

RENDICONTI *del* SEMINARIO MATEMATICO *della* UNIVERSITÀ DI PADOVA

CLAUDIA METELLI

**I gruppi semplici minimali sono individuati
reticolarmente in senso stretto**

Rendiconti del Seminario Matematico della Università di Padova,
tome 45 (1971), p. 367-378

http://www.numdam.org/item?id=RSMUP_1971__45__367_0

© Rendiconti del Seminario Matematico della Università di Padova, 1971, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

I GRUPPI SEMPLICI MINIMALI SONO INDIVIDUATI RETICOLARMENTE IN SENSO STRETTO

CLAUDIA METELLI *)

Un gruppo G si dice individuato reticolarmente in senso stretto se ogni isomorfismo reticolare di G su un gruppo G_1 è indotto da un isomorfismo gruppale.

In questa Nota si prova che sono individuati reticolarmente in senso stretto

- i gruppi semplici di Suzuki $S(q)$ ($q=2^{n+1}$, $n>0$) [8], e
- il gruppo proiettivo lineare speciale $PSL(3, 3)$.

Tenendo conto di [3] e [4], in cui si è dimostrato che di tale proprietà godono anche i gruppi semplici $PSL(2, p^f)$ (p primo, $p^f \geq 4$), e ricordando che i gruppi semplici finiti non abeliani minimali sono i seguenti [2]:

$$\begin{array}{ll} PSL(2, p) & (p \text{ primo } > 3, p^2 - 1 \not\equiv 0 \pmod{5}) \\ PSL(2, 2^f) & (f \text{ primo}) \\ PSL(2, 3^f) & (f \text{ primo } > 2) \\ S(q) & (q=2^p, p \text{ primo } > 2) \\ PSL(3, 3) & \end{array}$$

si ottiene in particolare il seguente

*) Indirizzo dell'A.: Seminario Matematico, Università, Padova.

Lavoro eseguito nell'ambito dei gruppi di ricerca del Comitato Nazionale per la Matematica del C.N.R.

TEOREMA. *I gruppi semplici finiti non abeliani minimali sono individuati reticolarmente in senso stretto.*

I.

TEOREMA I. *I gruppi semplici non abeliani $S(q)$ ($q=2^{2n+1}$, $n>0$) sono individuati reticolarmente in senso stretto.*

PROPOSIZIONE A. *Se il gruppo $G=S(q)$ è reticolarmente isomorfo a un gruppo G_1 , allora G è isomorfo a G_1 .*

La dimostrazione segue direttamente dalla caratterizzazione che Suzuki ha dato dei gruppi finiti non risolubili con partizione ([6]), e dal fatto che il gruppo G_1 nelle ipotesi considerate è un gruppo semplice non abeliano dello stesso ordine di G ([7]). La proprietà di un gruppo finito di ammettere una partizione in sottogruppi ciclici disgiunti si conserva per isomorfismi reticolari, quindi G_1 (nella cui partizione intervengono gruppi non ciclici) non può essere del tipo $PSL(2, p')$; è dunque necessariamente isomorfo a $S(q_1)$ per qualche q_1 ; ma ha lo stesso ordine di G , e quindi $q_1=q$ e $G_1 \simeq G$.

Per dimostrare il teorema, sarà allora sufficiente provare

PROPOSIZIONE B. *Ogni automorfismo reticolare di $G=S(q)$ è indotto da uno (e un solo) automorfismo di gruppo.*

1. Cominciamo col richiamare le proprietà di $G=S(q)$ che saranno usate nel seguito. Esse sono tratte esclusivamente da [8]; anche la notazione, per quanto possibile, seguirà quella di [8].

a) Il gruppo $G=S(q)$ è un gruppo semplice non abeliano di ordine $(q^2+1)q^2(q-1)$. Esso ammette una partizione $\mathfrak{F}$ (nel senso di Baer) in sottogruppi disgiunti di ordine rispettivamente q^2 , $q-1$, $q+r+1$ (dove $r^2=2q$); ogni sottogruppo di G di tale ordine è un elemento di $\mathfrak{F}$; elementi di $\mathfrak{F}$ dello stesso ordine sono coniugati tra loro.

Sia Q un sottogruppo di ordine q^2 (Q è dunque un 2-sottogruppo di Sylow di G), K un sottogruppo di ordine $q-1$, A_1 un sottogruppo di ordine $q+r+1$, A_2 un sottogruppo di ordine $q-r+1$. K , A_1 , A_2

sono ciclici; $D=N_G(K)$ è diedrale di ordine $2(q-1)$; se $B_i=N_G(A_i)$ ($i=1, 2$), B_i/A_i è ciclico di ordine 4.

$H=N_G(Q)$ è un gruppo di ordine $q^2(q-1)$, prodotto semidiretto di Q per un coniugato di K .

H, D, B_1, B_2 sono massimali in G .

Per ogni q_1 tale che $q_1^m=q$, G contiene un sottogruppo isomorfo a $S(q_1)$.

I sottogruppi dei gruppi elencati e i loro coniugati esauriscono i sottogruppi di G .

b) Fissiamo ora $Q, H=N_G(Q)$, e $K \subseteq H$ (dimodochè $H=QK$); fissiamo anche una involuzione $\tau \in D=N_G(K)$; risulterà $K=H \cap H^{\tau^{-1}}$.

