GENERATORS FOR ALTERNATING AND SYMMETRIC GROUPS

I. M. S. DEY and JAMES WIEGOLD

(Received 15 May 1969)

Communicated by G. E. Wall

1. Introduction and method

Let Γ denote the modular group, that is, the free product of a group of order 2 and a group of order 3. Morris Newman investigates in [2] the factor-groups of Γ and calls them Γ-groups for short; thus a group is a Γ-group if and only if it has a generating set consisting of an element of order dividing 2 and an element of order dividing 3. Newman's interest centres on finite simple Γ-groups. He proves that the linear fractional groups $LF(2, p)$ for primes p are Γ-groups, and poses the problem of deciding which of the alternating groups enjoy this property.

The authors tackled and solved this problem and the analogous one for symmetric groups, finding that all finite symmetric and alternating groups except S_5, A_6, S_6, A_7, A_8, S_8 fall into the class. Very soon afterwards a conversation with B. H. Neumann led to the discovery that G. A. Miller had proved this same result [1] in [1]. Miller's proof is based on the truth of Bertrand's postulate, and his generators depend on choosing a prime p in the range $n-2 > p > n/2$, n being the degree of the groups under discussion. As such they are not explicitly given. We offer here very explicit generators that are easily expressed in terms of the degree, and proofs that do not depend on results extraneous to the elementary theory of permutation groups. However, proofs are not short, and we shall restrict ourselves to giving a table of generators and to indicating briefly why they do what is required of them.

We are grateful to B. H. Neumann for pointing out Miller's work to us and for some ideas which have improved the exposition.

Notation is that of Wielandt's book [3]. The basis of the method is to give an element a of order 3 and two elements x, y of order 2 in the relevant symmetric group S_n, with x even and y odd, such that $\langle a, x\rangle$ and $\langle a, y\rangle$ are primitive on the n symbols and both contain some cyclic permutation of prime order p (the prime may differ in the two cases) such that $p < n-2$. But then a well-known theorem of Jordan applies to prove that both these groups contain A_n; that is, that $\langle a, x\rangle =$

[1] It has also come to our notice that Graham Higman has proved the similar but more difficult result that A_n is a factor group of $(2, 3, 7) = \langle a, b \mid a^2, b^3, (ab)^7\rangle$ for all large enough n; this work is unpublished.

https://doi.org/10.1017/S1446788700008302 Published online by Cambridge University Press

A_n and $\langle a, y\rangle = S_n$. A convenient reference for Jordan's theorem is page 39 of [3]. In fact the only primes which arise are 2, 3, 5, 7, 11, 13, and in all cases except two some power of ax (or ay) is a prime cycle; the exceptions are A_{11} and S_{16}, where we were obliged to take commutators. In each case we indicate the appropriate element.

The table in the next section is divided into eight parts I-VIII. The first six parts list suitable generators for all cases with $n \geqq 19$, the parts depending on the residue of n modulo 6. VII lists the generators for the S_n and A_n which are Γ-groups and not listed in I-VI; this section has a distinctly *ad hoc* flavour about it, though we have tried as far as possible to model the generators on those in I-VI. Just for completeness, VIII lists those A_n and S_n which are not Γ-groups. To use the table, proceed like this. If the degree n falls in the range covered by VII and VIII, that is, if $n \leqq 18$, everything is self-explanatory. If $n \geqq 19$, write $n = 6m+k$ with $0 \leqq k < 6$, and select the relevant section I-VI. If m is odd put $x = b_1$, $y = b_2$, and $x = b_2$, $y = b_1$ if m is even. That is, for odd m, $\langle a, b_1\rangle = A_n$ and $\langle a, b_2\rangle = S_n$; whereas for even m it is the other way round.

In § 3 we indicate a proof of primitivity in the 'general' cases $n \geqq 19$, and § 4 contains some comments on the exceptions.

