10. Il gruppo Speciale Lineare $SL(V)$

Siano F un campo e V uno spazio vettoriale di dimensione n su F. Indichiamo con $GL(V)$ l'insieme delle applicazioni lineari biiettive di V in sé. Con la composizione di funzioni, $GL(V)$ è un gruppo, detto *gruppo generale lineare*. Sia $\alpha \in GL(V)$. Fissata una base $\{v_1, \ldots, v_n\}$ di V, possiamo associare ad α una matrice quadrata n per n la cui i-esima riga è data dalle coordinate del vettore v_i^α rispetto alla base fissata. Il determinante di questa matrice, come è noto per il teorema di Binet, non dipende dalla base fissata, ma solo dall'applicazione α. Rimane ben definita quindi la funzione, che è un omomorfismo di gruppi,

$$det : GL(V) \longrightarrow F^*, \alpha \mapsto det\,\alpha.$$

Il nucleo della funzione det, cioè l'insieme degli elementi $\alpha \in GL(V)$ tali che $det\,\alpha = 1$, è un sottogruppo normale di $GL(V)$ che si chiama *gruppo speciale lineare* e si denota con $SL(V)$. Per il primo teorema di omomorfismo abbiamo che

$$GL(V)/SL(V) \cong F^*.$$

Il seguente lemma è di immediata verifica.

Lemma 10.1. *Il centro del gruppo $SL(V)$ è costituito dalle matrici scalari di determinante* 1.

Chiaramente ogni elemento di $SL(V)$ trasforma un sottospazio di dimensione 1 di V in un altro sottospazio di dimensione 1. Quindi il gruppo $SL(V)$ agisce sullo spazio proiettivo $P(V)$. Il nucleo dell'azione è costituito dalle trasformazioni lineari che fissano tutti i sottospazi di dimensione 1 di V, cioè da $Z(SL(V))$. Il gruppo quoziente $SL(V)/Z(SL(V))$ si chiama *gruppo speciale lineare proiettivo* e si denota con $PSL(V)$. In questo capitolo vogliamo dimostrare che il gruppo $PSL(V)$ è un gruppo semplice. Per far questo dobbiamo introdurre alcuni concetti e risultati sulle azioni di gruppi.

Definizione 10.2. *Sia Ω un insieme e sia G un gruppo che agisce su Ω. Una* partizione *di G è una famiglia $\mathcal{P}$ di sottoinsiemi di Ω tali che $\Omega = \bigcup_{X \in \mathcal{P}} X$ e per ogni $Y, Z \in \mathcal{P}$ si ha $Y \cap Z \neq \emptyset$ se e solo se $Y = Z$. La partizione si dice* non banale *se ogni suo elemento è diverso da Ω e ha cardinalità almeno* 2.

*Una partizione $\mathcal{P}$ di X si dice G-*invariante *se per ogni $Y \in \mathcal{P}$ e per ogni $g \in G$ si ha $Y^g \in \mathcal{P}$.*

Definizione 10.3. *Sia G un gruppo che agisce su un insieme Ω. Diremo che G agisce in modo* primitivo *(o semplivemente che G è* primitivo*) su Ω se G è transitivo e nessuna partizione non banale di Ω è G-invariante.*

Come nel Capitolo 4, se G è un gruppo che agisce su un insieme Ω e $\omega \in \Omega$, indichiamo con G_ω lo stabilizzatore di ω in G e con ω^G l'orbita di ω. È chiaro che G è transitivo su Ω se e solo se $\Omega = \omega^G$ per qualche (e quindi per tutti) $\omega \in \Omega$. Ci sarà molto utile il seguente lemma.