Ogni elemento $g \in G$ che non stia in H , si può esprimere in uno ed un solo modo nella forma $g=\eta\tau\pi$, con $\eta \in H$ e $\pi \in Q$; da ciò segue che i coniugati di H diversi da H sono proprio i q^2 gruppi distinti $H^{\tau\pi}$, $\pi \in Q$.

Nel corso delle successive dimostrazioni, spesso porremo

$$G_{\infty}=H, \quad G_{\pi}=H^{\tau\pi} \quad (\pi \in Q), \quad \Omega=\{G_{\infty}\} \cup \{G_{\pi} \mid \pi \in Q\}.$$

Gli automorfismi interni di G permutano i coniugati di H ; e anzi G agisce fedelmente come gruppo di permutazioni 2-transitivo nell'insieme Ω di tali coniugati.

In quest'ordine di idee, chiameremo $G_{x,y}$ il gruppo $G_x \cap G_y$ (che è isomorfo a K , e quindi ciclico di ordine $q-1$); e porremo $N_G(G_{x,y})=D_{x,y}$; dimodochè $K=G_{1,\infty}$; $D=D_{1,\infty}$.

c) Q è un gruppo di ordine q^2 ed esponente 4; il suo centro $Z(Q)$ è un gruppo abeliano elementare di ordine q , e contiene tutte le involuzioni di Q . Gli elementi di K operano transitivamente sulle involuzioni di Q , dimodochè se $1 \neq \sigma \in Z(Q)$, abbiamo $Z(Q)=\{1\} \cup \{\sigma^x \mid x \in K\}$; anzi, sarà utile nel seguito aver introdotto un insieme $\overline{K}=\{0\} \cup K$, sicchè, ponendo — come di consueto — $g^0=1$ per ogni $g \in Q$, avremo $Z(Q)=\{\sigma^x/x \in \overline{K}\}$.

¹⁾ Infatti $Q \neq Q^{\tau}$, altrimenti $H \supseteq \langle \tau, x \rangle = D$ che non sarebbe massimale; ma allora $Q \cap Q^{\tau} = 1$.

Fisseremo ora una volta per tutte gli elementi $\sigma \in Z(Q)$, $\rho \in Q$ individuati dalla $\rho^2 = \sigma \neq 1$ e dalla « identità fondamentale » $\tau\sigma\tau = \rho^{-1}\tau\rho$ [8].

Allora ogni elemento $\pi \in Q$ sarà esprimibile in modo unico nella forma $\pi = \rho^\lambda \sigma^\kappa$, con $\lambda, \kappa \in \overline{K}$.

2. Sia $\mathcal{A}$ il gruppo degli automorfismi di G , $\mathcal{A}^*$ il gruppo degli automorfismi reticolari di G . Poichè G è un gruppo semplice non abeliano, ogni automorfismo reticolare è indotto al più da un automorfismo gruppendale; previe ovvie identificazioni, si può dunque scrivere $G \subseteq \mathcal{A} \subseteq \mathcal{A}^*$. Si tratterà di provare che $\mathcal{A}^* = \mathcal{A}$.

PROPOSIZIONE 1. *$\mathcal{A}^*$ si rappresenta fedelmente come gruppo di permutazioni 2-transitivo su Ω .*

G è semplice, quindi ogni automorfismo reticolare di G conserva gli indici dei sottogruppi [7]; dunque ogni $\varphi \in \mathcal{A}^*$ induce una permutazione su Ω . Proviamo ora che la rappresentazione è fedele: cioè che un automorfismo reticolare φ che fissi tutti gli elementi di Ω è identico. Basterà far vedere che φ fissa tutti i sottogruppi ciclici di G .

Sia C_1 un sottogruppo ciclico di G , e $|C_1| \mid (q-1)$: allora C_1 è contenuto in un coniugato di K , ossia in un $G_{x,y} = G_x \cap G_y$ che è ovviamente fissato da φ , insieme ai suoi sottogruppi. φ fissa allora anche tutti i $D_{x,y}$, e con essi tutte le involuzioni di G : infatti tutte le involuzioni di G sono coniugate di σ , e $\langle \sigma \rangle = G_\infty \cap D_{1,\sigma}$ è fissata da φ .

Proviamo ora che φ fissa A_2 e (con lo stesso ragionamento) A_1 e tutti i loro coniugati: e quindi tutti i sottogruppi ciclici di G il cui ordine divide q^2+1 . Se $B_2/A_2 = \langle \alpha A_2 \rangle$, φ fissa tutte le $q-r+1$ involuzioni che costituiscono la classe laterale $\alpha^2 A_2$; poichè (se $q > 2$) è $q-r+1 > 3$, φ fissa un sottogruppo non identico di A_2 e quindi anche A_2 ²⁾.

Resta da provare che φ fissa tutti i sottogruppi ciclici di ordine 4. Ciò risulta immediato se si richiamano i seguenti due fatti [8], che saranno utili anche in seguito.

i) ogni elemento di ordine 4 di G è coniugato in G o a ρ , o a ρ^{-1} ;

2) Infatti $|A_2^\varphi| = |A_2|$, per cui $A_2^\varphi \in \mathcal{F}$ e quindi A_2^φ ed A_2 , se non hanno intersezione identica, coincidono.

ii) $\langle \sigma, \tau \rangle$ è contenuto in un coniugato di A_i , che chiameremo A ; e quindi $\langle \rho, \tau \rangle$ è contenuto in $N_G(A)$, che chiameremo B .

