
BOLLETTINO UNIONE MATEMATICA ITALIANA

LUIGI ANTONIO ROSATI

Piani proiettivi desarguesiani non ciclici.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. 12
(1957), n.2, p. 230–240.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1957_3_12_2_230_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

*Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI*

<http://www.bdim.eu/>

Piani proiettivi desarguesiani non ciclici.

Nota di LUIGI ANTONIO ROSATI (a Firenze)

Sunto. *Si determinano tutti i piani proiettivi finiti desarguesiani dotati di un gruppo non ciclico di collineazioni, transitivo su tutti i loro punti, d'ordine uguale al numero dei punti del piano e si dà la condizione perchè tutte le collineazioni di tale gruppo siano omografie.*

Summary. *All the projective finite desarguesian planes having a non cyclic group of collineations, transitive on all their points, with order is equal to the number of the points of the plane, are determined. It is also given the condition in order that all the collineations of such a group are projective.*

J. SINGER [4] ha dimostrato che ogni piano proiettivo finito irriducibile desarguesiano può riguardarsi come un piano ciclico perchè ammette un gruppo ciclico di collineazioni, transitivo su tutti i punti, di ordine uguale al numero dei punti del piano.

Facendo seguito a un lavoro analogo sui piani affini in corso di pubblicazione [3], in questa nota si determinano tutti i piani proiettivi desarguesiani irriducibili transitivi regolari non ciclici, cioè tutti i piani finiti proiettivi desarguesiani irriducibili dotati, oltre che del suddetto gruppo ciclico di collineazioni, di un gruppo non ciclico di collineazioni, E , di ordine uguale al numero dei punti del piano, transitivo su tutti i punti del piano stesso. Esempi di tali piani sono stati dati da G. ZAPPA [6] e da R. H. BRUCK [1].

Risulta da questa nota che per ogni piano proiettivo desarguesiano irriducibile transitivo regolare non ciclico di rango n esiste un pseudocorpo del DICKSON di ordine n^3 e quindi un piano proiettivo (non desarguesiano) di rango n^3 sopra tale pseudocorpo. Viceversa sono date le condizioni perchè ad un pseudocorpo del DICKSON di ordine n^3 corrisponda un piano proiettivo desarguesiano irriducibile transitivo regolare non ciclico.

Si determina infine la condizione perchè le collineazioni del suddetto gruppo non ciclico E siano omografie.

1. Vogliamo provare che

TEOREMA 1. *Ad ogni piano proiettivo π desarguesiano irriducibile transitivo regolare non ciclico di rango $n = p^t$ (p primo) corrisponde uno pseudocorpo del DICKSON ⁽¹⁾, K , di ordine n^3 e quindi un piano proiettivo di rango n^3 sopra tale pseudocorpo.*

Sia π un piano desarguesiano irriducibile di rango $n = p^t$ che ammetta un gruppo E regolare non ciclico, di ordine $n^2 + n + 1$, di collineazioni, transitivo sui suoi punti e siano (x_1, x_2, x_3) , (x'_1, x'_2, x'_3) le coordinate omogenee di due punti di π che si corrispondano in una collineazione ⁽²⁾ di π in sè. Si ha [5]

$$(1) \quad \rho x'_i = \sum_{k=1}^{1\dots 3} a_{ik} x_k^{\rho}, \quad i = 1, 2, 3,$$

dove i coefficienti a_{ik} e $\rho \neq 0$ appartengono a un campo di GALOIS di ordine n , $GF(n)$, e r è uno qualsiasi dei numeri $0, 1, \dots, t - 1$. Queste collineazioni costituiscono un gruppo, L , di ordine $t(n^2 + n + 1)(n + 1)(n - 1)^2 n^3$. Insieme ad esso consideriamo il gruppo, H , d'ordine $t(n^3 - 1)(n + 1)(n - 1)n^3$ delle trasformazioni

$$(2) \quad x'_i = \sum_{k=1}^{1\dots 3} a_{ik} x_k^{\rho}, \quad i = 1, 2, 3.$$

La corrispondenza, φ , che associa alla trasformazione (2) di H la collineazione (1) di L che ha gli stessi coefficienti a_{ik} è un omomorfismo di H su L e ogni collineazione di L proviene da $n - 1$ tra-

⁽¹⁾ Diciamo pseudocorpo del DICKSON un sistema, K , con doppia composizione definito dalle seguenti proprietà:

- 1) gli elementi di K , rispetto all'addizione, formano un gruppo abeliano;
- 2) gli elementi non nulli di K formano, rispetto alla moltiplicazione, un gruppo; inoltre, qualunque sia a in K , $a \cdot 0 = 0 \cdot a = 0$;
- 3) qualunque siano a, b, c in K , si ha $a(b + c) = ab + ac$.

