ON THE ARITHMETIC OF THE JOIN RINGS OVER FINITE FIELDS

SUNIL K. CHEBOLU, JONATHAN MERZEL, JÁN MINÁČ,
TUNG T. NGUYEN, FEDERICO PASINI, NGUYỄN DUY TÂN

Abstract. Given a collection $\{G_i\}_{i=1}^d$ of finite groups and a ring R, we have previously defined and studied certain foundational properties of the join ring $\mathcal{J}_{G_1,G_2,\ldots,G_d}(R)$. The introduction of this ring was motivated by various problems in graph theory, network theory, nonlinear dynamics, and neuroscience. In this paper, we study some further properties of this ring. In particular, we investigate its arithmetic when R is a finite field.

1. Introduction

Let G be a finite group. The study of G-circulant matrices has a long history in mathematics (see 2.1 for the precise definition of a G-circulant matrix). These matrices were introduced by Dedekind through his investigation of normal bases for Galois extensions. Shortly after its appearance, Frobenius showed that the determinant of a circulant matrix can be decomposed into a product of irreducible factors corresponding to the linear irreducible representations of G. In particular, when G is a cyclic group, we have an explicit description of the spectrum of G-circulant matrices. This description is often referred to as the Circiulant Diagonalization Theorem in the literature (see [10] for an extensive treatment of this topic). Due to their elegance and explicit nature, circulant matrices have found applications in many scientific fields such as spectral graph theory, coding theory, neuroscience, and nonlinear dynamics (see [1, 2, 4, 11, 13, 19, 27, 20, 33]).

In [9], we introduce a natural generalization of G-circulant matrices. More precisely, given a collection of finite groups $G_1, G_2, \ldots, G_d$ and a ring R, we introduce the join ring $\mathcal{J}_{G_1,G_2,\ldots,G_d}(R)$ (see Section 2.2 for the precise definition of this ring). When $d = 1$, the ring $\mathcal{J}_G(R)$ is exactly the ring all of G-circulant matrices with entries in R. Furthermore, $\mathcal{J}_G(R)$ is naturally isomorphic to the group ring $R[G]$. We also remark that when all G_i are the trivial group, the join ring is naturally isomorphic to $M_d(R)$, the algebra of all square matrices of size $d \times d$ with coefficients in R. The introduction of the join ring $\mathcal{J}_{G_1,G_2,\ldots,G_d}(R)$ is motivated by a construction in graph theory known as the joined union of graphs, and by a desire to understand nonlinear dynamics in multilayer networks of oscillators (see [11, 12, 28]). In [9], we discuss some fundamental ring theoretic properties of the join ring $\mathcal{J}_{G_1,G_2,\ldots,G_d}(R)$ such as their centers, its semisimplicity, its Jacobson radical, structure of its unit group, and much

Sunil Chebolu is partially supported by Simons Foundation's Collaboration Grant for Mathematicians (516354). Ján Mináč is partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) grant R0370A01. Ján Mináč also gratefully acknowledges Faculty of Sciences Distinguished Research Professorship award for 2020/21. Ján Mináč, Tung T Nguyen, and Federico Pasini acknowledge the support of the Western Academy for Advanced Research. Nguyễn Duy Tân is funded by Vingroup Joint Stock Company and supported by Vingroup Innovation Foundation (VinIF) under the project code VINIF.2021.DA00030.

more. In this present article, we discuss some further properties of this ring with a special focus on the case that R is a finite field. This article presents our continuing effort to develop a systematic understanding of the join ring $\mathcal{J}_{G_1,G_2,\dots,G_d}(R)$.

The structure of this article is as follows. In Section 2, we study some further ring theoretic properties of the join ring $\mathcal{J}_{G_1,G_2,\dots,G_d}(R)$. Among various things that we discover, we discuss a natural construction of the generalized augmentation map. Section 3 studies the zeta functions of the join ring $\mathcal{J}_{G_1,G_2,\dots,G_d}(R)$ when $R=\mathbb{F}_q$ is a finite field. More precisely, we describe how to explicitly calculate the zeta function of $\mathcal{J}_{G_1,G_2,\dots,G_d}(\mathbb{F}_q)$ in terms of the zeta functions of $\mathcal{J}_{G_i}(\mathbb{F}_q)$. In section 4, we discuss the order of the unit group of $\mathcal{J}_{G_1,G_2,\dots,G_d}(\mathbb{F}_q)$ and explain its connection with Artin's conjecture on primitive roots. Finally, in the last section, we classify all join rings $\mathcal{J}_{G_1,G_2,\dots,G_d}(\mathbb{F}_q)$ that are a Δ_{p^r}-ring where p is a prime number and r is a positive integer (we refer the readers to Definition 5.1 for the precise definition of this concept).

2. Some ring theoretic properties of $\mathcal{J}_{G_1,G_2,\dots,G_d}(R)$.

2.1. **The ring of circulant matrices.** Let G be a finite group. We first recall the definition of a G-circulant matrix (for more details, see [9, 17, 19]).

Definition 2.1. An $n\times n$ G-circulant matrix over R is an $n\times n$ matrix

$$A=\begin{bmatrix} a_{g_1,g_1} & a_{g_1,g_2} & \cdots & a_{g_1,g_n}\\ a_{g_2,g_1} & a_{g_2,g_2} & \cdots & a_{g_2,g_n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{g_n,g_1} & a_{g_n,g_2} & \cdots & a_{g_n,g_n}\end{bmatrix}$$

over R with the property that for all $g,g_i,g_j\in G$, $a_{g_i,g_j}=a_{gg_i,gg_j}$.

We remark that a circulant matrix A is completely determined by its first row and the multiplication table of G. For simplicity, we sometimes write $A=\mathrm{circ}([a_g]_{g\in G})$. Let $\mathcal{J}_G(R)$ be the set of all G-circulant matrices over R and

$$R[G]=\left\{\sum_{g\in G}a_g g\big|a_g\in R\right\},$$

the group ring of G with coefficients in R. In [9], we reproved the following theorem of Hurley.

Proposition 2.2. *(Hurley) Let $\alpha: R[G]\to\mathcal{J}_G(R)$ sending*

$$\sum_{g\in G}a_g g\mapsto circ([a_g]_{g\in G}),$$

is a ring isomorphism.

2.2. **The join rings $\mathcal{J}_{G_1,G_2,\dots,G_d}(R)$.** We recall the definition of the join matrix (see [9, Definition 3.1]).

Definition 2.3. Let R be a (unital, associative) ring, $G_1,\dots,G_d$ finite groups of respective orders $k_1,\dots,k_d$, and let C_i be G_i-circulant ($1\le i\le d$) over R. By a join of $C_1,\dots,C_d$ over R, we mean a matrix of the form

$$(*) \qquad A = \begin{bmatrix} C_1 & a_{12}J_{k_1,k_2} & \cdots & a_{1d}J_{k_1,k_d} \\ a_{21}J_{k_2,k_1} & C_2 & \cdots & a_{2d}J_{k_2,k_d} \\ \vdots & \vdots & & \vdots \\ a_{d1}J_{k_d,k_1} & a_{d2}J_{k_d,k_2} & \cdots & C_d \end{bmatrix},$$

where $a_{ij} \in R$ $(1 \leq i \neq j \leq d)$ and $J_{r,s}$ denotes the $r \times s$ matrix, all of whose entries are $1 \in R$.

As in [9], we will denote by $\mathcal{J}_{G_1,\ldots,G_d}(R)$, the set of all such joins as the C_i vary independently through all G_i-circulant matrices $(1 \leq i \leq d)$ and the a_{ij} vary independently through all elements of R $(1 \leq i \neq j \leq d)$. In [9], we showed the following.

