PROJECTIVE REPRESENTATIONS OF FINITE GROUPS IN CYCLOTOMIC FIELDS

BY
W. F. REYNOLDS

Introduction

In [2] Brauer proved that every representation of a finite group G in the field C of complex numbers is equivalent in C to a representation of G in the field of the $|G|$-th roots of unity, and in [3] he improved this by replacing $|G|$ by the exponent of G. In this paper we consider the corresponding question for projective representations. Our main result is contained in the following theorem.

THEOREM. *Every projective representation $\mathfrak{X}$ of G in C is projectively equivalent (see Section 2) in C to a projective representation $\mathfrak{Z}$ of G in the field of the $|G|$-th roots of unity. $\mathfrak{Z}$ can be chosen so that its factor set takes on only $|G|$-th roots of unity as values, and so that it is inflated from any quotient group G/H from which the factor set of $\mathfrak{X}$ is inflated.*

This result is given in a more precise form in Theorems 5 and 6, which also include a similar result for modular projective representations (see [10], [11]). It would be of interest to know whether $|G|$ could be replaced by the exponent of G in these results.

Our method combines those of Brauer [3] and Schur [13]. In Section 1 we give a modification (Theorem 1) of the Brauer induction theorem [4], [6, p. 283] which takes into account the behavior of characters on a given subgroup of the center $Z(G)$ of G; and we use this to prove in Theorem 3 that every representation of every subgroup of G in C is equivalent to a representation in the field of the $|G : Z(G) \cap G'|$-th roots of unity, where G' is the commutator subgroup of G. Schur's method is then applied in Section 2 to obtain the main result. In the final section we show that some basic results of Clifford [5] and Mackey [9] can be obtained within the field of the $|G|$-th roots of unity.

1. Characters and representations

Our first result is a modification of the Brauer induction theorem.

THEOREM 1. *Let A be a subgroup of the center of a finite group G; let ω be a linear character of A. Then every irreducible character χ of G such that $\chi \mid A$ contains ω can be expressed in the form*

$$(1) \qquad \chi = \textstyle\sum_i c_i \lambda_i^G,$$

Received October 28, 1963.

where c_i is an integer and λ_i is a linear character of a nilpotent subgroup J_i of G such that $J_i \supseteq A$ and $\lambda_i \mid A = \omega$.

Here $\chi \mid A$ denotes the restriction of χ to A; λ_i^G denotes the character of G induced by λ_i; and a *linear character* is a character of degree 1.

Proof. By the induction theorem, we can write

$$\chi = \sum_j b_j \theta_j^G = \sum_j b_j(\theta_j^{AE_j})^G,$$

where b_j is an integer and θ_j is an irreducible character of an elementary subgroup E_j of G. Decomposing $\theta_j^{AE_j}$ into its irreducible constituents ψ_i on AE_j, we obtain an equation

$$\chi = \sum_i c_i \psi_i^G, \tag{2}$$

where c_i is an integer and ψ_i is an irreducible character of AF_i, F_i being one of the groups E_j.

Since $A \subseteq Z(G)$, each $\psi_i \mid A$ is a multiple of some linear character ω_i of A; then also $\psi_i^G \mid A$ is a multiple of ω_i. Similarly $\chi \mid A$ is a multiple of ω. We can write

$$\chi - \sum_{i \in I'} c_i \psi_i^G = \sum_{i \in I''} c_i \psi_i^G,$$

where $i \in I'$ if $\omega_i = \omega$ and $i \in I''$ if $\omega_i \neq \omega$. The left side is a linear combination of those of the irreducible characters χ_l of G for which $\chi_l \mid A$ is a multiple of ω, while the right side is a linear combination of the remaining χ_l. By the linear independence of the χ_l, both sides vanish; hence we can discard those terms on the right side of (2) for which $\omega_i \neq \omega$.

