Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Giuseppe Pellegrino

Un'osservazione sul problema dei k-archi completi in $S_{2,q}$, con $q \equiv 1 \pmod 4$

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **63** (1977), n.1-2, p. 33–44.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1977_8_63_1-2_33_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1977.

Geometrie finite. — *Un'osservazione sul problema dei k-archi completi in* $S_{2,q}$, *con* $q \equiv 1 \pmod 4$. Nota(*) di GIUSEPPE PELLEGRINO, presentata dal Socio B. SEGRE.

SUMMARY. — In a Galois plane, $S_{2,q}$, $q \equiv 1 \pmod 4$, we study complete k-arcs different from an oval and containing $(q+3)/2$ points of an irriducible conic. For $q > 9$, we obtain two kinds of these arcs, having order $(q+7)/2$ and $(q+5)/2$ respectively; moreover, for $q \geq 9$, the value $k = (q+7)/2$ is the largest order of the considered arcs.

INTRODUZIONE

In un piano di Galois, $S_{2,q}$, cioè in uno spazio a due dimensioni costruito sopra un campo di Galois, $K = GF(q)$, di ordine $q = p^h$ (con h intero positivo e p numero primo), dicesi k-arco – oppure arco di ordine k – un insieme di k punti tre qualsiansi dei quali siano sempre non allineati. Una retta di $S_{2,q}$ dicesi secante (o corda), tangente, esterna a un k-arco secondo che contiene due, uno, nessun punto di questo. Un k-arco è completo se non è un sottoinsieme proprio di un $(k+1)$-arco; o anche, in forma equivalente, se ogni punto di $S_{2,q}$ (non sull'arco) appartiene a una corda almeno del k-arco. Dicesi inoltre ovale di $S_{2,q}$ un k-arco massimo, cioè un k-arco tale che ogni $(k+1)$-pla di punti di $S_{2,q}$ ammette almeno una terna di punti allineati.

Il problema della determinazione dell'ordine delle ovali di $S_{2,q}$ è risolto (cfr. [1], [2], [7], [8]): per q dispari, come qui sempre supponiamo, l'ordine di un'ovale è $q+1$; inoltre (cfr. ad esempio [7], [8]) ogni ovale è una conica irriducibile e viceversa. È invece aperto il problema consistente nella costruzione di k-archi completi di $S_{2,q}$ che non siano ovali.

L. Lombardo Radice ha costruito (cfr. [5], [7]) archi completi di ordine $(q+5)/2$ nel caso $q \equiv 3 \pmod 4$. Più recentemente G. Korchmaros (cfr. [4]) ha determinato altri archi completi diversi dalle ovali. Precisamente ha ritrovato $\frac{1}{2}(q+5)$-archi completi nel caso $q \equiv 3 \pmod 4$, mentre per $q \equiv 1 \pmod 4$ ha costruito $\frac{1}{2}(q+3)$-archi completi. Inoltre, sempre per $q \equiv 1 \pmod 4$, ha costruito archi di ordine $(q+7)/2$ e ne ha dimostrato la completezza nel caso particolare che q sia del tipo $q = 2p - 1$ con p numero primo dispari. In quest'ultimo caso ha anche precisato che per un k-arco, che non sia un'ovale e che contenga $(q+3)/2$ punti di una conica irriducibile, risulta $k \leq (q+7)/2$.

Gli archi completi suddetti si ottengono scegliendo opportunamente un insieme U di punti sopra una conica irriducibile $\mathscr{C}$ di $S_{2,q}$ e aggregando ad U altri punti secondo un procedimento indicato da B. Segre (cfr. [7]).

Seguendo questa indicazione, vengono qui dimostrate alcune proposizioni relative ai k-archi di $S_{2,q}$ con $q \equiv 1 \pmod 4$. Precisamente viene estesa ad ogni valore $q \geq 9$ la validità del risultato di G. Korchmaros relativa agli archi di ordine $(q+7)/2$. Inoltre, per $q > 9$, sono costruiti archi completi di ordine $(q+5)/2$, contenenti $(q+3)/2$ punti di un'ovale.

(*) Pervenuta all'Accademia il 4 luglio 1977.

1. Introdurremo le notazioni e richiameremo brevemente alcune note proprietà del campo $K = GF(q)$ di Galois, dove $q = p^h$ è potenza intera positiva del numero primo p. Qui e nel seguito supporremo p dispari e

$$q = 4t + 1 \equiv 1 \pmod 4 \tag{1.1}$$

(per le dimostrazioni si rinvia alla bibliografia e, in particolare, a [6], [7], [9]).

1.1) Gli elementi del campo minimo Z/p, contenuto in K, saranno indicati con $0, 1, \cdots, p-1$, essendo 0 e 1 lo zero e l'unità di K. Per $0 \neq z \in K$, porremo $z/0 = \infty$ e indicheremo con $\overline{K}$ l'insieme $\overline{K} = \{K \cup \infty\}$.

1.2) $(q-1)/2$ elementi di $\{K \setminus 0\}$ sono quadrati e gli altri non quadrati. Per indicare che $z \in K$ è oppure no un quadrato scriveremo, rispettivamente, $z \sim 1$, $z \nsim 1$.

1.3) In $GF(q)$, con q dato dalla (1.1), l'elemento -1 è un quadrato. Indicheremo con $\pm i$ le radici quadrate di -1.

1.4) Per ogni z_i, z_j appartenenti a $\{K \setminus 0\}$, risulta $z_i z_j \sim 1$, oppure $z_i z_j \nsim 1$ secondo che z_i e z_j hanno o no lo stesso carattere quadratico.

Sia $\mathscr{C}$ una conica irriducibile, cioè un $(q+1)$-arco del piano $S_{2,q}$ costruito sul campo K. Assumendo i punti fondamentali del piano come vertici di un triangolo autopolare rispetto a $\mathscr{C}$, l'equazione di questa assume la forma

$$ax^2 + by^2 + cz^2 = 0\,; \tag{1.2}$$

i coefficienti a, b, c, essendo la conica irriducibile, sono elementi non nulli di K.

Dal 1.1), 1.2), 1.3), 1.4) si deducono facilmente le seguenti proprietà elementari di $\mathscr{C}$.

