UNIVERSITÀ CATTOLICA DEL SACRO CUORE

Facoltà di Scienze Matematiche, Fisiche e Naturali

ISTITUZIONI DI ALGEBRA SUPERIORE I

Una introduzione ai gruppi classici

M. Chiara Tamburini

Anno Accademico 2016/2017

Indice

Capitolo I

La geometria dei gruppi classici

1 Forme sesquilineari sui campi

In questo Capitolo σ indica un automorfismo di un campo $\mathbb{K}$. Saremo interessati solo ai casi in cui $\sigma = \mathrm{id}_{\mathbb{K}}$ oppure σ ha periodo 2, ossia:

$$\sigma^2 = \mathrm{id}_{\mathbb{K}}\,.$$

Ad esempio ha periodo 2 l'automorfismo coniugio σ del campo complesso $\mathbb{C}$:

$$a + ib \mapsto a - ib.$$

La teoria di Galois ci dice che un campo finito $\mathbb{K}$ ha un automorfismo σ di periodo 2 se e solo se il suo ordine è un quadrato. In tal caso, posto $|\mathbb{K}| = q^2$, l'automorfismo σ è l'applicazione:

$$\alpha \mapsto \alpha^q, \quad \forall\ \alpha \in \mathbb{K}.$$

Per ogni $\alpha \in \mathbb{K}$ conviene porre $\sigma(\alpha) := \alpha^\sigma$.

(1.1) Definizione *Sia V uno spazio vettoriale su $\mathbb{K}$. Una forma* σ-sesquilineare *su V è una applicazione*

$$(\ ,\ ) : V \times V \to \mathbb{K}$$

tale che, per ogni $v, v_1, v_2, w, w_1, w_2 \in V$ e per ogni $\lambda, \mu \in \mathbb{K}$

$$\begin{aligned} (v_1 + v_2, w) &= (v_1, w) + (v_2, w) \\ (v, w_1 + w_2) &= (v, w_1) + (v, w_2) \\ (\lambda v, \mu w) &= \lambda\mu^\sigma\,(v, w) \end{aligned} \tag{1.2}$$

Una forma σ-sesquilineare su V si dice:

- bilineare *se $\sigma = \mathrm{id}_{\mathbb{K}}$;*

• hermitiana *se* σ *ha periodo* 2 *e* $(v,w) = (w,v)^\sigma$, *per ogni* $v, w \in V$.

Diciamo inoltre che la forma è :

• non singolare *se, per ogni vettore non nullo* v *di* V, *esiste* $u \in V$ *tale che* $(u,v) \neq 0_{\mathbb{K}}$.

• bilineare simmetrica *se* $\sigma = \mathrm{id}_{\mathbb{K}}$ *e, per ogni* $v, w \in V$, *si ha* $(v,w) = (w,v)$;

• bilineare antisimmetrica *se* $\sigma = \mathrm{id}_{\mathbb{K}}$ *e, per ogni* $v, w \in V$, *si ha* $(v,w) = -(w,v)$.

Chiaramente, per ogni $v \in V$:

$$((0_V, v)) = ((0_{\mathbb{K}} 0_V, v)) = 0_{\mathbb{K}} (0_V, v) = 0_{\mathbb{K}} = (v, 0_V) .$$

(1.3) Definizione *Un'* isometria *di una forma* σ-sesquilineare $(\ ,\ ) : V \times V \to \mathbb{K}$ *è un'applicazione lineare iniettiva* $f : V \to V$ *tale che*

$$(f(v), f(w)) = (v, w), \quad \forall\ v, w \in V.$$

Se W è un qualunque sottospazio di V, ogni forma sesquilineare su V induce una forma sesquilineare su W. Basta infatti considerare la restrizione:

$$(\ ,\ ) : W \times W \to \mathbb{K}.$$

(1.4) Lemma (di Witt) *Data una forma bilineare o hermitiana non singolare su* V, *siano* U, U' *sottospazi di* V *e* $f : U \to U'$ *una isometria (rispetto alle restrizioni della forma a* U, U'*). Allora* f *si estende a una isometria* $\widehat{f} : V \to V$.

Per una dimostrazione si veda [1, 20, pag. 81], o anche [4, Capitolo 6, pag. 369].

(1.5) Esempi

1) *Posto* $V = \mathbb{R}^n$, *l'applicazione*

$$(v, w) := v^T w, \quad \forall\ v, w \in V$$

è una forma bilineare simmetrica, non singolare su V. *Per* $n = 2$ *si ha:*

$$\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) := (x_1, x_2) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1 y_1 + x_2 y_2.$$

Nel caso $n = 3$ *tale forma induce la metrica usuale nello spazio* $\mathbb{R}^3$.

2) *Posto* $V = \mathbb{K}^n$ *e fissata una qualunque matrice* $J \in \mathrm{Mat}_n(\mathbb{K})$, *l'applicazione*

$$(v, w) := v^T J w, \quad \forall\ v, w \in V$$

è una forma bilineare su V. *Per* $\mathbb{K} = \mathbb{R}$, $J = I$ *si ha l'esempio* 1).

2 Forme sesquilineari e matrici

Date una forma σ sequilineare $(\ ,\ ) : V \times V \to \mathbb{K}$ e fissata una base

$$\mathcal{B} = \{v_1, \dots, v_n\}$$

di V, per ogni

$$v = \sum_{i=1}^{n} k_i v_i, \quad w = \sum_{i=1}^{n} h_i v_i, \quad k_i, h_i \in \mathbb{K}$$

in virtù degli assiomi (1.2) della definizione 1.1 si ha:

$$(v, w) = \sum_{i,j=1}^{n} k_i h_j^{\sigma} (v_i, v_j). \tag{2.1}$$

Introducendo la matrice

$$J := ((v_i, v_j)) \in \mathrm{Mat}_n(\mathbb{K}). \tag{2.2}$$

e passando ai vettori coordinate $v_{\mathcal{B}} = \begin{pmatrix} k_1 \\ \dots \\ k_n \end{pmatrix}$, $w_{\mathcal{B}} = \begin{pmatrix} h_1 \\ \dots \\ h_n \end{pmatrix}$, la (2.1) si scrive nella forma:

$$(v, w) = v_{\mathcal{B}}^T J w_{\mathcal{B}}^{\sigma}, \quad \forall\ v, w \in V. \tag{2.3}$$

(2.4) Lemma *Fissata la forma σ-sesquilineare $(\ ,\ ) : V \times V \to \mathbb{K}$ e la base $\mathcal{B}$ di V, l'unica matrice di* $\mathrm{Mat}_n(\mathbb{K})$ *che soddisfa* (2.3) *è J.*

Dimostrazione. Se $A = (a_{ij})$ soddisfa (2.3), da $v_{i\mathcal{B}} = e_i$ per $1 \le i \le n$, segue:

$$(v_i, v_j) \ = \ {v_i}_{\mathcal{B}}{}^T A {v_j}_{\mathcal{B}} \ = \ {e_i}^T A e_j = a_{ij}, \quad \forall\ i, j \le n.$$

Si conclude $A = J$. ■

È così giustificata la seguente:

(2.5) Definizione *$J = ((v_i, v_j))$ si dice la matrice della forma $(\ ,\ )$ rispetto a $\mathcal{B}$.*

In virtù di (2.3), ogni forma bilineare di $\mathbb{K}^n$ è del tipo descritto nell'esempio 2). In tale esempio J è la matrice della forma rispetto alla base canonica. Infatti, se $\mathcal{B}$ è la base canonica di $\mathbb{K}^n$, per ogni $v \in \mathbb{K}^n$ si ha $v = v_{\mathcal{B}}$.

