The isomorphism problem for group algebras: A criterion

Taro Sakurai

Communicated by Britta Spaeth

Abstract. Let $R$ be a finite unital commutative ring. We introduce a new class of finite groups, which we call hereditary groups over $R$. Our main result states that if $G$ is a hereditary group over $R$, then a unital algebra isomorphism between group algebras $RG \cong RH$ implies a group isomorphism $G \cong H$ for every finite group $H$. As application, we study the modular isomorphism problem, which is the isomorphism problem for finite $p$-groups over $R = \mathbb{F}_p$, where $\mathbb{F}_p$ is the field of $p$ elements. We prove that a finite $p$-group $G$ is a hereditary group over $\mathbb{F}_p$ provided $G$ is abelian, $G$ is of class two and exponent $p$, or $G$ is of class two and exponent four. These yield new proofs for the theorems by Deskins and Passi–Sehgal.

Introduction

Let $R$ be a unital commutative ring (throughout this paper, we do not impose a ring (or algebra) to have 1, but we impose $0 \neq 1$ if it has 1) and $G$ a finite group. The structure of the group algebra $RG$ of $G$ over $R$ reflects the structure of the group $G$ to some extent. The isomorphism problem asks whether a group algebra $RG$ determines the group $G$. See a survey by Sandling [20] for a historical account for this problem. In what follows, $p$ stands for a prime number, and $\mathbb{F}_p$ denotes the field of $p$ elements. The only classic isomorphism problem that is still open for more than 60 years is the modular isomorphism problem.

Problem. Let $G$ and $H$ be finite $p$-groups. Does a unital algebra isomorphism $\mathbb{F}_pG \cong \mathbb{F}_pH$ imply a group isomorphism $G \cong H$?

Several positive solutions for special classes of $p$-groups are known; see lists in the introduction of [6] or [8].

In this paper, we introduce a new class of finite groups, which we call hereditary groups over a finite unital commutative ring $R$ (Definition 1.4). Our main result (Criterion 1.6) states that if $G$ is a hereditary group over $R$, then a unital algebra isomorphism $RG \cong RH$ implies a group isomorphism $G \cong H$ for every finite group $H$. The proof rests on counting homomorphisms (Lemma 1.2) and
adjoint (Lemma 1.3) – this indirect approach is novel in the sense that it does not involve normalized isomorphisms, for example. As application, we study the modular isomorphism problem. We prove that a finite $p$-group $G$ is a hereditary group over $\mathbb{F}_p$ provided $G$ is abelian (Lemma 3.2), $G$ is of class two and exponent $p$ (Lemma 3.5), or $G$ is of class two and exponent four (Lemma 3.10). These yield new proofs for the theorems by Deskins (Theorem 3.1) and Passi–Sehgal (Theorems 3.4 and 3.7) which are early theorems on the modular isomorphism problem.

1 Criterion

This section is devoted to proving our main result (Criterion 1.6). The first lemma is an easy application of the inclusion-exclusion principle.

**Lemma 1.1.** Let $G$ and $H$ be finite groups. We denote by $\text{Epi}(G, H)$ the set of all epimorphisms from $G$ to $H$. Let $\mathcal{K}$ be the set of all maximal subgroups of $H$. Then

$$|\text{Epi}(G, H)| = \sum_{\mathcal{K} \subseteq \mathcal{J}} (-1)^{|\mathcal{K}|} \left| \text{Hom}(G, \bigcap_{K \in \mathcal{K}} K) \right|.$$ 

**Proof.** First, note that

$$\text{Epi}(G, H) = \{ f : G \to H \mid \text{im} \ f = H \}$$

$$= \bigcap_{K \in \mathcal{K}} \{ f : G \to H \mid \text{im} \ f \leq K \}.$$ 

Thus, by letting $\text{Hom}^K(G, H) = \{ f : G \to H \mid \text{im} \ f \leq K \}$, it becomes

$$\text{Epi}(G, H) = \text{Hom}(G, H) - \bigcup_{K \in \mathcal{K}} \text{Hom}^K(G, H).$$

