Can. J. Math., Vol. XXVII, No. 1, 1975, pp. 155–161

ON ISOMORPHISMS OF ABELIAN GROUP ALGEBRAS

EUGENE SPIEGEL

For F a field and G a group, let $FG = F(G)$ be the group algebra of G over F. If $\mathscr{S}$ is a class of finite abelian groups, F induces an equivalence relation on $\mathscr{S}$ by $G, H \in \mathscr{S}$ are equivalent if and only if $FG \simeq FH$. We will call two fields F and K equivalent on $\mathscr{S}$ if they induce the same equivalence relation on $\mathscr{S}$. We will say F is equivalent to isomorphism on $\mathscr{S}$ if $FG \simeq FH$ if and only if $G \simeq H$ for any two elements $G, H \in \mathscr{S}$.

It is well known, (e.g. [**2**]) that the field of rational numbers Q is equivalent to isomorphism on the class of all finite abelian groups. In this note, we investigate when two fields F and K are equivalent on $\mathscr{S}$, for various sets $\mathscr{S}$. In particular, we identify which fields are equivalent to isomorphism on the class of all finite abelian groups.

If n is a positive integer, let C_n denote the cyclic group of order n.

LEMMA 1. *Let F be a field. Suppose G and H are finite abelian groups of order n, $n = p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r}$, where the p_i are distinct primes $i = 1, \ldots, r$. Let G_{p_i} (H_{p_i}) denote the p_i-Sylow subgroup of $G(H)$ respectively. Then $FG \simeq FH \Leftrightarrow FG_{p_i} \simeq FH_{p_i}$, $i = 1, \ldots, r$.*

Proof. If the characteristic of F is relatively prime to n, the lemma is a result of Perlis-Walker [**2**]. If the characteristic of F is p_1, $FG \simeq FH \Rightarrow F(G/G_{p_1}) \simeq F(H/H_{p_1})$ and $G_{p_1} \simeq H_{p_1}$ by the results in [**1**]. As $|G/G_{p_1}|$ is relatively prime to the characteristic of F, the lemma follows by Perlis-Walker's theorem.

This lemma shows that to study the equivalence of two fields F and K on the class of all finite abelian groups, it is sufficient to restrict our study to the class of all finite abelian p-groups. We will always suppose that p denotes a fixed prime. If F is a field of characteristic p, and $\mathscr{S}$ is the class of all finite abelian p-groups, then F is equivalent to isomorphism on $\mathscr{S}$. Hence in the following we will always assume that all fields are of characteristic other than the fixed prime p.

If F is a field, define the p-sequence $\{\gamma_{F,p}(n)\}$ of $F(n \geqq 1)$ by

$$\gamma_{F,p}(n) = \deg\ (F(\zeta_{p^{n+1}})/F(\zeta_{p^n}))$$

where ζ_{p^n} is a primitive p^nth root of unity over F.

Received July 27, 1973 and in revised form, October 1, 1973.

https://doi.org/10.4153/CJM-1975-020-x Published online by Cambridge University Press

PROPOSITION 2. *Let F be a field. The p-sequence of F has one of the following forms*

$$1, 1, 1, \ldots$$
$$1, 1, \ldots, 1, p, p, \ldots \qquad (p \text{ odd})$$
$$p, p, p, \ldots$$

while if $p = 2$, there is arbitrary choice of 1 or p in the first component.

Proof. Suppose K is a field containing a primitive p^nth ($n \geqq 1$) root of unity and not containing a p^{n+1}st root of unity. Let $\zeta_{p^{n+2}}$ be a primitive p^{n+2} root of unity for K, and let $(\zeta_{p^{n+2}})^p = \alpha_1$ and $\alpha_1^p = \alpha_2, \alpha_2 \in K$. Then α_1 is a primitive p^{n+1} root of unity and α_2 is a primitive p^n root of unity. Assume $\zeta_{p^{n+2}} \in K[\alpha_1]$. Then $x^p - \alpha_2 = f(x)$ is irreducible in $K[x]$, and $g(x) = x^{p^2} - \alpha_2$ can be factored in $K[x]$ into the product of p irreducible polynomials $g_1(x), \ldots, g_p(x)$ each of degree p.

Suppose $g_1(\zeta_{p^{n+2}}) = 0$ and let $\zeta_{p^{n+2}} = \lambda_1, \lambda_2, \ldots \lambda_p$ be the roots of $g_1(x)$. If $h(x) = \prod_{i=1}^p (x - \lambda_i^p)$, $h(x) \in K[x]$ since the coefficients of $h(x)$ are symmetric functions of $\lambda_1^p, \lambda_2^p, \ldots, \lambda_p^p$ and can be expressed as polynomials in the coefficients of $g_1(x)$.

