ON SIMPLY TRANSITIVE PRIMITIVE PERMUTATION GROUPS

R. D. BERCOV

I. Introduction. In (**1**) we considered finite primitive permutation groups G with regular abelian subgroups H satisfying the following hypothesis:

(*) $H = A \times B \times C$, where A is cyclic of prime power order $p^\alpha \neq 4$, B has exponent $p^\beta < p^\alpha$, and C has order prime to p.

We remark that an abelian group fails to satisfy (*) (apart from the minor exception associated with the prime 2) if and only if it is the direct product of two subgroups of the same exponent.

We showed in (**1**) that such a group G is doubly transitive unless it is the direct product of two or more subgroups each of the same order greater than 2. This was done by showing that (in the terminology of (**3**)) the existence of a non-trivial primitive Schur ring over H implies such a direct decomposition of H.

It is our aim here to investigate these non-trivial primitive Schur rings in order to obtain information about the orbits of stabilizers of simply transitive primitive permutation groups.

II. Schur rings and permutation groups. Throughout we use the following notation. The number of elements of a subset K of H is $|K|$; 1 is the identity element of H, $K^\#$ the set difference $K - \{1\}$; $\bar{K}$ is the element $\sum_{k \in K} k$ of the group ring of H over the integers; the order of an element $h \in H$ is $o(h)$; and G_δ is the stabilizer of δ in G.

Definition 2.1. A Schur ring (S-ring) $\mathcal{S}$ over a group H is a subring of the group ring of H over the integers such that for some partition of H into subsets $\{1\} = S_0, S_1, \ldots, S_k$, called basis elements, we have:

(i) for each i there exists j with $S_j = \{h^{-1} | \ h \in S_i\}$, and

(ii) a group ring element x belongs to $\mathcal{S}$ if and only if for every i, all elements of S_i have the same coefficient in x.

Definition 2.2. An S-ring is *primitive* if S_i generates H for all $i \geqq 1$.

Definition 2.3. An S-ring over an abelian group H is *rational* if for every i and every integer q prime to $|H|$, we have $S_i = \{h^q | \ h \in S_i\}$.

Definition 2.4. $\mathcal{S}$ is *trivial* if it has the basis elements $S_0 = \{1\}$, $S_1 = H^\#$.

The following theorem which gives the basic connection between S-rings and permutation groups is due to Schur (**2**).

Received January 17, 1968 and in revised form July 14, 1969.

THEOREM 2.1. *Let G be a permutation group with regular subgroup H, $\{\delta\} = T_0, T_1, \ldots, T_k$ the orbits of G_δ, and $S_i = \{h \in H | \delta^h \in T_i\}$. Then the set $\mathcal{S}$ of all elements of the group ring of H which have constant coefficient on each S_i is an* S*-ring over H. Moreover,*

(i) *$\mathcal{S}$ is primitive if and only if G is a primitive group, and*

(ii) *$\mathcal{S}$ is trivial if and only if G is doubly transitive.*

Throughout, H will denote an abelian group satisfying (*) and for $K \subseteq H$ we use the unique representation $k = abc$ with $a \in A$, $b \in B$, $c \in C$ to put (as in (**1**)) $K_X = \{k \in K | o(a) = p^\alpha\}$, $K_Y = \{k \in K | o(b) < o(a) < p^\alpha\}$ and $K_Z = \{k \in K | o(b) \geqq o(a)\}$. Thus K is the disjoint union of K_X, K_Y, and K_Z.

Although the results of (**1**) are stated in the language of permutation groups rather than S-rings, the following is proved there.

THEOREM 2.2. *Let $\mathcal{S}$ be a non-trivial rational primitive* S*-ring over an abelian group H satisfying (*). Then H can be expressed as the direct product of two or more subgroups H_i, each of the same order greater than 2, such that A is contained in H_1, the union of the $H_i^\#$ is a basis element, and $(H_i^\#)_X$ is empty for $i \geqq 2$.*

III. The rational case. We assume now that $\mathcal{S}$ is a non-trivial rational primitive S-ring over an abelian group H with basis elements

$$\{1\} = S_0, S_1, \ldots, S_k$$

and that H satisfies the slightly stronger version of (*) obtained by replacing the hypothesis $p^\alpha \neq 4$ by $\alpha > \beta + 1$ if $p = 2$. By Theorem 2.2 we have $H = H_1 \times \ldots \times H_d$ with $|H_i| = |H_j| > 2$ for all i, j. We number the basis elements so that

$$(\dagger) \qquad S_1 = \bigcup_{i=1}^{d} H_i^\#.$$

Definition 3.1. The *length* $l(h)$ of $h \in H$ is the number of non-trivial components in the expression

$$h = \prod_{i=1}^{d} h_i, \qquad h_i \in H_i;$$

i.e. $l(h) = |\{i | h_i \neq 1\}|$.

