

Capitolo 6

Richiami di geometria proiettiva e affine su un campo

6.1 Gruppi lineari e semilineari

Sia V uno spazio vettoriale di dimensione finita n su un campo K . I vettori di V , tranne esplicito avviso, saranno sempre denotati con lettere latine minuscole in grassetto.

DEFINIZIONE 6.1.1. Ricordiamo che un *automorfismo* di V é una trasformazione lineare e biunivoca di V , cioè una permutazione L sugli elementi di V tale che

$$L(\alpha\mathbf{x} + \beta\mathbf{y}) = \alpha L(\mathbf{x}) + \beta L(\mathbf{y}),$$

per ogni $\alpha, \beta \in K$ e $\mathbf{x}, \mathbf{y} \in V$. Gli automorfismi di V formano un gruppo di permutazioni sui vettori di V che si denota con $GL(V)$ e si chiama *gruppo generale lineare*. \square

E' ben noto che un automorfismo $L \in GL(V)$, rispetto ad una base ordinata $\mathcal{B} = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$, si rappresenta con un'equazione del tipo

$$\begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix} = A_L \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

ove (x_i) e (x'_i) sono le componenti in \mathcal{B} rispettivamente di un generico vettore \mathbf{v} e della sua immagine $L(\mathbf{v})$, e A_L é la matrice quadrata invertibile le cui colonne sono ordinatamente uguali alle componenti dei vettori $L(\mathbf{e}_1), L(\mathbf{e}_2), \dots, L(\mathbf{e}_n)$.

Se denotiamo con $GL(n, K)$ il gruppo delle matrici quadrate invertibili di ordine n su K e fissiamo una base ordinata \mathcal{B} in V , l'applicazione

$$L \in GL(V) \rightarrow A_L \in GL(n, K) \tag{6.1}$$

é un isomorfismo di gruppi.

OSSERVAZIONE 6.1.2. L'isomorfismo (6.1) non é *canonico* in quanto dipende dalla scelta di una base in V . Saranno, quindi, *non canonici* tutti gli isomorfismi costruiti a partire da questo. \square

Ricordiamo che, fissato $L \in GL(V)$, al variare della base \mathcal{B} , la matrice A_L (cfr.6.1) descrive in $GL(n, K)$ una classe completa di matrici simili e quindi il determinante e la traccia di A_L non dipendono dalla base scelta ma sono degli invarianti di L ; essi si chiamano rispettivamente *determinante* e *traccia* di L .

DEFINIZIONE 6.1.3. Gli automorfismi di V con determinante uguale ad 1 formano un sottogruppo di $GL(V)$ che si denota con $SL(V)$ e si chiama *gruppo lineare speciale*. E' chiaro che $SL(V)$ é isomorfo al sottogruppo $SL(n, K)$ di $GL(n, K)$ formato dalle matrici a determinante 1. \square

ESERCIZIO 6.1.4. *Provare che ogni automorfismo di V trasforma sottospazi vettoriali di V in sottospazi vettoriali della stessa dimensione.* \square

ESERCIZIO 6.1.5. *Provare che $GL(V)$, e quindi $GL(n, K)$, hanno un'azione regolare sull'insieme delle basi ordinate di V .* \square

ESERCIZIO 6.1.6. *Provare che il centro di $GL(V)$ é isomorfo al gruppo delle matrici scalari e non nulle d'ordine n su K e, quindi, al gruppo moltiplicativo K^* di K . Dedurre che il centro di $SL(V)$ é isomorfo al gruppo delle radici n -esime dell'unitá di K .* \square

PROPOSIZIONE 6.1.7. $SL(V)$ é un sottogruppo normale di $GL(V)$ e il gruppo quoziente

$$GL(V)/SL(V)$$

é isomorfo al gruppo moltiplicativo K^* di K .

DIMOSTRAZIONE. L'applicazione

$$\det : L \in GL(V) \rightarrow \det(L) \in K^*$$

é un epimorfismo di gruppi il cui nucleo é $SL(V)$. Allora l'asserto segue dal teorema di omomorfismo dei gruppi. \square

DEFINIZIONE 6.1.8. Una permutazione T sugli elementi di V prende il nome di *automorfismo semilineare* se esiste un automorfismo σ del campo K tale che:

$$L(\alpha x + \beta y) = \alpha^\sigma L(x) + \beta^\sigma L(y),$$

per ogni $\alpha, \beta \in K$ e $x, y \in V$. L'automorfismo σ di K si dice *associato* a T . Gli automorfismi semilineari di V formano un gruppo di permutazioni sui vettori di V che si denota con $\Gamma L(V)$ e si chiama *gruppo semilineare*. \square

OSSERVAZIONE 6.1.9. Un automorfismo semilineare di V il cui automorfismo associato é l'identità di K é evidentemente un automorfismo di V e, quindi, risulta $GL(V) \leq \Gamma L(V)$. Ne segue che i gruppi $GL(V)$ e $\Gamma L(V)$ coincidono se, e solo se, l'identità é l'unico automorfismo del campo K .

Per evitare confusione fra gli elementi di $\Gamma L(V)$ e quelli di $GL(V)$, gli elementi di $GL(V)$ vengono talvolta chiamati *automorfismi lineari*. \square

Fissati un automorfismo σ di K e una base \mathcal{B} di V , per ogni vettore $\mathbf{v} \in V$ di componenti (x_1, x_2, \dots, x_n) , si denoti con \mathbf{v}^σ il vettore di componenti $(x_1^\sigma, x_2^\sigma, \dots, x_n^\sigma)$. Allora, detto L un automorfismo di V , l'applicazione

$$T_{L,\sigma} : \mathbf{v} \in V \rightarrow L(\mathbf{v}^\sigma) \in V \quad (6.2)$$

risulta un *automorfismo semilineare* di V che si dice *associato ad L e σ* nella base \mathcal{B} . L'automorfismo semilineare $T_{A,\sigma}$, nella base \mathcal{B} , si rappresenta con l'equazione

$$\begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix} = A \begin{pmatrix} x_1^\sigma \\ x_2^\sigma \\ \vdots \\ x_n^\sigma \end{pmatrix}, \quad (6.3)$$

ove A è la matrice di L nella base scelta.

ESERCIZIO 6.1.10. *Fissata una base \mathcal{B} di V , provare che l'applicazione*

$$(L, \sigma) \in GL(V) \times Aut(K) \rightarrow T_{L,\sigma} \in \Gamma L(V)$$

è un isomorfismo di gruppi.

PROPOSIZIONE 6.1.11. *Il gruppo $GL(V)$ è un sottogruppo normale di $\Gamma L(V)$ e il gruppo quoziente $\Gamma L(V)/GL(V)$ è isomorfo al gruppo $Aut(K)$ degli automorfismi del campo K .*

DIMOSTRAZIONE. Fissata una base $\mathcal{B} = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$ in V , in forza dell'esercizio precedente, l'applicazione

$$\varphi : T_{L,\sigma} \in \Gamma L(V) \rightarrow \sigma \in Aut(K)$$

è un omomorfismo di $\Gamma L(V)$ in $Aut(K)$ il cui nucleo è $GL(V)$. Tale omomorfismo è suriettivo perché, fissato un automorfismo σ di K , la funzione

$$\sum_{i=1}^n \lambda_i \mathbf{e}_i \rightarrow \sum_{i=1}^n \lambda_i^\sigma \mathbf{e}_i,$$

con $\lambda_i \in K$, è un automorfismo semilineare. Dal teorema di omomorfismo dei gruppi segue, allora, l'asserto □

ESERCIZIO 6.1.12. *Provare che ogni automorfismo semilineare di V trasforma sottospazi vettoriali di V in sottospazi vettoriali della stessa dimensione.* □

Riportiamo senza dimostrazione il seguente risultato fondamentale.

PROPOSIZIONE 6.1.13. *Sia V uno spazio vettoriale di dimensione maggiore di due. Allora, fissata una base di V , una permutazione su V è un automorfismo semilineare se, e solo se, insieme all'inversa, trasforma sottospazi vettoriali in sottospazi vettoriali della stessa dimensione.*

Sia ora $V = V(n, q)$ lo spazio vettoriale numerico di dimensione finita n sul campo di Galois F_q , $q = p^r$ e p primo e poniamo

$$GL(n, F_q) = GL(n, q), \quad SL(n, F_q) = SL(n, q), \quad \Gamma L(V) = \Gamma L(n, q).$$

Nel seguito riterremo sempre fissata una base ordinata $\mathcal{B} = (e_1, e_2, \dots, e_n)$, di $V(n, q)$ e identificheremo un automorfismo L di V con la matrice A_L che lo rappresenta in \mathcal{B} , porremo cioè $GL(V) = GL(n, q)$ e $SL(V) = SL(n, q)$.

PROPOSIZIONE 6.1.14. *Il numero delle basi ordinate di $V(n, q)$ é*

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Detto h un intero tale che $0 \leq h \leq n$, il numero dei sottospazi vettoriali h -dimensionali di $V(n, q)$ é dato da

$$\begin{bmatrix} n \\ h \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-h+1} - 1)}{(q^h - 1)(q^{h-1} - 1) \cdots (q - 1)}. \quad (6.4)$$

DIMOSTRAZIONE. Per costruire una base ordinata (e_1, e_2, \dots, e_n) , il vettore e_1 deve essere non nullo e quindi può essere scelto in $(q^n - 1)$ modi. Il vettore e_2 deve essere scelto tra quelli che non appartengono al sottospazio di dimensione 1 generato da e_1 e abbiamo esattamente $(q^n - q)$ possibilità per tale scelta. Allora, per induzione su n , si ha la prima parte dell'asserto.