(2.6) Lemma *Sia $J = ((v_i, v_j))$ la matrice di una forma bilineare o hermitiana su V, rispetto a una base $\mathcal{B} = \{v_1, \dots, v_n\}$.*

1) *La forma è non singolare se e solo se* $\det J \neq 0_{\mathbb{K}}$*;*

2) *se* $\sigma = \mathrm{id}_{\mathbb{K}}$, *la forma è simmetrica se e solo se* $J^T = J$;

3) *se* $\sigma = \mathrm{id}_{\mathbb{K}}$, *la forma è antisimmetrica se e solo se* $J^T = -J$;

4) *se* $\sigma \neq \mathrm{id}_{\mathbb{K}}$, *la forma è hermitiana se e solo se* $J^T = J^\sigma$.

Dimostrazione.
1) Fissato $v \in V$, per ogni $v_i \in \mathcal{B}$ si ha $(v_i, v) = {e_i}^T J v_{\mathcal{B}}^\sigma$.
Sia $\det J \neq 0_{\mathbb{K}}$. Consideriamo $v \in V$ non nullo. Se fosse ${e_i}^T J v_{\mathcal{B}}^\sigma = 0_{\mathbb{K}}$ per ogni i, si avrebbe $J v_{\mathcal{B}}^\sigma = 0_{\mathbb{K}^n}$ da cui, moltiplicando per J^{-1}, la contraddizione $v_{\mathcal{B}}^\sigma = 0_{\mathbb{K}^n}$. Pertanto $(v_i, v) \neq 0_{\mathbb{K}}$ per almeno un indice i. Concludiamo che la forma è non degenere.
Viceversa la forma sia non degenere. Se fosse $\det J = 0_{\mathbb{K}}$, esisterebbe $w \in V$ non nullo tale che $J w_{\mathcal{B}}^\sigma = 0_{\mathbb{K}^n}$. Ne seguirebbe $(v, w) = v_{\mathcal{B}}^T J w_{\mathcal{B}}^\sigma = 0_{\mathbb{K}}$ per ogni $v \in V$, contraddizione. Si conclude $\det J \neq 0_{\mathbb{K}}$.

2) e 4). Se la forma è simmetrica o hermitiana si ha, in particolare,

$$(v_j, v_i) = (v_i, v_j)^\sigma, \quad 1 \leq i, j \leq n$$

da cui $J^T = J^\sigma$.
Viceversa, sia $J^T = J^\sigma$. Notando che $(v, w) = (v, w)^T$ per ogni $v, w \in V$:

$$(v, w) = v_{\mathcal{B}}^T J w_{\mathcal{B}}^\sigma = \left(v_{\mathcal{B}}^T J w_{\mathcal{B}}^\sigma\right)^T = \left(w_{\mathcal{B}}^\sigma\right)^T J^\sigma \left(v_{\mathcal{B}}^\sigma\right)^\sigma = \left(w_{\mathcal{B}}^T J v_{\mathcal{B}}\right)^\sigma = (w, v)^\sigma.$$

Si conclude che la forma è simmetrica se $\sigma = \mathrm{id}_{\mathbb{K}}$, è hermitiana se $\sigma \neq \mathrm{id}_{\mathbb{K}}$.

3) Se la forma è antisimmetrica, da

$$(v_j, v_i) = -(v_i, v_j), \quad 1 \leq i, j \leq n$$

segue $J^T = -J$. Viceversa, se $J^T = -J$, per ogni $v, w \in V$:

$$(v, w) = v_{\mathcal{B}}^T J w_{\mathcal{B}} = \left(v_{\mathcal{B}}^T J w_{\mathcal{B}}\right)^T = -w_{\mathcal{B}}^T J v_{\mathcal{B}} = -(w, v).$$

Si conclude che la forma è antisimmetrica. ■

(2.7) Lemma *Sia* $J \in \mathrm{Mat}_n(\mathbb{K})$ *la matrice di una forma sesquilineare su* V, *rispetto a una base* $\mathcal{B} = \{v_1, \ldots, v_n\}$. *Una matrice* $J' \in \mathrm{Mat}_n(\mathbb{K})$ *è la matrice della stessa forma rispetto una base* $\mathcal{B}' = \{{v_1}', \ldots, {v_n}'\}$ *se e solo se esiste* $P \in \mathrm{GL}_n(\mathbb{K})$ *tale che:*

$$J' = P^T J P^\sigma. \tag{2.8}$$

Dimostrazione.
Supponiamo che J' sia la matrice della forma rispetto $\mathcal{B}'$ e sia

$$P := \left(\ (v'_1)_{\mathcal{B}} \ \middle| \ \dots \ \middle| \ (v'_n)_{\mathcal{B}} \ \right)$$

la matrice di passaggio da $\mathcal{B}$ a $\mathcal{B}'$. Per ogni $v \in V$ si ha: $v_{\mathcal{B}} = Pv_{\mathcal{B}'}$. Ne segue:

$$(v, w) = v_{\mathcal{B}}^T J w_{\mathcal{B}}^\sigma = \left(v_{\mathcal{B}'}^T P^T\right) J \left(P^\sigma w_{\mathcal{B}'}^\sigma\right) = v_{\mathcal{B}'}^T \left(P^T J P^\sigma\right) w_{\mathcal{B}'}^\sigma.$$

Pertanto $P^T J P^\sigma$ soddisfa (2.3), da cui $J' = P^T J P^\sigma$.
Viceversa, sia $J' = P^T J P^\sigma$, con $P \in \mathrm{GL}_n(\mathbb{K})$. Essendo P invertibile esiste una base $\mathcal{B}'$ di V tale che P è la matrice di passaggio da $\mathcal{B}$ a $\mathcal{B}'$. Per il punto precedente J' è la matrice della forma rispetto $\mathcal{B}'$. ■

(2.9) Definizione *Diremo che due matrici $J, J' \in \mathrm{Mat}_n(\mathbb{K})$ sono* congruenti *se esiste $P \in \mathrm{GL}_n(\mathbb{K})$ tale che $P^t J P = (J')^\sigma$.*

É facile verificare che la congruenza è una relazione di equivalenza.
Per il precedente lemma, se J è la matrice di una forma sesquilineare rispetto una data base di V, allora J' è congruente a J se e solo se è la matrice della stessa forma rispetto una conveniente base $\mathcal{B}'$.

3 Ortogonalità

In questo paragrafo consideriamo una forma $(\ ,\ ) : V \times V \to \mathbb{K}$ che sia bilineare simmetrica o antisimmetrica, oppure hermitiana.

(3.1) Definizione *Due vettori $u, w \in V$ si dicono* ortogonali *se $(u, w) = 0_{\mathbb{K}}$.*

In virtù dell'assioma $(w, u) = \pm(u, w)^\sigma$ l'ortogonalità fra vettori è simmetrica.

(3.2) Lemma *Per ogni sottoinsieme W di V il sottoinsieme $W^\perp$ dei vettori di V ortogonali a tutti i vettori di W è un sottospazio. Pertanto*

$$W^\perp := \{v \in V \mid (v, w) = 0, \ \forall \ w \in W\}$$

è detto il sottospazio ortogonale *a W.*

Dimostrazione.
• $0_V \in W^\perp$ poichè $(0_V, w) = 0$ per ogni $w \in W$.

