PACIFIC JOURNAL OF MATHEMATICS
Vol. 59, No. 2, 1975

ON SEMI-SIMPLE GROUP ALGEBRAS (I)

EUGENE SPIEGEL AND ALLAN TROJAN

For F a field and G a group, let FG denote the group algebra of G over F. Let $\mathscr{G}$ be a class of finite groups, and $\mathscr{F}$ a class of fields. Call the fields F_1 and F_2 ($F_i \in \mathscr{F} i = 1, 2$) equivalent on $\mathscr{G}$ if for all $G, H \in \mathscr{G}$, $F_1G \simeq F_1H$ if and only if $F_2G \simeq F_2H$. In this note we begin a study of this equivalence relation, taking the case where $\mathscr{G}$ consists of all finite p-groups and $\mathscr{F}$ those fields F, for which FG is simi-simple for all $G \in \mathscr{G}$.

1. Let ζ_n denote a primitive n^{th} root of unity (over the field under consideration). Throughout the paper, p will denote a fixed odd prime, and all fields will be assumed to be of characteristic distinct from p.

For reference, we begin with a result from field theory.

PROPOSITION 1.1. *Suppose F is a field and Ω an extension field of F. Let $K_i = 1, 2$ be fields such that $F \subset K_i \subset \Omega$, and assume that K_1/F is a finite Galois extension. Then the following are equivalent.*

(i) *K_1 and K_2 are linearly disjoint over F*

(ii) *$K_1 \otimes_F K_2$ is a field*

(iii) *$K_1 \otimes_F K_2 \simeq K_1K_2$*

(iv) *$K_1 \cap K_2 = F$.*

Proof. See [1] page 78 and page 149.

Let G be a group of order p^n and K a field. We discuss the structure of KG.

By Maschke's theorem $KG \simeq \sum A_i$, where $A_i \simeq [K]_{n_i} \otimes D_i$, D_i is a finite dimensional division algebra over K, and $[K]_{n_i}$ denotes the ring of $n_i \times n_i$ matrices over K.

If K is a perfect field, then $A_1 \simeq K$ and for $i \neq 1$, the center of D_i is isomorphic to $K(\chi_i) = K(\{\chi_i(g) \mid g \in G\})$, for some nonprincipal irreducible character χ_i of G, $K(\chi_i) \subset K(\zeta_{p^n})$. If T is any nonprincipal irreducible representation of G into the $m \times m$ matrices over an algebraically closed field F then $T(G)$ is a finite p-group and thus contains an element S of order p in its center. Since T is irreducible, this central element must be a scalar matrix of order p, that is, a scalar matrix with diagonal element ζp.

Let χ_T be the character associated with T. Then there is an element $g \in G$, such that $\chi_T(g) = m\zeta_p$. As (char $F, m) = 1$, we have $K(\zeta_p) \subset K(\chi_i) \subset K(\zeta_{p^n})$.

Suppose, first, that K is a prime subfield. If K is finite then D_i being a finite division ring must be the field $K(\chi_i)$, which if K is the rational field, by a theorem of Roquette [5], p. 249, again $D_i \simeq K(\chi_i)$.

Assume, now, that K is an arbitrary field with prime subfield F. $GF \simeq F \oplus \sum ([F]_{n_i} \otimes F(\chi_i))$ and $F(\zeta_p) \subset F(\chi_i) \subset F(\zeta_{p^n})$. Let $S_i = F(\chi_i) \cap K$ and $s_i = \deg [S_i/F]$.

Then

$$\begin{aligned} F(\chi_i) \otimes_F K &\simeq F(\chi_i) \otimes_F S_i \otimes_{S_i} K \\ &\simeq (\underbrace{F(\chi_i) \oplus \cdots \oplus F(\chi_i)}_{(s_i \text{ summands})}) \otimes_{S_i} K \quad \text{see, e.g. [3] p. 177} \\ &\simeq K(\chi_i) \oplus \cdots \oplus K(\chi_i) \quad \text{by Proposition 1.1} \end{aligned}$$

