THE DOUBLE TRANSITIVITY OF A CLASS OF PERMUTATION GROUPS

RONALD D. BERCOV

1. Introduction. Certain finite groups H do not occur as a regular subgroup of a uniprimitive (primitive but not doubly transitive) group G. If such a group H occurs as a regular subgroup of a primitive group G, it follows that G is doubly transitive. Such groups H are called B-groups **(8)** since the first example was given by Burnside **(1**, p. 343**)**, who showed that a cyclic p-group of order greater than p has this property (and is therefore a B-group in our terminology).

Burnside conjectured that all abelian groups are B-groups. A class of counter-examples to this conjecture due to W. A. Manning was given by Dorothy Manning in 1936 **(3)**. This class of counter-examples has been generalized by Wielandt, who showed that if H is the direct product of two or more groups of the same order greater than two, then H is not a B-group **(8**, p. 79**)**.

In 1933, Schur **(4)** developed a new method which he used to show that a cyclic group of composite order is a B-group.

In 1935, Wielandt **(6, 8)** used the method of Schur to show that if an abelian group H of composite order has a cyclic Sylow subgroup, then it is a B-group.

In 1937, Kochendörffer **(2)** used the Schur methods to show that if H is the direct product of two cyclic groups of order p^α, p^β respectively where $\alpha > \beta > 0$, then H is a B-group.

This paper is a generalization of these results. Let H be abelian, P a Sylow p-subgroup of H, and a an element of P of maximal order, p^α. Let A be the cyclic group generated by a. Then $H = A \times B \times C$, where $P = A \times B$ and C is of order prime to p. We prove that if $B \neq 1$ is of exponent $p^\beta < p^\alpha$ (with the additional assumption $\alpha \geqslant 3$ if $p = 2$), then either H is a direct product of groups of the same order greater than 2, or else H is a B-group. If $B = 1$, we have by the theorem of Wielandt that H is a B-group unless $C = 1$ and $\alpha = 1$. Thus apart from the case $p = 2$, $\alpha = 2$, $\beta = 1$, the question of whether or not the abelian group H is a B-group is settled unless H is the direct product of two groups of the same exponent.

We might also mention that two classes of non-abelian B-groups are known. Wielandt **(7)** has shown that dihedral groups are B-groups and Scott **(5)** has shown that generalized dicyclic groups are B-groups.

2. Notation, definitions, and theorems from the theory of Schur rings. Let G be a primitive permutation group on the letters $\{1, \ldots, n\}$. Let

Received August 27, 1963 and revised April, 1964. This work was supported by United States Office of Naval Research contract Nonr (G)00100-62.

https://doi.org/10.4153/CJM-1965-047-9 Published online by Cambridge University Press

H be a regular abelian subgroup of G. We denote the image of the letter j under the permutation $g \in G$ by j^g. Since H is regular, there is a unique $h \in H$ for which $1^h = j$. We call this element h_j. The correspondence $j \leftrightarrow h_j$ allows us to regard G as a permutation group on H. To the permutation $g \in G$ (on $\{1, \ldots, n\}$) corresponds the permutation $\binom{h}{h^g}$ (on H) where h^g is the element of H uniquely determined by the formula

$$1^{h^g} = 1^{hg}.$$

We continue to denote the permutation $\binom{h}{h^g}$ by g, and the group of such permutations by G.

Let $R(H)$ be the group ring of H over the rational integers. For

$$\eta = \textstyle\sum_{h \in H} \gamma(h)h \in R(H)$$

and any integer j we put $\eta^{(j)} = \sum_{h \in H} \gamma(h)h^j$. Let

$$|\eta| = |\textstyle\sum_{h \in H} \gamma(h)h| = \sum_{h \in H} \gamma(h).$$

With $K \subseteq H$ we associate the element

$$\overline{K} = \sum_{h \in H} \gamma(h)h \in R(H), \qquad \text{where } \gamma(h) = \begin{cases} 1 & \text{if} \quad h \in K, \\ 0 & \phantom{\text{if}} \quad h \notin K. \end{cases}$$

For $K \subseteq H$, let $|K| = |\bar{K}|$, the number of elements of K. Let $\langle K \rangle$ be the smallest subgroup of H containing K. Let G_1 be the subgroup of G (regarded as a permutation group on H) fixing 1, the identity element of H. Let $\{1\} = T_0, T_1, \ldots, T_k$ be the orbits of G_1, where $T_i \subseteq H$ for $i = 0, \ldots, k$. Let

$$R(H, G_1) = \left\{ \sum_{i=0}^{k} \gamma_i \overline{T_i} \right\}$$

be the additive subgroup of $R(H)$ spanned by the $\overline{T_i}$. Throughout this paper k will denote the number of orbits of G_1 different from $\{1\}$. G is doubly transitive if and only if $k = 1$.

THEOREM 1 (Schur, 1933).
(i) *$R(H, G_1)$ is a subring of $R(H)$.*
(ii) *$\langle T_i \rangle = H$ for $i = 1, \ldots, k$.*
(iii) *$\bar{T}_i^{(j)} = \bar{T}_q$ for appropriate q if $(j, |H|) = 1$.*

DEFINITION 1. *$\eta^{(j)}$ is said to be conjugate to $\eta \in R(H)$ if $(j, |H|) = 1$.*

DEFINITION 2. *If $\eta = \eta^{(j)}$ for all j with $(j, |H|) = 1$, then η is said to be rational.*

DEFINITION 3. *The sum of all distinct conjugates of $\eta \in R(H)$ is called the trace of η and is denoted by* tr η.

tr η is clearly rational and lies in $R(H, G_1)$ whenever η does, by Theorem 1.

DEFINITION 4. *For* $h \in H$, tr $\{h\}$ *is called the elementary trace of* h *and is denoted by* tr h.

Clearly if k has non-zero coefficient in tr h, then tr h = tr k.

By Theorem 1, tr $\overline{T_i}$ is a sum of distinct $\overline{T_q}$. Thus tr $\overline{T_i} = \overline{S_i}$, where

$$S_i = \{t^j | t \in T_i, (j, n) = 1\}.$$

If necessary by renumbering the T_i, we may assume without loss of generality that $S_1, \ldots, S_r$ are distinct and that for any $j > r$ there is an $i \leqslant r$ with $S_i = S_j$. Clearly $S_0 = 1$.

