Offprint from

PROCEEDINGS

OF THE

ROYAL IRISH ACADEMY

SECTION A — MATHEMATICAL AND PHYSICAL SCIENCES

ROYAL IRISH ACADEMY
19 DAWSON STREET
DUBLIN 2, IRELAND

ON DOUBLY HOMOGENEOUS GROUPS

By J. Siemons

Department of Mathematics, University College, Galway*

(Communicated by T. J. Laffey, M.R.I.A.)

[Received 29 June, 1981 Read 14 December, 1981. Published 23 July 1982.]

ABSTRACT

The following is proved: if G is a doubly homogeneous permutation group of degree n not contained in the affine group of the same degree, then G contains a normal simple subgroup H so that the number of H-orbits on unordered pairs of points divides $d(n)$. The integer function $d(n)$ is defined in the paper and is equal to 1 for a very large proportion of the composite integers. The theorem throws some light onto the peculiar representation of PSL (2, 8) as smallest 'Ree group' on 28 points. This group has $d(28) = 3$ orbits on unordered pairs. A further result is the following: let G and H be permutation groups of degree n and let a be a permutation of order 2 or 3 on the same set fixing exactly f points; suppose that G is doubly homogeneous normalizing H and that $a^G = a^H$; then the number of H-orbits on unordered pairs of points divides both n-1 and f-1.

1. Introduction

Let G be a doubly homogeneous group on a finite set S of n points. Suppose G is not a subgroup of the affine group $A\Gamma L(m, q)$ with $n = q^m$. We prove the following theorem.

Theorem 1. *G contains a unique simple normal subgroup H. H is doubly homogeneous if $d(n) = 1$.*

Here the function $d(n)$ is defined as the greatest common divisor of $\{n - 1, c_p(n) \mid p$ is a prime dividing $n\}$. For a prime $p \neq 2$, $c_p(n)$ is the least common multiple of $\{(p^i - 1)/2 \mid p^i$ divides $n\}$ and for $p = 2$, $c_2(n)$ is the least common multiple of $\{2^i - 1 \mid 2^i$ divides $n\}$. For composite integers (containing two or more primes) $d(n)$ equals 1 almost always. The lowest composite integer with $d(n) \neq 1$ is 28. In fact, the group $P\Gamma L(2, 8)$ has a doubly homogeneous representation of degree 28 where the normal subgroup $PSL(2, 8)$ is not doubly homogeneous. This is the only example known where the simple normal subgroup H is not doubly homogeneous as well.

We note that in Theorem 1 both G and H are even doubly transitive; this is a consequence of Kantor [2]. Since $d(n) = 1$ if $n \equiv 2 \bmod 4$, our first theorem contains Theorem 1 of Aschbacher [1]. Note also that $d(n) = 1$ if $n \equiv 3 \bmod 9$. More detailed information in the case $d(n) \neq 1$ will be given in section 2, Theorem 3.

The subvention granted by University College, Galway, towards the cost of publication of papers by members of its staff is gratefully acknowledged by the Royal Irish Academy.

*Present address: Department of Mathematics, University College, Cork.

Theorem 2. *Let H and G be permutation groups on S of degree n. Suppose that G is doubly homogeneous and normalizes H. Let a be a permutation on S of order 2 or 3 fixing exactly f points, such that $a^G = a^H$. Then H is doubly homogeneous if $n-1$ and $f-1$ are coprime.*

Here a^G stands for the set of all G-conjugates of a and we note that a does not need to be contained in G or H. If H is the simple group mentioned in Theorem 1 and contains just one class of fixed-point-free involutions (for instance), then H and G are both doubly transitive.

The paper is in most parts selfcontained and the notation used is standard. I wish to thank the referee for his suggestions (Proposition 1) which lead to a shortening of an earlier version of this paper.

2. Multiply homogeneous groups

Let S be a finite set of points $s_1, \ldots, s_n$ and let X be the family of all subsets of S. The subfamilies of k-elements subsets ($k \leqslant n$) are denoted by X_k and we will identify $X_0 = \emptyset$ and $X_1 = S$. Hence a group G on S is k-homogeneous if and only if G acts transitively on X_k.

