A CLASS OF PERMUTATION GROUPS OF PRIME DEGREE

K. D. FRYER

1. Introduction. In **(1)**, using the theory of group representations, Brauer studied groups $\mathfrak{G}$ of finite order g containing elements A of prime period p which commute only with their own powers A^i. If $\mathfrak{P}$ is a p-Sylow subgroup of $\mathfrak{G}$, the normalizer $\mathfrak{N} = \mathfrak{N}(\mathfrak{P})$ of $\mathfrak{P}$ can be generated by A and another element B such that

1.1 $$A^p = 1, \quad B^q = 1, \quad B^{-1}AB = A^{\gamma^t},$$

where γ is a primitive root (mod p), and t and q are positive integers such that

1.2 $$tq = p - 1.$$

For A, B satisfying 1.1, the group $\{A, B\}$ is of order pq. Carmichael **(3)** points out that if $t = 1$, the group $\{A, B\}$ is the so-called *metacyclic* group of order $p(p - 1)$, simply isomorphic with a doubly transitive group of degree p. Such a group contains a dihedral subgroup and is complete.

The permutations

$$A = (0\ 1 \ldots 6), \quad B = (1\ 2\ 4)(3\ 6\ 5)$$

in $GF(7)$ satisfy 1.1 with $p = 7$, $q = 3$, $t = 2$, $\gamma = 3$, and generate a group of order 21. If now a third permutation $C_1 = (2\ 4)(5\ 6)$ is added, the group $\{A, B, C_1\}$ generated is the linear fractional group $LF(2, 7)$ of order 168. If, instead of C_1, we add $C_2 = (2\ 4)(3\ 5)$, the group $\{A, B, C_2\}$ is the alternating group $\mathfrak{A}_7$, while for $C_3 = (1\ 6)(2\ 3)(4\ 5)$, $\{A, B, C_3\}$ is the symmetric group $\mathfrak{S}_7$.

The elements C_1, C_2, C_3 stand in the same relation to B as does B to A; that is, they satisfy the relations

1.3 $$B^q = 1, \quad C^r = 1, \quad C^{-1}BC = B^{\delta^s}.$$

where δ is a primitive root (mod q), and where s and r are positive integers such that

1.4 $$sr = q - 1.$$

For these elements, $q = 3$, $r = 2$, $s = 1$, $\delta = 2$.

The permutations

$$A = (0\ 1\ 2 \ldots 10), \quad B = (1\ 4\ 5\ 9\ 3)(2\ 8\ 10\ 7\ 6)$$

in $GF(11)$ satisfy 1.1 with $p = 11$, $q = 5$, $t = 2$, $\gamma = 2$.

Received June 2, 1953; in revised form March 30, 1954. This paper comprises the substance of the author's thesis, written under the direction of Professors R. Brauer and R. G. Stanton and accepted for a Ph.D. degree at the University of Toronto in June, 1952.

https://doi.org/10.4153/CJM-1955-004-3 Published online by Cambridge University Press

The additional permutations

$$\begin{aligned} C_1 &= (2\ 8)(6\ 10)(3\ 4)(5\ 9), & C_2 &= (2\ 7)(8\ 10)(3\ 4)(5\ 9),\\ C_3 &= (1\ 10)(2\ 5)(3\ 7)(4\ 8)(6\ 9), & C_4 &= (2\ 10\ 8\ 6)(3\ 9\ 4\ 5) \end{aligned}$$

yield respectively the following groups $\{A, B, C\}$:

$$LF(2, 11),\quad \mathfrak{A}_{11},\quad \mathfrak{S}_{11},\quad \mathfrak{M}_{11}.$$

The permutations C_i satisfy relations 1.3. For C_1, C_2, C_3, we have $q = 5$, $r = 2$, $\delta = 2$, $s = 2$; for C_4, $q = 5$, $r = 4$, $\delta = 2$, $s = 1$.

