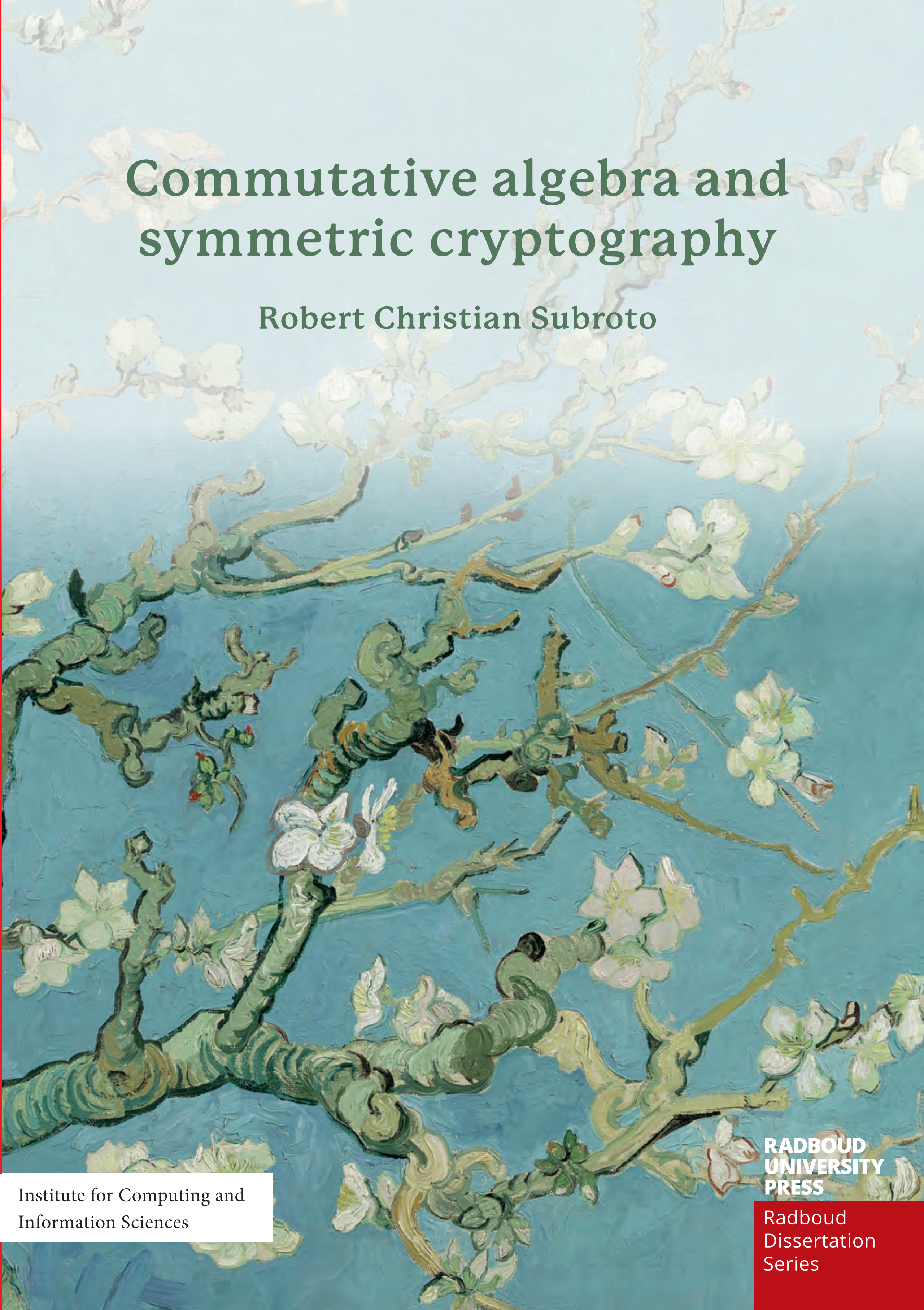

Commutative algebra and symmetric cryptography

Robert Christian Subroto

Institute for Computing and
Information Sciences

RADBOUD
UNIVERSITY
PRESS

Radboud
Dissertation
Series

Commutative algebra and symmetric cryptography

Robert Christian Subroto

Commutative algebra and symmetric cryptography
Robert Christian Subroto

Radboud Dissertation Series
ISSN: 2950-2772 (Online); 2950-2780 (Print)

Published by RADBOUD UNIVERSITY PRESS
Postbus 9100, 6500 HA Nijmegen, The Netherlands
www.radbouduniversitypress.nl

Design: Robert Christian Subroto
Cover: Robert Christian Subroto
Printing: DPN Rikken/Pumbo

ISBN: 9789465151472
DOI: 10.54195/9789465151472
Free download at: https://doi.org/10.54195/9789465151472

RADBOUD
UNIVERSITY
PRESS

Commutative algebra and symmetric cryptography

Proefschrift

ter verkrijging van de graad van doctor
aan de Radboud Universiteit Nijmegen
op gezag van de rector magnificus prof. dr. J.M. Sanders,
volgens besluit van het college voor promoties
in het openbaar te verdedigen op

vrijdag 21 november 2025
om 12.30 uur precies

door

Robert Christian Subroto

geboren op 2 juni 1995
te Jakarta, Indonesië

Promotor:

prof. dr. J.J.C. Daemen

Manuscriptcommissie:

prof. dr. B.J.J. Moonen (voorzitter)

prof. dr. S. Mesnager
Université Paris 8, Frankrijk

prof. dr. D. Kahrobaei
Queens College CUNY, Verenigde Staten

dr. M. Trimoska
Eindhoven University of Technology

dr. M. Borello
Université Paris 8, Frankrijk

Acknowledgments

First of all, I would like to thank prof. dr. Joan Daemen for being my supervisor, who provided me with valuable advice and research directions. I am especially grateful for the freedom he granted me for exploring more exotic aspects of symmetric cryptography, which led to a very enjoyable and rewarding PhD experience.

My family members are very dear to me, and I would like to thank them very much for their support. I am very grateful to my father Budi, my mother Liena and my sister Crista for their efforts in creating a supportive environment at home for me to work on my research, both during and after the COVID pandemic. I am also deeply thankful for the love and support of my girlfriend Jean. Her continuous support and efforts helped me go through difficult times during my PhD when I seemed to have lost vision and motivation.

I would like to thank my colleagues at the Digital Security department for our enjoyable conversations and discussions. Especially the people from the ESCADA group, Bart M, Bart van V, Vahid, Alireza, Yanis, Solane, Aldo, Charlotte, Mario, Silvia, Shahram, Lorenzo, Anna, Alex, Suprita and Cas. I would also like to thank the secretaries Janet, Shanley and Irma for making the department run smoothly. It is a blessing when you can consider your close colleagues as friends, like Daniël Kuijsters, Jan Schoone, Jonathan Fuchs, Marloes Venema and Koustabh Ghosh. I want to give a special thanks to Jan Schoone who not only put great effort into reviewing my papers and this thesis, but also for providing valuable input and being patient even in situations where others would most likely not be willing to.

I would like to thank my badminton friends like Zhenzhong, Yudai, Yining, Gilles, Niels, Kevin, Jian, Christiaan, Sinta, Sophia, Xinyue, Luuk and many others for the fun times on and off court. I would like to thank my friends Sven and Ernst for our fun times hanging out, and Timo and Stephan for our fun times together in Gielinor.

Contents

Chapter 1

Introduction

1.1 A brief introduction to symmetric cryptography

Cryptography is a subfield of computer science focussing on achieving secure communications. It can roughly speaking be split into two categories: symmetric cryptography and public-key cryptography. This thesis only discusses symmetric cryptography, which covers cryptographic techniques for encryption, data authentication and authenticated encryption where the sender and receiver share a single secret key. A cryptographic scheme consists of a set of functions and protocols enabling (one of) these cryptographic techniques. Let us go into these cryptographic techniques in more detail.

1.1.1 Cryptographic techniques

- **Encryption.** Encryption provides *confidentiality*, which means that no outside parties besides the sender and the receiver have access to the content of the transmitted data. This is achieved by encryption and decryption. Encryption involves transforming plaintext into ciphertext using the secret key which is unreadable. Decryption is the reverse process where one obtains the plaintext from the ciphertext. In general, an encryption scheme supports encryption and decryption of plaintexts of arbitrary length and ciphertexts respectively.

- **Data authentication.** Data authentication involves techniques proving authenticity of the transmitted data, i.e. proving that the data has not been tampered with. If for example Bob sends Alice a message, an adversary can intercept Bob's message and change it, and then send the altered message to Alice. When data authentication is applied, Alice can detect that the message she received was not the message sent by Bob. This is often done using a MAC function, which is a map with input the message and the secret key, and digest a fixed-length bit string called the tag. Bob sends this tag along with the message to Alice. Alice can then confirm the authenticity of the message by generating the tag herself from the received message and the shared secret key, and compare it to the tag she received.

- **Authenticated encryption.** Authenticated encryption involves techniques providing both confidentiality and data authentication for transmitted data. In many cases, schemes providing authenticated encryption are often the result of integrating both encryption and data authentication schemes simultaneously.

We discuss two types of cryptographic building blocks which are commonly used in designing cryptographic schemes: *Block ciphers* and *permutations*.

1.1.2 Block ciphers and modes

Mathematically speaking, a block cipher of block length n is a function $E: \mathbb{F}_2^n \times \mathbb{F}_2^k \to \mathbb{F}_2^n$ such that for any $K \in \mathbb{F}_2^k$, the induced map $E_K: \mathbb{F}_2^n \to \mathbb{F}_2^n$, $P \mapsto E(P, K)$ is a bijection. As such, a block cipher can be considered as a restricted encryption scheme which, given a key K of k bits, is only able to encrypt plaintexts and decrypt ciphertexts of length n. The block length n in common block ciphers is usually 64 or 128. A mode can be used on top of a given block cipher to design encryption schemes with arbitrary input and output bit length, or for designing any other cryptographic schemes mentioned above. Well-known examples of block ciphers are the Data Encryption Standard (DES) [SB88] and the Advanced Encryption Standard (AES) [DR20]. Examples of well-known modes are Electronic codebook (ECB) and Cipher block chaining (CBC) [FSK10].

The standard security goal of a block cipher E is that for any given key K, the map E_K should be hard to distinguish from an n-bit random permutation. When one can find properties of block ciphers which can distinguish them from a random permutation, it can be used to develop attacks for e.g. key recovery. Examples of such attacks are linear cryptanalysis [Mat93] and differential cryptanalysis [BS91].

1.1.3 Permutation-based cryptography

A permutation is a cryptographic building block which mathematically speaking is simply a bijective map $f: \mathbb{F}_2^b \to \mathbb{F}_2^b$, where b is called the width of the permutation f. Unlike block ciphers, a permutation does not have any key input. These permutations are then used in a higher level cryptographic construction, usually in a sponge [BDPV15] or duplex [BDPV11] construction, for designing cryptographic schemes.

Examples of permutations are Ascon-p [DEMS21] which is used in the lightweight cryptographic schemes specified in Ascon and Xoodoo [DHVV18] which is used in the deck function Xoofff and the cryptographic primitive Xoodyak.

Defining security goals for a cryptographic permutation f is not always straightforward. Instead, one usually defines security goals on the cryptographic constructions involving f. Examples of security goals for a sponge construction are pre-image resistance (it should be hard to find an input of a given digest) and second pre-image resistance (given an input and digest, it should be hard to find another input with the same digest). This indirectly sets security goals on f.

1.1.4 Iterated block ciphers and permutations

Most block ciphers and permutations are the result of multiple iterations of a simple round function R. A common technique of designing a round function consists of the composition of the following components:

- **Non-linear layer.** Examples are S-boxes and χ;
- **Linear layer.** These consist of all the linear step functions of the round function. The linear layers considered in this thesis are exclusively the composition of mixing- and shuffling step functions;
- **Round-constant addition.** In the case of block ciphers, this is usually a round key addition.

There are many other ways of designing round functions, which are not covered in this thesis. The design of the round function should be in such a way that the corresponding block cipher or permutation satisfies the above mentioned security claims. Examples of iterated permutations with this structure are Ascon-p, Xoodoo and the Subterranean 2.0 permutation [DMMR20]. An example of an iterated block cipher with the same structure is AES.

1.2 My PhD research

1.2.1 Motivation of my research

My research was motivated from an observation regarding the Xoodoo permutation. It was observed from numerical experiments that the order of the linear layer of Xoodoo only equals 32, which is surprisingly low given that Xoodoo operates on 384 bits. The order of the linear layer is defined as the order of the corresponding linear transformation when viewed as an element of the general linear group $\mathrm{GL}_{384}(\mathbb{F}_2)$. This might be a potential weakness against a cryptanalytic technique known as invariant subspace attacks [BCLR17].

An invariant subspace attack is a key recovery attack which is designed to attack iterated block ciphers whose round function consists of the stepfunctions mentioned above. The idea of invariant subspaces is as follows, as explained in [LAAZ11]: Consider an iterated block cipher E where its round function satisfies the structure discussed in Section 1.1.4. Denote a round function with round key addition k as $\mathrm{R}_k\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, and let $\mathrm{R}\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the composition of the linear and non-linear layer. We try to find proper linear subspaces $U \subset \mathbb{F}_2^n$ such that there exist constant values $c, d \in \mathbb{F}_2^n$ such that $\mathrm{R}(U + c) = U + d$. Such U is called an invariant subspace of R. If k is a round key which can be expressed as $k = u + c + d$ for some $u \in U$, observe that:

$$\mathrm{R}_k(U + d) = \mathrm{R}((U + d) + (u + c + d)) = U + c = U + d,$$

which implies that $U + d$ remains invariant under R_k. If all round keys are contained in $U + c + d$, then $U + d$ remains invariant under E, which yields a very efficient distinguisher for a fraction of the keys. Note that this only works when U is proper (i.e. not equal to the domain $\mathbb{F}_2^n$), as U is otherwise always invariant regardless of the round keys. However one should find proper U as large as possible to maximize the probability of the round keys being contained in $U + c + d$. A round function where its linear layer has a low order are more susceptible towards finding these invariant subspaces, as proven in [BCLR17].

As Xoodoo is a cryptographic permutation and not a block cipher, there is no concrete security claim. However, invariant subspace attacks do reveal structural properties of Xoodoo especially when the round constants are contained in the corresponding affine subspace $U + c + d$ of some invariant subspace U, which might be exploited for attacking cryptographic schemes using Xoodoo as permutation. A scenario where I can see this happening is that the structural properties might be used to construct second preimages of a class of preimages of for example a sponge construction using Xoodoo. Therefore, a proper mathematical framework which can explain the low order of the linear layer of Xoodoo can be used to analyse these properties in more detail, and possibly can lead to alternative designs which negates certain weaknesses. Finding such a mathematical framework however remained an open problem.

1.2.2 An unexpected solution

An unexpected result of my research is that such a mathematical framework can be found in the domain of commutative algebra. Commutative algebra is a branch of pure mathematics that focuses on the study of commutative rings and all related aspects. These vary from the internal algebraic structure of a commutative ring, to the theory of modules. An important observation is that the linear layer of Xoodoo can be described as a module homomorphism over some group algebra, where the key explanation of its low order lies in the algebraic structure of the underlying group algebra. The reason why the linear layer of Xoodoo can be interpreted this way is due to the fact that the construction of the linear step functions are based on cyclic shifts. Cyclic shifts are certain linear operators which are modelled by circulant matrices, and are a convenient tool for designing linear layers due to their simple description and their strong mixing and shuffling properties. Step functions whose designs rely on cyclic shifts, which we refer to for now as circulant step functions, can be interpreted as module homomorphisms over some group algebra. Examples of circulant step functions are circulant column parity mixers [SD18], which are a class of linear maps used as the mixing step in the round function of permutations like Xoodoo and Keccak-f [BDPV15]. The algebraic structure of the underlying group algebra reveals a lot about the algebraic structure of the related step functions.

Studying the structure of group algebras is interesting from both a mathematical and cryptographic point of view. From a mathematical perspective, finding the Krull-Remak-Schmidt decomposition [Sch12] (the group algebra equivalent of the prime number decomposition) reveals a lot about the internal algebraic structure of the group algebra. This is also very interesting from a cryptographic point of view, as the components of this decomposition can be used to construct linear subspaces which remain invariant under the circulant-based step functions, further enhancing the theory of invariant subspace attacks. In fact, one can construct a family of linear subspaces with this invariant property, such that their direct sum covers the whole domain. This is especially interesting for round functions where the linear layer consists only of circulant step functions such as Xoodoo, as this can be used to develop new distinguishers for the primitive, potentially leading to new cryptanalytic techniques.

1.2.3 Research goals

From a high level perspective, the main research questions of my PhD research can be formulated as follows:

1. How can linear mixing layers based on cyclic shifts be modelled as endomorphisms of free modules over group algebras over finite abelian groups?

2. What is the Krull-Remak-Schmidt decomposition of group algebras over finite abelian groups, with emphasis on the case where the base field is a finite field?

The first research question was motivated by the open problem to find a mathematical framework which can explain the low order of the linear layer of Xoodoo. The second research question was formulated to develop a complete algebraic framework of studying all linear layers which are constructed using cyclic shifts. I managed to answer these questions, which are covered in this thesis.

1.3 Contribution of the author

This thesis contains the main results based on the four single author papers produced by the author during his PhD, with the aim of answering the above formulated research questions. As such, all the main results are due to the author alone.

1.4 Thesis outline

Chapter 2 discusses some mathematical preliminaries required for the main results of the thesis.

Chapter 3 discusses the theory of group algebras over finite abelian groups. The results are based on the papers [Sub24c] and [Sub24b].

Chapter 4 discusses the theory of circulant modules, which form the theoretical foundation of connecting commutative algebra with symmetric cryptography. The results are based on the first part of the paper [Sub24a]. In this chapter, we elaborate on the technical details which were only briefly mentioned in the paper. The results of Chapter 3 are not required for this chapter, although we will refer to some notation which were introduced in Chapter 3.

Chapter 5 discusses the theory of circulant column parity mixers, which is a concrete application of the results in Chapter 4, although being still theoretical in nature. Therefore, Chapter 4 is required. The results of this chapter are based on the second part of the paper [Sub24a].

Chapter 6 discusses a mathematical analysis of the linear layer of Subterranean 2.0. The results of this chapter are based on the paper [Sub23]. This chapter serves as a stand-alone chapter.

Chapter 2

Preliminaries

This chapter serves as an overview of the mathematical background, including the notations and conventions used in this thesis. We assume the reader has a solid understanding and intuition of basic concepts of (abstract) algebra topics such as linear algebra, group theory, rings and fields. More advanced concepts from Galois theory, module theory and commutative algebra required for this thesis are briefly covered in this chapter, but having prior knowledge of these topics is strongly recommended.

2.1 Abstract algebra

We cover some concepts from abstract algebra which we utilise in this thesis.

2.1.1 Group action

Definition 2.1.1. Let G be a group and let X be a set. Then G is said to **act** on X if there is a function $\cdot : G \times X \to X$ satisfying two key properties:

- For $e \in G$ the identity element, we have $e \cdot x = x$ for all $x \in X$;
- For every $g, h \in G$ and $x \in X$, we have $(gh) \cdot x = g \cdot (h \cdot x)$.

Equivalently we say that such a function $\cdot : G \times X \to X$ induces a **group action** of G on X.

Such a group action induces a natural congruence relation on X: For $x, y \in X$, we say that x and y are congruent if and only if there exists $g \in G$ such that $g \cdot x = y$. The set of all elements in X congruent to x is called the **orbit** of x, and is denoted as $\mathrm{Orb}(x)$. Specifically:

$$\mathrm{Orb}(x) := \{g \cdot x : g \in G\}.$$

An immediate observation is that $\mathrm{Orb}(x) = \mathrm{Orb}(y)$ if and only if x and y are congruent. As such, we can choose a set of representatives in X for the orbits of the group action $\cdot$, where any element in an orbit can be chosen to represent the corresponding orbit.

2.1.2 Rings and ideals

Let R be a commutative ring with unity. We denote R^* as the set of multiplicatively invertible elements of R.

Let $\mathfrak{a}_1, \mathfrak{a}_2$ be ideals of R. We define addition of ideals as:

$$\mathfrak{a}_1 + \mathfrak{a}_2 := \{a_1 + a_2 : a_1 \in \mathfrak{a}_1 \text{ and } a_2 \in \mathfrak{a}_2\}.$$

We define multiplication of ideals as:

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 := \left\{ \sum_{i=1}^{n} a_i \cdot b_i : a_i \in \mathfrak{a}_1, b_i \in \mathfrak{a}_2, n \in \mathbb{Z}_{>0} \right\}.$$

We say that $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are coprime if and only if $\mathfrak{a}_1 + \mathfrak{a}_2 = R$. Equivalently, if and only if $1 \in \mathfrak{a}_1 + \mathfrak{a}_2$.

2.1.3 Fields and Galois theory

Let k be a field. We denote the algebraic closure of k by $\overline{k}$. For a field extension l/k, we represent the **degree of the extension** by $[l : k]$. Given an n-tuple $\vec{x} := (x_1, \ldots, x_n) \in \overline{k}^n$, we denote $k(\vec{x})$ as the smallest field extension of k that contains all entries of $\vec{x}$.

Galois theory is a profound and elegant branch of abstract algebra that establishes a deep connection between field theory and group theory. Named after the mathematician Évariste Galois, this theory provides a framework for understanding the solvability of polynomial equations by radicals and offers insight into the structure of field extensions.

Definition 2.1.2. Let k be a field, and l/k a finite dimensional field extension. The extension l/k is said to be a **Galois extension** if it is both **normal** and **separable**.

Given that l/k is a Galois extension, the **Galois group** of l/k is the group consisting of all field automorphisms $\sigma: l \to l$ that fix k, i.e., $\sigma(x) = x$ for all $x \in k$.

One of the most powerful results in Galois theory is the fundamental theorem of Galois theory, which establishes a one-to-one correspondence between the intermediate fields of a Galois extension l/k and the subgroups of its Galois group $\mathrm{Gal}(l/k)$.

Theorem 2.1.3 (**Fundamental theorem of Galois theory** [Ehr11, Theorem 4.10.1])**.** *Let l/k be a Galois extension with Galois group $\mathrm{Gal}(l/k)$. There is a one-to-one correspondence between the intermediate fields $k \subseteq h \subseteq l$ and the subgroups $H \subseteq \mathrm{Gal}(l/k)$. This correspondence is given by:*

- *For each intermediate field h, the corresponding subgroup H is $\mathrm{Gal}(l/h)$;*
- *For each subgroup H, the corresponding intermediate field h is the fixed field of H, denoted l^H, consisting of elements in l that are fixed by every automorphism in H.*

Additionally, h is a normal extension of k if and only if H is a normal subgroup of $\mathrm{Gal}(l/k)$. In this case, the Galois group $\mathrm{Gal}(h/k)$ is isomorphic to the quotient group $\mathrm{Gal}(l/k)/H$.

This theorem provides a powerful tool for analyzing the structure of field extensions and understanding their properties through the lens of group theory.

Cyclotomic extensions

A cyclotomic extension over a field k is defined as follows:

Definition 2.1.4. Let $\mu_m \subset \overline{k}$ be the set of all the roots of the polynomial $f_m(X) := X^m - 1 \in k[X]$. Then the m-th **cyclotomic extension** over k is defined as the field extension $k(\mu_m)/k$. For convenience, we sometimes denote the field $k(\mu_m)$ simply as k_m.

An important result is that every cyclotomic extension is a Galois extension with abelian Galois group, regardless of the base field k and the cyclotomic degree m. These insights are fundamental to many applications and results in this thesis.

2.1.4 Finite fields

A field is called a finite field if it has a finite number of elements. The number of elements in a finite field k is known as its order. A finite field of order q exists if and only if q is a power of a prime number p, meaning q must be of the form p^t for some positive integer t. Such a field must have characteristic p. All fields of the same order are isomorphic, and no finite field can have distinct subfields with the same order. Therefore, we can unambiguously denote a finite field of order q by $\mathbb{F}_q$.

Field extensions of finite fields

Every field extension of $\mathbb{F}_q$ is of the form $\mathbb{F}_{q^t}$ for some positive integer t, where it satisfies $[\mathbb{F}_{q^t} : \mathbb{F}_q] = t$. Conversely, for every positive integer t, there exists a unique field extension of $\mathbb{F}_q$ of degree t, which is isomorphic to the field $\mathbb{F}_{q^t}$. Finite field extensions behave very nicely in view of Galois theory.

Theorem 2.1.5 ([Lan04, Theorem 5.5, Chapter V.5])**.** *Every finite extension $\mathbb{F}_{q^t}/\mathbb{F}_q$ is a Galois extension, and the corresponding Galois group* $\mathrm{Gal}(\mathbb{F}_{q^t}/\mathbb{F}_q)$ *is a cyclic group of order t, generated by the field automorphism $\sigma\colon \mathbb{F}_{q^t} \to \mathbb{F}_{q^t}, x \mapsto x^q$, known as the* ***Frobenius automorphism****.*

Let $m > 0$ be coprime to $q = p^t$, and let μ_m denote the m-roots of unity in the algebraic closure $\overline{\mathbb{F}}_q$. Then $\mu_m \subseteq \mathbb{F}_q$ if and only if $m \mid q - 1$. If m does not divide $q - 1$, then $\mathbb{F}_q(\mu_m) = \mathbb{F}_{q^l}$ where l is the smallest possible integer such that $m \mid q^l - 1$. In other terms, l is the order of q in $(\mathbb{Z}/m\mathbb{Z})^*$.

2.1.5 Multivariate polynomials

Multivariate polynomials play an important role in this thesis. We introduce some common notation we use throughout the thesis when working with multivariate polynomials. We denote the multivariate polynomial ring with n indeterminates by $k[X_1, \dots, X_n]$. We refer to the set of monomials in n variables as $\mathrm{Mon}(n)$. For a polynomial $f \in k[X_1, \dots, X_n]$, we denote the coefficient of the monomial $M \in \mathrm{Mon}(n)$ in f as $\mathrm{coeff}_M(f)$.

For a monomial $M := \prod_{i=1}^n X_i^{m_i} \in \mathrm{Mon}(n)$, we define the **total degree** of M as $\deg(M) := \sum_{i=1}^n m_i$. We define the ***i*-th partial degree** of f as $\deg_i(f) := m_i$. For a polynomial $f \in k[X_1, \dots, X_n]$, we define the total degree of f as:

$$\deg(f) := \max(\deg(M) : M \in \mathrm{Mon}(n) \text{ and } \mathrm{coeff}_M(f) \neq 0).$$

Similarly, we define the i-th partial degree of f as:

$$\deg_i(f) := \max(\deg_i(M) : M \in \mathrm{Mon}(n) \text{ and } \mathrm{coeff}_M(f) \neq 0).$$

Example 2.1.6. *For example, take the multivariate polynomial:*

$$f(X_1, X_2, X_3) := X_1^2 - 6X_1X_2^2X_3^5 - 4X_1X_2^4 - 7X_1^2 \in \mathbb{R}[X_1, X_2, X_3].$$

Then the second term of f has the highest total degree which equals $1+2+5 = 8$. Hence the total degree of f equals $\deg(f) = 8$. Looking at the partial degrees, we have $\deg_1(f) = 2$, $\deg_2(f) = 4$ and $\deg_3(f) = 5$.

2.2 Module theory

Module theory is a branch of mathematics that generalizes concepts such as vector spaces, rings, linear representations, and various other algebraic structures. This unified approach enables the study of a wide range of algebraic objects under a common framework. In this section, we outline the essential aspects of module theory that are required for the analyses and results presented in this thesis.

2.2.1 Formal introduction

We provide formal definitions of basic module-theoretic concepts, which we split into several parts.

Modules and submodules

Definition 2.2.1. Let R be a ring with unity (not necessarily commutative), and let $(V, +)$ be an abelian group. A **left R-module** on V consists of an operation $\cdot : R \times V \to V$ such that for all $r, s \in R$ and $x, y \in V$, we have:

$$\begin{aligned} r \cdot (x + y) &= r \cdot x + r \cdot y \\ (r + s) \cdot x &= r \cdot x + s \cdot x \\ (rs) \cdot x &= r \cdot (s \cdot x) \\ 1 \cdot x &= x. \end{aligned}$$

If R and $\cdot$ are clear from the context, then the R-module is simply referred to as V. A **right R-module** is defined similarly, with the only difference that the operation is now defined as $\cdot : V \times R \to V$, where R and the V are switched.

When R is a commutative ring, both left and right modules are the same.

Example 2.2.2. *For an integer $n > 0$, the set R^n with coordinate-wise left (resp. right) scaling by R is an R-module. Such R-modules are called **free R-modules**.*

Definition 2.2.3. A **left R-submodule** V' of V is a subgroup of V such that $r \cdot v \in V'$ for all $r \in R$ and $v \in V'$. A right R-submodule is defined similarly.

Example 2.2.4. *Let R be a ring viewed as a left (or right) module over itself. Then the submodules of R are exactly the left (or right) ideals.*

Example 2.2.5. *Let V be a left R-module, let $\mathfrak{a}$ be a left ideal of R, and define:*

$$\mathfrak{a}V := \left\{ \sum_{i=0}^{t} a_i \cdot v_i \mid a_i \in \mathfrak{a}, v_i \in V, t \in \mathbb{Z}_{>0} \right\},$$

which means that $\mathfrak{a}V$ consists of finite sums of terms of the form $a \cdot v$ where $a \in \mathfrak{a}$ and $v \in V$. Unless $V = \{0\}$, $\mathfrak{a}V$ is in many cases a proper R-submodule of V. Nakayama's Lemma, which we introduce in Lemma 2.3.4, is very useful in studying these types of submodules.

Module homomorphism

Let V_1 and V_2 be left R-modules. A map $\theta\colon V_1 \to V_2$ is an R-module homomorphism (or is R-linear) if it satisfies the following properties:

$$\theta(x + y) = \theta(x) + \theta(y)$$
$$\theta(rx) = r \cdot \theta(x)$$

for all $x, y \in V_1$ and $r \in R$. If moreover θ is bijective, then V_1 and V_2 are called isomorphic to each other.

Induced modules

Let S be another ring, and let $\varphi\colon R \to S$ be a ring homomorphism. Let V be an abelian group, and assume it has both a left R- and S-module structure, which we denote by V_R and V_S respectively. We say that V_R is **induced** by V_S under φ if for every $r \in R$ and $v \in V$, we have:

$$r \cdot v = \varphi(r) \cdot v.$$

2.2.2 Types of modules

In this section, we summarize the specific types of modules utilized in this thesis. Throughout this discussion, R denotes a ring, and all R-modules considered are left R-modules.

Finitely generated modules

A left R-module V is said to be **finitely generated** if there exists a family of finitely many elements $v_1, ..., v_n \in V$ such that for every $v \in V$, there exists $r_1, ..., r_n \in R$ such that:

$$v = r_1 \cdot v_1 + \cdots + r_n \cdot v_n.$$

Free modules

A left R-module V is called **free** of rank m if it is isomorphic to the R-module R^m, where its elements are represented by the column vector $v = (r_0, ..., r_{m-1})^{\mathrm{T}}$, where addition is defined coordinate-wise. Equivalently, V is free if there exist elements $\mathrm{e}_0, ..., \mathrm{e}_{m-1} \in V$ such that every element $v \in V$ is **uniquely** expressed as:

$$v = \sum_{i=0}^{m-1} r_i \cdot \mathrm{e}_i, \tag{2.1}$$

where $r_i \in R$. The analogous definition holds for right R-modules, with the order reversed. We call $\{\mathrm{e}_0, ..., \mathrm{e}_{m-1}\}$ an R-**basis** of V.

Artinian modules

A family of left R-submodules $V_1, V_2, V_3, \ldots$ is said to be a **descending chain** if $V_1 \supseteq V_2 \supseteq V_3 \supseteq \ldots$. A left R-module V is said to be **Artinian** if every descending chain of left R-submodules $V_1, V_2, V_3, \ldots$ of V becomes stationary, i.e., there exists an integer $m > 0$ such that $V_n = V_m$ for all $n \geq m$.

Noetherian modules

Similarly, a family of left R-submodules $V_1, V_2, V_3, \ldots$ is said to be an **ascending chain** if $V_1 \subseteq V_2 \subseteq V_3 \subseteq \ldots$. A left R-module V is said to be **Noetherian** if every ascending chain of left R-submodules $V_1, V_2, V_3, \ldots$ of V becomes stationary, i.e., there exists an integer $m > 0$ such that $V_n = V_m$ for all $n \geq m$.

Faithful modules

A left R-module V is called **faithful** if for every $r \in R \setminus \{0\}$ there exists a $v \in V$ such that $r \cdot v \neq 0$. This implies that for all $x \neq y$ in R, there exists a $v \in V$ such that $x \cdot v \neq y \cdot v$. A straightforward but important example is when V equals R itself, where the left module action is the left ring multiplication of R.

Simple modules

A left R-module V is called **simple** if V is non-zero, and it contains no proper submodule.

Semisimple modules

A left R-module V is called **semisimple** if it can be expressed as a direct sum of a family of simple submodules.

Indecomposable modules

A left R-module V is said to be **indecomposable** if it cannot be written as a direct sum of two non-zero R-submodules of V. Observe that all simple modules are indecomposable, but the converse does not generally hold.

Projective modules

A left R-module V is called **projective** if it is a direct summand of a free R-module. An immediate consequence is that any direct summand of projective modules is also projective.