By the inclusion-exclusion principle, we have

$$|\text{Epi}(G, H)| = |\text{Hom}(G, H)| - \left| \bigcup_{K \in \mathcal{K}} \text{Hom}^K(G, H) \right|$$

$$= |\text{Hom}(G, H)| + \sum_{\emptyset \neq \mathcal{K} \subseteq \mathcal{J}} (-1)^{|\mathcal{K}|} \left| \bigcap_{K \in \mathcal{K}} \text{Hom}^K(G, H) \right|$$

$$= |\text{Hom}(G, H)| + \sum_{\emptyset \neq \mathcal{K} \subseteq \mathcal{J}} (-1)^{|\mathcal{K}|} \left| \text{Hom}(G, \bigcap_{K \in \mathcal{K}} K) \right|$$

$$= \sum_{\mathcal{K} \subseteq \mathcal{J}} (-1)^{|\mathcal{K}|} \left| \text{Hom}(G, \bigcap_{K \in \mathcal{K}} K) \right|.$$ 

(Note that if $\mathcal{K} = \emptyset$, then $\bigcap_{K \in \mathcal{K}} K = \{ h \in H \mid h \in K \ (K \in \mathcal{K}) \} = H$.) \qed
Lemma 1.2. Let $G$ and $H$ be finite groups. Then $G \cong H$ if and only if $|G| = |H|$ and

$$|\text{Hom}(G, K)| = |\text{Hom}(H, K)|$$

for every subgroup $K$ of $G$.

Proof. From $|\text{Hom}(G, K)| = |\text{Hom}(H, K)|$ for every subgroup $K$ of $G$, it follows that $|\text{Epi}(H, G)| = |\text{Epi}(G, G)| \geq 1$ by Lemma 1.1. Hence, we have an epimorphism from $H$ to $G$. It must be an isomorphism because $|G| = |H|$.

For a unital $R$-algebra $A$ over a unital commutative ring $R$, the unit group of $A$ is denoted by $A^*$. The following adjoint, which rephrases the universal property of group algebras [15, Proposition 3.2.7], is well-known.

Lemma 1.3. Let $R$ be a unital commutative ring, $G$ a group and $A$ a unital $R$-algebra. Then there is a bijection

$$\text{Hom}(RG, A) \cong \text{Hom}(G, A^*)$$

which is natural in $G$ and $A$. (Namely, the group algebra functor is left adjoint to the unit group functor.)

Proof. The restriction $(f : RG \to A) \mapsto (f |_G : G \to A^*)$ gives rise to the desired bijection; see [17, pp. 204–205, 490] for details.

Now we propose a definition of hereditary groups which is crucial in this study.

Definition 1.4. Set $M = \{ [G] \mid G$ is a finite group $\}$, where the symbol $[G]$ denotes the isomorphism class of a group $G$. It becomes a commutative monoid with an operation $[G] + [H] = [G \times H]$. Let $K(M)$ denote the Grothendieck group\(^1\) of $M$. As it is a $\mathbb{Z}$-module (abelian group), we can extend scalars and obtain a $\mathbb{Q}$-vector space $L(M) = \mathbb{Q} \otimes_{\mathbb{Z}} K(M)$. For a finite unital commutative ring $R$, define the $\mathbb{Q}$-subspace $S(R)$ of $L(M)$ by

$$S(R) = \sum_{\text{A is a finite unital } R\text{-algebra}} \mathbb{Q}[A^*].$$

Namely, $S(R)$ is the $\mathbb{Q}$-subspace of $L(M)$ spanned by the isomorphism classes of unit groups of finite unital $R$-algebras. We call a finite group $G$ a hereditary group over $R$ if $[K] \in S(R)$ for every subgroup $K$ of $G$.

\(^1\) This is also called the group completion of $M$. See [16, Theorem 1.1.3].
From the definition, being hereditary group is a subgroup-closed property. Note that the group completion $M \to K(M)$ is injective because $M$ is cancellative by the Krull–Schmidt theorem; the localization $K(M) \to L(M)$ is also injective because $K(M)$ is torsion-free. Thus, $M$ can be identified with a submonoid of $L(M)$.