Allora $\langle \rho \rangle = G_\infty \cap B$ è fissato da φ , e con esso i sottogruppi di ordine 4 di G , esaurendo così i sottogruppi ciclici di G .

Quanto alla 2-transitività di $\mathcal{A}^*$, basta ricordare che $\mathcal{A}^* \supseteq G$ che è appunto 2-transitivo su Ω . Con ciò la Proposizione 1 è dimostrata.

COROLLARIO 1. *Se $\mathcal{A}_{1,\infty}^*$ è il sottogruppo di $\mathcal{A}^*$ costituito dagli automorfismi reticolari che fissano $G_\infty = H$, $G_1 = H^\tau$, allora $\mathcal{A}^* = G\mathcal{A}_{1,\infty}^*$.*

3. Sia $F = GF(q)$ il corpo di Galois con q elementi. $\mathcal{A}/G$ è isomorfo al gruppo $\text{Aut}(F)$ degli automorfismi di F [8].

Dal corollario precedente, abbiamo che

$$[\mathcal{A}^* : G] = [G\mathcal{A}_{1,\infty}^* : G] = [\mathcal{A}_{1,\infty}^* : G \cap \mathcal{A}_{1,\infty}^*] = [\mathcal{A}_{1,\infty}^* : G_{1,\infty}] = [\mathcal{A}_{1,\infty}^* : K].$$

Notiamo ora che gli automorfismi di $\mathcal{A}_{1,\infty}^*$, fissando $G_\infty = H$, permutano tra loro le involuzioni di Q , mentre K è esattamente³⁾ transitivo su tali involuzioni; allora $\mathcal{A}_{1,\infty}^*$ si fattorizza in $K \cdot \mathcal{A}_{1,\infty,\sigma}^*$ (se con $\mathcal{A}_{1,\infty,\sigma}^*$ indichiamo il gruppo degli automorfismi di $\mathcal{A}_{1,\infty}^*$ che fissano $\langle \sigma \rangle$ ⁴⁾, e anzi $\mathcal{A}_{1,\infty,\sigma}^* \cap K = \{1\}$). Abbiamo allora

$$[\mathcal{A}_{1,\infty}^* : K] = [K\mathcal{A}_{1,\infty,\sigma}^* : K] = [\mathcal{A}_{1,\infty,\sigma}^* : K \cap \mathcal{A}_{1,\infty,\sigma}^*] = |\mathcal{A}_{1,\infty,\sigma}^*|.$$

Abbiamo così dimostrato

$$\text{PROPOSIZIONE 2. } [\mathcal{A}^* : G] = |\mathcal{A}_{1,\infty,\sigma}^*|;$$

dunque per provare che $\mathcal{A}^* = \mathcal{A}$ — ossia che $[\mathcal{A}^* : G] = [\mathcal{A} : G]$ — sarà sufficiente dimostrare che $|\mathcal{A}_{1,\infty,\sigma}^*| = |\text{Aut } F|$.

A questo scopo, procederemo nel modo seguente: ad ogni automorfismo $\varphi \in \mathcal{A}_{1,\infty,\sigma}^*$ assoceremo una applicazione α di F in sè; proveremo che la corrispondenza tra i φ e gli α è biunivoca, e che gli α sono proprio automorfismi di F .

³⁾ Segue subito dal fatto che $|K| = q - 1 = |Z(Q) - \{1\}|$.

⁴⁾ Tale notazione, che potrebbe sembrare scorretta, è giustificata dal fatto che se $\langle \sigma \rangle^\varphi = \langle \sigma \rangle$, allora $G_{\sigma^\varphi} = G_\sigma$, e viceversa (cfr. il successivo paragrafo 4).

4. Sia $\varphi \in \mathcal{A}_{1, \infty, \sigma}^*$. Definiamo una biiezione β di Q in sè ponendo $(G_\pi)^\varphi = G_{\pi^\beta}$, $\pi \in Q$: ciò è possibile perchè $G_\infty^\varphi = G_\infty$, e φ è una permutazione su Ω . È $1^\beta = 1$; proviamo che β conserva gli ordini degli elementi. Sia $1 \neq \pi \in Z(Q)$. Allora $(G_1)^\pi = (H^\pi)^\pi = H^{\pi\pi} = G_\pi$, quindi $\langle \pi \rangle = G_\infty \cap D_{1, \pi}$; ma $(D_{1, \pi})^\varphi = [N_G(G_1 \cap G_\pi)]^\varphi = N_G(G_1^\varphi \cap G_\pi^\varphi) = N_G(G_1 \cap G_{\pi^\beta}) = D_{1, \pi^\beta}$, per cui $\langle \pi \rangle^\varphi = G_\infty \cap (D_{1, \pi})^\varphi = G_\infty \cap D_{1, \pi^\beta} = \langle \pi^\beta \rangle$ che ha quindi ordine 2. È poi $\sigma^\beta = \sigma$: infatti $\langle \sigma \rangle = \langle \sigma \rangle^\varphi = G_\infty \cap (D_{1, \sigma})^\varphi = G_\infty \cap D_{1, \sigma^\beta} = \langle \sigma^\beta \rangle$.

