FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

MASTER THESIS

Bc. Marek Marko

Cryptographic application of codes over Galois rings

Department of Algebra

Supervisor of the master thesis: doc. Mgr. et Mgr. Jan Žemlička, Ph.D.
Study programme: Mathematics for Information Technologies
Study branch: Mathematics for Information Technologies

Prague 2024

I declare that I carried out this master thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In .... date ....

Author's signature

I dedicate this thesis to my supervisor, doc. Mgr. et Mgr. Jan Žemlička, Ph.D., whose expertise, guidance, and willingness during numerous consultations were pivotal throughout this journey. I also wish to honour the memory of my father, whose caring support was endless. I am grateful to my sisters for their continuous encouragement and, last but not least, to my fiancé for his constant belief in me, cheering me up, and giving me strength when I had none.

Title: Cryptographic application of codes over Galois rings

Author: Bc. Marek Marko

Department: Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: This thesis deals with Gabidulin codes over Galois rings and their application in public-key cryptography. The first objective is to demonstrate the construction of Galois rings and their essential properties to the reader. This step is necessary to provide the code theory over these rings and understand their differences from the standard one over finite fields. The cardinal rank and its induced metric are studied and utilised in linear codes. A significant part of the thesis is presenting an efficient decoding algorithm for the given error-correcting codes. The concluding part proposes a public key cryptosystem whose decryption is founded on the decoding algorithm.

Keywords: Galois Rings Error-Correcting Codes Gabidulin Codes Rank Metric Cardinal Rank Metric McEliece Cryptosystem

Contents

Introduction

The original idea of constructing a public-key cryptosystem (PKC) based on error--correcting codes came from McEliece [1]. The proposed PKC used Goppa codes with Hamming distance, and its security was derived from a general decoding problem for linear codes, which is NP-complete. Unfortunately, code parameters, and therefore public keys also, had to be taken large.

A further modification of the McEliece scheme was introduced by Gabidulin, Paramonov and Tretjakov [2]. Their cryptosystem was based on Maximum Rank Distance (MRD) codes, a class similar to Maximum Distance Separable (MDS) codes, but with the rank distance instead of Hamming distance. MRD codes are well-structured since they use a finite field extension and view the larger field as a vector space over its subfield. The distance between two codewords is given by the rank of the matrix representing their difference.

Several attacks on the GPT cryptosystem were published over the years, among which Overbeck's attacks [3] were some of the most efficient. Multiple countermeasures were reviewed to withstand Overbeck's attack, e.g. the Smart approach proposed in [4] with special choosing of a distortion matrix. However, some deficits of this approach were found, including the transformation of the public key to apply Overbeckeck's attack published by Kalachi [5].

In this thesis, another method is chosen. Instead of utilising linear codes over finite fields, codes over Galois rings are applied as in [6]. The first chapter deals with the construction and description of Galois rings. Linear codes based on the modul theory are studied within the second chapter. In Chapter Three, the distance of codewords different from Hamming one is presented. Moreover, its properties are there thoroughly examined to understand the generalisation of MRD codes. The final chapter focuses on Gabidulin codes over Galois rings, presenting the decoding algorithm and verifying that the GPT PKC is correct also in this scenario.

1. Galois Rings

First of all, it might be relevant to set up the terminology. Let a commutative ring $\mathbf{R}$, which always contains identity, be given. An ideal $I \subseteq \mathbf{R}$ shall be denoted by $I \leq \mathbf{R}$, and the fact that elements $a_1, \ldots, a_n \in \mathbf{R}$ generates the ideal I shall be expressed as $I = (a_1, a_2, \ldots, a_n) = a_1\mathbf{R} + a_2\mathbf{R} + \cdots + a_n\mathbf{R}$. If a maximal ideal $M \leq \mathbf{R}$ exists unique then $(\mathbf{R}, M)$ is a local ring, and $\mathbb{K} = {}^{\mathbf{R}}\!/_{M}$ is its residue field. The set of units of the ring $\mathbf{R}$ is $\mathbf{R}^* = \{a \in \mathbf{R} \mid \exists b \in \mathbf{R} : a \cdot b = 1\}$, and $b \in \mathbf{R}$ is said to be a nilpotent element of $\mathbf{R}$ provided $b^n = 0$ for some $n \in \mathbb{N}$. Any ring homomorphism $f : R \longrightarrow S$ satisfying $f(M_R) \subseteq M_S$, where $(\mathbf{R}, M_R), (\mathbf{S}, M_S)$ are local rings, will be called local.

Example 1. Let p be a prime and n be a positive integer. Then, $(\mathbb{Z}_{p^n}, p\mathbb{Z}_{p^n})$ is a local ring with the residue field ${}^{\mathbb{Z}_{p^n}}\!/_{p\mathbb{Z}_{p^n}} \simeq \mathbb{F}_p$.

Claim 1. Let $\mathbf{R}$ be a finite commutative ring with identity and M be the set containing all nilpotent elements of $\mathbf{R}$. Suppose that $\{0\} \subsetneq M$.

1. If $m \in M$ then $(1 - m) \in \mathbf{R}^*$.

2. M is an ideal.

3. If M is maximal then $M = \mathbf{R} \setminus \mathbf{R}^*$ and $(\mathbf{R}, M)$ is a local ring.

Proof. 1. Choose $m \in M$ and find $n \in \mathbb{N}$ such that $m^n = 0$. Thus,

$$(1 - m) \cdot \sum_{i=0}^{n-1} m^i = \sum_{i=0}^{n-1} \left(m^i - m^{i+1}\right) = 1 - m^n = 1.$$

2. Let $r \in \mathbf{R}, a, b \in M$ and $n_1, n_2 \in \mathbb{N}$ such that $a^{n_1} = 0 = b^{n_2}$. Assume, without loss of generality, $n_1 \geq n_2$. Clearly, $0 \in M$. Denote $n_0 = n_1 + n_2$. Compute

$$\begin{aligned}(a+b)^{n_0} &= a^{n_0} + b^{n_0} + \sum_{i=1}^{n_0-1} \binom{n_0}{i} a^i b^{n_0-1-i} \\ &= \sum_{i=1}^{n_1-1} \binom{n_0}{i} a^i b^{n_0-1-i} + \sum_{i=n_1}^{n_0-1} \binom{n_0}{i} a^i b^{n_0-1-i} \\ &= b^{n_2} \cdot \sum_{i=1}^{n_1-1} \binom{n_0}{i} a^i b^{n_1-1-i} + a^{n_1} \cdot \sum_{i=n_1}^{n_0-1} \binom{n_0}{i} a^{i-n_1} b^{n_0-1-i} = 0,\end{aligned}$$

so $(a + b) \in M$. It is apparent that $(r \cdot a)^{n_1} = r^{n_1} \cdot a^{n_1} = 0$. Hence, M is really an ideal of $\mathbf{R}$.

3. Since no nilpotent is a unit, it is enough to prove that any element which is not nilpotent is a unit. Choose $x \in \mathbf{R} \setminus M$. Clearly ${}^{\mathbf{R}}\!/_{M}$ is a field since M is maximal, and therefore, there exists $y \in \mathbf{R} \setminus M$ satisfying $x \cdot y = 1 - m$ for a appropriate $m \in M$. However, according to 1., the element $(1-m)$ is a unit, and for this reason, $x \cdot (y \cdot (1 - m)^{-1}) = 1$ and x is a unit.

Finally, every non-trivial ideal $I \leq \mathbf{R}$ must be a part of M because every non-nilpotent element of $\mathbf{R}$ is a unit. The uniqueness of M is now evident.

□

1.1 Polynomials Modulo Prime-Power Residues

Let a prime p and $n \in \mathbb{N}$ be determined subsequently. Irreducible polynomials over the commutative ring $\mathbb{Z}_{p^n}$ are pivotal for constructions in the succeeding sections. Thus, it is essential to properly define them and present their properties and connections to irreducible polynomials over $\mathbb{Z}_p$. To begin with, let us describe which polynomials in $\mathbb{Z}_{p^n}[x]$ are units and which are nilpotent elements. The proof of the following more general theorem will be omitted.

Theorem 2. [7, Proposition 1.3.1] Let $\mathbf{R}$ be a commutative ring with identity and $f(x) = \sum_{i=0}^{m} f_i x^i \in \mathbf{R}[x]$. Then,

1. f is a unit in $\mathbf{R}[x] \iff f_0 \in \mathbf{R}^*$ and $f_1, \dots, f_m$ are nilpotent in $\mathbf{R}$,
2. f is a nilpotent in $\mathbf{R}[x] \iff f_0, f_1, \dots, f_m$ are nilpotent in $\mathbf{R}$,
3. f is a zero-divisor $\iff \exists a \in \mathbf{R} \setminus \{0\}$ such that $a \cdot f(x) = 0$.

Consider a projection $\phi : \mathbb{Z}_{p^n} \longrightarrow \mathbb{Z}_p$ defined as $a \mapsto a \mod p$ and extend it to $\mu : \mathbb{Z}_{p^n}[x] \longrightarrow \mathbb{Z}_p[x]$, $\sum_{i=0}^{m} a_i x^i \mapsto \sum_{i=0}^{m} \phi(a_i) x^i$. It is not difficult to see that both the maps ϕ and μ are surjective ring homomorphism with kernels $p\mathbb{Z}_{p^n}$ and $p\mathbb{Z}_{p^n}[x]$, respectively. Let us clarify here that an epimorphism is always a surjective homomorphism and not a more general concept from the category theory. Our goal for the first two sections is to determine some induced ring epimorphism $\tilde{\mu}$ of quotient rings ${}^{\mathbb{Z}_{p^n}[x]}\!/_{I}$ and ${}^{\mathbb{Z}_p[x]}\!/_{J}$, where I and J are ideals of $\mathbb{Z}_{p^n}[x]$ and $\mathbb{Z}_p[x]$ in the specified order. For that, we need to explore the relation between polynomials over $\mathbb{Z}_p$ and $\mathbb{Z}_{p^n}$. In this chapter, we mind a construction from the work by Flamini et al. [7].

Definition 3. Let $f \in \mathbb{Z}_{p^n}[x]$ be non-zero. Then f is said to be:

- *regular* provided there is no non-zero $g \in \mathbb{Z}_{p^n}[x]$ such that $f \cdot g = 0$,
- *irreducible* provided it is not a unit, and if $g, h \in \mathbb{Z}_{p^n}[x]$ exist such that $f = g \cdot h$, then either g or h is a unit.

Lemma 4. Let $f \in \mathbb{Z}_{p^n}[x]$ be a regular polynomial such that $\mu(f)$ is an irreducible in $\mathbb{Z}_p[x]$. Then, f is irreducible in $\mathbb{Z}_{p^n}[x]$.

Proof. Firstly, observe that f cannot be a unit in $\mathbb{Z}_{p^n}[x]$ as $\mu(f)$ is irreducible in $\mathbb{Z}_p[x]$. Let $f \in \mathbb{Z}_{p^n}[x]$ be the product of polynomials $g, h \in \mathbb{Z}_{p^n}[x]$. It follows $\mu(f) = \mu(g) \cdot \mu(h)$. Since $\mu(f)$ is irreducible, then one of $\mu(g)$ and $\mu(h)$ must be a unit in $\mathbb{Z}_p[x]$ and the other cannot be. Suppose, without loss of generality, $\mu(g) = 1$, which means that $g(x) = 1 + p\tilde{g}(x)$ for suitable $\tilde{g} \in \mathbb{Z}_{p^n}[x]$. As stated by **Theorem 2**, $p\tilde{g}$ is nilpotent in $\mathbb{Z}_{p^n}[x]$. For arbitrary $a \in \mathbb{Z}_{p^n}$, the element $b = 1 + p \cdot a$ is a unit in $\mathbb{Z}_{p^n}$ according to **Claim 1**. **Theorem 2** asserts that $g(x) = 1 + p\tilde{g}(x) \in \mathbb{Z}_{p^n}[x]^*$. In conclusion, f is irreducible in $\mathbb{Z}_{p^n}[x]$. □

Let $\mathbb{F}_p \subseteq \mathbb{F}_{p^r}$ be a finite field extension for some $r \in \mathbb{N}$. Recall that an element $\alpha \in \mathbb{F}_{p^r}$ is primitive provided α generates the multiplicative group $\mathbb{F}_{p^r}^*$, denoted by $\mathbb{F}_{p^r}^* = \langle \alpha \rangle$. We shall say that an element β is primitive over $\mathbb{F}_p$, if an extension $\mathbb{F}_q$ of $\mathbb{F}_p$ exists such that $\beta \in \mathbb{F}_q$ is primitive. By a primitive polynomial over $\mathbb{Z}_p$, the minimal polynomial of a primitive element over $\mathbb{Z}_p$ is meant. Irreducible polynomials over $\mathbb{Z}_{p^n}$, whose projections to $\mathbb{Z}_p[x]$ are primitive polynomials, play a substantial role in the construction proposed in the ensuing chapter. Therefore, it is beneficial to name these polynomials and to provide a simple example of them.

Definition 5. A polynomial $f \in \mathbb{Z}_{p^n}[x]$ is *basic irreducible* if $\mu(f)$ is irreducible in $\mathbb{Z}_p[x]$. Furthermore, if $\mu(f)$ is the minimal polynomial of a primitive element over $\mathbb{Z}_p$, the polynomial f is said to be *basic primitive*.

Example 2. The list of all irreducible polynomials of degree 2 over $\mathbb{Z}_4$ together with their projections to $\mathbb{Z}_2[x]$ is provided in Table 1.1. The table indicates the irreducibility of the projections in $\mathbb{Z}_2[x]$, as well. Let us remark the presented polynomials from $\mathbb{Z}_4[x]$ were computed in Wolfram Mathematica by setting all possible coefficients and checking whether the constructed polynomial has roots over $\mathbb{Z}_4$.

Irreducible $f \in \mathbb{Z}_4[x]$	$\mu(f) \in \mathbb{Z}_2[x]$	$\mu(f)$ **irreducible**
$\pm(x^2+2)$ $\pm(x^2+2x+2)$	x^2	✗
$\pm(x^2+1)$ $\pm(x^2+2x+3)$	$(x+1)^2$	✗
$\pm(x^2+x+1)$ $\pm(x^2+x+3)$ $\pm(x^2+3x+1)$ $\pm(x^2+3x+3)$	x^2+x+1	✓

Table 1.1: Irreducible polynomials of degree 2 in $\mathbb{Z}_4[x]$

A natural question is how to find a polynomial f from $\mathbb{Z}_{p^n}[x]$, which projection $\mu(f)$ is irreducible in $\mathbb{Z}_p[x]$. The answer is to start with an irreducible polynomial over $\mathbb{Z}_p$ and lift it to the $\mathbb{Z}_{p^n}[x]$. In the rest of the first section, the Hensel's lift is described. Let us start by a lemma based on the Bezout's identity.

Lemma 6. Let $f, g, h \in \mathbb{Z}_p[x]$ be non-zero such that $\deg(f) < \deg(g) + \deg(h)$ and g, h are coprime. Then, the unique polynomials $u, v \in \mathbb{Z}_p[x]$ exist which satisfy $\deg(u) < \deg(h)$, $\deg(v) < \deg(g)$ and $f = u \cdot g + v \cdot h$.