Proposition 2.4. *(*[9, Section 3] *$\mathcal{J}_{G_1,\ldots,G_d}(R)$ has the structure of a unital ring. Furthermore, there is an augmentation map $\epsilon\colon \mathcal{J}_{G_1,\ldots,G_d}(R) \to M_d(R)$ that generalizes the augmentation map on group rings.*

2.3. **The generalized augmentation map.** Let G be a finite group and H be a normal subgroup of G. Then, there is a canonical ring map

$$\epsilon : R(G) \to R(G/H). \tag{2.1}$$

When $H = G$, this is exactly the classical augmentation map $\epsilon : R[G] \to R$ mentioned in the previous section. More concretely, this augmentation map is defined by

$$\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g.$$

In this section, we show that there is a natural analog of this augmentation map in the setting of the join ring $\mathcal{J}_{G_1,G_2,\ldots,G_d}(R)$. More precisely, let G_i be finite group and H_i a normal subgroup of G_i for all $1 \leq i \leq d$. Suppose that the orders of $G_i, H_i, G_i/H_i$ are k_i, r_i, s_i respectively (so $k_i = r_i s_i$). Let us consider the following map

$$\epsilon : \mathcal{J}_{G_1,G_2,\ldots,G_d}(R) \to \mathcal{J}_{G_1/H_1,G_2/H_2,\ldots,G_d/H_d}(R), \tag{2.2}$$

defined by

$$\begin{bmatrix} C_1 & a_{12}J_{k_1,k_2} & \cdots & a_{1d}J_{k_1,k_d} \\ a_{21}J_{k_2,k_1} & C_2 & \cdots & a_{2d}J_{k_2,k_d} \\ \vdots & \vdots & & \vdots \\ a_{d1}J_{k_d,k_1} & a_{d2}J_{k_d,k_2} & \cdots & C_d \end{bmatrix} \mapsto \begin{bmatrix} \epsilon(C_1) & r_2 a_{12}J_{s_1,s_2} & \cdots & r_d a_{1d}J_{s_1,s_d} \\ r_1 a_{21}J_{s_2,s_1} & \epsilon(C_2) & \cdots & r_d a_{2d}J_{s_2,s_d} \\ \vdots & \vdots & & \vdots \\ r_1 a_{d1}J_{s_d,s_1} & r_2 a_{d2}\mathcal{J}_{s_d,s_2} & \cdots & \epsilon(C_d). \end{bmatrix}$$

Here ϵ is the classical augmentation map $R[G_i] \to R[G_i/H_i]$ as defined in Equation 2.1. We have the following.

Proposition 2.5. *The map $\epsilon : \mathcal{J}_{G_1,G_2,\ldots,G_d}(R) \to \mathcal{J}_{G_1/H_1,G_2/H_2,\ldots,G_d/H_d}(R)$ is a ring homomorphism.*

Proof. This follows from direct calculations. Two key identities are the following.

(1) $J_{m,n} \times J_{n,p} = nJ_{m,p}$.
(2) $AJ_{m,n} = \epsilon(A)J_{m,n}$ where A is a semimagic square of size $m \times m$ and $\epsilon(A)$ is the row sum of A. Similarly $J_{m,n}B = \epsilon(B)J_{m,n}$ if B is a semimagic square of size $n \times n$.

□

2.4. **A decomposition of $\mathcal{J}_{G_1,G_2,\dots,G_d}(R)$.** Let $\epsilon : \Delta_R(G,H) := ker(R[G] \to R[G/H])$ be the augmentation map as defined in Equation 2.1 (when R is clearly from the context, we will simply write $\Delta(G,H)$.) Suppose further that $|H|$ is invertible in R. Let

$$e_H = \frac{1}{|H|}\sum_{h\in H} h.$$

We can see that e_H is a central idempotent in $R[G]$. Furthermore, by [24, Proposition 3.6.7], we have

Proposition 2.6. *We have a direct product of rings*

$$R[G] \cong R[G]e_H \times R[G](1-e_H).$$

Furthermore

$$R[G]e_H \cong R[G/H],$$

and

$$R[G](1-e_H) \cong \Delta_R(G,H).$$

Corollary 2.7. *(see* [24, Corollary 3.6.9]*) Suppose that $|G|$ is invertible in R. Let $\Delta_R(G)$ be the augmentation ideal. Then*

$$R[G] \cong R \times \Delta_R(G).$$

We can generalize this proposition to the join ring as follow.

Theorem 2.8. *Let $G_1,\dots,G_d$ be finite groups. For $1 \le i \le d$, let H_i is a normal subgroup such that $|H_i|$ is invertible in R. Then there exists an isomorphism*

$$\mathcal{J}_{G_1,\dots,G_d}(R) \cong \mathcal{J}_{G_1/H_1,\dots,G_d/H_d}(R) \times \prod_{i=1}^{d} \Delta_R(G_i,H_i).$$

Proof. Let $f_i = f_{H_i} = I_i - e_{H_i}$ where e_{H_i} is defined as above and I_i is the identity matrix of size $|G_i|$. Additionally $f_{d+1} = I - \sum_{i=1}^{d} f_i = \sum_{i=1} e_{H_i}$. Then we have the following ring isomorphism

$$\mathcal{J}_{G_1,\dots,G_d}(R) \cong f_{d+1}\mathcal{J}_{G_1,\dots,G_d}(R) \times \prod_{i=1}^{d} f_i\mathcal{J}_{G_1,\dots,G_d}(R).$$

We can see that for $1 \le i \le d$

$$f_i\mathcal{J}_{G_1,\dots,G_d}(R) \cong \Delta_R(G_i,H_i).$$

Additionally, the augmentation map

$$\varepsilon : \mathcal{J}_{G_1,G_2,\dots,G_d}(R) \to \mathcal{J}_{G_1/H_1,\dots,G_d/H_d}(R)$$

induces a ring isomorphism

$$\varepsilon : f_{d+1}\mathcal{J}_{G_1,G_2,\dots,G_d}(R) \to \mathcal{J}_{G_1/H_1,\dots,G_d/H_d}(R).$$

□

Here is a direct corollary of this theorem.

Corollary 2.9. *(See also* [9, Theorem 3.16]*) Suppose that $|G_i|$ are invertible in R. Then*

$$\mathcal{J}_{G_1,G_2,\dots,G_d}(R) \cong M_d(R) \times \prod_{i=1}^{d} \Delta_R(G_i).$$

3. Zeta functions of the join rings $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements where p is a prime number. In this section, we study the zeta function of the join algebra $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$. We first recall the definition of the zeta function of a finite-dimensional $\mathbb{F}_q$-algebra as defined in [14].

First, let us consider the case where R is a commutative finite dimensional $\mathbb{F}_q$-algebra. The Hasse-Weil zeta function of R is defined to be

$$\zeta_R(s) = \prod_{m \subset R} (1 - \#(R/m)^{-s})^{-1}. \tag{3.1}$$

where m runs over all maximal ideal of R (see [14]). As observed in [14], when R is not commutative, the Hasse-Weil zeta function of R can be defined as follow (we refer readers to [21, 22] for some further motivations for this definition).

Definition 3.1. (see [14]) Let R be a finite dimension $\mathbb{F}_q$-algebra. The Hasse-Weil zeta function of R is given by the following Euler product

$$\zeta_R(s) = \prod_{M} (1 - |\mathrm{End}_R(M)|^{-s})^{-1}, \tag{3.2}$$

where M runs over the isomorphism classes of (finite) simple left R-modules.

