ON A CLASS OF DOUBLY TRANSITIVE GROUPS[1]

J. L. ZEMMER[2]

The purpose of this note is to prove the following.

THEOREM. *Let G be a group of permutations on a set $\mathfrak{M}$. If* (i) *G is doubly transitive and only the identity fixes two letters, and* (ii) *the subgroup fixing one letter is Abelian, then G is isomorphic to the group of affine transformations $x \to ax+b$, $a \neq 0$, on a field.*

This theorem is related to a result of Hall [2, Theorem 5.6], which states that if a group G satisfies condition (i) above and in addition either

(i′) $\mathfrak{M}$ is finite,

or

(i″) for some $i, j \in \mathfrak{M}$ there is at most one element of G mapping i into j which displaces all of the letters, then G is isomorphic to the group of affine transformations, $x \to ax+b$, $a \neq 0$, on a near-field. A near-field is an algebraic system $(K, +, \cdot)$ consisting of a set K and two binary operations $+$ and $\cdot$ satisfying:

(a) $K(+)$ is an Abelian group with identity 0,

(b) the nonzero elements of K form a group with respect to $\cdot$ with identity 1,

(c) $x(y+z) = xy+xz$ for $x, y, z \in K$,

(d) $0 \cdot a = 0$ for each $a \in K$,

(e) if $a, b, c \in K$, $a \neq b$, the equation $au = bu+c$, has a unique solution u in K.

In [1], Gorenstein has called an *independent ABA group*, any group H which contains two subgroups A and B such that for $x \in H$, either $x \in A$, or x can be represented uniquely in the form a_1ba_2, $a_1, a_2 \in A$, $1 \neq b \in B$. The proof of the Theorem will consist of first showing that a doubly transitive group G, in which only the identity fixes two letters, is a special kind of independent ABA group. This is a corollary of Lemma 2. Using the structure of G as an independent ABA group, it will then be shown that, when A is Abelian, G satisfies condition (i″) of Hall's theorem, from which our theorem follows at once.

It should be pointed out that in the finite case Hall's result [2, Theorem 5.6] follows almost immediately from the corollary of

Received by the editors April 21, 1960 and, in revised form, August 8, 1960.

[1] This work was supported by the National Science Foundation.

[2] The author is indebted to the referee for several suggestions, in addition to his pointing out the validity of Lemma 2.

Lemma 2 together with a result of Gorenstein [1, Theorem 6].

The original version of this paper began with the Corollary to Lemma 2. The referee has suggested a more general lemma relating doubly transitive groups to certain kinds of ABA groups. This is stated as Lemma 2. To state Lemma 2 it is necessary first to generalize the notion of independent ABA group. This will be done with the aid of Lemma 1.

A group G with subgroups A and B is called an ABA group if for $x \in G$, $x = a_1 b a_2$, where $a_1, a_2 \in A$, $b \in B$. If G is an ABA group, and $b \in B$, $b \neq e$, the identity, define $L(G)$ and $R(G)$ as follows:

$$L(G) = \{x \in A \mid b = xby \text{ for some } y \in A\},$$
$$R(G) = \{x \in A \mid b = ybx \text{ for some } y \in A\}.$$

LEMMA 1. *If G is an ABA group with B of order two, then $L(G) = R(G)$ is a subgroup of A, say A'. Further, if A' is normal in A then A' is normal in G.*

PROOF. Let $x \in L(G)$, and choose y so that $b = xby$. Then $b = b^{-1} = (xby)^{-1} = y^{-1}bx^{-1}$, hence $ybx = b$ and $x \in R(G)$. Thus, $L(G) \subseteq R(G)$. A slight modification of this argument shows that $R(G) \subseteq L(G)$; it follows that $L(G) = R(G)$. Again, let $x \in A' = L(G) = R(G)$; then $b = xby = y^{-1}bx^{-1}$, which implies $x^{-1} \in A'$. If $x_1, x_2 \in A'$ then $b = x_1 b y_1$, $b = x_2 b y_2$. Clearly $b = x_1(x_2 b y_2) y_1 = x_1 x_2 b y_2 y_1$, and A' is a subgroup of A.

