ($ab = ba$)*, dalla relazione:

$$(a, a, b(a-1)) = b(a,0,-1) + a(1-b,1,b)\,.$$

□

ESEMPIO 1.6.8 (reti di iperpiani). Sia $H \subset \mathbb{P}^n$ un sottospazio proiettivo di dimensione r. L'insieme $\mathcal{F}$ di tutti gli iperpiani di $\mathbb{P}^n$ che contengono H viene detta una **rete di iperpiani**. È chiaro che se $r = n$ allora $\mathcal{F} = \emptyset$, mentre se $r = n-1$ allora $\mathcal{F} = \{H\}$. Il numero $n-r-1$ viene detto la dimensione della rete $\mathcal{F}$: una rete di iperpiani di dimensione 1 viene anche detta **fascio di iperpiani**.

Se $x_0, \dots, x_n$ è un sistema di coordinate omogenee tali che H è definito dalle equazioni $x_{r+1} = \cdots = x_n = 0$, allora gli elementi di $\mathcal{F}$ sono tutti e soli gli iperpiani definiti da una equazione del tipo

$$a_{r+1}x_{x+1} + \cdots + a_n x_n = 0, \qquad a_i \in \mathbb{K} \text{ non tutti nulli.} \tag{1.9}$$

È chiaro che ogni iperpiano definito come in (1.9) contiene H. Viceversa, se un iperpiano K di equazione $\sum_{i=0}^n a_i x_i = 0$ contiene H, allora contiene in particolare i punti

$$[\underbrace{0, \dots, 0}_{j \text{ zeri}}, 1, 0, \dots, 0], \qquad 0 \leq j < r$$

e questo è possibile se e solo se $a_i = 0$ per ogni $i = 0, \dots, r$. Si noti che siccome $\{x_i = 0\} \in \mathcal{F}$ per ogni $r < i \leq n$ si ha che $H = \bigcap_{K \in \mathcal{F}} K$.

Esercizi

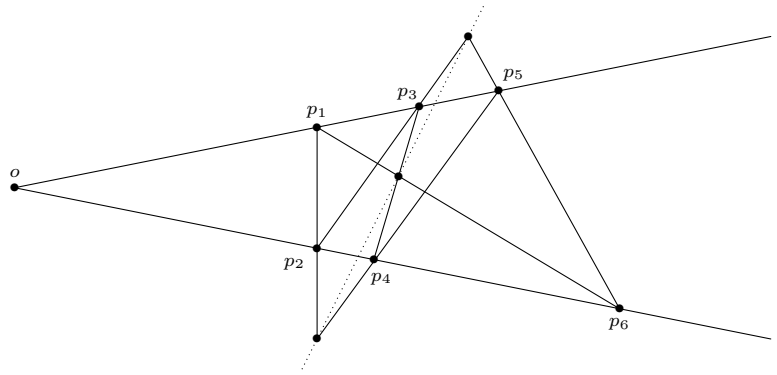


FIGURA 7. Il teorema di Pappo.

ESERCIZIO 13. Determinare le proiettività di $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ in sé che preservano i seguenti sottoinsiemi di $\mathbb{C}$:

$$\mathbb{R} = \{x + iy \mid y = 0\}, \qquad H = \{x + iy \mid y > 0\}, \qquad \overline{H} = \{x + iy \mid y \geq 0\},$$
$$\Delta = \{x + iy \mid x^2 + y^2 < 1\}, \qquad \overline{\Delta} = \{x + iy \mid x^2 + y^2 \leq 1\}\,.$$

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

1.7. Proiezioni

Prima di affrontare il tema proiezioni, osserviamo che per ogni proiettività $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ l'insieme dei suoi punti fissi si decompone nella forma

$$\mathrm{Fix}(\psi) = \{p \in \mathbb{P}^n \mid \psi(p) = p\} = H_1 \cup \cdots \cup H_h$$

dove gli H_i sono sottospazi proiettivi disgiunti e tali che $\sum_{i=1}^{h}(\dim H_i + 1) \leq n + 1$. Infatti se ψ è indotta da un'applicazione lineare invertibile $f\colon \mathbb{K}^{n+1} \to \mathbb{K}^{n+1}$, allora i punti fissi di ψ corrispondono agli autovettori di f. Se $\lambda_1, \ldots, \lambda_h \in \mathbb{K}$ sono gli autovalori di f, allora il luogo dei punti fissi di ψ coincide con l'unione dei sottospazi $H_i = \mathbb{P}(\ker(f - \lambda_i I))$. Tale unione è disgiunta in quanto ad ogni autovettore corrisponde un unico autovalore. Inoltre la dimensione di H_i è uguale alla molteplicità geometrica dell'autovalore λ_i diminuita di 1, e la disuguaglianza $\sum_{i=1}^{h}(\dim H_i + 1) \leq n + 1$ segua dai ben noti risultati di algebra lineare.

LEMMA 1.7.1. *Sia $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ una proiettività e siano H, K due sottospazi proiettivi contenuti nel luogo dei punti fissi* $\mathrm{Fix}(\psi)$. *Se $H \cap K \neq \emptyset$, allora $H + K \subset \mathrm{Fix}(\psi)$.*

DIMOSTRAZIONE. Siano $U, V \subset \mathbb{K}^{n+1}$ i due sottospazi vettoriali tali che $H = \mathbb{P}(U)$, $K = \mathbb{P}(V)$, e sia $f\colon \mathbb{K}^{n+1} \to \mathbb{K}^{n+1}$ un automorfismo lineare che induce ψ. Siccome $\psi_{|H}$ è l'identità esiste uno scalare non nullo $h \in \mathbb{K}$ tale che $f(u) = hu$ per ogni $u \in U$; similmente esiste $k \in \mathbb{K}$ tale che $f(v) = kv$ per ogni $v \in V$. Se $H \cap K \neq \emptyset$ allora $U \cap V$ contiene un vettore non nullo e questo implica $h = k$ ed allora $f(x) = hx = kx$ per ogni $x \in U + V$. □

Siano $o \in \mathbb{P}^n$ un punto e $L, M \subset \mathbb{P}^n$ due iperpiani tali che $o \notin M \cup L$. Allora, per ogni $p \in L$ si ha $o \neq p$ e la retta $\overline{op}$ interseca M in un unico punto, dato che $o \notin M$. Possiamo quindi definire un'applicazione

$$\varphi\colon L \to M, \qquad \phi(p) = \overline{op} \cap M\,,$$

detta **proiezione di centro** o (Figura 8).

È facile dimostrare che la proiezione φ appena definita è un isomorfismo proiettivo. Infatti, siccome $o \notin M$ possiamo scegliere un sistema di coordinate omogenee $x_0, \ldots, x_n$ tali che $o = [1, 0, \ldots, 0]$ e $M = \mathbb{P}(\{x_0 = 0\})$. Siccome $o \notin L$ l'equazione di L sarà del tipo $x_0 = \sum_{i=1}^{n} a_i x_i$ e possiamo considerare l'isomorfismo proiettivo

$$\psi\colon \mathbb{P}^{n-1} \to L, \qquad [y_1, \ldots, y_n] \mapsto [\sum a_i y_i, y_1, \ldots, y_n]\,.$$

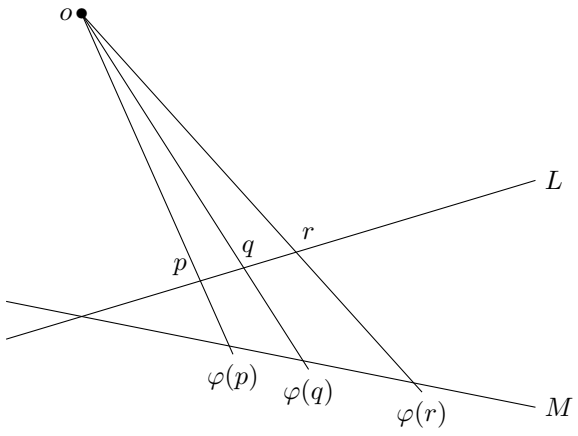


FIGURA 8. Proiezione $\varphi\colon L \to M$ di centro o.

Ma allora la composizione $\varphi\psi$ coincide con l'isomorfismo proiettivo

$$\varphi\psi\colon \mathbb{P}^{n-1} \to M, \qquad [y_1, \dots, y_n] \mapsto [0, y_1, \dots, y_n]\,.$$

Segue immediatamente dalle definizioni che se $\varphi\colon L \to M$ è la proiezione di centro o, allora anche $\varphi^{-1}\colon M \to L$ è la proiezione di centro o.

Dati due iperpiani distinti $L, M \subset \mathbb{P}^n$, non tutti gli isomorfismi proiettivi $L \to M$ sono proiezioni, come si evince dal seguente teorema.

TEOREMA 1.7.2. *Dati due iperpiani distinti $L, M \subset \mathbb{P}^n$, un isomorfismo proiettivo $\varphi\colon L \to M$ è una proiezione se e solo se $\varphi(p) = p$ per ogni $p \in L \cap M$.*

DIMOSTRAZIONE. Il risultato è ovvio se $n = 1$. Supponiamo $n \geq 2$. Una implicazione è banale: se φ è una proiezione di centro o, allora per ogni $p \in L \cap M$ si ha $\varphi(p) = \overline{op} \cap M = p$.

Viceversa sia $H = L \cap M$, che per la formula di Grassmann ha dimensione $n-2$, e fissiamo un sistema di riferimento proiettivo $p_0, \dots, p_n$ di L tale che $p_2, \dots, p_n \in H$ (Esercizio: dimostrare). Denotiamo $q_0 = \varphi(p_0)$, $q_1 = \varphi(p_1)$, $r = H \cap \overline{p_0 p_1}$.

Siccome $\varphi(r) = r$ le due rette distinte $\overline{p_0 p_1}$ e $\overline{q_0 q_1} = \varphi(\overline{p_0 p_1})$ di $\mathbb{P}^n$ hanno intersezione non vuota (entrambe contengono r) e quindi $P = \overline{p_0 p_1} + \overline{q_0 q_1}$ ha dimensione 2 per Grassmann. Abbiamo quindi dimostrato che i 4 punti p_0, p_1, q_0, q_1 appartengono ad un piano proiettivo P, nel quale ogni coppia di rette ha intersezione non vuota. Denotiamo $o = \overline{p_0 q_0} \cap \overline{p_1 q_1}$ e sia $\psi\colon L \to M$ la proiezione di centro o. Allora $\psi(p_0) = q_0$, $\psi(p_1) = q_1$ e $\psi(p_i) = p_i$ per ogni $i > 1$. Dunque φ e ψ coincidono in un sistema di riferimento proiettivo e dunque $\varphi = \psi$. □

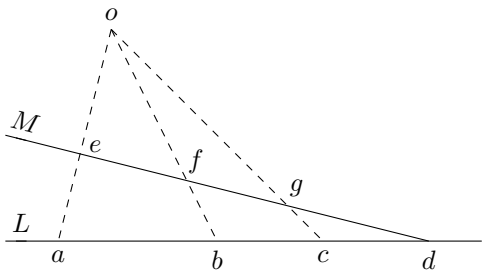
Il prossimo obiettivo è quello di dimostrare che ogni isomorfismo proiettivo tra due iperpiani si ottiene come composizione di un numero finito di proiezioni. Prima di trattare il caso generale è istruttivo considerare il caso delle rette nel piano proiettivo.

ESEMPIO 1.7.3. Siano a, b, c, d quattro punti distinti di una retta proiettiva L. Allora esiste una proiettività $\varphi\colon L \to L$ tale che

$$a\,b\,c\,d \xrightarrow{\varphi} b\,a\,d\,c\,,$$

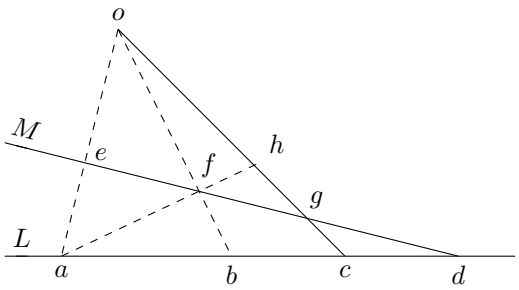
ossia $\varphi(a) = b$, $\varphi(b) = a$, $\varphi(c) = d$ e $\varphi(d) = c$. Siccome a, b, c a, b, d sono sistemi di riferimento proiettivi, ne segue che φ è unica e che φ^2 è uguale all'identità.

Un modo particolarmente carino di dimostrare tale fatto è quello di scrivere esplicitamente φ come composizione di 3 proiezioni. A tal fine consideriamo $L \subset \mathbb{P}^2$, sia $M \neq L$ una qualunque retta passante per d e sia $\alpha\colon L \to M$ una qualunque proiezione di centro $o \notin L \cup M$:



$$a\,b\,c\,d \xrightarrow{\alpha} e\,f\,g\,d\,,$$

Siano adesso $\beta\colon M \to \overline{oc}$ la proiezione di centro a e $\gamma\colon \overline{oc} \to L$ la proiezione di centro f. Allora



$$e\,f\,g\,d \xrightarrow{\beta} o\,h\,g\,c\,,$$

$$o\,h\,g\,c \xrightarrow{\gamma} b\,a\,d\,c\,.$$

In conclusione la proiettività $\varphi = \gamma\beta\alpha\colon L \to L$ scambia a con b e c con d. Per simmetria, esistono altresì due proiettività $\psi, \eta\colon L \to L$ tali che

$$a\,b\,c\,d \xrightarrow{\varphi} b\,a\,d\,c\,, \qquad a\,b\,c\,d \xrightarrow{\psi} c\,d\,a\,b\,, \qquad a\,b\,c\,d \xrightarrow{\eta} d\,c\,b\,a\,.$$

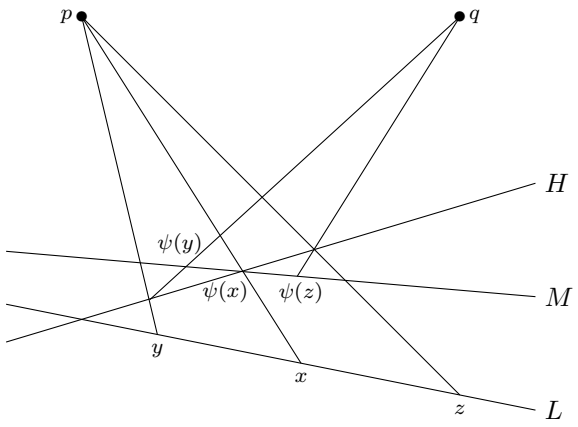
Vedremo più avanti che altre permutazioni di a, b, c, d sono ottenute per restrizione di una proiettività solamente in casi molto particolari.

PROPOSIZIONE 1.7.4. *Sia $\psi\colon L \to M$ una proiettività tra due rette distinte di $\mathbb{P}^2$ e sia $o = L \cap M$ il loro punto di intersezione;*

(1) *se $\psi(o) = o$, allora ψ è una proiezione;*
(2) *se $\psi(o) \neq o$, allora ψ è composizione di due proiezioni.*

DIMOSTRAZIONE. Ridimostriamo il caso $\psi(o) = o$ sebbene sia un caso particolare del Teorema 1.7.2. Se $\psi(o) = o$, estendiamo o ad un sistema di riferimento proiettivo $o, x, y \in L$ di L e sia p il punto di intersezione delle rette $\overline{x\psi(x)}$ e $\overline{y\psi(y)}$. Se $\varphi_p\colon L \to M$ è la proiezione di centro p, allora $\varphi_p(o) = o$, $\varphi_p(x) = \psi(x)$, $\varphi_p(y) = \psi(y)$ e questo implica che $\varphi_p = \psi$.

Se $\psi(o) \neq o$ fissiamo un sistema di riferimento proiettivo $x, y, z \in L$ tale che $\psi(x) \notin L \cap M$ e scegliamo una qualsiasi retta $H \subset \mathbb{P}^2$, diversa da M che contiene $\psi(x)$. Sia poi $p \notin L \cup H$ un punto allineato con $x, \psi(x)$ e consideriamo la proiezione $\varphi_p\colon L \to H$ di centro p. Allora $\varphi_p(x) = \psi(x)$ e per quanto visto prima esiste una proiezione $\varphi_q\colon H \to M$ tale che $\varphi_q\varphi_p(x) = \psi(x)$, $\varphi_q\varphi_p(y) = \psi(y)$ e $\varphi_q\varphi_p(z) = \psi(z)$: quindi $\varphi_q\varphi_p = \psi$.



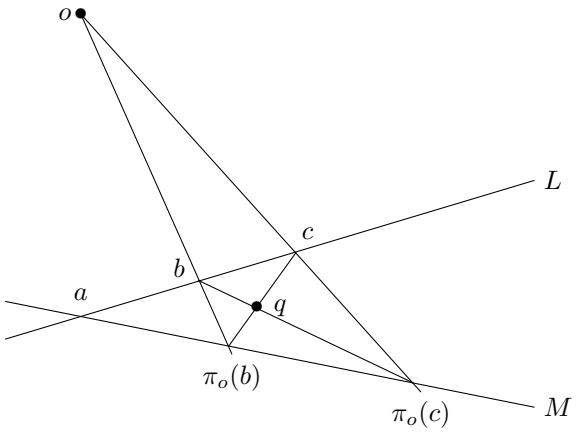


FIGURA 9. La composizione $\pi_q\pi_o\colon L \to L$ scambia b con c e lascia fisso a.

□

COROLLARIO 1.7.5. *Sia $L \subset \mathbb{P}^2$ una retta proiettiva. Allora ogni proiettività $\psi\colon L \to L$ è composizione di al più tre proiezioni.*

DIMOSTRAZIONE. Sia $\varphi\colon M \to L$ una qualunque proiezione, con $M \neq L$. Per il teorema la proiettività $\varphi^{-1}\psi\colon L \to M$ è composizione di al più due proiezioni. □

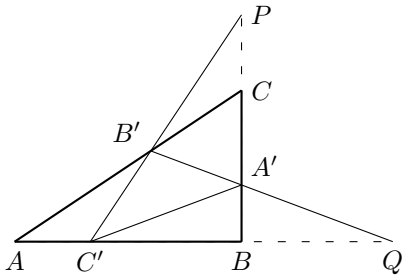
ESEMPIO 1.7.6. Siano a, b, c tre punti distinti di $\mathbb{P}^1$ e costruiamo l'unica proettività $\psi\colon \mathbb{P}^1 \to \mathbb{P}^1$ tale che $\psi(a) = a$, $\psi(b) = c$ e $\psi(c) = b$ come composizione di 2 proiezioni. A tal fine identifichiamo $\mathbb{P}^1$ con una retta proiettiva $L \subset \mathbb{P}^2$ e sia $M \subset \mathbb{P}^2$ un'altra retta tale che $L \cap M = \{a\}$. Siano $o \notin L \cup M$ un qualsiasi punto e $\pi_0\colon L \to M$ la proiezione di centro o; allora $\psi = \pi_q \circ \pi_o$ dove $\pi_q\colon M \to L$ è la proiezione di centro $q = \overline{b\pi_o(c)} \cap \overline{c\pi_o(b)}$ (Figura 9).

PROPOSIZIONE 1.7.7 (Steiner 1832). *In $\mathbb{P}^2$ si consideri un triangolo non degenere ABC ed un triangolo (non degenere) $A'B'C'$ ad esso iscritto, ossia $A' \in \overline{BC}$, $B' \in \overline{CA}$, $C' \in \overline{AB}$. Siano:*

(1) $\varphi_A\colon \overline{C'A'} \to \overline{A'B'}$ *la proiezione di centro A;*
(2) $\varphi_B\colon \overline{A'B'} \to \overline{B'C'}$ *la proiezione di centro B;*
(3) $\varphi_C\colon \overline{B'C'} \to \overline{C'A'}$ *la proiezione di centro C.*

Allora $\varphi_C\varphi_B\varphi_A = \mathrm{Id}$.

DIMOSTRAZIONE. Basta dimostrare che $\psi := \varphi_C\varphi_B\colon \overline{A'B'} \to \overline{C'A'}$ è la proiezione di centro A. Siccome $A' = \overline{A'B'} \cap \overline{C'A'}$ e A', B, C sono allineati, ne segue che $\varphi_C\varphi_B(A') = \varphi_C(P) = A'$ e quindi $\varphi_C\varphi_B$ è una proiezione.

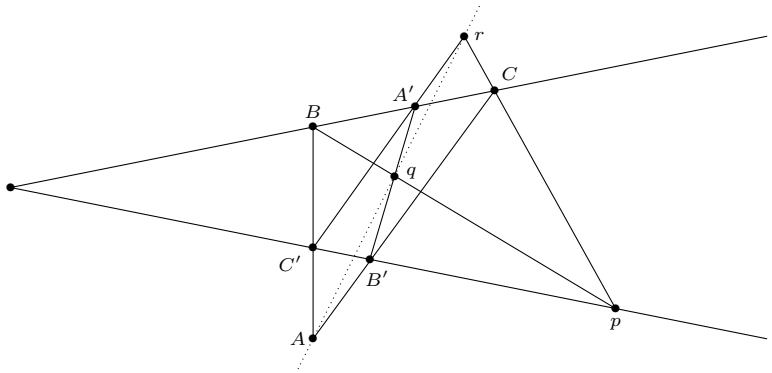


Inoltre se $Q = \overline{AB} \cap \overline{A'B'}$ si ha

$$\psi(B') = \varphi_C\varphi_B(B') = \varphi_C(B') \in \overline{B'C} = \overline{AB'},$$
$$\psi(Q) = \varphi_C\varphi_B(Q) = \varphi_C(C') = C' \in \overline{AB} = \overline{AQ}.$$

Ma le precedenti due relazioni impongono che il centro di prospettiva di ψ deve necessariamente essere A. □

Possiamo ridimostrare il teorema di Pappo come conseguenza della Proposizione 1.7.7. A tal fine riprendiamo la Figura 7 con i punti ridenominati nel modo seguente



Allora $\varphi_C\varphi_B(q) = \varphi_C(p) = r$, quindi $\varphi_A(q) = r$ ed in particolare A, q, r sono allineati.

TEOREMA 1.7.8. *Siano $L \subset \mathbb{P}^n$ un iperpiano e $\psi\colon L \to L$ una proiettività. Allora ψ è composizione di una successione finita di proiezioni del tipo*

$$\psi\colon L \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} L \xrightarrow{\varphi_3} M_3 \xrightarrow{\varphi_4} L \cdots \xrightarrow{\varphi_{2m}} L,$$

con $M_i \neq L$ per ogni i.

DIMOSTRAZIONE. Sia $H \subset L$ un sottospazio proiettivo di dimensione massima tra quelli contenuti nel luogo $\mathrm{Fix}(\psi)$ dei punti fissi di ψ. Dimostriamo il teorema per induzione su $d = \dim L - \dim H$. Se $d = 0$ vuol dire che ψ è l'identità e non c'è nulla da dimostrare. Supponiamo $d > 0$ ed il teorema vero per ogni proiettività $\phi\colon L \to L$ il cui luogo fisso contiene un sottospazio di dimensione $> \dim H$. Trattiamo separatamente i due casi $\mathrm{Fix}(\psi) \neq H$ e $\mathrm{Fix}(\psi) = H$.

Primo caso, $\mathrm{Fix}(\psi) \neq H$. In particolare $\mathrm{Fix}(\psi) \neq \emptyset$ e di conseguenza anche $H \neq \emptyset$, in quanto il vuoto non ha dimensione massima tra i sottospazi proiettivi di $\mathrm{Fix}(\psi)$.

Scegliamo un punto $p \in \mathrm{Fix}(\psi) - H$ ed un punto punto $r \in H$. Siccome p, r sono punti fissi di ψ, si ha $\psi(\overline{pr}) = \overline{pr}$. Sia $q \in \overline{pr}$ un qualsiasi punto diverso da p, r e denotiamo con $s = \psi(q) \in \overline{pr}$. Adesso prendiamo un qualsiasi iperpiano $M \subset \mathbb{P}^n$ tale che $p \notin M$ e $H \subset M$ ed un qualsiasi punto $o \notin L \cup M$. Siano $\varphi_1\colon M \to L$ e $\psi_1\colon L \to M$ le proiezioni di centro o e denotiamo $q_1 = \psi_1(q)$ e dunque $\varphi_1(q_1) = q$. Dato che q_1 appartiene al piano P generato da p, r, o, si ha che la retta $\overline{sq_1}$ interseca la retta $\overline{op}$ in un punto o'.

Denotiamo con $\varphi_2\colon L \to M$ e $\psi_2\colon M \to L$ le proiezioni di centro o'. Allora $\varphi_2(s) = q_1$ e quindi, ponendo $\widehat{\psi} = \varphi_1\varphi_2\phi\colon L \to L$ si ha $\widehat{\psi}(p) = p$, $\widehat{\psi}(q) = q$ e $\widehat{\psi}(x) = x$ per ogni $x \in H$. Siccome p, q, r sono un sistema di riferimento di $\overline{pr}$ ne segue che $\overline{pr} \subset \mathrm{Fix}(\widehat{\psi})$ e siccome $\overline{pr} \cap H \neq 0$ si ha che $\mathrm{Fix}(\widehat{\psi})$ contiene il sottospazio proiettivo $\overline{pr} + H$. Per induzione $\widehat{\psi}$ è composizione di proiezioni. Per concludere basta allora osservare che

$$\phi = \psi_2\psi_1\varphi_1\varphi_2\phi = \psi_2\psi_1\widehat{\psi}.$$

Secondo caso, $\mathrm{Fix}(\psi) = H$. Supponiamo adesso che $H = \mathrm{Fix}(\psi)$. Prendiamo un qualsiasi punto $p \in L - H$, denotiamo $q = \psi(p)$ e prendiamo un iperpiano $M \subset \mathbb{P}^n$ tale che $H \subset M$ e $p, q \notin M$.