• Siano $v_1, v_2 \in W^\perp$ e $\lambda_1, \lambda_2 \in \mathbb{K}$. Ne segue

$$(\lambda_1 v_1 + \lambda_2 v_2, w) = \lambda_1 (v_1, w) + \lambda_2 (v_2, w) = 0_\mathbb{K} + 0_\mathbb{K} = 0_\mathbb{K}, \quad \forall\, w \in W.$$

Si conclude che $\lambda_1 v_1 + \lambda_2 v_2 \in W^\perp$, che è pertanto un sottospazio. ■

(3.3) Definizione *Siano U, W due sottospazi di V. Scriviamo $V = U \perp W$ e diciamo che V è* somma ortogonale *di U e W se*

1) *$V = U \dot{+} W$ è somma diretta di U e W;*

2) *$U \leq W^\perp$, ossia $(u, w) = 0_\mathbb{K}$ per ogni $u \in U$, $w \in W$.*

Un sottospazio W si dice *totalmente isotropo* se $W \leq W^\perp$.

(3.4) Lemma *Supponiamo che la forma sia non degenere.*
Per ogni sottospazio W di V si ha:

$$\dim(W^\perp) = \dim(V) - \dim(W).$$

In particolare:

i) la dimensione di un sottospazio totalmente isotropo è $\leq \frac{1}{2} \dim V$;

ii) se la restrizione della forma a W è non degenere, si ha $V = W \perp W^\perp$.
Inoltre la restrizione della forma a $W^\perp$ è non degenere.

Dimostrazione. Sia $\{w_1, \ldots, w_m\}$ una base di W. Per ogni $v \in V$ si ha:

$$v \in W^\perp \iff (w_i, v) = 0_\mathbb{K},\ 1 \leq i \leq m. \tag{3.5}$$

Detta $\mathcal{B} = \{w_1, \ldots, w_m, w_{m+1}, \ldots, w_n\}$ una base di V che estende quella scelta per W, sia J la matrice della forma rispetto $\mathcal{B}$. Si ha allora:

$$v \in W^\perp \iff {e_i}^T J v_\mathcal{B}^\sigma = 0_\mathbb{K},\ 1 \leq i \leq m. \tag{3.6}$$

Ossia i vettori $v \in W^\perp$ sono quelli per cui $v_\mathcal{B}^\sigma$ è soluzione del sistema

$$\begin{cases} {e_1}^T J X = 0_\mathbb{K} \\ \ldots \\ {e_m}^T J X = 0_\mathbb{K}, \end{cases} \qquad X := (x_1, \ldots x_n)^T.$$

Si tratta di un sistema lineare omogeneo in m equazioni e $n = \dim V$ indeterminate. Essendo J non degenere, le sue righe (in particolare le prime m righe) sono indipendenti.

Ne segue che le equazioni del sistema sono indipendenti. Quindi le sue soluzioni formano un sottospazio di dimensione $n - m = \dim V - \dim W$.

i) Sia W totalmente isotropo. Da $W \leq W^\perp$ segue $\dim W^\perp \geq \dim W$. Quindi $\dim V - \dim W \geq \dim W$, da cui $\dim W \leq \frac{1}{2} \dim V$.

ii) Se la restrizione della forma a W è non degenere, allora $W \cap W^\perp = \{0_V\}$. Ne segue $\dim(W + W^\perp) = \dim W + \dim W^\perp = \dim V$, da cui $V = W \perp W^\perp$.
Infine sia u un vettore di $W^\perp$, ortogonale a tutti i vettori di $W^\perp$. Da $V = W \perp W^\perp$ segue che u è ortogonale a tutti i vettori di V. Quindi $u = 0_V$ perchè la forma considerata è non degenere. ■

(3.7) Teorema *Ogni sottospazio totalmente isotropo di V è contenuto in sottospazio totalmente isotropo massimale.*

Dimostrazione. Siano U, W sottospazi totalmente isotropi di V, con W di dimensione massima fra quelle dei sottospazi totalmente isotropi. Ogni applicazione lineare iniettiva $f : U \to W$ soddisfa l'ipotesi del Lemma di Witt, e può quindi essere estesa a un isometria $\widehat{f} : V \to V$. Ne segue $U \leq \widehat{f}^{-1}(W)$, con $\widehat{f}^{-1}(W)$ totalmente isotropo massimale. ■

4 Spazi simplettici

(4.1) Definizione *Uno spazio vettoriale V su $\mathbb{K}$ si dice* simplettico *se su di esso è definita una forma bilineare, non degenere, tale che ogni vettore $v \in V$ è isotropo, ossia*

$$(v, v) = 0_{\mathbb{K}}.$$

Scopo di questo paragrafo è dimostrare che esiste essenzialmente un unico spazio simplettico su $\mathbb{K}$ per ogni n pari.
Per la bilinearità, un prodotto simplettico è *antisimmetrico*. Infatti, per ogni $v, w \in \mathbb{K}^n$:

$$0 = (v + w, v + w) = (v, v) + (v, w) + (w, v) + (w, w) = (v, w) + (w, v).$$

Ne segue $(w, v) = -(v, w)$.

(4.2) Teorema *Sia V uno spazio simplettico su $\mathbb{K}$, di dimensione n.*

1) *$n = 2m$ è pari;*

2) *esiste una base $\mathcal{B}$ di V rispetto alla quale la forma ha matrice:*

$$J = \begin{pmatrix} \boldsymbol{0} & I_m \\ -I_m & \boldsymbol{0} \end{pmatrix}. \tag{4.3}$$

Dimostrazione. Induzione su n.
Se fosse $n = 1$, per qualunque base $\{v\}$ di V si avrebbe $(v, v) = 0_{\mathbb{K}}$, in contrasto con l'ipotesi che V è non degenere. Quindi $n \geq 2$.

Per la non-degenericità della forma, esistono $v_1, w \in V$ tali che $\lambda := (v_1, w) \neq 0_{\mathbb{K}}$.
In particolare v_1 e w sono linearmente indipendenti. Posto $w_1 := \lambda^{-1}w$, si ha:

$$(v_1, w_1) = \left(v_1, \lambda^{-1}w\right) = \lambda^{-1}(v_1, w) = 1_{\mathbb{K}}.$$

Se $n = 2$ abbiamo l'asserto. Infatti la matrice della forma rispetto $\mathcal{B} = \{v_1,\ w_1\}$ è

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Per $n > 2$, il sottospazio $W := \langle v_1, w_1 \rangle$ è non singolare. Ne segue

$$V = W\ \perp\ W^{\perp}.$$

$W^{\perp}$ è non degenere, quindi è uno spazio simplettico di dimensione $n-2$. Per induzione su n si ha $n-2 = 2(m-1)$ pari. Inoltre $W^{\perp}$ ammette una base $\{v_2,\ \ldots,\ v_m,\ w_2,\ \ldots,\ w_m\}$ rispetto alla quale la matrice della forma è del tipo di (4.3). Scegliendo

$$\mathcal{B} = \{v_1,\ \ldots,\ v_m,\ w_1,\ \ldots,\ w_m\}$$

si ha la tesi. ■

5 Spazi ortogonali e spazi unitari

Su un campo $\mathbb{K}$ di caratteristica 2, le forme bilineari simmetriche sono antisimmetriche. Per tale ragione, per studiare gli spazi ortogonali in caratteristica 2, è necessario introdurre e classificare le forme quadratiche. Siccome qui non le trattiamo, per gli spazi ortogonali ci limitiamo al caso di caratteristica $\neq 2$.