Osserviamo che l'argomentazione precedente prova che il numero di h -ple di vettori indipendenti di $V(n, q)$ é esattamente

$$(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{h-1}).$$

Allora il numero dei sottospazi V_h di dimensione h di $V(n, q)$ si ottiene dividendo il numero delle h -ple di vettori indipendenti di $V(n, q)$ per il numero delle basi di un V_h e da ciò segue l'asserto. \square

DEFINIZIONE 6.1.15. I numeri $\begin{bmatrix} n \\ h \end{bmatrix}_q$ definiti dalla (6.4) si chiamano *coefficienti gaussiani*. \square

ESERCIZIO 6.1.16. *Provare che i coefficienti gaussiani verificano l'identità*

$$\begin{bmatrix} n \\ h \end{bmatrix}_q = \begin{bmatrix} n \\ n-h \end{bmatrix}_q$$

ESERCIZIO 6.1.17. *Tenendo presente la prop.6.1.7, provare che $SL(n, q)$ ha indice $q - 1$ in $GL(n, q)$ e quindi*

$$|GL(n, q)| = (q - 1)|SL(n, q)|.$$

Sappiamo che, fissate due basi ordinate \mathcal{B} e \mathcal{B}' di $V(n, q)$, esiste un unico automorfismo $L \in GL(n, q)$ che trasforma \mathcal{B} in \mathcal{B}' . Questo significa che l'ordine di $GL(n, q)$ é pari al numero delle

basi ordinate di $V(n, q)$ e quindi (cfr. prop.6.1.14, 6.1.17)

$$\begin{aligned} |GL(n, q)| &= (q^n - 1)(q^n - q) \cdots (q^n - q^{n-2})(q^n - q^{n-1}) \\ &= q^{\frac{n(n-1)}{2}} \prod_{j=1}^n (q^j - 1) \end{aligned} \quad (6.5)$$

e

$$|SL(n, q)| = q^{\frac{n(n-1)}{2}} \prod_{j=2}^n (q^j - 1). \quad (6.6)$$

ESERCIZIO 6.1.18. *Provare che $GL(n, q)$ è 2-transitivo su $V(n, q) \setminus \{\mathbf{0}\}$ se, e soltanto se, $q = 2$.*

ESERCIZIO 6.1.19. *Provare che il centro di $SL(n, q)$ è isomorfo al gruppo delle radici n -esime dell'unità in F_q .*

ESERCIZIO 6.1.20. *Ricordando che abbiamo posto $q = p^r$, provare che*

$$|\Gamma L(n, q)| = r|GL(n, q)|.$$

PROPOSIZIONE 6.1.21. *$GL(n, q)$ è un sottogruppo normale di $\Gamma L(n, q)$.*

DIMOSTRAZIONE. L'applicazione

$$T_{A, \sigma} \in \Gamma L(n, q) \rightarrow \sigma \in \text{Aut}(F_q)$$

è un epimorfismo di gruppi il cui nucleo coincide con $GL(n, q)$ e da ciò segue subito l'asserto. \square

6.2 Spazi proiettivi

Sia V uno spazio vettoriale di dimensione finita $n + 1$ su un campo K e denotiamo con $PG(V)$ l'insieme dei sottospazi 1-dimensionali di V , che chiameremo *punti* di $PG(V)$.

Se W è un sottospazio vettoriale di V di dimensione $h + 1$, $0 \leq h \leq n$, denotiamo con $[W]$ il sottoinsieme di $PG(V)$ costituito dai sottospazi 1-dimensionali di V contenuti in W , poniamo cioè $[W] = PG(W)$; un insieme di questo tipo prende il nome di *sottospazio proiettivo*, o semplicemente *sottospazio*, di $PG(V)$ di dimensione h . Per convenzione, assumiamo che il sottoinsieme vuoto sia un sottospazio di $PG(V)$ di dimensione -1 . I sottospazi di $PG(V)$ di dimensione 0 sono ovviamente i punti di $PG(V)$, quelli di dimensione 1, 2, $n - 1$ prendono rispettivamente il nome di *rette*, *piani*, *iperpiani*.

Se $\{U_j\}_{j \in J}$ è una famiglia di sottospazi vettoriali di V , risulta

$$[\bigcap_{j \in J} U_j] = \bigcap_{j \in J} [U_j].$$

Ne segue che l'intersezione di sottospazi di $PG(V)$ è ancora un sottospazio e quindi, per ogni sottoinsieme X di $PG(V)$, si può definire il sottospazio $\langle X \rangle$ generato da X come l'intersezione

di tutti i sottospazi che lo contengono. Il sottospazio generato dall'unione di due sottospazi H e T si denota con $H + T$ e si chiama *somma* di H e T ; nel caso $H \cap T = \emptyset$, H e T si dicono *sghembi* e la somma $H + T$ si dice *diretta* e si denota con $H \oplus T$. Due sottospazi la cui somma diretta è uguale a $PG(V)$ si dicono *supplementari*. Le dimensioni di due sottospazi H e T sono legate fra loro dalla *formula di Grassmann*

$$\dim(H) + \dim(T) = \dim(H \cap T) + \dim(H + T).$$

Le proprietà descritte negli esercizi da 6.2.1 a 6.2.6 si provano senza molte difficoltà usando le proprietà vettoriali di V .

ESERCIZIO 6.2.1. *Provare che in $PG(V)$ valgono le seguenti proprietà:*

- se X è un insieme di punti, risulta $\langle X \rangle = X$ se, e solo se, X è un sottospazio;
- due punti distinti appartengono ad un'unica retta;
- se H è un sottospazio e P un punto non appartenente ad H , risulta

$$\dim(H + P) = \dim(H) + 1;$$

- un iperpiano ed un sottospazio di dimensione $h+1$ non contenuto nell'iperpiano si intersecano in un sottospazio di dimensione h ;
- se H e T sono due sottospazi supplementari, risulta $\dim(H) = n - \dim(T) - 1$. □

Nel seguito, se A, B sono punti distinti di $PG(V)$, denoteremo con AB la retta contenente A e B .

ESERCIZIO 6.2.2. *Siano X un sottospazio di $PG(V)$ e P, P' due punti distinti di X . Provare che la retta passante per P e P' è contenuta in X . □*

ESERCIZIO 6.2.3. *Se X è un insieme non vuoto di punti di $PG(V)$ e P un punto non appartenente ad X , l'unione delle rette passanti per P e incidenti X si chiama cono di vertice P e base X .*

Provare che, se X è un sottospazio di dimensione h , il cono di base X e vertice un punto $P \notin X$ è un sottospazio di dimensione $h + 1$. □

ESERCIZIO 6.2.4. *Provare che un insieme X di punti di $PG(V)$ è un sottospazio se, e soltanto se, per ogni due punti distinti di X , la retta che li congiunge è contenuta in X . □*

ESERCIZIO 6.2.5. *Provare che due rette distinte di un piano di $PG(V)$ si intersecano in esattamente un punto. □*

ESERCIZIO 6.2.6. *Siano A, B, C, D quattro punti di $PG(V)$, con $A \neq B$, $C \neq D$, tali che le rette AB e CD abbiano un punto in comune. Provare che le rette AC e BD hanno un punto in comune. □*

DEFINIZIONE 6.2.7. Denotata con \mathcal{S}_j la famiglia di tutti i sottospazi proiettivi di $PG(V)$ di dimensione j , con $j = -1, 0, 1, 2, \dots, n$, la coppia

$$(PG(V), (\mathcal{S}_{-1}, \mathcal{S}_0, \mathcal{S}_1, \mathcal{S}_2, \dots, \mathcal{S}_{n-1}, \mathcal{S}_n))$$

prende il nome di *spazio proiettivo associato a V* , o anche *spazio proiettivo sul campo K* . Tale spazio, con abuso di notazione, sarà denotato semplicemente con $PG(V)$. L'intero $n = \dim(V) - 1$ si chiama *dimensione* di $PG(V)$. \square

DEFINIZIONE 6.2.8. Lo spazio proiettivo associato allo spazio vettoriale K^{n+1} si denota con $PG(n, K)$ e si chiama *spazio proiettivo numerico di dimensione n su K* . \square

OSSERVAZIONE 6.2.9. Ogni sottospazio proiettivo di dimensione h di $PG(V)$ può essere considerato spazio proiettivo di dimensione h sul campo K . \square

Se v è un vettore non nullo di V , il simbolo $\langle v \rangle$ denoterà il sottospazio vettoriale generato da v e denoteremo semplicemente con $[v]$ il corrispondente punto $[\langle v \rangle]$ di $PG(V)$.

DEFINIZIONE 6.2.10. Diciamo che m punti

$$P_1 = [v_1], P_2 = [v_2], \dots, P_m = [v_m]$$

di $PG(V)$ sono (linearmente) *dependenti* o *indipendenti* se tali risultano i vettori v_1, v_2, \dots, v_m . Notiamo che tale definizione è ben posta in quanto la dipendenza o indipendenza lineare di P_1, P_2, \dots, P_m non dipende dalla scelta di v_j nel sottospazio $\langle v_j \rangle$. Diciamo inoltre che un punto $P = [v]$ *dipende* (linearmente) da P_1, P_2, \dots, P_m se il vettore v dipende da v_1, v_2, \dots, v_m .

Un insieme X di punti di $PG(V)$ si chiama *generatore* se risulta $\langle X \rangle = PG(V)$. Un generatore formato da punti indipendenti si chiama *base*. \square

E' immediato rendersi conto che un insieme di punti indipendenti

$$\{P_1 = [v_1], P_2 = [v_2], \dots, P_m = [v_m]\}$$

è una base se, e soltanto se, v_1, v_2, \dots, v_m è una base di V e di conseguenza è $m = n + 1$.