β induce dunque su $Z(Q) = \{\sigma^x \mid x \in \bar{K}\}$ una permutazione che fissa 1 e σ ; sia ora α la biiezione di $\bar{K}$ definita da $(\sigma^x)^\beta = \sigma^{x^\alpha}$. Notiamo subito che risulta $0^\alpha = 0$, $1^\alpha = 1$.

Istituiamo ora in $\bar{K}$ una somma e un prodotto, che lo rendano una copia isomorfa del corpo F . Per il prodotto, sarà sufficiente estendere quello vigente in K all'elemento $0 \in \bar{K}$, nel modo ovvio; quanto alla somma, assumeremo come definizione di $x + \lambda$ la $\sigma^x \sigma^\lambda = \sigma^{x+\lambda}$ ($x, \lambda \in \bar{K}$). Le verifiche sul buon funzionamento di tali definizioni sono immediate.

Siamo così giunti alla situazione descritta alla fine del paragrafo precedente. Si tratterà quindi di provare: 1) che se φ e φ' individuano la stessa α , coincidono: o, in altri termini, che α individua β , e quindi φ ; 2) che α è un automorfismo del corpo $\bar{K}$.

5. Premettiamo alcuni lemmi, che entrano più dettagliatamente nella struttura di G . Useremo tutte le informazioni del paragrafo 1, e in particolare l'identità fondamentale $\tau\sigma\tau = \rho^{-1}\tau\rho$. I simboli x, λ, μ indicheranno sempre elementi di $\bar{K}$ (o di K). Ricordiamo anche che $\tau x \tau = x^{-1}$ per ogni $x \in K$.

LEMMA 1. $\langle \tau \rangle^\varphi = \langle \tau \rangle$.

a) Se $(\rho)^\beta = \rho^\lambda \sigma^\mu$ ($\lambda, \mu \in \bar{K}$), allora $\mu = 0$.

Consideriamo $G_1 \cap D_{\infty, \rho} = \langle \tau\sigma\tau \rangle$ (infatti $(G_\infty)^{\tau\sigma\tau} = H^{\tau\sigma\tau} = H^{\rho^{-1}\tau\rho} = H^{\tau\rho} = G_\rho$). $\langle \tau\sigma\tau \rangle^\varphi = G_1 \cap D_{\infty, \rho}^\beta$. Essendo un'involuzione di G_1 , $\langle \tau\sigma\tau \rangle^\varphi = \langle \tau\sigma^{\lambda^{-1}}\tau \rangle$, $\lambda^{-1} \in K$; ma $\tau \in D = N_G(K)$ e quindi $\tau\lambda\sigma\lambda^{-1}\tau = \lambda^{-1}\tau\sigma\tau\lambda = (\tau\sigma\tau)^\lambda \in D_{\infty, \rho}^\lambda$ (infatti $H^{(\tau\sigma\tau)\lambda} = H^{\tau\sigma\tau\lambda} = H^{\rho^{-1}\tau\rho\lambda} = H^{\lambda\tau\rho\lambda} = H^{\tau\rho\lambda}$), e quindi $(\rho)^\beta = \rho^\lambda$ ($\lambda \in K$).

b) Se $\mu, \lambda \in K$, $\sigma\tau^\mu\sigma \in G_{\rho^\lambda}$ se e solo se $\mu = \lambda = 1$.

Intanto $\sigma\tau\sigma = \rho^{-1}(\rho^{-1}\tau\rho)\rho = \rho^{-1}\tau\sigma\tau\rho \in G_{\rho^\lambda}$. Quanto all'implicazione opposta, se $\sigma\tau^\mu\sigma$ è un'involuzione di G_{ρ^λ} , sarà un elemento del tipo

$(\rho^{-1})^\lambda \tau \sigma^\kappa \tau \rho^\lambda$, $\kappa \in K$. Quindi $\tau^\mu = \sigma(\rho^{-1})^\lambda \tau \sigma^\kappa \tau \rho^\lambda \sigma = \sigma(\rho^{-1})^\lambda (\rho^{-1})^\mu (\rho^\mu \tau \sigma^\kappa \tau (\rho^{-1})^\mu) \rho^\mu \rho^\lambda \sigma$. Ma si verifica subito che $\tau^\mu \in G_{(\rho^{-1})^\mu}$; allora l'elemento $\pi = \rho^\kappa \rho^\lambda \sigma$ induce un automorfismo interno che fissa $G_{(\rho^{-1})^\mu}$, e quindi $\pi \in G_{(\rho^{-1})^\mu} \cap \Omega = \{1\}$. Ma allora, $\mu = \lambda = 1$.

c) Essendo $\langle \sigma \tau \sigma \rangle = G_\rho \cap D_{\infty, \sigma}$, sarà $\langle \sigma \tau \sigma \rangle^\varphi = G_{\rho^\lambda} \cap D_{\infty, \sigma} = \langle \pi \rangle$ (come segue da a)). Ma π , essendo un'involuzione di $D_{\infty, \sigma}$, sarà del tipo $\sigma \tau^\mu \sigma$, $\mu \in K$; quindi — come si è visto al punto precedente — deve essere $\mu = \lambda = 1$, in particolare $\rho^\beta = \rho$. Allora φ fissa $\langle \tau \sigma \tau \rangle = G_1 \cap D_{\infty, \rho}$, quindi anche $\langle \sigma, \tau \sigma \tau \rangle$, e con esso anche $\langle \tau \rangle = \langle \sigma, \tau \sigma \tau \rangle \cap D_{1, \infty}$ ⁵⁾.

