Czechoslovak Mathematical Journal, 71 (146) (2021), 1011–1014

SUMMANDS OF FINITE GROUP ALGEBRAS

Carsten Dietzel, Stuttgart, Gaurav Mittal, Roorkee

Received May 1, 2020. Published online December 14, 2020.

Abstract. We study the inverse problem of the determination of a group algebra from the knowledge of its Wedderburn decomposition. We show that a certain class of matrix rings always occur as summands of finite group algebras.

Keywords: Wedderburn decomposition; group algebra

MSC 2020: 20C05

Let $\mathbb{F}_q$ be the field with $q = p^k$ elements, where p is a prime and $k \in \mathbb{Z}^+$. It is well known that the group algebra $\mathbb{F}_qG$ of a finite group G is semisimple and therefore isomorphic to a direct sum of matrix rings over finite fields of characteristic p if and only if p does not divide $|G|$, see [1]. The problem of determining the matrix rings corresponding to a semisimple group algebra is rather classical. Its inverse, however, is less studied, namely: given a ring $\bigoplus\limits_{t=1}^{j} M_{n_t}(\mathbb{F}_{q_t})$, where each $\mathbb{F}_{q_t}$ is a finite field of characteristic p, does there exist a semisimple group algebra $\mathbb{F}_qG$ such that $\bigoplus\limits_{t=1}^{j} M_{n_t}(\mathbb{F}_{q_t}) \cong \mathbb{F}_qG$?

The main aim of this paper is to study the above-said inverse problem. From [1], Proposition 3.6.11, it is known that if RG is a semisimple group algebra, then

$$RG \cong R(G/G') \bigoplus \Delta(G, G'),$$

where G' is the commutator subgroup of G, $R(G/G')$ is the sum of all commutative simple components of RG, and $\Delta(G, G')$ is the sum of all others. Since $|G/G'|$ is at least 1, we conclude that the Wedderburn decomposition of any semisimple group algebra must have some abelian part, so there are plenty of semisimple finite rings which fail to be group rings (up to isomorphism). Therefore, we now look for the

DOI: 10.21136/CMJ.2020.0171-20

solution of a slightly modified problem, i.e., whether direct sums of matrix rings over a field of characteristic p occur as summands of some group algebra. With the help of Proposition 1, we show that this modified problem has a negative answer.

Proposition 1. *If $R = \bigoplus_{t=1}^{j} M_{n_t}(\mathbb{F}_{q_t})$ is a summand of a semisimple group ring $\mathbb{F}_q G$ $(q = p^k)$, then p does not divide any of the n_t.*

Proof. We can assume that each $\mathbb{F}_{q_t} = \mathbb{F}_{q^{m_t}}$ for some positive integer m_t. The extension $\mathbb{F}_{q^{m_t}}/\mathbb{F}_q$ is separable, therefore

$$\mathbb{F}_{q^{m_t}} \bigotimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q \cong \overline{\mathbb{F}}_q^{m_t}.$$

Therefore, $\overline{R} := R \bigotimes_{\mathbb{F}_q} \bigoplus_{t=1}^{j} \overline{\mathbb{F}}_q \cong \bigoplus_{t=1}^{j} M_{n_t}(\overline{\mathbb{F}}_q)^{m_t}$, and this ring must be a summand of $\overline{\mathbb{F}}_q G$. This means that the degrees of the irreducible representations of G over $\overline{\mathbb{F}}_q$ include the n_t $(1 \leqslant t \leqslant j)$. But it is well-known that the degree of an irreducible representation of G over a splitting field divides $|G|$.[1] But $p \nmid |G|$, due to $\mathbb{F}_q G$ being semisimple. □

Proposition 1 clearly tells us that many semisimple matrix rings fail to be summands of finite group rings. However, we can prove Proposition 1 to be the only obstruction to the above-said inverse problem by showing the following:

Theorem 1. *Let p be a fixed prime and $R = \bigoplus_{t=1}^{j} M_{n_t}(\mathbb{F}_{p^{m_t}})$ with all n_t being integers not divisible by p. Then there is a group G with order not divisible by p such that R is a summand of $\mathbb{F}_p G$.*

To prove this, we first show:

Proposition 2. *Let k be a positive integer. Then there is a group G, $p \nmid |G|$, such that $\mathbb{F}_{p^k}$ is a summand of $\mathbb{F}_p G$.*

Proof. Take $G = \mathbb{F}_{p^k}^{\times}$, the unit group of $\mathbb{F}_{p^k}$. Then the map

$$\pi\colon\ \mathbb{F}_p G \to \mathbb{F}_{p^k},$$
$$\sum_{g\in G} a_g[g] \mapsto \sum_{g\in G} a_g \cdot g,$$

is an epimorphism, which means that $\mathbb{F}_{p^k}$ is an epimorphic image of $\mathbb{F}_p G$, and thus a summand thereof. □

[1] It follows, for example, from [2], Corollary 6.5.2 and Proposition 15.5.43.

