A NOTE ON DOUBLY TRANSITIVE GROUPS

PETER LORIMER

(Received 22 November 1965)

W. Feit [1], N. Itô [2] and M. Suzuki [3] have determined all doubly transitive groups with the property that only the identity fixes three symbols. It is of interest to the theory of projective planes to determine whether any of these groups contain a sharply doubly transitive subset (see Definition 1). It is found that if such a group G contains such a subset R then R is a normal subgroup of G, i.e. R is a doubly transitive normal subgroup of G in which only the identity fixes two symbols.

Definition 1. If R is a set of permutations on a set Σ of n symbols, then R is said to be *sharply doubly transitive* on Σ if the identity 1 is a member of R, R contains $n(n-1)$ elements and R is doubly transitive on Σ.

It should be noted that the definition implies that if (a, b) and (c, d) are two pairs of symbols of Σ then there is exactly one $r \in R$ with the properties $r(a) = c$, $r(b) = d$.

In the sequel, G is to be a doubly transitive group on a set Σ of n elements, only the identity of G is to fix three symbols of Σ and G is to contain a sharply doubly transitive subset R.

It is clear that the subset K_a of R which consists of those elements which fix $a \in \Sigma$ contains $n-1$ elements. Also the subset R^* of R which consists of those elements of R which fix no symbol of Σ together with the identity contains n elements.

Let G_a be the subgroup of G consisting of those elements of G which fix the symbol $a \in \Sigma$.

Lemma 1. *If $a \in \Sigma$, then K_a is a subgroup of G and consists of all those elements of G which fix a alone, together with the identity.*

Proof. Consider G_a as a group of permutations on the set $\Sigma' = \Sigma - \{a\}$. G_a is transitive and only the identity fixes two symbols of Σ'. Hence, by Frobenius' Theorem, G_a contains $n-2$ elements which fix no symbol of Σ', and these, together with the identity, form a normal subgroup of H_a. It is clear that this subgroup consists of the elements of K_a.

Lemma 2. *If $r_1, r_2 \in R^*$, then either $r_1 = r_2$ or $r_1^{-1}r_2$ fixes no symbol of Σ.*

LEMMA 3. *If* $r_1, r_2 \in R$, *then either* $r_1 = r_2$ *or both* $r_1^{-1}r_2$ *and* $r_1 r_2^{-1}$ *fix at most one symbol of* Σ.

LEMMA 4. *Suppose* $a, b \in \Sigma$ *and* $a \neq b$. *If* $k_a \in K_a$, *then there exists exactly one* $k_b \in K_b$ *with the property:* $k_a k_b$ *fixes no symbol of* Σ.

PROOF. Suppose $c \in \Sigma$, $c \neq a$, $c \neq b$. Then there exists $k_b \in K$ with the property $k_a^{-1}(c) = k_b(c)$. i.e. $k_a k_b(c) = c$. If $k_a k_b(c) = k_a k_b'(c) = c$, then $k_b(c) = k_b'(c)$ so that $k_b = k_b'$. Hence there are $n-2$ elements k_b of K_b with the property $k_a k_b(c) = c$ for some c in Σ.

K_b contains $n-1$ elements which proves the theorem.

LEMMA 5. *If* $a \in \Sigma$ *then* $R = R^*K_a$.

PROOF. We show firstly that if $r_1 k_1 = r_2 k_2$, $r_i \in R^*$, $k_i \in K_a$ then $r_1 = r_2$, $k_1 = k_2$.

If $r_1 k_1 = r_2 k_2$, then $r_1^{-1} r_2 = k_2 k_1^{-1}$. Now $k_2 k_1^{-1} \in K_a$ so that $r_1^{-1} r_2$ fixes a. Hence, by lemma 2, $r_1 = r_2$ and therefore $k_1 = k_2$.

Hence each element of R^*K_a is represented uniquely in the form rk, $r \in R^*$, $k \in K_a$, so that R^*K_a contains $n(n-1)$ elements.

$R^* \subseteqq R^*K_a$ as $1 \in K_a$.

If $b \in \Sigma$, it follows from lemma 3 that R^*K_a contains $n-1$ elements fixing b and no other symbol. Hence, by lemma 1, $K_b \subseteqq R^*K_a$.