But,

$$\begin{aligned} KG &\simeq FG \otimes_F K \\ &\simeq (F \oplus \sum ([F]_{n_i} \otimes_F (F(\chi_i))) \otimes_F K \\ &\simeq K \oplus \sum ([F]_{n_i} \otimes_F (K(\chi_i) \oplus \cdots \oplus K(\chi_i))) \\ &\simeq K \oplus \sum ([K(\chi_i)]_{n_i} \oplus \cdots \oplus [K(\chi_i)]_{n_i}) \\ &\simeq K \oplus \sum s_i([K]_{n_i} \otimes_K K(\chi_i)) \,. \end{aligned}$$

Hence we have shown

LEMMA 1.2. *Let K be a field and G a group of order p^n. Then $KG \simeq K \oplus \sum B_i$ where $B_i \simeq [K]_{n_i} \otimes_K K_i$ and K_i are fields such that $K(\zeta_p) \subset K_i \subset K(\zeta_{p^n})$.*

THEOREM 1.3. *Let L be an extension field of the field K. Let G and H be groups of order p^n. Suppose $K(\zeta_{p^n})$ is linearly disjoint from $L(\zeta_p)$ over $K(\zeta_p)$. Then $KG \simeq KH$ if and only if $LG \simeq LH$.*

Proof. If $KG \simeq KH$, then $LG \simeq KG \otimes_K L \simeq KH \otimes_K L \simeq LH$.

Conversely, suppose $LG \simeq LH$.

From Lemma 1.2, $KG \simeq K \oplus \sum ([K]_{n_i} \otimes_K K_i)$, where K_i is a field such that $K(\zeta_p) \subset K_i \subset K(\zeta_{p^n})$. By Proposition 1.1, $K(\zeta_{p^n}) \cap L(\zeta_p) = K(\zeta_p)$. Let $R_i = L \cap K_i$. Then $R_i \subset (L(\zeta_p) \cap K(\zeta_{p^n})) \subset K(\zeta_p)$, so that $R_i = L \cap K(\zeta_p)$, i.e. R_i is independent of i. Write $R_i = R$ and $r = \dim [R/K]$.

$$\begin{aligned} K_i \otimes_K L &\simeq K_i \otimes_K R \otimes_R L \\ &\simeq (\underbrace{K_i \oplus \cdots \oplus K_i}_{(r \text{ summands})}) \otimes_R L \\ &\simeq LK_i \oplus \cdots \oplus LK_i \qquad \text{by Proposition 1.1} \\ &\simeq rLK_i \end{aligned}$$

Let $LK_i = L_i$ so that

$$L(\zeta_p) \subset L_i \subset L(\zeta_{p^n}) .$$

Then

$$\begin{aligned} LG &\simeq KG \otimes_K L \\ &\simeq (K \oplus \sum ([K]_{n_i} \otimes_K K_i)) \otimes_K L \\ &\simeq L \oplus \sum r([K]_{n_i} \otimes_K L_i) \\ &\simeq L \oplus \sum r([L_i]_{n_i}) \\ &\simeq L \oplus \sum r([L]_{n_i} \otimes_L L_i) . \end{aligned} \tag{*}$$

Pick s_i such that $K_i = K(\zeta_{p^{s_i}})$ and $1 \leqq s_i \leqq n$.
We clearly have

$$\deg [L(\zeta_{p^n})/L(\zeta_{p^{s_i}})] \leqq \deg [K(\zeta_{p^n})/K(\zeta_{p^{s_i}})]$$

and

$$\deg [L(\zeta_{p^{s_i}})/L(\zeta_p)] \leqq \deg [K(\zeta_{p^{s_i}})/K(\zeta_p)] .$$

But $L(_{p^n}) = LK(\zeta_{p^n})$ is a Galois extension of L, so that

$$\begin{aligned} \deg [L(\zeta_{p^n})/L(\zeta_p)] &= \deg [K(\zeta_{p^n})/(K(\zeta_{p^n}) \cap L(\zeta_p))] \\ &= \deg [K(\zeta_{p^n})/K(\zeta_p)] . \end{aligned}$$

Thus

$$\deg [L(\zeta_p n)/L(\zeta_{p^{s_i}})] = \deg [K(\zeta_{p^n})/K(\zeta_{p^{s_i}})] .$$

Since

$$\deg [L(\zeta_{p^n})/L(\zeta_{p^{s_i}})] = \deg [L_i K(\zeta_{p^n}))/L_i] = \deg [K(\zeta_{p^n})/(K(\zeta_{p^n} \cap L_i)] .$$

We must have

$$K(\zeta_{p^n}) \cap L_i = K(\zeta_{p^{s_i}}) = K_i .$$

This together with (*) shows that KG is determined by LG. The result follows.