**Example 1.5.** Let $C_q$ denote the cyclic group of order $q$. Then, from $\mathbb{F}_5^* \cong C_4$ and $(\mathbb{F}_5C_5)^* \cong C_4 \times (C_5)^4$, we have

$$[C_5] = \frac{1}{4}[(\mathbb{F}_5C_5)^*] - \frac{1}{4}[\mathbb{F}_5^*] \in S(\mathbb{F}_5).$$

In particular, $C_5$ is a hereditary group over $\mathbb{F}_5$.

The next criterion – our main result – shows that hereditary groups are determined by their group algebras.

**Criterion 1.6.** Let $G$ and $H$ be finite groups, and let $R$ be a finite unital commutative ring. Suppose $G$ is a hereditary group over $R$. If $RG \cong RH$, then $G \cong H$.

The proof is done by describing the number of group homomorphisms in terms of the number of unital algebra homomorphisms.

**Proof of Criterion 1.6.** Since a unital commutative ring $R$ has invariant basis number (IBN) property, we have $|G| = |H|$ from $RG \cong RH$. Hence, by Lemma 1.2, it suffices to prove that $|\text{Hom}(G, K)| = |\text{Hom}(H, K)|$ for every subgroup $K$ of $G$.

Since $G$ is a hereditary group over $R$, we have $[K] \in S(R)$. Therefore, there is a positive integer $n$ and finite unital $R$-algebras $A, B$ such that

$$[K] = \frac{1}{n}[A^*] - \frac{1}{n}[B^*].$$

Namely, $A^* \cong B^* \times K^n$. Hence,

$$|\text{Hom}(G, A^*)| = |\text{Hom}(G, B^* \times K^n)| = |\text{Hom}(G, B^*)| \times |\text{Hom}(G, K)|^n.$$

Thus, by Lemma 1.3, we can obtain

$$|\text{Hom}(G, K)| = \left(\frac{|\text{Hom}(G, A^*)|}{|\text{Hom}(G, B^*)|}\right)^{1/n} = \left(\frac{|\text{Hom}(RG, A)|}{|\text{Hom}(RG, B)|}\right)^{1/n}.$$

We can calculate $|\text{Hom}(H, K)|$ similarly and conclude that

$$|\text{Hom}(G, K)| = |\text{Hom}(H, K)|$$

from $RG \cong RH$. \qed
Remark 1.7. Studying a finite group that is a “linear combination” of unit groups, precisely an element of $S(R)$, is essential because even the cyclic group of order five cannot be realized as a unit group of any unital ring. (See a theorem by Davis and Occhipinti [4, Corollary 3], for example.) This is quite different from the fact that every finite abelian $p$-group is a hereditary group over $\mathbb{F}_p$ (Lemma 3.2).

It also should be noted that no examples of non-hereditary groups are hitherto found.

Using this criterion, we provide new proofs for some early theorems on the modular isomorphism problem in the last section.

2 Quasi-regular groups

We show that, with Criterion 1.6, study of quasi-regular groups can be used to study the isomorphism problem. Throughout this section, $R$ denotes a unital commutative ring.

Definition 2.1. Let $A$ be an $R$-algebra. Define the quasi-multiplication on $A$ by

$$x \circ y = x + y + xy.$$  

An element $x \in A$ is called quasi-regular if there is an element $y \in A$ such that $x \circ y = 0 = y \circ x$. We denote the set of all quasi-regular elements by $Q(A)$. It forms a group under the quasi-multiplication, and we call it the quasi-regular group of $A$. If $A = Q(A)$, then $A$ is called quasi-regular (or radical).

Quasi-multiplication is also called circle operation or adjoint operation. Accordingly, quasi-regular groups are also called circle groups or adjoint groups. As these terms have completely different meaning in other contexts, we avoid using them.

If an $R$-algebra $A$ has a multiplicative identity, then there is an isomorphism $Q(A) \rightarrow A^*$ that is defined by $x \mapsto 1 + x$. We study how quasi-regular groups are related to unit groups, especially when algebras do not have multiplicative identities, in the rest of this section.

Definition 2.2. Let $A$ be an $R$-algebra. We denote the unitization of $A$ by $A_{\text{un}}$: it is a direct product $A_{\text{un}} = A \times R$ as $R$-modules, and its multiplication is defined by

$$(x, r) \times (y, s) = (sx + ry + xy, rs).$$

Note that $(0, 1) \in A_{\text{un}}$ is the multiplicative identity. The unitization is also called the Dorroh extension, especially the case $R = \mathbb{Z}$.
Lemma 2.3. Let $A$ be a quasi-regular $R$-algebra. Then an element $(x, r) \in A_{un}$ is a unit if and only if $r \in R$ is a unit.

