Can. J. Math., Vol. XXII, No. 5, 1970, pp. 1040–1046

SYSTEMS OF EQUATIONS AND GENERALIZED CHARACTERS IN GROUPS

I. M. ISAACS

Let F be the free group on n generators $X_1, \ldots, X_n$ and let G be an arbitrary group. An element $\omega \in F$ determines a function $x \to \omega(x)$ from n-tuples $x = (x_1, x_2, \ldots, x_n) \in G^n$ into G. In a recent paper [**5**] Solomon showed that if $\omega_1, \omega_2, \ldots, \omega_m \in F$ with $m < n$, and $K_1, \ldots, K_m$ are conjugacy classes of a finite group G, then the number of $x \in G^n$ with $\omega_i(x) \in K_i$ for each i, is divisible by $|G|$. Solomon proved this by constructing a suitable equivalence relation on G^n.

Another recent application of an unusual equivalence relation in group theory is in Brauer's paper [**1**], where he gives an elementary proof of the Frobenius theorem on solutions of $x^k = 1$ in a group.

In this paper we define an equivalence relation on G^n which reduces to Brauer's when $n = 1$. This relation is quite similar to Solomon's, and using it together with some of Solomon's methods and a crucial lemma from Brauer's paper, the following common generalization of Frobenius' and Solomon's results is proved.

THEOREM A. *Let G be a finite group and suppose that $\omega_1, \omega_2, \ldots, \omega_m \in F$ with $m < n$. Let K_i and L_j be conjugacy classes of G for $1 \leqq i \leqq m$ and $1 \leqq j \leqq n$. Suppose that $k \big| |G|$. Then the number of $x = (x_1, \ldots, x_n) \in G^n$ with $\omega_i(x) \in K_i$ and $x_j^k \in L_j$ for all i and j is divisible by k.*

Finally, using Brauer's characterization of characters, we prove the following result which was conjectured by Solomon and proved by him for "special" ω_i. (See the definition preceding Lemma 4.)

THEOREM B. *Let G, ω_i, and K_i be as in Theorem A. For $1 \leqq j \leqq n$ and $t \in G$, let $\theta_j(t)$ be the number of $x = (x_1, \ldots, x_n) \in G^n$ with $x_j = t$, such that $\omega_i(x) \in K_i$ for each i. Then θ_j is an R-linear combination of characters of G, where $R = \mathbf{Z}[\epsilon]$, ϵ a primitive $|G|$th root of 1.*

1. In this section, let G be an arbitrary group and fix a subgroup $H \subseteq G$. For $x = (x_1, x_2, \ldots, x_n) \in G^n$ set $H_x = \{h \in H \,|\, h^{x_j} = h^{x_1} \text{ for } 1 \leqq j \leqq n\}$. Thus if $n = 1$, we have $H_x = H$. For $x \in G^n$, write $\langle x \rangle = \langle x_1, x_2, \ldots, x_n \rangle \subseteq G$. Define

$$N_x = \bigcap_{g \in \langle x \rangle} H_x^{\,g}.$$

Received January 12, 1970.

https://doi.org/10.4153/CJM-1970-120-0 Published online by Cambridge University Press

We have then $\langle x\rangle \subseteq \mathbf{N}(N_x)$ and $N_x \subseteq H_x \subseteq H$. Note that H_x and N_x are subgroups of G. For $x = (x_1, \ldots, x_n)$ and $t \in G$, write $xt = (x_1t, x_2t, \ldots, x_nt)$. Now, for $x, y \in G^n$, write $x \equiv y$ if there exists $t \in N_x$ with $y = xt$. To emphasize the dependence on H, we will sometimes write $x \equiv_H y$.

LEMMA 1. *The relation $\equiv$ is an equivalence relation on G^n.*

Proof. First we show that if $x \equiv y$, then $N_y \supseteq N_x$. We have $y = xs$ for $s \in N_x$. Let $h \in N_x \subseteq H_x$. Then $h^{x_js} = h^{x_1s}$ and $h \in H_y$. Thus $N_x \subseteq H_y$. Now $\langle y\rangle \subseteq \langle\langle x\rangle, s\rangle \subseteq \mathbf{N}(N_x)$. Hence, if $g \in \langle y\rangle$, then $H_y{}^g \supseteq N_x{}^g = N_x$. Therefore $N_y = \bigcap H_y{}^g \supseteq N_x$.