Ordine di uno pseudocorpo finito è il numero dei suoi elementi. Gli pseudocorpi del DICKSON finiti, che non siano campi di GALOIS, coincidono con i vollständige Fastkörper considerati da H. ZASSENHAUS in [8] In questo lavoro, dicendo pseudocorpo del DICKSON, intendiamo uno pseudocorpo che non sia un campo di GALOIS.

⁽²⁾ Dati due piani lineari π e π' , chiamiamo collineazione fra essi una qualunque corrispondenza biunivoca fra i punti di π e quelli di π' che conservi gli allineamenti. Chiamiamo invece omografia una collineazione fra π e π' che conservi i birapporti.

sformazioni di H . Quindi una collineazione di π può rappresentarsi con un sistema di equazioni (1) o con $n - 1$ sistemi di equazioni (2) a coefficienti proporzionali. Per ipotesi, L deve contenere E come sottogruppo. Questo, avendo ordine $n^2 + n + 1$, è tale che l'unica collineazione di E che lasci fermo un punto di π è l'identità. Le trasformazioni di H che sono portate da φ in collineazioni in E formano un sottogruppo non ciclico di H , che chiameremo G , di ordine $n^3 - 1$, tale che l'unica trasformazione di esso che lascia ferma una terna (x_1, x_2, x_3) di tre elementi di $GF(n)$ non tutti nulli è l'identità. Se, considerate due generiche terne di elementi di $GF(n)$, $\xi \equiv (x_1, x_2, x_3)$, $\eta \equiv (y_1, y_2, y_3)$, si pone $\xi + \eta \equiv (x_1 + y_1, x_2 + y_2, x_3 + y_3)$, si ha che le terne di elementi di $GF(n)$ costituiscono rispetto a tale operazione un gruppo abeliano additivo, A , di ordine n^3 e tipo $(1, 1, \dots, 1)_{3t}$. Si vede subito che una trasformazione generica, g , di G determina su A un automorfismo. Infatti, se per effetto di g , si ha $\xi \rightarrow \xi'$, per effetto di g^{-1} si ha $\xi' \rightarrow \xi$; inoltre a causa delle (2), ricordando che in $GF(n)$ è $(x+y)^{p^r} = x^{p^r} + y^{p^r}$, se $\xi \rightarrow \xi'$ e $\eta \rightarrow \eta'$, allora $\xi + \eta \rightarrow \xi' + \eta'$. D'altra parte è noto che nel gruppo di automorfismi, F , di un gruppo abeliano elementare di ordine m esistono sottogruppi di ordine $m - 1$ non ciclici, semplicemente transitivi sugli elementi diversi dall'identità, per quei valori di m per cui esistono pseudocorpi del DICKSON di ordine m e viceversa, e F risulta isomorfo al gruppo moltiplicativo dello pseudocorpo [2, 7]. Ne risulta che a π corrisponde uno pseudocorpo del DICKSON, K , d'ordine n^3 . Risulta inoltre che il gruppo moltiplicativo di K è isomorfo a G .

TEOREMA 2. — *Sia K un generico pseudocorpo del Dickson di ordine n^3 (di tipo $K_{p^1, m}$) corrispondente a un piano proiettivo desarguesiano transitivo regolare non ciclico di rango $n = p^t$. Allora, se $GF(q)$ è il centro di K ed è $q^m = n^3$, si ha*

$$(3) \quad n^3 + n^2 + 1 \equiv 0 \quad (\text{mod } m).$$

Ricordiamo anzitutto come si può costruire, secondo H. ZASSEN-HAUS [8], un qualunque pseudocorpo del DICKSON K di ordine n^3 . Si parta da un campo di GALOIS $GF(n^3)$ di ordine n^3 . Questo, a sua volta, si può considerare ottenuto ampliando un campo di GALOIS $GF(n)$ di ordine n nel modo seguente. Sia

$$x^3 + ax^2 + bx + c = 0$$

una equazione cubica a coefficienti in $GF(n)$ ed ivi irriducibile.

