Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

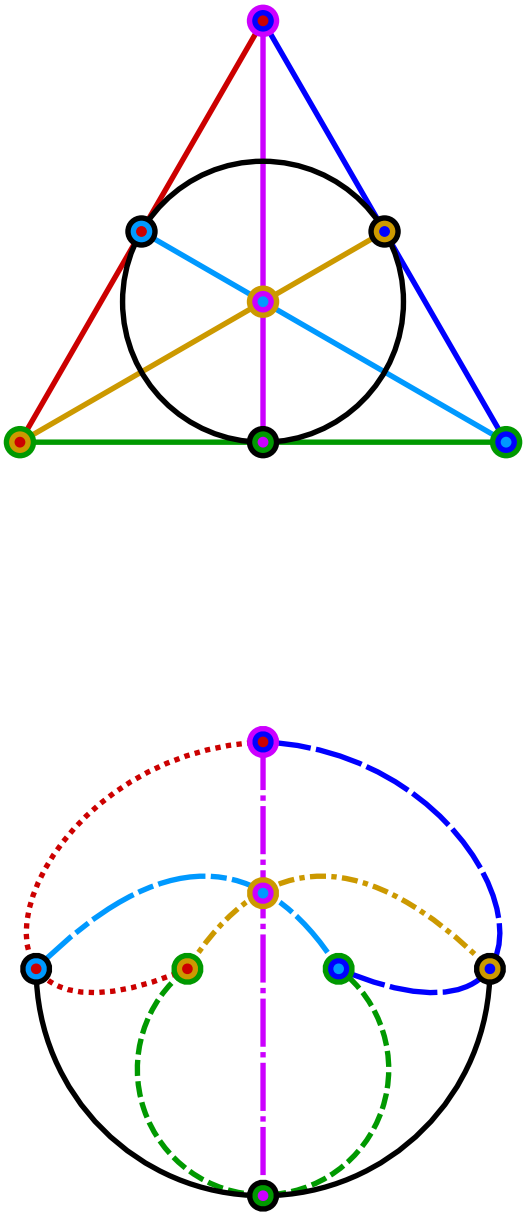
IL GRUPPO PSL(2, 7) E UNA SUA REALIZZAZIONE COME GRUPPO DI GALOIS

Tesi di Laurea in Algebra

Relatore:
Prof.ssa Marta Morigi

Presentata da:
Davide Ricci

II Sessione
Anno Accademico 2020/21



Due rappresentazioni grafiche del piano di Fano.

Introduzione

Uno dei problemi aperti della Teoria di Galois è stabilire quando un gruppo finito si realizza come gruppo di Galois di un polinomio a coefficienti in $\mathbb{Q}$. Per quanto riguarda i gruppi risolubili il problema è stato risolto in modo del tutto generale utilizzando profondi risultati di Hilbert. È quindi interessante realizzare i gruppi semplici finiti su $\mathbb{Q}$. Il più piccolo di questi, tra i non abeliani, è A_5, che ha ordine 60 e che si realizza con $x^5 + 20x + 16 \in \mathbb{Q}[x]$ (si veda [4], p.406). Il secondo è $\mathrm{PSL}(2, 7)$, il gruppo proiettivo speciale lineare di grado 2 costruito sul campo con 7 elementi, di ordine 168. Descriveremo una sua realizzazione come gruppo di Galois del polinomio $x^7 - 154x + 99 \in \mathbb{Q}[x]$, tratta da [5].

Per poter capire al meglio questi argomenti, che verranno trattati nel Capitolo 4, introdurremo prima dei risultati su $\mathrm{PSL}(2, 7)$. Vedremo che i gruppi di tipo $\mathrm{PSL}(n, q)$ sono generati dalle trasvezioni e che la proprietà di semplicità li accomuna quasi tutti. Il caso $\mathrm{PSL}(2, 7)$ si differenzia per il suo isomorfismo con $\mathrm{GL}(3, 2)$, che vedremo attraverso delle descrizioni funzionali dei due gruppi in questione. Di conseguenza, dato che $\mathrm{GL}(3, 2)$ è anche il gruppo degli automorfismi del Piano di Fano, il più piccolo piano proiettivo finito, avremo la possibilità di studiare alcune proprietà di $\mathrm{PSL}(2, 7)$ anche attraverso dei disegni molto intuitivi. Inoltre, avremo bisogno di alcuni risultati sui gruppi di permutazioni, in particolare che $\mathrm{PSL}(2, 7)$ è l'unico sottogruppo proprio di A_7 contenente il prodotto di due trasposizioni disgiunte e un 7-ciclo. Infine, non ci addentreremo nella Teoria di Galois, ma ne richiameremo alcuni essenziali risultati di base.

Indice

Capitolo 1

Gruppi proiettivi lineari

Iniziamo questa illustrazione introducendo i *gruppi proiettivi lineari* in tutte le loro versioni. La descrizione che ne verrà data è totalmente algebrica. In realtà, essi si possono anche caratterizzare come gli automorfismi di spazi proiettivi.

1.1 Prime definizioni

Sia R un anello commutativo unitario, ricordiamo $\mathrm{GL}(n, R)$ è il gruppo generale lineare di grado n su R e $\mathrm{SL}(n, R)$ è il gruppo speciale lineare, il sottogruppo di $\mathrm{GL}(n, q)$ delle le matrici unitarie.

Scriveremo E_{ij} per indicare una matrice elementare $n \times n$, con un 1 in posizione (i, j) e 0 altrove.

Teorema 1.1.1. *Il centralizzante di* $\mathrm{SL}(n, R)$ *in* $\mathrm{GL}(n, R)$ *è il gruppo delle matrici scalari invertibili* aI_n *con* $a \in R^*$.

Dimostrazione. Chiaramente le matrici scalari invertibili commutano con tutte le matrici di $\mathrm{GL}(n, R)$. Viceversa, sia $A = (a_{ij})$ una matrice del centralizzante di $\mathrm{SL}(n, R)$ in $\mathrm{GL}(n, R)$. Le matrici della forma $I + E_{ij}$ appartengono a in $\mathrm{SL}(n, R)$ se $i \neq j$ e quindi A ed $I + E_{ij}$ commutano, per cui deve essere soddisfatta la relazione $AE_{ij} = E_{ij}A$. Il (k, j)-esimo coefficiente di AE_{ij} è a_{ki}, mentre quello di $E_{ij}A$ è 0 se $k \neq i$ ed è a_{jj} altrimenti. Dal momento che $a_{ki} = 0$ se $k \neq i$ e $a_{ii} = a_{jj}$, A è necessariamente scalare. □

Corollario 1.1.2. *Il centro* $Z(\mathrm{SL}(n,R))$ *di* $\mathrm{SL}(n,R)$ *è il gruppo delle matrici scalari* aI_n *dove* $a^n = 1$.

Definizione 1.1.3. Il *gruppo proiettivo generale lineare* di grado n su un anello R è definito come

$$\mathrm{PGL}(n,R) = \frac{\mathrm{GL}(n,R)}{Z(\mathrm{GL}(n,R))}$$

e il *gruppo proiettivo speciale lineare* è

$$\mathrm{PSL}(n,R) = \frac{\mathrm{SL}(n,R)}{Z(\mathrm{SL}(n,R))} = \frac{\mathrm{SL}(n,R)}{\mathrm{SL}(n,R) \cap Z(\mathrm{GL}(n,R))}.$$

Nel caso in cui R sia il campo finito $\mathbb{F}_q$ di ordine q, usiamo le notazioni

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

Lemma 1.1.4.

i) $\left|\mathrm{GL}(n,q)\right| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

ii) $\left|\mathrm{SL}(n,q)\right| = \left|\mathrm{GL}(n,q)\right| / (q-1) = \left|\mathrm{PGL}(n,q)\right|$.

iii) $\left|\mathrm{PSL}(n,q)\right| = \left|\mathrm{GL}(n,q)\right| / (q-1)d$ *dove* $d = \mathrm{MCD}(n, q-1)$.

Dimostrazione. i) Per definire una matrice di $\mathrm{GL}(n,q)$ abbiamo $q^n - 1$ scelte per gli elementi della prima riga, escludendo la riga nulla, $q^n - q$ per la seconda, escludendo righe multiple della prima, $q^n - q^2$ per la terza, escludendo combinazioni lineari delle prime due righe, e così via. Moltiplicando questi numeri otteniamo il numero delle matrici di $\mathrm{GL}(n,q)$.

ii) La mappa $A \mapsto \det A$ è un morfismo suriettivo da $\mathrm{GL}(n,q)$ a $\mathbb{F}_q^*$ con nucleo $\mathrm{SL}(n,q)$. Siccome $\left|\mathbb{F}_q^*\right| = q-1$, la formula segue. L'ordine di $\mathrm{PGL}(n,q)$ è lo stesso dal momento che possiamo costruire $q-1$ matrici scalari invertibili in $\mathrm{GL}(n,q)$.

iii) l'ordine di $\mathrm{SL}(n,q) \cap C(\mathrm{GL}(n,q))$ è dato dal numero di soluzioni in $\mathbb{F}_q^*$ di $x^n = 1$, che è $d = mcd(n, q-1)$ dal momento che $\mathbb{F}_q^*$ è ciclico e di ordine $q-1$.

□

Proposizione 1.1.5. $\mathrm{GL}(n,2) \cong \mathrm{SL}(n,2) \cong \mathrm{PGL}(n,2) \cong \mathrm{PSL}(n,2)$.

Dimostrazione.

- L'inclusione di $\mathrm{SL}(n,2)$ in $\mathrm{GL}(n,2)$ è un isomorfismo;
- L'inclusione di $\mathrm{PSL}(n,2)$ in $\mathrm{PGL}(n,2)$ è un isomorfismo;
- La proiezione al quoziente di $\mathrm{GL}(n,2)$ in $\mathrm{PGL}(n,2)$ ha nucleo banale;
- La proiezione al quoziente di $\mathrm{SL}(n,2)$ in $\mathrm{PSL}(n,2)$ ha nucleo banale.

□

1.2 Semplicità di PSL(n, q)

I gruppi $\mathrm{PSL}(n,q)$, introdotti per la prima volta da Galois e studiati da Jordan [9], formano una famiglia infinita di gruppi semplici finiti. Ciò è quello che dimostreremo in questa sezione, anche se vedremo che servono alcune ipotesi, che lasciano fuori due eccezioni.

Vediamo innanzitutto la definizione di gruppo semplice e l'esempio più noto di gruppo con questa proprietà.

Definizione 1.2.1. Un gruppo non banale G si dice *semplice* se i suoi unici sottogruppi normali sono 1 e G stesso.

Teorema 1.2.2. *A_n è generato dai 3-cicli se $n \geq 3$.*

Dimostrazione. S_n è generato dalle trasposizioni, ergo 2-cicli. Dal momento che $(a,b)(a,c) = (a,b,c)$ e $(a,b)(c,d) = (a,b,c)(a,d,c)$, con i 3-cicli riusciamo a generare tutte le permutazioni di S_n prodotto di un numero pari di trasposizioni. Queste sono però esattamente gli elementi di A_n. □

Teorema 1.2.3. *A_n è semplice se e solo se $n \neq 1, 2, 4$.*

Dimostrazione. A_1 e A_2 sono gruppi banali. A_3 non ha sottogruppi propri non banali.

In A_4, gli elementi $(1,2)(3,4), (1,3)(2,4), (1,4)(2,3)$ formano un sottogruppo proprio.