We remark that since R is a finite ring, all simple left R-modules are automatically finite. Furthermore, by [14, Lemma 2.7.1], another equivalent definition of $\zeta_R(s)$ is

$$\zeta_R(s) = \prod_{m \in \mathfrak{P}(R)} (1 - N(\mathfrak{m})^{-s})^{-1}, \tag{3.3}$$

where $\mathfrak{P}(R)$ is the set of all two-sided ideals $\mathfrak{m}$ in R such that $A/\mathfrak{m}$ is isomorphic to the matrix ring $M_r(k)$ with k is a finite extension of $\mathbb{F}_q$ and $N(\mathfrak{m}) = |k|$.

For a finite dimension $\mathbb{F}_q$-algebra R, we denote

$$R^{\mathrm{ss}} = R/Rad(R).$$

where $Rad(R)$ is the Jacobson radical of R. It is well-known that $Rad(R^{\mathrm{ss}}) = 0$. Additionally since R is Artinian, R^{ss} is Artinian as well. Consequently, R^{ss} is a semisimple algebra. We have the following observation.

Proposition 3.2. *Let R be a finite dimensional $\mathbb{F}_q$ algebra and $Rad(R)$ the Jacobson radical of R. Let $\mathfrak{m} \in \mathfrak{P}(R)$. Then*

1. *$Rad(R) \subset \mathfrak{m}$.*
2. *The map $\mathfrak{m} \mapsto \overline{\mathfrak{m}} := \mathfrak{m}/Rad(R)$ from $\mathfrak{P}(R) \to \mathfrak{P}(R^{ss})$ is a bijection. Furthermore $N(\mathfrak{m}) = N(\bar{\mathfrak{m}})$.*

Proof. By definition $R/\mathfrak{m} \cong M_r(k)$ for some $r \geq 1$ and a field k. The first statement hence follows from [30, Section 4.3, Lemma b]. The second statement then follows naturally from the first statement. □

A direct consequence of this proposition is the following.

Proposition 3.3. *Suppose R is a finite-dimensional $\mathbb{F}_q$-algebra. Then*

$$\zeta_R(s) = \zeta_{R^{ss}}(s).$$

We discuss some further properties of the zeta function of a finite dimension $\mathbb{F}_q$-algebra.

Proposition 3.4. *(*[14, Proposition 2.2] *Let R, T be two finite-dimensional $\mathbb{F}_q$-algebras. Then*

(1) $\zeta_{R\times T}(s) = \zeta_R(s)\zeta_T(s)$.
(2) *If R and T are Morita equivalent, then $\zeta_R(s) = \zeta_T(s)$.*

We discuss some concrete examples of R and their zeta functions.

Example 3.5. Let us consider $R = M_n(\mathbb{F}_q)$. Since $M_n(\mathbb{F}_q)$ is Morita equivalent to $\mathbb{F}_q$, Proposition 3.4 shows that

$$\zeta_{M_n(\mathbb{F}_q)}(s) = \zeta_{\mathbb{F}_q}(s) = (1 - q^{-s})^{-1}.$$

Example 3.6. Let G be a finite group such that $|G|$ is invertible in $\mathbb{F}_q$. Let $R = \mathbb{F}_q[G]$. Suppose further that G splits over $\mathbb{F}_q$; i.e,

$$\mathbb{F}_q[G] = \prod_{i=1}^{d} M_{n_i}(\mathbb{F}_q).$$

Then

$$\zeta_{\mathbb{F}_q[G]}(s) = \prod_{i=1}^{d} \zeta_{M_{n_i}(\mathbb{F}_q)}(s) = (1 - q^{-s})^{-d}.$$

In general, if G does not splits over $\mathbb{F}_q$ then the calculation of $\zeta_{\mathbb{F}_q[G]}(s)$ is less explicit. When G is abelian, however, we can describe the zeta function of $\mathbb{F}_q[G]$ explicitly. Before we state the key theorem, we recall the following definition.

Definition 3.7. Let d be a positive integer number and a an integer such that $\gcd(a, d) = 1$. The order of a with respect to d, denoted by $\mathrm{ord}_d(a)$ is the smallest positive integer t such that $a^t \equiv 1 \pmod{d}$.

We are now ready to state the key theorem that allows us to compute the zeta function of $\mathbb{F}_q[G]$ where G is an abelian group.

Theorem 3.8. [25, Theorem 3.5.4] *Let G be a finite abelian group of order n which is prime to q. Then*

$$\mathbb{F}_q[G] \cong \bigoplus_{d|n} a_d \mathbb{F}_q[\zeta_d],$$

where ζ_d is a primitive root of unity of order d and $a_d = \frac{n_d}{[\mathbb{F}_q(\zeta_d):\mathbb{F}_q]}$. Here n_d is the number of elements of order d in G. Note also that

$$[\mathbb{F}_q(\zeta_d) : \mathbb{F}_q] = ord_d(q).$$

Corollary 3.9. *Let G be a finite abelian group of order n which is prime to q. Then*

$$\zeta_{\mathbb{F}_q[G]}(s) = \prod_{d|n} (1 - q^{-ord_d(q)s})^{a_d},$$

where a_d and $ord_d(q)$ are as above.

We also remark that in some special cases, the zeta function of $\zeta_{\mathbb{F}_q[G]}(s)$ in the modular case (namely $|G| = 0$ in $\mathbb{F}_q$) can be deduced from the semisimple case (namely $|G|$ is invertible in $\mathbb{F}_q$). This is a consequence of Proposition 3.3 and the following theorem.

Theorem 3.10. *([29, Theorem 16.6]) Let G be a finite group. Suppose that H is a normal p-Sylow subgroup of G. Then, the Jacobson radical of $\mathbb{F}_q[G]$ is the kernel of the augmentation map*

$$\epsilon : \mathbb{F}_q[G] \to \mathbb{F}_q[G/H].$$

Consequently, $\mathbb{F}_q[G]^{ss} \cong \mathbb{F}_q[G/H]$ and

$$\zeta_{\mathbb{F}_q[G]}(s) = \zeta_{F_q[G/H]}(s).$$

We next consider the ring of semimagic squares. First, we need to recall their definition.

Definition 3.11. (see [26]) Let k be a field. A matrix $A \in M_n(k)$ is called a semimagic square if its row and column sums are equal; i.e there exists a constant $\sigma(A)$ such that

$$\sum_{i=1}^{n} a_{ij} = \sum_{j=1}^{n} a_{ji} = \sigma(A).$$

We can check that the set of all semimagic squares of size $n \times n$ has a natural ring structure. For simplicity, we will denote this ring by $SM_n(k)$. By [26], we can describe the semisimplification of $SM_n(k)$ explicitly.

Theorem 3.12. [26, Theorem 2, Theorem 3] *Let k be a field of characteristic $p \geq 0$. Then*

(1) *If $p \nmid n$ then*
$$SM_n(k) \cong k \times M_{n-1}(k).$$
(2) *If $p|n$ then the algebra $SM_n(k)$ is not semisimple. Its simplification is given by*
$$SM_n(k)^{ss} \cong k \times M_{n-2}(k).$$

Corollary 3.13. *Let $SM_n(\mathbb{F}_q)$ be the ring of all semimagic squares of size $n \times n$ over $\mathbb{F}_q$ with $n \geq 3$. Then*

(1) *If $n = 1$ then $\zeta_{SM_1(\mathbb{F}_q)}(s) = (1 - q^{-s})^{-1}$.*
(2) *If $n = 2$ then*
$$\zeta_{SM_2(\mathbb{F}_q)}(s) = \begin{cases} (1-q^{-s})^{-2} & char(\mathbb{F}_q) \neq 2 \\ (1-q^{-s})^{-1} & char(\mathbb{F}_q) = 2. \end{cases}$$
(3) *If $n \geq 3$ then*
$$\zeta_{SM_n(\mathbb{F}_q)}(s) = (1 - q^{-s})^{-2}.$$