2. Tables

It will be useful to have a shorthand for certain permutations of order 2 and 3. Firtly, let n be a positive integral multiple of 3. Then by a_n we mean the permutation $(1, 2, 3)(4, 5, 6)\dots(n-2, n-1, n)$ of degree n. Next, for any $k \geqq 1$, c_k stands for the product $\prod_{r=1}^{k}(6r, 6r+3)(6r+1, 6r+4)(6r+2, 6r+5)$, so that c_k has degree $6k$.

I. $\underline{n\ = 6m,\ m \geqq 4}$

$a\ = a_{n-3}$,
$b_1 = (1, 4)(2, n-2)(3, n-1)(n-6, n-3)(n-5, n)c_{m-2}$,
$b_2 = b_1(n-11, n-8)$,
$(ab_1)^{42}$ and $(ab_2)^{78}$ are 11-cycles.

II. $\underline{n\ = 6m+1,\ m \geqq 3}$

$a\ = a_{n-1}$,
$b_1 = (1, 4)(2, n)(3, n-1)(n-6, n-3)(n-5, n-2)c_{m-2}$,
$b_2 = b_1(n-12, n-9)$;

(i) $\underline{m \geqq 4}$

$(ab_1)^6$ and $(ab_2)^{18}$ are 13-cycles.

(ii) $\underline{m = 3}$

$(ab_1)^6$ is a 13-cycle, $(ab_2)^{16}$ is a 3-cycle.

https://doi.org/10.1017/S1446788700008302 Published online by Cambridge University Press

III. $\underline{n \ = 6m+2, m \geqq 3}$

$a \ = a_{n-2}$,
$b_1 = (1, 4)(2, n-1)(3, n)(n-8, n-5)(n-6, n-3)c_{m-2}$,
$b_2 = b_1(n-7, n-4)$,
$(ab_1)^{18}$ and $(ab_2)^6$ are 11-cycles.

IV. $\underline{n \ = 6m+3, m \geqq 3}$

$a \ = a_{n-3}$,
$b_1 = (1, 4)(2, n-2)(3, n-1)(n-3, n)c_{m-1}$,
$b_2 = b_1(n-8, n-5)$,
$(ab_1)^{12}$ and $(ab_2)^{60}$ are 11-cycles.

V. $\underline{n \ = 6m+4, m \geqq 3}$

$a \ = a_{n-1}$,
$b_1 = (1, 4)(2, n)(3, n-3)(n-10, n-7)(n-8, n-5)c_{m-2}$,
$b_2 = b_1(n-9, n-6)$,
$(ab_1)^{18}$ and $(ab_2)^6$ are 13-cycles.

VI. $\underline{n \ = 6m+5, m \geqq 3}$

$a \ = a_{n-2}$,
$b_1 = (1, 4)(2, n-1)(3, n)(n-5, n-2)c_{m-1}$,
$b_2 = b_1(n-10, n-7)$,
$(ab_1)^6$ and $(ab_2)^{12}$ are 11-cycles.

VII. *Γ-groups with $n \leqq 18$.*

We shall not list the cases $n \leqq 4$; they are trivial. Primitivity proofs are omitted except for the following simple observations, which deal with most of the cases in this part of the table. Transitive groups of prime degree are automatically primitive; any transitive group of degree n and containing a prime cycle of degree more than n/p, p being the smallest prime divisor of n, is primitive. The remaining cases can be dealt with ın a completely straightforward fashion.

n

5 $a = a_3$, $x = (1, 4)(2, 5)$.

7 $a = a_6$, $y = (1, 4)(2, 7)(3, 5)$,
$(ay)^5$ is a 2-cycle.

9 $a = a_9$, $x = (1, 4)(2, 9)(3, 7)(5, 6)$, $y = (1, 4)(2, 8)(5, 9)$,
$(ax)^5$ is a 3-cycle, $(ay)^4$ is a 5-cycle.

10 $a = a_9$, $x = (1, 4)(6, 9)(3, 10)(2, 8)$, $y = (1, 4)(2, 10)(3, 7)(5, 9)(6, 8)$,
$(ax)^7$ is a 3-cycle, $(ay)^{15}$ is a 2-cycle.

https://doi.org/10.1017/S1446788700008302 Published online by Cambridge University Press

11 $a = a_9$, $x = (1, 4)(2, 10)(3, 11)(6, 9)$, $y = (1, 4)(2, 7)(5, 8)(6, 11)(3, 10)$,
$[a, x, a]^5$ is a 3-cycle, $(ay)^{11}$ is an 11-cycle.

