ON A THEOREM OF BURNSIDE

BY

RICHARD BRAUER[1]

A celebrated theorem of Burnside states that the order g of a non-cyclic finite simple group G is divisible by at least three distinct prime numbers. In other words, if we set $g = p^a q^b g_0$ where p and q are primes and a, b, g_0 are positive integers, then $g_0 > 1$. We prove a refinement.

THEOREM 1. *Let G be a simple group of finite order*

$$g = p^a q^b g_0 \tag{1}$$

where p, q are distinct primes, and where a, b, g_0 are integers, $a > 0$. If $g \neq p$, then

$$g_0 - 1 > \log p / \log 6. \tag{2}$$

Proof. We denote the irreducible characters of G by $\chi_1 = 1, \chi_2, \cdots$ and set $x_j = \chi_j(1)$. Let $\mathfrak{p}$ be a prime ideal divisor of p in the field of g-th roots of unity. If $\sigma \in G$, denote by $c(\sigma)$ the order of the centralizer $C(\sigma)$ of $\sigma \in G$. The principal p-block $B_0(p)$ of G consists of those characters χ_n for which

$$(g/c(\sigma))(\chi_n(\sigma)/x_n) \equiv g/c(\sigma) \pmod{\mathfrak{p}} \tag{3}$$

for every $\sigma \in G$. If $\tau \in G$ has an order divisible by p, then by Theorem VIII of [4],

$$\sum\nolimits_{\chi_n \in B_0(p)} x_n \chi_n(\tau) = 0. \tag{4}$$

Of course, $\chi_1 \in B_0(p)$. Now (4) shows that there exist $\chi_j \in B_0(p)$ with $j \neq 1$ for which x_j is not divisible by q. Let p^h be the highest power of p dividing x_j so that

$$x_j = p^h m, \qquad m \mid g_0 . \tag{5}$$

Let X_j denote the irreducible representation of G with the character χ_j. Since G is simple and $j \neq 1$, X_j is a faithful representation. It follows from a theorem of Feit and Thompson [5] that $p \leqq 2x_j + 1$.

If $h = 0$, then $x_j = m \leqq g_0$. Hence $p \leqq 2g_0 + 1$, that is, $g_0 \geqq (p-1)/2$. This implies (2) for $p \geqq 5$. Since $g_0 \geqq 2$, (2) also holds for $p \leqq 3$.

Assume now that $h > 0$. Take σ as an element of order p in the center of a p-Sylow subgroup P of G. Then $g/c(\sigma)$ is not divisible by p. The left side of (3) represents an algebraic integer. It follows that $\chi_j(\sigma)$ is divisible by p^h in the ring of algebraic integers and that

$$\chi_j(\sigma)/p^h \equiv x_j/p^h = m \pmod{\mathfrak{p}}. \tag{6}$$

Received January 17, 1967.

[1] This work has been supported by a National Science Foundation grant.

Let ε be a primitive p-th root of unity. If a_n is the multiplicity of ε^n as characteristic root of $X_j(\sigma)$, we have

$$x_j = \sum_{n=0}^{p-1} a_n , \qquad \chi_j(\sigma) = \sum_{n=0}^{p-1} a_n \varepsilon^n = \sum_{n=1}^{p-1} (a_n - a_0)\varepsilon^n.$$

Now, $\varepsilon, \varepsilon^2, \cdots, \varepsilon^{p-1}$ form an integral basis for the integers in the field of the p-th roots of unity. Hence each $a_n - a_0$ is divisible by p^h, say

$$a_n = a_0 + p^h b_n .$$

Then

$$x_j = pa_0 + p^h \sum_{n=1}^{p-1} b_n , \qquad \chi_j(\sigma) = p^h \sum_{n=1}^{p-1} b_n \varepsilon^n.$$

It now follows from (5) that pa_0 is divisible by p^h. Since $\varepsilon \equiv 1 \pmod{\mathfrak{p}}$, (6) shows that $pa_0/p^h \equiv 0 \pmod{p}$. This means that a_0 and then all a_n are divisible by p^h.

Thus all characteristic roots of $X_j(\sigma)$ have a multiplicity divisible by p^h. In particular, $X_j(\sigma)$ has at most $x_j/p^h = m$ distinct characteristic roots.