Now $\equiv$ is clearly reflexive. If $x \equiv y$, then $y = xs$ for $s \in N_x \subseteq N_y$, and so $x = ys^{-1}$ and $s^{-1} \in N_y$. Thus $y \equiv x$. Also $N_x = N_y$.

Finally, if $y = xs$ and $z = yt$ with $s \in N_x$ and $t \in N_y = N_x$, then $z = xst$ and $st \in N_x$, so that $\equiv$ is transitive. The proof is complete.

For $\omega \in F$, we define the length $l(\omega)$ to be the sum of the absolute values of the exponents in a reduced word defining ω. We have for $\omega \neq 1$, $\omega = X\omega_0$, where $X = X_j$ or $X = X_j{}^{-1}$ and $l(\omega_0) = l(\omega) - 1$.

LEMMA 2. *Let $\omega \in F$. Then there exist $\omega_i \in F$ for $1 \leqq i \leqq l(\omega)$ and $\epsilon_i = \pm 1$ such that*

$$\omega(xt) = \omega(x) \prod_i (t^{\epsilon_i})^{\omega_i(x)},$$

for all $x \in G^n$ and $t \in G$.

Proof. By induction on $l(\omega)$. The lemma is trivial when $l(\omega) = 0$. Suppose then that $\omega = X\omega_0$, where $X = X_j$ or $X_j{}^{-1}$ and $l(\omega_0) = l(\omega) - 1$. By the inductive hypothesis, ω_i and ϵ_i can be defined for ω_0, with $2 \leqq i \leqq l(\omega)$ and

$$\omega_0(xt) = \omega_0(x) \prod_{i=2}^{l(\omega)} (t^{\epsilon_i})^{\omega_i(x)}.$$

Suppose that $X = X_j$. Then

$$\omega(xt) = x_jt\omega_0(xt) = x_jt\omega_0(x) \prod_{i=2}^{l(\omega)} (t^{\epsilon_i})^{\omega_i(x)}.$$

However, $t\omega_0(x) = \omega_0(x)t^{\omega_0(x)}$ and we may take $\omega_1 = \omega_0$ and $\epsilon_1 = 1$ to prove the result in this case. If we have $X = X_j{}^{-1}$, then

$$\omega(xt) = (x_jt)^{-1}\omega_0(xt) = t^{-1}x_j{}^{-1}\omega_0(x) \prod_{i=2}^{l(\omega)} (t^{\epsilon_i})^{\omega_i(x)} = \omega(x)(t^{-1})^{\omega(x)} \prod_{i=2}^{l(\omega)} (t^{\epsilon_i})^{\omega_i(x)}$$

and the result follows if we take $\omega_1 = \omega$ and $\epsilon_1 = -1$.

COROLLARY 3. *Let $\omega \in F$ and let $x \equiv y$. Then $\omega(y) = \omega(x)s$ for some $s \in N_x$.*

Proof. We have $y = xt$ with $t \in N_x$. By Lemma 2, we may take $s = \prod_i (t^{\epsilon_i})^{\omega_i(x)}$. However, $\omega_i(x) \in \langle x\rangle \subseteq \mathbf{N}(N_x)$ so that $s \in N_x$ and the result follows.

For $x = (x_1, x_2, \ldots, x_n) \in G^n$, let $\bar{x} = (x_1, x_1, \ldots, x_1)$. For $\omega \in F$, define the degree, $d(\omega)$, to be the algebraic sum of the exponents of a reduced word for ω. If $\omega(\bar{x}) = 1$ for all $x \in G^n$, we shall call ω *special*. Clearly, ω is special if $d(\omega) = 0$.