1.5) Uno almeno dei lati di un triangolo autopolare rispetto a $\mathscr{C}$ è secante $\mathscr{C}$; gli altri due sono o entrambi secanti oppure entrambi esterni a $\mathscr{C}$. Supponendo che i lati del triangolo fondamentale siano tutti secanti di $\mathscr{C}$ questa può essere rappresentata dall'equazione canonica

$$f(x, y, z) = x^2 + y^2 + z^2 = 0\,. \tag{1.3}$$

1.6) Un punto $P(\alpha, \beta, \gamma)$ di $S_{2,q}$ risulta esterno o interno a $\mathscr{C}$ secondo che risulta, rispettivamente, $f(P) \sim 1$ oppure $f(P) \nsim 1$.

Una retta $y = mx$, passante per il punto $O(0, 0, 1)$ risulta esterna o secante secondo che $(m^2 + 1) \nsim 1$ oppure $(m^2 + 1) \sim 1$. Per $m = \pm i$ si hanno le tangenti passanti per O.

1.7) Le equazioni

$$x = -i(u^2 + 1) \quad ; \quad y = u^2 - 1 \quad ; \quad z = 2u \tag{1.4}$$

al variare di u in K danno una rappresentazione parametrica dei $q+1$ punti di $\mathscr{C}$, quando si associa al punto $(-i, 1, 0)$ il valore $u = \infty$ del parametro. Nel seguito con l'espressione «punto u di $\mathscr{C}$» si intenderà il punto $P(u)$ di $\mathscr{C}$, avente coordinata parametrica u.

1.8) L'involuzione τ su $\mathscr{C}$, avente come punti doppi 0 e ∞, è rappresentata dalla equazione

$$u + v = 0\,. \tag{1.5}$$

Pertanto i punti (non uniti) di $\mathscr{C}$ che si corrispondono nella τ hanno coordinate parametriche opposte.

Ripartiamo i $q-1$ punti di $\mathscr{C}$, diversi da 0 e ∞, in due insiemi disgiunti U e V secondo il criterio seguente:

«se u è un punto di $\mathscr{C}$ appartenente ad U, il suo opposto $v = -u$ è in V». Ogni ripartizione $\lambda = \{U, V\}$ di $\mathscr{C}$ effettuata applicando il suddetto criterio, sarà detta λ-partizione di $\mathscr{C}$.

1.9) Le λ-partizioni distinte dei punti di $\mathscr{C}$ costituiscono un insieme $\mathscr{R}$ di potenza $|\mathscr{R}| = 2^{\frac{1}{2}(q-1)}$.

Sia $U = \{u_i\}$, $V = \{v_i\}$ $(i = 1, 2, \cdots, \frac{1}{2}(q-1))$ una fissata λ-partizione di $\mathscr{C}$. Posto $U' = \{U \cup \{\infty, o\}\}$, consideriamo l'insieme $\mathscr{C}_\lambda = \{U' \cup O\}$ ottenuto associando all'insieme U' il punto $O(o, o, 1)$, polo della retta $z = o$ rispetto a $\mathscr{C}$. Dalle proprietà di $\mathscr{C}$ e dal fatto che due punti di U' non sono mai allineati con O, segue:

1.10) $\mathscr{C}_\lambda$ è un $\frac{1}{2}(q+5)$-arco di $S_{2,q}$ contenente $(q+3)/2$ punti di $\mathscr{C}$.

Le considerazioni dei successivi paragrafi porteranno alla dimostrazione delle seguenti proposizioni:

TEOREMA 1. *In un piano di Galois* $S_{2,q}$, *con* $q \equiv 1 \pmod 4$, $q \neq 5$, *l'ordine massimo di un arco, diverso da un'ovale e contenente* $(q+3)/2$ *punti di una conica irriducibile, è* $k = (q+7)/2$.

TEOREMA 2. *Se* $q > 9$ *e* $q \equiv 1 \pmod 4$, *fissata una conica irriducibile* $\mathscr{C}$ *in* $S_{2,q}$, *esiste almeno una* λ*-partizione di* $\mathscr{C}$ *tale che l'arco* $\mathscr{C}_\lambda$ *risulta completo e quindi di ordine* $(q+5)/2$.

2. Cominciamo col rilevare alcune proprietà elementari dell'arco $\mathscr{C}_\lambda$ definito nel n. 1. Per brevità, con l'espressione « punti U, V » intenderemo punti appartenenti all'insieme U, V rispettivamente.

2.1) Un punto P di $S_{2,q}$, che sia interno a $\mathscr{C}$, appartiene a una corda di $\mathscr{C}_\lambda$.

Dimostrazione. Dal punto P escono $\frac{1}{2}(q+1)$ secanti di $\mathscr{C}$. Poiché $|V| = \frac{1}{2}(q-1)$, esiste almeno una secante, s, di $\mathscr{C}$ passante per P e contenente due punti U; ma allora s è anche secante di $\mathscr{C}_\lambda$.

2.2) Un punto P, che appartenga a una delle tangenti a $\mathscr{C}$ uscenti da O, appartiene a una secante di $\mathscr{C}_\lambda$.

2.3) Un punto P, che appartenga a una secante di $\mathscr{C}$ uscente da O, appartiene a una secante di $\mathscr{C}_\lambda$.

Dimostrazione. Per la (1.5), la retta OP interseca $\mathscr{C}$ in due punti P_i $(i = 1, 2)$ uno solo dei quali (ad esempio P_1) appartiene a $\mathscr{C}_\lambda$. Allora P appartiene alla corda OP_1 di $\mathscr{C}_\lambda$.

2.4) Sia P un punto esterno a $\mathscr{C}$; se la polare p di P (rispetto a $\mathscr{C}$) contiene un punto V, per P passa (almeno) una secante di $\mathscr{C}_\lambda$.

Dimostrazione. Nell'ipotesi ammessa, per il punto P passano $\frac{1}{2}(q-1)$ secanti di $\mathscr{C}$ sopra le quali sono distribuiti non più di $\frac{1}{2}(q-3)$ punti V. Valgono allora le considerazioni di 2.1).

