# On $\mathbb{Z}_n \rtimes \mathbb{Z}_2$-Hopf-Galois structures and unit group of some group algebras

A thesis
submitted in partial fulfillment of the requirements
of the degree of

**Doctor of Philosophy**

by

**Namrata Arvind**
ID: 20173544

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH PUNE

April 13, 2023

[1-3]

**Dedicated to Alexandra Elbakyan**

[46]

# Certificate

Certified that the work incorporated in the thesis entitled " *On* $\mathbb{Z}_n \rtimes \mathbb{Z}_2$-*Hopf-Galois structures and unit group of some group algebras*", submitted by *Namrata Arvind* was carried out by the candidate, under my supervision. The work presented here or any part of it has not been included in any other thesis submitted previously for the award of any degree or diploma from any other university or institution.

*Date: April 13, 2023*

*Dr. Manish Mishra*
Thesis Supervisor

# Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that violation of the above will be cause for disciplinary action by the institute and can also, evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

*Date: April 13, 2023*

*Namrata Arvind*
*Roll Number: 20173544*

# Acknowledgements

I would like to begin my acknowledgements by thanking my PhD supervisor Dr. Manish Mishra. Sir(as i call him) has been a source of massive support and encouragement throughout my PhD. Apart from sharing his mathematical knowledge with me he has also been a wonderful friend with whom I could share my problems.

I am greatful to my parents V. Arvind and R. Chitra and my family for consistently believing in me and for being very proud of my achievements.

I would like to thank the faculty members and administration staff of the mathematics department at IISER Pune for all their help and assistance. Particularly, I would like to thank Prof. Anupam Kumar Singh and the printer he had provided to his students.

One of the most important people during my time as a PhD student at IISER Pune has been my colleague and collaborator Dr. Saikat Panja. I am extremely thankful to him for choosing to work with me. Our mathematical discussions in the past three years, both online and offline, have been a great learning period for me.

Getting to do a PhD is a privilege and getting to do it happily is one of the greatest blessings. It is fair to say that I have remained sane and happy during the past five years due to my two closest friends Visakh Narayanan and Sandra Aravind. No matter how tough, frustrating or exhausting my day would be, I always had these two to cheer me up and keep me going.

Next I would like to thank my friends at IISER Pune including Ramya, Hitendra, Ravi, Basudev, Ramandeep, Biswanath, Dhruv, Pranjal, Pavan, Mitesh, Divyashree, Prachi, Tumpa, Darshan, Prashant, Tushar, Ajinkya, Rajeshwari, Dilsha, Mayuresh, Fido, Neetu, Swapna, Poornima, Shreeram, Nazia, Adityan, Arghya and Neeraj.

I am indebted to the badminton court at IISER Pune for giving me a great sense of satisfaction almost every evening. I am grateful to Pune city for loving me and accepting me.

Finally I would like to thank MHRD for funding my research.

# Contents

# Abstract

This thesis is divided in two parts. The first part talks about Hopf-Galois structures on groups of the form $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$. Let $K/F$ be a finite Galois extension of fields with $\mathrm{Gal}(K/F) = \Gamma$. We enumerate the Hopf-Galois structures with Galois group $\Gamma$ of type $G$, where $\Gamma, G$ are groups of the form $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$ when $n$ is odd with radical of $n$ being a Burnside number. These findings have applications in the study of solutions to the Yang-Baxter equations and also give application in the field of Galois module theory.

The second part entails unit groups of some finite semisimple group algebra. This is further divided into two subsections. Firstly we provide the structure of the unit group of $\mathbb{F}_{p^k}(\mathrm{SL}(3,2))$, where $p \geq 11$ is a prime and $\mathrm{SL}(3,2)$ denotes the $3 \times 3$ invertible matrices over $\mathbb{F}_2$. Secondly we give the structure of the unit group of $\mathbb{F}_{p^k}S_n$, where $p > n$ is a prime and $S_n$ denotes the symmetric group on $n$ letters. This provide the complete characterization of the unit group of the group algebra $\mathbb{F}_{p^k}A_6$ for $p \geq 7$, where $A_6$ is the alternating group on 6 letters.

# Chapter 1

# INTRODUCTION

## 1.1 Hopf-Galois structures

The theory of Hopf-Galois structures for separable field extensions has been studied by number theorists under the field of Galois-Module theory. This is closely related to the theory of skew braces.

**Definition 1.1.1.** A left skew brace is a triple $(\Gamma, +, \times)$ ,where $(\Gamma, +), (\Gamma, \times)$ are groups and satisfy

$$a \times (b + c) = (a \times b) + a^{-1} + (a \times c),$$

for all $a, b, c \in \Gamma$.

Skew braces give non-degenerate set theoretic solutions of the Yang-Baxter equation. It initially appeared in the PhD thesis of D. Bachiller and has been studied in [8], [13] et cetera. Skew braces provide group theoretic and ring theoretic methods to understand solutions of the Yang Baxter equations. Solutions to Yang-Baxter equations are studied as part of statistical mechanics and knot theory.

We are interested in enumerating the Hopf-Galois structures when both the Galois group of a given field extension and type of the Hopf-Galois structure is isomorphic to groups of the form $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$ when $n$ is odd with radical of $n$ being a Burnside number. Before we state our main results we give the definition of a Hopf-Galois strucutre and some known results which will help us in our enumaration.

Let $\mathcal{R}$ be a commutative ring with unity. Then $\mathcal{H}$ will be called an $\mathcal{R}$-*Hopf algebra* if there is an $\mathcal{R}$-module homomoprhism $\lambda : \mathcal{H} \to \mathcal{H}$ (the antipode map), which is both an $\mathcal{R}$-algebra and an $\mathcal{R}$-coalgebra antihomomophism such that:

$$\lambda(h \otimes h') = \lambda(h) \otimes \lambda(h'),$$
$$\Delta\lambda(h) = (\lambda \otimes \lambda)\tau\Delta,$$
$$\mu(1 \otimes \lambda)\Delta = i\epsilon = \mu(\lambda \otimes 1)\Delta,$$

where $\Delta$ is the comultiplication map, $\tau$ is the switch map $\tau(h_1 \otimes h_2) = h_2 \otimes h_1$, $i : \mathcal{R} \hookrightarrow \mathcal{H}$ is the unit map and $\epsilon : \mathcal{H} \to \mathcal{R}$ is the counit map.

Now assume that $\mathcal{H}$ is commutative. An $\mathcal{R}$-Hopf algebra $\mathcal{H}$ is called a *finite algebra* if it is finitely generated and a projective $\mathcal{R}$-module. Now if $\mathcal{S}$ is an $\mathcal{R}$-algebra which is an $\mathcal{H}$-module, then $\mathcal{S}$ is called an $\mathcal{H}$*-module algebra* if

$$h(st) = \sum h_{(1)}(s)h_{(2)}(t) \text{ and } h(1) = \epsilon(h)1$$

for all $h \in \mathcal{H}, s, t \in \mathcal{S}$, where $\Delta(h) = \sum\limits_{(h)} h_{(1)} \otimes h_{(2)} \in \mathcal{H} \otimes \mathcal{H}$ according to Sweedler's ([16]) notation and $\epsilon : \mathcal{H} \to \mathcal{R}$ is the co-unit map.

Then $\mathcal{S}$, a finite commutative $\mathcal{R}$-algebra is called an $\mathcal{H}$*-Galois extension* over $\mathcal{R}$ if $\mathcal{S}$ is a left $\mathcal{H}$-module algebra and the $\mathcal{R}$-module homomorphism

$$j : \mathcal{S} \otimes_{\mathcal{R}} \mathcal{H} \to \mathrm{End}_{\mathcal{R}}(\mathcal{S}),$$

given by $j(s \otimes h)(s') = sh(s')$ for $s, s' \in \mathcal{S}, h \in \mathcal{H}$, is an isomorphism. Now we define a Hopf-Galois structure on a Galois field extension. Assume $K/F$ is a finite Galois field extension. An $F$-Hopf algebra $\mathcal{H}$, with an action on $K$ such that $K$ is an $(H)$-module algebra and the action makes $K$ into an $\mathcal{H}$-Galois extension, will be called a *Hopf-Galois structure* on $K/F$.

### 1.1.1 Greither-Pareigis theory [14] and Byott's translation [5]

Given a group $G$ we define the *holomorph* of $G$ as a semidirect product $G \rtimes_\psi \mathrm{Aut}(G)$, where $\psi$ is the identity map. The holomorph of a group $G$ (denoted by $\mathrm{Hol}(G)$) sits inside $\mathrm{Perm}(G)$ (set of permutations on $G$) as follows

$$\mathrm{Hol}(G) = \{\eta \in \mathrm{Perm}(G) : \eta \text{ normalizes } \lambda(G)\},$$

where $\lambda$ is the left regular representation. We also recall that a subgroup $\Lambda \subseteq \mathrm{Perm}(\Omega)$ is called regular if $|\Lambda| = |\Omega|$ and $\Lambda$ acts freely on $\Omega$.

Now we state some results which will help us count the number of Hopf-Galois structures on a given field extension. The following result is due to [14].

**Proposition 1.1.2.** *[10, Theorem 6.8] Let $K/F$ be a Galois extension of fields and $\Gamma = \mathrm{Gal}(K/F)$. Then there is a bijection between Hopf-Galois structures on $K/F$ and regular subgroups $G$ of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, where $\lambda$ is the left regular representation.*

In the proof of the above proposition, given a regular subgroup $G \leq \mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$, the Hopf-Galois structure on $K/F$ corresponding to $G$ is $K[G]^\Gamma$. Here $\Gamma$ acts on $G$ by conjugation inside $\mathrm{Perm}(\Gamma)$ and it acts on $K$ by field automorphism, which induces an action of $\Gamma$ on $K[G]$. This $G$ is called the *type* of the Hopf-Galois extension.

Although Greither-Pareigis theory simplifies the problem of counting the number of Hopf-Galois structure for a given Galois extension, the size of $\mathrm{Perm}(\Gamma)$ is large ($|\Gamma|!$) in general. The next theorem (also known as Byott's translation) further simplifies the problem by considering regular embeddings in $\mathrm{Hol}(G)$, which is comparatively smaller in size. From the proof of [5, Proposition 1] we have the following:

Let $\Gamma$ be a finite group and $G$ be group of order $|\Gamma|$. Then there is a bijection between the following sets:

1. $\{\alpha : G \to \text{Perm}(\Gamma)$ a monomorphism, $\alpha(G)$ is regular$\}$

2. $\{\beta : \Gamma \to \text{Perm}(G)$ a monomorphism $\}$

Let $e(\Gamma, G)$ be the number of regular subgroups in $\text{Perm}(\Gamma)$ isomorphic to $G$ which is normalized by $\lambda(\Gamma)$, i.e. the number of Hopf-Galois structures on $K/F$ of type $G$. Let $e'(\Gamma, G)$ denote the number of subgroups $\Gamma^*$ of $\text{Hol}(G)$ isomorphic to $\Gamma$, such that the stabilizer in $\Gamma^*$ of $e_G$ is trivial. Then we have the following result.

**Theorem 1.1.3.** *[5, See Proposition 1] With the notations as above we have,*

$$e(\Gamma, G) = \frac{|\text{Aut}(\Gamma)|}{|\text{Aut}(G)|} e'(\Gamma, G).$$

Note that $\Gamma^*$ is a regular subgroup of $\text{Hol}(G)$ implies $\Gamma^*$ has the same cardinality as $G$. A typical element of $\text{Hol}(G)$ is of the form $(g, \zeta)$ where $g \in G, \zeta \in \text{Aut}(G)$. Hence to say $\Gamma^*$ is a regular subgroup of $\text{Hol}(G)$ it suffices to check that there is exactly one element $(e_G, \zeta) \in \Gamma^*$ with $\zeta = I$, the identity automorphism. Indeed, if $\Gamma^*$ is not regular, it is neither transitive nor fixed-point free. Therefore, the stabilizer of $e_G$ in $\Gamma^*$ is non-trivial by the orbit-stabilizer theorem, since orbit of $e_G$ has cardinality strictly less than $|G|$. Since $|G| = |\Gamma^*|$, this forces the stabilizer of $e_G$ in $\Gamma^*$ to be a proper subgroup and hence there exists an element $(e_G, \zeta) \in \Gamma^*$ with $\zeta \neq I$. We will use this condition to check regular embeddings of the groups of the form $\mathbb{Z}_n \rtimes \mathbb{Z}_2$.

In [5] the author has proved that if $K/F$ is a finite Galois extension of field of degree $T$, then this extension admits a unique Hopf-Galois structure if and only if $T$ is a Burnside number. Since in our case $n > 1$ is odd and hence $2n$ is not Burnside, the extension has at least 2 Hopf-Galois structures. The number of Hopf-Galois structure for various groups have been studied by E. Campedel et al. [12], T. Kohl [15], Carnahan S. et al [11] et cetera. For an extensive literature review one may look at the PhD thesis of K. N. Zenouz [18]. In [15], T. Kohl has computed $e(G,G)$ when $G$ is a dihedral group. Let $\mathcal{C}_l$ be a cyclic group of order $l$ and $\mathcal{D}_{2k}$ be a dihedral group of order $2k$. For $n$ odd we look at groups of order $2n$ of the form $\mathfrak{M}_{l,k} := \mathcal{C}_l \times \mathcal{D}_{2k}$ where $kl = n, (k,l) = 1$, whenever the radical of $n$ is a Burnside number. Our main result is the following.