ESERCIZIO 6.2.11. *Provare che due basi*

$$\{v_0, v_1, \dots, v_n\} \text{ e } \{w_0, w_1, \dots, w_n\}$$

dello spazio vettoriale V individuano una stessa base di $PG(V)$ se, e soltanto se, ogni v_i è proporzionale ad un w_j . \square

DEFINIZIONE 6.2.12. Una $(n + 2)$ -pla

$$\mathfrak{R} = (A^0, A^1, \dots, A^n, A)$$

di punti di $PG(V)$ a $n + 1$ a $n + 1$ indipendenti prende il nome di *referimento proiettivo* di $PG(V)$. I punti A^0, A^1, \dots, A^n si chiamano *punti fondamentali* e A *punto unità* del riferimento. Un sottospazio h -dimensionale di $PG(V)$ contenente $h + 1$ punti di \mathfrak{R} diversi da A si chiama *sottospazio fondamentale* del riferimento \mathfrak{R} . \square

DEFINIZIONE 6.2.13. Se $\mathcal{B} = (e_0, e_1, \dots, e_n)$ é una base ordinata di V , si ha che

$$\mathfrak{R}(\mathcal{B}) = (E_0 = [e_0], E_1 = [e_1], \dots, E_n = [e_n], E = [\sum_{j=0}^n e_j])$$

é un riferimento proiettivo di $PG(V)$, detto *associato* a \mathcal{B} , e non é difficile provare che ogni riferimento proiettivo \mathfrak{R} di $PG(V)$ si ottiene in questo modo. Fissato dunque il riferimento proiettivo $\mathfrak{R} = \mathfrak{R}(\mathcal{B})$, ad ogni punto

$$P = [v = \sum_{j=0}^n x_j e_j]$$

resta associata la $(n+1)$ -pla $(x_0, x_1, \dots, x_n) \in K^{n+1} \setminus \{\mathbf{0}\}$ delle componenti di v nella base \mathcal{B} . Gli elementi di tale $(n+1)$ -pla si chiamano *coordinate proiettive (omogenee)* di P nel riferimento \mathfrak{R} e sono definiti a meno di un fattore comune non nullo di proporzionalitá in quanto dipendono dalla scelta di un vettore non nullo nel sottospazio vettoriale $\langle v \rangle$ di V . Resta cosí definita anche la funzione biunivoca, detta *coordinazione*,

$$\gamma_{\mathfrak{R}} : P = [\sum_{j=0}^n x_j e_j] \in PG(V) \rightarrow [(x_0, x_1, \dots, x_n)] \in PG(n, K) \quad (6.7)$$

con la quale si possono identificare i punti di $PG(V)$ con quelli dello spazio proiettivo numerico $PG(n, K)$. \square

Quando, fissato un riferimento proiettivo in $PG(V)$, scriveremo $P = (x_0, x_1, \dots, x_n)$, intenderemo che x_0, x_1, \dots, x_n sono le coordinate proiettive del punto P . Ovviamente, per i punti fondamentali del riferimento si ha

$$\begin{aligned} E_0 &= (1, 0, 0, \dots, 0, 0) \\ E_1 &= (0, 1, 0, \dots, 0, 0) \\ &\vdots \\ E_n &= (0, 0, 0, \dots, 0, 1) \\ E &= (1, 1, 1, \dots, 1, 1) \end{aligned}$$

OSSERVAZIONE 6.2.14. Ricordiamo che ogni sottospazio vettoriale W di dimensione $h+1$ di V , rispetto ad una base ordinata $\mathcal{B} = (e_i)$, si rappresenta mediante un sistema di $k = n - h$ equazioni omogenee indipendenti del tipo

$$\begin{cases} a_{10}x_0 + a_{11}x_1 + \dots + a_{1n}x_n = 0 \\ a_{20}x_0 + a_{21}x_1 + \dots + a_{2n}x_n = 0 \\ \vdots \\ a_{k0}x_0 + a_{k1}x_1 + \dots + a_{kn}x_n = 0 \end{cases} \quad (6.8)$$

Si ha allora facilmente che ogni sottospazio h -dimensionale di $PG(V)$, nel riferimento $\mathfrak{R}(\mathcal{B})$, si rappresenta con un sistema del tipo (6.8). In particolare, gli iperpiani di $PG(V)$ si rappresentano con equazioni lineari omogenee. Notiamo che il sottospazio fondamentale di dimensione h contenente i punti fondamentali del riferimento $E_{i_0}, E_{i_1}, \dots, E_{i_h}$ é rappresentato dal sistema

$$\{x_j = 0 \quad : \quad j \neq i_0, i_1, \dots, i_h\}.$$

□

ESERCIZIO 6.2.15. Siano $\mathcal{B} = (e_i)$ e $\mathcal{B}' = (e'_i)$ due basi ordinate di V . Provare che \mathcal{B} e \mathcal{B}' individuano lo stesso riferimento proiettivo di $PG(V)$ se, e soltanto se, sono basi proporzionali, cioè se esiste $\lambda \in K$ tale che $e_i = \lambda e'_i$, per ogni $i = 0, 2, \dots, n$. □

DEFINIZIONE 6.2.16. Se L è un automorfismo di V , possiamo considerare la permutazione σ_L sui punti di $PG(V)$ definita da

$$\sigma_L : P = [v] \rightarrow P' = [L(v)].$$

Una permutazione di questo tipo prende il nome di *proiettività*. Le proiettività di $PG(V)$ formano un gruppo che si denota con $PGL(V)$ e si chiama *gruppo (lineare generale) proiettivo*. Lo studio delle proprietà di $PG(V)$ invarianti rispetto a tale gruppo si chiama *geometria proiettiva* di $P(V)$. L'applicazione

$$L \in GL(n+1, K) \rightarrow \sigma_L \in PGL(V)$$

è un epimorfismo di gruppi il cui nucleo è il centro di $GL(n+1, K)$ e quindi

$$PGL(V) \sim \frac{GL(n+1, K)}{Z(GL(n+1, K))} \sim \frac{GL(V)}{Z(GL(V))}. \quad (6.9)$$

In modo analogo si definisce il gruppo

$$PSL(V) \sim \frac{SL(n+1, K)}{Z(SL(n+1, K))}, \quad (6.10)$$

che si chiama *gruppo (lineare) speciale proiettivo*. □

DEFINIZIONE 6.2.17. Siano V, V' due spazi vettoriali su K di dimensione maggiore di due. Una biiezione f fra i punti di $PG(V)$ e quelli di $PG(V')$ prende il nome di *collineazione* se f , insieme alla sua inversa, trasforma rette in rette. Nel caso V e V' hanno dimensione due, una *collineazione* fra $PG(V)$ e $PG(V')$ è una funzione del tipo

$$P = [v] \rightarrow P' = [T(v)],$$

ove T è una funzione semilineare fra V e V' .

Dalla definizione segue subito che l'applicazione inversa di una collineazione è ancora una collineazione e che le collineazioni di $PG(V)$ in se stesso formano un gruppo, il *gruppo delle collineazioni di $PG(V)$* , che si denota con $P\Gamma L(V)$. Lo studio delle proprietà di $PG(V)$ invarianti rispetto a tale gruppo prende il nome di *geometria di incidenza* di $PG(V)$. □

Si prova senza difficoltà che la funzione (6.7) è una collineazione fra $PG(V)$ e $PG(n, K)$. Da ciò segue che, se V e V' sono spazi vettoriali isomorfi, allora esiste una collineazione fra $PG(V)$ e $PG(V')$. Infatti, se \mathfrak{R} è un riferimento proiettivo di $PG(V')$, l'applicazione

$$\gamma_{\mathfrak{R}} \gamma_{\mathfrak{R}'}^{-1} : PG(V) \rightarrow PG(V') \quad (6.11)$$

è una collineazione fra $PG(V)$ e $PG(V')$.

DEFINIZIONE 6.2.18. Le collineazioni definite dalla (6.11) prendono il nome di *proiettività o omografie*. \square

ESEMPIO 6.2.19. Se T è un automorfismo semilineare di V , possiamo considerare la permutazione σ_T sui punti di $PG(V)$ definita da

$$P = [v] \rightarrow P' = [T(v)].$$

È facile verificare che σ_T è una collineazione di $PG(V)$. \square

ESERCIZIO 6.2.20. Siano $PG(V)$ e $PG(V')$ due spazi proiettivi. Provare che una biiezione f fra $PG(V)$ e $PG(V')$ è una collineazione se e soltanto se trasforma, insieme alla sua inversa, sottospazi proiettivi in sottospazi proiettivi della stessa dimensione. Ne segue che esiste una collineazione fra $PG(V)$ e $PG(V')$ se, e soltanto se, $\dim(V) = \dim(V')$. \square

ESERCIZIO 6.2.21. Siano V, V' due spazi vettoriali della stessa dimensione finita su K . Provare che $PGL(V) \sim PGL(V')$ e $P\Gamma L(V) \sim P\Gamma L(V')$. \square

ESERCIZIO 6.2.22. Siano $PG(V)$ e $PG(V')$ due spazi proiettivi e d un intero tale che $0 \leq d < n$. Provare che una biiezione f fra $PG(V)$ e $PG(V')$ è una collineazione se, e solo se, trasforma, insieme alla sua inversa, sottospazi proiettivi di dimensione d in sottospazi proiettivi di dimensione d . \square

Nel seguito supporremo sempre che V sia uno spazio vettoriale numerico e ciò, in forza delle precedenti considerazioni, non è restrittivo ai fini dello studio delle proprietà proiettive e di incidenza di $PG(V)$.

