A REDUCTION THEOREM FOR THE ISOMORPHISM PROBLEM OF GROUP ALGEBRAS OVER FIELDS

DIEGO GARCÍA-LUCAS AND ÁNGEL DEL RÍO

Abstract. We prove that the Isomorphism Problem for group algebras reduces to group algebras over finite extensions of the prime field. In particular, the Modular Isomorphism Problem reduces to finite modular group algebras.

Let R be commutative ring. The Isomorphism Problem for group rings over R asks whether the isomorphism type of G is determined by the isomorphism type of RG as R-algebra. More precisely:

> **Isomorphism Problem for Group Rings**: Let R be a commutative ring and let G and H be groups. If RG and RH are isomorphic as R-algebras, are G and H isomorphic groups?

This problem has been studied extensively, with special emphasis on the cases where the groups are finite and the coefficient ring is either the integers or a field. One of the first results is due to G. Higman who proved that if G and H are finite abelian groups and $\mathbb{Z}G \cong \mathbb{Z}H$, then $G \cong H$ [Hig40a, Hig40b]. This was extended to finite metabelian groups by A. Whitcomb [Whi68], and later extended to abelian-by-nilpotent groups by K. W. Roggenkamp and L. Scott [RS87] and to nilpotent-by-abelian groups by W. Kimmerle (see [RT92, Section XII]). However, M. Hertweck founded two non-isomorphic finite solvable groups with isomorphic integral group rings [Her01]. See [MR18, Section 3] for an overview on the Isomorphism Problem for integral group rings.

In this note we only consider finite groups and fields as coefficient rings. It is easy to obtain non-isomorphic finite groups with isomorphic group algebras. For example, if G and H are abelian groups of the same order n and F is an algebraically closed field of characteristic not dividing n, then $FG \cong FH$. However, by a result of S. Perlis and G. L. Walker, if G and H are non-isomorphic abelian groups, then $\mathbb{Q}G \ncong \mathbb{Q}H$ [PW50]. A more elaborated counterexample, given by E. Dade, consists in two non-isomorphic finite metabelian groups G and H with $FG \cong FH$ for every field F [Dad71]. The order of these groups is divisible by two different primes. On the other hand, D. S. Passman proved the following two results (see [Pas65b] or [Pas77, Theorems 1.9 and 1.11]). If G and H are finite groups with $\mathbb{Q}G \cong \mathbb{Q}H$, then $FG \cong FH$ for every field F of characteristic coprime with the order of G. If p is prime and n is a positive integer, then there are at least $p^{\frac{2}{27}n^2(n-23)}$ pairwise non-isomorphic groups of order p^n with isomorphic group algebras over any field of characteristic different from p.

These motivated the so-called Modular Isomorphism Problem (abbreviated MIP), which is the version of the Isomorphism Problem for group algebras of finite p-groups over the field with p elements, or more generally over fields of characteristic $p > 0$. This turned out to be quite different, and definitive answers more difficult to obtain. Some partial positive solutions where obtained by a number of authors [Pas65a, PS72, BC88, San89, Dre89, SS96, Bag99, Her07, EK11, BK19, BdR21, MM20, MSS21, MS22, GLdRS22], and recently a negative solution for $p = 2$ was given in [GLMdR22].

The previous discussion shows that, even in the same characteristic, changing the field may alter the answer to the Isomorphism Problem. Yet, if the Isomorphism Problem for FG and FH has a positive solution and K is a subfield of F, then it also has a positive solution for KG and KH because $FG \cong F \otimes_K KG$. Hence, the larger the field, the greater the chances for the Isomorphism Problem to have a negative answer are. The aim of this note is to bound the class of coefficient fields when searching for negative solutions for the Isomorphism Problem. Namely, we prove the following:

Date: September 4, 2023.

2020 *Mathematics Subject Classification.* 20C05, 16S34.

Key words and phrases. Finite groups, group algebra, isomorphism problem.

Partially supported by grant PID2020-113206GB-I00 funded by MCIN/AEI/10.13039/501100011033 and by grant 22004/PI/22 funded by Fundación Séneca.