We say that an irreducible representation X of a finite group G is *quasi-primitive*, if for every normal subgroup H of G the restriction $X \mid H$ does not have non-equivalent irreducible constituents. In particular, if G is simple, every non-principal irreducible representation is quasi-primitive. It has been proved by Blichfeldt [1, Theorem 9, p. 101] that if X is a faithful quasi-primitive representation of degree x of a group G and if for an element σ of G of order p not in the center of G the transformation $X(\sigma)$ has w distinct characteristic roots, then

$$p < 6^{w-1}.$$

Actually, Blichfeldt states his theorem only for primitive representations, but his proof remains valid for quasi-primitive representations as defined above. Applying this with $X = X_j$ we obtain

$$\log p < (w - 1) \log 6 \leqq (m - 1) \log 6 \leqq (g_0 - 1) \log 6$$

and this implies (2).

As a corollary, we note:

THEOREM 1*. *If G is a finite group of order* (1) *and if G is not p-solvable, the inequality* (2) *holds.*

Indeed, we may assume that G is not simple. Let H be a non-trivial normal subgroup of G. At least one of the groups H and G/H is not p-solvable and we can use induction.

It is likely that the lower bound (2) in these theorems can be improved substantially. We can prove this when the p-Sylow group P of G is of certain special types.

THEOREM 2. *Let G be a group of an order $g = p^a q^b g_0$ as in* (1) *and assume* *that G is not p-solvable. If the p-Sylow group P of G is abelian then*

$$g_0 \geqq \sqrt{\frac{p-1}{2}}. \tag{7}$$

Proof. Again, it will suffice to prove this for simple groups G. Choose X_j as in the proof of Theorem 1. If again $x_j = DgX_j$ has the form (5) and if $h = 0$, then as we have seen above, $g_0 \geqq (p-1)/2$ and this implies (7) for $p \neq 2$. The case $p = 2$ is trivial.

Suppose that $h > 0$. Since the p-Sylow subgroups of G are abelian, the method in the proof of Theorem 1 applies for any element $\sigma \in G$ of order p. It follows that $X_j(\sigma)$ has at most g_0 distinct characteristic roots. Now a method of Speiser [6, Theorem 202] shows that if $2g_0^2 < p - 1$, the set of elements of G of order 1 or p forms a normal subgroup of G and this leads to a contradiction. Again, (7) must hold.

Remarks. 1. The preceding proof still applies, if G is a simple group with a non-abelian p-Sylow group P satisfying the following condition: If Y is a faithful (reducible or irreducible) representation of G and if σ is an element of order p of P not belonging to the center of P, then $Y(\sigma)$ has more than $(p-1)/2$ distinct characteristic roots. For instance, this condition is satisfied, when P is a non-abelian group of order p^3.

2. Other theorems of a similar type are given in [2].

If g_0 in Theorem 1 is a fixed number, then there are only finitely many possibilities for p and for q. One may conjecture that there exist only finitely many simple groups G of an order (1) with a given value of g_0. We can only prove this for groups G with abelian p-Sylow groups P of given rank.

THEOREM 3. *Let G be a simple group of order g of the form* (1) *considered in Theorem* 1. *Assume that the p-Sylow group P is abelian of rank N. Then there exists a bound $\beta(g_0, N)$ depending only on the integers g_0 and N only such that*

$$g \leqq \beta(g_0, N).$$

Proof. Again, determine X_j as in the proof of Theorem 1. If $x_j = Dg\ X_j$ is given by (3), then X_j is of height h. It follows that h lies below a bound $\beta_1(N)$ depending on p and N; (cf. [3]). Then x_j lies below a bound depending on g_0 and N. Now, Jordan's theorem (cf. [1]) implies the existence of bounds $\beta(g_0, N)$ as stated in the theorem.

REFERENCES

1. H. F. BLICHFELDT, *Finite collineation groups*, University of Chicago Press, Chicago, 1917.
2. R. BRAUER, *On some conjectures concerning finite simple groups*, Studies in mathematical analysis and related topics, Stanford University Press, Palo Alto, 1962.
3. ———, *On blocks and sections in finite groups II*, Amer. J. Math., to appear.

4. R. Brauer and C. Nesbitt, *On the modular characters of groups of finite order*, University of Toronto Studies, Mathematical Series no. 4, 1937.
5. W. Feit and J. G. Thompson, *On groups which have a faithful representation of degree less than* $(p - 1)/2$, Pacific J. Math., vol. 4 (1961), pp. 1257–1262.
6. A. Speiser, *Theorie der Gruppen von endlicher Ordnung*, third edition, Springer, Berlin, 1937.

Harvard University
Cambridge, Massachusetts