Supponiamo ora che $\mathscr{C}_\lambda$ sia incompleto; è possibile allora associare a $\mathscr{C}_\lambda$ almeno un altro punto P del piano in modo che l'insieme $\{\mathscr{C}_\lambda \cup P\}$ sia ancora un arco. Per le proprietà 2.1), 2.2), 2.3), 2.4), un tale punto P – che diremo compatibile con $\mathscr{C}_\lambda$ – soddisfa le seguenti proprietà:

i) è esterno a $\mathscr{C}$ e appartiene a una retta esterna a $\mathscr{C}$ uscente da O;

ii) la polare p di P contiene due (distinti) punti di U;

iii) detti $U_i\,(i = 1, 2)$ i punti $p \cap \mathscr{C}$, su ciascuna delle $\frac{1}{2}(q-1)$ secanti di $\mathscr{C}$ uscenti da P si trovano un punto U' (distinto dagli U_i) e un punto V. In altri termini, l'involuzione σ su $\mathscr{C}$, avente polo in P, lascia fermi i punti U_i $(i = 1, 2)$ e porta l'insieme $\{U' \setminus \{U_i\}\}$ sull'insieme V.

Le condizioni *i*), *ii*), *iii*) sono necessarie e sufficienti affinché il punto P sia compatibile con $\mathscr{C}_\lambda$.

Denoti $\mathscr{P}$ l'insieme, di potenza $(q-1)^2/4$, dei punti P di $S_{2,q}$ che soddisfano la condizione *i*). Dalle proprietà 1.2), $\cdots$, 1.6) di $\mathscr{C}$, segue che le coordinate (α, β, γ) di ogni punto $P \in \mathscr{P}$ soddisfano le seguenti condizioni:

$$(2.1) \qquad \alpha \neq 0 \quad ; \quad \beta \neq 0 \qquad \gamma \neq 0 \quad ; \quad \beta \pm i\alpha \neq 0 \,;$$

$$(2.2) \qquad f(P) = \alpha^2 + \beta^2 + \gamma^2 \sim 1$$

(2.3) posto $\beta = m\alpha$ $(m \neq 0, \infty, \pm i)$, risulta $\alpha^2 + \beta^2 = \alpha^2(m^2 + 1) \sim 1$.

Se sono soddisfatte queste condizioni, l'involuzione σ su $\mathscr{C}$, avente per polo $P(\alpha, \beta, \gamma)$, è rappresentata dall'equazione

$$(2.4) \qquad w = \frac{\gamma v - (i\alpha + \beta)}{(i\alpha - \beta)v - \gamma} = \frac{v - \dfrac{\gamma}{\alpha(i-m)}\,\dfrac{i+m}{i-m}}{v - \dfrac{\gamma}{\alpha(i-m)}}$$

ed è caratterizzata dalle seguenti proprietà:

σ_1) i coefficienti che compaiono nel secondo membro della (2.4) sono tutti diversi da zero;

σ_2) fissata una determinazione di $\sqrt{f(P)}$, i punti uniti di σ (punti comuni a $\mathscr{C}$ e alla polare p di P) hanno in K coordinate (parametriche)

$$v_1 = \frac{\gamma + \sqrt{f(P)}}{i\alpha - \beta} \quad , \quad v_2 = \frac{\gamma - \sqrt{f(P)}}{i\alpha - \beta} \quad .$$

σ_3) gli elementi v_1 e v_2 di K hanno opposto carattere quadratico dato che risulta $v_1 v_2 = -(i+m)/(i-m) \sim 1$.

Si nota ancora che il prodotto $v_1 v_2$ dipende soltanto dal parametro m della retta $l = OP$, ma non dal punto $P \in \mathscr{P}$ variabile su l. Poiché $(i+m)/(i-m)$ può assumere in K $\frac{1}{2}(q-1)$ valori distinti, indicheremo con m_r $(r = 1, 2, \cdots, \frac{1}{2}(q-1))$ i parametri delle rette l_r passanti per O ed esterne a $\mathscr{C}$; conseguentemente porremo

$$(2.5) \qquad \pi_r = (i + m_r)/(i - m_r) \; (r = 1, 2, \cdots, \tfrac{1}{2}(q-1) \; ; \; \pi_r \neq 0, \infty) \,.$$

Inoltre, per ogni intero r, cioè per ogni retta l_r passante per O ed esterna a $\mathscr{C}$, denoteremo con $P_n^{(r)} = (\alpha_n^{(r)}, \beta_n^{(r)}, \gamma_n^{(r)})$ i $(q-1)/2$ punti $P \in \mathscr{P}$ appartenenti alla retta l_r $(n = 1, 2, \cdots, \frac{1}{2}(q-1))$ e porremo

$$(2.6) \qquad \xi_n^{(r)} = \frac{\gamma_n^{(r)}}{i\alpha_n^{(r)} - \beta_n^{(r)}} = \frac{\gamma_n^{(r)}}{\alpha_n^{(r)}(1 - m_r)} \qquad (\xi_r^{(n)} \neq 0, \infty) \,.$$

Dopo di che l'equazione (2.4) di σ – che denoteremo anche con $\sigma_{r,n}$ per evidenziare che è associata al punto $P_n^{(r)} \in \mathscr{P}$ – diventa

$$w = \frac{\xi_n^{(r)} v - \pi_r}{v - \xi_n^{(r)}} . \tag{2.7}$$

σ_4) Il modulo di $\sigma_{r,n}$, riguardata come sostituzione lineare su K, è un quadrato.

σ_5) Diciamo Σ l'insieme delle involuzioni $\sigma_{r,n}$ su $\mathscr{C}$. Gli insiemi Σ e $\mathscr{P}$ risultano biunivocamente riferiti, corrispondendo a ogni $\sigma_{r,n}$ il punto $P_n^{(r)} \in \mathscr{P}$ avente coordinate $(\alpha_n^{(r)}, \beta_n^{(r)}, \gamma_n^{(r)})$ che si deducono dalle (2.5), (2.6), (2.7); e viceversa.

Dalla discussione fatta segue che il problema di stabilire se il punto $P_n^{(r)}$ di $\mathscr{P}$ sia o no compatibile con $\mathscr{C}_\lambda$ (incompleta) è spostato in quello di stabilire se l'involuzione $\sigma_{r,n}$, associata a $P_n^{(r)}$, soddisfa le condizioni *ii*) e *iii*).