Theorem A. *Let F be a field, $\mathbb{P}$ the prime field of F, and G and H finite groups. If $FG \cong FH$, then there exist a finite extension F_0 of $\mathbb{P}$ such that $F_0G \cong F_0H$.*

If the characteristic of $\mathbb{P}$ is coprime with the order of the group G, then a finite extension of $\mathbb{P}$ split $\mathbb{P}G$ and $\mathbb{P}H$ and hence, in this case, a proof of Theorem A is straightforward. However, we present a unified proof for any characteristic. In contrast with Theorem A, it is easy to see that there is no absolute bound for the index of $\mathbb{P}$ in the field F_0 of Theorem A (see Example 3).

The application of Theorem A to the MIP shows that this question can be regarded as exclusively about finite objects. Formally:

Corollary B. *Let G and H finite p-groups such that $FG \cong FH$ for some field F of characteristic p. Then there exists a finite field F_0 of characteristic p such that $F_0G \cong F_0H$.*

The fact that this last reduction is not (to the best of our knowledge) mentioned elsewhere is somehow surprising, since, although most of the results known about the MIP depend heavily on the primality of the field (e.g. [San89]), some authors were interested in the question substituting the prime field for arbitrary fields of characteristic p. For instance, in [Dre89], V. Drensky showed that the Isomorphism Problem for fields of characteristic p and finite p-groups with center of index p^2 has a positive solution , even though the result for the prime field was already known by a result of I. B. N. Passi and S. K. Sehgal [PS72]. Further classical results on the MIP which are only stated over the prime field are known to hold for arbitrary fields of the same characteristic (see e.g. [San96]). A complete list of results about the MIP, distinguishing which ones are known for every field of characteristic p, and which ones only for the prime field, can be found in the recent survey [Mar22]. Moreover, some of the techniques used to study the MIP, mainly the ones consisting on counting elements in the group algebra verifying some property, as suggested by R. Brauer in [Bra63], are only available for finite fields. This, apparently, makes the reduction in Corollary B a potentially useful tool in the study of the extended version of the MIP.

The state of the art in the extended version of the MIP suggests the following question.

Question. Let G and H be finite p-groups such that $FG \cong FH$ for some field F of characteristic p. Does it imply that $\mathbb{F}_pG \cong \mathbb{F}_pH$, for the field $\mathbb{F}_p$ with p elements?

For the proofs we use standard algebraic notation. For example, given rings $R \subseteq S$ and T a subset of S, $R[T]$ denotes the subring of S generated by $R \cup T$. In case R and S are fields, $R(T)$ denotes the smallest subfield of S containing $R \cup T$. When $T = \{t_1, \dots, t_n\}$ we write $R[t_1, \dots, t_n]$ and $R(t_1, \dots, t_n)$ rather than $R[\{t_1, \dots, t_n\}]$ or $R(\{t_1, \dots, t_n\})$. If $\psi : R \to R'$ is a ring homomorphism and Z is an indeterminate, then we also denote ψ the natural extension of ψ to a homomorphism $R[Z] \to R'[Z]$. Let E/F be a field extension. If $\alpha \in E$ is algebraic over F, then $\mathrm{Min}_F(\alpha)$ denotes the minimal polynomial of α over F. Observe that if $FG \cong FH$ for groups G and H, then $EG \cong EH$, because $EG \cong E \otimes_F FG$. We will use this frequently to replace F by a convenient overfield.

We will use another trivial observation:

Fact 1. *Let F be a field and $\phi : FG \to FH$ be an algebra isomorphism. Write $\phi(g) = \sum_{h \in H} a_{gh}h$ for each $g \in G$, where $a_{gh} \in F$. If $L = \mathbb{P}(a_{gh} : g \in G, h \in H)$, then $LG \cong LH$.*

Proof. Immediate, as the homomorphism $\tilde{\phi} : LG \to LH$ given by $\tilde{\phi}(g) = \sum_{h \in H} a_{gh}h$ is an isomorphism, because the matrix $(a_{gh})_{g \in G, h \in H}$ is non-singular. □