Since F_i is nilpotent, so is AF_i. Therefore each ψ_i is the character of a monomial representation of AF_i; that is, $\psi_i = \lambda_i^{AF_i}$ for some linear character λ_i of a subgroup J_i of AF_i (see [4, Lemma 3] or [6, pp. 273 and 356]). By the formula for induction, ψ_i vanishes except on the AF_i-conjugates of J_i; because $\psi_i \mid A$ is a multiple of ω, this implies that $J_i \supseteq A$ and $\lambda_i \mid A = \omega$. Since J_i is nilpotent, and since (2) implies (1), the theorem is proved.

Remark. In the same way we could obtain a modification of the Witt-Berman induction theorem [14, Theorem 1], [6, §42], provided that the field which appears in that theorem contains the values of ω.

The next theorem is obtained by a method of Schur [13, §5].

THEOREM 2. *Let G, A, and J be finite groups such that $A \subseteq G' \cap Z(G)$ and $A \subseteq J \subseteq G$. Then for any linear character λ of J, the multiplicative order of $\lambda \mid A$ divides $\mid G{:}J \mid$.*

Proof. Let $\omega = \lambda \mid A$, and let r be the order of ω in the group of linear characters of A. There exists $a \in A$ such that $\omega(a)$ is a primitive r-th root of unity. Let $\mathfrak{T}$ be the representation of G corresponding to λ^G; $\mathfrak{T}$ has degree $\mid G{:}J \mid$. Since $a \in Z(G)$, det $\mathfrak{T}(a)$ = det $(\omega(a)I) = \omega(a)^{\mid G:J \mid}$, where I denotes the identity matrix. On the other hand, since $a \in G'$, det $\mathfrak{T}(a) = 1$. Therefore r divides $\mid G{:}J \mid$, as required.

We now use Theorems 1 and 2 to strengthen the main result of [3].

THEOREM 3. *Let G and A be finite groups such that $A \subseteq Z(G) \cap G'$. Then for every subgroup S of G, every representation of S in C is equivalent in C to a representation of S in the field K of the d-th roots of unity, where d is the greatest common divisor of $| G:A |$ and the exponent of G.*

Proof. We may suppose that the representation $\mathfrak{X}$ of S in C is irreducible. Let χ be the character of $\mathfrak{X}$; since $A \cap S \subseteq Z(S)$, $\chi \mid A \cap S$ is a multiple of some linear character ω of $A \cap S$. There exists a linear character ω_1 of the abelian group A such that $\omega_1 \mid A \cap S = \omega$. For $a \in A$ and $s \in S$, set $\mathfrak{X}_1(as) = \omega_1(a)\mathfrak{X}(s)$; $\mathfrak{X}_1$ is well defined and is an irreducible representation of the group AS such that $\mathfrak{X}_1 \mid S = \mathfrak{X}$. Now we can replace S by AS, $\mathfrak{X}$ by $\mathfrak{X}_1$, and ω by ω_1, and assume without loss of generality that $A \subseteq S$.

Now ω is a linear character of A; the kernel N of ω is normal in G, because $N \subseteq Z(G)$. Since $A/N \subseteq Z(G/N) \cap (G/N)'$, and since $\mathfrak{X}$ gives rise to a representation of S/N, it is sufficient to prove the theorem with G and A replaced by G/N and A/N. After this replacement, A is cyclic and the order of ω is $| A |$.

By Theorem 1 for S, $\chi = \sum_i c_i \lambda_i^S$ where c_i is an integer and λ_i is a linear character of a nilpotent group J_i, $A \subseteq J_i \subseteq S$, with $\lambda_i \mid A = \omega$. By Theorem 2, $| A |$ divides $| G:J_i |$ for each i; that is, $| J_i |$ divides $| G:A |$. Therefore the exponent of J_i divides d, and the values of λ_i lie in K, so that the representation with character λ_i^S is equivalent in C to a representation in K. We can then conclude by the argument of [3, Theorem 1] or [6, p. 294] that $\mathfrak{X}$ is equivalent in C to a representation in K.

Combining Theorem 3 with the result of [6, p. 592], we obtain the following analogue of Theorem 3 for irreducible modular representations and finite fields.