Se λ è una sua radice, è noto che, al variare di x_1, x_2, x_3 in $GF(n)$, l'espressione

$$(4) \quad x_1\lambda^2 + x_2\lambda + x_3$$

fornisce tutti gli elementi di un campo di GALOIS $GF(n^3)$, contenente $GF(n)$, ciascuno una volta sola. Si vede poi che, se h è un elemento qualsiasi di $GF(n)$ e $\xi = x_1\lambda^2 + x_2\lambda + x_3$ è un elemento qualsiasi di $GF(n^3)$ si ha

$$(5) \quad h\xi = hx_1\lambda^2 + hx_2\lambda + hx_3.$$

Per costruire uno pseudocorpo del DICKSON di ordine n^3 dobbiamo ora considerare un campo di GALOIS $GF(q)$ contenuto in $GF(n^3)$, con $n^3 = q^m$, in modo che ogni fattore primo di m sia un divisore di $q - 1$ e che inoltre sia $m \equiv 0 \pmod{4}$, se $q \equiv 3 \pmod{4}$. Si fissi poi un generatore ω del gruppo moltiplicativo (ciclico) di $GF(n^3)$ e si consideri l'automorfismo ρ di $GF(n^3)$ tale che, per ogni ξ di $GF(n^3)$, si abbia

$$(6) \quad \rho(\xi) = \xi^q.$$

Sia ora α un qualunque elemento non nullo di $GF(n^3)$: esiste allora uno ed un solo intero d ($0 \leq d < n^3 - 1$) tale che $\alpha = \omega^d$. Si consideri ora la congruenza nell'incognita u

$$(7) \quad q^u \equiv 1 + d(q - 1) \pmod{(q - 1)m}.$$

Essa ammette sempre soluzioni in u : se inoltre u_1 e u_2 sono due tali soluzioni, si ha [8] $\rho^{u_1} = \rho^{u_2}$. Il numero d (e quindi l'elemento α) determina pertanto l'automorfismo

$$(8) \quad \rho_\alpha = \rho^u,$$

ove u è una qualunque soluzione della (7) corrispondente al dato valore di d . Definiamo allora, qualunque sia β in $GF(n^3)$,

$$(9) \quad \alpha \circ \beta = \alpha\rho_\alpha(\beta), \quad 0 \circ \beta = 0.$$

Uno pseudocorpo del DICKSON di ordine n^3 e tipo, secondo H. ZASSENHAUS [8], $K_{p^l, m}$, si può considerare come costituito dagli stessi elementi di $GF(n^3)$, definendo l'addizione allo stesso modo che in $GF(n^3)$ e definendo invece la moltiplicazione mediante la (9). Tenuto conto che ogni pseudocorpo del DICKSON di ordine n^3

è di tipo $K_{p^l, m}$, perchè uno pseudocorpo del DICKSON che non sia di tipo $K_{p^l, m}$ è di ordine p^2 , possiamo allora ritenere che K sia stato costruito a partire da $GF(n^3)$ nel modo anzidetto. Diremo allora che $GF(n^3)$ è il campo di GALOIS associato a K . Risulta inoltre che il centro di K è $GF(q)$ [8].

È noto che, fissato $\eta \neq 0$ in K , al variare di α in K , la corrispondenza $\alpha \rightarrow \eta \circ \alpha$ è un automorfismo, σ_η , del gruppo additivo A' di K . Di più si sa che, al variare di η fra gli elementi diversi da zero dello pseudocorpo, gli automorfismi σ_η costituiscono un gruppo, che diremo G' , isomorfo al gruppo moltiplicativo di K , di ordine $n^3 - 1$, non ciclico, semplicemente transitivo sugli elementi diversi da zero di A' [2]. Per quanto abbiamo già osservato alla fine della dimostrazione del teorema 1 G' risulta isomorfo a G .

