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

GIORGIO FAINA
GÁBOR KORCHMÁROS

# Il sottogruppo generato dalle involuzioni regolari di un $B$-ovale 2-transitivo

*Rendiconti del Seminario Matematico della Università di Padova*, tome 74 (1985), p. 139-145
<http://www.numdam.org/item?id=RSMUP_1985__74__139_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 74 (1985)

# Il sottogruppo generato dalle involuzioni regolari di un $B$-ovale 2-transitivo.

GIORGIO FAINA - GÁBOR KORCHMÁROS (*)

SUMMARY - Let $B = (M, F)$ be a Buekenhout oval ($B$-oval) of even order with the automorphism group $G$ doubly transitive. Let $R$ be the set of regular involutions of $B$ and let $\langle R\rangle$ denote the subgroup of $G$ generated by $R$. The purpose of the present paper is to prove that one of the following holds:

(i) $|M| = p^h$, where $p$ is odd prime, and $\langle R\rangle$ is a soluble group,

(ii) $|M| = 2^d + 1$, $\langle R\rangle$ is a 2-transitive simple group on $M$ and either $\langle R\rangle \cong PSL(2, 2^d)$ or $\langle R\rangle \cong Sz(2^a)$, with $2a = d$, or $\langle R\rangle = PSU(3, 2^{2b})$, with $2b = 3d$.

Furthermore, we prove that if $\langle R\rangle$ is a regular normal subgroup of $G$ then either (iii) $|M| = p$, $p$ prime, and $G$ acts on $M$ as $AG(2, p)$ on $GF(p)$, or (iv) $|M| = 9$ and $G$ acts on $M$ as $3^2\cdot SL(2, 3)$ in its usual doubly transitive representation.

## 1. Introduzione.

Un $B$-ovale (od ovale astratto nel senso di Buekenhout) $B = (M, F)$ è un insieme $M$ di oggetti, $|M|\geqslant 3$, detti *punti*, dotato di una famiglia di permutazioni di ordine $\leqslant 2$, dette *involuzioni*, quasi strettamente

(*) Indirizzo degli AA.: G. FAINA: Dipartimento di Matematica, Università degli Studi, Via Vanvitelli 1, 06100 Perugia; G. KORCHMÁROS: Dipartimento di Matematica, Università della Basilicata, Via Nazario Sauro 85, 85100 Potenza.

Lavoro eseguito nell'ambito del G.N.S.A.G.A. del C.N.R.

2-transitiva, su $M$, nel senso che per ogni due coppie $(a_1, a_2)$, $(b_1, b_2) \in \in M \times M$, con $a_i \neq b_j$ $(i, j = 1, 2)$, esiste una ed una sola involuzione $f \in F$ tale che $f(a_1) = a_2$ e $f(b_1) = b_2$.

Se $|M| = n + 1$, l'ovale si dice (finito) di ordine $n$. Se $B = (M, F)$ e $B' = (M', F')$ sono due $B$-ovali, un *isomorfismo* tra $B$ e $B'$ è una applicazione biunivoca $h: M \to M'$ tale che, per ogni $f \in F$, $h \circ f \circ h^{-1} \in F'$. Un *automorfismo* di un $B$-ovale $B$ è un isomorfismo di $B$ su sé stesso; una involuzione $f \in F$ si dice *regolare* se è anche un automorfismo di $B$.

Denotiamo con $R$ l'insieme delle involuzioni regolari di $B$ e con $\langle R \rangle$ il gruppo da esso generato. Un $B$-ovale $B = (M, F)$ si dice 2-transitivo se il suo gruppo degli automorfismi $G$ è 2-transitivo su $M$.

Scopo del presente lavoro è di determinare $\langle R \rangle$ per i $B$-ovali 2-transitivi di ordine pari provando i seguenti Teoremi 1 e 2.

TEOREMA 1. Se $B = (M, F)$ è un $B$-ovale 2-transitivo di ordine pari, allora $\langle R \rangle$ è di uno dei seguenti tipi:

(i) $|M| = p^h$, con $p$ primo dispari, ed $\langle R \rangle$ è risolubile;

(ii) $|M| = 2^d + 1$, $\langle R \rangle$ è semplice, 2-transitivo su $M$ ed isomorfo ad uno dei seguenti gruppi: (j) $PSL(2, 2^d)$, (jj) $Sz(2^a)$, con $2a = d$, (jjj) $PSU(3, 2^{2b})$, con $2b = 3d$.

TEOREMA 2. Se $B = (M, F)$ è un $B$-ovale 2-transitivo di ordine pari ed $\langle R \rangle$ è di tipo (i), allora

($i_1$) $|M| = p$, con $p$ primo, e $G$ opera su $M$ allo stesso modo di $AG(2, p)$ su $GF(p)$, oppure

($i_2$) $|M| = 9$ e $G$ opera su $M$ allo stesso modo di $3^2 \cdot SL(2, 3)$ nella sua usuale rappresentazione 2-transitiva.

