PACIFIC JOURNAL OF MATHEMATICS
Vol. 66, No. 2, 1976

ON SEMI-SIMPLE GROUP ALGEBRAS II

EUGENE SPIEGEL AND ALLAN TROJAN

For F a field and G a group, let FG denote the group algebra of G over F. Let $\mathcal{G}$ be a class of finite groups. Call the fields F and $\bar{F}$ equivalent on $\mathcal{G}$ if for all $G, H \in \mathcal{G}$, $FG \simeq FH$ if and only if $\bar{F}G \simeq \bar{F}H$. In [9] we began a study of this equivalence relation, discussing the case when $\mathcal{G}$ consists of all finite p-groups, for p an odd prime. In this note we continue our study of the equivalence relation. Section one deals with some general results, section two solves the equivalence problem when $\mathcal{G}$ is the class of all finite 2-groups, and some remarks about the results are made in section three.

1. Throughout this paper we assume that all group algebras FG are semi-simple, that is, the characteristic of F is zero or does not divide the order of G. As usual, ζ_n denotes a primitive nth root of unity, Z_p is the field of p elements, and Q_p is the p-adic field.

Let G be a finite group of order n, and K a field. Then $KG \simeq \Sigma_i A_i$, with $A_i \simeq [K]_{u_i} \otimes D_i$, where D_i is a finite dimensional division algebra over K and $[K]_{u_i}$ represents the ring of $u_i \times u_i$ matrices over K. Call D_i the division algebra of A_i. If C_i is the center of D_i then $K \subset C_i \subset K(\zeta_n)$.

Let K_1G (K_2G) represent the sum of those A_i for which the division algebra is (is not) commutative. Then $KG \simeq K_1G \oplus K_2G$. If char $k \neq 0$, then $KG \simeq K_1G$.

THEOREM 1.1. *Let L be a field extension of the field K. Let G and H be groups of order n. Suppose that L is linearly disjoint from $K(\zeta_n)$ over K, and $KG \simeq K_1G$. 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 $LG \simeq LH$. Then $KG \simeq \Sigma_i [K]_{u_i} \otimes K_i$ where $K \subset K_i \subset K(\zeta_n)$. So

$$LG \simeq \left(\Sigma [K]_{u_i} \underset{K}{\otimes} K_i\right) \underset{K}{\otimes} L$$

$$\simeq \Sigma [K]_{u_i} \underset{K}{\otimes} \left(K_i \underset{K}{\otimes} L\right)$$

$$\simeq \Sigma [K]_{u_i} \underset{K}{\otimes} K_iL \quad \text{since } K_i \text{ and } L \text{ are linearly disjoint.}$$

$$\simeq \Sigma [L]_{u_i} \underset{L}{\otimes} L_i \quad \text{where } L_i = K_iL.$$

This shows that the numbers u_i are determined by LG. Also $L_i \cap K(\zeta_n) = LK_i \cap K(\zeta_n) = K_i$ by linear disjointness. So each L_i determines a K_i. Thus LG determines KG. This proves the converse.

COROLLARY 1.2. *If the field K is algebraically closed in the extension field L, and* $KG \simeq K_1G$, *then* $KG \simeq KH$ *if and only if* $LG \simeq LH$.

The next two results apply to the case where $KG \not\simeq K_1G$.

THEOREM 1.3. *Let* L/K *be a field extension of degree* $r \neq \infty$. *Let* G, H *be groups of order n. Assume that* $(r, n) = 1$ *and L is linearly disjoint from* $K(\zeta_n)$ *over K. Then* $KG \simeq KH$ *if and only if* $LG \simeq LH$.

Proof. Suppose $LG \simeq LH$. As before, we show that LG determines KG. Let $KG \simeq \Sigma A_i$, where the A_i are simple algebras. Then $LG \simeq \Sigma \bar{A}_i$, where $\bar{A}_i \simeq A_i \otimes_K L$. Each $\bar{A}_i$ is also a simple algebra. For example, let $A = A_1 \simeq [D]_u$, where D is the division algebra of A. Let C be the center of D. Then $K \subset C \subset K(\zeta_n)$, and so, by linear disjointness, $A \otimes_K L \simeq [D]_u \otimes_C C \otimes_K L \simeq [D]_u \otimes_C CL \simeq [D \otimes_C CL]_u$, and $[CL: C] = [L: K] = r$ is relatively prime to the index of D, $(\operatorname{ind} D)$. Consequently, $D \otimes_C CL$ is also a division algebra. (Corollary, Theorem 20, p. 60, **[1]**.) It is the division algebra of the simple algebra $A \otimes_K L$, and its center is CL. So what is necessary is to check that $A \otimes_K L$ determines A uniquely, that is, $D \otimes_C CL$ determines D. But the center C of D is uniquely determined by $CL \cap K(\zeta_n) = C$. Now suppose $D \otimes_K L = D' \otimes_K L$ for some second division algebra, D', whose center also is C. Let D^{-1} be the inverse of D in the Brauer group. Then, for some integers l and v:

$$[CL]_l \simeq [C]_l \otimes L \simeq D^{-1} \underset{C}{\otimes} D \underset{K}{\otimes} L \simeq D^{-1} \underset{C}{\otimes} D' \underset{K}{\otimes} L \simeq [D'']_v \underset{K}{\otimes} L$$
$$\simeq \left[D'' \underset{C}{\otimes} CL\right]_v$$

where D'' is a division algebra whose center, again, is C. So CL splits D''. But $(r, \operatorname{ind} D'') = 1$ because $\operatorname{ind} D''$ divides $(\operatorname{ind} D)^2$. So $D'' \simeq C$, so that D^{-1} is the inverse of D', that is, $D = D'$.

THEOREM 1.4. *Suppose L is a purely transcendental extension of the field K. Then* $KG \simeq KH$ *if and only if* $LG \simeq LH$.

Proof. We show once again that LG determines KG.

Case i. $L = K(x)$, x transcendental.

Again, $KG \simeq \Sigma [D_i]_{u_i}$, D_i a division algebra with center $C_i \supset K$. And again we examine a particular $D_i = D$, ($C_i = C$, $u_i = u$). Then $L \otimes_K D \simeq L \otimes_K C \otimes_C D \simeq LC \otimes_C D$ is simple. (68.1 of **[5]**.) So there is an integer, t, and a division algebra, E, such that $L \otimes_K D \simeq [E]_t$. If $t \neq 1$, $L \otimes_K D$ must have zero-divisors. Suppose $\alpha, \beta \in L \otimes_K D$ with $\alpha \cdot \beta = 0$. Then $\alpha = \Sigma r_i(x) \otimes a_i$, $\beta = \Sigma s_i(x) \otimes b_i$, where $r_i(x), s_i(x) \in L$ and $a_i, b_i \in D$. Multiplying by a suitable $p(x) \otimes 1 \in L \otimes D$ we can assume that $r_i(x), s_i(x)$ are polynomials in x. We then obtain an equation of the form $0 = (\Sigma c_i x^i) \cdot (\Sigma d_i x^i)$ with $c_i, d_i \in D$. Obviously either $\alpha = 0$ or $\beta = 0$. So $t = 1$ and $L \otimes D = E$ is also a division algebra. And E determines D. For suppose $L \otimes_K D \simeq L \otimes_K D'$. Then, as in the previous proof, there exist integers u, v such that:

$$[LC]_u \simeq \left[L \underset{K}{\otimes} C\right]_u \simeq L \underset{K}{\otimes} [C]_u \simeq L \underset{K}{\otimes} D \underset{C}{\otimes} D^{-1} \simeq L \underset{K}{\otimes} D' \underset{C}{\otimes} D^{-1}$$

$$\simeq L \underset{K}{\otimes} [D'']_v \simeq \left[L \underset{K}{\otimes} D''\right]_v$$

for some division algebra D'' with center C. But since $L \otimes_K D''$ is a division algebra, $v = u$ and $L \otimes_K D'' \simeq LC$. Thus $D'' = C$ and so $D^{-1} = (D')^{-1}$, i.e. $D = D'$.

Case ii. L has finite transcendence degree over K.

The result follows immediately from i by induction.

Case iii. I is an index set and $L = K\{x_i \mid i \in I\}$.

Let $G = \{g_1, \cdots, g_n\}$, $H = \{h_1, \cdots, h_n\}$ and suppose $\psi: LG \to LH$ is an L-algebra onto isomorphism. Write $\psi(g_i) = \Sigma_{j=1}^n \alpha_{ij} h_j$, $i = 1, \cdots, n$ and $\alpha_{ij} \in L$. Then each α_{ij} is the quotient of two polynomials with coefficients in K, each involving only a finite number of the indeterminates $\{x_i \mid i \in I\}$. Let B be the set of all indeterminates which appear in any of the α_{ij}, $1 \leqq i, j \leqq n$. Then $|B| < \infty$. Also $\psi(g_i) \in K(B)H$, $i = 1, \cdots, n$. And $\psi: K(B)G \to K(B)H$. But ψ is a $K(B)$ isomorphism of the finite dimensional vector space $K(B)G$ into $K(B)H$. So it is onto. So $LG \simeq LH$ implies $K(B)G \simeq K(B)H$. Since $K(B)$ is a purely transcendental extension of K, of finite transcendence degree, the result follows by Case ii.

