GABRIELE KORCHMÁROS (*)

Su una classificazione delle ovali dotate di automorfismi (**)

SUMMARY. — Following F. Buekenhout [2], the incidence structure $\pi(\mathscr{B})$ of an oval $\mathscr{B}$ is regular if every involution is an automorphism of B. Buekenhout has proved that a regular $\pi(\mathscr{B})$, whose order is even or an odd prime, is a conic. Here the last result is extended to every odd order, with the possibility of a few exceptions.

La presente Memoria, con l'esclusione di alcuni casi particolari, rende completa la classificazione delle ovali dotate di automorfismi data da F. Buekenhout ([1], [2], [9]) (***).

Conviene notare, rinviando agli stessi lavori o all'introduzione che segue, come la nozione di «ovale» e più precisamente di «ovale libera», sia il portato di una sintesi di quella di «ovale proiettiva», ben nota nelle geometrie di Galois il cui studio è stato ampiamente svolto e generalizzato da B. Segre e dai suoi discepoli [9].

INTRODUZIONE

Ricordiamo che – con J. Tits – chiamasi *ovale proiettiva* un insieme K di punti a tre a tre non allineati di un piano proiettivo finito se fra le rette uscenti da uno qualsivoglia dei punti di K ce n'è una sola non passante per nessuno dei rimanenti punti di K.

Si osservi che le ovali proiettive di un piano di Galois d'ordine q non sono altre che $(q+1)$-archi introdotti da B. Segre.

Un bel risultato di Buekenhout dice che, se ogni esagono inscritto in K soddisfa al teorema di Pascal, allora nel piano vale il teorema di Pappo, talché l'ambiente è un piano di Galois e K è una conica.

Dato un insieme finito $\mathscr{B}$ di elementi, che chiameremo «*punti*», ed un sottoinsieme I di permutazioni sopra $\mathscr{B}$, che chiameremo «*involuzioni*», la coppia $(\mathscr{B}, \mathrm{I})$ – o per semplicità (quando non vi sia possibilità di equivoco) l'insieme $\mathscr{B}$ stesso – si dice *un'ovale* (*libera*) se:

(i) ogni involuzione è d'ordine due;

(ii) per ogni coppia $(a_1, a_2), (b_1, b_2)$ di punti con $a_i \neq b_j$ $(i, j = 1, 2)$ esiste una e una sola involuzione f tale che $f(a_1) = a_2, f(b_1) = b_2$;

(iii) vi sono almeno tre punti.

(*) Budapest (Ungheria).

(**) Memoria presentata dall'Accademico dei XL BENIAMINO SEGRE, il 25 febbraio 1975.

(***) [1], [9] sono espositivi e [2] contiene le dimostrazioni.

Un'ovale ha *ordine* n se contiene $n+1$ punti.

Per meglio intendere la portata di questa nozione, rammentiamo che un'ovale proiettiva in un piano proiettivo π ha la struttura naturale di un'ovale, dove le involuzioni possono venir identificate dai punti non situati sopra K del piano nel modo seguente: Se $O \in \pi - K$, due punti di K risultano una coppia nell'involuzione determinata da O qualora giacciano sopra la stessa retta uscente da O.

Una conica irriducibile di un piano di Galois è dunque un caso particolare di un'ovale proiettiva. In seguito, un'ovale isomorfa alla struttura naturale di ovale inerente ad una conica irriducibile di un piano di Galois sarà brevemente chiamata una « *conica* ».

Sia $\mathscr{A}$ un'ovale d'ordine n. In modo del tutto immediato si stabiliscono le seguenti proprietà:

1) le involuzioni sono in numero di n^2;

2) n risulta dispari se, e soltanto se, ogni involuzione o muove tutti i punti di $\mathscr{A}$ o ne lascia fissi esattamente 2;

3) n risulta pari se, soltanto se, la permutazione della identità sopra K è un'involuzione.

Una permutazione dei punti di $\mathscr{A}$ ottenibile quale prodotto di involuzioni prende il nome di proiettività. Il gruppo G generato dalle involuzioni – ossia il gruppo delle proiettività di $\mathscr{A}$ – risulta triplamente transitivo su $\mathscr{A}$. È noto che una condizione necessaria e sufficiente affinché un'ovale $\mathscr{A}$ sia una conica è che G risulti isomorfo al gruppo lineare $PGL(2, n)$ (cfr. [2], 2.4).

