Some permutation groups of degree $p=6q+1$

By

M. D. Atkinson

Abstract. Transitive permutation groups of degrees 43, 67, 79, 103 and 139 are classified.

In this note we consider insoluble transitive permutation groups of degree $p = 6q + 1$ where $p$ and $q$ are primes and summarise the computations whereby these groups have been classified for some small values of $q$. The result which allows progress on this problem is due to McDonough [1]; he showed that if such a group has a Sylow $p$-normaliser of order $3p$ then it is isomorphic either to $PSL(3, 3)$ or $PSL(3, 5)$ (of degrees 13, 31 respectively). Using this theorem machine computations along the lines of those done by Parker, Nikolai and Appel [3, 2] for degrees $p = 2q + 1$ and $p = 4q + 1$ give the following

Theorem. Every insoluble transitive permutation group of degree 43, 67, 79, 103, 139 contains the alternating group of that degree.

To describe the calculations leading to this result we let $G$ denote an insoluble transitive group of degree $p = 6q + 1$, $p$ and $q$ prime, with $q > 5$ and let $P$ be a Sylow $p$-subgroup of $G$. In trying to prove that $G \cong A_p$ or $S_p$ we can of course assume that $G \leq A_p$. Because of this we have $|N(P)| = kp$ where $k$ divides $\frac{1}{2}(p - 1) = 3q$. However, Burnside's transfer theorem ensures that $k \equiv 1$ and McDonough's theorem ensures that $k \neq 3$; thus $q$ divides $k$. Moreover a theorem of [3] guarantees that $N(P)$ contains a Sylow $q$-subgroup $Q$ of $G$.

Hence $G$ contains the metacyclic (non-abelian) group $PQ$ of order $pq$ and degree $p$. All such metacyclic groups are isomorphic as permutation groups and so we may take the set of symbols permuted by $G$ to be the residues modulo $p$, $P$ to be generated by an element

$$a: \alpha \mapsto \alpha + 1 \mod p$$

and $Q$ to be generated by an element

$$b: \alpha \mapsto r^\alpha \mod p$$

where $r$ is a primitive root modulo $p$.

Again by Burnside's transfer theorem there is an element $c \in N(Q) - C(Q)$ and, as $c \notin N(P)$, $\langle a, c \rangle$ is insoluble. To prove that $G = A_p$ it is clearly sufficient to
prove that \( \langle a, c \rangle = A_p \). A large part of what follows is concerned with showing that \( c \) may be assumed to satisfy several restrictive conditions.

Because \( N(Q)/C(Q) \) is cyclic of order dividing \( q - 1 \), we may assume that \( c \) has order \( t \), where \( t \) is a prime dividing \( q - 1 \) and we may also assume that \( c^t \in C(Q) \). Then \( c^{-1}bc = b^s \) where \( s \) has order \( t \) modulo \( q \). The residue classes modulo \( q \) which have order \( t \) are all powers of each other and therefore for a given \( t \) we need consider only one value \( s \) (because we can replace \( c \) by an appropriate power).

Next, \( b \) is represented as a product of \( 6 q \)-cycles \( \gamma_0, \gamma_1, \ldots, \gamma_5 \) and one fixed point \( 0 \). The element \( c \) permutes the orbits of \( Q = \langle b \rangle \) and transforms each \( \gamma_i \) to the \( s \)-th power of some \( \gamma_j \). As a permutation of the \( 6 q \)-cycles \( c \) has one of the following cycle structures:

(i) \( 1^6 \), (ii) \( 1^5 \), (iii) \( 1^3 \), (iv) \( 1^2 \), (v) \( 1^1 \), (vi) \( 2^{14} \)
(vii) \( 1^{14} \), (viii) \( 2^3 \), (ix) \( 1^{12} \), (x) \( 1^{12} \), (xi) \( 6^1 \).