Come prima sia $o \notin L \cup M$ e $\varphi_1\colon L \to M$ la proiezione di centro o. Sia poi $\varphi_2\colon M \to L$ la proiezione con centro un qualsiasi punto appartenente alla retta $\overline{q\varphi_1(p)}$. Allora $\varphi_2\varphi_1(p) = q$ e dunque la proiettività $\varphi_1^{-1}\varphi_2^{-1}\psi$ contiene sia H che p nel suo luogo fisso e ci si riconduce al caso precedentemente trattato.

□

1.8. Prospettive

TEOREMA 1.8.1. *Per una proiettività $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ le seguenti condizioni sono equivalenti:*

(1) *i punti fissi di ψ contengono un iperpiano H;*
(2) *esiste un punto $o \in \mathbb{P}^n$ tale che $\psi(o) = o$ e $\psi(p) \in \overline{op}$ per ogni $p \neq o$;*
(3) *esiste un sistema di riferimento proiettivo $p_0, \dots, p_{n+1}$ tale che $\psi(p_0) = p_0$ e $\psi(p_i) \in \overline{p_0 p_i}$ per ogni $i = 1, \dots, n+1$.*

Inoltre, se $n > 1$ e $\psi \neq \mathrm{Id}$ soddisfa le precedenti condizioni, allora il punto o e l'iperpiano H sono unici e $\mathrm{Fix}(\psi) = H \cup \{o\}$.

DIMOSTRAZIONE. Possiamo chiaramente supporre ψ diversa dall'identità.

[1 implica 2]: Osserviamo innanzitutto che la condizione 2) è del tutto equivalente a dire che $\psi(p) \in o + p$ per ogni $p \in \mathbb{P}^n$. Sia $\psi = [f]$ e fissiamo una base $v_0, \dots, v_n$ tale che $[v_i] \in H$ per ogni $i = 1, \dots, n$. La restrizione di ψ ad H è l'identità, quindi a meno di moltiplicare f per uno scalare possiamo supporre $f(v_i) = v_i$ per ogni $i > 0$. Se $f(v_0) = \sum_{i=0}^n a_i v_i$ consideriamo il punto $o = [f(v_0) - v_0]$. Allora per ogni vettore $w = \sum b_i v_i$ si ha

$$f(w) = b_0 f(v_0) + f(w - b_0 v_0) = b_0 f(v_0) + w - b_0 v_0 = b_0(f(v_0) - v_0) + w\,,$$

ed in particolare $f(w) \in \mathrm{Span}(f(v_0) - v_0, w)$.

[2 implica 3]: Basta estendere il punto o ad un sistema di riferimento proiettivo.

[3 implica 1]: Possiamo prendere una base $v_0, \dots, v_n$ di $\mathbb{K}^{n+1}$ tale che $p_i = [v_i]$ per ogni i e $p_{n+1} = [v_0 + \cdots + v_n]$. Siccome $\psi(p_0) = p_0$ esiste un unico isomorfismo lineare f che induce ψ e tale che $f(v_0) = v_0$. Per ipotesi esistono $a_i, b_i \in \mathbb{K}$, $i = 1, \dots, n+1$ tali che

$$f(v_i) = a_i v_0 + b_i v_i, \qquad i = 1, \dots, n$$

$$f(\sum v_i) = a_{n+1} v_0 + b_{n+1} \sum v_i\,.$$

Ponendo, per semplicità notazionale $b = b_{n+1}$ si ha

$$a_{n+1} v_0 + b \sum v_i = f(\sum v_i) = \sum f(v_i) = v_0 + \sum_{i=1}^n (a_i v_0 + b_i v_i)$$

e dato che $v_0, \dots, v_n$ sono linearmente indipendenti si ricava in particolare che $b_i = b \neq 0$ per ogni $i = 1, \dots, n$. Dunque, in tale base, la proiettività ψ è indotta dall'applicazione lineare definita dalla matrice

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_n \\ 0 & b & 0 & \cdots & 0 \\ 0 & 0 & b & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b \end{pmatrix}, \qquad a_0, b \neq 0, \qquad a_1, \dots, a_n \in \mathbb{K}\,.$$

Siccome A non è un multiplo dell'identità (altrimenti $\psi = \mathrm{Id}$), l'autovalore b ha molteplicità geometrica n e quindi un iperpiano di punti fissi per ψ è

$$\mathbb{P}(\ker(A - bI)) = \{[x_0, \dots, x_n] \mid (a_0 - b)x_0 + \sum_{i=1}^n a_i x_i = 0\}\,.$$

Per future applicazioni osserviamo che, poiché A è definita a meno di moltiplicazione per scalari non nulli, non è restrittivo assumere $a_0 = 1$ oppure $b = 1$.

Mostriamo adesso che se $n > 1$ e $\psi \neq \mathrm{Id}$ allora o ed H sono unici. L'unicità di H è facile: infatti se M è un altro iperpiano di punti fissi, siccome $n > 1$ si ha $H \cap M \neq \emptyset$ e quindi $\mathbb{P}^n = H + M \subset \mathrm{Fix}(\psi)$ per il Lemma 1.7.1.

Sia $q \neq o$ un punto tale che $\psi(q) = q$ e $\psi(p) \in \overline{pq}$ per ogni $p \neq q$. Allora possiamo completare o, q ad un sistema di riferimento proiettivo $o, q, p_1, \dots, p_n$. Siccome $n > 1$, per ogni $i = 1, \dots, n$ i punti o, q, p_i non sono allineati e quindi le due rette $\overline{op_i}$ e $\overline{qp_i}$ si intersecano nell'unico punto p_i. Quindi

$$\psi(p_i) \in \overline{op_i} \cap \overline{qp_i} = \{p_i\}$$

da cui segue che ψ lascia fisso un sistema di riferimento proiettivo, ma questo è possibile solo se $\psi = \mathrm{Id}$.

Per finire, dimostriamo che se $n > 1$ e $\psi \neq \mathrm{Id}$ allora non esistono altri punti fissi oltre o ed H, ossia $\mathrm{Fix}(\psi) = H \cup \{o\}$. Sia q un punto fisso di ψ; se $q \notin H$ allora ogni retta L passante per q viene trasformata in se stessa da ψ. Infatti $L \not\subset H$ e quindi L interseca H in un unico punto, diciamo $r = L \cap H$, $r \neq q$. Allora $L = \overline{qr}$ e $\psi(L) = \overline{\psi(q)\psi(r)} = L$, in contraddizione con l'unicità del punto o. □

Definizione 1.8.2. Una proiettività $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ che soddisfa le tre condizioni equivalenti del Teorema 1.8.1 viene detta **prospettiva**.

Qualora $n > 2$ e ψ non sia l'identità, l'iperpiano H viene detto **asse di prospettiva** ed il punto o **centro di prospettiva**.

Osservando con un pizzico di attenzione la dimostrazione del Teorema 1.8.1 si osserva che entrambe le possibilità $o \notin H$ e $o \in H$ sono possibili. Più precisamente, se ψ è una prospettiva indotta da un endomorfismo lineare $f\colon V \to V$, allora vale $o \notin H$ se e solo se f è diagonalizzabile (1 autovalore di molteplicità geometrica n ed un altro di molteplicità geometrica 1), mentre vale $o \in H$ se e solo se f non è diagonalizzabile (1 autovalore di molteplicità algebrica $n+1$ e molteplicità geometrica n.)

Definizione 1.8.3. Una prospettiva di centro o ed asse H viene detta: **omologia**[4] se $o \notin H$; **trasvezione** od **omologia speciale** se $o \in H$.

Osservazione 1.8.4. Per quanto dimostrato in precedenza le nozioni di omologia e trasvezione sono ben definite per prospettive diverse dall'identità su spazi proiettivi di dimensione maggiore di 1. Tuttavia possiamo estendere in maniera ovvia tali nozioni anche a prospettive diverse dall'identità su $\mathbb{P}^1$: omologia se ha due punti fissi, trasvezione se ha un solo punto fisso. Siccome tre punti distinti di $\mathbb{P}^1$ formano un sistema di riferimento, l'unica proiettività con più di due punti fissi è l'identità.

Sia $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ una prospettiva di centro o e siano $L, M \subset \mathbb{P}^n$ due iperpiani tali che $o \notin M$ e $\psi(L) \subset M$. Allora la restrizione $\psi_{|L}\colon L \to M$ ha una evidente interpretazione geometrica. Osserviamo innanzitutto che $o \notin L$, altrimenti $o = \psi(o) \in M$, e quindi per ogni $p \in L$ abbiamo una retta $\overline{op}$ che interseca M in un unico punto.

Siano $L, M \subset \mathbb{P}^n$ due iperpiani, $p, q \notin L \cup M$ due punti e

$$\phi_p,\ \phi_q\colon L \to M$$

le proiezioni di centro p e q rispettivamente. Allora l'applicazione

$$\psi = \phi_q \phi_p^{-1}\colon M \to M$$

è una prospettiva di centro $o = M \cap \overline{pq}$ ed asse $H = L \cap M$. Infatti H è un iperpiano di M di funti fissi di ψ e per ogni $r \in M$ il punto $\psi(r)$ appartiene all'intersezione di M con il piano $p + q + r$, ossia $\psi(r) \in \overline{or}$ (Figura 10).

Lemma 1.8.5. *Siano $L, M \subset \mathbb{P}^n$ due iperpiani distinti ed $o \notin L \cup M$. Esiste allora una unica prospettiva $\psi\colon \mathbb{P}^n \to \mathbb{P}^n$ di centro o e tale che $\psi(L) = M$, $\psi(M) = L$. Inoltre:*

1. *la prospettiva ψ è una involuzione, ossia $\psi^2 = Id$, ed è una omologia se e solo se il campo ha caratteristica $\neq 2$.*
2. *le restrizioni $\psi\colon L \to M$ e $\psi\colon M \to L$ coincidono con le proiezioni di centro o.*

Dimostrazione. Fissiamo un sistema di coordinate omogenee $x_0, \dots, x_n$ tale che

$$o = [1, 0, \dots, 0], \qquad L \cap M = \{x_0 = x_1 = 0\}\,.$$

Le equazioni di L, M saranno allora del tipo

$$L = \{x_0 = l x_1\}, \qquad M = \{x_0 = m x_1\}, \qquad l, m \in \mathbb{K}\,.$$

[4] Nulla a che vedere con l'analogo concetto in algebra omologica.

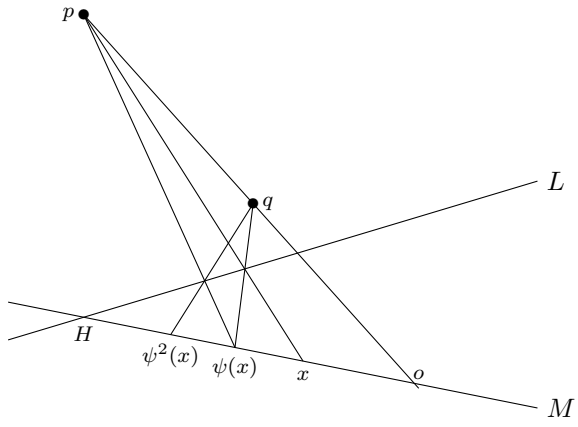


FIGURA 10. Una prospettiva $\psi\colon M \to M$ di centro o ed asse $H = L \cap M$, composizione della proiezione $M \to L$ di centro p e della proiezione $L \to M$ di centro q.

Il ragionamento fatto nella dimostrazione del Teorema 1.8.1 mostra che le prospettive di centro o sono tutte e sole le proiettività rappresentate da una matrice della forma

$$A = \begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_n \\ 0 & b & 0 & \cdots & 0 \\ 0 & 0 & b & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & b \end{pmatrix}, \qquad b \neq 0, \qquad a_1, \dots, a_n \in \mathbb{K}\,.$$

Si considerino i due punti $p = [l, 1, 0, \dots, 0] \in L$ e $q = [m, 1, 0, \dots, 0] \in M$. Poiché

$$L = (L \cap M) + p, \qquad M = (L \cap M) + q,$$

le due condizioni $\psi(L) = M$, $\psi(M) = L$ sono equivalenti alle tre condizioni

$$\psi(L \cap M) \subset L \cap M, \qquad \psi(p) \in M, \qquad \psi(q) \in L\,.$$

La condizione $\psi(L \cap M) \subset L \cap M$ è equivalente all'annullamento $a_2 = \cdots = a_n = 0$, mentre le condizioni $\psi(p) \in M$ e $\psi(q) \in L$ equivalgono al sistema lineare nelle incognite a_1, b

$$l + a_1 = mb, \qquad m + a_1 = lb$$

che ha come unica soluzione $b = -1$ e $a_1 = -l - m$. La verifica che $A^2 = I$ è immediata. □

COROLLARIO 1.8.6. *Dati tre punti distinti $o, p, q \in \mathbb{P}^1$ esiste una prospettiva ψ di centro o tale che $\psi(p) = q$ e $\psi(q) = p$.*

LEMMA 1.8.7. *Sia $U \subset \mathbb{P}^n$ sottospazio proiettivo e $\psi\colon U \to U$ una prospettiva di centro o ed asse H. Allora ψ si estende ad una prospettiva $\phi\colon \mathbb{P}^n \to \mathbb{P}^n$ di centro o il cui asse contiene H.*

DIMOSTRAZIONE. Se $U = \mathbb{P}(V)$ con $V \subset \mathbb{K}^{n+1}$, possiamo scegliere una base $v_0, \dots, v_n$ tale che $v_0, \dots, v_p$ sia una base di V e $v_1, \dots, v_p$ base dell'asse di prospettiva. Possiamo allora rappresentare la prospettiva con $f\colon V \to V$ lineare e tale che $f(v_i) = v_i$ per $0 < i \leq p$. Basta allora estendere f ponendo $f(v_i) = v_i$ per ogni $i > 0$.

□

TEOREMA 1.8.8. *Sia ψ una proiettività di $\mathbb{P}^n$ e sia $H \subset \mathrm{Fix}(\psi)$ un sottospazio proiettivo di dimensione $r \leq n$. Allora ψ è composizione di $s \leq n - r$ prospettive i cui assi contengono H.*

DIMOSTRAZIONE. Se $n - r \leq 1$ non c'è nulla da dimostrare, per induzione su r basta provare che esiste una prospettiva ϕ tale che $\phi^{-1}\psi$ contiene un sottospazio di punti fissi di dimensione $> r$. Scegliamo $p \notin \mathrm{Fix}(\psi)$ e denotiamo $q = \psi(p) \neq p$

Se $H = \emptyset$ per il Corollario 1.8.6 esiste una prospettiva ϕ della retta $\overline{pq}$ tale che $\phi(p) = q$. Possiamo estendere ϕ ad una prospettiva di $\mathbb{P}^n$ e la proiettività $\phi^{-1}\psi$ possiede p come punto fisso.

Se $H \neq \emptyset$ denotiamo $L = H + p$, $\dim L = r + 1$. Se $q \in L$, allora $\psi(L) = L$ e la restrizione di ψ a L è una prospettiva che si può estendere ad una prospettiva ϕ di $\mathbb{P}^n$. Allora la proiettività $\phi^{-1}\psi$ contiene L come luogo di punti fissi.

Se $q \notin L$ allora $\overline{pq} \cap H = \emptyset$ scegliamo un qualunque punto $r \in H$, allora $q \notin \overline{rp}$, $\psi(\overline{rp}) = \overline{rq}$, le due rette $\overline{rp}$ e $\overline{rq}$ sono contenute nel piano P contenente i tre punti non allineati p, q, r. Poniamo $M = H + q$ e $K = H + P$. L ed M sono iperpiani di K che si intersecano in H.

Scegliamo un punto $s \in \overline{rp}$ diverso da r, p e poniamo $t = \psi(s)$. Sia $o \in P$ il punto di intersezione delle rette $\overline{pq}$ e $\overline{st}$. Sia $\phi\colon K \to K$ una prospettiva di centro o e tale che $\phi(L) = M$ ed estendiamola ad una prospettiva su $\mathbb{P}^n$ di centro o ed asse contenente H. Necessariamente $\phi(p) = q$, $\phi(s) = t$ e quindi p, s, r sono punti fissi di $\phi^{-1}\psi$. Essendo p, s, r un sistema di riferimento in $\overline{pr}$, anche la retta $\overline{pr}$ è contenuta nel luogo fisso di $\phi^{-1}\psi$. Poiché $\overline{rp} \cap H \neq \emptyset$ ne segue che anche L è contenuto nel luogo fisso di $\phi^{-1}\psi$. □

Esercizi

Esercizio 14. Siano date n rette proiettive $L_1, \dots, L_n \subset \mathbb{P}^n$, nessuna delle quali contenuta nell'iperpiano $H_0 = \{x_0 = 0\}$. Scriviamo $\mathbb{P}^n = \mathbb{K}^n \cup H_0$, per ogni $i = 1, \dots, n$ esiste una rappresentazione parametrica della retta affine $L_i \cap \mathbb{K}^n$ che possiamo scrivere nella forma

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

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

Esercizio 15 (∗). Siano date quattro rette $L_1, \dots, L_4 \subset \mathbb{P}^3(\mathbb{C})$. Provare che esiste almeno una retta in $\mathbb{P}^3$ che le interseca tutte e quattro. (Sugg.: se esiste un punto o appartenente all'intersezione di due rette distinte L_i, L_j considerare la proiezione di centro o. Altrimenti si prendano coordinate omogenee tali che $L_4 = \{x_0 = x_1 = 0\}$, $L_1 = \{x_2 = x_3 = 0\}$ e si consideri l'intersezione delle rette con i piani del fascio $F_t = \{x_1 = tx_0\}$, per $t \in \mathbb{K}$. Ad un certo punto servirà il risultato dell'Esercizio 14.)

1.9. Il birapporto

Sia $\mathbb{P}(V)$ uno spazio proiettivo di dimensione 1. Abbiamo visto che per ogni terna di punti distinti p_2, p_3, p_4 di $\mathbb{P}(V)$ esiste un'unica proiettività $\phi\colon \mathbb{P}(V) \to \mathbb{P}^1$ tale che:

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

Nelle precedenti uguaglianze $[0, 1] = \infty$ e $[1, t] = t$, abbiamo identificato $\mathbb{P}^1$ con $\mathbb{K} \cup \{\infty\}$ nel modo standard, ossia tramite il processo di disomogeneizzazione $[x_0, x_1] \leftrightarrow x_1/x_0$.

È allora chiaro che dati quattro punti distinti $p_1, \dots, p_4 \in \mathbb{P}(V)$, esistono unici una proiettività $\phi\colon \mathbb{P}(V) \to \mathbb{P}^1$ ed un elemento $\lambda \in \mathbb{K} - \{0, 1\}$ tali che

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

Definizione 1.9.1. Nella situazione precedente, la quantità $\lambda = [p_1, p_2; p_3, p_4]$ si dice **birapporto**[5] della quaterna ordinata $p_1, \dots, p_4$.

È immediato osservare che per ogni $\lambda \in \mathbb{P}^1 = \mathbb{K} \cup \{\infty\}$, $\lambda \neq 0, 1, \infty$, allora $\lambda = [\lambda, 1; 0, \infty]$. In particolare, il birapporto può assumere qualsiasi valore in $\mathbb{K} - \{0, 1\}$.

Proposizione 1.9.2. *Siano $\mathbb{P}(V)$ e $\mathbb{P}(U)$ due rette proiettive e $p_1, \dots, p_4 \in \mathbb{P}(V)$, $q_1, \dots, q_4 \in \mathbb{P}(U)$ due quaterne di punti distinti. Allora esiste una proiettività $\phi\colon \mathbb{P}(V) \to \mathbb{P}(U)$ tale che $\phi(p_i) = q_i$ per ogni i se e solo se $[p_1, p_2; p_3, p_4] = [q_1, q_2; q_3, q_4]$.*

[5] In inglese *cross ratio*; in francese *rapport anharmonique*.

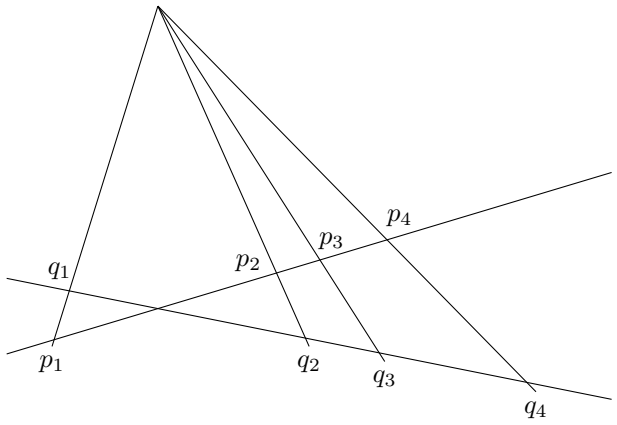


FIGURA 11. Le due quaterne p_1, p_2, p_3, p_4 e q_1, q_2, q_3, q_4 hanno lo stesso birapporto.

DIMOSTRAZIONE. Siano $\eta\colon \mathbb{P}(V) \to \mathbb{P}^1$ e $\mu\colon \mathbb{P}(U) \to \mathbb{P}^1$ le uniche proiettività tali che

$$\eta(p_2) = \mu(q_2) = 1, \qquad \eta(p_3) = \mu(q_3) = 0, \qquad \eta(p_4) = \mu(q_4) = \infty\,.$$

Allora $\phi = \mu^{-1}\eta\colon \mathbb{P}(V) \to \mathbb{P}(U)$ coincide con l'unica proiettività tale che $\phi(p_i) = q_i$, $i = 2, 3, 4$.

Ma allora $\phi(p_1) = q_1$ se e solo se $\eta(p_1) = \mu(q_1)$, ossia se e solo se le due quaterne hanno lo stesso birapporto. □

Dunque il birapporto è invariante per proiettività e quindi è invariante per prospettive e proiezioni (Figura 11).

Il nome birapporto è motivato dalla formula

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

da interpretarsi come nella seguente proposizione.

PROPOSIZIONE 1.9.3. *Siano $p_1 = [x_1, y_1]$,…,$p_4 = [x_4, y_4]$ punti distinti di $\mathbb{P}^1$. Allora vale la formula*

$$[p_1, p_2; p_3, p_4] = \frac{\begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}}{\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}} : \frac{\begin{vmatrix} x_1 & x_4 \\ y_1 & y_4 \end{vmatrix}}{\begin{vmatrix} x_2 & x_4 \\ y_2 & y_4 \end{vmatrix}} = \frac{x_1y_3 - x_3y_1}{x_2y_3 - x_3y_2} : \frac{x_1y_4 - x_4y_1}{x_2y_4 - x_4y_2}\,, \tag{1.10}$$

che nelle coordinate affini $t_i = \dfrac{y_i}{x_i} \in \mathbb{K} \cup \{\infty\}$, diventa

$$[p_1, p_2; p_3, p_4] = \frac{t_3 - t_1}{t_3 - t_2} : \frac{t_4 - t_1}{t_4 - t_2}\,. \tag{1.11}$$

DIMOSTRAZIONE. Osserviamo preliminarmente che la Formula (1.10) è ben definita, ossia è invariante per moltiplicazione della coppia x_i, y_i per uno scalare non nullo, ed applicata alla quaterna

$$p_1 = [1, \lambda], \quad p_2 = [1, 1], \quad p_3 = [1, 0], \quad p_4 = [0, 1],$$

restituisce il valore $[p_1, p_2; p_3, p_4] = \lambda$. Basta quindi provare che la Formula (1.10) è invariante per proiettività.

Sia $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ una proiettività indotta da una matrice invertibile $A \in \mathrm{GL}_2(\mathbb{K})$. Per ogni indice i si ha

$$\phi(p_i) = [z_i, w_i], \qquad \text{con} \quad A \begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} z_i \\ w_i \end{pmatrix}\,.$$

Per il teorema di Binet, per ogni coppia di indici i, j si ha:

$$A\begin{pmatrix} x_i & x_j \\ y_i & y_j \end{pmatrix} = \begin{pmatrix} z_i & z_j \\ w_i & w_j \end{pmatrix}, \qquad \det(A)\begin{vmatrix} x_i & x_j \\ y_i & y_j \end{vmatrix} = \begin{vmatrix} z_i & z_j \\ w_i & w_j \end{vmatrix},$$

e di conseguenza

$$\frac{\begin{vmatrix} z_1 & z_3 \\ w_1 & w_3 \end{vmatrix}}{\begin{vmatrix} z_2 & z_3 \\ w_2 & w_3 \end{vmatrix}} : \frac{\begin{vmatrix} z_1 & z_4 \\ w_1 & w_4 \end{vmatrix}}{\begin{vmatrix} z_2 & z_4 \\ w_2 & w_4 \end{vmatrix}} = \frac{\begin{vmatrix} x_1 & x_3 \\ y_1 & y_3 \end{vmatrix}}{\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}} : \frac{\begin{vmatrix} x_1 & x_4 \\ y_1 & y_4 \end{vmatrix}}{\begin{vmatrix} x_2 & x_4 \\ y_2 & y_4 \end{vmatrix}}.$$

□

Definizione 1.9.4. Denotiamo con Σ_4 il gruppo delle permutazioni dell'insieme $\{1, 2, 3, 4\}$. Il **gruppo trirettangolo**[6] Γ_4 è il sottogruppo di Σ_4 formato dall'identità e dalle tre permutazioni[7] di ordine 2

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

Il birapporto di una quaterna dipende dall'ordine in cui vengono presi i punti. Tuttavia segue immediatamente dalle Formule (1.10) e (1.11) che per ogni quaterna di punti distinti $p_1, \ldots, p_4$ si ha:

$$[p_1, p_2; p_3, p_4] = [p_2, p_1; p_4, p_3] = [p_3, p_4; p_1, p_2] = [p_4, p_3; p_2, p_1].$$

Possiamo esprimere questo fatto dicendo che *il birapporto è invariante per l'azione del gruppo trirettangolo.*

Più in generale è naturale chiedersi come agisce Σ_4 sul birapporto: in altri termini, data una permutazione $\sigma \in \Sigma_4$, siamo interessati alla relazione esistente tra i due birapporti $[p_1, p_2; p_3, p_4]$ e $[p_{\sigma(1)}, p_{\sigma(2)}; p_{\sigma(3)}, p_{\sigma(4)}]$.