**Theorem 1.1.4.** *[1, Theorem 1.3] Let $K/F$ be a Galois extension of fields with $\mathrm{Gal}(K/F) \cong \Gamma$ and $n \in \mathbb{N}$ be odd. If $\Gamma = \mathfrak{M}_{l_1,k_1}$ and $G = \mathfrak{M}_{l_2,k_2}$ where $k_1 l_1 = k_2 l_2 = n$ and $\mathfrak{R}(n)$ is a Burnside number, then the number of Hopf-Galois structure on $K/F$ of type $G$ is given by*

$$e(\Gamma, G) = \boxed{\frac{l_1 l_2}{(l_1, l_2)\mathfrak{R}(l_1)}} \cdot 2^{|\pi(k_2)|}.$$

## 1.2 Unit groups of group algebras

Let $q = p^k$ for some prime $p$ and $k \in \mathbb{N}$. Let $\mathbb{F}_q$ denote the finite field of cardinality $q$. For any group $G$, let $\mathbb{F}_q G$ denotes the group algebra of $G$ over $\mathbb{F}_q$. For basic notations and results on the subject of study, we refer the readers to the classic by Milies and Sehgal [33]. The group of units of $\mathbb{F}_q G$ has many applications. As an application of the unit groups of matrix rings, Hurley has proposed the constructions of convolutional codes (See [24],[25],[26]). The structure of unit group can also be used to deal with some problems in combinatorial number theory as well (See [22]). This has encouraged a lot of researchers to find out the explicit structure of the group of units of $\mathbb{F}_q G$.

A substantial amount of work has been done to find the structure of the algebra $\mathbb{F}_q G$, and also of the group of units of these algebras. For example in [34], the author has described units of $\mathbb{F}_q G$, where $G$ is a $p$-group. In a recent paper [9] the authors have discussed the groups of units for the group algebras over abelian groups of order 17 to 20. Howerver the complexity of the problem increases with increase in the size of the group and the number of conjugacy classes it has. For more, one can check [35],[36] et cetera.

Very little is known for $\mathbb{F}_qG$, when $G$ is a non-Abelian simple group. For the case $G = A_5$, this has been discussed in [31]. The next group in the family of non-Abelian simple groups is the group $\mathrm{SL}(3, 2)$.

The second part of this thesis is further divided into two sub-scetions. In the first subsection we we give a complete description of the unit group of $\mathbb{F}_q\mathrm{SL}(3, 2)$ for $p \geq 11$. In the second we start by investigation of $\mathbb{F}_qS_n$ where $p > n$. This is mainly a consequence of the representation theory of $S_n$ over $\mathbb{C}$ and the connection between the Brauer characters of the group when $p > n$ and the ordinary characters over $\mathbb{C}$. The group of units of the semisimple algebras $\mathbb{F}_qA_5$ and $\mathbb{F}_q\mathrm{SL}(3, 2)$ have been characterized in [31] and in the previous subsection respectively. In this subsection, we look at the next non-Abelian simple group $A_6$, the alternating group on six letters. We give a complete characterization of $\mathbb{F}_qA_6$ for the case $p \geq 7$. Our main result can be summarised in the following two theorems.

**Theorem 1.2.1.** *[2, Theorem 4.4] Let $\mathbb{F}_q$ be a field of characteristic $p$ and $p$ $\geq 11$. Let $G$ be the group $\mathrm{SL}(3, 2)$. Then the unit group $\mathcal{U}(\mathbb{F}_qG)$ is as listed in the following table:*

| $p \mod 7$ | $k$ | $\mathcal{U}(\mathbb{F}_q\mathrm{SL}(3,2))$ |
|---|---|---|
| $\pm1, \pm2, \pm3$ | $6l$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6, \mathbb{F}_q) \oplus \mathrm{GL}(7, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(3, \mathbb{F}_q)^2$ |
| $1, 2, -3$ | $6l + 1$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6, \mathbb{F}_q) \oplus \mathrm{GL}(7, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(3, \mathbb{F}_q)^2$ |
| $-1, -2, 3$ | $6l + 1$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6, \mathbb{F}_q) \oplus \mathrm{GL}(7, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(3, \mathbb{F}_{q^2})$ |
| $\pm1, \pm2, \pm3$ | $6l + 2$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6, \mathbb{F}_q) \oplus \mathrm{GL}(7, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(3, \mathbb{F}_q)^2$ |
| $1, 2, -3$ | $6l + 3$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6, \mathbb{F}_q) \oplus \mathrm{GL}(7, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(3, \mathbb{F}_q)^2$ |
| $-1, -2, 3$ | $6l + 3$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6, \mathbb{F}_q) \oplus \mathrm{GL}(7, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(3, \mathbb{F}_{q^2})$ |
| $\pm1, \pm2, \pm3$ | $6l + 4$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6, \mathbb{F}_q) \oplus \mathrm{GL}(7, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(3, \mathbb{F}_q)^2$ |
| $1, 2, -3$ | $6l + 5$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6, \mathbb{F}_q) \oplus \mathrm{GL}(7, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(3, \mathbb{F}_q)^2$ |
| $-1, -2, 3$ | $6l + 5$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6, \mathbb{F}_q) \oplus \mathrm{GL}(7, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(3, \mathbb{F}_{q^2})$ |

**Theorem 1.2.2.** *[3, Theorem 4.8] Let $\mathbb{F}_{p^k}$ be a field of characteristic $p \geq 7$ and $A_6$ denotes the alternating group on six letters. Then the unit group of the*

*algebra,* $\mathcal{U}(\mathbb{F}_{p^k}A_6)$ *is*

$$\mathbb{F}_q^\times \oplus \mathrm{GL}(5,\mathbb{F}_q) \oplus \mathrm{GL}(5,\mathbb{F}_q) \oplus \mathrm{GL}(9,\mathbb{F}_q) \oplus \mathrm{GL}(10,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_{q^2}), \quad (1.2.1)$$

*when* $p \equiv \pm 2 \mod 5, k \equiv 1 \mod 2$ *and*

$$\mathbb{F}_q^\times \oplus \mathrm{GL}(5,\mathbb{F}_q) \oplus \mathrm{GL}(5,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(9,\mathbb{F}_q) \oplus \mathrm{GL}(10,\mathbb{F}_q), \quad (1.2.2)$$

*otherwise.*

## 1.3 Notations

For $a, b \in \mathbb{Z}$ we will use $(a, b)$ to denote the g.c.d. of $a$ and $b$. For a number $n$, we take $\pi(n) = \{p : p \text{ divides } n, p \text{ prime}\}$. The notation $v_p(n)$, the exponent of the highest power of the prime number $p$ that divides $n$, denotes the $p$-valuation of $n$. For $n \in \mathbb{N}$, the radical of $n$ is defined to be product of the distinct primes in $\pi(n)$, which will be denoted as $\mathfrak{R}(n)$. The symbol $\varphi(n)$ denotes the Euler's totient function at $n \in \mathbb{N}$. A number $n \in \mathbb{N}$ is called a Burnside number if $(n, \varphi(n)) = 1$.

# Chapter 2

# HOPF-GALOIS STRUCTURES

## 2.1 Preliminaries

In this section we give complete description of groups of the form $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ and state some basic number theoretic results which will be used in Section 3 to enumerate the regular embeddings.

### 2.1.1 Groups of the form $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$, $n$ odd

Note that if $n = \prod_{t=1}^{m} p_t^{\alpha_t}$, where $p_i$'s are all distinct primes, then

$$\begin{aligned} \mathbb{Z}_n &\cong \bigoplus_{t=1}^{m} \mathbb{Z}_{p_t^{\alpha_t}}, \\ \text{and } \operatorname{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^* &\cong \prod_{t=1}^{m} \mathbb{Z}_{p_t^{\alpha_t}}^* \\ &\cong \bigoplus_{t=1}^{m} \mathbb{Z}_{p_t^{\alpha_t - 1}(p_t - 1)}. \end{aligned}$$

For $x \in \mathbb{Z}_n$ we have $x = (x_1, x_2, \cdots, x_m)$ where $x_u \in \mathbb{Z}_{p_u^{\alpha_u}}$. We define $p_u(x) = x_u$ for $p_u \in \pi(n)$.

If $\phi : \mathbb{Z}_2 = \{\pm 1\} \to \operatorname{Aut}(\mathbb{Z}_n)$ is a group homomorphism with $p_u(\phi(-1)(x)) =$

$-p_u(x)$ for all $p_u \in \pi(n)$, then $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$ is the dihedral group of order $2n$ and we will denote this group by $\mathfrak{D}$. When $p_u(\phi(-1)(x)) = p_u(x)$ for all $p_u \in \pi(n)$, then $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$ is the cyclic group of order $2n$ and we will denote this group by $\mathfrak{C}$. Now suppose $p_u(\phi(-1)(x)) = p_u(x)$ for some $p_u \in \pi(n)$ and $p_{u'}(\phi(-1)(x)) = -p_{u'}(x)$ for some $p_{u'} \in \pi(n)$, then the group is isomorphic to $\mathcal{D}_{2k} \times \mathcal{C}_l$ for some $k, l \in \mathbb{N}$ with $kl = n$. We denote this group by $\mathfrak{M}_{l,k}$. We have to consider the regular embeddings for the following cases:

1. $\mathfrak{M}_{l_1,k_1} \hookrightarrow \mathrm{Hol}(\mathfrak{M}_{l_2,k_2})$ where $k_1 l_1 = k_2 l_2 = n$ and $(k_1, l_1) = (k_2, l_2) = 1$,

2. $\mathfrak{D} \hookrightarrow \mathrm{Hol}(\mathfrak{M}_{l,k})$ with $k, l > 1$,

3. $\mathfrak{C} \hookrightarrow \mathrm{Hol}(\mathfrak{M}_{l,k})$ with $k, l > 1$,

4. $\mathfrak{D} \hookrightarrow \mathrm{Hol}(\mathfrak{C})$

5. $\mathfrak{C} \hookrightarrow \mathrm{Hol}(\mathfrak{D})$

6. $\mathfrak{M}_{l,k} \hookrightarrow \mathrm{Hol}(\mathfrak{C})$ with $k, l > 1$,

7. $\mathfrak{M}_{l,k} \hookrightarrow \mathrm{Hol}(\mathfrak{D})$ with $k, l > 1$,

8. $\mathfrak{D} \hookrightarrow \mathrm{Hol}(\mathfrak{D})$

9. $\mathfrak{C} \hookrightarrow \mathrm{Hol}(\mathfrak{C})$

While counting the regular embeddings we consider the first case and all other cases are special cases of it. We must mention here that the last two cases have been previously discussed in [15] and [7] respectively and our answers match with the results therein.

## 2.2 Basic results

**Lemma 2.2.1.** *Let $p > 2$ be a prime and $\gamma \equiv 1 \mod p$. Define $f_\gamma(0) = 0$ and for each $\delta \in \mathbb{Z}_{>0}$ define*

$$f_\gamma(\delta) = \sum_{i=0}^{\delta-1} \gamma^i.$$

*Then*

$$f_\gamma(\delta_1) \equiv f_\gamma(\delta_2) \mod p^n \textit{ iff } \delta_1 \equiv \delta_2 \mod p^n.$$

*Proof.* See the proof of Lemma 2.17 in [12]. □

**Corollary 2.2.2.** *Let $p$ be a prime and $b \in \mathbb{Z}$ such that $b^{p^m} \equiv 1 \mod p^n$. Then*

$$p^m | f_b(p^m) \textit{and } p^{m+1} \nmid f_b(p^m).$$

*Proof.* This follows from the observation that $b \equiv 1 \mod p$. □

## 2.3 Regular embeddings and Hopf-Galois structure

We start with a presentation of the group $\mathfrak{M}_{l,k} = \mathcal{C}_l \times \mathcal{D}_{2k}$. It is given by

$$\mathfrak{M}_{l,k} = \left\langle r, s, t : r^k, s^2, t^l, srsr, sts^{-1}t^{-1}, rtr^{-1}t^{-1} \right\rangle.$$

For the rest of the section we assume that $lk = n, (l,k) = 1$ and $\mathfrak{R}(n)$ is a Burnside number. Now observe that $\mathrm{Hol}(\mathcal{C}_l) = \mathrm{Hol}(\mathbb{Z}_l)$ is isomorphic to the matrix group

$$\left\{ \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}_l^*, a \in \mathbb{Z}_l \right\}.$$

From the above representation we conclude that

$$\begin{aligned} \mathrm{Aut}(\mathcal{D}_{2k}) &\cong \left\{ \begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix} : d \in \mathbb{Z}_k^*, c \in \mathbb{Z}_k \right\} \\ \text{where } &\begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix} \cdot r = r^d, \begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix} \cdot s = r^c s, \end{aligned}$$

since $\mathrm{Aut}(\mathcal{D}_{2k}) \cong \mathrm{Hol}(\mathbb{Z}_k)$.