Proof. Since $\mathbb{Z}_p[x]$ is an Euclidean domain, it is possible to perform the Extended Euclidean Algorithm (EEA) on the given polynomials g, h to compute the coefficients $u_0, v_0 \in \mathbb{Z}_p[x]$ of the Bezout's identity. Thus, $\deg(u_0) < \deg(h), \deg(v_0) < \deg(g)$ and $1 = u_0 g + v_0 h$. Multiply the equation by f to obtain $f = (u_0 f)g + (v_0 f)h$. Compute $u = (u_0 f) \mod h$, $q = (u_0 f) \text{ div } h$

and $v = qg + v_0 f$. Apparently, $u_0 f = qh + u$ and $\deg u < \deg h$. Furthermore,

$$\begin{aligned} f &= (qh+u)g + (v_0 f)h = ug + (qg + v_0 f)h = ug + vh, \\ \deg(v) + \deg(h) &= \deg(vh) = \deg(g(qh) + v_0 fh) = \deg(gu_0 f + v_0 fh - gu) \\ &= \deg(f - gu) \leq \max(\deg(f), \deg(u) + \deg(g)) \\ &< \deg(h) + \deg(g), \end{aligned}$$

and therefore, $\deg(v) < \deg(g)$.

It remains to show the uniqueness. Assume that the proposition hold for two pairs $u, v, \tilde{u}, \tilde{v} \in \mathbb{Z}_p[x]$, i.e. $ug + vh = \tilde{u}g + \tilde{v}h$. Clearly, $(u - \tilde{u})g = (\tilde{v} - v)h$, which implies $g \mid (\tilde{v} - v)$ as g, h are coprime. Since $\deg g > \deg{(\tilde{v} - v)}$, the difference $\tilde{v} - v$ must be the constant zero. Consequently, $u - \tilde{u} = 0$ as well.

□

The prior lemma may be generalised for more than just two polynomials g, h. The generalised version is vital in order to justify lifting of polynomials from $\mathbb{Z}_p[x]$ to $\mathbb{Z}_{p^n}[x]$.

Lemma 7. Let $f, g_1, \ldots, g_m \in \mathbb{Z}_p[x]$ satisfy $\deg(f) < \sum\limits_{i=1}^{m} \deg(g_i)$ and each pair g_i, g_j is coprime for $i, j \in \mathbb{N}, i < j \leq m$. There exist the unique polynomials $u_1, \ldots, u_m \in \mathbb{Z}_p[x]$ satisfying $\deg(u_i) < \deg(g_i)$ for every positive integer i, $i \leq m$, and $f = \sum\limits_{i=1}^{m} u_i \prod\limits_{\substack{j=1 \\ j \neq i}}^{m} g_j$.

Proof. Set $d_0 = f$ and, for every $i \in \mathbb{N}, i \leq n$, $g_i^* = \prod\limits_{j=i+1}^{m} g_j$ and $\tilde{g}_i = \prod\limits_{\substack{j=1 \\ j \neq i}}^{m} g_j$. It is evident that $g_m^* = 1$ and $\deg(d_0) = \deg(f) < \sum\limits_{i=1}^{m} \deg(g_i)$. According to **Lemma 6** applied to d_0, g_1, g_1^*, the unique $d_1, u_1 \in \mathbb{Z}_p[x]$ exist satisfying $d_0 = d_1 \cdot g_1 + u_1 \cdot g_1^*, \deg(d_1) < \deg(g_1^*)$ and $\deg(u_1) < \deg(g_1)$. Now, assume that we already have $d_j, u_j \in \mathbb{Z}_p[x]$ such that $d_{j-1} = d_j \cdot g_j + u_j \cdot g_j^*, \deg(d_j) < \deg(g_j^*)$ and $\deg(u_j) < \deg(g_j)$ for every positive integer $j, j < i$, where $i \in \mathbb{N}, i < m$. It directly follows that $\deg(d_{i-1}) < \deg(g_{i-1}^*) = \deg\left(\prod_{j=i}^{m} g_j\right) = \deg(g_i) + \deg(g_i^*)$. Apply **Lemma 6** again to obtain the unique $d_{i+1}, u_{i+1} \in \mathbb{Z}_p[x]$ which fulfill $\deg(d_{i+1}) < \deg(g_{i+1}^*), \deg(u_{i+1}) < \deg(g_{i+1})$ and $d_i \overset{\star}{=} d_{i+1} \cdot g_{i+1} + u_{i+1} \cdot g_{i+1}^*$.

Put $e_i = d_i \prod\limits_{j=1}^{i} g_j$ for every $i, 0 \leq i \leq m$. Choose $i \in \mathbb{N}, i \leq m$, and compute $u_i \tilde{g}_i = u_i g_i^* \cdot \prod\limits_{j=1}^{i-1} g_j \overset{\star}{=} (d_{i-1} - d_i g_i) \prod\limits_{j=1}^{i-1} g_j = d_{i-1} \prod\limits_{j=1}^{i-1} g_j - d_i \prod\limits_{j=1}^{i} g_j = e_{i-1} - e_i$. In addition, $e_0 = d_0 = f$ and $e_m = d_m g_0^* = 0$ because $\deg(d_m) < \deg(g_m^*) = 0$. Altogether, $\sum\limits_{i=1}^{m} u_i \tilde{g}_i = \sum\limits_{i=1}^{m} (e_{i-1} - e_i) = e_0 + e_m = f + 0 = f$.

Assume that the proposition is true for $u_1, \ldots, u_m, \tilde{u}_1, \ldots, \tilde{u}_m \in \mathbb{Z}_p[x]$. Now, we show, without loss of generality, $u_1 = \tilde{u}_1$. Since $\sum\limits_{i=1}^{m} u_i \tilde{g}_i = \sum\limits_{i=1}^{m} \tilde{u}_i \tilde{g}_i$, then also $(u_1 - \tilde{u}_1)\tilde{g}_1 = \sum\limits_{i=2}^{m} (\tilde{u}_i - u_i)\tilde{g}_i$. Note that g_1 divides $\sum\limits_{i=2}^{m} (\tilde{u}_i - u_i)\tilde{g}_i$ as $\tilde{g}_2, \ldots, \tilde{g}_m$ are divisible by g. Consequently, $g_1 \mid (u_1 - \tilde{u}_1)\tilde{g}_1$. However, g_1 and $\tilde{g}_1$ are coprime, so g_1 must divide $(u_1 - \tilde{u}_1)$. Deduce that $u_1 - \tilde{u}_1 = 0$ as $\deg(u_1 - \tilde{u}_1) < \deg g_1$.

□

The constructive approaches from the last two proofs can be easily converted into algorithms. The same may be said about the construction, which we present in the proof of the theorem below known as Hensel's lemma. So, the question of how to find a basic irreducible polynomial over $\mathbb{Z}_{p^n}$ is answered. Moreover, it provides the means to produce even basic primitive polynomials.

Theorem 8 (Hensel's lemma)**.** Let $f \in \mathbb{Z}[x]$ be monic and $g_1, \dots, g_m \in \mathbb{Z}_p[x]$ be pairwise coprime monic polynomials satisfying $f \equiv \prod_{i=1}^{m} g_i \pmod{p}$. For every $k \in \mathbb{N}$, polynomials $g_1^{(k)}, \dots, g_m^{(k)} \in \mathbb{Z}_{p^k}[x]$ exist, which meet the conditions:

1. $f \equiv \prod_{i=1}^{m} g_i^{(k)} \pmod{p^k}$,
2. $\forall 1 \leq i \leq m : g_i^{(k)} \equiv g_i \pmod{p}$,
3. $\forall 1 \leq i \leq m : \operatorname{lc}\left(g_i^{(k)}\right) = 1$.

Proof. Choose $k \in \mathbb{N}$ and define the sets $K = \{1, \dots, k\}$ and $M = \{1, \dots, m\}$. Denote $\tilde{g}_i = \prod_{\substack{j=1 \\ j \neq i}}^{m} g_j$ and $g_i^{(1)} = g_i$ for every $i \in M$. The plan is to use **Lemma 7** iteratively for $j \in K$ to construct $g_1^{(j)}, \dots, g_m^{(j)} \in \mathbb{Z}_{p^j}[x]$ meeting the conditions. Notice that the case $j = 1$ follows from the hypothesis. Assume that we already have $g_1^{(j)}, \dots, g_m^{(j)} \in \mathbb{Z}_{p^j}[x]$ fulfilling the conditions 1.-3. for some $j \in K, j < k$. Define $d = \mu\left(\left(f - \prod_{i=1}^{m} g_i^{(j)}\right) / p^j\right) \in \mathbb{Z}_p[x]$ and $\tilde{g}_i{}^{(j)} = \prod_{\substack{s=1 \\ s \neq i}}^{m} g_s^{(j)}$ for each $i \in M$. Evidently, $\deg(d) < \deg(f) = \sum_{i=1}^{m} g_i$. For $d, g_1, \dots, g_m$, **Lemma 7** states that $u_1, \dots, u_m \in \mathbb{Z}_p[x]$ exist unique which satisfy $\deg(u_i) < \deg(g_i)$ for each $i \in M$, and $d = \sum_{i=1}^{m} u_i \tilde{g}_i$ in $\mathbb{Z}_p[x]$. Derived from 2., $d \equiv \sum_{i=1}^{m} u_i \tilde{g}_i \equiv \sum_{i=1}^{m} u_i \tilde{g}_i{}^{(j)} \pmod{p}$.

Set $g_i^{(j+1)} = g_i^{(j)} + p^j u_i$ for every $i \in M$. Since $p^j d = f - \prod_{i=1}^{m} g_i^{(j)} \pmod{p^{j+1}}$, then $\prod_{i=1}^{m} g_i^{(j)} = f - p^j d \pmod{p^{j+1}}$. Verify that the first condition is fulfilled

$$\begin{aligned} \prod_{i=1}^{m} g_i^{(j+1)} = \prod_{i=1}^{m} \left(g_i^{(j)} + p^j u_i\right) &\equiv \prod_{i=1}^{m} g_i^{(j)} + p^j \sum_{i=1}^{m} u_i \tilde{g}_i{}^{(j)}, \\ &\equiv f + p^j \left(\sum_{i=1}^{m} u_i \tilde{g}_i{}^{(j)} - d\right) \equiv f \pmod{p^{j+1}}. \end{aligned}$$

The second condition is clear as $g_i^{(j+1)} \equiv g_i^{(j)} \equiv g_i \pmod{p}$. Choose $i \in M$, and observe $\deg(u_i) < \deg(g_i)$, so $\operatorname{lc}\left(g_i^{(j+1)}\right) = \operatorname{lc}\left(g_i^{(j)}\right) = \operatorname{lc}(g_i) = 1$.

□

Corollary 9. Let $r \in \mathbb{N}$. Then, a monic basis primitive polynomial in $\mathbb{Z}_{p^n}[x]$ of degree r, which divides $x^{p^r-1} - 1$, exists.

Proof. Denote $k = p^r - 1$. From finite fields construction, we know there exists a monic irreducible polynomial $f_p \in \mathbb{Z}_p[x]$ of degree r which divides $(x^k - 1)$.

Thus, f is primitive. Since $(x^k-1)' = k \cdot x^{k-1} = -x^{p^r-2}$ in $\mathbb{Z}_p[x]$, it cannot have multiple roots. Set $g_p(x) = \frac{x^k-1}{f_p} \in \mathbb{Z}_p[x]$, which seems to be monic and coprime with f_p. **Theorem 8** yields monic polynomials $f, g \in \mathbb{Z}_{p^n}[x]$ such that $\mu(f) = f_p$, $\mu(g) = g_p$ and $(x^k-1) = f(x)g(x)$ in $\mathbb{Z}_{p^n}[x]$. Hence, f is monic basic primitive.

□

We reformulate the constructions from the proofs of **Lemma 6, Lemma 7** and **Theorem 8** to algorithms. Remark that EEA on input $g, h \in \mathbb{Z}_p[x]$ outputs the tuple $(a, b, d) \in \mathbb{Z}_p[x]^3$ such that $\gcd(g, h) = a \cdot g + b \cdot h$.

Algorithm 1 Linear combination of two coprime polynomials

```
Require: $p$ prime, $f, g, h \in \mathbb{Z}_p[x] \setminus \{0\}, \deg(f) < \deg(g) + \deg(h)$, $\gcd(g, h) = 1$
Ensure: $u, v \in \mathbb{Z}_p[x], \deg(u) < \deg(h), \deg(v) < \deg(g) : f = u \cdot g + v \cdot h$
  $(u_0, v_0, g) \leftarrow \mathrm{EEA}(g, h)$
  $u \leftarrow (u_0 \cdot f) \bmod h$; $q \leftarrow (u_0 \cdot f)$ div $h$; $v \leftarrow q \cdot g + v_0 \cdot f$
  return $(u, v)$
```

Algorithm 2 Linear combination of multiple coprime polynomials

```
Require: $p$ prime, $m \in \mathbb{N}$, $f, g_1, \ldots, g_m \in \mathbb{Z}_p[x] \setminus \{0\}, \deg(f) < \sum_{i=1}^{m} \deg(g_i)$
  and $\forall i, j \in \mathbb{N}, i < j \leq m : \gcd(g_i, g_j) = 1$
Ensure: $u_1, \ldots, u_m \in \mathbb{Z}_p[x], \forall i \in \mathbb{N}, i \leq m : \deg(u_i) < \deg(g_i)$, $f = \sum_{i=1}^{m} u_i \prod_{\substack{j=1 \\ j \neq i}}^{m} g_j$
  $d_0 \leftarrow f$; $g_0^* \leftarrow \prod_{i=1}^{m} g_i$; $i \leftarrow 1$
  while $i \leq m$ do
    $g_i^* \leftarrow g_{i-1}^*$ div $g_i$
    $(d_i, u_i) \leftarrow$ Algorithm 1$(p, d_{i-1}, g_i, g_i^*)$; $i \leftarrow i + 1$
  end while
  return $(u_1, \ldots, u_m)$
```

Algorithm 3 Hensel's lift

```
Require: $p$ prime, $m, k \in \mathbb{N}$, $f \in \mathbb{Z}[x]$ monic, $g_1, \ldots, g_m \in \mathbb{Z}_p[x]$ monic, $\forall i, j \in \mathbb{N}$,
  $i < j \leq m : \gcd(g_i, g_j) = 1$ and $f \equiv \prod_{i=1}^{m} g_i \pmod{p}$
Ensure: $g_1^{(k)}, \ldots, g_m^{(k)} \in \mathbb{Z}_{p^k}[x]$ monic, $\forall i, j \in \mathbb{N}$, $i < j \leq m : g_i^{(k)} \equiv g_i \pmod{p}$
  and $f \equiv \prod_{i=1}^{m} g_i^{(k)} \pmod{p^k}$
  $i \leftarrow 1$; $j \leftarrow 1$
  while $i \leq m$ do
    $g_i^{(1)} \leftarrow g_i$; $i \leftarrow i + 1$
  end while
  while $j < k$ do
    $d \leftarrow \left(\left(f - \prod_{i=1}^{m} g_i^j\right) \text{ div } p^j\right) \bmod p^{j+1}$, $i \leftarrow 1$
    $(u_1, \ldots, u_m) \leftarrow$ Algorithm 2$(p, m, d, g_1, \ldots, g_m)$
    while $i \leq m$ do
      $g_i^{(j+1)} \leftarrow g_i^{(j)} + p^j u_i$; $i \leftarrow i + 1$
    end while
    $j \leftarrow j + 1$
  end while
  return $\left(g_1^{(k)}, \ldots, g_m^{(k)}\right)$
```

1.2 The Construction of Galois Rings

Due to **Corollary 9**, it is possible to determine an induced ring epimorphism $\tilde{\mu}$ of quotient rings $\mathbb{Z}_{p^n}[x]/_I$ and $\mathbb{Z}_p[x]/_J$ for $I \leq \mathbb{Z}_{p^n}[x]$ and $J \leq \mathbb{Z}_p[x]$. Firstly, recall the ring epimorphisms:

$$\phi : \mathbb{Z}_{p^n} \longrightarrow \mathbb{Z}_p, \qquad a \mapsto a \mod p, \tag{1.1}$$

$$\mu : \mathbb{Z}_{p^n}[x] \longrightarrow \mathbb{Z}_p[x], \sum_{i=0}^{m} a_i x^i \mapsto \sum_{i=0}^{m} \phi(a_i) x^i, \tag{1.2}$$

Now, consider a monic basic irreducible polynomial $G_{p,r} \in \mathbb{Z}_{p^n}[x]$ of degree r such that it divides $x^k - 1$ in $\mathbb{Z}_{p^n}[x]$ for $k = p^r - 1$. The existence of such $G_{p,r}$ follows from **Corollary 9**. Denote $g_{p,r}(x) = \mu(G_{p,r}(x)) \in \mathbb{Z}_p[x]$. Clearly, $g_{p,r}$ is a monic primitive polynomial of degree r dividing $x^k - 1$ in $\mathbb{Z}_p[x]$. We can define

$$\tilde{\mu} : \mathbb{Z}_{p^n}[x]/_{(G_{p,r})} \longrightarrow \mathbb{Z}_p[x]/_{(g_{p,r})} \simeq \mathbb{F}_{p^r},\ f + (G_{p,r}) \mapsto \mu(f) + (g_{p,r}). \tag{1.3}$$

Elements of the quotient ring $\mathbb{Z}_{p^n}[x]/_{(G_{p,r})}$ are of the form $\sum_{i=0}^{r-1} a_i x^i + (G_{p,r})$, where $a_0, \ldots, a_{r-1} \mathbb{Z}_{p^n}$, so there is $(p^n)^r = p^{nr}$ of them. The next step is to verify that $\tilde{\mu}$ is a well-defined homomorphism of rings with the kernel $(p + (G_{p,r}))$.