Lemma 10.4. *Sia G un gruppo che agisce su un insieme Ω in modo transitivo e sia H un sottogruppo di G. Allora H è transitivo su Ω se e solo se per ogni $\omega \in \Omega$ si ha $G = G_\omega H$.*

Proof. Supponiamo che H sia transitivo su Ω. Sia $\omega \in \Omega$ e sia $g \in G$. Poichè H è transitivo su Ω, esiste $h \in H$ tale che $\omega^g = \omega^h$. Allora $gh^{-1} \in G_\omega$ e $g \in G_\omega H$.

Viceversa supponiamo che $G = G_\omega H$. Sia $\sigma \in \Omega$. Poichè G è transitivo su Ω, esiste $g \in G$ tale che $\sigma = \omega^g$. Ora da $G = G_\omega H$ segue che $g = ah$ con $a \in G_\omega$ e $h \in H$. Così

$$\sigma = \omega^g = \omega^{ah} = \omega^h$$

ovvero H è transitivo su Ω. □

Lemma 10.5. *Sia G un gruppo primitivo su un insieme Ω e sia N un sottogruppo normale di G. Allora o N fissa tutti i punti di Ω oppure N è transitivo su Ω.*

Proof. Basta mostrare che l'insieme delle orbite di N su Ω è una partizione G-invariante. Che sia una partizione di Ω segue dai risultati del Capitolo 4. Vediamo che è G-invariante.

Sia $Y = \omega^N$ una N-orbita e sia $g \in G$. Abbiamo che

$$Y^g = \{y^g \mid y \in Y\} = \{\omega^{ng} \mid n \in N\} = \{\omega^{g(g^{-1}ng)} \mid n \in N\}$$

poichè al variare di n in N gli elementi $g^{-1}ng$ stanno in N (perchè N è normale in G) e descrivono tutto N, segue che

$$Y^g = \{\omega^{gn} \mid n \in N\} = (\omega^g)^N.$$

Quindi Y^g è ancora una N-orbita.

Poichè G è primitivo, si ha che l'insieme delle N-orbite deve essere una partizione banale. Quindi o ogni orbita contiene un solo elemento e quindi N fissa tutti gli elementi di Ω, oppure c'è una sola N-orbita e quindi N è transitivo. □

Lemma 10.6 (Lemma di Iwasawa)**.** *Sia G un gruppo che agisce su un insieme Ω. Supponiamo che*

(1) *$G' = G$;*
(2) *G sia primitivo su Ω;*
(3) *per $\omega \in \Omega$, lo stabizzatore G_ω contenga un sottogruppo normale risolubile R tale che $G = \langle R^g \mid g \in G\rangle$.*

Allora ogni sottogruppo normale proprio di G fissa tutti i punti di Ω.

Proof. Sia N un sottogruppo normale di G e supponiamo che N non fissi tutti i punti di Ω. Poichè G è primitivo, per il Lemma 10.5 N è transitivo su Ω. Allora per ogni $\omega \in \Omega$, per il Lemma 10.4, $G = G_\omega N$. Dall'ipotesi (3) segue che

$$G = \langle R^g \mid g \in G\rangle = \langle R^{an} \mid a \in G_\omega, n \in N\rangle = \langle R^n \mid n \in N\rangle = RN.$$

Per il Teorema del parallelogramma, $G/N = RN/N \cong R/R \cap N$ e quindi G/N è risolubile (perchè R è risolubile). D'altra parte, $(G/N)' = G'N/N = G/N$ per l'ipotesi (1). Pertanto G/N è il gruppo identico e $N = G$. □

Definizione 10.7. *Sia G un gruppo che agisce su un insieme Ω. G si dice* 2-transitivo *se per ogni $(\alpha, \beta), (\gamma, \delta) \in \Omega \times \Omega$, con $\alpha \neq \beta$ e $\gamma \neq \delta$, esiste $g \in G$ tale che $\alpha^g = \gamma$ e $\beta^g = \delta$.*

È immediato verificare che "2-transitivo" implica "transitivo".