If L is an extension field of the field K, we call A the maximal abelian p-extension of K in L if A is the composite of all finite abelian p-extensions (of degree a power of p) of K in L.

COROLLARY 1.4. *Let L be an extension field of the field K. Suppose A is the maximal abelian p-extension of K in L. Let G and H be groups of order p^n. Then $LG \simeq LH$ if and only if $AG \simeq AH$.*

Proof. $L \cap A(\zeta_{p^n}) \subset A(\zeta_p)$, and $(\deg [L(\zeta_p)/L], p) = 1$, so that

$L(\zeta_p) \cap A(\zeta_{p^n}) = A(\zeta_p)$. The conclusion now follows from Proposition 1.1 and the theorem.

COROLLARY 1.5. *Let L be an extension field of the field K. Suppose that K is algebraically closed in L. Let G and H be groups of order p^n. Then $KG \simeq KH$ if and only if $LG \simeq LH$.*

2. Let K be a field. The p-sequence $\{\gamma_p(n)\}$, $n = 0, 1, 2, \cdots$, of K is defined as $\gamma_p(n) = \deg [K(\zeta_{p^{n+2}})/K(\zeta_{p^{n+1}})]$. $\{\nu_p(n)\}$ is of one of the following three types, (see [8]).

$$\begin{gathered} p, p, p, \cdots \\ 1, 1, 1, \cdots 1, p, p, p, \cdots \\ 1, 1, 1, \cdots . \end{gathered}$$

Define the p-index of $K = 0$ if $\gamma_p(0) = p$

$$\begin{aligned} &n \text{ if } \gamma_p(n) = p \text{ and } \gamma_p(n-1) = 1 \\ &\infty \text{ if } \gamma_p(n) = 1 \text{ for all } n. \end{aligned}$$

In [8] the following proposition is proved.

PROPOSITION 2.1. *Let K and L be fields. Then K and L are equivalent on the class of all finite abelian p-groups if and only if the p-index of K equals the p-index of L.*

PROPOSITION 2.2. *Let K and L be fields of the same characteristic. Then K and L are equivalent on the class of all finite p-groups if and only if the p-index of K equals the p-index of L.*

Proof. Suppose the p-index of K equals the p-index of L. Let G and H be groups of order p^n. Let F be the prime subfield of K. If the p-index of $K = r < \infty$, let $T = F(\zeta_{p^{r+1}})$, while if the p-index of $K = \infty$, define $T = F(\zeta_p, \zeta_{p^2}, \zeta_{p^3}, \cdots)$. Then $T \subset K(\zeta_p)$ and the p-index of T equals the p-index of K.

$KG \simeq KH$ if and only if $K(\zeta_p)G \simeq K(\zeta_p)\ H$, by Theorem 1.3. Noting that $T(\zeta_{p^n}) \cap K(\zeta_p) = T(\zeta_p)$, we have, by Theorem 1.3, that $KG \simeq KH$ if and only if $TG \simeq TH$. But T depends only upon the characteristic and the p-index of K, and these invariants are indentical for L. Hence $LG \simeq LH$ if and only if $TG \simeq TH$, and the result follows.

The converse follows from Proposition 2.1.

In order to solve the equivalence problem of the introduction we must eliminate the requirement on the characteristic in Proposition 2.2.

For q a prime, let Q_q denote the field of q-adic numbers.

LEMMA 2.3. *Let $q \neq p$ be a prime, and F a finite extension of Q_q. Suppose R denotes the ring of integers of F. If G is a finite p-group and χ an irreducible character of G, then $R(\chi) =$ integers $F(\chi)$.*

Proof. Passman's proof of Lemma 1, [5], p. 562, immediately generalizes to this case when we substitute R for Z and F for Q.