2.2.3 Krull-Remak-Schmidt decomposition

Indecomposable modules serve as fundamental building blocks for a wide class of modules, similar to the way positive integers can be uniquely decomposed into prime factors. The Krull-Remak-Schmidt theorem formalizes this analogy, demonstrating that given a left R-module V, V can be uniquely expressed as a direct sum of indecomposable submodules under certain conditions on the underlying ring R and the module V. This decomposition provides a deeper understanding of the module's structure, similar to how the prime factorization of an integer reveals its fundamental properties.

Theorem 2.2.6 (**Krull-Remak-Schmidt** [Sch12, Theorem 1.4.7]). *Let R be a left Artinian ring, and let V be a finitely generated left R-module. Then the following statements hold:*

1. *There exists an R-module decomposition $V \cong \bigoplus_{i=1}^{s} V_i$ where the V_i are indecomposable left R-modules;*

2. *This decomposition is unique up to isomorphism, meaning that if V has another decomposition $\bigoplus_{j=1}^{s'} V_j'$ into indecomposable left R-modules, then:*

   i. *$s = s'$;*

   ii. *there is a permutation σ of $\{1, \ldots, s\}$ such that $V_i' \cong V_{\sigma(i)}$ for all $1 \leq i \leq s$.*

The unique decomposition provided by the Krull-Remak-Schmidt theorem is known as the **Krull-Remak-Schmidt decomposition**. In the special case where V is semisimple and satisfies the conditions of the Krull-Remak-Schmidt theorem, the components of its decomposition are necessarily simple modules. This specific scenario, where the sole focus is on the decomposition of semisimple R-modules into simple components, is known as the **semisimple decomposition**.

2.2.4 Jacobson radical and projective envelopes

Let R be a ring. The **Jacobson radical** $\operatorname{Jac}(R)$ of R consists of all elements $r \in R$ such that $r \cdot M = 0$ for all simple R-modules M.

Theorem 2.2.7 ([Sch12, Proposition 1.2.1]). *We have the following equivalent criteria for* $\operatorname{Jac}(R)$*:*

1. $\operatorname{Jac}(R)$ *is the smallest submodule of R such that $R/\operatorname{Jac}(R)$ is a semisimple R-module;*

2. $\operatorname{Jac}(R)$ *is the intersection of all maximal left ideals of R;*

3. $\operatorname{Jac}(R)$ *is the largest nilpotent left ideal of R (a left ideal I is nilpotent if $I^n = 0$ for some integer n);*

4. $\operatorname{Jac}(R)$ *is the intersection of all maximal right ideals of R;*

3. $\operatorname{Jac}(R)$ *is the largest nilpotent right ideal of R (a right ideal I is nilpotent if $I^n = 0$ for some integer n).*

The Jacobson radical is closely related to the Krull-Remak-Schmidt decompositions of finitely generated left R-modules. This is explained using the theory of projective modules and projective covers:

An R-module homomorphism $f: M \to M'$ is called **essentially surjective** if f is surjective, but its restriction to any proper submodule of M is not. A **projective cover** of an R-module M is a projective R-module P together with an essential homomorphism $f: P \to M$.

Theorem 2.2.8 ([Sch12, Proposition 1.6.10])**.** *Let R be a left Artinian ring. Then we have the following statements regarding projective covers:*

- *Every finitely generated left R-module M has a projective cover, and it is unique up to isomorphism;*
- *If P is a finitely generated projective left R-module, then the quotient map $P \to P/\operatorname{Jac}(R)P$ is essentially surjective;*
- *The projective indecomposable left R-modules are in bijection with the simple left R-modules. In this bijection, the projective indecomposable P corresponds with the simple left R-module $M = P/\operatorname{Jac}(R)P$. The projective cover of M is P.*

The theory of projective modules and projective covers connects the indecomposable components of the Krull-Remak-Schmidt decomposition of the R-module V, to the simple components of the semisimple decomposition of the semisimple R-module $V/\operatorname{Jac}(R)V$.

2.3 Commutative algebra

Commutative algebra is a branch of abstract algebra focused exclusively on the properties and structures related to commutative rings. This includes a wide range of topics, from the internal algebraic structure of commutative rings to the study of modules over these rings. In this section, we present the essential aspects of commutative algebra that are utilized in this thesis.

2.3.1 Chinese remainder theorem

The Chinese remainder theorem is a fundamental result in number theory. It has numerous applications within and outside of mathematics. A notable example of its application is in the RSA encryption scheme. The number-theoretic version of the Chinese remainder theorem can be stated as follows:

Theorem 2.3.1 (**Chinese remainder theorem**). *Let $n_1, \ldots, n_k$ be positive integers which are pairwise coprime, which we call the coprime moduli. Define $N = \prod_{i=1}^{k} n_i$. Let $a_1, \ldots, a_k$ be integers such that $0 \leq a_i < n_i$ for every i. Then there exists a unique integer $0 \leq a < N$ such that for all $1 \leq i \leq k$, we have:*

$$a \equiv a_i \bmod n_i.$$

The number-theoretic statement of the Chinese remainder theorem provides a way to solve systems of simultaneous congruences with pairwise coprime moduli. This result can be extended to a more general framework within ring theory, which is stated as follows:

Theorem 2.3.2 (**Chinese remainder theorem for rings**). *Let R be a commutative ring with unity, and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be pairwise coprime ideals of R. Then the following natural ring homomorphism is a ring isomorphism:*

$$R/\bigcap_{i=1}^{n} \mathfrak{a}_i \to (R/\mathfrak{a}_1) \times (R/\mathfrak{a}_2) \times \ldots \times (R/\mathfrak{a}_n).$$

This version of the Chinese remainder theorem is of particular interest in this thesis, especially in the case where R is a quotient ring of a multivariate polynomial ring.

2.3.2 Local rings and localization

We briefly discuss some concepts related to local rings.

Local rings

Definition 2.3.3. A commutative ring R is called **local** if it has exactly one maximal ideal, denoted by $\mathfrak{m}$. The field $R/\mathfrak{m}$ is called the **residue field** of R.

A notable characteristic of local rings is that an element $r \in R$ is invertible if and only if $r \notin \mathfrak{m}$.

Local rings have been well studied in commutative algebra, resulting in many interesting properties. For example, a local ring R viewed as a left module over itself is always indecomposable, though not simple. Moreover, Nakayama's lemma [Ati18, Proposition 2.6], a fundamental result in module theory over commutative rings, restricted to local rings establishes a close relation between modules over local rings and vector spaces.

Lemma 2.3.4 (**Nakayama's lemma for local rings**)**.** *Let R be a local ring, $\mathfrak{m}$ its maximal ideal, and $k = R/\mathfrak{m}$ the residue field. Let V be a finitely generated left R-module with the quotient map $\mathfrak{q}_{\mathfrak{m}}: V \to V/\mathfrak{m}V$. Then for any generating set $\{v_1, \ldots, v_n\}$ of V, the set $\{\mathfrak{q}_{\mathfrak{m}}(v_1), \ldots, \mathfrak{q}_{\mathfrak{m}}(v_n)\}$ is a generating set of the k-vector space $V/\mathfrak{m}V$.*

Conversely, given any generating set $\{a'_1, \ldots, a'_m\}$ of the k-vector space $V/\mathfrak{m}V$, any subset $\{a_1, \ldots, a_m\}$ of V such that $\mathfrak{q}_{\mathfrak{m}}(a_i) = a'_i$ for all $1 \le i \le m$ is a generating set of V.

Localization at a prime ideal

Localization at a prime ideal $\mathfrak{p}$ is a process applied to a commutative ring R and a prime ideal $\mathfrak{p}$. The intuition behind localization of R at $\mathfrak{p}$ is to construct a local ring denoted $R_{\mathfrak{p}}$ in which one can embed R such that, roughly speaking, elements of $S := R \setminus \mathfrak{p}$ become invertible. We now give the concrete construction.

Given R and S as above, consider the product space $R \times S$. One can define an equivalence relation on $R \times S$ as follows: the elements (r_1, s_1) and (r_2, s_2) are equivalent if there exists a $t \in S$ such that $t(s_1 r_2 - s_2 r_1) = 0$. The equivalence class of $(r, s) \in R \times S$ is denoted as $\frac{r}{s}$. The localization $R_{\mathfrak{p}}$ is defined as the set of the equivalence classes of the above equivalence relation. The set $R_{\mathfrak{p}}$ forms a commutative ring where addition and multiplication is defined as follows:

$$\begin{aligned} \frac{r_1}{s_1} + \frac{r_2}{s_2} &= \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} && \text{(addition)}, \\ \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} &= \frac{r_1 r_2}{s_1 s_2} && \text{(multiplication)}. \end{aligned}$$

Here we have additive identity $\frac{0}{1}$ and multiplicative identity $\frac{1}{1}$. Moreover, $R_{\mathfrak{p}}$ is local with maximal ideal $\mathfrak{p} \cdot R_{\mathfrak{p}} := \left\{ \frac{x}{s} : x \in \mathfrak{p} \text{ and } s \in S \right\}$.

This construction allows for the examination of properties of R in a more localized context, due to the ring homomorphism:

$$l_{\mathfrak{p}}: R \to R_{\mathfrak{p}}, \ r \mapsto \frac{r}{1}.$$

It is worth mentioning that $l_{\mathfrak{p}}$ is in general not injective, only if $R \setminus \mathfrak{p}$ contains no zero divisors. A more detailed discussion about localization including proof of the above made claims can be found in [Kem10].

2.3.3 Decomposition of commutative Artinian unital rings

Let R be a commutative Artinian unital ring. When viewed as a left module over itself, the Krull-Remak-Schmidt theorem (Theorem 2.2.6) implies that there exists a family of finitely many indecomposable left R-modules $V_1, \ldots, V_n$ such that $R \cong \bigoplus_{i=1}^n V_i$. As such, for each $1 \leq i \leq n$, there exists a family of left R-submodules R_i of R such that $R \cong \bigoplus_{i=1}^n R_i$ and $R_i \cong V_i$ as left R-modules. This means that there is an isomorphism $\pi \colon R \to \bigoplus_{i=1}^n R_i$, from which we define the projection maps $\pi_i \colon R \to R_i$. Observe that R_i itself is a commutative unital ring: It is closed under multiplication by being an R-submodule, and $\pi_i(1)$ acts as the unit element in R_i. One can immediately verify that R_i viewed as a left R-submodule, is in fact induced from the ring R_i viewed as a left module over itself under π_i. Since R_i as a left R-module is indecomposable, so too must R_i as a left module over itself.

Indecomposable rings are closely related to local rings. Though all local rings are indecomposable, the reverse statement is not true. However, the indecomposable rings considered in this thesis are also local rings.

Every commutative ring viewed as a module over itself is a simple module if and only if it is a field. As such, the module R over itself is semisimple if and only if the ring components in the decomposition are fields. These types of rings are also called **semisimple rings**.

2.3.4 Free modules over commutative rings

Consider the free R-module R^n, where R is a commutative ring. Each matrix $M \in \operatorname{Mat}_n(R)$ induces the following R-endomorphism:

$$\hat{M} \colon R^n \to R^n, \; v \mapsto M \cdot v.$$

Here we view v as an n-dimensional column vector. This gives rise to a natural ring homomorphism:

$$\operatorname{Mat}_n(R) \to \operatorname{End}_R(R^n).$$

An important observation is that this map is bijective, meaning every endomorphism of R^n has a unique matrix representation in $\operatorname{Mat}_n(R)$.

Many concepts from matrices over fields extend naturally to the setting of matrices over general commutative rings. The determinant of a matrix over R is defined in the same way as the determinant over fields. For $A \in \operatorname{Mat}_n(R)$, we denote the **determinant** by $\det(A)$. For matrices $A, B \in \operatorname{Mat}_n(R)$, the determinant satisfies

$$\det(A \cdot B) = \det(A) \cdot \det(B).$$

A matrix $A \in \operatorname{Mat}_n(R)$ is invertible if and only if $\det(A)$ is invertible in R.

The notions of eigenvectors and eigenvalues are similar to those in linear algebra. A vector $v \in R^n$ is an eigenvector of A if there exists $\lambda \in R$ such that $A(v) = \lambda \cdot v$. Here, λ is called the eigenvalue of v under A. The concept of an eigenbasis is also analogous: A has an eigenbasis if there exists a basis of V consisting of eigenvectors of A.

2.3.5 Algebraic geometry

We cover some basic notions and results from affine algebraic geometry.

Definition 2.3.5. Let k be a field, and let $\mathfrak{a}$ be an ideal in the polynomial ring $k[X_1, \ldots, X_n]$. The **vanishing set** of $\mathfrak{a}$, denoted by $\mathcal{V}(\mathfrak{a})$, is defined as the set:

$$\mathcal{V}(\mathfrak{a}) := \{\mathbf{x} := (x_1, \ldots, x_n) \in \overline{k}^n \mid f(\mathbf{x}) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

For k an algebraically closed field, there is a fundamental result relating the vanishing sets in k^n and the radical ideals in $k[X_1, \ldots, X_n]$. This result is known as Hilbert's Nullstellensatz.

Theorem 2.3.6 (**Hilbert's Nullstellensatz** [Kem10, Theorem 1.17])**.** *Let k be an algebraically closed field. Then the following map is a bijection:*

$$\begin{aligned} \{\textit{radical ideals of } k[X_1, \ldots, X_n]\} &\to \{\textit{vanishing sets in } k^n\}, \\ \mathfrak{a} &\mapsto \mathcal{V}(\mathfrak{a}). \end{aligned}$$

Hilbert's Nullstellensatz is a powerful result, but requires the base field to be algebraically closed. This is not the case when looking at applications in cryptography, since the base field is usually a finite field. The Combinatorial Nullstellensatz is a weaker version of Hilbert's Nullstellensatz, but with the added benefit that it does not require the base field to be algebraically closed. This result together with its applications will be discussed in Chapter 3.

2.4 Representation theory

2.4.1 Introduction to representation theory

Let G be a finite group (not necessarily abelian), and let V be a finite-dimensional vector space over some field k. A linear representation of G is defined as a group homomorphism:

$$\rho\colon G \to \mathrm{GL}(V) = \mathrm{Aut}(V).$$

For convenience, we refer to V as the representation when ρ is clear from the context. For a linear subspace $W \subset V$, we say that W is a subrepresentation of V if for all $g \in G$ and $w \in W$, $\rho(g)(w) \in W$. Observe that W naturally inherits a linear representation of G from V. We say that a linear representation V is irreducible if it does not contain non-trivial subrepresentations.

Theorem 2.4.1 (**Maschke's theorem** [Lan04, Theorem 1.2, Chapter XVIII.1])**.** *Let k be a field, p its characteristic, and let G be a finite group. Let $\rho\colon G \to \mathrm{GL}(V)$ be a linear representation, where the order of G is coprime to p. Let W be a subrepresentation of V. Then there exists a complement subspace W^0 of W such that W^0 is a subrepresentation of V.*

A consequence of Maschke's theorem is that when the order of G is coprime to the characteristic of k, any finite-dimensional representation V is isomorphic to a direct sum of irreducible representations. Concretely, this means that $V \cong V_1 \oplus V_2 \oplus \ldots \oplus V_n$, where $V_1, \ldots, V_n$ are irreducible representations of G. These components are unique up to isomorphism. An important part of representation theory is classifying the irreducible representations of a given group G, in which the group algebra $k[G]$ plays a significant role.

2.4.2 Group algebras and regular representations

The **group algebra** $k[G]$ is a ring whose elements are formal k-linear combinations of elements of G. Concretely:

$$k[G] \coloneqq \left\{ \sum_{g \in G} c_g \cdot g : c_g \in k \right\}.$$

For $a \coloneqq \sum_{g \in G} a_g \cdot g \in k[G]$ and $b \coloneqq \sum_{g \in G} b_g \cdot g \in k[G]$, addition is given by adding the coefficients component-wise:

$$a + b \coloneqq \sum_{g \in G} (a_g + b_g) \cdot g,$$

and multiplication is the convolution product, which is defined as:

$$a \cdot b := \sum_{g \in G} \sum_{g' \in G} (a_g b_{g'}) \cdot gg' = \sum_{g \in G} \left(\sum_{g' \in G} a_{g \cdot (g')^{-1}} b_{g'} \right) \cdot g. \tag{2.2}$$

The group algebra $k[G]$ inherits a natural linear representation denoted $\rho_G : G \to \mathrm{GL}(k[G])$, where for every $g' \in G$ and $a := \sum_{g \in G} a_g \cdot g \in k[G]$, we have:

$$\rho_G(g')(a) := \sum_{g \in G} a_g \cdot gg' \in k[G].$$

This representation on $k[G]$ is also known as the **regular representation** of G over k. A key insight in representation theory is that any irreducible representation over G is isomorphic to an irreducible component of ρ_G. Hence, classifying all irreducible representations over G up to isomorphism is equivalent to finding all irreducible components of ρ_G.

2.4.3 Module theoretic approach

Building on the earlier discussion of Maschke's theorem and the group algebra $k[G]$, the module-theoretic approach to representation theory offers an alternative and more abstract point of view.

In this approach, a finite-dimensional representation V of a finite group G over a field k is viewed as a $k[G]$-module. The group algebra $k[G]$ acts on V through the representation $\rho : G \to \mathrm{Aut}(V)$. More concretely, the left module action of $k[G]$ on V is defined as:

$$k[G] \times V \to V, \left(\sum_{g \in G} a_g \cdot g, v \right) \mapsto \sum_{g \in G} a_g \cdot \rho(g)(v).$$

This action aligns with the module axioms. Subrepresentations of V correspond to left $k[G]$-submodules, providing a natural way to study their structure.

From a module-theoretic approach, the irreducible representations of G correspond to simple left $k[G]$-modules and vice versa. Hence if the conditions of Maschke's theorem are met (where the order of G is coprime to the characteristic of k), all left $k[G]$-modules are semisimple modules, meaning that every left $k[G]$-module can be decomposed into a direct sum of simple left $k[G]$-modules. These components are unique up to isomorphism. The decomposition of semisimple modules into simple components is simply referred to as the semisimple decomposition.

When viewing the group algebra $k[G]$ as a left module over itself under the regular representation ρ_G, the action of an element $a \in k[G]$ on $b \in k[G]$ is the same as the multiplication $a \cdot b$ as defined in Eq. (2.2). A crucial insight from the module-theoretic approach is that every irreducible representation of G can be identified with a simple component of ρ_G. This equivalence means that understanding the algebraic structure of $k[G]$-modules directly informs the classification of all possible representations of G. In the case where the conditions of Maschke's theorem are met, the semisimple decomposition of $k[G]$ classifies all irreducible representations of G over k.

2.4.4 Modular representation theory

Modular representation theory studies the algebraic structure of $k[G]$-modules where we drop the assumption that the order of G is coprime to the characteristic p of k. Since this fails the assumptions of Maschke's theorem, $k[G]$ as a left module over itself is not guaranteed to be semisimple anymore. The assumption that $k[G]$ can be decomposed into simple components is too strong. Instead, one should consider indecomposable modules in view of the Krull-Remak-Schmidt decomposition (Theorem 2.2.6). Since $k[G]$ is Artinian when G is finite, it satisfies the conditions of the Krull-Remak-Schmidt theorem, and thus allows such a decomposition.

Chapter 3

Group algebras over finite abelian groups

3.1 Introduction

In this chapter, we present the Krull-Remak-Schmidt decomposition of group algebras over finite abelian groups, when viewed as a left module over itself. We achieve this by studying a special type of coordinate rings that we call circulant rings. These are regarded as the geometric analogue of commutative group algebras, as they contain all the algebraic information of these group algebras.

This chapter is a compilation of the results in the papers [Sub24c] and [Sub24b].

3.2 Circulant rings: A geometric approach

We introduce circulant rings, which are a type of coordinate ring considered to be the geometric analogue of group algebras over finite abelian groups.

3.2.1 Introducing circulant rings

We provide a formal definition of circulant rings.

Definition 3.2.1. Let k be a field, and let $\vec{m} := (m_1, \ldots, m_n) \in \mathbb{Z}^n_{>0}$ be an n-tuple of positive integers. A **circulant ring** over k with parameters $\vec{m}$, denoted by $\mathcal{C}_{\vec{m}/k}$, is defined as the coordinate ring:

$$\mathcal{C}_{\vec{m}/k} := k[X_1, \dots, X_n]/(X_1^{m_1} - 1, \dots, X_n^{m_n} - 1).$$

The ideal $(X_1^{m_1} - 1, \dots, X_n^{m_n} - 1)$ is denoted by $\mathfrak{a}_{\vec{m}}$.

Observe that $\mathcal{C}_{\vec{m}/k}$ can also be expressed as $k[X_1, \dots, X_n]/\mathfrak{a}_{\vec{m}}$.

Proposition 3.2.2. *The set:*

$$\{f \in k[X_1, \dots, X_n] \mid \deg_i(f) < m_i \text{ for all } 1 \le i \le n\},$$

is a set of representatives of $\mathcal{C}_{\vec{m}/k}$, which we call the ***standard set of representatives****.*

Proof. This follows by applying long division with respect to the partial polynomial degrees. □

Remark 3.2.3. Define the set of monomials:

$$M_{\vec{m}} := \left\{ \prod_{i=1}^{n} X_i^{j_i} \mid 0 \le j_i < m_i \right\}.$$

Proposition 3.2.2 implies that $M_{\vec{m}}$ is a basis of $\mathcal{C}_{\vec{m}/k}$ viewed as a vector space over k. This insight is especially useful in Chapter 4.

3.2.2 Group algebras and circulant rings

We show the connection between circulant rings and group algebras of finite abelian groups.

Theorem 3.2.4. *Consider the group $G = \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ where the m_i are positive integers. Then the following map is an isomorphism of k-algebras:*

$$\Phi_G \colon k[G] \to \mathcal{C}_{\vec{m}/k}, \ \sum_{g \in G} f_g \cdot g \mapsto \sum_{g \in G} f_g \cdot \prod_{i=1}^{n} X_i^{g_i},$$

where $g := (g_1, \dots, g_n) \in G$ and $\vec{m} = (m_1, \dots, m_n)$.

Proof. The following set of polynomials:

$$\left\{ f_g \cdot \prod_{i=1}^{n} X_i^{g_i} : 0 \le g_i < m_i \text{ and } f_g \in k \right\},$$

is simply another representation of the set of standard representatives introduced in Proposition 3.2.2. Therefore, Φ_G is a well-defined bijective map. The identities $\Phi_G(f+f') = \Phi_G(f)+\Phi_G(f')$ and $\Phi_G(c\cdot f) = c\cdot\Phi_G(f)$ for $f, f' \in k[G]$ and $c \in k$ are immediate.

For multiplication, define the set $\hat{G} := \{(g_1,\dots,g_n) \in \mathbb{Z}^n_{\geq 0} : 0 \leq g_i < m_i\}$, which is the underlying set of G viewed as a subset of the n-tuples of integers ≥ 0. Observe that:

$$\begin{aligned}\Phi_G(f)\cdot\Phi_G(f') &= \left(\sum_{g\in\hat{G}} f_g \cdot \prod_{i=1}^n X_i^{g_i}\right)\cdot\left(\sum_{g'\in\hat{G}} f'_{g'} \cdot \prod_{i=1}^n X_i^{g'_i}\right)\\ &= \sum_{\gamma\in\mathbb{Z}^n_{\geq 0}}\left(\sum_{g+g'=\gamma} f_g f'_{g'}\right)\prod_{i=1}^n X_i^{\gamma}.\end{aligned}$$

The standard representative in $\mathcal{C}_{\vec{m}/k}$ of the latter expression is the polynomial:

$$\sum_{\gamma\in\hat{G}}\left(\sum_{g+g'\equiv\gamma \bmod \vec{m}} f_g f'_{g'}\right)\prod_{i=1}^n X_i^{\gamma},$$

where $g + g' \equiv \gamma \bmod \vec{m}$ means that $g_i + g'_i \equiv \gamma_i \bmod m_i$ for all $1 \leq i \leq n$.

On the other hand:

$$\begin{aligned}\Phi_G(f\cdot f') &= \Phi_G\left(\sum_{\gamma\in G}\left(\sum_{g+g'=\gamma} f(g)f'(g')\right)\gamma\right)\\ &= \sum_{\gamma\in\hat{G}}\left(\sum_{g+g'\equiv\gamma \bmod \vec{m}} f_g f'_{g'}\right)\prod_{i=1}^n X_i^{\gamma},\end{aligned}$$

which shows that $\Phi_G(f)\cdot\Phi_G(f') = \Phi_G(f\cdot f')$. □

The above theorem applies to all finite abelian groups, due to the fundamental theorem of finite abelian groups.

Theorem 3.2.5 (**Fundamental theorem of finite abelian groups [Lan04]**). *Let G be a finite abelian group. Then there exists a unique tuple of integers $(m_1,\dots,m_n)$ such that $m_i \mid m_{i+1}$ for all $1 \leq i \leq n-1$, and such that:*

$$G \cong \mathbb{Z}_{m_1}\times\ldots\times\mathbb{Z}_{m_n}.$$

3.3 Semisimple circulant rings

Semisimple circulant rings can be characterized by the following theorem:

Theorem 3.3.1 (Maschke's theorem for circulant rings). *A circulant ring $\mathcal{C}_{\vec{m}/k}$ is semisimple if and only if all entries of $\vec{m}$ are coprime to the characteristic of k.*

Proof. This is immediate from Theorem 2.4.1. □

Semisimple circulant rings encompass a large part of all circulant rings. A notable example is the class of circulant rings over fields of characteristic 0, which are necessarily semisimple regardless of the parameters.

In this section, we present the decomposition of semisimple circulant rings into their simple components. Hence we assume $\mathcal{C}_{\vec{m}/k}$ to be semisimple for the remainder of this section.

3.3.1 Combinatorial Nullstellensatz

The Combinatorial Nullstellensatz plays an important role in the decomposition of circulant rings.

Theorem 3.3.2 (Combinatorial Nullstellensatz [Alo01]). *Let k be an arbitrary field, and let $f = f(X_1, \ldots, X_n)$ be a polynomial in $k[X_1, \ldots, X_n]$. Let $S_1, \ldots, S_n$ be nonempty subsets of k and define $g_i(X_i) = \prod_{s \in S_i}(X_i - s)$. If f vanishes over all the common zeroes of $g_1, \ldots, g_n$ (that is, if $f(s_1, \ldots, s_n) = 0$ for all $s_i \in S_i$), then there are polynomials $h_1, \ldots, h_n \in k[X_1, \ldots, X_n]$ satisfying $\deg(h_i) \leq \deg(f) - \deg(g_i)$ so that:*

$$f = \sum_{i=1}^{n} h_i g_i.$$

We show how the Combinatorial Nullstellensatz is used for constructing the semisimple decomposition of semisimple circulant rings, under certain restrictions on the base field k.

Lemma 3.3.3. *Let k be any field of characteristic p, and let $\vec{m} := (m_1, \ldots, m_n)$ whose entries are coprime to p. Then:*

$$\mathcal{V}(\mathfrak{a}_{\vec{m}}) = \mu_{m_1} \times \ldots \times \mu_{m_n}.$$

Proof. This is immediate. □

Theorem 3.3.4. *Consider the semisimple circulant ring $\mathcal{C}_{\vec{m}/k}$, with the n-tuple $\vec{m} = (m_1, \dots, m_n)$, and k a field such that $\mu_{m_i} \subset k$ for all $1 \leq i \leq n$. Then we have the following well-defined ring isomorphism:*

$$\tau_{\vec{m}/k} \colon \mathcal{C}_{\vec{m}/k} \to k^{\oplus \mathcal{V}(\mathfrak{a}_{\vec{m}})},\ f \mapsto (f(\mathbf{x}))_{\mathbf{x} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})}, \tag{3.1}$$

where $k^{\oplus \mathcal{V}(\mathfrak{a}_{\vec{m}})}$ is defined as the direct sum of $\#\mathcal{V}(\mathfrak{a}_{\vec{m}})$ copies of k, indexed by $\mathcal{V}(\mathfrak{a}_{\vec{m}})$.

Proof. Let $f \in k[X_1, \dots, X_n]$ and consider the ring homomorphism:

$$\tau'_{\vec{m}/k} \colon k[X_1, \dots, X_n] \to k^{\oplus \mathcal{V}(\mathfrak{a}_{\vec{m}})},\ f \mapsto (f(\mathbf{x}))_{\mathbf{x} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})}.$$

This is a well-defined map since $f(\mathbf{x}) \in k$ whenever $\mathbf{x} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$, and since $\mu_{m_i} \subset k$ for all $1 \leq i \leq n$.

The kernel of $\tau'_{\vec{m}/k}$ consists of exactly the polynomials $f \in k[X_1, \dots, X_n]$ which vanish over $\mathcal{V}(\mathfrak{a}_{\vec{m}})$, which translates to $f(s_1, \dots, s_n) = 0$ if and only if $s_i \in \mu_{m_i}$ for all $1 \leq i \leq n$. Since m_i is coprime to the characteristic of k, we have the identity $X_i^{m_i} - 1 = \prod_{s_i \in \mu_{m_i}} (X_i - s_i)$. Hence by the Combinatorial Nullstellensatz (Theorem 3.3.2), a polynomial $f \in k[X_1, \dots, X_n]$ vanishes over $\mathcal{V}(\mathfrak{a}_{\vec{m}})$ if and only if $f \in (X_1^{m_1} - 1, \dots, X_n^{m_n} - 1)$, which is by definition the ideal $\mathfrak{a}_{\vec{m}}$. As such, $\ker(\tau'_{\vec{m}/k}) = \mathfrak{a}_{\vec{m}}$, which induces the injective homomorphism:

$$k[X_1, \dots, X_n] / \ker(\tau'_{\vec{m}/k}) := \mathcal{C}_{\vec{m}/k} \to k^{\oplus \mathcal{V}(\mathfrak{a}_{\vec{m}})}.$$

This is exactly the map $\tau_{\vec{m}/k}$ in Eq. (3.1), which proves well-definedness and injectivity.

We only need to show surjectivity. Looking at the dimension viewed as vector spaces over k, we have:

$$\dim_k(\mathcal{C}_{\vec{m}/k}) = \#\mathcal{V}(\mathfrak{a}_{\vec{m}}) = \dim_k\left(k^{\oplus \mathcal{V}(\mathfrak{a}_{\vec{m}})}\right).$$

Since $\tau_{\vec{m}/k}$ is an injective linear map, it must thus also be surjective due to the dimensions of the vector spaces being equal. □

3.3.2 Galois group actions

Theorem 3.3.4 presents the simple components of semisimple circulant rings, given that their base field k is “large enough”. We refine this decomposition to any field k, which requires some results from Galois theory and cyclotomic extensions.

Definition 3.3.5. Let k be a field of characteristic p, and consider an n-tuple $\vec{m} = (m_1, \ldots, m_n) \in \mathbb{Z}_{>0}$ whose entries are coprime to p. Then $k_{\vec{m}}$ is defined as the cyclotomic extension $k(\mu_{m_1}, \ldots, \mu_{m_n})$, which is the smallest field extension of k containing μ_{m_i} for all $1 \leq i \leq n$.

Since $k_{\vec{m}}/k$ is a cyclotomic extension, it is a Galois extension with abelian Galois group $\mathrm{Gal}(k_{\vec{m}}/k)$. In this section, we discuss three group actions by $\mathrm{Gal}(k_{\vec{m}}/k)$ which are key to constructing the semisimple decomposition of circulant rings.

Definition 3.3.6 (Classical group action). We define the classical group action as:

$$\mathrm{Gal}(k_{\vec{m}}/k) \times k_{\vec{m}} \to k_{\vec{m}}, \ (\sigma, x) \mapsto \sigma(x).$$

Definition 3.3.7 (Algebraic group action). For any $\sigma \in \mathrm{Gal}(k_{\vec{m}}/k)$ and for any $f \in \mathcal{C}_{\vec{m}/k_{\vec{m}}}$, we define $\sigma(f) \coloneqq \sum_{M \in \mathrm{Mon}(n)} \sigma(\mathrm{coeff}_M(f)) \cdot M$. This induces the group action:

$$\mathrm{Gal}(k_{\vec{m}}/k) \times \mathcal{C}_{\vec{m}/k_{\vec{m}}} \to \mathcal{C}_{\vec{m}/k_{\vec{m}}}, \ (\sigma, f) \mapsto \sigma(f),$$

which we call the **algebraic group action**.

Remark 3.3.8. The $\mathrm{Gal}(k_{\vec{m}}/k)$-invariants of $\mathcal{C}_{\vec{m}/k_{\vec{m}}}$ equals the set $\mathcal{C}_{\vec{m}/k}$. To see this, note that for $f \in \mathcal{C}_{\vec{m}/k_{\vec{m}}}$, $\sigma(f)$ only affects the coefficients of the terms of f. As such by Proposition 3.2.2, given that f is contained in the standard set of representatives, so is $\sigma(f)$. Hence $f = \sigma(f)$ in $\mathcal{C}_{\vec{m}/k_{\vec{m}}}$ if and only if the coefficients of f stay invariant under σ. By the fundamental theorem of Galois theory [Ehr11, Theorem 4.10.1], this happens if and only if all coefficients of f are contained in k, or equivalently when $f \in \mathcal{C}_{\vec{m}/k}$.

We now introduce the group action whose structure plays a key role in the decomposition of semisimple circulant rings.