Siccome ogni permutazione σ si scrive in modo unico nella forma $\gamma\tau$, con $\gamma \in \Gamma_4$, $\gamma(4) = \sigma(4)$ e $\tau(4) = 4$, basta vedere come cambia il birapporto per effetto delle 6 permutazioni che fissano il numero 4.

Lemma 1.9.5. *Sia $\lambda = [p_1, p_2; p_3, p_4]$ il birapporto di una quaterna di punti distinti sulla retta proiettiva. Allora si hanno le 6 uguaglianze:*

$$\begin{array}{lll} [p_1, p_2; p_3, p_4] = \lambda & [p_2, p_3; p_1, p_4] = \dfrac{\lambda - 1}{\lambda} & [p_3, p_1; p_2, p_4] = \dfrac{1}{1 - \lambda} \\ [p_2, p_1; p_3, p_4] = \dfrac{1}{\lambda} & [p_3, p_2; p_1, p_4] = \dfrac{\lambda}{\lambda - 1} & [p_1, p_3; p_2, p_4] = 1 - \lambda \end{array}.$$

Dimostrazione. La dimostrazione non presenta alcuna difficoltà, anche perché possiamo sempre trovare un sistema di coordinate affini tali che

$$p_1 = \lambda, \quad p_2 = 1, \quad p_3 = 0, \quad p_4 = \infty.$$

□

Possiamo riassumere le precedenti considerazioni nel seguente risultato:

Lemma 1.9.6. *Il birapporto di una quaterna di punti distinti di $\mathbb{P}^1$ è invariante per l'azione del gruppo trirettangolo. Se $[p_1, p_2; p_3, p_4] = \lambda$, allora sotto l'azione del gruppo simmetrico il birapporto assume i valori*

$$\lambda, \quad \frac{1}{\lambda}, \quad 1 - \lambda, \quad 1 - \frac{1}{\lambda}, \quad \frac{1}{1 - \lambda}, \quad \frac{\lambda}{\lambda - 1}. \tag{1.12}$$

Per un generico $\lambda \in \mathbb{K} - \{0, 1\}$ le sei espressioni in (1.12) forniscono sei birapporti distinti; si hanno tuttavia le seguenti eccezioni:

(1) Caratteristica $\neq 2$ e $\lambda = -1, 2, \frac{1}{2}$. In questo caso la quaterna è detta **armonica**.

[6] In inglese *Klein fourgroup*.

[7] Con la notazione $\sigma = (a_1, \ldots, a_n)$ si intende la permutazione tale che $\sigma(i) = a_i$.

(2) Caratteristica $\neq 3$, $\xi^2 - \xi + 1 = 0$ e $\lambda = \xi, \xi^{-1}$. In questo caso la quaterna è detta **equianarmonica**.

Lasciamo per esercizio la verifica delle seguenti affermazioni, la prima delle quali giustifica il termine di quaterna armonica:

(1) In caratteristica $\neq 2$, dati tre valori distinti $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{K} - \{0\}$ si ha $[0, \lambda_1; \lambda_2, \lambda_3] = -1$ se e solo se λ_1 è la media armonica di λ_2, λ_3, ossia se e solo se

$$\lambda_1 = \frac{2}{\dfrac{1}{\lambda_2} + \dfrac{1}{\lambda_3}} = \frac{2\lambda_2\lambda_3}{\lambda_2 + \lambda_3}\,.$$

In particolare per ogni $x \in \mathbb{K}$ si ha

$$\left[0, \frac{1}{x}; \frac{1}{x-1}, \frac{1}{x+1}\right] = \left[\frac{1}{x+1}, \frac{1}{x-1}; \frac{1}{x}, 0\right] = \left[\frac{1}{x+1}, \frac{1}{x-1}; 0, \frac{1}{x}\right] = -1\,.$$

(2) Mentre non ha senso definire le quaterne armoniche in caratteristica 2 in quanto $-1 = 1$ e $2 = 0$, avrebbe senso considerare le quaterne equianarmoniche anche in caratteristica 3; tuttavia, in tal caso si ha $\xi^2 - \xi + 1 = (1+\xi)^2 = (1-2\xi)^2 = (2-\xi)^2$ e quindi si ricade nel caso armonico. Si noti inoltre che, sempre in caratteristica 3 si hanno le uguaglianze $-1 = 2 = 1/2$ e quindi nelle quaterne armoniche il birapporto è invariante per permutazioni.

(3) Su $\mathbb{C}$, rappresentato dal piano di Gauss, la quaterna formata dai vertici di un triangolo equilatero e dal suo baricentro è equianarmonica, mentre i vertici di un quadrato formano una quaterna armonica.

TEOREMA 1.9.7 (Quadrilatero armonico). *Sia $\mathbb{P}^2$ il piano proiettivo su di un campo di caratteristica $\neq 2$, e siano $a, b, c, d \in \mathbb{P}^2$ i vertici di un quadrilatero completo non degenere, ossia con nessuna terna allineata. Allora i seguenti 4 punti allineati (Figura 12):*

$$p_1 = \overline{ab} \cap \overline{cd}, \quad p_2 = \overline{ac} \cap \overline{bd}, \quad p_3 = \overline{p_1p_2} \cap \overline{bc}, \quad p_4 = \overline{p_1p_2} \cap \overline{ad}\,.$$

formano una quaterna armonica, e più precisamente $[p_1, p_2; p_3, p_4] = -1$.

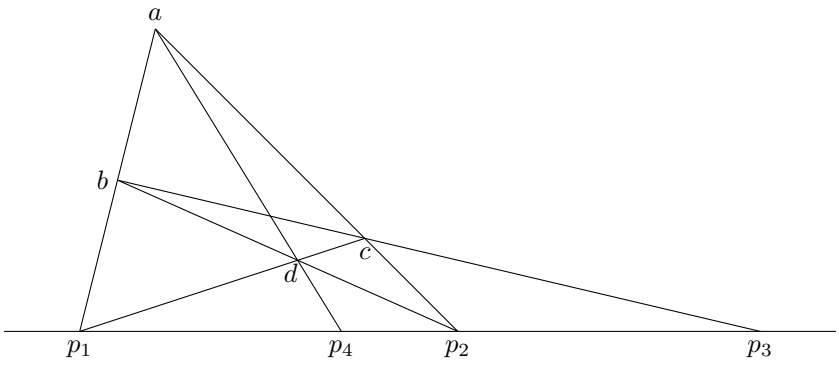


FIGURA 12. Il quadrilatero "armonico": $[p_1, p_2; p_3, p_4] = [p_3, p_4; p_1, p_2] = -1$.

DIMOSTRAZIONE. Sia $[p_1, p_2; p_3, p_4] = \lambda \neq 1, 0$ e di conseguenza $[p_2, p_1; p_3, p_4] = \lambda^{-1}$. Si considerino adesso le due prospettive $\overline{p_1p_2} \to \overline{ad}$ di centro b e $\overline{ad} \to \overline{p_1p_2}$ di centro c. Se indichiamo con o il punto di intersezione di $\overline{ad}$ e $\overline{bc}$, dalla prima prospettiva ricaviamo che $[p_1, p_2; p_3, p_4] = [a, d; o, p_4]$ e dalla seconda che $[a, d; o, p_4] = [p_2, p_1; p_3, p_4]$. Quindi

$$[p_1, p_2; p_3, p_4] = [a, d; o, p_4] = [p_2, p_1; p_3, p_4]$$

e dunque $\lambda = \lambda^{-1}$ che ha come unica soluzione $\lambda = -1$. □

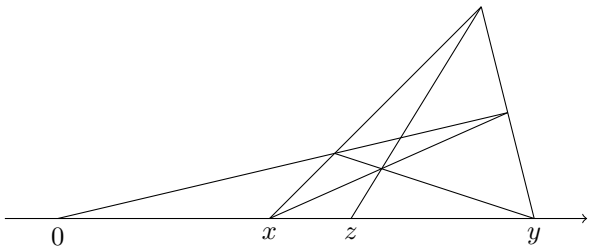
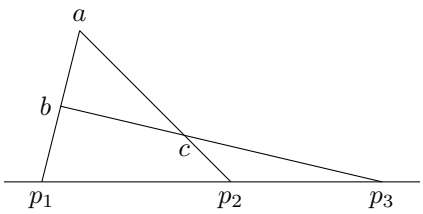
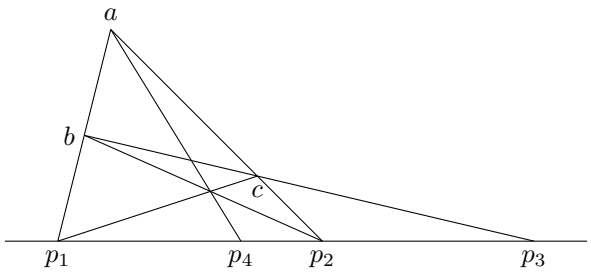


FIGURA 13. Il punto z è uguale alla media armonica di x e y.

Dati tre punti distinti p_1, p_2, p_3 di $\mathbb{P}^1$, possiamo applicare il il Teorema 1.9.7 per costruire "con la sola riga" l'unico punto p_4 tale che $[p_1, p_2; p_3, p_4] = -1$. Si consideri infatti $\mathbb{P}^1$ come una retta proiettiva $M \subset \mathbb{P}^2$ e per ogni $i = 1, 2, 3$ si prenda una qualunque retta proiettiva L_i tale che $L_i \cap M = p_i$. Denotiamo $a = L_1 \cap L_2$, $b = L_1 \cap L_3$ e $c = L_2 \cap L_3$:

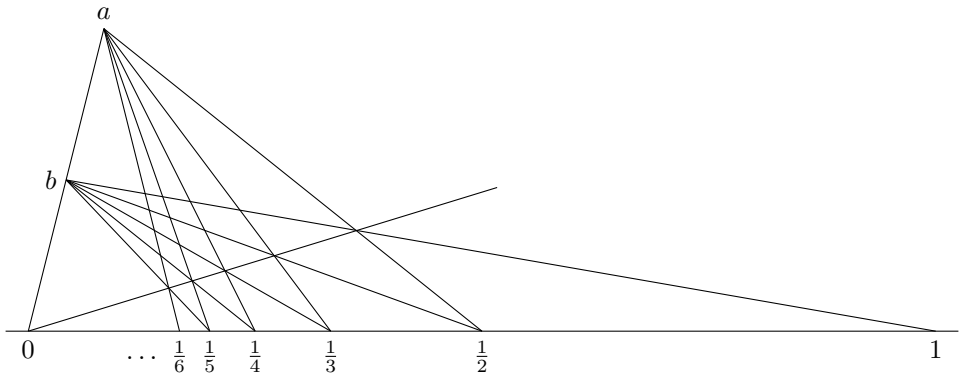


Adesso si definisca d come il punto di intersezione delle rette $\overline{p_1 c}$ e $\overline{p_2 b}$, allora il punto cercato p_4 è dato dall'intersezione di M con $\overline{ad}$:



La precedente costruzione si applica anche per calcolare graficamente la media armonica $z = \dfrac{2xy}{x+y}$ ossia l'unico numero tal che $[x, y; 0, z] = -1$ (Figura 13).

Siccome $\left[0, \frac{1}{n}; \frac{1}{n-1}, \frac{1}{n+1}\right] = -1$ per ogni intero positivo n, la precedente costruzione dà un metodo "con sola riga" per costruire la serie armonica partendo da $0, 1, \frac{1}{2}$, e ben raffigurato dal seguente disegnino,



nel quale, ribadiamo, la scelta delle tre rette $\overline{0a}$, $\overline{\frac{1}{2}a}$ e $\overline{1b}$ è arbitraria, dopo di che tutte le altre rette seguono in maniera univoca. Inoltre il disegno illustra la proiettività $\phi(x) = x/(x+1)$ di $\mathbb{P}^1$ (x=coordinata affine) come composizione di due proiezioni di centri b ed a rispettivamente.

Esercizi

ESERCIZIO 16. Sia $\mathbb{K}$ un campo infinito. Provare che per ogni $n \geq 5$ esiste un insieme $S \subset \mathbb{P}^1$ di n punti tale che, se $\phi \in \mathrm{Aut}(\mathbb{P}^1)$ e $\phi(S) \subset S$, allora $\phi = Id$.

ESERCIZIO 17. Sia $p \in \mathbb{P}^n$ e $G \subset \mathrm{Aut}(\mathbb{P}^n)$ il sottogruppo delle proiettività ϕ tali che $\phi(H) \subset H$ per ogni iperpiano H contenente p. Provare che G agisce transitivamente sull'insieme degli iperpiani di $\mathbb{P}^n$ che non contengono p.

ESERCIZIO 18. Sia $\lambda \in \mathbb{K} - \{0, 1\}$ fissato, $L \subset \mathbb{P}^2$ una retta e $\pi\colon \mathbb{P}^2 - \{o\} \to L$ la proiezione di centro $o \notin L$. Definiamo un'applicazione $\phi\colon \mathbb{P}^2 \to \mathbb{P}^2$ nel modo seguente:

$\phi(o) = o$ e $\phi(p) = p$ per ogni $p \in L$; se $p \neq o$ e $p \notin L$, allora si pone $r = \pi(p)$ e $\phi(p) = q$, dove $q \in o + p$ è l'unico punto tale che $[o, r; p, q] = \lambda$.
Provare che ϕ è una proiettività. Provare inoltre ϕ è un involuzione (cioè $\phi^2 = Id$) se e solo se $\lambda = -1$.

ESERCIZIO 19. Sia $\mathbb{K}$ algebricamente chiuso e $\phi \in \mathrm{Aut}(\mathbb{P}^1)$ una proiettività di ordine finito e non divisibile per la caratteristica di $\mathbb{K}$. Provare che ϕ ha esattamente due punti fissi.

ESERCIZIO 20. (caratteristica $\neq 2$) Una quaterna ordinata $p_1, \ldots, p_4$ di punti distinti di $\mathbb{P}^1$ definisce un omomorfismo iniettivo di gruppi $h\colon \Gamma_4 \to \mathrm{PGL}(2, \mathbb{K}) = \mathrm{Aut}(\mathbb{P}^1)$ caratterizzato dalla proprietà che per ogni permutazione $\sigma \in \Gamma_4$ vale $h(\sigma)(p_i) = p_{\sigma(i)}$. Provare che non esiste alcun sollevamento di h ad un omomorfismo $\Gamma_4 \to \mathrm{GL}(2, \mathbb{K})$. (Sugg.: non è restrittivo assumere $\mathbb{K}$ algebricamente chiuso; si prenda una coordinata affine tale che la quaterna sia $1, -1, a, -a$ con $a \neq \pm 1$.)

ESERCIZIO 21. Trovare una elemento di ordine 2 di $\mathrm{PGL}(2, \mathbb{Q})$ che non si rappresenta con elementi di ordine finito di $\mathrm{GL}(2, \mathbb{Q})$.

ESERCIZIO 22. Sia $\mathbb{K}^* = \mathbb{K} - \{0\}$ il gruppo moltiplicativo, $n \geq 2$ un intero e si assuma che esista un sottogruppo finito $H \subset \mathbb{K}^*$ di ordine d tale che $\mathbb{K}^*$ è generato da H e dalle potenze n-esime di elementi di $\mathbb{K}^*$. Sia inoltre h il massimo divisore di n non divisibile dalla caratteristica di $\mathbb{K}$.

Dimostrare che per ogni sottogruppo finito $\Gamma \subset \mathrm{PGL}(n, \mathbb{K})$ di ordine m esiste un sottogruppo finito $\Gamma' \subset \mathrm{GL}(n, \mathbb{K})$ di ordine $\leq hdm$ che si mappa surgettivamente su Γ tramite la proiezione naturale $\mathrm{GL}(n, \mathbb{K}) \to \mathrm{PGL}(n, \mathbb{K})$.

ESERCIZIO 23. (caratteristica $\neq 2, 3$) Sia $p_1, \ldots, p_4$ una quaterna di punti distinti di $\mathbb{P}^1$. Provare che:

- La quaterna è armonica se e solo se il birapporto $[p_1, \ldots, p_4]$ è invariante per l'azione di un sottogruppo di ordine 8 di Σ_4. Dedurre che il gruppo simmetrico Σ_4 contiene esattamente tre sottogruppi di ordine 8 (2-Sylow) tra loro coniugati ed isomorfi al gruppo diedrale D_4.
- La quaterna è equianarmonica se e solo se il birapporto $[p_1, \ldots, p_4]$ è invariante per l'azione del gruppo alterno A_4.

ESERCIZIO 24. Si consideri l'applicazione $v_n\colon \mathbb{P}^1 \to \mathbb{P}^n$, definita in coordinate omogenee da

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

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

ESERCIZIO 25. Si consideri il piano $\mathbb{R}^2$ con la metrica euclidea usuale, per ogni $p \in \mathbb{R}^2$ sia $F_p \cong \mathbb{P}^1_{\mathbb{R}}$ il fascio di rette passanti per il punto p. Verificare che l'applicazione $F_p \to F_p$ che manda ogni retta nella sua perpendicolare è una proiettività. Tale proiettività è chiamata *involuzione degli angoli retti*.

ESERCIZIO 26. Sia $o \in \mathbb{P}^1$ e G un insieme di n punti distinti $p_1, \dots, p_n$ di $\mathbb{P}^1$, con $n \geq 2$. Si definisce il luogo polare di o rispetto a G come l'insieme dei punti $q \in \mathbb{P}^1$ tali che

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

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

ESERCIZIO 27 $(*)$. Con l'utilizzo della sola riga dividere un rettangolo del piano euclideo in n parti uguali, per ogni $n \geq 2$. (Sugg.: quadrilatero armonico.)

ESERCIZIO 28. Sia $p \in \mathbb{P}^2$, siano L, H, T tre rette distinte di $\mathbb{P}^2$ passanti per il punto p e $q, r \in T$ punti distinti da p. Si consideri le proiettività $\phi\colon L \to H$ e $\psi\colon H \to L$ ottenute per proiezione di centro q ed r rispettivamente. Detta $\eta\colon L \to L$ la composizione di ϕ e ψ calcolare il valore del birapporto $[p, s; \eta(s), \eta^2(s)]$ al variare di s in $L - \{p\}$.

CAPITOLO 2

Curve algebriche piane

Per evitare eccessivi tecnicismi, in questo capitolo non tutti i risultati sono dimostrati completamente: alcune dimostrazioni sono omesse, altre fatte sotto ipotesi aggiuntive ed altre ancora sostituite con argomenti euristici.

Sempre per semplicità espositiva, da questo momento in poi e salvo avviso contrario, con il simbolo $\mathbb{K}$ denoteremo sempre un campo *algebricamente chiuso*, sebbene molti risultati esposti siano validi per una classe di campi più estesa; in alcuni casi metteremo delle condizioni sulla caratteristica di $\mathbb{K}$.

Giova ricordare che ogni campo algebricamente chiuso $\mathbb{K}$ è infinito: infatti se contenesse un numero finito di elementi $a_1, \ldots, a_n$, allora il polinomio

$$p(t) = 1 + \prod_{i=1}^{n}(t - a_i)$$

non avrebbe radici in $\mathbb{K}$, contraddicendo la chiusura algebrica.

Supporremo che il lettore abbia conoscenza delle nozioni e delle principali proprietà dei campi e degli spazi proiettivi. Il simbolo $\mathbb{N} = \{0, 1, \ldots\}$ denota l'insieme degli interi non negativi, mentre indicheremo con $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ i campi dei numeri razionali, reali e complessi, rispettivamente. Infine, se X è un insieme finito, indichiamo con $|X| \in \mathbb{N}$ il suo numero di elementi.

2.1. Polinomi numerici

Dati due interi non negativi $n, d \in \mathbb{N}$, il coefficiente binomiale

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

può essere definito come il numero dei sottoinsiemi di cardinalità d contenuti in un insieme di n elementi e sono ben note le formule:

$$\binom{n}{0} = \binom{n}{n} = 1, \qquad \binom{n}{d} = \frac{1}{d!}\prod_{i=0}^{d-1}(n-i), \qquad d > 0\,,$$

$$\binom{n}{d} = \binom{n-1}{d-1} + \binom{n-1}{d}, \qquad d, n > 0\,.$$

$$(x+y)^n = \sum_{d=0}^{n}\binom{n}{d}x^d y^{n-d}.$$

Osserviamo anche che $\binom{n}{d} = 0$ se $d > n$ e che per $0 \le d \le n$ vale $\binom{n}{d} = \dfrac{n!}{d!(n-d)!}$.

Più in generale, se t è una indeterminata, $n \in \mathbb{Z}$, $d \in \mathbb{N}$ e consideriamo i polinomi

$$\binom{t+n}{0} = 1, \qquad \binom{t+n}{d} = \frac{1}{d!}\prod_{i=0}^{d-1}(t+n-i) \in \mathbb{Q}[t], \qquad d > 0\,,$$

allora continua a valere la formula

$$\binom{t+n}{d} = \binom{n+t-1}{d-1} + \binom{n+t-1}{d}.$$

Basta infatti osservare che

$$\binom{n+t-1}{d-1} = \binom{t+n}{d}\frac{d}{n+t}, \qquad \binom{n+t-1}{d} = \binom{t+n}{d}\frac{n+t-d}{n+t}\,.$$

Per ogni $a \in \mathbb{Z}$ ed ogni $n > 0$ il polinomio

$$\binom{t+a}{n} = \frac{1}{n!}\prod_{i=0}^{n-1}(t+a-i) = \frac{1}{n!}t^n + \cdots \tag{2.1}$$

ha grado n, coefficiente direttivo $1/n!$ e n radici distinte $-a, -a+1, \ldots, -a+n-1$.

DEFINIZIONE 2.1.1. Un polinomio $p(t) \in \mathbb{Q}[t]$ si dice un **polinomio numerico** se esiste un intero N tale che $p(n) \in \mathbb{Z}$ per ogni intero $n \geq N$.

Ogni polinomio a coefficienti interi è numerico, ma esistono anche polinomi numerici a coefficienti razionali: ad esempio il polinomio $\binom{t+n}{d}$ è numerico in quanto uguale ad un coefficiente binomiale per ogni intero e $t \geq d-n$.

LEMMA 2.1.2. *Se $p(t) \in \mathbb{Q}[t]$ è un polinomio numerico, allora $p(n) \in \mathbb{Z}$ per ogni $n \in \mathbb{Z}$.*

DIMOSTRAZIONE. Induzione sul grado di $p(t)$. Se $p(t)$ è una costante, allora tale costante deve essere intera. Se $p(t)$ ha grado $n > 0$, allora il polinomio $q(t) = p(t) - p(t-1)$ è numerico di grado $n-1$ e per l'ipotesi induttiva $q(n) \in \mathbb{Z}$ per ogni intero n. Ne consegue inevitabilmente che anche $p(n) \in \mathbb{Z}$ per ogni $n \in \mathbb{Z}$. □

È chiaro che somme e differenza di polinomi numerici sono ancora polinomi numerici. Se $p(t)$ è un polinomio numerico allora anche $p(t-a)$ è un polinomio numerico per ogni $a \in \mathbb{Z}$.

LEMMA 2.1.3. *Sia $p(t)$ un polinomio numerico di grado n. Per ogni $a, b \in \mathbb{Z}$ il polinomio numerico*

$$p(t) + p(t-a-b) - p(t-a) - p(t-b)$$

ha grado $\leq n-2$.