LEMMA 4. *Let $t \in N_x$ and $\omega \in F$. Then $t^{\omega(x)} = t^{\omega(\bar{x})}$.*

Proof. Use induction on $l(\omega)$. If $l(\omega) = 0$, the result is trivial. Assume that $l(\omega) > 0$ and write $\omega = \omega_0 X$ where $X = X_j$ or X_j^{-1} and $l(\omega_0) = l(\omega) - 1$. We have $t^{\omega(x)} = t^{\omega_0(x)x_j^\epsilon} = t^{\omega_0(\bar{x})x_j^\epsilon}$, where $\epsilon = \pm 1$. Now $s = t^{\omega_0(\bar{x})} \in N_x$ and $t^{\omega(\bar{x})} = t^{\omega_0(\bar{x})x_1^\epsilon} = s^{x_1^\epsilon}$. It thus suffices to show $s^{x_j^\epsilon} = s^{x_1^\epsilon}$. If $\epsilon = +1$, this is immediate since $s \in N_x \subseteq H_x$. Now $s^{x_j^{-1}} \in N_x$ and hence

$$s^{x_1^{-1}x_1} = s = (s^{x_j^{-1}})^{x_j} = s^{x_j^{-1}x_1}.$$

Thus $s^{x_1^{-1}} = s^{x_j^{-1}}$ and the lemma follows.

LEMMA 5. *Let $\omega \in F$ be special and suppose that $x \equiv y$. Then $\omega(x) = \omega(y)$.*

Proof. We have $y = xt$ for $t \in N_x$ and thus

$$\omega(y) = \omega(x) \prod (t^{\epsilon_i})^{\omega_i(x)} = \omega(x)s.$$

Since $t^{\epsilon_i} \in N_x$, it follows by Lemma 4 that $s = \prod (t^{\epsilon_i})^{\omega_i(\bar{x})}$. Therefore, $\omega(\bar{y}) = \omega(\bar{x})s$ by Lemma 2. However, since ω is special, we have $\omega(\bar{x}) = \omega(\bar{y}) = 1$ and thus $s = 1$ and the result follows.

Now any automorphism σ of G permutes the elements of G^n by

$$x^\sigma = (x_1, \ldots, x_n)^\sigma = (x_1^\sigma, \ldots, x_n^\sigma).$$

If σ fixes H and $x \equiv_H y$, then clearly $x^\sigma \equiv_H y^\sigma$ and thus σ permutes the $\equiv_H$ conjugacy classes. In particular, conjugation by elements of H permutes these classes and we shall denote by $\sim_H$ the equivalence relation on G^n whose classes are the unions of sets of $\equiv_H$ classes, conjugate under the action of H. If there is no danger of ambiguity we shall write $\sim$ instead of $\sim_H$. Note that $x \sim y$ if and only if there exists $t \in N_y$ and $h \in H$ with $x = (yt)^h$.

COROLLARY 6. *Let $\omega \in F$ be special and suppose that $x \sim y$. Then $\omega(y) = \omega(x)^h$ for some $h \in H$.*

Proof. We have $x \equiv z$ and $y = z^h$ for some $z \in G^n$ and $h \in H$. Then

$$\omega(y) = \omega(z^h) = \omega(z)^h = \omega(x)^h,$$

where the last equality follows by Lemma 5.

LEMMA 7. *Assume that H is finite and let $x \in G^n$. Then the class of x under $\sim$ has cardinality $|H|$ and is the union of $|H:N_x|$ classes under $\equiv$.*

Proof. Let $\mathscr{C}$ be a class under $\equiv$, and let $\mathscr{O} = \{\mathscr{C}^h | \, h \in H\}$. Then the $\sim$ class containing $\mathscr{C}$ has cardinality $|\mathscr{O}| \, |\mathscr{C}|$. Let $x \in \mathscr{C}$, so that $|\mathscr{C}| = |N_x|$.

Let $T = \{h \in H | \mathscr{C}^h = \mathscr{C}\}$. We claim that $T = N_x$ and thus $|\mathscr{O}| = |H:N_x|$ and the result will follow.

First, $N_x \subseteq T$ for if $t \in N_x$ then $x_j^t = t^{-1}x_jt = x_j(t^{-1})^{x_j}t = x_j(t^{-1})^{x_1}t$. Now $s = (t^{-1})^{x_1}t \in N_x$ is independent of j and so $x^t = xs \equiv x$. Thus $\mathscr{C}^t = \mathscr{C}$.

