T_2-GROUPS AND A CHARACTERIZATION OF THE FINITE GROUPS OF MOEBIUS TRANSFORMATIONS

P. J. LORIMER

In recent years a number of algebraic characterizations of the groups of Moebius transformations over finite fields have been given in the literature; see **(1, 3, 6)**. H. W. E. Schwerdtfeger has noticed **(4)** that the group G of Moebius transformations over the real, complex, and certain other fields has the property:

G contains a subgroup H such that

(i) *if $a \notin H$, $bab^{-1} \notin H$, and $a^2 \neq 1$, then there exists exactly one $h \in H$ such that $hah^{-1} = bab^{-1}$;*

(ii) *if $a \notin H$, $bab^{-1} \notin H$, and $a^2 = 1$, then there exist exactly two $h_1, h_2 \in H$ such that $h_1 ah_1^{-1} = h_2 ah_2^{-1} = bab^{-1}$.*

Any group G having this property he has called a T_2-group with respect to the subgroup H; and H is said to be a T_2-subgroup of G. If, further, $G - H$ contains an involution, then G is called an S_2-group with respect to the subgroup H; and H is called an S_2-subgroup of G.

This paper is a study of S_2-groups, and includes a description of all finite S_2-groups. The following theorem is the main one of interest.

THEOREM. *If G is a finite group, then G is an S_2-group and the centre of G is trivial if and only if G is one of the groups of Moebius transformations over a finite field of characteristic $\neq 2$.*

Many of the results of this paper are also proved for infinite groups and are stated without restriction. In particular, all S_2-groups with non-trivial centre, whether finite or infinite, may be considered together, and are shown to lie in one of two well-known families of groups.

1. Notations. Upper case latin letters stand for groups and fields; lower case latin letters, and sometimes greek letters, for their elements. $C(a)$ is the centralizer of the element a, $N(K)$ the normalizer of the subgroup K, and $Z(K)$ the centre of the group K. $|K|$ is the order of the group K and $(0, 1)$ is the group with two elements.

Received February 10, 1964. Most of this paper is contained in the author's Ph.D. thesis submitted to McGill University in May 1963. The author is indebted to Professor H. W. E. Schwerdtfeger, who laid the ground for this research, for his help and advice. The author also wishes to thank the Canadian Government, who made his stay at McGill possible by granting him a Commonwealth Scholarship.

2. Examples of S_2-groups.

Example I. Let F be any field of characteristic $\neq 2$. Let G be the group of all regular Moebius transformations

$$z \to \frac{az+b}{cz+d}, \qquad a, b, c, d \in F \text{ and } ad - bc \neq 0$$

and let H be the subgroup of G of all similarities

$$z \to \frac{az+b}{d}, \qquad a, b, d \in F, ad \neq 0.$$

Then H is an S_2-subgroup of G. Schwerdtfeger has given a geometrical proof of this result for certain fields in **(4)**.

G may be represented as a group of congruence classes of elements of the group $\mathrm{GL}(2, F)$ of all regular 2×2 matrices over F. If $A, B \in \mathrm{GL}(2, F)$ we define $A \sim B$ if and only if there exists a $\lambda \in F$, $\lambda \neq 0$ such that $A = \lambda B$. We denote the congruence class containing A by $[A]$. H is then the subgroup of congruence classes

$$\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right]$$

with $c = 0$. We use these congruence classes in the following proof that G is an S_2-group.

Proof. Suppose that

$$[A] = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \in G$$

and that

$$[P] = \left[\begin{pmatrix} p & q \\ r & s \end{pmatrix}\right]$$

is a conjugate of $[A]$. Then there exists a $\lambda \in F$ such that λP is a conjugate of A in $\mathrm{GL}(2, F)$. Without loss of generality we may suppose that $\lambda = 1$. Then

(1) $$p + s = a + d,$$

(2) $$ps - qr = ad - bc.$$

Suppose that $[A] \notin H$, $[P] \notin H$. Then

(3) $$r \neq 0, \qquad c \neq 0.$$

Further

(4) $$[A]^2 = [P]^2 = 1 \leftrightarrow p + s = a + d = 0.$$

We seek solutions $[H] \in H$ to the equation $[H][A] = [P][H]$, which is equivalent to seeking solutions to $HA = \lambda PH$, $\lambda \in F$, where to maintain the

https://doi.org/10.4153/CJM-1965-036-5 Published online by Cambridge University Press

values of the determinants we must have $\lambda^2 = 1$. Now char $F \neq 2$. Thus the equation $\lambda^2 = 1$ has two distinct solutions in F, viz. 1 and -1.

Suppose that

$$H = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}.$$

Then $xz \neq 0$ and hence

(5) $$x \neq 0, \qquad z \neq 0.$$

Now $HA = \lambda PH$ implies that

(6) $$(a - \lambda p)x + cy = 0,$$

(7) $$\lambda rx - cz = 0,$$

(8) $$bx + (d - \lambda p)y - \lambda qz = 0,$$

(9) $$\lambda ry + (\lambda s - d)z = 0.$$

From (6) and (3)

(10) $$y = -c^{-1}(a - \lambda p)x$$

and from (7) and (3)

(11) $$z = c^{-1}\lambda rx.$$

These solutions for y and z are consistent with (8) if and only if $p(p + s)(\lambda - 1) = 0$ and with (9) if and only if $(\lambda - 1)(p + s) = 0$.