LEMMA 2. Se $\pi, \pi_1 \in Q$ con $\pi^2 = \pi_1^2$, allora $(\pi^\beta)^2 = (\pi_1^\beta)^2$.

Se $\pi^2 = 1$, l'affermazione è stata provata all'inizio del paragrafo 4. Sia dunque $\pi^2 = \pi_1^2 \neq 1$; allora $\pi = \rho^\kappa \sigma^\lambda$, $\pi_1 = \rho^\kappa \sigma^\mu$ ($\kappa \in K$, $\lambda, \mu \in \bar{K}$). Se $\lambda = \mu$, è $\pi = \pi_1$ e l'affermazione è vera. Se $\lambda \neq \mu$, allora $G_\infty \cap D_{\pi, \pi_1} = \langle \sigma^{\lambda+\mu} \rangle \neq 1$. Quindi anche $(G_\infty \cap D_{\pi, \pi_1})^\varphi = G_\infty \cap D_{\pi^\beta, \pi_1^\beta} = \langle \sigma^\nu \rangle \neq 1$, ossia $\pi^\beta \sigma^\nu = \pi_1^\beta$ e $(\pi^\beta)^2 = (\pi_1^\beta)^2$, come si voleva.

LEMMA 3. $(\rho^\kappa)^\beta = \rho^{\kappa^\beta}$, $[(\rho^{-1})^\kappa]^\beta = (\rho^{-1})^{\kappa^\beta}$ per ogni $\kappa \in \bar{K}$.

Per $\kappa = 0, 1$ la cosa è già stata dimostrata⁶⁾. Sia dunque $\kappa = 0, 1$, e consideriamo l'immagine attraverso φ del gruppo

$$L = \langle (\sigma \tau \sigma)^\kappa \rangle = \langle \sigma^\kappa \tau^\kappa \sigma^\kappa \rangle = \langle \sigma^\kappa, \tau^\kappa \rangle \cap D_{\infty, \sigma^\kappa} \cap G_{\rho^\kappa} \cap D_{1, (\rho^{-1})^\kappa}.$$

Poichè $\langle \sigma^\kappa, \tau^\kappa \rangle \neq D_{\infty, \sigma^\kappa}$, quella intersezione è già individuata dai primi due gruppi: $L^\varphi = \langle \sigma^\kappa, \tau^\kappa \rangle^\varphi \cap D_{\infty, (\sigma^\kappa)^\beta} = \langle \sigma^{\kappa^\beta}, \tau^\mu \rangle \cap D_{\infty, \sigma^{\kappa^\beta}}$, essendo $\langle \tau^\kappa \rangle^\varphi = \langle \tau^\mu \rangle$ ($\mu \in K$) perchè τ^κ è un'involuzione di $D_{1, \infty}$ che è fissato da φ . D'altra parte $\langle \sigma^{\kappa^\beta}, \tau^\mu \rangle \cap D_{\infty, \sigma^{\kappa^\beta}} = \langle \sigma^{\kappa^\beta} \tau^\mu \sigma^{\kappa^\beta} \rangle$, e quindi

$$\langle \sigma^{\kappa^\beta} \tau^\mu \sigma^{\kappa^\beta} \rangle = (G_{\rho^\kappa} \cap D_{1, (\rho^{-1})^\kappa})^\varphi = G_{(\rho^\kappa)^\beta} \cap D_{1, [(\rho^{-1})^\kappa]^\beta}.$$

D'altra parte

$$\sigma^{\kappa^\beta} \tau^\mu \sigma^{\kappa^\beta} = \sigma^{\kappa^\beta} \mu^{-1} (\rho \tau \sigma \tau \rho^{-1}) \mu \sigma^{\kappa^\beta} = \sigma^{\kappa^\beta} \rho^\mu \tau \sigma^{\mu-1} \tau (\rho^{-1})^\mu \sigma^{\kappa^\beta}$$

5) Ciò segue dal fatto che $\langle \sigma, \tau \sigma \tau \rangle \neq D_{1, \infty}$.

6) La $(\rho^{-1})^\beta = \rho^{-1}$ si ricava subito da $\rho^\beta = \rho$ e $\langle \sigma \rangle = G_\infty \cap D_{\rho, \rho^{-1}}$.

e quindi appartiene a $G_{(\rho^{-1})^{\mu}\sigma^{\alpha}}$; mentre

$$G_1^{\sigma^{\alpha}\tau^{\mu}\sigma^{\alpha}} = H^{\tau\sigma^{\alpha}\tau^{\mu}\sigma^{\alpha}} = H^{\alpha\tau\sigma\tau(\alpha)^{-1}\mu^2\sigma^{\alpha}} = H^{\rho^{-1}\tau\rho(\alpha)^{-1}\mu^2\sigma^{\alpha}} = G_1^{\rho(\alpha)^{-1}\mu^2\sigma^{\alpha}}$$

Dunque

$$(\rho^{\alpha})^{\beta} = (\rho^{-1})^{\mu}\sigma^{\alpha}, \quad ((\rho^{-1})^{\alpha})^{\beta} = \rho^{(\alpha)^{-1}\mu^2\sigma^{\alpha}}.$$

Ma $(\rho^{\alpha})^2 = [(\rho^{-1})^{\alpha}]^2$, e quindi per il lemma 2

$$[(\rho^{\alpha})^{\beta}]^2 = \sigma^{\mu} = \sigma^{(\alpha)^{-1}\mu^2} = [((\rho^{-1})^{\alpha})^{\beta}]^2;$$

da cui $\mu = \alpha$ che porta con sè le conclusioni desiderate.