2. Let K be a field. Let $\gamma_K(n) = \deg(K(\zeta_{2^{n+2}})/K(\zeta_{2^{n+1}}))$. We call $\{\gamma_K(n)\}$ $n = 1, 2, \cdots$ the 2-sequence of K. This sequence has one of the following forms:

$1, 1, 1, \cdots$
$1, 1, 1, \cdots, 1, 2, 2, \cdots$
$2, 2, 2, \cdots$.

Define:

$$\operatorname{ind}_2 K = \begin{cases} 1 \text{ if } \gamma_K(1) = 2 \\ n \text{ if } \gamma_K(n) = 2, \ \gamma_K(n-1) = 1, \ n \geqq 2 \\ \infty \text{ if } \gamma_K(n) = 1, \ n = 1, 2, 3, \cdots \end{cases}$$

$$t(K) = \begin{cases} 1 \text{ if } X^2 + Y^2 = -1 \text{ is solvable in } K \\ 0 \text{ if } X^2 + Y^2 = -1 \text{ is not solvable in } K. \end{cases}$$

$$O(K) = \begin{cases} 1 \text{ if } X^2 + 1 = 0 \text{ is solvable in } K \\ 0 \text{ if } X^2 + 1 = 0 \text{ is not solvable in } K. \end{cases}$$

We call $\operatorname{ind}_2(K)$, $t(K)$ and $O(K)$ the 2-invariants of K. In **[8]** the following proposition was proven:

PROPOSITION 2.1. *Let K, L be fields. Then K and L are equivalents on the class of all finite abelian 2-groups if and only if $O(K) = O(L)$ and* $\operatorname{ind}_2(K) = \operatorname{ind}_2(L)$.

This result is generalized here to all finite 2-groups.

LEMMA 2.2. *Let p be an odd prime. Then the equation $X^2 + Y^2 = -1$ is solvable in Z_p and in Q_p.*

Proof. Any homogeneous polynomial equation of degree 2 in 3 variables has a nontrivial solution over a finite field, $X^2 + Y^2 + Z^2 = 0$ in particular. This leads to a solution of $X^2 + Y^2 = -1$. Let $a, b \in Z_p$ satisfy $a^2 + b^2 = -1$. Regarding a as an integer in Q_p, the equation $Y^2 = -1 - a^2$ is solvable in Z_p and hence in Q_p. This yields a solution of $X^2 + Y^2 = -1$ in Q_p.

LEMMA 2.3. *Let F be a field of characteristic 0. Let a, b be elements transcendental over F such that $a^2 + b^2 = -1$. Then the algebraic closure of F in $F(a, b)$ is F.*

Proof. $\deg(F(a, b)/F(a)) = 2$. So if $\alpha \in F(a, b)$ and α is algebraic over F then $\deg(F(\alpha)/F) \leqq 2$. Suppose $\alpha \notin F$ and $\alpha = \sqrt{d}$, $d \in F$. Then $F(a, b) = F(a, \sqrt{d})$. So $b = p(a) + q(a)\sqrt{d}$ for some $p(a), q(a) \in F(a)$. $-1 - a^2 = p^2(a) + q^2(a)d + 2p(a)q(a)\sqrt{d}$. Thus $p(a) = 0$ or $q(a) = 0$. If $q(a) = 0$, then $b \in F(a)$, which is impossible. So $b = q(a)\sqrt{d}$. Write $q(a) = q_1(a)/q_2(a)$ where $q_1(a), q_2(a) \in F[a]$. Now $(-1)(1 + a^2) = d(q_1(a))^2/(q_2(a))^2$. But $1 + a^2$ is either irreducible in $F[a]$ or the product of two primes, while the prime factorization of $(q_1(a))^2/(q_2(a))^2$ involves only squares of primes. This contradicts the assumption that $\alpha \not\in F$.

If $n \geqq 2$ is a positive integer, the field $Q(\zeta_{2^n})$ contains a unique cyclic, real extension of Q, of degree 2^{n-2}. Call this field R_n. Then $R_2 \subset R_3 \subset R_4 \subset \cdots$.