We also need to show that certain matrix rings are epimorphic images of semisimple group rings:

Proposition 3. *Let n be a positive integer not divisible by p. Then there is a group G, $p \nmid |G|$, such that $M_n(\mathbb{F}_p)$ is a summand of $\mathbb{F}_pG$.*

Proof. As $\mathbb{F}_p$-vector spaces $V := \mathbb{F}_{p^n} \cong \mathbb{F}_p^n$. Take $G = C_n \ltimes \mathbb{F}_{p^n}^{\times}$, where $C_n = \langle\sigma\rangle$ is a cyclic group of order n and acts on the second factor via ${}^{\sigma}x = x^p$ (note that $x^{p^n} = x$ for all $x \in \mathbb{F}_{p^n}^{\times}$). Furthermore, note that $|G| = n(p^n - 1)$ is not divisible by p. For all $x, y \in \mathbb{F}_{p^n}$, $x \neq 0$, we have $\sigma(x \cdot y) = x^p\sigma(y)$. Therefore V becomes a left $\mathbb{F}_pG$-module by defining the scalar multiplication by

$$\sigma^k \cdot y = y^{p^k},$$
$$x \cdot y = xy \quad (x \in \mathbb{F}_{p^n}^{\times}).$$

We claim that mapping each element of G to the respective left-multiplication map in $\mathrm{End}_{\mathbb{F}_p}(V)$ makes $\mathrm{End}_{\mathbb{F}_p}(V)$ an epimorphic image of $\mathbb{F}_pG$.

A classical theorem of Artin tells us that the $\mathbb{F}_p$-endomorphisms $\tau_k \colon V \to V$, $y \mapsto \sigma^k \cdot y = y^{p^k}$ $(0 \leqslant k < n)$ are linearly independent over $\mathbb{F}_{p^n}$, where we identify $\mathbb{F}_{p^n}$ as a subalgebra of $\mathrm{End}_{\mathbb{F}_p}(V)$ via left multiplication. So $\mathbb{F}_{p^n}$, together with the τ_k $(0 \leqslant k < n)$, span an n^2-dimensional subalgebra of $\mathrm{End}_{\mathbb{F}_p}(V)$ which must therefore be the whole of $\mathrm{End}_{\mathbb{F}_p}(V) \cong M_n(\mathbb{F}_p)$.

This shows that the latter is a summand of $\mathbb{F}_pG$. □

Proof of Theorem 1. Let k be a positive integer and let n be not divisible by p. Take G, H – of order not divisible by p – such that $\mathbb{F}_{pk}$ is a summand of $\mathbb{F}_pG$ (see Proposition 2) and $M_n(\mathbb{F}_p)$ is a summand of $\mathbb{F}_pH$ (see Proposition 3).

Then $M_n(\mathbb{F}_{p^k}) \cong \mathbb{F}_{p^k} \bigotimes_{\mathbb{F}_p} M_n(\mathbb{F}_p)$ is a summand of $\mathbb{F}_pG \bigotimes_{\mathbb{F}_p} \mathbb{F}_pH \cong \mathbb{F}_p(G \times H)$, which is still semisimple.

Let now $R = \bigoplus_{t=1}^{j} M_{n_t}(\mathbb{F}_{p^{m_t}})$. Choose G_t $(1 \leqslant t \leqslant j)$ such that $M_{n_t}(\mathbb{F}_{p^{m_t}})$ is a summand of $\mathbb{F}_pG_t$ and $p \nmid |G_t|$.

Each $\mathbb{F}_pG_t$ has $\mathbb{F}_p$ as a summand. Therefore $\bigoplus_{t=1}^{s} \mathbb{F}_pG_t$ is a summand of

$$\mathbb{F}_pG_1 \bigotimes_{\mathbb{F}_p} \ldots \bigotimes_{\mathbb{F}_p} \mathbb{F}_pG_t \cong \mathbb{F}_p(G_1 \times \ldots G_t),$$

which is clearly semisimple. Also it follows that R is a summand of the latter. □

References

[1] *C. Polcino Milies, S. K. Sehgal*: An Introduction to Group Rings. Algebras and Applications 1. Kluwer Academic Publishers, Dordrecht, 2002. zbl MR

[2] *J.-P. Serre*: Linear Representations of Finite Groups. Graduate Texts in Mathematics 42. Springer, New York, 1977. zbl MR doi

Authors' addresses: Carsten Dietzel, Institute of Algebra and Number Theory, University of Stuttgart, Pfaffenwaldring 57, 70569 Stuttgart, Germany, e-mail: `carstendietzel@gmx.de`; Gaurav Mittal (corresponding author), Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee, Uttarakhand 247667, India, e-mail: `gmittal@ma.iitr.ac.in`.