Definition 3.2. For any permutation σ of $\{1, \ldots, d\}$ and any integer j with $1 \leqq j \leqq d$, we call $H_\sigma{}^j = \prod_{i=1}^{j} H_{\sigma(i)}{}^\#$ the *j-product* associated with σ.

The following lemma follows easily from the rationality of $\mathcal{S}$; see (**1**, Lemmas 3.1 and 4.1).

LEMMA 3.1. *Let S be a basis element of $\mathcal{S}$ and u an element of A of order p. Then*

$$s \in (S_X \cup S_Y) - uC \rightarrow s^{-1}u \in S.$$

This lemma states that all elements of $(S_X \cup S_Y) - uC$ contribute to the coefficient of u in $(\bar{S})^2$. Since A is a subset of S_1, each $x \in (S_1)_X$ must have the

https://doi.org/10.4153/CJM-1969-117-5 Published online by Cambridge University Press

same coefficient in $(\bar{S})^2$ as u. We now make use of this to obtain information about S.

LEMMA 3.2. *Let S and u be as in Lemma* 3.1, $x \in (S_1)_X$, *and* $\{w, w^{-1}u\} \subseteq S$. *Then*

$$wx^{-1} \notin H_Z \cup (uC) \rightarrow w^{-1}x \in S.$$

Proof. Let $m(x)$ and $m(u)$ be the coefficients of x and u, respectively, in $(\bar{S})^2$. By the previous lemma, if $s \in S$ contributes to $m(x)$ but not to $m(u)$, it must belong to $S_Z \cup (uC)$. We have $s^{-1}x \in S$ and $s^{-1}u \notin S$; hence, by the rationality of $\mathcal{S}$, $sx^{-1} \in S$ and $su^{-1} \notin S$. Since $s^{-1}x \in S_X$, we have by Lemma 3.1 that $s^{-1}xu \in S$. This means that $s^{-1}xu$ contributes to $m(u)$ but not to $m(x)$. Since u and x are fixed, the correspondence $s \rightarrow s^{-1}xu$ is one-to-one. From $m(x) = m(u)$ we conclude that if w contributes to $m(u)$ but not to $m(x)$, we must have $w = s^{-1}xu$ for some $s \in S_Z \cup (uC)$; hence $wx^{-1} = s^{-1}u$ is in $H_Z \cup (uC)$. The lemma asserts the contrapositive.

LEMMA 3.3. *For each basis element S, all elements of S have the same length.*

Proof. If S is S_0 or S_1, it consists of all elements of length 0 (Definition 2.1) or 1 (see (†)), respectively. Let $s \in S$ have minimal length $j > 1$. Since s has non-zero coefficient in $(\bar{S}_1)^j$, this must be true for all elements of S. Thus every element of S has length at most j since it is the product of j elements of length one, and at least j by the minimality of j.

LEMMA 3.4. *Let $v \in \prod_{i=2}^{d} H_i$, $a \in A$ with $o(a) = p^\alpha$, and S the basis element in which av occurs. Then hv belongs to S for all $h \in (S_1)_X$.*

Proof. (i) We assume first that $p \neq 2$. Then by Lemma 3.1, $w = a^{-1}v^{-1}$ satisfies the hypothesis of Lemma 3.2. We put $x = a$ to obtain $a^2v \in S$. We note that by Theorem 2.2, a^{-1}, a^{-2}, and h belong to H_1, hence to $S_1 \cup \{1\}$. We have $h = a^ibc$, with $(i, p) = 1$, $b \in B$, $c \in C$. A second application of Lemma 3.2 with $w = a^{-1}v^{-1}$ and $x = a^{-1}h$ or $w = a^{-2}v^{-1}$ and $x = a^{-2}h$, according as p does not or does divide $i - 1$, yields $w^{-1}x = hv \in S$.