If A' is a normal subgroup of A, and $x \in A'$, $g \in G$, then $g^{-1}xg = a_2^{-1} b a_1^{-1} x a_1 b a_2 = a_2^{-1} b x_1 b a_2$, where $x_1 \in A'$. Since $b = x_1 b y$, $b x_1 b = y^{-1} \in A'$. Hence $g^{-1}xg = a_2^{-1} y^{-1} a_2 \in A'$. Thus A' is normal in G.

The following definition is a generalization of an independent ABA group for the special case where B has order two. An ABA group G, where B has order two, is called an *n-independent ABA group* if n is the order of the subgroup A', described in Lemma 1.

LEMMA 2. *If G is a doubly transitive group with subgroup fixing two letters finite, of order n, then G is an n-independent ABA group.*

PROOF. Let G be a group satisfying the hypotheses of the lemma. Denote by 0 and 1 a pair of distinct letters of the set on which G acts. Let A be the subgroup of G which fixes 0, and A' the subgroup of A which fixes 0 and 1. If c is an element of G which interchanges 0 and 1, then the subgroup, $\{A', c\}$, of G generated by A' and c is finite of order $2n$. Thus, $\{A', c\}$ contains an element of order two. The double transitivity of G implies the existence of an element b, of order two, which interchanges 0 and 1.

Now, let $g \in G$, $g(0) = \alpha$, $g(1) = \beta$, then $\alpha \neq \beta$. If $\alpha = 0$, then $g \in A$;

if $\alpha \neq 0$, let a_1 be an element of A such that $a_1(1) = \alpha$. Since $a_1(1) = \alpha \neq \beta$, it follows that $a_1^{-1}(\beta) \neq 1$, and hence $ba_1^{-1}(\beta) = \eta \neq 0$. Let a_2^* be an element of A such that $a_2^*(1) = \eta = ba_1^{-1}(\beta)$; then $a_1 ba_2^*(1) = \beta$, and $a_1 ba_2(0) = a_1 b(0) = a_1(1) = \alpha$. It follows that $(a_1 ba_2^*)^{-1} g$ fixes both 0 and 1, hence $(a_1 ba_2^*)^{-1} g = a \in A'$, and $g = a_1 ba_2^* a = a_1 ba_2$. Thus G is an ABA group.

With the notation of Lemma 1, let $x \in L(G) \subseteq A$, so that $b = xby$ for some y in A. Since $x \in A$, $x(0) = 0$, and since $x = by^{-1}b$, $x(1) = by^{-1}b(1) = by^{-1}(0) = b(0) = 1$. Thus x fixes 1 as well as 0 and $x \in A'$, whence $L(G) \subseteq A'$. Conversely, let $a \in A'$; then $ba^{-1}b$ fixes 0 and 1. Thus, $ba^{-1}b = a' \in A'$, and $b = aba'$, and $a \in L(G)$. It follows that $A' \subseteq L(G)$. Thus $L(G) = A'$ has order n, and it is seen that G is an n-independent ABA group.

The converse of Lemma 2 is false. Consider, for example, the non-cyclic group of order ten. It is a 5-independent ABA group and is not isomorphic to any doubly transitive group. Several modifications of the converse are true, and a particular one is proved in the following.

COROLLARY. *A group G is doubly transitive, with only the identity fixing two letters if and only if G is an independent ABA group with B of order two.*

PROOF. Let G be a doubly transitive group in which only the identity fixes two letters. It follows from Lemma 2 that G is a 1-independent ABA group, that is, an independent ABA group with B of order two.