Osserviamo ora che ogni elemento $\xi = x_1\lambda^2 + x_2\lambda + x_3$ diverso da zero di K determina univocamente un punto di π , di coordinate omogenee (x_1, x_2, x_3) ; viceversa al punto (x_1, x_2, x_3) corrispondono $n - 1$ elementi diversi da zero di K che per la (5) hanno la forma $h\xi = hx_1\lambda^2 + hx_2\lambda + hx_3$, essendo h un qualsiasi elemento non nullo di $GF(n)$. Allora, considerato l'isomorfismo fra G e G' , se un elemento di G , g , porta la terna (x_1, x_2, x_3) nella terna (x'_1, x'_2, x'_3) , il corrispondente elemento di G' porta $\xi = x_1\lambda^2 + x_2\lambda + x_3$ in $\xi' = x'_1\lambda^2 + x'_2\lambda + x'_3$. D'altra parte per le (1) (2), se g porta (x_1, x_2, x_3) in (x'_1, x'_2, x'_3) , fissato comunque h in $GF(n)$, esiste un altro elemento di G , g , che porta (x_1, x_2, x_3) in (hx'_1, hx'_2, hx'_3) . Perciò se σ_η è l'automorfismo appartenente a G' tale che $\sigma_\eta(\xi) = \eta \circ \xi = \xi'$, fissato comunque $h \neq 0$ in $GF(n)$, esiste in G' un altro automorfismo, $\sigma_{\bar{\eta}}$, tale che sia $\sigma_{\bar{\eta}}(\xi) = \bar{\eta} \circ \xi = (\eta \circ \xi)h$. Quindi, qualunque sia ξ in K , si ha che $\bar{\eta} \circ \xi = (\eta \circ \xi)h$ e perciò, posto $\xi = 1$, $\bar{\eta} = \eta h$. Allora risulta $(\eta h) \circ \xi = (\eta \circ \xi)h$, qualunque siano $\eta \neq 0$ e ξ in K e h in $GF(n)$. In particolare, posto $\eta = 1$, si vede che si ha $h \circ \xi = \xi h$, qualunque siano h in $GF(n)$ e ξ in K .

D'altra parte, posto $h = \omega^{\bar{d}}$, per le (6) (8) (9) è $h \circ \xi = h\xi q^u$ e per la (7) $q^u \equiv 1 + \bar{d}(q - 1) \pmod{(q - 1)m}$. Ora, poichè il periodo di un generatore del gruppo moltiplicativo di $GF(n^3)$ è $n^3 - 1 = q^m - 1$, si ha $q^u \equiv 1 \pmod{(q^m - 1)}$. Ma $q^m - 1 \equiv 0 \pmod{(q - 1)m}$ [8], quindi si ha $q^u \equiv 1 \pmod{(q - 1)m}$ e perciò $\bar{d} \equiv 0 \pmod{m}$.

Siccome un gruppo ciclico possiede al più un sottogruppo di un determinato ordine, il gruppo moltiplicativo di $GF(n)$ è l'unico sottogruppo ciclico di ordine $n - 1$ del gruppo moltiplicativo di $GF(n^3)$. D'altra parte ω^{n^2+n+1} genera proprio un sottogruppo ciclico di ordine $n - 1$ del gruppo moltiplicativo di $GF(n^3)$, dunque il gruppo moltiplicativo di $GF(n)$ è generato da ω^{n^2+n+1} . Siccome per

ogni elemento $\omega^{\bar{d}}$ di $GF(n)$ si ha $\bar{d} \equiv 0 \pmod{m}$, lo stesso si avrà per il generatore ω^{n^2+n+1} del gruppo moltiplicativo di $GF(n)$. Si ha dunque $n^2 + n + 1 \equiv 0 \pmod{m}$, come si voleva dimostrare.

TEOREMA 3. - Se K è un generico pseudocorpo del Dickson di ordine $n^3 = p^{3t}$, $GF(q)$ è il suo centro ed è $n^3 = q^m$, allora la (3) del teorema 2 è verificata quando e soltanto quando è soddisfatta o l'una o l'altra delle seguenti condizioni a), b):

a) $q = n$

b) m non è divisibile per 3 e posto $t = s, m$ si ha

$$q = p^{3s_1} \quad e \quad p^{2s_1m} + p^{s_1m} + 1 \equiv 0 \pmod{m}.$$

Siccome si ha $n = p^t$, $n^3 = q^m$, posto $q = p^r$, risulta $3t = sm$ e quindi $t = sm/3$. Sono perciò possibili i seguenti due casi

1) 3 divide m

2) 3 non divide m e quindi divide s .