DIMOSTRAZIONE. Sia $p(t) = \sum_{i=0}^{n} c_i t^i$, allora per ogni intero d si ha

$$p(t+d) = \sum_{i=0}^{n} c_i (t+d)^i = \sum_{i=0}^{n}\sum_{j=0}^{i} c_i \binom{i}{j} t^j d^{i-j} = \sum_{j=0}^{n}\left(\sum_{i=j}^{n} c_i d^{i-j}\binom{i}{j}\right) t^j.$$

Dunque il coefficienti di t^n e t^{n-1} in $p(t+d)$ sono rispettivamente c_n e $c_{n-1} + nc_n d$. Di conseguenza, i coefficienti di t^n e t^{n-1} in $p(t) + p(t-a-b) - p(t-a) - p(t-b)$ sono, rispettivamente $c_n + c_n - c_n - c_n = 0$ e

$$c_{n-1} + c_{n-1} - nc_n(a+b) - c_{n-1} + nc_n a - c_{n-1} + nc_n b = 0\,.$$

□

TEOREMA 2.1.4. *Sia $p(t)$ un polinomio numerico di grado n. Allora esiste un'unica successione di interi $a_0, \ldots, a_n$ tale che*

$$p(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i}\,.$$

DIMOSTRAZIONE. Sia $V \subset \mathbb{Q}[t]$ il $\mathbb{Q}$-sottospazio vettoriale dei polinomi di grado $\leq n$. Per ogni $i = 0, \ldots, n$ il polinomio $\binom{t+i}{i}$ ha grado i, i polinomi

$$\binom{t+0}{0}, \ldots, \binom{t+n}{n},$$

sono linearmente indipendenti e siccome V ha dimensione $n+1$ sono anche generatori. Abbiamo provato quindi che esistono unici $a_0, \ldots, a_n \in \mathbb{Q}$ tali che

$$p(t) = \sum_{i=0}^{n} a_i \binom{t+i}{i}\,.$$

Dimostriamo per induzione su n che ogni a_i è intero; a tal fine basta provare che $a_n \in \mathbb{Z}$. Infatti se $a_n \in \mathbb{Z}$ allora il polinomio

$$p(t) - a_n\binom{t+n}{n} = \sum_{i=0}^{n-1} a_i\binom{t+i}{i}$$

è numerico di grado $< n$ e per l'ipotesi induttiva $a_i \in \mathbb{Z}$ per ogni i. Consideriamo adesso il polinomio numerico $q(t) = p(t+1) - p(t)$. I coefficienti direttori di $p(t)$ e $q(t)$ si calcolano facilmente:

$$p(t) = \frac{a_n}{n!}t^n + \cdots, \qquad q(t) = p(t+1) - p(t) = \frac{a_n}{n!}(nt^{n-1}) + \cdots$$

Per l'ipotesi induttiva esistono n interi $b_0, \ldots, b_{n-1}$ tali che

$$q(t) = \sum_{i=0}^{n-1} b_i\binom{t+i}{i} = \frac{b_{n-1}}{(n-1)!}t^{n-1} + \cdots$$

da cui segue $a_n = b_{n-1} \in \mathbb{Z}$. □

Per uso futuro diamo un'altra interpretazione combinatoria dei coefficienti binomiali $\binom{d+n}{n}$ per $d \geq 0$.

LEMMA 2.1.5. *Siano $x_0, \ldots, x_n$ indeterminate. Per ogni $d \geq -n$ il numero di monomi*

$$x_0^{a_0}x_1^{a_1}\cdots x_n^{a_n}$$

di grado $a_0 + \cdots + a_n = d$ è uguale al coefficiente binomiale $\binom{d+n}{n}$.

DIMOSTRAZIONE. Se $-n \leq d < 0$ si ha $\binom{d+n}{n} = 0$ che chiaramente concide con il numero dei monomi di grado d. Se $d \geq 0$, dobbiamo calcolare la cardinalità dell'insieme

$$A = \{(a_0, \ldots, a_n) \in \mathbb{N}^{n+1} \mid a_0 + \cdots + a_n = d\}.$$

A tal fine consideriamo gli insiemi

$$A' = \{(a_1, \ldots, a_n) \in \mathbb{N}^n \mid a_1 + \cdots + a_n \leq d\},$$
$$B = \{(b_1, \ldots, b_n) \in \mathbb{N}^n \mid 1 \leq b_1 < b_2 < \cdots < b_n \leq d+n\},$$

osservando che B è in bigezione con i sottoinsiemi di cardinalità n di $\{1, \ldots, d+n\}$ e pertanto $|B| = \binom{d+n}{n}$. Osserviamo poi che le applicazioni $A \xrightarrow{f} A' \xrightarrow{g} B$:

$$f(a_0, \ldots, a_n) = (a_1, \ldots, a_n), \quad g(a_1, \ldots, a_n) = (a_1 + 1, a_1 + a_2 + 2, \ldots, a_1 + \cdots + a_n + n),$$

sono bigettive con inverse

$$f^{-1}(a_1, \ldots, a_n) = (d - \sum a_i, a_1, \ldots, a_n),$$
$$g^{-1}(b_1, \ldots, b_n) = (b_1 - 1, b_2 - b_1 - 1, \ldots, b_n - b_{n-1} - 1).$$

Si noti che A' è in bigezione con l'insieme dei monomi $x_1^{a_1}\cdots x_n^{a_n}$ di grado $\leq d$. □

Esercizi

ESERCIZIO 5. Provare che per ogni $n, d \geq 0$ vale la formula

$$\binom{d+n}{n} = \sum_{k\geq 0}^{n}\binom{n}{k}\binom{d}{k} = \sum_{k\geq 0}^{n}\binom{n}{n-k}\binom{d}{k}$$

considerando un insieme X formato da d palline bianche, n palline nere ed i sottoinsiemi di X formati da k palline bianche e $n-k$ palline nere.

ESERCIZIO 6. Provare l'identità polinomiale

$$\binom{t+n}{n} = (-1)^n\binom{-t-1}{n}.$$

ESERCIZIO 7. Per ogni coppia di interi positivi n, m, denotiamo con $M(n,m)$ l'insieme di tutte e applicazioni

$$f\colon \{1,2,\dots,n\} \to \{1,2,\dots,m\}$$

non decrescenti, ossia tali che $f(i+1) \geq f(i)$ per ogni $i < n$. Calcolare le cardinalità di $M(n,m)$, del suo sottoinsieme delle applicazioni iniettive quando $n \leq m$ e del suo sottoinsieme delle applicazioni surgettive quando $n \geq m$.

ESERCIZIO 8. Siano

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

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

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

ESERCIZIO 9. Dimostrare il seguente risultato, generalmente noto come *Principio di inclusione-esclusione*.

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

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

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

ESERCIZIO 10. Dimostrare che per ogni $s \geq 0$ vale lo sviluppo di Taylor

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

(Sugg.: induzione su s, derivando $(1-t)^{-s}$.)

ESERCIZIO 11. Provare che con la relazione di ordine, $p \geq q$ se e solo se $p(n) \geq q(n)$ per $n >> 0$, i polinomi numerici sono un insieme totalmente ordinato.

2.2. Polinomi omogenei

Denotiamo con $\mathbb{K}[x_0,\dots,x_n]$ l'anello dei polinomi a coefficienti in $\mathbb{K}$ nelle indeterminate $x_0,\dots,x_n$: ogni polinomio in $\mathbb{K}[x_0,\dots,x_n]$ è una combinazione lineare finita a coefficienti in $\mathbb{K}$ di monomi $x_0^{a_0}\cdots x_n^{a_n}$, il grado $\deg(p)$ di un polinomio non nullo p è uguale al massimo grado dei monomi che vi compaiono con coefficiente diverso da 0. Con la convenzione che il grado del polinomio nullo è uguale a $-\infty$ le seguenti formule sono di immediata verifica:

$$\deg(fg) = \deg(f) + \deg(g), \quad \deg(f+g) \leq \max(\deg(f),\deg(g)), \quad f,g \in \mathbb{K}[x_0,\dots,x_n].$$

In particolare $fg = 0$ se e solo se $f = 0$ oppure $g = 0$, ossia $\mathbb{K}[x_0,\dots,x_n]$ è un dominio di integrità: il suo campo delle frazioni globali è detto **campo delle funzioni razionali** e viene denotato $\mathbb{K}(x_0,\dots,x_n)$:

$$\mathbb{K}(x_0,\dots,x_n) = \left\{ \frac{f}{g} \;\middle|\; f,g \in \mathbb{K}[x_0,\dots,x_n],\ g \neq 0 \right\}.$$

Ad ogni polinomio $f \in \mathbb{K}[x_0,\dots,x_n]$ è associata la corrispondente funzione polinomiale $f\colon \mathbb{K}^{n+1} \to \mathbb{K}$ ottenuta sostituendo gli elementi di $\mathbb{K}$ al posto delle indeterminate ed eseguendo le necessarie operazioni di somma e prodotto. Come nel caso di polinomi in una variabile, siccome il campo $\mathbb{K}$ è infinito, il polinomio è univocamente determinato dalla corrispondente funzione polinomiale: ciò segue immediatamente dal seguente lemma.

LEMMA 2.2.1. *Sia $\mathbb{K}$ un campo infinito. Allora per ogni polinomio non nullo $0 \neq f \in \mathbb{K}[x_0,\dots,x_n]$ esistono $a_0,\dots,a_n \in \mathbb{K}$ tali che $f(a_0,\dots,a_n) \neq 0$.*

DIMOSTRAZIONE. Sia d il grado di f e dimostriamo il lemma per induzione su n: se $n = 0$ il polinomio $f(x_0)$ ha al più d radici distinte e quindi esiste $a_0 \in \mathbb{K}$ tale che $f(a_0) \neq 0$. Se $n > 0$, raccogliendo a fattor comune le potenze di x_0 possiamo scrivere

$$f = f_0 + f_1 x_0 + f_2 x_0^2 + \cdots + f_d x_0^d,$$

con i polinomi $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ non tutti nulli. Per induzione possiamo trovare $a_1, \ldots, a_n \in \mathbb{K}$ tali che i valori $f_i(a_1, \ldots, a_n) \in \mathbb{K}$ non sono tutti nulli e quindi tali che il polinomio

$$g(x_0) = f(x_0, a_1, \ldots, a_n)$$

è non nullo. Come nel caso $n = 0$ esiste $a_0 \in \mathbb{K}$ tale che $g(a_0) \neq 0$. □

Un polinomio $f \in \mathbb{K}[x_0, \ldots, x_n]$ si dice **omogeneo** di grado d se è combinazione lineare a coefficienti in $\mathbb{K}$ di monomi di grado d. Con questa definizione cadiamo nella contraddizione che il polinomio nullo è contemporaneamente di grado $-\infty$ ed omogeneo dei grado d per ogni $d \in \mathbb{N}$: si tratta tuttavia di una contraddizione del tutto innocua che semplifica l'esposizione rispetto ad una trattazione più formale e rigorosa.

Equivalentemente, un polinomio $f(x_0, \ldots, x_n)$ è omogeneo di grado d se, nel campo delle funzioni razionali, vale l'uguaglianza

$$f(x_0, x_1, \ldots, x_n) = x_0^d f\left(1, \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right).$$

Notiamo infine che ogni polinomio f di grado $n \geq 0$ si scrive in modo unico come

$$f = f_0 + f_1 + \cdots + f_n,$$

con f_i polinomio omogeneo di grado i e $f_n \neq 0$.

LEMMA 2.2.2. *Siano $f, g \in \mathbb{K}[x_0, \ldots, x_n]$ con f che divide g e $g \neq 0$. Se g è omogeneo, allora anche f è omogeneo.*

DIMOSTRAZIONE. Per ipotesi esiste un polinomio h tale che $fh = g$ e siccome $g \neq 0$ anche $f, h \neq 0$. Se f ha grado n e h ha grado m possiamo scrivere

$$f = f_0 + f_1 + \cdots + f_n, \qquad h = h_0 + f_1 + \cdots + h_m, \qquad n, m \geq 0,$$

con f_i, h_i omogenei di grado i e f_n, h_m non nulli. Siano

$$r = \min\{i \mid f_i \neq 0\}, \qquad s = \min\{i \mid h_i \neq 0\},$$

e supponiamo per assurdo $r < n$; allora

$$g = f_r h_s + \sum_{r+s<i+j<n+m} f_i h_j + f_n h_m,$$

e siccome $f_r h_s \neq 0$ è omogeneo di grado $r + s$, $f_n h_m \neq 0$ è omogeneo di grado $n + m$ mentre ogni monomio della sommatoria rimanente ha grado strettamente compreso tra $r+s$ e $n+m$, ne segue che il polinomio g contiene sia monomi di grado $r + s$ che monomi di grado $n + m$, contraddicendo l'ipotesi di omogeneità. □

Un'altra fondamentale proprietà di $\mathbb{K}[x_0, \ldots, x_n]$, ben nota dai corsi di Algebra, è quella di essere un dominio a fattorizzazione unica: un polinomio f si dice **irriducibile** se ha grado positivo e se non è il prodotto di polinomi di grado strettamente inferiore. Ogni polinomio non nullo si scrive in maniera essenzialmente unica come prodotto di polinomi irriducibili. Più precisamente, se

$$f = p_1 \cdots p_n = q_1 \cdots q_m$$

con $p_1, \ldots, p_n, q_1, \ldots, q_m$ polinomi irriducibli, allora $n = m$ e, a meno dell'ordine, per ogni indice i vale $p_i = c_i q_i$ per qualche $c_i \in \mathbb{K}$.

Due polinomi f, g si dicono senza fattori comuni, o relativamente primi, se non esiste alcun polinomio irriducibile che li divide entrambi.

Ricordiamo che un diagramma in serie di spazi vettoriali ed applicazioni lineari

$$\cdots \to V_i \xrightarrow{f_i} V_{i+1} \xrightarrow{f_{i+1}} V_{i+2} \to \cdots$$

si dice una **successione esatta** se $\ker f_i$ è uguale all'immagine di f_{i-1}, beninteso ogni volta che f_i ed f_{i-1} fanno parte del diagramma.

Ad esempio la successione $0 \to V \xrightarrow{f} W$ è esatta se e solo se f è iniettiva, mentre $V \xrightarrow{f} W \to 0$ è una successione esatta se e solo se f è surgettiva. Segue dal teorema del rango che se $0 \to V \to W \to U \to 0$ è una successione esatta di spazi vettoriali di dimensione finita, allora $\dim W = \dim V + \dim U$.

Il conucleo di un'applicazione lineare $f\colon V \to W$ è definito come lo spazio vettoriale quoziente $\operatorname{coker}(f) = \dfrac{W}{f(V)}$: si ha dunque una successione esatta

$$0 \to \ker(f) \xrightarrow{i} V \xrightarrow{f} W \xrightarrow{p} \operatorname{coker}(f) \to 0$$

dove i e p sono le applicazioni di inclusione e proiezione al quoziente, rispettivamente. Similmente, ogni quadrato commutativo

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ A & \xrightarrow{g} & B \end{array}$$

si estende ab un diagramma commutativo con le righe esatte:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(f) & \longrightarrow & V & \xrightarrow{f} & W & \longrightarrow & \operatorname{coker}(f) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \beta} & & \\ 0 & \longrightarrow & \ker(g) & \longrightarrow & A & \xrightarrow{g} & B & \longrightarrow & \operatorname{coker}(g) & \longrightarrow & 0. \end{array}$$

Prima di proseguire, precisiamo cosa si intende quando diciamo che "i polinomi irriducibili sono invarianti per cambio di coordinate". Sia $A = (a_{ij}) \in M_{n+1,m+1}(\mathbb{K})$ una matrice e denotiamo con lo stesso simbolo $A\colon \mathbb{K}^{m+1} \to \mathbb{K}^{n+1}$ l'applicazione lineare associata, ossia l'applicazione che manda il punto y di coordinate $y_0, \dots, y_m$ nel punto $x = Ay$ di coordinate $x_i = \sum_j a_{ij} y_j$, $i = 0, \dots, n$.

Dato un polinomio $f(x_0, \dots, x_n)$ possiamo considerare il polinomio $A^* f \in \mathbb{K}[y_0, \dots, y_m]$ ottenuto sostituendo alla variabile x_i l'espressione $\sum_j a_{ij} y_j$:

$$A^* f(y_0, \dots, y_n) = f\Big(\sum_j a_{0j} y_j, \dots, \sum_j a_{nj} y_j\Big)\,.$$

Ad esempio, se $f(x_0, x_1) = x_0^1 - x_1^2$ e l'applicazione lineare A è data dalle relazioni

$$x_0 = y_0 + y_1, \qquad y_1 = x_0 - x_1$$

si ha:

$$A^* f(y_0, y_1) = (y_0 + y_1)^2 - (y_0 - y_1)^2 = 4 y_0 y_1\,.$$

Lasciamo per esercizio la verifica che l'applicazione $A^*\colon \mathbb{K}[x_0, \dots, x_n] \to \mathbb{K}[y_0, \dots, y_m]$ commuta con somme e prodotti e che il grado di $A^* f$ è minore od uguale al grado di f. La funzione polinomiale $A^* f\colon \mathbb{K}^{m+1} \to \mathbb{K}$ è uguale alla composizione $\mathbb{K}^{m+1} \xrightarrow{A} \mathbb{K}^{n+1} \xrightarrow{f} \mathbb{K}$.

Su A è invertibile, allora $(A^{-1})^* = (A^*)^{-1}$. In particolare A^* è un isomorfismo di anelli e di spazi vettoriali ed il grado di $A^* f$ è uguale al grado di f. Se f è irriducibile, allora anche $A^* f$ è irriducibile: infatti se fosse $A^* f = gh$ con g, h polinomi di grado positivo, allora si avrebbe $f = ((A^{-1})^* g)((A^{-1})^* h)$ ed i due polinomi $(A^{-1})^* g$, $(A^{-1})^* h$ hanno grado positivo.

Eliminazione semplice. Sia n un intero positivo fissato. Per ogni intero d denotiamo con $S_d \subset \mathbb{K}[x_0, \dots, x_n]$ il sottospazio vettoriale dei polinomi omogenei di grado d; in particolare $S_d = 0$ per ogni $d < 0$. Segue immediatamente dal Lemma 2.1.5 che per ogni $d \geq -n$ la dimensione di S_d è uguale a

$$\dim S_d = \binom{d+n}{n} = \frac{1}{n!} d^n + \frac{n+1}{2(n-1)!} d^{n-1} + \cdots\,, \quad d \geq -n\,.$$

Una dimostrazione alternativa della formula precedente si ottiene per induzione su $d+n$ ed osservando che per ogni $d>0$ si ha una successione esatta

$$0 \to S_{d-1} \xrightarrow{\cdot x_0} S_d \xrightarrow{x_0 \mapsto 0} S_d \cap \mathbb{K}[x_1, \dots, x_n] \to 0,$$

da cui segue

$$\dim S_d = \binom{d+n-1}{n} + \binom{d+n-1}{n-1}.$$

LEMMA 2.2.3. *Siano $f, g \in \mathbb{K}[x_0, \dots, x_n]$ polinomi omogenei non nulli e di grado $a, b > 0$ rispettivamente. Per ogni intero d si consideri il complesso di spazi vettoriali:*

$$0 \to S_{d-a-b} \xrightarrow{\alpha_d} S_{d-a} \oplus S_{d-b} \xrightarrow{\beta_d} S_d, \qquad \alpha_d(p) = (gp, fp), \quad \beta_d(q,r) = fq - gr\,. \tag{2.2}$$

Allora le seguenti condizioni sono equivalenti:

1. *f, g non hanno fattori comuni di grado positivo;*
2. *per ogni intero d il complesso (2.2) è una successione esatta;*
3. *esiste un intero $d \geq a+b-1$ per cui il complesso (2.2) è una successione esatta.*

DIMOSTRAZIONE. È chiaro che $\beta\alpha = 0$. Inoltre, per ipotesi f, g sono entrambi non nulli quindi α è iniettiva poiché $\mathbb{K}[x_0, \dots, x_n]$ è un dominio di integrità.

Supponiamo f, g senza fattori comuni, d qualsiasi e sia $(q,r) \in \ker \beta_d$, ossia $fq = gr$. Se $r = 0$, siccome $f \neq 0$ si ha $q = 0$ ed in tal caso la coppia $(q,r) = (0,0)$ appartiene all'immagine di α. Se $r \neq 0$, siccome nessun fattore di f divide g si ha $r = fp$ con $p \in S_{d-a-b}$. Dunque $gfp = fq$ da cui segue $q = gp$ e di conseguenza $(q,r) = \alpha_d(p)$.

Se f, g hanno un fattore comune h di grado positivo c, dimostriamo che per ogni $d \geq a+b-c$ il nucleo di β_d ha dimensione strettamente maggiore della dimensione di S_{d-a-b}. Infatti l'applicazione

$$\gamma \colon S_{d-a-b+c} \to \ker(\beta_d), \qquad \gamma(p) = \left(p\frac{g}{h}, p\frac{f}{h}\right),$$

è ben definita ed iniettiva, quindi

$$\dim \ker(\beta_d) \geq \dim S_{d-a-b+c} > \dim S_{d-a-b}\,.$$

□

TEOREMA 2.2.4 (Eliminazione semplice). *Siano $f, g \in \mathbb{K}[x_0, \dots, x_n]$ polinomi senza fattori comuni ed omogenei di gradi $a, b > 0$, rispettivamente. Allora esistono un intero d e due polinomi omogenei $h, k \in \mathbb{K}[x_0, \dots, x_n]$ di gradi $d-a, d-b$ rispettivamente tali che*

$$0 \neq hf - kg \in \mathbb{K}[x_1, \dots, x_n]\,.$$

Inoltre, se $n = 2$ è possibile scegliere l'intero d uguale al prodotto ab.

È chiaro l'uso del termine eliminazione nel Teorema 2.2.4 in quanto la variabile x_0 viene "eliminata" mediante la combinazione $hf - kg$.

DIMOSTRAZIONE. Sicomme $a, b > 0$, l'ipotesi che f, g non abbiano fattori comuni implica necessariamente $n > 0$. Per il Lemma 2.1.5 lo spazio vettoriale $R_d = S_d \cap \mathbb{K}[x_1, \dots, x_n]$ ha dimensione uguale a

$$\binom{d+n-1}{n-1} = \frac{d^{n-1}}{(n-1)!} + \cdots, \qquad d \geq 1-n.$$

Per il Lemma 2.2.3, per ogni intero d si ha una successione esatta

$$0 \to S_{d-a-b} \xrightarrow{\alpha_d} S_{d-a} \oplus S_{d-b} \xrightarrow{\beta_d} S_d \to \operatorname{coker}(\beta_d) \to 0,$$
$$\alpha_d(p) = (gp, fp), \quad \beta_d(q,r) = fq - gr\,.$$

Per ogni $d \geq a+b-1$ la dimensione del conucleo di β_d è quindi uguale a

$$\begin{aligned}\dim \operatorname{coker}(\beta_d) &= \dim S_d - \dim S_{d-a} - \dim S_{d-b} + \dim S_{d-a-b} \\ &= \binom{d+n}{n} - \binom{d-a+n}{n} - \binom{d-b+n}{n} + \binom{d-a-b+n}{n}.\end{aligned}$$

Per il Lemma 2.1.3 la dimensione di $\operatorname{coker}(\beta_d)$ è un polinomio numerico in d di grado $\leq n-2$ e dunque per d sufficientemente grande si ha $\dim R_d > \dim \operatorname{coker}(\beta_d)$. Ne segue che esiste d per cui la restrizione al sottospazio R_d della proiezione $S_d \to \operatorname{coker}(\beta_d)$ non è iniettiva, ossia esiste un elemento non nullo che appartiene all'intersezione di R_d con l'immagine di β_d, che è esattamente quello che volevamo dimostrare.

Se $n = 2$ allora allora lo spazio vettoriale $R_d = S_d \cap \mathbb{K}[x_1, x_2]$ ha dimensione $d+1$; si ha $ab \geq a+b-1$ e per ogni $d \geq a+b-1$ la dimensione del conucleo di β_d è

$$\begin{aligned}\dim \operatorname{coker}(\beta_d) &= \binom{d+2}{2} - \binom{d-a+2}{2} - \binom{d-b+2}{2} + \binom{d-a-b+2}{2} \\ &= \frac{1}{2}\left((d+2)(d+1) - (d-a+2)(d-a+1) - (d-b+2)(d-b+1)\right. \\ &\quad \left. +(d-a-b+2)(d-a-b+1)\right) \\ &= ab\,.\end{aligned}$$

Dunque per ogni $d \geq ab$ l'immagine di β_d ha intersezione non nulla con R_d. Un conto simile mostra pure che per $n = 1$ l'applicazione β_d è surgettiva per ogni $d \geq a+b-1$. □

Osservazione 2.2.5. I polinomi h, k nell'enunciato del Teorema 2.2.4 non sono unici, nemmeno nel caso in cui d sia il minimo intero per cui vale la proprietà. Abbiamo dato una dimostrazione non costruttiva della loro esistenza ma va segnalato che, usando tecniche più raffinate, ma sempre riconducibili all'algebra lineare, è possibile dare delle formula esplicite per k, h nel caso $d = ab$, in cui i coefficienti di h, k sono funzioni polinomiali dei coefficienti di f, g. Vedremo (implicitamente) tali formule (sotto l'ipotesi aggiuntiva che $f(1, 0, \ldots, 0) \neq 0$) nella Sezione **??**. Questo prova anche che per ogni $n \geq 2$ l'intero d può essere preso minore o uguale al prodotto ab.