(5.1) Definizione *Sia V uno spazio vettoriale su un campo $\mathbb{K}$.*

• *V si dice uno spazio* ortogonale *se $\mathbb{K}$ ha caratteristica $\neq 2$ ed è definita una forma bilineare simmetrica, non degenere $(\ ,\ ) : V \times V \to \mathbb{K}$.*

• *V si dice uno spazio* unitario *se $\mathbb{K}$ che ha un automorfismo di periodo 2 ed è definita una forma hermitiana, non degenere $(\ ,\ ) : V \times V \to \mathbb{K}$.*

(5.2) Definizione *Sia V uno spazio ortogonale o hermitiano e sia $\mathcal{B} = \{v_1, \ \ldots, \ v_n\}$ una sua base.*

• *$\mathcal{B}$ si dice* ortogonale *se $(v_i, v_j) = 0$ per ogni $i \neq j$.*

• *$\mathcal{B}$ si dice* ortonormale *se è ortogonale e $(v_i, v_i) = 1$ per ogni i.*

Equivalentemente $\mathcal{B}$ è una base ortogonale se la matrice della forma rispetto $\mathcal{B}$ è diagonale. $\mathcal{B}$ è una base ortonormale se la matrice della forma rispetto $\mathcal{B}$ è quella identica.

(5.3) Teorema *Sia V uno spazio ortogonale o hermitiano su $\mathbb{K}$. Nel caso in cui V è ortogonale si supponga* $\operatorname{char} \mathbb{K} \neq 2$. *Allora V ha una base ortogonale.*

Dimostrazione. Basta dimostrare che esiste $v \in V$ tale che $(v, v) \neq 0_{\mathbb{K}}$. Infatti, in tal caso, il sottospazio $\langle v \rangle$ è non-degenere. Ne segue

$$V = \langle v \rangle \perp \langle v \rangle^{\perp}.$$

Poichhè $\langle v \rangle^{\perp}$ ha dimensione $n-1$ possiamo supporre, per induzione su n, che abbia una base ortogonale $\overline{\mathcal{B}}$. Pertanto $\{v\} \cup \overline{\mathcal{B}}$ è una base ortogonale di V.

Resta da dimostrare l'esistenza di $v \in V$ tale che $(v, v) \neq 0_{\mathbb{K}}$.

Per la non-degenericità della forma, esistono $u, w \in V$ tali che $\lambda := (u, w) \neq 0_{\mathbb{K}}$.
Se $(u, u) \neq 0_{\mathbb{K}}$ oppure $(w, w) \neq 0_{\mathbb{K}}$ siamo a posto. Quindi possiamo supporre

$$(u, u) = (w, w) = 0.$$

Se $\operatorname{char} \mathbb{K} \neq 2$, ponendo $v = \lambda^{-1} u + w$ si ha:

$$(v, v) = \lambda^{-1}(u, w) + \left(\lambda^{-1}\right)^{\sigma} (w, u) = \lambda^{-1}\lambda + (\lambda^{\sigma})^{-1} \lambda^{\sigma} = 21_{\mathbb{K}} \neq 0_{\mathbb{K}}.$$

Se $\operatorname{char} \mathbb{K} = 2$, allora V è unitario. Poichè l'automorfismo σ di $\mathbb{K}$ che definisce la forma hermitiana non è $\mathrm{id}_{\mathbb{K}}$, esiste $\alpha \in \mathbb{K}$ tale che $\alpha^{\sigma} \neq \alpha$. Scegliendo $v = \lambda^{-1}\alpha u + w$ si ha

$$(v, v) = \alpha + \alpha^{\sigma} = \alpha - \alpha^{\sigma} \neq 0_{\mathbb{K}}.$$

■

(5.4) Osservazione *Se $\mathbb{K}$ ha caratteristica 2, una forma bilineare simmetrica può non ammettere basi ortogonali. Ad esempio, per $n = 2\ell$, consideriamo la forma bilineare indotta dalla matrice $\begin{pmatrix} 0 & I_\ell \\ I_\ell & 0 \end{pmatrix}$ rispetto alla base canonica di $\mathbb{K}^n$. Tale forma è non degenere (e definisce uno spazio simplettico in caratteristica 2), ma non ammette basi ortogonali dato che tutti i vettori sono isotropi.*

(5.5) Corollario

1) *Uno spazio ortogonale V su $\mathbb{C}$ ha una base ortonormale;*

2) *uno spazio hermitiano V su $\mathbb{C}$ (rispetto all'automorfismo coniugio σ di $\mathbb{C}$), tale che $(v, v) > 0$ per ogni $v \neq 0_V$, ha una base ortonormale;*

3) *uno spazio ortogonale V su $\mathbb{R}$, tale che $(v, v) > 0$ per ogni $v \neq 0_V$ in V, ha una base ortonormale.*

Dimostrazione.
Per il Teorema 5.3 esiste una base ortogonale $\mathcal{B} = \{v_1, \ldots, v_n\}$ di V. Poniamo

$$(v_i, v_i) := \lambda_i, \quad 1 \leq i \leq n.$$

1) Per ogni $i \leq n$ esiste $\mu_i \in \mathbb{C}$ tale che $\mu_i^2 = \lambda_i^{-1}$. Una base ortonormale è quindi:

$$\mathcal{B}' = \left\{\mu_1^{-1} v_1, \ldots, \mu_n^{-1} v_n\right\}.$$

2) e 3) Nel punto 2) notiamo che la condizione $(v, v) = (v, v)^\sigma$ implica $(v, v) \in \mathbb{R}$ per ogni $v \in V$. Ha quindi senso la condizione $(v, v) > 0$.
Per ipotesi ogni λ_i è un reale positivo. Esiste quindi $\mu_i \in \mathbb{R}$ tale che $\mu_i^2 = \lambda_i^{-1}$ per ogni $i \leq n$. Definendo $\mathcal{B}'$ come nel caso precedente si ottiene una base ortonormale. ∎

(5.6) Osservazione *Dal Teorema 5.3 segue facilmente che uno spazio ortogonale V, di dimensione n su $\mathbb{R}$, ha una base ortogonale rispetto alla quale la forma ha matrice*

$$D = \operatorname{diag}\left(\underbrace{1, \ldots, 1}_{h}, \underbrace{-1, \ldots, -1}_{n-h}\right)$$

per qualche h tale che $0 \leq h \leq n$. Per il Teorema di Sylvester [5, Cap. VIII, & 6, pag 165] due matrici D e D' di questo tipo sono congruenti solo se hanno lo stesso numero di componenti uguali a 1.

Come si intuisce dai casi fin qui considerati, la classificazione delle forme bilineari simmetriche e hermitiane dipende essenzialmente dal campo $\mathbb{K}$. Nel caso dei campi finiti si riesce a dare una classificazione completa, come vedremo nell'ultimo paragrafo di questo capitolo.

6 Alcune proprietà dei campi finiti

Per la classificazione delle forme bilineari e simmetriche sui campi finti avremo bisogno delle proprietà espresse dal seguente Lemma.

(6.1) Lemma *Siano $\mathbb{K}$ un campo finito e $X := \{\alpha^2 \mid \alpha \in \mathbb{K}\}$ l'insieme dei quadrati.*

1) *Se l'ordine di $\mathbb{K}$ è pari, allora $X = \mathbb{K}$;*

2) *se l'ordine di $\mathbb{K}$ è è dispari, allora $\mathbb{K} \setminus X \neq \emptyset$. Inoltre fissato $\epsilon \in \mathbb{K} \setminus X$ si ha:*

$$\mathbb{K} = X \cup X\epsilon = \{0\} \dot\cup \{\alpha^2 \mid \alpha \in \mathbb{K}^*\} \dot\cup \{\alpha^2\epsilon \mid \alpha \in \mathbb{K}^*\};$$

3) *ogni elemento di $\mathbb{K}$ è somma di due quadrati;*

4) *Se $|\mathbb{K}| = q^2$ è un quadrato, per ogni $\lambda \in \mathbb{F}_q$ (sottocampo di $\mathbb{K}$ di ordine q), l' equazione*

$$x^{q+1} = \lambda$$

ha $q+1$ radici in $\mathbb{K}$.