Studiamo il caso $n \geq 5$. Supponiamo che esista un sottogruppo normale non banale $N \leq A_n$.

Supponiamo che N contenga un 3-ciclo (a, b, c). Se $(a', b', c') \in A_n$ è un altro 3-ciclo e π è una permutazione in S_n che mappa a in a', b in b' e c in c', si ha $\pi^{-1}(a, b, c)\pi = (a', b', c')$. A meno di considerare $\pi(e, f)$ con e, f diversi da a', b', c' (che esistono perché $n \geq 5$), possiamo supporre che $\pi \in A_n$. In tal caso ogni $(a', b', c') \in N$ e quindi $N = A_n$. Segue che N non può contenere un 3-ciclo.

Supponiamo che N contenga una permutazione la cui decomposizione in cicli disgiunti coinvolga un ciclo di lunghezza almeno 4 che chiamiamo

$$\pi = (a_1, a_2, a_3, a_4, \dots) \dots .$$

Allora N contiene anche

$$\pi' = (a_1, a_2, a_3)^{-1}\pi(a_1, a_2, a_3) = (a_2, a_3, a_1, a_4, \dots) \dots ,$$

e anche $\pi^{-1}\pi' = (a_1, a_2, a_4)$, che è un 3-ciclo. Questo è assurdo, quindi la decomposizione in cicli disgiunti di un elemento non identico di N deve coinvolgere soltanto cicli di lunghezza $2, 3$. In tal caso, non può nemmeno coinvolgere soltanto un 3-ciclo, perché, elevando al quadrato otterremmo un 3-ciclo in N.

Supponiamo che N contenga una permutazione la cui fattorizzazione abbia almeno due 3-cicli disgiunti $\pi = (a, b, c)(a', b', c') \dots$. Allora N contiene anche

$$\pi' = (a', b', c)^{-1}\pi(a', b', c) = (a, b, a')(c, c', b') \dots$$

e quindi anche $\pi\pi' = (a, a', c, b, c') \dots$, che è assurdo.

In definitiva, ogni elemento di N è prodotto di un numero pari di 2-cicli disgiunti. Se $\pi = (a, b)(a', b') \in N$, allora per ogni c non coinvolto in π, $\pi' = (a, c, b)^{-1}\pi(a, c, b) = (a, c)(a', b')$. Così, $\pi\pi' = (a, b, c)$ e segue che se $1 \neq \pi \in N$, allora $\pi = (a_1, b_1)(a_2, b_2)(a_3, b_3)(a_4, b_4) \dots$ con numero di 2-cicli disgiunti almeno 4. In tal caso N contiene anche

$$\pi' = (a_3, b_2)(a_2, b_1)\pi(a_3, b_2)(a_2, b_1) = (a_1, a_2)(a_3, b_1)(b_2, b_3)(a_4, b_4) \dots$$

e finalmente $\pi\pi' = (a_1, a_3, b_2)(a_2, b_3, b_1)$ che è l'ultima contraddizione. □

Passiamo ora ai $\mathrm{PSL}(n, q)$. L'obiettivo è dimostrare il teorema che segue.

Teorema 1.2.4. *Siano F un campo e N è un sottogruppo normale di $\mathrm{SL}(n, F)$ non contenuto nel centro. Se $n > 2$ oppure valgono $n = 2$ e $|F| > 3$, allora $N = \mathrm{SL}(n, F)$.*

Corollario 1.2.5 (Teorema di Jordan-Dickson)**.** *Se $n > 2$ oppure valgono $n = 2$ e $|F| > 3$, allora $\mathrm{PSL}(n, F)$ è semplice.*

Questo corollario immediato è proprio il risultato che ci serve. Malgrado ciò, la dimostrazione del Teorema 1.2.4 è piuttosto lunga e necessità di parecchi risultati preliminari.

Definizione 1.2.6. Sia F un campo. Una *trasvezione* è una matrice della forma $1 + aE_{ij}$ dove $a \in F^*, i \neq j$.

Osservazione. Le trasvezioni differiscono dall'identità solo per a in posizione (i, j), perciò sono anche elementi di $\mathrm{SL}(n, F)$.

Osservazione. La moltiplicazione di matrici a sinistra per $1 + aE_{ij}$ ha l'effetto di sommare a volte la j-esima riga alla i-esima riga.

Lemma 1.2.7. *Le trasvezioni generano $\mathrm{SL}(n, F)$ se $n > 1$.*

Dimostrazione. Sicuramente le trasvezioni sono elementi di $\mathrm{SL}(n, F)$. Sia $A \in \mathrm{SL}(n, F)$. A meno di sommare una riga alla seconda, possiamo supporre $a_{21} \neq 0$. Sommando $a_{21}^{-1}(1 - a_{11})$ volte la seconda riga alla prima, otteniamo 1 in posizione $(1, 1)$. Sottraendo multipli della prima riga, possiamo ottenere zero come ogni elemento della prima colonna sotto la diagonale. Il minore $(1, 1)$ è appartiene a $\mathrm{SL}(n-1, F)$, e iterando il procedimento possiamo ottenere una matrice con 1 nella diagonale e zeri sotto. Altre operazioni sulle righe riducono la matrice all'identità. Queste operazioni per righe corrispondono ad un certo numero di moltiplicazioni a sinistra per opportune trasvezioni $T_1, \ldots, T_k$, quindi

$$T_k T_{k-1} \cdots T_1 A = I_n \qquad \text{e} \qquad A = T_1^{-1} \cdots T_{k-1}^{-1} T_k^{-1}.$$

Dal momento che le matrici inverse delle trasvezioni sono esse stesse trasvezioni, segue la tesi. □

Lemma 1.2.8. *Se $n > 2$, le trasvezioni sono coniugate in* $\mathrm{SL}(n, F)$.

Dimostrazione. Siano $a, b \in F$, siano $I + aE_{ij}$ e $I + bE_{ij}$ due trasvezioni e sia $c = a^{-1}b$. Consideriamo una matrice $n \times n$ diagonale D con 1 in posizione (i, i), c in posizione (j, j), c^{-1} in un'altra posizione diagonale e degli 1 come restanti elementi diagonali. Risulta

$$D \in \mathrm{SL}(n, F) \quad \text{e} \quad D^{-1}(1 + aE_{ij})D = 1 + bE_{ij}.$$

Siano ora due trasvezioni del tipo $I + aE_{ij}$ e $I + bE_{rj}$, con $r \neq i$. Consideriamo una matrice P di dimensione $n \times n$ e che differisce da I_n solo per un 1 in posizione (i, r) e un -1 in posizione (r, i) e 0 in posizione (i, i) e (r, r). Risulta

$$P \in \mathrm{SL}(n, F) \quad \text{e} \quad P^{-1}(1 + aE_{ij})P = 1 + aE_{rj}$$

dove $j \neq i, r$. Similmente, per una matrice $Q \in \mathrm{SL}(n, F)$ costruita in modo simile, otteniamo $Q^{-1}(1 + aE_{rj})Q = 1 + aE_{rs}$.

Di conseguenza, tutte le trasvezioni sono coniugate in $\mathrm{SL}(n, F)$. □

Ricordiamo che in $\mathrm{GL}(n, F)$ ogni matrice è coniugata ad una matrice in forma canonica razionale, ossia una matrice diagonale a blocchi dove ogni blocco è della forma

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & a_1 \\ 1 & 0 & \cdots & 0 & 0 & a_2 \\ 0 & 1 & \cdots & 0 & 0 & a_3 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & a_{s-1} \\ 0 & 0 & \cdots & 0 & 1 & a_s \end{pmatrix}$$

Lemma 1.2.9. *Se un sottogruppo normale N di* $\mathrm{SL}(2, F)$ *contiene una trasvezione, allora* $N = \mathrm{SL}(2, F)$.

Dimostrazione. Sia $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in N$ con $a \neq 0$. É sufficiente provare che N contiene $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ per ogni $x \in F$, perché, se N contiene una tale matrice, contiene anche

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -x & 1 \end{pmatrix}$$

e per il Lemma 1.2.7 si conclude. Supponiamo $|F| > 2$, altrimenti abbiamo solamente due trasvezioni coniugate tra loro.

Coniugando $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ per $\begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}$, otteniamo $\begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix}$. Per cui N contiene la matrice

$$\begin{pmatrix} 1 & ax^2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & ay^2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a(x^2 - y^2) \\ 0 & 1 \end{pmatrix} \tag{1.1}$$

per ogni $x, y \in F$. Se F ha caratteristica diversa da 2, allora per ogni $b \in F$ risulta $b = (2^{-1}(b+1))^2 - (2^{-1}(b-1))^2$, per cui ogni elemento di F è differenza di due quadrati e il risultato segue per (1.1).

Supponiamo che F abbia caratteristica 2. Se $a^{-1}r$ è un quadrato in F, allora N contiene $\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ e $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Coniugando queste matrici per $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, otteniamo $\begin{pmatrix} 1 & 0 \\ -r & 1 \end{pmatrix}$ e $\begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix}$ rispettivamente. Quindi N contiene

$$\begin{pmatrix} 1 & 0 \\ -a & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -r & 1 \end{pmatrix} = \begin{pmatrix} 1 - mr & m \\ amr - a - r & 1 - am \end{pmatrix},$$

dove $a^{-1}m$ è un quadrato in F. Supponiamo di poter scegliere m e r tali che $amr = a + r$. In tal caso N conterrà per y arbitraria

$$\left[\begin{pmatrix} 1 - mr & m \\ 0 & 1 - am \end{pmatrix}, \begin{pmatrix} 1 & -y \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & my(r-a)(1-mr)^{-1} \\ 0 & 1 \end{pmatrix}. \tag{1.2}$$

Scegliamo $l \in F^*$ tale che $l^4 \neq 1$: questo l esiste dal momento che se tutte le potenze quarte in F^* sono 1, dovremmo avere $|F| = 3$ o $|F| = 5$ ma questo non può essere vero dal momento che siamo in caratteristica 2. Definiamo $m = a^{-1}(1+l^{-2})$ e $r = al^2$: queste scelte sono opportune dal momento che $a^{-1}m = (a^{-1}(1 + l^{-1}))^2$ e $a^{-1}r = l^2$ sono entrambi dei quadrati e $amr = a + r$. Così abbiamo

$$my(r - a)(1 - mr)^{-1} = y(l^{-4} - 1)$$

che spazia su tutto F al variare di y. Finalmente possiamo concludere il risultato per (1.2). □

Teorema 1.2.10. *Se N è un sottogruppo normale di $\mathrm{SL}(2, F)$ non contenuto nel centro e se $|F| > 3$, allora $N = \mathrm{SL}(2, F)$.*

Dimostrazione. A meno di rimpiazzare N con un suo coniugato in $\mathrm{GL}(2, F)$, possiamo supporre che N contenga un elemento A non contenuto nel centro e in forma canonica razionale. Per il Lemma 1.2.9 possiamo supporre che N non contenga una trasvezione.

Come primo caso, supponiamo che $A = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ dove $a \neq a^{-1}$. Se $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, allora N deve contenere il commutatore

$$[A, B] = A^{-1}B^{-1}AB = \begin{pmatrix} 1 & 1 - a^{-2} \\ 0 & 1 \end{pmatrix},$$

che è una trasvezione dato che $a^2 \neq 1$.