Lemma 10.8. *Sia G un gruppo 2-transitivo sull'insieme Ω. Allora G è primitivo su Ω.*

Proof. Per l'osservazione precedente, G è transitivo su Ω. Sia $\mathcal{P}$ una partizione G-invariante di Ω e supponiamo che gli elementi di $\mathcal{P}$ non abbiano tutti cardinalità 1. Mostriamo che $\mathcal{P} = \{\Omega\}$. Sia $X \in \mathcal{P}$ con $|X| \geq 2$ a siano $\alpha, \beta \in X$ con $\alpha \neq \beta$. Per ogni $\omega \in \Omega \setminus \{\beta\}$ abbiamo che, poichè G è 2-transitivo, esiste $g \in G$ tale che $\alpha^g = \beta$ e $\beta^g = \omega$. Allora $\beta \in X \cap X^g$. Ma X^g è un elemento di $\mathcal{P}$ e quindi deve essere $X = X^g$, da cui segue che $\omega \in X$. Quindi $X = \Omega$. $\square$

Lemma 10.9. *Nella sua azione sui sottospazi di dimensione 1 di V, $SL(V)$ è 2-transitivo.*

Proof. Siano $\langle u_1 \rangle \neq \langle u_2 \rangle$ e $\langle w_1 \rangle \neq \langle w_2 \rangle$ sottospazi di V di dimensione 1. Allora u_1, u_2 (rispettivamente w_1, w_2) sono linearmente indipendenti e quindi esistono vettori $u_3, \ldots, u_n$ e $w_3, \ldots, w_n$ tali che $u_1, \ldots, u_n$ (rispettivamente $w_1, \ldots, w_n$) è una base di V. Allora esiste un unico elemento $\alpha \in GL(V)$ tale che $u_i^\alpha = w_i$ per ogni $i = 1, \ldots, n$. Così, $\langle u_1 \rangle^\alpha = \langle w_1 \rangle$ e $\langle u_2 \rangle^\alpha = \langle w_2 \rangle$. Se α ha determinante $a \neq 1$, al posto di α possiamo considerare l'elemento $\beta \in GL(V)$ definito da $u_1^\beta = a^{-1} w_1$, $u_i^\beta = w_i$ per $i = 2, \ldots, n$. Allora β ha determinante 1. $\square$

Definizione 10.10. *Per $v \in V$, $\alpha \in GL(V)$ il vettore*

$$[v, \alpha] := v^\alpha - v$$

si dice commutatore *di v e α.*

Se G è un sottogruppo di $GL(V)$ poniamo

$$[V, G] := \langle [v, g], \mid v \in V, g \in G \rangle$$

e per ogni $g \in G$ sciviamo $[V, g]$ al posto di $[V, \langle g \rangle]$.

Definizione 10.11. *Una* trasvezione *è un elemento $t \in GL(V)$ tale che:*

(1) *$[V, t]$ è un sottospazio di dimensione 1 di V;*
(2) *$C_V(t) = \{v \in V \mid v^t = v\}$ è un iperpiano di V;*
(3) *$[V, t] \leq C_V(t)$.*

$[V, t]$ si dice centro *di t e $C_V(t)$ si dice* asse *di t.*

Fissiamo una trasvezione t. Scegliamo una base di V in questo modo:

$$v_n \in V \setminus C_V(t),$$

$$v_1 := [v_n, t]$$

e $v_2, \ldots, v_{n-1}$ tali che $v_1, v_2, \ldots, v_{n-1}$ sia una base di $C_V(t)$.

Allora la matrice di t rispetto a questa base è $I + E_{n1}$ dove I denota la matrice identica di dimensione n ed $E_{ij} = (\delta_{ih}\delta_{jk})_{hk}$. Segue subito che $dett = 1$.