Next note that

$$\mathrm{Hol}(\mathfrak{M}_{l,k}) \cong \mathrm{Hol}(\mathcal{C}_l) \times \mathrm{Hol}(\mathcal{D}_{2k}) \text{ since } (k,l) = 1.$$

Hence from the above discussion, we have

$$\mathrm{Hol}(\mathfrak{M}_{l,k}) \cong \left\{ \left( \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix}, r^i s^j, \begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix} \right) : {\scriptstyle \substack{b \in \mathbb{Z}_l^*, a \in \mathbb{Z}_l, d \in \mathbb{Z}_k^*, c \in \mathbb{Z}_k, \\ 0 \le i \le k-1, j = 0,1}} \right\},$$

where $(r^i s^j, a)$ corresponds to the element of $\mathfrak{M}_{l,k}$.

Now we want to look at the embeddings $\Phi : \mathfrak{M}_{l_1,k_1} \to \mathrm{Hol}(\mathfrak{M}_{l_2,k_2})$. We take

$$\mathfrak{M}_{l_1,k_1} = \left\langle r_1, s_1, t_1 : r_1^{k_1}, s_1^2, t_1^{l_1}, s_1r_1s_1r_1, s_1t_1s_1^{-1}t_1^{-1}, r_1t_1r_1^{-1}t_1^{-1} \right\rangle,$$
$$\mathfrak{M}_{l_2,k_2} = \left\langle r_2, s_2, t_2 : r_2^{k_2}, s_2^2, t_2^{l_2}, s_2r_2s_2r_2, s_2t_2s_2^{-1}t_2^{-1}, r_2t_2r_2^{-1}t_2^{-1} \right\rangle.$$

Let us assume that

$$\Phi(r_1) = \left( \begin{pmatrix} b & a \\ 0 & 1 \end{pmatrix}, r_2^i s_2^j, \begin{pmatrix} d & c \\ 0 & 1 \end{pmatrix} \right),$$
$$\Phi(s_1) = \left( \begin{pmatrix} b' & a' \\ 0 & 1 \end{pmatrix}, r_2^{i'} s_2^{j'}, \begin{pmatrix} d' & c' \\ 0 & 1 \end{pmatrix} \right),$$
$$\Phi(t_1) = \left( \begin{pmatrix} b'' & a'' \\ 0 & 1 \end{pmatrix}, r_2^{i''} s_2^{j''}, \begin{pmatrix} d'' & c'' \\ 0 & 1 \end{pmatrix} \right).$$

We define the set $\mathfrak{V} = \{a, b, i, j, c, d, a', b', i', j', c', d', a'', b'', i'', j'', c'', d''\}$ and refer to the elements of the set as variables. Note that we can consider the element $a \in \mathbb{Z}_{l_2}$ (resp. $b \in \mathbb{Z}_{l_2}^*$) to be an element of $\mathbb{Z}_n$ (resp. $\mathbb{Z}_n^*$) by setting $p_u(a) = 0$ (resp. $p_u(b) = 1$) for all $p_u \in \pi(n) \setminus \pi(l_2)$. The same treatment will be applicable to all variables in $\mathfrak{V}$ accordingly. We observe that $N = (k_1, l_2)(l_1, l_2)(k_1, k_2)(l_1, k_2)$ and the four entities in the right are mutually coprime. Thus it is enough to count the total number of possibilities of the variables in each of $\mathbb{Z}_\beta$, where $\beta \in \{(k_1, l_2), (l_1, l_2), (k_1, k_2), (l_1, k_2)\}$. Now we look at the embeddings of the groups inside the holomorph. We will encounter several equations in this context. Since $\Phi$ is a homomorphism, we have the following relations:

$$
\begin{aligned}
\Phi(r_1)^{k_1} &= e_0 \\
\Phi(s_1)^2 &= e_0 \\
\Phi(t_1)^{l_1} &= e_0 \\
\Phi(s_1)\Phi(r_1)\Phi(s_1)\Phi(r_1) &= e_0 \\
\Phi(r_1)\Phi(t_1) &= \Phi(t_1)\Phi(r_1) \\
\Phi(s_1)\Phi(t_1) &= \Phi(t_1)\Phi(s_1),
\end{aligned}
$$

where

$$e_0 = \left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, r_2^0 s_2^0, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

is the identity element of $\mathrm{Hol}(\mathfrak{M}_{l_2,k_2})$. First we observe that if $j = 1$, then $\Phi(r_1)$ has even order. Indeed

$$
\begin{aligned}
\Phi(r_1)^2 &= \left( \begin{pmatrix} b^2 & a(1+b) \\ 0 & 1 \end{pmatrix}, r_2^{i(1-d)-c}, \begin{pmatrix} d^2 & c(1+d) \\ 0 & 1 \end{pmatrix} \right) \\
\implies \Phi(r_1)^{2m+1} &= \left( \begin{pmatrix} b^{2m+1} & a(1+b+\cdots+b^{2m}) \\ 0 & 1 \end{pmatrix}, r_2^{\bar{i}} s, \begin{pmatrix} d^{2m+1} & c(1+d+\cdots+d^{2m}) \\ 0 & 1 \end{pmatrix} \right).
\end{aligned}
$$

Since $k_1$ is odd, this possibility does not arise. Thus $j = 0$. Similarly we can conclude that $j'' = 0$, since $l_1$ is odd. Using $\Phi(r_1)^{k_1} = e_0$ we have

$$
\begin{aligned}
&\left( \begin{pmatrix} b^{k_1} & a(1+b+\cdots+b^{k_1-1}) \\ 0 & 1 \end{pmatrix}, r_2^{i(1+d+\cdots+d^{k_1-1})} s, \begin{pmatrix} d^{k_1} & c(1+d+\cdots+d^{k_1-1}) \\ 0 & 1 \end{pmatrix} \right) \\
&= \left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, r_2^0 s_2^0, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right),
\end{aligned}
$$

which implies that

$$b^{k_1} = 1 \mod l_2 \tag{2.3.1}$$
$$a(1 + b + \cdots + b^{k_1 - 1}) = 0 \mod l_2 \tag{2.3.2}$$
$$i(1 + d + \cdots + d^{k_1 - 1}) = 0 \mod k_2 \tag{2.3.3}$$
$$d^{k_1} = 1 \mod k_2 \tag{2.3.4}$$
$$c(1 + d + \cdots + d^{k_1 - 1}) = 0 \mod k_2. \tag{2.3.5}$$

Using $\Phi(t_1)^{l_1} = e_0$ we get that

$$(b'')^{l_1} = 1 \mod l_2 \tag{2.3.6}$$
$$a''(1 + b'' + \cdots + (b'')^{l_1 - 1}) = 0 \mod l_2 \tag{2.3.7}$$
$$i''(1 + d'' + \cdots + (d'')^{l_1 - 1}) = 0 \mod k_2 \tag{2.3.8}$$
$$(d'')^{l_1} = 1 \mod k_2 \tag{2.3.9}$$
$$c''(1 + d'' + \cdots + (d'')^{l_1 - 1}) = 0 \mod k_2. \tag{2.3.10}$$

Using $\Phi(r_1)\Phi(t_1) = \Phi(t_1)\Phi(r_1)$ we get that

$$a(1 - b'') = 0 \mod l_2 \tag{2.3.11}$$
$$i(1 - d'') = 0 \mod k_2 \tag{2.3.12}$$
$$c(1 - d'') = 0 \mod k_2. \tag{2.3.13}$$

Now we divide the set of equations in two parts considering $j' = 0$ and $j' = 1$.

### 2.3.1 Case 1: $j' = 0$.

Using $\Phi(s_1)^2 = e_0$ we have

$$(b')^2 = 1 \mod l_2 \tag{2.3.14}$$
$$a'(1+b') = 0 \mod l_2 \tag{2.3.15}$$
$$(d')^2 = 1 \mod k_2 \tag{2.3.16}$$
$$c'(1+d') = 0 \mod k_2 \tag{2.3.17}$$
$$i'(1+d') = 0 \mod k_2. \tag{2.3.18}$$

Using $\Phi(s_1)\Phi(r_1)\Phi(s_1)\Phi(r_1) = e_0$ we have

$$b^2 = 1 \mod l_2 \tag{2.3.19}$$
$$a(b+b') + a'(1+bb') = 0 \mod l_2 \tag{2.3.20}$$
$$(i+i')(1+d') = 0 \mod k_2 \tag{2.3.21}$$
$$d^2 = 1 \mod k_2 \tag{2.3.22}$$
$$c(d+d') + c'(1+dd') = 0 \mod k_2 \tag{2.3.23}$$

Note that $b = 1$ by equations 2.3.1 and 2.3.19, $d = 1$ by equations 2.3.4 and 2.3.22, since $(2, k_1) = 1$.

Using $\Phi(s_1)\Phi(t_1) = \Phi(t_1)\Phi(s_1)$ we have

$$a''(1-b') = a'(1-b'') \mod l_2 \tag{2.3.24}$$
$$i''(1-d') = i'(1-d'') \mod k_2 \tag{2.3.25}$$
$$c''(1-d') = c'(1-d'') \mod k_2. \tag{2.3.26}$$

### 2.3.2 Case 2: $j' = 1$.

Using $\Phi(s_1)^2 = e_0$ we have

$$(b')^2 = 1 \mod l_2 \tag{2.3.27}$$
$$a'(1+b') = 0 \mod l_2 \tag{2.3.28}$$
$$(d')^2 = 1 \mod k_2 \tag{2.3.29}$$
$$c'(1+d') = 0 \mod k_2 \tag{2.3.30}$$
$$i'(1-d') = c' \mod k_2. \tag{2.3.31}$$

Using $\Phi(s_1)\Phi(r_1)\Phi(s_1)\Phi(r_1) = e_0$ we have

$$b^2 = 1 \mod l_2 \tag{2.3.32}$$
$$a(b+b') + a'(1+bb') = 0 \mod l_2 \tag{2.3.33}$$
$$(i+i')(1-d') = d'c + c' \mod k_2 \tag{2.3.34}$$
$$d^2 = 1 \mod l_2 \tag{2.3.35}$$
$$c(d+d') + c'(1+dd') = 0 \mod l_2 \tag{2.3.36}$$

Note that $b = 1, d = 1$ by similar reasons as before.

Using $\Phi(s_1)\Phi(t_1) = \Phi(t_1)\Phi(s_1)$ we have

$$a''(1-b') = a'(1-b'') \mod l_2 \tag{2.3.37}$$
$$i' - i''d' = i'' + i'd'' + c'' \mod k_2 \tag{2.3.38}$$
$$c''(1-d') = c'(1-d'') \mod k_2. \tag{2.3.39}$$

## 2.4 Embeddings

We already have that $p_u(b) = 1$ and $p_u(d) = 1$ for all $p_u \in \pi(n)$. Since $|r_1| = k_1$ we get that $p_u(a)$ is a unit whenever $p_u \in \pi((k_1, l_2))$ and 0 for other primes (this is equivalent to saying $|a| = (k_1, l_2)$). Similarly

1. $p_u(i)$ is a unit for $p_u \in \pi((k_1, k_2))$ and 0 otherwise,

2. $p_u(c) = 0$ whenever $p_u \in \pi(n) \setminus \pi((k_1, k_2))$,

3. $p_u(i'')$ is a unit for $p_u \in \pi((l_1, k_2))$ and 0 otherwise,

4. $p_u(a'')$ is a unit for $p_u \in \pi((l_1, l_2))$ and 0 otherwise.

Point (3) and (4) follows from corollary 2.2.2. From equations 2.3.1 and 2.3.19 we have that $p_u(b) = 1$ for all $p_u \in \pi(n)$. In each of these following cases we only determine the coefficients of the variables for the primes relevant to that case.

**Case I: Inside $\mathbb{Z}_{(k_1,l_2)}$.** Using equations 2.3.15, 2.3.20 and $b = 1$, we have that $a(1 + b') = 0$ thus $p_u(b') = -1$ for $p_u \in \pi((k_1, l_2))$. Referring to equation 2.3.11 and $p_u(a)$ is a unit for $p_u \in \pi((k_1, l_2))$ we have that $p_u(b'') = 1$ for $p_u \in \pi(k_1, l_2)$. Using equation 2.3.37 we have $p_u(a'') = 0$ for all $p_u \in \pi((k_1, l_2))$ (since $(2, p_u) = 1$). All other variables have one possibility since $k_2$ is coprime to $(k_1, l_2)$. Hence

1. $a$ has $\varphi(k_1, l_2)$ possibilities,

2. $a'$ has $(k_1, l_2)$ possibilities.