We now compute explitcity the zeta function of $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ in terms of the zeta functions for $\mathbb{F}_q[G_i]$ for $1 \leq i \leq d$. We first consider the semisimple case, namely the case where all $|G_i|$ are invertible in $\mathbb{F}_q$. In this case, by Corollary 2.9, we have

$$\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q) \cong M_d(\mathbb{F}_q) \times \prod_{i=1}^{d} \Delta_{\mathbb{F}_q}(G).$$

Consequently

$$\zeta_{\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)}(s) = \zeta_{M_d(\mathbb{F}_q)} \times \prod_{i=1}^{d} \zeta_{\Delta_{\mathbb{F}_q}(G_i)}(s) = (1-q^{-s})^{-1} \times \prod_{i=1}^{d} \zeta_{\Delta_{\mathbb{F}_q}(G_i)}(s).$$

Furthermore, we also have

$$\mathbb{F}_q[G_i] \cong \mathbb{F}_q \times \Delta_{\mathbb{F}_q}(G_i),$$

and therefore

$$\zeta_{\mathbb{F}_q[G_i]}(s) = \zeta_{\mathbb{F}_q}(s)\zeta_{\Delta_{\mathbb{F}_q}(G_i)}(s) = (1-q^{-s})^{-1}\zeta_{\Delta_{\mathbb{F}_q}(G_i)}(s).$$

In summary, we have the following

Proposition 3.14. *Suppose that $|G_i|$ is invertible in $\mathbb{F}_q$ for $1 \leq i \leq d$. Then the zeta function of $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is given by*

$$(1-q^{-s})^{d-1} \times \prod_{i=1}^{d} \zeta_{\mathbb{F}_q[G_i]}(s).$$

We next consider the general case. We can assume that, up to an ordering, there exists a (unique) positive integer r such that

- $p \nmid |G_i|, 1 \leq i \leq r$.
- $p||G_i|, r < i \leq d$.

We recall the following construction in [9, Section 5]. Let A be a generic element of $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$

$$A = \left[\begin{array}{c|c|c|c} C_1 & a_{12}J & \cdots & a_{1d}J \\ \hline a_{21}J & C_2 & \cdots & a_{2d}J \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline a_{d1}J & a_{d2}J & \cdots & C_d \end{array}\right].$$

We can further partition A into the following blocks

$$A = \begin{bmatrix} A_1 & B_1 \\ B_2 & A_2 \end{bmatrix},$$

where A_1 is the union of the upper r blocks, A_2 is the union of the lower $d-r$ blocks, B_1 (respectively B_2) is the union of the upper right (respectively lower left) blocks. Concretely, we have

$$A_1 = \left[\begin{array}{c|c|c|c} C_1 & a_{12}J & \cdots & a_{1r}J \\ \hline a_{21}J & C_2 & \cdots & a_{2r}J \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline a_{r1}J & a_{r2}J & \cdots & C_r \end{array}\right],$$

$$A_2 = \left[\begin{array}{c|c|c|c} C_{r+1} & a_{r+1,r+2}J & \cdots & a_{r+1,d}J \\ \hline a_{r+2,r+1}J & C_2 & \cdots & a_{r+2,d}J \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline a_{d,r+1}J & a_{d,r+2}J & \cdots & C_d \end{array}\right].$$

Similarly for B_1, B_2. Note that we can consider A_1 (respectively A_2) as an element of $\mathcal{J}_{G_1,\ldots,G_r}(\mathbb{F}_q)$ (respectively $\mathcal{J}_{G_{r+1},\ldots,G_d}(\mathbb{F}_q)$.)

Theorem 3.15. *([9]) Let I_i be the Jacobson radical of $\mathbb{F}_q[G_i]$. Let ψ be the map*

$$\psi\colon \mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q) \to \mathcal{J}_{G_1,\ldots,G_r}(R) \times \prod_{r+1\leq i\leq d} \mathbb{F}_q[G_i]/I_i,$$

sending

$$A \mapsto (A_1, \overline{C_{r+1}}, \ldots, \overline{C_d}).$$

Then ψ is a surjective ring homomorphism. Furthermore, the kernel of ψ is the Jacobson radical of $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$. As a consequence,

$$\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)^{ss} \cong \mathcal{J}_{G_1,\ldots,G_r}(\mathbb{F}_q) \times \prod_{r+1\leq i\leq d} k[G_i]^{ss}.$$

Furthermore, by Corollary 2.9, we can further decompose

$$\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)^{ss} \cong M_r(\mathbb{F}_q) \times \prod_{i=1}^{r} \Delta_{\mathbb{F}_q}(G_i) \times \prod_{r+1\leq i\leq d} k[G_i]^{ss}.$$

By Theorem 3.15 and Proposition 3.14, we have the following corollary.

Corollary 3.16. *Let $G_1, G_2, \ldots, G_d$ be as above. Then the zeta function of $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is given by*

$$\zeta_{\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)}(s) = (1-q^{-s})^{r-1} \prod_{i=1}^{d} \zeta_{\mathcal{J}_{G_i}(\mathbb{F}_q)}(s).$$

Maybe: Add the same result for the join of semimagic squares.

4. q-rooted primes and the arithmetic of the join rings

In this section, we study the order of the unit group of the join algebra $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ where G_i is a cyclic of order p_i with p_i is a prime number different from q. This is a natural continuation of the work [7] where the author considers the case $d = 1$ and $q = 2$. We first recall the following definition.

Definition 4.1. Let p, q be two prime numbers. We say that p is a q-rooted prime if q is a primitive root modulo p; i.e q is a generator of the multiplicative group $\mathbb{F}_p^{\times}$ (which is a cyclic group of order $(p-1)$). Equivalently, p is a q-rooted prime if and only if $\mathrm{ord}_p(q) = p-1$.

A conjecture of Artin says that for a given q, there exists infinitely many p such that p is a q-rooted prime. This conjecture is still wide open, though some conditional results are known. For example, it is known that Artin's conjecture holds if we assume the Generalized Riemann Hypothesis (see [15, 16]). In [7], the authors provide an elegant characterization of q-root primes using circulant matrices when $q = 2$. We remark, however, that their proof remains valid for any prime number q. For the sake of completeness, we provide here the statement and a complete proof.

Theorem 4.2. *Let p be a prime number. Then the following statements are equivalent.*

1. *p is a q-rooted prime.*
2. *The order of the unit group of the group algebra $\mathbb{F}_q[\mathbb{Z}/p]$ is $(q^{p-1}-1)(q-1)$.*
3. *The number of invertible circulant matrices of size $p \times p$ over $\mathbb{F}_q$ is $(q-1)(q^{p-1}-1)$.*

Proof. We observe that

$$\mathbb{F}_q[\mathbb{Z}/p] \cong \mathbb{F}_q[x]/(x^p-1) = \mathbb{F}_q \times \mathbb{F}_q[x]/\Phi_p(x).$$

Here $\Phi_p(x) = \dfrac{x^p-1}{x-1}$ is the q-cyclotomic polynomial. By [7, Lemma 3.1], $\Phi_p(x)$ factors as a product of $m = \dfrac{p-1}{\mathrm{ord}_p(q)}$ distinct irreducible polynomials in $\mathbb{F}_q[x]$ of degree $n = \mathrm{ord}_p(q)$. Consequently, as a ring we have

$$\mathbb{F}_q[\mathbb{Z}/p] \cong \mathbb{F}_q \times \mathbb{F}_{q^n}^m.$$

We see that the order of the unit group of $\mathbb{F}_q[\mathbb{Z}/p]$ is given by $(q-1)(q^n-1)^m$. We also observe that

$$(q^n-1)^m \leq q^{mn}-1,$$

and the equality happens iff $m=1$. Theorem 4.2 then follows from these calculations.