Proof of Theorem A. Let F be a field, and let G and H be finite groups such that $FG \cong FH$. Let $\overline{F}$ be an algebraic closure of F. All our fields will be subfields of $\overline{F}$. By Fact 1 we can assume that $F = \mathbb{P}(a_{gh} : g \in G, h \in H)$. In particular F is finitely generated over $\mathbb{P}$. By [Bou90, §14 Theorem 1], there is an intermediate extension $\mathbb{P} \subseteq E \subseteq F$ with $E/\mathbb{P}$ purely transcendental, F/E algebraic and both finitely generated. Hence $E = \mathbb{P}(X_1, \dots, X_m)$, where the X_i's are algebraically independent over $\mathbb{P}$ and replacing F by the normal closure of F/E we may assume that F/E is a finite normal extension.

Fact 2. *There is a finite algebraic extension L of E such that $\mathbb{P} \subseteq L$ is purely transcendental with finite transcendence degree and LF/L is a finite Galois extension.*

Proof. Let p be the characteristic of F. The statement is clear if $p = 0$ so suppose that $p > 0$. By [Isa94, Theorem 19.18] there is a subextension $E \subseteq K \subseteq F$ with K/E purely inseparable, and F/K separable. Observe that all these extensions are finite and F/K is Galois.

Let $\alpha_1, \ldots, \alpha_m \in K$ such that $K = E(\alpha_1, \ldots, \alpha_{m_i})$. Each α_i is the unique root of a polynomial $T^{p^{m_i}} - \beta_i$ for some $\beta_i \in E$. Let $M = \max\{m_i : i = 1, \ldots, m\}$ and let T_i be the unique root of $T^{p^M} - X_i$ in $\overline{F}$, for $i \in \{1, \ldots, m\}$. Set $L = E(T_1, \ldots, T_m) = \mathbb{P}(T_1, \ldots, T_m)$. Then $L/\mathbb{P}$ is purely transcendental with finite transcendence degree and, as F/K is finite and Galois, to prove that so is LF/L, it suffices to show that $K \subseteq L$. As $E = \mathbb{P}(X_1, \ldots, X_m)$, each $\beta_i = \frac{\delta_i(X_1,\ldots,X_m)}{R_i(X_1,\ldots,X_m)}$ for some $\delta_i, R_i \in \mathbb{P}[X_1, \ldots, X_m]$ and therefore $\tilde{\beta}_i = \frac{\delta_i(T_1,\ldots,T_m)}{R_i(T_1,\ldots,T_m)}$ satisfies $\tilde{\beta}_i^{p^M} = \beta_i$. Then α_i is the unique root of $T^{p^{m_i}} - \beta_i = (T - \tilde{\beta}_i^{p^{M-m_i}})^{p^{m_i}}$, so $\alpha_i = \tilde{\beta}_i^{p^{M-m_i}} \in L$. Hence $K \subseteq L$, as desired. □

Let L be a field as in Fact 2. By replacing E and F by L and LF respectively, we may assume that F/E is a finite Galois extension. Then, by the Primitive Element Theorem, $F = E(\zeta)$ for some $\zeta \in F$.

Let $R = \mathbb{P}[X_1, \ldots, X_m] \subseteq E$. Let d be the determinant of the matrix $(a_{gh})_{g\in G, h\in H}$, $A = \mathrm{Min}_E(\zeta)$ and $B = \mathrm{Min}_E(d)$. Then

$$a_{gh} = \frac{\sum_{i=0}^{n_{gh}} P_{ghi}\zeta^i}{Q_{gh}}, \quad A = \sum_i \frac{\alpha_i}{\beta_i} Z^i \in E[Z] \quad \text{and} \quad B = \sum_i \frac{\gamma_i}{\delta_i} Z^i \in E[Z],$$

for some $P_{ghi}, Q_{gh}, \alpha_i, \beta_i, \gamma_i, \delta_i \in R$, with each Q_{gh}, β_i and δ_i different from 0. Let

$$Q = \gamma_0 \prod_i \delta_i \prod_i \beta_i \prod_{\substack{g\in G,\\ h\in H}} Q_{gh} \in \mathbb{P}[X_1, \ldots, X_n].$$