Ad ogni ovale resta associata una struttura d'incidenza $\pi(\mathscr{A})$ in cui

(i) i punti di $\pi(\mathscr{A})$ sono quelli di $\mathscr{A}$ e le involuzioni;

(ii) ogni retta di $\pi(\mathscr{A})$ contiene due punti a, b non necessariamente distinti di $\mathscr{A}$ e tutte le involuzioni che permutano a in b. Una retta si dice anche « corda » o « tangente » secondoché $a \neq b$ oppure $a = b$.

Osserviamo che due rette di $\pi(\mathscr{A})$ s'incontrano in un punto solo, ma in generale $\pi(\mathscr{A})$ non risulta un piano proiettivo.

Un automorfismo di un'ovale $\mathscr{A}$ è una permutazione sopra i punti di $\mathscr{A}$ che rispetta le involuzioni.

Data una struttura d'incidenza $\pi(\mathscr{A})$, una retta si dice regolare se tutte le involuzioni appartenenti a questa retta sono automorfismi. A norma di un teorema di Buekenhout ([2], Teorema 8.8) l'insieme delle rette regolari può essere:

(I) vuoto;
(II) una corda;
(III) una tangente;
(IV) tutte le tangenti;
(V) tutte le tangenti e corde.

Si noti che, se l'ordine è pari, la classe IV e quella V coincidono.

Si vede inoltre che l'appartenenza di un'ovale alla classe V si traduce nel supporre che tutte le sue involuzioni siano automorfismi. Per tale motivi un'ovale siffatta conviene chiamarla regolare.

Esaminando le ovali proiettive allora (nel 1966) note, F. Buekenhout ha verificato che tutte le cinque classi sono non vuote, e perfino che una qualunque delle prime tre ammette anche delle ovali non isomorfe aventi lo stesso ordinea Di un'ovale regolare il cui ordine sia pari o primo dispari, lo stesso Autore ha dimostrato invece che è necessariamente una conica.

Non mi risulta, come del resto afferma Buekenhout, che sia stato risolto il medesimo problema per un qualunque ordine dispari, né che si sappia se un'ovale dalla classe IV è regolare o no.

In questa Nota si affrontano queste due questioni, risolvendole nella sostanza e dimostrando precisamente che:

ogni ovale regolare d'ordine n dispari risulta conica; allorché $n > 59$, lo stesso può dirsi di un'ovale dalla classe IV.

Ne discende che per una struttura di incidenza $\pi(\mathscr{A})$, con $\mathscr{A}$ d'ordine > 59, l'insieme delle rette regolari di $\pi(\mathscr{A})$ può soltanto essere in realtà:

(I) vuoto;

(II) una sola corda;

(III) una sola tangente;

(IV) tutte le tangenti e corde, e in quest'ultimo caso B non è altro che una conica.

1. Come accennato nell'introduzione, il gruppo delle proiettività di un'ovale ci permette di riconoscere se essa è conica. Avuto riguardo alla questione posta, per questo motivo ci proponiamo di analizzare il gruppo delle proiettività di un'ovale d'ordine dispari del tipo IV, quindi, in particolare, quello delle proiettività di un'ovale regolare dello stesso ordine. A questo proposito converrà tener presente alcuni recenti risultati di grande portata sulla teoria dei gruppi finiti.

Passiamo ad ennunciarli, usando i termini abituali per cui rimandiamo ai libri [6], [10], [11] e le seguenti convenzioni:

1.1, la cardinalità di un insieme finito I sarà denotata con $|I|$;

1.2, una permutazione involutoria sopra un insieme I verrà detta *iperbolica* (risp. *ellittica*) se possiede 2 (risp. O) punti fissi;

1.3, i gruppi lineari che intervengono nella nostra trattazione vanno considerati come gruppi di permutazioni (almeno) 2-transitivi, per le cui descrizioni rimandiamo a [6] (Kapitel II), [10] (Cap. XIII). In particolare, facendo agire su di una conica di un piano di Galois d'ordine p^r, $p \neq 2$ primo, il gruppo delle proiettività della stessa conica, si ottiene $PGL(2, p^r)$, dove il sottogruppo generato delle involuzioni iperboliche rappresenta $PSL(2, p^r)$ (cfr. n. 2).