Dimostrazione.
1) Posto $|\mathbb{K}| = 2^a$, il monomorfismo di Frobenius $\varphi : \mathbb{K} \to \mathbb{K}$ definito ponendo $\varphi(\alpha) = \alpha^2$ per ogni $\alpha \in \mathbb{K}$, è una bijezione di $\mathbb{K}$ in sè . Quindi $X = \mathrm{Im}\varphi = \mathbb{K}$.

2) L'applicazione $\varphi : \mathbb{K}^* \to \mathbb{K}^*$, definita ponendo $\varphi(\alpha) = \alpha^2$ per ogni $\alpha \in \mathbb{K}^*$, è un omomorfismo di gruppi moltiplicativi. $\mathrm{Ker}\varphi = \{\alpha \mid \alpha^2 = 1\} = \{1, -1\}$ ha ordine 2.
Per il Teorema degli omomorfismi fra gruppi

$$\frac{\mathbb{K}^*}{\mathrm{Ker}\varphi} \simeq \mathrm{Im}\varphi.$$

Posto $|\mathbb{K}| = q$, si deduce $\frac{q-1}{2} = |\mathrm{Im}\varphi|$. Notando che $X = \{0\} \cup \mathrm{Im}\varphi$, si conclude

$$|X| = 1 + \frac{q-1}{2} = \frac{q+1}{2} < q.$$

Infine $\epsilon \notin \mathrm{Im}\varphi$ essendo un non-quadrato. Ne segue $\mathrm{Im}\varphi \cap (\mathrm{Im}\varphi)\,\epsilon = \emptyset$.

Poichè $|(\mathrm{Im}\varphi)\,\epsilon| = |\mathrm{Im}\varphi| = \frac{q-1}{2}$ si conclude

$$\mathbb{K}^* = \mathrm{Im}\varphi \,\dot\cup\, (\mathrm{Im}\varphi)\,\epsilon = \left\{\alpha^2 \mid \alpha \in \mathbb{K}^*\right\} \dot\cup \left\{\alpha^2\epsilon \mid \alpha \in \mathbb{K}^*\right\}.$$

3) Se $|\mathbb{K}| = 2^a$, ogni $\beta \in \mathbb{K}$ è un quadrato per il punto 1). Ne segue $\beta = \alpha^2 + 0^2$ per un opportuno $\beta \in \mathbb{K}$. Se $|\mathbb{K}| = q$ dispari, fissato $\beta \in \mathbb{K}$, consideriamo l'applicazione

$$t_\beta : X \to \mathbb{K} \quad \text{tale che} \quad x \mapsto \beta - x,\ \forall\ x \in X.$$

Essa è iniettiva, quindi $|t_\beta(X)| = |X| = \frac{q+1}{2}$. Ne segue $|X| + |t_\beta(X)| = q + 1$ da cui

$$X \cap t_\beta(X) \neq \emptyset.$$

Sia $\rho \in X \cap t_\beta(X)$. Da $\rho \in X$ segue $\rho = \alpha^2$ per qualche $\alpha \in \mathbb{K}$. Da $\rho \in t_\beta(X)$ segue $\rho = \beta - \gamma^2$ per qualche $\gamma \in \mathbb{K}$. Si conclude $\beta = \alpha^2 + \gamma^2$.

4) $\mathbb{F}_{q^2}$ contiene $\mathbb{F}_q$. Per ogni $\alpha \in \mathbb{F}_{q^2}$ si ha $\alpha\alpha^q \in \mathbb{F}_q$. Infatti $(\alpha\alpha^q)^q = \alpha^q\alpha^{q^2} = \alpha\alpha^q$. Possiamo quindi considerare l'omomorfismo $\tau : \mathbb{F}^*_{q^2} \to \mathbb{F}^*_q$ tale che

$$\alpha \mapsto \alpha\alpha^q,\ \forall\ \alpha \in \mathbb{F}^*_{q^2}.$$

$\mathrm{Ker}\,\tau = \left\{\alpha \mid \alpha^{q+1} = 1\right\}$ ha ordine $k \leq q+1$. Dal teorema degli omomorfismi fra gruppi segue $|\mathrm{Im}\,\tau| = \frac{q^2-1}{k} \geq q-1$. Poichè il codominio di τ ha ordine $q-1$ si conclude che $\mathrm{Ker}\,\tau$ ha ordine $q+1$ e che $\mathrm{Im}\,\tau$ ha ordine $q-1$, ossia τ è suriettiva.
Infine, detta $\overline{\lambda}$ una preimmagine di λ, per ogni $t \in \mathrm{Ker}\,\tau$ si ha $(t\overline{\lambda})^{q+1} = \tau(t\overline{\lambda}) = \lambda$. Pertanto i $q+1$ elementi $t\overline{\lambda}$, $t \in \mathrm{Ker}\,\tau$, sono le radici di $x^{q+1} = \lambda$. ∎

7 Spazi ortogonali e unitari sui campi finiti

In questo paragrafo supponiamo $\mathbb{K} = \mathbb{F}_q$ finito e descriviamo la classificazione completa degli spazi ortogonali e unitari su $\mathbb{F}_q$. Vedremo che, per ogni dimensione n fissata, esistono due spazi ortogonali non isometrici e un unico spazio hermitiano.

(7.1) Lemma *Sia V uno spazio ortogonale di dimensione $n \in \{2,3\}$ su $\mathbb{K}$, con $|\mathbb{K}| = q$ dispari, e sia ϵ un prefissato non-quadrato in $\mathbb{K}$.*

1) *Se $n = 2$ e V ha un vettore isotropo non nullo, esiste una base rispetto alla quale la matrice della forma è* $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;

2) *se $n = 2$ e V non ha vettori isotropi non nulli, esiste una base rispetto alla quale la matrice della forma è* $\begin{pmatrix} 1 & 0 \\ 0 & -\epsilon \end{pmatrix}$;

3) *se $n = 3$, per ogni $\lambda \in \mathbb{K}$ esiste $v \in V$, non nullo, tale che $(v, v) = \lambda$. In particolare in V ci sono vettori isotropi non nulli.*

Dimostrazione.

1) Sia v_1 un vettore isotropo non nullo di V. Poichè la forma è non-degenere, esiste $w \in V$ tale che $(v_1, w) \neq 0_{\mathbb{K}}$. In particolare v_1 e w sono linearmente indipendenti. Ponendo $w_1 := (v_1, w)^{-1} w$ si ha $(v_1, w_1) = 1_{\mathbb{K}}$. Sia $(w_1, w_1) = \alpha$. Definendo $v_2 := -\frac{\alpha}{2} v_1 + w_1$ si ottiene una base $\{v_1, v_2\}$ di V rispetto alla quale la matrice della forma è quella voluta.

2) Per il Teorema 5.3, esiste una base $\{w_1, w_2\}$ di V rispetto alla quale la forma ha matrice diagonale $\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$. Per il punto 2) del Lemma 6.1, possiamo supporre $\alpha = \alpha_1^2 \epsilon^i$, $-\beta = \beta_1^2 \epsilon^j$ con $i, j \in \{0, 1\}$. Quindi, rispetto alla base $\mathcal{B} = \left\{\alpha_1^{-1} w_1, \beta_1^{-1} w_2\right\}$ la matrice della forma è

$$\begin{pmatrix} \epsilon^i & 0 \\ 0 & -\epsilon^j \end{pmatrix}, \quad i, j \in \{0, 1\}.$$

Se fosse $i = j$ il vettore $e_1 + e_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ sarebbe isotropo. Scambiando eventualmente w_1 con w_2 possiamo pertanto supporre $i = 0$, $j = 1$, da cui l'asserto.