THEOREM 2 (Schur, 1933). *Let*

$$S = \left\{ \sum_{i=0}^{r} \gamma_i \overline{S_i} | \gamma_i \text{ rational integers} \right\}.$$

Then S *is a subring of* $R(H, G_1)$ *all of whose elements are rational.*

Our notation so far has been that of **(8)**. We now introduce further notation.

For $K, L \subseteq H$, let $K - L$ be the set of elements of K not belonging to L. For $K \subseteq H$ let $K^{\#} = K - \{1\}$. For $h \in H$, $K \subseteq H$, let

$$K(h) = \{k \in K \mid k^{-1}h \in K\}.$$

Thus $K(h)$ is the set of those elements of K which "hit" other elements of K in such a way as to contribute to the coefficient of h in $[\bar{K}]^2$, and $|K(h)|$ is this coefficient.

Let $H = A \times B \times C$, where $A = \langle a \rangle$ is cyclic of order p^α, B is of exponent p^β, $0 < \beta < \alpha$, and $(|C|, p) = 1$. Let $u = a^{p^{\alpha-1}}$ and $U = \langle u \rangle$; thus $|U| = p$.

We assume without loss of generality that $u \in T_1 \subseteq S_1$, and we put

$$T = T_1, \qquad S = S_1.$$

By Theorem 2, $[\bar{S}]^2$ is a linear combination of the $\overline{S_i}$ $(i = 0, \ldots, r)$. Thus we have

LEMMA 2.1. $|S(h)| = |S(k)|$ *for* $h, k \in S_i$ $(i = 1, \ldots, r)$.

$h \in H$ has a unique representation of the form $h = a^{sp^\lambda}bc$ where $(s, p) = 1$, $b \in B$, $c \in C$. For $K \subseteq H$ we define K_X, K_Y, K_Z as follows:

$K_X = \{k \in K | \lambda = 0\}$ is the set of all elements of K of order divisible by p^α.

$K_Y = \{k \in K | \lambda \neq 0, |\langle b \rangle| < p^{\alpha-\lambda}\}$ is the set of elements of K with p-part having order less than p^α but larger than the order of the B-component.

$K_Z = \{k \in K || \langle b \rangle| \geqslant p^{\alpha-\lambda}\}$ is the set of elements of K with p-part having order equal to the order of the B-component.

Thus K is the set union of the three disjoint sets K_X, K_Y, K_Z.

For $b \in B$, $K \subseteq H$, let $K^b = \{k \in K | k = a^{sp^\lambda}b^t c$, where $(t, p) = 1\}$, be the set of elements of K whose B component is a power of b with exponent prime to p. We have $(K_X)^b = (K^b)_X$ and denote this set by $K_X{}^b$. For $b \in B$, let C_b be the set of all elements of C which occur as the p'-part of some element of $S_X{}^b$.

We now show that by appropriate choice of a we may assume that C_1 is non-empty.

LEMMA 2.2. *If necessary by changing a (the generator of A) we have C_1 non-empty.*

Proof. By Theorem 1(ii), $\langle T\rangle = H$; hence $\langle S\rangle = H$. Thus S has an element of order divisible by p^α, say $a^s bc$. Now $H = \langle a^s b\rangle \times B \times C$ and since $\exp B < \alpha$ holds, we have $(a^s b)^{p^{\alpha-1}} = u^s$, which is in S since $u \in S$ and $\bar{S}$ is rational.

Henceforth we assume that C_1 is non-empty. We are now in a position to state the two theorems of this paper.

THEOREM A. *Assume that*

1. *G is a primitive group of degree n;*
2. *H is a regular abelian subgroup of G;*
3. *p is a prime dividing n;*
4. *P is a Sylow p-subgroup of H;*
5. *$P = A \times B$, where $A = \langle a\rangle$ is cyclic of order p^α and B is of exponent p^β, $0 \neq \beta < \alpha$;*
6. *$\{1\} = T_0, T_1, \ldots, T_k$ are the orbits of G_1 and $\overline{S_i} = \mathrm{tr}\,\overline{T_i} = \bar{H}^\#$ for $i = 1, \ldots, k$.*

Then G is doubly transitive (i.e. $k = 1$).

THEOREM B. *Let Hypotheses 1–5 of Theorem A hold. In addition if $p = 2$, let $\alpha \geqslant 3$. Then if G is not doubly transitive, there exist $e \geqslant 2$ subgroups H_i of G such that $H = H_1 \times \ldots \times H_e$ and*

$$|H_i| = |H_j| > 2 \qquad \text{for } i, j = 1, \ldots, e.$$

Remark. Schur **(4)** proved what I have called Theorem A for all abelian groups H which are not of prime power order. Thus Theorem A of this paper is new only in the case $C = 1$.

We first prove Theorem A and then devote the greater part of the paper to showing that Hypothesis 6 of Theorem A follows from the hypotheses of Theorem B unless H has the special direct product structure indicated.

3. Proof of theorem A.

We begin by proving a lemma which is of importance also in the proof of Theorem B.

LEMMA 3.1. *Let Hypotheses 1–5 of the above statement of Theorem* A *hold. Let $h \notin (H_X \cup H_Y) - UC$. Let $1 \leqslant j \leqslant p-1$. Then there exists $q \equiv 1 \pmod p$ with $(q, |H|) = 1$ such that*

$$h^q = u^j h.$$

Proof. Let $h = a^{sp^\lambda} bc$, where $(s, p) = 1$, $b \in B$, $c \in C$. Let $|C| = m$ and let s', m' satisfy $s's \equiv 1 \pmod{p^\alpha}$, and $m'm \equiv 1 \pmod{p^\alpha}$. Then it is easily seen that $q = 1 + mm's'jp^{\alpha-\lambda-1}$ has the desired properties.

https://doi.org/10.4153/CJM-1965-047-9 Published online by Cambridge University Press

For the remainder of Section 3 we assume that Hypotheses 1–6 in the above statement of Theorem A hold.

LEMMA 3.2. *$\overline{T_q}$ is conjugate to $\bar{T}$ for $q = 1, \ldots, k$.*

Proof. We have assumed tr $\overline{T_q} = \bar{H}^{\#}$ for $q = 1, \ldots, k$. Thus $T_q \cap U^{\#}$ is non-empty. Let $u^j \in T_q \cap U^{\#}$ and let $l \equiv j(p)$ with $(l, |H|) = 1$. By Theorem 1, $\bar{T}^{(l)}$ is a $\overline{T_i}$. Now since u^j belongs to both T_i and T_q it follows that these orbits are the same and $\overline{T_q} = \bar{T}^{(l)}$.