Derivate. In analogia con la teoria delle derivate parziali delle funzioni di variabile reale, per ogni indice $i = 0, \ldots, n$ indichiamo con

$$\frac{\partial}{\partial x_i} \colon \mathbb{K}[x_0, \ldots, x_n] \to \mathbb{K}[x_0, \ldots, x_n]$$

l'applicazione lineare definita sui monomi mediante la formula

$$\frac{\partial}{\partial x_i} x_0^{a_0} \cdots x_n^{a_n} = \frac{a_i}{x_i} x_0^{a_0} \cdots x_n^{a_n}\,.$$

Lasciamo per esercizio che continua a valere la **formula di Leibniz**:

$$\frac{\partial fg}{\partial x_i} = \frac{\partial f}{\partial x_i} g + f \frac{\partial g}{\partial x_i}\,.$$

Lemma 2.2.6. *Sia $f \in \mathbb{K}[x_0, \ldots, x_n]$ tale che $\dfrac{\partial f}{\partial x_i} = 0$ per ogni $i = 0, \ldots, n$:*

1. *se il campo $\mathbb{K}$ ha caratteristica 0, allora $f \in \mathbb{K}$ è una costante;*
2. *se il campo $\mathbb{K}$ è algebricamente chiuso di caratteristica positiva $p \geq 2$, allora esiste $g \in \mathbb{K}[x_0, \ldots, x_n]$ tale che $f = g^p$.*

In particolare se f è irriducibile e $\mathbb{K}$ algebricamente chiuso, allora esiste sempre un indice i tale che $\dfrac{\partial f}{\partial x_i} \neq 0$.

Dimostrazione. Segue dalla formula di Leibniz che se una delle due condizioni è soddisfatta allora tutte le derivate parziali di f si annullano. Dimostriamo le implicazioni inverse per induzione su n, osservando preliminarmente che per ogni $a \in \mathbb{K}$ ed ogni numero primo p esiste b tale che $b^p = a$: infatti siccome $\mathbb{K}$ è algebricamente chiuso il polinomio $t^p - a$ possiede radici.

Sia $n \geq 0$ e supponiamo il lemma vero in $\mathbb{K}[x_0, \ldots, x_{n-1}]$. Dato $f \in \mathbb{K}[x_0, \ldots, x_n]$ con $\dfrac{\partial f}{\partial x_i} = 0$ per ogni i, possiamo scrivere

$$f(x_0, \ldots, x_n) = \sum_{j=0}^{d} f_j(x_0, \ldots, x_{n-1}) x_n^j, \qquad \frac{\partial f}{\partial x_n}(x_0, \ldots, x_n) = \sum_{j=1}^{d} j f_j(x_0, \ldots, x_{n-1}) x_n^{j-1},$$

e quindi $\dfrac{\partial f}{\partial x_n} = 0$ se e solo se $j f_j = 0$ per ogni j.

Se $\mathbb{K}$ ha caratteristica 0, e $j f_j = 0$ per ogni j, allora $f_j = 0$ per ogni $j > 0$, ossia $f = f_0$ è un polinomio in $x_0, \ldots, x_{n-1}$ e la tesi segue dall'ipotesi induttiva.

Se $\mathbb{K}$ ha caratteristica $p > 0$, e $j f_j = 0$ per ogni j, allora $f_j = 0$ per ogni j non divisibile per p e quindi possiamo scrivere

$$f(x_0, \ldots, x_n) = \sum_{j=0}^{h} g_j(x_0, \ldots, x_{n-1}) x_n^{jp}, \qquad g_j = f_{pj}\,.$$

Siccome, per ogni $i < n$ si ha $\dfrac{\partial f}{\partial x_i} = \sum_j \dfrac{\partial g_j}{\partial x_i} x_n^{jp}$ ne consegue che $\dfrac{\partial g_j}{\partial x_i} = 0$ per ogni i, j e per l'ipotesi induttiva si può scrivere

$$g_j = h_j^p, \qquad f = \sum_j h_j^p (x_n^j)^p\,.$$

Per concludere basta osservare che, poiché $(a+b)^p = a^p + b^p$ (p divide i coefficienti binomiali $\binom{p}{i}$ per $0 < i < p$), si ha

$$\left(\sum_j h_j x_n^j \right)^p = \sum_j h_j^p (x_n^j)^p = f\,.$$

□

È immediato verificare la validità della seguente formula, detta **Formula di Eulero**: per ogni polinomio omogeneo $f \in \mathbb{K}[x_0, \ldots, x_n]$ di grado m vale

$$\sum_{i=0}^{n} x_i \frac{\partial f}{\partial x_i} = m\, f\,. \tag{2.3}$$

Infatti, per linearità non è restrittivo supporre che f sia un monomio del tipo $x_0^{a_0} \cdots x_n^{a_n}$ con $\sum a_i = m$. Allora

$$\frac{\partial x_0^{a_0} \cdots x_n^{a_n}}{\partial x_i} = \begin{cases} a_i x_0^{a_0} \cdots x_i^{a_i - 1} \cdots x_n^{a_n} & \text{se } a_i > 0 \\ 0 & \text{se } a_i = 0 \end{cases}$$

e quindi

$$\sum_{i=0}^{n} x_i \frac{\partial x_0^{a_0} \cdots x_n^{a_n}}{\partial x_i} = \sum_{\{i \mid a_i > 0\}} a_i x_0^{a_0} \cdots x_i^{a_i} \cdots x_n^{a_n} = m x_0^{a_0} \cdots x_n^{a_n}\,.$$

Osserviamo che se f è omogeneo di grado $m > 0$, allora le sue derivate sono polinomi omogenei di grado $m - 1$, possibilmente nulli.

Esercizi.

Esercizio 12. Siano $\mathbb{K}$ un campo infinito e $f \in \mathbb{K}[x_0, \ldots, x_n]$. Provare che f è omogeneo di grado $d \geq 0$ se e solo se per ogni $(a_0, \ldots, a_n) \in \mathbb{K}^{n+1}$ e $t \in \mathbb{K} - \{0\}$ vale

$$f(ta_0, \ldots, ta_n) = t^d f(a_0, \ldots, a_n)\,.$$

2.3. Ipersuperfici proiettive

Da questo punto in poi, e fino alla fine del capitolo, supporremo salvo avviso contrario che $\mathbb{K}$ sia un campo algebricamente chiuso, e quindi infinito.

Il prossimo lemma non è altro che la reinterpretazione della chiusura algebrica di $\mathbb{K}$ per polinomi omogenei in due variabili.

LEMMA 2.3.1. *Sia $\mathbb{K}$ un campo algebricamente chiuso. Allora ogni polinomio omogeneo $f \in \mathbb{K}[x_0, x_1]$ non nullo di grado d è il prodotto di d polinomi omogenei di grado 1.*

DIMOSTRAZIONE. Sia $h \leq d$ il grado del polinomio $f(1,t) \in \mathbb{K}[t]$. Siccome $\mathbb{K}$ è algebricamente chiuso si ha

$$f(1,t) = c(t-a_1)(t-a_2)\cdots(t-a_h), \qquad c, a_1, \ldots, a_h \in \mathbb{K},$$

e quindi

$$f(x_0,x_1) = x_0^d f\left(1, \frac{x_1}{x_0}\right) = c x_0^{d-h} \prod_{i=1}^{h} (x_1 - a_i x_0).$$

□

Indichiamo con $\mathbb{P}^n$ lo spazio proiettivo di dimensione n su $\mathbb{K}$. Se $f \in \mathbb{K}[x_0, \ldots, x_n]$ è omogeneo di grado $d \geq 0$, $(a_0, \ldots, a_n) \in \mathbb{K}^{n+1}$ e $t \in \mathbb{K} - \{0\}$, allora

$$f(ta_0, \ldots, ta_n) = t^d f(a_0, \ldots, a_n)$$

e quindi $f(a_0, \ldots, a_n) = 0$ se e solo se $f(ta_0, \ldots, ta_n) = 0$. Tali considerazioni permettono di dare senso alle seguente definizione.

DEFINIZIONE 2.3.2. Il luogo di zeri proiettivo $V(f)$ di un polinomio omogeneo $f \in \mathbb{K}[x_0, \ldots, x_n]$ è il sottoinsieme di $\mathbb{P}^n$ dato da:

$$V(f) = \{p \in \mathbb{P}^n \mid f(p) = 0\} = \{[a_0, \ldots, a_n] \in \mathbb{P}^n \mid f(a_0, \ldots, a_n) = 0\}.$$

Quando il contesto lo consente si può scrivere, con un leggero abuso di notazione, anche $f(x) = 0$ per indicare il luogo di zeri proiettivo $V(f)$ di un polinomio omogeneo. Il lettore tenga sempre presente che un polinomio omogeneo $f \in \mathbb{K}[x_0, \ldots, x_n]$ non definisce alcuna funzione $\mathbb{P}^n \to \mathbb{K}$ ma solamente il suo luogo di zeri $V(f)$.

In alcuni casi, motivi di chiarezza notazionale suggeriranno di usare lettere maiuscole per denotare polinomi omogenei $F \in \mathbb{K}[x_0, \ldots, x_n]$. L'uso della lettera V (dall'inglese vanishing) per indicare il luogo di zeri è quello utilizzato nella stragrande maggioranza della letteratura in geometria algebrica, anche se non mancano rispettabilissime eccezioni.

LEMMA 2.3.3. *Se $f \in \mathbb{K}[x_0, \ldots, x_n]$ è omogeneo e non nullo, allora $V(f)$ è un sottoinsieme proprio di $\mathbb{P}^n$.*

DIMOSTRAZIONE. Se f ha grado 0, ossia f è una costante non nulla, allora $f(x) = 0$ è l'insieme vuoto. Se il grado di f è positivo allora $f(0, \ldots, 0) = 0$, mentre per il Lemma 2.2.1 esistono $a_0, \ldots, a_n \in \mathbb{K}$ tali che $f(a_0, \ldots, a_n) \neq 0$. Dunque gli a_i non sono tutti nulli ed il punto $[a_0, \ldots, a_n]$ non appartiene a $V(f)$. □

DEFINIZIONE 2.3.4. Chiameremo **ipersuperfice proiettiva** ciascun sottoinsieme del tipo $V(f) \subset \mathbb{P}^n$, con f polinomio omogeneo *di grado positivo*.

Ogni ipersuperfice in $\mathbb{P}^1$ è un insieme finito e non vuoto di punti. Infatti, se $f \in \mathbb{K}[x_0, x_1]$ è omogeneo di grado $d > 0$ per il Lemma 2.3.1 esiste una scomposizione in fattori lineari

$$f(x_0, x_1) = \prod_{i=1}^{d} (a_i x_0 + b_i x_1)$$

e quindi $V(f) = \{[b_i, -a_i] \mid i = 1, \ldots d\}$. Lo stesso argomento prova che ogni sottoinsieme finito di $\mathbb{P}^1$ è una ipersuperfice. Da tale osservazione segue in particolare che per ogni coppia di polinomi omogenei $f, g \in \mathbb{K}[x_0, x_1]$ si ha $V(f) \cap V(g) \neq \emptyset$ se e solo se f, g hanno un fattore comune.

LEMMA 2.3.5. *Le ipersuperfici proiettive intersecano ogni retta, ossia per ogni $X \subset \mathbb{P}^n$ ipersuperfice ed ogni retta proiettiva $L \subset \mathbb{P}^n$ vale $L \cap X \neq \emptyset$. In particolare X è infinito se $n \geq 2$.*

DIMOSTRAZIONE. Fissiamo un sistema di coordinate omogenee tali che $L = \{x_2 = x_3 = \cdots = x_n = 0\}$, sia f un polinomio omogeneo tale che $X = V(f)$ e consideriamo il polinomio $g(x_0, x_1) = f(x_0, x_1, 0, \ldots, 0)$. Il polinomio g è nullo se e solo se $L \subset X$; se L non è contenuta in X allora g è omogeneo dello stesso grado di f ed i punti di $L \cap X$ corrispondono allora ai fattori lineari di g.

Se $n \geq 2$ e $o \in \mathbb{P}^n$ non appartiene ad X, allora ogni retta passante per o interseca X e l'applicazione

$$X \to \{\text{rette per } o\}, \qquad p \mapsto \overline{op},$$

è surgettiva. In particolare X è un sottoinsieme infinito di $\mathbb{P}^n$. □

Si osserva immediatamente che più polinomi omogenei possono definire la medesima ipersuperfice, ad esempio per ogni costante $c \neq 0$ e per ogni polinomio omogeneo f si ha $V(cf) = V(f)$, ed anche $V(f) = V(f^2) = V(f^3) = \cdots$. Per ogni coppia di polinomi omogenei f, g, vale la regola $V(fg) = V(f) \cup V(g)$, mentre l'intersezione $V(f) \cap V(g)$ può essere scritta convenientemente nella forma $f(x) = g(x) = 0$.

Fortunatamente, almeno nel caso in cui f è irriducibile, il seguente teorema permette di ricostruire f (a meno di costanti moltiplicative) dalla ipersuperfice $f(x) = 0$.

TEOREMA 2.3.6 (degli zeri per ipersuperfici). *Siano $\mathbb{K}$ algebricamente chiuso e $f, g \in \mathbb{K}[x_0, \ldots, x_n]$ polinomi omogenei con f irriducibile. Allora $V(f) \subseteq V(g)$ se e solo se f divide g.*

DIMOSTRAZIONE. Abbiamo già visto che se f divide g allora $V(f) \subseteq V(g)$. Viceversa se f è irriducibile e non divide g, allora ha grado positivo e per il Lemma 2.3.3 esiste un punto $o \notin V(f)$. A meno di un cambio lineare di coordinate, possiamo supporre che $o = [1, 0, \ldots, 0]$.

Siano a il grado di f e b il grado di g. Se f non divide g, allora f e g non hanno fattori comuni ed abbiamo visto nel Teorema 2.2.4 che esiste un intero $d > 0$ e due polinomi omogenei h, di grado $d - a$, e k, di grado $d - b$, tali che

$$0 \neq r = hf - kg \in \mathbb{K}[x_1, \ldots, x_n] .$$

Mostriamo adesso che l'ipersuperfice $V(r)$ è una unione di rette passanti per il punto o, ossia che se $p \in V(r) - \{o\}$, allora $\overline{op} \subset V(r)$.

Siccome r contiene solo monomi in $x_1, \ldots, x_n$ si ha $o \in V(r)$. Se $p \neq o$ e $p \in V(r)$, allora $p = [a_0, \ldots, a_n]$ con $a_1, \ldots, a_n$ non tutti nulli e tali che $r(a_1, \ldots, a_n) = 0$. Ne segue che $V(r)$ contiene tutti i punti della retta affine $\overline{op} - \{o\}$, ossia tutti i punti di coordinate omogenee $[a_0 + t, \ldots, a_n]$, $t \in \mathbb{K}$.

Supponiamo adesso per assurdo $V(f) \subset V(g)$, allora $V(f) \subset V(r)$. Infatti, se $p \in V(f)$ e $p = [x]$ con $x \in \mathbb{K}^{n+1} - \{0\}$, allora $p \in V(g)$ e quindi $f(x) = g(x) = 0$,

$$r(x) = h(x)f(x) - k(x)g(x) = 0 .$$

D'altra parte ogni retta passante per o interseca $V(f)$, quindi interseca $V(r)$ in un punto diverso da o, quindi è interamente contenuta in $V(r)$. Ma questo implicherebbe $V(r) = \mathbb{P}^n$ in contraddizione con la condizione $r \neq 0$. □

COROLLARIO 2.3.7. *Siano $\mathbb{K}$ campo algebricamente chiuso e $f, g \in \mathbb{K}[x_0, \ldots, x_n]$ polinomi omogenei iriducibili. Allora $V(f) = V(g)$ se e solo se f e g differiscono per una costante moltiplicativa. In particolare f e g hanno lo stesso grado.*

DIMOSTRAZIONE. Per il Teorema 2.3.6, siccome $V(f) = V(g)$ ne consegue che f divide g e g divide f. □

Notiamo che il Corollario 2.3.7 sarebbe falso senza l'ipotesi sulla chiusura algebrica del campo. Ad esempio per $\mathbb{K} = \mathbb{R}$ i polinomi $f = x_0^2 + x_1^2$, $g = x_0^2 + 2x_1^2$ sono irriducibli e $V(f) = V(g) = \emptyset$.

DEFINIZIONE 2.3.8. Se il campo $\mathbb{K}$ è algebricamente chiuso, chiemeremo **ipersuperfice proiettiva irriducibile di grado** d ciascun sottoinsieme del tipo $V(f)$, con f polinomio omogeneo irriducibile di grado d.

Ogni ipersuperfice proiettiva è unione finita di ipersuperfici irriducibili. Infatti se f è omogeneo e $f = f_1^{a_1} \cdots f_r^{a_r}$ è la sua decomposizione in fattori irriducibili, allora ciascun f_i è omogeneo e

$$V(f) = V(f_1^{a_1}) \cup \cdots \cup V(f_r^{a_r}) = V(f_1) \cup \cdots \cup V(f_r)\,.$$

Esercizi.

ESERCIZIO 13. Provare che l'applicazione

$$\mathbb{P}^1 \to \mathbb{P}^n, \qquad [t_0, t_1] \mapsto [t_0^n, t_0^{n-1}t_1, \ldots, t_0 t_1^{n-1}, t_1^n],$$

è ben definita, iniettiva ed ha come immagine il sottoinsieme

$$X = \left\{ [x_0, \ldots, x_n] \in \mathbb{P}^n \;\middle|\; \operatorname{rank} \begin{pmatrix} x_0 & x_1 & \cdots & x_{n-1} \\ x_1 & x_2 & \cdots & x_n \end{pmatrix} = 1 \right\}.$$

Scrivere inoltre X come intersezione finita di ipersuperfici.

2.4. Curve piane

Da questo punto, e fino alla fine del capitolo restringeremo la nostra attenzione alle ipersuperfici di $\mathbb{P}^2$, altrimenti dette curve piane. Salvo avviso contrario indicheremo con $S_d \subset \mathbb{K}[x_0, x_1, x_2]$ il sottospazio vettoriale dei polinomi omogenei di grado d. Abbiamo già provato che per ogni $d \geq -2$ la dimensione di S_d è uguale a

$$\binom{d+2}{2} = \frac{(d+2)(d+1)}{2}\,.$$

In prima approssimazione possiamo definire una curva algebrica piana come il luogo dei punti di $\mathbb{P}^2$ che annullano un polinomio omogeneo nelle coordinate omogenee di $\mathbb{P}^2$. Questa definizione, sebbene semplice, non è sufficientemente precisa e presenta qualche difficoltà operativa.

Già nella teoria delle coniche proiettive si incontrano certi oggetti detti "rette doppie" che, insiemisticamente sono rette, ma che appartengono allo spazio delle coniche di $\mathbb{P}^2$.

DEFINIZIONE 2.4.1. Sia x_0, x_1, x_2 un sistema di coordinate omogenee su $\mathbb{P}^2$. Un sottoinsieme $C \subset \mathbb{P}^2$ si dice una **curva irriducibile** di grado d se esiste un polinomio irriducibile omogeneo $f(x_0, x_1, x_2)$ di grado d tale che $C = V(f)$, cioè

$$C = \{[x_0, x_1, x_2] \in \mathbb{P}^2 \mid f(x_0, x_1, x_2) = 0\}.$$

Ad esempio le rette di $\mathbb{P}^2$ sono curve irriducibili di grado 1. La definizione di curva irriducibile non dipende dal particolare sistema di coordinate omogenee. Sia infatti y_0, y_1, y_2 un altro sistema e $x_i = \sum a_{ij} y_j$ con la matrice a_{ij} invertibile; se $f(x_0, x_1, x_2) = g(y_0, y_1, y_2)$, allora vale

$$f(y_0, y_1, y_2) = 0 \quad \text{ se e solo se } \quad [y_0, y_1, y_2] \in C.$$

Inoltre il grado di f è uguale al grado di g e f è irriducibile se e solo se g è irriducibile.

Fissato un sistema di coordinate omogenee x_i, una curva irriducibile C determina a meno di costante moltiplicativa il polinomio f di cui è luogo di zeri. Infatti se $g(x_0, x_1, x_2) = 0$ per ogni $[x] \in C$ allora, per il Teorema 2.3.6, f divide g e se g è irriducibile allora $g = af$ per qualche $a \in \mathbb{K}$.

DEFINIZIONE 2.4.2. Una curva algebrica piana è una combinazione lineare formale $C = m_1 C_1 + m_2 C_2 + \cdots + m_r C_r$ dove, per ogni indice i, C_i è una curva irriducibile e m_i è un intero positivo.

- Le curve C_i si dicono le **componenti irriducibili** di C.
- Per ogni $i = 1, \ldots, r$, il numero m_i viene detto la **molteplicità** della componente C_i.

- Il sottoinsieme $\mathrm{Supp}(C) = \cup C_i \subset \mathbb{P}^2$ è detto il **supporto** della curva. Con un leggero abuso di notazione, se C è una curva e $p \in \mathbb{P}^2$, scriveremo $p \in C$ per indicare che $p \in \mathrm{Supp}(C)$. Similmente se C, D sono due curve scriveremo $C \cap D$ per indicare l'intersezione dei supporti $\mathrm{Supp}(C) \cap \mathrm{Supp}(D)$.
- Se $n_1, \dots, n_r$ sono i gradi delle componenti irriducibili $C_1, \dots, C_r$, allora il numero $\deg(C) = n_1 m_1 + \cdots + n_r m_r$ è detto il **grado** di C.
- Una componente irriducibile C_i si dice **multipla** se la sua molteplicità m_i è maggiore di 1; la curva C si dice **ridotta** se non possiede componenti multiple, ovvero se $m_i = 1$ per ogni i.

Se C e D sono curve, la loro "somma" $C + D$ è la curva che ha come componenti irriducibili l'unione delle componenti di C e D e come molteplicità la somma delle stesse, dove si intende che la molteplicità di una curva irriducibile è uguale a 0 se tale curva non è una componente. Il grado della somma è uguale alla somma dei gradi.

Nel resto del capitolo, con il termine curva intenderemo sempre una curva algebrica piana. Le curve di grado $1, 2, 3, 4, 5$ e 6 si possono anche chiamare rispettivamente rette, coniche, cubiche, quartiche, quintiche e sestiche.

Fissato un sistema di coordinate omogenee x_0, x_1, x_2, esiste una bigezione fra l'insieme delle curve algebriche di grado n ed il proiettivizzato dello spazio vettoriale dei polinomi omogenei di grado n nelle variabili x_0, x_1, x_2. Infatti, se f è un polinomio omogeneo di grado n, allora esiste una decomposizione in fattori irriducibili $f = f_1^{m_1} \cdots f_r^{m_r}$: possiamo quindi associare ad f la curva le cui componenti irriducibili $C_i = V(f_i)$ sono i luoghi di zeri dei polinomi f_i aventi molteplicità m_i. Per l'unicità della fattorizzazione, la curva $C = m_1 C_1 + \cdots + m_r C_r$ risulta ben definita e la denoteremo spesso come la curva di equazione $f(x) = 0$.

Sia data viceversa una curva $C = \sum m_i C_i$; per definizione di curva irriducibile possiamo scrivere $C_i = V(f_i)$, con f_i polinomio omogeneo irriducibile per ogni i e considerare il prodotto $f = \prod f_i^{m_i}$. Essendo il polinomio f_i definito a meno di costante moltiplicativa, anche f è definito a meno di costante moltiplicativa.

Si noti che in tale corrispondenza biunivoca vale la relazione $\mathrm{Supp}(C) = V(f)$.

Ogni coppia di curve piane $V(f)$ e $V(g)$ ha intersezione non vuota: se f e g hanno un fattore comune $f = hf'$, $g = hg'$, allora $V(f) = V(h) \cup V(f')$, $V(g) = V(h) \cup V(g')$ e di conseguenza

$$\emptyset \neq V(h) \subseteq V(f) \cap V(g)\,.$$

Se f e g non hanno fattori comuni, il fatto che le due curve si intersecano segue dai seguenti due lemmi.

LEMMA 2.4.3. *Siano $f, g \in \mathbb{K}[x_0, x_1, x_2]$ polinomi senza fattori comuni ed omogenei di gradi $a, b > 0$, rispettivamente a coefficienti in un campo algebricamente chiuso. Allora esistono due polinomi omogenei $h, k \in \mathbb{K}[x_0, x_1, x_2]$ di gradi $(b-1)a, (a-1)b$ rispettivamente tali che $hf + kg$ è il prodotto di ab polinomi omogenei non nulli di grado 1.*

DIMOSTRAZIONE. Per il caso $n = 2$ del Teorema 2.2.4 esistono due polinomi omogenei $h, k \in \mathbb{K}[x_0, x_1, x_2]$ di gradi $(b-1)a, (a-1)b$ rispettivamente tali che

$$0 \neq hf + kg \in \mathbb{K}[x_1, x_2]\,,$$

mentre per il Lemma 2.3.1 ogni polinomio omogeneo in due variabili è un prodotto di fattori lineari. □

LEMMA 2.4.4. *Sia $\mathbb{K}$ algebricamente chiuso. Siano $f \in S_a$ e $g \in S_b$, $a, b > 0$, polinomi senza fattori comuni, allora $V(f) \cap V(g) \neq \emptyset$. Più precisamente, se è d il minimo intero per cui esiste una relazione del tipo*

$$0 \neq pf - qg = l_1 l_2 \cdots l_d \tag{2.4}$$

per opportuni $l_1, \dots, l_d \in S_1$, $p \in S_{d-a}$, $q \in S_{d-b}$. Allora $V(f) \cap V(g) \cap V(l_i) \neq \emptyset$ per ogni i.