6. Possiamo ormai procedere alla dimostrazione dei due punti indicati alla fine del paragrafo 4, concludendo così la dimostrazione del teorema.

PROPOSIZIONE 3. *L'applicazione α individua β , e quindi φ .*

Sarà sufficiente provare che $(\rho^{\alpha}\sigma^{\lambda})^{\beta} = \rho^{\alpha}\sigma^{\lambda^{\alpha}} (\alpha, \lambda \in \overline{K})$. Si è già visto nei paragrafi precedenti che l'uguaglianza vale se $\alpha=0$ oppure $\lambda=0$. Siano quindi $\alpha, \lambda \in K$; è $\langle \sigma^{\lambda} \rangle = G_{\infty} \cap D_{\rho^{\alpha}, \rho^{\alpha}\sigma^{\lambda}}$, da cui

$$\langle \sigma^{\lambda} \rangle^{\varphi} = \langle \sigma^{\lambda^{\alpha}} \rangle = G_{\infty} \cap D_{(\rho^{\alpha})^{\beta}, (\rho^{\alpha}\sigma^{\lambda})^{\beta}};$$

ma $(\rho^{\alpha})^{\beta} = \rho^{\alpha}$ (lemma 3), e quindi $\rho^{\alpha}\sigma^{\lambda^{\alpha}} = (\rho^{\alpha}\sigma^{\lambda})^{\beta}$, come si voleva.

PROPOSIZIONE 4. *L'applicazione α è un automorfismo di $\overline{K}$.*

Cominciamo col dimostrare che $(\alpha + \lambda)^{\alpha} = \alpha^{\alpha} + \lambda^{\alpha} (\alpha, \lambda \in \overline{K})$. La cosa è immediata se $\alpha=0$, oppure $\lambda=0$. Siano dunque $\alpha, \lambda \in K$, e consideriamo l'immagine di $\langle \sigma^{\alpha} \rangle = G_{\infty} \cap D_{\sigma^{\lambda}, \sigma^{\alpha+\lambda}}$. È

$$\langle \sigma^{\alpha} \rangle^{\varphi} = \langle \sigma^{\alpha^{\alpha}} \rangle = G_{\infty} \cap D_{\sigma^{\lambda^{\alpha}}, \sigma^{(\alpha+\lambda)^{\alpha}}};$$

ma allora $\sigma^{\alpha^{\alpha}}\sigma^{\lambda^{\alpha}} = \sigma^{(\alpha+\lambda)^{\alpha}}$, da cui la conclusione (visto che abbiamo definito $\sigma^{\alpha^{\alpha}+\lambda^{\alpha}} = \sigma^{\alpha^{\alpha}}\sigma^{\lambda^{\alpha}}$).

Per affermare che α è un automorfismo di $\bar{K}$, sarà sufficiente provare — in base a un noto teorema di Hua — che $(\chi^{-1})^\alpha = (\chi^\alpha)^{-1}$. Dimostriamo allora che $\rho^{(\chi^{-1})^\alpha} = \rho^{(\chi^\alpha)^{-1}}$. In base al lemma 1, abbiamo

$$\langle \sigma^\chi, \tau \rangle^q = \langle \sigma^\chi \rangle^q \cup \langle \tau \rangle^q = \langle \sigma^{\chi^\alpha}, \tau \rangle.$$

Allora

$$\langle \sigma^{x\tau} \rangle^q = (\langle \sigma^\chi, \tau \rangle \cap G_1 \cap D_{\infty, \rho^{\chi^{-1}}})^q = \langle \sigma^{\chi^\alpha}, \tau \rangle \cap G_1 \cap D_{\infty, (\rho^{\chi^{-1}})^\beta};$$

infatti

$$\sigma^{x\tau} = \tau \chi^{-1} \sigma \chi \tau = \chi \rho^{-1} \tau \rho \chi^{-1} \in D_{\infty, \rho^{\chi^{-1}}}.$$

Consideriamo ora il sottogruppo $M = \langle \sigma^{\chi^\alpha}, \tau \rangle \cap G_1$. M non coincide con G_1 (altrimenti si avrebbe $\langle \sigma^{\chi^\alpha}, \tau \rangle \supseteq \langle G_1, \tau \rangle = G$ mentre $\langle \sigma^{\chi^\alpha}, \tau \rangle \subseteq \subseteq N_G(\langle \tau \sigma^{\chi^\alpha} \rangle)$ che è un sottogruppo proprio di G), ma contiene l'involuzione $\tau \sigma^{\chi^\alpha} \tau \in G_1$. Allora $\tau \sigma^{\chi^\alpha} \tau$ è la sola involuzione di M : quindi

$$\langle \sigma^{x\tau} \rangle^q = \langle \sigma^{x^\alpha \tau} \rangle \subseteq D_{\infty, \rho^{(\chi^\alpha)^{-1}}},$$

da cui $\rho^{(\chi^\alpha)^{-1}} = (\rho^{\chi^{-1}})^\beta$ e, per il lemma 3, $(\rho^{\chi^{-1}})^\beta = \rho^{(\chi^{-1})^\alpha}$, c.v.d.