Finally, for $p = 23$, $q = 11$, $t = 2$, $\gamma = 5$, the permutations

$$\begin{aligned} A &= (0\ 1\ 2\ \ldots\ 22),\\ B &= (1\ 2\ 4\ 8\ 16\ 9\ 18\ 13\ 3\ 6\ 12)(5\ 10\ 20\ 17\ 11\ 22\ 21\ 19\ 15\ 7\ 14) \end{aligned}$$

in $GF(23)$ satisfy 1.1, and the additional permutations

$$\begin{aligned} C_1 &= (2\ 16\ 9\ 6\ 8)(4\ 3\ 12\ 13\ 18)(7\ 17\ 10\ 11\ 22)(14\ 19\ 21\ 20\ 15),\\ C_2 &= (2\ 12)(4\ 6)(8\ 3)(16\ 13)(9\ 18)(7\ 19)(14\ 21)(5\ 22)(10\ 11)(17\ 20),\\ C_3 &= (1\ 22)(2\ 11)(3\ 15)(4\ 17)(5\ 9)(6\ 19)(7\ 13)(8\ 20)(10\ 16)(12\ 21)(14\ 18) \end{aligned}$$

yield[1] in turn $\mathfrak{M}_{23}$, $\mathfrak{A}_{23}$, $\mathfrak{S}_{23}$. For C_1, $q = 11$, $r = 5$, $s = 2$, $\delta = 2$; for C_2 and C_3, $q = 11$, $r = 2$, $s = 5$, $\delta = 2$.

We have thus been led to a study of groups $\mathfrak{H} = \{A, B, C\}$ whose generators satisfy the following abstract relations:

$$1.5 \qquad A^p = B^q = C^r = 1, \quad B^{-1}AB = A^j, \quad C^{-1}BC = B^l,$$

where p and q are primes, $p = 2q + 1$, r is an arbitrary divisor of $q - 1$, $q = sr + 1$, j belongs to q modulo p, and l belongs to r modulo q.

We prove the following

THEOREM. *The groups $\{A, B, C\}$ described above fall into two classes: groups consisting entirely of even permutations* (*case* I), *and groups of even and odd permutations* (*case* II). *The groups in case* II *are the symmetric groups $\mathfrak{S}_p$. The groups in case* I *with r even and $\beta = q$ are the alternating groups $\mathfrak{A}_p$.* (The explanation of the symbol β is given in §2).

It is demonstrated by tables in the author's thesis, to be found in the library at the University of Toronto, that for $p \leqslant 59$, the groups $\mathfrak{H} = \{A, B, C\}$ in case I are the alternating groups $\mathfrak{A}_p$ with the exception of the four groups mentioned above; that is, $LF(2, 7)$, $LF(2, 11)$, $\mathfrak{M}_{11}$ and $\mathfrak{M}_{23}$. The same result also holds for $p = 83$.

We prove that the groups in case I are all simple. If it could be proved that there is an infinite number of prime pairs p, q with $p = 2q + 1$, we would

[1] Carmichael (**3**, p. 288) indicates that the groups $\mathfrak{M}_{11}$ and $\mathfrak{M}_{23}$ are generated by permutations similar to the A and C specifically mentioned above. It can be shown that the corresponding B in each case is expressible in terms of A and C. For further information on these groups, see (**6**).

have here an infinite class of simple groups containing in particular the two Mathieu groups $\mathfrak{M}_{11}$ and $\mathfrak{M}_{23}$.

2. The permutation representation of the generators. We proceed first to develop permutation representations for the generators A, B, C which satisfy the relations 1.5. It must be stressed that in the following we have $p = 2q + 1$ for p and q primes, and there exists a natural mapping of the integers mod q on the quadratic residues $\neq 0$ mod p and on the quadratic non-residues mod p. This fact enables us to prove

THEOREM 2.1. *The group generators A, B, and C of* §1 *may be represented by the following permutations in $GF(p)$:*

2.1
$$\begin{aligned} A&: \quad x' = x + 1,\\ B&: \quad x' = g^2 x,\\ C&: \quad x' = \tfrac{1}{2}(1 + \epsilon)\, g^{\alpha(1-l)} x^l + \tfrac{1}{2}(1 - \epsilon)\, g^{\beta(1-l)} x^l \end{aligned}$$

where $\epsilon = \pm 1$ according as x is a quadratic residue or non-residue mod p, *g is that primitive root* mod p *for which $g^2 = j$, and α and β are arbitrary fixed even and odd numbers, respectively.*

Our procedure is briefly as follows: we notice that A and B generate the metacyclic group $\{A, B\}$, and obtain representations on p symbols for A and B:

2.2 $$A:\ x' = f(x), \quad B:\ x' = g(x), \qquad x = 0, 1, \ldots p - 1.$$

B and C generate another metacyclic group, $\{B, C\}$, and we obtain representations on q symbols for B and C:

2.3 $$B:\ y' = g'(y), \quad C:\ y' = h'(y), \qquad y = 0, 1, \ldots, q - 1.$$

We then combine the representations 2.2 and 2.3, identifying the two representations for B, and obtain a representation for A, B, and C on p symbols:

2.4 $$A:\ x' = f(x), \quad B:\ x' = g(x), \quad C:\ x' = h(x) \qquad x = 0, 1, \ldots, p - 1.$$

Consider the relations involving A and B, namely

$$A^p = B^q = 1, \quad B^{-1}AB = A^j.$$

These imply

$$B^{-1}A^xB = A^{xj}$$

and

$$B^{-y}A^xB^y = A^{xj^y}.$$

Hence $A^xB^y = B^yA^{xj^y}$, and the pq elements A^xB^y correspond to the pq elements

$$B^yA^z, \qquad z = xj^y,$$

in some order. For as x ranges from 0 to $p - 1$, $x \rightarrow z = xj^y$ is a permutation

https://doi.org/10.4153/CJM-1955-004-3 Published online by Cambridge University Press

of the numbers $0, 1, \ldots, p-1$, for a fixed value of y. So the elements A and B generate the metacyclic group of order pq, the so-called *Cauchy* group **(2)**.

Let A be represented as the cycle $(0\,1\,2\ldots p-1)$, that is, the transformation $x' = x+1$ in $GF(p)$. Let B be the permutation $x' = g(x)$. Since $AB = BA^j$, we have

$$g(x+1) = g(x) + j.$$

Since B is of period q, it leaves one element fixed. We may set $g(0) = 0$, and the above recurrence relation then takes the simple form $g(x) = xj$.

Then, corresponding to 2.2, we have the representation

2.5 $$A\colon\ x' = x+1, \quad B\colon\ x' = jx, \qquad x = 0, 1, \ldots, p-1.$$

Further, letting g be that primitive root modulo p for which $g^2 = j$, B has the representation $x' = g^2x$ and, explicitly, our representations are

2.6 $$A = (0\,1\,2\ldots p-1), \quad B = (1\,g^2\,g^4\ldots g^{p-3})(g\,g^3\ldots g^{p-2}).$$

The two cycles of B contain, respectively, quadratic residues and non-residues mod p.

It can be readily verified that the same group is generated no matter which primitive root g (that is, which number j) is considered.

Now we see from 1.5 that C stands in the same relation to B as does B to A. So B and C generate the metacyclic group $\{B, C\}$ of order qr. On q symbols, B and C can be represented as

2.7 $$B\colon\ y' = y+1, \quad C\colon\ y' = m^s y, \qquad y = 0, 1, \ldots q-1,$$

or, explicitly,

2.8 $$\begin{aligned} B &= (0\,1\,2\ldots q-1), \\ C &= (1\,m^s\,m^{2s}\ldots)(m\,m^{s+1}\ldots)\ldots(m^{s-1}\,m^{2s-1}\ldots), \end{aligned}$$

where $q = sr+1$ and m is that primitive root mod q for which $m^s = l$.

We now see that the representations 2.5 and 2.7 can be combined. For in 2.5, B has the representation

$$(1\,g^2\,g^4\ldots g^{p-3})(g\,g^3\ldots g^{p-2}).$$

Let α be an arbitrary even integer. Then the cycle

$$(g^{\alpha}\,g^{\alpha+2}\,g^{\alpha+4}\ldots g^{\alpha+p-3})$$

is the same as $(1\,g^2\,g^4\ldots g^{p-3})$, so that, for every α, we may set up a correspondence between 0 and g^{α}, 1 and $g^{\alpha+2}, \ldots, q-1$ and $g^{p-3+\alpha}$; that is,

$$z \longrightarrow g^{\alpha+2z}.$$

In other words, the representation for B in 2.7 can be mapped on the first cycle of the representation for B in 2.5.

https://doi.org/10.4153/CJM-1955-004-3 Published online by Cambridge University Press