Definition 3.3.9 (Geometric group action). For any $\sigma \in \mathrm{Gal}(k_{\vec{m}}/k)$ and for any $\mathbf{x} \coloneqq (x_1, \ldots, x_n) \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$, we define $\sigma(\mathbf{x}) \coloneqq (\sigma(x_1), \ldots, \sigma(x_n))$. This induces the group action:

$$\alpha_{\vec{m}/k} \colon \mathrm{Gal}(k_{\vec{m}}/k) \times \mathcal{V}(\mathfrak{a}_{\vec{m}}) \to \mathcal{V}(\mathfrak{a}_{\vec{m}}), \ (\sigma, \mathbf{x}) \mapsto \sigma(\mathbf{x}),$$

which we call the **geometric group action**.

For $\mathbf{x} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$, we denote $\mathrm{Orb}(\mathbf{x})$ as the corresponding orbit of $\mathbf{x}$ under $\alpha_{\vec{m}/k}$.

The classical-, algebraic-, and the geometric group actions are related in the following way:

Lemma 3.3.10. *For any* $\sigma \in \mathrm{Gal}(k_{\vec{m}}/k)$, $\mathbf{x} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$ *and* $f \in \mathcal{C}_{\vec{m}/k_{\vec{m}}}$, *we have the following identity:*

$$\sigma(f(\mathbf{x})) = \sigma(f)(\sigma(\mathbf{x})).$$

Proof. Since σ as an automorphism preserves addition and multiplication of elements in $k_{\vec{m}}$, we have:

$$\begin{aligned}\sigma(f(\mathbf{x})) &= \sigma\left(\sum_{M \in \mathrm{Mon}(n)} \mathrm{coeff}_M(f) \cdot M(\mathbf{x})\right)\\ &= \sum_{M \in \mathrm{Mon}(n)} \sigma(\mathrm{coeff}_M(f)) \cdot \sigma(M(\mathbf{x}))\\ &= \sum_{M \in \mathrm{Mon}(n)} \sigma(\mathrm{coeff}_M(f)) \cdot M(\sigma(\mathbf{x}))\\ &= \sigma(f)(\sigma(\mathbf{x})).\end{aligned}$$

This concludes the proof. □

Corollary 3.3.11. *Let* $f \in \mathcal{C}_{\vec{m}/k_{\vec{m}}}$ *with all coefficients in* k. *Then for all* $\sigma \in \mathrm{Gal}(k_{\vec{m}}/k)$, *the identity* $\sigma(f(\mathbf{x})) = f(\sigma(\mathbf{x}))$ *holds.*

Lemma 3.3.12. *Let* $\mathbf{y} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$ *and let* $f \in \mathcal{C}_{\vec{m}/k}$. *Then:*

$$\prod_{\mathbf{x} \in \mathrm{Orb}(\mathbf{y})} f(\mathbf{x}) \in k.$$

Proof. Observe that any automorphism $\sigma \in \mathrm{Gal}(k_{\vec{m}}/k)$ induces a natural bijection $\mathrm{Orb}(\mathbf{y}) \to \mathrm{Orb}(\mathbf{y})$, $\mathbf{x} \mapsto \sigma(\mathbf{x})$. Thus:

$$\sigma\left(\prod_{\mathbf{x} \in \mathrm{Orb}(\mathbf{y})} f(\mathbf{x})\right) = \prod_{\mathbf{x} \in \mathrm{Orb}(\mathbf{y})} f(\sigma(\mathbf{x})) = \prod_{\sigma(\mathbf{x}) \in \mathrm{Orb}(\mathbf{y})} f(\mathbf{x}) = \prod_{\mathbf{x} \in \mathrm{Orb}(\mathbf{y})} f(\mathbf{x}).$$

From the fundamental theorem of Galois theory, we conclude that the expression $\prod_{\mathbf{x} \in \mathrm{Orb}(\mathbf{y})} f(\mathbf{x})$ is indeed contained in k. □

Lemma 3.3.13. *For* $\mathbf{x} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$, *we have* $[k(\mathbf{x}) : k] = \#\,\mathrm{Orb}(\mathbf{x})$.

Proof. The field extension $k(\mathbf{x})/k$ is a cyclotomic extension, which is always a Galois extension. The result now follows directly from the fundamental theorem of Galois theory. □

3.3.3 Semisimple decomposition

We present the semisimple decomposition of semisimple circulant rings.

Theorem 3.3.14. *Let $\mathbf{y} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$, then there exists a polynomial $\delta_{\mathrm{Orb}(\mathbf{y})} \in \mathcal{C}_{\vec{m}/k}$ such that:*

$$\delta_{\mathrm{Orb}(\mathbf{y})}(\mathbf{x}) = \begin{cases} 1 & \textit{if } \mathbf{x} \in \mathrm{Orb}(\mathbf{y}) \\ 0 & \textit{else.} \end{cases}$$

Proof. By Theorem 3.3.4 we have the isomorphism:

$$\tau_{\vec{m}/k_{\vec{m}}} : \mathcal{C}_{\vec{m}/k_{\vec{m}}} \to k_{\vec{m}}^{\oplus \mathcal{V}(\mathfrak{a}_{\vec{m}})}, \ f \mapsto (f(\mathbf{x}))_{\mathbf{x} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})}.$$

As such, there exists a polynomial $g \in \mathcal{C}_{\vec{m}/k_{\vec{m}}}$ satisfying:

$$g(\mathbf{x}) = \begin{cases} 1 \text{ if } \mathbf{x} \in \mathrm{Orb}(\mathbf{y}) \\ 0 \text{ else.} \end{cases}$$

We show that $g \in \mathcal{C}_{\vec{m}/k}$.

Assume to the contrary that $g \notin \mathcal{C}_{\vec{m}/k}$. Then there exists a coefficient c of g such that $c \notin k$. Remark 3.3.8 then implies that there exists a $\sigma \in \mathrm{Gal}(k_{\vec{m}}/k)$ such that $\sigma(g) \neq g$ in $\mathcal{C}_{\vec{m}/k_{\vec{m}}}$. The isomorphism $\tau_{\vec{m}/k_{\vec{m}}}$ implies that there exists $\mathbf{x} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$ such that:

$$\sigma(g)(\mathbf{x}) \neq g(\mathbf{x}). \tag{3.2}$$

By Lemma 3.3.10, we have that $\sigma(g(\mathbf{x})) = \sigma(g)(\sigma(\mathbf{x}))$. Since $\mathbf{x}$ and $\sigma(\mathbf{x})$ are in the same orbit, we get $\sigma(g)(\sigma(\mathbf{x})) = \sigma(g)(\mathbf{x})$ because g, and thus also $\sigma(g)$, is constant over orbits with values in k. This results into the equation $\sigma(g(\mathbf{x})) = \sigma(g)(\mathbf{x})$. Note however that since $g(\mathbf{x}) \in k$, we have $\sigma(g(\mathbf{x})) = g(\mathbf{x})$, which results into the equation $\sigma(g)(\mathbf{x}) = g(\mathbf{x})$. This is a contradiction to Eq. (3.2). Hence all coefficients of g are contained in k, which means that $g \in \mathcal{C}_{\vec{m}/k}$. Choosing $\delta_{\mathrm{Orb}(\mathbf{y})} = g$ concludes the proof. □

Lemma 3.3.15. *Let $\mathbf{x} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$ and let $a \in k(\mathbf{x})$. Then there exists a polynomial $p_{a,\mathbf{x}} \in \mathcal{C}_{\vec{m}/k}$ such that $p_{a,\mathbf{x}}(\mathbf{x}) = a$.*

Proof. Let us use the expression $\mathbf{x} = (x_1, \ldots, x_n)$. We proceed by induction on n. For $n = 1$, we have by basic field theory that there exists unique elements $c_0, c_1, \ldots, c_t$ in k with $t < [k(x_1) : k]$ such that:

$$a = c_0 + c_1 \cdot x_1 + c_2 \cdot x_1^2 + \ldots + c_t \cdot x_1^t.$$

Hence the polynomial:

$$p_{a,x_1}(X_1) \coloneqq \sum_{i=0}^{t} c_i \cdot X_1^i,$$

satisfies the assumption, thus proving the case for $n = 1$.

Now assume the lemma is true for $n = j$ for some integer $j > 1$, and consider $n = j + 1$. Observe that $k(x_1, \ldots x_j, x_{j+1}) = k(x_1, \ldots x_j)(x_{j+1})$. With a similar argument as in the case for $n = 1$, there exists unique elements $c_0, c_1, \ldots, c_t$ in $k(x_1, \ldots, x_j)$ with $t < [k(x_1, \ldots, x_j)(x_{j+1}) : k(x_1, \ldots, x_j)]$ such that:

$$a = c_0 + c_1 \cdot x_{j+1} + c_2 \cdot x_{j+1}^2 + \ldots + c_t \cdot x_{j+1}^t.$$

By the induction hypotheses, there exist polynomials $p_0, \ldots, p_t \in k[X_1, \ldots, X_j]$ such that $p_i(x_1, \ldots, x_j) = c_i$ for all $0 \leq i \leq t$. Hence the polynomial:

$$p_{a,\mathbf{x}} = \sum_{i=0}^{t} p_i(X_1, \ldots, X_j) \cdot X_{j+1}^t,$$

satisfies our assumptions, thus concluding the proof. □

Theorem 3.3.16. *Let $S \subset \mathcal{V}(\mathfrak{a}_{\vec{m}})$ be a set of representatives of the orbits of $\alpha_{\vec{m}/k}$. Assume that we have a map $F : S \to \overline{k}$ such that $F(\mathbf{x}) \in k(\mathbf{x})$ for all $\mathbf{x} \in S$. Then there exists a polynomial $f \in k[X_1, \ldots, X_n]$ such that $f(\mathbf{x}) = F(\mathbf{x})$.*

Proof. Consider the polynomial:

$$f = \sum_{\mathbf{y} \in S} p_{F(\mathbf{y}),\mathbf{y}} \cdot \delta_{\mathrm{Orb}(\mathbf{y})},$$

with $p_{F(\mathbf{y}),\mathbf{y}}$ as in Lemma 3.3.15 and $\delta_{\mathrm{Orb}(\mathbf{y})}$ as in Theorem 3.3.14. Then for any $\mathbf{x} \in S$, we have:

$$f(\mathbf{x}) = \sum_{\mathbf{y} \in S} p_{F(\mathbf{y}),\mathbf{y}}(\mathbf{x}) \cdot \delta_{\mathrm{Orb}(\mathbf{y})}(\mathbf{x}) = p_{F(\mathbf{x}),\mathbf{x}}(\mathbf{x}) \cdot \delta_{\mathrm{Orb}(\mathbf{x})}(\mathbf{x}) = F(\mathbf{x}) \cdot 1 = F(\mathbf{x}),$$

where the second equality is because $\delta_{\mathrm{Orb}(\mathbf{y})}(\mathbf{x}) = 0$ for $\mathbf{y} \neq \mathbf{x}$. This concludes the proof. □

Theorem 3.3.17 (**Semisimple decomposition of circulant rings**). *Let k be a field, and let $\mathcal{C}_{\vec{m}/k}$ be semisimple. Let $S \subset \mathcal{V}(\mathfrak{a}_{\vec{m}})$ be a set of representatives of the orbits of $\alpha_{\vec{m}/k}$. Then we have the isomorphism:*

$$\mathcal{C}_{\vec{m}/k} \to \bigoplus_{\mathbf{x} \in S} k(\mathbf{x}), \ f \mapsto (f(\mathbf{x}))_{\mathbf{x} \in S}, \tag{3.3}$$

where $[k(\mathbf{x}) : k] = \#\,\mathrm{Orb}(\mathbf{x})$.

Proof. Since the map $\tau_{\vec{m}/k_{\vec{m}}}$ from Theorem 3.3.4 is an isomorphism, the map $\tau_{\vec{m}/k_{\vec{m}}} \upharpoonright \mathcal{C}_{\vec{m}/k}$ (which is the map $\tau_{\vec{m}/k_{\vec{m}}}$ restricted to $\mathcal{C}_{\vec{m}/k}$) is an injective homomorphism. Using Corollary 3.3.11, we can refine $\tau_{\vec{m}/k_{\vec{m}}} \upharpoonright \mathcal{C}_{\vec{m}/k}$ to the injective homomorphism:

$$\mathcal{C}_{\vec{m}/k} \to (k_{\vec{m}})^{\oplus S},\ f \mapsto (f(\mathbf{y}))_{\mathbf{y}\in S}. \tag{3.4}$$

Clearly, $f(\mathbf{y}) \in k(\mathbf{y})$ for all $\mathbf{y} \in S$ and $f \in k[X_1, \dots, X_n]$. If given elements $a_{\mathbf{y}} \in k(\mathbf{y})$ for each $\mathbf{y} \in S$, we conclude from Theorem 3.3.16 that there exists a polynomial $f \in k[X_1, \dots, X_n]$ such that $f(\mathbf{y}) = a_{\mathbf{y}}$. Hence (3.4) induces the desired isomorphism (3.3). □

3.4 General circulant rings

In the previous section, we investigated the Krull-Remak-Schmidt decomposition of semisimple circulant rings. However, not all circulant rings are semisimple, for which the results and techniques presented in the previous section do not directly apply.

In this section, we present the Krull-Remak-Schmidt decomposition of circulant rings which are not necessarily semisimple. Our approach relies on some important results from modular representation theory, and the semisimple decomposition discussed in the previous section (Theorem 3.3.17). Most of the theory in this section is developed with the assumption that the underlying field has prime characteristic (unless stated otherwise) which we denote by p, as this is the only situation where a circulant ring can fail to be semisimple.

We introduce some additional notation which we use throughout the remainder of this chapter: Let p be a prime number and m be any positive integer. The p-adic valuation of m is defined as $v_p(m) := \max(j > 0 : p^j \mid m)$. We define $r_p(m) = \frac{m}{v_p(m)}$, which is the greatest divisor of m coprime to p.

For an n-tuple $\vec{m} := (m_1, \dots, m_n)$ consisting of positive integers, we define $v_p(\vec{m}) := (v_p(m_1), \dots, v_p(m_n))$ and $r_p(\vec{m}) := (r_p(m_1), \dots, r_p(m_n))$.

3.4.1 Indecomposable circulant rings

Let us start by discussing circulant rings which are indecomposable. These can be characterized as follows:

Theorem 3.4.1 (Indecomposable circulant rings). *A circulant ring $\mathcal{C}_{\vec{m}/k}$ is indecomposable if and only if all entries of $\vec{m}$ are powers of the characteristic of k.*

Proof (partially). The rightward implication is an immediate consequence of Proposition 2.9.7 of [Sch12]. The reverse implication however is not as straightforward, and requires more machinery. A proof is provided later in this thesis in the form of Corollary 3.4.17. □

Example 3.4.2. *An example of an indecomposable circulant ring is the ring* $\mathcal{C}_{(4,32)/\mathbb{F}_2} := \mathbb{F}_2[X_1, X_2]/(X_1^4 - 1, X_2^{32} - 1)$*, since* 4 *and* 32 *are powers of* 2.

Remark 3.4.3. Observe that if all the entries of $\vec{m}$ are powers of the characteristic of k, then $\mathcal{C}_{\vec{m}/k}$ is necessarily a local ring as the vanishing set of $\mathfrak{a}_{\vec{m}/k}$ consists of only a single element. As such we have in the case of circulant rings that $\mathcal{C}_{\vec{m}/k}$ is indecomposable as a left module over itself if and only if it is a local ring.

3.4.2 Structure of multivariate polynomial rings

We discuss some results regarding the structure of multivariate polynomial rings which are necessary for the proof of our main results in Section 3.4.4 (in particular Theorems 3.4.12 and 3.4.18).

Definition 3.4.4. Given n-tuples $j := (j_1, ..., j_n), t := (t_1, ..., t_n) \in \mathbb{Z}^n_{\geq 0}$, we define the polynomial $\mathcal{Y}_t^j := \prod_{i=1}^n (X_i^{t_i} - 1)^{j_i}$ in $k[X_1, \dots, X_n]$.

Moreover, we define:

$$\mathcal{R}_t := \{f \in k[X_1, \dots, X_n] \mid \deg_i(f) < t_i \text{ for all } 1 \leq i \leq n\}.$$

Also, we define:

$$\mathcal{R}_t \mathcal{Y}_t^j := \{f \cdot \mathcal{Y}_t^j \mid f \in \mathcal{R}_t\},$$

which we view as an additive subgroup of $k[X_1, \dots, X_n]$.

Theorem 3.4.5. *Let t be an n-tuple. We have the following statements:*

1. *For an n-tuple j, if $f \in \mathcal{R}_t \mathcal{Y}_t^j$ is non-zero, then $t_i \cdot j_i \leq \deg_i(f) < t_i \cdot (j_i + 1)$ for all $1 \leq i \leq n$;*
2. *Given two n-tuples j, j' such that $j \neq j'$, we have $\mathcal{R}_t \mathcal{Y}_t^j \cap \mathcal{R}_t \mathcal{Y}_t^{j'} = \{0\}$;*
3. *Let e_i be the i-th standard unit vector in $\mathbb{Z}^n_{\geq 0}$, then $\mathcal{R}_{t(\mathrm{e}_i + 1)} = \mathcal{R}_t \oplus \mathcal{R}_t \mathcal{Y}_t^{\mathrm{e}_i}$ for all $1 \leq i \leq n$;*
4. *Let j and t be n-tuples such that all their entries are non-zero, then $\mathcal{R}_{t \cdot j} := \bigoplus_{0^n \leq y \ll j} \mathcal{R}_t \mathcal{Y}_t^y$.*

Proof. We prove these statements separately.

Statement 1 Observe that $\deg_i(\mathcal{Y}_t^j) = j_i \cdot t_i$ for all $1 \leq i \leq n$. Also for any polynomial $f \in k[X_1, \ldots, X_n]$, we have that $\deg_i(f \cdot \mathcal{Y}_t^j) = \deg_i(f) + \deg_i(\mathcal{Y}_t^j)$. The statement follows from the fact that $0 \leq \deg_i(f) < t_i$ for all $f \in \mathcal{R}_t$.

Statement 2 Without loss of generality, assume that $j_1 \neq j_1'$. Statement 1 implies that the 1-th partial degree of the non-zero polynomials in $\mathcal{R}_t\mathcal{Y}_t^j$ and $\mathcal{R}_t\mathcal{Y}_t^{j'}$ cannot be in the same range. This proves the claim.

Statement 3 Without loss of generality, take $i = 1$. Consider the monomial $M := \prod_{l=1}^n X_l^{m_l}$ where $0 \leq m_l < t_l$ for all $2 \leq l \leq n$, and $t_1 \leq m_1 < 2t_1$. The goal is to show that such a monomial is contained in $\mathcal{R}_t \oplus \mathcal{R}_t\mathcal{Y}_t^{\mathrm{e}_1}$.

Observe that $\mathcal{Y}_t^{\mathrm{e}_1} = X_1^{t_1} - 1$. Since $M' := X_1^{m_1 - t_1} \cdot \prod_{l=2}^n X_l^{m_l} \in \mathcal{R}_t$, we have that $M' \cdot \mathcal{Y}_t^{\mathrm{e}_1} \in \mathcal{R}_t\mathcal{Y}_t^{\mathrm{e}_1}$. Observe that:

$$M' \cdot \mathcal{Y}_t^{\mathrm{e}_1} = X_1^{m_1 - t_1} \cdot \prod_{i=2}^n X_i^{m_i} \cdot \mathcal{Y}_t^{\mathrm{e}_1} = X_1^{m_1 - t_1} \cdot \prod_{i=2}^n X_i^{m_i} \cdot (X_1^{t_1} - 1) = M - M'.$$

This implies that M is contained in $\mathcal{R}_t \oplus \mathcal{R}_t\mathcal{Y}_t^{\mathrm{e}_1}$. Since this is true for any such monomial M, the claim follows.

Statement 4 Observe that every tuple $j = (j_1, \ldots, j_n)$ with non-zero entries equals $(1, \ldots, 1) + \sum_{i=1}^n (j_i - 1)\,\mathrm{e}_i$. Hence the claim follows from inductively applying Statement 3, given that the claim holds for the case $j = (1, \ldots, 1)$.

Observe that for $j = (1, \ldots, 1)$, the only tuple which is absolutely smaller than j is $j^0 := (0, \ldots, 0)$. Note that:

$$\mathcal{R}_t\mathcal{Y}_t^{j^0} = \left\{ f \cdot \prod_{i=1}^n (X_i^{t_i} - 1)^0 \mid f \in \mathcal{R}_t \right\} = \{ f \mid f \in \mathcal{R}_t \} = \mathcal{R}_t,$$

which proves the claim. □

As a consequence of Theorem 3.4.5, for every element $f \in \mathcal{R}_{t \cdot j}$, for each $0^n \leq y \ll j$, there exists a unique $f_y \in \mathcal{R}_t\mathcal{Y}_t^y$ such that $f = \sum_{0^n \leq y \ll j} f_y$.

Definition 3.4.6. For every $f \in \mathcal{R}_{t \cdot j}$, for each $0^n \ll y \ll j$, we define f_y as the $\mathcal{Y}_t^y$**-component** of f.

3.4.3 Field embedding

Consider the quotient map:

$$\mathfrak{q}_{\vec{m}/k} : \mathcal{C}_{\vec{m}/k} \to \mathcal{C}_{\vec{m}/k} / \operatorname{Jac}(\mathcal{C}_{\vec{m}/k}) \cong \mathcal{C}_{r_p(\vec{m})/k}. \tag{3.5}$$

From Theorem 3.3.17, we know that $\mathcal{C}_{r_p(\vec{m})/k}$ is isomorphic to the direct product of fields $\bigoplus_{\mathbf{x} \in S} k(\mathbf{x})$, where S is a set of representatives of the group action $\alpha_{\vec{m}/k}$ in Definition 3.3.9.

We construct injective group homomorphisms $k(\mathbf{x}) \to \mathcal{C}_{\vec{m}/k}$ for all $\mathbf{x} \in S$ which preserve multiplication, and are also k-linear maps. Observe that by Theorem 3.3.17, the field $k(\mathbf{x})$ corresponds to the set:

$$\{f \in \mathcal{R}_{r_p(\vec{m})} \mid f(\mathbf{y}) = 0 \text{ for all } \mathbf{y} \in S \setminus \{\mathbf{x}\}\}.$$

In words, the elements in $k(\mathbf{x})$ can be identified by the polynomials in $\mathcal{C}_{\vec{m}/k}$ with partial degrees strictly smaller than $r_p(\vec{m})$, such that it vanishes over all representatives in S other than $\mathbf{x}$. We use this identification of elements of $k(\mathbf{x})$ to construct such group homomorphisms.

Lemma 3.4.7. *Let $t \geq \sum_{i=1}^n v_p(m_i)$. Then for any $f(X_1, \ldots, X_n) \in \mathfrak{a}_{r_p(\vec{m})}$, we have $f(X_1^{p^t}, \ldots, X_n^{p^t}) = 0$ in $\mathcal{C}_{\vec{m}/k}$.*

Proof. Since $f \in \mathfrak{a}_{r_p(\vec{m})}$, f is of the form $f = \sum_{i=1}^n f_i(X_1, \ldots, X_n) \cdot \left(X_i^{r_p(m_i)} - 1\right)$ where $f_i \in \mathcal{C}_{\vec{m}/k}$. Observe that:

$$\begin{aligned} f(X_1^{p^t}, \ldots, X_n^{p^t}) &= \sum_{i=1}^n f_i(X_1^{p^t}, \ldots, X_n^{p^t}) \cdot \left(X_i^{p^t \cdot r_p(m_i)} - 1\right) \\ &= \sum_{i=1}^n f_i(X_1^{p^t}, \ldots, X_n^{p^t}) \cdot \left(X_i^{r_p(m_i) \cdot p^{v_p(m_i)}} - 1\right)^{p^{t - v_p(m_i)}} \\ &= 0, \end{aligned}$$

since for all $1 \leq i \leq n$, the polynomials $X_i^{r_p(m_i) \cdot p^{v_p(m_i)}} - 1 = X_i^{m_i} - 1$ vanish in the ideal $\mathfrak{a}_{\vec{m}}$. □

Lemma 3.4.8. *There exists an integer $t > 0$ such that $p^t \equiv 1 \bmod r_p(m_i)$ for all $1 \leq i \leq n$, and such that $t \geq \sum_{i=1}^n v_p(m_i)$.*

Proof. Let us fix some $1 \leq i \leq n$. Since p is coprime to $r_p(m_i)$, there exists a positive integer t_i such that $p^{t_i} \equiv 1 \bmod r_p(m_i)$. Observe that this is true for every multiple of t_i. As a result, we have that $p^{\prod_{i=1}^n t_i} \equiv 1 \bmod r_p(m_i)$ for all $1 \leq i \leq n$. Now simply find an integer $c > 0$ such that $c \cdot \prod_{i=1}^n t_i > \sum_{i=1}^n v_p(m_i)$, and set $t := c \cdot \prod_{i=1}^n t_i$. Then t satisfies all the conditions of the lemma. □

Proposition 3.4.9. *Let t be some fixed integer satisfying the conditions in Lemma 3.4.8. Then the map:*

$$\iota_{\mathbf{x}}: k(\mathbf{x}) \to \mathcal{C}_{\vec{m}/k}, \; f(X_1, \dots, X_n) \mapsto f\left(X_1^{p^t}, \dots, X_n^{p^t}\right),$$

is an injective k-linear map which preserves multiplication. Moreover, the composition $\mathfrak{q}_{\vec{m}/k} \circ \iota_{\mathbf{x}} : k(\mathbf{x}) \to k(\mathbf{x})$ is the identity map.

Proof. To ease notation in this proof, we denote $(X_1^c, \dots, X_n^c)$ by X^c for any positive integer c. Observe that k-linearity of $\iota_{\mathbf{x}}$ is immediate, since we simply replace X by X^{p^t}, and we work in characteristic p.

Let $h \in k(\mathbf{x})$ such that h equals $f \cdot g$ within the field $k(\mathbf{x})$. This means that in $\mathcal{C}_{\vec{m}/k}(\mathbf{x})$, there exists a polynomial $h^* \in \mathfrak{a}_{r_p(\vec{m})}$ such that $h = f \cdot g + h^*$. Now we have:

$$\begin{aligned}\iota_{\mathbf{x}}(f \cdot g) &= \iota_{\mathbf{x}}(h) = h(X^{p^t}) = (f \cdot g)(X^{p^t}) + h^*(X^{p^t}) = f(X^{p^t}) \cdot g(X^{p^t}) + 0 \\ &= \iota_{\mathbf{x}}(f) \cdot \iota_{\mathbf{x}}(g),\end{aligned}$$

where the fourth equation is due to Lemma 3.4.7, and also due to the fact that for polynomials the equation $(f \cdot g)(X^c) = f(X^c) \cdot g(X^c)$ holds up for any positive integer c. Hence $\iota_{\mathbf{x}}$ preserves multiplication.

Observe that for any $\mathbf{y} \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$, we have that $y_i^{p^t} = y_i$ since $p^t \equiv 1 \bmod m_i$ for all $1 \leq i \leq n$. As a result, we have for every $f \in k(\mathbf{x})$ and for every $\mathbf{y} \in S$ that $\iota_{\mathbf{x}}(f)(\mathbf{y}) = f(\mathbf{y})$. This implies that $\mathfrak{q}_{\vec{m}/k}(\iota_{\mathbf{x}}(f)) = f$, which shows that $\mathfrak{q}_{\vec{m}/k} \circ \iota_{\mathbf{x}}$ is the identity, which in particular implies that $\iota_{\mathbf{x}}$ is injective. □

Lemma 3.4.10. *Let $\mathbf{y} \neq \mathbf{x}$ be representatives of distinct orbits of the geometric group action $\alpha_{\vec{m}/k}$. Then for all $f_{\mathbf{x}} \in \operatorname{im}(\iota_{\mathbf{x}})$ and $f_{\mathbf{y}} \in \operatorname{im}(\iota_{\mathbf{y}})$, we have the identity $f_{\mathbf{x}} \cdot f_{\mathbf{y}} = 0$.*

Proof. Let $f'_{\mathbf{x}} \in k(\mathbf{x})$ and $f'_{\mathbf{y}} \in k(\mathbf{y})$ such that $\iota_{\mathbf{x}}(f'_{\mathbf{x}}) = f_{\mathbf{x}}$ and $\iota_{\mathbf{y}}(f'_{\mathbf{y}}) = f_{\mathbf{y}}$. Observe that the polynomial $f'_{\mathbf{x}} \cdot f'_{\mathbf{y}}$ vanishes everywhere on $\mathcal{V}(\mathfrak{a}_{\vec{m}})$, hence it must be contained in $\mathfrak{a}_{r_p(\vec{m})}$.

Note that we have the identities:

$$\begin{aligned}f_{\mathbf{x}} \cdot f_{\mathbf{y}} = \iota_{\mathbf{x}}(f'_{\mathbf{x}}) \cdot \iota_{\mathbf{y}}(f'_{\mathbf{x}}) &:= f'_{\mathbf{x}}(X_1^{p^t}, \dots, X_n^{p^t}) \cdot f'_{\mathbf{y}}(X_1^{p^t}, \dots, X_n^{p^t}) \\ &= (f'_{\mathbf{x}} \cdot f'_{\mathbf{y}})(X_1^{p^t}, \dots, X_n^{p^t}).\end{aligned}$$

From Lemma 3.4.7, we know that $(f'_{\mathbf{x}} \cdot f'_{\mathbf{y}})(X_1^{p^t}, \dots, X_n^{p^t})$ is contained in $\mathfrak{a}_{\vec{m}}$, which concludes the proof. □

3.4.4 Krull-Remak-Schmidt decomposition

We construct local rings which are the components of the local ring decomposition of $\mathcal{C}_{\vec{m}/k}$.

Definition 3.4.11. Let $S \subseteq \mathcal{V}(\mathfrak{a}_{\vec{m}})$ be a set of representatives of the orbits of $\alpha_{\vec{m}/k}$ as introduced in Definition 3.3.9. For $\mathbf{x} \in S$, we define the corresponding local coordinate ring:

$$\mathcal{C}_{\vec{m}/k}[\mathbf{x}] := k(\mathbf{x})[Y_1, \ldots, Y_n] / \left(Y_1^{p^{v_p(m_1)}}, \ldots, Y_n^{p^{v_p(m_n)}} \right),$$

where p is the characteristic of k. If $p = 0$, then we define $\mathcal{C}_{\vec{m}/k}[\mathbf{x}] := k(\mathbf{x})$. The ring $\mathcal{C}_{\vec{m}/k}[\mathbf{x}]$ is indeed local by Remark 3.4.3.

Theorem 3.4.12. *The map:*

$$F_{\mathbf{x}}: \mathcal{C}_{\vec{m}/k}[\mathbf{x}] \to \mathcal{C}_{\vec{m}/k}, \quad \sum_{j: j \ll p^{v_p(\vec{m})}} f_j \cdot Y^j \mapsto \sum_{j: j \ll p^{v_p(\vec{m})}} \iota_{\mathbf{x}}(f_j) \cdot \mathcal{Y}^j_{r_p(\vec{m})},$$

is a well-defined injective k-linear map which preserves multiplication. Here, $\mathcal{Y}^j_{r_p(\vec{m})}$ refers to the notation in Definition 3.4.4.

Proof. We divide the proof in two parts.

Well-definedness Consider the map:

$$\widetilde{F_{\mathbf{x}}}: k(\mathbf{x})[Y_1, \ldots, Y_n] \to \mathcal{C}_{\vec{m}/k}, \quad \sum_{j \in \mathbb{Z}^n_{\geq 0}} f_j \cdot Y^j \mapsto \sum_{j \in \mathbb{Z}^n_{\geq 0}} \iota_{\mathbf{x}}(f_j) \cdot \mathcal{Y}^j_{r_p(\vec{m})}.$$

This map is a k-linear map, and it preserves multiplication since $\iota_{\mathbf{x}}$ also satisfies these conditions (Proposition 3.4.9). The kernel of $\widetilde{F_{\mathbf{x}}}$ contains the ideal:

$$\left(Y_1^{p^{v_p(m_1)}}, \ldots, Y_n^{p^{v_p(m_n)}} \right).$$

This is because:

$$\widetilde{F_{\mathbf{x}}}\left(Y_i^{p^{v_p(m_i)}} \right) = \left(X_i^{r_p(m_i)} - 1 \right)^{p^{v_p(m_i)}} = X_i^{r_p(m_i) \cdot p^{v_p(m_i)}} - 1 = X_i^{m_i} - 1,$$

are exactly the generators of $\mathfrak{a}_{\vec{m}}$, which is the ideal quotient of $\mathcal{C}_{\vec{m}/k}$. Hence $\widetilde{F_{\mathbf{x}}}$ induces the map $F_{\mathbf{x}}$, which is thus also a k-linear map preserving multiplication.

Injectivity We show that $F_{\mathbf{x}}$ is an injective map.