Risultato 1. (Glauberman, [6] 22.10 Satz). Sia H un gruppo che non ammetta sottogruppi normali, non identico, d'ordine dispari e sia f un elemento di un 2-sottogruppo S di Sylow di H. Detto Z (H) il centro di H, $f \in \mathrm{Z}(\mathrm{H})$ equivale al sussistere di

$$\{hfh^{-1} \mid h \in \mathrm{H}\} \cap \mathrm{S} = \{f\}.$$

Risultato 2. (Feit, Thompson [4]). Il teorema sulla risolubilità dei gruppi d'ordine dispari.

Risultato 3. (Ch. Hering, W. M. Kantor, G. M. Seitz [5]). Sia H un gruppo 2-transitivo di permutazioni sopra un insieme finito $\mathscr{B}$. Supponiamo che lo stabilizzatore H_b contenuto in H, ossia il sottogruppo formato dalle permutazioni di H che lasciano fisso un punto $b \in \mathscr{B}$, ammetta un sottogruppo normale N regolare su $\mathscr{B} - b$. Allora $|\mathscr{B}| = p^r + 1$, p è primo e H contiene un sottogruppo normale M in maniera che $\mathrm{M} \leq \mathrm{H} \leq \mathrm{aut\,M}$ e H agisce sopra $\mathscr{B}$ come uno dei seguenti gruppi: un gruppo strettamente 2-transitivo, $\mathrm{PSL}(2, p^r)$, $\mathrm{Sz}(p^r)$, $\mathrm{PSU}(3, p^r)$ oppure un gruppo del tipo Ree.

Risultato 4. Lo stabilizzatore di un punto di uno qualunque dei gruppi figuranti nel risultato 3 è risolubile (cfr. [6], II. 1.18 Beispiel, 10.12 Satz, 10.15 Bemerkungen b, c).

Risultato 5. (Passmann [8], Ch. Hering, W. M. Kantor, G. M. Seitz [5], Corollary 10.1). Se H è un gruppo 5/2-volte transitivo (oppure 2-primitivo) sopra un insieme finito $\mathscr{B}$ e se lo stabilizzatore H_b contenuto in H è risolubile, $|\mathscr{B}| = p^r + 1$, p è primo e H rappresenta un gruppo proiettivo M dove $\mathrm{PSL}(2, p^r) \leq \mathrm{M} \leq \mathrm{P\Gamma L}(2, p^r)$.

Risultato 6. ([2], 5.13, 5.10, 3,8). Se $p \neq 2$, il sottogruppo generato dalle involuzioni ellittiche e iperboliche di $\mathrm{P\Gamma L}(2, p^r)$ è $\mathrm{PGL}(2, p^r)$.

Risultato 7. ([6] II.8.24 Fall 2.8.27 Haupsatz). Se T è un sottogruppo qualsiasi di $\mathrm{PSL}(2, p^r)$ e se p non divide $|\mathrm{T}|$, si presenta uno dei seguenti casi:

1.4, T è ciclico d'ordine z con $z/(p^r \pm 1)/2$;

1.5, T è diedrale d'ordine $2z$ con la stessa z come in 1.4;

1.6, $\mathrm{T} \simeq \mathscr{A}_4$, gruppo alterno su 4 oggetti;

1.7, $\mathrm{T} \simeq \mathscr{S}_4$, gruppo totale su 4 oggetti; per $p^{2r} - 1 = 0 \bmod 16$;

1.8, $\mathrm{T} \simeq \mathscr{A}_5$, gruppo alterno su 5 oggetti; per $p = 5$ oppure per $p^{2r} - 1 = 0 \bmod 5$.

Corollario 7. *Se, nelle ipotesi del risultato* 7, $p^r > 59$ *e* $|\mathrm{T}| \geq p^r + 1$, T *risulta diedrale d'ordine* $p^r + 1$.

Per concludere notiamo due risultati elementari pressoché immediati

Risultato 8. (Galois, [6] II. Satz 3.2, [11] 11.5, [10] XIII. 14.4). Se H è un gruppo primitivo di permutazioni sopra un insieme finito $\mathscr{C}$ e se N è un sottogruppo normale minimo e risolubile, N è regolare su $\mathscr{C}$.

Risultato 9. Se D^* è un gruppo di permutazioni sopra un insieme finito E e se $g \in E$, $|D^*| = |D^*_g|\,|D^*(g)|$.

2. Continuiamo i preliminari algebrici porgendo, in modo necessariamente sommario, la rappresentazione 3-transitiva di $PGL(2, p^r)$ e quella 2-transitiva di $PSL(2, p^r)$.