Supponiamo che A sia della forma $\begin{pmatrix} 0 & b \\ 1 & a \end{pmatrix}$. Necessariamente $b = -1$ poiché $\det A = 1$. Il commutatore di $\begin{pmatrix} 1 & 0 \\ x^2 & 1 \end{pmatrix}$ ed A è uguale a $\begin{pmatrix} 1 & -x^2 \\ -x^2 & 1 + x^4 \end{pmatrix}$ ed appartiene a N per ogni $x \in F$. Il coniugio di questa matrice per $\begin{pmatrix} x^{-1} & x^{-1} \\ 0 & x \end{pmatrix}$ dà

$\begin{pmatrix} 0 & 1 \\ -1 & 2+x^4 \end{pmatrix}$. Quindi N contiene per ogni x e y non nulle la matrice

$$\begin{pmatrix} 0 & 1 \\ -1 & 2+x^4 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 2+y^4 \end{pmatrix} = \begin{pmatrix} 1 & x^4-y^4 \\ 0 & 1 \end{pmatrix}.$$

Dal momento che N non contiene trasvezioni, la potenza quarta di ogni elemento non nullo di F deve necessariamente essere uguale a 1. Ma il polinomio t^4-1 ha al più 4 radici in F. Quindi F è finito e, detta q la sua cardinalità, deve risultare $q-1 \leq 4$. Dato che per ipotesi $q > 3$ si ha $q = 5$.

Ponendo $x = 1$, dal procedimento fatto prima otteniamo che N contiene $\begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix}$. Contiene anche il commutatore di $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ ed A, che è uguale a $\begin{pmatrix} 1 & -2 \\ -2 & 0 \end{pmatrix}$, siccome $q = 5$. Coniugando quest'ultima per $\begin{pmatrix} 2 & -1 \\ -2 & -1 \end{pmatrix}$ (che è un elemento di $N = \mathrm{SL}(2,5)$), otteniamo $\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ in N. Infine, N contiene $\begin{pmatrix} 0 & 1 \\ -1 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, una trasvezione. □

Siamo pronti a dimostrare il Teorema 1.2.4.

Dimostrazione di 1.2.4. In vista di 1.2.10, assumiamo $n > 2$. Per i Lemmi 1.2.7 e 1.2.8, è sufficiente produrre una trasvezione in N.

Sia A un elemento di N non contenuto nel centro, che possiamo supporre essere in forma canonica razionale. Vediamo il caso in cui tutte le matrici che formano i blocchi diagonali di A siano 1×1: questi blocchi saranno della forma $a_i I_{n_i}$, per $i = 1, \ldots, k$, con $a_i \neq a_j$ se $i \neq j$, e, dal momento che $A \neq I_n$, $k > 1$. Quindi N contiene il commutatore $[A, 1+E_{1,n_1+n_2}] = 1+(1-a_1^{-1}a_2)E_{1,n_1+n_2}$, una trasvezione.

Quindi supponiamo che A abbia un blocco diagonale, possiamo ipotizzare il primo, di dimensione $r > 1$. Quindi

$$A = \begin{pmatrix} \bar{A} & 0 \\ 0 & * \end{pmatrix} \quad \text{dove} \quad \bar{A} = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & a_1 \\ 1 & 0 & \cdots & 0 & 0 & a_2 \\ 0 & 1 & \cdots & 0 & 0 & a_3 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & a_{r-1} \\ 0 & 0 & \cdots & 0 & 1 & a_r \end{pmatrix}, \quad a_1 \neq 0.$$

Se $r > 2$, N contiene

$$[1 + E_{1r}, A^{-1}] = 1 + a_1^{-1}E_{21} - E_{1r}.$$

Quindi contiene anche

$$[1 + E_{1r}, (1 + a_1^{-1}E_{21} - E_{1r})^{-1}] = 1 + a_1^{-1}E_{2r},$$

una trasvezione.

Sia ora $r = 2$ e scriviamo $\bar{A} = \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$, con $a \neq 0$. Esiste qualche elemento di $\mathrm{SL}(2, F)$ che non commuta con $\bar{A}$, quindi commutando A con una matrice opportuna troviamo in N una matrice della forma $\begin{pmatrix} B & 0 \\ 0 & I_{n-2} \end{pmatrix}$, con $B \neq I_2$. Se B è scalare, allora è $-I_2$ dal momento che $\det B = 1$. In questo caso F non può avere caratteristica 2 e N contiene il commutatore di $\begin{pmatrix} -I_2 & 0 \\ 0 & I_{n-2} \end{pmatrix}$ con $1 + E_{23}$, che è esattamente la trasvezione $1 + 2E_{23}$. Altrimenti possiamo supporre che B sia della forma $\begin{pmatrix} 0 & 1 \\ -1 & c \end{pmatrix}$. Allora N contiene il commutatore tra $1 - E_{13}$ e $\begin{pmatrix} B & 0 \\ 0 & I_{n-2} \end{pmatrix}$, che è

$$1 + (1 - c)E_{13} - E_{23}.$$

Infine, commutando questo con $1 + E_{12}$, otteniamo $1 + E_{13} \in N$. □

Analizziamo il Corollario 1.2.5. Per il Lemma 1.1.4, $\mathrm{PSL}(2,2)$ e $\mathrm{PSL}(2,3)$ hanno cardinalità rispettivamente 6 e 12. Non esistono gruppi semplici con queste cardinalità, infatti si dimostra facilmente che $\mathrm{PSL}(2,2) \cong S_3$ e $\mathrm{PSL}(2,3) \cong A_4$. Dunque i casi con $n = 2$ e $|F| = 2, 3$ sono effettivamente delle eccezioni ai Teoremi 1.2.4 e 1.2.5.

$\mathrm{PSL}(2,4)$ e $\mathrm{PSL}(2,5)$ hanno entrambi cardinalità 60 e si dimostra che sono entrambi isomorfi ad A_5.

$\mathrm{PSL}(2,7)$ ha ordine 168 e questo non corrisponde all'ordine di nessun gruppo alterno: abbiamo un nuovo gruppo semplice.

$\mathrm{PSL}(3,4)$ è un gruppo semplice di ordine $20160 = |A_8|$. Comunque, si può dimostrare che $\mathrm{PSL}(3,4)$ non è isomorfo ad A_8, per cui ci sono due gruppi semplici distinti di ordine 20160.

Capitolo 2

Un isomorfismo eccezionale

In questo capitolo vogliamo dimostrare l'isomorfismo tra $\mathrm{PSL}(2,7)$ e $\mathrm{GL}(3,2)$. È già noto che tutti i gruppi semplici di ordine 168 sono isomorfi; ciò dà a $\mathrm{PSL}(2,7)$ la possibilità di meritarsi l'articolo determinativo nel titolo di essere *il gruppo semplice di 168 elementi*, ma omettiamo questo risultato dalla dimostrazione molto tortuosa. Piuttosto, quello che faremo è passare attraverso dei gruppi a loro isomorfi, senza utilizzare la semplicità o argomenti di geometria proiettiva. Proprio per questo motivo, abbiamo prima bisogno di alcuni fatti rilevanti sugli insiemi in questione e, poiché si tratta di gruppi finiti costruiti su campi con pochi elementi, riusciremo senza fatica a trovarne una descrizione esplicita.

2.1 Il gruppo GL(3, 2)

Sia $\mathbb{F}_2 = \{0,1\}$ il campo con due elementi. Il gruppo $\mathrm{GL}(3,2)$ è composto da tutte le matrici 3×3 invertibili con elementi in $\mathbb{F}_2$. Sia $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$ e sia $x = X+(X^3+X+1)$. Da un lato $\mathbb{F}_8$ è il campo con 8 elementi il cui sottogruppo moltiplicativo è generato da x, dall'altro è uno spazio vettoriale tridimensionale su $\mathbb{F}_2$ con base ordinata $B = \{x^0, x^1, x^2\}$. Sia $\mathrm{GL}(\mathbb{F}_8)$ il gruppo delle trasformazioni $\mathbb{F}_2$-lineari invertibili di questo spazio vettoriale, cioè delle biiezioni $L : \mathbb{F}_8 \to \mathbb{F}_8$ tali che $L(u+v) = L(u) + L(v)$ per ogni $u, v \in \mathbb{F}_8$ (essendo in caratteristica 2, la richiesta sul prodotto per scalare funziona in automatico). Per ogni L siffatta,

denotiamo con $[L]_B$ la sua matrice relativa nella base ordinata B. Un isomorfismo tra $\mathrm{GL}(\mathbb{F}_8)$ e $\mathrm{GL}(3,2)$ è dato dalla mappa $L \to [L]_B$, che ci consente di identificare questi due gruppi.

Ci farà comodo avere un insieme molto semplice di generatori per $\mathrm{GL}(3,2)$. Dalla Proposizione 1.1.5 combinata con il Lemma 1.2.7, sappiamo già che $\mathrm{GL}(3,2)$ è generato dalle trasvezioni, ma possiamo ridurre questo insieme.

Definiamo:

$$S_{12} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad S_{23} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad S_{13} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Le trasvezioni di $\mathrm{GL}(3,2)$ sono esattamente sei e a queste uniamo le tre matrici appena presentate, ottenendo un sistema generatori per $\mathrm{GL}(3,2)$. Ora troviamo delle relazioni che ci permettono di ridurlo:

$$S_{13} = S_{12}S_{23}S_{12}, \qquad E_{13} = S_{12}E_{23}S_{12}, \qquad E_{32} = S_{23}E_{23}S_{23},$$

$$E_{21} = S_{13}E_{23}S_{13}, \qquad E_{12} = S_{13}E_{32}S_{13}, \qquad E_{31} = S_{12}E_{32}S_{12}.$$

Dunque E_{23}, S_{12}, S_{23} già generano tutto il gruppo. Consideriamo ora le matrici

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Abbiamo $E_{23} = A_1A_3$, $S_{12} = A_2^2A_1A_2^3A_3$, $S_{23} = A_1$, e così $\mathrm{GL}(3,2)$ è generato da A_1, A_2, A_3.

2.2 Il gruppo PSL(2, 7)

Sia $\mathbb{F}_7 = \{0,1,2,3,4,5,6\}$ il campo con sette elementi. Il gruppo $\mathrm{SL}(2,7)$ è composto da tutte le matrici 2×2 con elementi in $\mathbb{F}_7$ e determinante 1. Il gruppo $\mathrm{PSL}(2,7)$ è il gruppo quoziente $\mathrm{SL}(2,7)/\{I, -I\}$. Definiamo

$$\overline{\mathbb{F}_7} = \mathbb{F}_7 \cup \{\infty\} = \{0,1,2,3,4,5,6,\infty\}$$

e consideriamo le trasformazioni di Möbius su $\overline{\mathbb{F}_7}$, ossia funzioni $f : \overline{\mathbb{F}_7} \to \overline{\mathbb{F}_7}$ della forma

$$f(k) = \frac{ak+b}{ck+d}, \qquad (k \in \overline{\mathbb{F}_7}),$$

dove $a, b, c, d \in \mathbb{F}_7$ sono costanti tali che $ad - bc \neq 0$. Chiaramente nella formula di $f(k)$ si intende che la divisione per $ck + d$ è in realtà la moltiplicazione per il suo inverso in $\mathbb{F}_7$; poniamo la divisione di ogni elemento non nullo per 0 uguale a ∞ e ogni elemento di $\mathbb{F}_7$ diviso per ∞ uguale a 0. Inoltre $f(\infty) = a/c$ se $c \neq 0$ e $f(\infty) = \infty$ se $c = 0$. La trasformazione f si dice *speciale* se $ad - bc = 1$. C'è una mappa naturale ϕ tra $\mathrm{SL}(2, 7)$ e l'insieme $\mathrm{SLF}(7)$ delle trasformazioni speciali di Möbius su $\overline{\mathbb{F}_7}$, che associa alla matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ alla funzione f definita come prima. Si verifica facilmente che $\phi(AB) = \phi(A) \circ \phi(B)$, ossia questa mappa è un morfismo di gruppi, e che $\phi(A) = \phi(B)$ se e solo se $A = B$ oppure $A = -B$. Segue che $\ker(\phi) = \{I, -I\}$, per cui ϕ induce un isomorfismo tra $\mathrm{PSL}(2, 7)$ e $\mathrm{SLF}(7)$, che nel seguito identificheremo.