Assume to the contrary that this is not true, then there must exist $f := \sum_{j:j \ll p^{v_p(\vec{m})}} f_j \cdot Y^j \in \mathcal{R}_{p^{v_p(\vec{m})}}$ such that $F_{\mathbf{x}}(f) \in \mathfrak{a}_{r_p(\vec{m})}$. Take any term of f which we denote as $f_j \cdot Y^j$ for some n-tuple j corresponding to the term. Note that there exists a non-zero $\overline{f_j} \in \mathcal{R}_{r_p(\vec{m})}$ and $O \in \mathfrak{a}_{r_p(\vec{m})}$ such that $\iota_{\mathbf{x}}(f_j)$ can be written as $\overline{f_j} + O$. This in particular means that $F_{\mathbf{x}}(f_j \cdot Y^j) = (\overline{f_j} + O) \cdot \mathcal{Y}^j_{r_p(\vec{m})} = \overline{f_j} \cdot \mathcal{Y}^j_{r_p(\vec{m})} + O \cdot \mathcal{Y}^j_{r_p(\vec{m})}$ where $O \cdot \mathcal{Y}^j_{r_p(\vec{m})} \notin \mathcal{R}_{r_p(\vec{m}) \cdot j}$. By Theorem 3.4.5, there exists a unique set of n-tuples $\mathcal{N}$ together with a unique family of corresponding non-zero polynomials $\{g_w : w \in \mathcal{N}\} \subset \mathcal{R}_{r_p(\vec{m})}$ such that:

$$O \cdot \mathcal{Y}^j_{r_p(\vec{m})} = \sum_{w \in \mathcal{N}} g_w \cdot \mathcal{Y}^w_{r_p(\vec{m})} \in \bigoplus_{w \in \mathcal{N}} \mathcal{R}_{r_p(\vec{m})} \mathcal{Y}^w_{r_p(\vec{m})}.$$

Observe that since $O \in \mathfrak{a}_{r_p(\vec{m})}$, we must have that $w > j$ for all $w \in \mathcal{N}$. Thus if we choose the term $f_j \cdot Y^j$ as the term of the lowest total degree of f (there can be multiple of such terms), then we are sure that $F_{\mathbf{x}}(f_j Y^j)$ has a non-zero $\mathcal{Y}^j_{r_p(\vec{m})}$-component, and that no other term of f mapped under $F_{\mathbf{x}}$ has a non-zero $\mathcal{Y}^j_{r_p(\vec{m})}$-component. This implies however that $F_{\mathbf{x}}(f)$ is non-zero by Theorem 3.4.5, which is a contradiction, hence $F_{\mathbf{x}}$ must be injective. □

Remark 3.4.13. The map $\iota_{\mathbf{x}}$ is not a ring homomorphism, as the unit element of $k(\mathbf{x})$ is not mapped to the unit element of $\mathcal{C}_{\vec{m}/k}$.

Definition 3.4.14. We denote the image of $F_{\mathbf{x}}$ by $\mathcal{C}_{\vec{m}/k}(\mathbf{x})$, which is a k-vector space.

Lemma 3.4.15. *Let $\mathbf{x}, \mathbf{x}' \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$ be two elements which represent different orbits under $\alpha_{\vec{m}/k}$. Then $\mathcal{C}_{\vec{m}/k}(\mathbf{x}) \cap \mathcal{C}_{\vec{m}/k}(\mathbf{x}') = \{0\}$. Moreover, if $f \in \mathcal{C}_{\vec{m}/k}(\mathbf{x})$ and $g \in \mathcal{C}_{\vec{m}/k}(\mathbf{x}')$, then $f \cdot g = 0$.*

Proof. Assume to the contrary that there exist non-zero $f \in \mathcal{C}_{\vec{m}/k}[\mathbf{x}]$ and $f' \in \mathcal{C}_{\vec{m}/k}[\mathbf{x}']$ such that $F_{\mathbf{x}}(f) = F_{\mathbf{x}'}(f')$. Then $\iota_{\mathbf{x}}(f_j) = \iota_{\mathbf{x}'}(f'_j)$ for all n-tuples $j \geq (0, \dots, 0)$. Since f and f' are non-zero, there exists an n-tuple j^* such that f_{j^*} is non-zero. Observe that $\iota_{\mathbf{x}}(f_{j^*})(\mathbf{x}) \neq 0$ since f_{j^*} is non-zero, but $\iota_{\mathbf{x}'}(f'_{j^*})(\mathbf{x}) = 0$ by assumption of $k(\mathbf{x}')$. Hence $\iota_{\mathbf{x}}(f_j) \neq \iota_{\mathbf{x}'}(f'_j)$, which is a contradiction.

The last statement is a direct consequence of Lemma 3.4.10. □

Theorem 3.4.16 (**Local ring decomposition**). *Let k be a field of characteristic p, and consider the product ring $\bigoplus_{\mathbf{x} \in S} \mathcal{C}_{\vec{m}/k}[\mathbf{x}]$. Then the following* *map is a ring isomorphism:*

$$F\colon \bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}[\mathbf{x}] \to \mathcal{C}_{\vec{m}/k}, \ (f_{\mathbf{x}})_{\mathbf{x}\in S} \mapsto \sum_{\mathbf{x}\in S} F_{\mathbf{x}}(f_{\mathbf{x}}).$$

Proof. We split the proof in two parts.

Bijectivity As a result of Lemma 3.4.15, the image of F is the direct sum $\bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}(\mathbf{x})$ within $\mathcal{C}_{\vec{m}/k}$. This implies that F is injective, as all the maps $F_{\mathbf{x}}$ are injective.

Let us show surjectivity. Since F is a k-linear map, we conclude that $\bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}(\mathbf{x})$ is a k-subspace of $\mathcal{C}_{\vec{m}/k}$ viewed as a k-vector space. Observe that:

$$\begin{aligned}\dim_k\left(\bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}(\mathbf{x})\right) &= \sum_{\mathbf{x}\in S} \dim_k(\mathcal{C}_{\vec{m}/k}[\mathbf{x}]) = \sum_{\mathbf{x}\in S}\left([k(\mathbf{x}):k]\cdot\prod_{i=1}^{n} p^{v_p(m_i)}\right)\\ &= \prod_{i=1}^{n} p^{v_p(m_i)}\cdot\left(\sum_{\mathbf{x}\in S}[k(\mathbf{x}):k]\right).\end{aligned}$$

Note that $\sum_{\mathbf{x}\in S}[k(\mathbf{x}):k] = \sum_{\mathbf{x}\in S} \#\operatorname{Orb}(\mathbf{x}) = \#\mathcal{V}(\mathfrak{a}_{r_p(\vec{m})}) = \prod_{i=1}^{n} r_p(m_i)$, hence:

$$\begin{aligned}\dim_k\left(\bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}[\mathbf{x}]\right) &= \left(\prod_{i=1}^{n} p^{v_p(m_i)}\right)\cdot\left(\prod_{j=1}^{n} r_p(m_j)\right) = \prod_{i=1}^{n} r_p(m_i)\cdot p^{v_p(m_i)}\\ &= \prod_{i=1}^{n} m_i.\end{aligned}$$

On the other hand, $\dim_k(\mathcal{C}_{\vec{m}/k}) = \prod_{i=1}^{n} m_i$, hence $\dim_k\left(\bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}[\mathbf{x}]\right) = \dim_k(\mathcal{C}_{\vec{m}/k})$. This implies that F is also surjective, hence a bijection.

Ring homomorphism Here we show that F is a ring homomorphism.

Observe that F preserves addition, as this is the sum of $F_{\mathbf{x}}$ which are all (additive) group homomorphisms.

Let $f = (f_{\mathbf{x}})_{\mathbf{x}\in S}, g = (g_{\mathbf{x}})_{\mathbf{x}\in S} \in \bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}(\mathbf{x})$, then:

$$\begin{aligned}F(f)\cdot F(g) &= \left(\sum_{\mathbf{x}\in S} F_{\mathbf{x}}(f_{\mathbf{x}})\right)\left(\sum_{\mathbf{x}\in S} F_{\mathbf{x}}(g_{\mathbf{x}})\right)\\ &= \sum_{\mathbf{x}\in S} F_{\mathbf{x}}(f_{\mathbf{x}})\cdot F_{\mathbf{x}}(g_{\mathbf{x}})\\ &= \sum_{\mathbf{x}\in S} F_{\mathbf{x}}(f_{\mathbf{x}}\cdot g_{\mathbf{x}})\\ &= F(f\cdot g),\end{aligned}$$

where the second equation is due to Lemma 3.4.15, and the third equation due to the fact that $F_{\mathbf{x}}$ preserves multiplication for all $\mathbf{x} \in S$. Hence F preserves multiplication.

Let 1_S be the identity in $\bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}[\mathbf{x}]$. We want to show that $F(1_S)$ is the identity in $\mathcal{C}_{\vec{m}/k}$. Let f be any element in $\mathcal{C}_{\vec{m}/k}$. Since F is bijective, there exists a unique element $f^* \in \bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}[\mathbf{x}]$ such that $F(f^*) = f$. Note that $F(1_S) \cdot f = F(1_S)F(f^*) = F(1_S f^*) = F(f^*) = f$. Since this is true for all $f \in \mathcal{C}_{\vec{m}/k}$, $F(1_S)$ must be the identity in $\mathcal{C}_{\vec{m}/k}$.

In conclusion, F is a well-defined bijective ring homomorphism, which makes it a ring isomorphism. □

Corollary 3.4.17. *Let k be a field of characteristic p, where p is either 0 or a prime number. If there exist entries of the n-tuple $\vec{m}$ which are not powers of p, then $\mathcal{C}_{\vec{m}/k}$ is not indecomposable.*

Proof. Since not all entries of $\vec{m}$ are coprime, the set of orbit representatives S of $\alpha_{\vec{m}/k}$ consists of more than one element. Hence by Theorem 3.4.16, $\mathcal{C}_{\vec{m}/k}$ is a direct sum of multiple indecomposable rings, hence not indecomposable. □

Theorem 3.4.18 (**Krull-Remak-Schmidt for circulant rings**). *Let $\mathcal{C}_{\vec{m}/k}$ be a circulant ring over a field k of characteristic p. Let S be a set of representatives of the orbits of $\alpha_{\vec{m}/k}$ introduced in Definition 3.3.9. Then $\mathcal{C}_{\vec{m}/k}$, viewed as a left module over itself, admits the module decomposition $\bigoplus_{\mathbf{x}\in S} \mathcal{C}_{\vec{m}/k}(\mathbf{x})$, where $\mathcal{C}_{\vec{m}/k}(\mathbf{x})$ is introduced in Definition 3.4.14. Moreover, for every $\mathbf{x} \in S$, $\mathcal{C}_{\vec{m}/k}(\mathbf{x})$ is an indecomposable left $\mathcal{C}_{\vec{m}/k}$-module, which for p prime is induced by the local circulant ring:*

$$k(\mathbf{x})[Y_1, ..., Y_n] / \left(Y_1^{p^{v_p(m_1)}} - 1, \dots, Y_n^{p^{v_p(m_n)}} - 1 \right). \tag{3.6}$$

For $p = 0$, $\mathcal{C}_{\vec{m}/k}(\mathbf{x})$ is isomorphic to $k(\mathbf{x})$.

Proof. All the claims except for Eq. (3.6) are direct consequences of Theorem 3.4.16. We only need to show that $\mathcal{C}_{\vec{m}/k}[\mathbf{x}]$ as defined in Definition 3.4.11 is isomorphic to Eq. (3.6). When p is prime, this is simply a matter of applying the variable transformation $Y_i \mapsto Y_i - 1$. The case for $p = 0$ is immediate. □

Remark 3.4.19. The fields $k(\mathbf{x})$ in Theorem 3.4.18 are the simple components of the semisimple circulant ring $\mathcal{C}_{r_p(\vec{m})/k}$. As such, if we know the simple components of $\mathcal{C}_{r_p(\vec{m})/k}$, we can deduce the indecomposable components of $\mathcal{C}_{\vec{m}/k}$.

3.5 Circulant rings over finite fields

The orbit structure of the geometric group action $\alpha_{\vec{m}/\mathbb{F}_q}$ over the finite field $\mathbb{F}_q$ (see Definition 3.3.9) has a particularly nice description in terms of number theory and modular arithmetic due to the unique properties of finite fields and their field extensions. In this section, we investigate this orbit structure, leading to an alternative formulation of the Krull-Remak-Schmidt decomposition only applicable to circulant rings over finite fields.

By Remark 3.4.19 and Theorem 3.4.1, we are only required to do this for the case that all entries in $\vec{m}$ are coprime to q, which we assume in the remainder of this section unless stated otherwise.

We introduce some additional notation related to the ring of integers modulo m, which we use throughout the remainder of this section. The multiplicative group of $\mathbb{Z}_m$ is denoted as $\mathbb{Z}_m^*$, We denote the order of $\mathbb{Z}_m^*$ by $\varphi(m)$, which is known as the Euler's totient function. Observe that $a \in \mathbb{Z}_m$ is contained in $\mathbb{Z}_m^*$ if and only if a is coprime to m. For $a \in \mathbb{Z}_m^*$, we denote the multiplicative order of a as $\operatorname{ord}_m(a)$.

We define Div_m as the set of all divisors of m including 1 and m itself. For an n-tuple $\vec{m} := (m_1, \dots, m_n) \in \mathbb{Z}_{>0}^n$, we define $\operatorname{Div}_{\vec{m}}$ as the Cartesian product $\operatorname{Div}_{m_1} \times \dots \times \operatorname{Div}_{m_n} \subset \mathbb{Z}_{>0}^n$.

3.5.1 Some modular arithmetic

Definition 3.5.1. For $\vec{d} = (d_1, \dots, d_n) \in \operatorname{Div}_{\vec{m}}$, we define the set:

$$\mathbb{Z}_{\vec{m}}(\vec{d}) := \{(x_1, \dots, x_n) \in \mathbb{Z}_{\vec{m}} : \gcd(x_i, m_i) = d_i \text{ for all } 1 \leq i \leq n\}.$$

Proposition 3.5.2. *We have the disjoint union $\mathbb{Z}_{\vec{m}} = \dot\bigcup_{\vec{d} \in \operatorname{Div}_{\vec{m}}} \mathbb{Z}_{\vec{m}}(\vec{d})$.*

Proof. First we show that the subsets $\mathbb{Z}_{\vec{m}}(\vec{d})$ where $\vec{d} \in \operatorname{Div}_{\vec{m}}$ cover $\mathbb{Z}_{\vec{m}}$. Let $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}_{\vec{m}}$, and let $\vec{d}^* := (d_1^*, \dots, d_n^*)$ where $d_i^* := \gcd(x_i, m_i)$. Then by definition, $\mathbf{x} \in \mathbb{Z}_{\vec{m}}(d^*)$. Since this is true for all $\mathbf{x} \in \mathbb{Z}_{\vec{m}}$, the subsets $\mathbb{Z}_{\vec{m}}(d)$ indeed cover $\mathbb{Z}_{\vec{m}}$.

We show that $\mathbb{Z}_{\vec{m}}(\vec{d})$ and $\mathbb{Z}_{\vec{m}}(\vec{d}')$ are disjoint for $\vec{d} \neq \vec{d}'$. Assume to the contrary that these sets are not disjoint. Then there exists an $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}_{\vec{m}}$ contained in both sets. Since $\vec{d} \neq \vec{d}'$, there exists an $1 \leq i \leq n$ such that $d_i \neq d_i'$. The assumption $x \in \mathbb{Z}_{\vec{m}}(\vec{d})$ implies $\gcd(x_i, m_i) = d_i$, and similarly, $x \in \mathbb{Z}_{\vec{m}}(\vec{d}')$ implies $\gcd(x_i, m_i) = d_i'$. But then $d_i = d_i'$, which is a contradiction. Hence $\mathbb{Z}_{\vec{m}}(\vec{d})$ and $\mathbb{Z}_{\vec{m}}(\vec{d}')$ must be disjoint. □

Lemma 3.5.3. *For each $\vec{d} = (d_1, \ldots, d_n) \in \mathrm{Div}_{\vec{m}}$, there is a natural bijection $\omega: \mathbb{Z}^*_{\vec{m}/\vec{d}} \to \mathbb{Z}_{\vec{m}}(\vec{d})$, $\vec{c} \mapsto \vec{d} \cdot \vec{c}$, where $\vec{m}/\vec{d} := (m_1/d_1, \ldots, m_n/d_n)$.*

Proof. The set of n-tuples of positive integers:

$$\{(d_1 \cdot c_1, \ldots, d_n \cdot c_n) \in \mathbb{Z}^n_{>0} : 1 \leq c_i \leq m_i/d_i \text{ and } \gcd(c_i, m_i/d_i) = 1\},$$

contains exactly the n-tuple integer representatives of all elements of $\mathbb{Z}_{\vec{m}}(\vec{d})$ viewed as a subset of $\mathbb{Z}_{\vec{m}}$. Observe that the elements in the set:

$$\{(c_1, \ldots, c_n) \in \mathbb{Z}^n_{>0} : 1 \leq c_i \leq m_i/d_i \text{ and } \gcd(c_i, m_i/d_i) = 1\},$$

are exactly the n-tuple integer representatives of $\mathbb{Z}^*_{\vec{m}/\vec{d}}$, which proves the claim. □

Remark 3.5.4. We state some trivial but useful facts:

1. $\mathbb{Z}_{\vec{m}}(\vec{m}) = \{\vec{0}\}$ and $\mathbb{Z}_{\vec{m}}(\vec{1}) = \mathbb{Z}^*_{\vec{m}}$ where $\vec{0} := (0 \bmod m_i)_{1 \leq i \leq n}$ and $\vec{1} := (1 \bmod m_i)_{1 \leq i \leq n}$;

2. By Lemma 3.5.3, we have $\#\mathbb{Z}_{\vec{m}}(\vec{d}) = \#\mathbb{Z}^*_{\vec{m}/\vec{d}} = \prod_{i=1}^n \varphi(m_i/d_i)$.

3.5.2 Modular group action

We construct a group action which is equivalent to $\alpha_{\vec{m}/\mathbb{F}_q}$ (Definition 3.3.9), but which is computationally more convenient.

Definition 3.5.5 (Modular group action). Let $\vec{m} := (m_1, \ldots, m_n)$ be an n-tuple of positive integers whose entries are coprime to q. Define the element:

$$\vec{q} := (q \bmod m_1, \ldots, q \bmod m_n) \in \mathbb{Z}^*_{\vec{m}},$$

which is indeed contained in $\mathbb{Z}^*_{\vec{m}}$ since q and m_i are coprime, and let $\langle \vec{q} \rangle$ be the cyclic subgroup of $\mathbb{Z}^*_{\vec{m}}$ generated by $\vec{q}$. For $\mathbf{x} := (x_1, \ldots, x_n) \in \mathbb{Z}_{\vec{m}}$ and for all $t \geq 1$, we define the **modular group action** as:

$$\alpha^*_{\vec{m}/\mathbb{F}_q}: \langle \vec{q} \rangle \times \mathbb{Z}_{\vec{m}} \to \mathbb{Z}_{\vec{m}}, \; (\vec{q}^{\,t}, \mathbf{x}) \mapsto (x_1 \cdot q^t \bmod m_1, \ldots, x_n \cdot q^t \bmod m_n).$$

If $\vec{m}$ and $\mathbb{F}_q$ are clear from context, we denote $\alpha^*_{\vec{m}/\mathbb{F}_q}(\vec{q}^{\,t}, \mathbf{x})$ simply by $\mathbf{x} \cdot \vec{q}^{\,t}$.

Theorem 3.5.6. *The group actions $\alpha^*_{\vec{m}/k}$ and $\alpha_{\vec{m}/k}$ from Definition 3.3.9 are equivalent.*

Proof. We construct a group isomorphism $\iota\colon \mathrm{Gal}(k_{\vec{m}}/k) \to \langle \vec{q} \rangle$ and a bijective map $\gamma\colon \mathcal{V}(\mathfrak{a}_{\vec{m}}) \to \mathbb{Z}_{\vec{m}}$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Gal}(k_{\vec{m}}/k) \times \mathcal{V}(\mathfrak{a}_{\vec{m}}) \arrow[r, "\alpha_{\vec{m}/k}"] \arrow[d, "\iota\times\gamma"'] & \mathcal{V}(\mathfrak{a}_{\vec{m}}) \arrow[d, "\gamma"] \\
\langle \vec{q} \rangle \times \mathbb{Z}_{\vec{m}} \arrow[r, "\alpha^*_{\vec{m}/k}"] & \mathbb{Z}_{\vec{m}}
\end{tikzcd}$$

The map ι The Galois group $\mathrm{Gal}(k_{\vec{m}}/k)$ is cyclic of order $\mathrm{lcm}_{i=1}^{n}(\mathrm{ord}_{m_i}(q))$, and it is generated by the Frobenius automorphism $\sigma_q\colon k_{\vec{m}} \to k_{\vec{m}},\ x \mapsto x^q$. Hence there is a natural group isomorphism:

$$\iota\colon \mathrm{Gal}(k_{\vec{m}}/k) \to \langle \vec{q} \rangle,\ \sigma_q^t \mapsto \vec{q}^{\,t}.$$

The map γ For each $1 \le i \le n$, let us fix some primitive m_i-th root ζ_{m_i}. Note that every element in μ_{m_i} can be uniquely expressed as $\zeta_{m_i}^{a_i}$ where $0 \le a_i < m_i$. Depending on the choice of the primitive roots, we can construct a natural bijective map:

$$\gamma\colon \mathcal{V}(\mathfrak{a}_{\vec{m}}) \to \mathbb{Z}_{\vec{m}},\ (\zeta_{m_1}^{x_1}, \dots, \zeta_{m_n}^{x_n}) \mapsto (x_1, \dots, x_n).$$

This map is bijective since $\#\mathcal{V}(\mathfrak{a}_{\vec{m}}) = \#\mathbb{Z}_{\vec{m}}$.

Commutativity Confirming commutativity of the diagram is a matter of writing down both compositions, and show that the outputs are equal: Assume we have some $\sigma_q^t \in \mathrm{Gal}(k_{\vec{m}}/k)$ and $(\zeta_{m_1}^{x_1}, \dots, \zeta_{m_n}^{x_n}) \in \mathcal{V}(\mathfrak{a}_{\vec{m}})$. Then we have:

$$\begin{aligned}
\gamma \circ \alpha_{\vec{m}/k}(\sigma_q^t, (\zeta_{m_1}^{x_1}, \dots, \zeta_{m_n}^{x_n})) &= \gamma\left(\zeta_{m_1}^{x_1\cdot q^t}, \dots, \zeta_{m_n}^{x_n\cdot q^t}\right) \\
&= (x_1 \cdot q^t \bmod m_1, \dots, x_n \cdot q^t \bmod m_n), \\
\alpha^*_{m/k} \circ (\iota \times \gamma)(\sigma_q^t, (\zeta_{m_1}^{x_1}, \dots, \zeta_{m_n}^{x_n})) &= \alpha^*_{m/k}\left(q^t \bmod m, (x_i \bmod m_i)_{1 \le i \le m}\right) \\
&= (x_1 \cdot q^t \bmod m_1, \dots, x_n \cdot q^t \bmod m_n).
\end{aligned}$$

This implies $\gamma \circ \alpha_{\vec{m}/k} = \alpha^*_{\vec{m}/k} \circ (\iota \times \gamma)$, which proves commutativity of the diagram. □

Remark 3.5.7. The equivalence of $\alpha_{\vec{m}/k}$ and $\alpha^*_{\vec{m}/k}$ is not canonical, as it depends on the choice of primitive roots.

3.5.3 Orbit structure

We discuss the orbit structure of the modular group action $\alpha^*_{\vec{m}/\mathbb{F}_q}$.

Lemma 3.5.8. *Let $\mathbf{x} \in \mathbb{Z}_{\vec{m}}(\vec{d})$, then $\operatorname{Orb}(\mathbf{x})$ is contained in $\mathbb{Z}_{\vec{m}}(\vec{d})$.*

Proof. Since q is coprime to m_i, $\gcd(m_i, x_i \cdot q^t) = \gcd(m_i, x_i) = d_i$ for all $1 \leq i \leq n$ and $t \geq 0$. As such, $\mathbf{x} \cdot \vec{q}^t \in \mathbb{Z}_{\vec{m}}(\vec{d})$, hence $\operatorname{Orb}(\mathbf{x}) \subseteq \mathbb{Z}_{\vec{m}}(\vec{d})$. □

From the above result, the group action $\alpha^*_{\vec{m}/\mathbb{F}_q}$ restricted to $\mathbb{Z}_{\vec{m}}(\vec{d})$ is a well-defined group action. As such, it induces an equivalence relation on $\mathbb{Z}_{\vec{m}}(\vec{d})$ where the orbits are the equivalence classes.

Consider the group $\mathbb{Z}^*_{\vec{m}/\vec{d}}$ with the equivalence relation induced from the quotient group $\mathbb{Z}^*_{\vec{m}/\vec{d}}/\langle \vec{q}_d \rangle$ where $\vec{q}_d \coloneqq (q \bmod m_i/d_i)_{1\leq i\leq n} \in \mathbb{Z}^*_{\vec{m}/\vec{d}}$.

Lemma 3.5.9. *Consider $\mathbb{Z}^*_{\vec{m}/\vec{d}}$ and $\mathbb{Z}_{\vec{m}}(\vec{d})$ with both their respective equivalence relations as defined above. Let $\omega\colon \mathbb{Z}^*_{\vec{m}/\vec{d}} \to \mathbb{Z}_{\vec{m}}(\vec{d})$ be the bijective map defined in Lemma 3.5.3. Then for every $\mathbf{x} \in \mathbb{Z}^*_{\vec{m}/\vec{d}}$, the image of the equivalence class of $\mathbf{x}$ under ω is exactly the equivalence class of $\omega(\mathbf{x})$.*

Proof. By definition, the equivalence class of $\mathbf{x} \coloneqq (x_1, \ldots, x_n)$ in $\mathbb{Z}^*_{\vec{m}/\vec{d}}$ consists of exactly the elements:

$$[\mathbf{x}] = \left\{ (x_i \cdot q^t \bmod (m_i/d_i))_{1\leq i\leq n} : t \geq 1 \right\}.$$

Observe that:

$$\omega([\mathbf{x}]) = \left\{ (d_i \cdot (x_i \cdot q^t \bmod (m_i/d_i)) \bmod m_i)_{1\leq i\leq n} : t \geq 1 \right\},$$

which by definition is exactly the orbit $\operatorname{Orb}(\omega(\mathbf{x}))$. □

Proposition 3.5.10. *Consider the group action $\alpha^*_{\vec{m}/\mathbb{F}_q}$ restricted to $\mathbb{Z}_{\vec{m}}(\vec{d})$. The number of orbits in $\mathbb{Z}_{\vec{m}}(\vec{d})$ equals:*

$$\frac{\prod_{i=1}^n \varphi(m_i/d_i)}{\operatorname{lcm}_{1\leq i\leq n}(\operatorname{ord}_{m_i/d_i}(q))}.$$

Moreover, all orbits in $\mathbb{Z}_{\vec{m}}(\vec{d})$ have the same length, being:

$$\operatorname{lcm}_{1\leq i\leq n}(\operatorname{ord}_{m_i/d_i}(q)).$$

Proof. By Lemma 3.5.9, the number of orbits equals $\#\mathbb{Z}^*_{\vec{m}/\vec{d}}/\langle \vec{q}_d\rangle = \frac{\#\mathbb{Z}^*_{\vec{m}/\vec{d}}}{\#\langle \vec{q}_d\rangle}$. It is immediate that $\#\mathbb{Z}^*_{\vec{m}/\vec{d}} = \prod_{i=1}^n \varphi(m_i/d_i)$. To see the expression of the denominator, observe that the order of $\langle \vec{q}_d\rangle$ is the smallest integer t such that $q^t \equiv 1 \bmod (m_i/d_i)$ for all $1 \le i \le n$ simultaneously. This number equals $\mathrm{lcm}_{1\le i\le n}(\mathrm{ord}_{m_i/d_i}(q))$, which proves the first claim.

Every equivalence class in $\mathbb{Z}^*_{\vec{m}/\vec{d}}$ has the same size, which equals $\#\langle \vec{q}_d\rangle = \mathrm{lcm}_{1\le i\le n}(\mathrm{ord}_{m_i/d_i}(q))$. This statement translates to the orbits of $\mathbb{Z}_{\vec{m}}(\vec{d})$ by Lemma 3.5.9. □

Theorem 3.5.11 (**Orbit structure theorem over finite fields**). *Consider the finite field $\mathbb{F}_q$, and let $\vec{m} = (m_1, \dots, m_n)$ be an n-tuple whose entries are coprime to q. Then the following statements hold regarding the orbits of $\alpha^*_{\vec{m}/\mathbb{F}_q}$:*

1. *For every orbit $\mathrm{Orb}(\mathbf{x})$ of $\alpha^*_{\vec{m}/\mathbb{F}_q}$, there exists a unique $\vec{d} \in \mathrm{Div}_{\vec{m}}$ such that $\mathrm{Orb}(\mathbf{x})$ is contained in $\mathbb{Z}_{\vec{m}}(\vec{d})$;*
2. *Let $\vec{d} := (d_1, \dots, d_n) \in \mathrm{Div}_{\vec{m}}$. Then every orbit in $\mathbb{Z}_{\vec{m}}(\vec{d})$ is of size $\mathrm{lcm}_{1\le i\le n}(\mathrm{ord}_{m_i/d_i}(q))$, and the number of orbits in $\mathbb{Z}_{\vec{m}}(\vec{d})$ equals:*
$$\frac{\prod_{i=1}^n \varphi(m_i/d_i)}{\mathrm{lcm}_{1\le i\le n}(\mathrm{ord}_{m_i/d_i}(q))};$$
3. *The total number of orbits of $\alpha^*_{\vec{m}/\mathbb{F}_q}$ equals:*
$$\sum_{(d_1,\dots,d_n)\in \mathrm{Div}_{\vec{m}}} \frac{\prod_{i=1}^n \varphi(d_i)}{\mathrm{lcm}_{1\le i\le n}(\mathrm{ord}_{d_i}(q))}.$$

Proof. Given some $\mathbf{x} \in \mathbb{Z}_{\vec{m}}$, there exists a unique $\vec{d} \in \mathrm{Div}_{\vec{m}}$ such that $\mathbf{x} \in \mathbb{Z}_{\vec{m}}(\vec{d})$ (see Proposition 3.5.2). By Lemma 3.5.8, $\mathrm{Orb}(\mathbf{x}) \subset \mathbb{Z}_{\vec{m}}(\vec{d})$, which proves the first statement.

The second statement is simply a reformulation of Proposition 3.5.10.

The third statement is an immediate consequence of the first and second statement, and the observation that the map $\mathrm{Div}_{\vec{m}} \to \mathrm{Div}_{\vec{m}}$, $\vec{d} \mapsto \vec{m}/\vec{d}$ is a bijection. □

Remark 3.5.12. In the univariate case ($n = 1$), the orbit structure provides a proof of Gauss's identity, which states that $m = \sum_{d|m} \varphi(d)$ for $m \in \mathbb{Z}_{>0}$. To see this, let p be any prime number coprime to m. The main idea is to express the size of $\mathbb{Z}_m(d)$ (which equals m) as the sum of the lengths of all orbits of $\alpha^*_{m/\mathbb{F}_p}$ in $\mathbb{Z}_m$. From Theorem 3.5.11, this idea translates as follows:

$$m = \#\mathbb{Z}_m = \sum_{d|m} \frac{\varphi(d)}{\mathrm{ord}_d(p)} \cdot \mathrm{ord}_d(p) = \sum_{d|m} \varphi(d),$$

which is Gauss's identity.

3.5.4 Krull-Remak-Schmidt over finite fields

We present the Krull-Remak-Schmidt decomposition of circulant rings over finite fields.

Theorem 3.5.13 (**Circulant Krull-Remak-Schmidt decomposition over finite fields**). *Let $\mathbb{F}_q$ be a finite field of characteristic p, and consider the circulant ring $\mathcal{C}_{\vec{m}/\mathbb{F}_q}$. For any $\vec{d} := (d_1, \ldots, d_n) \in \mathrm{Div}_{r_p(\vec{m})}$, define the expressions $\nu_{\vec{m}/\mathbb{F}_q}(\vec{d}) := \mathrm{lcm}_{1 \le i \le n}(\mathrm{ord}_{d_i}(q))$ and $\eta_{\vec{m}/\mathbb{F}_q}(\vec{d}) := \frac{\prod_{i=1}^n \varphi(d_i)}{\nu_{\vec{m},q}(\vec{d})}$. Then the Krull-Remak-Schmidt decomposition of $\mathcal{C}_{\vec{m}/\mathbb{F}_q}$ equals:*

$$\bigoplus_{\vec{d} \in \mathrm{Div}_{r_p(\vec{m})}} \left(\mathbb{F}_{q^{\nu_{\vec{m}/\mathbb{F}_q}(\vec{d})}}[Y_1, \ldots, Y_n] \Big/ \left(Y_1^{p^{v_p(m_1)}} - 1, \ldots, Y_n^{p^{v_p(m_n)}} - 1 \right) \right)^{\eta_{\vec{m}/\mathbb{F}_q}(\vec{d})}.$$

Proof. By Remark 3.4.19, we are only required to show that the semisimple decomposition of the semisimple circulant ring $\mathcal{C}_{r_p(\vec{m})/\mathbb{F}_q}$ equals:

$$\mathcal{C}_{r_p(\vec{m})/\mathbb{F}_q} \cong \bigoplus_{\vec{d} \in \mathrm{Div}_{r_p(\vec{m})}} \left(\mathbb{F}_{q^{\nu_{\vec{m}/\mathbb{F}_q}(\vec{d})}} \right)^{\eta_{\vec{m}/\mathbb{F}_q}(\vec{d})}.$$

Let S be a set of representatives of the orbits of the group action $\alpha_{r_p(\vec{m})/\mathbb{F}_q}$. From Theorem 3.3.17, the simple components of $\alpha_{r_p(\vec{m})/\mathbb{F}_q}$ are the field extensions $\mathbb{F}_q(\mathbf{x})$ for all $\mathbf{x} \in S$, where $[\mathbb{F}_q(\mathbf{x}) : \mathbb{F}_q] = \# \mathrm{Orb}(\mathbf{x})$. Every finite field is, up to isomorphism, uniquely determined by its cardinality. As such, $\mathbb{F}_q(\mathbf{x})$ is isomorphic to the field $\mathbb{F}_{q^{\# \mathrm{Orb}(\mathbf{x})}}$. From Theorem 3.5.6, $\alpha_{r_p(\vec{m})/\mathbb{F}_q}$ is equivalent to $\alpha^*_{r_p(\vec{m})/\mathbb{F}_q}$, of which the orbits are well-understood (see Theorem 3.5.11). The rest follows from the first and second statement of Theorem 3.5.11. □

3.5.5 An example: $\mathcal{C}_{(5,5,2^l)/\mathbb{F}_2}$

Let l be some positive integer, and let us compute the indecomposable components of:

$$\mathcal{C}_{(5,5,2^l)/\mathbb{F}_2} := \mathbb{F}_2[X_1, X_2, X_3]/(X_1^5 - 1, X_2^5 - 1, X_3^{2^l} - 1).$$

One might recognize this structure in the permutation Keccak-f relating to the θ-map [BDPV15].