Sia Ω una conica in $S_{2,q}$, piano di Galois d'ordine $q = p^r$ con p primo dispari. Se L, M e P sono tre punti allineati del piano con L, M non necessariamente distinti fra di loro, tali che $L, M \in \Omega$ e $P \notin \Omega$ per «$LP \cap \Omega$» si intenderà – convenzionalmente – il punto M. Preso quindi un punto qualsiasi del piano, ma non giacente su Ω, la corrispondenza $\varphi_P : L \to$ «$LP \cap \Omega$» per ogni L di Ω induce una permutazione dei punti della conica che si chiama, com'è ben noto, un'involuzione di centro P. φ_P risulta iperbolica oppure ellittica, secondoché P è esterno o interno rispetto a Ω.

Queste involuzioni dotate di centro generano un gruppo strettamente 3-transitivo, il quale non è altro che la rappresentazione 3-transitiva di $PGL(2, p^r)$, mentre il gruppo generato dalle involuzioni iperboliche (risp. ellittiche) risulta la rappresentazione di $PSL(2, p^r)$ con $p^r \equiv 1 \bmod 4$ (risp. con $p^r \equiv 3 \bmod 4$).

È noto cfr. [7] n. 1) che per una retta l del piano, l'ordine del gruppo Γ_l generato dalle involuzioni col centro appartenente a $l^* = l - \Omega$ vale $2\,|l^*|$, qualora l non sia tangente a Ω; cioè, se $|l^*| \in \{p^r + 1, p^r - 1\}$, valgono le seguenti proprietà:

2.1 Γ_l è diedrale;

2.2 per il polo P di l rispetto a Ω, φ_P è contenuto in Γ_l, anzi risulta un elemento involutorio di $PGL(2, p^r)$, che giace in $Z(\Gamma_l)$ ed è diverso dalla permutazione identica di Ω;

2.3 Γ_l contiene due sottogruppi diedrali d'ordine $|l^*|$, generati uno dalle involuzioni iperboliche e l'altro da quelle ellittiche; di conseguenza, uno di questi giace anche in $PSL(2, p^r)$.

Vogliamo ora far vedere che

2.4 i Γ_l, al variare di l nell'insieme delle rette secanti (risp. delle rette esterne) rispetto a Ω, percorrono i gruppi diedrali d'ordine $2(p^r - 1)$ (risp. $2(p^r + 1)$) di $PGL(2, p^r)$.

Osserviamo anzitutto che, essendo $PSL(2, p^r)$ il derivato di $PGL(2, p^r)$, un tal sottogruppo di $PGL(2, p^r)$ possiede sempre un sottogruppo diedrale d'ordine $|l^*|$.

Osserviamo poi che, come dimostrò Dickson ([3], § 260), i sottogruppi diedrali d'ordine sia $p^r - 1$ che $p^r + 1$ di $PSL(2, p^r)$ risultano fra loro coniugati e sono ordinatamente in numero di $p^r(p^r + 1)/2$ e di $p^r(p^r - 1)/2$. Ne consegue che sottogruppi diedrali d'ordine $2(p^r - 1)$ (risp. $2(p^r + 1)$) sono in numero di (al massimo) $p^r(p^r + 1)/2$ (risp. $p^r(p^r - 1)/2$).

D'altro canto i Γ_l, secondoché l si mantiene secante o esterna, sono altresì in numero di $p^r(p^r + 1)/2$ o di $p^r(p^r - 1)/2$. Ne discende facilmente l'asserto.

Concludiamo il nostro breve studio sulla rappresentazione 3-transitiva di $\mathrm{PGL}(2, p^r)$ stabilendo che:

2.5 *Ogni sottogruppo diedrale d'ordine* $p^r + 1$ *(risp.* $p^r - 1$*) di* $\mathrm{PSL}(2, p^r)$ *risulta esser immerso in uno e un solo sottogruppo diedrale d'ordine* $2(p^r + 1)$ *(risp.* $2(p^r - 1)$*) di* $\mathrm{PGL}(2, p^r)$.

Completeremo le osservazioni preliminari dimostrando due proposizioni.

