ON THE RADICAL OF A GROUP ALGEBRA

D. A. R. WALLACE[1]

Let G be a finite group of order $p^a m$ where p is prime and $(p, m)=1$. Let Ω be an algebraically closed field of characteristic p. We consider the group algebra $A(G, \Omega)$ of G over Ω; this group algebra possesses a radical which we denote by $N(G, \Omega)$. We give an upper bound for the dimension of $N(G, \Omega)$ and show that this upper bound is attained if and only if G has a normal p-Sylow subgroup.

We follow closely the nomenclature of Brauer and Nesbitt [2]. Let G have p-regular classes $C_1, C_2, \cdots, C_k$, where C_1 consists of the identity element of G and C_ν contains g_ν elements $(\nu=1, 2, \cdots, k)$. Let $F_1, F_2, \cdots, F_k$, and $U_1, U_2, \cdots, U_k$, be the absolutely irreducible and indecomposable representations of G over the field Ω with modular characters $\phi^1, \phi^2, \cdots, \phi^k$, and $\eta^1, \eta^2, \cdots, \eta^k$, of degrees $f_1, f_2, \cdots, f_k$ and $u_1, u_2, \cdots, u_k$ respectively. We assume that F_1 represents every element of G by the unit element of Ω and that F_κ is the first and last irreducible constituent of U_κ $(\kappa=1, 2, \cdots, k)$.

Denoting the dimension of $N(G, \Omega)$ by dim $N(G, \Omega)$, then we have the following upper bound due to Brauer and Nesbitt [2, p. 580]:

$$\dim N(G, \Omega) \leqq p^a m - \frac{p^a m}{u_1} \cdot$$

We prove:

THEOREM. $\dim N(G, \Omega)=p^a m-(p^a m/u_1)$ *if and only if* G *has a normal* p*-Sylow subgroup.*

If G has a normal p-Sylow subgroup G_p then there exists in G a subgroup of order m [3, p. 224] and consequently $u_1=p^a$ [2, p. 583]. Let $x_1, x_2, \cdots, x_{p^a}$, be the elements G_p and let $y_1, y_2, \cdots, y_m$ be a set of coset representatives of G_p in G. Then we may verify that the elements $(x_1-x_i)y_j$ $(i=2, 3, \cdots, p^a; j=1, 2, \cdots, m)$ form a basis for $N(G, \Omega)$ and thus $\dim N(G, \Omega)=p^a m-m$. (Cf. [6, p. 253].)

We now assume that

$$\dim N(G, \Omega) = p^a m - \frac{p^a m}{u_1} \cdot$$

This implies that

Received by the editors February 22, 1960.

[1] This work was partly supported by the Office of Ordnance Research under contract no. DA 19-020-ORD-3778.

$$\sum_{\kappa=1}^{k} f_\kappa^2 = \frac{p^a m}{u_1}.$$

Hence [2, p. 580]

$$\begin{aligned}\sum_{\kappa=1}^{k} f_\kappa(u_1 f_\kappa - u_\kappa) &= u_1 \sum_{\kappa=1}^{k} f_\kappa^2 - \sum_{\kappa=1}^{k} u_\kappa f_\kappa \\ &= p^a m - p^a m \\ &= 0.\end{aligned}$$

But we know that [2, p. 580]

$$u_1 f_\kappa \geqq u_\kappa \qquad (\kappa = 1, 2, \cdots, k)$$

and hence we find that

$$u_1 f_\kappa = u_\kappa \qquad (\kappa = 1, 2, \cdots, k).$$

Consider now the Kronecker product representation $U_1 \otimes F_\kappa$. This contains U_κ as a constituent [2, p. 579; 5, p. 413]. Thus, on comparing the degrees, we see that U_κ and $U_1 \otimes F_\kappa$ are equivalent representations ($\kappa = 1, 2, \cdots, k$).

For convenience we now assume that the absolutely irreducible and indecomposable representations have been written with entries in some finite normal algebraic extension Ω^* of the prime field Ω_0. We suppose that Ω^* contains the modular mth roots of unity. Let Γ be the Galois group of this extension. Let $\alpha \in \Gamma$. If we denote by $U_1\alpha$ the action of α on the entries of U_1 then $U_1\alpha$ is again a representation of G and is, in fact, an indecomposable representation of the regular representation of G since the indecomposable representations appearing in the regular representation are permuted amongst themselves by such Galois automorphisms. Thus we may write

$$U_1\alpha = T^{-1}(U_1 \otimes F_\lambda)T,$$

for some λ ($1 \leqq \lambda \leqq k$) and some nonsingular matrix T. By comparing degrees we have

$$f_\lambda = 1.$$

We therefore consider two cases.