THEOREM 4. *Let G, A, S, and K be as in Theorem 3; let K^* be any residue class field of K. Then every irreducible representation of S in the algebraic closure of K^* is equivalent in this algebraic closure to a representation of S in K^*.*

2. Projective representations

We begin this section by presenting some definitions of well-known concepts in the precise form which we shall use. By a *factor set* (or 2-cocycle) of a finite group G in a field K we mean a mapping ρ of $G \times G$ into the multiplicative group $K^\times$ of K such that for all $x, y, z \in G$,

$$\rho(x, y)\rho(xy, z) = \rho(x, yz)\rho(y, z), \qquad \rho(x, 1) = \rho(1, x) = 1.$$

The factor sets of G in K form an abelian multiplicative group, where

$$(\rho\sigma)(x, y) = \rho(x, y)\sigma(x, y).$$

A 1-*cochain* of G in K is a mapping μ of G into $K^\times$ such that $\mu(1) = 1$; the

1-cochains of G in K also form an abelian multiplicative group. The *coboundary* of a 1-cochain μ is the factor set $\delta\mu$ defined by

$$(\delta\mu)(x, y) = \mu(x)\mu(y)\mu(xy)^{-1}.$$

Two factor sets in K are *equivalent* (or cohomologous) in K if their quotient is a coboundary; the equivalence classes $\{\rho\}$ under this relation form the *multiplier* (or second cohomology group) $M(G, K)$, which is a finite abelian multiplicative group. Our use of normalized cochains is for convenience, and does not affect the generality of our results (see [7, §6] or [8, p. 237]).

The *restriction* $\rho \mid S$ of a factor set ρ of G in K to a subgroup S is defined by restricting its arguments to S. If ε is a factor set of a quotient group G/H in K, the *inflation* of ε to G is the factor set inf ε of G in K defined by

$$(\inf \varepsilon)(x, y) = \varepsilon(xH, yH).$$

Restrictions and inflations of 1-cochains are defined similarly.

A *projective representation* of G in K is a mapping $\mathfrak{X}$ of G into the set of $n \times n$ matrices over K such that for $x, y \in G$,

$$\mathfrak{X}(x)\mathfrak{X}(y) = \rho(x, y)\mathfrak{X}(xy), \qquad \mathfrak{X}(1) = I,$$

with $\rho(x, y) \in K$. Here ρ must be a factor set of G in K. If μ is a 1-cochain of G in K and if U is a non-singular $n \times n$ matrix over K, then the equations $\mathfrak{Y}(x) = \mu(x)U^{-1}\mathfrak{X}(x)U$ define a projective representation $\mathfrak{Y}$ of G in K with factor set $(\delta\mu)\rho$; we say that $\mathfrak{Y}$ is *projectively equivalent* to $\mathfrak{X}$ in K. If $\mu = 1$, we call $\mathfrak{Y}$ *linearly equivalent* to $\mathfrak{X}$ in K; observe that linearly equivalent projective representations have the same factor set.

Now we can state and prove our principal result.

THEOREM 5. *Let H be a normal subgroup of a finite group G, and let ε be any factor set of G/H in C. Then there exists a factor set η of G/H such that*

(i) *ε is equivalent to η in C;*

(ii) *the values of η are $|G|$-th roots of unity;*

(iii) *if S is any subgroup of G, then every projective representation of S in C with factor set $(\inf \eta) \mid S$ or $(\inf \eta)^{-1} \mid S$ is linearly equivalent in C to a projective representation of S in the field K of the $|G|$-th roots of unity. Furthermore if K^* is any residue class field of K, and if η^* is obtained from η by the residue class mapping, then every irreducible projective representation of S in the algebraic closure of K^* with factor set $(\inf \eta^*) \mid S$ or $(\inf \eta^*)^{-1} \mid S$ is linearly equivalent in this algebraic closure to a projective representation of S in K^*.*

Observe that this theorem implies that every projective representation of S in C with factor set $(\inf \varepsilon) \mid S$ is projectively equivalent in C to a projective representation of S in K with factor set $(\inf \eta) \mid S$; this gives us the theorem stated in the introduction.