Thus if $[A]^2 \neq 1$, (10) and (11) give a solution if and only if $\lambda = 1$, while if $[A]^2 = 1$, $p + s = 0$ and (10) and (11) give a solution for both values of λ; i.e. if $[A]^2 \neq 1$ the only solution is

$$[H] = \left[\begin{pmatrix} c & -a + p \\ 0 & r \end{pmatrix}\right],$$

while if $[A]^2 = 1$, there is a further solution

$$[H] = \left[\begin{pmatrix} c & -a - p \\ 0 & -r \end{pmatrix}\right].$$

The congruence class

$$\left[\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\right]$$

lies in $G - H$ and is an involution. Hence G is an S_2-group.

Example II. Let I be a commutative integral domain with unit 1 such that $1 + 1 \neq 0$, and let S be the set of all regular 2×2 matrices with elements in J. We define an equivalence relation $\sim$ on the elements $A, B, \ldots$ of S by setting $A \sim B$ if and only if there are non-zero λ, $\mu \in I$ such that $\lambda A = \mu B$. It is easily shown that $S/\sim$ is a group which is isomorphic to the group of Moebius transformations of the field of quotients of J and is hence an S_2-group.

Example III. Suppose that $G \simeq (0, 1)^\alpha$, where $(0, 1)$ is the group with two elements and α is any cardinal number. Let H be any subgroup of G such that $H \simeq (0, 1)$. Then H is a S_2-subgroup of G.

Example IV. Let H be any abelian group containing just one involution. We extend H to a group G by adjoining to H an element t: $t^2 = 1$ and $tht^{-1} = h^{-1}$ for all $h \in H$. H is then a S_2-subgroup of G.

In the following it is shown, in the case where G is a finite group, that groups of these types are the only S_2-groups. The result is extended to the infinite case when the centre of G is not trivial.

3. Five lemmas. The following five lemmas, giving general information on T_2-groups, will be useful in later theorems. The lemmas in this section are denoted by numbers; all other lemmas of the paper are denoted by upper case latin letters.

LEMMA 1. *If H is a T_2-subgroup of G, $h \in H$, and h commutes with an element of $G - H$, then $h^2 = 1$.*

LEMMA 2. *If H_1 and H_2 are proper T_2-subgroups of G and $H_1 \subseteq H_2$, then $H_1 = H_2$.*

LEMMA 3. *If H is a T_2-subgroup of G and K is a subgroup of G such that $H \subseteq K$, then H is a T_2-subgroup of K.*

LEMMA 4. *If H is a T_2-subgroup of G and $g \notin H$, then*
(i) *g has exactly $|H|$ conjugates in $G - H$ if $g^2 \neq 1$,*
(ii) *g has exactly $\frac{1}{2}|H|$ conjugates in $G - H$ if $g^2 = 1$.*

LEMMA 5. *If $H \simeq (0, 1)$ is an S_2-subgroup of a group G, then $G \simeq (0, 1)^\alpha$ for some α.*

Proof. Suppose that $H = \{1, h\}$, $h^2 = 1$. Then $C(h) = \{g | g \in G, g^2 = 1\}$. Thus every element of $C(h)$ is an involution and hence $C(h) \simeq (0, 1)^\alpha$ for some α.

Suppose that $a_1, a_2 \in C(h) - H$ and that a_2 is a conjugate of a_1. Then, by the property S_2 there is an $\bar{h} \in H$ such that $\bar{h}a_1\bar{h}^{-1} = a_2$, which is impossible as $\bar{h}$ commutes with both a_1 and a_2. Thus, if $a \in C(h) - H$ and a is not a conjugate of h, then $a \in Z(G)$. Furthermore, h has at most one conjugate in G.

Suppose that h_1 is a conjugate of h. Then $C(h) - Z(G) = \{h, h_1\}$. Hence, as $C(h) \cap Z(G)$ is a subgroup of $C(h)$, $C(h) \cap Z(G) = \{1, hh_1\}$ and thus $C(h) = \{1, h, h_1, hh_1\}$.

Now h has only one conjugate in G. Therefore $C(h)$ has only one coset in G. Suppose that $a \in G - C(h)$. Then $aha^{-1} = h_1$ and $a^2 \in C(h)$. Obviously a^2 is different from 1, h, or h_1 and $a^2 \neq hh_1$, for then $(ha)^2 = (hhh_1)^2 = h_1^2 = 1$ and thus $a \in H$.

Thus we have derived a contradiction and h can have no conjugates in G, i.e. $h \in Z(G)$. Hence $G = C(h) \simeq (0, 1)^\alpha$.

4. Normal S_2-subgroups. Suppose that G has the property S_2 with respect to H. The main result of this section is that the following are equivalent:

(i) $H \lhd G$,

(ii) $Z(G) \neq 1$,

(iii) G and H are described in either Example III or Example IV.

Many of the results have applications later in the paper.

THEOREM 1. *If H is a normal T_2-subgroup of G, then either*

(i) $g^2 = 1$ *for all* $g \in G - H$ *or*

(ii) $g^2 \neq 1$ *for all* $g \in G - H$.

Proof. Suppose that $a, g \in G - H$, $a^2 = 1$, $g^2 \neq 1$. By property T_2, there exists an $h \in H$, $h \neq 1$, such that $hah^{-1} = a$. Hence $C(a) \cap H = \{1, h\}$. But, as $H \lhd G$, $C(a) \cap H \lhd C(a)$, and hence every element of $C(a)$ is an involution. This is obviously true for every $b \in G - H$ satisfying $b^2 = 1$.

Suppose that $c \in G$. Then, as $H \lhd G$, $cac^{-1} \notin H$ and hence there is an $h_1 \in H$ such that $h_1 a h_1^{-1} = cac^{-1}$. Hence $c \in h_1 C(a) \subseteq HC(a)$. Here c is any element of G and thus $G = HC(a)$. Similarly $G = HC(g)$.