LEMMA 3.3. *Let $l = |T \cap U^{\#}|$, $n = |H|$.* Then

(i) $k = (p - 1)/l$,

(ii) $|T_q| = (n - 1)/k$ *for* $q = 1, \ldots, k$,

(iii) $|(T_q)_X| = \dfrac{p-1}{p}\dfrac{n}{k}$ *for* $q = 1, \ldots, k$.

Proof. Since each conjugate of $\bar{T}$ has l elements of $U^{\#}$ and $|U^{\#}| = p - 1$, it follows that $\bar{T}$ has $(p - 1)/l$ conjugates; thus $k = (p - 1)/l$. Since $\overline{T_q}$ is conjugate to $\bar{T}$, $|T_q| = |T|$. Moreover,

$$\left| \bigcup_{i=1}^{q} T_q \right| = n - 1$$

since $T_0 = 1$ and the T_q are disjoint. Thus each T_q has order $(n - 1)/k$. Since $\overline{T_q}$ is conjugate to $\bar{T}$, T_q and T have the same number of elements of H_X and T_0 has no such elements. Moreover, $|H_X| = ((p - 1)/p)|H|$. Thus we have

$$|(T_q)_X| = \frac{1}{k}\frac{p-1}{p} n.$$

LEMMA 3.4. *The coefficient of u^j in $\bar{T}\bar{T}^{(-1)}$ is $\geqslant |T_X|$ for $j = 1, \ldots, p - 1$.*

Proof. By Lemma 3.1 for $x \in T_X$, there is a $q \equiv 1 \pmod p$ with $(q, n) = 1$ such that $u^{-j}x$ has non-zero coefficient in $\bar{T}^{(q)}$. By Theorem 1, $\bar{T}^{(q)} = \overline{T_i}$ for some i. But $u^q = u$ since $q \equiv 1 \pmod p$. Thus u belongs to both T and T_i, and $T = T_i$. We conclude that $u^{-j}x \in T$. Thus $x(u^j x^{-1})$ contributes to the coefficient of u^j in $\bar{T}\bar{T}^{(-1)}$ for all $x \in T_X$, so this coefficient must be $\geqslant |T_X|$.

LEMMA 3.5. *The coefficient of $h \in H$ in $\bar{T}\bar{T}^{(-1)}$ is $\geqslant |T_X|$.*

Proof. By Theorem 1, $\bar{T}^{(-1)} \in R(H, G_1)$ holds and

$$\overline{T}\,\overline{T}^{(-1)} = \sum_{i=0}^{k} \gamma_i \overline{T_i}.$$

Since each T_i has an element of $U^{\#}$ and each element of $U^{\#}$ has coefficient $\geqslant |T_X|$, we have $\gamma_i \geqslant |T_X|$ for $i = 1, \ldots, k$. Clearly $\gamma_0 = |T| \geqslant |T_X|$, and $h \in H$ belongs to some T_i.

THEOREM A. $k = 1$.

Proof. By Lemma 3.5 we have that

$$|\bar{T}\bar{T}^{(-1)}| = |T|^2 \geqslant |T_X||H|.$$

By Lemma 3.3 we have

$$|T| = (n-1)/k$$

and

$$|T_X| = \frac{p-1}{p}\frac{n}{k}.$$

Thus we have

$$\left(\frac{n-1}{k}\right)^2 \geqslant \frac{p-1}{p}\frac{n}{k}n > \frac{p-1}{p}\frac{(n-1)^2}{k}$$

and

$$k < \frac{p}{p-1} \leqslant 2.$$

Since k is a positive integer, it follows that $k = 1$ and Theorem A is proved.

4. Proof of Theorem B. Throughout Section 4 we assume the hypotheses of Theorem B. We begin with two important lemmas.

LEMMA 4.1. *Let $R \subseteq H$ such that $\bar{R}$ is rational. Then*

$$(R_X \cup R_Y) - u^jC \subseteq R(u^j) \qquad \textit{for } j = 1, \ldots, p-1.$$

Proof. Let $h \in (R_X \cup R_Y) - u^jC$. By Lemma 3.1 if $h \notin UC$, there exists q prime to $|H|$ such that $h^q = u^{-j}h$. For $h = u^ic$, $i \neq j$ (and $0 < i \leqslant p-1$), $c \in C$, such a q obviously exists. Now $h^{-q} = h^{-1}u^j \in R$ holds by the rationality of $\bar{R}$. Thus we have $h \in R(u^j)$.

LEMMA 4.2. *Let $x \in H_X$ and let $R \subseteq H$ such that $\bar{R}$ is rational. Let $1 \leqslant j \leqslant p-1$. Then if h belongs to $R(x) - R(u^j)$, the element $u^jh^{-1}x$ belongs to $R(u^j) - R(x)$.*

Proof. Let $h, h^{-1}x \in R$. If $h \notin R(u^j)$ we have by Lemma 4.1 that $h \in R_Y \cup R_Z$. $h^{-1}x$ therefore lies in R_X. We may now conclude by Lemma 3.1 that $u^jh^{-1}x \in R_X$ holds, and Lemma 4.1 now tells us that $u^jh^{-1}x \in R(u^j)$ holds. We now assume that $u^jh^{-1}x \in R(x)$. This means that $(u^jh^{-1}x)^{-1}x = u^{-j}h \in R$ and by the rationality of $\bar{R}$ we would have $u^jh^{-1} \in R$. This contradicts $h \notin R(u^j)$. Thus we have $u^jh^{-1}x \in R(u^j) - R(x)$.

LEMMA 4.3. *Let $x \in H_X$ and let $R \subseteq H$ such that $\bar{R}$ is rational. Let $1 \leqslant j \leqslant p-1$ and $|R(x)| = |R(u^j)|$. Let $k \in R(u^j) - R(x)$. Then*

(i) $k \in H_X$,

(ii) $u^{-j}k \in R(x)$,

(iii) $k^{-1}x \in H_Z \cup (u^{-j}C)$.

https://doi.org/10.4153/CJM-1965-047-9 Published online by Cambridge University Press

Proof. By Lemma 4.2, $h \to u^j h^{-1}x$ is a 1–1 map of $R(x) - R(u^j)$ into $R(u^j) - R(x)$. Since $|R(x)| = |R(u^j)|$, this map must be onto $R(u^j) - R(x)$. Thus there exists $h \in R(x) - R(u^j)$ such that

$$k = u^j h^{-1}x.$$

Because of Lemma 4.1 we may conclude from $h \notin R(u^j)$ that $h \notin H_X$. Thus $k = u^j h^{-1}x \in H_X$ holds. Moreover, $u^{-j}k = h^{-1}x \in R(x)$ holds since $(h^{-1}x)^{-1}x = h \in R$. By Lemma 4.1, $h \in R_Z \cup (u^j C)$ holds since $h \notin R(u^j)$. Therefore $k^{-1}x = u^{-j}h$ belongs to H_Z unless $h \in C$, in which case we have $k^{-1}x \in u^{-j}C$.

