Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Claudia Metelli

Sugli isomorfismi reticolari di $PSL(2, p^f)$

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **47** (1969), n.6, p. 446–452.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1969_8_47_6_446_0>

Matematica. — *Sugli isomorfismi reticolari di* PSL $(2, p^f)$. Nota di CLAUDIA METELLI, presentata (*) dal Socio G. SCORZA DRAGONI.

SUMMARY. — In this paper we prove that the simple groups PSL $(2, p^f)$ (p a prime, $p^f \geq 4$) are strongly lattice determined.

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 [3] è stato dimostrato che i gruppi semplici non abeliani PSL $(2, p)$ (p primo > 3) sono individuati reticolarmente in senso stretto; scopo della presente Nota è di generalizzare il risultato ottenuto ai gruppi semplici non abeliani PSL $(2, p^f)$ (p primo, $p^f \geq 4$) se $f > 1$.

In [3] è anche stata dimostrata, valendosi di una caratterizzazione di Brauer, Suzuki e Wall [1], la seguente

PROPOSIZIONE 1: *Se il gruppo* $G = \mathrm{PSL}(2, p^f)$ (p *primo*, $p^f \geq 4$) *è reticolarmente isomorfo a un gruppo* G_1, *allora* G *è isomorfo a* G_1.

Per dimostrare che PSL $(2, p^f)$ è individuato reticolarmente in senso stretto, sarà dunque sufficiente provare il seguente

TEOREMA. *Ogni automorfismo reticolare di* $G = \mathrm{PSL}(2, p^f)$ *è indotto da uno* (*e un solo*) *automorfismo di gruppo.*

1. Richiamiamo alcune informazioni sul gruppo $G = \mathrm{PSL}(2, p^f)$ (1).

a) Consideriamo il gruppo $\bar{G} = \mathrm{PGL}(2, p^f)$ delle trasformazioni lineari fratte $x \to \frac{ax+b}{cx+d}$, con $a, b, c, d \in \mathrm{GF}(p^f)$ ed $ad - bc \neq 0$.

Come è noto, G è il sottogruppo di $\bar{G}$ costituito dalle trasformazioni per cui $ad - bc$ è un quadrato in $\mathrm{GF}(p^f)$; dimodoché $[\bar{G} : G] = 2$ se $p \neq 2$, $[\bar{G} : G] = 1$ se $p = 2$.

$\bar{G}$ si può rappresentare fedelmente come gruppo di permutazioni sull'insieme $\bar{\Omega} = \mathrm{GF}(p^f) \cup \{\infty\}$, associando ad ogni trasformazione $x \to \frac{ax+b}{cx+d}$ la permutazione $\begin{pmatrix} x \\ \frac{ax+b}{cx+d} \end{pmatrix}$, $x \in \bar{\Omega}$, dove per l'elemento ∞ si seguono le convenzioni usuali; in tale rappresentazione anzi $\bar{G}$ è esattamente 3–transitivo, mentre G (quando non coincide con $\bar{G}$) è 2–transitivo. Una rappresentazione equivalente per G si ottiene prendendo come insieme di oggetti l'insieme Ω degli stabilizzatori in G degli elementi di $\bar{\Omega}$.

(*) Nella seduta del 13 dicembre 1969.

(1) Per tutto questo paragrafo si può fare riferimento a [2], cap. II.

b) Sia $k = \text{MCD}(2, p^f - 1)$. Se G_w è lo stabilizzatore, in G, di $w \in \overline{\Omega}$, risulta $|G_w| = p^f \frac{p^f - 1}{k}$; e anzi, se un sottogruppo di G ha tale ordine, esso è lo stabilizzatore in G di un oggetto di $\overline{\Omega}$; inoltre $N_G(G_w) = G_w$.

Se u, v sono elementi distinti di $\overline{\Omega}$, lo stabilizzatore $G_{u,v} = G_u \cap G_v$ è ciclico di ordine $(p^f - 1)/k$, e ogni sottogruppo ciclico di tale ordine è lo stabilizzatore di due oggetti distinti di $\overline{\Omega}$.

Gli stabilizzatori di tre oggetti distinti di $\overline{\Omega}$ sono invece sempre identici.

Infine il normalizzante $N_G(G_{u,v})$ è un gruppo diedrale di ordine $2(p^f - 1)/k$ che indicheremo con $D_{u,v}$.

