A NOTE ON THEOREMS OF BURNSIDE AND BLICHFELDT

RICHARD BRAUER

1. The irreducible constituents of the tensor powers of a representation of a group. In his book [3], W. Burnside proved the following theorem (Theorem IV of Chapter XV):

Theorem 1. Let $G$ be a finite group and let $X$ be a faithful representation of $G$ over the field $\mathbb{C}$ of complex numbers. Each irreducible representation $X_\lambda$ of $G$ appears as a constituent in some tensor power of $X$.

Recently, R. Steinberg [5] has given a very simple proof of this theorem generalizing it at the same time. I shall give still another proof of Theorem 1. While this proof is less conceptual than Steinberg's proof, it is very short, and it refines the theorem in another direction.

Theorem 1*. Assume that the character $\chi$ of the representation $X$ in Theorem 1 takes on a total of $r$ distinct values $a_1, a_2, \ldots, a_r$ on $G$. Each irreducible character $\chi_\lambda$ of $G$ appears as a constituent of one of the characters $\chi_0 = 1, \chi, \chi^2, \ldots, \chi^{r-1}$.

Proof. Let $A_i$ be the set of elements $g \in G$ for which $\chi(g) = a_i$. Choose $g_i \in A_i$. If $\chi_\lambda$ is not contained in $\chi^i$, then

$$|G| (\chi^i, \chi_\lambda) = \sum_{i} \chi^i(g_i) \sum_{\xi \in A_j} \bar{\chi}_\lambda(g) = 0.$$

If this holds for $i = 0, 1, \ldots, r - 1$, it follows from the nonvanishing

Received by the editors December 1, 1962.
of the Vandermonde determinant that the inner sum vanishes for all \(j\). Since \(X\) is faithful, one of the \(A_j\) consists only of the unit element, and we would have \(D_g \chi_A = \chi_A(1) = 0\), which is absurd.

2. **Remarks.**

1. If \(n = D_g \chi\), it follows from Theorem 1* that the sum of the degrees of the irreducible representations of \(G\) is at most equal to

\[
s = 1 + n + n^2 + \cdots + n^{r-1}.
\]

This implies that the order \(|G|\) of \(G\) is at most equal to \(s^2\).

2. If it is known that all values of \(\chi\) lie in a fixed algebraic number field \(K\) of finite degree over the field \(\mathbb{Q}\) of rational numbers, then since \(|\chi(g)|\) and all its algebraic conjugates are at most equal to \(n\) for \(g \in G\), it follows that \(r\) lies below a bound depending only on \(K\) and \(n\). Hence \(|G|\) also lies below bounds depending only on \(K\) and \(n\). The existence of such bounds has first been observed by I. Schur [4]. We do not obtain here the sharp values given by Schur.

3. The proof of Theorem 1* shows that instead of \(1, \chi, \cdots, \chi^{r-1}\), we may take any \(r\) consecutive powers of \(\chi\). If \(\chi\) assumes the value 0, even \(r-1\) consecutive powers of \(\chi\) with positive exponents will do.

4. If \(C\) is replaced by an algebraically closed field \(K\) of prime characteristic \(p\), the same result will hold for the irreducible representations \(X_\lambda\) of \(G\) in \(K\). If we take for \(\chi\) the character of the indecomposable component of the regular representation, associated with \(X_\lambda\), the same proof applies. Here, \(a_1, a_2, \cdots, a_r\), are to be taken as the values assumed by \(\chi\) for \(p\)-regular elements of \(G\). (See [2] for the basic properties of "modular" characters.)

5. The proof of Theorem 1* remains the same if \(C\) is replaced by an algebraically closed field \(K\) of characteristic 0. It is immediate that here and in Remark 4 the condition that \(K\) be algebraically closed can be dropped.

3. A result on the conjugates of a character. We show now

**Theorem 2.** Let \(\chi\) be an irreducible character of a finite group \(G\). Let \(\Omega\) be the field obtained by adjoining the values of \(\chi\) to the field \(\mathbb{Q}\) of rational numbers and let \(\Gamma\) be the Galois group of \(\Omega\) over \(\mathbb{Q}\). If \(\theta_1, \theta_2, \cdots, \theta_n\) is a system of \(n\) elements of \(\Gamma\), we have one of the following two cases.

**Case A.** There exists an element \(g \in G\) such that \(\theta_i \chi(g) \neq \chi(g)\) for \(i = 1, 2, \cdots, n\).

**Case B.** There exists a product \(\theta_\alpha \theta_\beta \cdots \theta_\rho\) with \(1 \leq \alpha < \beta < \cdots < \rho \leq n\) with an odd number of factors which leaves \(\chi\) invariant.

**Proof.** If \(\xi\) is an element of the group ring of \(\Gamma\) over the ring of
rational integers, we define $\xi \cdot \chi$ in the natural manner by linearity. Note that $\theta_i \theta_j = \theta_j \theta_i$. Form

$$P = \prod_i (1 - \theta_i) \cdot \chi.$$ 

If there exists an element $g \in G$ with $P(g) \neq 0$, we must have $\theta_i\chi(g) \neq \chi(g)$ for all $i$ and this leads to Case A. If $P$ vanishes identically, this yields

$$\sum_{i<j} \theta_i \theta_j \chi + \cdots = \sum_i \theta_i \chi + \sum_{i<j<k} \theta_i \theta_j \theta_k \chi + \cdots.$$ 

It follows that the irreducible character $\chi$ appears on the right and this means that we have the result of Case B.