Il seguente teorema, diretta conseguenza della prop.6.1.13, è uno dei risultati fondamentali della geometria d'incidenza di $PG(V)$.

PROPOSIZIONE 6.2.23. (teorema fondamentale) Sia V uno spazio vettoriale di dimensione maggiore di due. Allora ogni collineazione σ di $PG(V)$ è del tipo σ_T , (cfr.es.6.2.19) con T opportuno elemento di $\Gamma L(V)$. Ne segue che

$$P\Gamma L(V) \sim \frac{\Gamma L(V)}{Z(GL(V))}.$$

6.3 Dualità

Sia V uno spazio vettoriale di dimensione finita $n + 1$ su un campo K e sia V^* il duale di V , cioè lo spazio vettoriale delle funzioni lineari di V in K , che chiamiamo *funzionali lineari* su V . Detta $\mathcal{B} = (e_0, e_1, \dots, e_n)$ una base ordinata di V , denotiamo con $\mathcal{B}^* = (e_0^*, e_1^*, \dots, e_n^*)$ la *base duale* di \mathcal{B} . Ricordiamo che gli elementi di \mathcal{B}^* sono definiti da

$$e_i^*(e_j) = \delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

e quindi, per ogni $\mathbf{a} = (a_1, a_2, \dots, a_n) \in V$, risulta

$$\mathbf{e}_i^*(\mathbf{a}) = \mathbf{e}_i^* \left(\sum_{j=1}^n a_j \mathbf{e}_j \right) = \sum_{j=1}^n a_j \mathbf{e}_i^*(\mathbf{e}_j) = a_i = i\text{-esima componente di } \mathbf{a} \text{ in } \mathcal{B}.$$

DEFINIZIONE 6.3.1. Lo spazio proiettivo $PG(V^*)$ si chiama *duale* di $PG(V)$ e si denota anche con $PG(V)^*$.

Se

$$\mathfrak{R} = \left(E_i = \langle \mathbf{e}_i \rangle, E = \langle \sum_{j=0}^n \mathbf{e}_j \rangle \right)$$

é un riferimento proiettivo di $PG(V)$, allora

$$\mathfrak{R}^* = \left(E_i^* = \langle \mathbf{e}_i^* \rangle, E^* = \langle \sum_{j=0}^n \mathbf{e}_j^* \rangle \right)$$

é un riferimento di $PG(V)^*$ che si dice *duale* di \mathfrak{R} . □

Nel seguito, quando é fissata una base ordinata in V , (risp. un riferimento in $PG(V)$), riterremo contemporaneamente fissata la base duale in V^* (risp. il riferimento duale in $PG(V)^*$).

Fissato un riferimento proiettivo in $PG(V)$, ogni iperpiano $\pi_{\mathbf{a}}$ di $PG(V)$ di equazione

$$a_0 x_0 + a_1 x_1 + \dots + a_n x_n = 0$$

individua il punto $\pi_{\mathbf{a}}^* = (a_0, a_1, \dots, a_n)$ di $PG(V)^*$ e l'applicazione

$$\pi_{\mathbf{a}} \rightarrow \pi_{\mathbf{a}}^* \tag{6.12}$$

porta biunivocamente gli iperpiani di $PG(V)$ nei punti di $PG(V)^*$. In altre parole, fissato un riferimento in $PG(V)$, é possibile identificare mediante la (6.12), gli iperpiani di $PG(V)$ con i punti di $PG(V)^*$. L'insieme degli iperpiani di $PG(V)$ corrispondente ai punti di un sottospazio h -dimensionale di $PG(V)^*$ prende il nome di *sistema lineare di iperpiani* di dimensione h . Le nozioni di dipendenza e indipendenza lineare tra punti possono dunque interpretarsi, mediante la (6.12), sull'insieme degli iperpiani. In particolare, diremo che gli iperpiani di $PG(V)$

$$\pi_{\mathbf{a}_1}, \pi_{\mathbf{a}_2}, \dots, \pi_{\mathbf{a}_h}$$

sono *indipendenti* se sono tali i punti

$$\pi_{\mathbf{a}_1}^*, \pi_{\mathbf{a}_2}^*, \dots, \pi_{\mathbf{a}_h}^*$$

di $PG(V)^*$. Ora, osservando che $h + 1$ iperpiani indipendenti di $PG(V)$ si intersecano in un sottospazio di dimensione $n - h - 1$, si ha che la (6.12) induce un'applicazione biunivoca fra i sottospazi di dimensione $n - h - 1$ di $PG(V)$ e quelli di dimensione h di $PG(V)^*$; vale cioè il seguente teorema.

PROPOSIZIONE 6.3.2. (teorema della stella) Nello spazio proiettivo $PG(V)$, un insieme Σ_h di iperpiani é un sistema lineare di dimensione h se, e soltanto se, é l'insieme di tutti gli iperpiani contenente un fissato sottospazio S_{n-h-1} di dimensione $n-h-1$ (stella di iperpiani di centro S_{n-h-1}).

Due sottospazi di $PG(V)$ di dimensioni rispettivamente h e $n-h-1$ si dicono di *dimensioni duali*.

Se, usando la prop.6.3.2, identifichiamo i sottospazi di $PG(V)^*$ con le stelle di iperpiani di $PG(V)$ e se denotiamo con S_h^* la stella di iperpiani di $P(V)$ di centro S_h , abbiamo le seguenti proprietà:

- (1) $\dim(X^*) = n - \dim(X) - 1$,
- (2) $X \subseteq Y \Leftrightarrow Y^* \subseteq X^*$,
- (3) $(X \cup Y)^* = Y^* \cap X^*$,
- (3) $(X \cap Y)^* = Y^* \cup X^*$,

per ogni X, Y sottospazi di $PG(V)$.

DEFINIZIONE 6.3.3. Una collineazione

$$\gamma : PG(V) \rightarrow PG(V)^*$$

prende il nome di *correlazione* di $PG(V)$. □

DEFINIZIONE 6.3.4. Una correlazione γ di $PG(V)$ si chiama *polarità* se verifica la seguente proprietà di reciprocità:

$$P \in \gamma(T) \Leftrightarrow T \in \gamma(P),$$

con P e T punti di $PG(V)$.

Un punto $P \in PG(V)$ si dice *autoconiugato*, o *assoluto*, rispetto a γ se accade che $P \in \gamma(P)$. L'insieme dei punti autoconiugati rispetto a γ si chiama *assoluto* di γ e, quando tale assoluto coincide con tutti i punti di $PG(V)$, la polarità si dice *nulla*, o *simplettica*. □

ESERCIZIO 6.3.5. Nell'ipotesi che K abbia caratteristica diversa da 2, sia $A = (a_{ij})$ una matrice simmetrica non degenere su K d'ordine $n+1$. Fissato un riferimento proiettivo di $PG(V)$, provare che l'applicazione che ad ogni punto di coordinate (a_0, a_1, \dots, a_n) associa l'iperpiano di equazione

$$(a_0, a_1, \dots, a_n)A \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$$

é una polarità di $PG(V)$. □

Usando la (6.12) é possibile dimostrare il seguente teorema.

PROPOSIZIONE 6.3.6. (*principio di dualitá*) Sia

$$\Pi = \Pi(j_1, j_2, \dots, j_s, +, \cap, \subseteq)$$

una proprietá della geometria d'incidenza di $PG(V)$ nell'enunciato della quale intervengano sottospazi di dimensioni j_1, j_2, \dots, j_s , le operazioni di somma e intersezione di sottospazi e la relazione di inclusione fra sottospazi. Sia

$$\Pi^* = \Pi(n - j_1 - 1, n - j_2 - 1, \dots, n - j_s - 1, \cap, +, \supseteq)$$

la proprietá di $PG(V)$ ottenuta dall'enunciato della Π sostituendo ad ogni dimensione j_t quella duale $n - j_t - 1$, scambiando fra loro le operazioni di somma e intersezione di sottospazi e invertendo le relazioni di inclusione fra sottospazi. Allora Π e Π^* sono o entrambe vere o entrambe false.

Due proprietá Π e Π^* , come nell'enunciato del precedente teorema, si dicono l'una *duale* dell'altra.

ESEMPIO 6.3.7. In $PG(2, K)$, la proprietá *due punti distinti appartengono ad un' unica retta* ha per duale *due rette distinte hanno esattamente un punto in comune*. \square

ESERCIZIO 6.3.8. *Provare che in $PG(V)$ vale la seguente proprietá: Se X, Y sono sottospazi supplementari, ogni punto $P \notin X \cup Y$ appartiene ad un' unica retta incidente sia X che Y . Trovare la proprietá duale della precedente.* \square

6.4 Spazi affini

In $PG(n, K)$ si fissi un iperpiano π_∞ e, per ogni sottospazio proiettivo $S_h \not\subseteq \pi_\infty$ di dimensione h , si consideri il sottospazio $(h - 1)$ -dimensionale $S_h^\infty = S_h \cap \pi_\infty$. I punti dell'insieme $AG(n, K) = PG(n, K) \setminus \pi_\infty$ si dicono *punti affini* di $PG(n, K)$, rispetto a π_∞ , e gli insiemi del tipo $A_h = S_h \setminus S_h^\infty$ si chiamano *sottospazi affini* di dimensione h di $AG(n, K)$. Il sottospazio S_h^∞ si chiama *sottospazio improprio* di A_h . Come nel caso proiettivo, i sottospazi affini di $AG(n, K)$ di dimensione $0, 1, 2, n - 1$ si chiamano rispettivamente *punti, rette, piani, iperpiani*. Per convenzione assumiamo che l'insieme vuoto sia un sottospazio affine di dimensione -1 .