3. Le proprietà che ci interessano della $\sigma_{r,n}$ possono essere agevolmente dedotte considerando in K la sostituzione lineare $\omega = \omega_{r,n}$ di equazione [1]

$$\omega = \frac{\xi_n u + \pi_r}{u + \xi_n} \qquad (n, r = 1, 2, \cdots, \tfrac{1}{2} q - 1)) \tag{3.1}$$

associata biunivocamente al punto $P_n^{(r)} \in \mathscr{P}$ mediante il prodotto operatorio

$$\omega = \sigma_{r,n} \cdot \tau \tag{3.2}$$

essendo $\sigma_{r,n}$ e τ definite dalle (2.7) e (1.5).

Si rilevano subito le seguenti proprietà della ω.

ω_1) I coefficienti della ω sono diversi da zero e da ∞ (cioè nella (3.1) non figurano mai né la sostituzione $uw = \pi_r$ né l'identità); inoltre il modulo della ω è un quadrato. Tali proprietà derivano direttamente da quelle di $\sigma_{r,n}$.

ω_2) ω non lascia fermo nessun elemento dell'insieme $\overline{K} = \{K \cup \infty\}$ (cfr. 2.5).

ω_3) Se alle (3.1) si aggiunge la sostituzione identica (cioè si ammette per ξ_n anche il valore ∞) le $(q-1)/2$ sostituzioni (3.1) che si ottengono al variare di $P_n^{(r)}$ sulla retta l_r, formano, insieme con l'identità, un gruppo commutativo G_r di ordine $(q+1)/2$.

(1) Per semplificare le notazioni, scriveremo ξ_n in luogo di $\xi_n^{(r)}$.

Dimostrazione. Il prodotto $\omega_{r,n_1}\cdot\omega_{r,n_2}$ dà luogo alla sostituzione [2]

$$w = \frac{\xi_n u + \pi_r}{u + \xi_n} \qquad \text{con} \quad \xi_n = \frac{\xi_{n_1}\xi_{n_2} + \pi_r}{\xi_{n_1} + \xi_{n_2}}$$

il cui modulo è un quadrato e che è ancora del tipo (3.1). Pertanto, tenuto conto di σ_5), $\omega_{r,n_1}\cdot\omega_{r,n_2}$ è la sostituzione lineare associata al punto $P \in l_r$ (eventualmente coincidente con O) di coordinate $(\alpha\,,\, m\alpha\,,\, \gamma)$ con

$$\frac{\alpha}{\gamma} = \frac{\xi_{n_1} + \xi_{n_2}}{(i - m)(\xi_{n_1}\xi_{n_2} + \pi_r)}$$

Ciò prova che le sostituzioni $\omega_{r,n}$ (r fisso) formano un gruppo G_r di ordine $\frac{1}{2}(q+1)$, ovviamente abeliano.

Dimostriamo ora la seguente proposizione:

ω_4) Il gruppo G_r è ciclico.

Dimostrazione. Consideriamo la (3.1) immersa nel campo $K' = GF(q^2)$, di cui sia ε una radice primitiva. Ogni elemento non nullo del sottocampo K di K' è del tipo $z' = \varepsilon^{h(q+1)}$ con $h = 1\,,\, 2\,,\cdots,\,(q-1)$; in particolare si ha

$$\pi_r = \varepsilon^{(2r-1)(q+1)} \quad , \qquad (r = 1\,,\, 2\,,\cdots,\, \tfrac{1}{2}(q-1)) \tag{3.2}$$

(in questo caso h non può essere pari, diversamente π_r risulta un quadrato in K, contro la (2.5)).

D'altra parte, poiché $\varepsilon^{\frac{1}{2}(q^2-1)} = 1$, π_r risulta un quadrato in K'; onde ponendo

$$\sqrt{\pi_r} = \varepsilon^{(2r-1)\frac{1}{2}(q+1)}\,, \tag{3.3}$$

si deduce

$$(\sqrt{\pi_r})^q = -\sqrt{\pi_r}\,. \tag{3.4}$$

Ciò premesso, fissato $\xi_n = \xi \in K$, esiste in K' uno ed un sol elemento $j_n = j$ tale che

$$\sqrt{\pi_r}\,\frac{1+j}{1-j} = \xi\,, \tag{3.5}$$

avendosi

$$j = \frac{\xi - \sqrt{\pi_r}}{\xi + \sqrt{\pi_r}} \tag{3.6}$$

con $0 \neq j \notin K$, dato che $\xi \in K$, $\sqrt{\pi_r} \notin K$.

(2) Si noti che è certamente $\xi_{n_1}\xi_{n_2} + \pi_r \neq 0$. In caso contrario ω_{r,n_2} proverrebbe, per la (3.1) dalla involuzione $\bar{\sigma}_{n,r_2}$ di equazione

$$w = \frac{(-\pi_r/\xi_{n_1})\,u - \pi_r}{u + (\pi_r/\xi_{n_1})}$$

il cui modulo è $\pi_r(-\pi_r + \xi_{n_1}^2)/\xi_{n_1}^2 \sim 1$. Ma allora $\bar{\sigma}_{r,n_2}$ non appartiene all'insieme delle involuzioni da noi prese in esame (cfr. σ_4).

Per la (3.5), l'equazione (3.1) di $\omega_{r,n} = \omega_r$ si trasforma in

$$\frac{w - \sqrt{\pi_r}}{w + \sqrt{\pi_r}} = j \frac{u - \sqrt{\pi_r}}{u + \sqrt{\pi_r}} . \tag{3.7}$$

Con ragionamento del tutto analogo, l'equazione di una sostituzione ω'_r, diversa dalla ω_r ora considerata, si otterrà dalla (3.7) sostituendo j con un opportuno j'. Si controlla poi facilmente che il prodotto operatorio $\omega_r \cdot \omega'_r$ è rappresentato dall'equazione

$$\frac{w - \sqrt{\pi_r}}{w + \sqrt{\pi_r}} = jj' \frac{u - \sqrt{\pi_r}}{u + \sqrt{\pi_r}} .$$

Da ciò si deduce, in particolare, che per ogni intero k la potenza ω_r^k si ottiene dalla (3.7) sostituendo j con j^k. Possiamo allora assumere j come generatore del gruppo ciclico $\overline{G}_r$, generato dalle potenze di ω e contenuto in G_r. Precisiamo ora l'espressione di j.

