SOME RESULTS ON THE GROUP ALGEBRA OF A GROUP OVER A PRIME FIELD

by

H. N. Ward

This note concerns the following situation: let p be a prime and let G be a finite p - group. Let K be the field $GF(p)$, and form the group algebra $A(G,k)$ of G over k. (Call it $A(G)$ for short.) The radical N of $A(G)$ has a basis consisting of all elements $g - 1$, where $g \neq 1$ is a member of G. For, since there are no p- regular classes in G, the trivial representation is the only irreducible representation of G in k. Relative to a proper basis, each $g - 1$ in the regular representation has 0's on its diagonal and so generates a nilpotent ideal.

Because of this there is a unique algebra homomorphism f: $A(G)$ onto k, and it is given by $f(\sum_G a_g g) = \sum_G a_g$. The kernel of f is the radical, and u is a unit iff $f(u) \neq 0$.

§ I. Theorem: Let G be any finite group (p - group or not). Let C be an Abelian finite p - group. Then there is an algebra homomorphism of $A(G)$ onto $A(C)$ iff there is a(group) homomorphism of G onto C.

One direction is immediate, for any homomorphism of G onto C extends linearly to one of $A(G)$ onto $A(C)$. For the other direction, there are a number of steps:

First, $A(C)$ determines C. For the dimension of $A(C)^{(p^m)}$ is the order of $C^{(p^m)}$ for any m; but those orders determine C (up to isomorphism). (Here $A^{(p^m)}$ means the set of p^m-th powers of elements of A). Next, regarding in general G as a subgroup of the group of units $A(G)^u$ of $A(G)$, one has that C is a direct factor of $A(C)^u$. For, $A(C)^u = k^*1.A(C)^1$, where $A(C)^1 = f^{-1}(1)$ and k^* is the multiplicative group of k. C is in $A(C)^1$; and if for u in $A(C)^1$, u has order p^m relative to C, a check of the coefficients in u^{p^m} shows that $u^{p^m} = g^{p^m}$ for some g in C. Thus the elements of a basis for $A(C)^1/C$ can be taken as images of elements with the same orders as these images; the group generated in $A(C)^1$ by these pre-images gives the desired complement for C. That complement times k^*1 is the complement for C in $A(C)^u$.

The methods in the reference (Jennings) show this: If C is a direct product of cyclic groups all of the same order, say n of them, and N is the radical of A(C), then any n elements $b_1, \ldots, b_n$ in A(C) for which the $b_i - 1$ are in N and are independent modulo N^2 generate a group isomorphic to C whose elements are a basis of A(C). (So if the group they generate is B, A(C) can be regarded as A(B).)

If C is cyclic, there must be an element g of G, mapping onto g' in A(C), for which $g' - f(g')$ is in N but not in N^2, N = radical of A(C); otherwise the homomorphism is not onto A(C) but at best onto $N^2 + k1$. One may take a power of g if needed for which the new g has $f(g') = 1$, but $g' - 1$ still not in N^2. If C' is the group generated by g', the previous remarks show A(C) can be regarded as A(C'). Find a complement of C' in $A(C')^u$; if H is the set of elements of G mapping into that complement, then G/H will be isomorphic to C' (and thereby to C).

If C is a direct product of cyclic groups all of the same order, say $C = C_1 \cdot C_2 \cdots C_n$; Form the projection p_1 of C onto C_1 corresponding to this product. If one extends this to the algebras, one has a homomorphism of $A(C_1)$. Find g_1 as before for this map. If the image of g_1 in A(C) generates the group C_1', considerations like those above show A(C) may be taken as $A(C_1' \cdot C_2 \cdots C_n)$. Let q_1 be the projection of $C_1' \cdot C_2 \cdots C_n$ onto $C_2 \cdot C_3 \cdots C_n$.

Composing q_1 extended to the algebras with the original homomorphism, one gets a map of $A(G)$ onto $A(C_2 \cdot C_3 \ldots C_n)$. One goes through the same sort of argument with C_2 now, and so on: finally one has elements $g_1, g_2, \ldots, g_n$ whose images in $A(C)$ generate a group isomorphic to C and consisting of independent elements, say C'. The elements of G mapping into a complement of C' in $A(C)^u$ then form a subgroup H of G for which G/H is isomorphic to C' (and thereby to C).