Cerchiamo ora un sistema di generatori conveniente per $\mathrm{PSL}(2, 7)$, utilizzando la descrizione funzionale appena vista. Definiamo tre trasformazioni speciali di Möbius r, t, δ come:

- $r(k) = -1/k$, la mappa di "riflessione";
- $t(k) = k + 1$, la mappa di "traslazione";
- $\delta(k) = 2k$, la mappa di "duplicazione".

Proposizione 2.2.1. $\mathrm{SLF}(7)$ *è generato da* r, t *e* δ.

Dimostrazione. Consideriamo una generica trasformazione di Möbius speciale della forma $f(k) = (ak + b)/(ck + d)$. Se $c = 0$, necessariamente $ad = 1$ e quindi $d = a^{-1}$, così $f(k) = a^2k + ab$. I quadrati $\neq 0$ modulo 7 sono 1,2 e 4, quindi $f = t^{ab} \circ \delta^j$ per un opportuno $j \in \{1, 2, 4\}$.

Se $c \neq 0$, dividendo otteniamo

$$f(k) = (ac^{-1}) + \frac{bc - ad}{c(ck + d)} = (ac^{-1}) + \frac{-1}{c^2k + cd}.$$

Scriviamo $c^2 = 2^j$. Risulta che $f = t^{ac^{-1}} \circ r \circ t^{cd} \circ \delta^j$, per cui SLF(7) è generato da r, t e δ. □

2.3 L'isomorfismo

Per provare l'isomorfismo tra PSL$(2,7)$ e GL$(3,2)$, usiamo le descrizioni funzionali appena viste di questi gruppi: sarà sufficiente trovare un isomorfismo tra SLF(7) e GL$(\mathbb{F}_8)$.

Osservazione. Ponendo $x^\infty = 0$, risulta che $\mathbb{F}_8 = \{x^k : k \in \overline{\mathbb{F}_7}\}$.

L'osservazione ci suggerisce un modo, data una funzione con dominio $\overline{\mathbb{F}_7}$, per provare a costruire una mappa con dominio $\mathbb{F}_8$. Per un primo tentativo possiamo usare $x^k \mapsto x^{f(k)}$. Sfortunatamente questa non è sempre lineare, dato che manda lo zero in zero solamente se $f(\infty) = \infty$. Grazie alla caratteristica 2, possiamo ovviare a questo problema facendo una semplice correzione, che è $x^k \mapsto x^{f(k)} + x^{f(\infty)}$.

Definiamo T : SLF(7) $\to$ GL$(\mathbb{F}_8)$ tale che, per ogni funzione $f \in$ SLF(7), $T(f) = T_f$ dove

$$T_f(x^k) = x^{f(k)} + x^{f(\infty)}, \quad k \in \overline{\mathbb{F}_7}. \tag{2.1}$$

Come già osservato, con questa definizione si ha sempre $T_f(0) = 0$, ma, per poter dire che l'applicazione sia ben posta, dobbiamo verificare che T_f appartenga effettivamente a GL$(\mathbb{F}_8)$.

Utilizziamo il sistema di generatori trovato prima calcolando $T(r), T(t)$ e $T(\delta)$. Se queste tre appartengono a GL$(\mathbb{F}_8)$, allora sarà così per ogni funzione in SLF(7).

Osservazione. Dal momento che $x^3 + x + 1 = 0$ in $\mathbb{F}_8$, valgono:

$$x^3 = x + 1, \quad x^4 = x^2 + x, \quad x^5 = x^2 + x + 1, \quad x^6 = x^2 + 1.$$

Utilizziamo la seguente comoda notazione: rappresentiamo un elemento in $\mathbb{F}_8$ della forma $b_2x^2 + b_1x^1 + b_0x^0$ con la stringa $b_2b_1b_0$. In questo modo abbiamo:

$$x^0 = 001, \qquad x^1 = 010, \qquad x^2 = 100, \qquad x^3 = 011,$$

$$x^4 = 110, \qquad x^5 = 111, \qquad x^6 = 101, \qquad x^\infty = 000.$$

La funzione $r(k) = -1/k$ agisce in $\overline{\mathbb{F}_7}$ in questo modo:

$$r = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \\ \infty & 6 & 3 & 2 & 5 & 4 & 1 & 0 \end{pmatrix}.$$

Inseriamo queste relazioni in (2.1), possiamo concludere che:

$$T(r) = \begin{pmatrix} 001 & 010 & 100 & 011 & 110 & 111 & 101 & 000 \\ 001 & 100 & 010 & 101 & 110 & 111 & 011 & 000 \end{pmatrix}.$$

Notiamo che T_r scambia i primi due bit, quindi è la mappa lineare e invertibile in $\mathbb{F}_8$ scambia i vettori di base x^1 e x^2. Inoltre la matrice associata a T_r nella base $B = \{x^0, x^1, x^2\}$ è

$$\big[T(r)\big]_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = A_1.$$

Per quanto riguarda T_t, notiamo innanzitutto che $T_t(0) = 0$ e, per $k \neq \infty$,

$$T_t(x^k) = x^{t(k)} + x^{t(\infty)} = x^{k+1} = x(x^k).$$

Quindi T_t è la moltiplicazione a sinistra per x in $\mathbb{F}_8$. Questa è lineare, grazie alla proprietà distributiva, e invertibile e ha come inversa la moltiplicazione a sinistra per $x^{-1} = x^6$. La matrice associata a T_t è

$$\big[T(t)\big]_B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = A_2.$$

Infine, $T_\delta(0) = 0$ e, per $k \neq \infty$, $T_\delta(x^k) = x^{2k} = (x^k)^2$. Quindi T_δ è l'elevamento al quadrato in $\mathbb{F}_8$. Questa mappa è lineare e morfismo di anelli dal momento che lavoriamo in caratteristica 2. Inoltre è biunivoca poiché il nucleo contiene come unico elemento lo zero. La matrice di T_δ è

$$\big[T(\delta)\big]_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = A_3.$$

Finalmente abbiamo concluso le nostre verifiche e sappiamo che l'applicazione T è ben posta.

Teorema 2.3.1. $\mathrm{PSL}(2,7)$ *e* $\mathrm{GL}(3,2)$ *sono isomorfi.*

Dimostrazione. Dimostriamo che $\mathrm{SLF}(7)$ e $\mathrm{GL}(\mathbb{F}_8)$ sono isomorfi, provando che la mappa T definita in (2.1) è un isomorfismo. Verifichiamo innanzitutto che sia un morfismo. Siano $f, g \in \mathrm{SLF}(7)$. Per ogni $k \in \overline{\mathbb{F}_7}$, si ha:

$$\begin{aligned} T_f \circ T_g(x^k) &= T_f(x^{g(k)} + x^{g(\infty)}) \\ &= T_f(x^{g(k)}) + T_f(x^{g(\infty)}) \quad (\text{linearità di } T_f) \\ &= (x^{f(g(k))} + x^{f(\infty)}) + (x^{f(g(\infty))} + x^{f(\infty)}) \\ &= x^{f(g(k))} + x^{f(g(\infty))} \\ &= T_{f\circ g}(x^k). \end{aligned}$$

Inoltre, l'immagine di T è generata da $T(r)$, $T(t)$ e $T(\delta)$, quindi da A_1, A_2 e A_3, che sappiamo generare tutto $\mathrm{GL}(\mathbb{F}_8)$. Abbiamo la suriettività, ma conosciamo già dal Lemma 1.1.4 che 168 è la cardinalità di entrambi i gruppi, quindi è una corrispondenza biunivoca. Mettendo insieme le cose, T è un isomorfismo. □

Una cosa notevole da osservare, è che dalla Proposizione 1.1.5 otteniamo una catena ben più lunga di isomorfismi:

$$\mathrm{PSL}(2,7) \cong \mathrm{GL}(3,2) \cong \mathrm{SL}(3,2) \cong \mathrm{PGL}(3,2) \cong \mathrm{PSL}(3,2).$$

Capitolo 3

Il Piano di Fano

Premettiamo subito che questo capitolo sarà una digressione di geometria proiettiva. Abbiamo già visto che $\mathrm{PSL}(2,7)$ è isomorfo a $\mathrm{PGL}(3,2)$; quest'ultimo, come vedremo, è il gruppo degli automorfismi del cosiddetto piano di Fano, in onore del matematico italiano Gino Fano. In particolare capiremo anche il collegamento tra i gruppi proiettivi lineari e i piani proiettivi. Tutto questo ci permetterà di studiare $\mathrm{PSL}(2,7)$ mediante semplici ragionamenti fatti su dei disegni.

3.1 Piani proiettivi astratti

Definizione 3.1.1. Un *piano proiettivo astratto* è una terna ordinata $(\mathcal{P}, \mathcal{R}, \mathcal{I})$ dove $\mathcal{P}$ è un insieme non vuoto i cui elementi sono detti punti, $\mathcal{R}$ è un insieme non vuoto i cui elementi sono detti rette, ed $\mathcal{I}$ è una relazione tra punti e rette, detta *incidenza*, tali che:

i) due punti distinti sono incidenti ad una ed una sola retta;

ii) per ogni coppia di rette distinte esiste un punto incidente ad entrambe;

iii) esistono quattro punti tre a tre non allineati, cioè nessuna retta è incidente a tre dei quattro punti.

Definizione 3.1.2. Due piani proiettivi $(\mathcal{P}, \mathcal{R}, \mathcal{I})$ e $(\mathcal{P}', \mathcal{R}', \mathcal{I}')$ si dicono *isomorfi* se esistono due biiezioni $\phi : \mathcal{P} \to \mathcal{P}'$ e $\psi : \mathcal{R} \to \mathcal{R}'$ tali che per ogni $P \in \mathcal{P}$, per

ogni $r \in \mathcal{R}$, $P\mathcal{I}r$ se e solo se $\phi(P)\mathcal{I}'\psi(r)$. Un isomorfismo di un piano con se stesso è detto *automorfismo* o *proiettività* o *collineazione*. Gli automorfismi formano un gruppo rispetto alla composizione, che denotiamo $\mathrm{Aut}(\mathcal{P})$.