LEMMA 4.4. *Let $x \in S_X$, $1 \leqslant j \leqslant p - 1$, and $k \in S(u^j)$. Then $k^{-1}x \in S$ holds whenever any one of the following four conditions are satisfied:*

(i) $k \notin H_X$,

(ii) $u^{-i}k \notin S(x)$ *for some i such that* $1 \leqslant i \leqslant p - 1$,

(iii) $k^{-1}x \notin H_Z \cup (uC)$,

(iv) $k^{-1}x \notin H_Z$ *and* $p \neq 2$.

Proof. $\bar{S}$ is rational and $|S(x)| = |S(u^i)|$ for $i = 1, \ldots, p - 1$ by Lemma 2.1. If $k^{-1}x \notin S$ we have $k \in S(u^j) - S(x)$. Thus $k \in H_X$ by Lemma 4.3 and $k \in S(u^i) - S(x)$ by Lemma 4.1 for $i = 1, \ldots, p - 1$. Thus we have by Lemma 4.3 that

(i) $k \in H_X$,

(ii) $u^{-i}k \in S(x)$, $i = 1, \ldots, p - 1$,

(iii) $k^{-1}x \in H_Z \cup (u^{-i}C)$, $i = 1, \ldots, p - 1$.

If p is odd we cannot have $k^{-1}x \in u^{-i}C$ for all $i = 1, \ldots, p - 1$ and we conclude that $k^{-1}x \in H_Z$.

Remark. Lemma 4.4 allows us to conclude that certain elements $k^{-1}x$ lie in S. This will enable us to determine S and in the case $S \neq H^{\#}$ we will be able to get information about the structure of H from S.

LEMMA 4.5. *Let $c \in C_1$, the set of elements $d \in C$ for which some element $a^q d$ belongs to S, where $(q, p) = 1$. Then*

(i) $S_X^1 = A_X C_1$,

(ii) $S_Y^1 = A_Y C_1 c$ *if* $p \neq 2$,
$S_Y^1 - uC = (A_Y - \{u\})C_1 c$ *if* $p = 2$.

Proof. Since $\overline{A_X} = \operatorname{tr}(a)$ and for $d \in C_1$, $\operatorname{tr} ad = \operatorname{tr} a \operatorname{tr} d$, it is immediate from the definition of C_1 that $S_X^1 = A_X C_1$.

For $d \in C_1$, $(s, p) = 1$, $0 < \lambda \leqslant \alpha - 1$ we have $k = a^{1-sp^\lambda} d \in S(u^j)$ by Lemma 4.1, and $x = ac \in S_X$. Moreover,

$$k^{-1}x = (a^{1-sp^\lambda}d)^{-1}ac = a^{sp^\lambda}d^{-1}c.$$

If $p \neq 2$ or $\lambda \neq \alpha - 1$, Lemma 4.4 implies $a^{sp^\lambda}d^{-1} c \in S$. If $p = 2$, $\lambda = \alpha - 1$, we have $a^{sp\lambda} d^{-1} c \in uC$. But $C_1 = \{d^{-1} | d \in C_1\}$ since $\bar{S}$ is rational. Thus we have

$$S_Y^1 \supseteq A_Y C_1 c \qquad \text{if } p \neq 2$$

and

$$S_Y^1 \supseteq (A_Y - u)C_1 c \qquad \text{in any case.}$$

Now let $yd \in S_Y^1 - UC$, $y \in A$, $d \in C$. By Lemmas 4.1 and 4.4, $y^{-1}ad^{-1}c \in S$ holds. This is clearly an element of $A_X C$. Hence from the definition of C_1 we conclude that $d^{-1}c$, and hence dc^{-1}, belongs to C_1 and d belongs to $C_1 c$. Thus $S_Y^1 - UC \subseteq (A_Y - U)C_1 c$. If $p = 2$, this completes the demonstration that

$$S_Y^1 - UC = (A_Y - u)C_1 c.$$

If $p \neq 2$, let $yd \in U^\# C \cap S$, say $y = u^i$, $d \in C$. Then if $u^j \neq u^i$, $u^j \in U^\#$, we have $u^{i-j}d \in S$ since $\bar{S}$ is rational. Thus we have $u^{j-i}d^{-1} \in S$ and $u^i d \in S(u^j)$. By Lemma 4.4 we have that $(u^i d)^{-1}ac \in S$. We conclude, as before, since this is an element of $A_X C$, that $d^{-1}c$ and dc^{-1} are in C_1 and d is in $C_1 c$. Thus we have $U^\# C \cap S \subseteq U^\# C_1 c$. This completes the demonstration, in the case $p \neq 2$, that $S_Y^1 = A_Y C_1 c$.

LEMMA 4.6. *C_1 is a subgroup of C.*

Proof. C_1 is non-empty by Lemma 2.2. We consider two cases.

Case 1. $p \neq 2$. Let $c, d \in C_1$. We have $a^2 c$, $ad \in S_X^1$, and $(ad)^{-1}a^2 c = ad^{-1}c \notin H_Z$. We conclude by Lemmas 4.4 and 4.5 that $d^{-1}c \in C_1$.

Case 2. $p = 2$. The additional hypothesis $\alpha \geqslant 3$ allows us to conclude in this case that $a^2 \notin U$, and Lemma 4.5(ii) tells us that $a^2 C_1 c \subseteq S_Y^1 - uC = (A_Y - u)C_1 d$ for $c, d \in C_1$. We conclude that $C_1 c = C_1 d = C_1^2$, $C_1 d^2 = C_1^3$ for $d \in C_1$, and $|C_1| = |C_1^3|$. But $C_1 \subseteq C_1^3$ since $d^{-1} \in C_1$ holds for $d \in C_1$; thus $C_1 = C_1^3$ and $C_1^2 = (C_1^2)^2$. C_1^2 is therefore a subgroup of C containing $|C_1|$ elements. Since C is a p-complement and we are considering the case $p = 2$, we conclude from $|C_1| = |C_1^2|$ and the rationality of $\bar{S}$ that $C_1^2 = \{d^2 | d \in C_1\} = C_1$.