**Case II: Inside $\mathbb{Z}_{(l_1,l_2)}$.** Here $p_u(a) = 0$ for all $p_u \in \pi((l_1, l_2))$. Using equation 2.3.14 (equiv. 2.3.27) we have $p_u(b') = \pm 1$ for all $p_u \in \pi((l_1, l_2))$. Considering equation 2.3.24 (equiv. 2.3.37) and that $1-p_u(b'')$ is a zero divisor for $p_u \in \pi((l_1, l_2))$, using equation 2.3.15 (equiv. 2.3.28) we get $p_u(b') = 1$ which implies that $p_u(a') = 0$ in this case. Since $\mathfrak{R}(n)$ is a Burnside number, from equation 2.3.6 we have that

$$p_u(b'')^{p_u^{\alpha_u - 1}} = 1 \text{ for all } p_u. \tag{2.4.1}$$

Hence

1. $(a', b')$ has 1 possibility,

2. $a''$ has $\varphi(l_1, l_2)$ possibilities,

3. $b''$ has $\dfrac{(l_1, l_2)}{\mathfrak{R}((l_1, l_2))}$ possibilities.

**Remark 2.4.1.** Note that the above two cases do not depend on $j'$.

**Case III: Inside $\mathbb{Z}_{(k_1,k_2)}$ ($j' = 0$).** We have $p_u((i))$ is a unit for all $p_u \in \pi((k_1, k_2))$. Combining equations 2.3.18 and 2.3.21 we have $p_u(d') = -1$ for all $p_u \in \pi((k_1, k_2))$. Since $(k_1, k_2)$ is coprime to $l_1$ and $\mathfrak{R}(n)$ is a Burnside number, using equation 2.3.9 we conclude that $p_u(d'') = 1$ for all $p_u \in \pi((k_1, k_2))$. This implies that $p_u(i'') = p_u(c'') = 0$ for all $p_u \in \pi((k_1, k_2))$, since $(l_1, (k_1, k_2)) = 1$. Hence

1. $i$ has $\varphi((k_1, k_2))$ possibilities,

2. each of $c, i', c'$ has $(k_1, k_2)$ possibilities.

**Case IV: Inside $\mathbb{Z}_{(l_1,k_2)}$ ($j' = 0$).** We have $p_u(i) = p_u(c) = 0$ for all $p_u \in \pi((l_1, k_2))$. Note that $p_u(d') = \pm 1$ for all $p_u \in \pi((l_1, k_2))$. Using equation 2.3.25 we have

$$p_u(i'')(1 - p_u(d')) = p_u(i')(1 - p_u(d'')) \mod p_u^{\alpha_u} \text{ for all } p_u \in \pi((l_1, k_2)).$$

Then $p_u(d') = -1$ for some $p_u \in \pi((l_1, k_2))$ implies that

$$2p_u(i'') = p_u(i')(1 - p_u(d'')) \mod p_u^{\alpha_u} \text{ for all } p_u \in \pi((l_1, k_2)).$$

Since $2p_u(i'')$ is a unit and $1 - p_u(d'')$ ($\neq 0$) is a zero divisor, this case does not arise. Hence we get that $p_u(d') = 1$ for all $p_u \in \pi((l_1, k_2))$. This implies that $p_u(i') = p_u(c') = 0$ for all $p_u \in \pi((l_1, k_2))$. Similar to equation 2.4.1 $p_u(d'')^{p_u^{\alpha_u - 1}} = 1$ for all $p_u \in \pi((l_1, k_2))$, since $\mathfrak{R}(n)$ is Burnside. Hence

1. $i''$ has $\varphi((l_1, k_2))$ possibilities,

2. $c''$ has $(l_1, k_2)$ possibilities,

3. $d''$ has $\dfrac{(l_1, k_2)}{\mathfrak{R}((l_1, k_2))}$ possibilities.

**Case V: Inside $\mathbb{Z}_{(k_1,k_2)}$ ($j' = 1$).** We have $p_u(d'') = 1, p_u(c'') = p_u(i'') = 0$ for all $p_u \in \pi((k_1, k_2))$ (as in Case III). Note that $p_u(d') = \pm 1$ for all $p_u \in \pi((k_1, k_2))$. First let us assume that $p_u(d') = 1$ for some $p_u$. Then $p_u(c') = 0$ and hence $i'' \in \mathbb{Z}_{p_u^{\alpha_u}}$. Using equation 2.3.36 we conclude that $p_u(c) = 0$.

Next, if $p_u(d') = -1$ for some $p_u$, using equation 2.3.34

$$p_u(c') = 2p_u(i') \mod p_u^{\alpha_u}.$$

Also combining equations 2.3.31, 2.3.34 we get that $2p_u(i) = -p_u(c)$. Hence

1. $i$ has $\varphi((k_1, k_2))$ possibilities,

2. $(d', i')$ has $2^{|\pi((k_1,k_2))|}(k_1, k_2)$ possibilities.

**Case VI: Inside $\mathbb{Z}_{(l_1,k_2)}$ ($j' = 1$).** We have $p_u(i) = p_u(c) = 0$ for all $p_u \in \pi((l_1, k_2))$. Let us assume that $p_u(d') = 1$ for some $p_u \in \pi((l_1, k_2))$. Then $p_u(c') = 0$. Then using equation 2.3.38 we have

$$p_u(i')(1 - p_u(d'')) = 2p_u(i'') + p_u(c'') \mod p_u^{\alpha_u}.$$

On the other hand if $p_u(d') = -1$ for some $p_u \in \pi((l_1, k_2))$ we get that $p_u(c') = 2p_u(i')$ and using equation 2.3.38 we get

$$p_u(i')(1 - p_u(d'')) = p_u(c'') \mod p_u^{\alpha_u}.$$

Hence in either of the cases $p_u(c'), p_u(c'')$ get fixed by $p_u(d'), p_u(i')$. Hence

1. $(d', i')$ has $2^{|\pi((l_1,k_2))|}(l_1, k_2)$ possibilities,

2. $i''$ has $\varphi((l_1, k_2))$ possibilities (as in Case IV),

3. $d''$ has $\dfrac{(l_1, k_2)}{\mathfrak{R}((l_1, k_2))}$ possibilities (as in Case IV).

## 2.5 Regularity

Now we check for the regularity of these groups. Note that any element $\sigma$ in the image of $\Phi$ is of the form

$$\left(\begin{pmatrix}\widetilde{b} & \widetilde{a}\\ 0 & 1\end{pmatrix}, r_2^{\widetilde{i}}s_2^{\widetilde{j}}, \begin{pmatrix}\widetilde{d} & \widetilde{c}\\ 0 & 1\end{pmatrix}\right).$$

Since $\Phi$ is a homomorphism, this element corresponds to some $\Phi(r_1)^{\lambda}\Phi(s_1)^{\lambda'}\Phi(t_1)^{\lambda''}$, where $0 \leq \lambda \leq l_1 - 1, 0 \leq \lambda' \leq 1, 0 \leq \lambda'' \leq k_1 - 1$. First we consider the case when $j' = 0$. Note that in this case

$$\begin{aligned}
&\Phi(r_1)^{\lambda}\Phi(s_1)\\
&= \left(\begin{pmatrix}1 & \lambda a\\ 0 & 1\end{pmatrix}, r_2^{\lambda i}, \begin{pmatrix}1 & \lambda c\\ 0 & 1\end{pmatrix}\right)\left(\begin{pmatrix}b' & a'\\ 0 & 1\end{pmatrix}, r_2^{i'}, \begin{pmatrix}d' & c'\\ 0 & 1\end{pmatrix}\right)\\
&= \left(\begin{pmatrix}b' & \lambda a + a'\\ 0 & 1\end{pmatrix}, r_2^{\lambda i + i'}, \begin{pmatrix}d' & \lambda c + c'\\ 0 & 1\end{pmatrix}\right).
\end{aligned}$$

By the Chinese Remainder theorem, there exists $0 < \lambda < k_1$, such that $\lambda a + a' = 0 \mod (k_1, l_2)$ and $\lambda i + i' = 0 \mod (k_1, k_2)$. Also we have

$$p_u(b') = \begin{cases} -1 & \text{for all } p_u \in \pi((k_1, l_2))\\ 1 & \text{for all } p_u \in \pi((l_1, l_2))\end{cases},$$

$$p_u(d') = \begin{cases} -1 & \text{for all } p_u \in \pi((k_1, k_2))\\ 1 & \text{for all } p_u \in \pi((l_1, k_2))\end{cases},$$

since for any such $0 < \lambda < k_1$ the element $\Phi(r_1)^{\lambda}\Phi(s_1)$ is non-trivial. Hence the group generated in this case is not regular. Thus $j' = 0$ is not possible.

In case $j' = 1$, any term of the form $\Phi(r_1)^{\lambda}\Phi(s_1)\Phi(t_1)^{\lambda''}$ is an element of a regular subgroup. Hence to check regularity we need to consider the terms

$\Phi(r_1)^\lambda \Phi(t_1)^{\lambda''}$ with $\widetilde{a} = 0, \widetilde{i} = 0$. We have,

$$\begin{aligned} a''(1 + b'' + \cdots + (b'')^{\lambda''-1}) &= -\lambda a \mod l_2 \\ i''(1 + d'' + \cdots + (d'')^{\lambda''-1}) &= -\lambda i \mod k_2. \end{aligned}$$

Since $p_u(i'') = 0$ and $p_u(i)$ is a unit for all $p_u \in \pi((k_1, k_2))$, we get that $p_u(\lambda) = 0$ therein. One can also check that $p_u(\lambda) = 0$ for all $p_u \in \pi((k_1, l_2))$. Hence $\lambda = 0$. Similar as before, using corollary 2.2.2, we have $\lambda'' = 0$.

**Proposition 2.5.1.** *If $\Gamma = \mathfrak{M}_{l_1,k_1}$ and $G = \mathfrak{M}_{l_2,k_2}$, where $k_1 l_1 = k_2 l_2 = n$ is an odd number and $\mathfrak{R}(n)$ is a Burnside number then*

$$e'(\mathfrak{M}_{l_1,k_1}, \mathfrak{M}_{l_2,k_2}) = \frac{l_1 n}{k_1 (l_1, l_2) \mathfrak{R}(l_1)} \cdot 2^{|\pi(k_2)|}.$$

*Proof.* From the above discussion it is evident that $j' = 1$. Thus to determine the total number of regular embeddings we have to multiply the number of possibilities obtained in Cases **I,II,V,VI** and divide it by $\mathrm{Aut}(\Gamma)$. Indeed, if $\Phi_1(\Gamma) = \Phi_2(\Gamma)$ for two different embeddings $\Phi_1, \Phi_2$ then $\Phi_1^{-1}\Phi_2$ is an automorphism of $\Gamma$. Also if $\xi$ is an automorphism of $\Phi(\Gamma)$, then $\xi\Phi$ is also a regular embedding of $\Gamma$. Hence

$$\begin{aligned} & e'(\mathfrak{M}_{l_1,k_1}, \mathfrak{M}_{l_2,k_2}) \\ =& \frac{\varphi((k_1, l_2))(k_1, l_2)\varphi((l_1, l_2))(l_1, l_2)\varphi(k_1, k_2)2^{|\pi((k_1,k_2))|}(k_1, k_2)2^{|\pi((l_1,k_2))|}(l_1, k_2)^2\varphi(l_1, k_2)}{\mathfrak{R}((l_1, l_2))|\mathrm{Aut}(\mathfrak{M}_{l_1,k_1})|\mathfrak{R}((l_1, k_2))} \\ =& \frac{\varphi(n)(l_1, k_2)n2^{|\pi(k_2)|}}{\mathfrak{R}(l_1)|\mathrm{Aut}(\mathfrak{M}_{l_1,k_1})|} \\ =& \frac{\varphi(n)(l_1, k_2)n2^{|\pi(k_2)|}}{\mathfrak{R}(l_1)\varphi(n)k_1} \\ =& \frac{l_1(l_1, k_2)2^{|\pi(k_2)|}}{\mathfrak{R}(l_1)} \\ =& \frac{l_1 n}{k_1(l_1, l_2)\mathfrak{R}(l_1)} \cdot 2^{|\pi(k_2)|}. \end{aligned}$$

The last equality is obvious and this finishes the proof. □

***Proof of Theorem 1.1.4.*** Using Lemma 1.1.3, we have that

$$
\begin{aligned}
&e(\mathfrak{M}_{l_1,k_1}, \mathfrak{M}_{l_2,k_2})\\
=&\frac{\mathrm{Aut}(\mathfrak{M}_{l_1,k_1})}{\mathfrak{M}_{l_2,k_2}} e'(\mathfrak{M}_{l_1,k_1}, \mathfrak{M}_{l_2,k_2})\\
=&\frac{l_1 l_2}{(l_1, l_2)\mathfrak{R}(l_1)} \cdot 2^{|\pi(k_2)|}.
\end{aligned}
$$

□

**Remark 2.5.2.** If $l_1 = 1$ i.e. when $\mathfrak{M}_{l_1,k_1} \cong \mathcal{D}_{2n}$, the assumption that $\mathfrak{R}(n)$ is a Burnside number is not necessary.