Proof. Let r be the order of the equivalence class $\{\inf \varepsilon\}$ of $\inf \varepsilon$ in $M(G, C)$. Then this class also contains at least one factor set ρ of G such that ρ itself has order r in the multiplicative group of factor sets of G in C (see [1, §1] or [6, p. 360]). Here

$$\rho = (\delta\mu)(\inf \varepsilon) \tag{3}$$

for some 1-cochain μ of G in C.

We now use an adaptation of an argument of Schur [13, §§2, 3]. Let A be the character group of the multiplicative cyclic group generated by ρ; A is cyclic of order r. For any $x, y \in G$, let $a_{x,y} \in A$ be the character such that $a_{x,y}(\rho^i) = \rho(x, y)^i$. Then the ordered pairs (a, x), $a \in A$, $x \in G$, form a group G^* under the multiplication

$$(a, x)(b, y) = (aba_{x,y}, xy).$$

If A^* consists of the pairs of form $(a, 1)$ and S^* consists of all pairs (a, s) with $s \in S$, then clearly $A^* \subseteq Z(G^*)$, $A^* \cong A$, $G^*/A^* \cong G$, and $S^*/A^* \cong S$. Furthermore $A^* \subseteq (G^*)'$ by the following argument. For any linear character λ of G^*, $\lambda(a, 1) = a^j(\rho)$ for some j and for all $a \in A$; in particular $\lambda(a_{x,y}, 1) = \rho(x, y)^j$. Since $\lambda(1, x)\lambda(1, y) = \rho(x, y)^j\lambda(1, xy)$, we have $\{\inf \varepsilon\}^j = \{\rho\}^j = 1$, so that r divides j and $\lambda \mid A^* = 1$; since λ is arbitrary, $A^* \subseteq (G^*)'$.

To each projective representation $\mathfrak{Y}$ of S in C with factor set $\rho \mid S$, there corresponds an ordinary representation $\mathfrak{X}$ of S^* defined by

$$\mathfrak{X}(a, s) = a(\rho)\mathfrak{Y}(s).$$

We can now apply Theorem 3 to G^* to see that $\mathfrak{X}$ is equivalent to a representation of S^* in K, since $| G^*:A^* | = | G |$; then $\mathfrak{Y}$ is linearly equivalent to a projective representation of S in K. The same holds true for projective representations with factor set $\rho^{-1} \mid S$; and Theorem 4 gives the corresponding modular statement.

The order r of $\{\rho\} = \{\inf \varepsilon\}$ divides the order e of the class $\{\varepsilon\}$ of ε in $M(G/H, C)$. But e divides $| G:H |$ by [13], [1], or [6, p. 359]; hence

$$\rho^{|G:H|} = 1. \tag{4}$$

This proves the theorem in the case $H = 1$, by taking $\eta = \rho$. But in general we must argue further, since ρ may not be the inflation of a factor set of G/H.

Since $\varepsilon(1, 1) = 1$, (3) implies that $(\delta\mu) \mid H = \rho \mid H$. By (4),

$$((\delta\mu) \mid H)^{|G:H|} = 1;$$

in other words, $(\mu \mid H)^{|G:H|}$ is a linear character of H. Therefore

$$(\mu \mid H)^{|G|} = ((\mu \mid H)^{|G:H|})^{|H|} = 1. \tag{5}$$

For each element $u \in G/H$, choose a representative $g_u \in g$ such that $g_u H = u$, with $g_1 = 1$. A 1-cochain γ of G/H is defined by setting $\gamma(u) = \mu(g_u)$. We shall show that the factor set $\eta = (\delta\gamma)\varepsilon$ of G/H satisfies conditions (i), (ii) and (iii). Condition (i) holds by definition.