Since $g^2 \neq 1$, property T_2 implies that $C(g) \cap H = 1$. Hence $C(g) \simeq G/H$. Also $C(a) \cap H = \{1, h\}$; therefore $C(a)/\{1, h\} \simeq G/H$ and $C(g) \simeq C(a)/\{1, h\}$. But every element of $C(a)$ is an involution. Hence every element of $C(g)$ is an involution, which is a contradiction as $g^2 \neq 1$.

THEOREM 2. *If H is a normal S_2-subgroup of G and $g \in G - H$, $h \in H$, then $ghg^{-1} = h^{-1}$.*

Proof. $G - H$ contains an involution and hence, by Theorem 1, *every element of $G - H$ is an involution. Therefore $g^2 = 1$ and if $h \in H$, $(gh)^2 = 1$, i.e. $ghg^{-1} = h^{-1}$.*

COROLLARY 1. *H contains exactly one involution*; for if $h \in H$ is an involution, $ghg^{-1} = h$.

COROLLARY 2. *H is abelian*; for $h \to h^{-1}$ is an automorphism of H.

COROLLARY 3. *If h is the involution of H, then $Z(G) = \{1, h\}$.*

THEOREM 3. *If H is a normal S_2-subgroup of G, then either* (i) $H \simeq (0, 1)$ *and* $G \simeq (0, 1)^\alpha$ *for some α or* (ii) $G/H \simeq (0, 1)$.

Proof. Suppose that $t \in G - H$. Then $t^2 = 1$ and $|C(t) \cap H| = 2$. Suppose that $|G|/|H| > 2$.

Suppose that $u \notin H$, $u \notin tH$. Then $ut \notin H$ and hence by Theorem 1, $u^2 = 1$ $(ut)^2 = 1$. Thus $utu^{-1} = t$. Hence t commutes with every element of $G - \{H \cup tH\}$. Thus t commutes with every element of uH and hence with every element of H. This yields

$$H \subseteq C(t) \cap H \simeq (0, 1).$$

https://doi.org/10.4153/CJM-1965-036-5 Published online by Cambridge University Press

Hence $H \simeq (0, 1)$ and every element of G is an involution, i.e. $G \simeq (0, 1)^\alpha$ for some α.

Alternatively $G/H \simeq (0, 1)$.

THEOREM 4. *H is a normal S_2-subgroup of G if and only if H and G are described by either Example* III *or Example* IV.

THEOREM 5. *Let H be a T_2-subgroup of G but not necessarily a normal subgroup of G. Let h be an involution of H. Then $C(h) \cap H$ is a normal T_2-subgroup of $C(h)$.*

Proof. Write $C(h) \cap H = K$ and suppose that $a \in C(h) - K$. Let bab^{-1} be any conjugate of a such that $bab^{-1} \in C(h) - K$. Suppose that $h_1 \in H$ and $h_1 a h_1^{-1} = bab^{-1}$. Then $bab^{-1} \in C(h)$ and thus $h_1 a h_1^{-1} \in C(h)$, i.e.

$$h_1 a h_1^{-1} h = h . h_1 a h_1^{-1}.$$

Therefore $h_1^{-1} h h_1 \in C(a) \cap H$. But $C(a) \cap H = \{1, h\}$. Hence $h_1^{-1} h h_1 = h$, i.e. $h_1 \in C(h)$. This yields $h_1 \in C(h) \cap H$.

Now $a \in C(h)$ and hence $a^2 = 1$. Hence by the property T_2, there are $h_1 h_2 \in H$ such that

$$h_1 a h_1^{-1} = h_2 a h_2^{-1} = bab^{-1},$$

and by the above $h_1, h_2 \in C(a) \cap H$. Thus $C(a) \cap H$ is a T_2-subgroup of $C(a)$.

Suppose that $t \in C(a) - K$, $h_1 \in K$. Then $t^2 = 1$ and $(th_1)^2 = 1$. Hence $th_1 t^{-1} = h_1^{-1}$. Therefore $tKt^{-1} = K$, i.e. $K \lhd C(a)$, i.e. $C(a) \cap H \lhd C(a)$.

COROLLARY. *If h is an involution of H and h commutes with an element of $G - H$, then $C(h) \cap H$ contains just one involution*, viz. h.

Proof. From Theorem 4, $C(h) \cap H$ must be one of the T_2-subgroups of Examples III or IV.

The following theorem based on Theorems 4 and 5 will be useful in later sections.

THEOREM 6. $(0, 1)^2$ *cannot be an S_2-subgroup of any group.*

Proof. By Theorem 4, $(0, 1)^2$ cannot be a *normal* S_2-subgroup of any group.

Suppose that $H \simeq (0, 1)^2$ is an S_2-subgroup of G and $h \in H$. Then $h^2 = 1$, and by Theorem 5 $C(h) \cap H$ is a normal S_2-subgroup of $C(h)$. But H is abelian and hence $C(h) \cap H = H$. Hence $C(h) = H$. Thus no element of H commutes with an element of $G - H$ and G is not an S_2-group.

THEOREM 7. *If H is an S_2-subgroup of G and $Z(G) \neq 1$, then $H \lhd G$.*

Proof. Suppose that $Z(G) \cap H \neq 1$. Let $h \in Z(G) \cap H$. Then h commutes with an element of $G - H$. Hence $h^2 = 1$, and by Theorem 5 $C(h) \cap H \lhd C(h)$, i.e. $H \lhd G$.