## 2.6 Further results

### 2.6.1 Non-classical Dihedral Hopf-Galois structures

**Corollary 2.6.1.** *Let $L/K$ be a finite Galois extension with Galois group isomorphic to $\mathcal{D}_{2n}$ where $n$ is odd. Then the number of Hopf-Galois structures on $L/K$ is at least*

$$\sum_{m=0}^{n} 2^m \chi(n-m),$$

*where $\chi(w)$ is the coefficient of $x^w$ in the polynomial $\prod_{p_u \in \pi(n)} (x + p_u^{\alpha_u})$.*

*Proof.* Firstly assume that $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$. Next consider all the groups of the form $\mathfrak{M}_{l,k}$ where $lk = n, (l,k) = 1$. Then by theorem 1.1.4

$$e(\mathcal{D}_{2n}, \mathcal{C}_l \times \mathcal{D}_{2k}) = l2^{|\pi(k)|}.$$

Hence the number of Hopf-Galois structure on $L/K$ with Galois group $\mathcal{D}_{2n}$,

$$\begin{aligned} e(\mathcal{D}_{2n}) &\geq \sum_{(l,k)=1, lk=n} e(\mathcal{D}_{2n}, \mathfrak{M}_{l,k}) \\ &= \sum_{(l,k)=1, lk=n} l2^{|\pi(k)|} \\ &= 2^t + 2^{t-1} \left( \sum_{i=1}^{t} p_i^{\alpha_i} \right) + 2^{t-1} \left( \sum_{i \neq j} p_i^{\alpha_i} p_j^{\alpha_j} \right) + \dots + n \\ &= \sum_{m=0}^{n} 2^m \chi(n-m), \end{aligned}$$

where $\chi(w)$ is the coefficient of $x^w$ in the polynomial $\prod_{p_u \in \pi(n)} (x + p_u^{\alpha_u})$. $\square$

Now consider the group $\mathcal{C}_l \times \mathcal{D}_{2k}$, where $kl = n, (k,l) \neq 1$. We show that $\mathcal{D}_{2n} \not\hookrightarrow \mathrm{Hol}(\mathcal{C}_l \times \mathcal{D}_{2k})$, where $n$ is odd. We will need the following lemma.

**Lemma 2.6.2.** *[6, Theorem 3.2] Let $G = H \times K$, where $H$ and $K$ have no common direct factor. Then*

$$\mathrm{Aut}(G) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \middle| \begin{array}{cc} A \in \mathrm{Aut}(H), & B \in \mathrm{Hom}(K, Z(H)), \\ C \in \mathrm{Hom}(H, Z(K)), & D \in \mathrm{Aut}(K), \end{array} \right\}.$$

**Corollary 2.6.3.** *If $kl = n$ is odd and $(k,l) \neq 1$, then the group $\mathrm{Hol}(\mathcal{C}_l \times \mathcal{D}_{2k})$ does not have any element of order $p^{v_p(n)}$ for $p|(k,l)$.*

*Proof.* Setting $H = \mathcal{C}_l, K = \mathcal{D}_{2k}$, we observe that

1. $\mathrm{Hom}(K, Z(H)) = 1$. Indeed $Z(H) = \mathcal{C}_l$ is a group of odd order, it has no element of order 2,
2. $\mathrm{Hom}(H, Z(K)) = 1$ since $Z(K)$ is trivial.

This along with Lemma 2.6.2 implies that $\mathrm{Aut}(\mathcal{C}_l \times \mathcal{D}_{2k}) = \mathrm{Aut}(\mathcal{C}_l) \times \mathrm{Aut}(\mathcal{D}_{2k})$. Hence

$$\begin{aligned} \mathrm{Hol}(\mathcal{C}_l \times \mathcal{D}_{2k}) &= \mathcal{C}_l \times \mathcal{D}_{2k} \rtimes_{id} \mathrm{Aut}(\mathcal{C}_l \times \mathcal{D}_{2k}) \\ &\cong \mathrm{Hol}(\mathcal{D}_{2k}) \times \mathrm{Hol}(\mathcal{C}_l). \end{aligned}$$

Since none of $\mathrm{Hol}(\mathcal{D}_{2k}), \mathrm{Hol}(\mathcal{C}_l)$ has elements of order $p^{v_p(n)}$, the result follows. □

**Corollary 2.6.4.** *If $n$ is odd, then $e(\mathcal{D}_{2n}, \mathcal{C}_l \times \mathcal{D}_{2k}) = 0$, whenever $(k,l) \neq 1$.*

**Corollary 2.6.5.** *If $(\Gamma, +) \cong \mathfrak{M}_{l_1,k_1}$ and $(\Gamma, \times) \cong \mathfrak{M}_{l_2,k_2}$, where $k_1 l_1 = k_2 l_2 = n$ is an odd number and $\mathfrak{R}(n)$ is a Burnside number then the number of skew braces of the form $(\Gamma, +, \times)$ is given by*

$$\frac{l_1 n}{k_1 (l_1, l_2) \mathfrak{R}(l_1)} \cdot 2^{|\pi(k_2)|}.$$

*Proof.* Follows from Proposition 2.5.1. □

## 2.7 Future plan

### 2.7.1 Realizability problem

What is the realizability problem ?

It says given any two finite groups $G, N$ of the same order, does there exist a Hopf-Galois structure with Galois group isomorphic to $G$ and the type of the Hopf-Galois structure isomorphic to $N$. If it exists then we say the pair $(G, N)$ is Hopf-Galois realizable. In the language of skew braces a pair $(G, N)$ is called (skew brace) realizable if there exits a skew brace with additive group isomorphic to $N$ and the multiplicative group isomorphic to $G$. Since a pair $(G, N)$ being Hopf-Galois is makes the pair Skew brace realizable, from now on we will just say a pair is realizable.

In this chapter we enumerated the Hopf-Galois structures when both $G$ and $N$ are groups isomorphic to $\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$ whenever radical of $n$ is a burnside number. In [4] the authors have solved the realizability problem in this case. In future we are interested in checking for realizability of pairs of groups $(G, N)$ whenever $N$ is isomorphic to the following:

- $GL(n, q)$
- a non-abelian finite simple group
- a quasi-simple group.

# Chapter 3

# UNIT GROUPS OF GROUP ALGEBRAS

## 3.1 Preliminaries

We start by fixing some notations. Already mentioned notations from section 1 are adopted. For a field extension $E/\mathbb{F}_q$, $\mathrm{Gal}(E/\mathbb{F}_q)$ will denote the Galois group of the extension. For $m \in \mathbb{N}$, the notation $\mathrm{M}(m, R)$ denotes the ring of $m \times m$ matrices over $R$ and $\mathrm{GL}(m, R)$ will denote the set of all invertible matrices in $\mathrm{M}(m, R)$. For a ring $R$, the set of units of $R$ will be denoted by $R^{\times}$. Let $Z(R)$ and $J(R)$ denote the center and the Jacobson radical respectively. If $G$ is a group and $x \in G$, then $[x]$ will denote the conjugacy class of $x$ in $G$. For the group ring $\mathbb{F}_qG$, the group of units will be denoted as $\mathcal{U}(\mathbb{F}_qG)$. For the notations on projective spaces, we follow [23].

We say an element $g \in G$ is a $p'$-element if the order of $g$ is not divisible by $p$. Let $e$ be the exponent of the group $G$ and $\eta$ be a primitive $r$th root of unity, where $e = p^f r$ and $p \nmid r$. Let

$$I_{\mathbb{F}_q} = \left\{ l \pmod{e} : \text{ there exists } \sigma \in \mathrm{Gal}(\mathbb{F}_q(\eta)/\mathbb{F}_q) \text{ satisfying } \sigma(\eta) = \eta^l \right\}.$$

**Definition 3.1.1.** For a $p'$-element $g \in G$, the cyclotomic $\mathbb{F}_q$-class of $g$, denoted by $S_{\mathbb{F}_q}(\gamma_g)$, is defined as $\{\gamma_{g^l} : l \in I_{\mathbb{F}_q}\}$, where $\gamma_{g^l} \in \mathbb{F}_q G$ is the sum of all conjugates of $g^l$ in $G$.

Then we have the following results, which are crucial in determining the Artin-Wedderburn decomposition of $\mathbb{F}_q G$.

**Lemma 3.1.2.** *[20, Proposition 1.2] The number of simple components of $\mathbb{F}_q G/J(\mathbb{F}_q G)$ is equal to the number of cyclotomic $\mathbb{F}_q$-classes in $G$.*

**Definition 3.1.3.** Let $\pi$ be a representation of a group $G$ over a field $F$. $\pi$ is said to be absolutely irreducible if $\pi^E$ is irreducible for every field $F \subseteq E$, where $\pi^E$ is the representation $\pi \otimes E$ over $E$.

**Definition 3.1.4.** A field $F$ is a splitting field for $G$ if every irreducible representation of $G$ over $F$ is absolutely irreducible.

**Lemma 3.1.5.** *[20, Theorem 1.3] Let $n$ be the number of cyclotomic $\mathbb{F}_q$-classes in $G$. If $L_1, L_2, \cdots, L_n$ are the simple components of $Z(\mathbb{F}_q G/J(\mathbb{F}_q G))$ and $S_1, S_2, \cdots, S_n$ are the cyclotomic $\mathbb{F}_q$-classes of $G$, then with a suitable reordering of the indices,*

$$|S_i| = [L_i : \mathbb{F}_q].$$

**Lemma 3.1.6.** *[30, Lemma 2.5] Let $K$ be a field of characteristic $p$ and let $A_1$, $A_2$ be two finite dimensional $K$-algebras. Assume $A_1$ to be semisimple. If $g : A_2 \longrightarrow A_1$ is a surjective homomorphism of $K$-algebras, then there exists a semisimple $K$-algebra $l$ such that $A_2/J(A_2) = l \oplus A_1$.*

## 3.2 Unit group of $\mathbb{F}_q\mathbf{SL}(3,2)$

We will be using various descriptions of $\mathrm{SL}(3,2)$ in the sequel, which are well known. From [38], it is known that

$$\mathrm{SL}(3,2) = \mathrm{GL}(3,2) \cong \mathrm{PGL}(2,7) \cong \mathrm{PSL}(2,7).$$

We have an embedding of $\mathrm{SL}(3,2)$ inside $S_8$ as follows:

$$\mathrm{SL}(3,2) \cong \langle (3,7,5)(4,8,6), (1,2,6)(3,4,8) \rangle.$$

This group has 7 conjugacy classes and using [21], we have the following table:

| Class | Representative | Order | No. of elements |
|---|---|---|---|
| $\mathcal{C}_1$ | $\alpha_1 = (1)$ | 1 | 1 |
| $\mathcal{C}_2$ | $\alpha_2 = (1,2)(3,4)(5,8)(6,7)$ | 2 | 21 |
| $\mathcal{C}_3$ | $\alpha_3 = (3,5,7)(4,6,8)$ | 3 | 56 |
| $\mathcal{C}_4$ | $\alpha_4 = (1,2,3,5)(4,8,7,6)$ | 4 | 42 |
| $\mathcal{C}_5$ | $\alpha_5 = (2,3,5,4,7,8,6)$ | 7 | 24 |
| $\mathcal{C}_6$ | $\alpha_6 = (2,4,6,5,8,3,7)$ | 7 | 24 |

.

We note down the following relations

$$[\alpha_5] = [\alpha_5^2] = [\alpha_5^4]. \tag{3.2.1}$$

and

$$[\alpha_6] = [\alpha_5^3] = [\alpha_5^5] = [\alpha_5^6] = [\alpha_6]. \tag{3.2.2}$$

### 3.2.1 On some simple components of $\mathbb{F}_q\mathbf{SL}(3,2)$

The next few lemmas are crucial for determining the different $n_i$'s occurring in the Artin-Wedderburn decomposition of $\mathbb{F}_q\mathrm{SL}(3,2)$.

**Lemma 3.2.1.** *Let $G$ be a group of order $n$ and $\mathbb{F}$ be a field of characteristic $p > 0$. Let $G$ acts on a finite set $X = \{1, 2, \cdots, k\}$ doubly transitively. Set $G_i = \{g \in G : g \cdot i = i\}$ and $G_{i,j} = \{g \in G : g \cdot i = i, g \cdot j = j\}$. Then the $\mathbb{F}G$ module*

$$W = \left\{ x \in \mathbb{F}^k : \sum_{i=1}^{k} x_i = 0, i \in X \right\}$$

*is an irreducible $\mathbb{F}G$ module if $p \nmid k, p \nmid |G_{1,2}|$.*

*Proof.* Let $U \subseteq W$ be a non-zero invariant space under the action of $G$. Since the action is doubly transitive, it is enough to show that we have $(1, -1, \underbrace{0, \ldots, 0}_{(k-2) \text{ times}}) \in U$.