DIMOSTRAZIONE. Osserviamo preliminarmente che l'enunciato del lemma ha senso in virtù del Lemma 2.4.3 e che inoltre vale $\min(a, b) \leq d \leq ab$. Per evidenti motivi di simmetria

basta dimostrare che $V(f)\cap V(g)\cap V(l_1)\neq\emptyset$ e fissiamo un sistema di coordinate omogenee x_0,x_1,x_2 tali che $l_1=x_2$. In linea teorica abbiamo la seguente dicotomia:

(1) i due polinomi $f(x_0,x_1,0),g(x_0,x_1,0)$ hanno fattori comuni, oppure

(2) i due polinomi $f(x_0,x_1,0),g(x_0,x_1,0)$ sono relativamente primi.

Nel primo caso se h è un polinomio omogeneo di grado positivo che divide $f(x_0,x_1,0)$ e $g(x_0,x_1,0)$, allora $V(h)\cap V(l_1)$ è non vuoto (intersezione di ipersuperfice con una retta) ed è contenuto in $V(f)\cap V(g)\cap V(l_1)$.

Proviamo adesso che il secondo caso conduce ad una contraddizione e quindi va escluso dalla lista delle possibilità. Supponiamo per assurdo che i polinomi $f(x_0,x_1,0)$ e $g(x_0,x_1,0)$ non abbiano fattori comuni e siano p,q come nell'enunciato.

Siccome x_2 divide $pf-qg$ si ha

$$p(x_0,x_1,0)f(x_0,x_1,0)-q(x_0,x_1,0)g(x_0,x_1,0)=0$$

e per la fattorizzazione unica in $\mathbb{K}[x_0,x_1,x_2]$ esiste $r\in S_{d-a-b}$ tale che

$$p(x_0,x_1,0)=g(x_0,x_1,0)r(x_0,x_1,0),\qquad q(x_0,x_1,0)=f(x_0,x_1,0)r(x_0,x_1,0)\,. \tag{2.5}$$

I due polinomi omogenei $p-gr$ e $q-fr$ sono entrambi divisibili per x_2, ossia esistono $h\in S_{d-a-1}$ e $k\in S_{d-b-1}$ tali che $x_2h=p-gr$ e $x_2k=q-fr$. Ma allora

$$x_2hf-x_2kg=(p-gr)f-(q-fr)g=pf-qg=x_2l_2\cdots l_d$$

da cui segue $hf-kg=l_2\cdots l_d$, in contraddizione con la minimalità di d. □

Osservazione 2.4.5. Nella situazione del Lemma 2.4.4, le rette $V(l_i)$ non sono univocamente determinate da f,g, anche nel caso in cui l'intero d è il minimo possibile.

Il caso limite è quando f,g hanno entrambi grado 1 ed al variare di $(p,q)\in\mathbb{K}^2-\{0\}$ le rette $V(pf-qg)$ sono tutte e sole le rette passanti per il punto $f(x)=g(x)=0$.

Come ulteriore esempio si considerino i polinomi di secondo grado $f=x_0x_1$, $g=x_2(x_0+x_1+x_2)$. Allora, oltre alle ovvie scomposizioni in fattori lineari $1f+0g=x_0x_1$ e $0f+1g=x_2(x_0+x_1+x_2)$ si ha:

$$f+g=(x_0+x_2)(x_1+x_2)\,.$$

Lemma 2.4.6. *Siano $X\subset\mathbb{P}^2$ e d un intero positivo. Se per ogni punto $q\in\mathbb{P}^2$ l'insieme X è contenuto nell'unione di d rette passanti per q, allora X contiene al più d punti distinti.*

Dimostrazione. Supponiamo per assurdo che esistano $p_0,\dots,p_d\in X$ punti distinti; siccome il campo $\mathbb{K}$ è infinito possiamo trovare un punto $p\in\mathbb{P}^2$ non appartenente all'unione delle $d(d+1)/2$ rette $\overline{p_ip_j}$, $0\le i<j\le d$. Dunque per ogni $i\neq j$ i tre punti q,p_i,p_j non sono allineati, ogni retta per q contiene al più un punto p_i e quindi X non è contenuto in d rette passanti per q. □

Teorema 2.4.7 (Bézout debole). *Siano $f,g\in\mathbb{K}[x_0,x_1,x_2]$ polinomi omogenei senza fattori comuni di gradi $a,b>0$. Allora l'intersezione $f(x)=g(x)=0$ delle corrispondenti ipersuperfici proiettive è non vuota e contiene al più ab punti distinti.*

Dimostrazione. Abbiamo già dimostrato che $V(f)\cap V(g)\neq\emptyset$. Per il lemma precedente basta dimostrare che per ogni punto $q\in\mathbb{P}^2$, l'intersezione è contenuta nell'unione di ab rette passanti per q. A meno di un cambio di coordinate omogenee possiamo supporre $q=[1,0,0]$ e per il Lemma 2.4.3 esistono due polinomi omogenei h,k tali che $hf+kg$ è un polinomio omogeneo non nullo di grado ab in x_1,x_2. Dunque

$$0\neq hf+kg=\prod_{i=1}^{ab}(a_ix_1+b_ix_2)$$

per opportune costanti $a_i,b_i\in\mathbb{K}$ e $V(f)\cap V(g)$ è contenuto nell'unione delle rette di equazione $a_ix_1+b_ix_2=0$, $i=1,\dots,ab$. □

Esempio 2.4.8. Su $\mathbb{K}=\mathbb{C}$, per ogni $n>0$ consideriamo i tre di polinomi omogenei di grado n:

$$f_n=\prod_{i=1}^{n}(x_0-ix_1),\quad g_n=\prod_{j=1}^{n}(x_2-jx_1),\quad h_n=\prod_{i=1}^{n}(x_0+ix_1)\,.$$

Allora per ogni $a, b > 0$ l'intersezione $V(f_a) \cap V(h_b)$ contiene solo il punto $[0, 0, 1]$, mentre $V(f_a) \cap V(g_b)$ è formata dagli ab punti distinti $[i, 1, j]$, $i = 1, \ldots, a$, $j = 1, \ldots, b$.

COROLLARIO 2.4.9. *Sia f polinomio omogeneo di grado n e sia $L \subset \mathbb{P}^2$ una retta. Se $L \cap V(f)$ contiene almeno $n+1$ punti distinti, allora l'equazione di L divide f.*

DIMOSTRAZIONE. L'equazione di L è un polinomio omogeneo l di grado 1. Se l non divide f, siccome l è irriducibile, i polinomi l, f non hanno fattori comuni. Per il teorema di Bézout 2.4.7 l'intersezione $L \cap V(f)$ contiene al più n punti distinti. □

Possiamo accomunare e riscrivere in modo "geometrico" il Lemma 2.4.4 ed il Teorema 2.4.7.

TEOREMA 2.4.10. *Siano C e D due curve algebriche di gradi a e b rispettivamente. Allora:*

(1) *$C \cap D \neq \emptyset$.*
(2) *Se $C \cap D$ contiene più di ab punti, allora C e D hanno una componente irriducibile in comune.*

COROLLARIO 2.4.11. *Due curve irriducibili distinte di gradi a, b hanno al più ab punti in comune.*

DIMOSTRAZIONE. Immediata. □

Sia $f(x_0, x_1, x_2) = 0$ l'equazione di una curva C e sia $p = [v_0, v_1, v_2] \in \mathbb{P}^2$. Diremo che p è un **punto singolare** di C se

$$f(v_0, v_1, v_2) = 0 \quad \text{e} \quad \frac{\partial f}{\partial x_i}(v_0, v_1, v_2) = 0 \quad \text{per ogni } i = 0, 1, 2.$$

Si noti che:

1) La definizione di punto singolare è una buona definizione: infatti essendo f omogeneo, anche le sue derivate parziali sono omogenee. Inoltre se y_0, y_1, y_2 è un diverso sistema di coordinate e g è un'equazione di C nelle coordinate y_i, allora si ha $g(y) = af(x)$ per qualche $a \in \mathbb{K}$ e quindi

$$\frac{\partial g}{\partial y_i} = a \sum_{j=0}^{2} \frac{\partial g}{\partial x_j} \frac{\partial x_j}{\partial y_i}$$

2) Se il campo $\mathbb{K}$ ha caratteristica 0, e più in generale se la caratteristica del campo non divide il grado di f, allora dalla formula di Eulero segue che un punto p è singolare per la curva di equazione f se e solo se p annulla tutte le derivate parziali di f.

3) Se C è irriducibile di grado n e di equazione $f(x) = 0$ allora, essendo $\mathbb{K}$ algebricamente chiuso, per il Lemma 2.2.6 esiste una derivata parziale di $\frac{\partial f}{\partial x_i}$ non nulla. Il Teorema Teorema 2.4.10 applicato alle curve C e $V(\frac{\partial f}{\partial x_i})$ implica che C ha al più $n(n-1)$ punti singolari.[1]

I punti di una curva che non sono singolari si dicono **lisci**. Una curva **singolare** è una curva che contiene almeno un punto singolare. Una curva che non ha punti singolari si dice **non singolare** oppure **liscia**.

ESEMPIO 2.4.12. Sul campo dei numeri complessi consideriamo la curva C di equazione $f(x_0, x_1, x_2) = x_0^3 + ax_1^3 + bx_2^3 = 0$, $a, b \in \mathbb{C}$. Allora C è singolare se e solo se $ab = 0$. Infatti

$$\frac{\partial f}{\partial x_0} = 3x_0^2, \qquad \frac{\partial f}{\partial x_1} = 3ax_1^2, \qquad \frac{\partial f}{\partial x_2} = 3bx_2^2\,.$$

Se $a = 0$ allora $[0, 1, 0]$ è un punto singolare, se $b = 0$ allora $[0, 0, 1]$ è un punto singolare. Se $a, b \neq 0$ allora non esistono punti di $\mathbb{P}^2$ che annullano tutte e tre le derivate.

PROPOSIZIONE 2.4.13. *Siano $C_1, \ldots, C_r$ curve algebriche (non necessariamente irriducibili e/o distinte) e sia $C = C_1 + \cdots + C_r$. Allora:*

[1] In realtà una curva irriducibile di grado n ha al più $(n-1)(n-2)/2$ punti singolari, ma la dimostrazione di questo fatto richiede alcune tecniche leggermente più sofisticate che non sono trattate in queste note, cf. [1].

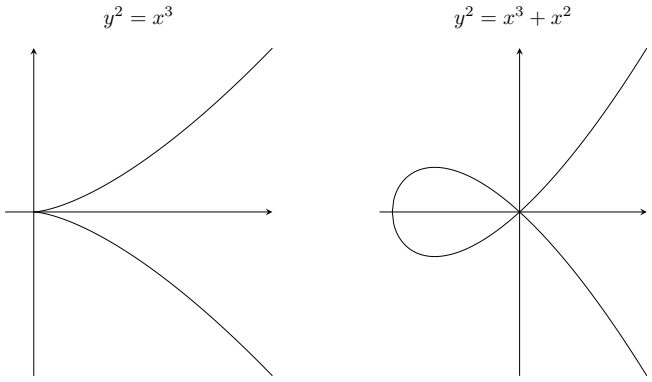


FIGURA 1. Due esempi di cubiche irriducibili singolari

(1) *Se $p \in C_i \cap C_j$ per qualche $i \neq j$, allora p è un punto singolare di C. In particolare ogni curva liscia è irriducibile.*
(2) *Se $p \in C_i$ e $p \notin C_j$ per ogni $j \neq i$, allora p è un punto singolare di C se e solo se è un punto singolare di C_i.*
(3) *Una curva è ridotta se e solo se possiede un numero finito di punti singolari.*

DIMOSTRAZIONE. Sia f_i un'equazione della curva C_i, allora $f = f_1 \cdots f_r$ è un'equazione per C. Se $p \in C_i \cap C_j$, con $i \neq j$, allora $f_i(p) = f_j(p) = 0$ e per la regola di Leibniz ogni derivata parziale di f si annulla in p; questo prova 1). Se la curva C non è irriducibile, allora si può scrivere $C = C_1 + C_2$ ed abbiamo già dimostrato che $C_1 \cap C_2 \neq \emptyset$.

Se invece $f_i(p) = 0$ e $f_j(p) \neq 0$ per ogni $j \neq i$, allora la regola di Leibniz implica che, per ogni $h = 0, 1, 2$ vale $\dfrac{\partial f}{\partial x_h}(p) = 0$ se e solo se $\dfrac{\partial f_i}{\partial x_h}(p) = 0$, e questo prove il punto 2).

Siccome una curva $C = C_1 + \cdots + C_r$, con le C_i irriducibili, è ridotta se e solo se le C_i sono distinte, il punto 3) segue dai punti precedenti e dal fatto che ogni curva irriducibile possiede un numero finito di punti singolari. □

Dunque ogni curva piana liscia è irriducibile, mentre il viceversa è falso. Ad esempio sono irriducibili e singolari nel punto $[1, 0, 0]$ tutte le cubiche di equazione

$$x_0 x_2^2 = x_1^3 + \lambda x_0 x_1^2 , \qquad \lambda \in \mathbb{K} .$$

Osserviamo che a meno di proiettività la precedente famiglia di cubiche si riduce all'insieme delle due di equazioni $x_0 x_2^2 = x_1^3$ e $x_0 x_2^2 = x_1^3 + x_0 x_1^2$. Infatti se $\lambda \neq 0$ e $\xi \in \mathbb{K}$ è una radice quadrata di λ, la proiettività

$$[x_0, x_1, x_2] \mapsto [\xi x_0, \xi^3 x_1, \xi^4 x_2]$$

trasforma la cubica di equazione $x_0 x_2^2 = x_1^3 + \lambda x_0 x_1^2$ in quella di equazione $x_0 x_2^2 = x_1^3 + x_0 x_1^2$.

ESEMPIO 2.4.14. Al variare dei parametri $p, q \in \mathbb{K}$, si consideri le cubica $C \subset \mathbb{P}^2$ di equazione

$$x_0 x_2^2 = x_1^3 + p x_0^2 x_1 + q x_0^3,$$

che nelle coordinate affini $x = x_1/x_0$ e $y = x_2/x_0$ diventa

$$y^2 = x^3 + px + q, \qquad p, q \in \mathbb{K} .$$

Definiamo il suo *discriminante* come $\Delta = 4p^3 + 27q^2$. Se il campo ha caratteristica diversa da 2, allora C è singolare se e solo se $\Delta = 0$.

Per definizione i punti singolari di C sono le soluzioni in $\mathbb{P}^2$ del sistema di equazioni omogeneee

$$\begin{cases} x_0x_2^2 = x_1^3 + px_0^2x_1 + qx_0^3 \\ x_2^2 = 2px_0x_1 + 3qx_0^2 \\ 0 = 3x_1^2 + px_0^2 \\ 2x_0x_2 = 0 \end{cases}$$

Osserviamo preliminarmente che non esistono punti singolari sulla retta di equazione $x_0 = 0$. Infatti se $x_0 = 0$ dalla prima equazione segue $x_1^3 = 0$ e dalla seconda $x_2^2 = 0$, da cui $x_0 = x_1 = x_2 = 0$ che non definisce alcun punto del piano proiettivo. Quindi ogni eventuale punto singolare sarà del tipo $[1, x, y]$ con $x, y \in \mathbb{K}$ soluzioni del sistema di equazioni

$$\begin{cases} y^2 = x^3 + px + q \\ y^2 = 2px + 3q \\ 0 = 3x^2 + p \\ 2y = 0 \end{cases}$$

Si noti che in caratteristica 2 tale sistema ammette l'unica soluzione $x = \sqrt{p}$, $y = \sqrt{q}$, mentre in caratteristica $\neq 2$ segue dall'ultima equazione che $y = 0$ e $x \in \mathbb{K}$ è una soluzione del sistema

$$\begin{cases} 0 = x^3 + px + q \\ 0 = 2px + 3q \\ 0 = 3x^2 + p \end{cases}$$

Consideriamo separatamente i due casi $p = 0$ e $p \neq 0$. Se $p = 0$ si ha $\Delta = -27q^2$, $q\Delta = (-3q)^3$ e quindi $\Delta = 0$ se e solo se $3q = 0$. Il sistema di equazioni diventa

$$0 = x^3 + q = 3q = 3x^2$$

che ammette soluzioni se e solo se $3q = 0$: infatti se $3q = 0$ e x è una soluzione di $x^3 + q = 0$, si ha $(3x^2)^3 = 27x^6 = 27q^2 = 0$.

Se $p \neq 0$, dalla seconda equazione segue $x = -\dfrac{3q}{2p}$ ed il sistema si riduce a

$$0 = -\frac{27q^3}{8p^3} - \frac{3q}{2} + q = \frac{27q^2}{4p^2} + p \iff 0 = -q(27q^2 + 4p^3) = 27q^2 + 4p^3\,.$$

Esercizi.

Esercizio 14. Provare che per ogni curva algebrica C, il supporto $\mathrm{Supp}(C)$ è un sottoinsieme proprio e infinito di $\mathbb{P}^2$.

Esercizio 15. Mostrare che in caratteristica 0, per ogni intero positivo n la curva di equazione $x_0^n + x_1^n + x_2^n = 0$ è liscia.

Esercizio 16. In caratteristica $\neq 2, 3$, determinare per quali valori del parametro $\lambda \in \mathbb{K}$ risultano singolari le cubiche di equazioni

$$x_0x_2^2 = x_1(x_1 + x_0)(x_1 + \lambda x_0), \qquad x_0^3 + x_1^3 + x_2^3 - 3\lambda x_0x_1x_2 = 0.$$

Esercizio 17. Siano $C_1, \ldots, C_r$ curve piane di gradi $n_1 \geq n_2 \geq \cdots \geq n_r$ e sia $V = C_1 \cap \cdots \cap C_r$. Dimostrare che se V è finito, allora contiene al più n_1n_r punti.

Esercizio 18. Determinare e descrivere i punti singolari (su $\mathbb{C}$) delle curve di equazioni

$$y^3(4z - y)^3 - 4x^4(x + 3z)^2 = 0, \quad (8y - x - z)^3 = 216xyz, \quad (x^2 - z^2)^2y = (y^2 - z^2)^2x.$$

2.5. Retta tangente e punti di flesso

Sia C una curva algebrica piana di grado n ed equazione $f(x) = 0$ e sia $L \subset \mathbb{P}^2$ una retta. Se L è contenuta nel supporto di C, allora L è una componente irriducibile di C; se invece L non è una componente irriducibile di C, allora presi due punti distinti $p = [p_0, p_1, p_2]$ e $q = [q_0, q_1, q_2]$ sulla retta L, il polinomio

$$F(t_0, t_1) = f(t_0 p_0 + t_1 q_0, t_0 p_1 + t_1 q_1, t_0 p_2 + t_1 q_2)$$

è non nullo ed omogeneo di grado n. Esistono dunque n punti di L, *contati con molteplicità* in cui $f = 0$: chiaramente tali punti corrispondono all'intersezione della curva C con la retta L.

Se il punto p appartiene all'intersezione $L \cap C$, il calcolo della molteplicità di intersezione di L con C in p è molto semplice. Basta infatti calcolare la molteplicità di $t = 0$ come radice del polinomio (non omogeneo)

$$F(1, t) = f(p_0 + tq_0, p_1 + tq_1, p_2 + tq_2)\,.$$

Esempio 2.5.1. Il punto $p = [0, 0, 1]$ appartiene all'intersezione della cubica C di equazione $f = x_0 x_2^2 - x_1^3 - x_0^3$ con la retta L di equazione $x_0 + x_1 = 0$. Calcoliamo la molteplicità di intersezione di L con C in p. Siccome il punto $q = [1, -1, 0] \neq p$ appartiene a L basta calcolare la molteplicità in $t = 0$ del polinomio $f(t, -t, 1)$. Dato che $f(t, -t, 1) = t$ la molteplicità è 1. Notiamo inoltre che anche $q \in L \cap C$ e dato che $f(1, -1, t) = t^2$ la molteplicità di intersezione in q è uguale a 2.

Definizione 2.5.2. Siano L una retta, C una curva e $p \in L \cap C$. Diremo che L è **tangente** a C nel punto p se la molteplicità di intersezione di L con C in p è strettamente maggiore di 1.

Diremo che L è tangente a C se lo è in qualche punto di $C \cap L$; diremo che è trasversale se non è tangente.

Notiamo che, se esiste una retta trasversale ad una curva C, allora C deve essere necessariamente ridotta.

Proposizione 2.5.3. *Siano dati una curva C di equazione f e due punti distinti $p = [p_0, p_1, p_2]$ e $q = [q_0, q_1, q_2]$, con $p \in C$. Allora la retta $L = \overline{pq}$ è tangente a C in p se e solo se*

$$\sum_{i=0}^{2} q_i \frac{\partial f}{\partial x_i}(p_0, p_1, p_2) = 0\,.$$

Dimostrazione. La retta L è tangente a C in p se e solo se $t = 0$ è una radice multipla del polinomio $g(t) = f(x_0 + ty_0, x_1 + ty_1, x_2 + ty_2)$, cioè se e solo se $g'(0) = 0$, dove g' denota la derivata di f rispetto a t. Basta adesso applicare la regola di derivazione della funzione composta. □

Corollario 2.5.4. *Sia $p = [p_0, p_0, p_1]$ un punto di una curva C di equazione f:*

1. *Se p è singolare, allora ogni retta per p è tangente a C in p.*
2. *Se p è liscio, allora esiste unica una retta tangente a C in p la cui equazione è*

$$\sum_{i=0}^{2} x_i \frac{\partial f}{\partial x_i}(p_0, p_1, p_2) = 0\,.$$

Dimostrazione. Conseguenza immediata della Proposizione 2.5.3. □

Esempio 2.5.5. Su campi di caratteristica $\neq 2$, l'equazione della retta tangente alla curva di equazione $x_0^4 - x_1^2 x_2^2 = 0$ nel punto $[1, 1, 1]$ è $4x_0 - 2x_1 - 2x_2 = 0$.

Le precedenti considerazioni forniscono un metodo per il calcolo delle rette tangenti ad una curva C passanti per un punto $q \in \mathbb{P}^2$. Se $f(x) = 0$ è l'equazione di f e $q = [q_0, q_1, q_2]$ abbiamo visto che, dato un punto $p \in C$, $p \neq q$, la retta $\overline{pq}$ è tangente a C in p se e solo se

$\sum_i q_i f_i(p) = 0$. Quindi se $q \notin C$ le rette tangenti a C passanti per q sono tutte e sole quelle del tipo $\overline{pq}$ al variare di p tra le soluzioni del sistema di due equazioni

$$f(p) = \sum_i q_i f_i(p) = 0\,. \tag{2.6}$$

Se invece $q \in C$ è un punto liscio, oltre a considerare le rette $\overline{pq}$ con $p \neq q$ che soddisfa (2.6) bisogna ovviamente aggiungere le retta tangente a C in q. Infine, se $q \in C$ è singolare, ogni retta passante per q è tangente a C.

Esempio 2.5.6. Su di un campo di caratteristica $\neq 3$, calcoliamo le rette passanti per il punto $q = [1, 0, 0]$ e tangenti alla cubica di equazione $x_0^3 + x_1^3 + x_2^3 = 0$. Per determinare i punti $p \in C$ tali che la retta $\overline{pq}$ è tangente a C nel punto p bisogna risolvere il sistema di equazioni $x_0^3 + x_1^3 + x_2^3 = 3x_0^2 = 0$ che è equivalente a $x_0 = x_1^3 + x_2^3 = 0$ le cui soluzioni in $\mathbb{P}^2$ sono

$$[0, -1, \xi], \quad [0, -1, \xi^2], \quad [0, -1, 1],$$

dove ξ è una radice cubica primitiva di 1. Le tre rette passanti per q e per i tre punti suddetti sono quelle di equazioni:

$$x_2 + \xi x_1 = 0, \quad x_2 + \xi^2 x_1 = 0, \quad x_2 + x_1 = 0,.$$

Definizione 2.5.7. Data una curva C ed un suo punto liscio p denoteremo con $\mathbb{T}_p C$ la retta tangente a C in p. Diremo che un punto liscio $p \in C$ è un **flesso**, o un **punto di flessione**, di C se la molteplicità di intersezione di $\mathbb{T}_p C$ con C nel punto p è maggiore od uguale a 3

Ad esempio, in una retta tutti i punti sono di flesso. Più in generale se la curva C è unione di rette allora ogni punto liscio di C è un flesso. Per il teorema di Bezout una conica possiede punti di flesso se e solo se è unione di rette.

Dato un polinomio omogeneo $f \in \mathbb{K}[x_0, x_1, x_2]$, per semplicità notazionale indichiamo

$$f_i = \frac{\partial f}{\partial x_i}, \qquad f_{ij} = f_{ji} = \frac{\partial^2 f}{\partial x_i \partial x_j}\,.$$

Si definisce la matrice Hessiana di f come:

$$H(x) = \begin{pmatrix} f_{00} & f_{01} & f_{02} \\ f_{10} & f_{11} & f_{12} \\ f_{20} & f_{21} & f_{22} \end{pmatrix}.$$

Se f ha grado $d \geq 2$ i coefficienti di $H(x)$ sono polinomi di grado $d-2$ ed il suo determinante $\det(H(x))$ è un polinomio omogeneo di grado $3(d-2)$.