Choose $f, g \in \mathbb{Z}_{p^n}[x]$, then

$$\begin{aligned} \tilde{\mu}(f + (G_{p,r})) \circ \tilde{\mu}(g + (G_{p,r})) &= (\mu(f) + (g_{p,r})) \circ (\mu(g) + (g_{p,r})) \\ &= \mu(f) \circ \mu(g) + (g_{p,r}) = \mu(f \circ g) + (g_{p,r}) \\ &= \tilde{\mu}(f \circ g + G_{p,r}), \text{ where } \circ \in \{+, \cdot\}. \end{aligned}$$

Now, consider $\bar{f}, \bar{g} \in \mathbb{Z}_p[x]$. As stated by **Theorem 8**, there are $f, g \in \mathbb{Z}_{p^n}[x]$ fulfilling $\mu(f) = \bar{f}$ and $\mu(g) = \bar{g}$. Subsequently, we have $\tilde{\mu}(f + (G_{p,r})) = \bar{f} + (g_{p,r})$ and $\tilde{\mu}(g + (G_{p,r})) = \bar{g} + (g_{p,r})$. Moreover, if $\bar{f} \not\equiv \bar{g} \pmod{g_{p,r}}$ then, inevitably, $f \not\equiv g \pmod{p, G_{p,r}}$, which implies $f \not\equiv g \pmod{G_{p,r}}$. It results in $\tilde{\mu}$ being a well-defined ring epimorhism. Compute the kernel of $\tilde{\mu}$:

$$\begin{aligned} f \in \ker(\tilde{\mu}) &\iff \tilde{\mu}(f + (G_{p,r})) = (g_{p,r}) \iff (\mu(f) = 0 \lor \mu(f) \in (g_{p,r})) \\ &\iff (f \in (p) \lor f \in (G_{p,r})) \iff f \in (p + (G_{p,r})), \end{aligned}$$

which means $\ker(\tilde{\mu}) = (p + (G_{p,r}))$. Utilising the first isomorphism theorem,

$$\left(\mathbb{Z}_{p^n}[x]/_{(G_{p,r})}\right)/_{(p + (G_{p,r}))} \simeq \mathbb{F}_{p^r}. \tag{1.4}$$

This give us $M = (p + (G_{p,r}))$ is a maximal ideal of $\mathbb{Z}_{p^n}[x]/_{(G_{p,r})}$, which consists of all nilpotent elements. Based on **Claim 1**, the set of all nilpotents of a finite commutative ring composes an ideal, which is unique provided it is maximal. Therefore, $\left(\mathbb{Z}_{p^n}[x]/_{(G_{p,r})}, M\right)$ is a local ring.

Define $\xi = x + (G_{p,r})$ and $\mathbf{R} = \mathbb{Z}_{p^n}[x]/_{(G_{p,r})}$. Then, $\xi \in \mathbf{R}$ and it is a root of the polynomial $G_{p,r}$ over $\mathbf{R}$, because $G_{p,r}(\xi) = G_{p,r}(x) + (G_{p,r}) = (G_{p,r})$, and the evaluation map is a polynomial ring homomorphism. It is clear that $\mathbf{R} = \mathbb{Z}_{p^n}[\xi]$, and, for arbitrary $f \in \mathbb{Z}_{p^n}[x]$, there exist unique $z_0, \dots, z_{r-1} \in \mathbb{Z}_{p^n}$ such that $f + (G_{p,r}) = \sum\limits_{i=0}^{r-1} z_i \xi^i$.

Denote by α the projection $\tilde{\mu}(\xi)$, then considering the construction, α must be a primitive root of $g_{p,r} = \mu(G_{p,r}) \in \mathbb{Z}_p[x]$. Based on the fact that α is of order $k = p^r - 1$, we show ξ is also of order k. Denote by l the order of ξ. Since ξ is the root of $G_{p,r}$, which divides $(x^k - 1)$, it is apparent that $\xi^k - 1 = 0$ and $l \mid k$. If $l < k$ then $1 = \tilde{\mu}(1) = \tilde{\mu}\left(\xi^l\right) = \tilde{\mu}(\xi)^l = \alpha^l$, which contradicts the order of α is k. Thence, $l = k$.

Now, the definition (1.3) can be expressed in a more understandable and still equivalent form:

$$\tilde{\mu} : \mathbb{Z}_{p^n}[\xi] \longrightarrow {}^{\mathbb{Z}_p[x]}\!\big/_{(g_{p,r})} = \mathbb{Z}_p[\alpha], \ \sum_{i=0}^{r-1} z_i \xi^i \mapsto \sum_{i=0}^{r-1} \phi(z_i) \alpha^i \tag{1.5}$$

Remark. Let $\mathbf{R} = {}^{\mathbb{Z}_{p^n}[x]}\!\big/_{(G_{p,r})}$. Then,

- $\tilde{\mu}$ defined as in (1.5) is a ring epimorphism with the kernel $p\mathbf{R}$,
- $\mathbf{R}$ is a commutative ring of characteristic p^n and cardinality $(p^n)^r = p^{nr}$,
- $\mathbf{R}^* = \mathbf{R} \setminus p\mathbf{R}$, and $p\mathbf{R}$ is the unique maximal ideal of $\mathbf{R}$ containing all nilpotent elements of $\mathbf{R}$,
- $(\mathbf{R}, p\mathbf{R})$ is a local ring with the residue field ${}^{\mathbf{R}}\!\big/_{p\mathbf{R}} \simeq \mathbb{F}_{p^r}$,
- There exists an element ξ of order $k = p^r - 1$ in $\mathbf{R}$.

The following theorem, which proof is beyond the scope of this thesis, is crucial to justify the consecutive definition. Readers can find more about the Galois theory for local rings in Bini and Flamini's work [7].

Theorem 10. [7, Theorem 5.1.8] Let f, $g \in \mathbb{Z}_{p^n}[x]$ be monic basic irreducible polynomials of degree r. Then, ${}^{\mathbb{Z}_{p^n}[x]}\!\big/_{(f)} \simeq {}^{\mathbb{Z}_{p^n}[x]}\!\big/_{(g)}$.

Definition 11. Let $r \in \mathbb{N}$. The finite, commutative, local ring of cardinality $(p^n)^r$ and characteristic p^n is called the *Galois ring* $\mathrm{GR}(p^n, r)$. The *additive representation* of any element $z \in \mathrm{GR}(p^n, r)$ is $z = \sum\limits_{i=0}^{r-1} z_i \xi^i$, where $\xi \in \mathrm{GR}(p^n, r)$ has order $p^r - 1$ and $z_0, \dots, z_{r-1} \in \mathbb{Z}_{p^n}$.

Example 3. Trivial cases:

- $\mathrm{GR}(p^1, r) = {}^{\mathbb{Z}_p[x]}\!\big/_{(g_{p,r})} \simeq \mathbb{F}_{p^r}$, where $g_{p,r} \in \mathbb{Z}_p[x]$ is the minimal polynomial of some primitive $\alpha \in \mathbb{F}_{p^r}$,
- $\mathrm{GR}(p^n, 1) = {}^{\mathbb{Z}_{p^n}[x]}\!\big/_{(x - \alpha)} \simeq \mathbb{Z}_{p^n}$ for some $\alpha \in \mathbb{Z}_{p^n}$.

1.3 The Structure of Galois Rings

In the previous section, the construction of the Galois ring $\mathrm{GR}(p^n, r)$ was shown together with the additive representation of its elements. Now, it is vital to look closer at the structure of the Galois rings and their ideals. The primary idea is to determine when p and its powers divide $a \in \mathrm{GR}(p^n, r)$. Division by prime p is meant in a formal sense as p is not invertible, i.e. p divides a, denoted by $p \mid a$, provided $b \in \mathrm{GR}(p^n, r)$ exists such that $a = p \cdot b$.

Definition 12. $\mathbf{R}$ is called *chain ring* if $\mathbf{R}$ is a principal ideal ring, which is local.

Claim 13. Let $\mathrm{GR}(p^n, r)$ be a Galois ring. Then, for any ideal I of $\mathrm{GR}(p^n, r)$, a non-negative integer j exists satisfying $j \leq n$ and $I = (p^j)$. Thus, $\mathrm{GR}(p^n, r)$ is a principal ideal ring.

Proof. Firstly, recall that $\mathbb{Z}$ is a Noetherian ring since it is the principal ideal domain. Then $\mathbb{Z}_{p^n} \simeq {}^{\mathbb{Z}}\!/_{(p^n)}$, $\mathbb{Z}_{p^n}[x]$ and ${}^{\mathbb{Z}_{p^n}[x]}\!/_{(G_{p,r})}$, where $G_{p,r} \in \mathbb{Z}_{p^n}[x]$ basic irreducible, are Noetherian too. Properties of Noetherian rings are described in the publication by Grove [8].

Secondly, we show that $\mathbf{R} = \mathrm{GR}(p^n, r)$ is uniserial. Consider I, J ideals of $\mathbf{R}$ such that $I \not\subseteq J$, $J \not\subseteq I$ and choose $i \in I, j \in J$. Then $i, j \notin \mathbf{R}^*$, because if $i \in \mathbf{R}^*$ then $J \subseteq I = \mathbf{R}$, and symmetrically $I \subseteq \mathbf{R} = J$, if $j \in \mathbf{R}^*$. As a result, i, j are nilpotents, so $i, j \in (p)$, and one may find exponents $e_i, e_j \in \mathbb{N}$ and elements $a, b \in \mathbf{R} \setminus p\mathbf{R} = \mathbf{R}^*$ such that $i = ap^{e_i}$ and $j = bp^{e_j}$. Suppose, WLOG, that $e_i \geq e_j$. Then, $i = ap^{e_i} = ap^{e_i - e_j} b^{-1} \cdot bp^{e_j} \in J$ as $bp^{e_j} = j \in J$, and therefore, $I \subseteq J$, a contradiction.

Let I be an ideal of $\mathbf{R}$. If $(p) \subset I$ then $I = (1) = (p^0)$ as (p) is the maximal ideal. Assume that $I \subseteq (p)$. There must exist elements $a_1, \ldots, a_l \in \mathbf{R}$ such that $I = (a_1, \ldots, a_l)$, because $\mathbf{R}$ is Noetherian. Moreover, it is possible to find an positive integer $i, i \leq l$, which satisfies $(a_j) \subseteq (a_i)$ for each $j = 1, \ldots, l$ since $\mathbf{R}$ is uniserial. Thence, $I = (a_i) \subseteq p\mathbf{R}$, which is equivalent with that p divides a_i. As a result, $a_i = z \cdot p^j$ for appropriate $j \in \mathbb{N}$ and $z \in \mathbf{R}^*$.

□

Corollary 14. A Galois ring $\mathrm{GR}(p^n, r)$ is a chain ring.

We proved that $(0) \subset (p^n) \subset (p^{n-1}) \subset \cdots \subset (p) \subset (p^0) = (1)$ are the only ideals of $\mathrm{GR}(p^n, r)$. Observe that x can be expressed as $x = y_i + \cdots + y_{n-1}$ provided $x \in (p^i)$, where $y_j \in (p^j)$, $j = i, \ldots, n-1$. Let us now formalise this representation of the Galois ring's elements using powers of p.

Theorem 15. Let $k = p^r - 1$, $\mathbf{R} = \mathrm{GR}(p^n, r)$ be a Galois ring and $\xi \in \mathbf{R}$ have order k. The unique monic basic primitive polynomial $G_{p,r} \in \mathbb{Z}_{p^n}[x]$ of degree r exists which divides $(x^k - 1)$ in $\mathbb{Z}_{p^n}[x]$ and has a root ξ. Moreover, the ring $\mathbf{R} = \mathbb{Z}_{p^n}[\xi] = {}^{\mathbb{Z}_{p^n}[x]}\!/_{(G_{p,r})}$, and any $z \in \mathbf{R}$ has the unique *p-adic representation*

$$z = \sum_{i=0}^{n-1} z_i p^i, \text{ where } z_0, \ldots, z_{n-1} \in \{0\} \cup \{\xi^i \mid i = 0, 1, \ldots, k-1\}. \tag{1.6}$$

Furthermore, $z \in \mathbf{R}^*$ if and only if $z_0 \neq 0$, and z is 0 or a zero divisor otherwise.

Proof. Let us start with the uniqueness of the polynomial $G_{p,r}$ as its existence follows from **Corollary 9** and the existence of element ξ of order $k = p^r - 1$ from the remark above **Theorem 10**. Assume that $G_{p,r}, \tilde{G}_{p,r} \in \mathbb{Z}_{p^n}[x]$ exist and meet the given conditions. Then, $\gcd_{\mathbb{Z}_{p^n}[x]}(G_{p,r}, \tilde{G}_{p,r}) \neq 1$ as both share the same root ξ. Since both $G_{p,r}, \tilde{G}_{p,r}$ are irreducible and have the same degree, one can be rewritten using the other as $G_{p,r} = a \cdot \tilde{G}_{p,r}$, where $a \in \mathbb{Z}_{p^n}$. Since both are monic, $a = 1$.

Define $S = \left\{ \sum\limits_{i=0}^{n-1} z_i p^i \mid z_0, \ldots, z_{n-1} \in \{0\} \cup \{\xi^i \mid 0 \leq i < k\} \right\}$ and choose some $z = \sum\limits_{i=0}^{n-1} z_i p^i \in S$. Set $y_{i,0} = z_i p^i$ and $x_{i,0} = y_{i,0} \bmod \xi$ for every integer i, $0 \leq i < r$. Recursively compute $y_{i,j} = \frac{y_{i,j-1} - x_{i,j-1}}{\xi}$ and $x_{i,j} = y_{i,j} \bmod \xi$ for $j \in \mathbb{N}$, $j < n$. Notice that every $z_i p^i \in \mathbb{Z}_{p^n}[\xi]$, and therefore, $x_{i,j} \in \mathbb{Z}_{p^n}$ for every pair i, j as before. It can be concluded $z = \sum\limits_{j=0}^{r-1} \left(\sum\limits_{i=0}^{n-1} x_{i,j} \right) \xi^j \in \mathbb{Z}_{p^n}[\xi]$ and $S \subseteq \mathbb{Z}_{p^n}[\xi]$.