Let $S = \{Q^k : k \geq 0\}$, a multiplicative subset of R, and let $D = S^{-1}R$ be the ring of fractions of R by S. As R is a unique factorization domain, so is D. Let $\overline{\mathbb{P}}$ be the algebraic closure of $\mathbb{P}$ in $\overline{F}$. By Hilbert's Nullstellensatz, there is an evaluation homomorphism $\psi : R \to \overline{\mathbb{P}}$ such that $\psi(Q) \neq 0$. By the universal property of the ring of fractions, ψ extends to a homomorphism $D \to \overline{\mathbb{P}}$, which we also denote ψ. As $A \in D[Z]$, by Gauss Lemma the kernel of the evaluation homomorphism $\delta : D[Z] \to D[\zeta]$ mapping Z to ζ is generated by A. Let $\bar{\zeta}$ be a root of the polynomial $\psi(A)$ in $\overline{\mathbb{P}}$. The homomorphism $\psi' : D[Z] \to \overline{\mathbb{P}}$ which extends ψ and maps Z to $\bar{\zeta}$ has A in its kernel, so there is a homomorphism $\psi'' : D[\zeta] \to \overline{\mathbb{P}}$ making commutative the diagram

$$\begin{array}{ccc} D[Z] & \xrightarrow{\delta} & D[\zeta] \\ & \searrow^{\psi'} & \downarrow{\scriptstyle \psi''} \\ & & \overline{\mathbb{P}} \end{array} .$$

Let $\bar{a}_{gh} = \psi''(a_{gh})$ and $\bar{d} = \psi''(d)$. Then $\bar{d}$ is the determinant of the matrix $(\bar{a}_{gh})_{g\in G, h\in H}$, and a root of the polynomial $\psi''(B)$. As the independent term of $\psi''(B)$ is $\psi''(P_0) = \psi(P_0) \neq 0$, we conclude that $\bar{d} \neq 0$. Let $F_0 = \mathbb{P}(\bar{a}_{gh} : g \in G, h \in H) \subseteq \overline{\mathbb{P}}$. Then F_0 is a finite extension of $\mathbb{P}$. Moreover, the map $G \mapsto (F_0H)^\times$ given by $g \mapsto \sum_{h\in H} \bar{a}_{gh}h$ is an homomorphism of groups, as it is just the composition of the inclusion $G \subseteq D[\zeta]G$, the restriction $\phi|_{D[\zeta]G} : D[\zeta]G \to D[\zeta]H$, and the homomorphism $D[\zeta]H \to F_0H$ induced by $\psi'' : D[\zeta] \to F_0$. Therefore there is a homomorphism of F_0-algebras $\bar{\phi} : F_0G \to F_0H$ such that $\bar{\phi}(g) = \sum_{h\in H} \bar{a}_{gh}h$ for each $g \in G$. As $\bar{d} \neq 0$, the set $\bar{\phi}(G)$ is a basis of F_0H. Thus $\bar{\phi}$ is an isomorphism. □

We denote the cyclic group of order n by C_n. For m and n coprime integers, let $o_m(n)$ denote the multiplicative order of n modulo m, i.e. the smallest positive integer t with $n^t \equiv 1 \mod m$.

Example 3. *For every prime field $\mathbb{P}$ and every positive integer n there exist a prime integer q different than the characteristic of $\mathbb{P}$, and a positive integer k such that $FC_q^k \ncong FC_{q^k}$ for every field extension F of $\mathbb{P}$ with $[F : \mathbb{P}] \leq n$, but $EC_q^k \cong EC_{q^k}$ for some field extension E of $\mathbb{P}$.*

Proof. We first suppose that $\mathbb{P}$ is of characteristic 0. In this case we take $q = 2$ and k the least positive integer with $2^{k-1} > n$. To prove that q and k satisfy the desired condition we use a Theorem of Perlis and Walker [PW50] (see also [JdR16, Theorem 3.3.6]). Let F be a field extension of $\mathbb{P}$. Then $FC_2^k \cong F^{2^k}$, and if F contains a primitive 2^k-root of unity ζ, then $FC_{2^k} \cong F^{2^k}$. Thus, if $E = \mathbb{P}(\zeta)$ then $EC_2^k \cong EC_{2^k}$, while if $[F : \mathbb{P}] \leq n$ then $\zeta \notin F$, so FC_{2^k} has a factor isomorphic to $F(\zeta)$ and hence $FC_2^k \ncong FC_{2^k}$.