Proposition 1. *Let G, H and N be permutation groups on S such that G normalizes H, $G \subseteq H \cdot N$ and G is transitive on S. Suppose that $S_1, \ldots, S_t$ are distinct subsets of S which are permuted by N. Then the number of orbits of H on S divides $\Sigma_{i=1}^t | S_i |$.*

PROOF. Let $0_1, \ldots, 0_r$ be the orbits of H on S. Since G normalizes H and is transitive on S, G permutes the 0_j transitively. Hence, for a given j there are elements h in H and m in N such that $0_j = 0_1^{hm} = 0^{m}{}_1$. Therefore $\Sigma_{i=1}^t | S_i \cap 0_j | = \Sigma_{i=1}^t | S_i^{m^{-1}} \cap 0_1 | = \Sigma_{i=1}^t | S_i \cap 0_1 |$ and hence we obtain $\Sigma_{i=1}^t | S_i | = \Sigma_{i=1}^t (\Sigma_{j=1}^r | S_i \cap 0_j |) = \Sigma_{j=1}^r (\Sigma_{i=1}^t | S_i \cap 0_j |) = r \cdot \Sigma_{i=1}^t |S_i \cap 0_1|$. So r divides the sum of the sizes of the S_1.□

Let A be a permutation group on S and consider the orbits of A on X_k for some $k = \leqslant n$. Let n_{1k} be the number of all orbits of shortest length l_{1k}, n_{2k} the number of all orbits of second shortest length l_{2k}, and so on. If N is a group normalizing A then N permutes all k-element subsets contained in A-orbits of a given length. We use this fact together with the previous proposition to obtain the following divisibility conditions for multiply homogeneous groups.

Proposition 2. *Let G be a k-homogeneous group on S of degree n, $k \leqslant 1/2 \cdot n$, and let H, A be groups on S such that G normalizes H and $A^G = A^H$. Let n_{ik} be the number of A-orbits of length l_{ik} on X_k. For any $k' \leqslant k$ let r be the number of H-orbits on $X_{k'}$. Then r divides*

(i) $n_{ik} \cdot l_{ik} \cdot \binom{k}{k'-p} \cdot \binom{n-k}{p}$ *for all i and $p \leqslant k'$, and*

(ii) $\binom{l_{i1}}{l} \cdot \binom{n_{i1}}{m} \cdot \binom{l \cdot m}{k'-p} \cdot \binom{n-l \cdot m}{p}$ *for all i, $l \leqslant l_{i1}$, $m \leqslant n_{i1}$ and $p \leqslant k'$.*

PROOF. Here A^G stands for the class of all G-conjugates of A and $A^{G=}A^H$ implies $G \subseteq H \cdot N$ where N is the normalizer of A in the symmetric group. By a theorem of Livingstone and Wagner (a very short proof can be found in [4]), G is also k'-homogeneous and hence is transitive on $X_{k'}$. We apply Proposition 1 to the action of G, H and N on $X_{k'}$ and produce subsets S_i of $X_{k'}$ for which $\Sigma \mid S_i \mid$ are the corresponding expressions in the proposition.

In the first case let $x_1, \ldots, x_t$ be the collection of all k-element subsets contained in A-orbits of length l_{ik}. For a given $p \leqslant k'$ we define $S_i = \{x' \mid x'$ in $X_{k'}$ and $\mid x' \cap x_i \mid = k' - p\}$. It is easy to see that the S_i are permuted by N and are all distinct except in the case $k = n/2$ and $p = k'/2$ when each S_i occurs twice. Since each S_i contains $\binom{k}{k'-p} \cdot \binom{n-k}{p}$ sets, we obtain $\Sigma \mid S_i \mid = n_{ik} \cdot l_{ik} \cdot \binom{k}{k'-p} \cdot \binom{n-k}{p}$ as required.

For the remainder we consider the n_{i1} A-orbits on S of length l_{i1}. For given values $m \leqslant n_{i1}$ and $l \leqslant l_{i1}$ we select m orbits among n_{i1} and in each one of these we choose l points in order to obtain a set of size $l \cdot m$.

This can be done in $t = \binom{n_{i1}}{m} \cdot \binom{l_{i1}}{l}$ different ways.

Let $x_1, \ldots, x_t$ be all sets obtained in this fashion. Clearly N permutes the x_i and we define $S_i = \{x' \mid x'$ in $X_{k'}$ and $\mid x' \cap x_i \mid = k' - p\}$. Then N permutes also the S_i which are all distinct containing

$$\binom{l \cdot m}{k'-p} \cdot \binom{n - l \cdot m}{p}$$

subsets each. This proves the second statement. □

In this proposition all weakly closed subgroups of H are candidates for A, in particular all Sylow-p-subgroups of H. The orbit structure of a Sylow-subgroup therefore yields strong restrictions for the orbit numbers of H. The following theorem is based upon the fact that we may assume that a Sylow-p-subgroup acts semi-regularly if p divides n.

Theorem 3. *Let H ($\neq 1$) and G be permutation groups on a set S of n points. Suppose G is doubly homogeneous and normalizes H. Then H is transitive on S and the number of H-orbits on X_2 divides $d(n)$, the function defined in the introduction.*

We need the following lemma.