Conversely, let G be an ABA group of this type, and $\mathfrak{M}$ the set of right cosets of A in G. Each $g \in G$ determines a permutation T_g on $\mathfrak{M}$, namely the mapping $Ax \rightarrow Axg$. The set of mappings $\{T_g, g \in G\}$ forms a group of permutations on $\mathfrak{M}$, and it is readily seen that the mapping $g \rightarrow T_g$ is an isomorphism of G onto this permutation group. To see that this group is doubly transitive, let $Ax_1 \neq Ax_2$, $Az_1 \neq Az_2$ be any two pairs of left cosets. Since $x_2 x_1^{-1}$, $z_2 z_1^{-1} \notin A$, we have $x_2 x_1^{-1} = a' ba''$, $z_2 z_1^{-1} = \bar{a} b \hat{a}$. Let

$$y = x_1^{-1} a''^{-1} \hat{a} z_1;$$

then

$$Ax_1 y = Ax_1 x_1^{-1} a''^{-1} \hat{a} z_1 = Az_1$$

and

$$Ax_2 y = Ax_2 x_1^{-1} a''^{-1} \hat{a} z_1 = Aa' ba'' a''^{-1} \hat{a} z_1 = Ab\hat{a} z_1 = Abb\bar{a}^{-1} z_2 = Az_2.$$

Finally, to see that no element, other than the identity, has more than one fixed point, let $Ax_1 \neq Ax_2$ and suppose that for some $y \in G$, $Ax_1y = Ax_1$ and $Ax_2y = Ax_2$. Then $x_1y = a_1x_1$, $x_2y = a_2x_2$, where $a_1, a_2 \in A$. It follows that $y = x_1^{-1}a_1x_1 = x_2^{-1}a_2x_2$, or that

$$a_1x_1x_2^{-1} = x_1x_2^{-1}a_2.$$

But, $x_1x_2^{-1} \notin A$, so that $x_1x_2^{-1} = \bar{a}b\breve{a}$. Thus,

$$a_1\bar{a}b\breve{a} = \bar{a}b\breve{a}a_2,$$

which implies $a_1\bar{a} = \bar{a}$, $a_1 = e$, $x_1y = x_1$, $y = e$. Thus G is isomorphic to a doubly transitive group in which only the identity fixes two letters.

Before proceeding to the next two lemmas, we list some lemmas of Hall which will be needed. In [2] Hall proves that in a doubly transitive permutation group with only the identity fixing two letters, the following hold:

I. *There exists one and only one element of order* 2 *which interchanges a given pair of elements of* $\mathfrak{M}$.

II. *The elements of order* 2 *are in a single conjugate class.*

Two cases arise from II:

Case 1. The elements of order 2 displace all elements of $\mathfrak{M}$.

Case 2. Every element of order 2 fixes an element of $\mathfrak{M}$.

III. *In Case* 2 *there is one and only one element of order* 2 *with a given fixed point.*

IV. *If* b_1, b_2 *are distinct elements of order* 2 *then* b_1b_2 *displaces all elements of* $\mathfrak{M}$.

In terms of its representation as an ABA group we see that in Case 1, A contains no element of order 2; and in Case 2, A contains a unique element of order 2, which will be denoted by t.

With the notation of Lemma 2, let A^* be the set of nonidentity elements of A, and let $a \in A^*$. Then $bab \notin A$ and hence $bab = \phi(a)b\psi(a)$, where $\phi(a), \psi(a) \in A$. Further, $\phi(a) \neq e \neq \psi(a)$, so that ϕ, ψ are mappings of A^* into A^*. Also since b has order 2, $ba^{-1}b = (bab)^{-1}$, whence, $\phi(a^{-1})b\psi(a^{-1}) = [\phi(a)b\psi(a)]^{-1} = [\psi(a)]^{-1}b[\phi(a)]^{-1}$. From the uniqueness of the representation it follows that

$$\phi(a^{-1}) = [\psi(a)]^{-1}. \tag{1}$$

In the following two lemmas it is assumed that the subgroup A is Abelian. The element t_0 of A will be the identity, e, in Case 1 and the unique element, t, of order two in Case 2.

Lemma 3. *If* $a \in A$, $a \neq t_0$ *then* $\psi(t_0a) \cdot \phi(t_0a) = a$.