E' chiaro che l'intersezione di sottospazi di $AG(n, K)$ é ancora un sottospazio e quindi, per ogni sottoinsieme X di $AG(n, K)$, si puó definire il sottospazio affine $\langle X \rangle$ generato da X come l'intersezione di tutti i sottospazi affini che lo contengono. Il sottospazio affine generato dall'unione di due sottospazi affini H e T si denota con $H + T$ e si chiama *somma* di H e T . Le dimensioni di due sottospazi affini H e T sono legate fra loro dalla *formula di Grassmann affine*

$$\dim(H) + \dim(T) \geq \dim(H \cap T) + \dim(H + T).$$

Due sottospazi affini di dimensione maggiore di zero si dicono *paralleli* se il sottospazio improprio di uno dei due é contenuto in quello dell'altro. Si prova subito che, se due sottospazi affini sono paralleli, allora o sono ad intersezione vuota o uno dei due é contenuto nell'altro.

ESERCIZIO 6.4.1. *Provare che in $AG(n, K)$ valgono le seguenti proprietà:*

- se X è un insieme di punti, risulta $\langle X \rangle = X$ se, e solo se, X è un sottospazio affine;
- due punti distinti appartengono ad un'unica retta;
- se H è un sottospazio affine e P un punto non appartenente ad H , risulta

$$\dim(H + P) = \dim(H) + 1;$$

- un iperpiano ed un sottospazio affine di dimensione $h + 1$ non contenuto nell'iperpiano si intersecano in un sottospazio di dimensione h o sono paralleli.
- la relazione di parallelismo fra sottospazi affini della stessa dimensione è di equivalenza. \square

ESERCIZIO 6.4.2. *Siano X un sottospazio di $AG(n, K)$ e P, P' due punti distinti di X . Provare che la retta passante per P e P' è contenuta in X . \square*

ESERCIZIO 6.4.3. *Provare che due rette ad intersezione vuota e contenute in un piano di $AG(n, K)$ sono parallele. \square*

DEFINIZIONE 6.4.4. Per ogni $j = -1, 0, 1, 2, \dots, n$, denotata con \mathcal{A}_j la famiglia di tutti i sottospazi affini di $AG(n, K)$, la coppia

$$(AG(n, K), (\mathcal{A}_{-1}, \mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_{n-1}, \mathcal{A}_n))$$

prende il nome di *spazio affine su K* . Tale spazio, con abuso di notazione, sarà denotato semplicemente con $AG(n, K)$. L'intero n si chiama *dimensione* di $AG(n, K)$. \square

OSSERVAZIONE 6.4.5. Ogni sottospazio affine di dimensione h di $AG(n, K)$ può essere considerato spazio affine di dimensione h sul campo K . \square

Se $\mathfrak{R} = \{E_0, E_1, \dots, E_n, E\}$ è un riferimento proiettivo di $PG(n, K)$ nel quale π_∞ ha equazione $x_n = 0$, ogni punto affine $P = (x_0, x_1, \dots, x_n)$ ha l'ultima coordinata x_n diversa da zero. Gli elementi di K definiti da

$$y_1 = \frac{x_0}{x_n}, y_2 = \frac{x_1}{x_n}, \dots, y_n = \frac{x_{n-1}}{x_n}$$

si chiamano *coordinate affini* del punto P nel riferimento \mathfrak{R} e l'applicazione

$$P \in AG(n, K) \rightarrow (y_1, y_2, \dots, y_n) \in K^n \tag{6.13}$$

è biunivoca.

OSSERVAZIONE 6.4.6. Usando l'osservazione 6.2.14 si prova senza difficoltà che, in coordinate affini, ogni sottospazio affine h -dimensionale di $AG(n, K)$ si rappresenta mediante un sistema di $k = n - h$ equazioni lineari indipendenti del tipo

$$\begin{cases} a_{11}y_1 + a_{12}y_2 + \dots + a_{1n}y_n + b_1 = 0 \\ a_{21}y_1 + a_{22}y_2 + \dots + a_{2n}y_n + b_2 = 0 \\ \vdots \\ a_{k1}y_1 + a_{k2}y_2 + \dots + a_{kn}y_n + b_k = 0 \end{cases} \tag{6.14}$$

In particolare, gli iperpiani si rappresentano con equazioni lineari. \square

ESERCIZIO 6.4.7. *Provare che in $AG(n, K)$ le immagini nell'applicazione (6.13) dei sottospazi affini di dimensione maggiore di zero e contenenti il punto di coordinate affini $(0, 0, \dots, 0)$ sono tutti e soli i sottospazi vettoriali di K^n .* \square

ESERCIZIO 6.4.8. *Provare che le immagini dei sottospazi affini di dimensione maggiore di zero di $AG(n, K)$ nell'applicazione (6.13) sono tutti e soli i laterali dei sottospazi vettoriali di K^n .* \square

DEFINIZIONE 6.4.9. Si chiama *affinitá* di $AG(n, K)$ ogni permutazione L sui suoi punti rappresentata da una equazione del tipo

$$\begin{pmatrix} y'_1 \\ y'_2 \\ \vdots \\ y'_n \end{pmatrix} = A \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} + \mathbf{b},$$

ove (y_i) e (y'_i) sono le coordinate affini rispettivamente di un generico punto P e di $L(P)$, $A \in GL(n, K)$ e $\mathbf{b} \in K^n$. Le affinitá di $AG(n, K)$ formano un gruppo, il *gruppo delle affinitá*, che si denota con $AGL(n, K)$. Si verifica facilmente che ogni affinitá trasforma sottospazi affini in sottospazi affini della stessa dimensione. Lo studio delle proprietá di $AG(n, K)$ invarianti rispetto al gruppo $AGL(n, K)$ prende il nome di *geometria affine* di $AG(n, K)$. \square

ESERCIZIO 6.4.10. *Provare che $AGL(n, K)$ é isomorfo allo stabilizzatore dell'iperpiano π_∞ in $PGL(n+1, K)$.* \square

DEFINIZIONE 6.4.11. Per $n > 1$, una permutazione sui punti di $AG(n, K)$, che insieme all'inversa trasformi rette in rette, si chiama *collineazione* di $AG(n, K)$. Una collineazione di $AG(1, K)$ é, invece, una permutazione sui suoi punti del tipo

$$x \rightarrow ax^\sigma + b,$$

ove $a \in K^*$, $b \in K$ e σ é un automorfismo di K . Le collineazioni di $AG(n, K)$ formano un gruppo, il *gruppo delle collineazioni*, che si denota con $AFL(n, K)$ e evidentemente risulta $AGL(n, K) \leq AFL(n, K)$.

Lo studio delle proprietá di $AG(n, K)$ invarianti rispetto al gruppo $AFL(n, K)$ prende il nome di *geometria di incidenza* di $AG(n, K)$. \square

ESERCIZIO 6.4.12. *Provare che $AFL(n, K)$ é isomorfo allo stabilizzatore di π_∞ in $PGL(n+1, K)$.* \square

Analogamente al caso proiettivo, vale il seguente teorema fondamentale.

PROPOSIZIONE 6.4.13. *Sia n un intero maggiore di 1. Allora una permutazione sui punti di $AG(n, K)$ é una collineazione di $AG(n, K)$ se, e soltanto se, é rappresentata da una equazione del tipo*

$$\begin{pmatrix} y'_1 \\ y'_2 \\ \vdots \\ y'_n \end{pmatrix} = A \begin{pmatrix} y_1^\sigma \\ y_2^\sigma \\ \vdots \\ y_n^\sigma \end{pmatrix} + \mathbf{b},$$

ove $A \in GL(n, K)$, $\sigma \in \text{Aut}(K)$ e $\mathbf{b} \in K^n$.

ESERCIZIO 6.4.14. *Provare che una permutazione sui punti di $AG(n, K)$ è una collineazione di $AG(n, K)$ se, e soltanto se, insieme all'inversa, trasforma sottospazi affini in sottospazi affini della stessa dimensione.* \square

ESERCIZIO 6.4.15. *Sia d un intero tale che $0 \leq d < n$. Provare che una permutazione sui punti di $AG(n, K)$ è una collineazione di $AG(n, K)$ se, e soltanto se, insieme all'inversa, trasforma sottospazi affini di dimensione d in sottospazi affini di dimensione d .* \square

6.5 Spazi proiettivi e affini su campi di Galois

Sia $\mathcal{P} = PG(n, q)$ lo spazio proiettivo numerico di dimensione finita n sul campo di Galois F_q , $q = p^r$ e p primo. Sia inoltre $AG(n, F_q) = AG(n, q)$ lo spazio affine di dimensione n su F_q . Poniamo

$$PGL(\mathcal{P}) = PGL(n+1, q), \quad PSL(\mathcal{P}) = PSL(n+1, q), \quad P\Gamma L(\mathcal{P}) = P\Gamma L(n+1, q)$$

e

$$AGL(n, F_q) = AGL(n, q), \quad A\Gamma L(n, F_q) = A\Gamma L(n, q).$$

OSSERVAZIONE 6.5.1. Secondo quanto riportato da *H.S.M. Coxeter* in [33], gli spazi proiettivi su un campo finito $GF(q)$ furono introdotti nel 1892 da *Gino Fano* nel caso q primo. Successivamente nel 1906, *O. Veblen* e *W.H. Bussey* estesero la costruzione di Fano al caso di arbitrarie potenze di primi e introdussero la notazione $PG(n, q)$. \square

PROPOSIZIONE 6.5.2. *Sia h un intero tale che $0 \leq h \leq n$. Il numero dei sottospazi proiettivi h -dimensionali di $PG(n, q)$ è dato da*

$$\begin{bmatrix} n+1 \\ h+1 \end{bmatrix}_q = \frac{(q^{n+1}-1)(q^n-1)\cdots(q^{n+1-h}-1)}{(q^{h+1}-1)(q^h-1)\cdots(q-1)}. \quad (6.15)$$

In particolare il numero dei punti e il numero degli iperpiani di $PG(n, q)$ è dato da

$$\frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \cdots + q + 1. \quad (6.16)$$

Inoltre $AG(n, q)$ contiene esattamente q^n punti e

$$q^n + q^{n-1} + \cdots + q \quad (6.17)$$

iperpiani.