Si conoscono esempi riguardanti i casi (j), (jj) ed ($i_2$); per la relativa descrizione rimandiamo al successivo n. 2. Non si conoscono, invece, esempi riguardanti i casi ($i_1$) e (jjj).

## 2. Premesse ed esempi.

Sia $B = (M, F)$ un $B$-ovale di ordine $n$. Allora (cfr. [2]):

(1) $|F| = n^2$;

(2) $n$ è dispari se, e soltanto se, ogni involuzione fissa o zero o 2 punti;

(3) $n$ è pari se, e soltanto se, la permutazione identica $\varepsilon$ di $M$ appartiene ad $F$ ed ogni altra involuzione possiede uno, ed un solo, punto fisso.

*a) B-ovali associati al gruppo lineare $PGL(2, K)$ o B-coniche.*

Dato un campo $K$ si consideri il gruppo proiettivo lineare PGL$(2, K)$ nella sua usuale rappresentazione 3-transitiva su $K \cup \{\infty\}$. Gli elementi di ordine 2 di $PGL(2, K)$, con l'eventuale aggiunta dell'identità se $K$ è di caratteristica pari, costituiscono una famiglia $F$ quasi strettamente 2-transitiva su $K \cup \{\infty\}$. Il relativo gruppo $\langle R\rangle$ coincide con $PGL(2, K)$. Tale $B$-ovale fornisce un esempio per il caso (i) del Teorema 1, anzi (cfr. [6]) esso è l'unico esempio al riguardo.

*b) B-ovale di ordine 8 associato al gruppo delle trasvezioni dello spazio vettoriale $V$ di dimensione 2 sopra $GF(3)$.*

Tale $B$-ovale è stato fornito dal primo autore in [4] (cfr. anche [5]).

Si denoti con $H$ il gruppo di tutte le trasvezioni (shears) $f_{vt}$ di $V$, ove $f_{vt}(x) := v + t(x)$, $v \in V$ e $t \in SL(2, V)$. Per ogni biiezione involutoria $\varphi$ di $V$ tale che:

(1) $\varphi(v_0) = v_0$, per il vettore nullo $v_0 \in V$;

(2) $\varphi(v) \notin \{\lambda v | \lambda \in GF(3)\}$,

si definisce una famiglia $\Phi = \{h\varphi h^{-1} | h \in H\}$ di involuzioni su $V$. Denotata con $\varepsilon'$ l'applicazione di $V$ in sé che trasforma ogni $v \in V$ nel suo opposto $-v$, la famiglia

$$F = \Phi \cup \{f_{v\varepsilon'} | v \in V\} \cup \{\varepsilon\}$$

è quasi strettamente 2-transitiva su $V$. Il gruppo $G$ degli automorfismi di tale $B$-ovale $(V, F)$ coincide con $H$ e pertanto $G$ è 2-transitivo su $V$ e risulta essere il prodotto semidiretto di $SL(2, 3)$ per un gruppo abeliano elementare di ordine 9: $G \cong 3^2 \cdot SL(2, 3)$. Infine, $R$ si riduce all'insieme $\{f_{v\varepsilon'} | v \in V\}$.

*c) B-ovali associati ad ovali proiettivi.*

Un sottoinsieme di punti $\Omega$ di un piano proiettivo $\pi$, $|\Omega| \geqslant 3$, si dice *ovale proiettivo* in $\pi$ se una qualsiasi retta di $\pi$ interseca $\Omega$ in al più due punti e se per ogni punto $x$ di $\Omega$ passa una, ed una sola, retta di $\pi$ che interseca $\Omega$ solo in $x$. Un ovale proiettivo $\Omega$ di un piano proiettivo $\pi$ possiede una struttura naturale di $B$-ovale $(\Omega, F)$ le cui involuzioni possono essere identificate in modo canonico con i punti di $\pi \setminus \Omega$ nel modo seguente: se $p \in \pi \setminus \Omega$ e $a, b \in \Omega$, l'involuzione $j_p$ associata al punto $p$ permuta $a$ con $b$ se, e soltanto se, $p$ appartiene alla retta per $a$ e $b$ (se $a = b$, allora $j_p$ muta $a$ in sé se, e soltanto se, $p$ appartiene alla tangente ad $\Omega$ in $a$).