Lemma. *A doubly homogeneous group is primitive.*

PROOF. Suppose x is a block of imprimitivity containing the points s' and s''. Let s be any other point and g an element in the group such that $\{s', s''\}^g = \{s', s\}$. So x^g contains s' and s, i.e. $x^g = x$ contains all points and hence the group is primitive. □

PROOF OF THEOREM 3 . Since the H-orbits on S are blocks of imprimitivity of G, H is transitive by the preceding lemma. This implies that $\{G_s \mid s \text{ in } S\}$ is a class of H-conjugate groups. The set of points fixed by G_s forms a block of imprimitivity containing s, thus G_s fixes s only. We apply Proposition 2(ii) to $A = G_s$ and $A = 1$ and find that r, the number of H-orbits on X_2, divides

$$\binom{n-1}{2} \text{ and } \binom{n}{2},$$

hence r divides $n-1$. Let p be a prime dividing n, A a Sylow-p-subgroup of H and s a point in S.

Step 1. Assume that p does not divide the order of H_s. In this case A is semi-regular on S and has n/p^i orbits of length p^i on S where $|A| = p^i$ is the highest power of p dividing n. By Sylow's theorem $A^H = A^G$ and by Proposition 2(ii) r divides

$$\binom{p^i}{2} \cdot n/p^i = n \cdot (p^i - 1)/2.$$

Since r and n are coprime, r divides $(p^i - 1)/2$ or $p^i - 1$ if $p = 2$ and therefore r divides $c_p(n)$.

In general, however, the order of H_s may well be divisible by p so that much less is known about the orbit structure of A. For the remainder we may assume that H is a normal subgroup of G and that G is doubly transitive (using Kantor [2]).

Step 2. Let$U$ $(\neq 1)$ be a Sylow-p-subgroup of H_s and x the subset of all points fixed by U. If H' and G' are the groups induced on x, then G' is doubly transitive on x with normal transitive subgroup H'. For reference about these facts see Theorem 3.5 of [3]. The degree $n' = |x|$ is divisible by p and if p^j is the highest power of p dividing n', then p^j divides $|H : H_s| = n$. Finally observe that H'_s has order not divisible by p, by construction. In addition, as a consequence of 3.1 and 3.5 in [3], we have $r = r'$, the number of H'-orbits on the 2-element subsets of x. Therefore, Step 1 applied to the groups on x implies that r divides $(p^j - 1)/2$ or $p^j - 1$ for some power p^j dividing n. Hence r divides $c_p(n)$ for every prime dividing n and therefore r divides $d(n)$. □

3. Proofs of Theorems 1 and 2

Let G be the group in Theorem 1 and let H be a minimal normal subgroup. By Kantor's result [2] G is doubly transitive on S. By a classical result of Burnside, H is either elementary Abelian or non-Abelian simple. (It is less well known that Burnside's original proof is inconclusive!). In the first case G is an affine group on the vector space H, this possibility has been excluded. Therefore H is simple and the only minimal normal subgroup. The remainder is a direct consequence of Theorem 3. This concludes the proof of Theorem 1. □

The group $P\Gamma L(2, 8)$ is doubly transitive in its representation as smallest 'Ree group' on $3^3 + 1$ points. The normal simple subgroup $PSL(2, 8)$ is transitive and has exactly $d(28) = 3$ orbits on the 2-element subsets of 28 points and has also 3 orbits on the ordered pairs. This is the only known example of a doubly transitive permutation group whose simple normal subgroup is not doubly transitive as well. With the completion of the classification of all finite simple groups this will turn out to be the only example.

In order to prove Theorem 2, let G and H be the groups in the theorem and let r be the number of H-orbits on X_2. As in the proof of Theorem 3 one shows that r divides $n - 1$. Let $A = \langle a \rangle$ where a has order $p = 2$ or 3 and fixes exactly f points. Applying Proposition 2(ii) we obtain that r divides

$$\binom{p}{2} \cdot (n-f)/p = (n-f) \cdot (p-1)/2.$$

Since $n - 1 \equiv o \ mod \ r$ we have $o \equiv n - f \equiv (n-1) - (f-1) \equiv f - 1 \ mod \ r$ and hence r is a common divisor of $n - 1$ and $f - 1$. Therefore H is doubly homogeneous on S. □

REFERENCES

[1] ASCHBACHER, M. 1972 On doubly transitive permutation groups of degree $n \equiv 2 \ mod \ 4$. *Illinois J. Math.* **16**, 276–279.

[2] KANTOR, W. 1972 k-homogeneous groups. *Math.Z.* **124**, 261–265.

[3] SIEMONS, J. 1980 Normal subgroups of triply transitive permutation groups of degree divisible by 3. *Math.Z.* **174**, 95–105.

[4] WIELANDT, H. 1972 Endliche k-homogene Permutationsgruppen. *Math.Z.* **101**, 142.