II.

TEOREMA II. *Il gruppo proiettivo lineare speciale $PSL(3, 3)$ è individuato reticolarmente in senso stretto.*

PROPOSIZIONE C. *Sia $G = PSL(3, 3)$, e G_1 un gruppo reticolarmente isomorfo a G . Allora G_1 è isomorfo a G .*

In queste ipotesi infatti G_1 risulta essere un gruppo semplice dello stesso ordine di G , mentre i possibili ordini dei sottogruppi e dei quozienti di G_1 ci assicurano che esso è semplice minimale, e non è isomorfo ad alcun altro gruppo semplice minimale.

Per dimostrare il Teorema II, sarà allora sufficiente provare

PROPOSIZIONE D. Sia $G = PSL(3, 3)$, $\mathcal{A}$ il gruppo degli automorfismi di G , $\mathcal{A}^*$ il gruppo degli automorfismi reticolari di G . Allora è $\mathcal{A} = \mathcal{A}^*$.

Come è noto, il gruppo $G = PSL(3, 3)$, che è il gruppo delle matrici 3×3 a elementi nel corpo di Galois di ordine tre $GF(3)$ e a determinante uguale a 1, si può anche interpretare come gruppo degli automorfismi del piano proiettivo π sul corpo $GF(3)$; e $|G| = 2^4 \cdot 3^3 \cdot 13$. Sia $\Omega' = \{A, B, \dots, N, O\}$ l'insieme dei 13 punti di π , ed $\bar{\Omega}' = \{a, b, \dots, n, o\}$ quello delle 13 rette; G è gruppo di permutazioni 2-transitivo su Ω' , e analogamente su $\bar{\Omega}'$; detto G_P lo stabilizzatore in G di $P \in \Omega'$, e G_r lo stabilizzatore in G di $r \in \bar{\Omega}'$, G si può anche rappresentare come gruppo di permutazioni sull'insieme $\Omega = \{G_P \mid P \in \Omega'\}$, ponendo $g(G_P) = G_{P^g}$, tale rappresentazione risultando equivalente a quella realizzata su $\bar{\Omega}'$; e analogamente per l'insieme $\bar{\Omega} = \{G_r \mid r \in \bar{\Omega}'\}$.

La dimostrazione della Proposizione D avverrà in tre passi successivi; per le proprietà di $PSL(3, 3)$ che interverranno, si fa riferimento a [1], [5], o ad una verifica diretta.

1) $\mathcal{A}^*$ è gruppo di permutazioni su $\Omega \cup \bar{\Omega}$.

$\bar{\Omega} \cup \bar{\Omega}$ è l'insieme di tutti i sottogruppi di G di ordine $2^4 \cdot 3^3$, quindi $\varphi \in \mathcal{A}^*$ permuta gli elementi di $\Omega \cup \bar{\Omega}$; basterà provare che, se φ li fissa tutti, allora fissa tutti i sottogruppi ciclici di ordine primo di G (e quindi è identico).

Sia σ un elemento di ordine due. Allora σ fissa 5 punti, quattro dei quali allineati, ed è anzi individuato da tale condizione; posto $G_r = \bigcap_{P \in r} G_P$, avremo, per opportuni $A \in \Omega'$, $r \in \bar{\Omega}'$, $\langle \sigma \rangle = G_A \cap G_r$; da cui $\langle \sigma \rangle^* = \langle \sigma \rangle$. Con le involuzioni, φ fissa anche i sottogruppi di Klein $K \subseteq G$; questi sono in corrispondenza biunivoca con i triangoli non degeneri di π : per opportuni A, B, C non allineati, $K = G_A \cap G_B \cap G_C$. $N_G(K)$ è massimale in G , e ha ordine $2^3 \cdot 3$; quindi è fissato da φ .

I gruppi ciclici di ordine tre di G sono di due tipi:

a) quelli che fissano un solo punto Q , e una sola retta s per quel punto: se $\langle \rho \rangle$ è un tale gruppo, e se $P \notin s$, allora il gruppo $K = G_P \cap G_{\rho(P)} \cap G_{\rho^2(P)}$ è un gruppo di Klein, $\rho \in N_G(K)$, e si ha $\langle \rho \rangle = G_Q \cap N_G(K)$ e quindi φ fissa $\langle \rho \rangle$;

b) quelli che fissano quattro punti allineati, e le quattro rette per uno, Q , di tali punti; se H è un tale gruppo, si ha che $H = G_s \cap G_{\overline{Q}}$, dove s è la retta fissata « pointwise » da H , e $G_{\overline{Q}} = \bigcap_{r \ni Q} G_r$; dunque anche in questo caso $H^\varphi = H$.

Infine se C è ciclico di ordine 13 si ha che $N_G(C)$ è un sottogruppo massimale di ordine $3 \cdot 13$, quindi è fissato da φ , e con esso anche C .

2) $\mathcal{A}^*$ è imprimitivo, e ammette $\{\Omega, \overline{\Omega}\}$ come unico sistema non banale di imprimitività.