A tale scopo osserviamo che essendo q una potenza della caratteristica p di K', dalle (3.6) e (3.4) si deduce $j^q = j^{-1}$; quindi, essendo $q + 1$ un intero pari, $j^{\frac{1}{2}(q+1)} = \pm 1$. Inoltre, essendo pari anche $q - 1$, si ha che $j \in K'$ è un quadrato, onde è lecito porre

$$z = \sqrt{j} = \sqrt{\frac{\xi - \pi_r}{\xi + \pi_r}} .$$

Dimostriamo ora che è $j^{\frac{1}{2}(q+1)} = 1$. Infatti, se $j^{\frac{1}{2}(q+1)} = -1$, si ha $z^{q+1} = -1$; ma per (3.4) si ha anche $z^q = z^{-1}$, onde risulta $z = j = 0$, contro la (3.6). Ne segue senz'altro l'asserto e quindi $j = \varepsilon^{2h(q-1)}$ con h intero non multiplo di $(q + 1)/2$ (diversamente $j \in K$).

Dalla discussione svolta segue che ogni sottogruppo di G_r è generato da una potenza di $\varepsilon^{2(q-1)}$ con ε radice primitiva di K'.

Siccome l'ordine di G_r è $(q + 1)/2$, per le proprietà dei gruppi abeliani, si conclude che G_r è ciclico, generato da $\varepsilon^{2h(q-1)}$ con h primo con $\frac{1}{2}(q + 1)$.

Senza alterare le generalità, si può supporre che $j = \varepsilon^{2(q-1)}$ sia generatore di G_r.

ω_5) Dai risultati precedenti segue che nelle (3.1) esiste un $\xi_1 = \xi$ tale che $j_1 = j = \varepsilon^{2(q-1)}$ e la corrispondente sostituzione $\omega_{r,1} = \omega_r$ è generatrice del gruppo G_r. Scriveremo pertanto $\omega_{r,n} = \omega_r^n$; dopo di che le sostituzioni (3.1), non identiche, risultano rappresentate dall'equazione

$$w = \frac{\sqrt{\pi_r} g_n u + \pi_r}{u + \sqrt{\pi_r} g_n} , \tag{3.8}$$

essendo

$$g_n = \frac{1 + j^n}{1 - j^n} \tag{3.9}$$

$$(j = \varepsilon^{2(q-1)} ; r , n = 1 , 2 , \cdots , \tfrac{1}{2}(q - 1)) .$$

ω_6) Il gruppo G_r, avendo ordine $\frac{1}{2}(q+1)$ e spostando tutti i $q+1$ elementi di $\overline{K}$, opera su $\overline{K}$ secondo due orbite $\Omega_r^{(1)}$ e $\Omega_r^{(2)}$, ciascuna contenente $\frac{1}{2}(q+1)$ elementi di $\overline{K}$.

Dalla (3.8) si ha $\omega_r^n(\infty) \neq 0$, $\omega_r^n(0) \neq \infty$ per ogni r, n; ciò indica che gli elementi 0 e ∞ non appartengono mai a una stessa orbita $\Omega_r^{(i)}$ $(i = 1, 2)$. Pertanto, posto $g_{-n} = g_n^{-1}$, tenuto conto della (1.1) e del fatto che per $s = 0, 1, \cdots, t-1$ risulta $g_{t+s+1} = -g_{t-s}$; $g_{-(t+s+1)} = -g_{-(t-s)}$, risultano determinate le orbite secondo le quali opera G_r, avendosi precisamente

$$\begin{aligned} \Omega_r^{(1)} &= \{\infty, \sqrt{\pi_r}\, g_1, \cdots, \sqrt{\pi_r}\, g_t, -\sqrt{\pi_r}\, g_t, \cdots, -\sqrt{\pi_r}\, g_1\} \\ \Omega_r^{(2)} &= \{0, \sqrt{\pi_r}\, g_{-1}, \cdots, \sqrt{\pi_r}\, g_{-t}, -\sqrt{\pi_r}\, g_{-t}, \cdots, -\sqrt{\pi_r}\, g_{-1}\}. \end{aligned} \tag{3.10}$$

Gli elementi di $\Omega_r^{(1)}$ e $\Omega_r^{(2)}$ siano denotati ordinatamente con i simboli

$$\begin{aligned} &\theta_0, \theta_1, \cdots, \theta t, \theta_{t+1}, \cdots, \theta_{2t} \\ &\eta_0, \eta_1, \cdots, \eta t, \eta_{t+1}, \cdots, \eta_{2t}. \end{aligned} \tag{3.11}$$

Valgono allora le seguenti proprietà.

ω_7) Prendendo gli indici modulo $2t+1$ e per $i \not\equiv 0$ si ha

$$\theta_i + \theta_{-i} = 0 \;;\; \eta_i + \eta_{-i} = 0 \;;\; \theta_i \eta_i = \pi_r \quad (\theta_0 = -\theta_0 \;;\; \eta_0 = -\eta_0). \tag{3.12}$$

ω_8) Se $(n, 2t+1) = 1$, la sostituzione ω_r^n consta di due cicli di ordine $2t+1$. Si ha cioè $\omega_r^n = \Theta \cdot H$ con

$$\Theta = \{\theta_0, \theta_n, \theta_{2n}, \cdots, \theta_{2tn}\} \;;\; H = \{\eta_0, \eta_n, \eta_{2n}, \cdots, \eta_{2tn}\}, \tag{3.13}$$

gli indici essendo presi modulo $2t+1 = \frac{1}{2}(q+1)$.

Se invece $(n, 2t+1) = \delta \neq 1$, posto $n = \nu\delta$, $2t+1 = \chi\delta$, ω_r^n risulta composta dal prodotto di 2δ cicli di ordine χ; si ha cioè $\omega_r^n = \omega_r^{\nu\delta} = \prod_{k=0}^{\delta-1} \Theta_k H_k$ con

$$\begin{aligned} \Theta_k &= \{\theta_k, \theta_{k+\nu\delta}, \cdots, \theta_{k+(\chi-1)\nu\delta}\} \\ H_k &= \{\eta_k, \eta_{k+\nu\delta}, \cdots, \eta_{k+(\chi-1)\nu\delta}\} \end{aligned} \qquad (k = 0, 1, \cdots, \delta-1) \tag{3.14}$$

gli indici essendo presi modulo $2t+1$.

