ON GENERALIZED CONJUGATE CLASSES IN A FINITE GROUP[1]

BY
RIMHAK REE

Throughout this note G will denote a finite group, and σ a fixed homomorphism of G into itself. σ may be an automorphism of G. Two elements a and b in G will be called *σ-conjugate* if there exists an element x in G such that $a = x^{-1}bx^{\sigma}$. This is an equivalence relation, and all elements in G are partitioned into *σ-classes*. If σ is the identity automorphism, then σ-conjugacy reduces to the "ordinary" conjugacy in groups. A subset S of G will be called *σ-invariant* if $x \in S$ implies $x^{\sigma} \in S$. In this note we shall prove the following:

THEOREM 1. *The number of σ-classes equals the number of σ-invariant classes of conjugate elements in G.*

An interesting feature of the above theorem is that, although the theorem itself does not involve group characters, it does not seem to be proved easily without using group characters. The author has been unable to obtain such a proof.[2] Actually Theorem 1 is an immediate consequence of the following two theorems.

THEOREM 2. *The number of σ-classes in G is equal to the number of σ-invariant irreducible ordinary characters of G.*

THEOREM 3. *Let p be an arbitrary prime number. Then the number of σ-invariant irreducible modular characters (with respect to p) is equal to the number of σ-invariant p-regular classes of conjugate elements in G. In particular, the number of σ-invariant ordinary characters is equal to the number of σ-invariant classes of conjugate elements in G.*

Here, a function $\varphi(x)$ defined on a σ-invariant subset S of G is called *σ-invariant* if $\varphi(x^{\sigma}) = \varphi(x)$ for all $x \in S$; a class of conjugate elements is called *p-regular* if it consists of elements of order prime to p.

Theorem 2 above is a generalization of a result of Ado [1], who proved Theorem 2 for the case where σ is an automorphism. In his proof Ado made use of the inverse mapping σ^{-1}. The method we use here to prove Theorem 2 is a rather trivial modification of Ado's.

Proof of Theorem 2. Let $\chi_1, \cdots, \chi_k$ be all irreducible ordinary characters

Received May 12, 1958.

[1] This research was supported by the United States Air Force through the Air Research and Development Command.

[2] Ruth Rebekka Struik pointed out that such a proof can be obtained easily in case one of the numbers involved in Theorem 1 is 1.

of G. For each i take an arbitrary element a_i in G, and define a function $f_i(x) = f_i(x, a_i)$ by

$$f_i(x, a_i) = \sum_{s \in G} \chi_i(s^{-1}xs^{\sigma}a_i).$$

It is clear that $f_i(x, a_i) = f_i(y, a_i)$ whenever x and y are σ-conjugate. Thus we may consider $f_i(x, a_i)$ as a function defined on σ-classes of G. Hence the theorem will be proved if we can show (A) and (B) below:

(A) If $i \neq j$, then for any $a_i, a_j \in G$ we have

$$\sum_{x \in G} f_i(x, a_i)\overline{f_j(x, a_j)} = 0,$$

where $\overline{f_j(x, a_j)}$ denotes the complex conjugate of $f_j(x, a_j)$.

(B) For each σ-invariant χ_i we can choose a_i such that the function $f_i(x, a_i)$ is not identically zero. With such choice of a_i, if $x_1, \cdots, x_n$ is a complete system of representatives of all σ-classes of G, and if $\gamma_1, \cdots, \gamma_n$ are complex numbers such that

$$\sum_{\nu=1}^{n} \gamma_\nu f_i(x_\nu, a_i) = 0 \tag{1}$$

holds whenever χ_i is σ-invariant, then all $\gamma_\nu = 0$.

Before proving (A) and (B) above, we shall show

(C) If χ_i is not σ-invariant, then the function $f_i(x, a_i)$ is identically zero for any $a_i \in G$.

We need the following well known lemma of Schur: Let X_i and X_j be two nonequivalent irreducible ordinary representations of G. Let $X_i(x) = (\alpha_{\mu\nu}(x))$, $X_j(x) = (\beta_{\mu\nu}(x))$. Then

$$\sum_{x \in G} \alpha_{\mu\nu}(x)\beta_{\kappa\lambda}(x^{-1}) = 0, \tag{2}$$

$$\sum_{x \in G} \alpha_{\mu\nu}(x)\alpha_{\kappa\lambda}(x^{-1}) = g\delta_{\mu\lambda}\, \delta_{\nu\kappa}/d_i \tag{3}$$

for all $\mu, \nu, \kappa, \lambda$, where g denotes the order of G, d_i the degree of X_i, and $\delta_{\mu\nu}$ Kronecker deltas.