Suppose that $Z(G) \cap H = 1$. Then $G - H$ contains an element, g say, of the centre. g commutes with an element of H and hence $g^2 = 1$. Thus g commutes with exactly two elements of H and commutes with every element of G. Thus $H \simeq (0, 1)$. Hence, by Lemma 6, $G \simeq (0, 1)^\alpha$ for some α and $H \lhd G$.

We have now proved the main theorem of this section.

THEOREM 8. *If H is an S_2-subgroup of G, then the following are equivalent:*
(1) $H \lhd G$,
(2) $Z(G) \neq 1$,
(3) *H and G are described by either Example* III *or Example* IV.

5. Structure theorems for S_2-groups.

THEOREM 9. *If H and $\bar{H}$ are two T_2-subgroups of a group G and*
(1) $G \neq \bar{H}H$,
(2) $H \not\sim (0, 1)$,
then H and $\bar{H}$ are conjugate subgroups of G. In fact if $g \in G - \bar{H}H$, then $gHg^{-1} = \bar{H}$.

The proof proceeds by a number of lemmas.

LEMMA A. *Let $g \notin \bar{H}H$. If $\bar{h} \in \bar{H}$, then $g^{-1}\bar{h} \notin H$; and if $h \notin H$, then $gh \notin \bar{H}$.*

LEMMA B. *If $g \notin \bar{H}H$, $h \in H - \bar{H}$, and $h^2 \neq 1$, then $ghg^{-1} \in \bar{H}$.*

Proof. Suppose that $ghg^{-1} \notin \bar{H}$. Then $h \notin \bar{H}$, $ghg^{-1} \notin \bar{H}$, and hence by the property T_2 there is an $\bar{h} \in \bar{H}$ such that $ghg^{-1} = \bar{h}h\bar{h}^{-1}$. Then $g^{-1}\bar{h} \in C(h)$. But by Lemma A $g^{-1}\bar{h} \notin H$ and hence $h^2 = 1$.

LEMMA C. *If $g \notin \bar{H}H$, $\bar{h} \in \bar{H} - H$, and $\bar{h}^2 \neq 1$, then $g^{-1}\bar{h}g \in H$.*

The rest of the proof consists in proving the equivalent of Lemma B for the case $h^2 = 1$.

LEMMA D. *If $g \notin \bar{H}H$ and $g^2 = 1$, then $g \notin H$, $g \notin \bar{H}$ and hence, by the property T_2, there are $h \in H$, $\bar{h} \in \bar{H}$, $h \neq 1$, $\bar{h} \neq 1$ such that $gh = hg$ and $g\bar{h} = \bar{h}g$. We show that $h = \bar{h} \in H \cap \bar{H}$.*

Proof. Suppose that $\bar{h} \notin H$ and $h \notin \bar{H}$. We show firstly that $\bar{h}h\bar{h}^{-1} = h$. $\bar{h} \notin H$ and, by Lemma 1, $\bar{h}^2 = 1$. Thus there exists a unique $h_1 \in H$, $h_1 \neq 1$, such that $h_1\bar{h}h_1^{-1} = \bar{h}$. Then $\bar{h} = g\bar{h}g^{-1} = h_1\bar{h}h_1^{-1}$. Hence $g^{-1}h_1 \in C(\bar{h})$. But $g^2 = 1$; hence $g = g^{-1}$. Thus $gh_1 \in C(\bar{h})$ and by Lemma A, $gh_1 \notin \bar{H}$. Thus by the property T_2, $(gh_1)^2 = 1$, i.e. $h_1gh_1^{-1} = g$ as $h_1^2 = 1$, $g^2 = 1$. But $hgh^{-1} = g$ and h is determined uniquely. Hence $h = h_1$ and $h\bar{h}h^{-1} = \bar{h}$.

We now show that if $h_1 \in H - \bar{H}$, $h_1 \neq h$ and $h_1^2 = 1$, then $ghg^{-1} \in \bar{H}$. Suppose the contrary, i.e. there is an element

$$h_1 \in H - \bar{H},\ h_1 \neq h,\ h_1^2 = 1 \text{ and } gh_1g^{-1} \notin \bar{H}.$$

Then $h_1 \notin \bar{H}$, $gh_1g^{-1} \notin \bar{H}$ and hence by the property T_2, there are $\bar{h}_1$, $\bar{h}_2 \in \bar{H}$

such that $gh_1 g^{-1} = \bar{h}_1 h_1 \bar{h}_1^{-1} = \bar{h}_2 h_1 \bar{h}_2^{-1}$. Thus $g^{-1}\bar{h}_1 \in C(h_1)$ and by Lemma A, $g^{-1}\bar{h}_1 \notin H$. Hence, by the property T_2, $(g^{-1}\bar{h}_1)^2 = 1$, i.e. $g^{-1}\bar{h}_1 g = \bar{h}_1^{-1}$ as $g^2 = 1$.

Suppose that $\bar{h}_1 \notin H$, and thus $\bar{h}_1^{-1} \notin H$. Then $\bar{h}_1^2 = 1$; for if $\bar{h}_1^2 \neq 1$, we have by Lemma C that $g^{-1} \bar{h}_1 g \in H$, i.e. $\bar{h}_1 \in H$. Hence $g^{-1} \bar{h}_1 g = \bar{h}_1$. But $g^{-1}\bar{h}g = \bar{h}$ and this determines $\bar{h}$ uniquely. Hence $\bar{h}_1 = \bar{h}$ and

$$gh_1 g^{-1} = \bar{h}_1 h_1 \bar{h}_1^{-1} = \bar{h} h_1 \bar{h}^{-1}.$$

Therefore $g^{-1} \bar{h} \in C(h_1)$. But $g^{-1} \bar{h}$ commutes with $h \in H$ and this determines h uniquely. This yields $h = h_1$, contrary to supposition. Thus we must have $\bar{h}_1 \in H$; similarly $\bar{h}_2 \in H$.