Let $x = (x_1, x_2, \ldots, x_n) \in U$ be nonzero. Then we can assume that $x_1 \neq 0$, since $G$ acts transitively on $X$. Considering the element $y = \sum_{g \in G_1} gx \in U$, we see that

$$\begin{aligned} y_1 &= |G_1| x_1 \\ y_2 &= y_3 = \cdots = y_n \\ &= |G_{1,2}| \sum_{i=2}^{n} x_i, \end{aligned}$$

since $G$ permutes $X$. Note that $y_i \neq 0$ for all $1 \leq i \leq k$. Next taking a $g \in G$, which permutes $1, 2$ (this exists since the action is doubly transitive) we see that $(y_1 - y_2)(1, -1, 0, \ldots, 0) \in U$, which finishes the proof. □

**Corollary 3.2.2.** *The representation induced by the action of* $\mathrm{GL}(3, 2) = \mathrm{PGL}(3, 2)$ *on* $\boldsymbol{P}^2(\mathbb{F}_2)$ *has an irreducible component of degree* 6 *over* $\mathbb{F}_{p^k}$*, for* $p \geq 11$.

*Proof.* We know that the action of $\mathrm{GL}(3, 2)$ on $\mathbf{P}^2(\mathbb{F}_2)$ is doubly transitive (see [23, pp. 124]). Since $G_{1,2}$ is a subgroup of $\mathrm{GL}(3, 2)$ and $p \nmid |G|$, the result follows from Lemma 3.2.1. □

**Corollary 3.2.3.** *The representation induced by the action of* $\mathrm{GL}(3,2) \cong \mathrm{PSL}(2,7)$ *on* $\boldsymbol{P}^1(\mathbb{F}_7)$ *has an irreducible component of degree* 7 *over* $\mathbb{F}_{p^k}$*, for* $p \geq 11$.

*Proof.* The action of the group $\mathrm{PGL}(2,7)$ on $\mathrm{Perm}^1(\mathbb{F}_7)$, is transitive, as well as doubly transitive (see [23, pp. 157]). We see that $p \nmid |G_{1,2}|$, as $G_{1,2}$ is a subgroup of $\mathrm{PGL}(3,2)$ and $p \nmid 168$. □

**Remark 3.2.4.** Using Lemma 3.2.1, it can be seen that the regular representation of the symmetric group $S_n$, decomposes into the trivial representation and an irreducible representation of degree $n-1$ over the field $\mathbb{F}_{p^k}$, whenever $p > n$.

**Lemma 3.2.5.** *Let* $A_i$*,* $1 \leq i \leq n$ *be a family of unital algebra with unit* $1_i$ *and* $\mathcal{D}_i$ *be the set of representatives of simple* $A_i$*-modules. Then any simple* $\bigoplus_{i=1}^{n} A_i$*-module is of the form* $\bigoplus_{i=1}^{n} M_i$*, where not all* $M_i$*'s are zero and* $M_i \in \mathcal{D}_i$.

*Proof.* Since $1_{\bigoplus_{i=1}^{n} A_i} = \sum_{i=1}^{n} 1_{A_i}$ and hence for any $\bigoplus_{i=1}^{n} A_i$-module $M$, we have

$$\begin{aligned} M &= M \cdot 1_{\bigoplus_{i=1}^{n} A_i} \bigoplus_{i=1}^{n} A_i \\ &= \bigoplus_{i=1}^{n} M A_i. \end{aligned}$$

□

**Lemma 3.2.6.** *[37, Example 3.3] For any division algebra (in particular field)* $D$*, the only simple* $M(n,D)$*-module is* $D^n$ *upto isomorphism.*

**Corollary 3.2.7.** *Let* $G$ *be a finite group,* $k$ *be a finite field of characteristic* $p > 0$*,* $p \nmid |G|$*. Then if there exists an irreducible representations of degree* $n$ *over* $k$*, then one of the component of* $kG$ *is of the form* $M(n,k)$.

*Proof.* Since $p \nmid |G|$, by Maschke's theorem $kG$ is semisimple. Hence by Artin–Wedderburn theorem we have that

$$kG = \bigoplus_{i=1}^{n} M(n_i, k_i),$$

where $k_i$'s are finite extensions of $k$ (hence a field). It follows from Lemma 3.2.5 and Lemma 3.2.6 that for some $i$, we have $n_i = n, k_i = k$. Hence the result follows. $\square$

**Corollary 3.2.8.** *Two of the components of the group algebra* $\mathbb{F}_q\mathrm{SL}(3,2)$ *are* $\mathrm{M}(6,\mathbb{F}_q), \mathrm{M}(7,\mathbb{F}_q)$.

*Proof.* This follows immediately from Corollaries 3.2.2, 3.2.3 and 3.2.7. $\square$

## 3.3 Units in $\mathbb{F}_q\mathbf{SL}(3,2)$

**Proposition 3.3.1.** *Let $\mathbb{F}_q$ be a field of characteristic $p$ and $p \geq 11$, $q = p^k$. Let $G$ be the group $\mathrm{SL}(3,2)$. Then the Artin-Wedderburn decomposition of $\mathbb{F}_qG$ is one of the following:*

$$\mathbb{F}_q \oplus \bigoplus_{i=1}^{5} M(n_i, \mathbb{F}_q),$$
$$\mathbb{F}_q \oplus \bigoplus_{i=1}^{3} M(n_i, \mathbb{F}_q) \oplus M(n_4, \mathbb{F}_{q^2}).$$

*Proof.* Since $p \nmid |G|$, by Maschke's theorem we have $\mathbb{F}_qG$ is semisimple and hence $J(\mathbb{F}_qG)$ is zero. By its Wedderburn decomposition we have $\mathbb{F}_qG$ is isomorphic to $\bigoplus_{i=1}^{n} M(n_i, K_i)$, where $n_i > 0$ and $K_i$ is a finite extension of $\mathbb{F}_q$, for all $1 \leq i \leq n$.

Firstly from Lemma 3.1.6, we have

$$\mathbb{F}_qG \cong \mathbb{F}_q \bigoplus_{i=1}^{n-1} M(n_i, K_i), \tag{3.3.1}$$

taking $h$ to be the augmentation map. Now to compute these $n_i$'s and $K_i$'s we calculate the cyclotomic $\mathbb{F}_q$ classes of $G$. We do this in 6 cases, for $k = 6l + i$ , $0 \leq i \leq 5$. Note that $p$ can have the following possibilities, being a prime

$$\begin{aligned} p \in \{\pm 1\} &\mod 4,\\ p \in \{\pm 1\} &\mod 3,\\ p \in \{\pm 1, \pm 2, \pm 3\} &\mod 7. \end{aligned}$$

1. <u>The case ($k = 6l$)</u>: In this case $p^k \equiv 1 \mod 7, p^k \equiv 1 \mod 4$ and $p^k \equiv 1 \mod 3$, hence $p^k \equiv 1 \mod 84$ (using Chinese Remainder theorem). Thus $I_{\mathbb{F}_q} = \{1\}$ and $S_{\mathbb{F}_q}(\gamma_g) = \{\gamma_g\}$ for all $g \in G$. Thus by Lemma 3.1.2,

Lemma 3.1.5 and Equation (3.3.1)

$$\mathbb{F}_q G \cong \mathbb{F}_q \oplus \bigoplus_{i=1}^{5} M(n_i, \mathbb{F}_q).$$

When such a decomposition arises, we say that $(p, k)$ is of type 1.

2. The case $(k = 6l + 1)$: In this case if $p \equiv \pm 1 \mod 3, p \equiv \pm 1 \mod 4$ and $p \equiv 1, 2, -3 \mod 7$, $S_{\mathbb{F}_q}(\gamma_g) = \{\gamma_g\}$ for all $g \in G$, because we have

$$[\alpha_2] = [\alpha_2^{-1}], [\alpha_3] = [\alpha_3^{-1}], [\alpha_4] = [\alpha_4^{-1}].$$

Once again by Lemma 3.1.2 and Lemma 3.1.5 and Equation (3.3.1)

$$\mathbb{F}_q G \cong \mathbb{F}_q \oplus \bigoplus_{i=1}^{5} M(n_i, \mathbb{F}_q).$$

i.e $(p, k)$ is of type 1. Now if $p \equiv -1, -2, 3 \mod 7$, then we get that $S_{\mathbb{F}_q}(\gamma_g) = \{\gamma_g\}$ for $g \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ and $S_{\mathbb{F}_q}(\gamma_g) = (\gamma_g, \gamma_{g^{-1}})$ when $g \in \{\alpha_5, \alpha_6\}$ since $[\alpha_5] \neq [\alpha_5^{-1}]$. Hence in this case we have

$$\mathbb{F}_q G \cong \mathbb{F}_q \oplus \bigoplus_{i=1}^{3} M(n_i, \mathbb{F}_q) \oplus M(n_4, \mathbb{F}_{q^2}).$$

When such a decomposition arises, we say that $(p, k)$ is of type 2.

It can be further shown using Equation 3.2.1 and Equation 3.2.2 that $(p, k)$ is either of type 1 or 2. The possibilities are listed in the table below.

| $p \mod 7$ | $k$ | Type of $(p,k)$ |
|---|---|---|
| $\pm1, \pm2, \pm3$ | $6l$ | 1 |
| $1, 2, -3$ | $6l+1$ | 1 |
| $-1, -2, 3$ | $6l+1$ | 2 |
| $\pm1, \pm2, \pm3$ | $6l+2$ | 1 |
| $1, 2, -3$ | $6l+3$ | 1 |
| $-1, -2, 3$ | $6l+3$ | 2 |
| $\pm1, \pm2, \pm3$ | $6l+4$ | 1 |
| $1, 2, -3$ | $6l+5$ | 1 |
| $-1, -2, 3$ | $6l+5$ | 2 |

□

**Proposition 3.3.2.** *We have* $(n_1, n_2, n_3, n_4, n_5, n_6) = (1, 6, 7, 8, 3, 3)$ *up to some permutation.*

*Proof.* By Corollary 3.2.8, we have that for some $n_i = 6, n_j = 7$ for some $i, j \in \{1, 2, \ldots, 6\}$. Let us assume $n_2 = 6, n_3 = 7$. Since $n_1 = 1$, we are left with the equation $n_4^2 + n_5^2 + n_6^2 = 82$, with all $n_i > 0$. Since the only possibility is $8^2 + 3^2 + 3^2$, we are done. □

**Proposition 3.3.3.** *Let* $\mathbb{F}_q$ *be a field of characteristic* $p$ *and* $p \geq 11$, $q = p^k$. *Let* $G$ *be the group* $\mathrm{SL}(3, 2)$. *Then the Wedderburn decomposition of* $\mathbb{F}_q G$ *is as follows :*

$$\mathbb{F}_q \oplus \mathrm{M}(6, \mathbb{F}_q) \oplus \mathrm{M}(7, \mathbb{F}_q) \oplus \mathrm{M}(8, \mathbb{F}_q) \oplus \mathrm{M}(3, \mathbb{F}_q)^2 \text{ if } (p,k) \text{ is of type } 1,$$
$$\mathbb{F}_q \oplus \mathrm{M}(6, \mathbb{F}_q) \oplus \mathrm{M}(7, \mathbb{F}_q) \oplus \mathrm{M}(8, \mathbb{F}_q) \oplus \mathrm{M}(3, \mathbb{F}_{q^2}) \text{ if } (p,k) \text{ is of type } 2.$$

*Proof.* Follows immediately from Proposition 3.3.1 and Proposition 3.3.2. □

**Theorem 3.3.4.** *Let* $\mathbb{F}_q$ *be a field of characteristic* $p$ *and* $p \geq 11$. *Let* $G$ *be the group* $\mathrm{SL}(3, 2)$. *Then the unit group* $\mathcal{U}(\mathbb{F}_q G)$ *is as listed in the following table:*

| $p \mod 7$ | $k$ | $\mathcal{U}(\mathbb{F}_q\mathrm{SL}(3,2))$ |
|---|---|---|
| $\pm1, \pm2, \pm3$ | $6l$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6,\mathbb{F}_q) \oplus \mathrm{GL}(7,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(3,\mathbb{F}_q)^2$ |
| $1, 2, -3$ | $6l+1$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6,\mathbb{F}_q) \oplus \mathrm{GL}(7,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(3,\mathbb{F}_q)^2$ |
| $-1, -2, 3$ | $6l+1$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6,\mathbb{F}_q) \oplus \mathrm{GL}(7,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(3,\mathbb{F}_{q^2})$ |
| $\pm1, \pm2, \pm3$ | $6l+2$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6,\mathbb{F}_q) \oplus \mathrm{GL}(7,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(3,\mathbb{F}_q)^2$ |
| $1, 2, -3$ | $6l+3$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6,\mathbb{F}_q) \oplus \mathrm{GL}(7,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(3,\mathbb{F}_q)^2$ |
| $-1, -2, 3$ | $6l+3$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6,\mathbb{F}_q) \oplus \mathrm{GL}(7,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(3,\mathbb{F}_{q^2})$ |
| $\pm1, \pm2, \pm3$ | $6l+4$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6,\mathbb{F}_q) \oplus \mathrm{GL}(7,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(3,\mathbb{F}_q)^2$ |
| $1, 2, -3$ | $6l+5$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6,\mathbb{F}_q) \oplus \mathrm{GL}(7,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(3,\mathbb{F}_q)^2$ |
| $-1, -2, 3$ | $6l+5$ | $\mathbb{F}_q^\times \oplus \mathrm{GL}(6,\mathbb{F}_q) \oplus \mathrm{GL}(7,\mathbb{F}_q) \oplus \mathrm{GL}(8,\mathbb{F}_q) \oplus \mathrm{GL}(3,\mathbb{F}_{q^2})$ |

*Proof.* This follows immediately from Proposition 3.5.7 and the fact that given two rings $R_1, R_2$, we have $(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$. $\square$

**Remark 3.3.5.** Theorem 3.3.4 holds for $p = 5$ as well.

## 3.4 Units of $\mathbb{F}_{p^k}S_n$ for $p \nmid n$

Let $S_n$ denote the symmetric group on $n$ letters. We start the section by talking about representations of $S_n$ over a finite field. We define the Brauer character and state some important results about representations over an arbitrary field. See [27] for further details.