For positive characteristic we use a version of the Perlis-Walker Theorem for finite fields (see [JdR16, Problem 3.3.9]).

Suppose that $\mathbb{P}$ has characteristic $p > 2$ and let q be a prime divisor of $p-1$. The sequence $(o_{q^k}(p))_k$ is unbounded and we take a positive integer k such that $o_{q^k}(p) > n$. Let F be a finite field extension of $\mathbb{P}$ with $t = [F : \mathbb{P}]$. As in the previous case $FC_q^k \cong F^{q^k}$ and if $p^t \equiv 1 \mod q^k$, then $FC_{q^k} \cong F^{q^k}$. However, if $t \leq n$, then FC_{q^k} has an epimorphic image which is a field extension of F of degree $o_{q^k}(p^t) = \frac{o_{q^k}(p)}{\gcd(t, o_{q^k}(p))} > 1$ because $t < o_{q^k}(p)$. Thus $FC_q^k \ncong FC_{q^k}$.

Finally, suppose that $\mathbb{P}$ has characteristic 2. In this case we take $q = 3$ and k the least integer such that $3^{k-1} > n$. Let F be a field extension of $\mathbb{P}$ of degree t and K a field extension of F of degree 2. If t is even, then $FC_3 = F^3$. However, if t is odd, then $FC_3 \cong F \times K$. Therefore, FC_3^k is a direct product of fields isomorphic to F or K, and if t is even, then $FC_3^k \cong F^{3^k}$. If $2^t \equiv 1 \mod 3^k$, then t is even and $FC_{3^k} \cong F^{3^k}$. However, if $t \leq n$, then FC_{3^k} has an epimorphic image isomorphic to a field extension of F of degree $o_{3^k}(2^t) = \frac{o_{3^k}(2)}{\gcd(t, o_{3^k}(2))} = \frac{2 \cdot 3^{k-1}}{\gcd(t, 2 \cdot 3^{k-1})} > 2$ because $t < 3^{k-1}$. Thus $FC_3^k \ncong FC_{3^k}$. □

References

[Bag99] C. Bagiński, *On the isomorphism problem for modular group algebras of elementary abelian-by-cyclic p-groups*, Colloq. Math. **82** (1999), no. 1, 125–136.

[BC88] C. Bagiński and A. Caranti, *The modular group algebras of p-groups of maximal class*, Canad. J. Math. **40** (1988), no. 6, 1422–1435.

[BdR21] O. Broche and Á. del Río, *The Modular Isomorphism Problem for two generated groups of class two*, Indian J. Pure Appl. Math. **52** (2021), 721–728.

[BK19] C. Bagiński and J. Kurdics, *The modular group algebras of p-groups of maximal class II*, Comm. Algebra **47** (2019), no. 2, 761–771.

[Bou90] N. Bourbaki, *Algebra II: Chapters 4-7 (Pt.2)*, Springer, 1990.

[Bra63] R. Brauer, *Representations of finite groups*, Lectures on Modern Mathematics, Vol. I, Wiley, New York, 1963, pp. 133–175.

[Dad71] E. Dade, *Deux groupes finis distincts ayant la même algèbre de groupe sur tout corps*, Math. Z. **119** (1971), 345–348.

[Dre89] V. Drensky, *The isomorphism problem for modular group algebras of groups with large centres*, Representation theory, group rings, and coding theory, Contemp. Math., vol. 93, Amer. Math. Soc., Providence, RI, 1989, pp. 145–153.

[EK11] B. Eick and A. Konovalov, *The modular isomorphism problem for the groups of order 512*, Groups St Andrews 2009 in Bath. Volume 2, London Math. Soc. Lecture Note Ser., vol. 388, Cambridge Univ. Press, Cambridge, 2011, pp. 375–383.