We compute the semisimple decomposition of the semisimple circulant ring $\mathcal{C}_{r_2((5,5,2^l))/\mathbb{F}_2}$. Observe that $r_2((5,5,2^l)) = (5,5,1)$, hence:

$$\mathcal{C}_{r_2((5,5,2^l))/\mathbb{F}_2} \cong \mathcal{C}_{r_2((5,5,1))/\mathbb{F}_2} \cong \mathcal{C}_{(5,5)/\mathbb{F}_2}.$$

Observe that:

$$\mathrm{Div}_{(5,5)} := \{(1,1),(1,5),(5,1),(5,5)\}.$$

In view of Theorem 3.5.13, we compute the values of $\prod_{i=1}^2 \varphi(d_i)$, $\nu_{(5,5)/\mathbb{F}_2}(\vec{d})$ and $\eta_{(5,5)/\mathbb{F}_2}(\vec{d})$ for each $\vec{d} \in \mathrm{Div}_{(5,5)}$ which can be found in the table below:

$\vec{d} = (d_1, d_2)$	$\prod_{i=1}^2 \varphi(d_i)$	$\nu_{(5,5)/\mathbb{F}_2}(\vec{d})$	$\eta_{(5,5)/\mathbb{F}_2}(\vec{d})$
$(1,1)$	1	1	1
$(1,5)$	4	4	1
$(5,1)$	4	4	1
$(5,5)$	16	4	4

Table 3.1: Computing $\nu_{(5,5)/\mathbb{F}_2}(\vec{d})$ and $\eta_{(5,5)/\mathbb{F}_2}(\vec{d})$

By Theorem 3.5.13 with the above table, the semisimple decomposition of $\mathcal{C}_{(5,5)/\mathbb{F}_2}$ equals:

$$\mathcal{C}_{(5,5)/\mathbb{F}_2} \cong \mathbb{F}_2 \oplus \mathbb{F}_{2^4} \oplus \mathbb{F}_{2^4} \oplus (\mathbb{F}_{2^4})^4 = \mathbb{F}_2 \oplus (\mathbb{F}_{2^4})^6.$$

As a result, the indecomposable components of $\mathcal{C}_{(5,5,2^l)/\mathbb{F}_2}$ consist up to isomorphism of the following rings:

$$\mathbb{F}_2[Y_1, Y_2, Y_3]/(Y_1 - 1, Y_2 - 1, Y_3^{2^l} - 1) \cong \mathbb{F}_2[Y]/(Y^{2^l} - 1),$$
$$\mathbb{F}_{2^4}[Y_1, Y_2, Y_3]/(Y_1 - 1, Y_2 - 1, Y_3^{2^l} - 1) \cong \mathbb{F}_{2^4}[Y]/(Y^{2^l} - 1),$$

hence we have the decomposition:

$$\mathcal{C}_{(5,5,2^l)/\mathbb{F}_2} \cong \mathbb{F}_2[Y]/(Y^{2^l} - 1) \oplus \left(\mathbb{F}_{2^4}[Y]/(Y^{2^l} - 1)\right)^6.$$

Chapter 4

Circulant modules and applications

4.1 Introduction

The results in this chapter are based on the first part of the paper [Sub24a]. Here we dive into more details on the technical results, including a more comprehensive discussion compared to what was done in the paper. Also, we use the notation presented in Chapter 3, which differs slightly from the notation used in the paper.

4.2 Circulant modules

Let us introduce the concept of a circulant module.

Definition 4.2.1. Let $\mathcal{C}_{\vec{m},k}$ be a circulant ring, and let V be a $\mathcal{C}_{\vec{m},k}$-module. Then V is said to be a **circulant module** of rank ω if it is isomorphic to the free $\mathcal{C}_{\vec{m},k}$-module $(\mathcal{C}_{\vec{m},k})^{\omega}$.

In this section, we present a particular class of circulant modules which encapsulates the concept of shifting in vector spaces. This insight is useful in studying circulant properties in linear mappings, which is covered in subsequent sections.

4.2.1 Shifts as circulant modules

The underlying vector space $V_{\vec{m}/k}$

Let k be a field, and consider the n-tuple $\vec{m} := (m_1, \dots, m_n)$ consisting of positive integers. We define the k-vector space $V_{\vec{m}/k}$ as the tensor product:

$$V_{\vec{m}/k} := \bigotimes_{i=1}^{n} k^{m_i},$$

where k^{m_i} is a k-vector space of dimension m_i.

For all $1 \le i \le n$ and $0 \le j_i < m_i$, we denote the j_i-th unit vectors of k^{m_i} by $\mathrm{e}^i_{j_i}$, where $0 \le j_i < m_i$. Define the set:

$$B_{\vec{m}} := \left\{ \otimes_{i=1}^{n} \mathrm{e}_{j_i} \mid 0 \le j_i < m_i \right\},$$

which is a k-linear basis of $V_{\vec{m}/k}$.

Our goal is to induce $V_{\vec{m}/k}$ with a natural $\mathcal{C}_{\vec{m}/k}$-module structure.

Shifts in $V_{\vec{m}/k}$

Let $m > 0$ be an integer, and consider a vector $v := (v_0, \dots, v_{m-1}) \in k^m$. For another integer $0 \le s < m$, we define the shift map as:

$$\varsigma_{m,s} \colon k^m \to k^m, \ v \mapsto v^*,$$

where $v^*_j := v_{j-s \bmod m}$ for all $0 \le j < m$. This map is a bijective linear map.

Given n-tuples $\vec{m} := (m_1, \dots, m_n) \in \mathbb{Z}^n_{>0}$ and $\vec{s} := (s_1, \dots, s_n) \in \mathbb{Z}^n_{\ge 0}$ where $0 \le s_i < m_i$, we define the map:

$$\varsigma_{\vec{m},\vec{s}} \colon V_{\vec{m}/k} \to V_{\vec{m}/k}, \ \otimes_{i=1}^{n} v^i \mapsto \otimes_{i=1}^{n} \varsigma_{m_i,s_i}(v^i),$$

where v^i refers to a vector in k^{m_i}. Observe that this map is also a bijective linear map.

Modules over circulant rings

We induce $V_{\vec{m}/k}$ with a $\mathcal{C}_{\vec{m}/k}$-module structure based on the shift maps $\varsigma_{\vec{m},-}$. Let $M_{\vec{m}}$ be a set consisting of some monomials as defined in Remark 3.2.3. One can define the natural map:

$$\mu^*_{\vec{m}/k} \colon M_{\vec{m}} \times V_{\vec{m}/k} \to V_{\vec{m}/k}, \ \left(\prod_{i=1}^{n} X_i^{s_i}, v \right) \mapsto \varsigma_{\vec{m},\vec{s}}(v),$$

where $\vec{s} \coloneqq (s_1, \ldots, s_n)$. This map can be extended k-linearly to the map:

$$\mu_{\vec{m}/k} \colon \mathcal{C}_{\vec{m}/k} \times V_{\vec{m}/k} \to V_{\vec{m}/k}, \left(\sum_{M \in M_{\vec{m}}} c_M \cdot M, v \right) \mapsto \sum_{M \in M_{\vec{m}}} c_M \cdot \mu^*_{\vec{m}/k}(M, v),$$

where $c_M \in k$. One can verify that $V_{\vec{m}/k}$ is an $\mathcal{C}_{\vec{m}/k}$-module under $\mu_{\vec{m}/k}$. This module has the following property:

Proposition 4.2.2. *The $\mathcal{C}_{\vec{m}/k}$-module $V_{\vec{m}/k}$ under $\mu_{\vec{m}/k}$ is a free $\mathcal{C}_{\vec{m}/k}$-module of rank 1, hence a circulant module.*

Proof. Consider the following bijective map between the bases:

$$\vartheta^*_{\vec{m}/k} \colon B_{\vec{m}} \to M_{\vec{m}}, \ \otimes_{i=1}^n \mathrm{e}_{j_i} \mapsto \prod_{i=1}^n X_i^{j_i}.$$

This map k-linearly extends to the bijective map:

$$\vartheta_{\vec{m}/k} \colon V_{\vec{m}/k} \to \mathcal{C}_{\vec{m}/k}, \ \sum_{\beta \in B_{\vec{m}}} c_\beta \cdot \beta \mapsto \sum_{\beta \in B_{\vec{m}}} c_\beta \cdot \vartheta^*_{\vec{m}/k}(\beta), \tag{4.1}$$

which by construction is a linear map. One can verify that this map is also a $\mathcal{C}_{\vec{m}/k}$-module homomorphism, hence proving our claim. □

4.2.2 Univariate circulant modules: circulant matrices

Univariate circulant rings are of the form $\mathcal{C}_{m/k} \coloneqq k[X]/(X^m - 1)$ for some $m > 0$. The theory of circulant modules of rank 1 over univariate circulant rings is interesting as a topic on its own, as they are closely related to the theory of circulant matrices.

Definition 4.2.3 (**Circulant matrices**)**.** Let k be a field, and m some positive integer. Let $v \coloneqq (v_0, \ldots, v_{m-1}) \in k^m$ be an m-tuple. The m-dimensional **circulant matrix** over k parametrized by v, denoted by $\mathrm{circ}(v)$, is the matrix of the form:

$$\mathrm{circ}(v) \coloneqq \begin{pmatrix} v_0 & v_{m-1} & \cdots & v_2 & v_1 \\ v_1 & v_0 & \cdots & v_3 & v_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ v_{m-2} & v_{m-3} & \cdots & v_0 & v_{m-1} \\ v_{m-1} & v_{m-2} & \cdots & v_1 & v_0 \end{pmatrix},$$

We denote the set of all m-dimensional circulant matrices over k by $C_{m/k}$.

The set of circulant matrices form a k-algebra, where addition and multiplication is defined by their usual matrix operations. In fact, we have that the k-algebra of circulant matrices is isomorphic to a univariate circulant ring.

Theorem 4.2.4. *We have the isomorphism of k-algebras:*

$$\varpi_{m/k}\colon C_{m/k} \to \mathcal{C}_{m/k},\ \operatorname{circ}(v) \mapsto \sum_{i=0}^{m-1} v_i X^{v_i}.$$

Proof. See Theorem 4 of [KS12]. □

The vector space $V_{m/k}$ naturally inherits a $C_{m/k}$-module structure, where $\operatorname{circ}(v) \cdot w$ is defined as $\operatorname{circ}(v) \cdot w^t$ (standard matrix multiplication with the column vector w^t). We denote the module map by $\varrho_{m/k}\colon C_{m/k} \times V_{m/k} \to V_{m/k}$. We explore $\varrho_{m/k}$ in greater detail.

As a result of Theorem 4.2.4, the set $B_{C_{m/k}} := \{\operatorname{circ}(\mathrm{e}_i) \mid 0 \le i < m\}$ forms a natural basis of $C_{m/k}$ viewed as a k-linear vector space, where e_i is the i-th unit vector in k^m. Observe that for all $0 \le s < m$, we have:

$$\varrho_{m/k}(\operatorname{circ}(\mathrm{e}_s), w) := \varsigma_{m,s}(w) = \mu_{m/k}(X^s, w) = \mu_{m/k}(\varpi(\operatorname{circ}(\mathrm{e}_s)), w).$$

Proposition 4.2.5. *The modules on $V_{m/k}$ induced by $\varrho_{m/k}$ and $\mu_{m/k}$ are equivalent.*

Proof. Using the above observations, we have a commutative diagram on the level of bases:

$$\begin{tikzcd}
B_{C_{m/k}} \times V_{m/k} \arrow[r, "\varrho_{m/k}"] \arrow[d, "\varpi\times\mathrm{id}"'] & V_{m/k} \arrow[d, "\mathrm{id}"] \\
M_{\vec{m}} \times V_{m/k} \arrow[r, "\mu_{m/k}"] & V_{m/k}
\end{tikzcd}$$

This linearly extends to the bijective map $\varpi \times \mathrm{id}\colon C_{m/k} \times V_{m/k} \to \mathcal{C}_{m/k} \times V_{m/k}$ satisfying the identity:

$$\mathrm{id} \circ \varrho_{m/k} = \mu_{m/k} \circ (\varpi \times \mathrm{id}).$$

As such, $\varrho_{m/k}$ and $\mu_{m/k}$ are equivalent. □

4.2.3 General linear group over circulant rings

Let $\mathcal{C}_{\vec{m}/k}$ be a circulant ring with parameters $\vec{m} := (m_1, \ldots, m_n)$ and k a field of characteristic p. Endomorphisms of circulant modules of rank d over $\mathcal{C}_{\vec{m}/k}$

are uniquely represented by matrices in $\mathrm{Mat}_d(\mathcal{C}_{\vec{m}/k})$. In this section, we focus on the invertible matrices, or equivalently matrices in the general linear group $\mathrm{GL}_d(\mathcal{C}_{\vec{m}/k})$.

By Theorem 3.4.18, any circulant ring is a direct sum of local circulant rings. As such, $\mathrm{GL}_d(\mathcal{C}_{\vec{m}/k})$ is a direct sum of general linear groups over local circulant rings. Hence it suffices to only consider general linear groups over local circulant rings. For the remainder of this section, $\mathcal{C}_{\vec{m},k}$ is assumed to be local, where we denote its unique maximal ideal by $\mathfrak{m}$.

Define the quotient map $\mathfrak{q}_{\vec{m}/k}: \mathcal{C}_{\vec{m}/k} \mapsto \mathcal{C}_{\vec{m},k}/\mathfrak{m} \cong k$, which is the same map as in Eq. (3.5). This map extends to the map of $d \times d$-matrices:

$$\mathfrak{q}^d_{\vec{m}/k}: \mathrm{Mat}_d(\mathcal{C}_{\vec{m}/k}) \to \mathrm{Mat}_d(k),\ A := (A_{ij})_{0 \le i,j \le m-1} \mapsto (\mathfrak{q}_{\mathfrak{m}/k}(A_{ij}))_{0 \le i,j \le m-1}.$$

Observe that $\det(\mathfrak{q}^d_{\vec{m}/k}(A)) = \mathfrak{q}_{\vec{m}/k}(\det(A))$, since the expression of the determinant consists of finite sums of finite products of entries of A, which split under $\mathfrak{q}_{\vec{m}/k}$. This implies that $\mathfrak{q}^d_{\vec{m}/k}(\mathrm{GL}_d(\mathcal{C}_{\vec{m}/k})) \subseteq \mathrm{GL}_d(k)$. Moreover, the preimage of $\mathrm{GL}_d(k)$ under $\mathfrak{q}^d_{\vec{m}/k}$ is exactly $\mathrm{GL}_d(\mathcal{C}_{\vec{m}/k})$, as a result of the following lemma:

Lemma 4.2.6. *For a matrix $A \in \mathrm{Mat}_d(\mathcal{C}_{\vec{m}/k})$, we have that $A \in \mathrm{GL}_d(\mathcal{C}_{\vec{m}/k})$ if and only if $\mathfrak{q}^d_{\vec{m}/k}(A) \in \mathrm{GL}_d(k)$.*

Proof. This is due to the following equivalent statements:

$$\begin{aligned} A \in \mathrm{GL}_d(\mathcal{C}) \Leftrightarrow \det(A) \in \mathcal{C}^*_{\vec{m}/k} \Leftrightarrow \det(A) \notin \mathfrak{m} \Leftrightarrow \det(\mathfrak{q}^d_{\vec{m}/k}(A)) \in k^* \\ \Leftrightarrow \mathfrak{q}^d_{\vec{m}/k}(A) \in \mathrm{GL}_d(k). \end{aligned}$$

□

Lemma 4.2.6 implies that the map $\mathfrak{q}^d_{\vec{m}/k}|_{\mathrm{GL}_d(\mathcal{C}_{\vec{m}/k})}: \mathrm{GL}_d(\mathcal{C}_{\vec{m}/k}) \to \mathrm{GL}_d(k)$ is a surjective group homomorphism, which we denote by $\hat{\mathfrak{q}}^d_{\vec{m}/k}$. Lemma 4.2.6 also implies that:

$$\ker(\hat{\mathfrak{q}}^d_{\vec{m}/k}) = \{I_d + A : A \in \mathrm{Mat}_d(\mathfrak{m})\}.$$

This observation is particularly useful when k is a finite field $\mathbb{F}_q$, as we are now able to determine the order of $\ker(\hat{\mathfrak{q}}^d_{\vec{m}/\mathbb{F}_q})$:

$$\#\ker(\hat{\mathfrak{q}}^d_{\vec{m}/\mathbb{F}_q}) = \#\mathrm{Mat}_d(\mathfrak{m}) = (\#\mathfrak{m})^{d^2} = \left(q^{(\prod_{i=1}^n p^{v_p(m_i)})-1}\right)^{d^2}. \tag{4.2}$$

This implies in particular that the order of the group $\ker(\hat{\mathfrak{q}}^d_{\vec{m}/\mathbb{F}_q})$ is a power of p, hence making it a p-group. By Lagrange's theorem, the order of an element $I_d + A \in \ker(\hat{\mathfrak{q}}^d_{\vec{m}/\mathbb{F}_q})$, where $A \in \mathrm{Mat}_d(\mathfrak{m})$, is of the form p^λ for some $\lambda \geq 0$. Note that:

$$(I_d + A)^{p^\lambda} = I_d + A^{p^\lambda},$$

by the binomial theorem of Newton, and since $\mathcal{C}_{\vec{m}/\mathbb{F}_q}$ is of characteristic p. Newton's binomial theorem applies in this situation since the identity matrix I_d commutes with any matrix. Hence $\mathrm{ord}(I_d + A)$ is the smallest number of the form p^λ such that $A^{p^\lambda} = 0_{d\times d}$. In particular, A is a **nilpotent matrix**.

Lemma 4.2.7. *Let $A \in \mathrm{Mat}_d(\mathfrak{m})$ and define $l_{(\vec{m},p)} = \max(v_p(m_i) : 1 \leq i \leq n)$. Then we have $A^{d\cdot p^{l(\vec{m},p)}} = 0_{d\times d}$.*

Proof. In this proof, we use $\mathbb{Z}^d_{\geq 0}$ as an index set, and we let e_i be the i-th unit vector in $\mathbb{Z}^d_{\geq 0}$ where $0 \leq i \leq n-1$.

By assumption of the lemma, there exist matrices $A_{\mathrm{e}_i} \in \mathrm{Mat}_d(\mathcal{C}_{\vec{m}/\mathbb{F}_q})$ such that:

$$A = \sum_{i=1}^{n}(X_i - 1)\cdot A_{\mathrm{e}_i}. \tag{4.3}$$

From this, we can construct matrices $A_{j_1\mathrm{e}_1+\cdots+j_n\mathrm{e}_n} \in \mathrm{Mat}_d(\mathcal{C}_{\vec{m}/\mathbb{F}_q})$ such that:

$$A^2 = \sum_{\substack{0\leq j_1,\ldots,j_n\leq 2\\ j_1+\cdots+j_n=2}} A_{j_1\mathrm{e}_1+\cdots+j_n\mathrm{e}_n}\cdot\prod_{i=1}^{n}(X_i-1)^{j_i}. \tag{4.4}$$

Here we have:

$$A_{j_1\mathrm{e}_1+\cdots+j_n\mathrm{e}_n} = \sum_{\substack{0\leq j_1,\ldots,j_n\leq 2\\ j_1+\cdots+j_n=2}} A^{j_i}_{\mathrm{e}_i}.$$

Note that the matrices A_{e_i} satisfying (4.3) are not unique. For the proof, it suffices to only knowing its existence.

By inductively applying this reasoning, one can show that for all $r \in \mathbb{Z}_{>0}$, there exists a family of matrices $A_{j_1\mathrm{e}_1+\cdots+j_n\mathrm{e}_n} \in \mathrm{Mat}_d(\mathcal{C}_{\vec{m}/\mathbb{F}_q})$ where $j_1+\cdots+j_n = r$ such that:

$$A^r = \sum_{\substack{0\leq j_1,\ldots,j_n\leq r\\ j_1+\cdots+j_n=r}} A_{j_1\mathrm{e}_1+\cdots+j_n\mathrm{e}_n}\cdot\prod_{i=1}^{n}(X_i-1)^{j_i}. \tag{4.5}$$

When $r \geq n \cdot p^{l_{(\vec{m},p)}}$, we must have that $j_i \geq p^{v_p(m_i)}$ for some i, which implies that $\prod_{i=1}^{n}(X_i - 1)^{j_i} \in \mathfrak{m}$ for all $j_1, \ldots, j_n$ satisfying $j_1 + \cdots + j_n = r$. Hence we have $A^{n \cdot p^{l_{(\vec{m},p)}}} = 0_{d \times d} \in \mathrm{Mat}_d(\mathcal{C}_{\vec{m}/\mathbb{F}_q})$ by applying Equation (4.5), which concludes the proof. □

Corollary 4.2.8. *For $B \in \ker(\hat{\mathfrak{q}}^d_{\vec{m}/\mathbb{F}_q})$, we have that $\mathrm{ord}(B) \mid p^{l_{(\vec{m},p)} + \lceil \log_p(n) \rceil}$.*

Proof. To ease notation, we denote $l := l_{(\vec{m},p)}$. Every element $B \in \ker(\hat{\mathfrak{q}}^d_{\vec{m}/\mathbb{F}_q})$ is of the form $I_d + C$, where $C \in \mathrm{Mat}_d(\mathfrak{m})$. Observe that:

$$p^{l + \lceil \log_p(n) \rceil} = p^{\lceil \log_p(n) \rceil} \cdot p^l \geq n \cdot p^l.$$

From this identity together with Lemma 4.2.7, we have:

$$\begin{aligned} B^{p^{l+\lceil \log_p(n) \rceil}} &= (I_d + C)^{p^{l+\lceil \log_p(n) \rceil}} = I_d^{p^{l+\lceil \log_p(n) \rceil}} + C^{p^{l+\lceil \log_p(n) \rceil}} = I_d + 0_{d \times d} \\ &= I_d, \end{aligned}$$

which concludes the proof. □

4.3 Application: Linear layer of XOODOO

XOODOO is a permutation, used in the permutation-based scheme XOOFFF, that works on a 384 bit state.

In this section, we show how circulant modules can be used to study the linear layer of XOODOO. This also led to the solution to a previously open problem: A mathematical explanation of the low order of the linear layer of XOODOO.

4.3.1 XOODOO specifications

We present the specifications of XOODOO as explained in [DHVV18]. As such, this section is copied from that paper, with slight modifications to fit in with this thesis.

XOODOO has a classical iterated structure: It iteratively applies a round function to a state. The state consists of 3 equally sized horizontal *planes*, each one consisting of 4 parallel 32-bit *lanes*. Similarly, the state can be seen as a set of 128 *columns* of 3 bits, arranged in a 4×32 array. The planes are indexed by y, with plane $y = 0$ at the bottom and plane $y = 2$ at the top. Within a lane, we index bits with z. The lanes within a plane are indexed by x, so the position of a lane in the state is determined by the two coordinates

(x, y). The bits of the state are indexed by (x, y, z) and the columns by (x, z). *Sheets* are the arrays of three lanes on top of each other and they are indexed by x. The XOODOO state is illustrated in Figure 4.1.

The permutation consists of the iteration of a round function Ri that has 5 steps: a mixing layer θ, a plane shifting ρ_{west}, the addition of round constants ι, a non-linear layer χ and another plane shifting ρ_{east}. The composition $\rho_{\text{east}} \circ \theta \circ \rho_{\text{west}}$ form the *linear layer* of XOODOO().

We specify XOODOO in Algorithm 1, completely in terms of operations on planes and use thereby the notational conventions we specify in Table 4.1. We illustrate the step mappings in a series of figures: the χ operation in Figure 4.2, the θ operation in Figure 4.3, the ρ_{east} and ρ_{west} operations in Figure 4.4.

The round constants C_i are planes with a single non-zero lane at $x = 0$, denoted as c_i. The values of the round constants for any index can be found in the Appendix of [DHVV18].

Finally, in many applications the state must be specified as a 384-bit string s with the bits indexed by i. The mapping from the three-dimensional indexing (x, y, z) and i is given by $i = z + 32(x + 4y)$.

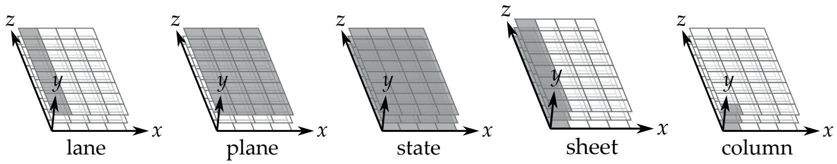

Figure 4.1: Toy version of the Xoodoo state, with lanes reduced to 8 bits, and different parts of the state highlighted.

A_y	Plane y of state A
$A_y \lll (t,v)$	Cyclic shift of A_y moving bit in (x,z) to position $(x+t,z+v)$
$\overline{A_y}$	Bitwise complement of plane A_y
$A_y + A_{y'}$	Bitwise sum (XOR) of planes A_y and $A_{y'}$
$A_y \cdot A_{y'}$	Bitwise product (AND) of planes A_y and $A_{y'}$

Table 4.1: Notational conventions

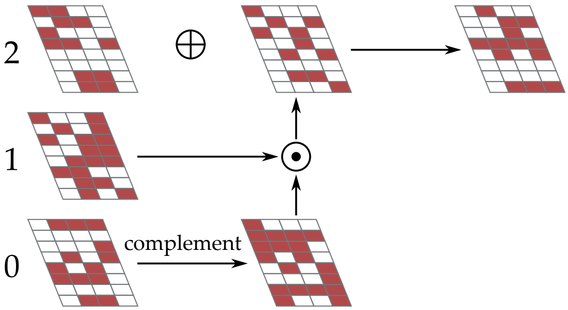

Figure 4.2: Effect of χ on one plane.

Algorithm 1 Definition of XOODOO$[n_\mathrm{r}]$ with n_r the number of rounds

```
**Parameters:** Number of rounds $n_\mathrm{r}$
**for** Round index $i$ from $1 - n_\mathrm{r}$ to 0 **do**
    $A = \mathrm{R}i(A)$

Here $\mathrm{R}i$ is specified by the following sequence of steps:
    $\theta$ :
        $P \leftarrow A_0 + A_1 + A_2$
        $E \leftarrow P \lll (1,5) + P \lll (1,14)$
        $A_y \leftarrow A_y + E$ for $y \in \{0,1,2\}$
    $\rho_\mathrm{west}$ :
        $A_1 \leftarrow A_1 \lll (1,0)$
        $A_2 \leftarrow A_2 \lll (0,11)$
    $\iota$ :
        $A_0 \leftarrow A_0 + \mathrm{C}_i$
    $\chi$ :
        $B_0 \leftarrow \overline{A_1} \cdot A_2$
        $B_1 \leftarrow \overline{A_2} \cdot A_0$
        $B_2 \leftarrow \overline{A_0} \cdot A_1$
        $A_y \leftarrow A_y + B_y$ for $y \in \{0,1,2\}$
    $\rho_\mathrm{east}$ :
        $A_1 \leftarrow A_1 \lll (0,1)$
        $A_2 \leftarrow A_2 \lll (2,8)$
```

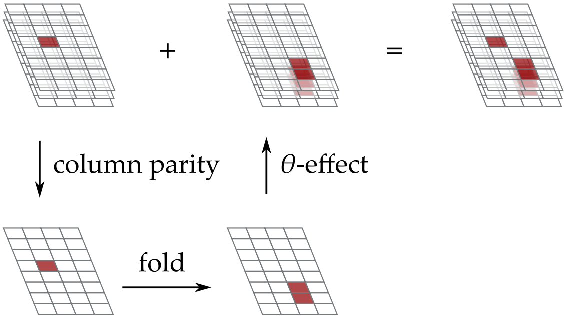

Figure 4.3: Effect of θ on a single-bit state.

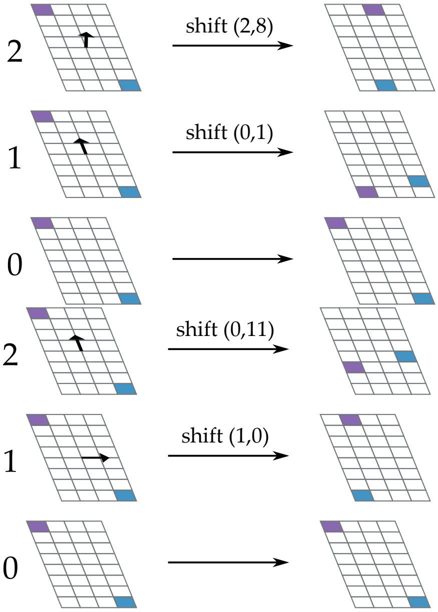

Figure 4.4: Illustration of ρ_{east} (left) and ρ_{west} (right).

4.3.2 Linear layer of Xoodoo and circulant modules

The linear layer of Xoodoo consists of the composition $\rho_{\text{east}} \circ \theta \circ \rho_{\text{west}}$. in this subsection, we establish the relation between this linear layer and the theory of circulant modules as described in the previous section. We start by observing that the vector space of 4×32-planes can be viewed as the tensor product $V_{(4,32)/\mathbb{F}_2} := \mathbb{F}_2^4 \otimes \mathbb{F}_2^{32}$, where a plane A_y is represented by the element:

$$A_y \mapsto \sum_{i=0}^{3} \sum_{j=0}^{31} A_y(i+1, j+1) \cdot (\mathrm{e}_i \otimes \mathrm{e}_j) \in V_{(4,32)/\mathbb{F}_2}.$$

Here, $A_y(i+1, j+1)$ represents the entry of the plane at coordinate $(i+1, j+1)$. The reason for the expression $(i+1, j+1)$ is the difference of indexing, as indexing in $V_{(4,32)/\mathbb{F}_2}$ starts by assumption from $i, j = 0$, while indexing in planes starts from $i, j = 1$.

Using this transformation, one can interpret the linear maps $\rho_{\text{east}}, \rho_{\text{west}}, \theta$ as maps over $V^3_{(4,32)/\mathbb{F}_2}$ instead. This turns out to be a very useful interpretation, as the following theorem shows:

Theorem 4.3.1. *The linear maps $\rho_{east}, \rho_{west}, \theta\colon V^3_{(4,32)/\mathbb{F}_2} \to V^3_{(4,32)/\mathbb{F}_2}$ are all $\mathcal{C}_{(4,32)/\mathbb{F}_2}$-endomorphisms.*

Proof. We only show this result for θ, as the method of proof is identical for ρ_{east} and ρ_{west}.

Since θ is a linear map over $\mathbb{F}_2$, it preserves addition. As such, we are only required to show that θ preserves scaling over $\mathcal{C}_{(4,32)/\mathbb{F}_2}$.

For $\vec{v} := (v_0, v_1, v_2) \in V^3_{(4,32)/\mathbb{F}_2}$, define $v_\Sigma := v_0 + v_1 + v_2 \in V_{(4,32)/\mathbb{F}_2}$ together with the vector $\vec{v}_\Sigma := (v_\Sigma, v_\Sigma, v_\Sigma) \in V^3_{(4,32)/\mathbb{F}_2}$. Moreover, let us denote the polynomial $f := X_1 X_2^5 + X_1 X_2^{14} \in \mathcal{C}_{(4,32)/\mathbb{F}_2}$. Then the map θ is formulated as:

$$\theta(\vec{v}) = \vec{v} + f \cdot \vec{v}_\Sigma,$$

where $f \cdot \vec{v}_\Sigma := \mu_{(4,32)/\mathbb{F}_2}(f, \vec{v}_\Sigma)$. Observe that for every $g \in \mathcal{C}_{(4,32)/\mathbb{F}_2}$, we have:

$$\theta(g \cdot \vec{v}) = g \cdot \vec{v} + f \cdot (g \cdot \vec{v}_\Sigma) = g \cdot \vec{v} + g \cdot (f \cdot \vec{v}_\Sigma) = g \cdot \vec{v} + f \cdot \vec{v}_\Sigma = g \cdot \theta(\vec{v}).$$

Hence θ indeed preserves scaling, which concludes the proof. □

As a result, each of $\rho_{\text{east}}, \rho_{\text{west}}, \theta$ have a unique matrix representation viewed as endomorphisms over $\mathcal{C}^3_{(4,32)/\mathbb{F}_2}$, after the domain transformation by $\vartheta^3_{\vec{m}/k}$ defined in Eq. 4.1.