For general C, write $C = C_1 \cdot C_2 \ldots C_n$ where each C_i is a direct product of cyclic groups of the same orders, but these orders decrease strictly with i. Again project onto C_1 and extend the projection to the algebras. The previous case gives elements of G whose images in $A(C)$ will form a group isomorphic to C_1 and such that C_1 can be replaced in the product by this image, say C_1'. (This comes from arguments of independence modulo N^2 as before.) C_1' can be factored out, and the process repeated. The intersection of the H's found at each stage gives a subgroup H of G for which G/H is isomorphic to C, as needed.

Here are some questions: How much can C = Abelian be weakened? Given any p - group G, does G have a normal complement in $A(G)^u$? It should be mentioned that if G' is the commutator subgroup of G, the kernel of the homomorphism of $A(G)$ induced by that of G onto G/G' (and therefore onto $A(G/G')$) is the ideal generated by the elements of the form $ab - ba$ in $A(G)$; and so (for p-groups at least) $A(G)$ determines the group G/G'. Exploiting this fact, Dr. Dr. Takahashi has another proof of this result.

§II. Here are some results in the case G is a p - group and is regarded as a subgroup of the group $A(G)^u$.

Theorem: Let H_1 and H_2 be two subgroups of G. Let $U = A(G)^u$ and consider the set M of elements in U, say u, for which $u^{-1}H_1u$ is contained in H_2. If M_G is M intersected with G, then one has $M = C_U(H_1)\cdot M_G$:

For, it is clear that $C_U(H_1)\cdot M_G$ is contained M. On the other hand, let a be in M. Write $a = \sum_G a_g g$, as before. For h in H_1, one has $a^{-1}ha = h^a$ belongs to H_2. In terms of the coefficients of a, this amounts to the requirement that $a_g = a_{(h^{-1}gh^a)}$ for all g in G and all h in H_1. But the map p_h which takes g onto $h^{-1}\,gh^a$ is a permutation of G (written on the right); and the map of h onto p_h is a permutation representation of H_1 on G. H_1 being a p - group, the orbits all have lengths which are powers of p. The coefficients of a are constant on these orbits. $f(a)$ will be 0 unless at least one orbit has only one element; and since a is a unit, that must be the case. So for some g in G, $gp_h = g$ for all h in H_1. That means $h^a = g^{-1}hg$. So g is in M_G; moreover, then, ag^{-1} is in $C_U(H_1)$. But then a is in $C_U(H_1)M_G$ as wished.

$C_U(H_1)$ can be got this way: in general, if $ah = ha$ for all h in H_1, where a is any element of $A(G)$, then one must have $a_g = a_{(h^{-1}gh)}$ for all H in H_1 and all g in G. A basis for the set of all such a's is the set of distinct elements K_i, where each K_i is the sum of the distinct conjugates by members of H_1 of a fixed g_i in G. $C_U(H_1)$ would be the units of this set.

If $H_1 = H_2 = H$, then $M = N_U(H)$. Then $N_U(H) = C_U(H)\cdot N_G(H)$. Using the fact that $C_U(H)$ is normal in $N_U(H)$ and that $C_U(H)$ meets $N_G(H)$ in exactly $C_G(H)$, one can show by some inequalities derived from the description of $C_U(H)$ given above, that the only way H can be normal in U is for H to be a subgroup of the center of G. (This can be proved another way by constructing suitable a's according to the equation on the coefficients given above.)

Another result is that there is no fusion of conjugate classes when one passes from G into U. For, if h_1 and h_2 are conjugate in U, the result, with H_1 equal to the group generated by h_1, H_2 the group by h_2, would show h_1 and h_2 already conjugate in G.

The method of proof of the preceding extends to a more general case:

Theorem: Let the hypotheses be as before, only now consider $A(H_1)$ and $A(H_2)$ as subalgebras of $A(G)$. Let M be the set of elements a of U for which $a^{-1}A(H_1)a$ is contained in $A(H_2)$. Let M_G be as before. Then

$M = C_U(H_1)\cdot M_G\cdot A(H_2)^u$.

Again, inclusion of the right side in the left is clear. For any a in M, collect together the elements of G belonging to the same left coset of H_2 when writing a out in terms of elements of G. Then $a = \sum_R g_r u_r$, where R is the left coset space G/H_2 and g_r is a fixed representative for r (a member of R). Also, u_r is in $A(H_2)$.