Lemma 10.12. *Ogni trasvezione sta in $SL(V)$.*

Lemma 10.13. *Le trasvezioni sono tutte coniugate in $GL(V)$.*

Proof. Segue dall'osservazione precedente e dal fatto che fissate due basi di V esiste sempre un elemento di $GL(V)$ che manda la prima base nella seconda base. $\square$

Lemma 10.14. *Le trasvezioni sono tutte coniugate in $SL(V)$ tranne nel caso in cui $n = 2$ e $F \neq F^2$.*

Proof. Fissiamo una trasvezione t e sia $v_1, \ldots, v_n$ una base rispetto alla quale la matrice di t è $I + E_{n1}$. Poniamo

$$A := \{\alpha \in GL(V) \mid v_2^\alpha \in \langle v_2 \rangle \text{ e } v_i^\alpha = v_i \ \forall i \neq 2\}$$

se $n > 2$, mentre poniamo

$$A := \{\alpha \in GL(V) \mid u^\alpha \in \langle u \rangle \ \forall u \in V\}$$

se $n = 2$. Si verifica facilmente che la funzione $det : A \longrightarrow F^*$ è suriettiva tranne nel caso in cui $n = 2$ e $F \neq F^2$. Quando la funzione è suriettiva abbiamo $GL(V) = ASL(V)$. Ora si ha che $A \leq C_{GL(V)}(t)$ e quindi $GL(V) = C_{GL(V)}(t)SL(V)$. Poichè $GL(V)$ è transitivo sull'insieme delle trasvezioni, dal Lemma 10.4 segue che $SL(V)$ è anch'esso transitivo. $\square$

Lemma 10.15. *Se $|F| > 3$ oppure $n > 2$, ogni trasvezione sta nel derivato di $SL(V)$.*

Proof. Sia t una trasvezione e sia $v_1, \ldots, v_n$ una base rispetto alla quale la matrice di t è $I+E_{n1}$. Supponiamo $n > 2$. Sia s una seconda trasvezione tale che $C_V(s) = C_V(t)$ e $[v_n, s] = v_2$. Allora st è ancora una trasvezione. Infatti chiaramente $C_V(t) \leq C_V(st)$. Inoltre

$$[v_n, st] = v_n^{st} - v_n = (v_n^s)^t - v_n = (v_n+v_2)^t - v_n = v_n^t + v_2^t - v_n = v_n + v_1 + v_2 - v_n = v_1 + v_2.$$

Quindi $v_n \notin C_V(st)$ e $C_V(st)$ è un iperpiano. Inoltre $[V, st] = \langle v_1 + v_2 \rangle \leq C_V(st)$. Poichè per il Lemma 10.14, $SL(V)$ è transitivo sulle trasvezioni, esiste $r \in SL(V)$ tale che $st = s^r$. Pertanto $t = [s, r]$ sta nel derivato di $SL(V)$.

Sia ora $n = 2$ e $|F| > 3$. Allora t ha matrice

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

Per ogni $b \in F^*$ definiamo la trasvezione $t(b)$ con asse $\langle v_1 \rangle$ e tale che $v_2^{t(b)} - v_2 = bv_1$. Allora $t(b)$ ha matrice

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

Sia $a \in F^*$ e poniamo

$$g := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}.$$

Allora $t(b)^g = t(a^2 b)$. Poichè $|F| > 3$ possiamo scegliere a tale che $a^2 \neq 1$. Così per $b = (a^2-1)^{-1}$ otteniamo

$$[t(b), g] = t(b)^{-1} t(b)^g = \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a^2 b & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ b(a^2-1) & 1 \end{pmatrix} = t.$$

Quindi t è contenuto nel derivato di $SL(V)$. □

Ci serve ora il seguente lemma tecnico.