□

The following theorem is a direct generalization of Theorem 4.2.

Theorem 4.3. *Let $q, p_1, p_2, \ldots, p_d$ be prime numbers such that $p_i \neq q$. Then the following are equivalent*

(1) *p_i is a q-rooted prime for all $1 \leq i \leq d$.*
(2) *The order of the unit group of the join algebra $\mathcal{J}_{\mathbb{Z}/p_1,\mathbb{Z}/p_2,\ldots,\mathbb{Z}/p_d}(\mathbb{F}_q)$ is*

$$\prod_{i=1}^{d}(q^{p_i-1}-1) \times \prod_{i=0}^{d-1}(q^d-q^i).$$

Proof. By corollary 2.9 we know that the join algebra $\mathcal{J}_{\mathbb{Z}/p_1,\mathbb{Z}/p_2,\ldots,\mathbb{Z}/p_d}(\mathbb{F}_q)$ is decomposed as

$$\mathcal{J}_{\mathbb{Z}/p_1,\mathbb{Z}/p_2,\ldots,\mathbb{Z}/p_d}(\mathbb{F}_q) \cong M_d(\mathbb{F}_q) \times \prod_{i=1}^{d}\Delta_{\mathbb{F}_q}(\mathbb{Z}/p_1).$$

Consequently, the order of the unit group of the join algebra $\mathcal{J}_{\mathbb{Z}/p_1,\mathbb{Z}/p_2,\ldots,\mathbb{Z}/p_d}(\mathbb{F}_q)$ is given by

$$|GL_d(\mathbb{F}_q)| \times \prod_{i=1}^{d}\Delta_{\mathbb{F}_q}(\mathbb{Z}/p_1)^{\times}.$$

By Theorem 4.2, we know that

$$|\Delta_{\mathbb{F}_q}(\mathbb{Z}/p_1)^{\times}| \leq q^{p_1-1}-1,$$

with equality happens when p_i is a q-rooted prime. Combining this with the fact that

$$|GL_d(\mathbb{F}_q)| = \prod_{i=0}^{d-1}(q^d-q^i),$$

we complete the proof of the above theorem.

□

5. $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ AND Δ_{p^r}-RINGS

In this section, we consider a special ring-theoretic property of the join ring $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$. Specifically, we are interested in the Δ_n-property of the join ring. To do so, we first recall the definition of a Δ_n-ring.

Definition 5.1. Let n be a positive integer. A ring R is said to be a Δ_n-ring if for each unit $u \in R^{\times}$, $u^n = 1$.

The Δ_n-property of a ring is well-studied in the literature. It was first introduced in [5]. There, the authors prove that the ring $\mathbb{Z}/n$ of integers modulo n is a Δ_2-ring if and only if n is a divisor of 24. In [8], the authors show that the ring $\mathbb{Z}/n[x_1, x_2, \ldots, x_m]$ is a Δ_2-ring if and only if n is a divisor of 12. Additionally, in [7], the authors classify all group algebras $k[G]$ which are a Δ_p-ring where G is an abelian group and p is a prime number (see [7, Theorem 1.4] and [7, Theorem 1.5].)

We remark that if R is a Δ_n ring then it is also a Δ_m ring if $n|m$. If n is the smallest positive integer such that R satisfies this property, then call R a strict Δ_n-ring. We refer the readers to [5, 7, 8] for some further discussions of this concept.

We next discuss the relationship between the Δ_n-property of R and its semisimplification R^{ss}. For this, we need the following proposition.

Proposition 5.2. *The canonical map $\Phi : R^\times \to (R^{ss})^\times$ is surjective.*

Proof. Let $a \in R^{\text{ss}}$ be a unit. Then there exist $b \in R^{\text{ss}}$ such that $ab = 1$. Let $a' \in R$ (respectively, $b' \in R$) be a preimage of a (respectively b). One has $a'b' = 1 + c$ for some $c \in \text{Rad}(R)$. Since $c \in \text{Rad}(R)$, $a'b' = 1 + c$ is right-invertible. This implies that a' is right-invertible. Similarly, $b'a' = 1 + d$ for some $d \in \text{Rad}(R)$. From this, we deduce that a' is also left-invertible. Thus a' is a unit and $\Phi(a') = a$. This shows that Φ is surjective. □

The following Lemma follows directly from Proposition 5.2

Lemma 5.3. *If R is a Δ_n-ring then so is R^{ss}.*

We remark that the converse of Lemma 5.3 is not true in general. For example, let G be a 2-group such as $\mathbb{Z}/8$. Then $R = \mathbb{F}_2[G]$ is a local ring and the Jacobson radical of R is exactly the augmentation ideal $\Delta_{\mathbb{F}_2}(G)$ (see [3, Corollary 1.4]). Consequently $R^{\text{ss}} \cong \mathbb{F}_2$ which is a Δ_2-ring. However, by [7, Theorem 1.4], we know that $\mathbb{F}_2[G]$ is not a Δ_2-ring unless $G = (\mathbb{Z}/2)^r$.

In the case where R is a field, we have the following observation.

Lemma 5.4. *Let k be a field. If k is a Δ_n-ring then k is a finite field.*

Remark 5.5. By Lemma 5.4, we can safely assume that all coefficient fields in the discussion below are finite fields.

In this section, we will focus on the case $n = p^r$ where p is a prime number and r is a positive integer. We remark that the case $r = 1$ was studied in [7] and our work here is a natural continuation of this line of research. We recall that for a group G, the exponent of G denoted by $\exp(G)$ is the smallest integer n such that $g^n = 1$ for all $g \in G$. The following simple observation follows directly from the definition of a Δ_{p^r}-ring.

Proposition 5.6. *If R is a Δ_{p^r}-ring then $R^\times$ is a p-group with exponent at most p^r.*

In practice, the precise determination of r is a challenging problem. For this reason, we introduce the following definition.

Definition 5.7. We say that R is a Δ_{p^∞} ring if $R^\times$ is a p-group.

We remark that if R is a finite ring then R is a Δ_{p^∞}-ring if and only if it is a Δ_{p^r}-ring for some $r > 0$. Here is an observation that we will use throughout this section (see **??** for a special case of this statement.)

Lemma 5.8. *Let q, p^r be two prime powers. The matrix algebra $M_n(\mathbb{F}_q)$ is a Δ_{p^r}-ring if and only if $n = 1$ and $\mathbb{F}_q$ is a Δ_{p^r}-ring.*

Proof. Let us assume that $M_n(\mathbb{F}_q)$ is a Δ_{p^r}-ring. By Proposition 5.6, we know that $|GL_n(\mathbb{F}_q)|$ must be a p-group. Additionally, we know that the order of $GL_n(\mathbb{F}_q)$ is

$$\prod_{i=0}^{n-1}(q^n - q^i) = \prod_{i=0}^{n-1} q^i(q^{n-i} - 1).$$

Suppose that $n \geq 2$. We see that $|GL_d(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i)$ has at least two distinct prime factors. This shows that $GL_d(\mathbb{F}_q)$ is not a p-group which contradicts the fact that $M_n(\mathbb{F}_q)$ is a Δ_{p^r}-ring. □

The main goal of this section is to classify all join algebras $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ which are a Δ_{p^r}-ring. To begin this study, we start with the simplest case namely $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is $\mathbb{F}_q$ (this corresponds to the case $d = 1$ and $G_1 = \{e\}$ the trivial group). To answer this question, we first recall the famous Catalan's conjecture, now a theorem of Mihailescu (see [31, 23].)

Theorem 5.9. *(See* [23]*) The only solution in the natural numbers of the Diophantine equation*

$$x^a - y^b = 1.$$

where $a, b > 1$ *and* $x, y > 0$ *is* $x = 3, a = 2, y = 2, b = 3$.