Una $B$-conica è il $B$-ovale associato ad una conica irriducibile di un piano proiettivo $PG(2, K)$ sopra un campo $K$. Le $B$-coniche sono esattamente i $B$-ovali introdotti in $a$). Si conoscono ovali proiettivi che non sono coniche e tra essi si trovano quelli introdotti in [7] sul duale del piano di Lüneburg $L(2^{2b})$ di ordine $2^b$. Ognuno di questi ultimi ovali, $\Omega$, ammette un gruppo di automorfismi che opera su $\Omega$ allo stesso modo di $Sz(2^b)$ nella sua usuale rappresentazione 2-transitiva. Il $B$-ovale associato ad $\Omega$ fornisce un esempio per il caso (jj) del Teorema 1 ed esso è l'unico esempio finora noto al riguardo.

## 3. Richiami sui gruppi 2-transitivi.

Adotteremo la terminologia usuale e quindi rimandiamo il lettore a [12].

TEOREMA DI BENDER [1]. Sia $G$ un gruppo di permutazioni 2-transitivo su un insieme finito $M$ tale che ogni elemento di ordine 2 di $G$ abbia un unico punto fisso su $M$ stesso. Se $N$ è il sottogruppo normale generato da tutti gli elementi di ordine 2 di $G$, allora si presenta uno dei seguenti casi:

(i) $|M| = p^h$, con $p$ primo, $N$ risolubile;

(ii) $|M| = 2^d + 1$, $N$ è semplice e 2-transitivo su $M$ ed inoltre, è isomorfo con uno dei seguenti tre gruppi: $PSL(2, 2^d)$, $Sz(2^a)$ con $2a = d$, $PSU(3, 2^{2b})$ con $2b = 3d$.

Un sottogruppo $H$ di un gruppo $G$ si dice *fortemente immerso* (strongly embedded subgroup) in $G$ se:

(1) il normalizzante di $H$ in $G$ è lo stesso $H$;

(2) $H$ contiene il centralizzante di ogni suo elemento di ordine 2.

Un insieme $I$ di involuzioni di un gruppo $G$ si dice triangolare (o $T$-set) se i suoi elementi sono invarianti (per coniugazione) in $G$ e contiene il prodotto di due qualsiasi suoi elementi che commutano tra loro.

Teorema di Shult [11]. Sia $G$ un gruppo di permutazioni di un insieme $M$ transitivo ed $I$ un $T$-set di $G$. Se ogni elemento di $I$ ha un solo punto fisso, allora $G_a \cap \langle I \rangle$ è fortemente immerso in $\langle I \rangle$, per ogni $a \in M$.

## 4. Dimostrazioni dei Teoremi.

Lemma 1. Se $B = (M, F)$ è un $B$-ovale di ordine $n \geqslant 4$ pari, dotato di un gruppo $G$ di automorfismi 2-transitivo, allora $R \neq \emptyset$.

Dim. Per $a \in M$, si denoti con $S_2(G_a)$ il 2-sottogruppo di Sylow dello stabilizzatore $G_a$ di $a$ in $G$. Poiché $2 \big| |G_a|$, essendo $|M|$ dispari, si ha che $S_2(G_a)$ è non banale. Proviamo che gli elementi di ordine 2 del centro $Z\big(S_2(G_a)\big)$ sono involuzioni regolari. A tale scopo ricordiamo (cfr. [2]) che gli automorfismi di ordine 2 di un $B$-ovale di ordine pari possono avere 1 oppure $\sqrt{n} + 1$ punti uniti su $M$. Poichè $G_a$ è transitivo su $M$, dal Lemma 15.4 di [10] discende che nessun elemento di ordine 2 appartenente a $Z\big(S_2(G_a)\big)$ può avere $\sqrt{n} + 1$ punti uniti su $M$. Ne segue che gli automorfismi di ordine 2 appartenenti a $Z\big(S_2(G_a)\big)$ hanno un solo punto fisso $a$. Tale proprietà caratterizza le involuzioni regolari, come provato in [2]. Ne segue l'asserto.

Lemma 2. Se $B = (M, F)$ è un $B$-ovale di ordine $n \geqslant 4$ pari con un gruppo di automorfismi $G$ 2-transitivo su $M$, allora $G$ contiene un $T$-set formato da involuzioni dotate di un solo punto fisso su $M$.

Dim. Proviamo che $R' = G \cap R$ è un $T$-set. In virtù del Lemma 1, $R'$ è non vuoto. Chiaramente $R'$ è un insieme invariante in $G$, pertanto è sufficiente provare che se $r_1 \circ r_2 = r_2 \circ r_1$, con $r_1, r_2 \in R$ e $r_1 \neq r_2$, allora $r_1 \circ r_2 \in R$.

Tenendo conto dei due risultati di Buekenhout già citati nella dimostrazione del Lemma 1, basta, a tale scopo, verificare che $r_1 \circ r_2$ non può avere $\sqrt{n} + 1$ punti fissi su $M$. Tale verifica è immediata, considerato che $R \subseteq F$ ed $F$ è quasi strettamente 2-transitiva su $M$.