PROPOSITION 2.4. *For q a prime, let F be a finite extension of Q_q. Let R be the ring of integers of F, and $\bar{R}$, the residue class field of F. Suppose G and H are finite groups of order s, with $(s, q) = 1$. Then the following are equivalent*

(i) $RG \simeq RH$

(ii) $FG \simeq FH$

(iii) $\bar{R}G \simeq \bar{R}H$

Proof. (i) $\Rightarrow$ (ii). If $RG \simeq RH$, then

$$FG \simeq RG \otimes_R F \simeq RH \otimes_R F \simeq FH$$

(ii) $\Rightarrow$ (iii).

F(G) determines the ordered pairs $\{f_i, F(\chi_i)\}$, where χ_i is an irreducible character, and $f_i = \deg \chi_i$. Also, $F(\chi_i) \subset F(\zeta_s)$. But F is of characteristic 0, so any absolutely irreducible representation of G can be realized in C, the complex numbers, and any character χ_i, has its values in $Z(\zeta_s)$.

Let Z_q denote the integers modulo q. $Z_q \subset \bar{R}$. As is well known, the characters $\bar{\chi}_i$ of $Z_q(G)$ are given by composition of χ_i with the mapping into the residue class field, which is a subfield of $\bar{R}(\zeta_s)$.

Let $\Pi \in R$ be such that $\operatorname{ord} \Pi = 1$. So π divides q. Then

$$G \xrightarrow{\chi_i} Z(\zeta_s) \longrightarrow \frac{Z(\zeta_s)}{\Pi R \cap Z(\zeta_s)} \simeq Z_q(\zeta_s) \subseteqq \bar{R}(\zeta_s) \quad \text{defines } \bar{\chi}_i .$$

Now $\deg \bar{\chi}_i = \deg \chi_i$ and by Lemma 2.3.

$$\frac{\operatorname{int}(F(\chi_i))}{(\Pi)} = \frac{R(\chi_i)}{(\Pi)} \simeq \bar{R}(\bar{\chi}) .$$

Since $(\operatorname{int} F(\chi_i))/(\Pi)$ is determined solely by FG, we have that the pairs $\{\deg \bar{\chi}_i, \bar{R}(\bar{\chi}_i)\}$ are determined by FG and in turn determine $\bar{R}G$.

Now the implication follows.

(iii) $\Rightarrow$ (i)

This implication is just a generalization of Sehgal's [6], Theorem 4, p. 504.

THEOREM 2.5. *Let K and L be fields. Then K and L are equivalent on the class of all finite p-groups if and only if the p-index of K equals the p-index of L.*

Proof. Suppose the p-index of K equals the p-index of L. Let S be the prime subfield of K.

Case (i) the p-index of $K = r < \infty$

Let $T = S(\zeta_{p^{r+1}})$. The p-index of K equals the p-index of T. By Proposition 2.2, K and T are equivalent on the class of all finite p-groups.

If K is of characteristic $q \neq 0$, then T is the residue class field of the local field $Q_q(\zeta_{p^{r+1}})$. By Proposition 2.4, $F = Q_q(\zeta_{p^{r+1}})$ is equivalent to T on the class of all finite p-groups. But adjoining a primitive p^nth root of unity to Q_q, gives a totally unramified extension of Q_q, so that the p-index of F equals the p-index of T.

If K is of characteristic 0 let $F = T$. No matter what the characteristic of K, we have associated to K a field F, of characteristic 0, of the same p-index as K, and equivalent to K on the class of all finite p-groups. In a similar fashion, associate to L a field F' of characteristic 0. By Proposition 2.2, we must have K and L equivalent on the class of all finite p-groups.