Proposizione 3.1.3. *Dato il piano proiettivo $(\mathcal{P}, \mathcal{R}, \mathcal{I})$, è dato un altro piano proiettivo definito da $(\mathcal{R}, \mathcal{P}, \mathcal{I}^t)$, in cui $r\,\mathcal{I}^t\,P$ se e solo se $P\,\mathcal{I}\,r$, per ogni $r \in \mathcal{R}$ e $P \in \mathcal{P}$.*

Dimostrazione. I tre assiomi consentono questa simmetria di situazioni:

i) Due rette distinte sono incidenti ad uno ed un solo punto, la cui esistenza segue dall'assioma 2 e l'unicità dall'assioma 1.

ii) Due punti distinti sono incidenti ad una retta per l'assioma 1.

iii) Esistono quattro rette a tre a tre non incidenti ad uno stesso punto. Siano infatti A, B, C, D punti che soddisfano l'assioma 3. Le quattro rette AB, BC, CD, DA a tre a tre non passano per uno stesso punto.

□

Definizione 3.1.4. Il piano $(\mathcal{R}, \mathcal{P}, \mathcal{I}^t)$ definito in 3.1.3 si dice *duale* del piano $(\mathcal{P}, \mathcal{R}, \mathcal{I})$. Nel caso un piano e il suo duale sono isomorfi, si dice *autoduale*.

Esempio 3.1.5 (Piano di Fano)**.** Il primo esempio di piano proiettivo, che è quello a cui è dedicato il capitolo, si ottiene dal disegno in figura 3.1, che raffigura un triangolo equilatero, detto *piano di Fano*.

- I *punti* sono i sette punti geometrici costituiti dai vertici, l'incentro e i punti medi dei lati.
- Le *rette* sono i lati, le mediane e la circonferenza inscritta, sette anch'esse.
- L'incidenza è quella geometrica.

La verifica degli assiomi è immediata. In particolare i tre vertici e l'incentro soddisfano il terzo assioma. Chiaramente il piano di Fano è autoduale.

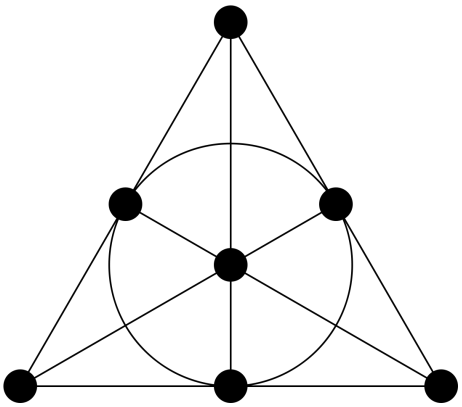


Figura 3.1: Il piano di Fano

Esempio 3.1.6. Dato F un campo, un esempio di piano proiettivo si ha considerando nello spazio vettoriale F^3:

- *punti*: le rette vettoriali, ossia i sottospazi di dimensione 1, o le rette per l'origine;
- *rette*: i piani vettoriali, ossia i sottospazi di dimensione 2, o i piani per l'origine;
- *incidenza*: l'inclusione.

Ogni retta per l'origine si individua mediante un suo vettore (x_0, y_0, z_0) non nullo, detto *vettore direttore*, ogni altro suo punto è del tipo $a(x_0, y_0, z_0) = (ax_0, ay_0, az_0)$ per $a \in F$ e possiamo rappresentarla con $[x_0, y_0, z_0]$, che è anche la rappresentazione del punto proiettivo corrispondente alla retta vettoriale. Ovviamente ogni terna proporzionale individua lo stesso punto.

Ogni piano per l'origine ha equazione $ax + by + cz = 0$ con a, b, c tre coefficienti non tutti nulli e individuati a meno di un fattore di proporzionalità. Possiamo rappresentare la retta con la scrittura $[a, b, c]$, analogamente al caso di prima.

L'incidenza del punto proiettivo $[x_0, y_0, z_0]$ con la retta $[a, b, c]$ è semplicemente data da $ax_0 + by_0 + cz_0 = 0$, poiché se un punto della retta vettoriale diverso dall'origine appartiene al piano vettoriale, tutti gli altri punti della retta vettoriale gli appartengono.

Verifichiamo ora che siano soddisfatti gli assiomi:

i) Due rette vettoriali distinte individuano un piano ed uno solo, quello che i loro vettori direttori generano. Pertanto, due punti proiettivi individuano una retta proiettiva ed una sola.

ii) Due piani vettoriali distinti di F^3 si intersecano necessariamente lungo una retta vettoriale, data dal sistema delle loro equazioni. Dunque per ogni coppia di rette proiettive distinte, queste sono incidenti ad un punto proiettivo.

iii) Le rette con vettore direttore $[1,0,0],[0,1,0],[0,0,1],[1,1,1]$ sono a tre a tre non complanari, e quindi abbiamo quattro punti proiettivi a tre a tre non incidenti ad una sola retta proiettiva.

Denotiamo questo piano proiettivo con $\mathcal{P}^2(F)$, e, nel caso $F = \mathbb{F}_q$, scriviamo $\mathcal{P}^2(q)$.

Studiamo ora il piano proiettivo $\mathcal{P}^2(2)$. Poiché $\mathbb{F}_2 = \{0,1\}$, abbiamo in totale otto vettori a disposizione in $(\mathbb{F}_q)^3$, sette escludendo la terna nulla, ciascuno dei quali individua un punto proiettivo. Cerchiamo la relazione con il piano di Fano.

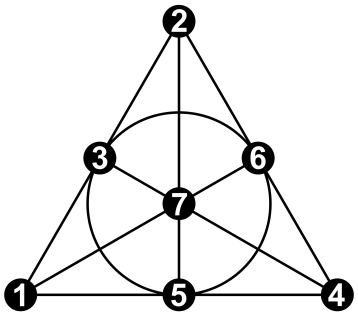


Figura 3.2

Dopo aver numerato i punti come in Figura 3.2, identifichiamo i tre vertici del triangolo con le terne $\underline{1} = (1,0,0)$, $\underline{2} = (0,1,0)$, $\underline{4} = (0,0,1)$. La retta incidente i vertici $\underline{1}$ e $\underline{2}$ ha così equazione $z = 0$; il punto $\underline{3}$ su questa retta ha la terza coordinata nulla, e poiché la terna $(0,0,0)$ non è ammessa, la sola disponibile è $(1,1,0)$. Analogamente, la retta per $\underline{2}$ e $\underline{4}$ ha equazione $x = 0$, dunque il punto

$\underline{6}$ ha coordinate $(0,1,1)$. La retta per $\underline{1}$ e $\underline{4}$ ha equazione $y=0$ e il punto $\underline{5}$ ha coordinate $(1,0,1)$. Per il punto $\underline{7}$ resta la sola possibilità $(1,1,1)$. Osserviamo che i tre punti sulla mediana per $\underline{1}$ hanno la seconda e la terza coordinata uguali, ossia $y=z$ oppure, tenuto conto che siamo in caratteristica 2, l'equazione diventa $y+z=0$. Analogamente per le altre due mediane risultano rispettivamente $x=y$ e $x=z$ e per la retta passante per $\underline{3}$, $\underline{5}$ e $\underline{6}$ si ha $x+y+z=0$.

Segue quindi che i sette punti e le sette rette del piano di Fano hanno coordinate ed equazioni identiche a quelle di $\mathcal{P}^2(2)$, ed anche l'incidenza punto-retta è la stessa, per costruzione. Possiamo dire quindi che i due piani sono in realtà uno stesso piano descritto in modo diverso: algebrico per $\mathcal{P}^2(2)$ e combinatorio per il piano di Fano. Più tecnicamente, i due piani sono isomorfi.

Per concludere la sezione, vale la pena fare un'osservazione piuttosto ovvia. Il piano di Fano è il più piccolo piano proiettivo finito che si può costruire, infatti la proprietà iii) cadrebbe se fossimo su un campo costituito da un solo elemento.

3.2 Il gruppo delle proiettività

Vediamo il teorema di collegamento tra i gruppi proiettivi lineari, visti nel primo capitolo, e il gruppo delle proiettività di un piano costruito su F^3.

Teorema 3.2.1. $\mathrm{Aut}(\mathcal{P}^2(F)) \cong \mathrm{PGL}(3,F)$.

Dimostrazione. Sia $T : \mathrm{GL}(3,F) \to \mathrm{Aut}(\mathcal{P}^2(F))$, definita da $T(A) = T_A$, dove $T_A : \mathcal{P}^2(F) \to \mathcal{P}^2(F)$ tale che $T_A([x,y,z]) = [x',y',z']$ e $(x',y',z') = A(x,y,z)$. Si verifica facilmente che T è ben definita, che è un omomorfismo e $\mathrm{Ker}\, T = Z(\mathrm{GL}(3,F))$. Passando al quoziente si conclude. □

Dal Teorema 3.2.1 segue che il gruppo degli automorfismi del piano di Fano è isomorfo a $\mathrm{PGL}(3,2) \cong \mathrm{GL}(3,2) \cong \mathrm{PSL}(2,7)$. Cerchiamo di capire meglio come questo gruppo agisce sul piano.

Proposizione 3.2.2. *L'azione di* $\mathrm{PGL}(3,F)$ *è 2-transitiva su* $\mathcal{P}^2(F)$.

Dimostrazione. Siano x, y, z, t vettori in $F^3 \setminus \{0\}$ tali che in $\mathcal{P}^2(F)$ valgano

$$[x_1, x_2, x_3] \neq [y_1, y_2, y_3] \quad \text{e} \quad [z_1, z_2, z_3] \neq [t_1, t_2, t_3].$$

Quindi x e y sono linearmente indipendenti in F^3 e lo stesso vale per z e t. Così possiamo estendere $\{x, y\}$ e $\{z, t\}$ a due basi di F^3 ed esiste una matrice tale che l'immagine di x è z e quella di y è t. La corrispondente proiettività è tale che $[z_1, z_2, z_3]$ e $[t_1, t_2, t_3]$ sono le rispettive immagini di $[x_1, x_2, x_3]$ e $[y_1, y_2, y_3]$. □

Osservazione. L'azione non è necessariamente 3-transitiva, poiché se prendiamo x, y e $x + y$, questi non possono avere come immagine in tre vettori indipendenti qualsiasi.

Ora che abbiamo tutti gli ingredienti, costruiamo esplicitamente un automorfismo del piano di Fano.

Teniamo come numerazione quella in Figura 3.2 e chiamiamo α il nostro automorfismo. Poiché per la Proposizione 3.2.2 si ha che $\mathrm{PGL}(3, F)$ è 2-transitivo, abbiamo 7 scelte per il trasformato di $\underline{1}$ e 6 scelte per il trasformato di $\underline{2}$, per un totale di 42 possibilità. Fissati $\alpha(\underline{1})$ e $\alpha(\underline{2})$, questi individuano una retta e di conseguenza non abbiamo libertà di scelta per $\alpha(\underline{3})$, che deve incidervi, confermando la non 3-transitività del gruppo degli automorfismi di questo piano. I quattro punti rimanenti sono congiunti da rette in tutti i modi possibili con i tre punti $\underline{1}$, $\underline{2}$, $\underline{3}$, quindi per $\alpha(\underline{4})$ ci possono essere 4 scelte. Infine, osserviamo che per i restanti tre punti la scelta è obbligata, in quanto sono tutti terzi punti di rette già determinate. Questo lo impone anche il fatto che per la quaterna $(\alpha(\underline{1}), \alpha(\underline{2}), \alpha(\underline{3}), \alpha(\underline{4}))$ abbiamo già fatto $42 \cdot 4 = 168$ scelte, esaurendo tutte le possibilità.