2.6 *Se* $\mathscr{B}$ *è un'ovale d'ordine* n *dispari, il gruppo* H *generato dalle involuzioni iperboliche di* $\mathscr{B}$ *è* $5/2$*-volte transitivo.*

Dimostrazione. Fissato un punto $b \in \mathscr{B}$, si verifica facilmente che il numero delle involuzioni che lasciano fisso b vale n. Poiché tutte queste risultano iperboliche, H_b è transitivo su $\mathscr{B} - b$. Essendo poi H transitivo sopra $\mathscr{B}$ resta da provare che H_b è $1/2$-transitivo, vale a dire che, preso un punto $c \in \{\mathscr{B} - b\}$ e facendo agire H_b sopra $\mathscr{B} - \{b, c\}$, tutte le orbite risultano della stessa lunghezza.

Denotiamo con F l'insieme delle involuzioni iperboliche che permutano fra loro i punti b, c. Analogamente a quanto accade per un'ovale proiettiva $|\mathrm{F}| = (n-1)/2$. Osserviamo poi che $\mathrm{FF} = \{f, g \in \mathrm{F}\} \subseteq \mathrm{H}_{b,c}$. Per un qualsiasi punto a di $\mathrm{B} - \{b, c\}$, indichi g l'involuzione individuata da $g(a) = a$ e da $g \in \mathrm{F}$. Allora le osservazioni fatte forniscono

$$\mathrm{F}(a) = \mathrm{F}(g(a)) = (\mathrm{F}g)(a) \subseteq \mathrm{FF}(a) \subseteq \mathrm{H}_{b,c}(a),$$

e in particolare, essendo attualmente $f(a) \neq g(a)$ se $f, g \in \mathrm{F}$ con $f \neq g$,

$$(n-1)/2 = |\mathrm{F}(a)| \leq |\mathrm{H}_{b,c}(a)|.$$

Ne segue, per definizione, che la lunghezza di ciascuna delle orbite di $\mathrm{H}_{b,c}$ vale almeno $(n-1)/2$.

Attualmente ci si presentano soltanto due alternative:

(i) tutte le lunghezze valgono $(n-1)/2$,

oppure

(ii) esiste almeno un'orbita la cui lunghezza supera $(n-1)/2$, avendo così intersezione non vuota con tutte le altre orbite di $\mathrm{H}_{b,c}$.

Nel primo caso, l'asserto segue subito; mentre nel secondo, per ottenerlo, abbiamo soltanto più da osservare che attualmente $\mathrm{H}_{b,c}$ agisce su di una sola orbita, e quindi dev'essere transitivo su $\mathscr{B} - \{b, c\}$, in quanto due orbite con punti comuni risultano necessariamente coincidenti.

2.7 *Se* $\mathscr{B}$ *è un'ovale d'ordine* n *dispari e se* H *è il gruppo generato dalle involuzioni iperboliche di* $\mathscr{B}$*, per ogni punto* $b \in \mathscr{B}$*, lo stabilizzatore* H_b*, contenuto in* H*, è primitivo.*

Dimostrazione. Procediamo per assurdo e supponiamo H_b imprimitivo. Sia $\mathrm{U} \subseteq \{\mathscr{B} - b\}$ un sistema di imprimitività, siano a, c due punti di U. Poiché $|\{\mathscr{B} - b\}| = n$, U può avere $(n-1)/2$ punti al massimo. D'altro canto, attualmente, giusto quanto è stato detto nella dimostrazione della 2.6, $|\mathrm{H}_{b,c}(a)|$

deve valere almeno $(n-1)/2$, sicché per U debbono valere, oltre alla precedente limitazione, anche le $|U| = |\{H_{b}, (a) \cup c\}| = (n+1)/2$. Confrontando le due stime ottenute per il numero dei punti situati su di U si raggiunge una contraddizione. Essendo H_b transitivo, ne segue l'asserto.

3. Sia $\mathscr{A}$ un'ovale d'ordine dispari e supponiamo che tutte le sue involuzioni iperboliche siano automorfismi, il che traduce l'ipotesi che, seguendo la classificazione data da F. Buekenhout, $\mathscr{A}$ sia di tipo IV. Denoteremo con H un gruppo di automorfismi di $\mathscr{A}$ che contenga tutte le involuzioni iperboliche di $\mathscr{A}$ e sia contenuto nel gruppo delle proiettività di $\mathscr{A}$, e chiameremo come di solito, H_b lo stabilizzatore di un punto $b \in \mathscr{A}$, contenuto in H. Conosciamo già – in forza delle 2.6, 2.7 – due proprietà di H, ossia che H è 5/2-transitivo e che H_b è primitivo sopra $\mathscr{A}$.