Case (ii). The p-index of $K = \infty$

Let G and H be groups of order p^n. $K(\zeta_p) \supset S(\zeta_{p^n})$

$$\begin{aligned} KG \simeq KH &\Longleftrightarrow K(\zeta_p)G \simeq K(\zeta_p)H \qquad \text{(by Theorem 1.3)} \\ &\Longleftrightarrow S(\zeta_{p^n})G \simeq S(\zeta_{p^n})H \qquad \text{(by Theorem 1.3)} \end{aligned}$$

If K is of characteristic 0, then

$$KG \simeq KH \text{ if and only if } Q(\zeta_{p^n})G \simeq Q(\zeta_{p^n})H\,.$$

Suppose K is of characteristic $q \neq 0$. Then $S(\zeta_{p^n})$ is the residue class field of the local field $Q_q(\zeta_{p^n})$. By Proposition 2.4, $S(\zeta_{p^n})G \simeq S(\zeta_{p^n})H$ if and only if $Q_q(\zeta_{p^n})G \simeq Q_q(\zeta_{p^n})H$. But $Q_q(\zeta_{p^n}) \supset Q(\zeta_{p^n})$, so that, by Theorem 1.3, $S(\zeta_{p^n})G \simeq S(\zeta_{p^n})H$ if and only if $Q(\zeta_{p^n})G \simeq Q(\zeta_{p^n})H$. No matter what characteristic K has, $KG \simeq KH$ if and only if $Q(\zeta_{p^n})G \simeq Q(\zeta_{p^n})H$. Since such a statement also holds for L, the result follows.

The converse is immediate by Proposition 2.2.

Let C_n denote a cyclic group of order n.

COROLLARY 2.6. *Let K be a field. Then K and Q are equivalent on the class of all finite p-groups if and only $K(C_{p^2}) \not\simeq K(C_p \oplus C_p)$.*

Proof. Assume K is equivalent to Q on all finite p-groups. As $Q(C_p \oplus C_p) \not\simeq Q(C_{p^2})$, then $K(C_p \oplus C_p) \not\simeq K(C_{p^2})$.

Conversely, suppose $K(C_p \oplus C_p) \not\simeq K(C_{p^2})$.

Let $\{\gamma_p(n)\} n = 0, 1, 2, \cdots$, be the p-sequence for K. If $\gamma_p(0) = 1$, then $\zeta_{p^2} \in K(\zeta_p)$, and by Lemma 1.2 $K(C_p \oplus C_p) \simeq K(C_{p^2}) \simeq K \oplus aK(\zeta_p)$ where a (deg $[K(\zeta_p)/K]) = (p^2 - 1)$. Thus $\gamma_p(0) = p$, and the p-index of K, like that of Q is 0. The result follows by Theorem 2.5.

Let $[K]_p$ denote the equivalence class of all fields F, such that the p-index of F equals the p-index of K. The equivalence classes consist of $[Q]_p = [Q(\zeta_p)]_p, [Q(\zeta_{p^2})]_p, [Q(\zeta_{p^3})]_p, \cdots$ and $[C]_p$. The class $[K]_p$, if $[K]_p \neq [C]_p$, contains an infinite number of prime subfields. For if the p-index of K is r, then by Dirichlet's theorem, there are an infinite number of primes q, such that $q \equiv (1 + p^{r+1})(\text{mod } p^{r+2})$. For any such prime q, $\zeta_{p^{r+1}} \in Z_q$, but $\zeta_{p^{r+2}} \notin Z_q$. If would be interesting to know if there is a prime q such that $[Z_q]_p = [Q]_p$ for all odd primes $p \neq q$. (When $q = 2$, for example, the first prime for which this fails is $p = 1093$.)

REFERENCES

1. N. Bourbaki, *Elements de Mathêmatique*, Fascicule XI chapitre 5, 1102, Hermann, Paris 1967.

2. C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience, New York, 1962.

3. N. Jacobson, *Structure of Rings*, American Mathematical Society, Vol. XXXVII, 1956.

4. D. Passman, *Isomorphic groups and group rings*, Pacific J. Math., **15** (1965), 561–583.

5. P. Roquette, *Realisierong von Darstellungen endlicher nilpotenter Gruppen*, Archiv der Math., **9** (1958), 241–250.

6. S. Sehgal, *Isomorphism of p-adic group rings*, J. Number Theory, **2** (1970), 500–508.

7. J.-P. Serre, *Corps Locaux*, Hermann, Paris 1968.

8. E. Spiegel, *On isomorphisms of Abelian group abgebras*, Canad J. Math., **XXVII** (1975), 155–161.

Received February 4, 1975, and in revised form May 23, 1975.

UNIVERSITY OF CONNECTICUT
AND
ATKINSON COLLEGE-YORK UNIVERSITY