Here is a direct corollary of this theorem which is a generalization of [7, Lemma 2.1] (see [6, Theorem 2.4] for a different but equivalent statement.)

Corollary 5.10. *Let* q *be a prime power. Then, the finite field* $\mathbb{F}_q$ *is a* Δ_{p^r}*-ring if and only if one the following conditions hold*

1. $p = 2, q = 2^{2^n} + 1$ *is a Fermat prime, and* $r \geq 2^n$*. In this case,* $\mathbb{F}_q$ *is a strict* $\Delta_{2^{2^n}}$*-ring.*
2. $p = 2^a - 1$ *is a Mersenne prime and* $q = p + 1 = 2^a$*. In this case* $\mathbb{F}_q$ *is a strict* Δ_p*-ring.*
3. $p = 2$*,* $q = 9$*, and* $r \geq 3$*. In this case,* $\mathbb{F}_q$ *is a strict* Δ_8*-ring.*
4. $q = 2$*,* p *and* r *are arbitrary.*

Proof. The unit group $\mathbb{F}_q^\times$ of $\mathbb{F}_q$ is a cyclic group of order $q-1$. Consequently, $\mathbb{F}_q$ is a Δ_{p^r}-ring if and only $q - 1 | p^r$. Since p is a prime number, there exists $0 \leq b \leq r$ such that $q - 1 = p^b$. Let us write $q = x^a$ where x is a prime and a is a positive integer. We then have the following Diophantine equation

$$x^a - p^b = 1.$$

If $a, b > 1$ then by Mihailescu's theorem 5.9 we know that $x = 3, a = 2, p = 2, b = 3$. This settles the third condition. If $b = 0$ then $x = 2, a = 1$. Consequently $q = 2$. This settles the last condition. Next, we consider the case either $a = 1$ or $b = 1$. First, let us consider the case $a = 1$. Then $x = p^b + 1$. Since $x > 2$, it must be odd. As a result, p is even hence $p = 2$. Therefore, $x = 2^b + 1$. From here, we can deduce that $b = 2^n$ and $x = 2^{2^n} + 1$ is a Fermat prime. This settles the first condition. Finally, let us consider the case $b = 1$. Then we have $p = x^a - 1$. If $p = 2$ then $x = 3, a = 1$ and this recovers the first condition. So, we can safely assume that p is odd. As a result, $x = 2$ and $p = 2^a - 1$ is a Mersenne prime. This covers the second case. □

Next, we will answer the following question: For which group G, the group algebra $\mathbb{F}_q[G]$ is Δ_{p^r}-ring? From the canonical embedding $G \hookrightarrow \mathbb{F}_q[G]^\times$, we conclude that if $\mathbb{F}_q[G]$ is an Δ_{p^r}-ring then G must be a p-group. In turns out that in most cases, G must be abelian as well. More precisely, we have the following proposition.

Proposition 5.11. *Assume that* $(p, q) \neq (2, 2)$ *and that* $\mathbb{F}_q[G]$ *is a* Δ_{p^r}*-ring. Then* G *is an abelian* p*-group.*

Proof. Since $\mathbb{F}_q \subset \mathbb{F}_q[G]$, we conclude that $\mathbb{F}_q$ is also a Δ_{p^r}-ring. Since $(p, q) \neq (2, 2)$, Corollary 5.10 implies that $\gcd(p, q) = 1$. Since G is a p-group, $|G|$ is invertible in $\mathbb{F}_q$. By Maschke's

theorem, $\mathbb{F}_q[G]$ is semisimple and by Artin-Wedderburn theorem we must have

$$\mathbb{F}_q[G] \cong \prod_{i=1}^{r} M_{n_i}(D_i),$$

where D_i is a division algebra over $\mathbb{F}_q$. Since $\mathbb{F}_q$ is a finite field, D_i is a finite field as well. By Lemma 5.8, we conclude that $n_i = 1$ and D_i is an Δ_{p^r}-algebra for all $1 \leq i \leq r$. This implies that $\mathbb{F}_q[G]$ is abelian and hence G is also abelian. □

We now deal with the case $(p, q) = (2, 2)$ separately. Here, instead of working with this particular case, we discuss a more general study of modular group rings, which might be of independent interest. Let k be a finite field of characteristics p and G is a finite p-group. Let $\Delta_k(G)$ be the augmentation ideal. It is known that $\Delta_k(G)$ is a nilpotent ideal; in fact $\Delta_k(G)^{|G|} = 0$ (see [3, Corollary 1.3]). Let $U_1(k[G]) := 1 + \Delta_k(G)$ be the set of all normalized units in $k[G]$. We remark that if $u = 1 + x \in U_1(k[G])$ with $x \in \Delta_k(G)$ then

$$u^{|G|} = 1 + x^{|G|} = 1.$$

This shows that $U_1(k[G])$ is a p-groups. From the isomorphism, $k[G]^\times \cong k^\times \times U_1(k[G])$, we conclude that $k[G]^\times$ is a p-group if and only if $k^\times$ is a p-group. Since $\mathrm{char}(k) = p$, this happens if and only if $k = \mathbb{F}_2$. In summary, we have.

Proposition 5.12. *Let $(p, q) = (2, 2)$ and G a 2-group. Then $\mathbb{F}_q[G]$ is a Δ_{2^r}-ring where $2^r = \exp(U_1(\mathbb{F}_q[G]))$. Furthermore, if G is abelian, $\mathbb{F}_q[G]$ is a strict $\Delta_{\exp(G)}$-ring.*

Proof. We already explained the proof of the first part. For the second part, we note that if G is abelian and

$$u = 1 + x = \sum_{g \in G} a_g g$$

is a normalized unit (so $a_e = 1$) then

$$u^{\exp(G)} = \sum_{g \in G} a_g^{\exp(G)} g^{\exp(G)} = \sum_{g \in G} a_g = 1.$$

□

Remark 5.13. It is worth mentioning that the problem of determining $\exp(U_1(\mathbb{F}_2[G]))$ is well-studied but still open in the literature. We refer interested readers to [18, 32] for further discussions.

With these preliminary results, we are now ready to classify all group algebras $\mathbb{F}_q[G]$ which are a Δ_{p^r}-ring.

Theorem 5.14. *Let q, p^r be prime powers. Let G be a finite group. The group algebra $\mathbb{F}_q[G]$ is a Δ_{p^r}-ring if and only if G is a p-group and one of the following conditions holds.*

1. *$p = 2, q = 2^{2^n} + 1$ is a Fermat prime, $r \geq 2^n$, G is abelian, and the exponent of G is a divisor of 2^{2^n}. In this case, $\mathbb{F}_q[G]$ is a strict $\Delta_{2^{2^n}}$-ring.*
2. *$p = 2^a - 1$ is a Mersenne prime, $q = p + 1 = 2^a$ and $G = (\mathbb{Z}/p)^s$ for some $s \geq 0$. In this case $\mathbb{F}_q[G]$ is a strict Δ_p-ring.*
3. *$p = 2^a - 1$ is a Mersenne prime, $q = 2$ and $G = (\mathbb{Z}/p)^s$ for some $s \geq 0$.*
4. *$p = 2, q = 3$, $r \geq 3$, G is abelian, and the exponent of G is 4 or 8.*
5. *$p = 2, q = 9, r \geq 3$, G is abelian, and the exponent of G is at most 8. In this case, $\mathbb{F}_q[G]$ is a strict Δ_8-ring.*

(6) $q = 2, p = 2$ *and* $2^r \geq \exp(U_1(\mathbb{F}_2[G]))$.