Nel caso 1), posto $m = 3r$, si trova $n = p^{rs} = q^r$. Allora la (3) diventa

$$(10) \quad q^{rr} + q^r + 1 \equiv 0 \pmod{3r}$$

e per ipotesi tutti i fattori primi di $3r$ sono divisori di $q - 1$. Sia allora z un fattore primo di $3r$. Si ha $q \equiv 1 \pmod{z}$ e $q^{rr} + q^r + 1 \equiv 3 \pmod{z}$; quindi, per la (10), $3 \equiv 0 \pmod{z}$ e $z = 3$. Dunque $3r = 3^v$, con v intero ≥ 1 , $q^{2r} + q^r + 1 \equiv 0 \pmod{3^v}$, $q \equiv 1 \pmod{3}$. Ora, se $v \geq 2$, r è divisibile per 3; perciò si ha $q^r = (3a + 1)^r = (3a)^r + r(3a)^{r-1} + \dots + 3ar + 1 \equiv 1 \pmod{9}$ e $q^{2r} + q^r + 1 \equiv 3 \pmod{9}$. Quindi, siccome, se $v \geq 2$, 3^v è divisibile per 9, dalla (10) seguirebbe, se $v \geq 2$, $q^{2r} + q^r + 1 \equiv 0 \pmod{9}$, contrariamente a quanto ora visto. Quindi $v = 1$, $r = 1$, $m = 3$ e dunque $q = n$. Nel caso 1) K ha per centro $GF(n)$.

Viceversa, se K ha per centro $GF(n)$ cioè se è $q = n$ ed $m = 3$, siccome si ha $q^m - 1 \equiv 0 \pmod{(q - 1)m}$ [8], in questo caso risulta $n^3 - 1 \equiv 0 \pmod{3(n - 1)}$ e quindi $n^2 + n + 1 \equiv 0 \pmod{3}$, che, essendo $m = 3$, coincide con la (3).

Consideriamo il caso 2). Posto $s = 3s_1$, allora $t = s, m$, $n = p^{s_1m}$, $q = p^{3s_1}$ e quindi la (3) diventa

$$(11) \quad p^{2s_1m} + p^{s_1m} + 1 \equiv 0 \pmod{m}.$$

Il teorema è così completamente dimostrato.

TEOREMA 4. - *Esistono pseudocorpi del Dickson di ordine $n^3 = p^{3s_1 m}$ che soddisfano le condizioni b) del teorema 3.*

Si vede facilmente che esistono pseudocorpi del DICKSON di ordine $n^3 = p^{3s_1 m}$, con m intero primo diverso da 3, aventi per centro un campo di GALOIS di ordine $q = p^{3s_1}$. Per essi si ha

$$(12) \quad p^{3s_1} - 1 \equiv 0 \pmod{m}.$$

D'altra parte non può essere $p^{s_1} \equiv 1 \pmod{m}$, perchè da questa, per la (11), risulta $3 \equiv 0 \pmod{m}$, cioè $m = 3$, contrariamente al supposto. Sarà allora

$$p^{2s_1} + p^{s_1} + 1 \equiv 0 \pmod{m}.$$

Essendo m primo si ha poi

$$(p^{2s_1} + p^{s_1} + 1)^m \equiv p^{2s_1 m} + p^{s_1 m} + 1 \pmod{m},$$

cioè la (11) risulta, per m primo diverso da 3, conseguenza della (12). La (11) risulta quindi soddisfatta per ogni pseudocorpo del DICKSON di ordine $n^3 = p^{3s_1 m}$, con m intero primo diverso da 3, avente per centro un campo di GALOIS di ordine $q = p^{3s_1}$.

Un tale pseudocorpo si ha, per esempio, per $p = 2$, $s_1 = 2$, $m = 7$, $n^3 = 2^{42}$, $q = 2^6$.

2. Viceversa vogliamo provare che per ogni pseudocorpo del DICKSON di ordine n^3 per cui siano soddisfatte le condizioni a) o b) del teorema 3 esiste un piano proiettivo desarguesiano irriducibile transitivo regolare non ciclico.

Cominciamo col provare il seguente

LEMMA 5. - *Se per uno pseudocorpo del Dickson, K , di ordine n^3 sono soddisfatte le condizioni a) o b) del teorema 3, allora per ogni elemento ξ di K e per ogni elemento h di K compreso fra gli elementi del campo di Galois $GF(n)$ contenuto nel campo di Galois $GF(n^3)$ associato a K si ha*

$$h \circ \xi = h\xi.$$

Infatti, se ω è un generatore del gruppo moltiplicativo del campo di GALOIS $GF(n^3)$ associato a K , ω^{n^2+n+1} genera il gruppo moltiplicativo di un campo di GALOIS $GF(n)$ contenuto in $GF(n^3)$;

quindi, per ogni elemento $h = \omega^d$ di $GF(n)$ si ha

$$d \equiv 0 \pmod{(n^2 + n + 1)}.$$

Ma nelle nostre ipotesi vale la (3), perciò si ha $d \equiv 0 \pmod{m}$ e $d(q-1) \equiv 0 \pmod{(q-1)m}$; di conseguenza, in tal caso, tra le soluzioni della (7) figura $u=0$. Pertanto, per la (8), ρ_a è l'automorfismo identico, onde per la (9) è $h \circ \xi = h\xi$, come si voleva dimostrare.