3) Sia $\mathcal{B}$ una base di V rispetto alla quale la forma ha matrice diagonale J. Almeno due degli elementi della diagonale principale di J sono entrambi dei quadrati o entrambi dei non quadrati. Pertanto, a meno di moltiplicazioni dei vettori della base per ϵ e di un loro riordinamento, possiamo supporre $J = \mathrm{diag}(\alpha, \alpha, \beta)$. Siano $x, y \in \mathbb{K}$ tali che

$$x^2 + y^2 = \frac{\lambda - \beta}{\alpha}.$$

Detto v il vettore di V tale che $v_{\mathcal{B}} = (x, y, 1)^T$ si ha $v \neq 0_V$ e $(v, v) = \lambda$.

■

(7.2) Teorema *Sia V uno spazio ortogonale o Hermitiano di dimensione $n \geq 2$ su un campo finito $\mathbb{K}$ di ordine q. Supponiamo inltre che ϵ sia un non-quadrato in $\mathbb{K}$.*

1) *se q è dispari e V è ortogonale, allora esiste una base rispetto alla quale la forma ha una delle seguenti matrici:*

$$J_1 = \begin{pmatrix} \boldsymbol{0} & I_m \\ I_m & \boldsymbol{0} \end{pmatrix}, \quad J_2 = \begin{pmatrix} \boldsymbol{0} & I_{m-1} & & \\ I_{m-1} & \boldsymbol{0} & & \\ & & 1 & 0 \\ & & 0 & -\epsilon \end{pmatrix}, \quad \text{se } n = 2m; \tag{7.3}$$

$$(7.4) \qquad K_1 = \begin{pmatrix} 1 & & \\ & \boldsymbol{0} & I_m \\ & I_m & \boldsymbol{0} \end{pmatrix}, \quad K_2 = \epsilon \begin{pmatrix} 1 & & \\ & \boldsymbol{0} & I_m \\ & I_m & \boldsymbol{0} \end{pmatrix}, \quad \text{se } n = 2m+1.$$

Le matrici J_1 e J_2 non sono congruenti. Analogamente K_1 e K_2 non sono congruenti.

2) *Se V è Hermitiano, esiste una base ortonormale di V.*

Dimostrazione.

1) Supponiamo $n = 2m$ e ragioniamo per induzione su m.

Il caso $m = 1$ è dimostrato nel Lemma 7.1. Supponiamo quindi $m \geq 2$ e consideriamo una base ortogonale $\{v_1, \ldots, v_n\}$ di V. Il sottospazio $\langle v_1, v_2, v_3 \rangle$ è non-degenere. Per il punto 3) del Lemma 7.1 ha un vettore isotropo non nullo w. Inoltre ha un vettore u tale che $(w, u) \neq 0$. Dal punto 1) dello stesso Lemma segue che il sottospazio non singolare $W = \langle w, u \rangle$ ammette una base $\{w_1, w_2\}$ tale che $(w_1, w_1) = (w_2, w_2) = 0$, $(w_1, w_2) = 1$. Consideriamo la decomposizione ortogonale

$$V = W \perp W^{\perp}.$$

Applicando l'ipotesi induttiva a $W^{\perp}$, che ha dimensione $n-2$, concludiamo che esiste una base di V rispetto alla quale la forma ha matrice una delle seguenti:

$$\begin{pmatrix} 0 & 1 & & & \\ 1 & 0 & & & \\ & & 0 & I_{m-2} & \\ & & I_{m-2} & 0 & \end{pmatrix} \equiv J_1, \quad \begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & I_{m-3} & & \\ & & I_{m-3} & 0 & & \\ & & & & 1 & 0 \\ & & & & 0 & -\epsilon \end{pmatrix} \equiv J_2.$$

La dimensione di un sottospazio totalmente isotropo massimale relativamente a J_1 è m. Infatti il sottospazio generato dai primi m vettori della base è totalmente isotropo. D'altra parte, per il punto i) del Lemma 3.4, un sottospazio totalmente isotropo non può avere dimensione superiore a $m = \frac{n}{2}$.

Invece la dimensione di un sottospazio totalmente isotropo massimale relativamente a J_2 è $m-1$. Infatti il sottospazio W, generato dai primi $m-1$ vettori della base, è totalmente isotropo. Se non fosse massimale, per il Lemma 3.7 sarebbe contenuto in un sottospazio isotropo massimale U, necessariamente contenuto in $W^{\perp}$. Ma $W^{\perp}$ ha dimensione $n-(m-1) = m+1$ e coincide quindi con il sottospazio generato da W e dagli ultimi due vettori della base. Un calcolo diretto mostra che W è isotropo massimale in $W^{\perp}$. Si conclude che J_1 non è congruente a J_2.

Supponiamo ora $n = 2m + 1$ e ragioniamo per induzione su n.
Se $n = 1$ l'asserto è ovvio. Se $n \geq 3$, esiste $v \in V$ tale che $(v, v) = 1$. Quindi

$$V = \langle v \rangle \perp \langle v \rangle^{\perp}.$$

La restrizione della forma al sottospazio di dimensione $2m$ deve avere matrice (rispetto a una data base) congruente a una delle due precedenti. Pertanto vi sono, al massimo, due matrici simmetriche non congruenti in $\mathrm{GL}_{2m+1}(\mathbb{K})$. D'altra parte K_1 e K_2 non sono congruenti. Infatti, se lo fossero, esisterebbe P non singolare tale che

$$P^T K_1 P = K_2 = \epsilon\, K_1$$

da cui

$$(\det P)^2 \det K_1 = \epsilon \det K_1.$$

In tal caso ϵ sarebbe un quadrato, contraddizione.

2) Se $\mathbb{K} = \mathbb{F}_q^2$ e V è Hermitiano, sappiamo che esiste una base ortogonale $\{v_1, \ldots, v_n\}$ di V, ossia una base rispetto alla quale la forma ha matrice diagonale

$$\mathrm{diag}(\lambda_1, \ldots, \lambda_n), \quad \lambda_i = \lambda_i^{\sigma} = \lambda_i^q, \quad 1 \leq i \leq n.$$

Per il punto 4) del Lemma 6.1, per ogni $i \leq n$ esiste $\mu_i \in \mathbb{F}_{q^2}$ tale che

$$\mu_i{}^{q+1} = \lambda_i^{-1}.$$

Ne segue che la base

$$\mathcal{B} := \{\mu_1 v_1, \ldots, \mu_n v_n\}$$

è ortonormale. ■

Capitolo II

I gruppi classici

Per la descrizione dei gruppi di matrici ci siamo basati sul libro di Carter [2].

1 Il gruppo generale lineare

Siano $\mathbb{K}$ un campo e n un numero naturale ≥ 1.

(1.1) Definizione *Il gruppo delle matrici $n \times n$, a elementi in $\mathbb{K}$, con determinante $\neq 0$, si dice* gruppo generale lineare *di rango n su $\mathbb{K}$, e si indica con* $\mathrm{GL}_n(\mathbb{K})$.