Then, in the representation for C in 2.7, in which $y' = m^s y$, we have

$$\begin{tikzcd} y \arrow[r] \arrow[d, leftrightarrow] & m^s y \arrow[d, leftrightarrow] \\ x = g^{\alpha+2y} \arrow[r] & g^{\alpha+2m^s y} = (x\,g^{-\alpha})^{m^s}.g^{\alpha} = g^{\alpha(1-m^s)}x^{m^s}. \end{tikzcd}$$

Now, let β be an arbitrary odd integer, and proceed as above with the second cycle of $B = (1\, g^2 \ldots g^{p-3})(g\, g^3 \ldots g^{p-2})$. We may again set up, for every β, a correspondence

$$z \longrightarrow g^{\beta+2z},$$

which maps the representation for B in 2.7 on the second cycle of the representation for B in 2.5. Then, under the permutation C, $y' = m^s y$, we have

$$x \longrightarrow g^{\beta(1-m^s)}x^{m^s}.$$

Now, for the first cycle of B in 2.5, that consisting of residues mod p, we set $z \longrightarrow g^{\alpha+2z}$ and see that under C the same elements map as follows:

$$x \longrightarrow g^{\alpha(1-m^s)}x^{m^s}.$$

For the second cycle of B, that consisting of non-residues mod p, we set $z \longrightarrow g^{\beta+2z}$ and find that under C the elements follow the mapping

$$x \longrightarrow g^{\beta(1-m^s)}x^{m^s}.$$

In other words, we demand that residues map on residues, non-residues on non-residues, and obtain the following representation on p symbols for C:

2.9
$$x' = g^{\alpha(1-m^s)}x^{m^s}, \qquad \epsilon = +1,$$
$$x' = g^{\beta(1-m^s)}x^{m^s}, \qquad \epsilon = -1.$$

It is easily shown that the choice of l among those numbers belonging to r mod q is an arbitrary one, and further that the same permutation C is obtained, with possibly a different order in the cycles, from different choices of pairs α and β. We may fix α, and then there will be q choices for β. So we obtain q permutations C. Indeed we might fix α at zero and have

2.10 $$C\colon\ x' = \tfrac{1}{2}(1+\epsilon)\,x^l + \tfrac{1}{2}(1-\epsilon)\,g^{\beta(1-l)}x^l.$$

C consists of $2s$ cycles of length r, and so is an even permutation. The elements 0, 1, and g^{β} remain fixed under C. A and B are even permutations, so the group $\{A, B, C\}$ consists entirely of even permutations.

In the above development of the permutation C, we required that residues mod p map on residues, non-residues on non-residues. This is not necessary; we might have obtained a representation for C by mapping residues on non-residues. C then takes the form

2.11 $$C\colon\ x' = \tfrac{1}{2}(1+\epsilon)\,g^{\beta}x^l + \tfrac{1}{2}(1-\epsilon)\,g^{-\beta l}x^l.$$

https://doi.org/10.4153/CJM-1955-004-3 Published online by Cambridge University Press

Since C consists of $2s$ cycles of length r, along with the transposition $(1\ g^{\beta})$, it is an odd permutation. Summarizing, we have

LEMMA 2.1. *The groups $\{A, B, C\}$ fall into two classes: those groups consisting entirely of even permutations generated with*

$$C: \begin{array}{ll} x' = x^{l}, & \epsilon = +1; \\ x' = g^{\beta(1-l)}x^{l}, & \epsilon = -1; \end{array}$$

and those groups consisting of even and odd permutations generated with

$$C: \begin{array}{ll} x' = g^{\beta}x^{l}, & \epsilon = +1; \\ x' = g^{-\beta l}x^{l}, & \epsilon = -1. \end{array}$$

We refer to these two classes as case I and case II, respectively, of our problem.

3. Certain relations among the groups $\{A, B, C\}$. For fixed p, q, and r, a set of $\frac{1}{2}(p+1)$ groups is obtained depending on the choice of β used in the permutation C. These groups are not all distinct up to isomorphism. The following lemma applies to these sets of groups.

LEMMA 3.1. (i) *In case* I, *for fixed p, the groups $\{A, B, C\}$ with $r = (q-1)/ks$ are respectively subgroups of the groups with $r = (q-1)/s$.*

(ii) *In case* II, *for fixed p, if the period of C is an odd multiple of the period of C', the groups $\{A, B, C'\}$ are respectively subgroups of the groups $\{A, B, C\}$.*

(iii) *In case* II, *for fixed p, the groups with $r = 2^{\lambda}\pi$, where $\lambda > 1$ and π is a product of powers of odd primes, contain as subgroups the corresponding groups from case* I, $r = 2$.