Let $E$ be a field of characteristic $p$. We choose a ring of algebraic integers $A$ in $\mathbb{C}$ such that $E = A/M$, where $M$ is a maximal ideal of $A$ containing $pA$. Take $f$ to be the natural map $A \longrightarrow E$. Take $W = \{z \in \mathbb{C} | z^m = 1 \text{ for some } m \in \mathbb{Z} \text{ with } p \nmid m\}$ (note that $W \subseteq A$). Now let $\pi$ be a representation of a finite group $G$ over $E$. Let $S$ be the set of $p'$ elements of $G$. For $\alpha \in S$, let $\epsilon_1, \epsilon_2, \dots, \epsilon_l \in E^\times$ be the eigenvalues of $\pi(\alpha)$ with multiplicities. Then for every $i$, there exists a unique $u_i \in W$ such that $f(u_i) = \epsilon_i$. Define $\phi : S \longrightarrow \mathbb{C}$ as $\phi(\alpha) = \Sigma u_i$. Then $\phi$ is called the Brauer character of $G$ afforded by $\pi$.

**Remark 3.4.1.** The description of Brauer character comes along with a choice of a maximal ideal $M$ of $A$.

Suppose $\pi_1, \pi_2, \ldots, \pi_k$ are all the non-isomorphic irreducible representations of $G$ over $E$ upto isomorphism. Let $\phi_i$ be the Brauer character afforded by $\pi_i$. Then $\phi_i' s$ are called irreducible Brauer characters and we denote by $IBr(G)$ the set $\{\phi_i\}$. We denote by $Irr(G)$ the set of irreducible characters of $G$ over $\mathbb{C}$. We have the following results.

**Lemma 3.4.2.** *[27, Theorem 15.13] For a finite group $G$, $IBr(G) = Irr(G)$ whenever $p \not| |G|$.*

For the rest of this section, take $G = S_n$, the symmetric group on $n$ letters. We say a partition $\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_l)$ of $n$ is p-singular if for some $j$ we have $\lambda_{j+1} = \lambda_{j+2} = \ldots = \lambda_{j+p}$. If a partition is not $p$-singular, it is called $p$-regular. Then we have the following.

**Lemma 3.4.3.** *[28, Theorem 11.5] If $F$ is a field of characteristic $p$, then as $\lambda$ varies over the $p$-regular partitions, $D^\lambda$ varies over the complete set of inequivalent irreducible $FS_n$-modules, where $D^\lambda = \dfrac{S^\lambda}{S^\lambda \cap (S^\lambda)^\perp}$ and $S^\lambda$ denotes the Specht-module corresponding to the partition $\lambda$. Moreover, every field is a splitting field for $S_n$.*

*Proof.* The proof follows immediately from the fact that every partition of $n$ is a $p$-regular partition. □

**Lemma 3.4.4.** *The dimensions of non-isomorphic irreducible representations of $S_n$ over $E$ coincides with the dimensions of non-isomorphic irreducible representations of $S_n$ over $\mathbb{C}$ when characteristic of the field $E$ is greater than $n$.*

*Proof.* Since the dimension of a representation is as same as the value of the corresponding character $\chi$ at the identity element of the group, the result follows from Lemma 3.4.2. □

**Proposition 3.4.5.** *Let $\mathbb{F}_{p^k}$ be a finite field where $p > n$. Then*

$$\mathbb{F}_{p^k} S_n \cong \bigoplus_{\chi \in Irr(G)} \mathrm{M}(\chi(1), \mathbb{F}_{p^k}).$$

*Proof.* Since being a semisimple algebra $\mathbb{C}S_n \cong \bigoplus_{\chi \in Irr(G)} \mathrm{M}(\chi(1), \mathbb{C})$, the result follows from corollary 3.2.7, and lemmas 3.4.2 and 3.4.4. □

**Theorem 3.4.6.** *Let $\mathbb{F}_{p^k}$ be a finite field where $p > n$. Then*

$$\mathcal{U}(\mathbb{F}_{p^k} S_n) \cong \bigoplus_{\chi \in Irr(G)} \mathrm{GL}(\chi(1), \mathbb{F}_{p^k}).$$

*Proof.* This follows immediately from Proposition 3.4.5 and the fact that given two rings $R_1, R_2$, we have $(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$. □

**Remark 3.4.7.** Theorem 3.4.6 improves the result of [29] and proves that when $p > 5$, unit group of $\mathbb{F}_{p^k} S_5$ is $\mathcal{U}(\mathbb{F}_{p^k} S_5)$ given by

$$\mathbb{F}_{p^k}^\times \oplus \mathbb{F}_{p^k}^\times \oplus \mathrm{GL}(4, \mathbb{F}_{p^k}) \oplus \mathrm{GL}(4, \mathbb{F}_{p^k}) \oplus \mathrm{GL}(5, \mathbb{F}_{p^k}) \oplus \mathrm{GL}(5, \mathbb{F}_{p^k}) \oplus \mathrm{GL}(6, \mathbb{F}_{p^k}).$$

**Remark 3.4.8.** For an irreducible representation $\chi$ of $S_n$ over a field of characteristic $p > n$, this is characterized by a partition $\lambda$ of $n$. The value $\chi(1)$ can be calculated as the number of standard Young tableaux of shape $\lambda$.

## 3.5 Units of $\mathbb{F}_{p^k} A_6$ for $p \geq 7$

We start with the description of the conjugacy classes in $A_6$. Using [21] the group has 7 conjugacy classes, of which the representatives are given by $(1), a = (1,2)(3,4), b = (1,2,3), c = (1,2,3)(4,5,6), d = (1,2,3,4)(5,6), e =$

$(1, 2, 3, 4, 5)$ and $f = (1, 2, 3, 4, 6)$. We have the following relations:

$$\text{for all } g \notin [e] \cup [f],\ [g] = [g^{-1}], \tag{3.5.1}$$

$$\text{and } [e] = [e^4], [e^2] = [e^3] = [f]. \tag{3.5.2}$$

**Proposition 3.5.1.** *Let $\mathbb{F}_q$ be a field of characteristic $p \geq 7$ and $G = A_6$. Then the Artin-Wedderburn decomposition of $\mathbb{F}_qG$ is one of the following:*

$$\mathbb{F}_q \oplus \bigoplus_{i=1}^{6} M(n_i, \mathbb{F}_q),$$
$$\mathbb{F}_q \oplus \bigoplus_{i=1}^{4} M(n_i, \mathbb{F}_q) \oplus M(n_5, \mathbb{F}_{q^2})$$

*Proof.* Since $p \geq 7$, we have $p \nmid |A_6|$, by Maschke's theorem we have $J(\mathbb{F}_qG) = 0$. Hence Wedderburn decomposition of $\mathbb{F}_qG$ is isomorphic to $\bigoplus_{i=1}^{n} M(n_i, K_i)$, where for all $1 \leq i \leq n$, we have $n_i > 0$ and $K_i$ is a finite extension of $\mathbb{F}_q$.

Firstly, from Lemma 3.1.6, we have

$$\mathbb{F}_qG \cong \mathbb{F}_q \bigoplus_{i=1}^{n-1} M(n_i, K_i), \tag{3.5.3}$$

taking $g$ to be the map $g(\sum_{x \in A_6} \alpha_x x) = \sum_{x \in A_6} \alpha_x$. Now to compute these $n_i$'s and $K_i$'s we calculate the cyclotomic $\mathbb{F}_q$ classes of $G$. Note that $p^k \equiv \pm 1 \mod 4, p^k \equiv \pm 1 \mod 3$ for any prime $p$. Hence $S_{\mathbb{F}_q}(\gamma_g) = \{\gamma_g\}$ whenever $g \notin [e] \cup [f]$ (by Equation 4.1). Hence we have to consider $S_{\mathbb{F}_q}(\gamma_g)$ in the other cases.

When $p \equiv \pm 1 \mod 5$, $S_{\mathbb{F}_q}(\gamma_e) = \{\gamma_e\}$ and $S_{\mathbb{F}_q}(\gamma_f) = \{\gamma_f\}$, by Equation 4.2 and the fact that $p^k \equiv \pm 1 \mod 5$. Thus by Lemma 3.1.2 and 3.1.5, there are seven cyclotomic $\mathbb{F}_q$-classes and $[K_i : \mathbb{F}_q] = 1$ for all $1 \leq i \leq 6$. This gives that in this case the Artin-Wedderburn decomposition is

$$\mathbb{F}_q \oplus \bigoplus_{i=1}^{6} M(n_i, \mathbb{F}_q).$$

When $p \equiv \pm 2 \mod 5$ and $k$ is even, then $p^k \equiv -1 \mod 5$. Similarly in this case the Artin-Wedderburn decomposition is

$$\mathbb{F}_q \oplus \bigoplus_{i=1}^{6} M(n_i, \mathbb{F}_q).$$

Lastly, when $p \equiv \pm 2 \mod 5$ and $k$ is odd, then $p^k \equiv \pm 2 \mod 5$ and $S_{\mathbb{F}_q}(\gamma_e) = \{\gamma_e, \gamma_f\}$ by Equation 4.2. Thus by Lemma 3.1.2 and 3.1.5, there are six cyclotomic $\mathbb{F}_q$-classes and $[K_i : \mathbb{F}_q] = 1$ for all $1 \leq i \leq 4$, $[K_5 : \mathbb{F}_q] = 2$ . In this case, the Artin-Wedderburn decomposition is

$$\mathbb{F}_q \oplus \bigoplus_{i=1}^{4} M(n_i, \mathbb{F}_q) \oplus M(n_5, \mathbb{F}_{q^2}).$$

$\square$

Since $\dim \mathbb{F}_q A_6 = |A_6| = 360$, Proposition 3.5.1 gives that the $n_i$'s should satisfy $n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 + n_6^2 = 359$ or $n_1^2 + n_2^2 + n_3^2 + n_4^2 + 2n_5^2 = 359$. Since these equations do not have a unique solution, we find some of the $n_i$'s using representations of $A_6$ over $\mathbb{F}_q$ and invoke Lemma 3.2.1 to reach a unique solution for the mentioned equations. We have the following results.

**Lemma 3.5.2.** *The group $S_6$ has four inequivalent irreducible representations of degree 5, which on restriction on $A_6$ give two inequivalent irreducible representations of $A_6$ over $\mathbb{F}_{p^k}$ for $p \geq 7$. Moreover, these irreducible representations are obtained from two non-isomorphic doubly transitive actions on a set of 6 points.*

*Proof.* Note that $S_6$ acts on $T = \{1, 2, 3, 4, 5, 6\}$ doubly transitively. Hence by Lemma 3.2.1, we get an irreducible representation of degree 5. Since tensoring with sign representation gives irreducible representations, we get two inequivalent irreducible representations of degree 5 of $S_6$, say $\pi_1$ and $\pi_2$.

For the other two irreducible representations of dimension 5, we consider the outer automorphism of $S_6$, say $\varphi$, given on generators as follows:

$$\begin{aligned}
\varphi((1,2)) &= (1,2)(3,4)(5,6)\\
\varphi((2,3)) &= (1,3)(2,5)(4,6)\\
\varphi((3,4)) &= (1,5)(2,6)(3,4)\\
\varphi((4,5)) &= (1,3)(2,4)(5,6)\\
\varphi((5,6)) &= (1,6)(2,5)(3,4).
\end{aligned}$$

This gives another doubly transitive action on $T$, which is not isomorphic to the previous action. Thus we get another 5 dimensional irreducible representation, say $\pi_3$. Tensoring $\pi_3$ with the sign representations, we get $\pi_4$ which is a 5 dimensional irreducible representation of $S_6$ different from $\pi_3$. By considering the characters of the corresponding representations, we see that $\pi_1, \pi_2, \pi_3$ and $\pi_4$ are all distinct.