Osservazione. Possiamo vedere il gruppo di automorfismi del piano di Fano, come gruppo di permutazioni che agiscono su 7 elementi, per cui $\mathrm{PSL}(2, 7)$ è isomorfo a un sottogruppo di S_7.

Pensare in termini di permutazioni risulta molto utile al fine di capire come si relazionano gli elementi di $\mathrm{PSL}(2, 7)$.

Capitolo 4

Una realizzazione come gruppo di Galois

L'obiettivo di questo capitolo è cercare una realizzazione di $\mathrm{PSL}(2,7)$ come gruppo di Galois di un polinomio sui razionali. Vedremo esplicitamente un esempio in cui questo accade. Partiamo prima da concetti e risultati di base di teoria di Galois, poi avremo bisogno di un risultato che richiede un po' di lavoro e a cui dedicheremo la seconda sezione per intero.

4.1 Gruppi di Galois e alcune proprietà

Senza addentrarci nello specifico nella teoria di Galois, ricordiamo solamente nozioni essenziali e proprietà che ci torneranno utili. Per le dimostrazioni, si veda [4].

Definizione 4.1.1. Siano F un campo e $x_1, \dots, x_n$ indeterminate. Definiamo

$$\begin{aligned}
\sigma_1 &= x_1 + \cdots + x_n \\
&\vdots \\
\sigma_r &= \sum_{1 \le i_1 < \cdots < i_r \le n} x_{i_1} x_{i_2} \cdots x_{i_r} \\
&\vdots \\
\sigma_n &= x_1 x_2 \cdots x_n
\end{aligned}$$

i *polinomi simmetrici elementari*. $\sigma_1, \dots, \sigma_n \in F[x_1, \dots, x_n]$.

Proposizione 4.1.2. *Sia $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ un polinomio monico di grado $n > 0$ a coefficienti in un campo F. Se P ha radici $\alpha_1, \dots, \alpha_n$ nel suo campo di spezzamento, allora i coefficienti di P si esprimono in termini delle sue radici come*

$$a_{n-r} = (-1)^r \sigma_r(\alpha_1, \dots, \alpha_n)$$

per ogni $r = 1, \dots, n$.

Corollario 4.1.3. *Se $P \in F[x]$ è un polinomio monico di grado $n > 0$ con radici $\alpha_1, \dots, \alpha_n$ nel suo campo di spezzamento, allora $\sigma_r(\alpha_1, \dots, \alpha_n) \in F$ per $r = 1, \dots, n$.*

Definizione 4.1.4. Sia F un campo e siano $x_1, \dots, x_n$ indeterminate. Un polinomio $P \in F[x_1, \dots, x_n]$ si dice *simmetrico* se per ogni $\sigma \in S_n$ si ha

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

Teorema 4.1.5. *Ogni polinomio simmetrico in $F[x_1, \dots, x_n]$ si può scrivere come un polinomio nelle $\sigma_1, \dots, \sigma_n$ a coefficienti in F e tale scrittura è unica.*

Corollario 4.1.6. *Se $P \in F[x]$ è un polinomio monico di grado $n > 0$ con radici $\alpha_1, \dots, \alpha_n$ nel suo campo di spezzamento, allora per ogni polinomio simmetrico $P(x_1, \dots, x_n)$ a coefficienti in F vale $P(\alpha_1, \dots, \alpha_n) \in F$.*

Definizione 4.1.7. Consideriamo un'estensione di campi $F \leq L$ e definiamo

$$\mathrm{Gal}(L/F) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(a) = a \text{ per ogni } a \in F\}.$$

Chiaramente questo è un gruppo rispetto alla composizione di funzioni e si chiama *gruppo di Galois* dell'estensione.

Se P è un polinomio in $F[x]$ e L è il suo campo di spezzamento, poniamo $\mathrm{Gal}(P) = \mathrm{Gal}(L/F)$.

Proposizione 4.1.8. *Siano $F \leq L$ è un'estensione finita e $\sigma \in \mathrm{Gal}(L/F)$. Valgono:*

i) Se $P \in F[x]$ è un polinomio non costante e α è una sua radice, allora $\sigma(\alpha)$ è anch'essa una radice di P.

ii) Se $L = F(a_1, \ldots, a_n)$, allora σ è univocamente determinata dai suoi valori in $a_1, \ldots, a_n$.

Proposizione 4.1.9. *Siano $F \leq L$ è un'estensione finita, sono equivalenti:*

i) L è il campo di spezzamento di un polinomio separabile in $F[x]$.

ii) $\left|\mathrm{Gal}(L/F)\right| = [L : F]$.

Definizione 4.1.10. Se valgono le precedenti condizioni equivalenti, l'estensione si dice *di Galois*.

Sia $P \in F[x]$ un polinomio separabile con radici $a_1, \ldots, a_n$ in L, il suo campo di spezzamento. In questa situazione, abbiamo una mappa $\mathrm{Gal}(L/F) \to S_n$ così definita: data $\sigma \in \mathrm{Gal}(L/F)$, per la Proposizione 4.1.8, $\sigma(a_i)$ è ancora radice di P, quindi $\sigma(a_i) = a_{\tau(i)}$ per qualche $\tau(i) \in \{1, \ldots, n\}$. Notiamo che $\tau(i)$ è univocamente determinata dal momento che le radici sono distinte e, poiché σ è un automorfismo, la mappa $\tau : \{1, \ldots, n\} \to \{1, \ldots, n\}$ è una corrispondenza biunivoca. Abbiamo così definito l'immagine di σ come τ che è una permutazione di S_n.

Si vede subito che la mappa appena descritta è un morfismo. Inoltre, dalla Proposizione 4.1.8, segue immediatamente l'iniettività. Questo ci permette di enunciare il seguente teorema.

Teorema 4.1.11. *Se $F \leq L = F(a_1, \ldots, a_n)$ è un'estensione di Galois, allora* $\mathrm{Gal}(L/F)$ *è isomorfo a un sottogruppo di S_n.*

Lemma 4.1.12. *Sia L il campo di spezzamento di un polinomio in $F[x]$ e sia $P \in F[x]$ irriducibile con due radici $\alpha, \beta \in L$. C'è un isomorfismo di campi $\sigma : L \to L$ che è l'identità su F e $\sigma(\alpha) = \beta$.*

Lemma 4.1.13. *Sia $P \in F[x]$ un polinomio separabile di grado n. Il sottogruppo di S_n corrispondente a* $\mathrm{Gal}(P)$ *è transitivo se e solo se P è irriducibile su F.*

Dimostrazione. Siano $a_1, \ldots, a_n$ le radici di P nel suo campo di spezzamento che denotiamo L. Queste sono tutte distinte.

Supponiamo prima che P sia irriducibile su F. Presi $i, j \in \{1, \ldots, n\}$, per il Lemma 4.1.12 possiamo costruire un automorfismo σ di L tale che $\sigma(a_i) = a_j$ ed è l'identità ristretto ad F. Così, $\sigma \in \mathrm{Gal}(P)$ e la permutazione se τ è la permutazione corrispondente in S_n si ha $\tau(i) = j$. Questo implica che $\mathrm{Gal}(P)$ dà un sottogruppo transitivo di S_n.

Viceversa, supponiamo che $\mathrm{Gal}(P)$ corrisponda ad un sottogruppo transitivo di S_n, e sia $\hat{P}$ un fattore irriducibile di P su F. Dal momento che $\hat{P}$ non è costante, possiamo trovare i tale che $\hat{P}(a_i) = 0$. Sia ora $j \in \{1, \ldots, n\}$. Per transitività, esiste $\sigma \in \mathrm{Gal}(P)$ tale che $\sigma(a_i) = (a_j)$, che è ancora una radice di $\hat{P}$ per la Proposizione 4.1.8. Questo prova che $\hat{P} = P$. □

Definizione 4.1.14. Se $P \in F[x]$ è un polinomio monico di grado $n \geq 2$ e con radici $a_1, \ldots, a_n$ nel suo campo di spezzamento, il *discriminante* di P è definito come

$$\Delta(P) = \prod_{1 \leq i < j \leq n} (a_j - a_i)^2.$$

Teorema 4.1.15. *Sia $P \in F[x]$ monico e di grado $n \geq 2$. Valgono le seguenti:*

i) $\Delta(P) \in F$.

ii) Se $\mathrm{char}\, F \neq 2$ *e $G \leq S_n$ è isomorfo a* $\mathrm{Gal}(P)$*, allora $G \leq A_n$ se e solo se* $\Delta(P)$ *è un quadrato in F.*

Lemma 4.1.16. *Sia $P \in \mathbb{Q}[x]$ un polinomio monico di grado $n > 1$ con radici $\{a_i\}_{i=1,\dots,n}$ e sia $K_1 = \mathbb{Q}(a_1, \dots, a_n)$ il suo campo di spezzamento. Sia $0 < r < n$ e $K_2 = \mathbb{Q}(b_1, \dots, b_m)$, dove $m = \binom{n}{r}$ e i $\{b_j\}_{j=1,\dots,m}$ sono somme di elementi distinti di $\{a_i\}_{i=1,\dots,n}$ presi r alla volta. Allora $K_1 = K_2$.*

Dimostrazione. Per $r = 1$ il risultato è ovvio. Supponiamo $r > 1$, chiaramente $K_2 \leq K_1$. Sia $c_i = \sum b_j$ dove la somma è ristretta ai soli b_j che contengono a_i. Allora

$$\begin{aligned} c_i =& \binom{n-1}{r-1} a_i + \binom{n-2}{r-2} \sum_{j \neq i} a_j \\ =& \binom{n-2}{r-1} a_i + \binom{n-2}{r-2} \sum_{j} a_j \end{aligned}$$

Il secondo addendo è un polinomio simmetrico nelle a_j, per cui, per il Corollario 4.1.6, è un elemento di $\mathbb{Q}$. Segue che K_2 contiene un multiplo non nullo di a_i, quindi a_i stesso. Dal momento che vale per ogni i, concludiamo $K_2 \leq K_1$. □

Lemma 4.1.17. *Usando le stesse notazioni del lemma precedente, con $n > 1$. Supponiamo che P_m sia il polinomio di grado m che ha come radici $\{b_j\}_{j=1,\dots,m}$. Se $\mathrm{Gal}(P)$ è il gruppo alterno A_n, allora P_m è un polinomio irriducibile su $\mathbb{Q}$ per ogni $0 < r < n$.*

Dimostrazione. Se $r \leq n-2$, dato che A_n è $(n-2)$-transitivo, $\mathrm{Gal}(P_m)$ è transitivo sulle radici di P_m. Se $r = n-1$, A_n è ancora transitivo sugli insiemi di cardinalità r (non ordinati), perché lo è sui loro complementari. La conclusione segue dal Lemma 4.1.13. □

Corollario 4.1.18. *Se P è irriducibile ed ha gruppo di Galois che non è transitivo sugli insiemi di cardinalità r delle sue radici, allora il polinomio P_m associato è riducibile.*

Dimostrazione. Abbiamo che P è separabile poiché $\mathrm{char}\,\mathbb{Q} = 0$ e $\mathrm{Gal}(P_m)$ non è transitivo sulle radici di P_m. Si conclude per il Lemma 4.1.13. □

4.2 PSL(2, 7) e il gruppo alterno

Lo scopo di questa sezione è dimostrare il seguente asserto.