Matrix representation of $\rho_{\textbf{east}}$

For $\vec{v} := (v_0, v_1, v_2) \in V^3_{(4,32)/\mathbb{F}_2}$, observe that:

$$\rho_{\text{east}}(\vec{v}) = (X_2 \cdot v_0, (X_1^2 X_2^8) \cdot v_1, v_2),$$

which is represented by the diagonal matrix:

$$\rho^*_{\text{east}} = \begin{pmatrix} X_2 & 0 & 0 \\ 0 & X_1^2 X_2^8 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Indeed, we have:

$$\begin{pmatrix} X_2 & 0 & 0 \\ 0 & X_1^2 X_2^8 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} v_0 \\ v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} X_2 \cdot v_0 \\ (X_1^2 X_2^8) \cdot v_1 \\ v_2 \end{pmatrix} = \rho_{\text{east}}(\vec{v}).$$

Matrix representation of $\rho_{\textbf{west}}$

For $\vec{v} := (v_0, v_1, v_2) \in V^3_{(4,32)/\mathbb{F}_2}$, observe that:

$$\rho_{\text{west}}(\vec{v}) = (X_1 \cdot v_0, X_2^{11} \cdot v_1, v_2),$$

which is represented by the diagonal matrix:

$$\rho^*_{\text{west}} = \begin{pmatrix} X_1 & 0 & 0 \\ 0 & X_2^{11} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Indeed, we have:

$$\begin{pmatrix} X_1 & 0 & 0 \\ 0 & X_2^{11} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} v_0 \\ v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} X_1 \cdot v_0 \\ X_2^{11} \cdot v_1 \\ v_2 \end{pmatrix} = \rho_{\text{west}}(\vec{v}).$$

Matrix representation of θ

Like in the proof of Theorem 4.3.1, we find expressions for θ on the level of coordinates. For $\vec{v} := (v_0, v_1, v_2)$ and $f := X_1 X_2^5 + X_1 X_2^{14} \in \mathcal{C}_{(4,32)/\mathbb{F}_2}$, we have:

$$\theta(\vec{v}) = (v_0 + f \cdot (v_0 + v_1 + v_2), v_1 + f \cdot (v_0 + v_1 + v_2), v_2 + f \cdot (v_0 + v_1 + v_2)).$$

Observe that this is represented by the matrix:

$$\theta^* = \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix}.$$

Indeed, we have:

$$\begin{aligned} \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix} \cdot \begin{pmatrix} v_0 \\ v_1 \\ v_2 \end{pmatrix} &= \begin{pmatrix} (1+f) \cdot v_0 + f \cdot v_1 + f \cdot v_2 \\ f \cdot v_0 + (1+f) \cdot v_1 + f \cdot v_2 \\ f \cdot v_0 + f \cdot v_1 + (1+f) \cdot v_2 \end{pmatrix} \\ &= \begin{pmatrix} v_0 + f \cdot (v_0 + v_1 + v_2) \\ v_1 + f \cdot (v_0 + v_1 + v_2) \\ v_2 + f \cdot (v_0 + v_1 + v_2) \end{pmatrix} \\ &= \theta(\vec{v}). \end{aligned}$$

4.3.3 Order of the linear layer of Xoodoo

An unexpected observation which was derived numerically, is that the linear layer of Xoodoo has a low order of only 32. This is surprising given the bit-state of 384 bits. Having a low order for the linear layer is in general undesired due to being a potential weakness against invariant subspace attacks [BCLR17]. A proper mathematical explanation of this phenomenon remained absent, until the module-theoretic approach covered in the previous section was introduced.

The maps ρ_{east}, ρ_{west} and θ are all bijective circulant endomorphisms. As such, their corresponding matrix representations are contained in $\mathrm{GL}_3(\mathcal{C}_{(4,32)/\mathbb{F}_2})$. Observe that $\mathcal{C}_{(4,32)/\mathbb{F}_2}$ is a local ring, as the parameters 4 and 32 are powers of 2 (see Theorem 3.4.1). Its unique maximal ideal is the ideal $(X_1 - 1, \ldots, X_n - 1)$, which we denote by $\mathfrak{m}$. Note that for $g \in \mathcal{C}_{(4,32)/\mathbb{F}_2}$, we have that $\hat{\mathfrak{q}}_{(4,32)/\mathbb{F}_2}(g) = g(1,1) \in \mathbb{F}_2$, which means we evaluate the polynomial g at $(1,1)$. Using this insight, we compute $\hat{\mathfrak{q}}^3_{(4,32)/\mathbb{F}_2}$ for the matrices

ρ^*_{east}, ρ^*_{west} and θ^* discussed in the previous section:

$$\hat{\mathfrak{q}}^3_{(4,32)/\mathbb{F}_2}(\rho^*_{\text{east}}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1^2 \cdot 1^8 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\hat{\mathfrak{q}}^3_{(4,32)/\mathbb{F}_2}(\rho^*_{\text{west}}) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1^{11} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\hat{\mathfrak{q}}^3_{(4,32)/\mathbb{F}_2}(\theta^*) = \begin{pmatrix} 1+f(1,1) & f(1,1) & f(1,1) \\ f(1,1) & 1+f(1,1) & f(1,1) \\ f(1,1) & f(1,1) & 1+f(1,1) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

as $f(1,1) = 1 \cdot 1^5 + 1 \cdot 1^{14} = 1 + 1 = 0$ in $\mathbb{F}_2$. Observe that all are the identity matrix in $\mathrm{GL}_3(\mathbb{F}_2)$, which implies that their composition is also the identity matrix. As such, $\rho_{\text{west}} \circ \theta \circ \rho_{\text{east}}$ is in the kernel of $\hat{\mathfrak{q}}^3_{(4,32)/\mathbb{F}_2}$. From Corollary 4.2.8, the order of this composition must be a divisor of:

$$2^{l((4,32),2)+\log_2(2)} = 2^{5+1} = 2^6 = 64,$$

which is only double the observed order. From this mathematical analysis, the main reason of the low order is due to being a circulant module endomorphism over a local circulant ring.

4.3.4 Alternative compositions

We present two alternative compositions for the linear layer of Xoodoo with a similar structure and bit-state, but a higher order.

Alternative 1: Same bit state

We give an example of an alternative linear layer of the same bit-state as Xoodoo, which is also a $\mathcal{C}_{(4,32)/\mathbb{F}_2}$-endomorphism over the free circulant module $(\mathcal{C}_{(4,32)/\mathbb{F}_2})^3$.

Consider the composition $\rho'_l \circ \theta' \circ \rho'_r$, consisting of the maps:

$$\rho'_l := \begin{pmatrix} 1 & 0 & 0 \\ 0 & X_1 & 0 \\ 0 & 0 & X_2^{11} \end{pmatrix} \quad \rho'_r := \begin{pmatrix} 1 & 0 & 0 \\ 0 & X_2 & 0 \\ 0 & 0 & X_1^2 X_2^8 \end{pmatrix} \quad \theta' := \begin{pmatrix} 1+f_1 & f_1 & f_1 \\ f_2 & 1+f_2 & f_2 \\ f_3 & f_3 & 1+f_3 \end{pmatrix},$$

where $f_1 = f_3 = X_1 X_2^5 + X_1 X_2^{11} + 1$ and $f_2 = X_1 X_2^5 + X_1 X_2^{11}$. We verified using SageMath that $\mathrm{ord}(\rho_l \circ \theta \circ \rho_r) = 128$, which is the maximal possible order of such a composition by the above theorem. The following code was used:

```
#Setting up the ring R_{4,32}
R.<s,t> = GF(2)[]
S.<x,y> = R.quo([s^4 - 1, t^32 - 1])

#Defining \rho_l, \rho_r and \theta for the composition DCD
f1 = x*y^5 + x*y^11 + 1
f2 = x*y^5 + x*y^11
f3 = x*y^5 + x*y^11 + 1

theta = matrix([[1+f1,f1,f1],[f2,1+f2,f2],[f3,f3,1+f3]])
p_l = matrix([[1,0,0],[0,x,0],[0,0,y^11]])
p_r = matrix([[1,0,0],[0,y,0],[0,0,x^2*y^8]])
DCD = p_l*theta*p_r

#Naively computing the order of DCD using brute force
i = 1
while DCD^i != matrix.identity(3):
    i = i + 1

print(i)
```

Alternative 2: Slightly larger bit state

Consider the univariate circulant ring $\mathcal{C}_{167/\mathbb{F}_2} := \mathbb{F}_2[X]/(X^{167}-1)$, and consider the composition $\rho''_l \circ \theta'' \circ \rho''_r \colon (\mathcal{C}_{167/\mathbb{F}_2})^3 \to (\mathcal{C}_{167/\mathbb{F}_2})^3$, consisting of the maps:

$$\rho''_l := \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X^{11} \end{pmatrix} \quad \rho''_r := \begin{pmatrix} 1 & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X^{10} \end{pmatrix} \quad \theta'' := \begin{pmatrix} 1+f & f & f \\ f & 1+f & f \\ f & f & 1+f \end{pmatrix},$$

where $f = X^6 + X^{15}$. It has a very high order of $\left(2^{83}-1\right) \cdot \lambda$, where:

$$\begin{aligned} \lambda = {} & 301\,541\,899\,055\,510\,925\,582\,216\,169\,150\,861\,286\,153\,081\,761\,757\,331\,612\,351 \\ & 867\,575\,029\,327\,375\,019 \\ \approx {} & 1.33 \cdot 2^{247}. \end{aligned}$$

This is significantly larger than 32, while only having an additional $3 \cdot 167 - 3 \cdot 4 \cdot 32 = 117$ bits compared to the bit state of Xoodoo. The design and derivation of this order is a combination of both a theoretical and numerical approach. We describe the techniques of the computation in two steps.

Step 1: Showing $2^{83}-1$ divides the order Let us look at the semisimple decomposition of $\mathcal{C}_{167/\mathbb{F}_2}$.

Proposition 4.3.2. *Let $f \in \mathcal{C}^*_{167/\mathbb{F}_2}$ not equal to 1, then* $\operatorname{ord}(f) = 2^{83} - 1$.

Proof. The circulant ring $\mathcal{C}_{167/\mathbb{F}_2}$ is semisimple due to Maschke's theorem (Theorem 3.3.1), since 167 is coprime to 2. Let us find the semisimple decomposition of $\mathcal{C}_{167/\mathbb{F}_2}$ using Theorem 3.5.13. Since 167 is a prime number, we have that $\mathrm{Div}_{167} = \{1, 167\}$. Observe that:

$$\begin{aligned} \nu_{167/\mathbb{F}_2}(1) &= \operatorname{ord}_1(2) = 1 \\ \eta_{167/\mathbb{F}_2}(1) &= \frac{\varphi(1)}{\nu_{167/\mathbb{F}_2}(1)} = 1 \\ \nu_{167/\mathbb{F}_2}(167) &= \operatorname{ord}_{167}(2) = 83 \\ \eta_{167/\mathbb{F}_2}(167) &= \frac{\varphi(167)}{\nu_{167/\mathbb{F}_2}(167)} = \frac{166}{83} = 2. \end{aligned}$$

Hence from Theorem 3.5.13, the semisimple decomposition of $\mathcal{C}_{167/\mathbb{F}_2}$ equals:

$$\mathcal{C}_{167/\mathbb{F}_2} \cong \mathbb{F}_2 \oplus (\mathbb{F}_{2^{83}})^2.$$

As a result, $\mathcal{C}^*_{167/\mathbb{F}_2} \cong \mathbb{F}_2^* \oplus (\mathbb{F}^*_{2^{83}})^2 \cong (\mathbb{F}^*_{2^{83}})^2$, hence $\operatorname{ord}(f)$ must be a divisor of $\#\mathbb{F}^*_{2^{83}} = 2^{83} - 1$. Observe that $2^{83} - 1$ is a Mersenne prime, which implies that $\operatorname{ord}(f) = 2^{83} - 1$ for $f \neq 1$. □

Observe that for any commutative ring R and any matrix $A \in \mathrm{GL}_n(R)$, we have that $\operatorname{ord}(\det(A)) \mid \operatorname{ord}(A)$ due to det preserving multiplication. As such, $\operatorname{ord}(\det(\rho_l'' \circ \theta'' \circ \rho_r'')) \mid \operatorname{ord}(\rho_l'' \circ \theta'' \circ \rho_r'')$. Since $\det(\rho_l'' \circ \theta'' \circ \rho_r'')$ is not equal to 1, Proposition 4.3.2 implies that $\operatorname{ord}(\det(\rho_l'' \circ \theta'' \circ \rho_r'')) = 2^{83} - 1$. This implies that $2^{83} - 1$ indeed divides the order of $\rho_l'' \circ \theta'' \circ \rho_r''$.

Step 2: Determining λ We illustrate a sketch on how we obtained λ, which requires a bit of mathematical reasoning.

In the proof of Proposition 4.3.2, we showed that $\mathcal{C}_{167/\mathbb{F}_2} \cong \mathbb{F}_2 \oplus (\mathbb{F}_{2^{83}})^2$. From this, we conclude that we have the isomorphism:

$$\mathrm{GL}_3(\mathcal{C}_{167/\mathbb{F}_2}) \cong \mathrm{GL}_3(\mathbb{F}_2) \oplus \mathrm{GL}_3(\mathbb{F}_{2^{83}}) \oplus \mathrm{GL}_3(\mathbb{F}_{2^{83}}).$$

As such, the order of every element in $\mathrm{GL}_3(\mathcal{C}_{167/\mathbb{F}_2})$ must divide:

$$\#\,\mathrm{GL}_3(\mathbb{F}_{2^{83}}) = \left(2^{3\cdot 83} - 1\right)\cdot\left(2^{3\cdot 83} - 2^{83}\right)\cdot\left(2^{3\cdot 83} - 2^{2\cdot 83}\right),$$

hence λ must be a divisor of $\left(2^{3\cdot 83}-1\right)\cdot\left(2^{3\cdot 83}-2^{83}\right)\cdot\left(2^{3\cdot 83}-2^{2\cdot 83}\right)$.

Using Sagemath, we verified that $\lambda \mid \left(2^{3\cdot 83}-1\right)\cdot\left(2^{3\cdot 83}-2^{83}\right)$. Note that:

$$\begin{aligned}
&\left(2^{3\cdot 83}-1\right)\cdot\left(2^{3\cdot 83}-2^{83}\right)\\
&=\left(2^{83}-1\right)\cdot\left(2^{2\cdot 83}+2^{83}+1\right)\cdot 2^{83}\cdot\left(2^{2\cdot 83}-1\right)\\
&=\left(2^{83}-1\right)\cdot\left(2^{2\cdot 83}+2^{83}+1\right)\cdot 2^{83}\cdot(2^{83}+1)\cdot\left(2^{83}-1\right)\\
&=\left(2^{83}-1\right)^2\cdot 2^{83}\cdot\left(\left(2^{2\cdot 83}+2^{83}+1\right)\cdot\left(2^{83}+1\right)\right).
\end{aligned}$$

Again using Sagemath, we verified that $\lambda \mid \left(2^{2\cdot 83}+2^{83}+1\right)\cdot\left(2^{83}+1\right)$. By exhaustive search over the divisors of $\left(2^{2\cdot 83}+2^{83}+1\right)\cdot\left(2^{83}+1\right)$, we managed to find λ. The details of the code used to compute λ can be found on the next page.

```
#Setting up the ring R_167
R.<s> = GF(2)[]
S.<x> = R.quo([s^167 - 1])

#Defining \rho_l, \rho_r and \theta for the composition DCD
f = x^6 + x^15

theta = matrix([[1+f,f,f],[f,1+f,f],[f,f,1+f]])
p_l = matrix([[1,0,0],[0,x,0],[0,0,x^11]])
p_r = matrix([[1,0,0],[0,x,0],[0,0,x^10]])
DCD = p_l*theta*p_r

#Checking/verifying invertibility of DCD
DCD^-1

#Lifting DCD to the order of \det(DCD) = 2^83 - 1, which we call DCD1
ord_det_LN = 2^83 - 1
DCD1 = DCD^ord_det_LN

#Checking/verifying if the order of DCD1 divides a = (2^(2*83) + 2^83
    + 1)*(2^(83) + 1) by verifying if DCD1^a is the identity matrix
a = (2^(2*83) + 2^83 + 1)*(2^(83) + 1)
DCD1^a

#Naively computing \lambda (the order of DCD1) using brute force
#\lambda must be a divisor of $a$
i = 0
while DCD1^(divisors(a)[i]) != matrix.identity(3):
    i = i + 1

print(divisors(a)[i])
```

Chapter 5

Column parity mixers

5.1 Introduction

Column parity mixers [SD18], or CPMs for short, are a particular type of linear maps which are a generalization of the θ mixing layers in the cryptographic permutations Xoodoo [DHVV18] and Keccak-f [BDPV15]. They provide a good trade-off between implementation cost and mixing power, making them well-suited for lightweight cryptography.

A formal approach in studying CPMs as a stand-alone topic is done in [SD18], where CPMs were formulated as linear maps between spaces of matrices. Each CPM θ, viewed as an endomorphism of the ring of $m \times d$-matrices, is uniquely determined by a $d \times d$-matrix called the parity folding matrix of θ. There has been some emphasis on studying CPMs where its parity folding matrix belongs to the class of circulant matrices. These are called circulant column parity mixers, which we abbreviate by CCPMs. We cover the structure of these CCPMs in greater detail in Section 5.2. Due to the symmetric properties of circulant matrices, CCPMs have a good worst-case behaviour for the purpose of mixing bits. The θ mixing layers of Xoodoo and Keccak-f are examples of CCPMs.

In this section, we introduce a new approach to studying CCPMs by viewing them as module endomorphisms over circulant modules. We show that many interesting algebraic properties can be deduced using this approach, and that known results regarding CCPMs resurface as trivial consequences of module-theoretic concepts.

The results in this chapter are based on the second part of the paper [Sub24a]. As was the case in the previous section, we present a more comprehensive discussion of the topic compared to what is presented in the paper, with more focus on mathematical proof.

5.2 Original approach to circulant column parity mixers

In this section, we present the original definition of circulant CPMs as explained in [SD18]. As such, this section is copied from the first part of Section 2 of that paper, with slight modifications to align with this thesis.

5.2.1 Matrices

We use $\mathbf{I}$ to denote a (square) identity matrix and $\mathbf{0}$ to denote an all-zero matrix. We assume that the dimensions of these matrices are determined by the context. The transpose of a matrix A is denoted as A^{T}.

We use $\mathbf{1}_x$ to denote a column vector of x components that are all equal to 1. Consequently, $\mathbf{1}_x^{\mathsf{T}}$ is an all-1 row vector with x components. We use $\mathbf{1}_x^y$ to denote a matrix with x rows and y columns with all components 1. It is clear that $\mathbf{1}_x^y = \mathbf{1}_x \mathbf{1}_y^{\mathsf{T}}$.

The element of a matrix A at row i and column j is denoted by $A_{i,j}$. If $B = A^{\mathsf{T}}$, we have $B_{i,j} = A_{j,i}$. The trace of a square matrix is the linear function that simply takes the sum of its diagonal elements. It is denoted by $\operatorname{tr}(A)$, so $\operatorname{tr}(A) = \sum_i A_{i,i}$.

5.2.2 Definition of column parity mixers

We consider linear mappings θ that operate on arrays with d rows and m columns.

Definition 5.2.1. The *column parity* of a matrix A is a (row) vector defined as $\mathbf{1}_d^{\mathsf{T}} A$.

In a matrix A, a column x is called even (odd) if the component with index x in $\mathbf{1}_d^{\mathsf{T}} A$ is zero (one).

Definition 5.2.2. The *expanded column parity* of A is a matrix with d rows all equal to the column parity of A, and it is given by $\mathbf{1}_d^d A$.

A column parity mixer (CPM) makes use of a linear transformation operating on the column parity of a matrix, called its *parity-folding transformation.*

We denote the parity-folding transformation by multiplying the column parity with a square matrix Z at the right. We call the $m \times m$ matrix Z the *parity-folding matrix* of θ. We are now ready to define the θ-effect of a matrix A.

Definition 5.2.3. The *θ-effect* of A with respect to Z is a row vector, denoted as $\mathbf{e_Z}(A)$ (or just $\mathbf{e}(A)$ if Z is clear from the context) and is defined by $\mathbf{e_Z}(A) = \mathbf{1}_d^{\mathsf{T}} AZ$.

For a given input A and parity-folding matrix Z, a column x is called *unaffected* (affected) if the component with index x in $\mathbf{e_Z}(A)$ is zero (nonzero). Whether a column is affected or not is fully determined by the column parity of A and the column x of the parity-folding matrix Z.

Definition 5.2.4. The *expanded θ effect* of A with respect to Z is a matrix with d rows all equal to the CPM effect, namely, $\mathbf{E_Z}(A) = \mathbf{1}_d^d AZ$.

A column parity mixer θ simply consists in computing the expanded θ-effect of a matrix A and adding it to A.

Definition 5.2.5. The *column parity mixer θ* using parity-folding matrix Z is defined as:

$$\theta(A) = A + \mathbf{E_Z}(A) = A + \mathbf{1}_d^d AZ\,.$$

This becomes a *circulant column parity mixer* when Z is a circulant matrix.

Note that a column parity mixer is fully defined by a parity-folding matrix Z and d.

Example 5.2.6. *Keccak [BDPV15] uses a three-dimensional structure, so, for the sake of this example, let us first 'flatten' the state by looking at a single sheet. With Keccak-f[200], this array would have $d = 5$ rows and $m = 8$ columns. Consider the following state A:*

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Then the column parity *of A is* $[1,1,0,0,0,1,0,0]$, *so the first two columns and the sixth column are* odd, *while the rest is* even. *The θ step in Keccak-f affects the adjacent sheets, but one can modify it slightly such that the operation* *is performed within the same sheet. To the reader who is familiar with the* Keccak *specification, we change $x - 1 \bmod 5$ and $x + 1 \bmod 5$ to $x \bmod 5$ in the computation of $D[x, z]$ given $C[x, z]$. This means that we can express the* parity-folding matrix *Z as follows:*

$$Z = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

*This yields a θ-*effect *of $\mathbf{e}(A) = [0, 1, 0, 0, 1, 1, 0, 1]$, so the second, fifth, sixth, and eighth column are* affected*, the rest is* unaffected*. The result of the* column parity mixer *defined by Z and m on A is then:*

$$\theta(A) = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

5.3 Useful matrix identities

We show some matrix identities which are useful for studying the new approach of column parity mixers presented in the next section. We assume that R is a commutative unital ring.

Definition 5.3.1. Let $\vec{a} = (a_0, \dots, a_{d-1}) \in R^d$ be an d-tuple viewed as a column vector. We define the **column matrix** of $\vec{a}$ as the $d \times d$-matrix:

$$\operatorname{col}(\vec{a}) = \begin{pmatrix} a_0 & a_0 & \cdots & a_0 \\ a_1 & a_1 & \cdots & a_1 \\ \vdots & \vdots & \vdots & \vdots \\ a_{d-1} & a_{d-1} & \cdots & a_{d-1} \end{pmatrix} \in \mathrm{Mat}_d(R).$$

Lemma 5.3.2. *Consider the column vector $\vec{b} = (b_0, \dots, b_{d-1}) \in R^d$, then:*

$$\operatorname{col}(\vec{a}) \cdot \vec{b} = \left(\sum_{i=0}^{d-1} b_i \right) \cdot \vec{a}.$$

Proof. Apply the standard matrix multiplication rules. □

Corollary 5.3.3. *Let $\vec{a}, \vec{b} \in R^d$, then:*

$$\mathrm{col}(\vec{a}) \cdot \mathrm{col}(\vec{b}) = \left(\sum_{i=0}^{d-1} b_i\right) \cdot \mathrm{col}(\vec{a}).$$

Proposition 5.3.4. *Let $\vec{a} \in R^d$. Then for any $t \in \mathbb{Z}_{>0}$, we have that:*

$$\mathrm{col}(\vec{a})^t = \left(\sum_{i=0}^{d-1} a_i\right)^{t-1} \cdot \mathrm{col}(\vec{a}).$$

Proof. We use induction on t. Let $t = 1$, then:

$$\left(\sum_{i=0}^{d-1} a_i\right)^{t-1} \cdot \mathrm{col}(\vec{a}) = \left(\sum_{i=0}^{d-1} a_i\right)^{0} \cdot \mathrm{col}(\vec{a}) = 1 \cdot \mathrm{col}(\vec{a}) = \mathrm{col}(\vec{a})^1,$$

which concludes the first induction step.

Now assume that our claim is true for $t = k$ for some $k > 1$. For $t = k + 1$, we get:

$$\begin{aligned}
\mathrm{col}(\vec{a})^{k+1} &= \mathrm{col}(\vec{a})^k \cdot \mathrm{col}(\vec{a}) \\
&= \left(\sum_{i=0}^{d-1} a_i\right)^{k-1} \cdot \mathrm{col}(\vec{a})^2 \\
&= \left(\sum_{i=0}^{d-1} a_i\right)^{k-1} \cdot \left(\sum_{i=0}^{d-1} a_i\right) \cdot \mathrm{col}(\vec{a}) \\
&= \left(\sum_{i=0}^{d-1} a_i\right)^{k} \cdot \mathrm{col}(\vec{a}).
\end{aligned}$$

□

5.4 A new approach to circulant column parity mixers

We briefly discuss how circulant column parity mixers described in Section 5.2 can be viewed as module endomorphisms over circulant modules.

Original approach reformulated

The following steps summarize how a circulant column parity mixer as described in Section 5.2 is constructed using a slightly different notation:

1. For an element $\vec{v} := (v_0, \ldots, v_{d-1}) \in (\mathbb{F}_2^m)^d$, compute $v_\Sigma := \sum_{i=0}^{d-1} v_i \in \mathbb{F}_2^m$;
2. Given a circulant matrix $Z \in C_{m/\mathbb{F}_2}$, compute $v_Z := Z \cdot v_\Sigma \in \mathbb{F}_2^m$;
3. The circulant column parity mixer θ_Z using Z is defined as:
$$\theta_Z \colon (\mathbb{F}_2^m)^d \to (\mathbb{F}_2^m)^d,\ v \mapsto v + \vec{v}_Z,$$
where $\vec{v}_Z := (v_Z, \ldots, v_Z) \in (\mathbb{F}_2^m)^d$.

The matrix Z is the parity-folding matrix of θ_Z.

Transition into a module-theoretic setting

Consider the transformation $\vartheta_{m/\mathbb{F}_2} \colon \mathbb{F}_2^m \to \mathcal{C}_{m/\mathbb{F}_2}$ as in Eq. (4.1), which induces the transformation $\vartheta_{m/\mathbb{F}_2}^d \colon (\mathbb{F}_2^m)^d \to (\mathcal{C}_{m/\mathbb{F}_2})^d$. We investigate how the circulant column parity mixer $\theta \colon (\mathbb{F}_2^m)^d \to (\mathbb{F}_2^m)^d$ translates under $\vartheta_{m/\mathbb{F}_2}^d$ as a map from $(\mathcal{C}_{m/\mathbb{F}_2})^d$ to itself.

Let $z := \varpi(Z) \in \mathcal{C}_{m/\mathbb{F}_2}$, where ϖ is defined in Theorem 4.2.4. Consider the $d \times d$-matrix:

$$\theta_{\vec{z}} = \begin{pmatrix} 1+z & z & z & \cdots & z \\ z & 1+z & z & \cdots & z \\ z & z & 1+z & \cdots & z \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z & z & z & \cdots & 1+z \end{pmatrix} \in \mathrm{Mat}_d(\mathcal{C}_{m/\mathbb{F}_2}),$$

which induces a $\mathcal{C}_{m/k}$-module endomorphism over $(\mathcal{C}_{m/k})^d$.

Proposition 5.4.1. *We have the identity* $\vartheta_{m/\mathbb{F}_2}^d \circ \theta_Z = \theta_{\vec{z}} \circ \vartheta_{m/\mathbb{F}_2}^d$.

Proof. Let $\vec{v} := (v_0, \ldots, v_{d-1}) \in (\mathbb{F}_2^m)^d$, and v_Σ, v_Z and $\vec{v}_Z$ as defined earlier. Additionally, define the vector $\vec{v}_\Sigma := (v_\Sigma, \ldots, v_\Sigma) \in (\mathbb{F}_2^m)^d$. Observe that:

$$v_Z = Z \cdot v_\Sigma = \mu_{m/\mathbb{F}_2}(\varpi(Z), v_\Sigma) = \mu_{m/\mathbb{F}_2}(z, v_\Sigma),$$

which implies:

$$\vartheta_{m/\mathbb{F}_2}(v_Z) = \vartheta_{m/\mathbb{F}_2}(\mu_{m/\mathbb{F}_2}(z, v_\Sigma)) = z \cdot \vartheta_{m/\mathbb{F}_2}(v_\Sigma).$$

As such, we have the identity:

$$\begin{aligned}\vartheta^d_{m/\mathbb{F}_2} \circ \theta_Z(\vec{v}) &= \vartheta^d_{m/\mathbb{F}_2}(\vec{v} + \vec{v}_Z) = \vartheta^d_{m/\mathbb{F}_2}(\vec{v}) + \vartheta^d_{m/\mathbb{F}_2}(\vec{v}_Z)\\ &= \vartheta^d_{m/\mathbb{F}_2}(\vec{v}) + z \cdot \vartheta^d_{m/\mathbb{F}_2}(\vec{v}_\Sigma).\end{aligned}$$

For $\vec{w} := (w_0, \ldots, w_{d-1}) \in (\mathcal{C}_{m/k})^d$, define $w_\Sigma := \sum_{i=0}^{d-1} w_i \in \mathcal{C}_{m/k}$ and the vector $\vec{w}_\Sigma := (w_\Sigma, \ldots, w_\Sigma) \in (\mathcal{C}_{m/k})^d$. By the standard matrix multiplication rules, we have the identity:

$$\theta_{\vec{z}} \cdot \vec{w} = \vec{w} + z \cdot \vec{w}_\Sigma. \tag{5.1}$$

In the case that $\vec{w} = \vartheta^d_{m/\mathbb{F}_2}(\vec{v})$, we have that $w_\Sigma = \vartheta_{m/\mathbb{F}_2}(v_\Sigma)$ since $\vartheta_{m/\mathbb{F}_2}$ preserves addition. This implies that $\vec{w}_\Sigma = \vartheta^d_{m/\mathbb{F}_2}(\vec{v}_\Sigma)$. Substituting this in Eq. (5.1), we obtain the identity:

$$\theta_{\vec{z}} \circ \vartheta^d_{m/\mathbb{F}_2}(\vec{v}) = \vartheta^d_{m/\mathbb{F}_2}(\vec{v}) + z \cdot \vartheta^d_{m/\mathbb{F}_2}(\vec{v}_\Sigma),$$

which is exactly the same expression as $\vartheta^d_{m/\mathbb{F}_2} \circ \theta_Z(\vec{v})$. □

Proposition 5.4.1 implies in particular that θ_Z is a $\mathcal{C}_{m/\mathbb{F}_2}$-endomorphism where $(\mathbb{F}_2^m)^d$ is viewed as a circulant module of rank d.

A new definition

Using the insights of Proposition 5.4.1, we can redefine and generalize circulant column parity mixers as follows:

Definition 5.4.2 (Column parity mixers). Let R be a commutative unital ring, and let $\vec{z} := (z_0, \ldots, z_{d-1})$ be a d-tuple with entries in R. The **column parity mixer** (CPM) parametrized by $\vec{z}$, denoted by $\theta_{\vec{z}}$, is an R-endomorphism over R^d represented by the $d \times d$-matrix:

$$\theta_{\vec{z}} = \begin{pmatrix} 1+z_0 & z_0 & z_0 & \cdots & z_0 \\ z_1 & 1+z_1 & z_1 & \cdots & z_1 \\ z_2 & z_2 & 1+z_2 & \cdots & z_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{d-1} & z_{d-1} & z_{d-1} & \cdots & 1+z_{d-1} \end{pmatrix}.$$

The set of all CPMs of dimension d over R is denoted by $\mathrm{CPM}_d(R)$.

A CPM over a circulant ring is called a **circulant column parity mixer**, or CCPM for short.

Remark 5.4.3. When $R = \mathcal{C}_{m/\mathbb{F}_2}$ and $\vec{z} := (z, \ldots, z) \in (\mathcal{C}_{m/\mathbb{F}_2})^d$, we have that $\theta_{\vec{z}}$ in Definition 5.4.2 coincides with $\theta_{\vec{z}}$ in Proposition 5.4.1. As such, Definition 5.4.2 is indeed a generalization of the original approach to circulant column parity mixers.

5.5 Characteristic polynomial and determinant

We give an expression of the characteristic polynomial and the determinant of an d-dimensional CPM $\theta_{\vec{z}}$ in terms of its parameters $\vec{z}$.