Ci proponiamo ora di dimostrare che $|\mathscr{A}| = p^r + 1$, con p primo dispari, ed inoltre, a meno di un isomorfismo, $PSL(2, p^r) \leq H \leq PGL(2, p^r)$.

Notiamo anzitutto che ogni elemento di H è un automorfismo, sicché $h^{-1}fh$, il trasformato di un'involuzione f mediante $h \in H$, è ancora un'involuzione.

Notiamo poi che, prese due involuzioni di $\mathscr{A}$, siano esse f e g, per le quali siano soddisfatte le $f(b) = b = g(b)$, le potenze di fg possono venir scritte sotto la forma fg_1, dove g_1 sia un'involuzione, risultando fra l'altro che tanto fg quanto le sue potenze sono prive di punti fissi sopra $\mathscr{A} - b$. Essendo n dispari se ne trae che:

3.1 *Il prodotto di due involuzioni giacenti in* H_b *è d'ordine p primo e dispari.*

Da ciò discendono facilmente la $|\mathscr{A}| = p^r + 1$ e la:

3.2 *Detto* F *l'insieme delle involuzioni figuranti in* H_b, *risulta* $F \cap Z(H_b) = \{0\}$

Sia $f \in F$ e denotiamo con S il 2-sottogruppo di Sylow di H_b contenente f. Poiché F si trasforma in sé mediante un automorfismo h giacente in H_b, dev'essere altresì $h^{-1}fh \in F$. Avuto riguardo alla 3.1, ne segue che l'ordine di $h^{-1}fhf$, che può rappresentarsi anche sotto la forma $(h^{-1}fh)f$, non sarà pari, risultando

$$\{h^{-1}fh \mid h \in H_b\} \cap S = \{f\}.$$

Questa è la 3.2, tenuto conto del risultato 1, implicano che H_b debba ammettere dei sottogruppi normali d'ordine dispari. Ne discende poi, a norma del teorema di Feit–Thompson sulla risolubilità dei gruppi d'ordine dispari, l'esistenza di un sottogruppo normale minimo d'ordine dispari, sia esso N, contenuto in H_b. Essendo H_b primitivo, tale proprietà, in forza del risultato 8, implica che N sia anche regolare su $\mathscr{A} - b$.

Possiamo ora usufruire del risultato 3, e poi di 4, con che si ottiene la risolubilità di H. Ciò, essendo H 5/2-volte transitivo, ci permette di applicare il risultato 5. Si avrà così, a meno di un isomorfismo, $PSL(2, p^r) \leq H \leq P\Gamma L(2, p^r)$, poi, in base del risultato 6, $PSL(2, p^r) \leq H \leq PGL(2, p^r)$, onde l'asserto.

Se $\mathscr{A}$ è un'ovale regolare d'ordine dispari, H può venir considerato come il gruppo della proiettività di $\mathscr{A}$. Essendo ora H 3-transitivo sopra $\mathscr{A}$, in base del teorema citato di J. Tits ([2], 2.4) sulla caratterizzabilità delle coniche mediante un gruppo di automorfismi strettamente tre volte transitivo, si perviene alla soluzione della questione posta sulle ovali regolari:

Ogni ovale regolare d'ordine dispari è una conica.

Se invece $\mathscr{A}$ è un'ovale appartenente alla classe IV, il gruppo generato dalle involuzioni iperboliche si può prendere in luogo di H. Avuto riguardo alle proposizioni del n. 2, si ottiene che:

Il gruppo H *generato dalle involuzioni iperboliche di una ovale d'ordine dispari appartenente alla classe IV risulta rappresentazione di* PSL $(2, p^r)$ *o di* PGL $(2, p^r)$, *e ciò a seconda che* $p^r = 1$ $(mod\ 4)$ *o* $p^r = 3$ $(mod\ 4)$.

4. Denotiamo d'ora in avanti con H il gruppo generato dalle involuzioni iperboliche di un'ovale d'ordine p^r dispari appartenente alla classe IV. Vogliamo dimostrare che il gruppo generato da un'involuzione ellittica g di $\mathscr{A}$ e da H risulta isomorfo a PGL $(2, p^r)$.

A tal scopo è opportuno stabilire che:

4.1 *Se* $h \in$ H *è l'ordine di* h *è* p, *allora* $h^{-1}gh \neq g$.