Now the element $\bar{h}_1^{-1} \bar{h}_2$ lies in $\bar{H}$ and commutes with $h_1 \notin \bar{H}$. Hence $(\bar{h}_1^{-1} \bar{h}_2)^2 = 1$. Also $\bar{h}_1^{-1} \bar{h}_2 \in H$ and $h_1 \in H$. Therefore, by Theorem 5, $C(h_1) \in H$. But $g^{-1} h_1 \in C(h_1)$ and $g^{-1} h_1 \notin H$, which is a contradiction. Thus, if $h_1 \in H - \bar{H}$, $h_1 \neq h$ and $h_1^2 = 1$, then $gh_1 g^{-1} \in \bar{H}$.

By this result and Lemma B, we have that if $h_1 \in H - \bar{H}$ and $gh_1 g^{-1} \notin \bar{H}$, then $h_1 = h$. Thus $gHg^{-1} - \bar{H}$ contains at most two elements. Therefore $|gHg^{-1}| \leqslant 4$ and hence $|H| \leqslant 4$. H contains the involution h. Hence either $H \simeq (0, 1)$ or $H \simeq (0, 1)^2$. The first possibility is excluded by the conditions of the theorem and the second by Theorem 5, Corollary, which gives a contradiction. Hence either $h \in \bar{H}$ or $\bar{h} \in H$. In either case, because of the uniqueness of h and $\bar{h}$, we have $h = \bar{h} \in H \cap \bar{H}$, which proves Lemma D.

Lemma E. *If $g \notin \bar{H}H$, $g^2 = 1$, and $h \in \bar{H} - H$, then $g^{-1} \bar{h}g \in H$.*

Proof. If $g^{-1} \bar{h}g \notin H$, then by the property T_2, there is an $h_1 \in H$ such that $g^{-1} \bar{h}g = h_1^{-1} \bar{h}h_1$. Thus $gh_1^{-1} \in C(\bar{h})$, and $gh_1^{-1} \notin \bar{H}H$ and hence by Lemma D, $\bar{h} \in \bar{H} \cap H$, which is a contradiction.

Proof of Theorem 9. Either gH contains an involution or it contains no such element. Suppose the former, i.e. $(gh)^2 = 1$ for some $h \in H$. Then, by Lemma E, $(gh)^{-1}(\bar{H} - H)(gh) \subseteq H$.

Suppose the latter and suppose that $\bar{h} \in \bar{H} - H$. Then if $g^{-1} \bar{h}g \notin H$, there is an $h_1 \in H$ such that $g^{-1} \bar{h}g = h_1 \bar{h}h_1^{-1}$. Thus $\bar{h}$ commutes with gh_1 and $gh_1 \in gH$. Hence $(gh_1)^2 = 1$ which is a contradiction. This yields

$$g^{-1}(\bar{H} - H)g \subseteq H.$$

Thus, in either case, there is an $h \in H$ such that $(gh)^{-1}(\bar{H})\ (gh) \subseteq H$, i.e. $g^{-1} \bar{H}g \subseteq H$. Hence by Lemma 2, $g^{-1}\bar{H}g = H$, which proves Theorem **9.**

Lemma F. *If K is a subgroup of G, $H \subseteq K$ and $H \neq K$, then $\bar{H} \subseteq K$, $\bar{H}H \subseteq K$.*

Corollary 1. $N(H) = H$.

Proof. Suppose that $H \neq N(H)$. Then by Lemma F, $\bar{H}H \subseteq N(H)$. But $G - \bar{H}H$ forms just one coset of H in G. Therefore $\bar{H}H = N(H)$ and hence

$N(H) \lhd G$. By Lemma F, $\bar{H} \subseteq N(H)$ and, as $N(H) \lhd G$ and as $g \notin \bar{H}H = N(H)$ implies $gHg^{-1} = \bar{H}$, we must have that H is a normal but not characteristic subgroup of $N(H)$.

If H is a T_1-subgroup of $N(H)$, then by **(5)**, H is a characteristic subgroup. Hence by Theorem 8, H and $N(H)$ must be described by either Example III or Example IV. Hence $H \simeq (0, 1)$, which is excluded by the conditions of Theorem 8.

COROLLARY 2. *If $g \in G - \bar{H}H$, then $G - \bar{H}H = gH$.*

COROLLARY 3. *H is a maximal subgroup of G.*

COROLLARY 4. *If K is an extension of G and H is a T_2-subgroup of K, then $G = K$.*

COROLLARY 5. *If G is a finite group,*

$$|G|/|H| = |H|/|H \cap \bar{H}| + 1.$$

THEOREM 10. *If H_1, H_2, and H_3 are three different conjugate S_2-subgroups of a group G, then $H_1 \cap H_2 \cap H_3 = 1$.*

The proof follows Theorem 11.