(ii) Since A is contained in H_1 and the groups $H_2, \ldots, H_d$ have the same order as H_1, it is clear that B is non-trivial. Thus if $p = 2$, we have $\alpha > \beta + 1 \geqq 2$ and $a^2v \in H_Y - uC$. We again use Lemmas 3.1 and 3.2 to first obtain $a^2v \in S$ (putting $w = a^{-1}v^{-1}$ and $x = a$); then $hv \in S$ (putting $w = a^{-2}v^{-1}$ and $x = a^{-2}h$).

We remark that since by Theorem 2.2 every element of H_X is a product hv of some $h \in (H_1)_X$ and some $v \in \prod_{i=2}^{d} H_i$, Lemma 3.4 tells us that the basis element which has av has every element of $H_X \cap H_1v$. This means that for any basis element S, if $S_X \cap H_1v$ is non-empty, it contains all of $(H_1v)_X$.

LEMMA 3.5. *Let v, a, and S be as in Lemma* 3.4. *Then hv belongs to S for all $h \in H_1^{\#}$.*

https://doi.org/10.4153/CJM-1969-117-5 Published online by Cambridge University Press

Proof. We compute the coefficients $m(a)$ and $m(h)$ of a and h, respectively, in $(\bar{S})^2$. Let

$$W = \left\{ w \in \prod_{i=2}^{d} H_i \,\middle|\, H_1 w \cap S_X \neq \emptyset \right\} \quad \text{and} \quad W' = \prod_{i=2}^{d} H_i - W.$$

By the rationality of $\mathscr{S}$, we have $W = \{w^{-1} | \, w \in W\}$; thus a cannot occur in $(\overline{H_1 W})(\overline{H_1 W'})$. It does not occur in $[\overline{H_1 W'}]^2$ since at least one factor must have p-part of order p^α in order that the product be equal to a. Thus $m(a)$ is the coefficient of a in $(\overline{H_1 W \cap S})^2$. For $y \in H_1 W - S$, we must have $y \notin H_X$ and $ay^{-1} \in S$ by the remark following the previous lemma. Since $y \notin S$ holds, ay^{-1} fails to contribute to $m(a)$. Thus for each element of $H_1 W - S$ we have an element of $H_1 W \cap S$ which does not contribute to $m(a)$. This means that $m(a)$ is as small as possible, namely

$$m(a) = |H_1 W \cap S| - |H_1 W - S|.$$

Since a and h both belong to S_1, we have $m(a) = m(h)$. The contribution to $m(h)$ from $(\overline{H_1 W \cap S})^2$ is at least $|H_1 W \cap S| - |H_1 W - S|$ and can only be this small if for every $t \in H_1 W - S$, $t^{-1}h \in S$ holds. Since v is in W by hypothesis, the lemma can only fail if for some $h \in H_1^{\#}$ we have

$$t = hv \in H_1 W - S$$

from which it would follow that $t^{-1}h = v^{-1} \in S$. Since $av \in S$ and $l(v^{-1}) = l(av) - 1$, this contradicts Lemma 3.3.

LEMMA 3.6. *Let v, a, and S be as in the previous lemmas and let h be an element of length 1 in H such that $l(av) = l(avh^{-1})$. Then avh^{-1} is in S.*

Proof. We denote by T the basis element in which avh^{-1} occurs. Then $a^{-1}v^{-1}h$ is also in T and h has non-zero coefficient in $\bar{S}\bar{T}$. Since h and a both belong to S_1, there exist $s \in S$, $t \in T$ with $st = a$. By Lemma 3.3, we have $l(s) = l(av)$ and $l(t) = l(avh^{-1})$ from which it follows that $l(s) = l(t)$. Since st would have length at least 2 if there were a component in which one factor had a non-trivial entry and the other did not, and the only non-trivial component of st is the first, we have for some $h_1 \in H_1^{\#}$ and some $w \in \prod_{i=2}^{d} H_i$ that $s = h_1 w$ and $t = ah_1^{-1}w^{-1}$. By Lemma 3.5 (with w in place of v) and the rationality of $\mathscr{S}$, we see that s and t belong to the same basis element as aw; hence $S = T$.