LEMMA 4.7. $S^1 - C = A^\# C_1$ *if* $p \neq 2$. $S^1 - UC = (A^\# - u)C_1$ *if* $p = 2$.

Proof. See Lemmas 4.5 and 4.6.

LEMMA 4.8. *Let* $1 \neq b \in B$ *such that* S_X^b *is non-empty. Then*

(i) $S_X^b = P_X^b C_b$,

(ii) $S_Y^b \supseteq P_Y^b C_b$,

(iii) $|S_Z^b \cap P_Z^b C_b| \geqslant \dfrac{p-1}{p} |P_Z^b C_b|$,

where C_b is the set of elements of C which occur as p'-part of some element of S_X^b.

Proof. Let $x \in P_X^b C_b$, say $x = a^s b^t c$, where $(s, p) = (t, p) = 1$, $c \in C_b$. By the definition of C_b, some element $a^e b^l c$ must lie in S with $(e, p) = (l, p) = 1$

and since $\bar{S}$ is rational, there is an element $a^q b^t c \in S_X$. If $q = s$ we have $x \in S$. If $a^{q-s} \in U^\#$, we have by Lemma 4.1 that $x = a^{s-q}a^q b^t c \in S$. If $a^{q-s} \in A - U$ we have $a^{q-s} \in S(u)$ by Lemma 4.7, and

$$(a^{q-s})^{-1}(a^q b^t c) = x \notin H_Z \cup (UC).$$

We conclude by Lemma 4.4 that $x \in S$. Thus in any case we have $x \in S$ and $P_X{}^b C_b \subseteq S_X{}^b$. But, by the definition of C_b, no elements outside $P_X{}^b C_b$ can belong to $S_X{}^b$.

Now let $y \in P_Y{}^b C_b$. By what we have just shown, $y^{-1}a \in S_X{}^b$ holds, and by Lemma 4.7, $a \in S$ holds. Moreover, $(y^{-1}a)a^{-1} \notin H_Z \cup (UC)$ since $b \neq 1$ and $y \in H_Y$. Thus again by Lemma 4.4 we have $y \in S$ and $P_Y{}^b C_b \subseteq S_Y{}^b$.

Now let $z \in P_Z{}^b C_b$. Again we have $z^{-1} a \in S_X{}^b$ and for $z = (z^{-1}a)^{-1}a \notin S$ we have by Lemma 4.4 that the $p - 1$ elements $u^i z^{-1}a$ lie in $S(a)$ for $i = 1, \ldots, p - 1$. This means that the elements $u^i z$ must lie in S and they clearly lie in $P_Z{}^b C_b$ since $b \neq 1$.

Thus with each $z \in P_Z{}^b C_b - S_Z{}^b$ we associate the $p - 1$ elements of $U^\# z$ which must belong to $S_Z{}^b$. It follows that

$$|S_Z{}^b \cap P_Z{}^b C_b| \geqslant \frac{p-1}{p} |P_Z{}^b C_b|.$$

LEMMA 4.9. *If $S_X{}^b$ is non-empty, then $C_b = C_1$.*

Proof. Let $c \in C_1$, $d \in C_b$. $a^{-2} c \in S_X$ holds if $p \neq 2$ and $a^{-2} c \in S_Y - uC$ if $p = 2$. Moreover, $a^{-1}bd \in S_X{}^b$ holds by Lemma 4.8. Thus since

$$(a^{-2}c)^{-1}(a^{-1}bd) = abc^{-1}d \in H_X,$$

we have by Lemma 4.4 that $abc^{-1}d \in S$ holds. Thus we have $c^{-1}d \in C_b$ for all $c \in C_1$ and $C_1 d \subseteq C_b$.

Similarly, for $c, d \in C_b$ we have $a^{-2}bc \in S_X{}^b$ if $p \neq 2$, $a^{-3}bc \in S_X{}^b$ if $p = 2$, and $a^{-1}bd \in S_X{}^b$ in either case.

Again by Lemma 4.4 we have, since $(a^{-2}bc)^{-1}a^{-1}bd = ac^{-1}d \in H_X$ and

$$(a^{-3}bc)^{-1}a^{-1}bd = a^2c^{-1}d \in H_Y - uC$$

if $p = 2$, that $ac^{-1}d \in S$ if $p \neq 2$, and $a^2c^{-1}d \in S$ if $p = 2$.

In either case, we have by Lemma 4.7 that $c^{-1}d \in C_1$ and $c \in C_1 d$; hence $C_b \subseteq C_1 d$. It follows that $C_b = C_1 d$ for all $d \in C_b$. We again consider two cases.

Case 1. $p \neq 2$. By Lemmas 4.8 and 4.4 we again have $a^{-2}b^{-2}d^{-1}, a^{-1}b^{-1}d \in S_X{}^b$ and $(a^{-2}b^{-2}d^{-1})^{-1}(a^{-1}b^{-1}d) = abd^2 \in S_X$. We therefore have $d^2 \in C_b = C_1 d$, $d \in C_1$, and $C_b = C_1 d = C_1$.

Case 2. $p = 2$. For $d \in C_b$, we have $d^{-1} \in C_b = C_1 d$, and $d^2 \in C_1$. Since C_1 is a subgroup of order prime to 2, it follows that $d \in C_1$ and $C_b = C_1 d = C_1$.

We now introduce further notation which we use for the remainder of the paper. We denote by B_1 the set of $b \in B$ for which $S_X{}^b$ is non-empty, and we put $K = AB_1 C_1$.

LEMMA 4.10.
(i) $K_X = S_X$;
(ii) $K_Y \subseteq S_Y$ *if* $p \neq 2$,
$K_Y - uC \subseteq S_Y$ *if* $p = 2$;
(iii) $|K_Z{}^b \cap S| \geqslant \dfrac{p-1}{p} |K_Z{}^b|$ *for* $1 \neq b \in B_1$.

Proof. See Lemmas 4.8 and 4.9.

LEMMA 4.11. *Let* $1 \leqslant q \leqslant p^\alpha - 1$, $c \in C_1$, *and if* $p = 2$, *let* $p^{\alpha-1} \nmid q$. *Then*
(i) $S(a^q c) \subseteq K$,
(ii) $|S(a^q c)| = |K| - 2|K - S|$.