2. Sia A il gruppo degli automorfismi di G, A^* il gruppo degli automorfismi reticolari di G. Dal fatto che G è un gruppo semplice non abeliano, segue che ogni automorfismo reticolare è indotto al più da un automorfismo di gruppo; previe ovvie identificazioni, possiamo dunque scrivere $A^* \supseteq A \supseteq \overline{G} \supseteq G$.

Relativamente alla struttura di A, ricordiamo che $|A| = f|\overline{G}|$, ed anzi ogni elemento φ di A si fattorizza nel prodotto $x\beta$ di un elemento x di $\overline{G}$ per un automorfismo β, indotto su G da un automorfismo $\overline{\beta}$ del corpo $GF(p^f)$ [4].

PROPOSIZIONE 2: A^* *si può rappresentare fedelmente come gruppo di permutazioni su* $\Omega = \{G_x \mid x \in \overline{\Omega}\}$, *e risulta anzi 3-transitivo su* Ω.

G è semplice, quindi ogni automorfismo reticolare di G conserva gli indici dei sottogruppi [5]; da ciò, e dal punto *b*) del paragrafo precedente, segue che ogni $\tau \in A^*$ induce una permutazione su Ω.

Per dimostrare che se τ induce su Ω la permutazione identica allora $\tau = 1$, possiamo valerci dell'esistenza in G di una partizione [2] in sottogruppi disgiunti (rispettivamente ciclici di ordine $(p^f - 1)/k$, ciclici di ordine $(p^f + 1)/k$, e abeliani elementari di ordine p^f), dimostrando che τ muta in sè ogni elemento di questa partizione e ogni suo sottogruppo.

Se $G_w = G_w^\tau$ per ogni $w \in \overline{\Omega}$, allora anche $(G_{u,v})^\tau = (G_u \cap G_v)^\tau = (G_u)^\tau \cap (G_v)^\tau = G_u \cap G_v = G_{u,v}$, ossia τ fissa tutti i sottogruppi ciclici di ordine $(p^f - 1)/k$, e quindi ogni loro sottogruppo. Inoltre $D_{u,v} = (D_{u,v})^\tau$, dimodoché τ fissa anche tutti i sottogruppi di ordine 2 di G [2], e tutti i sottogruppi diedrali di G.

Sia H un sottogruppo di G di ordine $(p^f + 1)/k$; $N_G(H)$ è diedrale di ordine $2(p^f + 1)/k$ [2]; allora τ fissa $N_G(H)$ e quindi H.

Quanto ai sottogruppi abeliani elementari di ordine p^f, ciascuno di essi è contenuto in uno e uno solo dei G_x, ed è quindi fissato da τ. Rimane da provare che τ fissa ogni sottogruppo di ordine p.

Se $p = 2$, ciò risulta dalle considerazioni precedenti.

(2) Infatti sia $1 \neq g \in G$, $g^2 = 1$, $g = (u, v)(w, z) \cdots (u, v, w, z \cdots \in \overline{\Omega})$ nella sua fattorizzazione in cicli disgiunti; allora $\langle g \rangle = N_G(G_{u,v}) \cap N_G(G_{w,z}) = D_{u,v} \cap D_{w,z}$.

Se $p > 2$, sia M un sottogruppo abeliano elementare di G di ordine p^f, ed h un suo elemento diverso da 1. Dimostreremo che τ fissa il sottogruppo ciclico generato da h.

I) Sia $p > 3$. Cominceremo col provare che $\langle h\rangle \subset \overline{K} \subset G$, con $\overline{K} \simeq PSL(2, p)$. A questo scopo, consideriamo il sottogruppo $K = \langle h, t, g\rangle \subseteq G$ dove t è un elemento di $N_G(\langle h\rangle)$ di ordine $(p-1)/2$, e g è un'involuzione di $N_G(\langle t\rangle)$ ma $g \notin \langle t\rangle$. Da [2], Lemma 8.26, sappiamo che risulta o $K \simeq PGL(2, p^m)$ oppure $K \simeq PSL(2, p^m)$, con $m \leq f$. Si tratterà dunque di dimostrare che si possono scegliere t e g in G in modo che $m = 1$.

