THE EXPONENT AND THE PROJECTIVE REPRESENTATIONS OF A FINITE GROUP

BY

J. L. ALPERIN AND TZEE-NAN KUO[1]

Since the time of the first investigations of the projective representations of finite groups [4], [5] there have been two approaches to the subject. The first consists of the homological techniques originating with Schur's factor sets and the second is the relation between the projective representations of a group and the ordinary representations of a covering group. We shall give, by a combination of these methods, a new short proof of a theorem of Reynolds [3]. This will be accomplished by proving a result which is of a group-theoretic nature and of independent interest and which gives a connection between the structure of a group and its covering groups. Reynolds' theorem will then be deduced by applying results of Brauer [1] to the ordinary representations of these covering groups.

All groups mentioned throughout this paper will be assumed to be finite. If G is a group then we denote its center by $Z(G)$ and its derived group by G'. If H is a subgroup of G then $| G:H |$ is the index of H in G. The exponent of G is the least common multiple of the orders of the elements of G. Therefore, the exponent of G is the product of the exponents of the Sylow p-subgroups of G as p runs over the distinct prime divisors of the order $| G |$ of G.

An ordinary n-dimensional representation of G in the field F is a homomorphism of G into the general linear group $GL(n, F)$; a projective n-dimensional representation of G in the field F is a homomorphism of G into the projective general linear group $PGL(n, F)$, the quotient of $GL(n, F)$ by the group of scalar matrices. If no field F is mentioned then any representation, ordinary or projective, is assumed to be written in the field C of complex numbers. Let F be some subfield of C. If ρ is an ordinary n-dimensional representation of G then we say that ρ can be written in F provided there is S in $GL(n, C)$ such that $S^{-1}\rho(x)S$ is in $GL(n, F)$ for all x in G. If ρ is an n-dimensional projective representation of G then we say that ρ can be written in F provided there is S in $PGL(n, C)$ such that for each x in G the *coset* $S^{-1}\rho(x)S$ contains elements of $GL(n, F)$ for each x in F. We shall be interested in the field of m^{th} roots of unity, which is the subfield of C generated by a primitive m^{th} root of unity.

A covering group (or representation group) $\hat{G}$ of G is a group $\hat{G}$ and a homomorphism φ of $\hat{G}$ onto G such that the following two conditions are fulfilled:

(1) The kernel of φ is contained in $Z(\hat{G}) \cap \hat{G}'$.

(2) If n is any positive integer and ρ is an n-dimensional projective representation of G then there is an ordinary n-dimensional representation $\hat{\rho}$ of $\hat{G}$

Received May 26, 1966.

[1] This research was partially supported by a National Science Foundation grant.

such that $\rho \circ \varphi = \psi \circ \hat{\rho}$, where ψ is the natural homomorphism of $GL(n, C)$ onto $PGL(n, C)$.

Any such representation $\hat{\rho}$ will be said to "lift" ρ. A theorem of Schur [4] asserts that every group G possesses covering groups $\hat{G}$. Furthermore, as is well-known, the kernel of φ is isomorphic to $H^2(G, C^*)$, where C^* is the multiplicative group of C. Moreover, the following assertions hold [6, Prop. 3.3. (2) on p. 164 and (3) on p. 166)]: If φ is a homomorphism of the group E onto the group G with kernel K such that $K \leq Z(E) \cap E'$, then K is a homomorphic image of $H^2(G, C^*)$. In particular, the exponent of K divides the exponent of $H^2(G, C^*)$.

We can now state the results of this paper, the first of which is a purely group-theoretic result:

THEOREM 1. *If G is a finite group then the product of the exponents of $Z(G) \cap G'$ and $G/Z(G) \cap G'$ is a divisor of the index of $Z(G) \cap G'$ in G.*

This has the following immediate consequence, in as much as the exponent of G divides the product of the exponents given in the theorem.

COROLLARY. *If G is a finite group then the exponent of G is a divisor of the index of $Z(G) \cap G'$ in G.*

This latter result is all that we shall need for the application to projective representations. It is interesting to note that, whereas the theorem is proved by homological methods, the corollary has a direct proof using the commutator calculus. For this reason, we shall give a sketch of this alternative procedure.

Our other result is as follows:

THEOREM 2. (Reynolds [3]) *Any projective representation of a finite group G may be written in the field of the g^{th} roots of unity, where g is the order of G.*

Actually, Reynolds has proved a stronger result: he has given further details concerning the relevant factor sets. However, our approach does not yield any of this additional information.

We shall first derive Reynolds theorem from the corollary. Let ρ be an n-dimensional projective representation of the group G and let $\hat{G}$ be a covering group of G. Let $\hat{\rho}$ be an n-dimensional ordinary representation of $\hat{G}$ which lifts ρ. We know, by Brauer's theorem [1], that $\hat{\rho}$ may be written in the field F of e^{th} roots of unity, where e is the exponent of $\hat{G}$. Thus, there is an element T of $GL(n, C)$ such that $T^{-1}\hat{\rho}(x)T$ is an element of $GL(n, F)$ for all x in $\hat{G}$. Hence, $S^{-1}\rho(y)S$ is an element of $PGL(n, F)$ for all y in G, where S is the natural image of T in $PGL(n, C)$, and so we have shown that ρ may be written in the field F. In order to complete the proof we need only show that F is in fact, a subfield of the field of the g^{th} roots of unity, where g is as in the theorem. However, this will hold provided that e divides g. An application of the corollary to $\hat{G}$ shows the e is a divisor of $|\hat{G}:Z(\hat{G}) \cap \hat{G}'|$. This index is, in turn, a divisor of g, in as much as the kernel of the homomorphism of $\hat{G}$ onto G, which defines $\hat{G}$ as a covering group of G, is contained in $Z(\hat{G}) \cap \hat{G}'$.