Teorema 4.2.1. *Se $G \leq A_7$ contiene un 7-ciclo e una permutazione prodotto di due trasposizioni disgiunte, allora G è isomorfo a* $\mathrm{PSL}(2,7)$ *oppure $G = A_7$.*

Per dimostrare ciò, abbiamo bisogno di alcuni risultati preliminari.

Osservazione. Siano $\sigma = (a_1, a_2, \dots, a_7)$ e $\tau = (1, b_2, \dots, b_k)(c_1, \dots, c_j)\dots$ rispettivamente un 7-ciclo e una permutazione non banale in A_7 e consideriamo $G = \langle \sigma, \tau \rangle$. A meno di rinumerare i sette elementi, che significa coniugare G con una opportuna permutazione in S_7, possiamo supporre che σ sia esattamente $(1, 2, \dots, 7)$ e contemporaneamente $\tau = (1, b_2, \dots, b_k)(c_1, \dots, c_j)\dots$. Poiché A_7 è normale in S_7, ciò che troveremo è un coniugato di G che è ancora sottogruppo di A_7.

A meno di sostituire σ con $\sigma^{b_2 - 1} = (1, b_2, \dots)$, dato che questo è ancora un 7-ciclo che genera lo stesso sottogruppo di σ, riusciamo a supporre infine che $\sigma = (1, 2, \dots, 7)$ e $\tau = (1, 2, \dots)(c_1, \dots, c_j)\dots$ valgano entrambe.

Definizione 4.2.2. Siano $\sigma_1, \dots, \sigma_r, \tau, \tau', \pi$ permutazioni in S_n. Diremo che τ' è *simmetrica di τ nei generatori $\sigma_1, \dots, \sigma_r$ mediante rinumerazione π* se valgono:

- π normalizza $\langle \sigma_1, \dots, \sigma_r \rangle$, cioé $\pi^{-1}\langle \sigma_1, \dots, \sigma_r \rangle \pi = \langle \sigma_1, \dots, \sigma_r \rangle$;
- τ' si ottiene da $\pi^{-1}\tau\pi$ per coniugio con varie potenze di $\sigma_1, \dots, \sigma_r$ e inversione.

In tutti in cui non ci sarà ambiguità ometteremo di specificare generatori e/o rinumerazione.

Osservazione. Ovviamente la definizione può essere letta anche come τ è simmetrica di τ' mediante la rinumerazione π^{-1}. Se π ha ordine 2, allora possiamo dire che τ e τ' sono *simmetriche* mediante π.

A motivare la precedente definizione sono i lemmi che seguono. Prendiamo $\sigma_1, \dots, \sigma_r, \tau, \tau', \pi$ permutazioni in S_n, con τ' simmetrica di τ nei i generatori $\sigma_1, \dots, \sigma_r$ mediante la rinumerazione π.

Lemma 4.2.3. *$\langle \sigma_1, \dots, \sigma_r, \tau \rangle$ e $\langle \sigma_1, \dots, \sigma_r, \tau' \rangle$ sono isomorfi.*

Dimostrazione. Segue immediatamente dalle proprietà della definizione che i due gruppi si ottengono uno dall'altro per coniugio mediante π. □

Lemma 4.2.4. *$\tau \in \langle \sigma_1, \dots, \sigma_r \rangle$ se e solo se $\tau' \in \langle \sigma_1, \dots, \sigma_r \rangle$.*

Dimostrazione. Abbiamo che $\tau \in \langle \sigma_1, \dots, \sigma_r \rangle$ se e solo se

$$\pi^{-1}\tau\pi \in \pi^{-1}\langle \sigma_1, \dots, \sigma_r \rangle \pi = \langle \sigma_1, \dots, \sigma_r \rangle$$

se e solo se $\tau' \in \langle \sigma_1, \dots, \sigma_r \rangle$. □

L'idea è quella di avere un modo per semplificare lo studio per casi: vogliamo stabilire quando delle permutazioni, che non riusciamo a ricondurre a casi già affrontati solamente con operazioni di coniugio e inversione, si comportano comunque in modo analogo.

Osserviamo che $\sigma = (1, 2, \dots, 7)$ e notiamo che $\sigma^{-1} = (7, 6, \dots, 1)$, per cui $\langle \sigma \rangle$ è normalizzato dalla permutazione

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

cioè $\pi^{-1}\langle \sigma \rangle \pi = \langle \sigma \rangle$. Da qui in avanti, utilizziamo questa rinumerazione, che ci permetterà di ridurre le prossime dimostrazioni ad un semplice studio per casi.

Lemma 4.2.5. *A_7 è generato da un 7-ciclo e un 3-ciclo.*

Dimostrazione. Vediamo innanzitutto che A_7 è generato da $\sigma = (1, 2, \dots, 7)$ e $\tau = (1, 2, 3)$. Notiamo che

$$\pi^{-1}\tau\pi = (7, 6, 5) = \sigma^3(1, 3, 2)\sigma^{-3} = \sigma^3\tau^{-1}\sigma^{-3}$$

per cui π normalizza $G = \langle \sigma, \tau \rangle$.

Mostriamo che tutti i 3-cicli di A_7 appartengono a G e utilizziamo il Lemma 1.2.2 per concludere. Sia $\alpha = \sigma^{-2}\tau\sigma^2 = (3, 4, 5) \in G$. Risulta che

$$\alpha^{-1}\tau\alpha = (1, 2, 4) \in G, \qquad \alpha\tau\alpha^{-1} = (1, 2, 5) \in G.$$

Analogamente $(1,2,6) \in G$ per il Lemma 4.2.4, in quanto è simmetrica di $(1,2,4)$. $(1,2,7) \in G$ poiché si ottiene coniugando τ con σ.

Ora, tutti i 3-cicli $(i,j,k) \in A_7$ dove due indici sono contigui possono essere ricondotti ad una permutazione del tipo $(1,2,k)$ coniugando tramite σ o per simmetria, quindi per il Lemma 4.2.4 sono in G. Se gli indici non sono contigui a due a due, a meno di coniugio con potenze di σ possiamo supporre che il 3-ciclo sia della forma $(1,j,k)$ con $2 < j < k-1 < 6$. Abbiamo solo tre casi che sono $(1,3,5)$, $(1,3,6)$ e $(1,4,6)$ e ognuno può essere ricavato dagli altri coniugando mediante σ. Risulta che

$$(1,3,5) = (2,3,6)^{-1}(1,2,5)(2,3,6) \in G$$

e quindi possiamo concludere che $G = A_7$.

Tornando al caso generale, come osservato precedentemente, possiamo supporre solamente che presi un 7-ciclo e un 3-ciclo in A_7 questi siano $\sigma = (1,2,\ldots,7)$ e $\tau = (1,2,k)$ con $3 \leq k \leq 7$. Vediamo che in ogni caso risulta che $(1,2,3) \in G = \langle \sigma, \tau \rangle$. Se $k = 3$ non c'è niente da mostrare. Studiamo i casi $k = 4,5$ e, come visto prima, $k = 6,7$ si ottengono dai precedenti rispettivamente per simmetria con $(1,2,4)$ e coniugando per σ il ciclo $(1,2,3)$ e in questo caso si potrà concludere per il Lemma 4.2.3. Se $\tau = (1,2,4)$:

$$\sigma^{-2}\tau\sigma^2 = (3,4,6) \qquad \text{e} \qquad (3,4,6)\tau(3,4,6)^{-1} = (1,2,3).$$

Se $\tau = (1,2,5)$:

$$\sigma^{-1}\tau\sigma = (2,3,6) \qquad \text{e} \qquad \sigma^{-3}(2,3,6)^{-1}\tau(2,3,6)\sigma^3 = (1,2,4),$$

ritornando al caso di prima.

Abbiamo dimostrato che per ogni $k = 3,\ldots,7$ risulta $(1,2,3) \in G$ e possiamo concludere per quanto dimostrato inizialmente. □

Possiamo finalmente procedere con la dimostrazione del Teorema 4.2.1.

Dimostrazione di 4.2.1. Come osservato, non è restrittivo supporre che il 7-ciclo sia $\sigma = (1,\ldots,7)$ e la permutazione prodotto di due trasposizioni disgiunte sia $\tau = (1,2)(i,j)$, con $i,j \in \{3,\ldots,7\}$ e $i \neq j$. Abbiamo $\binom{5}{2} = 10$ possibilità di scelta

per i e j, ma, per simmetria di alcuni dei casi mediante la permutazione π definita precedentemente, grazie al Lemma 4.2.3 possiamo ridurci a 6, che sono:

$$(1,2)(3,4), \qquad (1,2)(3,5), \qquad (1,2)(3,6),$$

$$(1,2)(3,7), \qquad (1,2)(4,5), \qquad (1,2)(4,6).$$

Studiamo il caso $\tau = (1,2)(3,6)$. Osserviamo che τ e σ sono entrambi automorfismi del piano di Fano numerato come in Figura 4.1. Questo fa sì che il gruppo G sia

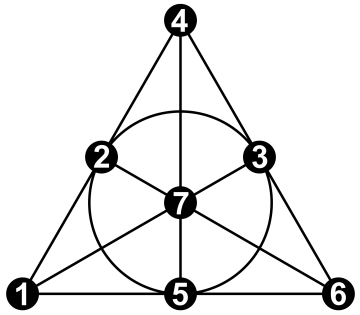


Figura 4.1

in realtà isomorfo un sottogruppo di $\mathrm{PSL}(2,7)$.

Per dimostrare l'uguaglianza, ragioniamo sulle cardinalità. Poiché i generatori di G hanno ordine 7 e 2, sicuramente 14 divide $|G|$ che a sua volta divide $\big|\mathrm{PSL}(2,7)\big| = 168 = 2^3 \cdot 3 \cdot 7$. Inoltre $\sigma\tau = (2,6,7)(3,4,5)$, da cui $|G| = 2^m \cdot 3 \cdot 7$ e resta solo da capire se m è uguale a 1,2 o 3. Chiamiamo $C_1 = \langle\sigma\rangle$ e osserviamo che questo è un 7-Sylow di G. Sia n_7 il numero dei coniugati di C_1 in G. Osserviamo che

$$\tau^{-1}\sigma\tau = (1,6,4,5,3,7,2) \notin C_1$$

e sia $C_2 = \langle(1,6,4,5,3,7,2)\rangle$ che è un coniugato di C_1 diverso da esso. G agisce su $Syl_7(G)$ per coniugio: è dato un morfismo $\rho : G \to S_{n_7}$. Siccome $\sigma^{-1}C_2\sigma \neq C_2$, $\rho(\sigma)$ è non banale e deve avere necessariamente periodo 7. Definiamo $C_3, \ldots, C_8$ a partire da C_2 come $C_{i+2} = \sigma^{-i}C_2\sigma^i$. Questi sono tutti distinti da C_1, altrimenti si avrebbe

$$C_2 = \sigma^i C_1 \sigma^{-i} = C_1.$$

Ora, $\tau^{-1}C_1\tau = C_2$ per definizione, quindi $\rho(\tau)$ ha ordine 2 e si trovano le seguenti relazioni:

$$\tau^{-1}C_3\tau = C_8, \qquad \tau^{-1}C_4\tau = C_5, \qquad \tau^{-1}C_6\tau = C_7.$$

Dal momento che i generatori di G sono σ e τ, questo prova che l'unica orbita dell'azione è $\{C_1, \ldots, C_8\}$ e che $n_7 = 8$. Per il terzo teorema di Sylow concludiamo che 8 divide $|G|$ e che $m = 2$. Quindi in questo caso G è isomofo a $\mathrm{PSL}(2, 7)$.