Conversely, suppose that $s \in T$. Then $x^s = xt$ for some $t \in N_x$. Thus $x_j^s = x_jt$ and we obtain $s^{x_j} = st^{-1}$ and is independent of j. Thus $T \subseteq H_x$. Furthermore, $st^{-1} \in T$ and the equation $s^{x_j} = st^{-1}$ shows that $x_j \in \mathbf{N}(T)$. Thus $\langle x \rangle \subseteq \mathbf{N}(T)$ and hence

$$T \subseteq \bigcap_{g \in \langle x \rangle} H_x^g = N_x.$$

The proof is complete.

2. The results already accumulated are sufficient to prove the theorems when only special $\omega \in F$ are involved. In this section we discuss a slight refinement of Solomon's method of treating the general situation.

For $\omega \in F$, we define a row vector $[\omega]$ over the integers, $\mathbf{Z}$. Set $[\omega] = (r_1, \ldots, r_n)$ where r_j is the sum of the exponents of X_j in a reduced word for ω. In particular then, the sum of the entries of $[\omega]$ is $d(\omega)$. For any group G, ω defines a map $G^n \to G$. Taking $G = F$ and $\alpha = (\alpha_1, \ldots, \alpha_n) \in F^n$, we have $\omega(\alpha) \in F$. It is clear that $[\omega(\alpha)]$ is given by $[\omega]M$, where $M = M(\alpha)$ is the $n \times n$ matrix whose ith row is $[\alpha_i]$.

Again let G be an arbitrary group. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in F^n$ and $x = (x_1, \ldots, x_n) \in G^n$. We define $\alpha \cdot x = (\alpha_1(x), \alpha_2(x), \ldots, \alpha_n(x)) \in G^n$. In particular, if $F = G$, this defines a product on F^n. If $\alpha, \beta \in F^n$, then the ith row of $M(\alpha \cdot \beta)$ is $[\alpha_i(\beta)] = [\alpha_i]M(\beta)$. It follows that $M(\alpha \cdot \beta) = M(\alpha)M(\beta)$.

LEMMA 8. *For $\alpha \in F^n$, $\omega \in F$, and $x \in G^n$, we have $\omega(\alpha \cdot x) = (\omega(\alpha))(x)$.*

Proof. Let π be the homomorphism from F into G with $\pi(X_j) = x_j$, where $x = (x_1, \ldots, x_n)$. Then $\pi(\omega) = \omega(x)$ for any $\omega \in F$. Then

$$(\omega(\alpha))(x) = \pi(\omega(\alpha)) = \omega(\pi(\alpha_1), \ldots, \pi(\alpha_n)) = \omega(\alpha_1(x), \ldots, \alpha_n(x)) = \omega(\alpha \cdot x).$$

COROLLARY 9. *For α, $\beta \in F^n$ and $x \in G^n$, we have $\alpha \cdot (\beta \cdot x) = (\alpha \cdot \beta) \cdot x$. Also, the product defined on F^n is associative.*

Proof. The first statement follows by applying Lemma 8 to $\alpha_i(\beta \cdot x)$. The second follows by taking $G = F$.

Let $I = (X_1, \ldots, X_n) \in F^n$. Then $\alpha \cdot I = \alpha = I \cdot \alpha$ for all $\alpha \in F^n$. Let $\mathfrak{G} \subseteq F^n$ consist of those elements which are invertible in the semigroup F^n, so that $\mathfrak{G}$ is a group. The permutations of F^n given by $\beta \to \alpha \cdot \beta$ for $\alpha \in \mathfrak{G}$ are called Neilsen transformations (see [**4**, Chapter 3]) and have been studied as part of the theory of free groups. The next result is essentially [**4**, Corollary 3.5.1].

LEMMA 10. *The restriction of the mapping M to $\mathfrak{G}$ is a homomorphism of $\mathfrak{G}$ onto* $\mathrm{GL}(n, \mathbf{Z})$.