Proof. We will discuss both directions of the above theorem simultaneously. First, let us assume that $\mathbb{F}_q[G]$ is a Δ_{p^r}-ring. Since $\mathbb{F}_q$ is a subring $\mathbb{F}_q[G]$ we conclude that if $\mathbb{F}_q[G]$ is a Δ_{p^r}-ring then so is $\mathbb{F}_q$. From the classification described in Corollary 5.10, we conclude that $p \neq \mathrm{char}(\mathbb{F}_q)$ unless $p = q = 2$. The case $(p, q) = (2, 2)$ is treated separately in Proposition 5.12. For now, let us assume that $(p, q) \neq (2, 2)$. By Proposition 5.11, we conclude that G is abelian. Since G is an abelian p-group with $\gcd(p, q) = 1$, Theorem 3.8 implies

$$\mathbb{F}_q[G] \cong \bigoplus_{d||G|} a_d \mathbb{F}_q[\zeta_d].$$

Here ζ_d is a primitive root of unity of order d and $a_d = \frac{n_d}{[\mathbb{F}_q(\zeta_d):\mathbb{F}_q]}$ where n_d is the number of elements of order d in G. From this formula, we conclude that $\mathbb{F}_q[G]$ is a Δ_{p^r}-ring if and only if each component $\mathbb{F}_q[\zeta_d]$ is. Since $|G|$ is a p-group and $\mathbb{F}_q[\zeta_{d'}] \subset \mathbb{F}_q[\zeta_d]$ if $d'|d$, we conclude that $\mathbb{F}_q[G]$ is a Δ_{p^r}-ring if and only if $\mathbb{F}_q[\zeta_D]$ is Δ_{p^r}-ring where D is largest number such that $n_D > 0$. Since G is a p-group, D is exactly the exponent of G. We remark that $\mathbb{F}_q[\zeta_D] = \mathbb{F}_{q^m}$ where

$$m = [\mathbb{F}_q(\zeta_D) : \mathbb{F}_q] = \mathrm{ord}_D(q).$$

We now consider a few cases based on the classification described in Corollary 5.10.

Case 1: $p = 2$ and $q^m = 2^{2^n} + 1$ is a Fermat prime. This shows that $m = 1$ and q is a Fermat prime. Furthermore, $m = 1$ means that $\mathrm{ord}_D(q) = 1$ or equivalently $D|q - 1 = 2^{2^n}$. This covers the first case of our theorem.

Case 2: $p = 2^a - 1$ is a Mersenne prime and $q^m = p + 1 = 2^a$. This shows that $q = 2^b$ with $bm = a$. By definition of m, we have $q^m \equiv 1 \pmod{D}$. Since $q^m = 2^a$, this is equivalent to $D|2^a - 1 = p$. This implies $D = 1$ or $D = p$. From this, we can conclude that $G = (\mathbb{Z}/p)^s$ for some $s \geq 0$. Furthermore, we remark that since $p = 2^a - 1$ is a prime number, a is a prime number. We then see that $(b, m) = (a, 1)$ or $(b, m) = (1, a)$. The case $(b, m) = (a, 1)$ covers the second case of our theorem and the case $(b, m) = (1, a)$ covers the third case of our theorem.

Case 3: $p = 2$, $q^m = 9$ and $r \geq 3$. Let us first consider the case where $(q, m) = (3, 2)$. Since $m = 2$, we know that $9 = q^m \equiv 1 \pmod{D}$ and $q \not\equiv 1 \pmod{D}$. This shows that $D \in \{4, 8\}$. This covers the fourth case of our theorem. Next, let us consider the case $(q, m) = (9, 1)$. Again, we see that $D|8$. This covers the fifth case of our theorem.

□

Definition 5.15. A ring R is said to have the *diagonal property* if it is a Δ_2-ring.

The classification given in Theorem 5.14 provides another proof for the following statements which were first proved in [7].

Corollary 5.16. *(*[7, Theorem 1.4] *and* [7, Theorem 1.5]*)*

(1) *Let G be a group and k a field. The group algebra $k[G]$ has the diagonal property iff $k[G]$ is either $\mathbb{F}_2[(\mathbb{Z}/2)^r]$ or $\mathbb{F}_3[(\mathbb{Z}/2)^r]$.*
(2) *Let G be a finite abelian group, let k be a field, and let p be an odd prime. The group algebra $k[G]$ is a Δ_p-ring if and only if p is a Mersenne prime and $k[G]$ is is either $\mathbb{F}_2[(\mathbb{Z}/p)^r]$ or $\mathbb{F}_{p+1}[(\mathbb{Z}/p)^r]$.*

Finally, we answer the following question: which join algebra $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is a Δ_{p^r}-ring.

Theorem 5.17. *Suppose that $d \geq 2$. Then the join algebra $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is a Δ_{p^r}-ring if and only if the following conditions are satisfied*

(1) $p = q = 2$.
(2) *G_i is a 2-group for all $1 \leq i \leq d$.*
(3) *There is at most one index i such that $G_i = \{e\}$ the trivial group.*
(4) $2^r \geq \max_{1\leq i\leq d} \exp(U_1(\mathbb{F}_2[G_i]))$.

Proof. Let us prove the "only if" part of the above theorem. Namely, let us assume $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is a Δ_{p^r}-ring. First, we claim that $(p, q) = 2$. In fact, suppose that $(p, q) \neq (2, 2)$. Let us consider the following embedding $\mathbb{F}_q[G_d]^\times \hookrightarrow \mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)^\times$ sending

$$C_1 \mapsto \left[\begin{array}{c|c|c|c} C_1 & 0 & \cdots & 0 \\ \hline 0 & I_{k_2} & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & I_{k_d} \end{array}\right].$$

Since $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is a Δ_{p^r}-ring, $k[G_1]$ is a Δ_{p^r}-ring as well. Similarly, $k[G_i]$ is a Δ_{p^r}-ring for all $1 \leq i \leq d$. We conclude that G_i is a p-group for all $1 \leq i \leq d$. Futhermore, By Theorem 5.14, we know that $\gcd(p, q) = 1$ since we assume that $(p, q) \neq (2, 2)$. Then by Corollary 2.9, $M_d(\mathbb{F}_q)$ is a direct factor of $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$. This shows that $M_d(\mathbb{F}_q)$ is a Δ_{p^r}-ring as well. However, Lemma 5.8 implies that $d = 1$ which is a contradiction. This shows that $(p, q) = (2, 2)$.

From now on, we will assume that $(p, q) = 2$. In particular, this implies that G_i is a 2-group. Suppose that there are exactly t elements amongst G_i which is the trivial group. We claim that $t \leq 1$. In fact, by Theorem 3.15, $M_t(\mathbb{F}_2)$ is a direct factor of $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_2)^{\mathrm{ss}}$ which is a Δ_{p^r}-ring by Lemma 5.3. This shows that $M_t(\mathbb{F}_2)$ is a Δ_{p^r}-ring. By Lemma 5.8, we conclude that $0 \leq t \leq 1$. Finally, the embedding $\mathbb{F}_2[G_i]^\times \hookrightarrow \mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_2)^\times$ explained above implies that

$$2^r \geq \exp(U_1(\mathbb{F}_2[G_i]), \forall 1 \leq i \leq d.$$

In summary, we have proved the "only if" part of the theorem. We now prove the converse. Let us consider the case all G_i are non-trivial 2-groups. Let

$$A = \left[\begin{array}{c|c|c|c} C_1 & a_{12}J & \cdots & a_{1d}J \\ \hline a_{21}J & C_2 & \cdots & a_{2d}J \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline a_{d1}J & a_{d2}J & \cdots & C_d \end{array}\right].$$

be an invertible element in $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_2)$. Then $\epsilon(A)$ is invertible where $\epsilon : \mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q) \to M_d(\mathbb{F}_2)$ is the augmentation map. By definition we have

$$\epsilon(A) = \left[\begin{array}{c|c|c|c} \epsilon(C_1) & 0 & \cdots & 0 \\ \hline 0 & \epsilon(C_2) & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & \epsilon(C_d) \end{array}\right] \in GL_d(\mathbb{F}_2).$$