Dimostrazione. Abbiamo visto nel numero precedente che H è un sottogruppo di PGL $(2, p^r)$, dunque, in particolare, H è privo sopra $\mathscr{A}$ di elementi con più di due punti fissi, ad eccezione dell'elemento unità di H. Se teniamo conto del fatto che $|\mathscr{A}|$ uguaglia $p^r + 1$, ne discende che h lascia attualmente fermo uno ed un solo punto di $\mathscr{A}$, sia esso a. Essendo g ellittica si ha $g(a) \neq a$. Da tutto ciò risulta: $h^{-1}gh(a) = h^{-1}(g(a)) \neq g(a)$, onde l'asserto.

Denotiamo con E l'insieme delle involuzioni ellittiche di $\mathscr{A}$. Poiché H è un gruppo di automorfismi su $\mathscr{A}$, gli elementi di H trasformano E in sè. Pertanto, fissato un elemento h di H, l'applicazione h^* che porta ciascuna involuzione ellittica g nel suo trasformato $h^{-1}gh$ mediante h risulta una permutazione delle involuzioni ellittiche, ossia di E. Resta in tal modo definito un gruppo di permutazioni sopra E, che denotiamo con H^*. È evidente che $\mathrm{H}^* \simeq \mathrm{H}$. Avuto riguardo al fatto che, a meno di un isomorfismo, PSL $(2, p^r) \leq \mathrm{H} \leq$ PGL $(2, p^r)$ H^* possiede un sottogruppo D^* isomorfo a PSL $(2, p^r)$.

Data un'involuzione ellittica g, $|\mathrm{D}^*(g)|$ non può superare $|\mathrm{E}| = p^r(p^r - 1)/2$, inoltre si ha $|\mathrm{D}^*| = |\mathrm{PSL}(2, p^r)| = p^r(p^r + 1)(p^r - 1)/2$ (cfr. [6], II.8.1 Hilfsatz), sicché il risultato 9 porge attualmente $|\mathrm{D}^*_g| \geq p^r + 1$; mentre la 4.1 esprime ora che, appena rimanga fissato un punto di E da un elemento h^* di D^*_g, l'ordine di h^* deve essere diverso da p.

Assunta la limitazione $p^r > 59$, ne consegue che per D^*_g le ipotesi del Corollario 7 risultano attualmente soddisfatte. Si perviene così alla:

4.5 *Se* $\mathscr{A}$ *è d'ordine* p^r *con* $p^r > 59$, *il sottogruppo* D^*_g *di* D^* *che lascia ferma un'involuzione ellittica risulta diedrale d'ordine* $p^r + 1$.

Nel caso in cui $p^r \equiv 3 \pmod 4$ e contemporaneamente $\mathrm{H} \simeq \mathrm{PGL}(2, p^r)$, la 4.5 si estende colla:

4.6 *Se $\mathscr{B}$ è d'ordine p^r con $p^r \equiv 3$ (mod 4) e $p^r > 59$, il sottogruppo H_g^* di H^* che lascia ferma un'involuzione ellittica g risulta diedrale d'ordine $2(p^r+1)$.*

Dimostrazione. In modo analogo alla dimostrazione della proposizione precedente, si ottiene $|\mathrm{H}_g^*| = 2(p^r+1)$. Poiché $\mathrm{D}_g^* \leq \mathrm{H}_g^* \leq \mathrm{H}^* \simeq \mathrm{PGL}(2, p^r)$, $|\mathrm{H}_g^*| = 2(p^r+1)$ e D_g^* è diedrale d'ordine di p^r+1, basta ricordare la descrizione della rappresentazione 3-transitiva di $\mathrm{PGL}(2, p^r)$, ed inspecie la 2.5, per ottenere l'asserto.

Possiamo ora provare la

4.7 *Se $\mathscr{B}$ è d'ordine p^r con $p^r > 59$, per un'involuzione ellittica g H_g^* contiene un sottogruppo $\overline{\mathrm{H}}_g$ diedrale d'ordine (p^r+1) in cui le involuzioni sono tutte iperboliche.*

Dimostrazione. Se $p^r \equiv 1 \pmod 4$, essendo $\mathrm{H}^* \simeq \mathrm{PSL}(2, p^r)$, H^* non contiene che involuzioni iperboliche; pertanto D_g^* si può prendere in luogo di $\overline{\mathrm{H}}_g$. Se invece $p^r \equiv 3 \pmod 4$, la 4.6 assicura l'esistenza di un sottogruppo diedrale H^* d'ordine $2(p^r+1)$. Essendo $\mathrm{H}_g^* \leq \mathrm{H}^* \simeq \mathrm{PGL}(2, p^r)$, H_g^* deve contenere – in virtù delle 2.4, 2.3 – $(p^r+1)/2$ involuzioni iperboliche che formano un gruppo diedrale d'ordine p^r+1. Resta così provato l'asserto.