Of these possibilities (x) and (xi) are immediately excluded because \( c \) would not have order \( t^k \). Case (ix) can also be excluded, for here \( t = 2 \), \( c^2 \in C(Q) \), and since \( c^3 \) fixes each \( \gamma_i \), setwise it fixes it pointwise; thus \( c^2 = 1 \) and \( c \) consists of \( 3q - 2 \) transpositions and 5 fixed points, i.e. \( c \) is an odd permutation. For similar reasons cases (vii) and (viii) do not occur: \( c \) would have cycle structure \( 1^{12} \) or \( 1^{12} \). Cases (i) to (v) cannot be excluded on these grounds but at least it follows that \( c \) has prime order \( t \). This leaves case (vi) where \( c^2 = 1 \). Here \( c^2 \) has cycle structure \( 1^{2q+1} \) and \( c^3 \) is of type (iii) except that \( c^2 \in C(Q) \).

Thus only cases (i) to (v) need be considered provided that in case (iii) we allow the possibility that \( c \in C(Q) \). In case (ii) \( t = 5 \), in case (iii) \( t = 2 \) and in cases (iv) and (v) \( t = 3 \). For a particular \( p \) not all of these cases may arise (for example when \( p = 103 \), \( q = 17 \) and only cases (i) and (iii) give possibilities for \( t \) dividing \( q - 1 \)).

To further reduce the possibilities that have to be considered for \( c \) we consider the element \( g \in S_p \) defined by

\[ g: x \mapsto x \mod p. \]

Clearly \( g^6 = b \) and \( g^{-1}ag = a' \). Since \( \langle a, c \rangle \cong \langle a, g^{-1}cg \rangle \) once we have dealt with one possibility for \( c \) we need not consider possibilities which are conjugate under \( \langle g \rangle \) to the first possibility.

The permutation \( c \) is determined uniquely by the number \( s \) and the image of 6 points, one from each cycle of \( b \). In case (i) it is most convenient to specify \( c \) by \( s \) and the 6 points, one in each cycle of \( b \), fixed by \( c \). If we choose the notation so that \( r^i \in \gamma_i \) then these 6 points may be denoted by

\[ r^{6u}, r^{6v+1}, r^{6w+2}, r^{6x+3}, r^{6y+4}, r^{6z+5}. \]

The fixed points of a suitable conjugate of \( c \) under a power of \( g^6 = b \) may then be taken to include the point 1, i.e. in specifying \( c \) we may take \( u = 0 \). Moreover, if \( c \) fixes

\[ 1, r^{6u+1}, r^{6w+2}, r^{6x+3}, r^{6y+4}, r^{6z+5} \]

then the conjugate of \( c \) under \( g^{-6v-1} \) has fixed points

\[ 1, r^{6(u-v)+1}, r^{6(w-v)+2}, r^{6(y-v)+3}, r^{6(z-v)+4}, r^{6(-1-v)+5}. \]
In this way the number of possibilities for $c$ with a fixed $s$ can be reduced from $q^6$ to about $q^{5/6}$.

In cases (ii), (iii) and (v) transformation by $g$ allows us to assume that $c$ fixes the cycle $\gamma_0$ setwise and the point 1 within this cycle. In case (iv) the number of possibilities for $c$ as a permutation of $\gamma_0, \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5$ may be reduced to just 10 and moreover for each of these 10 the image of the point 1 may be specified.

Subject to the above restrictions the possibilities for $c$ are generated in turn and for each one the group $\langle a, c \rangle$ is examined. Sample permutations in this group are formed and their cycle lengths calculated. These cycle lengths often imply that $\langle a, c \rangle$ is the alternating group by virtue of results of Manning and Jordan (see [4]). Manning's results concern the primes which divide the group order, for example if $p = 67$ no prime in the range 17 to 61 can divide the group order unless the group is alternating; Jordan's result is that the group is alternating if it contains a prime cycle with more than two fixed points.

When performed for $p = 43, 67, 79, 103, 139$ these calculations required several hours of machine time and all groups $\langle a, c \rangle$ were found to be alternating. The program was also run with $p = 31$ whereupon it discovered the following generators for $PSL(5, 2)$:

$$a = (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30),$$


References


Eingegangen am 28. 5. 1979

Anschrift des Autors:

M. D. Atkinson

Department of Computing Mathematics

University College

Cardiff, U.K.