Anziché studiare il caso in cui $\tau = (1, 2)(3, 5)$, usiamo $\tau = (1, 2)(5, 7)$, visto che le due permutazioni sono simmetriche. Detta $\tau' = (1, 2)(3, 6)$, vediamo che:

- $\tau' \in \langle \sigma, \tau \rangle$ poiché $\sigma^2\tau\sigma^3\tau\sigma^3 = (1, 2)(3, 6)$,
- $\tau \in \langle \sigma, \tau' \rangle$ poiché $\sigma^2\tau'\sigma^5\tau'\sigma^5\tau' = (1, 2)(5, 7)$.

Questo dimostra che $\langle \sigma, \tau \rangle = \langle \sigma, \tau' \rangle$ e dunque anche in questo caso $G \cong \mathrm{PSL}(2, 7)$.

Per provare che in tutti i casi rimanenti $G = A_7$, per il Lemma 4.2.5 è sufficiente esibire un 3-ciclo nel gruppo e concludiamo la dimostrazione:

$$\begin{aligned}
\tau = (1, 2)(3, 4) \quad &\Rightarrow \quad \sigma^3\tau\sigma^3\tau = (1, 6, 3) \in G, \\
\tau = (1, 2)(3, 7) \quad &\Rightarrow \quad \sigma^2\tau\sigma^2\tau = (2, 6, 4) \in G, \\
\tau = (1, 2)(4, 5) \quad &\Rightarrow \quad \sigma^4\tau\sigma^3\tau = (1, 7, 2) \in G, \\
\tau = (1, 2)(4, 6) \quad &\Rightarrow \quad \sigma^3\tau\sigma^3\tau = (3, 7, 4) \in G.
\end{aligned}$$

□

4.3 PSL(2, 7) come gruppo di Galois

Partiamo dal polinomio $P_7(x) = x^7 - 154x + 99 \in \mathbb{Q}[x]$. Questo è il polinomio che utilizzeremo e che vedremo avere gruppo di Galois $\mathrm{PSL}(2, 7)$.

Lemma 4.3.1. $\mathrm{Gal}(P_7)$ *è isomorfo a* $\mathrm{PSL}(2, 7)$ *oppure ad* A_7.

Dimostrazione. Sia $G = \mathrm{Gal}(P_7)$. Si può calcolare $\Delta(P_7) = 3^6 7^8 11^6 113^2$ (si veda [8], p.163) che è un quadrato, per cui $G \leq A_7$ per il Teorema 4.1.15. D'altra parte

P_7 è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein applicato al primo 11, dunque è un polinomio separabile e $|G| = [L : \mathbb{Q}]$ per la Proposizione 4.1.9, dove L è il campo di spezzamento di P. Sicuramente 7 divide il grado dell'estensione e di conseguenza, per il Teorema di Cauchy, G contiene un elemento di ordine 7, cioè un 7-ciclo. Un semplice studio di funzione mostra che P_7 ha esattamente tre radici reali, e le restanti devono essere due coppie distinte di radici complesse coniugate. Il coniugio del piano complesso è un automorfismo di G che in A_7 è il prodotto di due trasposizioni disgiunte. Sono soddisfatte le ipotesi del Teorema 4.2.1 e questo ci permette di concludere. □

Siano $a_1, \ldots, a_7$ le radici di P_7. Partendo da queste, costruiamo il polinomio P_{35} che ha come $\binom{7}{3} = 35$ radici $a_i + a_j + a_k$, per $1 \leq i < j < k \leq 7$.

Osservazione. È possibile calcolare P_{35} a partire dai coefficienti di P_7 senza doverne conoscere le radici.

Se P_7 è della forma $x^7 + ax + b$ con zeri $\{a_1, \ldots, a_7\}$, allora

$$\sigma_6(a_1, \ldots, a_7) = a = \sum_{1 \leq i_1 < \cdots < i_6 \leq 7} a_{i_1} \cdots a_{i_6},$$

$$\sigma_7(a_1, \ldots, a_7) = -b = a_1 \cdots a_7$$

sono polinomi simmetrici omogenei nelle $\{a_i\}$ di grado 6 e 7 rispettivamente. Inoltre, $P_{35}(x) = \sum_{j=0}^{35} c_j x^{35-j}$ è un polinomio simmetrico nelle $\{a_i\}$ per definizione, quindi per il Teorema 4.1.5 si ha $c_j \in \mathbb{Z}[a, b]$ per ogni j. Siccome questi coefficienti c_j sono dei polinomi simmetrici omogenei di grado $35 - j$ nelle radici $\{b_1, \ldots, b_{35}\}$ di P_{35}, e siccome le $\{b_k\}$ sono a loro volta dei polinomi omogenei di grado 1 nelle $\{a_i\}$, abbiamo che i $c_j \in \mathbb{Z}[a, b]$ sono polinomi simmetrici omogenei di grado $35 - j$ nelle $\{a_i\}$.

Sia $c_j = \sum \gamma_{st} a^s b^t$. Dato che a e b sono simmetrici omogenei nelle $\{a_i\}$ di grado 6 e 7 rispettivamente, e dato che $j = 6s + 7t$ ha al più una soluzione intera positiva per ogni j tale che $1 \leq j \leq 35$, abbiamo che $c_j = \gamma_{st} a^s b^t$. Le costanti

intere γ_{st} possono essere direttamente calcolate, con il risultato:

$$\begin{aligned}P_{35}(x) = x^{35} &+ 40ax^{29} + 302b^{28} - 1614a^2x^{23} + 2706abx^{22}\\ &+ 3828b^2x^{21} - 5072a^3x^{17} + 2778a^2bx^{16} - 18084ab^2x^{15}\\ &+ 36250b^3x^{14} - 5147a^4x^{11} - 1345a^3bx^{10} - 21192a^2b^2x^9\\ &- 26326ab^3x^8 - 7309b^4x^7 - 1728a^5x^5 - 1728a^4bx^4\\ &+ 720a^3b^2x^3 + 928a^2b^3x^2 - 64ab^4x - 128b^5.\end{aligned}$$

Proposizione 4.3.2. *P_7 ha gruppo di Galois* $\mathrm{PSL}(2,7)$.

Dimostrazione. Osserviamo che per com'è stato costruito P_{35}, sono soddisfatte le ipotesi del Lemma 4.1.16 e quindi ha lo stesso campo di spezzamento di P_7. Calcoliamo ora P_{35}:

$$\begin{aligned}P_{35}(x) = x^{35} &- 6160x^{29} + 29898x^{28} - 38277624x^{23} - 41255676x^{22}\\ &+ 37518228x^{21} + 18524283008x^{17} + 6522421752x^{16}\\ &+ 27295157736x^{15} + 35173338750x^{14} - 2894923232432x^{11}\\ &+ 489571380144x^{10} - 4925879415072x^9 + 3933790086996x^8\\ &- 702099623709x^7 + 149674336745472x^5 - 96219216479232x^4\\ &- 25773004414080x^3 + 21354775085952x^2 + 946763427456x\\ &- 1217267263872.\end{aligned}$$

Dal momento che i coefficienti di P_{35} sono limitati, possiamo testarne la riducibilità algoritmicamente come spiegato in [5]. Pertanto, risulta che P_{35} è riducibile e il polinomio $\hat{P}_7(x) = x^7 - 231x^3 - 462x^2 + 77x + 66$ è un suo fattore.

Riprendendo il lemma 4.1.17, necessariamente $G \ncong A_7$, da cui, per il Lemma 4.3.1, si ha $G \cong \mathrm{PSL}(2,7)$. □

Per capire la fattorizzazione di P_{35}, abbiamo bisogno del piano di Fano numerato come in Figura 4.1. Identifichiamo i punti del piano con gli zeri di P_7, $\{a_i\}$, e le somme $a_i + a_j + a_k$, $i < j < k$, con le configurazioni $\{i,j,k\}$ che rappresentano una retta o un triangolo. Il gruppo $\mathrm{PSL}(2,7)$ agisce intransitivamente sulle $\binom{7}{3}$ terne con due orbite, una di ordine 7 (quella delle rette) e una di ordine 28 (quella

dei triangoli). Notiamo che il fattore di P_{35} di grado 7 è $\hat{P}_7$, con le 7 rette come suoi zeri. Inoltre, possiamo verificare questa correlazione con le radici dei polinomi utilizzati calcolate approssimativamente, come riportate nella seguente tabella.

Polinomio	Radici	Parte reale	Parte immaginaria
$P_7(x) = x^7 - 154x + 99$	a_1	2.18	-
	a_2	0.64	-
$\Delta(P_7) = 3^6 7^8 11^6 113^2$	a_5	1.04	2.02
	a_6	1.04	-2.02
	a_7	-1.25	-2.01
$\hat{P}_7(x) = x^7 - 231x^3$	a_{124}	0.41	-
$-462x^2 + 77x + 66$	a_{235}	0.43	4.03
	a_{346}	-2.61	-0.01
$\Delta(\hat{P}_7) = 2^6 3^1 27^8 11^6$	a_{457}	-2.61	0.01
$a_{ijk} = a_i + a_j + a_k$	a_{561}	4.27	-
	a_{672}	0.43	-4.03
	a_{713}	-0.32	-

Abbiamo quindi trovato un polinomio razionale che ha PSL$(2, 7)$ come gruppo di Galois.

Però, possiamo notare che in realtà $P_7(x) = x^7 - 154x + 99$ non risulta essere centrale nelle dimostrazioni viste. Più specificamente, è stato descritto un metodo che permette di dedurre se PSL$(2, 7)$ si realizza come gruppo di Galois di un polinomio.

In generale, si verifica che un polinomio della forma $T_7(x) = x^7 + ax + b$ non può avere più di tre radici reali. Seguendo i passaggi fatti nel caso di P_7, otteniamo le seguenti condizioni necessarie e sufficienti affinché $\mathrm{PSL}(2,7)$ sia il suo gruppo di Galois:

1. T_7 è irriducibile su $\mathbb{Q}$,
2. il discriminante di T_7 è un quadrato,
3. T_7 ha esattamente tre radici reali,
4. T_{35} è riducibile su $\mathbb{Q}$.

Bibliografia

[1] *D. J. S. Robinson*, A Course in the Theory of Groups. Second edition. Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.

[2] *T. W. Hungerford*, Algebra. Reprint of the 1974 original. Graduate Texts in Mathematics, Springer-Verlag, New York-Berlin, 1980.

[3] *C. Sims*, Computational methods in the study of permutation groups. Proc. Oxford Conference, Pergamon, Oxford, 1970.

[4] *D. A. Cox*, Galois theory. Second edition. Pure and Applied Mathematics, John Wiley & Sons, Inc., Hoboken, NJ, 2012.

[5] *D. W. Erbach, J. Fisher, J. McKay*, Polynomials with PSL(2,7) as Galois Group, *J. Number Theory* **11** (1979), 69–75.

[6] *E. Brown, N. Loehr*, Why is PSL(2,7)≅GL(3,2)?, *Amer. Math. Monthly* **116** (2009), 727–732.

[7] *L. Verardi*, Piani Proiettivi, Dipartimento di Matematica, Bologna.

[8] *E. Berlekamp*, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

[9] *J. A. Gallian*, The Search for Finite Simple Groups, *Math. Mag.* **49** (1976), 163–180.