12 *Generators for A_{12}* $a = a_9$, $x = (1, 4)(2, 10)(3, 8)(6, 9)(7, 11)(5, 12)$,
$(ax)^7$ is a 5-cycle.

Generators for S_{12} $a = a_{12}$, $y = (1, 4)(2, 10)(3, 11)(6, 9)(7, 8)$,
$(ay)^8$ is a 3-cycle.

13 $a = a_{12}$, $x = (1, 4)(2, 13)(3, 5)(6, 9)(7, 10)(8, 11)$, $y = x(3, 5)$,
$(ax)^8$ and $(ay)^{10}$ are 3-cycles.

14 $a = a_{12}$,
$x = (1, 4)(2, 13)(3, 14)(6, 9)(7, 10)(8, 11)$,
$y = (1, 4)(2, 13)(3, 14)(5, 8)(6, 9)(7, 10)(11, 12)$,
$(ax)^{11}$ is a 3-cycle, $(ay)^8$ is a 5-cycle.

15 $a = a_{15}$, $x = (1, 4)(3, 14)(6, 9)(7, 10)(12, 15)(5, 13)$, $y = x(2, 8)$,
$(ax)^{35}$ is a 3-cycle, $(ay)^{12}$ is a 5-cycle.

16 $a = a_{15}$, $x = (1, 4)(2, 16)(6, 9)(7, 10)(8, 11)(3, 13)$, $y = x(5, 15)$,
$(ax)^{13}$ is a 3-cycle, $[a, y]^9$ is a 5-cycle.

17 $a = a_{15}$
$x = (1, 4)(2, 16)(3, 17)(12, 15)(6, 9)(7, 10)(8, 11)(13, 14)$, $y = x(13, 14)$,
$(ax)^5$ and $(ay)^6$ are 11-cycles.

18 *Generators for A_{18}* $a = a_{15}$,
$x = (1, 4)(2, 16)(3, 17)(12, 15)(13, 18)(6, 9)(7, 10)(8, 11)$,
$(ax)^{11}$ is a 7-cycle.

Generators for S_{18} $a = a_{18}$,
$y = (1, 8)(2, 16)(3, 4)(5, 7)(6, 10)(12, 13)(9, 14)$,
$(ay)^{42}$ is a 5-cycle.

VIII. *The exceptions*: S_5, A_6, S_6, A_7, A_8, S_8 are not Γ-groups.

3. Primitivity in the cases $n \geqq 19$

The proof of primitivity of $\langle a, x\rangle$ and $\langle a, y\rangle$ is straightforward[2] and essentially the same in all cases, though variations occur which are major enough to make a uniform proof impossible. But we can begin uniformly. Firstly, transitivity is clear. The generator a always fixes at least one symbol, and, if α is the least symbol fixed by a, then the generator of order 2, b for short, always contains the product $(1, 4)(2, \alpha)$ and fixes the symbol 5. Suppose that α lies in a block T which is not the whole of $\Omega = \{1, 2, \cdots, n\}$; then our aim is to show that T is the singleton $\{\alpha\}$. Firstly $Ta = T$ and it is clear that $2 \notin T$, else $Ta = T = Tb$ and $T = \Omega$ contrary to

[2] Especially on a blackboard!

assumption. Set $T_2 = Tb$ so that $2 \in T_2$ and $T_2 \cap T = \emptyset$. But then $1 \notin T_2$; otherwise $4 = 1b \in T$ so that $5 = 4a \in T$, which means that $Tb = T$ since b fixes 5. In this way it becomes quite evident that 1, 2, 3, α all lie in different blocks.