LEMMA 3.7. *Let S be an arbitrary non-trivial basis element of $\mathscr{S}$. Let $s \in S$ and $k \in H$ such that $l(s) = l(k)$ and $l(sk^{-1}) = 1$. Then k is in S.*

Proof. By Theorem 2.2 and the primitivity of $\mathscr{S}$, S has an element xv with $x \in (H_1)_X$ and $v \in \prod_{i=2}^{d} H_i$. By Lemma 3.4 we must also have $av \in S$ for any $a \in A$ with $o(a) = p^\alpha$. Lemma 3.6 now tells us that any element of length $l(av)$ which differs from av in exactly one component also belongs to S. But these are exactly the elements which contribute to the coefficient $n(av)$ of av

https://doi.org/10.4153/CJM-1969-117-5 Published online by Cambridge University Press

in $\tilde{S}_1\tilde{S}$. Thus $n(av) = l(av)(|H| - 2)$ since in each component exactly one of the $|H_i^\#|$ possible entries fails to differ from av in that component. Similarly, the coefficient $n(s)$ of s in $\tilde{S}_1\tilde{S}$ is the number of elements of S which differ from s in exactly one component. All $l(s)(|H_i| - 2)$ of these elements, one of which is k, must belong to S, in order that $n(s) = n(av)$.

LEMMA 3.8. *Let S be a basis element which intersects the j-product H_σ^j non-trivially. Then H_σ^j is contained in S.*

Proof. Any $h \in H_\sigma^j$ may be obtained from any $k \in H_\sigma^j$ by at most j applications of Lemma 3.7. We have proved the following result.

THEOREM A. *Let $\mathcal{S}$ be a rational primitive* S*-ring over an abelian group $H = A \times B \times C$, where A is cyclic of order p^α, B has exponent $p^\beta < p^\alpha$, C has order prime to p, and $\alpha > \beta + 1$ if $p = 2$. Then there exist subgroups H_i of H, each of the same order greater than 2, such that each basis element of $\mathcal{S}$ is a set union of j-products of these subgroups for some fixed $j \leqq d$.*

COROLLARY 1. *$\{h \in H | \, l(h) = d\}$ is a basis element of $\mathcal{S}$.*

Proof. This is the only d-product.

COROLLARY 2. *$\{h \in H | \, l(h) = d - 1\}$ is a basis element of $\mathcal{S}$.*

Proof. Let S be a basis element with elements of length $d - 1$ and let n_i be the number of $(d - 1)$-products contained in S in which H_i occurs as a factor. Then the coefficient of $h_i \in H_i$ in $(\tilde{S})^2$ is easily seen to be

$$n_i(|H_i| - 2)(|H_i| - 1)^{d-2}$$

since if $H_\sigma^{d-1} \neq H_\tau^{d-1}$, then $H_\sigma^{d-1}H_\tau^{d-1}$ has no words of length one. Since all elements of length 1 belong to S_1, we have $n_i = n_j$ for all i, j. If n is the number of $(d - 1)$-products contained in S, we have $dn_i = n(d - 1)$ from which it follows that $d|n$. Since the total number of $(d - 1)$-products is d, they must all be contained in S. S can have no additional elements by Lemma 3.3.

IV. The general case. We now drop the hypothesis that our primitive S-ring $\mathcal{S}$ is rational. With each basis element S we associate $S' = \{s^q | \, s \in S$ and $(q, |H|) = 1\}$. It is well known that the distinct S' are basis elements of a rational S-ring $\mathcal{S}'$.

We begin with a lemma which was proved (but not stated) by Schur (**2**, p. 608).

LEMMA 4.1. *Let S be a basis element of an* S*-ring over an abelian group H of order mn, where $(m, n) = 1$. If S has elements s, t such that $s^m = t^n = 1$, then $S = S'$.*

THEOREM B. *A primitive Schur ring $\mathcal{S}$ over an abelian group H which satisfies the hypotheses of Theorem* A *is rational if H does not have prime power order.*

Proof. Let the order of H be $p^\gamma n$ with $(p, n) = 1$, q a prime divisor of n, and S a non-trivial basis element of $\mathscr{S}$. S' is a set union of j-products by Theorem A. Since $|H| = |H_i|^d$, each H_i has elements of order p and q. Since H is abelian, each j-product has elements of order p and q. Thus there exist s, $t \in S$ and integers i, l prime to $|H|$ such that s^i has order p and t^l has order q. Since $s^{p^\gamma} = t^n = 1$, we have $S = S'$ by Lemma 4.1. Since clearly $S_0 = S_0'$, $\mathscr{S}$ is rational.

V. An example. Since all elements of length j belong to the same basis element of $\mathscr{S}$ for $j = 1$, $d - 1$, and d, one might conjecture that this were so for all j. Indeed, if one computes the S-rings associated with the simply transitive primitive groups given by Wielandt (**3**, p. 67) one sees that the basis elements are $S_0, \ldots, S_d$, where $S_j = \{h \in H \mid l(h) = j\}$.