CASE 1. We assume that we have chosen an automorphism α such that $\lambda \neq 1$.

In this case G has at least two linear modular representations and thus, by a result of Brauer and Nesbitt [2, p. 588] we know that the index of the derived group of G in G is divisible by a prime q distinct from p. Let H be a normal subgroup of prime index q. Put $m = qm'$.

Let $\tilde{\phi}^1, \tilde{\phi}^2, \cdots, \tilde{\phi}^t$, and $\tilde{\eta}^1, \tilde{\eta}^2, \cdots, \tilde{\eta}^t$, be the irreducible and indecomposable modular characters of H (where we assume that $\tilde{\phi}^1$ corresponds to the linear representations which represents all elements of H by the unity of Ω) of degrees $\bar{f}_1, \bar{f}_2, \cdots, \bar{f}_t$, and $\tilde{u}_1, \tilde{u}_2, \cdots, \tilde{u}_t$, respectively. Let $\tilde{\phi}^{1*}, \tilde{\phi}^{2*}, \cdots, \tilde{\phi}^{t*}$, be the characters of G induced by the characters $\tilde{\phi}^1, \tilde{\phi}^2, \cdots, \tilde{\phi}^t$, of H.

Consider $\tilde{\phi}^{\kappa *}$ $(1 \leqq \kappa \leqq t)$. Since H is normal of prime index either $\tilde{\phi}^{\kappa *}$ is an irreducible representation of G of degree $q\bar{f}_\kappa$ or $\tilde{\phi}^{\kappa *}$ contains, as irreducible constituents, q distinct irreducible representations of G each of degree $\bar{f}_\kappa$. By counting the irreducible representations of H and of G we find that

$$\sum_{\kappa=1}^{k} f_\kappa^2 = \sum_{\mu=1}^{t} q\bar{f}_\mu^2,$$

which implies that

$$\dim N(G, \Omega) = q \dim N(H, \Omega).$$

Further, by the modular analogue of the Frobenius reciprocity law [2, p. 583; 4, p. 366] we have

$$\tilde{\phi}^{\kappa *} = \sum_{\lambda=1}^{k} \beta_{\kappa\lambda}\phi^\lambda \quad \text{(for } p\text{-regular elements of } G)$$

$$\eta^\lambda = \sum_{\kappa=1}^{t} \beta_{\kappa\lambda}\tilde{\eta}^\kappa \quad \text{(for } p\text{-regular elements of } H).$$

Now $\tilde{\phi}^{1*}$ corresponds to a representation of G which contains F_1 as an irreducible constituent. Thus

$$\beta_{11} \geqq 1.$$

We have therefore

$$\begin{aligned} u_1 &= \sum_{\kappa=1}^{t} \beta_{\kappa 1}\tilde{u}_\kappa \\ &\geqq \tilde{u}_1. \end{aligned}$$

Hence we have the inequalities

$$\begin{aligned} \dim N(H, \Omega) &\leqq p^a m' - \frac{p^a m'}{\tilde{u}_1} \\ &\leqq p^a m' - \frac{p^a m'}{u_1} \\ &= \dim N(H, \Omega). \end{aligned}$$

Thus

$$\dim N(H, \Omega) = p^a m' - \frac{p^a m'}{u_1}.$$

We may make the induction hypothesis that the theorem has been proved for the groups of orders less than the order of G. This implies that H has a normal p-Sylow subgroup H_p. Since H_p is characteristic in H, H_p is normal in G and clearly H_p is a p-Sylow subgroup of G.

CASE 2. Here we assume that, for all choices of Galois automorphisms, $\lambda = 1$. Thus we have, for all $\alpha \in \Gamma$,

$$U_1\alpha = T^{-1}(U_1 \otimes F_1)T = T^{-1}U_1T.$$

We wish to show that this implies that η_ν^1 is a rational integer ($\nu = 1, 2, \cdots, k$).

First we observe that for $x \in G$, $U_1\alpha(x)$ and $U_1(x)$ have the same latent roots. This implies that α merely permutes the latent roots of $U_1(x)$. We suppose now that x is p-regular.