Proof. We have already seen that $M(\alpha \cdot \beta) = M(\alpha)M(\beta)$ for all $\alpha, \beta \in F^n$. Since $M(I)$ is the identity in $\mathrm{GL}(n, \mathbf{Z})$, it follows that M maps $\mathfrak{G}$ into $\mathrm{GL}(n, \mathbf{Z})$. It suffices to show that a set of generators for $\mathrm{GL}(n, \mathbf{Z})$ lies in $M(\mathfrak{G})$. For a permutation π of $\{1, 2, \ldots, n\}$, let $\alpha_\pi = (X_{\pi(1)}, \ldots, X_{\pi(n)}) \in F^n$. Clearly, $\alpha_\pi \in \mathfrak{G}$ and $M(\alpha_\pi)$ is the permutation matrix associated with π. Let $\beta = (X_1X_2, X_2, \ldots, X_n)$ and $\gamma = (X_1^{-1}, X_2, \ldots, X_n)$. Now $\beta \in \mathfrak{G}$ since $\beta^{-1} = (X_1X_2^{-1}, X_2, \ldots, X_n)$ and $\gamma^{-1} = \gamma$ so that $\gamma \in \mathfrak{G}$. By [**2**, p. 85], $M(\beta)$, $M(\gamma)$, and the permutation matrices generate $\mathrm{GL}(n, \mathbf{Z})$.

LEMMA 11. *Let $\omega_1, \omega_2, \ldots, \omega_m \in F$ with $m < n$. Then there exists $\alpha \in \mathfrak{G}$ such that $d(\omega_i(\alpha)) = 0$ for $1 \leqq i \leqq m$.*

Proof. Let A be the $m \times n$ matrix with rows $[\omega_i]$. Since $m < n$, the columns of A are linearly dependent. Let V be the n-dimensional column space over $\mathbf{Z}$ so that there exist $v \in V$ with $Av = 0$ but $v \neq 0$. Let $V_0 = \{v \in V | Av = 0\}$ so that V_0 is a pure submodule of V and thus is a direct summand of V. Let V_1 be the set of $v \in V$ with all entries equal. Then V_1 is also a pure submodule of V and hence a direct summand. It follows that for some $B \in \mathrm{GL}(n, \mathbf{Z})$ and $v_0 \in V_0$, $v_1 \in V_1$ with $v_1 \neq 0$, that $Bv_1 = v_0$. Then $(AB)v_1 = Av_0 = 0$. It follows that each row sum in the matrix AB is 0 and the ith row of AB is $[\omega_i]B$. Now $B = M(\alpha)$ for some $\alpha \in \mathfrak{G}$ and $[\omega_i]B = [\omega_i]M(\alpha) = [\omega_i(\alpha)]$. It follows that $d(\omega_i(\alpha)) = 0$.

3. In this section we prove three consequences of our lemmas, including the two theorems stated in the introduction. Let G be a finite group and let $\omega_1, \omega_2, \ldots, \omega_m \in F$, the free group on n generators. Assume either that $m < n$ or that all ω_i are special. Let $K_1, K_2, \ldots, K_m$ be normal subsets of G. We shall say that $x \in G^n$ is a *solution* if $\omega_i(x) \in K_i$ for all i, $1 \leqq i \leqq m$.

LEMMA 12. *There exists $\alpha \in \mathfrak{G}$ such that if x is a solution and $\alpha^{-1} \cdot x \sim_H \alpha^{-1} \cdot y$ for any subgroup $H \subseteq G$, then y is a solution.*

Proof. Choose $\alpha \in \mathfrak{G}$ such that $\omega_i(\alpha)$ is special for $1 \leqq i \leqq m$. (If $m < n$, this can be done by Lemma 11; otherwise, by hypothesis, each ω_i is special and we may take $\alpha = I$.) For any $z \in G^n$ we have (using Lemma 8)

$$\omega_i(\alpha)(\alpha^{-1} \cdot z) = \omega_i(\alpha \cdot (\alpha^{-1} \cdot z)) = \omega_i(I \cdot z) = \omega_i(z).$$

In particular, $\omega_i(\alpha)(\alpha^{-1} \cdot x) \in K_i$. By Corollary 6,

$$\omega_i(y) = \omega_i(\alpha)(\alpha^{-1} \cdot y) \in K_i^h = K_i$$

for some $h \in H$. The proof is complete.