Poiché G è 2-transitivo, possiamo limitarci al caso che sia $h \in G_\infty$, $t \in G_{0,\infty}$; proviamo che, per un'opportuna scelta di g, l'insieme $\Gamma = \{\infty, 0, h(0), \cdots \cdots, h^{p-1}(0)\} \subset \overline{\Omega}$ è una classe di transitività per K. Essendo h di ordine p, e $h(\infty) = \infty$, è $h(\Gamma) = \Gamma$; inoltre $t(0) = 0$, $t(\infty) = \infty$, $t \in N_G(\langle h\rangle)$ da cui $t(h^s(0)) = h^r(t(0)) = h^r(0)$, e dunque anche $t(\Gamma) = \Gamma$. Per procedere alla scelta di g, ricordiamo che h è una sostituzione del tipo $x \to x + b$ $(b \neq 0)$. Sia allora $g : x \to \frac{-b^2}{x}$; g è un'involuzione di G, $g(\infty) = 0$, e se $h^s(0) \neq 0$, $g(h^s(0)) = \frac{-b^2}{sb} = -bs^{-1} = h^{s'}(0)$, dimodoché $g(\Gamma) = \Gamma$. Dunque Γ è classe di transitività per K, per cui $m = 1$, e $\langle h\rangle \subset \overline{K} \simeq PSL(2, p) \subseteq K$; anzi, $\langle h\rangle = G_\infty \cap \overline{K}$.

Poiché τ fissa tutti i sottogruppi ciclici di G di ordine $(p \pm 1)/2$, τ fissa $\overline{K}$ (che è generato da due tali sottogruppi); allora $\langle h\rangle^\tau = (G_\infty \cap \overline{K})^\tau = G_\infty^\tau \cap \overline{K}^\tau = G_\infty \cap \overline{K} = \langle h\rangle$, c.v.d.

II) Sia infine $p = 3$, e costruiamo di nuovo il gruppo K. Qui $t^{(p-1)/2} = t = 1$, perciò $K = \langle h, g\rangle$; K è ancora rappresentabile come gruppo di permutazioni sull'insieme $\Gamma = \{\infty, 0, h(0), h^2(0)\}$, anzi è isomorfo al gruppo alterno A(4) su Γ, essendo la rappresentazione fedele (risulta infatti dal n. 1.b che due elementi di G che agiscano allo stesso modo su tre oggetti di $\overline{\Omega}$ coincidono). È

$$\langle h\rangle = \overline{K} \cap G_\infty \quad ; \quad A(4) \simeq \overline{K}^\tau = \langle h\rangle^\tau \cup \langle g\rangle^\tau = \langle h'\rangle \cup \langle g\rangle = \langle h', g\rangle ;$$

$$\langle h'\rangle = \langle h\rangle^\tau = (\overline{K} \cap G_\infty)^\tau = \overline{K}^\tau \cap G_\infty \qquad \text{per cui} \quad h'(\infty) = \infty .$$

Inoltre, dato che τ fissa i sottogruppi di ordine 2 di G, sarà $h' g h'^{-1} \in \overline{K}$, e quindi ad esempio $h' g h'^{-1}(\infty) = b$ [3]; allora $h'^{-1} g h'(\infty) = -b$, e

$$h'(0) = h' g(\infty) = h' g h'^{-1}(\infty) = b$$

$$h'^{-1}(0) = h'^{-1} g(\infty) = h^{-1} g h'(\infty) = -b \quad \text{da cui} \quad h'(-b) = 0$$

e h', operando come h su $\{\infty, 0, b\} \subseteq \overline{\Omega}$ coincide con h. Dunque $\langle h\rangle^\tau = \langle h\rangle$.

A* è dunque rappresentabile come gruppo di permutazioni su Ω; per provarne la 3-transitività, basterà individuare un suo sottogruppo che goda

(3) L'altra alternativa, cioè $h' g h'^{-1}(\infty) = -b$, porta ad analoghe conclusioni.

di tale proprietà. A^* contiene $\bar{G}$, che si rappresenta quindi fedelmente come gruppo di permutazioni su Ω; per riconoscere che in tale rappresentazione $\bar{G}$ è 3–transitivo, dimostriamo che essa è equivalente alla rappresentazione di $\bar{G}$ su $\bar{\Omega}$ introdotta nel n. 2.b).