Consider part (i). This says that for $r = (q-1)/ks$ we have a set of $\frac{1}{2}(p+1)$ groups, and for $r = (q-1)/s$ we have a second set of $\frac{1}{2}(p+1)$ groups. There is a one-to-one correspondence between the two sets such that each group of the first set is a subgroup of one of the groups of the second set. An expression can be found relating these two sets, but this is not necessary for our application of the lemma. Similar statements apply to parts (ii) and (iii).

Part (i) follows by taking the kth power of the permutation C of period $r = (q-1)/s$,

$$C^{k}: \begin{array}{ll} x' = x^{m^{ks}}, & \epsilon = +1, \\ x' = g^{\beta(1-m^{ks})}x^{m^{ks}}, & \epsilon = -1, \end{array}$$

and pointing out that this is the permutation C obtained for $r = (q-1)/ks$.

In case II, r must necessarily be even if C, of order r, is to be odd. C is given by

$$C: \begin{array}{ll} x' = g^{\beta}x^{l}, & \epsilon = +1, \\ x' = g^{-\beta l}x^{l}, & \epsilon = -1, \end{array}$$

https://doi.org/10.4153/CJM-1955-004-3 Published online by Cambridge University Press

and is of order $(q-1)/s$. Taking powers of C we obtain

$$C^{2k}: \begin{array}{ll} x' = x^{l^{2k}}, & \epsilon = +1, \\ x' = g^{\beta(1-l^{2k})}x^{l^{2k}}, & \epsilon = -1, \end{array}$$

and

$$C^{2k+1}: \begin{array}{ll} x' = g^{\beta}x^{l^{2k+1}}, & \epsilon = +1, \\ x' = g^{-\beta l^{2k+1}}x^{l^{2k+1}}, & \epsilon = -1. \end{array}$$

Obviously, only odd powers of C yield another odd permutation. Since C^{2k+1} is simply the permutation C obtained with $r = (q-1)/(2k+1)s$, we see that part (ii) of our lemma follows.

Finally, consider case II with $r = 2^{\lambda}\pi$, $\lambda > 1$, π a product of powers of odd primes. C is now given by

$$C: \begin{array}{ll} x' = g^{\beta}x^{l}, & \epsilon = +1, \\ x' = g^{-\beta l}x^{l}, & \epsilon = -1, \end{array}$$

implying

$$C^{\frac{1}{2}r}: \begin{array}{ll} x' = x^{l^{r/2}} & \epsilon = +1, \\ x' = g^{\beta(1-l^{r/2})}x^{l^{r/2}}, & \epsilon = -1. \end{array}$$

where $l^r \equiv 1 \bmod q$, and hence $l^{\frac{1}{2}r} \equiv q - 1 \bmod q$. Then

$$\beta(1 - l^{\frac{1}{2}r}) \equiv \beta(2-q) \bmod q.$$

As β runs over the odd numbers from 1 to $p-2$, $\beta(2-q) \bmod p-1$ does also. Hence the permutation $C^{\frac{1}{2}r}$ will be the same permutation C as in case I for $r = 2$, viz.,

$$C: \begin{array}{ll} x' = x^{q-1}, & \epsilon = +1, \\ x' = g^{\beta}x^{q-1}, & \epsilon = -1, \end{array}$$

and part (iii) of the lemma is demonstrated.

4. Certain properties of the groups $\{A, B, C\}$.

THEOREM 4.1. *In case* I, $\mathfrak{H} = \{A, B, C\}$ *is a simple group. In case* II, $\mathfrak{H}$ *contains a simple subgroup of index two.*

THEOREM 4.2. *The order of* $\{A, B, C\}$ *is* $h = \delta pq(1 + np)$, *where* $\delta = 1$ *in case* I *and* $\delta = 2$ *in case* II.

It is known **(1; 4)** that if a permutation group of prime degree p contains an element A of period p, such that the only elements commuting with A are its own powers, then the order of the group is $p(p-1)(1+np)/t$, where p is the period of A, t the number of conjugate classes in $\{A\}$, and $1 + np$ the number of Sylow subgroups of order p.

Now certainly in a group on p symbols, any cycle of length p commutes only with its own powers. Hence the order of $\{A, B, C\}$ has the above form.