For the 1-cochain $\nu = (\inf \gamma)\mu^{-1}$ of G, whenever $h \in H$ and $u \in G/H$ we have

$$\nu(hg_u) = \gamma(u)\mu(hg_u)^{-1} = \mu(g_u)\mu(hg_u)^{-1}.$$

But by (3),

$$\rho(h, g_u) = (\delta\mu)(h, g_u)\varepsilon(1, u) = \mu(h)\mu(g_u)\mu(hg_u)^{-1},$$

so that $\nu(hg_u) = \mu(h)^{-1}\rho(h, g_u)$. By (4) and (5) both factors on the right are $|G|$-th roots of unity; hence

$$\nu^{|G|} = 1. \tag{6}$$

By (3) and the definitions of η and ν,

$$\inf \eta = (\inf (\delta\gamma))(\inf \varepsilon) = (\delta(\inf \gamma))(\delta\mu)^{-1}\rho = (\delta\nu)\rho. \tag{7}$$

Then by (4) and (6), $\eta^{|G|} = 1$; this proves (ii).

Corresponding to each projective representation $\mathfrak{Z}$ of S with factor set $(\inf \eta)| S$, we can define a projective representation $\mathfrak{Y}$ with factor set $\rho \mid S$ by writing $\mathfrak{Y}(s) = \nu(s)^{-1}\mathfrak{Z}(s)$, $s \in S$; cf. (7). We have shown that $\mathfrak{Y}$ is linearly equivalent to a projective representation over K; but for any matrix U over C such that $U^{-1}\mathfrak{Y}(s)U$ lies in K for all $s \in S$, $U^{-1}\mathfrak{Z}(s)U$ also lies in K, by (6). This proves the part of (iii) concerning $(\inf \eta)| S$; the rest of (iii) follows from similar arguments. This completes the proof of Theorem 5.

COROLLARY. *If $H = 1$ in Theorem 5, we can choose η so that its order is the same as the order of its class $\{\eta\}$ in $M(G, C)$.*

This is true since we can take $\eta = \rho$ in this case. It is natural to ask whether, in the situation of Theorem 5, we can always choose η to be of the same order as its class in $M(G/H, C)$, and hence of order dividing $|G:H|$. While we cannot answer this question, the following theorem gives some information about the order of η.

THEOREM 6. *In the conclusion of Theorem 5, we can add the following statement:*

(iv) *every prime divisor of the order of η divides $|G:H|$.*

Proof. Since $\eta = (\delta\gamma)\varepsilon$, $\{\eta\} = \{\varepsilon\}$; thus the order of $\{\eta\}$ in $M(G/H, C)$ is e, so that $\eta^e = \delta\alpha$ for some 1-cochain α of G/H in C. Since e divides $|G:H|$, $|G|/e$ is an integer. Then by (ii), $1 = \eta^{|G|} = (\delta\alpha)^{|G|/e} = \delta(\alpha^{|G|/e})$. This means that $\alpha^{|G|/e}$ is a linear character of G/H. It follows that

$$1 = (\alpha^{|G|/e})^{|G:H|} = \alpha^{|H||G:H|^2/e}. \tag{8}$$

Let π be the set of all primes which divide $|G:H|$. Let α_π and α_0 denote the π-part and π-regular part, respectively, of α; that is, the unique elements α_π and α_0 of the abelian multiplicative group of all 1-cochains of G/H in C such that $\alpha_\pi \alpha_0 = \alpha$ while all the prime divisors of the order of α_π, and none of the prime divisors of the order of α_0, are in π (cf. [6, p. 284]). Since the prime divisors of $|G:H|^2/e$ are all in π, (8) implies that $\alpha_0^{|H|} = 1$.

Similarly, let η_π and η_0 be the π-part and π-regular part, respectively, of η. Since e is relatively prime to the order of η_0, η_0 is a power of η_0^e, say $\eta_0 = \eta_0^{ef}$. Since $\eta^e = \delta\alpha$, $\eta_0^e = \delta\alpha_0$, so that

$$\eta_0 = \eta_0^{ef} = (\delta\alpha_0)^f = \delta\beta,$$

where we set $\beta = \alpha_0^f$. Also $\beta^{|H|} = \alpha_0^{f|H|} = 1$.