Se $k \in \bar{G}$, indichiamo con lo stesso simbolo k la permutazione $\begin{pmatrix} x \\ k(x) \end{pmatrix}$ corrispondente a k nella rappresentazione di $\bar{G}$ su $\bar{\Omega}$; e sia $\bar{k} = \begin{pmatrix} G_x \\ kG_x k^{-1} \end{pmatrix}$ la permutazione corrispondente a k nella rappresentazione di $\bar{G}$ su Ω. Allora se $h , k \in \bar{G}$, $\overline{hk} = \bar{h} \cdot \bar{k}$; se per di più è $h \neq k$, allora $\begin{pmatrix} G_x \\ kG_x k^{-1} \end{pmatrix} \neq \begin{pmatrix} G_x \\ hG_x h^{-1} \end{pmatrix}$. Dall'eguaglianza infatti segue $(h^{-1}k)\, G_x (h^{-1}k)^{-1} = G_x$ per ogni x di Ω, da cui $h^{-1}k \in \bigcap_{x \in \Omega} N_{\bar{G}}(G_x) = \bigcap_{x \in \bar{\Omega}} \bar{G}_x = 1$, c.v.d.

3. Dalla 3–transitività di A^* consegue immediatamente

PROPOSIZIONE 3: $A^* = \bar{G} A^*_{0,1,\infty}$, $A = \bar{G} A_{0,1,\infty}$ (4)

e ciò ci consente di ricondurre la dimostrazione della $A^* = A$ alla $A^*_{0,1,\infty} = A_{0,1,\infty}$.

Ricordiamo a questo punto che gli elementi di $A_{0,1,\infty}$ sono proprio gli automorfismi indotti su G dagli automorfismi di $GF(p^f)$. Costruiremo ora una corrispondenza biunivoca tra l'insieme degli automorfismi di $GF(p^f)$ ed $A^*_{0,1,\infty}$; la quale, unita alla $A^*_{0,1,\infty} \supseteq A_{0,1,\infty}$, porterà alla conclusione che $A^*_{0,1,\infty} = A_{0,1,\infty}$ e quindi alla dimostrazione del Teorema.

Per ogni $\alpha \in A^*_{0,1,\infty}$, sia $\bar{\alpha}$ la permutazione degli elementi di $\bar{\Omega}$ $(= GF(p^f) \cup \{\infty\})$ definita da $(G_x)^\alpha = G_{x\bar{\alpha}}$. Poiché $\bar{\alpha}(\infty) = \infty$, $\bar{\alpha}$ induce sul corpo una biiezione che indicheremo ancora con $\bar{\alpha}$. Essa fissa gli elementi 0 , 1; nostro scopo sarà dimostrare che $\bar{\alpha}$ è anche un automorfismo di $GF(p^f)$; ossia provare che, se $u , v \in GF(p^f)$ risulta $G_{(u+v)\bar{\alpha}} = G_{u\bar{\alpha}+v\bar{\alpha}}$, e $G_{(uv)\bar{\alpha}} = G_{u\bar{\alpha}\, v\bar{\alpha}}$.

PROPOSIZIONE 4: $\bar{\alpha}$ *subordina l'identità sul sottocorpo fondamentale* $GF(p)$ *di* $GF(p^f)$.

Per $p = 2$, l'affermazione è vera.

Se $p = 3$, si tratterà di dimostrare che $(G_{-1})^\alpha = G_{-1}$.

A questo scopo, consideriamo il sottogruppo $K = \langle h , g \rangle \simeq A(4)$ (ved. Prop. 2), dove questa volta $b = 1$, ossia $h : x \to x+1$, $g : x \to -(1/x)$. Allora $K^\alpha \simeq A(4)$, $K^\alpha = \langle h \rangle^\alpha \cup \langle g \rangle^\alpha = \langle h' \rangle \cup \langle g' \rangle$ con $\langle h' \rangle \subset G_\infty$, $\langle g' \rangle \subset D_{0,\infty}$, per cui $h' : x \to x + b$, $g' : x \to -(c^2/x)$. Quanto alle altre due involuzioni di K, era $h^{-1}gh \in D_{0,1}$, $hgh^{-1} \in D_{1,\infty}$; quindi per i sottogruppi

(4) Indichiamo per brevità con A^*_x (con A_x) lo stabilizzatore in A^* (in A) dell'elemento G_x di Ω, ossia l'insieme degli automorfismi α di A^* (di A) per cui $(G_x)^\alpha = G_x$.