Theorem 5.5.1. *The characteristic polynomial $p_{\theta_{\vec{z}}}(\lambda)$ of $\theta_{\vec{z}}$ is:*

$$p_{\theta_{\vec{z}}}(\lambda) = \left(\left(1 + \sum_{i=0}^{d-1} z_i\right) - \lambda\right) \cdot (1-\lambda)^{d-1}. \tag{5.2}$$

Proof. By definition, $p_{\theta_{\vec{z}}}(\lambda) := \det(\theta_{\vec{z}} - \lambda \cdot I_d)$. To compute the determinant of $\theta_{\vec{z}} - \lambda \cdot I_d$, we use the property that adding up rows (or columns) to **other** rows (or columns) will not affect the determinant. By adding the first column vector to all the other column vectors of $\theta_{\vec{z}}$, followed by adding up all the row vectors from the second till the last row vector to the first row vector, we get:

$$\det(\theta_{\vec{z}} - \lambda \cdot I_d) = \begin{vmatrix} 1+z_0-\lambda & z_0 & z_0 & \cdots & z_0 \\ z_1 & 1+z_1-\lambda & z_1 & \cdots & z_1 \\ z_2 & z_2 & 1+z_2-\lambda & \cdots & z_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{d-1} & z_{d-1} & z_{d-1} & \cdots & 1+z_{d-1}-\lambda \end{vmatrix}$$

$$= \begin{vmatrix} 1+z_0-\lambda & \lambda-1 & \lambda-1 & \cdots & \lambda-1 \\ z_1 & 1-\lambda & 0 & \cdots & 0 \\ z_2 & 0 & 1-\lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{d-1} & 0 & 0 & \cdots & 1-\lambda \end{vmatrix}$$

$$= \begin{vmatrix} 1+\left(\sum_{i=0}^{d-1} z_i\right)-\lambda & 0 & 0 & \cdots & 0 \\ z_1 & 1-\lambda & 0 & \cdots & 0 \\ z_2 & 0 & 1-\lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{d-1} & 0 & 0 & \cdots & 1-\lambda \end{vmatrix}. \tag{5.3}$$

Let us denote the matrix in Eq. (5.3) by A, and write $A_{[i,j]}$ as the $(d-1) \times$

$(d-1)$-matrix by removing the i-th row and the j-th column of A. Then:

$$\begin{aligned}\det(\theta_{\bar{z}} - \lambda \cdot I_d) &= \det(A)\\ &= \sum_{j=0}^{d-1} (-1)^j \cdot A_{0,j} \cdot \det(A_{[0,j]})\\ &= A_{0,0} \cdot \det(A_{[0,0]}) + \sum_{j=1}^{d-1} (-1)^j \cdot A_{0,j} \cdot \det(A_{[0,j]})\\ &= A_{0,0} \cdot \det(A_{[0,0]}), \qquad (5.4)\end{aligned}$$

where the last equation holds because $A_{0,j} = 0$ for $j > 0$. Observe that $A_{0,0} = \left(1 + \sum_{i=0}^{d-1} z_i\right) - \lambda$ and $A_{[0,0]} = (1-\lambda) \cdot I_{d-1}$, the latter implying that $\det(A_{[0,0]}) = (1-\lambda)^{d-1}$. Substituting these values in (5.4), we obtain:

$$\det(\theta_{\bar{z}} - \lambda \cdot I_d) = A_{0,0} \cdot \det(A_{[0.0]}) = \left(\left(1 + \sum_{i=0}^{d-1} z_i\right) - \lambda\right) \cdot (1-\lambda)^{d-1},$$

which concludes the proof. □

Corollary 5.5.2. *The determinant of $\theta_{\bar{z}}$ equals:*

$$\det(\theta_{\bar{z}}) = 1 + \sum_{i=0}^{d-1} z_i.$$

Proof. The determinant equals the constant term of the characteristic polynomial of $\theta_{\bar{z}}$, which from Eq. (5.2) equals $1 + \sum_{i=0}^{d-1} z_i$. □

Remark 5.5.3. By the above corollary, $p_{\theta_{\bar{z}}}(\lambda)$ can be expressed as:

$$p_{\theta_{\bar{z}}}(\lambda) = (\det(\theta_{\bar{z}}) - \lambda) \cdot (1-\lambda)^{d-1}. \qquad (5.5)$$

We will use this expression for the remainder of this paper.

5.6 Eigenvectors and eigenspaces of column parity mixers

In this section, we present some results regarding the eigenvectors and eigenspaces of d-dimensional CCPMs. The first subsection provides the necessary mathematical prerequisites which are required to study these eigenvectors. Afterwards, we present the main results.

5.6.1 Induced homomorphisms and eigenvectors

Let R and S be commutative unital rings, and let $\varphi: R \to S$ be a ring homomorphism. In particular, φ induces on S a natural R-module structure where we define $r \cdot s := \varphi(r) \cdot s$ for all $r \in R$ and $s \in S$. Using this R-module structure on S, the map φ is an R-linear map. This naturally extends to an R-linear map of free modules of rank d, which we denote by φ^d:

$$\varphi^d: R^d \to S^d,\ (r_0, \dots, r_{d-1}) \mapsto (\varphi(r_0), \dots, \varphi(r_{d-1})).$$

Observe that φ^d also induces the (ring)-homomorphism of matrices:

$$\overline{\varphi^d}: \mathrm{Mat}_d(R) \to \mathrm{Mat}_d(S),\ A = (A_{ij})_{0 \le i,j \le d-1} \mapsto \varphi(A) := (\varphi(A_{ij}))_{0 \le i,j \le d-1}. \tag{5.6}$$

The homomorphism of matrices can be interpreted in terms of endomorphisms, meaning that $\overline{\varphi}$ naturally induces a map:

$$\overline{\varphi^d}: \mathrm{End}_R(R^d) \to \mathrm{End}_S(S^d),\ \theta \mapsto \overline{\varphi^d}(\theta),$$

satisfying the commutative diagram:

$$\begin{tikzcd}
R^d \arrow[r, "\theta"] \arrow[d, "\varphi^d"] & R^d \arrow[d, "\varphi^d"] \\
S^d \arrow[r, "\overline{\varphi^d}(\theta)"] & S^d
\end{tikzcd}.$$

For $\theta \in \mathrm{End}_R(R^d)$, we denote $\overline{\varphi^d}(\theta)$ the **induced S-endomorphism** induced by φ. Induced endomorphisms behave well with respect to eigenvectors.

Lemma 5.6.1. *Let $\vec{v} \in R^d$ be an eigenvector of $\theta \in \mathrm{End}_R(R^d)$ with eigenvalue λ. Then $\varphi^d(\vec{v})$ is an eigenvector of $\overline{\varphi^d}(\theta) \in \mathrm{End}_S(S^d)$ with eigenvalue $\varphi^d(\lambda)$.*

Proof. By commutativity of the above diagram, we get:

$$\overline{\varphi}(\theta)(\varphi(\vec{v})) = \varphi(\theta(\vec{v})) = \varphi(\lambda \cdot \vec{v}) = \varphi(\lambda) \cdot \varphi(\vec{v}),$$

which concludes the proof. □

If θ admits an eigenbasis in R^d, it is not always the case that $\varphi(\theta)$ also admits an eigenbasis in S^d. For our situation, we only need to consider two types of induced homomorphisms which do preserve the eigenbases.

Type I: Quotient map of local rings

Definition 5.6.2. For R a local ring with maximal ideal $\mathfrak{m}$ and the quotient map $\mathfrak{q}\colon R \to R/\mathfrak{m} \cong k$, we have the isomorphism $V/\mathfrak{m}V \cong k^d$, where $V := R^d$. For $\theta \in \operatorname{End}_R(V)$, we denote the **induced k-endomorphism** by $\mathfrak{q}^d(\theta) \in \operatorname{End}_k(V/\mathfrak{m}V)$.

The induced endomorphism $\mathfrak{q}^d(\theta)$ satisfies the following commutative diagram:

$$\begin{tikzcd}
R^d \arrow[r, "\theta"] \arrow[d, "\mathfrak{q}^d"] & R^d \arrow[d, "\mathfrak{q}^d"] \\
k^d \arrow[r, "\mathfrak{q}^d(\theta)"] & k^d
\end{tikzcd} .$$

Proposition 5.6.3. *Let R be a local ring with quotient field k, and assume that $\theta \in \operatorname{Mat}_d(R)$ has an eigenbasis over R. Then $\mathfrak{q}^d(\theta)$ has an eigenbasis over k in $V/\mathfrak{m}V$.*

The proof of Proposition 5.6.3 relies on the next two lemmas:

Lemma 5.6.4 (**Nakayama's Lemma over local rings**)**.** *Let R be a local ring, and let V be a finitely generated R-module. Then any set of generators of V over R naturally induces a generating set of the k-vector space $V/\mathfrak{m}V$. Conversely, any set of generators of V over R is induced by a unique basis of $V/\mathfrak{m}V$.*

Proof. This is a direct consequence of applying local rings to Nakayama's Lemma (Lemma 2.3.4). □

Lemma 5.6.5. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field k, let $V := R^d$ and let $\vec{v} \in V \setminus \mathfrak{m}V$ be an eigenvector of $\theta \in \operatorname{Mat}_d(R)$. Then $\mathfrak{q}^d(\vec{v})$ is a non-zero eigenvector of $\overline{\theta}$ with eigenvalue $\mathfrak{q}(\lambda) \in k$.*

Proof. Since $\vec{v} \notin \mathfrak{m}V$, we have that $\mathfrak{q}(\vec{v})$ is non-zero in $V/\mathfrak{m}V$. The rest is an immediate consequence of Lemma 5.6.1. □

Proof of Proposition 5.6.3. This is a direct consequence of Lemmas 5.6.4 and 5.6.5. □

Type II: Localization map

Definition 5.6.6. Let R be any commutative ring and let $V := R^d$. For $\mathfrak{p} \in \operatorname{Spec}(R)$, we define the localized free $R_\mathfrak{p}$-module $R_\mathfrak{p}^d$ by $V_\mathfrak{p}$, where the ring homomorphism $l_\mathfrak{p}\colon R \to R_\mathfrak{p}$ induces the R-linear map $l_\mathfrak{p}^d\colon V \to V_\mathfrak{p}$. For $\theta \in \operatorname{End}_R(V)$, we denote the **induced $R_\mathfrak{p}$-endomorphism** by $\theta_\mathfrak{p} \in \operatorname{End}_{R_\mathfrak{p}}(V_\mathfrak{p})$.

The induced endomorphism $\theta_\mathfrak{p}$ satisfies the following commutative diagram:

$$\begin{tikzcd}
R^d \arrow[r, "\theta"] \arrow[d, "l_\mathfrak{p}^d"] & R^d \arrow[d, "l_\mathfrak{p}^d"] \\
R_\mathfrak{p}^d \arrow[r, "\theta_\mathfrak{p}"] & R_\mathfrak{p}^d
\end{tikzcd}.$$

Proposition 5.6.7. *Assume that $\theta \in \operatorname{Mat}_d(R)$ has an eigenbasis, then $\theta_\mathfrak{p}$ has an eigenbasis.*

We require the following lemma to prove Proposition 5.6.7:

Lemma 5.6.8. *Let $\mathfrak{p} \in \operatorname{Spec}(R)$, and let $B_V := \{v_0, \ldots, v_{d-1}\} \subset V$ a basis of V, then $B_{V_\mathfrak{p}} := \left\{\frac{v_0}{1}, \ldots, \frac{v_{d-1}}{1}\right\}$ is a basis of $V_\mathfrak{p}$.*

Proof. Let $\vec{v}_\mathfrak{p} = \left(\frac{a_0}{b_0}, \ldots, \frac{a_{d-1}}{b_{d-1}}\right) \in V_\mathfrak{p}$. Define $\hat{b} := \prod_{i=0}^{d-1} b_i$ and $\hat{b}_j := \prod_{0 \le i \le d-1, i \ne j} b_i$, which are elements in $R \setminus \mathfrak{p}$ since this set is closed under multiplication. Observe that:

$$\hat{b} \cdot \vec{v}_\mathfrak{p} = \left(\frac{\hat{b}_0 \cdot a_0}{1}, \ldots, \frac{\hat{b}_{d-1} \cdot a_{d-1}}{1}\right),$$

which is contained in the image of $l_\mathfrak{p}^d$. Hence there exist $r_0, \ldots, r_{d-1} \in R$ such that $\hat{b} \cdot \vec{v}_\mathfrak{p} = \sum_{i=0}^{d-1} r_i \cdot \left(\frac{v_i}{1}\right)$, which implies that:

$$\vec{v}_\mathfrak{p} := \sum_{i=0}^{d-1} \frac{r_i}{\hat{b}} \cdot \left(\frac{v_i}{1}\right).$$

Hence $B_{V_\mathfrak{p}}$ is a generating set of $V_\mathfrak{p}$. Since $B_{V_\mathfrak{p}}$ has d elements, and $V_\mathfrak{p}$ has dimension d as a free $R_\mathfrak{p}$-module, we conclude that $B_{V_\mathfrak{p}}$ is a basis of $V_\mathfrak{p}$. □

Proof of Proposition 5.6.7. By Lemma 5.6.1, if $\vec{v} \in V$ is an eigenvector of $\theta \in \operatorname{End}_R(V)$ with eigenvalue λ, then $l_\mathfrak{p}^d(\vec{v})$ is an eigenvector of $\theta_\mathfrak{p}$ with eigenvalue $l_\mathfrak{p}(\lambda) = \frac{\lambda}{1}$. The claim follows directly from Lemma 5.6.8. □

5.6.2 Eigenvectors and eigenspaces

We use the results in the above subsection to study the eigenvectors and eigenspaces of a d-dimensional column parity mixer $\theta_{\vec{z}} \in \mathrm{CPM}_d(R)$.

Definition 5.6.9. For $\theta_{\vec{z}} \in \mathrm{CPM}_d(R)$, we consider the following submodules of R^d:

$$\begin{aligned} E_1 &:= \left\{ \vec{v} = (v_0, \ldots, v_{d-1}) \in R^d : \sum_{i=0}^{d-1} v_i = 0 \right\}, \\ E_2 &:= \{ r \cdot \vec{z} : r \in R \} \subseteq R^d. \end{aligned}$$

Lemma 5.6.10. *For any $\theta_{\vec{z}} \in \mathrm{CPM}_d(R)$, all elements in E_1 remain invariant under $\theta_{\vec{z}}$.*

Proof. Observe that for all $\vec{v} \in E_1$, we have:

$$\theta_{\vec{z}}(\vec{v}) = (I_d + \mathrm{col}(\vec{z})) \cdot \vec{v} = \vec{v} + \left(\sum_{i=0}^{d-1} v_i \right) \cdot \vec{z} = \vec{v} + 0 \cdot \vec{z} = \vec{v},$$

which proves the claim. □

Lemma 5.6.11. *For any $\theta_{\vec{z}} \in \mathrm{CPM}_d(R)$, the d-tuple $\vec{z}$ viewed as a vector in R^d is an eigenvector of $\theta_{\vec{z}}$ with eigenvalue* $\det(\theta_{\vec{z}})$.

Proof. Observe that:

$$\begin{aligned} \theta_{\vec{z}}(\vec{z}) &= (I_d + \mathrm{col}(\vec{z})) \cdot \vec{z} = \vec{z} + \mathrm{col}(\vec{z}) \cdot \vec{z} = \vec{z} + \left(\sum_{i=0}^{d-1} z_i \right) \cdot \vec{z} = \left(1 + \sum_{i=0}^{d-1} z_i \right) \cdot \vec{z} \\ &= \det(\theta_{\vec{z}}) \cdot \vec{z}, \end{aligned}$$

which finishes the proof. □

Lemma 5.6.12. *Assume that* $\det(\theta_{\vec{z}}) - 1$ *is invertible in R. Then E_2 is a free R-submodule of rank* 1, *and* $E_1 \cap E_2 = \{0\}$.

Proof. Observe that for all $r_1, r_2 \in R$ such that $(r_1 - r_2) \cdot \vec{z} = 0_d$, we have that $(r_1 - r_2) \cdot \left(\sum_{i=0}^{d-1} z_i \right) = 0$. Since $\sum_{i=0}^{d-1} z_i = \det(\theta_{\vec{z}}) - 1$ is invertible, it must be true that $r_1 - r_2 = 0$, hence $r_1 = r_2$. This shows that E_2 is a free R-submodule of rank 1.

Let $\vec{x} \in E_2$, then there exists $r_{\vec{x}} \in R$ such that $\vec{x} = r_{\vec{x}} \cdot \vec{z} \in E_2$. Note that:

$$\vec{x} = r_{\vec{x}} \cdot \vec{z} \in E_1 \Longleftrightarrow \sum_{i=0}^{d-1} r_{\vec{x}} \cdot z_i := r_{\vec{x}} \cdot \left(\sum_{i=0}^{d-1} z_i \right) := r_{\vec{x}} \cdot (\det(\theta_{\vec{z}}) - 1) = 0. \tag{5.7}$$

Since by our assumption $\det(\theta_{\vec{z}}) - 1$ is invertible in R, Equation (5.7) holds if and only if $r_{\vec{x}} = 0$, which implies that $\vec{x} \in E_1$ if and only if $\vec{x} = \vec{0}$. This implies that $E_1 \cap E_2 = \{\vec{0}\}$, which concludes the proof. □

Proposition 5.6.13. *Assume that* $\det(\theta_{\vec{z}}) - 1$ *is invertible in* R*. Then* R^d *is a direct sum of eigenspaces* E_1 *and* E_2 *of* $\theta_{\vec{z}}$ *with eigenvalues* 1 *and* $\det(\theta_{\vec{z}})$ *respectively.*

Proof. This is immediate from Lemmas 5.6.10, 5.6.11 and 5.6.12. □

Theorem 5.6.14. *Assume that* $\det(\theta_{\vec{z}}) - 1$ *is not invertible, then* $\theta_{\vec{z}}$ *does not have an eigenbasis.*

Proof. Since $\det(\theta_{\vec{z}}) - 1$ is not invertible in R, there exists a maximal ideal $\mathfrak{m}$ of R such that $\det(\theta_{\vec{z}}) - 1 \in \mathfrak{m}$. In particular, $\det(\theta_{\vec{z}}) \equiv 1 \bmod \mathfrak{m}$. We consider the local ring $R_{\mathfrak{m}}$, the localization of R at $\mathfrak{m}$, together with the quotient map and residue field $\mathfrak{q}\colon R_{\mathfrak{m}} \to R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}} := k_{\mathfrak{m}}$. We also denote $V := R^d$ and $V_{\mathfrak{m}} := R^d_{\mathfrak{m}}$.

Assume to the contrary that $\theta_{\vec{z}}$ has an eigenbasis. Then by Proposition 5.6.7, the induced $R_{\mathfrak{m}}$-endomorphism:

$$(\theta_{\vec{z}})_{\mathfrak{m}}\colon V_{\mathfrak{m}} \to V_{\mathfrak{m}},$$

also has an eigenbasis.

Consider the $k_{\mathfrak{m}}$-module $V_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})V_{\mathfrak{m}}$. Note that $V_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})V_{\mathfrak{m}}$ is a d-dimensional vector space over $k_{\mathfrak{m}}$, which implies that $V_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})V_{\mathfrak{m}} \cong k^d_{\mathfrak{m}}$. By Proposition 5.6.3, the vector space $k^d_{\mathfrak{m}}$ has an eigenbasis of the induced map $\mathfrak{q}^d((\theta_{\vec{z}})_{\mathfrak{m}})\colon k^d_{\mathfrak{m}} \to k^d_{\mathfrak{m}}$. Since $k_{\mathfrak{m}} := R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}} \cong R/\mathfrak{m}$, the corresponding matrix of $\mathfrak{q}^d((\theta_{\vec{z}})_{\mathfrak{m}})$ is the matrix of $\theta_{\vec{z}}$ where all entries are taken modulo $\mathfrak{m}$. For this reason, the characteristic polynomial of $\mathfrak{q}^d((\theta_{\vec{z}})_{\mathfrak{m}})$ is the polynomial:

$$p_{\mathfrak{q}^d((\theta_{\vec{z}})_{\mathfrak{m}})}(\lambda) = \left(\mathfrak{q}(\det(\theta_{\vec{z}})) - \lambda\right) \cdot (1 - \lambda)^{d-1}. \tag{5.8}$$

Since $\det(\theta_{\vec{z}}) \equiv 1 \bmod \mathfrak{m}$, we have that $\mathfrak{q}(\det(\theta_{\vec{z}})) = 1$ which implies that the only eigenvalue of $\mathfrak{q}^d((\theta_{\vec{z}})_{\mathfrak{m}})$ is 1. Let $\overline{E}_1$ be the eigenspace of $\mathfrak{q}^d((\theta_{\vec{z}})_{\mathfrak{m}})$ with eigenvalue 1. By standard linear algebra over fields, we get:

$$\overline{E}_1 := \ker\left(\mathfrak{q}^d((\theta_{\vec{z}})_{\mathfrak{m}}) - I_d\right) = \ker(I_d + \operatorname{col}(\mathfrak{q}^d(\vec{z})) - I_d) = \ker(\mathfrak{q}^d(\vec{z})).$$

Note that $\dim(\overline{E}_1) = d - 1$ since $\operatorname{col}(\mathfrak{q}^d(\vec{z}))$ has rank 1. But then:

$$\dim\left(\overline{E}_1\right) < \dim(V_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})V_{\mathfrak{m}}) = d,$$

which means that $\overline{E}_1$ is not an eigenbasis of $\mathfrak{q}^d((\theta_{\vec{z}})_{\mathfrak{m}})$. This contradicts our assumption, hence $\theta_{\vec{z}}$ does not have an eigenbasis. □

5.7 Invertible column parity mixers

We discuss some properties of CPMs that are invertible.

Lemma 5.7.1. *Let* $\theta_{\vec{z}}, \theta_{\vec{z}'} \in \mathrm{CPM}_d(R)$*, then:*

$$\theta_{\vec{z}} \cdot \theta_{\vec{z}'} = \theta_{\vec{z}'+\det(\theta_{\vec{z}'})\cdot\vec{z}} \in \mathrm{CPM}_d(R),$$

which in particular implies that $\mathrm{CPM}_d(R)$ *is closed under multiplication.*

Proof. This is due to the following:

$$\begin{aligned}\theta_{\vec{z}} \cdot \theta_{\vec{z}'} &= (I_d + \mathrm{col}(\vec{z})) \cdot (I_d + \mathrm{col}(\vec{z}')) \\ &= I_d + \mathrm{col}(\vec{z}) + \mathrm{col}(\vec{z}') + \mathrm{col}(\vec{z}) \cdot \mathrm{col}(\vec{z}') \\ &= I_d + \mathrm{col}(\vec{z}) + \mathrm{col}(\vec{z}') + \left(\sum_{i=0}^{d-1} z'_i\right) \cdot \mathrm{col}(\vec{z}) \\ &= I_d + \mathrm{col}\left(\vec{z}' + \left(1 + \sum_{i=0}^{d-1} z'_i\right) \cdot \vec{z}\right) \\ &= I_d + \mathrm{col}(\vec{z}' + \det(\theta_{\vec{z}'}) \cdot \vec{z}) \\ &= \theta_{\vec{z}'+\det(\theta_{\vec{z}'})\cdot\vec{z}},\end{aligned}$$

where the third equation is due to Corollary 5.3.3. □

Lemma 5.7.2. *Let* $\theta_{\vec{z}} \in \mathrm{CPM}_d(R)$ *be invertible, then:*

$$\theta_{\vec{z}}^{-1} = \theta_{-\vec{z}\cdot\det(\theta_{\vec{z}})^{-1}} \in \mathrm{CPM}_d(R).$$

Proof. Since $\theta_{\vec{z}}$ is invertible, we have that $\det(\theta_{\vec{z}})$ is invertible in R, hence $\det(\theta_{\vec{z}})^{-1}$ is well-defined. Then:

$$\theta_{\vec{z}'} \cdot \theta_{\vec{z}} = I_d \iff \vec{z} + \det(\theta_{\vec{z}}) \cdot \vec{z}' = 0 \iff \vec{z}' = -\vec{z} \cdot \det(\theta_{\vec{z}})^{-1},$$

which concludes the proof. □

We denote the set of invertible CPMs in $\mathrm{CPM}_d(R)$ by $\mathrm{CPM}^*_d(R)$. This set is non-empty, as for example the identity matrix is contained in $\mathrm{CPM}^*_d(R)$.

Proposition 5.7.3. *The set* $\mathrm{CPM}^*_d(R)$ *forms a subgroup of* $\mathrm{GL}_d(R)$*.*

Proof. By Lemma 5.7.1, $\mathrm{CPM}^*_d(R)$ is closed under multiplication. Moreover, the inverse of a CPM is also a CPM by Lemma 5.7.2. This implies that $\mathrm{CPM}^*_d(R)$ is indeed a subgroup of $\mathrm{GL}_d(R)$. □

Lemma 5.7.4. *Let R be a commutative unital ring of prime characteristic p, and let $\theta_{\vec{z}} \in \mathrm{CPM}_d^*(R)$ such that $\det(\theta_{\vec{z}}) = 1$ and $\theta_{\vec{z}} \neq I_d$. Then $\mathrm{ord}(\theta_{\vec{z}}) = p$.*

Proof. Observe that:

$$\theta_{\vec{z}}^p = (I_d + \mathrm{col}(\vec{z}))^p = I_d^p + \mathrm{col}(\vec{z})^p = I_d + \left(\sum_{i=0}^{d-1} z_i\right)^{p-1} \cdot \mathrm{col}(\vec{z}),$$

where the second equation is due to Newton's binomial theorem combined with the fact that all multiples of p vanish in rings of characteristic p, and where the third equation is due to the identity in Proposition 5.3.4. Since $\det(\theta_{\vec{z}}) = 1$, we have that $\sum_{i=0}^{d-1} z_i = 0$, which implies that $\theta_{\vec{z}}^p = I_d$. This means that $\mathrm{ord}(\theta_{\vec{z}}) \mid p$, which implies that $\mathrm{ord}(\theta_{\vec{z}})$ equals either 1 or p since p is prime. Because $\theta_{\vec{z}} \neq I_d$, we have $\mathrm{ord}(\theta_{\vec{z}}) \neq 1$, which means $\mathrm{ord}(\theta_{\vec{z}}) = p$. □

Lemma 5.7.5. *Let R be a ring of prime characteristic p, and let $\theta_{\vec{z}} \in \mathrm{CPM}_d^*(R)$ such that $\det(\theta_{\vec{z}})$ has finite order in R^*. Then $\mathrm{ord}(\theta_{\vec{z}})$ is either $\mathrm{ord}(\det(\theta_{\vec{z}}))$ or $p \cdot \mathrm{ord}(\det(\theta_{\vec{z}}))$.*

Proof. Observe that:

$$\mathrm{ord}(\det(\theta_{\vec{z}})) \mid \mathrm{ord}(\theta_{\vec{z}}).$$

Note that:

$$\mathrm{ord}(\theta_{\vec{z}}) = \mathrm{ord}(\det(\theta_{\vec{z}})) \cdot \mathrm{ord}\left(\theta_{\vec{z}}^{\mathrm{ord}(\det(\theta_{\vec{z}}))}\right).$$

As a result, we get:

$$\det\left(\theta_{\vec{z}}^{\mathrm{ord}(\det(\theta_{\vec{z}}))}\right) = \det(\theta_{\vec{z}})^{\mathrm{ord}(\det(\theta_{\vec{z}}))} = 1.$$

Hence by Lemma 5.7.4, $\mathrm{ord}\left(\theta_{\vec{z}}^{\mathrm{ord}(\det(\theta_{\vec{z}}))}\right)$ is either 1 or p, which concludes the proof. □

Proposition 5.7.6. *Let $\theta_{\vec{z}} \in \mathrm{CPM}_d^*(R)$ such that $\det(\theta_{\vec{z}}) - 1 \in R^*$. Then:*

$$\mathrm{ord}(\theta_{\vec{z}}) = \mathrm{ord}(\det(\theta_{\vec{z}})).$$

Proof. By Proposition 5.6.13, $\theta_{\vec{z}}$ admits an eigenbasis with eigenvalues $\lambda_1 = 1$ and $\lambda_2 = \det(\theta_{\vec{z}})$. From this, we conclude that:

$$\mathrm{ord}(\theta_{\vec{z}}) = \mathrm{lcm}(\mathrm{ord}(\lambda_1), \mathrm{ord}(\lambda_2)) = \mathrm{lcm}(1, \mathrm{ord}(\det(\theta_{\vec{z}}))) = \mathrm{ord}(\det(\theta_{\vec{z}})),$$

which completes the proof. □

We conclude this section by briefly considering CPMs over $\mathbb{F}_2$ and over local circulant rings over this field.

Lemma 5.7.7. *Let $\theta_{\vec{z}} \in \mathrm{CPM}_d^*(\mathbb{F}_2)$ such that $\theta \neq I_d$. Then $\mathrm{ord}(\theta_{\vec{z}}) = 2$.*

Proof. By Lemma 5.7.5, we have that $\mathrm{ord}(\theta_{\vec{z}})$ is either equal to $\mathrm{ord}(\det(\theta_{\vec{z}}))$ or $2 \cdot \mathrm{ord}(\det(\theta_{\vec{z}}))$. Since $\theta_{\vec{z}}$ is invertible, we know that $\det(\theta_{\vec{z}}) \in \mathbb{F}_2^*$, which implies $\det(\theta_{\vec{z}}) = 1$. Hence $\mathrm{ord}(\det(\theta_{\vec{z}})) = 1$, which means that $\mathrm{ord}(\theta_{\vec{z}})$ is either 1 or 2. Since $\theta_{\vec{z}} \neq I_d$, we must have that $\mathrm{ord}(\theta_{\vec{z}}) = 2$, which completes the proof. □

Proposition 5.7.8. *Let $R = \mathcal{C}_{\vec{m}/\mathbb{F}_2}$ be a local circulant ring where $\vec{m} := (m_1, \dots, m_n)$, and define $l = \max(v_2(m_i) : 1 \leq i \leq n)$. Then for any $\theta_{\vec{z}} \in \mathrm{CPM}_d^*(R)$, we have that $\mathrm{ord}(\theta_{\vec{z}}) \mid 2^{l+2}$.*

Proof. Let us denote the unique maximal ideal of R by $\mathfrak{m}$, and its quotient map by $\mathfrak{q}$. The map $\mathfrak{q}^d$ restricted to $\mathrm{CPM}_d^*(R)$ induces a surjective map to $\mathrm{CPM}_d^*(\mathbb{F}_2)$.

Let us first consider the case that $\theta_{\vec{z}} \in \ker(\mathfrak{q}^d)$. Since $\theta_{\vec{z}} = I_d + \mathrm{col}(\vec{z})$, we have that $z_0, \dots, z_{d-1} \in \mathfrak{m}$. Observe that:

$$\theta_{\vec{z}}^{2^{l+1}} = (I_d + \mathrm{col}(\vec{z}))^{2^{l+1}} = I_d + \mathrm{col}(\vec{z})^{2^{1+1}} = I_d + \left(\sum_{i=0}^{d-1} z_i\right)^{2^{l+1}} \cdot \mathrm{col}(\vec{z}).$$

Since $\sum_{i=0}^{d-1} z_i \in \mathfrak{m}$, we have that $\left(\sum_{i=0}^{d-1} z_i\right)^{2^l} = 0$. Hence $\left(\sum_{i=0}^{d-1} z_i\right)^{2^{l+1}} = 0$, which implies that $\theta_{\vec{z}}^{2^{l+1}} = I_d$.

Now assume that $\theta_{\vec{z}} \notin \ker(\mathfrak{q}^d)$. This means that $\mathfrak{q}^d(\theta_{\vec{z}}) \in \mathrm{CPM}_d^*(\mathbb{F}_2)$ is not the identity, which means that $\mathfrak{q}(\theta_{\vec{z}})$ has order 2. Hence $\theta_{\vec{z}}^2 \in \ker(\mathfrak{q})$, which implies that $\mathrm{ord}(\theta_{\vec{z}}^2) \mid 2^{l+1}$ as shown earlier. As a result, we have that $\mathrm{ord}(\theta_{\vec{z}}) \mid 2 \cdot 2^{l+1} = 2^{l+2}$, which concludes the proof. □

Chapter 6

The linear layer of Subterranean 2.0

Subterranean 2.0 [DMMR20] is a lightweight permutation-based cryptographic algorithm, which almost reached the final round of the NIST lightweight competition. Its round function works on a 257 bit state, and its linear layer differs from that of Xoodoo in the sense that the shuffling layer is not based on cyclic shifts. Instead, it is based on another type of shuffle known as the multiplicative shuffle. As such, the linear layer of the round function cannot be interpreted as a module endomorphism over circulant modules, and requires a different mathematical approach than what has been presented in this thesis so far. In this chapter, we provide a mathematical analysis of the linear layer of Subterranean 2.0. The results presented in this paper are based on [Sub23], published in the journal "Cryptography and Communications".

This chapter is not entirely related to the other chapters in this thesis, except for the discussion of circulant matrices in Chapter 4. As such, this chapter serves as a stand-alone chapter.

6.1 Specifications of the Subterranean 2.0 round function R

In this section, we present the specifications of the Subterranean 2.0 round function R as described in [DMMR20]. As such, this section is copied from that paper, with slight modifications to fit in with this thesis.

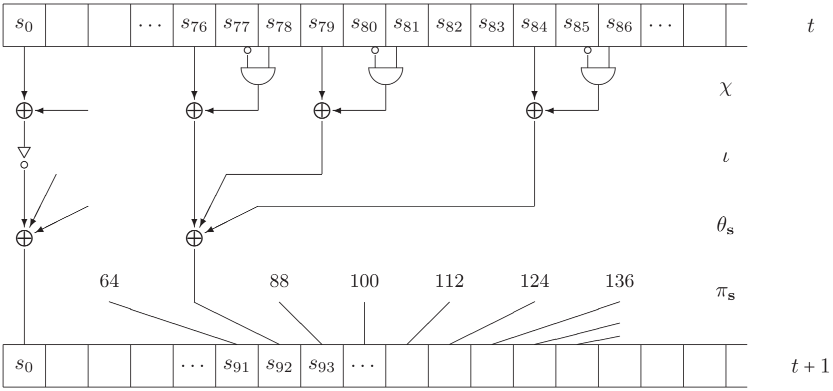

Figure 6.1: Subterranean round function, illustrated for bit s_{92}

The round function R operates on a 257-bit state and has four steps:

$$\mathrm{R} = \pi_{\mathbf{s}} \circ \theta_{\mathbf{s}} \circ \iota \circ \chi \ . \tag{6.1}$$

Each step of the round function has a particular purpose: χ for non-linearity, ι for asymmetry, $\theta_{\mathbf{s}}$ for mixing and $\pi_{\mathbf{s}}$ for dispersion.