**Remark.** It is trivial that Theorem 2 remains valid, if $\Omega$ is replaced by a larger field normal over $\mathbb{Q}$.

### 4. Existence of elements of certain orders in $G$

It will be convenient to say that a number $\omega$ "requires" the $m$th roots of unity, if $\omega$ lies in the field of the $m$th roots of unity over $\mathbb{Q}$, and if $m$ is the least positive integer for which this is true. If $m$ here is even, it will be divisible by 4. We shall also say that a character $\chi$ "requires" the $m$th roots of unity, if all values of $\chi$ lie in the field of the $m$th roots of unity, and if again $m$ cannot be replaced by a smaller integer.

We now give some corollaries of Theorem 2. The first one is due to Blichfeldt [1] and Burnside [3, Theorem X of Chapter XVI].

**Corollary 1.** Let $\chi$ be an irreducible character of a finite group. Let $\pi_1, \pi_2, \ldots, \pi_n$ be distinct primes, and assume that there exist elements $g_1, g_2, \ldots, g_n$ of $G$ such that $\chi(g_i)$ requires the $\pi_i^{th}$ roots of unity for some $a_i > 0$, $i = 1, 2, \ldots, n$. Then $G$ contains elements of order $\pi_1^{a_1} \pi_2^{a_2} \cdots \pi_n^{a_n}$.

**Proof.** Let $\Omega$ be the field of the $|G|$th roots of unity over $\mathbb{Q}$ (see the Remark in 3). If $\pi_i$ divides $|G|$ with the exact exponent $r_i$, $(i = 1, 2, \cdots, n)$, then $a_i \leq r_i$. Let $\Omega_i$ be the field of the $(|G|/\pi_i^{a_i}$)st roots of unity over $\mathbb{Q}$. Since $\chi(g_i) \in \Omega_i$, we can find an element $\theta_i$ of the Galois group of $\Omega$ over $\Omega_i$ such that $\theta_i \chi(g_i) \neq \chi(g_i)$. On the other hand, by construction $\theta_i \chi(g_i) = \chi(g_i)$ for $j \neq i$, $1 \leq j \leq n$. If we now apply Theorem 2, we cannot have Case B since a product $\theta_1 \theta_2 \cdots$ will not leave $\chi(g_a)$ fixed. Hence there exist $g \in G$ such that $\theta_i \chi(g) \neq \chi(g)$ for $i = 1, 2, \ldots, n$. Then $\chi(g) \in \Omega_i$, and this implies that the order of $g$ is divisible by $\pi_i^{a_i}$ for $i = 1, 2, \cdots, n$. This proves the corollary.

A similar method yields the slightly more general result.

**Corollary 2.** Let $\chi$ be an irreducible character of the finite group $G$
and assume that $G$ contains elements $g_1, g_2, \ldots, g_n$ such that $\chi(g_i)$ requires the $h_i$th roots of unity where the rational integers $h_1, h_2, \ldots, h_n$ are pairwise coprime. If $p_i^a$ is a prime power dividing $h_i$ then $G$ contains elements of order $p_1^a p_2^a \cdots p_n^a$.

Another result of the same type is the following one.

**Corollary 3.** Let $\chi$ be an irreducible character of the finite group $G$ which requires the $m$th roots of unity. Let $m_0$ be the product of those prime power factors $p_i^a$ of $m$ whose exponent $a_i$ is greater than 1. Then $G$ contains elements of order $m_0$.

**Proof.** Let $\Omega$ be the field of the $m$th roots of unity, and let $\Omega_i$ here be the field of the $(m/p_i)$th roots of unity with $p_i$ ranging over those primes for which $p_i^2 \mid m$. Then $\Omega$ is cyclic of degree $p_i$ over $\Omega_i$. Choose $\theta_i$ as a generator of the Galois group of $\Omega$ over $\Omega_i$. Suppose that a product $n$ of different $\theta_i$ left $\chi$ invariant. Since $\theta_i$ has order $p_i$ and $(p_i, p_j) = 1$ for $i \neq j$, each factor $\theta_i$ appearing in $n$ leaves $\chi$ fixed. Then $\chi$ would lie in $\Omega_i$ and this is not consistent with the choice of $m$.

Thus, we have Case A in Theorem 2. If $\theta_i(\chi(g)) \neq \chi(g)$ for all $i$ in question, then the order of $g$ is divisible by $p_i^a$ for all these $i$ and this proves the corollary.

There are still other results which can be obtained by this type of method, but it does not seem to be worthwhile to go into details. It should be mentioned that we have not used (1) fully in the proof of Theorem 2 and that more precise information is available. For instance, if $n = 3$ in Theorem 2, and if we do not have Case A, then either one of the $\theta_i$ leaves $\chi$ fixed, or the four elements $\theta_1^2, \theta_2^3, \theta_3, \theta_1 \theta_2 \theta_3$ all leave $\chi$ fixed.

**References**


*Harvard University*