di ordine due di K^α potranno verificarsi due casi:

I) $\langle h'^{-1}g'h'\rangle = \langle h^{-1}gh\rangle^\alpha \subset D_{0,1}$, e $\langle h'\,g'\,h'^{-1}\rangle \subset D_{1,\infty}$, e allora

$$1 = h'g'\,h'^{-1}(\infty) = h'g'(\infty) = h'(0) = b$$

$$1 = h'^{-1}g'\,h'(0) = h'^{-1}g'(b) = h'^{-1}(-c^2/b) = -c^2/b - b$$

da cui $c^2 = b = 1$, e $h = h', g = g'$;

II) $\langle h^{-1}gh\rangle^\alpha = \langle h'g'\,h'^{-1}\rangle \subset D_{0,1}$, $\langle h'^{-1}g'h'\rangle \subset D_{1,\infty}$, e allora

$$1 = h'^{-1}g'h'(\infty) = h'^{-1}g'(\infty) = h'^{-1}(0) = -b$$

$$1 = h'g'h'^{-1}(0) = h'g'(-b) = h'(c^2/b) = c^2/b + b$$

da cui $b = -1$, $c^2 = 1$ e $h' = h^2, g = g'$.

In ogni caso dunque $K^\alpha = K$; ma allora i sottogruppi di ordine tre di K–rispettivamente $K_\infty = G_\infty \cap K$ $(= \langle h\rangle)$, $K_0 = G_0 \cap K$, $K_1 = G_1 \cap K$, K_{-1} sono fissati da α; e poiché $K_{-1} \subset G_{-1}$, mentre $K_{-1} \cap G_x = 1$ per ogni $x \neq -1$ di $\bar{\Omega}$, allora $(G_{-1})^\alpha = G_{-1}$ c.v.d.

Sia infine $p > 3$. Consideriamo in G il sottogruppo $H \simeq PSL(2, p)$ costituito dagli elementi $x \to \frac{ax+b}{cx+d}$ di G per cui $a, b, c, d \in GF(p)$; sia $\Gamma = GF(p) \cup \{\infty\} \subset \bar{\Omega}$. Allora $H_{0,1}$ è il sottogruppo di ordine $(p-1)/2$ di $G_{0,1}$, quindi $(H_{0,1})^\alpha = H_{0,1}$; analogamente $(H_{1,\infty})^\alpha = H_{1,\infty}$ e $(H_{0,\infty})^\alpha = H_{0,\infty}$. Essendo $H = H_{0,1} \cup H_{1,\infty} \cup H_{0,\infty}$, si ha che α induce su H un automorfismo reticolare che fissa H_0 $(= H_{0,1} \cup H_{0,\infty})$, e similmente H_1, H_∞; ma allora $(H_x)^\alpha = Hr$ per ogni x in Γ (come è provato in [3]). Poiché se $y \in \Gamma$ allora $G_y \supset H_x$ se e solo se $y = x$, allora anche $(G_x)^\alpha = G_x$ per ogni x in Γ, in particolare pe$_x$ ogni $x \in GF(p)$, c.v.d.

PROPOSIZIONE 5. *Se* $\alpha \in A^*_{0,1,\infty}$, $\bar{\alpha}$ *è un automorfismo del semigruppo moltiplicativo di* $GF(p^f)$.

Anzitutto $(0x)^{\bar{\alpha}} = 0x^{\bar{\alpha}} = 0$ per ogni $x \in GF(p^f)$: infatti $(G_x)^\alpha = G_{x^{\bar{\alpha}}} \neq G_\infty$, e $G_{(0x)^{\bar{\alpha}}} = (G_{0x})^\alpha = (G_0)^\alpha = G_0 = G_{0x^{\bar{\alpha}}}$.