DIMOSTRAZIONE. E' una conseguenza della prop.6.1.14. \square

PROPOSIZIONE 6.5.3. *Siano h, n, k interi tali che $0 \leq h, n-h-1 \leq n-1$ e $h < k \leq n-1$. Siano S_h e S_{n-h-1} due fissati sottospazi proiettivi supplementari di $PG(n, q)$. Allora in $PG(n, q)$ il numero di sottospazi proiettivi k -dimensionali contenenti S_h è uguale al numero dei sottospazi*

proiettivi $(k-h-1)$ -dimensionali contenuti in S_{n-h-1} . Inoltre, il numero dei sottospazi proiettivi k -dimensionali di $PG(n, q)$ contenenti un fissato sottospazio di dimensione h é dato da

$$\begin{bmatrix} n-h \\ k-h \end{bmatrix}_q = \frac{(q^{n-h}-1)(q^{n-h-1}-1)\cdots(q^{n-k+1}-1)}{(q^{k-h}-1)(q^{k-h-1}-1)\cdots(q-1)}. \quad (6.18)$$

DIMOSTRAZIONE. Se S_h e S_{n-h-1} sono sottospazi supplementari di $PG(n, q)$, la formula di Grassmann assicura che ogni sottospazio S_k di dimensione k contenente S_h interseca S_{n-h-1} in un sottospazio S_{k-h-1} di dimensione $k-h-1$. L'applicazione

$$S_k \supset S_h \rightarrow S_{k-h-1} = S_k \cap S_{n-h-1} \subset S_{n-h-1}$$

é una biiezione fra i sottospazi di dimensione k contenenti S_h e quelli di dimensione $k-h-1$ contenuti in S_{n-h-1} e abbiamo cosí la prima parte dell'asserto. La seconda parte segue dalla 6.15. \square

ESERCIZIO 6.5.4. Siano h, n, k interi tali che $0 \leq h < k \leq n-1$. Provare che il numero dei sottospazi affini k -dimensionali di $AG(n, q)$ contenenti un fissato sottospazio di dimensione h é dato da

$$\begin{bmatrix} n-h \\ k-h \end{bmatrix}_q = \frac{(q^{n-h}-1)(q^{n-h-1}-1)\cdots(q^{n-k+1}-1)}{(q^{k-h}-1)(q^{k-h-1}-1)\cdots(q-1)}. \quad (6.19)$$

ESERCIZIO 6.5.5. Ricordando che abbiamo posto $q = p^r$, provare che

$$|PGL(n, q)| = q^{\frac{n(n-1)}{2}} \prod_{j=2}^n (q^j - 1),$$

$$|PSL(n, q)| = \frac{|PGL(n, q)|}{MCD(q-1, n)},$$

$$|P\Gamma L(n, q)| = r|PGL(n, q)|,$$

$$|AGL(n, q)| = q^n |GL(n, q)|,$$

$$|A\Gamma L(n, q)| = q^n |\Gamma L(n, q)|.$$

PROPOSIZIONE 6.5.6. I gruppi $PGL(n+1, q)$ e $PSL(n+1, q)$ sono 2-transitivi sui punti di $PG(n, q)$.

DIMOSTRAZIONE. Siano $([x], [y])$ e $([x'], [y'])$ due coppie di punti distinti di $PG(n, q)$ e siano $(e_i), (e'_i)$ due basi ordinate di $V(n+1, q)$ tali che $e_0 = x, e_1 = y, e'_0 = x'$ e $e'_1 = y'$. Allora, se L é l'unico automorfismo di $V(n+1, q)$ che porta (e_i) in (e'_i) , la proiettività σ_L associata ad L porta $[x]$ in $[x']$ e $[y]$ in $[y']$. Ora, se il determinante d di L é diverso da 1, possiamo ragionare come prima sostituendo il vettore $e'_1 = y'$ nella base e'_i con il vettore $d^{-1}y'$. In questo modo otteniamo un automorfismo L' di $V(n, q)$ con determinante 1 la cui proiettività associata appartiene a $PSL(n+1, q)$ e porta ancora $[x]$ in $[x']$ e $[y]$ in $[y']$. \square

ESERCIZIO 6.5.7. *Provare che $PGL(n+1, q)$ é strettamente transitivo sui riferimenti proiettivi di $PG(n, q)$, cioè sulle $(n+2)$ -ple di punti di $PG(n, q)$ a $n+1$ a $n+1$ indipendenti. Se ne deduca che $PGL(2, q)$ é strettamente 3-transitivo sui punti di $PG(1, q)$.*

ESERCIZIO 6.5.8. *Provare che una proiettività di $PG(n, q)$ che fissa tutti i punti fondamentali e il punto unità di un riferimento proiettivo é necessariamente l'identità. Provare inoltre che una proiettività di $PG(1, q)$ che ha tre punti uniti é necessariamente l'identità.*

Riportiamo senza dimostrazione il seguente teorema di cui faremo uso nel seguito.

PROPOSIZIONE 6.5.9. *Ad eccezione dei casi $(n, q) = (2, 2), (2, 3)$, $PSL(n, q)$ é un gruppo semplice, per ogni intero $n \geq 2$.*

Osserviamo che $PSL(2, 2)$ e $PSL(2, 3)$ non sono semplici perché rispettivamente isomorfi ai gruppi S_3 e A_4 . Risulta inoltre

$$PSL(2, 4) \sim PSL(2, 5) \sim A_5; \quad PSL(2, 7) \sim PSL(3, 2); \quad PSL(2, 9) \sim A_6.$$

Concludiamo osservando che $PSL(4, 2)$ e $PSL(3, 4)$ hanno lo stesso ordine 20.160 ma non sono isomorfi; é infatti possibile provare che $PSL(4, 2)$ é isomorfo ad A_8 mentre $PSL(3, 4)$ non lo é. Da notare che 20.160 é il piú piccolo intero positivo che risulta ordine di due gruppi semplici non isomorfi.

6.6 Forme sesquilineari e polarità in $PG(n, q)$

Siano V, W due spazi vettoriali su $GF(q)$. Un'applicazione

$$L : V \rightarrow W$$

si dice *semilineare*, o σ -lineare, se esiste un automorfismo σ di $GF(q)$ tale che

$$(1) \quad L(\mathbf{a} + \mathbf{b}) = L(\mathbf{a}) + L(\mathbf{b}),$$

$$(2) \quad L(\alpha \mathbf{a}) = \alpha^\sigma L(\mathbf{a}),$$

per ogni $\mathbf{a}, \mathbf{b} \in V$ e $\alpha \in GF(q)$. L'automorfismo σ si dice *associato* alla funzione semilineare L e, quando σ é l'identità, L é una funzione lineare.

ESERCIZIO 6.6.1. *Sia V uno spazio vettoriale su $GF(q)$ e σ un automorfismo di $GF(q)$. Si definisca su V un nuovo prodotto " \cdot " fra scalari e vettori nel seguente modo*

$$\alpha \cdot \mathbf{a} = \alpha^\sigma \mathbf{a}, \quad \text{per ogni } \alpha \in GF(q), \mathbf{a} \in V.$$

Provare che $V^\sigma = (V, +, \cdot)$ é uno spazio vettoriale su $GF(q)$ della stessa dimensione di V . Provare inoltre che una funzione L fra V e W é σ -lineare se, e solo se, L é lineare fra V e W^σ .

OSSERVAZIONE 6.6.2. L'esercizio 6.6.1 prova che lo studio delle funzioni semilineari fra due spazi vettoriali é equivalente a quello delle funzioni lineari. \square

Sia ora V uno spazio vettoriale di dimensione finita n su $GF(q)$.

DEFINIZIONE 6.6.3. Una funzione

$$\langle , \rangle : (\mathbf{x}, \mathbf{y}) \in V \times V \rightarrow \langle \mathbf{x}, \mathbf{y} \rangle \in GF(q)$$

si chiama *forma sesquilineare*, o *semibilineare*, su V se é lineare nel primo argomento e σ -lineare nel secondo, cioè se verifica le seguenti proprietà:

$$(F1) \quad \langle \mathbf{x}_1 + \mathbf{x}_2, \mathbf{y} \rangle = \langle \mathbf{x}_1, \mathbf{y} \rangle + \langle \mathbf{x}_2, \mathbf{y} \rangle \quad \text{e} \\ \langle \mathbf{x}, \mathbf{y}_1 + \mathbf{y}_2 \rangle = \langle \mathbf{x}, \mathbf{y}_1 \rangle + \langle \mathbf{x}, \mathbf{y}_2 \rangle,$$

$$(F2) \quad \langle \alpha \mathbf{x}, \mathbf{y} \rangle = \alpha \langle \mathbf{x}, \mathbf{y} \rangle,$$

$$(F3) \quad \langle \mathbf{x}, \alpha \mathbf{y} \rangle = \alpha^\sigma \langle \mathbf{x}, \mathbf{y} \rangle,$$

per ogni $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}, \mathbf{y}_1, \mathbf{y}_2, \mathbf{y} \in V$ e $\alpha \in GF(q)$, ove σ é un automorfismo di $GF(q)$.