THEOREM 13. *Let $H \subseteq G$ and let k_j be an integer for $1 \leqq j \leqq n$. Then the number of solutions $x = (x_1, x_2, \ldots, x_n)$ with the additional property that $x_j^{k_j} \in H$ for all j, is divisible by $|H|$.*

Proof. Choose $\alpha \in \mathfrak{G}$ as in Lemma 12. Suppose that x is a solution with $x_j^{k_j} \in H$. Let $\mathscr{S} = \{y \in G^n | \alpha^{-1} \cdot x \sim_H \alpha^{-1} \cdot y\}$. By Corollary 9, it follows

https://doi.org/10.4153/CJM-1970-120-0 Published online by Cambridge University Press

that the functions $u \to \alpha \cdot u$ and $u \to \alpha^{-1} \cdot u$ are inverses on G^n and thus $|\mathscr{S}| = |H|$ since the $\sim_H$ class of $\alpha^{-1} \cdot x$ contains exactly $|H|$ elements by Lemma 7. By Lemma 12, each $y \in \mathscr{S}$ is a solution and the proof will be complete when we show that $y_j^{k_j} \in H$ for $y = (y_1, \ldots, y_n) \in \mathscr{S}$. Let $\alpha = (\alpha_1, \ldots, \alpha_n)$, and let $u = \alpha^{-1} \cdot x$, $v = \alpha^{-1} \cdot y$ and $u \equiv_H w$, $v = w^h$ with $h \in H$. Then $y_j = \alpha_j(v) = \alpha_j(w^h) = \alpha_j(w)^h$ and $y_j^{h^{-1}} = \alpha_j(w) = \alpha_j(u)t$ for some $t \in N_u$ by Corollary 3. Now $x_j = \alpha_j(u) \in \langle u \rangle \subseteq \mathbf{N}(N_u)$ and thus $(y_j^{h^{-1}})^{k_j} = (x_j t)^{k_j} \in x_j^{k_j} N_u \subseteq H$. It follows that $y_j^{k_j} \in H$, and the proof is complete.

THEOREM 14. *Let $k \,\|\, |G|$ and let $L_1, L_2, \ldots, L_n$ be conjugacy classes of G. Then the number of solutions $(x_1, \ldots, x_n) = x$ with the additional property that $x_j^k \in L_j$ is divisible by k.*

Proof. Choose α as in Lemma 12. Let $p^a | k$ for prime p. We show that the number of $x \in G^n$ satisfying the conditions is divisible by p^a. Since $p^a \,\|\, |G|$, we may choose $H \subseteq G$ so that $|H| = p^a$. Let x be a solution satisfying $x_j^k \in L_j$ for all j and let $\mathscr{S} = \{y \in G^n | \alpha^{-1} \cdot x \sim_H \alpha^{-1} \cdot y\}$. Then as before, $|\mathscr{S}| = |H| = p^a$ and every $y \in \mathscr{S}$ is a solution. Our proof will be complete if we show for $y = (y_1, \ldots, y_n) \in \mathscr{S}$, that $y_j^k \in L_j$. Suppose that $\alpha = (\alpha_1, \ldots, \alpha_n)$ and let $u = \alpha^{-1} \cdot x$, $v = \alpha^{-1} \cdot y$ and $u \equiv_H w$, $w^h = v$ for $h \in H$. Then, as in the previous proof, $y_j^{h^{-1}} = x_j t$ with $t \in N_u$ and $x_j \in \mathbf{N}(N_u)$. Consider the group $B = \langle N_u, x_j \rangle$. By the lemma of Brauer's paper [**1**] applied to B, it follows that x_j^ν and $(x_j t)^\nu$ are conjugate in B, where $\nu = |N_u|$ divides k. Thus x_j^k and y_j^k are conjugate in G and the result follows.

THEOREM 15. *Let $R = \mathbf{Z}[\epsilon]$, where ϵ is a primitive $|G|$th root of 1. Suppose that the K_j are conjugacy classes of G. Let $\mathscr{S}_j(g) = \{x = (x_1, \ldots, x_n) \in G^n | x$ is a solution and $x_j = g\}$. Set $\theta_j(g) = |\mathscr{S}_j(g)|$. Then θ_j is an R-linear combination of characters of G.*