LEMMA 6. - *Fissati tre elementi $\eta \neq 0$, α , β , di K si possono determinare due corrispondenze biunivoche φ e ψ di $GF(n)$ su di sé tali che, per h e k in $GF(n)$ (e in K), si abbia*

$$(13) \quad \eta \circ (\alpha h + \beta k) = (\eta \circ \alpha)\varphi(h) + (\eta \circ \beta)\psi(k).$$

Siano α e β due elementi di K che basterà supporre diversi da zero; allora ρ_α e ρ_β mutano ciascuno ogni elemento di K in una sua potenza, e quindi se h e k sono elementi di $GF(n)$, anche $\rho_\alpha(h)$ e $\rho_\beta(k)$ lo sono. Quindi, se η è un elemento diverso da zero di K

$$\begin{aligned} \eta \circ (\alpha h + \beta k) &= \eta \circ (\alpha h) + \eta \circ (\beta k) = \eta \circ [\alpha(\rho_\alpha^{-1}(h))] + \\ &+ \eta \circ [\beta(\rho_\beta^{-1}(k))] = \eta \circ [\alpha \circ (\rho_\alpha^{-1}(h))] + \eta \circ [\beta \circ (\rho_\beta^{-1}(k))] = \\ &= (\eta \circ \alpha)\rho_{\eta \circ \alpha}[\rho_\alpha^{-1}(h)] + (\eta \circ \beta)\rho_{\eta \circ \beta}[\rho_\beta^{-1}(k)]. \end{aligned}$$

Posto $\varphi = \rho_\alpha^{-1}\rho_{\eta \circ \alpha}$ e $\psi = \rho_\beta^{-1}\rho_{\eta \circ \beta}$, si ha che $\eta \circ (\alpha h + \beta k) = (\eta \circ \alpha)\varphi(h) + (\eta \circ \beta)\psi(k)$, con φ e ψ automorfismi di $GF(n)$, cioè la (13).

TEOREMA 7. - *Per ogni pseudocorpo del Dickson, K , di ordine n^3 , soddisfacente le condizioni a) o b) del teorema 3, esiste un piano proiettivo desarguesiano irriducibile transitivo regolare non ciclico.*

K si può considerare costruito, secondo il procedimento del n. 1, a partire da un campo di GALOIS $GF(n^3)$ e quindi ogni suo elemento si può rappresentare in modo unico nella forma $x_1\lambda^2 + x_2\lambda + x_3$, ove x_1, x_2, x_3 sono elementi del sottocampo $GF(n)$ di $GF(n^3)$ e λ è un elemento fisso di $GF(n^3)$ non contenuto in $GF(n)$. Si consideri ora il piano proiettivo desarguesiano π su $GF(n)$ e sia r una retta di π . Indicando con (x_1, x_2, x_3) le coordinate correnti di un punto di r e con h e k due parametri variabili in $GF(n)$, mai entrambi nulli, r si potrà rappresentare con le equazioni parametriche

$$x_i = ha_i + kb_i, \quad i = 1, 2, 3,$$

essendo a_i e b_i , $i = 1, 2, 3$, elementi fissi di $GF(n)$, o anche, posto $\xi = x_1\lambda^2 + x_2\lambda + x_3$, $\alpha = a_1\lambda^2 + a_2\lambda + a_3$, $\beta = b_1\lambda^2 + b_2\lambda + b_3$, con la equazione parametrica « vettoriale »

$$\xi = h\alpha + k\beta, \quad (\xi, \alpha, \beta \text{ elementi di } K).$$

Fissato un qualsiasi elemento diverso da zero di K , η , al variare di l fra gli elementi non nulli di $GF(n)$, gli $n - 1$ automorfismi appartenenti a G' , $\sigma_{\eta l}$, definiscono la stessa collineazione di π in sè. Infatti, tenuto conto del lemma 5

$$(\eta l) \circ \xi = (l \circ \eta) \circ \xi = l \circ (\eta \circ \xi) = l(\eta \circ \xi).$$

Cioè gli $n - 1$ automorfismi considerati trasformano un elemento di K in altri $n - 1$ che definiscono lo stesso punto e quindi determinano la stessa corrispondenza di π in sè. Inoltre, siccome vale la (13), questa corrispondenza cambia rette in rette e, poichè è evidentemente biunivoca, essa è una collineazione di π in sè. Ne viene che al gruppo non ciclico G' degli automorfismi σ_{η} , d'ordine $n^3 - 1$, semplicemente transitivo sugli elementi di K diversi da zero, corrisponde un gruppo, E , non ciclico, di collineazioni di π in sè, di ordine $n^2 + n + 1$, semplicemente transitivo su tutti i punti di π . Il teorema è così dimostrato.