L'automorfismo σ si dice *associato* alla forma sesquilineare. Quando σ é l'identità, la forma sesquilineare si dice *bilineare*. \square

In tutto il paragrafo la parola *forma* senza alcun aggettivo sarà sinonimo di forma sesquilineare e ne riterremo fissata una \langle , \rangle con automorfismo associato σ .

Sia $\mathcal{B} = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$ una base ordinata di V e, come al solito, scriviamo $\mathbf{a} = (a_1, a_2, \dots, a_n)$ per indicare che a_1, a_2, \dots, a_n sono le componenti del vettore $\mathbf{a} \in V$ nella base \mathcal{B} .

Se $\mathbf{x}, \mathbf{y} \in V$, risulta

$$\langle \mathbf{x}, \mathbf{y} \rangle = \left\langle \sum_{i=1}^n x_i \mathbf{e}_i, \sum_{j=1}^n y_j \mathbf{e}_j \right\rangle \\ = \sum_{i=1}^n x_i \left\langle \mathbf{e}_i, \sum_{j=1}^n y_j \mathbf{e}_j \right\rangle = \sum_{i,j=1}^n x_i y_j^\sigma \langle \mathbf{e}_i, \mathbf{e}_j \rangle,$$

e, se poniamo $a_{ij} = \langle \mathbf{e}_i, \mathbf{e}_j \rangle$ e $A = (a_{ij})$, é

$$\langle \mathbf{x}, \mathbf{y} \rangle = (x_1, x_2, \dots, x_n) A \begin{pmatrix} y_1^\sigma \\ y_2^\sigma \\ \vdots \\ y_n^\sigma \end{pmatrix} = \mathbf{x} A (\mathbf{y}^\sigma)^t. \quad (6.20)$$

La matrice $A = (a_{ij} = \langle \mathbf{e}_i, \mathbf{e}_j \rangle)$ si dice *associata* alla forma nella base \mathcal{B} ed é chiaro che ogni matrice A ad elementi in $GF(q)$, mediante la 6.20, definisce una forma su V . Due forme su V si dicono *equivalenti* se, in basi diverse, possono essere rappresentate da una stessa matrice.

ESERCIZIO 6.6.4. Sia $GF(q)$ di caratteristica p e $q = p^r$. Provare che il numero delle forme sesquilineare su uno spazio vettoriale di dimensione n su $GF(q)$ é rq^{n^2} .

Per ogni sottospazio vettoriale $X \subseteq V$, poniamo

$$X_d^\perp = \{ \mathbf{y} \in V : \langle \mathbf{x}, \mathbf{y} \rangle = 0, \text{ per ogni } \mathbf{x} \in X \},$$

e

$$X_s^\perp = \{ \mathbf{y} \in V : \langle \mathbf{y}, \mathbf{x} \rangle = 0, \text{ per ogni } \mathbf{x} \in X \}.$$

Si ha che X_d^\perp e X_s^\perp sono sottospazi vettoriali di V e risulta

$$X \subseteq (X_d^\perp)_s^\perp, \quad X \subseteq (X_s^\perp)_d^\perp \quad (6.21)$$

$$Y \subseteq X \Rightarrow X_d^\perp \subseteq Y_d^\perp, \quad X_s^\perp \subseteq Y_s^\perp. \quad (6.22)$$

I sottospazi V_d^\perp e V_s^\perp si chiamano *radicale sinistro* e *destro* della forma e si può provare che hanno la stessa dimensione.

La forma si dice *non degenera* se uno dei suoi radicali, e di conseguenza l'altro, é nullo. E' facile rendersi conto che, nel caso $GF(q)$ abbia caratteristica dispari, una forma é non degenera se, e solo se, una qualunque matrice associata A ha determinante non nullo, cioè $A \in GL(n, q)$.

Consideriamo ora lo spazio proiettivo $PG(V)$ e supponiamo che la nostra forma sia non degenera, allora le applicazioni

$$D^\perp : [U] \rightarrow [U_d^\perp]$$

e

$$S^\perp : [U] \rightarrow [U_s^\perp]$$

sono permutazioni sull'insieme dei sottospazi di $PG(V)$. Se

$$S_0 \subset S_1 \subset \cdots \subset S_{n-2}$$

é una catena di sottospazi di $PG(V)$, con $\dim(S_j) = j$, in forza di 6.22 abbiamo

$$(S_0)_d^\perp \supset (S_1)_d^\perp \supset \cdots \supset (S_{n-2})_d^\perp, \quad (S_0)_s^\perp \supset (S_1)_s^\perp \supset \cdots \supset (S_{n-2})_s^\perp,$$

cioé D^\perp e S^\perp trasformano ogni sottospazio di $PG(V)$ in uno di dimensione duale. Ne segue che le funzioni

$$\Delta : \langle \mathbf{x} \rangle \in PG(V) \rightarrow \langle \mathbf{x} \rangle_d^\perp \in PG(V)^*$$

e

$$\Sigma : \langle \mathbf{x} \rangle \in PG(V) \rightarrow \langle \mathbf{x} \rangle_s^\perp \in PG(V)^*$$

sono correlazioni di $PG(V)$ (cfr.6.3.3). Tali correlazioni si dicono *associate* alla forma e quando sono uguali danno luogo ad una polarità (cfr.6.3.4), come specificato nel seguente teorema.

PROPOSIZIONE 6.6.5. Sia \langle , \rangle una forma non degenera su F_q . Allora le seguenti affermazioni sono equivalenti:

- (1) $\langle \mathbf{x}, \mathbf{y} \rangle = 0 \Leftrightarrow \langle \mathbf{y}, \mathbf{x} \rangle = 0$,
- (2) Δ é una polaritá;
- (3) Σ é una polaritá;
- (4) $\Delta = \Sigma$.

Negli esempi che seguono, descriviamo tre classi di forme che ammettono una polaritá associata.

ESEMPIO 6.6.6. Una forma bilineare \langle , \rangle su V si dice *simmetrica* se

$$\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle, \text{ per ogni } \mathbf{x}, \mathbf{y} \in V$$

e *antisimmetrica* se

$$\langle \mathbf{x}, \mathbf{y} \rangle = -\langle \mathbf{y}, \mathbf{x} \rangle, \text{ per ogni } \mathbf{x}, \mathbf{y} \in V.$$

Si noti che le due definizioni coincidono nel caso q sia pari.

Una forma bilineare simmetrica non singolare su V prende il nome di *forma ortogonale* e, verificando la (1) di 6.6.5, definisce una polaritá su $P(V)$. Una forma ortogonale si chiama anche *prodotto scalare* e, in questo caso, l'elemento $\langle \mathbf{x}, \mathbf{y} \rangle$ di $GF(q)$ si dice *prodotto scalare* di \mathbf{x} e \mathbf{y} .

Se $A = (a_{ij} = \langle \mathbf{e}_i, \mathbf{e}_j \rangle)$ é la matrice di una forma ortogonale in una base $\mathcal{B} = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n)$, deve aversi

$$a_{ij} = \langle \mathbf{e}_i, \mathbf{e}_j \rangle = \langle \mathbf{e}_j, \mathbf{e}_i \rangle = a_{ji},$$

per ogni $i, j = 1, 2, \dots, n$, e quindi A é simmetrica. La forma ortogonale corrispondente alla matrice identitá si chiama *prodotto scalare standard* nella base \mathcal{B} e per essa risulta

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1y_1 + x_2y_2 + \dots + x_ny_n.$$

□

ESEMPIO 6.6.7. Una forma bilineare \langle , \rangle su V si dice *alternante* se

$$\langle \mathbf{x}, \mathbf{x} \rangle = 0, \quad \forall \mathbf{x} \in V.$$

Si noti che una forma bilineare alternante é anche antisimmetrica; infatti, per ogni $\mathbf{x}, \mathbf{y} \in V$, risulta

$$\begin{aligned} 0 &= \langle \mathbf{x} + \mathbf{y}, \mathbf{x} + \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{x} \rangle + \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{y}, \mathbf{x} \rangle + \langle \mathbf{y}, \mathbf{y} \rangle \\ &= \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{y}, \mathbf{x} \rangle \end{aligned}$$

e quindi

$$\langle \mathbf{x}, \mathbf{y} \rangle = -\langle \mathbf{y}, \mathbf{x} \rangle.$$

Una forma bilineare alternante non degenera si dice *simplettica* e, verificando la (1) di 6.6.5, definisce una polaritá su $PG(V)$.

Se $A = (a_{ij} = \langle e_i, e_j \rangle)$ é la matrice di una forma simplettica in una base $\mathcal{B} = (e_1, e_2, \dots, e_n)$, deve aversi

$$a_{ij} = \langle e_i, e_j \rangle = - \langle e_j, e_i \rangle = -a_{ji},$$

per ogni $i, j = 1, 2, \dots, n$, e quindi A é antisimmetrica. \square

ESEMPIO 6.6.8. Sia $q = p^{2t}$ una potenza pari della caratteristica p di $GF(q)$ e consideriamo l'unico automorfismo involutorio di $GF(q)$ (cfr.4.2.6) definito da

$$\alpha \in GF(q) \rightarrow \bar{\alpha} = \alpha^{p^t}.$$

Una forma sesquilineare non singolare su V si dice *unitaria* o *hermitiana* se

$$\langle x, y \rangle = \overline{\langle y, x \rangle}.$$

Ogni forma unitaria, verificando la (1) di 6.6.5 induce una polaritá su $PG(V)$.