Proof. The “only if” part is trivial. Let us assume $r \in R^*$ to show $(x, r) \in A^*$. As $r^{-1} \in R$ exists and $r^{-1}x \in A$, there is an element $y \in A$ such that

$$(r^{-1}x) \circ y = 0 = y \circ (r^{-1}x)$$

because $A$ is quasi-regular. Then it can be shown that $(x, r)^{-1} = (r^{-1}y, r^{-1})$ by direct calculation. \qed

Lemma 2.4. Let $A$ be a quasi-regular $R$-algebra. Then $A^*_{un} \cong Q(A) \times R^*$. In particular, $[Q(A)] \in S(R)$ if $R$ and $A$ are finite.

Proof. Note that there are homomorphisms

$$Q(A) \leftarrow A^*_{un} \rightarrow R^*$$

$$r^{-1}x \leftarrow (x, r) \rightarrow r$$

which are well-defined by Lemma 2.3. It is straightforward to check that these satisfy the universal property of a direct product. \qed

Remark 2.5. For determining whether a finite group is a quasi-regular group of an $R$-algebra, a theorem by Sandling [18, Theorem 1.7] would be helpful. It should be noted that quasi-regular groups also have severely restricted structure as unit groups. See [19, p. 343].

3 Modular isomorphism problem

As application of Criterion 1.6, we provide new proofs for theorems by Deskins [5] and Passi–Sehgal [13] which are early theorems on the modular isomorphism problem.

3.1 Abelian (class at most one)

Let us state a well-known theorem by Deskins [5, Theorem 2].

Theorem 3.1 (Deskins). Let $G$ and $H$ be finite $p$-groups. Suppose $G$ is abelian. If $\mathbb{F}_p G \cong \mathbb{F}_p H$, then $G \cong H$.

To use our criterion, we need to prove the following, which is also useful to prove Theorems 3.4 and 3.7.
Lemma 3.2. Every finite abelian $p$-group is a hereditary group over $\mathbb{F}_p$.

Proof. Let $C_{p^n}$ be the cyclic $p$-group of order $p^n$. Since a finite abelian $p$-group is a direct product of finite cyclic $p$-groups and being finite cyclic $p$-group is a subgroup-closed property, it suffices to prove that $[C_{p^n}] \in S(\mathbb{F}_p)$. We prove it by induction on $n$.

Base case ($n = 0$). Clear by Definition 1.4.

Inductive case ($n > 0$). Let $\Delta(C_{p^n})$ denote the augmentation ideal of $\mathbb{F}_p C_{p^n}$. Then

$$[C_{p^n}] = \frac{1}{a_n} [V] - \sum_{i=1}^{n-1} \frac{a_i}{a_n} [C_{p^i}]$$

and we have $[C_{p^n}] \in S(\mathbb{F}_p)$ by induction. (This lemma can be also proved by appealing to the structure theorem of $(\mathbb{F}_p C_{p^n})^*$ by Janusz [9, Theorem 3.1].) \qed

With this lemma, we provide a new proof of the Deskins theorem.

Proof of Theorem 3.1. Since the finite abelian $p$-group $G$ is a hereditary group over $\mathbb{F}_p$ by Lemma 3.2, $\mathbb{F}_p G \cong \mathbb{F}_p H$ implies $G \cong H$ by Criterion 1.6. \qed

Remark 3.3. Besides the original proof by Deskins, an alternative simple proof is given by Coleman [3, Theorem 4]. Proofs can be found in monographs such as [10, Theorem 2.4.3], [14, Lemma 14.2.7], [22, (III.6.2)], [15, Theorem 9.6.1], or [23, Theorem 4.10] as well.

3.2 Class two and exponent $p$

The aim of this subsection is to provide a new proof of the following theorem by Passi and Sehgal [13, Corollary 13].

Theorem 3.4 (Passi–Sehgal). Let $G$ and $H$ be finite $p$-groups. Suppose $G$ is of class two and exponent $p$. If $\mathbb{F}_p G \cong \mathbb{F}_p H$, then $G \cong H$.