Proof. By Brauer's theorem on induced characters, every character of G is a $\mathbf{Z}$-Linear combination of induced characters of linear characters of subgroups of G (see [**3**, Theorem 40.1]). By Frobenius reciprocity, it suffices to show, for $H \subseteq G$ and λ a linear character of H, that

$$\frac{1}{|H|} \sum_{h \in H} \theta_j(h) \lambda(h) \in R.$$

Fix a particular subgroup H and linear character λ and denote the above sum by ξ. Choose $\alpha \in \mathfrak{G}$ as in Lemma 12 and let $\mathscr{T}_j(g) = \{\alpha^{-1} \cdot x | x \in \mathscr{S}_j(g)\}$. Then if $\alpha = (\alpha_1, \ldots, \alpha_n)$, we have $g = \alpha_j(y)$ for $y \in \mathscr{T}_j(g)$. Since $\theta_j(g) = |\mathscr{T}_j(g)|$, we have

$$\begin{aligned} \xi &= \frac{1}{|H|} \sum_{h \in H} \sum_{y \in \mathscr{T}_j(h)} \lambda(\alpha_j(y)) \\ &= \frac{1}{|H|} \sum_{y \in \mathscr{T}_j} \lambda(\alpha_j(y)) \end{aligned}$$

where $\mathscr{T}_j = \bigcup_{h \in H} \mathscr{T}_j(h)$. Clearly, $y \in \mathscr{T}_j$ if and only if $\alpha \cdot y$ is a solution and $\alpha_j(y) \in H$. Suppose that $y \in \mathscr{T}_j$ and $y \sim_H z$. Then $\alpha \cdot z$ is a solution and $\alpha_j(z) = (\alpha_j(y)s)^h$ for some $s \in N_y$ and $h \in H$ by Corollary 3. Since $\alpha_j(y) \in H$, it follows that $\alpha_j(z) \in H$ and $z \in \mathscr{T}_j$. Therefore, $\mathscr{T}_j$ is a union of classes under $\sim_H$. Let $\mathscr{C}$ be the class of y under $\equiv_H$ and let

$$\eta = \frac{1}{|N_y|} \sum_{z \in \mathscr{C}} \lambda(\alpha_j(z)).$$

If $\mathscr{C}$ is replaced by $\mathscr{C}^h$ for any $h \in H$, then the value of η remains unchanged since

$$\lambda(\alpha_j(z^h)) = \lambda(\alpha_j(z)^h) = \lambda(\alpha_j(z)).$$

Since the $\sim_H$ class $\mathscr{C}^*$, containing y, is the union of $|H:N_y|$ such conjugates of $\mathscr{C}$, by Lemma 7, it follows that

$$\eta = \frac{1}{|H|} \sum_{z \in \mathscr{C}^*} \lambda(\alpha_j(z)).$$

Thus ξ is a sum of quantities of the form η and it suffices to show that $\eta \in R$.

Apply Lemma 2 to α_j and pick $\omega_i \in F$ and $\epsilon_i = \pm 1$ with $\alpha_j(yt) = \alpha_j(y) \prod (t^{\epsilon_i})^{\omega_i(y)}$. Since $\mathscr{C} = \{yt | \, t \in N_y\}$, we have

$$\eta = \frac{\lambda(\alpha_j(y))}{|N_y|} \sum_{t \in N_y} \lambda(\Pi(t^{\epsilon_i})^{\omega_i(y)}).$$

Now $\omega_i(y) \in \mathbf{N}(N_y)$ and thus $\mu(t) = \lambda(\prod (t^{\epsilon_i})^{\omega_i(y)})$ defines a linear character of N_y. It follows that $\eta = \lambda(\alpha_j(y))$ if $\mu = 1$ and $\eta = 0$ otherwise. In any case, $\eta \in R$, and the proof is complete.

REFERENCES

1. R. Brauer, *On a theorem of Frobenius*, Amer. Math. Monthly *76* (1969), 12–15.
2. H. S. M. Coxeter and W. O. Moser, *Generators and relations for discrete groups*, Second Ed. (Springer-Verlag, New York, 1965).
3. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras* (Interscience, New York, 1962).
4. W. Magnus, A. Karrass, and D. Solitar, *Combinational group theory* (Interscience, New York, 1966).
5. L. Solomon, *The solution of equations in groups*, Arch. Math. *20* (1969), 241–247.

University of Wisconsin,
Madison, Wisconsin