Se $A = (a_{ij} = \langle e_i, e_j \rangle)$ é la matrice di una forma unitaria in una base $\mathcal{B} = (e_1, e_2, \dots, e_n)$, deve aversi

$$a_{ij} = \langle e_i, e_j \rangle = \overline{\langle e_j, e_i \rangle} = \bar{a}_{ji},$$

per ogni $i, j = 1, 2, \dots, n$. Le matrici i cui elementi verificano le relazioni precedenti si dicono *hermitiane*. \square

Vale il seguente teorema fondamentale che riportiamo senza dimostrazione.

PROPOSIZIONE 6.6.9. Sia \langle, \rangle una forma sesquilineare e non degenera su uno spazio vettoriale V di dimensione n su $GF(q)$ e supponiamo che \langle, \rangle induca una polaritá su $PG(V)$. Allora si ha una delle seguenti possibilitá:

- (1) \langle, \rangle é una forma ortogonale,
- (2) n é pari e \langle, \rangle é una forma simplettica,
- (3) q é una potenza pari di p e \langle, \rangle é una forma unitaria.

Consideriamo una forma sesquilineare e non degenera su V che induca una polaritá su $PG(V)$. Poiché é $D^\perp = S^\perp$ (cfr.6.6.5), conviene porre

$$X^\perp = X_d^\perp = X_s^\perp,$$

per ogni sottospazio X di V . Il sottospazio X^\perp prende il nome di *sottospazio ortogonale*, o *coniugato*, a X e risulta

$$(X^\perp)^\perp = X \quad , \quad \dim(X^\perp) = \dim(V) - \dim(X). \quad (6.23)$$

Il sottospazio X si dice *autoconiugato* se risulta contenuto nel proprio sottospazio ortogonale.

Le forme simplettiche e quelle unitarie possono scriversi in *forma canonica*, nel senso precisato dai seguenti due teoremi.

PROPOSIZIONE 6.6.10. Per ogni forma simplettica sullo spazio vettoriale V di dimensione pari $n = 2h$, esiste una base di V rispetto alla quale la matrice della forma é

$$\begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ -1 & 0 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ -1 & -1 & -1 & \cdots & 0 \end{pmatrix}, \quad (6.24)$$

cioé

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 y_2 - x_2 y_1 + x_1 y_3 - x_3 y_1 + \cdots + x_{n-1} y_n - x_n y_{n-1}. \quad (6.25)$$

PROPOSIZIONE 6.6.11. Sia q un quadrato. Per ogni forma unitaria sullo spazio vettoriale V di dimensione n , esiste una base di V rispetto alla quale risulta

$$\langle \mathbf{x}, \mathbf{y} \rangle = x_1 \bar{y}_1 + x_2 \bar{y}_2 + \cdots + x_n \bar{y}_n, \quad (6.26)$$

ove $\alpha \rightarrow \bar{\alpha}$ é l'unico automorfismo involutorio di $GF(q)$.

DEFINIZIONE 6.6.12. Se abbiamo una forma unitaria su V , possiamo considerare il luogo $H(n, q)$ dei punti di $PG(V)$ autoconiugati rispetto alla forma, cioè

$$\{\langle \mathbf{x} \rangle \in PG(V) : \langle \mathbf{x} \rangle \in \langle \mathbf{x} \rangle^\perp\} = \{\langle \mathbf{x} \rangle \in PG(V) : \langle \mathbf{x}, \mathbf{x} \rangle = 0\}.$$

L'insieme dei punti cosí definito prende il nome di *varietà hermitiana* ed esiste un riferimento proiettivo di $PG(V)$ nel quale ha equazione (cfr.6.26)

$$x_1 \bar{x}_1 + x_2 \bar{x}_2 + \cdots + x_n \bar{x}_n = x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} + \cdots + x_n^{\sqrt{q}+1} = 0. \quad (6.27)$$

Le varietà hermitiane di $PG(2, q)$ si chiamano piú propriamente *curve hermitiane*. \square

ESERCIZIO 6.6.13. Siano q un quadrato e $H(2, q)$ la curva hermitiana del piano $PG(2, q)$ individuata da una forma unitaria \langle, \rangle di $V(3, q)$. Provare che

(1) se $\langle \mathbf{a} \rangle, \langle \mathbf{b} \rangle$ sono punti distinti di $H(2, q)$, risulta $\langle \mathbf{a}, \mathbf{b} \rangle \neq 0$.

(2) la retta A^\perp coniugata ad un punto A di $H(2, q)$ interseca $H(2, q)$ nel solo punto A .

Lo studio delle forme canoniche nel caso ortogonale é piú complesso rispetto ai casi unitario e simplettico, in modo particolare per la caratteristica 2. Esso puó ridursi allo studio delle forme quadratiche (cfr.5.19), delle quali riportiamo di seguito la classificazione.

Consideriamo una forma ortogonale su V e sia $A = (a_{ij})$ la matrice associata in una fissata base ordinata \mathcal{B} di V , cioè

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i,j}^n a_{ij} x_i y_j.$$

La forma quadratica nelle variabili x_1, x_2, \dots, x_n (cfr.5.3.5) definita da

$$\langle \mathbf{x}, \mathbf{x} \rangle = \sum_{i,j}^n a_{ij} x_i x_j \quad (6.28)$$

si dice *associata* alla forma ortogonale nella base \mathcal{B} e risulta non degenera. Le forme quadratiche non degeneri sono classificate dal seguente teorema.

PROPOSIZIONE 6.6.14. *Sia V uno spazio vettoriale di dimensione n su $GF(q)$ e consideriamo le seguenti forme quadratiche nelle variabili x_1, x_2, \dots, x_n :*

$$Q(\mathbf{x}) = x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2, \quad (6.29)$$

$$Q^+(\mathbf{x}) = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n \quad (6.30)$$

$$Q^-(\mathbf{x}) = x_1x_2 + x_3x_4 + \cdots + \alpha x_{n-1}^2 + \beta x_{n-1}x_n + \gamma x_n^2, \quad (6.31)$$

ove $\alpha x_{n-1}^2 + \beta x_{n-1}x_n + \gamma x_n^2$ è un polinomio irriducibile su $GF(q)$. Allora, ogni forma quadratica non degenera su V è equivalente a $Q(\mathbf{x})$, se n è dispari, è equivalente a $Q^+(\mathbf{x})$ o a $Q^-(\mathbf{x})$, se n è pari.

DEFINIZIONE 6.6.15. Consideriamo lo spazio proiettivo $PG(V)$ con un fissato riferimento proiettivo. Il luogo dei punti di $PG(V)$ le cui coordinate annullano una forma quadratica F su V prende il nome di *quadrica* di $PG(V)$ di equazione $F(\mathbf{x}) = 0$. Tale equazione, scritta in forma esplicita, è del tipo

$$\sum_{i,j=1}^n a_{ij}x_i x_j = 0.$$

È facile verificare che la definizione data è ben posta, nel senso che non dipende dal riferimento scelto in $PG(V)$. Una quadrica si dice *non degenera* se la forma quadratica che la definisce è non degenera (cfr.5.19). Nel caso $PG(V)$ sia un piano proiettivo, le sue quadriche prendono il nome di *coniche*. \square

Osserviamo esplicitamente che, nel caso q dispari, la teoria delle quadriche negli spazi proiettivi su F_q è del tutto simile a quella negli spazi proiettivi sul campo reale.

ESERCIZIO 6.6.16. *Provare che una conica non degenera $Q(2, q)$ di $PG(2, q)$ contiene esattamente $q + 1$ punti. Provare inoltre che tali punti risultano a tre a tre non allineati.*

La 6.6.14 fornisce una classificazione delle quadriche non degeneri di uno spazio proiettivo su F_q , nel senso precisato dal seguente teorema.

PROPOSIZIONE 6.6.17. *Sia V uno spazio vettoriale di dimensione n su F_q e Ω una quadrica non degenera di $PG(V)$. Allora è verificata una soltanto delle seguenti possibilità:*

(1) n è dispari ed esiste un riferimento proiettivo di $PG(V)$ nel quale Ω ha equazione

$$Q(\mathbf{x}) = x_1x_2 + x_3x_4 + \cdots + x_{n-2}x_{n-1} + x_n^2 = 0; \quad (6.32)$$

(2) n è pari ed esiste un riferimento proiettivo di $PG(V)$ nel quale Ω ha equazione

$$Q^+(\mathbf{x}) = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n = 0, \quad (6.33)$$

oppure

$$Q^-(\mathbf{x}) = x_1x_2 + x_3x_4 + \cdots + \alpha x_{n-1}^2 + \beta x_{n-1}x_n + \gamma x_n^2 = 0, \quad (6.34)$$

ove $\alpha x_{n-1}^2 + \beta x_{n-1}x_n + \gamma x_n^2$ è un polinomio irriducibile su $GF(q)$.

Il teorema precedente stabilisce che in uno spazio proiettivo su F_q di dimensione pari tutte le quadriche non degeneri sono proiettivamente equivalenti, mentre nel caso della dimensione dispari esistono esattamente due tipi di quadriche non degeneri non equivalenti proiettivamente. Le quadriche non degeneri di $PG(n, q)$ con n pari si dicono di tipo *parabolico* e saranno denotate con $Q(n, q)$. Nel caso n dispari le quadriche non degeneri si dicono di tipo *iperboliche* o *ellittiche* secondo che appartengano alla classe individuata dalla 6.33 o 6.34; esse saranno rispettivamente denotate con $Q^+(n, q)$ e $Q^-(n, q)$.

ESERCIZIO 6.6.18. *Provare che una quadrica ellittica $Q^-(3, q)$ di $PG(3, q)$ contiene esattamente $q^2 + 1$ punti. Provare inoltre che tali punti risultano a tre a tre non allineati.*