See also Remark 3.8. To use our criterion, we need to prove the following.
Lemma 3.5. Every finite $p$-group of class two and exponent $p$ is a hereditary group over $\mathbb{F}_p$.

A key ingredient for the proof is a slight modification of the theorem by Ault and Watters [1, 7].

Theorem 3.6 (Ault–Watters). Let $G$ be a finite $p$-group. Suppose $G$ is of class two and exponent $p$. Then there is a finite quasi-regular $\mathbb{F}_p$-algebra $A$ with $Q(A) \cong G$.

Proof. It is proved in [1] that there is a finite quasi-regular ring $A = G$ with operations defined by
\[
g + h = g \cdot h \cdot m(g, h)^{-1}, \quad g \times h = m(g, h)
\]
and $Q(A) \cong G$; here $m: G \times G \to \zeta(G)$ is a certain map, where $\zeta(G)$ is the center of $G$. In particular, $1 \in G$ is the additive identity of $A$. By induction, it can be shown that
\[
g + \cdots + g = g^n \cdot m(g, g)^{-n(n-1)/2}
\]
for a positive integer $n$. Since the prime $p$ is odd because a group of exponent two cannot be of class two, we can prove
\[
g + \cdots + g = 1.
\]

Therefore, there is a canonical $\mathbb{F}_p$-algebra structure on $A$. \hfill \Box

Proof of Lemma 3.5. Since finite abelian $p$-groups are hereditary groups over $\mathbb{F}_p$ by Lemma 3.2, it suffices to prove that $[G] \in S(\mathbb{F}_p)$ for every finite $p$-group $G$ of class two and exponent $p$. Because such $p$-group $G$ is a quasi-regular group of some finite quasi-regular $\mathbb{F}_p$-algebra by Theorem 3.6, $[G] \in S(\mathbb{F}_p)$ follows from Lemma 2.4. \hfill \Box

Now we are in position to prove the theorem by Passi and Sehgal.

Proof of Theorem 3.4. Since the finite $p$-group $G$ of class two and exponent $p$ is a hereditary group over $\mathbb{F}_p$ by Lemma 3.5, $\mathbb{F}_pG \cong \mathbb{F}_pH$ implies $G \cong H$ by Criterion 1.6. \hfill \Box

---

2 Beware that the operations defined in [1] are incorrect; it is corrected in [7].
3.3 Class two and exponent four

The aim of this subsection is to prove the even prime counterpart of Theorem 3.4.

**Theorem 3.7** (Passi–Sehgal). Let $G$ and $H$ be finite 2-groups. Suppose $G$ is of class two and exponent four. If $F_2 G \cong F_2 H$, then $G \cong H$.

**Remark 3.8.** Note that the third dimension subgroup of $G$ modulo $p$ is $G^p \gamma_3(G)$ if $p \neq 2$ and $G^4(G')^2 \gamma_3(G)$ if $p = 2$, where $\gamma_3(G)$ denotes the third term of the lower central series of $G$. Thus, the assumption for a group in Theorem 3.4 or Theorem 3.7 holds if $G$ has the trivial third modular dimension subgroup. Actually, this is how assumption is stated by Passi and Sehgal [13, Corollary 7].

Nowadays, more is known. A theorem by Sandling [21, Theorem 1.2] provides a positive solution for a finite $p$-group of class two with elementary abelian commutator subgroup.

A strategy for the proof is the same as Theorem 3.4. The even prime counterpart of the Ault–Watters theorem is the following theorem by Bovdi [2].

**Theorem 3.9** (Bovdi). Let $G$ be a finite 2-group. Suppose $G$ is of class two and exponent four. Then there is a finite quasi-regular $F_2$-algebra $A$ with $Q(A) \cong G$.

**Lemma 3.10.** Every 2-group of class two and exponent four is a hereditary group over $F_2$.

**Proof.** As all finite abelian 2-groups are hereditary groups over $F_2$ by Lemma 3.2, it suffices to prove that $[G] \in S(F_2)$ for every finite 2-group $G$ of class two and exponent four. Because such 2-group $G$ is a quasi-regular group of some finite quasi-regular $F_2$-algebra by Theorem 3.9, $[G] \in S(F_2)$ follows from Lemma 2.4.