THEOREM 11. *If H_1, H_2, and H_3 are three different conjugate S_2-subgroups of a group G, then $H_1 \cap H_2$ is abelian, contains exactly one involution, and there exists an element $h_1 \in H_1$ such that $h_1 H_2 h_1^{-1} = H_3$. Further, if a is the involution of $H_1 \cap H_2$, then*

$$C(a) \cap H_1 = C(a) \cap H_2 = H_1 \cap H_2.$$

Proof. H_1 is an S_2-subgroup of G and hence $G - H_1$ contains an involution, say t. Suppose that t commutes with $a_1 \in H_1$, $a_1^2 = 1$. Now $a_1 \in H_1 \cap tH_1 t^{-1}$ and it is easily seen, by Theorem 6, that

$$C(a_1) \cap H_1 \subseteq H_1 \cap tH_1 t^{-1}.$$

An argument similar to that in Theorem 5 shows that $H_1 \cap tH_1 t^{-1}$ is a normal S_2-subgroup of the group

$$(H_1 \cap tH_1 t^{-1}) \cup t(H_1 \cap t H_1 t^{-1}).$$

Hence $H_1 \cap t H_1 t^{-1}$ is abelian and so

$$C(a_1) \cap H_1 = H_1 \cap tH_1 t^{-1}.$$

Similarly,

$$C(a_1) \cap tH_1 t^{-1} = H_1 \cap tH_1 t^{-1}.$$

Furthermore, $H_1 \cap tH_1 t^{-1}$ contains just one involution, viz. a_1.

We now prove that if $\bar{H}$ is any other conjugate of H_1, then there exists $h \in H_1$ such that $h\bar{H}h^{-1} = tH_1 t^{-1}$. By Theorem 9, if $g \notin tH_1 t^{-1} \bar{H}$, then

https://doi.org/10.4153/CJM-1965-036-5 Published online by Cambridge University Press

$g\bar{H}g^{-1} = tH_1t^{-1}$. It is thus sufficient to prove that there exists $h \in H_1$ such that $h \notin tH_1t^{-1}\bar{H}$.

Suppose the contrary. Then $H_1 \subseteq tH_1t^{-1}\bar{H}$ and hence $H_1\bar{H} \subseteq tH_1t^{-1}\bar{H}$. Thus, by Theorem 9, if $g \notin tH_1t^{-1}\bar{H}$, then $g\bar{H}g^{-1} = H_1$, which is a contradiction as $g\bar{H}g^{-1} = tH_1t^{-1} \neq H_1$. Thus there exists $h \in H_1$ such that $h\bar{H}h^{-1} = tH_1t^{-1}$.

Theorem 11 now follows easily.

Proof of Theorem 10. Suppose that $h \in H_1 \cap H_2 \cap H_3$, $h \neq 1$. Then $H_1 \cap H_2 \subseteq H_1 \cap H_2 \cap H_3$, for otherwise $h \in H_3$ commutes with an element k of $H_1 \cap H_2$, $k \notin H_3$. Now, by Theorem 11, either $h^2 \neq 1$ or $k^2 \neq 1$ which contradicts either the definition of T_2, or Lemma 1. Therefore

$$H_1 \cap H_2 = H_1 \cap H_2 \cap H_3.$$

Hence, by the principle of generalization, if H is any conjugate of H_1 different from H_1 and H_2, then $H_1 \cap H_2 = H_1 \cap H_2 \cap H$. Thus

$$H_1 \cap H_2 = \bigcap_{g \in G} gH_1g^{-1}.$$

Therefore, $H_1 \cap H_2$ is a normal subgroup of G and a is the only involution of $H_1 \cap H_2$. Hence $a \in Z(G)$, which contradicts Theorem 8, as H_1 is not a normal subgroup of G. Thus $H_1 \cap H_2 \cap H_3 = 1$.

THEOREM 12. *If H_1 and H_2 are any two conjugate S_2-subgroups of a group G and $|H_1|/|H_1 \cap H_2| = s$, then*

$$|H_1 \cap H_2| = s - 1, \qquad |H_1| = (s-1)s, \qquad \text{and } |G| = (s-1)s(s+1).$$

Proof. In the light of Theorem 9, Corollary 5, it is sufficient to prove that $|G|/|H_1| = |H_1 \cap H_2| + 2$.

LEMMA A. *If $a \in H_1$, a commutes with $t \in G - H_1$ and $bab^{-1} \in H_1$ for some $b \in H$, then $hah^{-1} = bab^{-1}$ for some $h \in H_1$.*

Proof. If $b \in H_1$, the result is obvious.

If $b \in tH_1$, take $h = bt^{-1}$.

If $b \notin H_1$, $b \notin tH_1$, then H_1, bH_1b^{-1}, and tH_1t^{-1} are three different conjugate S_2-subgroups of G. Hence by Theorem 11, there is an $h \in H_1$ such that $h(tH_1t^{-1})h^{-1} = bH_1b^{-1}$. Therefore

$$h(H_1 \cap tH_1t^{-1})h^{-1} = H_1 \cap bH_1b^{-1}.$$

But a is the only involution of $H_1 \cap tH_1t^{-1}$ and bab^{-1} is the only involution of $H_1 \cap bH_1b^{-1}$. Hence $hah^{-1} = bab^{-1}$.

LEMMA B. *If $a \in H_1$ and a commutes with $t \in G - H_1$, then*

$$C(a) = (C(a) \cap H_1) \cup t(C(a) \cap H_1).$$

Proof. Suppose that $u \in C(a)$, $u \notin C(a) \cap H_1$, $u \notin t(C(a) \cap H_1)$. Then $u \notin H$, $u \notin tH$. Thus H, tHt^{-1}, and uHu^{-1} are three different conjugate S_2-subgroups of G and $a \in H \cap tHt^{-1} \cap uHu^{-1}$, which contradicts Theorem 10. Hence $C(a) = (C(a) \cap H_1) \cup t(C(a) \cap H_1)$.