Per dimostrare che $(uv)^{\bar{\alpha}} = u^{\bar{\alpha}} v^{\bar{\alpha}}$ $(u, v \in GF(p^f), uv \neq 0)$ dovremo distinguere due casi. Sia Q l'insieme degli elementi di $GF(p^f)$ che sono dei quadrati in $GF(p^f)$, e $-Q$ l'insieme degli opposti dei quadrati. Notiamo subito – cosa che risulterà utile nel corso delle dimostrazioni successive – che se $p \neq 2$, $p^f \not\equiv 1 \pmod 4$, allora $GF(p^f) = -Q \cup Q$ e $(-Q) \cap Q = \{0\}$; se $p \neq 2$, $p^f \equiv 1 \pmod 4$ allora $Q = -Q$, e $GF(p^f) = Q \cup \sigma Q$, dove σ è un generatore del gruppo ciclico moltiplicativo di $GF(p^f)$; se $p = 2$, $-Q = Q = GF(p^f)$.

I. Siano $u, v \in GF(p^f)$, con $0 \neq uv \in -Q$; proviamo che $u^{\bar{\alpha}} v^{\bar{\alpha}} = (uv)^{\bar{\alpha}}$. In queste ipotesi, $g : x \to \frac{uv}{x}$ è un'involuzione di G, $g = (0, \infty)(u, v)(1, uv)\cdots$. Dunque $\langle g\rangle = D_{0,\infty} \cap D_{u,v} = D_{0,\infty} \cap D_{1,uv}$. Ricordando che $(D_{0,\infty})^\alpha = D_{0,\infty}$,

$(G_1)^\alpha = G_1$, sarà $\langle g\rangle^\alpha = D_{0,\infty} \cap D_{1,(uv)^{\bar\alpha}}$. D'altra parte $(G_{u,v})^\alpha = (G_u \cap G_v)^\alpha = (G_u)^\alpha \cap (G_v)^\alpha = G_{u^{\bar\alpha}} \cap G_{v^{\bar\alpha}} = G_{u^{\bar\alpha}, v^{\bar\alpha}}$ e quindi è anche $\langle g\rangle^\alpha = D_{0,\infty} \cap D_{u^{\bar\alpha}, v^{\bar\alpha}}$. Sia $\langle g\rangle^\alpha = \langle g_1\rangle$; $g_1 \in D_{0,\infty}$, dunque sarà del tipo $x \to \frac{-c^2}{x}$; ma $(uv)^{\bar\alpha} = g_1(1) = -c^2 = u^{\bar\alpha} g_1(u^{\bar\alpha}) = u^{\bar\alpha} v^{\bar\alpha}$.

A questo punto, se $p = 2$, la proposizione è dimostrata.

II. Sia $0 \neq st \notin -Q$; $s, t \in GF(p^f)$; e sia $p \neq 2$.

a) $p^f \equiv 1 \pmod 4$. Se σ è un generatore del gruppo ciclico moltiplicativo di $GF(p^f)$, allora $st = \sigma^{2k+1}$, e ad esempio $s = \sigma^{2n+1}$, $t = \sigma^{2m}$; quindi $\sigma st \in -Q\ (= Q)$, $\sigma s \in -Q$. Possiamo allora scrivere

$$(\sigma st)^{\bar\alpha} = \sigma^{\bar\alpha} (st)^{\bar\alpha}$$

$$(\sigma st)^{\bar\alpha} = (\sigma s)^{\bar\alpha} t^{\bar\alpha} = \sigma^{\bar\alpha} s^{\bar\alpha} t^{\bar\alpha}$$

da cui $(st)^{\bar\alpha} = s^{\bar\alpha} t^{\bar\alpha}$.

b) $p^f \not\equiv 1 \pmod 4$. σ abbia ancora il significato precedente. Allora $st \notin -Q$ se e solo se $st = \sigma^{2k}$.

Se $s = \sigma^{2n}$, $t = \sigma^{2m}$, si ha $\sigma st \in -Q$, $\sigma s \in -Q$, e un ragionamento analogo al precedente porta a concludere che $(st)^{\bar\alpha} = s^{\bar\alpha} t^{\bar\alpha}$.