To prove the p-adic representation is now enough to show no ξ^i is divisible by p, where $i \in \mathbb{Z}, 0 \leq i < k$. As a consequence, we have $|S| = (p^r)^n = |\mathbb{Z}_{p^n}[\xi]|$ and $S = \mathbb{Z}_{p^n}[\xi]$. Assume, for a contradiction, a non-negative integer i exists such that $i < k$ and p divides ξ^i. Thus, $\xi^i = p \cdot \tilde{\xi}$ for some $\tilde{\xi} \in \mathbb{Z}_{p^n}[x]$. In this scenario, $(\xi^i)^n = p^n \tilde{\xi}^n = 0$, which contradicts that the order of ξ is k.

Denote $\mathbf{R} = \mathrm{GR}(p^n, r)$. It has been shown in **Section 1.2** that $\mathbf{R}^* = \mathbf{R} \setminus p\mathbf{R}$ and $p\mathbf{R}$ contains all nilpotent elements of $\mathbf{R}$. Now, it is apparent the element $z = \sum\limits_{i=0}^{n-1} z_i p^i$ is a unit in $\mathbf{R}$ if and only if $p \nmid z$, which can happen if and only if $z_0 \neq 0$. Hence, if $z_0 = 0$ then z is zero or a zero divisor.

□

Definition 16. Let $\xi \in \mathrm{GR}(p^n, r)$ be of order $k = p^r - 1$. The *Teichmüller set* of the Galois ring $\mathrm{GR}(p^n, r)$ is $\mathcal{T}_r = \{0\} \cup \{\xi^i \mid i = 0, \ldots, k-1\}$.

Based on the previous theorem, every power of the element ξ of order $p^r - 1$ is a unit in $\mathrm{GR}(p^n, r)$. Recall the ring epimorphism $\tilde{\mu} : \mathbb{Z}_{p^n}[\xi] \to \mathbb{Z}_p[\alpha]$ defined as $\tilde{\mu}(\xi) = \alpha$ in (1.5), where α is primitive of order $p^r - 1$. Based on the p-adic representation, it can be deduced $\tilde{\mu}$ maps the Teichmüller set $\mathcal{T}_r$ to the residue field of $\mathrm{GR}(p^n, r)$. Let us define operations $\oplus$ and $\ominus$ on $\mathcal{T}_r$ as $\xi_1 \oplus \xi_2 = \xi_3$ provided $\tilde{\mu}(\xi_1) + \tilde{\mu}(\xi_2) = \tilde{\mu}(\xi_3)$, and $\ominus \xi_1 = \xi_2$ if $-\tilde{\mu}(\xi_1) = \tilde{\mu}(\xi_2)$ for any $\xi_1, \xi_2, \xi_3 \in \mathcal{T}_r$. Then, it is an immediate result that $(\mathcal{T}_r, \oplus, \ominus, \cdot, 0, 1)$ is a finite field, and $\tilde{\mu}$ restricted to $\mathcal{T}_r$ is a field isomorphism.

Corollary 17. Let $\mathbf{R} = \mathrm{GR}(p^n, r), k = p^r - 1$, an integer $i \in \mathbb{Z}$ satisfy $0 \leq i < k$, and $c \in p\mathbf{R}$. Then

1. $p\mathbf{R} = \left\{ \sum\limits_{i=1}^{n-1} z_i p^i \mid z_1, \ldots, z_{n-1} \in \mathcal{T}_r \right\}$,
2. $|\mathbf{R}^*| = kp^{(n-1)r}$ since $\mathbf{R}^* = \langle \xi \rangle \cdot \pi$, where $\langle \xi \rangle$ is the cyclic group of order k generated by ξ and $\pi = \{1 + d \mid d \in p\mathbf{R}\}$ is a group of order $(p^r)^{n-1}$,
3. The order of ξ^i is $j \in \mathbb{N}$ which satisfies $j \mid k$, and the order of $1 + c$ is a $l \in \mathbb{N}$ fulfilling $l \mid p^{n-1}$,

4. If $z \in \mathbf{R}^*$ is of order l dividing k, then $z = \xi^j$ for $0 \leq j < k$. Specially, for $l = k$, we have $z = \xi^j$, where $1 \leq j < k$ and $\gcd(j, k) = 1$.

We commence this section by demonstrating the proposed properties of Galois rings, their additive representation and Teichmüller sets.

Example 4. Let p be an odd prime, n be a positive integer and $r = 1$. This example provides the Teichmüller set $\mathcal{T}$ of the Galois ring $\mathrm{GR}(p^n, 1) \simeq \mathbb{Z}_{p^n}$.

Consider a generator $\alpha \in \mathbb{Z}_p$ of the cyclic multiplicative group $\mathbb{Z}_p^*$. Certainly, α is of order $(p-1)$ in $\mathbb{Z}_p^*$. In this trivial situation, Hensel's lift is not necessary because $\mathbb{Z}_p \subseteq \mathbb{Z}_{p^n}$ and α also lies in $\mathbb{Z}_{p^n}$. Since $|\mathbb{Z}_{p^n}| = \varphi(p^n) = (p-1) \cdot p^{n-1}$, where φ is Euler's totient function, the order of α in $\mathbb{Z}_{p^n}^*$ needs to be $(p-1) \cdot p^e$ for some $e \in \{0, \ldots, n-1\}$.

Define $\xi = \alpha^{p^{n-1}}$. Note that $\xi^{p-1} = \left(\alpha^{p^{n-1}}\right)^{p-1} = \left(\alpha^{(p-1)p^e}\right)^{p^{n-1-e}} = 1$ and $\xi^i \neq 1$ for all $i \in \mathbb{N}, i < p$, or otherwise $1 = (\alpha^{ip^e})^{p^{n-1-e}}$, a contradiction. In conclusion, ξ is of order $(p-1)$ in $\mathbb{Z}_{p^n}$ and $\mathcal{T} = \{0\} \cup \langle \xi \rangle$.

Example 5. This example describes the Galois ring for $p = 2, n = 2$, and $r = 3$. We have to find some ξ of order $2^3 - 1 = 7$ over $\mathbb{Z}_4$. Fortunately, it is possible to choose ξ as any root of basic primitive polynomial of degree 3 in $\mathbb{Z}_{2^2}[x]$ since 7 is a prime number, e.g.

$$G_{2,3}(x) = x^3 + 3x^2 + 2x + 3 \in \mathbb{Z}_4[x] \quad \text{and} \quad \xi = x + (G_{2.3}).$$

Recall the ring epimorphisms:

$$\begin{aligned}
&\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2, && a \mapsto a \bmod 2,\\
&\mu : \mathbb{Z}_4[x] \longrightarrow \mathbb{Z}_2[x], && \sum_{i=0}^{m} a_i x^i \mapsto \sum_{i=0}^{m} \phi(a_i) x^i,\\
&\tilde{\mu} : \mathbb{Z}_4[x]/(G_{2,3}) = \mathbb{Z}_4[\xi] \longrightarrow \mathbb{Z}_2[x]/(g_{2,3}) = \mathbb{Z}_2[\alpha], && \sum_{i=0}^{2} z_i \xi^i \mapsto \sum_{i=0}^{2} \phi(z_i) \alpha^i,
\end{aligned}$$

where $g_{2,3} = \mu(G_{2,3}) = x^3 + x^2 + 1$ and $\alpha = \tilde{\mu}(\xi)$. Doubtless, $\mathbb{Z}_4[\xi] \simeq \mathrm{GR}(2^2, 3)$ and $\mathbb{Z}_2[\alpha] \simeq \mathbb{F}_8$.

Teichmüller set is $\mathcal{T}_3 = \{0, 1, \xi, \xi^2, \xi^2{+}2\xi{+}1, 3\xi^2{+}3\xi{+}1, 2\xi^2{+}3\xi{+}3, \xi^2{+}3\xi{+}2\}$ and $\tilde{\mu}(\mathcal{T}_3) = \{0, 1, \alpha, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha + 1, \alpha + 1, \alpha^2 + \alpha\} = \mathbb{Z}_2[\alpha]$. The unique maximal ideal of $\mathbb{Z}_4[\xi]$ is $2\mathbb{Z}_4[\xi] = \{a + b\xi + c\xi^2 \mid a, b, c \in \{0, 2\}\}$, which is the only non-trivial ideal of this ring.

Example 6. Let $p = 2, n = 3, r = 4$. Now, some ξ generating a cyclic group of order $2^4 - 1 = 15 = 3 \cdot 5$ has to be chosen. Thus, it is not possible to choose arbitrary ξ like in the previous example.

Consider $g_{2,4} = x^4 + x + 1 \in \mathbb{Z}_2[x]$, which is irreducible polynomial of degree 4. Moreover, $g_{2,4}$ divides $(x^{15} - 1)$ and is primitive. Compute by **Algorithm 3** (Hensel's lift) the polynomial $G_{2,4} = x^4 + 4x^3 + 6x^2 + 3x + 1 \in \mathbb{Z}_{2^3}[x]$ satisfying $G_{2,4} \equiv g_{2,4} \pmod 2$ and $G_{2,4} \mid (x^{15} - 1)$ in $\mathbb{Z}_{2^3}[x]$. Define ξ as the formal root $x + (G_{2,4})$ of $G_{2,4}$ in $\mathbb{Z}_{2^3}[x]/(G_{2,4})$, and, analogously, $\alpha = x + (g_{2,4}) \in \mathbb{Z}_2[x]/(g_{2,4})$.

Hence, we have the ring epimorphisms:

$$\begin{aligned}
&\phi : \mathbb{Z}_8 \longrightarrow \mathbb{Z}_2, && a \mapsto a \bmod 2,\\
&\mu : \mathbb{Z}_8[x] \longrightarrow \mathbb{Z}_2[x], && \sum_{i=0}^{m} a_i x^i \mapsto \sum_{i=0}^{m} \phi(a_i) x^i,\\
&\tilde{\mu} : \mathbb{Z}_8[x]/(G_{2,4}) = \mathbb{Z}_8[\xi] \longrightarrow \mathbb{Z}_2[x]/(g_{2,4}) = \mathbb{Z}_2[\alpha], && \sum_{i=0}^{3} z_i \xi^i \mapsto \sum_{i=0}^{3} \phi(z_i) \alpha^i.
\end{aligned}$$

In this scenario, $\mathbb{Z}_8[\xi] \simeq \mathrm{GR}(2^3, 4)$ and $\mathbb{Z}_2[\alpha] \simeq \mathbb{F}_{16}$.

Now, the Teichmüller set $\mathcal{T}_4 = \{0\} \cup \{\xi^i\}_{i=0}^{14}$ has 16 elements. Remark that any element of $\mathbb{Z}_8[\xi]$ can be expressed as $\sum_{i=0}^{3} z_i \xi^i \mapsto z_3 z_2 z_1 z_0$. Thus,

$$\mathcal{T}_4 = \begin{Bmatrix} 0000, & 0001, & 0010, & 0100, & 1000, & 4257, & 2534, & 5766, \\ 3073, & 4525, & 5214, & 6353, & 3112, & 5715, & 3363, & 7425 \end{Bmatrix},$$

$$\tilde{\mu}(\mathcal{T}_4) = \begin{Bmatrix} 0000, & 0001, & 0010, & 0100, & 1000, & 0011, & 0110, & 1100, \\ 1011, & 0101, & 1010, & 0111, & 1110, & 1111, & 1101, & 1001 \end{Bmatrix} \simeq \mathbb{F}_{16}.$$

Finally, non-trivial ideals of $\mathbb{Z}_8[\xi]$ are:

$$(2) = \left\{ \sum_{i=0}^{3} z_i \xi^i \mid z_0, \ldots, z_3 \in \{0, 2, 4, 6\} \right\} = \{z_3 z_2 z_1 z_0 \mid z_0, \ldots, z_3 \in \{0, 2, 4, 6\}\},$$

$$\left(2^2\right) = (4) = \left\{ \sum_{i=0}^{3} z_i \xi^i \mid z_0, \ldots, z_3 \in \{0, 4\} \right\} = \{z_3 z_2 z_1 z_0 \mid z_0, \ldots, z_3 \in \{0, 4\}\}.$$

Therefore, $(0) \leq (4) \leq (2) \leq \mathbb{Z}_8[\xi]$ and (2) is the maximal ideal.

1.4 Automorphisms of Galois Rings

Let $\mathbb{F}_p \leq \mathbb{F}_{p^m}$ be an extension of finite fields of degree $m \in \mathbb{N}$. Recall the Galois group of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ is $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$ consisting of all $\mathbb{F}_p$-automorphisms of $\mathbb{F}_{p^m}$ with respect to the composition of maps. It is well known fact of finite field theory that the Frobenius automorphism $\sigma : \mathbb{F}_{p^m} \longrightarrow \mathbb{F}_{p^m}$ defined as $\sigma(a) = a^p$ for $a \in \mathbb{F}_{p^m}$ generates $\mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$. Let us begin by presenting a generalisation of the Frobenius automorphism. In this section, we refer to Chapter 14.6 of Wan's work [9].

Theorem 18. Let $\mathcal{T}_r = \{0\} \cup \langle \xi \rangle$ be the Teichüller set of $\mathrm{GR}(p^n, r)$ for $r \in \mathbb{N}$. Define a map

$$\tau : \mathrm{GR}(p^n, r) \longrightarrow \mathrm{GR}(p^n, r), \quad \sum_{i=0}^{r-1} a_i \xi^i \mapsto \sum_{i=0}^{r-1} a_i \xi^{pi}. \tag{1.7}$$

Then, τ is a $\mathbb{Z}_{p^n}$-automorfphism of $\mathrm{GR}(p^n, r)$ called *the generalised Frobenius automorphism.*

Proof. Choose $a_0, \dots, a_{r-1}, b_0, \dots, b_{r-1} \in \mathbb{Z}_{p^n}$. Then

$$\begin{aligned}
\tau\left(\sum_{i=0}^{r-1} a_i\xi^i\right) + \tau\left(\sum_{i=0}^{r-1} b_i\xi^i\right) &= \sum_{i=0}^{r-1} a_i\xi^{pi} + \sum_{i=0}^{r-1} b_i\xi^{pi} = \sum_{i=0}^{r-1}(a_i+b_i)\xi^{pi} \\
&= \tau\left(\sum_{i=0}^{r-1}(a_i+b_i)\xi^i\right) = \tau\left(\sum_{i=0}^{r-1} a_i\xi^i + \sum_{i=0}^{r-1} b_i\xi^i\right), \\
\tau\left(\sum_{i=0}^{r-1} a_i\xi^i\right) \cdot \tau\left(\sum_{i=0}^{r-1} b_i\xi^i\right) &= \sum_{i=0}^{r-1} a_i\xi^{pi} \cdot \sum_{i=0}^{r-1} b_i\xi^{pi} = \sum_{k=0}^{r-1} \sum_{\substack{0\le i,j<r \\ (i+j) \bmod r = k}} a_ib_j\xi^{pk} \\
&= \tau\Bigg(\sum_{k=0}^{r-1} \sum_{\substack{0\le i,j<r \\ (i+j) \bmod r = k}} a_ib_j\xi^{k}\Bigg) = \tau\left(\sum_{i=0}^{r-1} a_i\xi^i \cdot \sum_{i=0}^{r-1} b_i\xi^i\right), \\
\tau(a) = a \quad \forall a \in \mathbb{Z}_{p^n}.
\end{aligned}$$

Thus, τ is a non-zero endomorphism fixing the subring $\mathbb{Z}_{p^n}$ of $\mathrm{GR}(p^n, r)$. For all i, $0 \le i < r$, we have $\xi^{pi} \neq 0$, so it can be deduced the kernel of τ is trivial, and τ is injective. Consequently, τ is the ring automorphism.