Intanto $\mathcal{A}^* \supseteq \mathcal{A}$ che è transitivo su $\Omega \cup \overline{\Omega}$ (si consideri ad es. l'automorfismo indotto su G dall'automorfismo di $GL(3,3)$ che associa ad ogni matrice la trasposta dell'inversa), ed $\mathcal{A}^* \supset G$ che è 2-transitivo su Ω e su $\overline{\Omega}$, quindi un eventuale sistema di imprimitività non banale non può essere diverso da quello indicato; proviamo che Ω è effettivamente un blocco di $\mathcal{A}^*$.

Sia $\varphi \in \mathcal{A}^*$, $G_A \in \Omega$, $G_A^\varphi = G_s \in \overline{\Omega}$: si tratterà di dimostrare che per ogni $G_P \in \Omega$ è $G_P^\varphi \in \overline{\Omega}$. Sia per assurdo $G_P^\varphi = G_Q \in \Omega$.

Allora $(G_A \cap G_P)^\varphi = G_s \cap G_Q$. Ora se $Q \in s$, $G_s \cap G_Q$ contiene un 3-Sylow-gruppo di G , mentre $3^3 \nmid |G_A \cap G_P|$; se $Q \notin s$, $G_s \cap G_Q$ contiene un 2-Sylow-gruppo di G , mentre $2^4 \nmid |G_A \cap G_P|$; poichè φ conserva gli ordini, in ambedue i casi si raggiunge una contraddizione.

Sia $\psi \in \mathcal{A}^*$, $G_P \in \Omega$. Allora, per la transitività di $\mathcal{A}$, esiste un $\alpha \in \mathcal{A}$ tale che $G_P^\psi = G_P^\alpha$; e $\varphi = \psi\alpha^{-1} \in \mathcal{A}_\Omega^*$. Proveremo ora che $\mathcal{A}_\Omega^* = G$; dimodochè $\psi\alpha^{-1} = g \in G$, e $\psi = g\alpha \in \mathcal{A}$, e quindi $\mathcal{A} = \mathcal{A}^*$, che è la conclusione cercata.

3) $\mathcal{A}_\Omega^* = G$.

Sia $\varphi \in \mathcal{A}_\Omega^*$. Essendo G 2-transitivo su Ω , moltiplicando φ per un opportuno $g_1 \in G$ si ottiene $\varphi g_1 = \varphi_1 \in \mathcal{A}_{A, B}^*$ (indichiamo qui con $\mathcal{A}_{A, B}^*$ lo stabilizzatore in $\mathcal{A}^*$ di $G_A, G_B \in \Omega$). Se C, D sono gli altri due punti della retta r per A, B , si ha $G_{A, B, C} = G_{A, B, D} = G_r$ e $|G_r| = 3^2 \cdot 2$, mentre, se $P \notin r$, $G_{A, B, P}$ è un gruppo di Klein, quindi $G_P^{\varphi_1} = G_Q$ con $Q \notin r$. Ma G_r è transitivo sull'insieme dei punti di π che non stanno su r : quindi in G_r si potrà trovare un elemento g_2 tale che $\varphi_1 g_2 = \varphi_2 \in \mathcal{A}_{A, B, E}^*$ con $E \notin r$. Dall'osservazione precedente segue che se φ_2 non fissa G_C e

G_D allora li scambia; in tal caso, moltiplicando φ_2 per una delle due involuzioni di $G_{A, B, E}$ che non stanno in G_r^* , chiamiamola g_3 , si ottiene $\varphi_2 g_3 = \varphi_3 \in \mathcal{A}_{r, E}^*$ (se invece φ_2 fissa G_C e G_D , basta porre $\varphi_2 = \varphi_3 \in \mathcal{A}_{r, E}^*$).

Con una semplice analisi delle possibili azioni di φ_3 sull'insieme Ω , associato ormai strettamente al piano π anche nelle proprietà di appartenenza, si verifica che $|\mathcal{A}_{r, E}^*| = 2$; ossia che $\mathcal{A}_{r, E}^* = G_{r, E} \ni \varphi_3$. Ma da $\varphi_3 = \varphi g_1 g_2 g_3$ segue $\varphi \in G$, c.v.d.

BIBLIOGRAFIA

- [1] DICKSON, L. E.: *Linear groups, with an exposition of the Galois field theory*, Dover, New York 1958.
- [2] HUPPERT, B.: *Endliche Gruppen I*, Springer, Berlin 1967.
- [3] METELLI, C.: *Sugli isomorfismi reticolari del gruppo proiettivo lineare speciale $PSL(2, p)$* , Atti Ist. Veneto SS.LL.AA., a.a. 1968/69, T. CXXVII, pp. 73-78.
- [4] METELLI, C.: *Sugli isomorfismi reticolari di $PSL(2, p')$* , Rend. Accad. Naz. Lincei Cl. scienze, s. VIII, vol. XLVII, fasc. 6 (1969).
- [5] MITCHELL, H. H.: *Determination of the ordinary and modular ternary linear groups*, Trans. Amer. Math. Soc., 12 (1911), 207-242.
- [6] SUZUKI, M.: *On a finite group with a partition*, Arch. Math. 12 (1961), 241-254.
- [7] SUZUKI, M.: *Structure of a group and the structure of its lattice of subgroups*, Springer, Berlin, 1956.
- [8] SUZUKI, M.: *On a class of doubly transitive groups*, Annals of Math., vol. 75, n. 1 (1962), 105-145.

Manoscritto pervenuto in redazione il 5 aprile 1971.