We shall prove (C). Let X_i be the irreducible representation which gives rise to χ_i. If χ_i is not σ-invariant, then the representation X_i^{σ} of G defined by $X_i^{\sigma}(x) = X_i(x^{\sigma})$ is not equivalent to X_i. Moreover X_i cannot appear as an irreducible constituent of X_i^{σ}, since the degree of X_i and X_i^{σ} coincide. Hence

$$f_i(x, a_i) = \sum_{s \in G} \operatorname{tr}(X_i(s^{-1})X_i(x)X_i^{\sigma}(s)X_i(a_i))$$

is a linear combination of sums of the form $\sum_{s \in G} \alpha_{\mu\nu}(s^{-1})\beta_{\kappa\lambda}(s)$. Then by (2) we have $f_i(x, a_i) = 0$ for all $x \in G$. Thus (C) is proved.

We shall prove (A). For any fixed elements a, b, c, d in G, $\chi_i(axb)$ is a linear combination of $\alpha_{\mu\nu}(x)$, and $\overline{\chi_j(cxd)} = \chi_j(d^{-1}x^{-1}c^{-1})$ is a linear combination of $\beta_{\kappa\lambda}(x^{-1})$. Hence (2) implies that

$$\sum_{x \in G} \chi_i(axb)\, \overline{\chi_j(cxd)} = 0.$$

From this (A) follows immediately.

We shall prove (B). Since χ_i is σ-invariant, X_i and X_i^σ are equivalent. Hence there exists a nonsingular matrix U such that $X_i(s^\sigma) = UX_i(s)U^{-1}$ for all $s \in G$. By (3) we have

$$f_i(x, a_i) = \sum_{s \in G} \operatorname{tr}(X_i(s^{-1})X_i(x)UX_i(s)U^{-1}X_i(a_i)) \tag{4}$$
$$= g \operatorname{tr}(X_i(x)U) \operatorname{tr}(U^{-1}X_i(a_i))/d_i .$$

Since X_i is irreducible, any $x_i \times x_i$ matrix (with complex entries), and in particular U, can be written as a linear combination of the matrices $X_i(a)$, $a \in G$. Hence it follows that there exists an element $a_i \in G$ such that

$$\operatorname{tr}(U^{-1}X_i(a_i)) \neq 0. \tag{5}$$

Similarly there exists $x \in G$ such that $\operatorname{tr}(X_i(x)U) \neq 0$. Now the first half of (B) is clear from (4) and (5). To prove the second half, suppose that the function $f_i(x, a_i)$ is not identically zero when χ_i is σ-invariant. Then we have (5), as is seen from (4). Also from (4) it follows that for any fixed $a \in G$ there exists a complex number α_i for each σ-invariant χ_i such that

$$f_i(x, a) = \alpha_i f_i(x, a_i) \qquad (x \in G).$$

Hence if (1) is true, then

$$\sum_{\nu=1}^{n} \gamma_\nu f_i(x_\nu , a) = 0 \tag{6}$$

holds for all $a \in G$ and i for which χ_i is σ-invariant. If χ_i is not σ-invariant, then by (C) we have $f_i(x_\nu , a) = 0$ for all x_ν. Thus (6) holds for all irreducible characters χ_i of G. Let

$$y = \sum_{\nu=1}^{n} \gamma_\nu \sum_{s \in G} s^{-1} x_\nu s^\sigma.$$

Then (6) implies that $\chi_i(ya^{-1}) = 0$ for all $a \in G$ and i. Let $y = \sum_{t \in G} \beta_t t$ with complex coefficients β_t. Then

$$0 = \sum_{i=1}^{k} \chi_i(ya^{-1}) = g\beta_a$$

for all $a \in G$. Thus $y = 0$. Denote by z_ν the sum of elements in the σ-class represented by x_ν. Then $y = 0$ implies $\sum_\nu \gamma_\nu k_\nu z_\nu = 0$ with certain positive integers k_ν. Hence $\gamma_\nu k_\nu = 0$, $\gamma_\nu = 0$ for all ν. Thus the second half of (B) is also proved. This completes the proof of Theorem 2.

Proof of Theorem 3. Let $\varphi_1, \cdots, \varphi_l$ be all irreducible modular characters of G, and d_{ij} decomposition numbers. Set as usual

$$\Phi_i = \sum_{j=1}^{k} d_{ji} \chi_j \qquad (i = 1, 2, \cdots, l),$$

where $\chi_1, \cdots, \chi_k$ are ordinary irreducible characters of G. It is easy to see that $\varphi_i(x^\sigma)$ is the modular character of the modular representation F_i^σ which is defined by $F_i^\sigma(x) = F_i(x^\sigma)$, where F_i is the irreducible modular representation which gives rise to φ_i. Hence φ_i is σ-invariant if and only if F_i^σ is equivalent to F_i, and if F_i^σ is not equivalent to F_i, then F_i cannot appear as an irreducible constituent in F_i^σ. Therefore if we set