□

Choose ζ from the Teichmüller set $\mathcal{T}_r$. Then $\tau(\zeta) = \zeta^p$, and the generalised Frobenius automorphism τ acts on $\mathcal{T}_r$ identical to the Frobenius automorphism σ on $\mathbb{F}_{p^r}$. However, it should not be surprising since $\mathcal{T}_r \simeq \mathbb{F}_{p^r}$. Being equipped with the generalised Frobenius automorphism, the next step is to introduce Galois groups over Galois rings.

Definition 19. Let $\mathbf{R}$ be a Galois ring $\mathrm{GR}(p^n, r)$ and $\mathbf{S}$ be a subring of $\mathbf{R}$. The *Galois group* of $\mathbf{R}$ over $\mathbf{S}$, denoted by $\mathrm{Gal}(\mathbf{R}/\mathbf{S})$, is the group consisting of all $\mathbf{S}$-automorphisms of $\mathbf{R}$ with the operation composition of maps.

Recall the ring epimorphism $\tilde{\mu} : \mathrm{GR}(p^n, r) \to \mathbb{K}, a \mapsto a + (p)$ defined in (1.5), where $\mathbb{K} \simeq \mathbb{F}_{p^r}$ is the residue field of $\mathrm{GR}(p^n, r)$. The symbol $^-$ is written over an argument instead of $\tilde{\mu}$ for brevity from now on, i.e. $\overline{a} = \tilde{\mu}(a)$ for any $a \in \mathrm{GR}(p^n, r)$. The relation between the Galois groups $\mathrm{Gal}(\mathrm{GR}(p^n, r)/\mathbb{Z}_{p^n})$ and $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_p)$ can be established after verifying that the composition of $^-$ with any ring automorphism of $\mathrm{GR}(p^n, r)$, which fixes $\mathbb{Z}_{p^n}$, is well-defined.

Lemma 20. Let $\omega \in \mathrm{Gal}(\mathrm{GR}(p^n, r)/\mathbb{Z}_{p^n})$. Define a map

$$\bar{\omega} : \overline{\mathrm{GR}(p^n, r)} \longrightarrow \overline{\mathrm{GR}(p^n, r)}, \quad a \mapsto \overline{\omega(A)}, \tag{1.8}$$

where $A \in \mathrm{GR}(p^n, r)$ satisfies $\overline{A} = a$. Then, $\bar{\omega}$ is a well-defined $\mathbb{F}_p$-automorphism of the residue field.

Proof. Consider $A, B, C, D \in \mathrm{GR}(p^n, r)$ such that $A = B + pC$. Denote $a = \overline{A}, b = \overline{B}$ and $d = \overline{D}$. For these elements,

$$\begin{aligned}
\bar{\omega}(a) &= \overline{\omega(A)} = \overline{\omega(B) + \omega(pC)} = \overline{\omega(B)} + \overline{\omega(pC)} = \bar{\omega}(b) + \overline{p \cdot \omega(C)} = \bar{\omega}(b), \\
\bar{\omega}(a + d) &= \overline{\omega(A + D)} = \overline{\omega(A) + \omega(D)} = \overline{\omega(A)} + \overline{\omega(D)} = \bar{\omega}(a) + \bar{\omega}(d), \\
\bar{\omega}(a \cdot d) &= \overline{\omega(A \cdot D)} = \overline{\omega(A) \cdot \omega(D)} = \overline{\omega(A)} \cdot \overline{\omega(D)} = \bar{\omega}(a) \cdot \bar{\omega}(d),
\end{aligned}$$

so $\bar{\omega}$ is a well-defined endomorphism.

If $0 = \bar{\omega}(a) = \overline{\omega(A)}$, then $\omega(A) = p \cdot E$ for $E \in \mathrm{GR}(p^n, r)$. Furthermore, $\omega(A^n) = \omega(A)^n = 0$, which means $A^n = 0$. It directly follows that $A \in p\mathrm{GR}(p^n, r)$ and $a = \overline{A} = 0$, so $\ker(\bar{\omega}) = \{0\}$. Now, $\bar{\omega}$ is the injective endomorphism, and therefore, an automorphism of $\overline{\mathrm{GR}(p^n, r)}$. Finally, observe that for every $A \in \mathbb{Z}_{p^n}$ and $a = \overline{A}$, we have $\bar{\omega}(a) = \overline{\omega(A)} = \overline{A} = a$.

□

Finally, the promised relation between the Galois groups over Galois rings and finite fields can be figured. We state the connection between the generalised and the classical Frobenius automorphism of $\mathrm{GR}(p^n, r)$ and $\overline{\mathrm{GR}(p^n, r)} \simeq \mathbb{F}_{p^r}$ respectively, from which the relation will become clear.

Theorem 21. Let τ be the generalised Frobenius automorphism of $\mathrm{GR}(p^n, r)$. Then, $\bar{\tau} = \sigma$ is the Frobenius automorphism of $\overline{\mathrm{GR}(p^n, r)} \simeq \mathbb{F}_{p^r}$, and τ generates the Galois group $\mathrm{Gal}(\mathrm{GR}(p^n, r)/\mathbb{Z}_{p^n})$.

Proof. Let $\mathbb{K}$ be the residue field $\overline{\mathrm{GR}(p^n, r)} \simeq \mathbb{F}_{p^r}$. **Lemma 20** asserts that $\bar{\tau}$ is a well-defined $\mathbb{F}_p$-automorphism of $\mathbb{K}$. Let $\xi \in \mathrm{GR}(p^n, r)$ be of order $p^r - 1$, and set $\alpha = \overline{\xi}$. Then, α is primitive in $\mathbb{K}$ and $\bar{\tau}(\alpha) = \overline{\tau(\xi)} = \overline{\xi^p} = \alpha^p = \sigma(\alpha)$. As a result, $\bar{\tau} = \sigma$ since an image of a primitive element uniquely determines a field homomorphism.

Choose $\omega \in \mathrm{Gal}(\mathrm{GR}(p^n, r)/\mathbb{Z}_{p^n})$. Note that a field automorphism must map a primitive element to another primitive element, or otherwise it is not bijective. Combining this argument with **Corollary 17**, $\omega(\xi) = \xi^i$ for some i such that $0 \leq i < p^r - 1$ and $\gcd(i, p^r - 1) = 1$. It is apparent that $\bar{\omega}(\alpha) = \overline{\omega(\xi)} = \overline{\xi^i} = \alpha^i$. According to **Lemma 20**, the automorphism $\bar{\omega}$ lies in $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_p)$, so $j \in \mathbb{N}$ exists, which fulfills $\bar{\omega} = \sigma^j$ as σ generates $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_p)$. It can be concluded that $i = p^j$ and $\omega = \tau^j$, because $\alpha^i = \bar{\omega}(\alpha) = \sigma^j(\alpha) = \alpha^{p^j}$.

□

2. Codes over a Galois ring

Let $\mathbf{R}$ be a Galois ring $\mathrm{GR}(p^n, r)$ and $\mathcal{T}_r$ its Teichmüller set for some prime number p and natural numbers n and r, fixed from now on. The i^{th} coordinate of $\mathbf{x} \in \mathbf{R}^m$ will be denoted by x_i, where $i, m \in \mathbb{N}$ satisfying $i \leq m$.

2.1 Modules over Galois Rings

It is essential to introduce other important concepts before describing codes over a ring. A set M with binary operations $+ : M \times M \to M$ and $\cdot : \mathbf{R} \times M \to M$ is said to be an $\mathbf{R}$-module provided $M(+)$ is an abelian group and for each $r_1, r_2 \in \mathbf{R}$ and $\mathbf{m}_1, \mathbf{m}_2 \in M$, the ensuing properties are valid

1. $r_1 \cdot (\mathbf{m}_1 + \mathbf{m}_2) = r_1 \cdot \mathbf{m}_1 + r_2 \cdot \mathbf{m}_2$,
2. $r_1 \cdot (r_2 \cdot \mathbf{m}_1) = (r_1 \cdot r_2) \cdot \mathbf{m}_1$,
3. $(r_1 + r_2) \cdot \mathbf{m}_1 = r_1 \cdot \mathbf{m}_1 + r_2 \cdot \mathbf{m}_1$,
4. $1 \cdot \mathbf{m}_1 = \mathbf{m}_1$.

Consider a non-empty subset N of M. Then, N is a submodule of M, denoted by $N \leq M$, on the condition that N is closed under the addition and the scalar multiplication inherited from M. Let $X = \{\mathbf{x}_1, \dots, \mathbf{x}_k\}$ be a subset of M for some $k \in \mathbb{N}$ and $\langle X \rangle = \sum\limits_{i=1}^{k} \mathbf{x}_i \mathbf{R} = \{r_1 \cdot \mathbf{x}_1 + \dots + r_k \cdot \mathbf{x}_k \mid r_1, \dots, r_k \in \mathbf{R}\}$, where the operations $+$ and $\cdot$ are inherited from M. It is evident that $X \subseteq \langle X \rangle$ and $\langle X \rangle \leq M$. Furthermore, $\langle X \rangle$ is the smallest submodule of M which contains X with respect to inclusion.

Definition 22. Elements $\mathbf{x}_1, \dots, \mathbf{x}_k$ are called *generators* of an $\mathbf{R}$-module M given that k is an positive integer and $M = \sum\limits_{i=1}^{k} \mathbf{x}_i \mathbf{R}$, which will be represented by $M = \langle \mathbf{x}_1, \dots, \mathbf{x}_k \rangle$. A tuple $X = (\mathbf{x}_1, \dots, \mathbf{x}_k)$ is known as a *basis* of the module M. If X has minimal cardinality among the bases of M then X is *minimal* and k is defined to be the *rank* of M, written as $\mathrm{rank}(M)$. The minimal basis X is *free* if the following implication is valid

$$\forall \mathbf{x} \in X \, \exists z_{\mathbf{x}} \in \mathbf{R} : \sum_{\mathbf{x} \in X} z_{\mathbf{x}} \cdot \mathbf{x} = \mathbf{o} \implies \forall \mathbf{x} \in X : z_{\mathbf{x}} = 0. \tag{2.1}$$

Finally, an $\mathbf{R}$-module, for which exists an free basis, is *free.*

Example 7. A module $\mathbf{R}^k$ is free for every $k \in \mathbb{N}$. On contrary, $(p^i\mathbf{R})^k$ is not free for every $i, k \in \mathbb{N}$.

Definition 23. The *Kronecker delta* is a function $\delta_{ij} : \mathbb{N} \times \mathbb{N} \to \{0, 1\} \subseteq \mathbf{R}$ defined as $\delta_{ii} = 1$ and $\delta_{ij} = 0$ for each $i, j \in \mathbb{N}$ which differs. The *standard basis* of an module $\mathbf{R}^k$ is $(\boldsymbol{\delta}_1, \dots, \boldsymbol{\delta}_k)$, where $k \in \mathbb{N}$ and $\boldsymbol{\delta}_i = (\delta_{i1}, \dots, \delta_{ik})$ for every $i \in \mathbb{N}$ non-greater than k.

Let N be a submodule of M. Then, the submodule N defines an equivalence $\sim_N$ on M by the rule $\mathbf{x} \sim_N \mathbf{y}$ if and only if $(\mathbf{x} - \mathbf{y}) \in N$. The set of equivalence classes of $\sim_N$ with operations $+, \cdot$ specified for every $r \in \mathbf{R}$ and elements $\mathbf{x}, \mathbf{y} \in M$ as $(\mathbf{x}+N)+(\mathbf{y}+N) = (\mathbf{x}+\mathbf{y})+N$ and $r\cdot(\mathbf{x}+N) = (r\cdot\mathbf{x})+N$ forms an $\mathbf{R}$-module called a factor (or quotient) module, represented by ${}^{M}\!/\!{}_{N}$.

Mappings between modules preserving operations play a substantial role. More precisely, let M and N be modules over $\mathbf{R}$ and a map φ from M to N satisfy $\varphi(r \cdot \mathbf{x} + s \cdot \mathbf{y}) = r \cdot \varphi(\mathbf{x}) + s \cdot \varphi(\mathbf{y})$ for all $r, s \in \mathbf{R}$, $\mathbf{x}, \mathbf{y} \in M$. Then, φ is called a module homomorphism, especially a monomorphism if injective, an epimorphism if surjective, or an isomorphism if bijective. The kernel of φ is $\ker(\varphi) = \{\mathbf{x} \in M \mid \varphi(\mathbf{x}) = \mathbf{o}\}$ and the image of φ is $\mathrm{Im}(\varphi) = \{\varphi(\mathbf{x}) \mid \mathbf{x} \in M\}$. The fundamental properties of every module homomorphism are summarized in the remark below, which proof is omitted as it basically copies the group version.

Remark. Let M and N be two $\mathbf{R}$-modules and $\varphi : M \longrightarrow N$ a homomorhism between them.

1. φ is fully determined by images of basis elements.
2. $\ker(\varphi)$ is a submodule of M and $\mathrm{Im}(\varphi)$ is a submodule of N.
3. φ is injective if and only if its kernel is trivial.
4. $\tilde{\varphi} : {}^{M}\!/\!{}_{\ker(\varphi)} \to N, \mathbf{x} + \ker(\varphi) \mapsto \varphi(\mathbf{x})$ is a well-defined monomorphism and ${}^{M}\!/\!{}_{\ker(\varphi)} \simeq \mathrm{Im}(\varphi)$.

Example 8. Any abelian group $G(\oplus)$ with inverse operation $\ominus$ and an identity element e can be viewed as a module over $\mathbb{Z}$ with the scalar product $\odot : \mathbb{Z}\times G \to G$ defined for all $n \in \mathbb{N}$ and $g \in G$ as follow:

- $n \odot g = g \oplus g \oplus \cdots \oplus g$ with n operands g,
- $0 \odot g = e$,
- $(-n) \odot g = \ominus(n \odot g)$.

Being able to determine whether the given $\mathbf{R}$-module M is free or not has a significant impact, as displayed in upcoming sections. Let us present the first, almost trivial characterisation of free $\mathbf{R}$-modules.

Theorem 24. Let M be an $\mathbf{R}$-module of rank k. Then, M is free if and only if $M \simeq \mathbf{R}^k$. Besides, if M is free then any minimal basis of M is free.

Proof. Choose some $\mathbf{R}$-module M of rank $k \in \mathbb{N}$. Remark that $\mathbf{R}^k$ is free by *Example* 7, so any module isomorphic to $\mathbf{R}^k$ is free. Suppose that M is free. Let $B = (\mathbf{m}_1, \ldots, \mathbf{m}_k)$ be a minimal basis of M and S be the standard basis of $\mathbf{R}^k$. Define a map $\varphi : \mathbf{R}^k \mapsto M$ by the formula $\varphi(\boldsymbol{\delta}_i) = \mathbf{m}_i$, where $i \in \mathbb{N}, i \leq k$. It is apparent that φ is a module homomorphism, which is surjective as it maps the free basis of $\mathbf{R}^k$ to the given minimal basis of M of rank k. Due to M being free, $|M| = (|\mathbf{R}|)^k = |\mathbf{R}^k|$ and φ is a module isomorphism.

Let scalars $z_1, \dots, z_k \in \mathbf{R}$ satisfy $\sum\limits_{i=1}^{k} z_i \mathbf{m}_i = \mathbf{o}$. By applying the isomorphism, $\varphi\left(\sum\limits_{i=1}^{k} z_i \boldsymbol{\delta}_i\right) = \sum\limits_{i=1}^{k} z_i \varphi(\boldsymbol{\delta}_i) = \sum\limits_{i=1}^{k} z_i \mathbf{m}_i = \mathbf{o}$ and $\sum\limits_{i=1}^{k} z_i \boldsymbol{\delta}_i \in \ker(\varphi)$. Consequently, all the scalars $z_1, \dots, z_k$ are zero as $\ker(\varphi) = \{\mathbf{o}\}$, and B is a free basis.