Se $s = \sigma^{2n+1}$, $t = \sigma^{2m+1}$, allora $\sigma st \in -Q$, da cui

$$(\sigma st)^{\bar\alpha} = (\sigma s)^{\bar\alpha} t^{\bar\alpha} = \sigma^{\bar\alpha} (st)^{\bar\alpha}$$

cioè

$$(st)^{\bar\alpha} = (\sigma^{\bar\alpha})^{-1} (\sigma s)^{\bar\alpha} t^{\bar\alpha}.$$

Proviamo che $(\sigma^{\bar\alpha})^{-1} (\sigma s)^{\bar\alpha} = s^{\bar\alpha}$; ossia, essendo $s \in -Q$ e quindi $s^{\bar\alpha} = (\sigma^{-1}\sigma s)^{\bar\alpha} = (\sigma^{-1})^{\bar\alpha} (\sigma s)^{\bar\alpha}$, proviamo che $(\sigma^{\bar\alpha})^{-1} = (\sigma^{-1})^{\bar\alpha}$; anzi, più in generale:

PROPOSIZIONE 5*: *Sia* $p \neq 2$, $p^f \not\equiv 1$ *(mod. 4), e* $0 \neq x \in GF(p^f)$. *Allora è* $(x^{-1})^{\bar\alpha} = (x^{\bar\alpha})^{-1}$ *per ogni* $\alpha \in A^*_{0,1,\infty}$.

Sia $b \in GF(p^f)$ tale che $b^2 - 1 \in Q$; allora $g : x \to \frac{x-b}{bx-1}$ è un'involuzione di G, e $g = (1, -1)(0, b)(\infty, b^{-1}) \cdots$.

Notiamo subito che, se $b \neq 0$, e $b^2 - 1 = z^2$, si ha $b^{-2} - 1 = \frac{1-b^2}{b^2} = -\frac{z^2}{b^2}$, e quindi, nelle nostre ipotesi, $b^{-2} - 1 \notin Q$, e viceversa; in altri termini, per ogni $b \neq 0$ in $GF(p^f)$ esiste un'involuzione g di G tale che o $g(b) = 0$ o $g(b) = \infty$.

Sia dunque $0 \neq b \in GF(p^f)$, e ad esempio $g(b) = 0$. Allora $\langle g\rangle = D_{1,-1} \cap D_{0,b} = D_{1,-1} \cap D_{\infty, b^{-1}}$; e $\langle g\rangle^\alpha = D_{1,-1} \cap D_{0, b^{\bar\alpha}} = D_{1,-1} \cap D_{\infty, (b^{-1})^{\bar\alpha}}$ (infatti è $(-1)^{\bar\alpha} = -1$ per la Prop. 4). È inoltre $\langle g\rangle^\alpha = \langle g_1\rangle$ con $g_1 \in D_{1,-1}$; ma allora g_1 è del tipo $x \to \frac{x-b_1}{b_1 x - 1}$, da cui $(b^{-1})^{\bar\alpha} = g_1(\infty) = b_1^{-1} = g_1(0)^{-1} = (b^{\bar\alpha})^{-1}$.

Con ciò la Proposizione 5 è completamente dimostrata.

Concludiamo la dimostrazione del Teorema provando che

PROPOSIZIONE 6: *Se* $\alpha \in A^*_{0,1,\infty}$, $\bar\alpha$ *è un automorfismo del gruppo additivo di* $GF(p^f)$.

Si tratterà di dimostrare che, per ogni coppia di elementi u, v di GF (p^f), risulta $(u+v)^{\bar\alpha} = u^{\bar\alpha} + v^{\bar\alpha}$. Se $u = v$, dalle Prop. 4 e 5 consegue che $(u+v)^{\bar\alpha} = (2u)^{\bar\alpha} = 2u^{\bar\alpha} = u^{\bar\alpha} + v^{\bar\alpha}$; considereremo quindi nel seguito $u \neq v$.

I. Sia $p = 2$, oppure $p^f \equiv 1 \pmod 4$. Consideriamo in G l'involuzione $g: x \to -x + (u+v), g = (\infty)(u,v)(0, u+v)\cdots$. Allora $\langle g\rangle = G_\infty \cap D_{u,v} \cap D_{0,u+v}$; dimodoché $\langle g_1\rangle = \langle g\rangle^\alpha = G_\infty \cap D_{u^{\bar\alpha}, v^{\bar\alpha}} \cap D_{0,(u+v)^{\bar\alpha}}$. Da $g_1 \in G_\infty$ segue che g_1 è del tipo $x \to -x + g_1(0)$; anzi $g_1(0) = (u+v)^{\bar\alpha}$. Ma $g_1 \in D_{u^{\bar\alpha}, v^{\bar\alpha}}$, quindi $u^{\bar\alpha} = -v^{\bar\alpha} + g_1(0) = -v^{\bar\alpha} + (u+v)^{\bar\alpha}$.