Per il Teorema di Binet, l'applicazione

$$\delta : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$$

tale che $A \mapsto \det A$, è un epimorfismo di gruppi moltiplicativi. Il nucleo di δ è costituito dal *gruppo speciale lineare* $\mathrm{SL}_n(\mathbb{K})$ delle matrici di determinante 1. $\mathrm{SL}_n(\mathbb{K})$ è quindi un sottogruppo normale di $\mathrm{GL}_n(\mathbb{K})$. Inoltre, dal teorema degli omomorfismi segue che

$$\frac{\mathrm{GL}_n(\mathbb{K})}{\mathrm{SL}_n(\mathbb{K})} \sim \mathbb{K}^*.$$

Indichiamo con Z il centro di $\mathrm{GL}_n(\mathbb{K})$, cioè l'insieme degli elementi che commutano con tutti gli altri. Esso risulta essere l'insieme delle matrici scalari λI con $\lambda \in \mathbb{K}^*$.

(1.2) Definizione

- *Si dice* gruppo proiettivo generale lineare *il quoziente*

$$\frac{\mathrm{GL}_n(\mathbb{K})}{Z} := \mathrm{PGL}_n(\mathbb{K}).$$

- *Si dice* gruppo proiettivo speciale lineare *il quoziente*

$$\frac{\mathrm{SL}_n(\mathbb{K})}{Z \cap \mathrm{SL}_n(\mathbb{K})} := \mathrm{PSL}_n(\mathbb{K}).$$

Se $\mathbb{K}$ è finito e ha ordine q tali gruppi si indicano rispettivamente con

$$\mathrm{GL}_n(q),\ \mathrm{SL}_n(q),\ \mathrm{PGL}_n(q),\ \mathrm{PSL}_n(q).$$

Sia data una forma bilineare o Hermitiana, rispetto un automorfismo σ di $\mathbb{K}$:

$$(\ ,\ ) : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}. \tag{1.3}$$

Ricordiamo che un'*isometria* di (1.3) è un elemento $g \in \mathrm{GL}_n(\mathbb{K})$ tale che

$$(gv, gw) = (v, w), \quad \forall\ v, w \in \mathbb{K}^n.$$

Sia J la matrice di (1.3) rispetto alla base canonica $\mathcal{B}$ di $\mathbb{K}^n$. Poichè ogni vettore $v \in \mathbb{K}^n$ coincide con il proprio vettore coordinate $v_{\mathcal{B}}$ si ha:

$$(v, w) = v^T J w^\sigma, \quad \forall\ v, w \in V.$$

Ne segue che un elemento g di $\mathrm{GL}_n(\mathbb{K})$ è una isometria se e solo se

$$v^T J w^\sigma = (gv)^T J (gw)^\sigma = v^T (g^T J g^\sigma) w^\sigma, \quad \forall\ v, w \in \mathbb{K}^n$$

se e solo se (applicando la precedente condizione ai vettori della base canonica):

$$g^T J g^\sigma = J.$$

(1.4) Lemma

1) *L'insieme H delle isometrie di* (1.3) *è un sottogruppo di* $\mathrm{GL}_n(\mathbb{K})$.

2) *Per ogni matrice invertibile P, il coniugato $P^{-1}HP$ è il gruppo delle isometrie del prodotto scalare la cui matrice, rispetto alla base canonica, è*

$$J' = P^T J P^\sigma.$$

Dimostrazione. Per quanto sopra osservato si ha:

$$H := \left\{ h \in \mathrm{GL}_n(\mathbb{K}) \mid h^T J h^\sigma = J \right\}.$$

1) $I \in H$. Se $x, y \in H$, allora

$$(xy)^T J (xy)^\sigma = y^T (x^T J x^\sigma) y^\sigma = y^T J y^\sigma = J,$$

da cui $xy \in H$. Inoltre $x^{-1} \in H$. Infatti, da $x^T J x^\sigma = J$ segue

$$(x^T)^{-1} x^T J x^\sigma x^{-\sigma} = (x^T)^{-1} J x^{-\sigma},$$

ossia $J = (x^{-1})^T J \left(x^{-1}\right)^\sigma$.

2) Per ogni $h \in H$, si ha: $(P^{-1}hP)^T J' (P^- hP)^\sigma = J'$ se e solo se $h^T J h^\sigma = J$. ■

(1.5) Osservazione *È importante osservare che due gruppi coniugati H e $P^{-1}HP$ sono isomorfi, tramite l'isomorfismo $h \mapsto P^{-1}hP$. Pertanto, se $\mathcal{B}$ e $\mathcal{B}'$ sono due basi di $\mathbb{K}^n$, e J, J' le corrispondenti matrici di una stessa forma, i relativi gruppi di isometrie sono in generale diversi, ma hanno la stessa struttura, essendo isomorfi.*

2 Il gruppo simplettico

(2.1) Definizione *Il gruppo delle isometrie di uno spazio simplettico si dice* gruppo simplettico *e si indica con* $\mathrm{Sp}_n(\mathbb{K})$.

Per quanto visto nel capitolo precedente, uno spazio simplettico ha dimensione pari $n = 2\ell$ e ammette una base rispetto alla quale il prodotto ha matrice

$$J = \begin{pmatrix} \mathbf{0} & I_\ell \\ -I_\ell & \mathbf{0} \end{pmatrix}.$$

Pertanto, a meno di coniugio, si può supporre

$$\mathrm{Sp}_{2\ell}(\mathbb{K}) = \left\{ g \in \mathrm{GL}_{2\ell}(\mathbb{K}) \mid g^t J g = J \right\}.$$

Notiamo che $\langle e_1, \ldots, e_\ell \rangle$, è un sottospazio totalmente isotropo massimale.
Si dimostra che tutti gli elementi di $\mathrm{Sp}_{2\ell}(\mathbb{K})$ hanno determinante 1.
Inoltre il centro di $\mathrm{Sp}_{2\ell}(\mathbb{K})$ è il sottogruppo generato da $-I$.

(2.2) Definizione *Si definisce* gruppo proiettivo simplettico *il gruppo quoziente:*

$$\frac{\mathrm{Sp}_{2\ell}(\mathbb{K})}{\langle -I \rangle} := \mathrm{PSp}_{2\ell}(\mathbb{K}).$$

Se $\mathbb{K}$ è finito, di ordine q, tali gruppi si indicano rispettivamente con

$$\mathrm{Sp}_{2\ell}(q),\ \mathrm{PSp}_{2\ell}(q).$$

3 I gruppi ortogonali in caratteristica $\neq 2$.

(3.1) Definizione *Supponiamo che $\mathbb{K}$ abbia caratteristica diversa da 2. Il gruppo delle isometrie di uno spazio ortogonale su $\mathbb{K}$ si dice* gruppo ortogonale

In generale, essendoci spazi ortogonali non isometrici, vi sono più gruppi ortogonali. Nel caso in cui $\mathbb{K}$ è finito, di ordine q, per quanto visto nel capitolo precedente esistono due spazi ortogonali non isometrici, definiti dalle seguenti matrici, in cui $\langle\epsilon\rangle = \mathbb{K}^*$.

Se $n = 2\ell$:

$$J_1 = \begin{pmatrix} \mathbf{0} & I_\ell \\ I_\ell & \mathbf{0} \end{pmatrix}, \quad J_2 = \begin{pmatrix} \mathbf{0} & I_{\ell-1} & & \\ I_{\ell-1} & \mathbf{0} & & \\ & & 1 & \\ & & & -\epsilon \end{pmatrix}.$$

Se $n = 2\ell + 1$:

$$K_1 = \begin{pmatrix} 1 & & & \\ & \mathbf{0} & I_\ell \\ & I_\ell & \mathbf{0} \end{pmatrix}, \quad K_2 = \epsilon K_1.$$

(3.2) Definizione *Nel caso $|\mathbb{K}| = q$, dispari, le notazioni per i gruppi ortogonali:*

- $\mathrm{O}^+_{2\ell}(q) = \left\{h \in \mathrm{GL}_{2\ell}(q) \mid h^T J_1 g = J_1\right\}$;
- $\mathrm{O}^-_{2\ell}(q) = \left\{h \in \mathrm{GL}_{2\ell}(q) \mid h^T J_2 g = J_2\right\}$;
- $\mathrm{O}^+_{2\ell+1}(q) = \left\{h \in \mathrm{GL}_{2\ell+1}(q) \mid h^T K_1 g = K_1\right\}$.