□

The fundamental objective of this section is to comprehend the structure of an $\mathbf{R}$-module and to be able to decompose it into powers of p, as shown in Drápal's work [10, Section I.5].

Definition 25. Let M be an $\mathbf{R}$-module and $\mathbf{u} \in M$. The *height* of $\mathbf{u}$ is minimal non-negative integer i meeting the condition $p^i \cdot \mathbf{u} = \mathbf{o}$. The *socle* of M, denoted by $\mathrm{Soc}(M)$, is the set of all elements of M which have height at most 1.

Choose $m \in \mathbb{N}$. It is not difficult to notice the socle of a free module $\mathbf{R}^m$ is $(p^{n-1} \cdot \mathbf{R})^m$. Furthermore, it can be extended to a statement that $(p^{n-i} \cdot \mathbf{R})^m$ consists of elements with height at most i, for $i = 0, \dots, n$. The following claim introduces the basic properties of an element's height and how to compute it.

Claim 26. Let M be an $\mathbf{R}$-module, $\mathbf{u} = (u_1, \dots, u_m) \in M$ and $k \in \{0, 1, \dots, n\}$. Then,

1. $\mathbf{u}$ has height $n - k$ if and only if $\mathbf{v}$ with at least one coordinate invertible exists and satisfies $\mathbf{u} = p^k \cdot \mathbf{v}$,
2. $\mathbf{u}$ has height 0 if and only if $\mathbf{u} = \mathbf{o}$, and $\mathbf{u}$ has height n if and only if at least one coordinate of $\mathbf{u}$ is a unit,
3. $\forall r \in \mathbf{R}^* : r \cdot \mathbf{u}$ has the same height as $\mathbf{u}$,
4. if $\mathbf{u}$ has height $h \in \mathbb{N}$ then $\mathbf{u}\mathbf{R} \simeq \mathbf{R}/_{p^h\mathbf{R}}$,
5. elements of M with height at most i form a submodule M_i of M for each $i \in \mathbb{Z}, 0 \leq i \leq n$. If M is a submodule of $\mathbf{R}^m$, then $M_i = M \cap (p^{n-i}\mathbf{R})^m$, and $M_i = \langle p^{n-i}\mathbf{b}_1, \dots, p^{n-1}\mathbf{b}_l \rangle$ whenever M has a free basis $(\mathbf{b}_1, \dots, \mathbf{b}_l)$.

Proof. Consider the p-adic representation, presented in **Theorem 15**, of each coordinate $u_i = \sum\limits_{j=0}^{n-1} z_{i,j} \cdot p^j$, $i = 1, \dots, m$, with the coefficients from the Teichmüller set $\mathcal{T}_r$. Set $h = n - \min(h_1, \dots, h_m)$, where h_i is for $i = 1, \dots, m$ defined as

$$h_i = \begin{cases} \min\{0 \leq j < n \mid z_{i,j} \neq 0\}, & \text{if } u_i \neq 0, \\ n, & \text{otherwise.} \end{cases}$$

For each $i = 1, \dots, m$, observe that $p^h \cdot u_i = p^h \cdot \sum\limits_{j=h_i}^{n-1} z_{i,j} \cdot p^j = \sum\limits_{j=h_i}^{n-1} z_{i,j} \cdot p^{h+j} = 0$ as $j \geq h_i \geq n - h$. Furthermore, we have $h_k = n - h$ for some $k = 1, \dots, m$, i.e. $p^{h-1} \cdot u_k = \sum\limits_{j=h_k}^{n-1} z_{k,j} \cdot p^{h+j-1} = z_{k,h_k} \cdot p^{n-1} \neq 0$. Hence, the height of $\mathbf{u}$ is h.

1. Assume that $\mathbf{u}$ has height $n - k$. Then, $n - k = h = n - \min(h_1, \dots, h_m)$, which can happen if and only if $i \in \mathbb{N}$ exists for all $j \in \mathbb{N}$ which fulfills $i, j \leq m$

and $h_i = k \leq h_j$. It can be equivalently rewritten as $u_j = \sum\limits_{l=k}^{n-1} z_{jl} \cdot p^l$ for all $j = 1, \dots, m$, where at least one $z_{ik} \neq 0$, $i = 1, \dots, m$. Let $\mathbf{v}$ have the coordinates $v_i = \sum\limits_{l=k}^{n-1} z_{il} \cdot p^{l-k}$, $i = 1, \dots, m$. In conclusion, $\mathbf{u}$ has height $h = n - k$ if and only if $\mathbf{u} = p^k \cdot \mathbf{v}$ and $v_i \in \mathbf{R} \setminus p\mathbf{R} = \mathbf{R}^*$ for some $i \in \mathbb{N}, i \leq n$.

2. It is a direct consequence of 1.

3. For any $r \in \mathbf{R}^*$ we can write $\mathbf{u} = r^{-1} \cdot (r \cdot \mathbf{u})$ from what is clear that both elements need to have the same height.

4. Assume that $\mathbf{u}$ has height $h \in \mathbb{N}$. Define a map $\varphi : \mathbf{R} \to \mathbf{uR}, x \mapsto x \cdot \mathbf{u}$. Then, for any $x, y \in \mathbf{R}$, we have $\varphi(x + y) = (x + y)\mathbf{u} = x\mathbf{u} + y\mathbf{u} = \varphi(x) + \varphi(y)$ and $\varphi(x \cdot y) = (x \cdot y)\mathbf{u} = x(y \cdot \mathbf{u}) = x \cdot \varphi(y)$. Furthermore, $\varphi(x) = x \cdot \mathbf{u} = \mathbf{o}$ for $x \in \mathbf{R}$ if and only if p^h divides x, which is equivalent to $x \in p^h\mathbf{R}$. Thus, φ is a module homomorphism with $\ker(\varphi) = p^h\mathbf{R}$ and the assertion is implied by the first isomorphism theorem as $\mathbf{R}/p^h\mathbf{R} \simeq \mathbf{uR}$.

5. Choose $i \in \mathbb{N}, i \leq n$, and define M_i as the set composed of all elements of M with height at most i. Pick any $\mathbf{v}, \mathbf{w} \in M_i$ and $r \in \mathbf{R}$. Then $r \cdot \mathbf{v} \in M_i$ can be deduced from that $p^i \cdot (r \cdot v_j) = r \cdot (p^i \cdot v_j) = r \cdot 0 = 0$, $j \in \mathbb{N}, j \leq m$, which means $p^i \cdot (r \cdot \mathbf{v}) = \mathbf{o}$. Analogically, $p^i \cdot (v_j + w_j) = p^i \cdot v_j + p^i \cdot w_j = 0$ for every $j \in \mathbb{N}, j \leq m$, so $p^i \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{o}$ and $\mathbf{v} + \mathbf{w} \in M_i$.

Let M be a submodule of $\mathbf{R}^m$. In accordance with 1., $\mathbf{a} \in M_i$ if and only if p^{n-i} divides all $a_1, \dots, a_m$, which occurs if and only if $\mathbf{a} \in M \cap (p^{n-i}\mathbf{R})^m$.

Finally, let M has a free basis $(\mathbf{b}_1, \dots, \mathbf{b}_l)$. Denote $N = \langle p^{n-i}\mathbf{b}_1, \dots, p^{n-i}b_l \rangle$, so clearly $N \subseteq M_i$. Let $\mathbf{a} \in M_i \setminus N$. Then, $\mathbf{a} \neq \mathbf{o}$ and $\mathbf{a} = \sum\limits_{j=1}^{l} z_j \mathbf{b}_j$ for some $z_1, \dots, z_l \in \mathbf{R}$ such that p^{n-i} does not divide z_j for some $j = 1, \dots, l$. Thus, $p^i z_j \neq 0$ and $\mathbf{o} = p^i \mathbf{a} = \sum\limits_{t=1}^{l} p^i z_t \mathbf{b}_t$. In consequence, $(\mathbf{b}_1, \dots, \mathbf{b}_l)$ is not the free basis, a contradiction. Hence, $M_i \subseteq N$ and $M_i = N$.

□

Derived from the initial point of **Claim 26**, the height of an element $\mathbf{u}$ over $\mathbf{R}$ can be computed as the maximal $e = 0, 1, \dots, n$ satisfying $p^e \mid \mathbf{u}$, which means that p divides all coordinates of $\mathbf{u}$. In other words, all the coordinates of $\mathbf{u}$ lie in $p^e\mathbf{R}$. Obviously, $\mathbf{v}$ such that $\mathbf{u} = p^e \cdot \mathbf{v}$ cannot be defined as $\frac{\mathbf{u}}{p^e}$, because there is no inverse of p. However, the symbol $\frac{\cdot}{p}$ can be viewed as the map from $p\mathbf{R}$ to $\mathbf{R}$ determined by $\sum\limits_{i=a}^{n-1} \zeta_i p^i \mapsto \sum\limits_{i=a}^{n-1} \zeta_i p^{i-1}$. Evidently, this map can be coordinate-wise expanded to the map $\frac{\cdot}{p} : (p\mathbf{R})^m \to \mathbf{R}^m$ for any $m \in \mathbb{N}$.

Lemma 27. Algorithm 4 is correct and runs in time $\mathcal{O}(m \cdot n^2 \cdot r \cdot \log^2(p))$.

Proof. The correctness follows from **Claim 26**. Note that the cycle iterates at most n times, in each iteration it computes m divisions $\frac{u_i}{p}$, which can be done in time $\mathcal{O}(n \cdot r \cdot \log^2(p))$. Thus, the algorithm runs in $\mathcal{O}(m \cdot n^2 \cdot r \cdot \log^2(p))$.

□

Based on the second and the fifth point of **Claim 26**, $\{\mathbf{o}\}$ and $\operatorname{Soc}(M)$ are the only submodule of an $\mathbf{R}$-module M with elements of height at most 0 and 1, respectively. However, the socle of M can be viewed as a vector space over the finite field $\mathcal{T}_r \simeq \mathbf{R}/p\mathbf{R} \simeq \mathbb{F}_{p^r}$, where the first isomorphism

Algorithm 4 Computing the element's height

```
Require: $\mathbf{u}$
Ensure: $\mathbf{u} = p^{n-h} \cdot \mathbf{v}$, where $h$ is height of $\mathbf{u}$ and $\mathbf{v}$ has the height $n$
  if $\mathbf{u} = \mathbf{o}$ then
      return $0, \boldsymbol{\delta}_1$
  end if
  $h \leftarrow n$
  $\mathbf{v} \leftarrow \mathbf{u}$
  while $h > 0$ do
      if $p \mid \mathbf{u}$ then
          $h \leftarrow h - 1$
          $\mathbf{v} \leftarrow \frac{\mathbf{u}}{p}$
      else
          break
      end if
  end while
  return $h, \mathbf{v}$
```

is shown in the paragraph under **Definition 16** while introducing operations on $\mathcal{T}_r$, and the second one is presented in (1.4). In conclusion, $\mathrm{Soc}(M)$ is free over the field $\mathcal{T}_r$ and a criterion for the module M to be free can be derived.

Lemma 28. Let M be an $\mathbf{R}$-module generated by $\mathbf{b}_1, \ldots, \mathbf{b}_l$. Then, $(\mathbf{b}_1, \ldots, \mathbf{b}_l)$ is a free basis of M over $\mathbf{R}$ if and only if the socle of M has a free basis $(p^{n-1}\mathbf{b}_1, \ldots, p^{n-1}\mathbf{b}_l)$ over $\mathcal{T}_r$.

Proof. Set $I = \{1, \ldots, l\}$, $B = (\mathbf{b}_1, \ldots, \mathbf{b}_l)$ and $C = (p^{n-1}\mathbf{b}_1, \ldots, p^{n-1}\mathbf{b}_l)$.

" $\Longleftarrow$ ": Every $\mathbf{b}_1, \ldots, \mathbf{b}_l$ appears to have height n. Assume that $\sum\limits_{i=1}^{l} a_i\mathbf{b}_i = \mathbf{o}$ for some $a_1, \ldots, a_l \in \mathbf{R}$, where at least one of them is non-zero. Take the minimal exponent $e \in \mathbb{N} \cup \{0\}$ meeting the condition $p^e a_i \mathbf{b}_i \in \mathrm{Soc}(M)$ for every $i \in I$, which is, according to **Claim 26**, equivalent to that p^{n-1} divides all $p^e a_1, \ldots, p^e a_l$. Since C is a free basis of $\mathrm{Soc}(M)$, $p^e a_i \mathbf{b}_i = \mathbf{o}$ for all $i \in I$. Find $f \in \mathbb{N} \cup \{0\}$, $f < e$, such that p^{n-1} divides each $p^f a_1, \ldots, p^f a_l$, and $p^f a_i \mathbf{b}_i \in \mathrm{Soc}(M) \setminus \{\mathbf{o}\}$ for some $i \in I$. It can be done as there exist $i \in I$ satisfying $a_i\mathbf{b}_i \neq \mathbf{o}$, but this contradicts the minimality of e.

" $\Longrightarrow$ ": Suppose that M has a free basis B over $\mathbf{R}$. Undoubtedly, the socle of M is generated by C over $\mathcal{T}_r$ as **Claim 26** implies $p^{n-1}\mathbf{b}_i \in \mathrm{Soc}(M)$ for every $i \in I$. Let $a_1, \ldots, a_l \in \mathcal{T}_r$ satisfy $\sum\limits_{i=1}^{l} a_i p^{n-1}\mathbf{b}_i = \mathbf{o}$. It is a direct consequence that $a_i p^{n-1} = 0$ for each $i \in I$ since B is the free basis of M. Equivalently, p divides $a_1, \ldots, a_l \in \mathcal{T}_r$, and therefore, $a_i = 0$ for every $i \in I$.

□

Keep in mind in the third assertion of **Claim 26** that the $\mathbf{R}$-module generated by some element $\mathbf{u}$ of height h over $\mathbf{R}$ is isomorphic to the factor module $\mathbf{R}/_{p^h\mathbf{R}}$. A further step is to show that any $\mathbf{R}$-module can be decomposed into cyclic submodules of certain heights.

Lemma 29. Every finitely generated $\mathbf{R}$-module can be expressed as a direct sum of cyclic modules $\bigoplus\limits_{i=0}^{t} \mathbf{u}_i\mathbf{R}$ such that $\mathbf{u}_j\mathbf{R} \simeq {}^{\mathbf{R}}\!/_{p^{m_j}\mathbf{R}}$ for every $j = 1, \dots, l$ and some positive integer m_j.

Proof. Choose an $\mathbf{R}$-module M and consider a submodule M_i of M composed by elements of height at most i, where $i \in \mathbb{Z}, 0 \leq i \leq n$. Find the minimal $k \in \mathbb{Z}, 0 \leq k \leq n$, such that $M_k = M$. The lemma is proven by mathematical induction on k. Firstly, assume $k = 0$. Then $M = \{\mathbf{o}\}$, and there is nothing to prove. Secondly, if $k = 1$ then $M = \operatorname{Soc}(M)$ and it is enough to take $\mathbf{u}_1, \dots, \mathbf{u}_t$ a basis over the finite field $\mathcal{T}_r$.