Proof of Theorem 12. By the property S_2 and Theorem 11, $H_1 \cap H_2$ contains exactly one involution which commutes with an element of $G - H_1$. Now, a has $|H_1|/|C(a) \cap H_1|$ conjugates in H_1 by elements of H_1; and by Lemma B it has no others. Further, a has $|G|/|C(a)|$ conjugates in G. Thus, by Lemma 4,

$$|G|/|C(a)| - |H_1|/|C(a) \cap H_1|$$

is either equal to zero or to $|H_1|$. In the first case $|G| = 2|H_1|$, in which case H is a normal subgroup of G, which is impossible. Hence the second case holds. Replacing $|C(a) \cap H_1|$ by $|H_1 \cap H_2|$ (Theorem 11) and $|C(a)|$ by $2|H_1 \cap H_2|$ (Lemma B), we have $|G|/|H_1| = |H_1 \cap H_2| + 2$.

6. A characterization of the Moebius groups. The object of this section is to prove:

THEOREM 14. *If G is a finite S_2-group with trivial centre, then G is one of the groups of Moebius transformations over a finite field of characteristic $\neq 2$.*

We use the method developed by H. Zassenhaus **(6)**. We first represent G as a permutation group.

The symbols of the permutations are the members of the set $\Sigma = \{H\}$ of S_2-subgroups of G. The permutation g representing the element g of G is the permutation $g: H \to gHh^{-1}$ for all H in Σ. This is obviously a faithful representation of G.

THEOREM 13. *As a permutation group on the symbols of Σ, G is three-fold transitive and any element of G is uniquely determined by the image of any three symbols of Σ.*

Proof. Suppose that H_i and $\bar{H}_i$, $i = 1, 2, 3$, are any two triples of symbols of Σ. Then we must prove that there is a $g \in G$ such that $gH_i g^{-1} = \bar{H}_i$, $i = 1, 2, 3$.

Now the elements of Σ are conjugate subgroups and hence there are elements x, y, z in G satisfying $xH_1 x^{-1} = \bar{H}_i$, $yH_2 y^{-1} = \bar{H}_2$, $zH_3 z^{-1} = \bar{H}_3$.

LEMMA A. $|xH_1 \cap yH_2| \neq 0$.

Proof. Suppose that $|xH_1 \cap yH_2| = 0$. Then $xH_1 \subseteq G - yH_2 = \bar{H}_2 H_2$ by Theorem 9. Hence $xH_1 H_2 \subseteq \bar{H}_2 H_2$. Now

$$|xH_1 H_2| = |H_1 H_2| = |H_1||H_2|/|H_1 \cap H_2| = s^2(s - 1),$$

where $s = |H_1|/|H_1 \cap H_2|$, and similarly $|\bar{H}_2 H_2| = s^2(s - 1)$. Thus $xH_1 H_2 = \bar{H}_2 H_2$. Hence

$$G - xH_1 H_2 = G - H_2 H_2 = yH_2.$$

This yields $x(G - H_1 H_2) = yH_2$ or $G - H_1 H_2 = x^{-1}yH_2$. Hence

$$(x^{-1}y)H_2(x^{-1}y)^{-1} = H_1.$$

Thus $yH_2 y^{-1} = xH_1 x^{-1}$, i.e. $\bar{H}_1 = \bar{H}_2$, which is impossible as the symbols of Σ are distinct.

LEMMA B. $|xH_1 \cap yH_2 \cap zH_3| \neq 0$.

Proof. Suppose that $|xH_1 \cap yH_2 \cap zH_3| = 0$. Then $zH_3 \subseteq G - (xH_1 \cap yH_2)$. By Lemma A, there is an $\alpha \in xH_1 \cap yH_1$. Then $xH_1 \cap yH_2 = \alpha(H_1 \cap H_2)$. Therefore $zH_3 \subseteq G - \alpha(H_1 \cap H_2)$ and hence

$$\alpha^{-1} zH_3 \subseteq G - (H_1 \cap H_2) = (G - H_1) \cup (G - H_2).$$

Thus $\alpha^{-1} z \in (G - H_1 H_3) \cup (G - H_2 H_3)$. Hence either $\alpha^{-1}z \in G - H_1 H_3$ or $\alpha^{-1}z \in G - H_2 H_3$. Suppose the former. Then $(\alpha^{-1}z)H_3(\alpha^{-1}z)^{-1} = H_1$. Therefore

$$zH_3 z^{-1} = \alpha H_1 \alpha^{-1} = xH_1 x^{-1}.$$

Thus $\bar{H}_3 = \bar{H}_1$, which is a contradiction. Thus we must have

$$|xH_1 \cap yH_2 \cap zH_3| \neq 0,$$

which proves Lemma B.

Proof of Theorem 13. By Lemma B, there is a $g \in xH_1 \cap yH_2 \cap zH_3$. Obviously $gG_i g^{-1} = \bar{H}_i$, $i = 1, 2, 3$. The second part follows by Theorem 10.

We now apply the method of Zassenhaus to this three-fold transitive group. Denote the symbols of Σ by $a, b, c, \ldots, x, y, z, \ldots$ and choose three of them, arbitrarily, to be denoted by 0, 1, and ∞. Now the symbols of Σ are S_2-subgroups. Denote the subgroup corresponding to a in Σ by H_a, and if $g \in G$, write $g(a) = b$ if and only if $gH_a g^{-1} = H_b$. Now, because $N(H_a) = H_a$ for all $a \in \Sigma$, we have $H_a = \{g \in G: g(a) = a\}$. We are interested particularly in H_0 and H_∞ and it is convenient to denote the elements of H_∞ by upper case latin letters.