Data un'involuzione ellittica g, dalla 4.7 discende l'esistenza di un sottogruppo $\overline{\mathrm{H}}$ di H avente le seguenti proprietà:

4.8 *è diedrale d'ordine p^r+1;*

4.9 *tutte le involuzioni di $\overline{\mathrm{H}}$ risultano iperboliche;*

4.10 *$\bar{h}^{-1} g \bar{h} = g$ per ogni $\bar{h} \in \overline{\mathrm{H}}$, in altre parole $g \in \mathrm{Z}(\overline{\mathrm{H}})$.*

Esaminiamo ora l'azione di $\overline{\mathrm{H}}$ sopra $\mathscr{B}$. Osserviamo anzitutto che ogni punto di $b \in \mathscr{B}$ resta fissato da una e una sola involuzione contenuta in $\overline{\mathrm{H}}$, e ciascuna involuzione di $\overline{\mathrm{H}}$ lascia fissi due punti di $\mathscr{B}$. In tal modo i punti di $\mathscr{B}$ possono venir accoppiati, due punti formando una coppia se, e soltanto se, esiste un'involuzione di $\overline{\mathrm{H}}$ che li lascia fissi. Ne segue facilmente che una permutazione involontaria priva di punti fissi, contenuta nel gruppo totale sopra $\mathscr{B}$, è commutabile con tutti gli elementi di $\overline{\mathrm{H}}$ deve permutare i punti giacenti nella stessa coppia. Ciò fornisce ovviamente l'unicità delle permutazioni involutorie prive di punti fissi appartenenti a $\mathrm{Z}(\overline{\mathrm{H}})$.

D'altro canto, in virtù delle 2.4 e 2.2, per $p^r \equiv 3 \pmod 4$ $\overline{\mathrm{H}}$ stesso, mentre per $p^r \equiv 1 \pmod 4$ il sottogruppo diedrale d'ordine $2(p^r+1)$ di $\mathrm{PGL}(2, p^r)$ contenente $\overline{\mathrm{H}}$, possiede un tal elemento. Si ottiene così quanto enunciato al principio del presente numero.

Avuto riguardo al teorema di J. Tits citato alla fine del n. 3, abbiamo in conclusione che:

Ogni ovale d'ordine dispari del tipo IV ha l'ordine p^r, con p primo. Se $p^r > 59$, la classe IV non contiene che coniche.

Bibliografia

[1] F. Buekenhout (1966) – *Ovals et ovales projectifs*, « Rend. dell'Accad. Naz. Lincei », *8*, 40, 346–51.

[2] F. Buekenhout (1966) – *Étude intrinsèque des ovales*, « Rendiconti di Matematica », *25*, 333–393.

[3] L. E. Dickson (1961) – *Linear groups*, Leipzig.

[4] W. Feit–J. G. Thompson (1963) – *Solvability of groups of odd order*, « Pacific J. Math. », *13*, 755–1029.

[5] Ch. Hering–W. M. Kantor–G. M. Seitz (1970) – *Finite groups with a Split BN-pair of Rank 1*, « J. of Algebra », *20*, 435–475.

[6] B. Huppert (1967) – *Endliche Gruppen I*, Berlin, Heidelberg.

[7] G. Korchmáros (1974) – *Osservazioni sui risultati di B. Segre relativi ai k-archi contenenti h — 1 punti di un'ovale*, « Rend. dell'Accad. Naz. Lincei », *8*, 56, 905–913.

[8] D. S. Passmann (1969) – *Some 5/2-transitiv permutations groups*, « Pacific J. Math. », *28*, 157–171.

[9] B. Segre (1967) – *Introduction to Galois geometries*, « Atti dell'Accad. Naz. Lincei, Mem., Cl. Sc. Mat. Natur », *8*, vol. VIII, fasc. 5, 135–236.

[10] G. Zappa (1965, 1970) – *Fondamenti di teoria dei gruppi*, I–II, Edizione Cremonese.

[11] H. Wielandt (1964) – *Finite permutation groups*, New York and London, Academic Press.