We give the following example to show that this need not be the case.

Example. Let $H = H_1 \times H_2 \times H_3 \times H_4$, where the H_i are abelian groups each of the same order greater than 2.

We put

$$
\begin{aligned}
S_0 &= \{1\},\\
S_1 &= H_1^\# \cup H_2^\# \cup H_3^\# \cup H_4^\#,\\
S_2 &= H_1^\# H_2^\# \cup H_3^\# H_4^\#,\\
S_3 &= H_1^\# H_3^\# \cup H_2^\# H_4^\#,\\
S_4 &= H_1^\# H_4^\# \cup H_2^\# H_3^\#,\\
S_5 &= H_1^\# H_2^\# H_3^\# \cup H_1^\# H_2^\# H_4^\# \cup H_1^\# H_3^\# H_4^\# \cup H_2^\# H_3^\# H_4^\#,\\
S_6 &= H_1^\# H_2^\# H_3^\# H_4^\#.
\end{aligned}
$$

It is not difficult to see that the S_i are basis elements of a rational primitive S-ring over H in which the elements of length 2 split into three basis elements. Although we do not do so here, it can be shown that there exists a simply transitive primitive permutation group G with regular subgroup H for which this is the associated S-ring (in the sense of Theorem 2.1). The groups H_i can easily be chosen so that H satisfies the hypotheses of Theorems A and B, for example by taking H_1 to be the direct product of cyclic groups of order 9 and 2 and H_2, H_3, H_4 to each be the direct product of groups of order 3, 3, and 2 (in which case A has order 9, B has order 729 and exponent 3, and C has order 16).

VI. The permutation group application.

THEOREM C. *Let G be a simply transitive primitive permutation group with regular abelian subgroup $H = A \times B \times C$, where A is cyclic of prime-power order p^α, B has exponent $p^\beta < p^\alpha$, C is non-trivial of order prime to p, and $\alpha > \beta + 1$ if $p = 2$. Then H is the direct product of two or more subgroups $H_1, \ldots, H_d$, each of order $m \geqq 3$ such that:*

https://doi.org/10.4153/CJM-1969-117-5 Published online by Cambridge University Press

(1) *if h and k belong to the same j-product H_σ^j, then δ^h and δ^k belong to the same orbit of G_δ,*
(2) *for $j = 0, \ldots, d$ there are positive integers n_{ij}, $i = 1, \ldots, r_j$, such that the orbits T_{ij} of G_δ are in one-to-one correspondence with the integers n_{ij} and $|T_{ij}| = n_{ij}(m-1)^j$,*
(3) $r_0 = r_1 = r_{d-1} = r_d = 1$; $n_{10} = 1$, $n_{11} = d$, $n_{1,d-1} = d$, $n_{1d} = 1$, *and*
(4) $\sum_{i=1}^{j} n_{ij} = \binom{d}{j}$ *for* $j = 0, \ldots, d$.

Proof. By Theorem 2.1, the orbits of G_δ induce a primitive S-ring $\mathscr{S}$ whose "rational closure" $\mathscr{S}'$ has basis elements which are set unions of j-products by Theorem A. $\mathscr{S} = \mathscr{S}'$ by Theorem B. If we denote by r_j the number of basis elements which have elements of length j, by S_{ij} the ith such basis element for $i = 1, \ldots, r_j$, and by n_{ij} the number of j-products contained in S_{ij}, we have $|S_{ij}| = n_{ij}(m-1)^j$. By Theorem 2.1, the orbits T_{ij} of G_δ are in one-to-one correspondence with the S_{ij} in such a way that $|T_{ij}| = |S_{ij}|$. By Definition 2.1, Theorem 2.2, and the corollaries to Theorem A, we have $r_j = 1$ for $j = 0, 1, d-1, d$. Since for any j there are $\binom{d}{j}$ j-products, we have $\sum_{i=1}^{r_j} n_{ij} = \binom{d}{j}$; hence $n_{10} = n_{1,d} = 1$ and $n_{11} = n_{1,d-1} = d$.

References

1. R. D. Bercov, *The double transitivity of a class of permutation groups*, Can. J. Math. *17* (1965), 480–493.
2. I. Schur, *Zur theorie der einfach transitiviten permutationsgruppen*, Sitz. Preuss. Akad. Wiss. Phys.-Math. Kl. *1933*, 598–623.
3. H. Wielandt, *Finite permutation groups* (Academic Press, New York, 1964).

University of Alberta,
Edmonton, Alberta