Lemma 2.5.8. *Siano $\mathbb{K}$ un campo algebricamente chiuso e $H \in M_{3,3}(\mathbb{K})$ una matrice 3×3 simmetrica. Denotando con $\mathbb{K}^3$ lo spazio vettoriale numerico dei vettori colonna, le seguenti condizioni sono equivalenti:*

1. $\det(H) = 0$;
2. *per ogni vettore non nullo $v \in \mathbb{K}^3$ tale che $v^T H v = 0$ esiste un vettore $u \in \mathbb{K}^3$ linearmente indipendente da v tale che $u^T H v = u^T H u = 0$.*
3. *esistono due vettori linearmente indipendenti $v_1, v_2 \subset \mathbb{K}^3$ tali che $v_i^T H v_j = 0$ per ogni i, j;*

Dimostrazione. *1 implica 2.* Trattiamo separatamente i due casi $Hv = 0$ e $Hv \neq 0$. Se $Hv = 0$ completiamo v ad una base $v_1, v_2, v_3 = v$ di $\mathbb{K}^3$ e consideriamo il polimonio omogeneo di secondo grado

$$f(t_1, t_2) = (t_1 v_1 + t_2 v_2)^T H (t_1 v_1 + t_2 v_2)\,.$$

Per ipotesi il campo $\mathbb{K}$ è algebricamente chiuso e quindi esiste una coppia (t_1, t_2) non nulla tale che $f(t_1, t_2) = 0$. Allora il vettore $u = t_1 v_1 + t_2 v_2$ è quello cercato.

Se $Hv \neq 0$ è sufficiente prendere u un qualsiasi vettore non nullo tale che $Hu = 0$.

2 implica 3. Basta provare che esiste un vettore non nullo $v \in \mathbb{K}^3$ tale che $v^T H v = 0$. Questo si prova esattamente come sopra, considerando due vettori linearmente indipendenti v_1, v_2 ed il polinomio omogeneo $f(t_1, t_2) = (t_1 v_1 + t_2 v_2)^T H (t_1 v_1 + t_2 v_2)$.

3 implica 1. Supponiamo per assurdo che H sia invertibile, allora i vettori Hv_1, Hv_2 sono linearmente indipendenti e la matrice $A = (Hv_1, Hv_2) \in M_{3,2}(\mathbb{K})$ ha rango massimo. D'altra parte, il nucleo dell'applicazione lineare

$$A^T \colon \mathbb{K}^3 \to \mathbb{K}^2$$

coincide con l'insieme dei vettori u tali che $u^T H v_1 = u^T H v_2 = 0$ e quindi contiene v_1, v_2, in contraddizione con il fatto che A^T ha rango 2.

Notiamo che quest'ultima implicazione non richiede che il campo sia algebricamente chiuso. D'altra parte se $\mathbb{K} = \mathbb{R}$, la coppia

$$H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad v = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

soddisfa la condizione 1 ma non le condizioni 2 e 3. Sempre su $\mathbb{R}$, la matrice identità soddisfa la condizione 2 ma non soddisfa 3 ed 1.

□

TEOREMA 2.5.9. *Sia C una curva piana di grado d ed equazione $f(x) = 0$ e sia $h(x)$ il determinate della matrice Hessiana $H(x)$ di f. Se il campo base ha caratteristica 0 oppure ha caratteristica positiva p, con $p \geq \max(3, d)$, allora un punto liscio $p \in C$ è un flesso di C se e solo se $h(p) = 0$.*

DIMOSTRAZIONE. Il teorema è banalmente verificato per le rette, non è quindi restrittivo supporre $d \geq 2$; in tal caso le ipotesi sulla caratteristica del campo ci dicono che i numeri 2 e $d-1$ sono non nulli e quindi invertibili.

Fissiamo $v \in \mathbb{K}^3 - \{0\}$ tale che $p = [v]$. Supponiamo che la matrice $A = H(v)$ non sia invertibile, per la formula di Eulero

$$0 = d(d-1)f(v) = (d-1)\sum_i v_i f_i(v) = \sum_{i,j} v_i v_j f_{ij}(v) = v^T A v\,.$$

Per il Lemma 2.5.8 esiste un punto $q = [u] \neq p$ tale che $u^T A v = u^T A u = 0$. Proviamo che la retta $\overline{pq}$ è la retta tangente a C in p e che p è un punto di flesso, ossia che $t = 0$ è una radice di molteplicià > 2 del polinomio

$$g(t) = f(v + tu) = t\sum_i f_i(v)u_i + \frac{t^2}{2}\sum_{ij} f_{ij}(v)u_i u_j + t^3(\cdots)\,. \tag{2.7}$$

Adesso basta osservare che

$$\sum_{ij} f_{ij}(v)u_i u_j = u^T A u = 0$$

e che per la formula di Eulero

$$\sum_i f_i(v)u_i = \frac{1}{d-1}\sum_{ij} f_{ij}(v)v_j u_i = \frac{1}{d-1} v^T A u = 0\,.$$

Viceversa, supponiamo che p sia un punto di flesso e che $\overline{pq}$ sia la retta tangente a C in p, con $p \neq q = [u]$. Per (2.7) questo implica che

$$0 = (d-1)\sum_i f_i(v)u_i = \sum_{ij} f_{ij}(v)v_i u_j = v^T A u, \qquad 0 = \sum_{ij} f_{ij}(v)u_i u_j = u^T A u,$$

e per il Lemma 2.5.8 la matrice A non è invertibile.

□

COROLLARIO 2.5.10. *In un campo algebricamente chiuso di caratteristica 0 ogni curva piana liscia di grado ≥ 3 possiede punti di flesso.*

DIMOSTRAZIONE. il determinante della matrice Hessiana definisce una curva di grado $3(d-2) > 0$ che quindi interseca C. □

COROLLARIO 2.5.11. *In un campo algebricamente chiuso di caratteristica $\neq 2$ ogni curva piana liscia di grado 3 possiede punti di flesso.*

DIMOSTRAZIONE. Per le cubiche il Teorema 2.5.9 vale su campi di caratteristica $\neq 2$ e si ragiona come nel corollario precedente. □

Esercizi.

ESERCIZIO 19. Sul campo dei numeri complessi, si determini il numero di rette passanti per il punto $[1,1,0]$ e tangenti alla curva di Fermat $x_0^n + x_1^n + x_2^n = 0$.

ESERCIZIO 20. Provare che in caratteristica positiva esistono curve irriducibili C e punti $q \notin C$ tali che ogni retta passante per q è tangente a C.

2.6. Le coniche

In questa sezione assumeremo, salvo avviso contrario, che $\mathbb{K}$ sia un campo algebricamente chiuso di caratteristica diversa da 2.

Una conica è una curva algebrica piana di grado 2. Due coniche si dicono proiettivamente equivalenti se esiste una proiettività di $\mathbb{P}^2$ che trasforma l'una nell'altra. Una conica non irriducibile è unione di due rette che possono essere distinte o coincidenti. Chiameremo **rango** di una conica di equazione $f(x_0,x_1,x_2)=0$, il il rango della matrice Hessiana

$$H = \begin{pmatrix} f_{00} & f_{01} & f_{02} \\ f_{10} & f_{11} & f_{12} \\ f_{20} & f_{21} & f_{22} \end{pmatrix} \in M_{3,3}(\mathbb{K}), \qquad f_{ij} = \frac{\partial^2 f}{\partial x_i \partial x_j}.$$

Il rango di una conica non dipende dalla scelta del sistema di coordinate omogenee.

TEOREMA 2.6.1. *Due coniche sono proiettivamente equivalenti se e solo se hanno lo stesso rango. In particolare ogni conica è proiettivamente equivalente ad una delle seguenti:*

(1) $x_0^2 = 0$, *retta doppia.*
(2) $x_0 x_1 = 0$, *rette incidenti.*
(3) $x_0 x_2 = x_1^2$, *conica liscia.*

DIMOSTRAZIONE. Sia C una conica di equazione $f(x_0,x_1,x_2)$ e matrice Hessiana H. Dato un punto $p=[v_0,v_1,v_2]=[v]\in\mathbb{P}^2$ per la formula di Eulero vale

$$v^T H = (f_0(v), f_1(v), f_2(v)), \qquad 2f(v) = v^T H v,$$

e quindi p è un punto singolare di C se e solo se $v^T H = (Hv)^T = 0$.

Se il rango di H è 1, allora esiste una retta L composta di punti singolari di C e quindi deve necessariamente essere $C = 2L$. Se il rango è 2, allora esiste un unico punto singolare $p=[v]$: proviamo che C è unione di rette passanti per p, per ragioni di grado tali rette dovranno essere esattamente due. Se $q=[y]\in C$, allora per ogni $a,b\in\mathbb{K}$ vale

$$2f(av+by) = (av+by)^T H (av+by) = b^2 y^T H y = 0\,.$$

Infine se il rango è 3 la conica è liscia; siano p,q e r tre punti distinti di C e denotiamo con $o = \mathbb{T}_p C \cap \mathbb{T}_q C$ il punto di intersezione delle rette tangenti a C nei punti p e q rispettivamente. La quaterna p,q,r,o è un sistema di riferimento di $\mathbb{P}^2$, possiamo quindi supporre a meno di proiettività che

$$p=[1,0,0], \qquad q=[0,0,1], \qquad r=[1,1,1], \qquad o=[0,1,0]\,.$$

Dalla condizione $p,q\in C$ si deduce che $f_{00}=f_{22}=0$. Le equazioni di $\mathbb{T}_p C = \overline{op}$ e $\mathbb{T}_q C = \overline{oq}$ sono rispettivamente $x_2=0$ e $x_0=0$; si deduce quindi che $f_{01}=f_{12}=0$ e si ha $f = ax_0x_2 - bx_1^2$. La condizione $r\in C$ impone infine che $a=b$. □

La dimostrazione appena terminata è costruttiva e fornisce un metodo effettivo per il calcolo della proiettività che trasforma una conica nella sua forma canonica. Tale calcolo richiede la soluzione di una equazione di secondo grado ed alcuni sistemi di equazioni lineari.

COROLLARIO 2.6.2. *Siano p,q,r tre punti distinti di una conica irriducibile C. Allora esiste un sistema di coordinate omogenee x_0,x_1,x_2 tale che $p=[1,0,0]$, $q=[0,0,1]$, $r=[1,1,1]$ e l'equazione di C è $x_0x_2 = x_1^2$.*

DIMOSTRAZIONE. Basta osservare che, nella dimostrazione del Teorema 2.6.1, la scelta dei punti p,q e r è arbitraria. □

TEOREMA 2.6.3 (Steiner, 1832). *Siano p e q due punti di una conica liscia C e denotiamo con F_p e F_q i fasci di rette passanti per p e q rispettivamente. Allora l'applicazione $F_p \to F_q$ definita da $F_p \ni L \mapsto \overline{qs}$, dove s è il punto di intersezione di L con C diverso da p, è una proiettività.*

DIMOSTRAZIONE. Per il Corollario 2.6.2 possiamo supporre che C sia la conica di equazione $x_0x_2 = x_1^2$ e che $p = [1, 0, 0]$, $q = [0, 0, 1]$.

Si consideri adesso l'applicazione $v\colon \mathbb{P}^1 \to C$ descritta in coordinate omogenee da $v([t_0, t_1]) = [t_0^2, t_0t_1, t_1^2]$; si vede facilmente che v è biiettiva.

Dato un punto $[a, b] \in \mathbb{P}^1$, la retta di $\mathbb{P}^2$ di equazione $bx_1 - ax_2$ interseca C nei punti $p = [1, 0, 0]$ e $v([a, b]) = [a^2, ab, b^2]$, mentre la retta di equazione $ax_1 - bx_0$ interseca C nei punti $q = [0, 0, 1]$ e $v([a, b]) = [a^2, ab, b^2]$.

L'applicazione $[a, b] \mapsto ax_1 - bx_2$ è una proiettività tra $\mathbb{P}^1$ ed il fascio di rette passanti per p; similmente l'applicazione $[a, b] \mapsto ax_1 - bx_0$ è una proiettività tra $\mathbb{P}^1$ ed il fascio di rette passanti per il punto $q = [0, 0, 1]$. L'applicazione descritta nel teorema è la composizione della seconda proiettività con l'inversa della prima. □

Il Teorema di Steiner 2.6.3 permette di definire sulla conica liscia C una struttura di retta proiettiva mediante l'applicazione v introdotta nella dimostrazione. In particolare è ben definito il birapporto di una quaterna ordinata di punti su C: basta fissare un punto $p \in C$ e considerare il birapporto delle 4 rette passanti per p ed i punti della quaterna.

Esercizi.

ESERCIZIO 21. Provare che il Corollario 2.6.2 è vero anche in caratteristica 2.

ESERCIZIO 22. Trovare le componenti irriducibili della conica di equazione

$$3x_0^2 + 5x_0x_1 + 2x_0x_2 + 2x_1^2 + x_1x_2 - x_2^2 = 0.$$

2.7. Sistemi lineari

Abbiamo già osservato che le curve piane di grado n sono in corrispondenza biunivoca con il proiettivizzato $\mathbb{P}(S_n)$ dello spazio vettoriale $S_n \subset \mathbb{K}[x_0, x_1, x_2]$ dei polinomi omogenei di grado n. Abbiamo già visto che S_n ha dimensione $\binom{n+2}{2}$ e quindi, prendendo i monomi come base canonica di S_n si ottiene un isomorfismo di spazi proiettivi

$$\mathbb{P}(S_n) \simeq \mathbb{P}^N, \qquad N = \binom{n+2}{2} - 1 = \frac{n(n+3)}{2}.$$

Alla curva di equazione $\sum_{ijk} a_{ijk}x_0^i x_1^j x_2^k = 0$ corrisponde il punto di $\mathbb{P}^N$ di coordinate omogenee $[a_{ijk}]$.

DEFINIZIONE 2.7.1. Un sottospazio proiettivo di $\mathbb{P}(S_n)$ si dice un **sistema lineare** di curve di grado n. Lo stesso spazio $\mathbb{P}(S_n)$ è un sistema lineare che viene detto **completo**.

Se $D_0, \dots, D_r$ sono curve di grado n denotiamo con $\langle D_0, \dots, D_r\rangle \subset \mathbb{P}(S_n)$ il sistema lineare da esse generato: se $f_i \in S_n$ è l'equazione di D_i, allora le curve del sistema lineare $\langle D_0, \dots, D_r\rangle$ sono esattamente quelle di equazione

$$a_0f_0(x) + \cdots + a_rf_r(x) = 0$$

dove $a_0, \dots, a_r \in \mathbb{K}$ sono coefficienti tali che il polinomio $a_0f_0 + \cdots + a_rf_r$ sia non nullo.

Se V è un sistema lineare, indicheremo con $\dim V$ la sua dimensione. Ad esempio se D_0, D_1 sono curve distinte, allora $\dim\langle D_0\rangle = \dim\langle D_1\rangle = 0$, $\dim\langle D_0, D_1\rangle = 1$: un sistema lineare di dimensione 1 si dice un **fascio** od anche **pennello**[2] o **schiera**.

[2]In inglese **pencil**, in francese **pinceau**.

ESEMPIO 2.7.2. Se $V \subset \mathbb{P}(S_n)$ è un sistema lineare di curve di grado n e C è una curva di grado m, allora l'insieme

$$W = \{C + D \mid D \in V\} \subset \mathbb{P}(S_{n+m})$$

è un sistema lineare della stessa dimensione di V. Infatti se $V = \mathbb{P}(H)$ con $H \subset S_n$ e $F \in S_m$ è una equazione di C, allora $W = \mathbb{P}(K)$, dove K è l'immagine dell'applicazione lineare iniettiva

$$S_n \to S_{n+m}, \qquad G \mapsto FG.$$

Sia V un sistema lineare di curve, un punto $p \in \mathbb{P}^2$ si dice un **punto base** di V se per ogni curva $D \in V$ vale $p \in D$. Se V è un sistema lineare di dimensione r e $f_0, \dots, f_r$ sono equazioni di un insieme di curve indipendenti di V, allora le curve di V sono tutte e sole quelle di equazione $\sum \lambda_i f_i$ e quindi i punti base di V sono quelli determinati dal sistema di equazioni

$$f_0(x) = \cdots = f_r(x) = 0\,.$$

L'equazione di un iperpiano in $\mathbb{P}(S_n)$ si dice una **condizione lineare** sulle curve di grado n.

ESEMPIO 2.7.3. Sia $p \in \mathbb{P}^2$ un punto fissato. La relazione $p \in D$, con D curva di grado n, viene detta **condizione di passaggio per** p **su** $\mathbb{P}(S_n)$. Essa impone una condizione lineare sul sistema lineare completo: infatti se $p = [v_0, v_1, v_2]$, allora una curva di equazione $\sum a_{ijk} x_0^i x_1^j x_2^k$ contiene p se e solo se vale $\sum a_{ijk} v_0^i v_1^j v_2^k = 0$ e quest'ultima condizione è esattamente l'equazione, nelle coordinate omogenee $\{a_{ijk}\}$, di un iperpiano in $\mathbb{P}(S_n)$.

Più in generale, sia $\mathcal{P}$ una proprietà definita sulle curve di grado n e $V \subset \mathbb{P}(S_n)$ un sistema lineare; diremo che $\mathcal{P}$ impone r condizioni lineari su V se l'insieme delle $D \in V$ che soddisfano $\mathcal{P}$ è un sottospazio proiettivo di V di codimensione r. Ad esempio la condizione di passaggio per un punto p (il termine passaggio nasce dal fatto di pensare intuitivamente un sistema lineare come una curva che si muove in $\mathbb{P}^2$) induce una condizione lineare su un sistema V se e solo se p non è un punto base di V.

LEMMA 2.7.4. *Sia V un sistema lineare di curve e siano $p_1, \dots, p_s$ punti di $\mathbb{P}^2$. Allora il passaggio per $p_1, \dots, p_s$ induce r condizioni lineari su V, con $0 \le r \le s$.*

In altri termini, l'insieme W delle curve $D \in V$ tali che $p_1, \dots, p_s \in D$ è un sistema lineare di dimensione $\dim W \ge \dim V - s$.

DIMOSTRAZIONE. Sia n il grado delle curve del sistema lineare V. Abbiamo visto che per ogni $i = 1, \dots, s$ l'insieme $W_i = \{D \in \mathbb{P}(S_n) \mid p_i \in D\}$ è un iperpiano e quindi

$$W = V \cap W_1 \cap \cdots \cap W_s$$

è un sottospazio proiettivo. La formula $\dim W \ge \dim V - s$ segue immediatamente dalla formula di Grassmann. □

DEFINIZIONE 2.7.5. Diremo che un insieme di punti $p_1, \dots, p_s$ induce **condizioni di passaggio indipendenti** su un sistema lineare V di curve se il passaggio per $p_1, \dots, p_s$ induce s condizioni lineari su V.

Ricordiamo che l'insieme vuoto, quando considerato come spazio proiettivo, ossia $\emptyset = \mathbb{P}(0)$ ha dimensione -1. Per il Lemma 2.7.4, affinché s punti inducano condizioni di passaggio indipendenti su un sistema lineare V è necessario che $s \le \dim V + 1$.

LEMMA 2.7.6. *Sia V un sistema lineare di curve e siano $p_1, \dots, p_s$ punti di $\mathbb{P}^2$. Allora $p_1, \dots, p_s$ inducono condizioni di passaggio indipendenti su V se e solo se per ogni $i = 1, \dots, s$ esiste una curva $D_i \in V$ tale che*

$$p_i \notin D_i, \qquad p_j \in D_i \quad \textit{per ogni } j < i\,.$$

DIMOSTRAZIONE. Sia n il grado delle curve del sistema lineare V e per ogni $i = 1, \dots, s$ consideriamo l'iperpiano $W_i = \{D \in \mathbb{P}(S_n) \mid p_i \in D\}$. Per la formula di Grassmann si ha che $\dim(V \cap W_1 \cap \cdots \cap W_s) = \dim V - s$ se e solo se per ogni indice $i = 1, \dots, s$ vale

$$V \cap W_1 \cap \cdots \cap W_i \neq V \cap W_1 \cap \cdots \cap W_{i-1}$$

Gli elementi di $V \cap W_1 \cap \cdots \cap W_{i-1} - V \cap W_1 \cap \cdots \cap W_i$ sono esattamente le curve D del sistema lineare tali che $p_i \notin D_i$ e $p_j \in D_i$ per ogni $j < i$. □

È utile osservare che se $p_1, \ldots, p_s$ inducono condizioni di passaggio indipendenti su V lo stesso vale per ogni sottoinsieme di $p_1, \ldots, p_s$.

Una conseguenza immediata del Lemma 2.7.6 è il seguente corollario, che sebbene più debole ha il vantaggio di essere invariante per permutazione dei punti.

COROLLARIO 2.7.7. *Sia V un sistema lineare di curve e siano $p_1, \ldots, p_s$ punti di $\mathbb{P}^2$. Allora $p_1, \ldots, p_s$ inducono condizioni di passaggio indipendenti su V se e solo se per ogni $i = 1, \ldots, s$ esiste una curva $D_i \in V$ tale che*

$$p_i \notin D_i, \qquad p_j \in D_i \quad \textit{per ogni } j \neq i\,.$$

ESEMPIO 2.7.8. Un punto p induce una condizione di passaggio indipendente, ossia non nulla, su un sistema lineare se e solo se p non è un punto base del sistema lineare. In particolare se V è un fascio di curve e p non è un punto base, allora esiste ed è unica una curva $C \in V$ tale che $p \in C$.

ESEMPIO 2.7.9. Tre punti inducono condizioni indipendenti sulle rette, ossia sul sistema lineare completo delle curve di grado 1, se e solo se non sono allineati.

ESEMPIO 2.7.10. Se $k \leq n+1$ allora k punti distinti inducono condizioni di passaggio indipendenti sul sistema lineare completo delle curve di grado n. Per dimostrare questo fatto non è restrittivo supporre $k = n+1$; siano $p_0, \ldots, p_n \in \mathbb{P}^2$ punti distinti e scegliamo un punto q non appartenente all'unione delle rette $\overline{p_i p_j}$. Allora le curve $D_i = \sum_{j \neq i} \overline{q p_j}$ soddisfano le condizioni del Lemma 2.7.6.

ESEMPIO 2.7.11. Quattro punti distinti inducono condizioni di passaggio indipendenti sulle coniche, ossia sul sistema lineare completo delle curve di grado 2, se e solo se non sono allineati.

Ricordiamo che il sistema lineare completo delle coniche ha dimensione 5. Se i quattro punti appartengono ad una retta L, le coniche del tipo $L + M$, con M retta, formano un sistema lineare di dimensione 2 che passa per i quattro punti, i quali pertanto non inducono condizioni di passaggio indipendenti.

Viceversa, dati 4 punti non allineati, per ciascuno di essi, chiamiamolo p, esiste una conica C che non contiene p e contiene gli altri tre, che chiameremo r, s, t. Infatti p può appartenere al massimo ad una delle tre rette $\overline{rs}, \overline{st}, \overline{rt}$. Se, per fissare le idee, $p \notin \overline{rs} \cup \overline{st}$, allora $C = \overline{rs} + \overline{st}$ è la conica cercata.

ESEMPIO 2.7.12. Cinque punti distinti inducono condizioni di passaggio indipendenti sulle coniche se e solo se non ve ne sono quattro allineati.

Abbiamo già visto che 4 punti allineati inducono condizioni dipendenti sulle coniche; a maggior ragione 5 punti di cui 4 allineati inducono condizioni di passaggio dipendenti.

Viceversa se 5 punti inducono condizioni dipendenti, esistono almeno due coniche distinte C_1, C_2 che li contengono. Per Bézout le due coniche devono avere una retta L in comune, ossia $C_1 = L + M_1$ e $C_2 = L + M_2$ con M_1, M_2 rette distinte. Siccome M_1, M_2 hanno un solo punto in comune, almeno 4 dei 5 punti devono appartenere alla retta L.

ESEMPIO 2.7.13. Siano dati 8 punti distinti $p_1, \ldots, p_8$ contenuti nell'unione di tre rette L_1, L_2, L_3 e tali che ciascuna retta L_i contenga al più 3 punti p_j. Allora $p_1, \ldots, p_8$ inducono condizioni di passaggio indipendenti sulle cubiche.

Per simmetria basta dimostrare che esiste una cubica C che contiene $p_2, \ldots, p_8$ ma non contiene p_1. Osserviamo che $p_1 \notin L_1 \cap L_2 \cap L_3$, altrimenti ciascuna retta L_i potrebbe contenere al più due dei rimanenti punti $p_2, \ldots, p_8$ e quindi i punti sarebbero al massimo 7.

Dunque, a meno di permutazioni degli indici delle rette si ha uno dei seguenti due casi:

(1) $p_1 \in L_1 \cap L_2$, $p_1 \notin L_3$;
(2) $p_1 \in L_1$, $p_1 \notin L_2 \cup L_3$.

Nel primo caso l'unione $L_1 \cup L_2$ contiene esattamente 5 punti p_i e la retta L_3 i rimanenti 3; nel secondo caso l'unione $L_2 \cup L_3$ contiene almeno 5 punti p_i ed a meno di scambiare L_2 con L_3 si ha che L_3 contiene 3 punti p_i.

A meno di permutazioni degli indici possiamo quindi supporre che $p_1 \notin L_3$ e $p_6, p_7, p_8 \in L_3$.

Ma adesso tra i 5 punti $p_1, \dots, p_5$ non ve ne sono 4 allineati e per l'esempio precedente esiste una conica Q tale che $p_1 \notin Q$ e $p_2, \dots, p_4 \in Q$. Basta allora considerare la cubica $C = L_3 + Q$.

Prima di proseguire con lo studio dell'indipendenza delle condizioni di passaggio vediamo alcune interessanti applicazioni dei sistemi lineari.