THEOREM 2.4. *Let K, L be fields. Then K and L are equivalent on the class of all finite 2-groups if and only if $t(K) = t(L)$, $O(K) = O(L)$, $\mathrm{ind}_2(K) = \mathrm{ind}_2(L)$.*

Proof. Let $\mathcal{H}$ be the classical quaternion algebra of Hamilton over Q. Let F be a field extension of Q. Then F splits $\mathcal{H}$ if and only if $t(F) = 1$. ([3], problem 12, page 149.) Suppose K and L are equivalent on the class of all finite 2-groups. By Proposition 2.1, $O(K) = O(L)$ and $\mathrm{ind}_2(K) = \mathrm{ind}_2(L)$. Let G be the quaternion group of order 8 and H the dihedral group of order 8. Then $QG \simeq Q \oplus Q \oplus Q \oplus Q \oplus \mathcal{H}$ and $QH \simeq Q \oplus Q \oplus Q \oplus Q \oplus [Q]_2$. (This can be deduced, for example, from the examples on page 339 of [5], plus the fact that the characters of G and H are all real.) So $KG \not\simeq KH$ if and only if $\mathcal{H}$ does not split over K, i.e. $t(K) = 0$.

Conversely, suppose $t(K) = t(L)$, $O(K) = O(L)$, $\mathrm{ind}_2(K) = \mathrm{ind}_2(L)$.

Case i. $t(K) = t(L) = 0$.

Then $O(K) = O(L) = 0$. By Lemma 2.2 $\mathrm{char}\, K = \mathrm{char}\, L = 0$. Assume first that $\mathrm{ind}_2 K = n < \infty$. Then $R_{n+1} \subset K$, $R_{n+1} \subset L$, and the 2-invariants of R_{n+1} and K agree. It is sufficient to show that R_{n+1} and K are equivalent on the class of all finite 2-groups. Let G be a group of order 2^r. Write $R_{n+1}G \simeq R_{n+1,1}G \oplus R_{n+1,2}G$ and $KG \simeq K_1G \oplus K_2G$ as in §1. But the only division algebra that can occur at a simple component of KG (or $R_{n+1}G$) is $\mathcal{H} \otimes_Q K$ (or $\mathcal{H} \otimes_Q R_{n+1}$). ([7].) So K_2G determines $R_{n+1,2}G$. As in the proof of Theorem 1.1, K_1G determines $R_{n+1,1}G$. So KG determines LG.

If $\mathrm{ind}_2 K = \infty$, and $|G| = |H| = 2^r$, then $R_r \subset K$ and $R_r \subset L$, so that by an argument similar to the previous, $KG \simeq KH$ if and only if $R_rG \simeq R_rH$ if and only if $LG \simeq LH$.

Case ii. $t(K) = t(L) = 1$ and $\mathrm{char}\, K = \mathrm{char}\, L = 0$.

Now, if G is a 2-group, $KG \simeq K_1G$. Suppose $\mathrm{ind}_2(K) = n < \infty$. If $O(K) = 1$, then $Q(\zeta_{2^{n+1}}) \subset K$ and $Q(\zeta_{2^{n+1}}) \subset L$. The result follows by Theorem 1.1. If $O(K) = 0$, then $R_{n+1} \subset K$. Let a, b be transcendental over K, satisfying $a^2 + b^2 = -1$. Then K is algebraically closed in $K(a, b)$. By Corollary 1.2, K and $K(a, b)$ are equivalent on finite

2-groups. $R_{n+1}(a, b) \subset K(a, b)$. So by Proposition 1.1 of **[9]** $R_{n+1}(a, b, \zeta_{2^r})$ and $K(a, b)$ are linearly disjoint over $R_{n+1}(a, b)$, because $R_{n+1}(a, b, \zeta_{2^r}) \cap K(a, b) = R_{n+1}(a, b, \alpha)$ for some $\alpha \in Q(\zeta_{2^r})$, and by Lemma 2.3, $\alpha \in K$ and $R_{n+1}(a, b, \zeta_{2^r}) \cap K(a, b) = R_{n+1}(a, b)$. Therefore, by Theorem 1.1, $R_{n+1}(a, b)$ and $K(a, b)$ are equivalent on 2-groups. Similarly, let $\bar{a}, \bar{b}$ be transcendental over L, satisfying $\bar{a}^2 + \bar{b}^2 = -1$. Then $R_{n+1}(\bar{a}, \bar{b})$ and L are equivalent on all finite 2-groups. It is sufficient, therefore, to check that $R_{n+1}(a, b)$ and $R_{n+1}(\bar{a}, \bar{b})$ are equivalent on finite 2-groups. But $\psi: R_{n+1}(a, b) \to R_{n+1}(\bar{a}, \bar{b})$ given by $\psi(r) = r$ if $r \in R_{n+1}$, $\psi(a) = \bar{a}$, $\psi(b) = \bar{b}$ extends to an isomorphism of $R_{n+1}(a, b)G$ onto $R_{n+1}(\bar{a}, \bar{b})G$. If $\operatorname{ind}_2 K = \infty$, proceed as in Case i.