Lemma 10.16. *Sia l un intero con $0 \leq l \leq n-3$, siano $v_0, \ldots, v_l, v, w$ vettori di V linearmente indipendenti e supponiamo che $v \notin \langle v_0, v_1, \ldots, v_l, v-w \rangle$. Allora esiste una trasvezione τ tale che $\langle v_0, v_1, \ldots, v_l, v-w \rangle \leq C_V(\tau)$ e $v^\tau = w$.*

Proof. Sia U un iperpiano di V contenente $\langle v_0, v_1, \ldots, v_l, v-w \rangle$ con $v \notin U$. Se $u_1, \ldots, u_{n-1}$ è una base di U, allora $u_1, \ldots, u_{n-1}, v$ e $u_1, \ldots, u_{n-1}, w-v$ sono basi di V e la mappa τ definita da $u_i^\tau = u_i$ per ogni $i = 1, \ldots, n-1$ e $v^\tau = w - v$ è una trasvezione. □

Lemma 10.17. *Se $|F| > 3$ o $n > 2$, $SL(V)$ è generato da trasvezioni.*

Proof. Sia T il sottogruppo di $SL(V)$ generato dalle trasvezioni. Sia

$$\Omega := \{(\langle x_1 \rangle, x_2, \ldots, x_n) \mid x_1, \ldots, x_n \in V, \text{ linearmente indipendenti}\}.$$

Il gruppo $SL(V)$ agisce su Ω nel modo naturale e se $\omega \in \Omega$ abbiamo che l'unico elemento di $SL(V)$ che fissa ω è l'identità.

Proviamo che T è transitivo su Ω. Per far questo, per ogni $1 \leq t \leq n$ poniamo

$$\Omega_t := \{(\langle x_1 \rangle, x_2, \ldots, x_t) \mid x_1, \ldots, x_t \in V, \text{ linearmente indipendenti}\}$$

e *dimostriamo per induzione su t che T è transitivo su Ω_t.* Se $t = 1$, Ω_1 è l'insieme dei sottospazi di dimensione 1 di V. Siano $\langle x \rangle \neq \langle y \rangle$ due sottospazi non nulli. Allora $x \notin \langle x - y \rangle$ e per il Lemma 10.16 con $l = 0$ esiste una trasvezione τ tale che $x^\tau = y$, da cui $\langle x \rangle^\tau = \langle y \rangle$. Sia ora $t > 1$ e supponiamo per ipotesi induttiva che la tesi sia vera per $t-1$. Siano $(\langle x_1 \rangle, x_2, \ldots, x_t) \neq (\langle y_1 \rangle, y_2, \ldots, y_t)$ due elementi di Ω_t. Allora $(\langle x_1 \rangle, x_2, \ldots, x_{t-1})$ e $(\langle y_1 \rangle, y_2, \ldots, y_{t-1})$ sono elementi di Ω_{t-1} e per l'ipotesi induttiva esiste un elemento $\gamma \in T$ tale che $(\langle x_1 \rangle, x_2, \ldots, x_{t-1})^\gamma = (\langle y_1 \rangle, y_2, \ldots, y_{t-1})$. Possiamo quindi supporre direttamente che $x_i = y_i$ per ogni $i = 1, \ldots, t-1$. Applicando il Lemma 10.16 all'insieme $x_2, \ldots, x_{t-1}, x_1, x_t$ otteniamo una trasvezione τ tale che $\langle x_2, \ldots, x_{t-1}, x_1 - x_t \rangle \leq C_V(\tau)$ e $x_t^\tau = x_1$. Analogamente, applicando il Lemma 10.16 all'insieme $x_2, \ldots, x_{t-1}, y_t, x_1$, otteniamo una trasvezione σ tale che $\langle x_2, \ldots, x_{t-1}, x_1 - y_t \rangle \leq C_V(\sigma)$ e $y_t^\sigma = x_1$. Siano $x_1^\tau = u$ e $x_1^\sigma = z$. Per concludere resta quindi da dimostrare solo che esiste un elemento δ di T che fissa x_i per $i = 1, \ldots, t-1$ e tale che $\langle u \rangle^\delta = \langle z \rangle$. Ovviamente possiamo supporre $\langle u \rangle \neq \langle z \rangle$ altrimenti basta prendere δ uguale all'identità. Poniamo

$$U := \langle u, x_1, \ldots, x_{t-1} \rangle, \; Z := \langle z, x_1, \ldots, x_{t-1} \rangle, \; W := \langle x_1, \ldots, x_{t-1} \rangle.$$

Se $u \notin \langle x_1, \ldots, x_{t-1}, u - z \rangle$, allora di nuovo per il Lemma 10.16 esiste una trasvezione con asse contenente $\langle x_1, \ldots, x_{t-1}, u - z \rangle$ che manda u in z e così abbiamo finito.