We denote the state as s and its bits as s_i with position index i ranging from 0 to 256, where any expression in the index must be taken modulo 257. For all $0 \leq i < 257$:

$$\begin{aligned} \chi: &\quad s_i \leftarrow & s_i + (s_{i+1} + 1)s_{i+2} \ , \\ \iota: &\quad s_i \leftarrow & s_i + \delta_i \ , \\ \theta_{\mathbf{s}}: &\quad s_i \leftarrow & s_i + s_{i+3} + s_{i+8} \ , \\ \pi_{\mathbf{s}}: &\quad s_i \leftarrow & s_{12i} \ . \end{aligned}$$

Here the addition and multiplication of state bits are in $\mathbb{F}_2$, and δ_i is a Kronecker delta: $\delta_i = 1$ if $i = 0$ and 0 otherwise. The composition $\pi_{\mathbf{s}} \circ \theta_{\mathbf{s}}$ forms the *linear layer* of the Subterranean 2.0 round function. Figure 6.1 illustrates the round function by the computational graph of a single bit of the state.

6.2 Multiplicative shuffles and $\pi_{\mathbf{s}}$

The map $\pi_{\mathbf{s}}$ belongs to a family of maps known as a multiplicative shuffle, which we discuss in this section.

Definition 6.2.1. Let us consider the m-dimensional vector space k^m where k is a field. Let $g \in \mathbb{Z}^*_m$. The multiplicative shuffle with shuffling factor g is the linear map:

$$\pi_g \colon k^m \to k^m,\ \vec{x} \to \vec{x}',$$

where $x'_i \coloneqq x_{g^{-1} \cdot i \bmod m}$. The set of multiplicative shuffles is denoted by $\mathcal{S}_m$.

Multiplicative shuffles have the following properties:

- π_g is invertible for all $g \in \mathbb{Z}^*_m$;
- $\pi_1 = \mathrm{id}$;
- $\pi_g \circ \pi_{g'} = \pi_{g'} \circ \pi_g = \pi_{g \cdot g' \bmod m}$ for all $g, g' \in \mathbb{Z}^*_m$.

These statements imply that $\mathcal{S}_m$ forms a finite abelian group under matrix multiplication independent of the field k, which is isomorphic to the group $\mathbb{Z}^*_m$ by the map:

$$\mathbb{Z}^*_m \to \mathcal{S}_m,\ g \mapsto \pi_g.$$

This immediately implies the identity:

$$\mathrm{ord}(\pi_g) = \mathrm{ord}_m(g). \tag{6.2}$$

Remark 6.2.2. In Subterranean 2.0, we have the parameters $m = 257$ and $k = \mathbb{F}_2$. The linear component $\pi_{\mathbf{s}}$ of the linear layer of Subterranean is a multiplicative shuffle with shuffling factor 12, which is denoted as π_{12} using the above notation.

6.3 Group composition of $\mathcal{S}_m$ and $\mathcal{C}^*_{m/k}$

The groups $\mathcal{S}_m$ and $\mathcal{C}^*_{m/k}$ are both subgroups of the general linear group $\mathrm{GL}_m(k)$. We investigate the algebraic behaviour of the linear layer of Subterranean 2.0 by studying the group structure of the composition group $\mathcal{S}_m \cdot \mathcal{C}^*_{m/k}$ viewed as subgroup of $\mathrm{GL}_m(k)$, which we denote by $\mathcal{G}_m$. For the remainder of this chapter, the circulant matrices in $\mathcal{C}^*_{m/k}$ will be represented by their polynomial representation.

Lemma 6.3.1. *For $\theta \in \mathcal{C}^*_{m/k}$ and $\pi \in \mathcal{S}_m$, we have:*

$$\pi_g \cdot \theta \circ \pi_g^{-1} = \theta(X^g).$$

Proof. We only need to show this for the special case where θ is a monomial, since the monomials up to degree $m-1$ form a k-linear basis of $\mathcal{C}_{m/k}$.

Consider the monomial $\theta = X^t$. We prove the identity $\pi_g \circ X^t = X^{gt} \circ \pi_g$, which we do by considering these as maps acting on the vector space k^m.

Let $0 \leq j < m$ and $s \in k^m$. Looking at the mappings coordinate-wise, we obtain:

$$(\pi_g \circ X^t(s))_j = (X^t(s))_{g^{-1}j \bmod m} = s_{g^{-1}j-t \bmod m}.$$

On the other hand, we have that:

$$\left(X^{gt \bmod m} \circ \pi_g(s)\right)_j = (\pi_g(s))_{j-gt \bmod m} = s_{g^{-1}(j-gt) \bmod m} = s_{g^{-1}j-t \bmod m},$$

which coincides with $(\pi_g \circ X^t(s))_j$. Since this is true for all $0 \leq j < m$, we have the desired equality. □

It turns out that $\mathcal{G}_m$ is a **semidirect product** of $\mathcal{S}_m$ and $\mathcal{C}^*_{m/k}$. Let us revisit this concept.

Definition 6.3.2. Let G be a group with identity element e. Let H be a subgroup, and N be a normal subgroup of G. Then G is a **semidirect product** of H acting on N if $G = N \cdot H$ and $N \cap H = \{e\}$. This is denoted by $G = H \ltimes N$.

Remark 6.3.3. A semidirect product $G = H \ltimes N$ has the property that for every $g \in G$, there are unique $h \in H$ and $n \in N$ such that $g = hn$.

Theorem 6.3.4. *Let $\mathcal{G}_m = \mathcal{S}_m \cdot \mathcal{C}^*_{m/k} < \mathrm{GL}_m(k)$. Then $\mathcal{G}_m$ is a semidirect product of $\mathcal{S}_m$ acting on $\mathcal{C}^*_{m/k}$, or equivalently $\mathcal{G}_m = \mathcal{S}_m \ltimes \mathcal{C}^*_{m/k}$.*

Proof. Observe that that the only linear map which is both contained in $\mathcal{S}_m$ and $\mathcal{C}^*_{m/k}$ is the identity map, hence $\mathcal{S}_m \cap \mathcal{C}^*_{m/k} = \{I_m\}$.

All elements in $\mathcal{G}_m$ can be expressed as finite products of elements in $\mathcal{S}_m$ and $\mathcal{C}^*_{m/k}$. Using this observation together with Lemma 6.3.1, we can conclude that $\mathcal{C}^*_{m/k}$ is a normal subgroup of $\mathcal{G}_m$. This concludes the proof. □

6.4 Invariant circulant resultant

Since $\mathcal{G}_m = \mathcal{S}_m \ltimes \mathcal{C}^*_{m/k}$, we have by Remark 6.3.3 that every element in $\mathcal{G}_m$ is of the form $\pi_g \circ \theta$ for unique $\pi_g \in \mathcal{S}_m$ and $\theta \in \mathcal{C}^*_{m/k}$. Also, we have the quotient group $\mathcal{G}_{m/k}/\mathcal{C}^*_{m/k} \cong \mathcal{S}_m$. Note that $\pi_g \circ \theta \equiv \pi_g \bmod \mathcal{C}^*_{m/k}$ in the quotient group.

Since $\mathcal{S}_m$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^*$, π_g is of finite order, which equals $\mathrm{ord}_m(g)$. As such, $(\pi_g \circ \theta)^{\mathrm{ord}_m(g)}$ is contained in $\mathcal{C}^*_{m/k}$. This element plays an important role in analysing $\pi_g \circ \theta$, and we define it explicitly below.

Definition 6.4.1. For $\theta \in \mathcal{C}^*_{m/k}$, we define the **$g$-invariant circulant resultant** θ_g of θ as:

$$\theta_g := (\pi_g \circ \theta)^{\mathrm{ord}_m(g)}.$$

In this subsection, we derive an explicit expression for θ_g.

Proposition 6.4.2. *For all integers $j > 0$, we have*

$$(\pi_g \circ \theta(X))^j = \pi_g^j \circ \left(\prod_{i=0}^{j-1} \theta\left(X^{(g^{-1})^i} \right) \right),$$

where g^{-1} is the inverse of g in $(\mathbb{Z}/m\mathbb{Z})^*$.

Proof. We proceed by induction on j. For $j = 1$, the result is immediate. Now assume this is true for $j = l$ for some $l > 1$ and consider $j = l + 1$. Observe that:

$$\begin{aligned}(\pi_g \circ \theta(X))^{l+1} &= (\pi_g \circ \theta(X))^l \circ (\pi_g \circ \theta(X)) \\ &= \pi_g^l \circ \left(\prod_{i=0}^{l-1} \theta(X) \left(X^{(g^{-1})^i} \right) \right) \circ (\pi_g \circ \theta(X)). \qquad (6.3)\end{aligned}$$

By Lemma 6.3.1, we get:

$$\begin{aligned}\left(\prod_{i=0}^{l-1} \theta\left(X^{(g^{-1})^i} \right) \right) \circ \pi_g &= \pi_g \circ \left(\prod_{i=0}^{l-1} \theta\left(X^{g^{-1}(g^{-1})^i} \right) \right) \\ &= \pi_g \circ \left(\prod_{i=0}^{l-1} \theta\left(X^{(g^{-1})^{i+1}} \right) \right) \\ &= \pi_g \circ \left(\prod_{i=1}^{l} \theta\left(X^{(g^{-1})^i} \right) \right). \qquad (6.4)\end{aligned}$$

By substituting Eq. (6.4) into (6.3), we obtain the identity:

$$\begin{aligned}\pi_g^l \circ \left(\prod_{i=0}^{l-1} \theta\left(X^{(g^{-1})^i} \right) \right) \circ (\pi_g \circ \theta) &= \pi_g^l \circ \pi_g \circ \left(\prod_{i=1}^{l} \theta\left(X^{(g^{-1})^i} \right) \right) \circ \theta \\ &= \pi_g^{l+1} \circ \left(\prod_{i=0}^{l} \theta\left(X^{(g^{-1})^i} \right) \right),\end{aligned}$$

which concludes the induction hypothesis. □

Proposition 6.4.3. *Consider the subgroup $\langle g\rangle$ of $(\mathbb{Z}/m\mathbb{Z})^*$. Then:*

$$\theta_g(X) = \prod_{\gamma\in\langle g\rangle} \theta(X^\gamma).$$

Proof. We have:

$$(\pi_g \circ \theta(X))^{\mathrm{ord}_m(g)} = \pi_g^{\mathrm{ord}_m(g)} \circ \left(\prod_{i=0}^{\mathrm{ord}_m(g)-1} \theta\left(X^{(g^{-1})^i}\right)\right) = \prod_{i=0}^{\mathrm{ord}_m(g)-1} \theta\left(X^{(g^{-1})^i}\right),$$

from Proposition 6.4.2 and equation (6.2) respectively. Observe that:

$$\left\{(g^{-1})^i : 0 \le i \le \mathrm{ord}_m(g) - 1\right\} = \left\{g^i : 0 \le i \le \mathrm{ord}_m(g) - 1\right\} = \langle g\rangle.$$

Hence:

$$\prod_{i=0}^{\mathrm{ord}_m(g)-1} \theta\left(X^{(g^{-1})^i}\right) = \prod_{\gamma\in\langle g\rangle} \theta(X^\gamma).$$

Observe that reordering within the product sign is possible because $\mathcal{C}^*_{m/k}$ is a abelian group, which proves the equation. □

6.5 Order of the invariant circulant resultant

When the base field k is a finite field $\mathbb{F}_q$, then $\mathcal{C}^*_{m/\mathbb{F}_q}$ is of finite order. With this assumption, we provide two upper bounds for the order of θ_g in terms of m, θ and the characteristic of $\mathbb{F}_q$, which we denote by p. These upper bounds are derived independent of each other. Additionally, we assume that m is coprime to p.

Lemma 6.5.1. *For any $f \in \mathcal{C}^*_{m/\mathbb{F}_q}$, we have that:*

$$\mathrm{ord}(f) = \mathrm{lcm}_{\zeta\in\mu_m}(\mathrm{ord}(\theta(\zeta))).$$

Proof. Consider the embedding $\iota : \mathcal{C}^*_{m/\mathbb{F}_q} \to \mathcal{C}^*_{m/\overline{\mathbb{F}}_q}$. It is immediate that $\mathrm{ord}(\theta) = \mathrm{ord}(\iota(\theta))$, where the latter equals $\mathrm{lcm}_{\zeta\in\mu_m}(\mathrm{ord}(\theta(\zeta)))$ by Theorem 3.3.4. □

Theorem 6.5.2 (First upper bound)**.** *Let m be coprime to p. Then for all $\theta \in \mathcal{C}^*_{m/\mathbb{F}_q}$ and $g \in (\mathbb{Z}/m\mathbb{Z})^*$, we have:*

$$\mathrm{ord}(\theta_g) \mid \mathrm{ord}(\theta).$$

Proof. For $\zeta \in \mu_m$, observe that ζ^t is still contained in μ_m for all $t \geq 1$. As such, $\operatorname{lcm}(\operatorname{ord}(\theta(\zeta^t)) : \zeta \in \mu_m)$ divides $\operatorname{lcm}(\operatorname{ord}(\theta(\zeta)) : \zeta \in \mu_m)$, which implies $\operatorname{ord}(\theta(X^t)) \mid \operatorname{ord}(\theta(X))$ for any $t \in \mathbb{Z}_{>0}$ by Lemma 6.5.1. Using this result, we get:

$$\theta_g^{\operatorname{ord}(\theta)} = \left(\prod_{\gamma \in \langle g \rangle} \theta(X^\gamma) \right)^{\operatorname{ord}(\theta)} = \prod_{\gamma \in \langle g \rangle} \theta(X^\gamma)^{\operatorname{ord}(\theta)} = \prod_{\gamma \in \langle g \rangle} 1 = 1,$$

hence $\operatorname{ord}(\theta_g) \mid \operatorname{ord}(\theta)$. □

In contrast to the first upper bound, the second upper bound does not rely on θ, and is instead based on field extensions of $\mathbb{F}_q$. For this, we first define a weaker version of the discrete logarithm.

Definition 6.5.3. Let G be a finite group, S be a subgroup of G and g an element in G. The **discrete group log** of g over S is defined as:

$$\operatorname{dlog}_S(g) := \min\left(t \in \mathbb{Z}_{>0} : g^t \in S \right).$$

Remark 6.5.4. Observe that if S is a normal subgroup of G, then $\operatorname{dlog}_S(g) = \operatorname{ord}(gS)$, which is the order of gS in the quotient group G/S.

Theorem 6.5.5 (Second upper bound)**.** *Let $\langle g \rangle$ be a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$. Then:*

$$\operatorname{ord}(\theta_g) \mid q^{\operatorname{dlog}_{\langle g \rangle}(q)} - 1.$$

Proof. Let $\zeta \in \mu_m$ and let σ be the Frobenius endomorphism as defined in Theorem 2.1.5. Since all coefficients of θ_g are contained in $\mathbb{F}_q$, we have for all $t \in \mathbb{Z}_{>0}$ that:

$$\sigma^{\log_p(q)\cdot t}\left(\theta_g(\zeta)\right) = \theta_g\left(\sigma^{\log_p(q)\cdot t}(\zeta)\right) = \theta_g\left(\zeta^{p^{\log_p(q)\cdot t}}\right) = \theta_g\left(\zeta^{q^t}\right).$$

Observe that $\theta_g(X^\gamma) = \theta_g(X)$ for all $\gamma \in \langle g \rangle$ due to symmetry in the expression of $\theta_g(X)$. Since $q^{\operatorname{dlog}_{\langle g \rangle}(q)} \in \langle g \rangle$, we have:

$$\theta_g\left(\zeta^{q^{\operatorname{dlog}_{\langle g \rangle}(q)}}\right) = \theta_g(\zeta),$$

which implies that $\theta_g(\zeta) \in \mathbb{F}_{q^{\operatorname{dlog}_{\langle g \rangle}(q)}}$ by Galois theory (Theorem 2.1.3). Note that $\theta_g(\zeta) \in \mathbb{F}^*_{q^{\operatorname{dlog}_{\langle g \rangle}(q)}}$ since θ_g is invertible in $\mathcal{C}_{m/\mathbb{F}_q}$, from which Lagrange's theorem [Arm97, Theorem 11.1] implies:

$$\operatorname{ord}\left(\theta_g(\zeta) \in \overline{\mathbb{F}}_p^*\right) \mid q^{\operatorname{dlog}_{\langle g \rangle}(q)} - 1.$$

Since this is true for all $\zeta \in \mu_m$, we conclude from Lemma 6.5.1 that $\mathrm{ord}(\theta_g) \mid q^{\mathrm{dlog}_{\langle g \rangle}(q)} - 1$. □

For the case that m is prime, we can alternatively compute the discrete group log as follows:

Lemma 6.5.6. *Let m be a prime number different from p, then:*

$$\mathrm{dlog}_{\langle g \rangle}(q) = \min\left(t \in \mathbb{Z}_{>0} : \frac{\mathrm{ord}_m(q)}{\gcd(t, \mathrm{ord}_m(q))} \middle| \mathrm{ord}_m(g) \right).$$

Proof. Since m is prime, $(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic. Note that in a finite cyclic group G, we have for $a, b \in G$ that $a \in \langle b \rangle$ if and only if $\mathrm{ord}(a) \mid \mathrm{ord}(b)$. Observe that:

$$\mathrm{ord}_m\left(q^t\right) = \frac{\mathrm{ord}_m(q)}{\gcd(t, \mathrm{ord}_m(q))},$$

which concludes the proof. □

Remark 6.5.7. Lemma 6.5.6 is also valid when m is of the form ρ^k or $2\rho^k$ with ρ an odd prime different from p. This is because for these values of m, the group $(\mathbb{Z}/m\mathbb{Z})^*$ is also cyclic [Con, Theorem A.2].

6.6 Revisiting the linear layer of Subterranean 2.0

The order of the linear layer of Subterranean 2.0 equals 256, which was presented in [DMMR20]. We present a mathematical explanation of this order using the mathematical framework presented above. This provides insight in the algebraic structure in the design of the linear layer of Subterranean 2.0.

Lemma 6.6.1. *Consider the binary field $\mathbb{F}_2$ and let m be a prime number of the form $2^k + 1$. For $g \in (\mathbb{Z}/m\mathbb{Z})^*$, if $\mathrm{ord}_m(g) \geq \mathrm{ord}_m(2)$, then:*

$$\mathrm{ord}(\theta_g) = 1.$$

Proof. Since m is prime, $(\mathbb{Z}/m\mathbb{Z})^*$ is a cyclic group with order $m - 1 = 2^k$. By Lagrange's theorem, we have that $\mathrm{ord}_m(2) \mid \mathrm{ord}_m(g)$ whenever $\mathrm{ord}_m(g) \geq \mathrm{ord}_m(2)$, thus $\mathrm{dlog}_{\langle g \rangle}(2) = 1$. From Theorem 6.5.5, we conclude that:

$$\mathrm{ord}(\theta_g) \mid 2^{\mathrm{dlog}_{\langle g \rangle}(2)} - 1 = 2^1 - 1 = 1,$$

which implies $\mathrm{ord}(\theta_g) = 1$. □

Corollary 6.6.2. *The order of the linear layer of Subterranean 2.0 Cipher Suite equals* 256*.*

Proof. The linear layer of Subterranean 2.0 consists of the composition $\pi_{\mathbf{s}} \circ \theta_{\mathbf{s}} : \mathbb{F}_2^{257} \to \mathbb{F}_2^{257}$, where $\pi_{\mathbf{s}} = \pi_{12}$, and where $\theta_{\mathbf{s}}$ is a circulant matrix represented by the polynomial $1+X^{249}+X^{254}$. Observe that $\mathrm{ord}_{257}(12) = 256 > 16 = \mathrm{ord}_{257}(2)$, which by Lemma 6.6.1 implies that $\mathrm{ord}(\theta_{12}) = 1$. Hence we have that:

$$\mathrm{ord}(\pi_{12} \circ \theta_{\mathbf{s}}) = \mathrm{ord}_{257}(12) \cdot \mathrm{ord}(\theta_{12}) = 256 \cdot 1 = 256.$$

□

Chapter 7

Conclusions and Outlook

In this thesis, we showed how linear maps constructed from circulant shifts can be interpreted as module endomorphisms of free modules over group algebras over finite abelian groups. This interpretation adds much more algebraic structure on top of simply linearity, where these additional properties can be derived from the algebraic structure of the underlying group algebras. As such, we also provided a full description of group algebras over finite abelian groups, with a bit of emphasis on the case where the base field is a finite field. This completes the theoretical framework of studying these types of linear layers from a module theoretic point of view.

I believe this opens up many research opportunities. One example is based on the following observation: For a commutative ring R, an ideal I of R, and a bijective R-endomorphism $f\colon R^m \to R^m$, the submodule $I^m \subset R^m$ remains invariant under f in the sense that f restricted to I^m is a bijective map from I^m to itself. Using this observation, one can construct many invariant subspaces of the linear layer from the components of the Krull-Remak-Schmidt decomposition of the underlying group algebra.

Additionally, one should also consider the effect of the non-linear layer applied on these invariant subspaces. Taking XOODOO as an example, a very interesting line of research would be to study the effect of χ. If certain patterns can be found, e.g. invariance or predictable images of certain subspaces under χ, then one can find distinguishers for the XOODOO permutation, which may lead to new cryptanalytic techniques. Same ideas may be applicable to other such permutations such as the ASCON permutation.

Finally, the mathematical framework developed in this thesis can also be applied to analyse permutation-based constructions over non-binary fields. These type of permutation are being considered more and more in novel designs. An example is the hash function Troika [KTDB20], where they use $\mathbb{F}_3$ as base field.

The framework presented in this thesis can lead to new and interesting research directions within symmetric cryptography and beyond. It is possible that the structure of the Krull-Remak-Schmidt decomposition can be used for algorithm designs related to group algebras.

Bibliography

[Alo01] Noga Alon. Combinatorial nullstellensatz. *Combin. Probab. Comput*, 8(1-2):7–29, 2001.

[Arm97] Mark A Armstrong. *Groups and symmetry.* Springer Science & Business Media, 1997.

[Ati18] Michael Atiyah. *Introduction to commutative algebra.* CRC Press, 2018.

[BCLR17] Christof Beierle, Anne Canteaut, Gregor Leander, and Yann Rotella. Proving resistance against invariant attacks: How to choose the round constants. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 647–678. Springer, 2017.

[BDPV11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Duplexing the sponge: Single-pass authenticated encryption and other applications. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 320–337. Springer, 2011.

[BDPV15] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak. *IACR Cryptol. ePrint Arch.*, page 389, 2015.

[BS91] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. *J. Cryptol.*, 4(1):3–72, 1991.

[Con] Keith Conrad. Subgroups of cyclic groups.

[DEMS21] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2: Lightweight authenticated encryption and hashing. *J. Cryptol.*, 34(3):33, 2021.

[DHVV18] Joan Daemen, Seth Hoffert, Gilles Van Assche, and Ronny Van Keer. The design of Xoodoo and Xoofff. *IACR Trans. Symmetric Cryptol.*, 2018(4):1–38, 2018.

[DMMR20] Joan Daemen, Pedro Maat Costa Massolino, Alireza Mehrdad, and Yann Rotella. The Subterranean 2.0 Cipher Suite. *IACR Trans. Symmetric Cryptol.*, 2020(S1):262–294, 2020.

[DR20] Joan Daemen and Vincent Rijmen. *The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition*. Information Security and Cryptography. Springer, 2020.

[Ehr11] Gertrude Ehrlich. *Fundamental concepts of abstract algebra*. Courier Corporation, 2011.

[FSK10] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. *Cryptography Engineering - Design Principles and Practical Applications*. Wiley, 2010.

[Kem10] Gregor Kemper. *A course in commutative algebra*, volume 256. Springer Science & Business Media, 2010.

[KS12] Irwin Kra and Santiago R Simanca. On circulant matrices. *Notices of the AMS*, 59(3):368–377, 2012.

[KTDB20] Stefan Kölbl, Elmar Tischhauser, Patrick Derbez, and Andrey Bogdanov. Troika: a ternary cryptographic hash function. *Des. Codes Cryptogr.*, 88(1):91–117, 2020.

[LAAZ11] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda Alkhzaimi, and Erik Zenner. A cryptanalysis of printcipher: The invariant subspace attack. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 206–221. Springer, 2011.

[Lan04] Serge Lang. Algebra, volume 211 of. *Graduate Texts in Mathematics*, 2004.

[Mat93] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer, 1993.

[SB88] Miles E. Smid and Dennis K. Branstad. Data encryption standard: past and future. *Proc. IEEE*, 76(5):550–559, 1988.

[Sch12] Peter Schneider. *Modular representation theory of finite groups*. Springer Science & Business Media, 2012.

[SD18] Ko Stoffelen and Joan Daemen. Column parity mixers. *IACR Trans. Symmetric Cryptol.*, 2018(1):126–159, 2018.

[Sub23] Robert Christian Subroto. An algebraic approach to symmetric linear layers in cryptographic primitives. *Cryptogr. Commun.*, 15(6):1053–1067, 2023.

[Sub24a] Robert Christian Subroto. An algebraic approach to circulant column parity mixers. *Designs, Codes and Cryptography*, pages 1–27, 2024.

[Sub24b] Robert Christian Subroto. The Krull-Remak-Schmidt decomposition of commutative group algebras, 2024.

[Sub24c] Robert Christian Subroto. Wedderburn decomposition of commutative semisimple group algebras using the Combinatorial Nullstellensatz, 2024.

Research data management

This thesis research has been carried out under the institute policy of the institute for Computing and Information Sciences (iCIS) of the Radboud University Nijmegen. The author declares that no additional data have been used in his research. Also no additional code besides the ones already processed in this thesis was applied.

Summary

This thesis summarizes the results of my research in the last four years. The research was focussed on developing a mathematical framework to study a specific class of linear maps known as circulant column parity mixers (CCPMs). This was motivated by some numerical observations of CCPMs which could not be explained using the original approach.

A surprising result is the discovery that CCPMs can be effectively studied using concepts from commutative algebra. One of the key contributions of this work is establishing a link between CCPMs and module theory. Specifically, I demonstrated that CCPMs can be interpreted as endomorphisms of free modules over group algebras over finite abelian groups. Conceptually, a free module is a generalization of a vector space, where scaling is defined over a ring instead of a field. This allows for the extension of familiar linear algebra concepts, such as dimension (known as rank in module theory) and linear operators, to module theory. However, some extra caution is needed in the study of modules when using intuition from linear algebra, as properties like a set of independent vectors matching the module's rank do not necessarily form a basis.

The module theoretic interpretation of CCPMs offers some significant advantages compared to the original interpretation, particularly in investigating and deriving the algebraic properties of CCPMs. From a complexity standpoint, viewing CCPMs as linear maps typically involves a high-dimensional vector space, which adds complications when analytically studying CCPMs. In the module theoretic approach, the same CCPMs have a much lower rank, making it a more suitable candidate for an analytical approach. A clear example is the linear layer of the Xoodoo permutation, where the underlying $\mathbb{F}_2$-vectorspace has dimension $3 \cdot 4 \cdot 32 = 384$. In the module theoretic setting, the linear layer of the Xoodoo permutation has a rank of only 3, which is a substantial reduction. However, this method does require a solid under-

standing of the underlying group algebra, which is a complex mathematical construct.

A large portion of my research was focussed on understanding the algebraic structure of group algebras over finite abelian groups, with the primary objective of determining the Krull-Remak-Schmidt decomposition of these group algebras. This decomposition for group algebras is the analogue of the prime number decomposition of integers, where its components reveal a lot of information about the structure of the main object of interest This was successfully achieved by using techniques from various branches of mathematics, including Galois theory, group actions, affine algebraic geometry and modular representation theory. Roughly speaking, the behaviour of such group algebras rely on the orbit structure of certain Galois group actions, which can be analysed through the study of cyclotomic extensions over the given base field of the group algebra. This is particularly beneficial for cryptographic applications, where the base field is usually a finite field whose Galois extensions are well-understood. Consequently, my research provides a detailed description of the Krull-Remak-Schmidt decomposition of group algebras over finite fields.

Samenvatting

Dit proefschrift vat de resultaten samen van mijn onderzoek van de afgelopen vier jaar. Het onderzoek richtte zich op het ontwikkelen van een wiskundig kader om een specifieke klasse van lineaire afbeeldingen, bekend als circulant column parity mixers (CCPMs), te bestuderen. De motivatie hiervoor kwam voort uit numerieke waarnemingen van CCPMs die niet konden worden verklaard met de oorspronkelijke aanpak.

Een verrassende uitkomst is de ontdekking dat CCPMs effectief bestudeerd kunnen worden met behulp van concepten uit de commutatieve algebra. Eén van de belangrijkste bijdragen van dit werk is het leggen van een verband tussen CCPMs en de theorie der modulen. Ik heb aangetoond dat CCPMs kunnen worden geïnterpreteerd als endomorfismen van vrije modulen over groepsalgebras over eindige abelse groepen. Conceptueel is een vrij moduul een generalisatie van een vectorruimte, waarbij scalairen gedefinieerd zijn over een ring in plaats van over een lichaam. Dit maakt het mogelijk om bekende concepten uit de lineaire algebra, zoals dimensie (bekend als rang wanneer gewerkt wordt met modulen) en lineaire operatoren, uit te breiden naar de theorie van modulen. Er is echter extra voorzichtigheid geboden bij het toepassen van intuïtie uit de lineaire algebra op modulen, omdat eigenschappen zoals een verzameling onafhankelijke vectoren die overeenkomt met de rang van het moduul niet per se impliceren dat het een basis vormt.

De moduul-theoretische interpretatie van CCPMs biedt aanzienlijke voordelen ten opzichte van de oorspronkelijke interpretatie, met name bij het onderzoeken en afleiden van de algebraïsche eigenschappen van CCPMs. Vanuit een complexiteitsperspectief houdt het bekijken van CCPMs als lineaire afbeeldingen doorgaans in dat er gewerkt wordt met een hoog-dimensionale vectorruimte, wat een analytische aanpak bemoeilijkt. In de moduul-theoretische benadering hebben dezelfde CCPMs een veel lagere rang, waardoor ze beter geschikt zijn voor een analytische aanpak. Een duidelijk voorbeeld is de lineaire laag van de XOODOO-permutatie, waar de onderliggende $\mathbb{F}_2$-vectorruimte een dimensie heeft van $3 \cdot 4 \cdot 32 = 384$. In de moduul-theoretische aanpak heeft de afbeelding van de XOODOO-permutatie echter een rang van slechts 3, wat een aanzienlijke vereenvoudiging is. Deze methode vereist echter wel een gedegen begrip van de onderliggende groepsalgebra, wat op zichzelf een ingewikkeld wiskundig object is.

Een groot deel van mijn onderzoek richtte zich op het begrijpen van de algebraïsche structuur van groepsalgebras van eindige abelse groepen, met als belangrijkste doel het bepalen van de Krull-Remak-Schmidt-ontbinding van deze groepsalgebras. Deze ontbinding is voor groepsalgebras vergelijkbaar met de priemontbinding van gehele getallen, waarbij de componenten veel inzicht geven in de structuur van het hoofdobject. Dit doel werd met succes bereikt door het gebruik van technieken uit diverse takken van de wiskunde, waaronder de Galoistheorie, groepswerkingen, affine algebraïsche meetkunde en de modulaire representatietheorie. Grofweg gezegd hangt het gedrag van zulke groepsalgebras af van de orbitaalstructuur van bepaalde Galois-groepswerkingen die kunnen worden geanalyseerd door te kijken naar cyclotomische lichaamsuitbreidingen over het gegeven basislichaam van de groepsalgebra. Dit is bijzonder gunstig voor toepassingen in de cryptografie, waar het basislichaam doorgaans een eindig lichaam is waarvan de Galois-uitbreidingen goed begrepen zijn. Als gevolg biedt mijn onderzoek een gedetailleerde beschrijving van de Krull-Remak-Schmidt-ontbinding van groepsalgebras over eindige lichamen.

About the Author

Robert Christian Subroto was born in 1995 in Jakarta, Indonesia, after which he moved to the Netherlands with his parents at the age of 3. He obtained his master's degree in mathematics in 2019 at the University of Amsterdam, after which he tried out a career in industry. He returned however to academics in 2020 as a PhD student at the Radboud University in Nijmegen. Under supervision of prof. dr. Joan Daemen, Robert performed research which lies at the intersection between commutative algebra and symmetric key cryptography. Motivated by problems in cryptography, Robert developed a mathematical theory where he managed to classify all the indecomposable components of group algebras over finite abelian groups.

List of Publications and Preprints

1. "The Krull-Remak-Schmidt decomposition of commutative group algebras"
2. "Wedderburn decomposition of commutative semisimple group algebras using the Combinatorial Nullstellensatz"
3. "An algebraic approach to circulant column parity mixers"
4. "An algebraic approach to symmetric linear layers in cryptographic primitives"

9 789465 151472 >

Radboud Universiteit

IN·DEI·NOMINE·FELICITER