ω_9) Sempre prendendo gli indici modulo $2t+1$, gli elementi, con indice non nullo, dei cicli Θ ed H sono due a due opposti, avendosi

$$\theta_{in} + \theta_{-in} = 0 \;;\; \eta_{in} + \eta_{-in} = 0 \qquad (i = 1, 2, \cdots, t). \tag{3.15}$$

Analogamente, gli elementi con indice non nullo, dei cicli Θ_0 ed H_0 sono due a due opposti, avendosi

$$\theta_{s\nu\delta} + \theta_{-s\nu\delta} = 0 \;;\; \eta_{s\nu\delta} + \eta_{-s\nu\delta} = 0 \qquad (s = 1, 2, \cdots, \tfrac{1}{2}(\chi-1)) \tag{3.16}$$

Invece, per $k \neq 0$, l'opposto dell'elemento $\theta_{k+s\nu\delta}$ di Θ_k appartiene al ciclo $\Theta_{\nu\delta-k}$ (analogamente per gli elementi di H_k), avendosi

$$\begin{aligned} &\theta_{k+s\nu\delta} + \theta_{\nu\delta-k-(s+1)\nu\delta} = 0 && (s = 0, 1, \cdots, \chi - 1; \\ &\eta_{k+s\nu\delta} + \eta_{\nu\delta-k-(s+1)\nu\delta} = 0 && k = 1, 2, \cdots, \delta - 1). \end{aligned} \tag{3.17}$$

ω_{10}) Tenuto conto che prendendo gli indici modulo $2t+1$ risulta

$$\begin{aligned} &g_{(s+1)n} = \frac{g_{sn} g_n + 1}{g_{sn} + g_n}, \quad \text{si ha} \\ &\omega_r^n(\theta_{in}) = \theta_{(i+1)n} \quad ; \\ &\omega_r^n(\eta_{in}) = \eta_{(i+1)n} && (n, 2t+1) = 1 \\ &\omega_r^{\nu\delta}(\theta_{k+s\nu\delta}) = \theta_{k+(s+1)\nu\delta} \\ &\omega_r^{\nu\delta}(\eta_{k+s\nu\delta}) = \eta_{k+(s+1)\nu\delta} && (n, 2t+1) = \delta \neq 1. \end{aligned} \tag{3.18}$$

4. Consideriamo ora l'involuzione $\sigma_{r,n}$ su $\mathscr{C}$, a coefficienti in K, definita dalla (2.7). Per la (1.5) e per i risultati del n. 3, essa può scriversi sotto la forma

$$w = \frac{\sqrt{\pi_r}\, g_n\, u - \pi_r}{u - \sqrt{\pi_r}\, g_n} \qquad (r, n = 1, 2, \cdots, 2t). \tag{4.1}$$

Si ha allora:

4.1) I punti uniti della (4.1), tenuto conto che $\sqrt{j^n} = (-1)^{nj-t_n}$ sono dati da

$$u' = -\theta_{tn} \quad ; \quad u'' = -\eta_{tn} \quad (n \text{ pari}) \tag{4.2'}$$

$$u' = -\eta_{tn} \quad ; \quad u'' = -\theta_{tn} \quad (n \text{ dispari}) \tag{4.2''}$$

gli indici essendo presi, come al solito, modulo $2t+1$. Pertanto i punti u' e u'' di $\mathscr{C}$ appartengono, per ogni n, l'uno a $\Omega_r^{(1)}$, l'altro a $\Omega_r^{(2)}$. In particolare, se $(n, 2t+1) = \delta \neq 1$ – quindi $n = \nu\delta$; $2t+1 = \chi\delta$; χ, δ entrambi dispari – posto $\delta = 2\delta' + 1$, si ha $tn = \frac{1}{2}(\chi - 1)\delta\nu = [\delta'\chi + \frac{1}{2}(\chi - 1)]\delta\nu \equiv \frac{1}{2}(\chi - 1)\delta\nu \pmod{2t+1}$, onde u' e u'' appartengono l'uno a Θ_0, l'altro a H_0.

La conoscenza delle orbite $\Omega_r^{(1)}$ e $\Omega_r^{(2)}$ permette di precisare in che modo $\sigma_{r,n}$ opera sugli elementi di $\overline{K}$ (ovvero sui punti di $\mathscr{C}$).

Valgono infatti le seguenti proprietà.

4.2) Se $(n, 2t+1) = 1$, tenuto conto di (3.15), dalla (4.1) si deduce (sempre prendendo gli indici modulo $2t+1$)

$$\begin{aligned} &\sigma_{r,n}(\theta_{-in}) = \sigma_{r,n}(-\theta_{in}) = \omega_r^n(\theta_{in}) = \theta_{(i+1)n} \\ &\sigma_{r,n}(\theta_{(t+1)n}) = \sigma_{r,n}(-\theta_{tn}) = -\theta_{tn} \\ &\sigma_{r,n}(\eta_{-in}) = \sigma_{r,n}(-\eta_{in}) = \omega_r^n(\eta_{in}) = \eta_{(i+1)n} \\ &\sigma_{r,n}(\eta_{(t+1)n}) = \sigma_{r,n}(-\eta_{tn}) = -\eta_{tn}. \end{aligned} \qquad (i = 0, 1, \cdots, t-1) \tag{4.2}$$

Le (4.2) indicano che $\sigma_{r,n}$ muta in sé ciascuno dei cicli Θ ed H (lasciandone fermo un elemento) e porta l'uno sull'altro i due insiemi

$$(4.3) \qquad U = \{-\theta_{in}, -\eta_{in}\} \;\; ; \;\; V = \{\theta_{(i+1)n}, \eta_{(i+1)n}\} \qquad (i = 0, 1, \cdots, t-1).$$

Ma allora i due insiemi (4.3) costituiscono una λ–partizione di $\mathscr{C}$ tale che l'involuzione $\sigma_{r,n}$ su $\mathscr{C}$, di polo $P_n^{(r)} \in \mathscr{P}$, soddisfa le condizioni *ii*) e *iii*) del n. 2. In altri termini il punto $P_n^{(r)}$ è compatibile con l'arco $\mathscr{C}_\lambda$ relativo alla partizione (4.3).