Sia quindi $u \in \langle x_1, \dots, x_{t-1}, u - z \rangle$. Allora $U = Z$ e W è un iperpiano di U. Pertanto esiste $a \in F^*$ tale che $u - az \in W$. Allora $u \notin \langle u - az, x_1, \dots, x_{t-1} \rangle = W$ e sempre per il Lemma 10.16 esiste una trasvezione ρ tale che $W \leq C_V(\rho)$ e $u^\rho = az$. Così $\langle u \rangle^\rho = \langle z \rangle$. Questo prova che T è transitivo su Ω_t per ogni $1 \leq t \leq n$. In particolare T è transitivo su Ω.

Infine per il Lemma 10.4 e il Lemma 10.14 abbiamo $SL(V) = SL(V)_\omega T = T$ perchè come abbiamo osservato all'inizio della dimostrazione $SL(V)_\omega = 1$. □

Teorema 10.18. *Se $|F| > 3$ oppure $n > 2$, il gruppo $PSL(V)$ è semplice.*

Proof. Per il teorema di corrispondenza basta dimostrare che ogni sottogruppo normale proprio di $SL(V)$ è contenuto in $Z(SL(V))$. Ciò seguirà dal Lemma di Iwasawa una volta provato che $SL(V)$ soddisfa le ipotesi del lemma.

Dai Lemmi 10.17 e 10.15 segue subito che se $|F| > 3$ o $n > 2$, $SL(V)$ coincide con il suo sottogruppo derivato.

Dai Lemmi 10.8 e 10.9 segue che $SL(V)$ agisce in modo primitivo sull'insieme dei sottospazi di dimensione 1 di V. Il nucleo di questa azione è l'insieme delle matrici scalari, cioè $Z(SL(V))$.

Sia ora U un sottospazio di dimensione 1 di V. Poniamo

$$R := C_{SL(V)}(U) \cap C_{SL(V)}(V/U).$$

Vogliamo mostrare che R è un sottogruppo normale risolubile dello stabilizzatore in $SL(V)$ di U e $SL(V) = \langle R^g \mid g \in SL(V) \rangle$. Se fissiamo una base $v_1, \dots, v_n$ di V tale che $\langle v_1 \rangle = U$, allora gli elementi di $C_{SL(V)}(U)$ sono tutti rappresentati da matrici del tipo

$$\left(\begin{array}{c|ccc} a & 0 & \cdots & 0 \\ \hline * & & & \\ \vdots & & A & \\ * & & & \end{array} \right)$$

con $a \in F^*$, $A \in GL_{n-1}(F)$ e $detA = a^{-1}$, mentre gli elementi di R sono tutti rappresentati da matrici del tipo

$$\left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline * & & & \\ \vdots & & I_{n-1} & \\ * & & & \end{array} \right).$$

Una facile verifica mostra che R è abeliano ed è un sottogruppo normale di $C_{SL(V)}(U)$. Inoltre è chiaro che R contiene le trasvezioni di asse $\langle v_1, \dots, v_{n-1} \rangle$ e centro $\langle v_1 \rangle$. Poichè per il Lemma 10.17, $SL(V)$ è generato dalle trasvezioni e le trasvezioni sono tutte coniugate in $SL(V)$ per il Lemma 10.14, abbiamo anche che $SL(V)$ è generato dai coniugati di R. □