Proof. First, from $bab = \phi(a)b\psi(a)$, we obtain $ab = b\phi(a)b\psi(a) = \phi^2(a)b\psi(\phi(a))\psi(a)$, whence, $\phi^2(a) = a$, and

$$\psi(\phi(a))\cdot\psi(a) = e. \tag{2}$$

Similarly, $\psi^2(a)=a$ and it follows that ϕ, ψ are 1-1 mappings of A^* onto A^*. From $ba_1b=\phi(a_1)b\psi(a_1)$ and $ba_2b=\phi(a_2)b\psi(a_2)$, we obtain,

$$\begin{aligned} ba_1a_2b &= \phi(a_1)b\psi(a_1)\phi(a_2)b\psi(a_2) \\ &= \phi(a_1)\phi[\psi(a_1)\phi(a_2)]b\psi[\psi(a_1)\phi(a_2)]\psi(a_2). \end{aligned}$$

Also, $ba_1a_2b=\phi(a_1a_2)b\psi(a_1a_2)$, whence,

$$\phi(a_1a_2) = \phi(a_1)\phi[\psi(a_1)\phi(a_2)], \tag{3}$$

$$\psi(a_1a_2) = \psi[\psi(a_1)\phi(a_2)]\cdot\psi(a_2). \tag{4}$$

Since A is Abelian we may interchange a_1 and a_2 in the right-hand sides of (3) and (4) to obtain

$$\phi(a_1a_2) = \phi(a_2)\cdot\phi[\psi(a_2)\cdot\phi(a_1)], \tag{5}$$

$$\psi(a_1a_2) = \psi[\psi(a_2)\cdot\phi(a_1)]\cdot\psi(a_1). \tag{6}$$

Now, suppose that for some $a\neq e$, we have $\psi(a)\neq a$, so that $[\psi(a)]^{-1}a\neq e$, and $d=\phi([\psi(a)]^{-1}a)$ is defined. It follows that $\phi(d) = [\psi(a)]^{-1}a$, or

$$\psi(a)\phi(d) = a. \tag{7}$$

Upon replacing a_1 by a and a_2 by d in (3), (4), (5) and (6) and using (7), we obtain

$$\phi(ad) = \phi(a)\cdot\phi(a), \tag{8}$$

$$\psi(ad) = \psi(a)\cdot\psi(d), \tag{9}$$

$$\phi(ad) = \phi(d)\cdot\phi[\psi(d)\cdot\phi(a)], \tag{10}$$

$$\psi(ad) = \psi[\psi(d)\phi(a)]\cdot\psi(a). \tag{11}$$

Comparison of (9) and (11) yields,

$$\psi(d) = \psi[\psi(d)\cdot\phi(a)],$$

or

$$d = \psi(d)\phi(a).$$

Replacing $\psi(d)\phi(a)$ by d in (10), we obtain

$$\phi(ad) = \phi(d)\cdot\phi(d). \tag{12}$$

Comparing (8) and (12) we obtain $[\phi(a)]^2=[\phi(d)]^2$, or $(\phi(a)[\phi(d)]^{-1})^2 = e$.

In Case 1, we note that $a\neq e$ implies $\psi(a)\neq a$. For otherwise bab

$=\phi(a)ba$, from which it follows that $ba=\phi(a)bab=[\phi(a)]^2ba$, or $[\phi(a)]^2=e$, which is not possible, since A contains no element of order 2. Thus, we have shown that $a\neq e$ implies the existence of an element d in A, such that $\psi(a)\cdot\phi(d)=a$ and $(\phi(a)[\phi(d)]^{-1})^2=e$. The last equation implies $\phi(a)=\phi(d)$, whence $a=d$, and $\psi(a)\phi(a)=a$. This completes the proof for Case 1.