LEMMA 4.1. *There are at most two conjugate sets in* $\{A\}$.

For $B^{-1}AB = A^j$ and hence $A \sim \ldots \sim A^{j^{q-1}} \sim A^{j^q} = A, A^g \sim A^{gj} \sim \ldots .$

LEMMA 4.2. *In case* I, *there are exactly two conjugate sets in* $\{A\}$.

If $X^{-1}AX = A^g$, then, using the same procedure as in §2, X can be shown to have the form

$$X = (0 \;\; u \;\; u + gu \quad u + gu + g^2u \ldots);$$

that is, X is a cycle of order $p - 1$. Such a cycle is odd and not possible in case I.

Thus in case I, $t = 2$, and $h = pq(1 + np)$.

LEMMA 4.3. *The orders of the first and second commutator groups* $\mathfrak{H}'$ *and* $\mathfrak{H}''$ *contain the factor* p.

$A^{-1}B^{-1}AB = A^{j-1}$, so $\mathfrak{H}'$ contains a power, and hence all powers, of A. Also $B^{-1}C^{-1}BC = B^{l-1}$ and so $\mathfrak{H}'$ contains B. Thus $\mathfrak{H}' > \{A, B\}$, and pq divides h'. Similarly $\mathfrak{H}'' > \{A\}$, and the order of the second commutator subgroup, h'', is divisible by p.

LEMMA 4.4. *In case* I, *the commutator subgroup* $\mathfrak{H}'$ *is equal to* $\mathfrak{H}$.

According to Brauer we have three possibilities:

(1) $\mathfrak{H}$ has a normal subgroup of order $1 + np$; $t = p - 1$. This is impossible, since in case I, $t = 2$ and in case II, $t \leqslant 2$.

(2) $\mathfrak{H}$ has a normal subgroup of order $1 + np$; $t \leqslant p - 1$ and $\mathfrak{H}' \neq \mathfrak{H}''$, $\mathfrak{H}''$ has order $1 + np$, $\mathfrak{H}'$ has order $p(1 + np)$. This possibility is ruled out since, by the preceding lemma, $p|h''$.

We have then the third possibility holding, viz.,

(3) $\mathfrak{H}$ does not contain a normal subgroup of order $1 + np$, and $\mathfrak{H}'$ has order

$$h' = p\frac{p-1}{t'}(1 + np),$$

where $t|t', t'|p - 1$, and $t \leqslant t' < p - 1$. Further, $\mathfrak{H}' = \mathfrak{H}''$, and the group $\mathfrak{H}/\mathfrak{H}'$ is cyclic. Here t' denotes the number of classes of conjugate elements in H' which contain elements of order p.

Now in case I, $t = 2$; so t' is even, and, since $p - 1 = 2q$, with $t' < p - 1$, we have $t' = 2$. Thus $h' = h$ and $\mathfrak{H} = \mathfrak{H}'$.

LEMMA 4.5. *In case* II, *there is only one conjugate set in* $\{A\}$.

In case II, the commutator subgroup is a normal subgroup, proper or improper, of $\mathfrak{H}$. But it consists entirely of even permutations, and so $\mathfrak{H}'$ is properly contained in $\mathfrak{H}$. Now $t \neq 2$, since otherwise $\mathfrak{H} = \mathfrak{H}'$. So in case II, $t = 1$, and $h = 2pq(1 + np)$, completing the proof of Theorem 4.2.

https://doi.org/10.4153/CJM-1955-004-3 Published online by Cambridge University Press

LEMMA 4.6. *In case* II *the commutator subgroup* $\mathfrak{H}'$ *consists of all the even permutations in* $\mathfrak{H}$ *and has index two in* $\mathfrak{H}$.

For, the commutator subgroup has order

$$h' = p\frac{p-1}{t'}(1 + np).$$

We proved $pq|h'$. Also $t|t'|p - 1$, $t \leqslant t' < p - 1$. The only possibilities for t' are 1, 2, q. But $t' \neq 1$, as $h' < h$. And $t' \neq q$, since $B^{-1}AB = A^j$ in $\mathfrak{H}'$ and so $t' \leqslant 2$. Thus $t' = 2$ and $\mathfrak{H}'$ is the subgroup of index 2 consisting of all even permutations.