[GLdRS22] D. García-Lucas, Á. del Río, and M. Stanojkowski, *On group invariants determined by modular group algebras: even versus odd characteristic*, Algebr. Represent. Theory. https://doi.org/10.1007/s10468-022-10182-x (2022).

[GLMdR22] D. García-Lucas, L. Margolis, and Á. del Río, *Non-isomorphic 2-groups with isomorphic modular group algebras*, J. Reine Angew. Math. **154** (2022), no. 783, 269–274.

[Her01] M. Hertweck, *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math. (2) **154** (2001), no. 1, 115–138.

[Her07] Martin Hertweck, *A note on the modular group algebras of odd p-groups of M-length three*, Publ. Math. Debrecen **71** (2007), no. 1-2, 83–93.

[Hig40a] G. Higman, *Units in group rings*, 1940, Thesis (Ph.D.)–Univ. Oxford.

[Hig40b] ———, *The units of group-rings*, Proc. London Math. Soc. (2) **46** (1940), 231–248.

[Isa94] I. Martin Isaacs, *Algebra, a graduate course*, 1 ed., Mathematics, Brooks/Cole Pub. Co, 1994.

[JdR16] E. Jespers and Á. del Río, *Group ring groups. Volume 1: Orders and generic constructions of units*, Berlin: De Gruyter, 2016.

[Mar22] L. Margolis, *The Modular Isomorphism Problem: A Survey*, Jahresber. Dtsch. Math. Ver. (2022).

[MM20] L. Margolis and T. Moede, *The Modular Isomorphism Problem for small groups – revisiting Eick's algorithm*, arXiv:2010.07030, https://arxiv.org/abs/2010.07030.

[MR18] L. Margolis and Á. del Río, *Finite subgroups of group rings: A survey*, preprint, arxiv.org/abs/1809.00718 (2018), 23 pages.

[MS22] L. Margolis and M. Stanojkovski, *On the modular isomorphism problem for groups of class 3 and obelisks*, J. Group Theory **25** (2022), no. 1, 163–206.

[MSS21] L. Margolis, T. Sakurai, and M. Stanojkovski, *Abelian invariants and a reduction theorem for the modular isomorphism problem*, https://arxiv.org/abs/2110.10025.

[Pas65a] D. S. Passman, *The group algebras of groups of order p^4 over a modular field*, Michigan Math. J. **12** (1965), 405–415. MR 0185022

[Pas65b] ———, *Isomorphic groups and group rings*, Pacific J. Math. **15** (1965), 561–583.

[Pas77] ———, *The algebraic structure of group rings*, Pure and Applied Mathematics, Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1977.

[PS72] I. B. S. Passi and S. K. Sehgal, *Isomorphism of modular group algebras*, Math. Z. **129** (1972), 65–73.

[PW50] S. Perlis and G. L. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), 420–426.

[RS87] K. W. Roggenkamp and L. Scott, *Isomorphisms of p-adic group rings*, Ann. of Math. (2) **126** (1987), no. 3, 593–647.

[RT92] K. W. Roggenkamp and M. J. Taylor, *Group rings and class groups*, DMV Seminar, vol. 18, Birkhäuser Verlag, Basel, 1992.

[San89] R. Sandling, *The modular group algebra of a central-elementary-by-abelian p-group*, Arch. Math. (Basel) **52** (1989), no. 1, 22–27.

[San96] ———, *The modular group algebra problem for metacyclic p-groups*, Proc. Amer. Math. Soc. **124** (1996), no. 5, 1347–1350.

[SS96] M. A. M. Salim and R. Sandling, *The modular group algebra problem for groups of order p^5*, J. Austral. Math. Soc. Ser. A **61** (1996), no. 2, 229–237.

[Whi68] A. Whitcomb, *The Group Ring Problem*, ProQuest LLC, Ann Arbor, MI, 1968, Thesis (Ph.D.) – The University of Chicago.

Departamento de Matemáticas, Universidad de Murcia, Spain
Email address: diego.garcial@um.es

Departamento de Matemáticas, Universidad de Murcia, Spain
Email address: adelrio@um.es