Next, assume $k > 1$ and the hypothesis is valid for $k - 1$. Consider a factor module ${}^{M}\!/_{M_1}$, which is finitely generated, and its every element is of height less than k. According to the inductive hypothesis, there are $\mathbf{v}_1, \dots, \mathbf{v}_s \in M$ satisfying ${}^{M}\!/_{M_1} = \bigoplus\limits_{j=1}^{s} (\mathbf{v}_j + M_1)\mathbf{R}$. For every $j = 1, \dots, s$, denote by h_j the height of $\mathbf{v}_j + M_1$ in M/M_1, i.e. $0 < h_j < k$. So, $p^{h_j}(\mathbf{v}_j + M_1) = \mathbf{o} + M_1$, which implies $p^{h_j}\mathbf{v}_j \in M_1 \setminus \{\mathbf{o}\}$ because h_j is the minimal such integer. Furthermore, $p^{h_j+1}\mathbf{v}_j = \mathbf{o}$ in M, and $\mathbf{v}_j\mathbf{R} \simeq {}^{\mathbf{R}}\!/_{p^{h_j+1}\mathbf{R}}$ as stated by **Claim 26**.

Now, denote by N a submodule of M generated by $\mathbf{v}_1, \dots, \mathbf{v}_s$. If it is shown $r_1\mathbf{v}_1 = \dots = r_s\mathbf{v}_s = \mathbf{o}$ whenever $\sum\limits_{j=1}^{s} r_j\mathbf{v}_j = \mathbf{o}$ for some $r_1, \dots, r_s \in \mathbf{R}$, then $N = \bigoplus\limits_{j=1}^{s} \mathbf{v}_j\mathbf{R}$. Let $r_1, \dots, r_s \in \mathbf{R}$ satisfy $\sum\limits_{j=1}^{s} r_j\mathbf{v}_j = \mathbf{o}$. For every $j = 1, \dots, s$, compute the exponent $e_j \in \mathbb{N} \cup \{0\}$ and the unit $q_j \in \mathbf{R}^*$ such that $r_j = p^{e_j} \cdot q_j$. Thus, $\sum\limits_{j=1}^{s} r_j(\mathbf{v}_j + M_1) = \mathbf{o} + M_1$ in ${}^{M}\!/_{M_1}$, and based on the already proven part, $r_1(\mathbf{v}_1 + M_1) = \dots = r_s(\mathbf{v}_s + M_1) = \mathbf{o} + M_1$. Choose $i \in \mathbb{N}, i \leq s$. Note that $q_i(\mathbf{v}_i + M_1)$ has the same height as $\mathbf{v}_i + M_1$ according to **Claim 26**, and $p^{h_i-1}\mathbf{v}_i$ is not in M_1 by the properties of h_i. As a result, $e_i \geq h_i \geq 1$. Additionally, the sum $\mathbf{o} = \sum\limits_{j=1}^{s} r_j\mathbf{v}_j = \sum\limits_{j=1}^{s} p^{e_j}q_j\mathbf{v}_j = p \cdot \sum\limits_{j=1}^{s} p^{e_j-1}q_j\mathbf{v}_j$ implies that $\sum\limits_{j=1}^{s} p^{e_j-1}q_j\mathbf{v}_j \in M_1$ and $\sum\limits_{j=1}^{s} p^{e_j-1}q_j(\mathbf{v}_j + M_1) = \mathbf{o} + M_1$ in ${}^{M}\!/_{M_1}$. Repeating the exact argument, $p^{e_1-1}q_1(\mathbf{v}_1 + M_1) = \dots = p^{e_s-1}q_s(\mathbf{v}_s + M_1) = \mathbf{o} + M_1$. Specially, $e_i - 1 \geq h_i$. It is now clear that all $p^{e_1}q_1\mathbf{v}_1, \dots, p^{e_s}q_s\mathbf{v}_s$ are $\mathbf{o}$ in M.

Define $N_1 = N \cap M_1$. It is possible to find the complement $N^\perp$ of N_1 in M_1 because $M_1 = \operatorname{Soc}(M)$ can be regarded as a vector space over $\mathcal{T}_r$. $N^\perp$ seems to be a subspace of M_1, and so $\mathbf{w}_1, \dots, \mathbf{w}_t \in \mathbf{R}^m$, which satisfy $N^\perp = \bigoplus\limits_{i=1}^{t} \mathbf{w}_i\mathbf{R}$, exist. Particularly,

$$\left.\begin{aligned} N \cap N^\perp &\overset{N^\perp \subseteq M_1}{=} N \cap N^\perp \cap M_1 = N^\perp \cap N_1 = \{\mathbf{o}\} \\ N + N^\perp &\overset{N_1 \subseteq N}{=} N + N_1 + N^\perp = N + M_1 = M \end{aligned}\right\} \implies M = N \oplus N^\perp.$$

Finally, we have $M = \left(\bigoplus\limits_{j=1}^{s} \mathbf{v}_j\mathbf{R}\right) \oplus \left(\bigoplus\limits_{i=1}^{t} \mathbf{w}_i\mathbf{R}\right)$.

□

Consider $\mathbf{u}_1, \dots, \mathbf{u}_l$ specifying the cyclic decomposition of some module M over $\mathbf{R}$. It is demonstrated in the ensuing theorem that $\mathbf{u}_1, \dots, \mathbf{u}_l$ correspond to elements of a free basis over $\mathbf{R}$ lifted to appropriate heights. In other words, let $\mathbf{v}_1, \dots, \mathbf{v}_l \in \operatorname{Soc}(M) \setminus \{\mathbf{o}\}$ be p multiples of $\mathbf{u}_1, \dots, \mathbf{u}_m$ in the specified order. For each $i = 1, \dots, l$, run **Algorithm 4** on $\mathbf{v}_i$ to obtain $\mathbf{w}_i$ of height n satisfying $\mathbf{v}_i = p^{n-1}\mathbf{w}_i$. In the described situation, $(\mathbf{w}_1, \dots, \mathbf{w}_l)$ is a free basis and

$$\operatorname{Soc}(M) = \bigoplus_{i=1}^{l} \mathbf{v}_i\mathbf{R} \leq M = \bigoplus_{i=1}^{l} \mathbf{u}_i\mathbf{R} \leq \bigoplus_{i=1}^{l} \mathbf{w}_i\mathbf{R}. \tag{2.2}$$

Theorem 30. Let $m \in \mathbb{N}$ and M be an $\mathbf{R}$-submodule of $\mathbf{R}^m$. There exists a free basis $(\mathbf{v}_1, \dots, \mathbf{v}_m)$ of $\mathbf{R}^m$, which satisfies $M = \bigoplus_{i=1}^{m} p^{e_i}\mathbf{v}_i\mathbf{R}$ for some exponents $e_1, \dots, e_m \in \{0, 1, \dots, n\}$.

Proof. **Lemma 29** affirms that $M = \bigoplus_{i=1}^{l} \mathbf{u}_i\mathbf{R}$ for some $\mathbf{u}_1, \dots, \mathbf{u}_l \in M$. Denote by I the set $\{1, \dots, l\}$. For every $i \in I$, execute **Algorithm 4** on the input $\mathbf{u}_i$ to obtain the height $h_i \in \{0, 1, \dots, n-1\}$ of $\mathbf{u}_i$ and $\mathbf{v}_i \in \mathbf{R}^m$ of height n fulfilling $\mathbf{u}_i = p^{n-h_i} \cdot \mathbf{v}_i$. Set $V = \langle \mathbf{v}_1, \dots, \mathbf{v}_l \rangle$. Let $a_1, \dots, a_l \in \mathbf{R}$ satisfy $\sum_{i=1}^{l} a_i\mathbf{v}_i = \mathbf{o}$. Assume, for a contradiction, there exists $j \in I$, for which is a_j non-zero. Find the minimal $e \in \mathbb{N} \cup \{0\}$ meeting the condition $p^e a_i \mathbf{v}_i \in M$ for each $i \in I$. Since $M = \bigoplus_{i=1}^{l} p^{n-h_i}\mathbf{v}_i\mathbf{R}$, then, for every $i \in I$,

$$p^e a_i \mathbf{v}_i = \mathbf{o} \iff p^n \mid p^e a_i \mathbf{v}_i \overset{p \nmid \mathbf{v}_i}{\iff} p^n \mid p^e a_i \iff p^e a_i = 0.$$

However, $a_j \neq 0$, thus $f \in \mathbb{N} \cup \{0\}$ must exist satisfying $f < e$ and $p^f a_i \mathbf{v}_i \in M$ for every $i \in I$, a contradiction with the minimality of e. Hence, V has a free basis $(\mathbf{v}_1, \dots, \mathbf{v}_l)$. As a result of **Claim 26** and **Lemma 28**, $\operatorname{Soc}(V)$ has a free basis $C = (p^{n-1}\mathbf{v}_1, \dots, p^{n-1}\mathbf{v}_l)$.

Remind that the socles $\operatorname{Soc}(M)$ and $\operatorname{Soc}(\mathbf{R}^m)$ may be viewed as vector spaces over the finite field $\mathcal{T}_r$. Moreover, $\operatorname{Soc}(M) = \operatorname{Soc}(V)$ and $\operatorname{Soc}(M)$ is a subspace of $\operatorname{Soc}(\mathbf{R}^m)$, because M is the submodule of $\mathbf{R}^m$. Thus, it is possible to extend C by $\mathbf{u}_{l+1}, \dots, \mathbf{u}_m \in \mathbf{R}^m$ into a basis of the $\operatorname{Soc}(\mathbf{R}^m)$ of dimension m. Thence, the outputs of **Algorithm 4** run gradually on $\mathbf{u}_{l+1}, \dots, \mathbf{u}_m$ are $\mathbf{v}_{l+1}, \dots, \mathbf{v}_m$, each of the height n, such that $\mathbf{u}_i = p^{n-1}\mathbf{v}_i$ for every $i = l+1, \dots, m$.

Define N as a submodule of $\mathbf{R}^m$ generated by $\mathbf{v}_1, \dots, \mathbf{v}_m$. Apparently, $\operatorname{Soc}(N)$ has a basis $(p^{n-1}\mathbf{v}_1, \dots, p^{n-1}\mathbf{v}_m)$, which means that N is free in accordance with **Lemma 28**. Derived from **Theorem 24**, $N \simeq \mathbf{R}^m$, which implies $N = \mathbf{R}^m$ because $N \subseteq \mathbf{R}^m$. Consequently, $M = \bigoplus_{i=1}^{l} p^{e_i}\mathbf{v}_i\mathbf{R} = \bigoplus_{i=1}^{m} p^{e_i}\mathbf{v}_\mathbf{i}\mathbf{R}$, where $e_i = n - h_i$ for $1 \leq i \leq l$ and $e_i = n$ for $l < i \leq m$.

□

The preceding lemma and theorem do not explain how to acquire some free basis over $\mathbf{R}$, which can be lifted by multiplying by p into the cyclic decomposition of an $\mathbf{R}$-module M. However, **Algorithm 5** introduced in **Section 2.3** solves this issue.

2.2 Matrices over Galois Rings

Let $\mathbf{R}^{k \times l}$ represent the module composed of all matrices over $\mathbf{R}$ of type $k \times l$, where $k, l \in \mathbb{N}$. Pick a matrix $A \in \mathbf{R}^{k \times l}$ and indices $i, j \in \mathbb{N}$ satisfying $i \leq k$

and $j \leq l$. The i^{th} row of A will be represented by $\mathbf{A}^r_i$, the j^{th} column of A by $\mathbf{A}^c_j$ and the entry of A at position (i, j) by a_{ij}, alternatively $A[i, j]$ if more clarity is needed. An identity matrix of order k will be denoted by I_k and a zero matrix of type $k \times l$ (or order k) by $0_{k\times l}$ (or 0_k).

Definition 31. Let $k, l \in \mathbb{N}$ and $A \in \mathbf{R}^{k\times l}$. Select any $i, j \in \mathbb{N}$ such that $i, j \leq k$ and $i \neq j$. *Elementary row operations* are

- $\mathbf{A}^r_i \leftrightarrow \mathbf{A}^r_j$: switching the i^{th} and j^{th} row within A,
- $\mathbf{A}^r_i \leftarrow u \cdot \mathbf{A}^r_i; u \in \mathbf{R}^*$: multiplying the i^{th} row by a unit,
- $\mathbf{A}^r_i \leftarrow \mathbf{A}^r_i + t \cdot \mathbf{A}^r_j; t \in \mathbf{R}$: adding a multiple of j^{th} row to the i^{th}.

Elementary column operations can be defined symmetrically. A matrix E of order k is *elementary* if E was obtained from I_k by only one elementary operation.

Gauss elimination works almost the same as in linear algebra over a field. The only exception is that it is impossible to multiply rows or columns of a given matrix by non-invertible elements, which was the main reason for the preceding definition.

Definition 32. Let $k, l \in \mathbb{N}$ and $A \in \mathbf{R}^{k\times l}$. If there exists $B \in \mathbf{R}^{l\times k}$ satisfying $B \cdot A = I_l$ then A is *left invertible* and B is A's *left inverse.* Symmetrically for $C \in \mathbf{R}^{k\times l}$ fulfilling $A \cdot C = I_k$, A is *right invertible* and C is its *right inverse.* If $k = l$ and there exists $B \in \mathbf{R}^{k\times k}$ such that $B \cdot A = I_k = A \cdot B$ then A is *invertible* and B is the inverse of A, denoted by A^{-1}.

The product of matrices over Galois rings preserves the invertibility exactly as in linear algebra over finite fields. Since it is applicable, the formalisation of this statement is to be found below.

Lemma 33. Let $k, l \in \mathbb{N}$ and $A \in \mathbf{R}^{k\times l}, B \in \mathbf{R}^{l\times m}$ be left (right) invertible. Then $A \cdot B$ is left (right) invertible.

Proof. Since A and B are left invertible, matrices $X \in \mathbf{R}^{l\times k}$ and $Y \in \mathbf{R}^{m\times l}$, which satisfy $X \cdot A = I_l$ and $Y \cdot B = I_m$, exist. The product $Y \cdot X$ is a left inverse of $A \cdot B$ because $Y \cdot X \cdot (A \cdot B) = Y \cdot (X \cdot A) \cdot B = Y \cdot B = I_m$. Thence, $A \cdot B$ is left invertible. Since $(A \cdot X)^\top = X^\top \cdot A^\top$, the same holds for right invertible matrices.

□

Now, it is substantial to display that invertible matrices over Galois rings exist. We present the most fundamental invertible matrices, but they are beneficial in the following sections on multiple occasions.

Example 9. Let $k \in \mathbb{N}$. The following matrices of order k over $\mathbf{R}$ are invertible:

1. **An elementary matrix:** It is enough to take an elementary matrix of the opposite elementary operation ($\mathbf{A}^r_i \leftrightarrow \mathbf{A}^r_j, \mathbf{A}^r_i \leftarrow u^{-1} \cdot \mathbf{A}^r_i, \mathbf{A}^r_i \leftarrow \mathbf{A}^r_i - t \cdot \mathbf{A}^r_j$).
2. **A permutation matrix**, i.e. there is only one entry equal 1 in each row and each column, others are 0: Observe that $(\mathbf{P}^c_i)^\top \cdot \mathbf{P}^c_j = \delta_{ij}$ for any permutation matrix $P \in \mathbf{R}^{k\times k}$ and integers i, j such that $0 \leq i, j \leq k$. Hence, $P^\top \cdot P = I_k$.

3. **A triangular matrix with units on the main diagonal**: Let a matrix U be a such upper triangular. Define entries $d_{ij} = 0$ for $1 \leq j < i \leq k$, $d_{ii} = u_{ii}^{-1}$ for $1 \leq i \leq n$, and $d_{ij} = -u_{jj}^{-1} \sum_{h=i}^{j-1} d_{ih} u_{hj}$ for $1 \leq i < j \leq k$. Then, $D = (d_{ij})_{i,j=1}^{k}$ is the inverse of U since $D \cdot U$ is an upper triangular matrix as the product of two upper triangular matrices and for every $i.j \in \mathbb{N}, i \leq j \leq k$, we have

$$\sum_{h=1}^{k} d_{ih} u_{hj} = \sum_{h=i}^{j} d_{ih} u_{hj} = \sum_{h=i}^{j-1} d_{ih} u_{hj} + d_{ij} u_{jj} = \sum_{h=i}^{j-1} d_{ih} u_{hj} + \left(-u_{jj}^{-1} \sum_{h=i}^{j-1} d_{ih} u_{hj} \right) \cdot u_{jj},$$

which apparently equals δ_{ij}.