Brauer has shown in the same paper that $\mathfrak{H}'$ is a simple group. But in case I, $\mathfrak{H}' = \mathfrak{H}$, and so $\mathfrak{H}$ is a simple group. In case II, $\mathfrak{H}''$ is a simple group and $\mathfrak{H}$ is like the symmetric group in that it contains a simple subgroup of index 2. Thus Theorem 4.1 is proved.

5. Case I, r even, $\beta = q$.

THEOREM 5.1. *The groups generated for* $r = 2$, $\beta = q$, *in case* I *are the alternating groups* $\mathfrak{A}_p$.

Here we have

$$C: \quad x' = \tfrac{1}{2}(g^\beta + 1)\,x^l - \tfrac{1}{2}(g^\beta - 1)\,x^{l+q},$$

and for $\beta = q$, $r = 2$, $l = q - 1$

$$C: \quad x' = x^{2q-1} = 1/x$$

$(x \neq 0)$. C leaves 0, 1 and -1 invariant.

Under the permutation $A^{-1}CA\ CA^{-1}C$, $x \rightarrow -x$ for $x \neq 0, 1$, and

$$0 \rightarrow -1, \quad -1 \rightarrow 1, \quad 1 \rightarrow 0.$$

This permutation, therefore, contains the cycle $(0\ -1\ 1)$, and the remaining elements form transpositions, since $A^{-1}CA\ CA^{-1}C$ is of period 2. Since $p = (p - 3) + 3 = 2m + 3$, all elements are involved, and

$$A^{-1}CA\ CA^{-1}C = (0\ -1\ 1)(\text{product of transpositions}).$$

Squaring this permutation leaves the cycle $(0\ 1\ -1)$. Applying Netto's Theorem **(5)**, "If a transitive group of degree n contains a circular permutation of prime order $q < \frac{2}{3}n$, then the group is either non-primitive, or it contains the alternating group," we see that $\mathfrak{H} = \mathfrak{A}_p$, since $\mathfrak{H}$ is primitive. (In this case, the presence of the cycle $(0\ 1\ 2\ldots p - 1)$ and the triplet $(0\ 1\ p - 1)$ is sufficient for the proof that $\mathfrak{H} = \mathfrak{A}_p$.)

Now since the groups generated for even values of r with $\beta = q$ contain the groups generated for $r = 2$, $\beta = q$, from Lemma 3.1, part (i), we have at once

COROLLARY 5.1. *The groups generated for even values of* r, $\beta = q$, *case* I *are the alternating groups* $\mathfrak{A}_p$.

6. The groups $\{A, B, C\}$, case II. For fixed p, q is fixed, and we consider the possibilities for r. We have seen that in case II, r must be even. Then $r = 2$, an odd multiple of 2, or an even multiple of 2.

THEOREM 6.1. *If $r = 2$ in case* II, *the groups $\{A, B, C\}$ are the symmetric groups $\mathfrak{S}_p$.*

For in case II we may write

$$C:\quad x' = \tfrac{1}{2}(g^{\beta} + g^{-\beta l})\,x^{l} + \tfrac{1}{2}(g^{\beta} - g^{-\beta l})\,x^{l+q};$$

and for $r = 2$, $l = q - 1$, $g^{-\beta l} = g^{-\beta(q-1)} \equiv - g^{\beta}$; hence we have

$$C:\quad x' = g^{\beta}x^{2q-1}.$$

For $x \neq 0$, this can be written $x' = g^{\beta}/x$.

Consider the permutation

$$R = A^{-1}CA^{g^{\beta}}CA^{-1}:\quad x' = -\,1/x, \qquad\qquad x \neq 0, 1.$$

Under this permutation, $0 \to -\,1$, $-1 \to 1$, $1 \to 0$, and in standard form $R = (0\ {-1}\ 1) \cdot$ (product of transpositions). Then $R^2 = (0\ 1\ {-1})$, $A^{-1}\,R^2\,A = (0\ 1\ 2)$; this permutation and $A = (0\ 1\ 2 \ldots p - 1)$ generate $\mathfrak{A}_p$. Since C itself is an odd permutation, $\{A, B, C\} = \mathfrak{S}_p$.

COROLLARY. *If r is an odd multiple of* 2 *in case* II *the groups $\{A, B, C\}$ are the symmetric groups $\mathfrak{S}_p$.*

This follows immediately from Lemma 3.1, part (ii), and Theorem 6.1.