II. Sia $p \neq 2$, $p \not\equiv 1 \pmod 4$; allora si ha:

PROPOSIZIONE 6*: *Sia $p \neq 2$, $p^f \not\equiv 1$ (mod. 4), w un elemento di* GF (p^f). *Allora è* $(w-1)^{\bar\alpha} = w^{\bar\alpha} - 1$ *per ogni* $\alpha \in A^*_{0,1,\infty}$.

Per $w = 0$, e $w = 1$, la proposizione è vera, come si verifica immediatamente. Sia dunque $w \neq 0, 1$, e consideriamo in G l'involuzione $g: x \to \frac{x-1}{(2/w)x - 1}$, dove w è un elemento di GF (p^f) tale che $-1 + (2/w) \in Q$. Allora $g = (0,1)(\infty, w/2)(w, w-1)\cdots$, $\langle g\rangle = D_{0,1} \cap D_{\infty, w/2} \cap D_{w, w-1}$; e $\langle g_1\rangle = \langle g\rangle^\alpha = D_{0,1} \cap D_{\infty,(w/2)^{\bar\alpha}} \cap D_{w^{\bar\alpha},(w-1)^{\bar\alpha}}$. Da $g_1 \in D_{0,1}$ segue che g_1 è del tipo $x \to \frac{x-1}{(2/w_1)x - 1}$, ossia $w_1/2 = g_1(\infty) = (w/2)^{\bar\alpha} = w^{\bar\alpha}/2$ (ved. Prop. 5). Allora sarà

$$(w-1)^{\bar\alpha} = g_1(w^{\bar\alpha}) = g_1(w_1) = w_1 - 1 = w^{\bar\alpha} - 1 .$$

Sia ora $t \in$ GF (p^f) tale che $-1 + 2/t \notin Q$, e dimostriamo che anche per t vale la Prop. 6*. È $-1 + (2/t) = -z^2 \in -Q$; $t = \frac{2}{1-z^2}$, $t - 1 = \frac{1+z^2}{1-z^2}$. Chiamiamo w l'elemento $\frac{2}{1+z^2}$, dato che $-1 + (2/w) = z^2 \in Q$ e quindi $(w-1)^{\bar\alpha} = w^{\bar\alpha} - 1$. Allora $w - 1 = \frac{1}{t-1}$, $t = \frac{w}{w-1}$; e dunque $(t-1)^{\bar\alpha} = \left(\frac{1}{w-1}\right)^{\bar\alpha} = \frac{1}{w^{\bar\alpha} - 1} = \frac{w^{\bar\alpha}}{w^{\bar\alpha} - 1} - 1 = \left(\frac{w}{w-1}\right)^{\bar\alpha} - 1 = t^{\bar\alpha} - 1$, come volevamo.

Presi ora $u, v \in$ GF (p^f), sia w tale che $u + v = uw$ se $u \neq 0$ ($u + v = vw$ se $v \neq 0$). Si ha $(u+v)^{\bar\alpha} = u^{\bar\alpha} w^{\bar\alpha}$; $v^{\bar\alpha} = (uw - u)^{\bar\alpha} = u^{\bar\alpha}(w-1)^{\bar\alpha} = u^{\bar\alpha}(w^{\bar\alpha} - 1) = u^{\bar\alpha} w^{\bar\alpha} - u^{\bar\alpha}$, da cui $u^{\bar\alpha} + v^{\bar\alpha} = u^{\bar\alpha} w^{\bar\alpha} = (uw)^{\bar\alpha} = (u+v)^{\bar\alpha}$ c.v.d.

BIBLIOGRAFIA.

[1] R. BRAUER, M. SUZUKI e E. WALL, *A characterization of the one-dimensional unimodular projective groups over finite fields*, « Illinois J. Math. », 2, 718–745 (1958).

[2] B. HUPPERT, *Endliche Gruppen I.*, Springer, Berlin 1967.

[3] C. METELLI, *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] O. SCHREIER e B. L. VAN DER WAERDEN, *Die Automorphismen der projektiven Gruppen*, « Abh. Math. Sem. Univ. Hamburg », 6, 303–322 (1928).

[5] M. SUZUKI, *Structure of a group and the structure of its lattice of subgroups*. Springer, Berlin 1956.