Hence $R \subseteqq R^*K_a$ and even $R = R^*K_a$ as both sets contain $n(n-1)$ elements.

LEMMA 6. *If* a, $b \in \Sigma$, *then* $K_a K_b \subseteqq R$.

PROOF. If $k_a k_b \in K_a K_b$ and $k_a k_b$ fixes a symbol of Σ, then, by lemma 3, $k_a k_b$ fixes exactly one symbol of Σ so that, by lemma 1, $k_a k_b \in K_c$ for some $c \in \Sigma$. Hence $k_a k_b \in R$.

Now, if k_a is given, there exists unique $k_b \in K_b$ such that $k_a k_b$ fixes no symbol of Σ. But $R = R^*K_b$ so that there exists $h_b \in K_b$ and $r \in R^*$ with the property $k_a = r h_b^{-1}$. Then $r = k_a h_b$ so that, because of the uniqueness of k_b we have $h_b = k_b$. Thus $k_a k_b = r \in R$.

Hence $K_a K_b \subseteqq R$.

LEMMA 7. *If* $a \in \Sigma$, *then* $RK_a = R$.

PROOF. $R = R^*K_a$ so that $RK_a = R^*K_a K_a = R^*K_a$ (as K_a is a subgroup) $= R$.

LEMMA 8. *If* $a \neq b$, $r \in R$, $r \notin K_a K_b$, *then* $r^{-1}K_a r = K_b$.

PROOF. If $r \in K_a K_b$, say $r = k_a k_b$, then $r^{-1} K_a r = k_b^{-1} K_a k_b \neq K_b$.

But $n-1$ elements r of R have the property $r^{-1}K_a r = K_b$ and $K_a K_b$ contains $(n-1)^2$ elements. The result follows.

https://doi.org/10.1017/S1446788700004900 Published online by Cambridge University Press

LEMMA 9. *If a, b, c are three different elements of Σ and $r \in R$, then either $r \in K_a K_b$ or $r \in K_a K_c$.*

PROOF. If $r \notin K_a K_b$ and $r \notin K_a K_c$, then by lemma 8, $r^{-1} K_a r = K_b$ and $r^{-1} K_a r = K_c$ which is a contradiction.

LEMMA 10. *If a, b, c are three different elements of Σ, then $R = K_a K_b K_c$.*

PROOF. By lemma 6 $K_a K_b \subseteqq R$. Thus $K_a K_b K_c \subseteqq R K_c = R$ by lemma 7.
If $r \in R$, then by lemma 9 either $r \in K_a K_b \subseteqq K_a K_b K_c$ or $r \in K_a K_c \subseteqq K_a K_b K_c$.
Hence $R = K_a K_b K_c$.
We can now prove

THEOREM 1. *If G is a doubly transitive group on a set Σ, only the identity fixes three symbols of Σ, and G contains a sharply doubly transitive subset R, then R is a normal subgroup of G.*

PROOF. If Σ contains less than three symbols the theorem is obvious.
Suppose Σ contains three or more symbols and that $a, b, c \in \Sigma$ are all different.
Then, by lemma 10, $R = K_a K_b K_c$. Therefore

$$\begin{aligned} R^2 &= K_a K_b K_c K_a K_b K_c \\ &\subseteqq R K_c K_a K_b K_c \text{ by lemma 6} \\ &= R \text{ by repeated application of lemma 7.} \end{aligned}$$

This proves the theorem.
The following application to projective planes is noted.

THEOREM 2. *Let R be a ternary ring of a projective plane of order n. Then the elements of R may be regarded as a set of permutations on a set Σ of n elements and as such they form a sharply doubly transitive set. Let $G(R)$ be the permutation group generated by R. Then either $G(R) = R$ or $G(R)$ contains a permutation, not the identity, which fixes three symbols of Σ.*

References

[1] W. Feit, 'On a class of doubly transitive permutation groups', *Illinois J. Math.* 4 (1960), 170–186.
[2] N. Itô, 'On a class of doubly transitive permutation groups', *Illinois J. Math.* 6 (1962), 341–352.
[3] M. Suzuki, 'On a class of doubly transitive groups', *Ann. of Math.* 75 (1962), 105–145.

University of Auckland
Auckland, New Zealand