Let θ be a primitive mth root of unity in the complex field. Let $\bar{\theta}$ be the corresponding primitive mth root of unity in Ω^* in the 1-1 correspondence between the mth roots of unity in the complex and modular fields [2, p. 560]. Let $\bar{\theta}^d$ be a latent root of $U_1(x)$. Then all conjugates of $\bar{\theta}^d$ appear as latent roots of $U_1(x)$ and each such conjugate appears the same number of times as $\bar{\theta}^d$. Now $\bar{\theta}^c$ is a conjugate of $\bar{\theta}^d$ in Ω^* if and only if θ^c is a conjugate of θ^d in the complex field. Thus in $\eta^1(x)\theta^d$ and all its conjugates appear, each the same number of times. Hence $\eta^1(x)$ is rational and so, being an algebraic integer, is a rational integer. Thus η_ν^1 is a rational integer ($\nu = 1, 2, \cdots, k$).

Now since U_κ and $U_1 \otimes F_\kappa$ are equivalent we have [2, p. 561]

$$\overset{1}{\eta}_\nu \overset{\kappa}{\phi}_\nu = \overset{\kappa}{\eta}_\nu = \sum_{\lambda=1}^{k} c_{\kappa\lambda} \overset{\lambda}{\phi}_\nu \qquad (\nu = 1, 2, \cdots, k),$$

where $C = (c_{\kappa\lambda})$ is the Cartan matrix. Thus we have

$$\sum_{\lambda=1}^{k} (c_{\kappa\lambda} - \delta_{\kappa\lambda}\overset{1}{\eta}_\nu)\overset{\lambda}{\phi}_\nu = 0 \qquad (\nu = 1, 2, \cdots, k),$$

where $\delta_{\kappa\lambda} = 0$ ($\kappa \neq \lambda$) and $\delta_{\kappa\kappa} = 1$. Hence the rational integers η_ν^1 ($\nu = 1, 2, \cdots, k$) are the k latent roots of the matrix C and so

$$\det C = \overset{1}{\eta}_1 \overset{1}{\eta}_2 \cdots \overset{1}{\eta}_k.$$

Let

$$\frac{p^a m}{g_\nu} = p^{e_\nu} g'_\nu \quad \text{where} \quad (p, g'_\nu) = 1 \qquad (\nu = 1, 2, \cdots, k).$$

Then the elementary divisors of C are $p^{s_1}, p^{s_2}, \cdots, p^{s_k}$, [2, p. 568] and thus

$$\det C = p^{s_1+s_2+\cdots+s_k}.$$

But we know that p^{s_ν} divides η_ν^1 $(\nu=1, 2, \cdots, k)$ [1, p. 15] and hence

$$\eta_\nu^1 = p^{s_\nu} \qquad (\nu = 1, 2, \cdots, k).$$

Now every element a of G can be written uniquely as $a=bc=cb$ where b is p-regular and c has order a power of p. Letting b range over the p-regular classes $C_1, C_2, \cdots, C_k$, and choosing for each such b all possible prime power elements c we shall obtain each element of G exactly once. But if $b\in C_\nu$ the centralizer of b has order $p^{s_\nu}g'_\nu$ and thus the number of choices for c is the number of solutions in this centralizer of the equation $y^{p^{s_\nu}}=e$, e being the identity of G. By a theorem of Frobenius [3, p. 136] this number is of the form $h_\nu p^{s_\nu}$ where h_ν is an integer. Hence finally we must have

$$\sum_{\nu=1}^{k} h_\nu p^{s_\nu} g_\nu = p^a m.$$

But [2, p. 562]

$$\sum_{\nu=1}^{k} g_\nu p^{s_\nu} = \sum_{\nu=1}^{k} g_\nu \eta_\nu^1 = p^a m.$$

Hence we see that

$$h_\nu = 1 \qquad (\nu = 1, 2, \cdots, k).$$

In particular the number of solutions of the equation $y^{p^a}=e$ in G is p^a. This implies that G has a unique p-Sylow subgroup which is consequently normal.

In conclusion the author wishes to thank Dr. Green for helpful discussions concerning the material of the latter part of this paper.

References

1. R. Brauer and C. Nesbitt, *On the modular representations of groups of finite order*, University of Toronto Studies, Mathematics Series, no. 4, 1937.

2. ———, *On the modular characters of groups*, Ann. of Math. vol. 42 (1941) pp. 556–590.

3. M. Hall, *Theory of groups*, New York, Macmillan 1959.

4. T. Nakayama, *Some studies on regular representations, induced representations and modular representations*, Ann. of Math. vol. 39 (1938) pp. 361–369.

5. M. Osima, *Note on the Kronecker product of representations of a group*, Proceedings of the Imperial Academy of Tokyo vol. 17 (1941) pp. 411–413.

6. L. Lombardo-Radice, *Intorno alle algebre legate ai gruppi di ordine finito.* II, Rend. Sem. Mat. Roma vol. 3 (1939) pp. 239–256.

Harvard University