Proof. $[\bar{S}]^2 = [\overline{S_X}]^2 + 2\overline{S_X}[\overline{S_Y} + \overline{S_Z}] + [\overline{S_Y} + \overline{S_Z}]^2$. Clearly the contribution to $|S(a)|$ comes only from the first two terms. Since $k^{-1}a \in K$ holds for $k \in K$, and S_X lies entirely inside K, we see that the full contribution to $|S(a)|$ comes from $[\bar{K}]^2$; thus $S(a) \subseteq K$. Now it follows from Lemma 4.10 that all elements h of $K - S$ lie outside of K_X and satisfy $h^{-1}a \in K_X \subseteq S$. This means that $|S(a)|$ is as small as possible since $k \in S$ does not belong to $S(a)$ precisely when $k^{-1}a \notin S$ holds, and as many elements of $K \cap S$ as possible have this property, namely one for every element of $K - S$. We therefore have that $|S(a)| = |K| - 2|K - S|$. It is easy to see that the contribution of $[\overline{K - S}]^2$ to $|S(a^q c)|$ is at least $|K| - 2|K - S|$ since $k^{-1} a^q c$ belongs to K for all $k \in K$. But $|S(a)| = |S(a^q c)|$. This completes the proof.

LEMMA 4.12. *Let* $1 \neq b \in B_1$, *such that* $P_Y{}^b$ *is empty. Then*

$$|S_Z{}^b \cap K| > \tfrac{1}{2}|K_Z{}^b|.$$

Proof. By Lemma 4.10 we have

$$|S_Z{}^b \cap K| \geqslant \frac{p-1}{p} |K_Z{}^b|.$$

We assume that $p = 2$, and $|S_Z{}^b \cap K| = \frac{1}{2}|K_Z{}^b|$, since if not, there is nothing to prove. Since $P_Y{}^b$ is empty, we must have $|\langle b \rangle| = 2^{\alpha-1}$.

By Lemma 4.11 we have for $q = 2, 6$, and $z \in K_Z{}^b$ that z and $a^{-q}z$ cannot both lie outside of K since $|S(a^q)|$ would then be too large. Thus with each $z \in K_Z{}^b - S$ we have associated two elements, $a^{-2}z$ and $a^{-6}z$, of $K_Z{}^b \cap S$. It follows that

$$|K_Z{}^b \cap S| \geqslant \tfrac{2}{3}|K_Z{}^b| > \tfrac{1}{2}|K_Z{}^b|.$$

LEMMA 4.13. *K is a subgroup of H.*

Proof. $K = AB_1 C_1$, where A and C_1 are subgroups of H. It suffices to show that B_1 is a subgroup of H. We have $1 \in B_1$ and since $S^b = S^{b^{-1}}$, it follows that b^{-1} is in B_1 for $b \in B_1$. Now let $1 \neq b_1, b_2 \in B_1$. We shall show that $b_1^{-1} b_2 \in B_1$

holds. If $P_Y^{b_1}$ is non-empty, we have $a^p b_1 \in S$ by Lemmas 4.8 and 4.9 and $(a^p b_1)^{-1} x \in S$ for $x \in S_X$ by Lemmas 4.1 and 4.4. Since $ab_2 \in S_X$ also holds (again by Lemmas 4.8 and 4.9), we have by Lemmas 4.1 and 4.4 that $(a^p b_1)^{-1} ab_2 = a^{1-p} b_1^{-1} b_2$ lies in S; hence $b_1^{-1} b_2$ is in B_1.

If $P_Y^{b_1}$ is empty, we have by Lemma 4.12 that at least one pair $\{z, z^{-1}u\}$ from $K_Z^{b_1}$ must belong to S. Then $\{z^s, z^{-s} u^s\} \subseteq S$ will hold for $(s, |H|) = 1$ and for an appropriate such s we get an element $z^s = a^q b_1 c \in S(u^s)$, where $q \equiv 0 \pmod{p}$, $c \in C_1$. By an argument similar to the one just given we get $ab_2 c \in S_X$, $z^{-s} ab_2 c = a^{1-q} b_1^{-1} b_2 \in S$, and $b_1^{-1} b_2 \in B_1$.

Lemma 4.14. $K^\# \subseteq S$.

Proof. Assume the contrary. Let $1 \neq k \in K - S$. k must belong to $K_Y \cup K_Z$ since $K_X \subseteq S$, and to some S_i, $i \geqslant 2$. Since $\langle S_i \rangle = H$ by Theorem 1, S_i has an element $x \in H_X$. By Lemma 2.1, we have $|S(x)| = |S(k)|$. As before we have

$$[\overline{S}]^2 = [\overline{K_X}]^2 + 2\overline{K_X}[\overline{S_Y} + \overline{S_Z}] + [\overline{S_Y} + \overline{S_Z}]^2.$$

Since $x \notin K_X$, the first term does not contribute to $|S(x)|$ (because K is a subgroup). Since $x \in H_X$, the third term does not contribute. Thus $|S(x)| = 2|K_X \cap S(x)|$. Let $h \in K_X \cap S(x)$. Then $h^{-1} x \in S - K$ holds since $x \notin K$.

If $a^q h \in K_X \cap S(x)$ held, we would have $a^{-q} h^{-1} x \in S - K$. Hence $a^q hx^{-1} \in S - K$ and $h^{-1} x \in S(a^q)$, which cannot happen by Lemma 4.11 unless $a^q = 1$ (or $a^q = u$ if $p = 2$) since then $S(a^q) \subseteq K$ holds. It follows for $h \in K_X \cap S(x)$ that $a^q h \in K_X - S(x)$ for $q = jp^{\alpha-1}$ and $j = 1, \ldots, p-1$ if $p \neq 2$, and for $q = 2, 6$ if $p = 2$. Thus only one of p elements of K_X can belong to $S(x)$ if $p \neq 2$ and one of three elements if $p = 2$, since $a^2 h_1 = a^6 h_2$ cannot occur for $h_1, h_2 \in K_X \cap S(x)$ by Lemma 4.4 if $\alpha = 3$ and by the above argument if $\alpha \neq 3$. In any case we have

$$|S(x)| \leqslant 2|K_X \cap S(x)| \leqslant 2.\tfrac{1}{3}|K_X| < |K_X|.$$

Now for $h \in K_X$, $h^{-1}k \in K_X$ holds since $k \in K_Y \cup K_Z$. Thus $K_X \subseteq S(k)$ and $|K_X| \leqslant |S(k)| = |S(x)|$, contradicting the above inequality. Thus our assumption $k \in S_i$, $i \geqslant 2$ is wrong and we conclude that $K^\# \subseteq S$.