Case iii. $t(K) = t(L) = 1$, $\operatorname{char} K = p > 2$.

Suppose $\operatorname{ind}_2 K = n < \infty$. It is sufficient to show that there is a field $\bar{K}$ of characteristic 0 with the same 2-invariants as those of K, and which is equivalent to K on the class of all finite 2-groups. If $O(K) = 0$, let $T = Z_p$. If $O(K) = 1$, let $T = Z_p(\zeta_{p^{n+1}})$. In either case $T \subset K$, T and K have the same 2-invariants, and by Theorem 1.1 T and K are equivalent on finite 2-groups. Let $\bar{K}$ be a totally unramified extension of Q_p which has residue class field T. By Proposition 2.4 of **[9]** and Lemma 2.2, $\bar{K}$ and T have the same 2-invariants and are equivalent on the class of finite 2-groups. For $\operatorname{ind}_2 K = \infty$, we proceed again as in Case i.

COROLLARY 2.5. *Q and Q_2 are equivalent on the class of all finite 2-groups.*

Proof. By Eisenstein's criterion, the 2^r-th cyclotomic polynomial is irreducible over Q_2. Hence $\operatorname{ind}_2(Q_2) = \operatorname{ind}_2(Q)$. We must check $t(Q_2) = 0$.

If $X^2 + Y^2 = -1$ is solvable in Q_2, with X, Y 2-adic integers, then the equation $X^2 + Y^2 \equiv -1 \pmod 8$ is solvable, a contradiction. Otherwise, we can assume the solution of $X^2 + Y^2 = -1$ in Q_2 has the form $X = \alpha/2^r$ $y = \beta/2^r$ with $r > 0$, α and β 2-adic integers and $\alpha \equiv 1 \pmod 2$. Then $\alpha^2 + \beta^2 \equiv 0 \pmod 4$. This leads to a solution of $Z^2 \equiv -1 \pmod 4$, a contradiction.

3. (i) The hypotheses of Theorem 1.3 are all necessary. The two non-abelian groups of order 8 suffice to check this.

(ii) In Theorem 1.4 we cannot just assume that K is algebraically closed in L. For if $K = Q$, $L = Q(a, b)$, with a, b transcendental over Q and $a^2 + b^2 = -1$, by Theorem 2.4, K and L are not equivalent on 2-groups.

(iii) If K is an algebraic number field, by the results in **[6]** we can say exactly when $X^2 + Y^2 = -1$ is solvable in K.

(iv) In **[9]** we asked whether there is a prime field Z_q that is equivalent to Q on the class of all p-groups, for p odd. This says that $q^{p-1} \not\equiv 1 \bmod p^2$ for all $p \neq q$. Such primes q are studied in relation to the Fermat problem, and numerical indications can be found in **[4]**.

REFERENCES

1. A. A. Albert, *Structure of Algebras*, Amer. Math. Soc. Colloquium Publications, Vol. 24, Providence, R.I., 1961.
2. Benard, *Quaternion Constituents of Group Algebras*, Proceedings, Amer. Math. Soc., **30** (1971), 217–219.
3. Bourbaki, *Eléments de Mathématique*, Fascicule 23.
4. Brillhard, Jonascia and Weinberger, *On the Fermat Quotient, in Computers in Number Theory*, 1971, Academic Press, Atkin and Birch editors, p. 213–222.
5. C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience, New York, 1962.
6. Fein, Gordon and Smith, *On the Representations of* -1 *as a Sum of Two Squares in an Algebraic Number Field*, Number Theory, **3** (1971), 310–315.
7. Roquette, *Realisierung von Darstellungen Endlicher Nilpotenter Gruppen*, Archiv der Math., **9** (1958), 241–250.
8. Spiegel, *On Isomorphisms of Abelian Group Algebras*, Canad. J. Math., **27** (1975), 155–161.
9. Spiegel and Trojan, *On Semi-Simple Group Algebras I*, Pacific J. Math., **59** (1975), 549–555.

Received July 22, 1975

THE UNIVERSITY OF CONNECTICUT
AND
ATKINSON COLLEGE