Since $A_6$ acts doubly transitively on $T$ via the restrictions of these two actions, we obtain two non-isomorphic 5-dimensional irreducible representations of $A_6$. $\square$

**Corollary 3.5.3.** *The algebra $\mathbb{F}_q A_6$ has two components which are both isomorphic to* $\mathrm{M}(5, \mathbb{F}_q)$*, for $p \geq 7$.*

*Proof.* Immediately follows from Lemma 3.5.2 and Lemma 3.2.1. $\square$

**Corollary 3.5.4.** *There does not exist any 4 dimensional irreducible representations of $A_6$ over $\mathbb{F}_{p^k}$ for $p \geq 7$.*

*Proof.* From Lemma 3.4.3, we know that any field $\mathbb{F}_{p^k}, p \geq 7$ is a splitting field of $S_6$. Hence by Proposition 3.4.5, we have degrees of irreducible representations of $S_6$ are $\{1, 5, 9, 10, 16\}$.

Recall that by Frobenius reciprocity we have the following bijection

$$\mathrm{Hom}_{\mathbb{F}_q S_6}(\mathrm{Ind}V, W) \cong \mathrm{Hom}_{\mathbb{F}_q A_6}(V, \mathrm{Res}W),$$

where Ind, Res denote the induction functor, restriction functor, respectively. Here $V$ is an irreducible representation of $A_6$ and $W$ is an irreducible representation of $S_6$. Suppose $A_6$ has an irreducible representation $V$ with $\dim V = 4$. Since $[S_6 : A_6] = 2$, we have that $\dim \mathrm{Ind}V = 8$. Since $S_6$ does not have any irreducible representation of dimension 8, the induced representation splits. Being $\dim \mathrm{Ind}V = 8$, $\mathrm{Ind}(V)$ does not have any component of dimensions $9, 10$ and 16. Now, let us assume that $\dim W = 5$. Then by Lemma 3.5.2, $\mathrm{Res}W$ is an irreducible representation. Hence $\mathrm{Hom}_{\mathbb{F}_q A_6}(V, \mathrm{Res}W) = 0$, which implies that $\mathrm{Ind}V$ does not have any irreducible component of dimension 5. Similarly, $\mathrm{Ind}V$ does not have any irreducible component of dimension 1. This completes the proof. □

**Corollary 3.5.5.** *The algebra $\mathbb{F}_q A_6$ has one component to be $\mathrm{M}(9, \mathbb{F}_q)$ for $p \geq 7$.*

*Proof.* The group $A_6$ being isomorphic to $\mathrm{PSL}(2, \mathbb{F}_9)$ acts doubly transitively on a set with 10 points (See [23]). Hence the conclusion. □

**Corollary 3.5.6.** *We have $(n_1, n_2, n_3, n_4, n_5, n_6) = (5, 5, 9, 8, 8, 10)$ or $(n_1, n_2, n_3, n_4, n_5) = (5, 5, 9, 10, 8)$ upto permutation.*

*Proof.* Since $A_6$ has one 1-dimensional, two 5-dimensional and one 9-dimensional irreducible representations, we can assume that $n_1 = 5, n_2 = 5, n_3 = 9$. Hence we are left with the equation

$$n_4^2 + n_5^2 + n_6^2 = 228 \text{ or } n_4^2 + 2n_5^2 = 228.$$

Then $(n_4, n_5, n_6) \in \{(4, 4, 14), (8, 8, 10)\}, (n_4, n_5) \in \{(14, 4), (10, 8)\}$. Hence, the result is obvious from Corollary 3.5.4. □

**Proposition 3.5.7.** *Let $\mathbb{F}_{p^k}$ be a field of characteristic $p \geq 7$ and $A_6$ denotes the alternating group on six letters. Then the Artin-Wedderburn decomposition of $\mathbb{F}_{p^k} A_6$ is*

$$\mathbb{F}_q \oplus \mathrm{M}(5, \mathbb{F}_q) \oplus \mathrm{M}(5, \mathbb{F}_q) \oplus \mathrm{M}(9, \mathbb{F}_q) \oplus \mathrm{M}(10, \mathbb{F}_q) \oplus \mathrm{M}(8, \mathbb{F}_{q^2}),$$

*when* $p \equiv \pm 2 \mod 5, k \equiv 1 \mod 2$ *and the decomposition is*

$$\mathbb{F}_q \oplus \mathrm{M}(5, \mathbb{F}_q) \oplus \mathrm{M}(5, \mathbb{F}_q) \oplus \mathrm{M}(8, \mathbb{F}_q) \oplus \mathrm{M}(8, \mathbb{F}_q) \oplus \mathrm{M}(9, \mathbb{F}_q) \oplus \mathrm{M}(10, \mathbb{F}_q),$$

*in other cases.*

*Proof.* Follows from Proposition 3.5.1 and Corollary 3.5.6. □

**Theorem 3.5.8.** *Let* $\mathbb{F}_{p^k}$ *be a field of characteristic* $p \geq 7$ *and* $A_6$ *denotes the alternating group on six letters. Then the unit group of the algebra,* $\mathcal{U}(\mathbb{F}_{p^k} A_6)$ *is*

$$\mathbb{F}_q^\times \oplus \mathrm{GL}(5, \mathbb{F}_q) \oplus \mathrm{GL}(5, \mathbb{F}_q) \oplus \mathrm{GL}(9, \mathbb{F}_q) \oplus \mathrm{GL}(10, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_{q^2}), \quad (3.5.4)$$

*when* $p \equiv \pm 2 \mod 5, k \equiv 1 \mod 2$ *and the decomposition is*

$$\mathbb{F}_q^\times \oplus \mathrm{GL}(5, \mathbb{F}_q) \oplus \mathrm{GL}(5, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(8, \mathbb{F}_q) \oplus \mathrm{GL}(9, \mathbb{F}_q) \oplus \mathrm{GL}(10, \mathbb{F}_q), \quad (3.5.5)$$

*in other cases.*

*Proof.* This follows immediately from Proposition 3.5.7 and the fact that given two rings $R_1, R_2$, we have $(R_1 \times R_2)^\times = R_1^\times \times R_2^\times$. □

# Bibliography


[1] Arvind, N.; Panja, S. *On $\mathbb{Z}_n \rtimes \mathbb{Z}_2$-Hopf-Galois structures*, Journal of Algebra, Volume 596, 2022, Pages 37-52.

[2] N. Arvind, S. Panja, *"Unit group of* $\mathbb{F}_q\mathrm{SL}(3,2), p \geq 11$*"* arXiv:2106.07261.

[3] Arvind, N.; Panja, S. *Unit group of some finite semisimple group algebras*, Journal of Egypitian Mathematical Society, https://doi.org/10.1186/s42787-022-00151-0.

[4] N. Arvind, S. Panja, *"Hopf-Galois realizability of* $Zn2$*"*, Journal of Pure and Applied Algebra, Volume 227, Issue 4, 2023.

[5] N.P. Byott, *Uniqueness of Hopf Galois structure of separable field extensions*, Comm. Algebra 24 (1996), 3217-3228.

[6] Bidwell J. N. S. *Automorphisms of direct products of finite groups: II*, Arch. Math. (Basel) 91 (2008), no. 2, 111–121.

[7] Byott N. P., *Nilpotent and abelian Hopf–Galois structures on field extensions*, Journal of Algebra, Volume 381, 2013, Pages 131-139.

[8] Bachiller D., Cedó F., Jespers E. *Solutions of the Yang-Baxter equation associated with a left brace*, J. Algebra 463 (2016), 80–102.

[9] Y. Bai, Y. Li, J. Peng, *"Unit groups of finite group algebras of Abelian groups of order 17 to 20"*, AIMS Mathematics, 2021, 6(7): 7305-7317.

[10] Childs L. N. *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, 80. American Mathematical Society, Providence, RI, 2000. viii+215 pp. ISBN: 0-8218-2131-8.

[11] Carnahan Sc., Childs L. *Counting Hopf Galois structures on non-abelian Galois field extensions*, J. Algebra 218 (1999), no. 1, 81–92.

[12] Campedel E., Caranti A., Corso I. D., *Hopf-Galois structures on extensions of degree $p^2q$ and skew braces of order $p^2q$: The cyclic Sylow $p$-subgroup case*, Journal of Algebra, Volume 556, 2020, Pages 1165-1210.

[13] Cedó F., Jespers E., Okniński J. *Braces and the Yang-Baxter equation*, Comm. Math. Phys. 327 (2014), no. 1, 101–116.

[14] Greither C., Pareigis B., *Hopf Galois theory for separable field extensions*, Journal of Algebra, Volume 106, Issue 1, 1987, Pages 239-258.

[15] Kohl T. *Enumerating dihedral Hopf-Galois structures acting on dihedral extensions*, J. Algebra 542 (2020), 93–115.

[16] Sweedler M. E. *Hopf algebras*, Mathematics Lecture Note Series W. A. Benjamin, Inc., New York 1969 vii+336 pp.

[17] Smoktunowicz A., Vendramin L. *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra 2 (2018), no. 1, 47–86.

[18] Zenouz N. K. *On Hopf-Galois Structures and Skew Braces of Order $p^3$*, PhD thesis, The University of Exeter, UK, (2018).

[19] N. Arvind, S. Panja, *"Unit group of $\mathbb{F}_q\mathrm{SL}(3,2), p \geq 11$"* arXiv:2106.07261

[20] R. A. Ferraz, *"Simple components of the center of $FG/J(FG)$"*, Comm. Algebra 36 (2008), no. 9, 3191–3199.

[21] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.11.1; 2021. (https://www.gap-system.org)

[22] W. D. Gao, A. Geroldinger, F. Halter-Koch, *"Group algebras of finite abelian groups and their applications to combinatorial problems"*, Rocky Mountain J. Math., 39 (2008), 805–823.

[23] J. W. P. Hirschfeld, *"Projective geometries over finite fields"*, Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1979. xii+474 pp. ISBN: 0198535260.

[24] T. Hurley, *"Group rings and rings of matrices"*, Int. J. Pure Appl. Math. 31 (2006), no. 3, 319–335. 20C05.

[25] T. Hurley, *"Convolutional codes from units in matrix and group rings"*, Int. J. Pure Appl. Math. 50 (2009), no. 3, 431–463.

[26] P. Hurley, T. Hurley *"Codes from zero-divisors and units in group rings"*, International Journal of Information and Coding Theory (IJICOT), Vol. 1, No. 1, 20.

[27] I. M. Isaacs, *"Character theory of finite groups"*, Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. AMS Chelsea Publishing, Providence, RI, 2006. xii+310 pp. ISBN: 978-0-8218-4229-4; 0-8218-4229-3

[28] G. D. James, *"The representation theory of the symmetric groups"*, Lecture Notes in Mathematics, 682. Springer, Berlin, 1978. v+156 pp. ISBN: 3-540-08948-9

[29] Y. Kumar, R. K. Sharma and J. B. Srivastava, *"The structure of the unit group of the group algebra $\mathbb{F}S_5$ where $\mathbb{F}$ is a finite field with* $\mathrm{Char}\mathbb{F} = p > 5$*"*, ActaMath. Acad. Paedagog. Nyh azi. (N.S.), 33(2) (2017), 187-191.

[30] S. Maheshwari, R. Sharma, *"The unit group of group algebra $\mathbb{F}_q\mathrm{SL}(2; Z_3)$"*, J. Algebra Comb. Discrete Appl. 3(1), 1-6, 2016

[31] N. Makhijani, R. K. Sharma, J. B. Srivastava, *"A note on the structure of $\mathbb{F}_{p^k}A_5/J(\mathbb{F}_{p^k}A_5)$"*, Acta Sci. Math. (Szeged) 82 (2016), no. 1-2, 29–43.

[32] G. Mittal, R. K. Sharma, *"Unit group of semisimple group algebras of some non-metabelian groups of order 120"*, Asian-European Journal of Mathematics, doi:https://doi.org/10.1142/S1793557122500590

[33] P. C. Milies, S. Sudarshan, *"An Introduction to Group Rings"*, ISBN: 978-1-4020-0238-0, Springer Science and Business Media, 31-Jan-2002 - Mathematics - 371 pages.

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

[35] M. Sahai, S. F. Ansari (2021) *"Unit groups of group algebras of groups of order 18"*, Communications in Algebra, DOI: 10.1080/00927872.2021.1893740.

[36] G. H. Tang, Y. Y. Gao, *"The unit group of FG of group with order* 12*"*, Int. J. Pure Appl. Math., 73 (2011), 143–158.

[37] R.S. Pierce, *"Associative Algebras"*, Graduate Texts in Mathematics, Springer-Verlag, New York (1982).

[38] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson "$\mathbb{ATLAS}$ *of finite groups. Maximal subgroups and ordinary characters for simple groups With computational assistance from J. G. Thackray"* Oxford University Press, Eynsham, 1985. xxxiv+252 pp. ISBN: 0-19-853199-0.