THEOREM 6.2. *If $r = 2^{\lambda}\pi$, $\lambda > 1$, π odd, in case* II, *the groups $\{A, B, C\}$ are the symmetric groups $\mathfrak{S}_p$.*

It follows from Lemma 3.1, part (iii), that for fixed p, and for C with $r = 2^{\lambda}\pi$, the permutations $C^{\frac{1}{2}r}$ are the same as those obtained in case I with $r = 2$, viz.,

$$C^{\frac{1}{2}r}:\quad \begin{array}{ll} x' = x^{q-1}, & \qquad\qquad \epsilon = +\,1, \\ x' = g^{\beta}x^{q-1}, & \qquad\qquad \epsilon = -\,1. \end{array}$$

Then if $\beta = q$, $\{A, B, C\}$ must contain $\mathfrak{A}_p$, from Theorem 5.1; hence $\{A, B, C\}$ is $\mathfrak{S}_p$.

In the following we will assume $\beta \neq q$. In Lemma 4.5 we proved that in case II, there is only one conjugate set in $\{A\}$. Then $\mathfrak{H}$ must contain an element S such that $S^{-1}\,AS = A^{g}$. Such an S must be of the form

$$S:\quad x' = u + gx, \qquad\qquad u \text{ fixed},$$

and under $SA^{-u}\,B^{\frac{1}{2}(q-1)}$, $x \to -\,x$. That is, in case II, $\mathfrak{H}$ contains the permutation

$$T:\ x' = -\,x.$$

https://doi.org/10.4153/CJM-1955-004-3 Published online by Cambridge University Press

The permutation $C^{\frac{1}{2}r}$ leaves 0 fixed and, for $x \neq 0$, may be written

$$C^{\frac{1}{2}r}: \quad \begin{array}{ll} x' = 1/x, & \epsilon = +1, \\ x' = -g^{\beta}/x, & \epsilon = -1. \end{array}$$

Then

$$C^{\frac{1}{2}r}T: \quad \begin{array}{ll} x' = -1/x, & \epsilon = +1, \\ x' = g^{\beta}/x, & \epsilon = -1, \end{array}$$

maps quadratic residues mod p on quadratic non-residues, quadratic non-residues on quadratic residues, and leaves 0 fixed. Squaring this permutation we obtain

$$(C^{\frac{1}{2}r}T)^2: \quad \begin{array}{ll} x' = g^{q+\beta}x, & \epsilon = +1, \\ x' = g^{q-\beta}x, & \epsilon = -1, \end{array}$$

$(x \neq 0)$. (Note here that if $\beta = q$, this permutation is the identity.) Finally,

$$(C^{\frac{1}{2}r}T)^2\, B^{\frac{1}{2}(q+\beta)}: \quad \begin{array}{ll} x' = g^{2\beta}x, & \epsilon = +1, \\ x' = x, & \epsilon = -1, \end{array}$$

is a cyclic permutation of period q, viz.,

$$(1\ g^{2\beta}\ g^{4\beta} \ldots g^{2\beta(q-1)})$$

and applying Netto's theorem we obtain $\mathfrak{H} = \mathfrak{S}_p$.

7. Conclusion. It had been hoped that groups other than $\mathfrak{A}_p$, possibly multiply transitive groups such as the Mathieu groups $\mathfrak{M}_{11}$ and $\mathfrak{M}_{23}$, might appear in case I, but investigations have so far failed to produce any such groups.

References

1. R. Brauer, *On permutation groups of prime degree and related classes of groups*, Ann. Math., *44* (1943), 59–79.
2. R. D. Carmichael, *Abstract definitions of the symmetric and alternating groups and other permutation groups*, Quarterly J. Math., *49* (1923), 226–283.
3. ———, *Introduction to the theory of groups of finite order* (New York, Ginn and Co., 1937).
4. E. Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, J. Math. pur. et app. (2), *6* (1861), 241–323.
5. E. Netto, *The theory of substitutions*, tr. F.N. Cole (Ann Arbor, Michigan, Inland Press, Register Publishing Co., 1892).
6. R. G. Stanton, *The Mathieu groups*, Can. J. Math., *3* (1951), 164–174.

Royal Military College of Canada

https://doi.org/10.4153/CJM-1955-004-3 Published online by Cambridge University Press