Dimostrazione del Teorema 1. Per il Lemma 2, si può applicare il Teorema di Shult riportato nel precedente n. 3. Risulta, allora che, per ogni $a \in M$, $G_a \cap R'$ è un sottogruppo fortemente immerso in $\langle R' \rangle$. Proviamo che l'unica involuzione di $\langle R' \rangle$ con più di un punto fisso su $M$ è l'idendità di $M$. A tale scopo si consideri $g \in \langle R' \rangle$ tale che $g^2 = \varepsilon$ e $g \in G_a \cap G_b$, con $a, b \in M$ e $a \neq b$. Sia $S_2(G_a)$ un 2-sottogruppo di Sylow di $G_a$ contenente $g$. Come abbiamo visto nella dimostrazione del Lemma 1, esiste una involuzione $r \in Z(S_2(G_a)) \cap R'$. Risulta, inoltre, $g \circ r = r \circ g$. Poiché $g \in G_b \cap \langle R' \rangle$ e $G_b \cap \langle R' \rangle$ è un sottogruppo fortemente immerso in $\langle R' \rangle$, ne segue che anche $r \in G_b \cap \cap \langle R' \rangle$, a meno che $g$ sia l'identità di $M$. L'eventualità che $r \in G_b \cap \cap \langle R' \rangle$ non si verifica, essendo $r \notin G_b$. Possiamo infine applicare il Teorema di Bender, riportato nella sezione 3, e da esso discende senz'altro il Teorema 1.

Dimostrazione del Teorema 2. Supponiamo che $B = (M, F)$ sia un $B$-ovale di ordine $n = 2^m$ con un gruppo di automorfismi $G$ 2-transitivo su $M$ che risulti, inoltre, di tipo (i) nel Teorema di Bender. Si ha allora che $2^m + 1 = p^h$ con $p$ primo. Tale equazione diofantea ammette soluzioni solo se $h = 1$ oppure $h = 2$, $p = 3$, $f = 3$. In [5] è stato provato che esiste un solo $B$-ovale di ordine 8 il cui gruppo degli automorfismi $G$ è 2-transitivo. Infine, in [4] è stato provato che tale gruppo $G$ è isomorfo a $3^2 \cdot SL(2,3)$. In tal caso, come è noto [10], $G$ agisce su $M$ allo stesso modo di $AG(2, p)$ su $GF(p)$. Ciò completa la dimostrazione del Teorema 2.

## BIBLIOGRAFIA


[1] H. Bender, *Endliche zweifach transitive Permutationsgruppen deren Involutionen keine Fixpunte haben*, Math. Z., **104** (1968), pp. 175-204.

[2] F. Buekenhout, *Etude intrinsèque des ovales*, Rend. Mat., (5), **25** (1966), pp. 333-393.

[3] P. Dembowski, *Finite Geometries*, Springer-Verlag, Berlin, 1968.

[4] G. Faina, *Un esempio di ovale astratto non proiettivo a tangenti pascaliane il cui gruppo degli automorfismi è risolubile e due volte transitivo*, Rend. Sem. Mat. Brescia, **7** (1982), pp. 289-296.

[5] G. Faina, *The B-ovals of order $q \leq 8$*, J. Comb. Theory, **36**-A (1984), pp. 307-314.

[6] G. FAINA - G. KORCHMÁROS, *Una caratterizzazione del gruppo lineare $PGL(2, K)$ e delle coniche astratte nel senso di Buekenhout*, Boll. Un. Mat. Ital. Suppl., no. 2 (1980), pp. 195-208.

[7] G. KORCHMÁROS, *Le ovali di linea del piano di Lüneburg di ordine $2^{2r}$ che possono venir mutate in sé da un gruppo di collineazioni isomorfo al gruppo semplice $S(2^r)$ di Suzuki*, Memorie Accad. Naz. Lincei, (8) **15** (1979), pp. 295-315.

[8] G. KORCHMÁROS, *Collineation groups doubly transitive on the points at infinity in an affine plane of order $2^r$*, Arch. Math. (Basel), **37** (1981), pp. 572-576.

[9] H. LÜNEBURG, *Die Suzukigruppen und ihre Geometrien*, Lecture Notes in Math., no. 10 (1965).

[10] H. LÜNEBURG, *Translation Planes*, Springer-Verlag, Berlin, 1980.

[11] E. SHULT, *Permutation groups with few fixed points*, Nato Advanced Study Inst. Series: Geometry-von Staudt's Points of View, Reidel, Dordrecht, **70** (1980), pp. 275-311.

12] G. ZAPPA, *Fondamenti di teoria dei gruppi*, Cremonese, Roma, 1965, 1970.

Manoscritto pervenuto in redazione il 23 luglio 1984.