Let the constant term of $g_1(x)$ be $(-1)^p c = \lambda_1\lambda_2 \ldots \lambda_p$. Then the constant term of $h(x)$ is $(-1)^p c^p = \lambda_1^p\lambda_2^p \ldots \lambda_p^p$. But $h(x)$ is a monic polynomial of degree p which is satisfied by $\lambda_1^p = \alpha_2$, and so must coincide with the minimal polynomial for α_2; i.e., $h(x) = x^p - \alpha_2 = f(x)$. In particular, $-\alpha_2 = (-1)^p c^p$.

If p is odd, $c^p = \alpha_2$, and c is a root of $f(x)$. This contradicts the irreducibility of $f(x)$.

If $p = 2$, and $n > 1$, then α_2 is a primitive 2^nth root of unity if and only if $-\alpha_2$ is a primitive 2^nth root of unity. Thus $x^p + \alpha_2 = \bar{f}(x)$ is also irreducible over $K[x]$. But $-\alpha_2 = c^p$ and c is a root of $\bar{f}(x)$, contradicting our assumption. We thus conclude that if p is odd or if $n > 1$ and $p = 2$, whenever p appears in the p-sequence of K all remaining terms must also be p.

PROPOSITION 3. *Let K/F be an extension of fields. Let M be the maximal abelian extension of F in K. Then the p-sequence of K equals the p-sequence of M.*

Proof. Let ζ_n be a primitive nth root of unity over F. $F(\zeta_n)$ and M are abelian extensions of F, so the composite $M(\zeta_n)$ is an abelian extension of F. $M \subset (K \cap M(\zeta_n))$. But $K \cap M(\zeta_n)$ is an abelian extension of F contained in K. Hence $K \cap M(\zeta_n) = M$. $M(\zeta_n)$ is Galois over M, so that $K(\zeta_n)$ is Galois over K with Galois group isomorphic to the Galois group of $M(\zeta_n)/M$. In particular, if $n = p^r$, deg $(M(\zeta_{p^r})/M) =$ deg $(K(\zeta_{p^r})/K)$, so K and M have the same p-sequences.

Let K/F be an extension of fields. Call M_p the maximal abelian p-extension of F in K if M_p is the composite of all finite abelian p-extensions of F in K.

PROPOSITION 4. *Let K/L be an extension of fields. Let M_p be the maximal* *abelian p-extension of L in K. Then the p-sequence for M_p equals the p-sequence for K.*

Proof. Let M be the maximal abelian extension of L in K, and M_p the maximal abelian p-extension of L in K. If $\alpha \in M(\zeta_p)$, $(\deg (M_p(\zeta_p)(\alpha)/M_p(\zeta_p)), p) = 1$. Let n be a positive integer. The $\deg(M_p(\zeta_{p^n})/M_p(\zeta_p))$ is a power of p, so that $M(\zeta_p) \cap M_p(\zeta_{p^n}) = M_p(\zeta_p)$. Hence $\deg (M(\zeta_{p^n})/M(\zeta_p)) = \deg (M_p(\zeta_{p^n})/M_p(\zeta_p))$. This means that the p-sequence of M_p is equal to that of M. By Proposition 3, the result follows.

COROLLARY 5. *Let K/L be a finite extension of fields of degree n. Suppose $(p, n) = 1$. Then the p-sequences of K and of L coincide.*

We now investigate the relationship between the equivalence of two fields on the set of abelian p-groups and their respective p-sequences.

THEOREM 6. *Suppose K and F are fields. If K and F have the same p-sequences, then they are equivalent on the class of all finite abelian p-groups. If, however, the p-sequences differ first at the nth place, then there exist abelian groups of order p^{n+1} (p^{n+2}, if $p = 2$) which are equivalent over one field but not the other.*

Proof. If L is a field and G is an abelian group of order p^s, then

$$L(G) \simeq \sum_{i=1}^{n} a_i L(\zeta_{p^i}),$$

where $a_i = n_i/v_i$, n_i is the number of elements of G of order p^i and $v_i = \deg(L(\zeta_{p^i})/L)$.

Define the sequence $\alpha_1, \alpha_2, \ldots$ as follows. $\alpha_1 = 1$. If α_n is defined, define α_{n+1} to be the least integer r such that $v_r > v_{\alpha_n}$, if this is possible; otherwise, let $\alpha_{n+1} = \alpha_{n+2} = \ldots = \infty$.