4.3) Se $(n, 2t+1) = \delta \neq 1$, sempre prendendo gli indici modulo $2t+1$, con le notazioni già introdotte, tenuto conto di (3.16), (3.17), (3.18), dalla (4.1) si deduce

$$(4.4) \quad \begin{cases} \sigma_{r,n}(\theta_{-s\nu\delta}) = \sigma_{r,n}(-\theta_{s\nu\delta}) = \omega_r^n(\theta_{s\nu\delta}) = \theta_{(s+1)\nu\delta} \\ \sigma_{r,n}(\eta_{-s\nu\delta}) = \sigma_{r,n}(-\eta_{s\nu\delta}) = \omega_r^n(\eta_{s\nu\delta}) = \eta_{(s+1)\nu\delta} \quad (s = 0, 1, \cdots, \tfrac{1}{2}(\chi-3)) \\ \sigma_{r,n}(-\theta_{\frac{1}{2}(\chi-1)\nu\delta}) = -\theta_{\frac{1}{2}(\chi-1)\nu\delta} \;\; ; \;\; \sigma_{r,n}(-\eta_{\frac{1}{2}(\chi-1)\nu\delta}) = -\eta_{\frac{1}{2}(\chi-1)\nu\delta} \end{cases}$$

$$(4.5) \quad \begin{cases} \sigma_{r,n}(\theta_{\nu\delta-k-(s+1)\nu\delta}) = \sigma_{r,n}(-\theta_{k+s\nu\delta}) = \omega_r^n(\theta_{k+s\nu\delta}) = \theta_{k+(s+1)\nu\delta} \\ \sigma_{r,n}(\eta_{\nu\delta-k-(s+1)\nu\delta}) = \sigma_{r,n}(-\eta_{k+s\nu\delta}) = \omega_r^n(\eta_{k+s\nu\delta}) = \eta_{k+(s+1)\nu\delta} \end{cases}$$
$$(k = 1, 2, \cdots, \delta-1 \;\; ; \;\; s = 0, 1, \cdots, \chi-1)$$

Dalle (4.4) e (4.5) si ha: $\sigma_{r,n}$ muta in sé gli elementi dei cicli Θ_0 e H_0 (lasciando fermo un elemento in ciascun ciclo) e porta gli elementi dei cicli Θ_k, H_k ($k \neq 0$) in quelli di $\Theta_{\nu\delta-k}$, $H_{\nu\delta-k}$ rispettivamente (e viceversa). Inoltre porta l'uno sull'altro gli insiemi

$$(4.6) \qquad U = \{-\theta_{k+s\nu\delta}, -\eta_{k+s\nu\delta}\} \;\; ; \;\; V = \{\theta_{k+(s+1)\nu\delta}, \eta_{k+(s+1)\nu\delta}\}$$
$$(k = 0, s = 0, 1, \cdots, \tfrac{1}{2}(\chi-3) \;\; ; \;\; k = 1, 2, \cdots, \delta-1,$$
$$s = 0, 1, \cdots, \chi-1).$$

Ma allora gli insiemi (4.6) costituiscono una λ–partizione di $\mathscr{C}$ tale che l'involuzione $\sigma_{r,n}$ su $\mathscr{C}$ di polo $P_n^{(r)} \in \mathscr{P}$ soddisfa le condizioni *ii*) e *iii*) del n. 2. In altri termini il punto $P_n^{(r)}$ è compatibile con l'arco $\mathscr{C}_\lambda$ relativo alla λ–partizione (4.6).

5. Indichiamo con Λ l'insieme delle λ–partizioni di $\mathscr{C}$ che si possono ottenere applicando il procedimento del n. 4. La partizione $\lambda_n^{(r)} = \{U_n^{(r)}, V_n^{(r)}\}$ di Λ sarà detta associata al punto $P_n^{(r)}$ di $\mathscr{P}$; indicheremo con $\mathscr{C}_n^{(r)}$ l'arco $\mathscr{C}_\lambda$ relativo a $\lambda_n^{(r)}$.

Sussistono le seguenti proposizioni.

LEMMA 1. *Sia* $P_n^{(r)} \in \mathscr{P}$ *e* $(n, \frac{1}{2}(q+1)) = \delta$; *al punto* $P_n^{(r)}$ *sono associate* $2^{\delta-1}$ *distinte* $\lambda_n^{(r)}$*–partizioni di* $\mathscr{C}$; *ovvero* $P_n^{(r)}$ *è compatibile con* $2^{\delta-1}$ *archi* $\mathscr{C}_n^{(r)}$.

Dimostrazione. Sia $\lambda_n^{(r)} = \{U_n^{(r)}, V_n^{(r)}\}$ una partizione di $\mathscr{C}$ associata a $P_n^{(r)}$, che quindi è compatibile con l'arco $\mathscr{C}_n^{(r)}$ per i risultati del n. 4.

Un'altra ripartizione $\lambda = \{U , V\}$ di $\mathscr{C}$ differisce dalla $\lambda_n^{(r)}$ per il fatto che qualche punto $u_s \in U_n^{(r)}$ è in V e, conseguentemente, $v_s = -u_s \in V_n^{(r)}$ è in U. Ora, se $u_s \in \Theta_0$, si ha $u_s = -\theta_{s\nu\delta}$ e, dalle (4.4), $\sigma_{r,n}(u_s) = \theta_{(s+1)\nu\delta} = v_{s+1}$.

Allora, se $u_s \in V$, il punto $P_n^{(r)}$ risulta compatibile con $\mathscr{C}_\lambda$ se e solo se $v_{s+1} \in U$; ma ciò comporta che $u_{s+1} = -\theta_{(s+1)\nu\delta}$ sia in V. Proseguendo in modo analogo, si trova che deve appartenere ad U il punto $\theta_{\nu\delta} = \sigma_{r,n}(\infty)$. Ma ciò è assurdo, perché avendosi $\infty \in U$, $P_n^{(r)}$ non può essere compatibile con $\mathscr{C}_n^{(r)}$, contro l'ipotesi. La stessa conclusione vale se $u_s \in H_0$.

Se invece $u_s \in \Theta_k$ $(k \neq 0)$, con analogo ragionamento si prova che può essere $u_s \in V$ a patto che siano in V anche tutti i punti u_s di Θ_k e $\Theta_{\nu\delta-k}$, e, conseguentemente, tutti i punti v_s di Θ_k e $\Theta_{\nu\delta-k}$ siano in U.