We could push this general argument a little further, but it seems preferable to prove one case in detail as an example. The worst case seems to be $n = 6m$, for then a fixes 3 symbols and n is guaranteed to have several divisors, giving the highest likelihood of imprimitivity. We shall, then, establish the primitivity of the group of degree $6m$ generated by

$$\begin{aligned} a &= (1, 2, 3)(4, 5, 6) \cdots (6m-5, 6m-4, 6m-3), \\ b &= (1, 4)(2, 6m-2)(3, 6m-1)(6m-6, 6m-3) \\ &\qquad (6m-5, 6m) \prod_{r=1}^{m-2} (6r, 6r+3)(6r+1, 6r+4)\ (6r+2, 6r+5), \end{aligned}$$

with $m \geqq 4$.

As we have seen already, we can assume that $6m-2$, 1, 2, 3 lie in different blocks, say T, T_1, T_2, T_3 respectively; the aim is to prove that $6m-2$ is the only symbol in T. Let β denote an element of T, and remember that $Ta = T$, $T_1 a = T_2$, $T_2 a = T_3$, $T_3 a = T_1$, $Tb = T_2$, $T_2 b = T$. We eliminate the possibilities for β as follows.

(a) If $\beta \in \{6r+1, 6r+2, 6r+3\}$ for some r with $1 \leqq r < m-1$, then βa and βa^2 lie in T since $Ta = T$. Thus in this case $\{6r+1, 6r+2, 6r+3\} \subseteq T$ so that T_2 contains $(6r+1)b = 6r+4$ and $(6r+2)b = 6r+5$. But $(6r+4)a = 6r+5$ and a fixes T_2, a contradiction.

(b) If $\beta \in \{6m-5, 6m-4, 6m-3\}$ then $6m-4 \in T$. But $6m-4$ is fixed by b and T is not.

(c) If $\beta \in \{6r+4, 6r+5, 6r+6\}$ with $1 < r < m-1$, then as before we conclude that T_2 contains $(6r+4)b = 6r+1$, $(6r+5)b = 6r+2$; this again gives the contradiction that $T_2 a = T_2$.

(d) If $\beta \in \{4, 5, 6\}$ then $5 \in T$, which is false since b fixes 5.

There are just two possibilities left, namely $\beta = 6m-1$ and $\beta = 6m$. If $\beta = 6m-1$, then T_2 contains $(6m-1)b = 3$, which is false. Thus T can contain at most 2 elements, and the same goes for all the other blocks. If $6m \in T$ it must be the case that $6m-5 \in T_2$, and then that $6m-4 \in T_3$, $6m-3 \in T_1$. However, b fixes $6m-4$ so that $T_3 b = T_3$; since $3b = 6m-1$ it follows that T_3 contains the three distinct elements 3, $6m-1$, $6m-4$, and this is our final contradiction. Thus $T = \{6m-2\}$ and $\langle a, b \rangle$ is primitive, as required.

4. The exceptions

We shall not verify the exceptional nature of S_5, A_6, S_6, A_7, A_8, S_8, but one or two remarks are perhaps in order. Any subgroup of S_5 which is a Γ-group and

https://doi.org/10.1017/S1446788700008302 Published online by Cambridge University Press

not in A_5 is intransitive, as may be readily checked. The only Γ-group which is primitive of degree 6 is the A_5 in its usual primitive representation of degree 6. The largest Γ-group which is a transitive subgroup of A_7 is PSL(2, 7) in its natural representation of degree 7; this is perhaps the most surprising result in view of the small size of PSL(2, 7) and the fact that S_7 is a Γ-group. The only primitive groups of degree 8 which are Γ-groups are PSL(2, 7) and PGL(2, 7) in their representations of degree 8.

This work was done while the authors were at the Australian National University.

References

[1] G. A. Miller, 'On the groups generated by two operators', *Bull. Amer. Math. Soc.* 7 (1901), 424–426.

[2] Morris Newman, 'Maximal normal subgroups of the modular group, *Proc. Amer. Math. Soc.* 19 (1968), 1138–1144.

[3] Helmut Wielandt, *Finite permutation groups* (Academic Press, New York, 1964).

The Open University
Walton, Bletchley, Bucks, U.K.
and
University College
Cardiff

https://doi.org/10.1017/S1446788700008302 Published online by Cambridge University Press