Notiamo che, in dimensione dispari, nonostante vi siano due spazi ortogonali non isometrici, i relativi gruppi di isometrie coincidono. Infatti, essendo K_2 multipla di K_1, si ha:

$$h^T K_2 g = K_2 \iff h^T \epsilon K_1 g = \epsilon K_1 \Leftrightarrow h^T K_1 g = K_1.$$

Tutti questi gruppi sono costituiti da matrici di determinante ± 1. Le loro intersezioni con il gruppo speciale lineare si indicano rispettivamente con

- $\mathrm{SO}^+_{2\ell}(q)$;
- $\mathrm{SO}^-_{2\ell}(q)$;
- $\mathrm{SO}_{2\ell+1}(q)$.

(3.3) Definizione *Si chiama* sottogruppo derivato *di un gruppo G e si indica con G' il sottogruppo generato dai commutatori, ossia:*

$$G' := \left\langle x^{-1}y^{-1}xy \mid x, y \in G \right\rangle.$$

Segue da tale definizione che il sottogruppo derivato di un qualunque gruppo di matrici è costituito da matrici di determinante 1, ossia che

$$\mathrm{GL}_n(\mathbb{K})' \leq \mathrm{SL}_n(\mathbb{K}).$$

In realtà $\mathrm{GL}_n(\mathbb{K})' = \mathrm{SL}_n(\mathbb{K})$, con l'unica eccezione di $\mathrm{GL}_2(2)$.
I sottogruppi derivati dei gruppi ortogonali i loro gruppi quozienti rispetto al centro (le cui matrici appartengono a $\{\pm I\}$) si indicano rispettivamente con

- $\Omega^+_{2\ell}(\mathbb{K})$, $P\Omega^+_{2\ell}(\mathbb{K})$;
- $\Omega^-_{2\ell}(\mathbb{K})$, $P\Omega^-_{2\ell}(\mathbb{K})$;
- $\Omega_{2\ell+1}(\mathbb{K})$, $P\Omega^-_{2\ell}(\mathbb{K})$.

4 I gruppi unitari.

(4.1) Definizione *Supponiamo che* $\mathbb{K}$ *abbia un automorfismo* σ *di periodo* 2. *Il gruppo delle isometrie di uno spazio hermitiano* V*, di dimensione* n *su* $\mathbb{K}$*, si dice* gruppo unitario *e si indica con* $\mathrm{U}_n(\mathbb{K})$. *Si definisce inoltre*

$$\mathrm{SU}_n(\mathbb{K}) := \mathrm{U}_n(\mathbb{K}) \cap \mathrm{SL}_n(\mathbb{K}).$$

Il centro Z di $\mathrm{SU}_n(\mathbb{K})$ è costituito da matrici scalari. Il gruppo quoziente rispetto a Z

$$\mathrm{PSU}_n(\mathbb{K}) := \frac{\mathrm{SU}_n(\mathbb{K})}{Z}$$

si dice il gruppo unitario speciale proiettivo.
Se V ha una base ortonormale (ad esempio nel caso in cui $\mathbb{K}$ è finito di ordine q^2), a meno di coniugio, si può supporre

$$\mathrm{GU}_n(\mathbb{K}) = \left\{ g \in \mathrm{GL}_{2\ell}(\mathbb{K}) \mid g^T g^\sigma = I \right\}$$

dove g^σ si ottiene da g applicando l'automorfismo σ a tutti i suoi elementi.
Se $\mathbb{K}$ è finito e ha ordine q^2 tali gruppi si indicano rispettivamente con

$$\mathrm{U}_n(q^2),\ \mathrm{SU}_n(q^2),\ \mathrm{PSU}_n(q^2).$$

5 I gruppi semplici

(5.1) Definizione *Un gruppo* G *si dice* semplice *se* $G \neq \{1\}$ *e i suoi unici sottogruppi normali sono* $\{1\}$ *e* G.

La classificazione dei gruppi semplici finiti è ritenuta completa. Essi si suddividono in molte classi, delle quali siamo in grado di elencare le seguenti.

• Per ogni primo p il gruppo C_p di ordine p;

• per ogni $n \neq 5$ il gruppo alterno $\mathrm{Alt}(n)$;

• i gruppi classici:

$\mathrm{PSL}_n(q)$ con $n \geq 2$, tranne nei casi $n = 2$ e $q = 2, 3$;

$\mathrm{PSp}_{2\ell}(q)$, tranne nei casi $\ell = 1$ e $q = 2, 3$, $\ell = 2$ e $q = 2$;

$P\Omega_{2\ell+1}(q)$ per $\ell \geq 2$,

$P\Omega^+_{2\ell}(q)$, $P\Omega^-_{2\ell}(q)$, per $\ell \geq 3$;

$\mathrm{PSU}_n(q^2)$ con $n \geq 2$ tranne nei casi $n = 2$ e $q = 2, 3$, $n = 3$ e $q = 2$.

Gli ordini dei gruppi classici sono riportati nella seguente tabella:

$$
\begin{array}{rcl}
|\mathrm{PSL}_n(q)| & = & \frac{1}{(n,q-1)}\, q^{\frac{n(n-1)}{2}}(q^2-1)\cdots(q^n-1) \\
|\mathrm{PSp}_{2\ell}(q)| & = & \frac{1}{(2,q-1)}\, q^{\ell^2}(q^2-1)(q^4-1)\cdots(q^{2\ell}-1) \\
|P\Omega_{2\ell+1}(q)| & = & \frac{1}{(2,q-1)}\, q^{\ell^2}(q^2-1)(q^4-1)\cdots(q^{2\ell}-1) \\
\left|P\Omega^+_{2\ell}(q)\right| & = & \frac{1}{(4,q^\ell-1)}\, q^{\ell(\ell-1)}(q^2-1)(q^4-1)\cdots(q^{2\ell-2}-1)(q^\ell-1) \\
\left|P\Omega^-_{2\ell}(q)\right| & = & \frac{1}{(4,q^\ell-1)}\, q^{\ell(\ell-1)}(q^2-1)(q^4-1)\cdots(q^{2\ell-2}-1)(q^\ell+1) \\
\left|\mathrm{PSU}_n(q^2)\right| & = & \frac{1}{(n,q+1)}\, q^{\frac{n(n-1)}{2}}(q^2-1)(q^3+1)(q^4-1)\cdots(q^n-(-1)^n)
\end{array}
$$

Bibliografia

[1] M.Aschbacher, Finite group theory, Cambridge University Press, 1986.

[2] R.W.Carter, Simple groups of Lie type, John Wiley and sons (1972).

[3] L.Dickson, Linear Groups, Dover Publications, Inc. (1958).

[4] N.Jacobson, Basic Algebra I, W.H.Freeman and company, San Francisco,1974.

[5] S.Lang, Linear Algebra, Addison-Wesley Publishing Company.

[6] M.C. Tamburini, Algebra I unità , Dispensa in rete.

[7] M.C. Tamburini, Algebra II unità , Dispensa in rete.

[8] M.C. Tamburini, Approfondimenti di Algebra, Dispensa in rete.