In altri termini si possono scambiare soltanto (tutti gli elementi de) gli insiemi $U_n^{(r)}$, $V_n^{(r)}$ appartenenti alle coppie di cicli $(\Theta_k , \Theta_{\nu\delta-k})$ $(H_k , H_{\nu\delta-k})$ $(k \neq 0)$. Poiché si hanno $\delta - 1$ coppie di tali cicli, gli scambi possibili sono $2^{\delta-1}$. Con ciò il lemma è dimostrato.

LEMMA 2. *Il punto* $P_n^{(r)} \in \mathscr{P}$ *è compatibile con l'arco* $\mathscr{C}_\lambda$, *relativo alla partizione* $\lambda = \{U , V\}$ *se e solo se* λ *è una* $\lambda_n^{(r)} = \{U_n^{(r)} , V_n^{(r)}\}$ *associata a* $P_n^{(r)}$.

Dimostrazione. Che la condizione sia sufficiente risulta dalle considerazioni precedentemente svolte. La condizione è anche necessaria. Infatti, per il Lemma 1, una partizione $\lambda = \{U , V\}$, distinta dalle $\lambda_n^{(r)}$ associate a $P_n^{(r)}$, comporta lo scambio di punti $U_n^{(r)}$ con punti $V_n^{(r)}$ nell'insieme dei punti di $\mathscr{C}$ che appartengono ai cicli Θ_0 ed H_0 (ovvero Θ ed H). Ma ciò è impossibile per il Lemma 1.

LEMMA 3. *Fissata una* $\lambda_n^{(r)}$*-partizione di* $\mathscr{C}$, *l'arco* $\mathscr{C}_n^{(r)}$ *è compatibile soltanto col punto* $P_n^{(r)}$.

Dimostrazione. Se $\mathscr{C}_n^{(r)}$ è compatibile anche con $P_m^{(s)}$, quest'ultimo punto sarebbe compatibile con gli archi $\mathscr{C}_n^{(r)}$ e $\mathscr{C}_m^{(s)}$, contro il Lemma 2.

Dai Lemmi 1., 2., 3. segue la dimostrazione del Teorema 1 precedentemente enunciato.

6. Sia $\delta < 2t + 1$ un divisore di $2t + 1 = (q + 1)/2$. I punti $P_n^{(r)} \in \mathscr{P}$, tali che $(n , 2t + 1) = \delta$, sono in numero di $\varphi\left(\frac{2t+1}{\delta}\right)$ e sono associati a $\varphi\left(\frac{2t+1}{\delta}\right) \cdot 2^{\delta-1}$ $\lambda_n^{(r)}$-partizioni di $\mathscr{C}$, essendo φ l'indicatore di Eulero. La potenza dell'insieme Λ è allora data da

$$(6.1) \qquad |\Lambda| = \frac{1}{2}(q-1)\left(\sum_{\delta|2t+1} \varphi\left(\frac{2t+1}{\delta}\right) \cdot 2^{\delta-1}\right) , \quad (\delta < 2t+1).$$

Sia $\overline{\delta}$ il più grande dei divisori di $2t + 1$ (con $\overline{\delta} < 2t + 1$); si ha $2t + 1 = \overline{\delta} \cdot h$ con $h \geq 3$ e quindi $\overline{\delta} \leq t - 1$. Inoltre, come è noto, $\sum_{\substack{\delta|2t+1 \\ \delta \neq 2t+1}} \varphi\left(\frac{2t+1}{\delta}\right) = 2t$.

Pertanto $|\Lambda| < 2t \cdot 2t \cdot 2^{t-2} = t^2 \cdot 2^t$. D'altra parte (cfr. 1.8) è $|\mathscr{R}| = 2^{2t}$. Poiché la funzione $f(t) = 2^{2t} - t^2 \cdot 2^t$ diverge positivamente, esiste un t_0 tale che per $t > t_0$ risulta $f(t) \geq 1$. Si controlla facilmente che è $t_0 = 4$ e quindi, per $q > 17$, risulta

$$|\mathscr{R}| - |\Lambda| \geq 1 . \tag{6.2}$$

Con calcolo diretto, partendo dalla (6.1), si può verificare che la (6.2) è vera anche per $q = 17$ e per $q = 13$. Pertanto se $q > 9$ esistono λ–partizioni di $\mathscr{C}$ che non appartengono a Λ; allora, per il Lemma 3, l'arco $\mathscr{C}_\lambda$, di ordine $(q + 5)/2$, relativo a una tale partizione risulta completo.

Per $q = 9$ dalla (6.1) si deduce $|\mathscr{R}| = |\Lambda|$ e quindi in $S_{2,9}$ non esistono archi completi di ordine $\frac{1}{2}(q + 5)$ contenenti $\frac{1}{2}(q + 3)$ punti di una conica.

Con ciò il Teorema 2, precedentemente enunciato, è dimostrato.

Bibliografia

[1] A. Barlotti (1965) – *Some topics in finite geometrical structures*, n. 493 of Mimeo series, Chapell Hill, N. Carolina.

[2] R. C. Bose (1947) – *Mathematical theory of the symmetrical factorial designs*, « Sankhya », 107–166.

[3] W. Burnside (1955) – *Theory of groups of finite order*, Dover publ., Toronto.

[4] G. Korchmaros (1974) – *Osservazioni sui risultati di B. Segre relativi ai k-archi contenenti k — 1 punti di un'ovale*, « Atti Acc. Naz. Lincei », *8*, 56.

[5] L. Lombardo Radice (1956) – *Sul problema dei k-archi completi in* $S_{2,q}$ « Boll. UMI », (3), *11*, 178–181.

[6] B. Segre (1948) – *Lezioni di Geometria moderna*, Zanichelli, Bologna.

[7] B. Segre (1957) – *Le Geometrie di Galois*, « Ann. Mat. pura appl. » (4), *48*, 1–97.

[8] B. Segre (1961) – *Lectures on modern Geometry*, Cremonese, Roma.

[9] B. Segre (1967) – *Introduction to Galois Geometries*, « Atti Acc. Naz. Lincei, Mem. Cl. Sc. Fis. Mat. Natur. » (5), 7, 10.

[10] B. Segre (1973) – *Proprietà elementari relative ai segmenti e alle coniche sopra un campo qualsiasi ed una congettura di Seppo Ilkka per il caso dei campi di Galois*, « Ann. Mat. pura appl. » (4), *96*, 289–337.