TEOREMA 8. — *E è transitivo anche sulle rette di π .*

Infatti, se non lo fosse, una retta r di π sarebbe portata, dalle varie collineazioni di E , solo in un numero di rette minore di $n^2 + n + 1$, e quindi vi dovrebbero essere due collineazioni a e b che portano r nella stessa retta, onde la collineazione non identica $ab^{-1} = f$ porterebbe r in sè. Ma ciò è assurdo: infatti f in tal caso permuterebbe fra loro gli $n + 1$ punti di r , e poichè nessuna collineazione non identica di E , quindi nemmeno alcuna potenza non identica di f , lascia fermo alcun punto del piano, f dovrebbe determinare una sostituzione regolare sugli $n + 1$ punti di r , onde il suo ordine dovrebbe dividere $n + 1$: e ciò non può essere perchè $n^2 + n + 1$ è primo con $n + 1$. Dall'assurdo discende quanto si voleva dimostrare.

3. Vogliamo ora determinare gli pseudocorpi del DICKSON di ordine n^3 per cui le collineazioni di E sono omografie. Cominciamo col dimostrare il seguente

LEMMA 9. — *E è un gruppo di omografie quando, e soltanto*

quando, un elemento di G' , σ_η , che porta ξ in ξ' , porta di conseguenza $h\xi$ in $h\xi'$, qualunque sia h in $GF(n)$.

Infatti la (1) rappresenta una omografia se, e soltanto se, $p^r = 1$. Se pertanto una trasformazione di G associata a una omografia porta (x_1, x_2, x_3) in (x'_1, x'_2, x'_3) , essa porta (hx_1, hx_2, hx_3) in (hx'_1, hx'_2, hx'_3) , qualunque sia h in $GF(n)$. Viceversa, se una trasformazione di equazioni (2), tutte le volte che porta (x_1, x_2, x_3) in (x'_1, x'_2, x'_3) , porta anche (hx_1, hx_2, hx_3) in (hx'_1, hx'_2, hx'_3) , deve essere come si vede facilmente, $p^r = 1$, onde la collineazione associata è una omografia. Pertanto una trasformazione $\mathfrak{S}$ determina una omografia quando e soltanto quando, comunque si prendano x_1, x_2, x_3 e h in $GF(n)$, detto (x'_1, x'_2, x'_3) il corrispondente di (x_1, x_2, x_3) nella $\mathfrak{S}$, si ha che il corrispondente di (hx_1, hx_2, hx_3) è (hx'_1, hx'_2, hx'_3) . Ricordando che il gruppo G di trasformazioni (2) è isomorfo al gruppo G' degli automorfismi σ_η , si ha quanto si voleva dimostrare.

Finalmente dimostriamo il

TEOREMA 10. — *Condizione necessaria e sufficiente perchè tutte le collineazioni di E siano omografie è che K abbia per centro un campo di Galois di ordine n .*

Supponiamo che la collineazione di E determinata dall'automorfismo $\xi \mapsto \eta \circ \xi$ del gruppo additivo A di K sia una omografia. Allora se fissato $\alpha \neq 0$ in K e h in $GF(n)$ si ha, come risulta dalle (6) (8) (9), $\alpha \circ h = \alpha h q^n$, preso un qualunque elemento $\eta \neq 0$ di K , per il lemma 9 si deve avere $\sigma_\eta(\alpha h q^n) = \sigma_\eta(\alpha) h q^n$; cioè $\eta \circ (\alpha h q^n) = (\eta \circ \alpha) h q^n$ ossia $\eta \circ \alpha \circ h = (\eta \circ \alpha) h q^n$: quindi, posto $\alpha' = \eta \circ \alpha$, si deve avere $\alpha' \circ h = \alpha' h q^n$. Siccome poi, fissati in K due elementi diversi da zero, esiste sempre un automorfismo appartenente a G' (e uno solo) che porta α in α' , risulta che se, per $\alpha \neq 0$, si ha $\alpha \circ h = \alpha h q^n$, q^n è indipendente da α (e da h), qualunque sia h in $GF(n)$. Consideriamo ora un altro elemento, k , di $GF(n)$. Si ha

$$\begin{aligned} h \circ k \circ h &= (h \circ k) \circ h = (h k q^n) \circ h = h k q^n h q^n = h q^{2n+1} k q^n; \\ h \circ k \circ h &= h \circ (k \circ h) = h \circ (k h q^n) = h k q^n h q^n = h q^{2n+1} k q^n. \end{aligned}$$

Da queste risulta $h q^n = h q^{2n}$, qualunque sia h in $GF(n)$; cioè $h q^n = h$ e $\alpha \circ h = \alpha h$.