For the group G, we can define the sequence

$$b_i = \sum_{j=\alpha_i}^{\alpha_{i+1}-1} a_j$$

where $a_r = 0$ if $r > n$ and $b_i = 0$ if $\alpha_i = \infty$. Then

$$L(G) \simeq \sum_{i=1}^{n} b_i L(\zeta_{p^{\alpha_i}}).$$

If $\alpha_i < \alpha_j < \infty$, $L(\zeta_{p^{\alpha_i}}) \not\simeq L(\zeta_{p^{\alpha_j}})$ since the fields contain different collections of pth roots of unity. Thus b_i is characterized as the number of maximal ideals such that the quotient is isomorphic to $L(\zeta_{p^{\alpha_i}})$. If we similarly define a sequence of b's for $L(H)$, say $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n$, such that $L(H) \simeq \sum_{i=1}^n \bar{b}_i L(\zeta_{p^{\alpha_i}})$, then $L(G) \simeq L(H)$ if and only if $b_i = \bar{b}_i$, $i = 1, \ldots, n$. Recalling the definition of the b's, this says that the number of elements in G and H of order at most p^{α_i}, $i = 1, 2, \ldots, n$, are equal.

https://doi.org/10.4153/CJM-1975-020-x Published online by Cambridge University Press

Let

$$v_F(s) = \deg(F(\zeta_{p^s})/F), \qquad s = 1, 2, \ldots$$
$$v_k(s) = \deg(K(\zeta_{p^s})/K), \qquad s = 1, 2, \ldots$$

For $s = 2, 3, \ldots n$,

$$v_F(s) = v_F(1) \prod_{i=1}^{s-1} \gamma_{F,p}(i)$$

$$v_K(s) = v_K(1) \prod_{i=1}^{s} \gamma_{K,p}(i).$$

Let $\lambda = v_K(1)/v_F(1)$, so that $v_K(s) = \lambda v_F(s)$, $s = 1, 2, \ldots, n$. Let G and H be abelian groups of order at most p^n and suppose $FG \simeq FH$.

$$FG \simeq \sum_{i=1}^{n} a_i F(\zeta_{p^i}) \simeq FH \simeq \sum \bar{a}_i F(\zeta_{p^i})$$
$$KG \simeq \sum \lambda a_i K(\zeta_{p^i})$$
$$KH \simeq \sum \lambda \bar{a}_i K(\zeta_{p^i}).$$

But the b sequence for KG is just λ times the b sequence for FG, and similarly the b sequence for KH is just λ times the b sequence for FH, while $FG \simeq FH$ implies their b sequences are equal. Therefore $KG \simeq KH$.

If $\gamma_{F,p}(n) > \gamma_{K,p}(n)$, then $\gamma_{F,p}(n) = p$ and $\gamma_{K,p}(n) = 1$. Let

$$G \simeq C_{p^{n+1}}, \qquad H \simeq C_{p^n} \oplus C_p.$$

$KG \simeq KH$ since G and H have the same number of elements of order at most p^{n+1}, but $FG \not\simeq FH$ since G and H do not have the same number of elements of order at most p^n.

COROLLARY 7. *Let K be a field. Then K is equivalent to isomorphism on the set of all finite abelian p-groups if and only if $\gamma_{K,p}(n) = p$, $n = 1, 2, \ldots$.*

Proof. $\gamma_{Q,p}(n) = p$, $n = 1, 2, \ldots$. Now apply Theorem 6.

COROLLARY 8. *Let F be a field and suppose p is odd. Then F is equivalent to isomorphism on the class of all finite abelian p-groups if and only if $F(C_p \times C_p) \not\simeq F(C_{p^2})$.*

Proof. If $\zeta_{p^2} \in F(\zeta_p)$ and $v_p = \deg(F(\zeta_p)/F)$, then

$$F(C_p \times C_p) \simeq F \oplus \frac{p^2 - 1}{v_p} F(\zeta_p) \simeq F(C_{p^2}).$$

Thus $\gamma_{F,p}(1) = p$. By Proposition 2, $\gamma_{F,p}(n) = p$, $n = 1, 2, \ldots$ and by Corollary 7 the result follows.

COROLLARY 9. *Let Q_p be the field of p-adic numbers. Let G and H be abelian groups of order p^n. Then $Q_pG \simeq Q_pH \Leftrightarrow G \simeq H$.*

Proof. Let

$$\phi_{p^n}(x) = \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1}$$

be the p^nth cyclotomic polynomial. It is irreducible over Q_p, by Eisenstein's criterion. Hence $\gamma_{Q_p,p}(n) = p, n = 1, 2, \ldots$. By Corollary 7 the result follows.