We conclude that $\epsilon(C_i) = 1$ for all $1 \leq i \leq d$. This implies that C_i is invertible for $1 \leq i \leq d$ since $\mathbb{F}_2[G_i]$ is a local ring with $\Delta_{\mathbb{F}_2}(G_i)$ is the maximal ideal. We then see that

$$A^2 = \left[\begin{array}{c|c|c|c} C_1^2 & 0 & \cdots & 0 \\ \hline 0 & C_2^2 & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & C_d^2 \end{array}\right].$$

Consequently

$$A^{2^r} = \left[\begin{array}{c|c|c|c} C_1^{2^r} & 0 & \cdots & 0 \\ \hline 0 & C_2^{2^r} & \cdots & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & C_d^{2^r} \end{array}\right].$$

Since $\mathbb{F}_2[G_i]$ is a a Δ_{2^r}-ring, we conclude that $C_i^{2^r} = I$. As a result, $A^{2^r} = I$. This shows that $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_2)$ is a Δ_{2^r}-ring. The case there is one $G_i = \{e\}$ can be proved using similar calculations. □

A direct corollary of the above theorem is the following.

Corollary 5.18. *Suppose that $d \geq 2$. Then the join algebra $\mathcal{J}_{G_1,G_2,\ldots,G_d}(k)$ has the diagonal properties iff $\mathcal{J}_{G_1,G_2,\ldots,G_d}(\mathbb{F}_q)$ is $\mathcal{J}_{(\mathbb{Z}/2)^{r_1},(\mathbb{Z}/2)^{r_2},\ldots,(\mathbb{Z}/2)^{r_d}}(\mathbb{F}_2)$ where $r_i \in \mathbb{Z}_{\geq 0}$ and at most one of the r_i is equal to* 0.

References

[1] F. Boesch and R. Tindell. Circulants and their connectivities. *Journal of Graph Theory*, 8(4):487–499, 1984.

[2] R. C. Budzinski, T. T. Nguyen, J. Doan, J. Mináč, T. J. Sejnowski, and L. E. Muller. Geometry unites synchrony, chimeras, and waves in nonlinear oscillator networks. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 32(3):031104, 2022.

[3] J. F. Carlson. *Modules and group algebras*. Birkhäuser, 2012.

[4] C.-Y. Chao. Circulant matrices (philip j. davis). *SIAM Review*, 24(3):356, 1982.

[5] S. K. Chebolu. What is special about the divisors of 24? *Mathematics Magazine*, 85(5):366–372, 2012.

[6] S. K. Chebolu and K. Lockridge. Fields with indecomposable multiplicative groups. *Expositiones Mathematicae*, 34(2):237–242, 2016.

[7] S. K. Chebolu, K. Lockridge, and G. Yamskulna. Characterizations of mersenne and 2-rooted primes. *Finite Fields and Their Applications*, 35:330–351, 2015.

[8] S. K. Chebolu and M. Mayers. What is special about the divisors of 12? *Mathematics Magazine*, 86(2):143–146, 2013.

[9] S. K. Chebolu, J. L. Merzel, J. Mináč, L. Muller, T. T. Nguyen, F. W. Pasini, and N. D. Tân. On the joins of group rings. *Journal of Pure and Applied Algebra*, 227(9):107377, 2023.

[10] P. J. Davis. *Circulant matrices*. American Mathematical Soc., 2013.

[11] J. Doan, J. Mináč, L. Muller, T. T. Nguyen, and F. W. Pasini. Joins of circulant matrices. *Linear Algebra and its Applications*, pages 190–209, 2022.

[12] J. Doan, J. Mináč, L. Muller, T. T. Nguyen, and F. W. Pasini. On the spectrum of the joins of normal matrices and applications. *arXiv e-prints arXiv:2207.04181*, 2022.

[13] B. Elspas and J. Turner. Graphs with circulant adjacency matrices. *Journal of Combinatorial Theory*, 9(3):297–307, 1970.

[14] T. Fukaya. Hasse zeta functions of non-commutative rings. *Journal of Algebra*, 208(1):304–342, 1998.

[15] R. Gupta and M. R. Murty. A remark on Artin's conjecture. *Inventiones mathematicae*, 78(1):127–130, 1984.

[16] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math*, 225:209–220, 1967.

[17] T. Hurley. Group rings and rings of matrices. *Int. J. Pure Appl. Math*, 31(3):319–335, 2006.

[18] D. Johnson. The modular group-ring of a finite p-group. *Proceedings of the American Mathematical Society*, 68(1):19–22, 1978.

[19] S. Kanemitsu and M. Waldschmidt. Matrices of finite abelian groups, finite Fourier transform and codes. *Proc. 6th China-Japan Sem. Number Theory, World Sci. London-Singapore-New Jersey*, pages 90–106, 2013.
[20] D. Kasatkin and V. Nekorkin. Transient circulant clusters in two-population network of Kuramoto oscillators with different rules of coupling adaptation. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 31(7):073112, 2021.
[21] N. Kurokawa. On some euler products, i. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 60(9):335–338, 1984.
[22] N. Kurokawa. Special values of selberg zeta functions. *Contemp. Math*, 83:133–150, 1989.
[23] P. Mihailescu. Primary cyclotomic units and a proof of Catalan's conjecture. 2004.
[24] C. P. Milies, S. K. Sehgal, and S. Sehgal. *An introduction to group rings*, volume 1. Springer Science & Business Media, 2002.
[25] C. P. Milies, S. K. Sehgal, and S. Sehgal. *An introduction to group rings*, volume 1. Springer Science & Business Media, 2002.
[26] I. Murase. Semimagic squares and non-semisimple algebras. *The American Mathematical Monthly*, 64(3):168–173, 1957.
[27] T. T. Nguyen, R. C. Budzinski, J. Doan, F. W. Pasini, J. Mináč, and L. E. Muller. Equilibria in kuramoto oscillator networks: An algebraic approach. *SIAM Journal on Applied Dynamical Systems*, 22(2):802–824, 2023.
[28] T. T. Nguyen, R. C. Budzinski, F. W. Pasini, R. Delabays, J. Mináč, and L. E. Muller. Broadcasting solutions on networked systems of phase oscillators. *Chaos, Solitons & Fractals*, 168:113166, 2023.
[29] D. S. Passman and R. Passman. *Infinite group rings*, volume 6. M. Dekker, 1971.
[30] R. S. Pierce. *Associative algebras*, volume 9 of *Studies in the History of Modern Science*. Springer-Verlag, New York-Berlin, 1982.
[31] P. Ribenboim. Catalan's conjecture. *Séminaire de Philosophie et Mathématiques*, (6):1–11, 1994.
[32] A. Shalev. Lie dimension subgroups, lie nilpotency indices, and the exponent of the group of normalized units. *Journal of the London Mathematical Society*, 2(1):23–36, 1991.
[33] A. Townsend, M. Stillman, and S. H. Strogatz. Dense networks that do not synchronize and sparse ones that do. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 30(8):083142, 2020.

Illinois State University
Email address: schebol@ilstu.edu

Soka University
Email address: jmerzel@soka.edu

University of Western Ontario
Email address: minac@uwo.ca

University of Western Ontario
Email address: tungnt@uchicago.edu

University of Western Ontario
Email address: f.pasini1@campus.unimib.it

Hanoi University of Science and Technology
Email address: tan.nguyenduy@hust.edu.vn