Lemma 4.15. *Let $h \in H^\# - S$. Then $|S(h)| \leqslant 2$.*

Proof. Let $h \in S_i$, $i \geqslant 2$. As above, let $x \in (S_i)_X$. We again have $|S(x)| = |S(h)|$ and $|S(x)| = 2|K_X \cap S(x)|$. Let $k_1, k_2 \in K_X \cap S(x)$. Then $k_1^{-1} x, k_2^{-1} x \in S - K$ since $x \notin K$. Thus $(k_1^{-1} x)^{-1} \in S - K$ holds and $k_1 k_2^{-1}$ has non-zero coefficient in $[\overline{S - K}]^2$. Clearly $[\overline{K^\#}]^2 = |K^\#| \cdot \overline{1} + [|K^\#| - 1]\overline{K^\#}$. By Lemma 4.11 we have $|S(a)| = |K| - 2$ and if $k_1 \neq k_2$, the coefficient of $k_1 k_2^{-1}$ in $[\overline{K^\#}]^2$ is $|K| - 2$. Thus since we have a further contribution to $k_1 k_2^{-1}$ from $[\overline{S - K}]^2$, we have a contradiction to $|S(a)| = |S(k_1 k_2^{-1})|$ unless $k_1 = k_2$. Thus $|K_X \cap S(x)| \leqslant 1$ and $|S(h)| = |S(x)| = 2|K_X \cap S(x)| \leqslant 2$.

Lemma 4.16. *Let $h \in S$, $h^2 \neq 1$. Then $h^2 \in S$.*

https://doi.org/10.4153/CJM-1965-047-9 Published online by Cambridge University Press

Proof. $|S(h)| = |S(a)| \geqslant |K| - 2 \geqslant |A| - 2 \geqslant 6$. Thus we may choose $x, y \in S(h)$ with $x \notin \{y, y^{-1}h\}$. Then

$$\{x^{-1}, y^{-1}h, y^{-1}, x^{-1}h\} \subseteq S(x^{-1}y^{-1}h).$$

We have $|S(x^{-1}y^{-1}h)| > 2$ unless $x^{-1} = y^{-1}h$ and $y^{-1} = x^{-1}h$ in which case $x^{-1} = x^{-1}h^2$, contradicting $h^2 \neq 1$. Moreover, $x^{-1}y^{-1}h \neq 1$ since x was assumed different from $y^{-1}h$. Thus we may conclude by Lemma 4.15 that $x^{-1}y^{-1}h \in S$. Since $\{x^{-1}, y^{-1}, h^{-1}, x^{-1}y^{-1}h\} \subseteq S(x^{-1}y^{-1})$ we have by Lemma 4.15 that $x^{-1}y^{-1} = 1$ or $x^{-1}y^{-1} \in S$. If $x^{-1}y^{-1} \in S$ we have $xy \in S$ (because $\bar{S}$ is rational) and $\{x, h, xy, y^{-1}h\} \subseteq S(xh)$. By Lemma 4.15 we conclude that $xh \in S$ unless $xh = 1$. If $x^{-1}y^{-1} = 1$, we have $xh = y^{-1}h \in S$. In any case we have $xh \in S$ unless $xh = 1$. By a similar argument we conclude that $yh \in S$ unless $yh = 1$. If xh and yh are both different from 1, we have $\{h, xh, x^{-1}h, yh, y^{-1}h\} \subseteq S(h^2)$; thus $h^2 \in S$ by Lemma 4.15. If $xh = 1$ we have $h^2 = x^{-1}h \in S$; and if $yh = 1$ we have $h^2 = y^{-1}h \in S$.

LEMMA 4.17. *Let $h \in S$. Then $\langle h\rangle^\# \subseteq S$.*

Proof. If $|\langle h\rangle| = 2$, there is nothing to prove. If $|\langle h\rangle| = 3$, see Lemma 4.16. If $|\langle h\rangle| = 4$, we have $h^2 \in S$ by Lemma 4.16 and $h^3 = h^{-1} \in S$ by the rationality of $\bar{S}$.

We now assume that $|\langle h\rangle| \geqslant 5$. Then we have $h^2, h^4 \in S$ by Lemma 4.16, and $h^3 \in S$ by Lemma 4.15, since $\{h, h^2, h^4, h^{-1}\} \subseteq S(h^3)$.

We now proceed by induction. We assume that $h^i \in S$ for $i = 1, \ldots, m$, where $4 \leqslant m < |\langle h\rangle| - 1$. Then $\{h, h^m, h^2, h^{m-1}\} \subseteq S(h^{m+1})$ and $h^{m+1} \in S$ by Lemma 4.15.

LEMMA 4.18. *Let $h \in S$, and let M be a subgroup of H maximal with respect to being contained in $S \cup \{1\}$ and containing h. Then $M^\# = S(h) \cup \{h\}$.*

Proof. That such an M exists follows from Lemma 4.17. Clearly since $M \subseteq S \cup \{1\}$ is a subgroup and $h \in M$, we have $M^\# \subseteq S(h) \cup \{h\}$. Suppose there exists $x \in S(h) - M$. Then $x^{-1}h \in S(h) - M$. By Lemma 4.17 we have $\langle x\rangle^\#, \langle x^{-1}h\rangle^\# \subseteq S$. We claim that $(\langle x\rangle M)^\# \subseteq S$.

Let $j < |\langle x\rangle|$, $y \in M$, $x^j y \neq 1$. If $x^j \in M$, we have $x^j y \in M^\# \subseteq S$. Suppose now that $x^j \notin M$. If $y \in \langle x\rangle$ we have $x^j y \in \langle x\rangle^\# \subseteq S$. Thus we may assume that $y \notin \langle x\rangle$. If $y = h^{-1}$, we have $x^{-1}h \in S$; hence $xh^{-1} = xy \in S$. If $y \neq h^{-1}$, we have $hy \in M^\# \subseteq S$, $\{x, y, xh^{-1}, hy\} \subseteq S(xy)$ and $|\{x, y, hy\}| = 3$ since $h \neq 1$ and $x \notin M$. Moreover, $xy \neq 1$ since $x \notin M$. Hence we have $xy \in S$ by Lemma 4.15. Now $\{x^j, y, xy, x^{j-1}\} \subseteq S(x^jy)$ and $|\{x^j, y, xy\}| = 3$ since $x \neq 1$ and $y \notin \langle x\rangle$. We conclude by Lemma 4.15 that $x^jy \in S$; thus $(\langle x\rangle M)^\# \subseteq S$, contradicting the maximality of M. We therefore have $S(h) \subseteq M^\#$; thus $S(h) \cup \{h\} \subseteq M^\# \cup \{h\} = M^\#$.