We now apply the theorem to algebraic number fields. Suppose p is odd. Then $Q(\zeta_{p^2})$ is a cyclic extension of Q of degree $p(p-1)$ and contains a unique field of degree p over Q. Call this field F_p; i.e., $Q \subset F_p \subset Q(\zeta_{p^2})$ and $\deg(F_p/Q) = p$.

THEOREM 10. *Let p be an odd prime. Let $\mathscr{S}$ be the set of all finite abelian p-groups. Let K be an extension of Q.*

Then the following are equivalent.

(i) *K is equivalent to isomorphism on $\mathscr{S}$.*

(ii) $K(C_p \times C_p) \not\simeq K(C_{p^2})$

(iii) $F_p \not\subset K$

(iv) *There does not exist a field L such that L properly contains Q and is contained in K, L is an abelian extension of Q of degree a power of p, and the discriminant of L is a power of p.*

Proof. (i) $\Rightarrow$ (ii). This is obvious.

(ii) $\Rightarrow$ (iii). If $F_p \subset K$, then $K(\zeta_p) = K(\zeta_{p^2})$. Let $\alpha = \deg(K(\zeta_p)/K) = \deg(K(\zeta_{p^2})/K)$. Then

$$K(C_{p^2}) \simeq \frac{p(p-1)}{\alpha} K(\zeta_{p^2}) \simeq \frac{(p-1)}{\alpha} K(\zeta_p) \oplus K \simeq \frac{p^2 - 1}{\alpha} K(\zeta_p) \oplus K,$$

while

$$K(C_p \times C_p) \simeq \left(\frac{p^2 - 1}{\alpha}\right) K(\zeta_p) \oplus K.$$

Thus $K(C_{p^2}) \simeq K(C_p \times C_p)$.

(iii) $\Rightarrow$ (iv). Suppose such a field L exists and let $\deg(L/Q) = p^r$. As L is an abelian extension of Q of degree a power of p, by the Kronecker-Weber theorem, L is contained in a cyclotomic extension. In fact, since the discriminant of L is a power of p, $L \subset Q(\zeta_{p^{r+1}})$. See, e.g., [**3**, p. 233]. But $Q(\zeta_{p^{r+1}})$ is a cyclic extension of Q and contains a unique field L of degree p^r over Q. This field must also contain F_p, contradicting (iii).

(iv) $\Rightarrow$ (i). Let M_p be the maximal abelian p-extension of Q in K. By Proposition 4, the p-sequence of M_p equals the p-sequence of K. Let ζ_{p^n} be a primitive p^nth root of unity in Q. $Q(\zeta_{p^n}) \cap M_p$ is an extension of Q of degree a power of p, since M_p is, and has discriminant a power of p since it is contained in $Q(\zeta_{p^n})$. By (iv), we conclude that $Q(\zeta_{p^n}) \cap M_p = Q$. From Galois theory we have $\deg(M_p(\zeta_{p^n})/M_p) = \deg(Q(\zeta_{p^n})/Q)$ so that the p-sequence of M_p and of Q coincide. By Theorem 6 the result follows.

THEOREM 11. *Suppose $p = 2$. Let $\mathscr{S}$ be the set of all finite abelian 2-groups and let $\mathscr{T} = \{C_8 \oplus C_2, C_4 \oplus C_4, C_4 \oplus C_2 \oplus C_2\}$. Let K be an extension of Q. Then the following are equivalent.*

(i) *K is equivalent to isomorphism on $\mathscr{S}$.*

(ii) *K is equivalent to isomorphism on $\mathscr{T}$.*

(iii) $\{\sqrt{2}, i, \sqrt{-2}\} \cap K = \emptyset$.

Proof. (i) $\Rightarrow$ (ii). This is obvious.

(ii) $\Rightarrow$ (iii). If $i \in K$, $K(C_4 \oplus C_4) \simeq K(C_4 \oplus C_2 \oplus C_2)$. If $\sqrt{2}$ or $\sqrt{-2} \in K$, $K(C_8 \oplus C_2) \simeq K(C_4 \oplus C_4)$.