TEOREMA 2.7.14 (Gergonne, 1827). *Siano C e D due curve piane di grado n che si intersecano in esattamente n^2 punti distinti. Se nm di questi punti appartengono ad una curva E di grado $m \leq n$, allora i restanti $n(n-m)$ punti appartengono ad una curva H di grado $n-m$.*

DIMOSTRAZIONE. Siano $p_1, \dots, p_{n^2}$ i punti di intersezione di C e D, dal teorema di Bézout segue che necessariamente C, D, E sono curve ridotte.

Infatti C e D non hanno componenti in comune e se $C = \sum a_i C_i$ con le C_i irriducibili, allora $C \cap D = \cup_i C_i \cap D$,

$$n^2 = n(\sum a_i \deg(C_i)) = |C \cap D| \leq \sum |C_i \cap D| \leq \sum n \deg(C_i)$$

e questo prova che $a_i = 1$ per ogni i, ossia che C è ridotta. Per simmetria anche D è una curva ridotta.

Per mostrare che anche E è ridotta, scriviamo $E = \sum a_i E_i$; allora con E_i irriducibile per ogni i. Siccome C, D non hanno componenti in comune si ha $E_1 \not\subset C$ oppure $E_1 \not\subset D$; supponiamo per fissare le idee che $E_1 \not\subset C$, allora

$$|E_1 \cap C \cap D| \leq |E_1 \cap C| \leq n \deg(E_1).$$

Similmente $|E_i \cap C \cap D| \leq n \deg(E_i)$ per ogni i e quindi

$$nm = |E \cap C \cap D| \leq \sum_i |E_i \cap C \cap D| \leq \sum_i n \deg(E_i) \leq \sum_i n a_i \deg(E_i) = nm.$$

Dunque $\sum_i n \deg(E_i) = \sum_i n a_i \deg(E_i)$ da cui segue $a_i = 1$ per ogni i; dalla condizione $|E \cap C \cap D| = \sum_i |E_i \cap C \cap D|$ segue che $|E_i \cap E_j \cap C \cap D| = \emptyset$ per ogni $i \neq j$. Infine, dalla condizione $|E_i \cap C \cap D| \leq n \deg(E_i)$ segue che $E_i \cap C \cap D$ contiene esattamente $n \deg(E_i)$ punti.

Siano C_t, con $t \in \mathbb{P}^1$, le curve del fascio V generato da C e D; notiamo che i punti base del fascio generato da C, D sono esattamente $C \cap D$. Sia $E = E_1 + \cdots + E_r$ la decomposizione in componenti irriducibili e denotiamo con m_i il grado di E_i. Siccome $E_i \cap D \cap D \subset E_i \cap C_t$ per ogni t, dal teorema di Bezout segue che per ogni $t \in \mathbb{P}^1$ vale una, ed una soltanto delle seguenti alternative:

(1) $E_i \cap C_t = E_i \cap C \cap D$;
(2) E_i è una componente di C_t.

Per ogni $i = 1, \dots, m$, sia $q_i \in E_i - (C \cap D)$ un punto fissato, allora esiste un unico $t_i \in \mathbb{P}^1$ tale che $q_i \in C_{t_i}$; quindi E_i è una componente di C_{t_i}. Osserviamo che se $q = q_i = q_j \in E_i \cap E_j$, con $i \neq j$, allora q non appartiene ai punti base di V, ragionando come sopra ne segue che $t_i = t_j = t$ per ogni i, j. Dunque E è contenuta in una curva C_t del fascio, basta quindi prendere $H = C_t - E$. □

COROLLARIO 2.7.15. (Teorema di Pappo-Pascal, III sec d.C.-1640) *Le coppie di lati opposti di un esagono inscritto in una conica ridotta si intersecano in punti allineati.*

DIMOSTRAZIONE. (Plücker, 1828) Siano $L_1, L_2, \dots, L_6$ i lati successivi di un esagono inscritto in una conica E. In virtù del teorema di Gergonne 2.7.14, basta osservare che le due cubiche $C = L_1 + L_3 + L_5$ e $D = L_2 + L_4 + L_6$ si intersecano in 9 punti e 6 di questi appartengono a E. □

È facile dimostrare che ogni fascio di coniche contiene almeno una conica riducibile. Infatti siano C_1, C_2 coniche di equazioni f_1, f_2 e matrici Hessiane H_1, H_2 rispettivamente. Sappiamo che la conica di equazione $af_0 + bf_1$ è riducibile se e solo se (a, b) è una radice

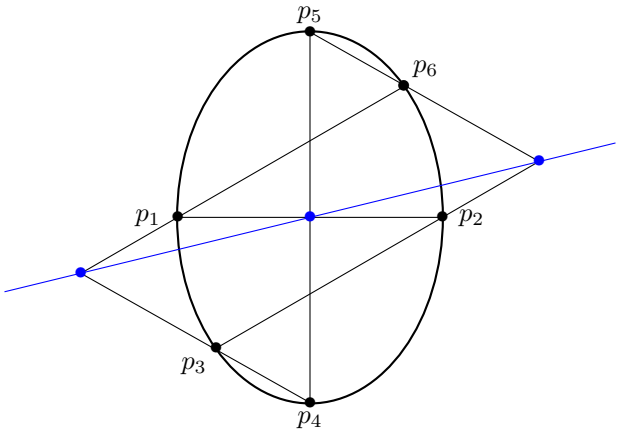


FIGURA 2. Il teorema di Pascal

del polinomio omogeneo $p(t_1, t_2) = \det(t_1 H_1 + t_2 H_2)$. Se vogliamo determinare i punti di intersezione di due coniche C_1, C_2 si può procedere nel modo seguente.

Se C_2 è riducibile, si determinano le sue componenti (sono due rette) e per ciascuna di esse si calcola l'intersezione con C_1: il procedimento richiede la soluzione di alcune equazioni di secondo grado. Se invece C_2 è irriducibile si determina (risolvendo un'equazione di terzo grado) una conica riducibile $C_0 \neq C_2$ appartenente al fascio generato da C_1 e C_2 e quindi ricondursi al caso precedente osservando che $C_1 \cap C_2 = C_0 \cap C_2$.

LEMMA 2.7.16. *Sia X un insieme finito con $2d$ elementi e sia $\sim$ una relazione di equivalenza su X tale che ciascuna classe di equivalenza contenga al più d elementi. Allora possiamo scrivere $X = \{a_1, b_1, \ldots, a_d, b_d\}$ con $a_i \not\sim b_i$ per ogni $i = 1, \ldots, d$.*

DIMOSTRAZIONE. Induzione su d, essendo il risultato evidente per $d = 1$. Sia dunque $d > 1$ e scriviamo X come unione disgiunta delle sue classi di equivalenza, ordinate per cardinalità decrescente.

$$X = S_1 \cup S_2 \cup \cdots , \qquad d \geq |S_1| \geq |S_2| \geq \cdots .$$

Siccome S_1, S_2 non sono vuote e $d-1 \geq |S_3|$ possiamo scegliere $a_1 \in S_1$, $b_1 \in S_2$ ed applicare l'ipotesi induttiva all'insieme $Y = X - \{a_1, b_1\}$. □

LEMMA 2.7.17. *Siano $n > 0$, $V = \mathbb{P}(S_n)$ il sistema lineare completo delle curve di grado n e $k \leq 2n + 1$ un intero. Allora k punti distinti di $\mathbb{P}^2$ inducono condizioni di passaggio indipendenti su V se e solo se non ve ne sono $n + 2$ allineati. In particolare, $n + 2$ punti distinti inducono condizioni di passaggio indipendenti su V se e solo se non sono allineati.*

DIMOSTRAZIONE. Consideriamo k punti distinti $p_1, \ldots, p_k$ e supponiamo che ne esistano $n+2$ contenuti in una retta L: supponiamo per fissare le idee che $p_1, \ldots, p_{n+2} \in L$, allora per Bezout ogni curva di grado n che contiene $p_1, \ldots, p_{n+1}$ contiene L e di conseguenza contiene anche p_{n+2}.

Supponiamo adesso che in un insieme $S \subset \mathbb{P}^2$ di k punti non ne esistano $n + 2$ allineati: vogliamo dimostrare che per ogni $s \in S$ esiste una curva C di grado n che contiene $S - \{s\}$ ma non contiene s. A meno di aggiungere ad S un numero opportuno di punti in posizione generica non è restrittivo supporre $k = 2n + 1$.

Considerando su $S - \{s\}$ la relazione di equivalenza $p \sim q$ se e solo se i punti s, p, q sono allineati, abbiamo una partizione in classi di equivalenza

$$S - \{s\} = S_1 \amalg S_2 \amalg \cdots \amalg S_h .$$

Per ipotesi ciascuna classe di equivalenza contiene al massimo n punti, quindi $h \geq 2$ e per il Lemma 2.7.16 possiamo ordinare i punti $S - \{s\} = \{p_1, \ldots, p_{2n}\}$ in modo tale che p_{2i} non sia equivalente a p_{2i-1} per ogni $i = 1, \ldots, n$. (vedi Esercizio).

Ma allora l'unione delle n rette $C = \overline{p_1p_2} + \cdots + \overline{p_{2n-1}p_{2n}}$ è una curva di grado n con le proprietà richieste. □

Il passo successivo al Lemma 2.7.17, ossia determinare sotto quali condizioni $2n+2$ punti distinti inducono condizioni indipendenti sulle curve di grado n, inizia ad essere geometricamente non banale e precursore di importanti teoremi.

Senza entrare in dettaglio, se studiamo le condizioni di passaggio delle coniche per 6 punti distinti, osserviamo che il teorema di Steiner 2.6.3 può essere interpretato come una condizione necessaria e sufficiente sulle sestuple di punti distinti affinché siano contenute in una conica.

Anche il caso delle condizioni imposte da 8 punti sulle cubiche rimane tutto sommato abbordabile.

LEMMA 2.7.18. *Otto punti distinti $p_1, \ldots, p_8$ inducono condizioni indipendenti sulle cubiche piane se e solo se non sono contenuti in una conica e non ve ne sono 5 allineati.*

DIMOSTRAZIONE. Dire che $p_1, \ldots, p_8$ inducono condizioni indipendenti vuol dire che le cubiche passanti per tali punti sono un sistema lineare di dimensione 1. Questo esclude immediatamente che gli 8 punti possano appartenere ad una conica Q, altrimenti tutte le cubiche del tipo $Q+L$, con L retta, passano per $p_1, \ldots, p_8$ e formano un sistema lineare di dimensione 2. Che non vi possano essere 5 punti allineati è stato dimostrato nel Lemma 2.7.17.

Viceversa, supponiamo gli $p_1, \ldots, p_8$ non contenuti in una conica e che non ve ne sono 5 allineati: bisogna dimostrare che esiste una cubica che contiene $p_1, \ldots, p_7$ ma non p_8.

Per ogni $i = 1, \ldots, 7$ indichiamo con l_i il numero dei punti $p_1, \ldots, p_7$ che appartengono alla retta $\overline{p_ip_8}$. Per ipotesi ciascun l_i è minore od uguale a 3 e quindi l'insieme delle rette $\overline{p_ip_8}$, $i = 1, \ldots, 7$ contiene almeno tre elementi. A meno di di permutazioni sull'insieme $p_1, \ldots, p_7$ possiamo supporre che $\overline{p_1p_8}$, $\overline{p_2p_8}$ e $\overline{p_3p_8}$ sia una terna di rette distinte che massimizza la somma $l_1 + l_2 + l_3$. In particolare:

(1) le rette $\overline{p_1p_2}$, $\overline{p_1p_3}$ e $\overline{p_2p_3}$ non contengono p_8;
(2) per ogni $i = 4, \ldots, 7$ se p_i non appartiene a $\overline{p_1p_8} \cup \overline{p_2p_8} \cup \overline{p_3p_8}$, allora la retta $\overline{p_ip_8}$ non contiene alcun punto del tipo p_j con $j \neq i, 8$.

Se i punti p_4, p_5, p_6, p_7 appartengono ad una retta L, la cubica $L + \overline{p_1p_2} + \overline{p_1p_3}$ contiene $p_1, \ldots, p_7$ ma non p_8.

Se p_4, p_5, p_6, p_7 non sono allineati, per ogni $i = 1, 2, 3$ sia Q_i una conica passante per i cinque punti p_i, p_4, p_5, p_6, p_7 e mostriamo che l'ipotesi $p_8 \in Q_1 \cap Q_2 \cap Q_3$ conduce ad una contraddizione. Se $Q_1 = Q_2 = Q_3$ allora gli 8 punti sarebbero contenuti in una conica; se invece i punti p_4, p_5, p_6, p_7, p_8 sono contenuti in due coniche distinte allora 4 di essi sono contenuti in una retta M. Dato che i punti p_4, p_5, p_6, p_7 non sono allineati la retta M contiene p_8 e tre dei 4 punti p_4, p_5, p_6, p_7. Siccome abbiamo ordinato i punti in modo tale cha la somma $l_1 + l_2 + l_3$ sia massima deve necessariamente essere $M = \overline{p_hp_8}$ per qualche $h = 1, 2, 3$, ma questo implicherebbe che in $p_h, p_4, p_5, p_6, p_7, p_8$ vi sono 5 punti allineati.

Quindi p_8 non appartiene ad almeno una delle tre coniche Q_1, Q_2, Q_3: se per fissare le idee $p_8 \notin Q_1$, allora la cubica $Q_1 + \overline{p_2, p_3}$ contiene $p_1, \ldots, p_7$ ma non p_8. □

Esercizi.

ESERCIZIO 23. Provare il risultato dell'Esempio 2.7.13 come conseguenza del Lemma 2.7.18.

ESERCIZIO 24. Sia dato un fascio di coniche generato da due rette doppie. Provare che ogni conica di tal fascio è singolare.

ESERCIZIO 25. Calcolare i punti di intersezione delle coniche di equazioni

$$x_0^2 + x_1^2 + x_2^2 = 0, \qquad x_1^2 + x_2^2 - x_0x_1 - x_0x_2 = 0.$$

2.8. Curve ellittiche

Continuiamo con la convenzione che $\mathbb{K}$ sia un campo algebricamente chiuso di caratteristica 0.

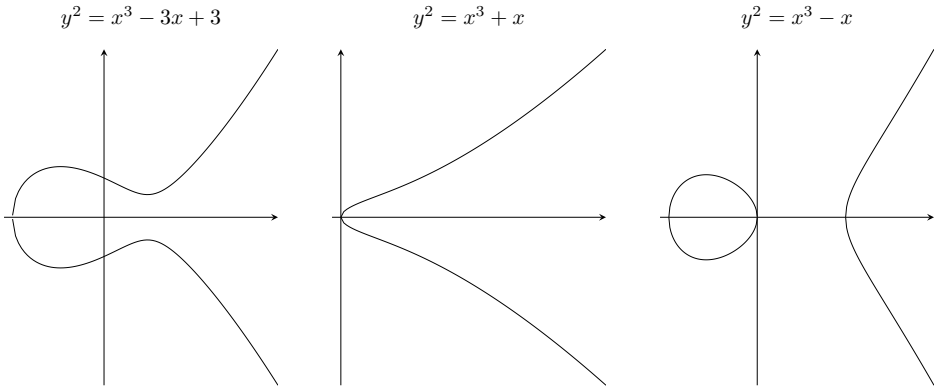


FIGURA 3. Tre esempi di cubiche lisce.

Le curve piane di grado 3 sono dette cubiche piane. Siccome $3 = 2 + 1 = 1 + 2$ sono gli unici modi in cui possiamo scrivere 3 come somma di due interi positivi, una cubica è riducibile se e solo se contiene una retta. Ogni cubica riducibile è singolare mentre, a differenza di quanto accade per le coniche, esistono cubiche singolari irriducibili.

Abbiamo visto che ogni cubica liscia possiede punti di flesso: è possibile dimostrare che esistono esattamente 9 punti di flesso distinti, ma la dimostrazione di questo fatto va oltre gli obiettivi di questo capitolo.

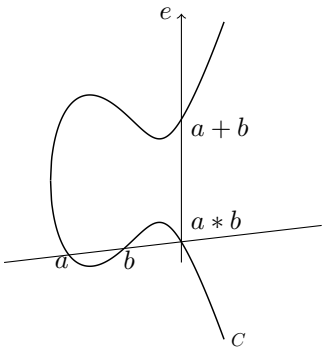
Se C è una cubica liscia ed $e \in C$ è un suo punto di flesso, allora la retta tangente a C in e non interseca C al di fuori di e. Infatti tale retta interseca C in esattamente 3 punti contati con molteplicità e, per definizione di flesso, la molteplicità di intersezione nel punto e è almeno 3.

Chiameremo (provvisoriamente) **curva ellittica** una coppia (C, e) dove C è una cubica liscia ed $e \in C$ è un punto di flesso. Data una curva ellittica (C, e) possiamo definire due operazioni

$$C \times C \xrightarrow{*} C, \qquad C \times C \xrightarrow{+} C,$$

nel modo seguente:

(1) $a * b =$ terzo punto di intersezione, oltre a e b, della retta $\overline{ab}$ con la cubica C, con la convenzione che se $a = b$ per retta $\overline{ab}$ si intende la tangente a C nel punto $a = b$.
(2) $a + b = (a * b) * e$.



$C: \; x_0x_2^2 = x_1^3 - 4x_0^2x_1 + 5x_0^3$

$e = [0, 0, 1]$

È chiaro dalla definizione che $a * b = b * a$, $a + b = b + a$ e $a * (a * b) = b$ per ogni coppia $a, b \in C$, e poichè e è un flesso si ha $e * e = e$. Inoltre per ogni punto $a \in C$ vale

$$a + e = e * (e * a) = a, \qquad a + (a * e) = e * (a * (a * e)) = e * e = e\,.$$

TEOREMA 2.8.1. *Sia (C, e) una curva ellittica. Allora l'operazione binaria $+$ induce su C una struttura di gruppo abeliano su C con elemento neutro e ed inverso $-a = a * e$.*

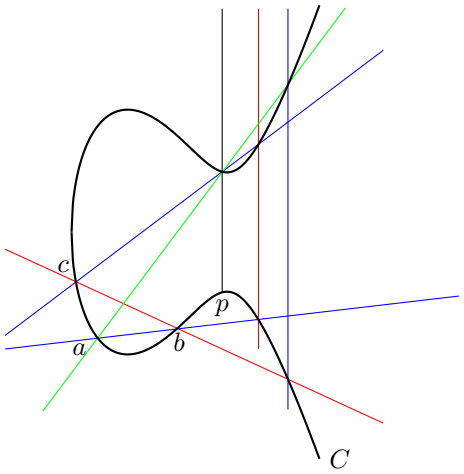


FIGURA 4. Legge associativa sulla cubica C, e cioè $p = (a+b)+c = a+(b+c)$. Nelle notazioni della dimostrazione le tre rette blu sono la cubica B, le due rette rosse sono la conica Q e la retta L è disegnata in verde. L'elemento neutro è il punto all'infinito corrispondente alla direzione verticale.

DIMOSTRAZIONE. Tra i vari assiomi di gruppo rimane solo da verificare la proprietà associativa della somma $a + (b + c) = (a + b) + c$. La dimostrazione completa di questo fatto richiede strumenti non ancora sviluppati. Tuttavia, possiamo utilizzare il teorema di Gergonne per dare una dimostrazione per triple a, b, c in posizione generica e più precisamente sotto l'ipotesi aggiuntiva che i $9 = 3 \times 3$ punti della tabella

$$\begin{array}{ccc} a & b+c & (a+b)*c \\ b & b*c & c \\ a*b & e & a+b \end{array} \tag{2.8}$$

siano tutti distinti (Figura 4).

Dalla definizione delle operazioni $*$ e $+$ segue che ciascuna colonna della Tabella (2.8) è formata da tre punti allineati e quindi i nove punti coincidono con l'intersezione di C con una cubica B unione di tre rette. Similmente la seconda e terza riga della tabella sono formate da terne allineate di punti; in particolare i 6 punti delle ultime due righe coincidono con l'intersezione di C con una conica Q unione di due rette.

Per il teorema di Gergonne 2.7.14 i tre punti della prima riga appartengono ad una retta L, ossia i tre punti a, $b + c$ e $(a + b) * c$ sono allineati, e questo è possible se e solo se $(a + b) * c = a * (b + c)$. Quindi

$$(a + b) + c = e * ((a + b) * c) = e * (a * (b + c)) = a + (b + c)\,.$$

□

Osserviamo che un punto a in una curva ellittica (C, e) è un punto di flesso se e solo se $a * a = a$, o equivalentemente se e solo se $3a = a + a + a = e$. L'equivalenza tra flessi e punti a tali che $a * a = a$ segue immediatamente dalle definizioni. Se $a * a = a$, allora

$$2a = a + a = e * (a * a) = e * a, \qquad 3a = a + 2a = e * (a * (e * a)) = e * e = e\,.$$

Viceversa, se $3a = e$ allora $e * (a * a) = 2a = -a = e * a$ e quindi $a = a * a$.

Analogamente si osserva che tre punti $a, b, c \in C$ sono allineati se e solo se $a + b + c = e$: la condizione $a + b + c = e$ è equivalente a dire che $e * (a * b) = a + b = -c = e * c$ che a sua volta equivale a dire che $a * b = c$.

COROLLARIO 2.8.2. *Dati due punti di flesso distinti $a, b \in C$, il terzo punto c di intersezione di C con la retta $\overline{ab}$ è ancora un flesso.*

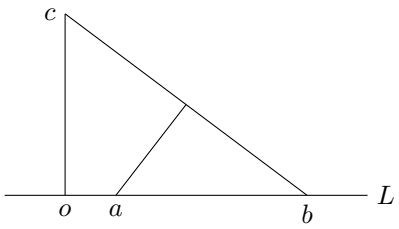


FIGURA 5. La distanza tra il punto a e la retta $\overline{bc}$ è strettamente minore della distanza del punto c dalla retta L.

DIMOSTRAZIONE. Fissiamo un flesso $e \in C$ (non necessariamente uguale ad a o b), abbiamo visto che rispetto alla struttura di gruppo sulla curva ellittica (C, e) si ha $a+b+c = e$, ossia $c = -a - b$. Allora $3c = -3a - 3b = -e - e = e$ e quindi anche c è un flesso. □

ESEMPIO 2.8.3. Sia $\xi \in \mathbb{K} = \mathbb{C}$ una radice cubica primitiva di 1, ossia una radice del polinomio $\xi^2 + \xi + 1$. Allora i flessi della cubica di Fermat $x_0^3 + x_1^3 + x_2^3$ sono le intersezioni con la Hessiana $6^3 x_0 x_1 x_2 = 0$ e sono rappresentati nella tabella

$$\begin{array}{lll} [0,-1,1] & [0,1,\xi] & [0,-1,\xi^2] \\ [-1,0,1] & [-1,0,\xi^2] & [-1,0,\xi] \\ [-1,1,0] & [-1,\xi,0] & [-1,\xi^2,0] \end{array} .$$

Senza usare il precedente corollario si verifica direttamente e facilmente che dati due punti della tabella ne esiste un terzo allineato.

Nel precedente esempio i flessi a coordinate reali sono esattamente i tre della prima colonna. Più in generale ogni cubica liscia complessa può avere al massimo tre flessi reali, come segue immediatamente dal Corollario 2.8.2 e dal seguente classico risultato di geometria proiettiva reale.

TEOREMA 2.8.4. *Sia $S \subset \mathbb{P}^n_{\mathbb{R}}$ un insieme* finito *di punti che soddisfa la seguente proprietà:*

- *per ogni coppia di punti distinti $p, q \in S$ esiste un punto $r \in S$, diverso da p, q e appartenente alla retta $\overline{pq}$. Equivalentemente, se ogni retta di $\mathbb{P}^n_{\mathbb{R}}$ interseca S in un sottoinsieme di cardinalità diversa da 2.*

Allora i punti di S sono tutti allineati.

DIMOSTRAZIONE. Supponiamo per assurdo che esistano tre punti $p, q, r \in S$ non allineati e sia $H \subset \mathbb{P}^n_{\mathbb{R}}$ il piano che li contiene. A meno di sostituire $\mathbb{P}^n_{\mathbb{R}}$ con H e S con $S \cap H$ non è restrittivo supporre $n = 2$. Infine, prendendo come retta all'infinito una qualsiasi retta che non interseca S possiamo ridurci al casi in cui $S \subset \mathbb{R}^2$ è un sottoinsieme finito che soddisfa la proprietà (P). Abbiamo supposto per assurdo che l'insieme T formato dalle terne ordinate $(p, q, r) \in S^3$ di punti non allineati sia non vuoto. Scegliamo un elemento $(u, v, c) \in T$ tale che la distanza di c dalla retta $L = \overline{uv}$ sia la minore possibile. Detta M la retta perpendicolare ad L passante per c, la distanza di c da L è uguale alla distanza di c dal punto o di intersezione di L con M. Il punto o divide la retta L in due semirette, ed L contiene almeno tre punti di S. Possiamo quindi trovare $a \neq b \in S \cap L$ tali che a è contenuto nel segmento di estremi o, b. Ma allora la distanza di a dalla retta $\overline{cb}$ è strettamente minore della distanza tra o e c (Figura 5), in contraddizione con le ipotesi. □

Bibliografia

[1] Walker, R. J.: *Algebraic curves.* Princeton (1950). 53