LEMMA 4.19. *Let $x, h, k \in S$ such that $x \in (S(h) \cup \{h\}) \cap (S(k) \cup \{k\})$. Then $S(h) \cup \{h\} = S(k) \cup \{k\}$.*

https://doi.org/10.4153/CJM-1965-047-9 Published online by Cambridge University Press

Proof. By Lemma 4.18 we have $S(h) \cup \{h\} = S(x) \cup \{x\} = S(k) \cup \{k\}$.

LEMMA 4.20. *K is a maximal subgroup in $S \cup \{1\}$.*

Proof. Let M be a maximal subgroup in $S \cup \{1\}$ containing K. Since $a \in K$, we have $|S(a)| \geqslant |M| - 2$. By Lemma 4.11 we have $|S(a)| \leqslant |K| - 2$. It follows that $K = M$.

LEMMA 4.21. *Let $K = H_1, \ldots, H_e$ be a complete set of maximal subgroups in $S \cup \{1\}$. Then $|H_i| = |H_j| > 2$ for $i, j = 1, \ldots, e$.*

Proof. By Lemma 4.18 for $h \in H_i$, $k \in H_j$, we have $H_i = S(h) \cup \{h\}$ and $H_j = S(k) \cup \{k\}$. $h \notin S(h)$, $k \notin S(k)$ since $1 \notin S$. Thus $|H_i| = |S(h)| + 1 = |S(k)| + 1 = |H_j|$ and $|H_1| = |K| \geqslant |A| \geqslant 8$.

LEMMA 4.22. *Let $K = H_1, \ldots, H_e$ as above. Then $H = H_1 \times \ldots \times H_e$.*

Proof. $\langle S \rangle = H_1 \ldots H_e = H$ by Theorem 1. $H_i \cap H_j = 1$ for $i \neq j$ by Lemma 4.19. $h \in H$ can be written in the form

$$h = h_1 \ldots h_e, \qquad h_i \in H_i, \qquad i = 1, \ldots, e.$$

We say that $h \in H$ has "length" t if the number of $h_i \neq 1$ in some such representation of h is t. It suffices to show that no element of length one has length greater than one as well. Suppose the contrary and choose $j > 1$ minimal such that h of length one is also of length j. We have $\bar{S} = \overline{H_1^\#} + \ldots + \overline{H_e^\#}$. Since $|H_i| = |H_j|$ for $i, j = 1, \ldots, e$ we have that in

$$[\bar{S}]^j = \sum_{i=1}^{e} (\overline{H_i^\#})^j + \sum_{i_1 < i_2 \ldots < i_j} \overline{H_{i_1}^\#} \ldots \overline{H_{i_j}^\#} + \sum (\overline{H_{i_1}^\#})^2 \overline{H_{i_2}} \ldots \overline{H_{i_s}}$$

each element of S has the same coefficient in the first term. Because of the minimality of j, each element of S has the same coefficient in the third term as well (since the elements of S are precisely the elements of length one). In the second term h occurs with non-zero coefficient. Since $[\bar{S}]^j$ is a linear combination of the $\overline{S_i}$, a and h have the same coefficient in $[\bar{S}]^j$. Thus a must also be of length j, say $a = x_1 \ldots x_j$, where $x_i \neq 1$ for $i = 1, \ldots, j$ and each x_i is from a different H_s. Since $S_X = K_X = (H_1)_X$, a is not in $H_2 \ldots H_e$ since all elements of $H_2 \ldots H_e$ are of the form $a^{qp}bc$. Thus some x_i, say x_j, is in H_1. Then $ax_j^{-1} = x_1 \ldots x_{j-1}$. If $x_j \neq a$, we have $ax_j^{-1} \in S$ written as an element of length $j - 1$, contradicting the minimality of j unless $j = 2$. If $j = 2$, we have $ax_j^{-1} = x_1$; but x_1 and x_j come from different H_s. If $a = x_j$, we have $x_1 \ldots x_{j-1} = 1$ and $j \neq 2$ since $x_1 \neq 1$. Now $x_{j-1}^{-1} = x_1 \ldots x_{j-2}$ is a word of length one and $j - 2$, contradicting the minimality of j unless $j = 3$, in which case $x_2^{-1} = x_1$, which cannot occur. This completes the proof of Lemma 4.22.

THEOREM B. *G is doubly transitive unless $H = H_1 \times \ldots \times H_e$ where $e > 1$ and $|H_i| = |H_j| > 2$ for $i, j = 1, \ldots, e$.*

Proof. Let $H_1, \ldots, H_e$ be as in Lemmas 4.21 and 4.22. If $e > 1$, there is nothing to prove. If $e = 1$, we have $S = H_1^{\#} = H^{\#}$. This means that $r = 1$ in the notation of Theorem 2, and Hypothesis 6 of Theorem A is satisfied. Thus G is doubly transitive.

References

1. W. Burnside, *Theory of groups of finite order*, 2nd ed. (Cambridge, 1911).
2. R. Kochendörffer, *Untersuchungen über eine Vermutung von W. Burnside*, Schriften math. Sem. Inst. angew. Math. Univ. Berlin, *3* (1937), 155–180.
3. D. Manning, *On simply transitive groups with transitive abelian subgroups of the same degree*, Trans. Amer. Math. Soc., *40* (1936), 324–342.
4. I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*, Sitzungsberichte Preuss. Akad. Wiss., phys.-math. Kl. (1933), 598–623.
5. W. R. Scott, *Solvable factorizable groups*, Illinois J. Math., *1* (1957), 389–394.
6. H. Wielandt, *Zur Theorie der einfach transitiven Permutationsgruppen*, Math. Z., *40* (1935), 582–587.
7. ——— *Zur Theorie der einfach transitiven Permutationsgruppen, II*, Math. Z., *52* (1949), 384–393.
8. ——— *Permutation groups*, Lectures at the University of Tübingen, 1954–55, prepared by J. Andre, translated from the German by R. Bercov (Cal. Tech., 1962).

Cornell University and
University of Alberta, Edmonton