Let H_1 act on R by left multiplication in G, and let q be the resulting representation of H_1; that is, for h in H_1, $h(g_r H_2) = g_{q_h(r)}H_2$. Say $hg_r = g_{q_h(r)}(h,r)$ where (h,r) is in H_2. If one writes out the equation $a^{-1}ha = h^a, h^a$ in $A(H_2)$ with respect to these coefficients, then one will get similar to before, $(h,r)u_r = u_{q_h(r)}h^a$, for all h and all r. Apply f and note $f((h,r)) = f(h^a) = 1$. One gets $f(u_r) = f(u_{q_h(r)})$. This corresponds to the old $a_g = a_{(h^{-1}gh^a)}$. Again, for a to be a unit, at least one orbit has only one element, say r, and also $f(u_r) \neq 0$. Then $hg_r = g_r(h,r)$; so $(h,r) = g_r^{-1}hg_r$ and g_r is in M_G. Then $h^a = u_r^{-1}g_r^{-1}hg_r u_r$. So $au_r^{-1}g_r^{-1}$ is in $C_U(H_1)$: And then the result follows. Again one can show that $A(H)^u$ will be normal in U only when H is in the center of G.

§III. Finally, the two propositions proved here involve the same lemma:

Lemma: Let H be a subgroup of G. Recall the structure of the algebra $C(H)$ of elements of $A(G)$ commuting elementwise with H. In $C(H)$ let J be the space spanned by those K_i which are sums of more than one element. Then J is an ideal in $C(H)$.

For, $C(H)$ is spanned by J and the elements of $C_G(H)$ (those are the K_i with only one element). Say $K_i = \sum h_j^{-1} g h_j$, where the h_j are in H. For h in $C_{G(H)}$, $hK_i = \sum h_j^{-1} hgh_j$ and that is another K_i, since anything commuting with hg commutes with g (in $C_G(H)$). Similarly for $K_i h$. Secondly, $K_i K_j$ can have no element with non-0 coefficient in $C_G(H)$. For, if so, one may assume that K_i and K_j are the sums of the conjugates by members of H of g_i and g_j and $g_i g_j$ is in $C_G(H)$. Then for h in H, h commutes with g_i iff it commutes with g_j. Then $K_i = \sum h_s^{-1} g_i h_s$ and $K_j = \sum h_s^{-1} g_j h_s$, summed over the same h_s's. Because of this, $g_i g_j = (h_s^{-1} g_i {}^{h}s)$ iff $s = t$; so $g_i g_j$ appears with a coefficient which is a power of p (as an integer) and therefore 0. So $K_i K_j$ is in J.

Theorem: If for u in $A(G)$, u^{p^m} is in G for some m, then there is a g in G appearing with non-0 coefficient in u for which $u^{p^m} = g^{p^m}$.

For, let $h = u^{p^m}$, and let h generate the subgroup H of G. Then u is in $C_U(H)$. Keeping the notation of the lemma, one then has $u = a + b$, where b is in J and a is in $A(C_G(H))$. J being an ideal of $C(H)$, $u^{p^m} = a^{p^m} + b'$, b' still in J. In fact, $b' = 0$, since no member of $C_G(H)$ appears in an element of J. Now apply an induction. When G is Abelian the result holds, from §I. And, if $C_G(H)$ is a proper subgroup of G, apply the induction to a and get the result (anything appearing in with non-0 coefficient appears that way in u). So say $C_G(H) = G$. h is in the center of G, then. Then $h = (\sum a_g g)p^m = \sum a_g g^{p^m} + \ldots$, where the "..." represents the cross-terms. But h cannot appear among those; for if a product of p^m elements of G is h, so are all the cyclic permutations of that product, and the sum has coefficient 0 (as a member of k). So h must be g^{p^m} for some g with $a_g \neq 0$, as asserted.

Theorem: Let Z be the center of A(G): then A = C(G); then Z = C(G) in the notation of the lemma. In this case, J is the intersection of Z with the linear space generated by all elements ab-ba in A(G). Moreover, Z/J is isomorphic to A(Z(G)), Z(G) the center of G.

For, as pointed out in the lemma, C(G) will be generated by J and A(Z(G)); consequently Z/J will be just A(Z(G)). Since for g, h in G, $g - h^{-1}gh = (gh)h^{-1} - h^{-1}(gh)$, g and $h^{-1}gh$ are congruent modulo the space mentioned. Since any g in G has a power of p conjugates, and K_1 (with more than one summand) is in this space. Yet no element of Z(G) can appear with non-0 coefficient as a member of this space,for by linearity this space is spanned by all elements gh - hg, g and h in G; and if gh = z in Z(G), hg = z also. So the intersection is exactly J, as asserted. This implies that A(G) determines Z(G) up to isomorphism.

Reference: S. A. Jennings, Structure of the group ring of a p-group over a modular field. Trans. A. M. S., v. 50, p. 175 (1941)