$$\sum \varphi_i(x^\sigma)\overline{\Phi_i(x)} = g\alpha_i, \tag{7}$$

where the summation runs over all p-regular elements x in G, then by the orthogonality relation for modular characters [2, p. 561], α_i is 1 or 0 according as φ_i is σ-invariant or not. Let $\{x_1, \cdots, x_l\}$ be a complete set of representatives of the p-regular classes $K_1, \cdots, K_l$. Let g_ν denote the number of elements in K_ν. Then, denoting by n the number of σ-invariant φ_i, we have from (7)

$$gn = \sum_{\nu=1}^{l} g_\nu \sum_{i=1}^{l} \varphi_i(x_\nu^\sigma)\overline{\Phi_i(x_\nu)} = \sum_{\nu=1}^{l} g_\nu\, gb_\nu/g_\nu = g\sum_{\nu=1}^{l} b_\nu, \tag{8}$$

where

$$b_\nu = g_\nu \sum_{i=1}^{l} \varphi(x_\nu^\sigma)\overline{\Phi(x_\nu)}/g$$

is 1 or 0 according as x_ν^σ and x_ν are conjugate or not (orthogonality relation for modular characters). Hence our theorem follows immediately from (8).

We shall now derive a few consequences of Theorem 2. Let σ be an automorphism of a finite group G which leaves invariant all classes of conjugate elements in G. By Theorem 2 all irreducible ordinary characters of G are σ-invariant. This implies that for every simple ideal A_i of the group algebra A of G over the complex number field Ω we have $A_i^\sigma = A_i$, where σ denotes the automorphism of A induced naturally by the automorphism σ of G. Since every A_i is a full matrix algebra, σ induces an inner automorphism in every A_i. From this it follows that σ is an inner automorphism of A. Thus *any automorphism of a finite group G which leaves invariant all classes of conjugate elements in G is induced by an inner automorphism of the group algebra of G over Ω.* It is known [3, p. 181] that such an automorphism of G is not necessarily an inner automorphism of G.

Now let the automorphism σ of G be as above, and consider the group $\bar{G}$ obtained by extending G by σ. If m is the order of σ, then $\bar{G}$ is characterized by the following properties: $\bar{G}$ contains G as a normal subgroup of index m; $\bar{G}$ is generated by G and an element a of order m such that $a^{-1}xa = x^\sigma$ for all x in G. It is easy to see that σ is an inner automorphism of G if and only if G is a direct factor of $\bar{G}$. We shall show that *the group algebra $\bar{A}$ of $\bar{G}$ over Ω is isomorphic to the group algebra over Ω of the direct product of G and a cyclic group of order m.* Let A be the subalgebra of $\bar{A}$ spanned by elements in G. It is shown above that there exists an invertible element $u \in A$ such that $u^{-1}xu = x^\sigma = a^{-1}xa$ for all $x \in G$. Let $ua^{-1} = v$. Then v commutes with every element in A, and $v^m \in A$. Thus v^m is an invertible element belonging to the center of A. Now, since A is a direct sum of full matrix algebras, every invertible element in the center of A can be written as z^m, where z is an invertible element in the center of A. Let $v^m = z^m$, $w = vz^{-1}$. Then w generates a cyclic group of order m; w commutes with every element in A; $\bar{A} = A \times B$, where B is the subalgebra of $\bar{A}$ spanned by powers of w. Hence

$\bar{A}$ is isomorphic to the group algebra of the direct product of G and a cyclic group of order m.

Added in proof. Recently, Dr. Hirosi Nagao succeeded in giving a simple direct proof of Theorem 1, which, with his permission, we shall outline here.

Consider the number n of solutions (x, y) of the equation $x^{-1}yx^{\sigma} = y$. The number of solutions with y in any fixed σ-class is easily seen to be g, the order of G. Hence $n = gs$, where s is the number of σ-classes. On the other hand, the number of solutions (x, y) of $y^{-1}xy = x^{\sigma}$ with x in any fixed σ-invariant conjugate class is again g, and hence $n = gr$, where r is the number of σ-invariant conjugate classes. Therefore $gs = gr$, $s = r$.

REFERENCES

1. I. D. ADO, *On the theory of linear representations of finite groups*, Mat Sbornik, N. S., vol 36(78) (1955), pp. 25–30 (Russian).
2. R. BRAUER AND C. NESBITT, *On the modular characters of groups*, Ann. of Math. (2), vol. 42(1941), pp. 556–590.
3. H. ZASSENHAUS, *The theory of groups*, 2nd ed. New York, Chelsea Publishing Co., 1958.

THE UNIVERSITY OF BRITISH COLUMBIA
VANCOUVER, CANADA