(iii) $\Rightarrow$ (i). Let M_2 be the maximal abelian 2-extension of Q in K. We must check that the 2-sequence of M_2 coincide with the 2-sequence of Q. Suppose $n \geqq 3$ and ζ_{2^n} is a primitive 2^nth root of unity over Q. $Q(\zeta_{2^n})$ is an abelian extension of Q and contains exactly three quadratic extensions; namely, $Q(i)$, $Q(\ /2)$, $Q(\sqrt{-2})$. By (iv),

$$\{i, \sqrt{2}, \sqrt{-2}\} \cap K = \{i, \sqrt{2}, \sqrt{-2}\} \cap M_2 = \emptyset,$$

so that $Q(\zeta_{2^n}) \cap M_2 = Q$. Then $\deg(M_2(\zeta_{2^n})/M_2) = \deg(Q(\zeta_{2^n})/Q)$ and the 2-sequences of K and Q coincide.

If q is a prime and n is a positive integer, let $GF(q^n)$ denote the finite field of order q^n.

THEOREM 12. *Suppose p is odd and K is a field of characteristic q ($q \neq 0$, $q \neq p$). Let e be the exponent of q modulo p. Then K is equivalent to isomorphism on all finite abelian p-groups if and only if $q^e \not\equiv 1$ (modulo p^2) and $GF(q^p) \not\subset K$.*

Proof. Suppose K is equivalent to isomorphism on all finite abelian p-groups. By Corollary 7, $\gamma_{K,p}(n) = p$, $n = 1, 2, \ldots$. Let ζ_p be a primitive pth root of unity for K, and let $\deg[GF(q)(\zeta_p)/GF(q)] = l$. The order of the multiplicative group of $GF(q)(\zeta_p)$ is $q^l - 1$, and it contains an element of order p. Thus $q^l \equiv 1$ (modulo p). But e is the smallest positive integer such that $q^e \equiv 1 \pmod p$, so that $l = e$. $\gamma_{K,p}(1) = p$ implies $\zeta_{p^2} \notin K[\zeta_p]$, so that $\zeta_{p^2} \notin GF(q)$; i.e., $q^e \not\equiv 1 \pmod{p^2}$.

$\zeta_{p^2} \notin K[\zeta_p]$, so that ζ_{p^2} is of degree p over $GF(q)(\zeta_p) = GF(q^e)$. Therefore, $GF(q)(\zeta_{p^2}) = GF(q^{pe})$. Since $1 \leqq e \leqq p - 1$ and $GF(q^{pe})$ is just the composite of $GF(q^e)$ and $GF(q^p)$, we conclude $GF(q^p) \not\subset K[\zeta_p]$. Hence $GF(q^p) \not\subset K$.

Conversely, since $p^e \not\equiv 1 \pmod{p^2}$, $\zeta_{p^2} \notin GF(q)(\zeta_p) = GF(q^e)$. If $\zeta_{p^2} \in K[\zeta_p]$, then $GF(q^p) \subset GF(q^{pe}) \subset K[\zeta_p]$. Let λ be a generator for the multiplicative group of $GF(q^p)$. Then λ satisfies an irreducible polynomial $f(x) \in GF(q)[x]$ of degree p, which remains irreducible in $K[x]$. But $(\deg(K(\zeta_p)/K), p)$

$= 1$, so $f(x)$ remains irreducible over $K(\zeta_p)[x]$; i.e., $\zeta_{p^2} \notin K[\zeta_p]$. Thus $\gamma_{K,p}(1) = p$. Since p is odd, by Proposition 2 we must have $\gamma_{K,p}(n) = p$, $n = 1, 2, \ldots$ so that the result follows by Corollary 7.

THEOREM 13. *Let q be an odd prime. If $q \equiv 1 \pmod 4$, then $K(C_4) \simeq K(C_2 \times C_2)$. If $q \equiv 3 \pmod 4$, then $K(C_8) \simeq K(C_4 \times C_2)$.*

Proof. If $q \equiv 1 \pmod 4$, then the equation $x^2 + 1 = 0$ splits in K, so that $\gamma_{K,p}(1) = 1$. Hence $K(C_4) \simeq K(C_2 \times C_2)$. If $q \equiv 3 \pmod 4$, then $GF(q^2) \subset K(\zeta_2)$. As $q^2 \equiv 1 \pmod 8$, $\zeta_2 \in GF(q^2)$. Thus $\gamma_{K,2}(1) = 2$ and $\gamma_{K,2}(2) = 1$. By Theorem 6,

$$K(C_8) \simeq K(C_4 \times C_2).$$

REFERENCES

1. W. May, *Commutative group algebras*, Trans. Amer. Math. Soc. *136* (1969), 139–149.
2. S. Perlis and G. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. *68* (1950), 420–426.
3. P. Ribenboim, *Algebraic numbers* (Wiley-Interscience, New York, 1972).
4. E. Spiegel, *Abelian p-adic group rings* (to appear in Comment. Math. Helv.).

University of Connecticut,
Storrs, Connecticut