In Case 2, $t_0=t$, the unique element of order 2 in A. In this case, if $a\neq e$, and $a\neq\phi(t)$ then $\psi(a)\neq a$. Otherwise, we have, as in Case 1, $[\phi(a)]^2=e$, which implies $\phi(a)=t$, or $a=\phi(t)$. Thus, there exists a $d\in A$ such that $\psi(a)\cdot\phi(d)=a$ and $(\phi(a)\cdot[\phi(d)]^{-1})^2=e$. This last equation implies that either $\phi(a)=\phi(d)$ or $\phi(a)=t\phi(d)$. Suppose that $\phi(a)=\phi(d)$; then $a=d$ and we have $\psi(a)\cdot\phi(a)=a$. Consider the two elements of order 2, b and aba^{-1}. Since $a\neq e$, they are distinct, and hence by IV, their product $baba^{-1}$ displaces all elements of $\mathfrak{M}$. We see, however, that $baba^{-1}=\phi(a)b\psi(a)a^{-1}$, and since $\psi(a)\cdot\phi(a)=a$, $\psi(a)a^{-1}=[\phi(a)]^{-1}$, and hence $baba^{-1}=\phi(a)b[\phi(a)]^{-1}$ is conjugate to b. Since b fixes an element of $\mathfrak{M}$, so do its conjugates. This contradiction implies $\phi(a)=t\phi(d)$. We see, then, that for $a\neq e$, $a\neq\phi(t)$,

$$\psi(a)\phi(a) = ta. \tag{13}$$

If $a=\phi(t)$, then $\psi(a)\cdot\phi(a)=\psi(\phi(t))\cdot t=[\psi(t)]^{-1}\cdot t$, by (2). Further, by (1) $[\psi(t)]^{-1}\cdot t=\phi(t^{-1})\cdot t=\phi(t)\cdot t$. Hence (13) holds for all $a\neq e$. It follows that

$$\psi(ta)\cdot\phi(ta) = a$$

for all $a\neq t$. This completes the proof of the lemma.

The next lemma follows readily from the preceding one.

LEMMA 4. *With t_0 defined as in Lemma 3, if $a\in A$, $a\neq t_0$ then there exists an $x\in A$ such that $[\psi(x)]^{-1}\cdot x=a$.*

PROOF. Since $a\neq t_0$, $t_0a\neq e$. Let $x=\phi(t_0a)$. By (2) we have $\psi(x)=\psi(\phi(t_0a))=[\psi(t_0a)]^{-1}$, and hence $[\psi(x)]^{-1}=\psi(t_0a)$. Thus, $[\psi(x)]^{-1}\cdot x=\psi(t_0a)\cdot\phi(t_0a)=a$, by Lemma 3.

PROOF OF THE THEOREM. A group G, satisfying the hypotheses of the theorem is, by the Corollary to Lemma 2, an independent ABA group, with B of order two. As such it can be represented isomorphically as a group of permutations of the right cosets $\{Ax\}$ of A in G. To see that G is isomorphic to the group of affine transformation on a near-field, it is sufficient, in view of Hall's theorem, to show that there is exactly one element $g\in G$ which maps A into Ab and displaces every coset. It is clear that the set of elements of G which map A into Ab are all of the form ab, where a ranges over A. From IV it follows that $t_0 b$ displaces all of the cosets. Suppose then that $a \neq t_0$. By Lemma 4 there exists an $x \in A$ such that $[\psi(x)]^{-1} \cdot x = a$. Let $a' = xa^{-1}$; then $x = a'a$ and we have $[\psi(a'a)]^{-1} \cdot a'a = a$. Hence, $a' = \psi(a'a)$. We then see that the coset Aba' is fixed by ab, thus $(Aba')ab = A\phi(a'a)b\psi(a'a) = Aba'$. That is, of all the elements ab, mapping A into Ab, only $t_0 b$ displaces all of the cosets. Thus, G is isomorphic to the group of affine transformations on a near-field $(K, +, \cdot)$, in which the multiplicative group $K(\cdot)$ is isomorphic to the subgroup A of G, and hence is Abelian. Since a commutative near-field is a field, the proof of the theorem is completed.

References

1. Daniel Gorenstein, *A class of Frobenius groups*, Canad. J. Math. vol. 11 (1959) pp. 39–47.

2. Marshall Hall, *Projective planes*, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 229–277. Correction, ibid. vol. 65 (1949) pp. 473–474.

University of Missouri