D'altra parte si ha che $h \circ \alpha = h \alpha$, qualunque siano h in $GF(n)$ e α in K . Dunque, se tutte le collineazioni di E sono omografie, per ogni elemento h di $GF(n)$, qualunque sia α in K , si ha

$$h \circ \alpha = \alpha \circ h = \alpha h.$$

Perciò $GF(n)$ appartiene al centro di K che risulterà quindi un campo di GALOIS $GF(n^l)$ tale che sia $n^l = n^3$, con $m > 1$. Sarà allora $l = 1$ e il centro di K è proprio $GF(n)$.

Viceversa, supponiamo che K abbia per centro $GF(n)$ e sia h un elemento di $GF(n)$. Allora nella (6) è $q = n$, onde si ha $\rho(h) = h^n = h$, e pertanto, in base alla (8), la (9) fornisce $\alpha \circ h = \alpha \rho^n(h) = \alpha h$. Se η è un qualunque elemento di K diverso da zero si ha allora

$$\eta \circ (\alpha h) = \eta \circ (\alpha \circ h) = (\eta \circ \alpha) \circ h = (\eta \circ \sigma)h.$$

Ne segue che se la (1) rappresenta la collineazione data dalla trasformazione $\alpha \rightarrow \eta \circ \alpha$, posto $\xi = x_1 \lambda' + x_2 \lambda + x_3$, $\xi' = x_1' \lambda'^2 + x_2' \lambda + x_3'$, si ha allora che, da $\xi \rightarrow \eta \circ \xi = \xi'$, si deduce $h \xi \rightarrow (\eta \circ \xi)h = h \xi'$. Tenuto conto del lemma 9, risulta così che E è un gruppo di omografie. Il teorema è dunque completamente dimostrato.

4. In definitiva possiamo riassumere i risultati del lavoro nel seguente

TEOREMA 11. - Vi è una corrispondenza biunivoca fra i piani proiettivi desarguesiani irriducibili di rango n , dotati di un gruppo E non ciclico di collineazioni, di ordine $n^2 + n + 1$, transitivo su tutti i punti del piano e gli pseudocorpi del Dickson di ordine n^3 che soddisfano una delle condizioni a), b) del teorema 3. Inoltre tutte le collineazioni di E sono omografie se, e soltanto se, lo pseudocorpo relativo ha per centro un campo di Galois di ordine n .

BIBLIOGRAFIA

- [1] R. H. BRUCK, *Difference sets in a finite group*, « Trans. Amer. Math. Soc. », 78 (1955), pp. 463-481.
- [2] L. LOMBARDO-RADICE, *Piani grafici finiti a coordinate di Veblen-Wedderburn*, « Ricerche di Matematica », 2, 1953, pp. 266-273.
- [3] L. A. ROSATI, *Piani desarguesiani affini « non-ciclici »*, « Rend. Acc. Naz. Lincei », s. VIII, vol. XXII, fasc. 4 (1957).
- [4] J. SINGER, *A theorem in finite projective geometry and some applications to number theory*, « Trans. Amer. Math. Soc. », 43 (1938), pp. 377-385.
- [5] O. VEBLEN e V. H. BUSSEY, *Finite projective geometries*, « Trans. Amer. Math. Soc. », 7 (1906), pp. 241-259.
- [6] G. ZAPPA, *Sui piani grafici finiti transitivi e quasi transitivi*, « Ricerche di Matematica », 2, (1953), pp. 274-287.
- [7] G. ZAPPA, *Sui piani grafici finiti h-l-transitivi*, « Boll. U. M. I. », s. III, a. IX, n. 1, pp. 16-24.
- [8] H. ZASSENHAUS, *Über endliche Fastkörper*, « Abhandlungen aus dem Mathem. Seminar der Hamburg. Univ. », 11 (1935), pp. 187-220.