**Proof of Theorem 3.7.** Since the finite 2-group $G$ of class two and exponent four is a hereditary group over $F_2$ by Lemma 3.10, $F_2 G \cong F_2 H$ implies $G \cong H$ by Criterion 1.6.

**Bibliography**

[1] J. C. Ault and J. F. Watters, Circle groups of nilpotent rings, *Amer. Math. Monthly* **80** (1973), 48–52.

[2] A. A. Bovdi, On circle groups of nilpotent rings of characteristic 2, *Period. Math. Hungar.* **32** (1996), 31–34.

[3] D. B. Coleman, On the modular group ring of a $p$-group, *Proc. Amer. Math. Soc.* **15** (1964), 511–514.
[4] C. Davis and T. Occhipinti, Which finite simple groups are unit groups?, *J. Pure Appl. Algebra* **218** (2014), 743–744.

[5] W. E. Deskins, Finite abelian groups with isomorphic group algebras, *Duke Math. J.* **23** (1956), 35–40.

[6] B. Eick and A. Konovalov, The modular isomorphism problem for the groups of order 512, in: *Groups St. Andrews 2009. Vol. 2*, Cambridge University, Cambridge (2011), 375–383.

[7] R. Gilmer and D. Roselle, Complements and comments, *Amer. Math. Monthly* **80** (1973), 1116–1118.

[8] M. Hertweck and M. Soriano, On the modular isomorphism problem: groups of order $2^6$, in: *Groups, Rings and Algebras*, Contemp. Math. 420, American Mathematical Society, Providence (2006), 177–213.

[9] G. J. Janusz, Faithful representations of $p$ groups at characteristic $p$. I, *J. Algebra* **15** (1970), 335–351.

[10] R. L. Kruse and D. T. Price, *Nilpotent Rings*, Gordon and Breach Science, New York, 1969.

[11] L. Lovász, Operations with structures, *Acta Math. Acad. Sci. Hung.* **18** (1967), 321–328.

[12] L. Lovász, Direct product in locally finite categories, *Acta Sci. Math. (Szeged)* **33** (1972), 319–322.

[13] I. B. S. Passi and S. K. Sehgal, Isomorphism of modular group algebras, *Math. Z.* **129** (1972), 65–73.

[14] D. S. Passman, *The Algebraic Structure of Group Rings*, Pure Appl. Math., John Wiley & Sons, New York, 1977.

[15] C. Polcino Milies and S. K. Sehgal, *An Introduction to Group Rings, Algebra and Applications. I*, Kluwer Academic, Dordrecht, 2002.

[16] J. Rosenberg, *Algebraic K-theory and its Applications*, Grad. Texts in Math. 147, Springer, New York, 1994.

[17] L. H. Rowen, *Graduate Algebra: Noncommutative View*, Grad. Stud. Math. 91, American Mathematical Society, Providence, 2008.

[18] R. Sandling, Group rings of circle and unit groups, *Math. Z.* **140** (1974), 195–202.

[19] R. Sandling, Units in the modular group algebra of a finite Abelian $p$-group, *J. Pure Appl. Algebra* **33** (1984), 337–346.

[20] R. Sandling, The isomorphism problem for group rings: a survey, in: *Orders and Their Applications*, Lecture Notes in Math. 1142, Springer, Berlin (1985), 256–288.

[21] R. Sandling, The modular group algebra of a central-elementary-by-abelian $p$-group, *Arch. Math. (Basel)* **52** (1989), 22–27.
[22] S. K. Sehgal, *Topics in Group Rings*, Monogr. Textb. Pure Appl. Math. 50, Marcel Dekker, New York, 1978.

[23] S. K. Sehgal, Group rings, in: *Handbook of Algebra. Vol. 3*, Elsevier/North-Holland, Amsterdam (2003), 457–541.

Received May 16, 2019; revised November 19, 2019.

**Author information**

Taro Sakurai, Department of Mathematics and Informatics, Graduate School of Science, Chiba University, 1-33, Yayoi-cho, Inage-ku, Chiba-shi, Chiba, 263-8522, Japan. E-mail: tsakurai@math.s.chiba-u.ac.jp