We now turn to the proof of Theorem 1. Let $H = G/Z(G) \cap G'$ be of order h and exponent e and let f be the exponent of $Z(G) \cap G'$. We must show that f divides h/e so that, by the remarks before Theorem 1, it suffices to demonstrate that $H^2(H, C^*)$ is of exponent dividing h/e. For each prime divisor p of h let H_p be a Sylow p-subgroup of H and let h_p and e_p be the order and exponent of H_p, respectively. Thus $h = \prod h_p$, $e = \prod e_p$ as p runs over the distinct prime divisors of h. Hence, since $H^2(H, C^*)$ is a direct sum of subgroups of the groups $H^2(H_p, C^*)$ [2], it is enough to establish that, for each prime p, the exponent of $H^2(H_p, C^*)$ divides h_p/e_p. However, H_p is of order a power of p so there is a cyclic subgroup K of H_p whose order is e_p. The composition of the restriction homomorphism of $H^2(H_p, C^*)$ to $H^2(K, C^*)$ and the transfer homomorphism of $H^2(K, C^*)$ to $H^2(H_p, C^*)$ is the endomorphism of $H^2(H_p, C^*)$ given by multiplication by $| H_p{:}K |$ [2], which is, of course, h_p/e_p. Therefore, we need only prove that this composition is the zero map. However, $H^2(K, C^*) = 0$ since K is cyclic and the theorem is proved.

We now conclude by sketching the direct proof of the corollary. We first discuss the case of a p-group P. Let $A = Z(P) \cap P'$ so that we wish to show that the exponent of P divides $| P{:}A |$. Let $P = P_1, P' = P_2, P_3, \cdots$ denote the lower central series of P. Let $A_i = P_i \cap A$, for each positive integer i, so that $A = A_1 = A_2$. Finally, let $Q_i = (P_i \cap A)P_{i+1}$, for each $i \geq 1$, so that Q_i is a subgroup of P_i containing P_{i+1} and $Q_1 = P'$.

Therefore, $A_i/A_{i+1} \cong Q_i/P_{i+1}$ and so

$$| A | = \textstyle\prod_{i \geq 1} | A_i{:}A_{i+1} | = \prod | Q_i{:}P_{i+1} |.$$

Hence

$$| P{:}A | = | P |/| A | = \textstyle\prod | P_i{:}Q_i |.$$

Denote $| P_i{:}Q_i | = p^{n_i}$ and let p^{e_i} be the exponent of P_i/P_{i+1}. Since the exponent of P is a divisor of $\prod_i p^{e_i}$ we need only establish that $\sum e_i \leq \sum n_i$. We shall, in fact, prove the following two assertions, which give a stronger result:

(a) $e_1 + e_2 \leq n_1$,
(b) $e_i \leq n_{i-1}$, for $i \geq 3$.

If P is cyclic these statements are clear so that we shall assume P is not cyclic. Thus, P/P' is not cyclic so there exist m elements, $m > 1, x_1, \cdots, x_m$ of P such that the cosets $P'x_i$ form a basis of P/P'. Let $P'x_i$ have order p^{a_i} where we assume $a_1 \geq \cdots \geq a_m$. Thus, $e_1 = a_1$ and $n_1 = \sum a_i$. Furthermore, P_2/P_3 is generated by the elements $P_3[x_i, x_j]$, $1 \leq i < j \leq m$. However, $P_3[x_i, x_j]$ has order at most p^{a_j} so that $e_2 \leq a_2$. Hence

$$e_1 + e_2 \leq a_1 + a_2 \leq n_1$$

and (a) is proved

As for (b), P_i/P_{i+1} is generated by all the elements $P_{i+1}[x, g]$ where x is in P_{i-1} and g is in P. Since P_{i-1}/Q_{i-1} has order $p^{n_{i-1}}$ we have $x^{p^{n_{i-1}}} = zy$ where z is in A and y is in P_i. However, z is in $Z(P)$ so it follows that $P_{i+1}[x, g]$ has order at most $p^{n_{i-1}}$. Thus $e_i \leq n_{i-1}$ and (b) is established.

We now consider the general case of the corollary. In view of the above discussion and since the exponent of G is the product of the exponents of the Sylow subgroups, it suffices to show that the following assertion holds: If S is a Sylow subgroup of G then

$$Z(G) \cap G' \cap S \leq Z(S) \cap S'.$$

Let x be an element of the subgroup on the left so that x is in $Z(S)$. However, since x is in $Z(G)$, the image of x under the transfer homomorphism of G into S/S' is $S'x^n$ where $n = | G:S |$. Therefore, if x is not in S' then x is not in G' and the proof is complete.

References

1. R. Brauer, *Applications of induced characters*, Amer. J. Math., vol. 69 (1947), pp. 709–16.
2. H. Cartan and S. Eilenberg, *Homological algebra*, Princeton, Princeton University Press, 1956.
3. W. F. Reynolds, *Projective representations of finite groups*, Illinois J. Math., vol. 9 (1965), pp. 191–9.
4. I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math., vol. 127 (1904), pp. 20–50.
5. ———, *Untersuchungen uber die Darstellung der endlichen Gruppen gebrochene lineare Substitutionen*, J. Reine Angew. Math., vol. 132 (1907), pp. 85–137.
6. Yamazaki, K., *On projective representations and ring extensions of finite groups*, J. Fac. Sci. Univ. Tokyo, vol. 10 (1964), pp. 147–195.

University of Chicago
Chicago, Illinois