In the proof of Theorem 5, set $\mathfrak{W}(s) = (\inf\beta)^{-1}(s)\mathfrak{Z}(s)$, $s \in S$. Since $\eta_\pi = \eta_0^{-1}\eta = (\delta\beta)^{-1}\eta$, $\mathfrak{W}$ has factor set $(\inf \eta_\pi)| S$, and $\mathfrak{W}$ lies in K since $\beta^{|G|} = 1$. Then if we replace η by η_π, (iv) holds as well as (i), (ii), and (iii).

3. Applications

Let H be any normal subgroup of a finite group G, and $\mathfrak{X}$ an irreducible representation of G in an algebraically closed field of any characteristic. According to Clifford [5], $\mathfrak{X}$ is induced from a representation $\mathfrak{X}'$ of a certain "inertial" group S, $H \subseteq S \subseteq G$, while $\mathfrak{X}'$ is a tensor product $\mathfrak{Y} \times \mathfrak{A}$ of two projective representations of S, with factor sets inflated from inverse factor sets ε^{-1} and ε of S/H, where $\mathfrak{Y} \mid H$ is irreducible and $\mathfrak{A}$ is inflated from a projective representation of S/H. By applying Theorems 5 and 6 to S (in the roles of both G and S), we can choose ε so that $\mathfrak{Y}$ and $\mathfrak{A}$, and hence also $\mathfrak{X}$, lie in a subfield isomorphic to the field K of $|S|$-th roots of unity or to a residue class field of K while $\varepsilon^{|S|} = 1$ and every prime divisor of the order of ε divides $|S:H|$.

Replacing $\mathfrak{X}$ by a projective representation of G, we can find a similar statement concerning the finite-group case of Mackey's generalization [9] of Clifford's results, taking the G and S of Theorems 5 and 6 to be the same as the G and S of this section.

Another application of Theorems 5 and 6 appears in the Addendum to [12], where they are used to find a field in which the constructions of [12] can be carried out.

References

1. K. Asano and K. Shoda, *Zur Theorie der Darstellungen einer endlichen Gruppe durch Kollineationen*, Compositio Math., vol. 2 (1935), pp. 230–240.
2. R. Brauer, *On the representation of a group of order g in the field of the g-th roots of unity*, Amer. J. Math., vol. 67 (1945), pp. 461–471.
3. ———, *Applications of induced characters*, Amer. J. Math., vol. 69 (1947), pp. 709–716.
4. ———, *A characterization of the characters of groups of finite order*, Ann. of Math. (2), vol. 57 (1953), pp. 357–377.
5. A. H. Clifford, *Representations induced in an invariant subgroup*, Ann. of Math. (2), vol. 38 (1937), pp. 533–550.
6. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, New York, Interscience, 1962.
7. S. Eilenberg and S. MacLane, *Cohomology theory in abstract groups, I*, Ann. of Math. (2), vol. 48 (1947), pp. 51–78.
8. M. Hall, *The theory of groups*, New York, Macmillan, 1959.
9. G. W. Mackey, *Unitary representations of group extensions, I*, Acta Math., vol. 99 (1958), pp. 265–311.

10. H. NAGAO, *On the theory of representation of finite groups*, Osaka Math. J., vol. 3 (1951), pp. 11–20.
11. M. OSIMA, *On the representations of groups of finite order*, Math. J. Okayama Univ vol. 1 (1952), pp. 33–61.
12. W. F. REYNOLDS, *Blocks and normal subgroups of finite groups*, Nagoya Math. J., vol. 22 (1963), pp. 15–32.
13. I. SCHUR, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math., vol. 127 (1904), pp. 20–50.
14. L. SOLOMON, *The representation of finite groups in algebraic number fields*, J. Math. Soc. Japan, vol. 13 (1961), pp. 144–164.

TUFTS UNIVERSITY
MEDFORD, MASSACHUSETTS