Consider $H_\infty \cap H_0$. From Theorem 13, $H_\infty \cap H_0$ is obviously a transitive group on the symbols of $\Sigma_2 = \Sigma - \{0, \infty\}$ and each element of $H_\infty \cap H_0$ is uniquely determined by the image of any one symbol of Σ_2. We denote the element of $H_\infty \cap H_0$ which takes 1 onto x by M_x and define a binary relation, on the symbols of Σ_2, by defining $xy = M_x(y)$.

LEMMA A. *Σ_2 is a group isomorphic to $H_\infty \cap H_0$.*

Proof. It is sufficient to show that $M_x M_y = M_{xy}$. We have

(i) $x1 = x$ for $M_x(1) = x$,

(ii) $M_{xy}(1) = (xy)1 = xy$ by (i),

$M_x M_y(1) = x(y1) = xy$ by (i).

Hence $M_{xy}(1) = M_x M_y(1)$ and hence $M_{xy} = M_x M_y$. Thus the group Σ_2 is

https://doi.org/10.4153/CJM-1965-036-5 Published online by Cambridge University Press

isomorphic to $H_\infty \cap H_0$. In particular we have that Σ_2 is abelian and contains an involution.

Now H_∞ is a two-fold transitive group on the symbols of $\Sigma_1 = \Sigma - \{\infty\}$ and only the unit element of H leaves two symbols fixed. Therefore, by the Theorem of Frobenius (**2**, p. 181), the elements of H which leave no symbol of Σ_1 fixed form a transitive normal abelian subgroup K of H_∞. Obviously each element of K is uniquely determined by the image of one symbol of Σ_1. We denote the element of K which takes 0 onto x by A_x, and define a binary relation $+$ on Σ_1 by defining $x + y = A_x(y)$.

LEMMA B. *Σ_1 is a group isomorphic to K.*

Proof. It is sufficient to prove that $A_{x+y} = A_x A_y$. We have
(i) $x + 0 = x$ for $A_x(0) = x$,
(ii) $A_{x+y}(0) = (x + y) + 0 = x + y$ by (i),
$A_x A_y(0) = x + (y + 0) = x + y$ by (i).
Therefore $A_{x+y} = A_x A_y$ and hence Σ_1 is isomorphic to K. In particular Σ_1 is abelian.

LEMMA C. *Σ_1 with the two binary relations is a field.*

Proof. As both the groups of Σ_1 are abelian it is sufficient to prove the distributive law $x(y + z) = xy + xz$. We have
(i) $M_x^{-1} = M_{x^{-1}}$ for $M_{x^{-1}} M_x(1) = x^{-1}(x1) = 1$; hence $M_{x^{-1}} M_x = 1$;
(ii) $M_x(0) = 0$ for $M_x \in H_0$.
Now K is a normal subgroup of H; hence, if $M_x \in H_\infty \cap H_0$ and $A_y \in K$, then $M_x A_y M_x^{-1} = A_z$ for some $z \in \Sigma_1$. Now

$$M_x A_y M_x^{-1}(0) = M_x A_y(0) = M_x(y) = xy$$

and $A_z(0) = z$. Therefore $z = xy$ and hence $M_x A_y M_x^{-1} = A_{xy}$ or

$$M_x A_y = A_{xy} M_x.$$

But $M_x A_y(z) = x(y + z)$ and $A_{xy} M_x(z) = xy + xz$. Hence

$$x(y + z) = xy + xz.$$

Thus Σ_1 is a field.

Now G contains an involution T such that $TM_x T^{-1} = M_x^{-1} = M_{x^{-1}}$ for all $M_x \in H_\infty \cap H_0$. Thus $TM_x = M_{x^{-1}} T$ and in particular

$$TM_x(1) = M_{x^{-1}} T(1).$$

Hence

$$T(x) = x^{-1}T(1) = T(1)x^{-1}$$

as Σ_1 is abelian.
Put $I = M_{T(1)^{-1}} T$. Then

$$I(x) = M_{T(1)^{-1}}T(x) = T(1)^{-1}T(1)x^{-1} = x^{-1}.$$

Thus G contains the permutation $x \to x^{-1}$. Furthermore G contains the permutations $M_a{:}x \to ax$ and $A_a{:}x \to a + x$. Thus G contains the group of Moebius transformations of the field Σ_1 of order s. But the order of G is $(s - 1)s(s + 1)$ and hence G is the group of Moebius transformations over the field Σ_1. Further, $H_\infty \cap H_0$ has order $s - 1$ and contains an involution. Thus s and hence the characteristic of Σ_1 is odd. This completes the proof of Theorem 14.

References

1. R. Brauer, M. Suzuki, and G. E. Wall, *A characterisation of the one-dimensional unimodular projective groups over finite fields*, Ill. J. Math., *2* (1958), 718–45.
2. W. Burnside, *Theory of groups of finite order* (New York, 1955).
3. Daniel Gorenstein and John H. Walter, *On finite groups with dihedral Sylow 2-subgroups*, Ill. J. Math., *6*, (1962), 533–93.
4. H. W. E. Schwerdtfeger, *On a property of the Moebius group*, Annali di Mat. (IV), *54* (1961), 23–32.
5. ——— *Über eine spezielle Klasse Frobeniusscher Gruppen*, Arch. d. Math., *13* (1962), 283–9.
6. H. Zassenhaus, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem. Univ. Hamburg, *11* (1936), 17–40.

University of Canterbury,
Christchurch, New Zealand