Now, it is sufficient to state that any transposed lower triangular matrix is an upper triangular matrix and, therefore, invertible.

It is evident that a triangular matrix over $\mathbf{R}$ with zero divisor z on the main diagonal is not invertible as there is no $r \in \mathbf{R}$ for which $r \cdot z = 1$. Another example of an invertible matrix over $\mathbf{R}$ is a transition matrix between free bases of a free $\mathbf{R}$-module.

Lemma 34. Let M be a free $\mathbf{R}$-module of rank $m \in \mathbb{N}$, and B and C be two free bases of M. Denote by B' and C' the matrices of order m over $\mathbf{R}$, where the rows are the basis elements of B and C, respectively. Then, the unique invertible matrix Q of order m over $\mathbf{R}$, which satisfies $Q \cdot B' = C'$, exists.

Proof. Choose a free $\mathbf{R}$-module M be of rank $m \in \mathbb{N}$. Let $B = (\mathbf{b}_1, \dots, \mathbf{b}_m)$ and $C = (\mathbf{c}_1, \dots, \mathbf{c}_m)$ be two free bases of M. Since $M = \langle B \rangle$, for each $i \in \mathbb{N}$, $i \leq M$, there exist $x_{i1}, \dots, x_{im} \in \mathbf{R}$ satisfying $\mathbf{c}_i = \sum_{j=1}^{m} x_{ij} \mathbf{b}_j$. Symmetrically, $y_{i1}, \dots, y_{im} \in \mathbf{R}$ exist such that $\mathbf{b}_i = \sum_{j=1}^{m} y_{ij} \mathbf{c}_j$ as $M = \langle C \rangle$, where $i \in \mathbb{N}, i \leq m$. Set $Q = (x_{ij})_{i,j=1}^{m}$ and $P = (y_{ij})_{i,j=1}^{m}$. Then, we have

$$Q \cdot B' = \left(\sum_{t=1}^{m} x_{it} \cdot b_{tj} \right)_{i,j=1}^{m} = (c_{ij})_{i,j=1}^{m} = C', \tag{2.3}$$

$$P \cdot C' = \left(\sum_{t=1}^{m} y_{it} \cdot c_{tj} \right)_{i,j=1}^{m} = (b_{ij})_{i,j=1}^{m} = B'. \tag{2.4}$$

Observe that $B' \overset{(2.4)}{=} P \cdot C' \overset{(2.3)}{=} P \cdot Q \cdot B'$, which implies $P \cdot Q = I_m$ and $P = Q^{-1}$.

Suppose that matrices Q_1, Q_2 of order m over $\mathbf{R}$ are invertible and satisfy $Q_1 \cdot B' = C' = Q_2 \cdot B'$. It is apparent that $B' = Q_1^{-1} \cdot C' = Q_1^{-1} \cdot Q_2 \cdot B'$. Consequently, $Q_1^{-1} \cdot Q_2 = I_m$ and $Q_1 = Q_2$.

□

The determinant of a matrix A over a Galois ring, denoted by $\det(A)$, may be defined analogously to the case over a finite field. Terminology from linear algebra concerning determinants, e.g. minors, cofactors and adjugate matrices, may be straightforwardly generalised for Galois rings. Now, we can propose a condition for a matrix to be invertible based on its determinant.

Theorem 35. Let $k \in \mathbb{N}$ and $A \in \mathbf{R}^{k \times k}$. Then A is invertible if and only if the determinant of A is a unit, which can happen if and only if the determinant of A is not divisible by p.

Proof. It can be proven in the same way as in linear algebra. Let A be a matrix of order k over $\mathbf{R}$. Define $K = \{1, \dots, k\}$ and a matrix M_{ij} of order $(k-1)$ created from A by omitting the i^{th} row and j^{th} column, where $i, j \in K$. Recall the adjugate matrix of A defined as $\text{adj}(A) = ((-1)^{i+j}\det(M_{ji}))_{i,j=1}^{k}$. Then, $\text{adj}(A) \cdot A = \det(A) \cdot I_k$ is a consequence of the Laplace expansion. Clearly, if $\det(A) \in \mathbf{R}^*$ then $A^{-1} = \det(A)^{-1}\text{adj}(A)$. On the other hand, if A^{-1} exists then $1 = \det(I_k) = \det(A^{-1}A) = \det(A^{-1}) \cdot \det(A)$, and so $\det(A) \in \mathbf{R}^*$.

Let us suggest an alternative, algorithmic approach. Let a matrix $A \in \mathbf{R}^{k\times k}$ be given. Then A can be transformed into its row echelon form B by elementary row operations. It is well-known that switching rows may change only the sign of the determinant, multiplying a row by a unit u increase the determinant u-times and adding a multiple of one row to another does not change the determinant. The same holds for matrices over Galois rings, as these properties are based solely on the definition of the determinant and application of permutations. Hence, $\det(A) = \det(B)$.

Derived from the third point in *Example* 9 and the ensuing observation, the matrix B is invertible if and only if its main diagonal consists of units. This is equivalent to saying that the product of main diagonal entries is a unit, which is exactly $\det(B) = \prod_{i=1}^{k} b_{ii}$. The last equivalence is based on **Theorem 15**.

□

Consider a matrix $A \in \mathbf{R}^{k\times l}$ for some $k, l \in \mathbb{N}$ and define $f_A : \mathbf{R}^l \to \mathbf{R}^k$ by the formula $f_A(\mathbf{x}) = A \cdot \mathbf{x}$ for $\mathbf{x} \in \mathbf{R}^l$. The map f_A appears to be a module homomorphism. Thus, the image and the kernel of the matrix A can represent the homomorphism f_A's image and kernel, written as $\text{Im}(A) = \text{Im}(f_A) \leq \mathbf{R}^k$ and $\ker(A) = \ker(f_A) \leq \mathbf{R}^l$. In this situation, the rank of $\text{Im}(A)$ is meant by the *rank* of the matrix A, written as $\text{rank}(A)$.

Claim 36. Let $k, l \in \mathbb{N}$ and $A \in \mathbf{R}^{k\times l}$. Then $|\text{Im}(A)| \cdot |\ker(A)| = p^{lnr}$.

Proof. Apply the first isomorphism theorem on an $\mathbf{R}$-module homomorhism $f_A : \mathbf{R}^l \longrightarrow \mathbf{R}^k, \mathbf{x} \mapsto A\mathbf{x}$ and obtain $\text{Im}(A) = \text{Im}(f_A) \simeq \mathbf{R}^l/\ker(f_A) = \mathbf{R}^l/\ker(A)$. Hence, $|\text{Im}(A)| \cdot |\ker(A)| = |\mathbf{R}|^l = p^{lnr}$.

□

Let us finish this section about matrices by proposing another characterisation of the left (right) invertible matrices, depending on whether the module generated by A's columns (rows) is free. These conditions are the direct generalisation of equivalences that a matrix over a finite field is left or right invertible if and only if it has the full column or row rank.

Theorem 37. Let $k, l \in \mathbb{N}$ and $A \in \mathbf{R}^{k\times l}$.

1. A is right invertible if and only if $(\mathbf{A}_1^r, \dots, \mathbf{A}_k^r)$ is a free basis of $\text{Im}(A^\top)$,

2. A is left invertible if and only if $(\mathbf{A}_1^c, \dots, \mathbf{A}_k^c)$ is a free basis of $\text{Im}(A)$,

Proof. 1. Let $B \in \mathbf{R}^{l\times k}$ satisfy $A \cdot B = I_k$. Then, for any $i \in \mathbb{N}, i \leq k$, we have $\boldsymbol{\delta}_i = \mathbf{A}_i^r \cdot B$. Find $z_1, \dots, z_k \in \mathbf{R}$ fulfilling $\sum_{i=1}^{k} z_i \cdot \mathbf{A}_i^r = \mathbf{o}$. Therefore,

$\mathbf{o} = \left(\sum_{i=1}^{k} z_i \cdot \mathbf{A}_i^r\right) \cdot B = \sum_{i=1}^{k} z_i \cdot \mathbf{A}_i^r \cdot B = \sum_{i=1}^{k} z_i \cdot \boldsymbol{\delta}_i$, but $(\boldsymbol{\delta}_1, \dots, \boldsymbol{\delta}_k)$ is a free basis of $\mathbf{R}^k$. Hence all $z_1, \dots, z_k$ must be zero, so $\mathbf{A}_1^r, \dots, \mathbf{A}_k^r$ is a free basis of $\operatorname{Im}(A^\top)$.

Suppose that $B = (\mathbf{A}_1^r, \dots, \mathbf{A}_k^r)$ is a free basis of $\operatorname{Im}(A^\top)$, i.e. $k \leq l$. Consider a homomorhism $f_A : \mathbf{R}^l \to \mathbf{R}^k$ defined as $\mathbf{x} \mapsto A \cdot \mathbf{x}$, which needs to be surjective for the same reason as in linear algebra. Consequently, there exists a preimage $\mathbf{x}_j \in \mathbf{R}^l$ such that $f_A(\mathbf{x}_j) = A \cdot \mathbf{x}_j = \boldsymbol{\delta}_j$, where $j \in \mathbb{N}$ and $j \leq k$. Define a matrix $X = (\, \mathbf{x}_1 \mid \cdots \mid \mathbf{x}_k \,) \in \mathbf{R}^{l \times k}$ and compute $A \cdot X = (\, A\mathbf{x}_1 \mid \cdots \mid A\mathbf{x}_k \,) = I_k$.

2. A consequence of 1. applied on $A^\top$ since $(A \cdot B)^\top = B^\top \cdot A^\top$.

□

2.3 Linear Codes

The significant difference between defining linear codes over a field and a Galois ring is the necessity of utilising modules instead of vector spaces. Remark that the subsequent definition yields also for any commutative ring. In this section, terminology and notation from the work of Dougherty and collaborators [11] are adopted.

Definition 38. Any $\mathbf{R}$-submodule $\mathcal{C}$ of $\mathbf{R}^m$ is said to be a *linear code of length m and rank l* over $\mathbf{R}$, referred to as an $[m, l]_{\mathbf{R}}$-code, assuming $\mathcal{C}$ is of rank l. Elements of a linear code are called *codewords.*

Let $\mathcal{C}$ be an $[m, l]_{\mathbf{R}}$-code. The *free rank* of the code $\mathcal{C}$, denoted by $\operatorname{frank}(\mathcal{C})$, is defined as the rank of the largest free submodule of $\mathcal{C}$ with respect to inclusion. The linear code $\mathcal{C}$ is called *free* provided $\operatorname{rank}(\mathcal{C}) = \operatorname{frank}(\mathcal{C})$. The *Hamming weight* of $\mathbf{c} \in \mathcal{C}$, denoted by $\mathrm{w}_{\mathcal{H}}(\mathbf{c})$, is the number of its non-zero coordinates, and the *Hamming distance* between $c, d \in \mathcal{C}$ is $\mathrm{d}_{\mathcal{H}}(\mathbf{c}, \mathbf{d}) = \mathrm{w}_{\mathcal{H}}(\mathbf{c} - \mathbf{d})$. Finally, the number $\mathrm{d}_{\mathcal{H}}(\mathcal{C}) = \min\{\mathrm{d}_{\mathcal{H}}(\mathbf{c}, \mathbf{d}) \mid \mathbf{c}, \mathbf{d} \in \mathcal{C} : \mathbf{c} \neq \mathbf{d}\}$ is known as *minimum Hamming distance* of the linear code $\mathcal{C}$.

Some examples illustrating linear codes over the Galois ring $\mathbf{R}$ are provided. To determine if the given code is free, **Theorem 24**, which claims that any $\mathbf{R}$-module is free if and only if it is isomorphic to $\mathbf{R}^l$ for some $l \in \mathbb{N}$, comes handy.

Example 10. Let $\mathbf{R} = \mathrm{GR}(3^2, 2) = \mathbb{Z}_{3^2}[\xi]$ be a Galois ring with operations defined modulo polynomial $G_{3,2}(x) = x^2 + x + 2 \in \mathbb{Z}_{3^2}[x]$. Consider the following codes:

1. $\mathcal{C} = \{(a0, b1, 00) \mid a, b \in \mathbb{Z}_{3^2}\}$, then the code $\mathcal{C}$ is not linear as it is not $\mathbf{R}$-submodule of $\mathbf{R}^3$ (e.g. $2 \cdot (10, 31, 00) = (20, 62, 00) \notin \mathcal{C}$).

2. $\mathcal{C} = \{(ab, 00, 00) \mid a, b \in \mathbb{Z}_{3^2}\}$, thus the code $\mathcal{C}$ is free linear of the rank 1 as $\mathcal{C} = \mathbf{R} \times \{0\} \times \{0\}$.

3. $\mathcal{C} = \{(ab, cd, ab + cd) \mid a, b, c, d \in \mathbb{Z}_{3^2}\}$, so a map $(ab, cd, ab + cd) \mapsto (ab, cd)$ appears to be an isomorphism between $\mathcal{C}$ and $\mathbf{R}^2$. Therefore, $\mathcal{C}$ is the free linear code of the rank 2.

4. $\mathcal{C} = \{(ab, cd, ef) \mid a, b, c, d \in \mathbb{Z}_{3^2}, e, f \in \{0, 3, 6\}\}$. In this situation, the code $\mathcal{C}$ is generated by codewords $(1, 0, 0), (0, 1, 0)$ and $(0, 0, 3\xi + 6)$, i.e. linear of rank 3, but not free.

Definition 39. Let $\mathcal{C}$ be a $[m, l]$-code over $\mathbf{R}$ and $\mathbf{b}_1, \ldots, \mathbf{b}_l \in \mathbf{R}^m$ be generators of $\mathcal{C}$. A *generator matrix* of $\mathcal{C}$ is $G = \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_l \end{pmatrix} \in \mathbf{R}^{l \times m}$ and a *parity-check matrix* of $\mathcal{C}$ is $H \in \mathbf{R}^{(m-l) \times m}$ provided $H \cdot \mathbf{c}^\top = \mathbf{o}^\top$ if and only if $\mathbf{c} \in \mathcal{C}$. The dual code of $\mathcal{C}$ is a linear code $\mathcal{C}^\perp$ generated by H.

Let $\mathbb{K}$ be the residue field ${}^{\mathbf{R}}\!/_{p\mathbf{R}}$. Once again, recall the ring epimorhism $^-$ (or $\tilde{\mu}$): $\mathbf{R} \to \mathbb{K}$ from **Section 1.2** defined by $a \mapsto a + p\mathbf{R}$. Consider an induced map $^{-m} : \mathbf{R}^m \to \mathbb{K}^m$ for $m \in \mathbb{N}$ as element-wise application of the epimorhism $^-$, i.e. $\overline{\mathbf{a}}^m = \overline{(a_1, \ldots, a_m)}^m = (\overline{a_1}, \ldots, \overline{a_m})$. Then, for any $\mathbf{a}, \mathbf{b} \in \mathbf{R}^m$ and any $t \in \mathbf{R}$:

$$\overline{\mathbf{a}}^m + \overline{\mathbf{b}}^m = (\overline{a_1}, \ldots, \overline{a_m}) + \left(\overline{b_1}, \ldots, \overline{b_m}\right) = \left(\overline{a_1 + b_1}, \ldots, \overline{a_m + b_m}\right) = \overline{\mathbf{a} + \mathbf{b}}^m,$$
$$t \cdot \overline{\mathbf{a}}^m = \overline{t} \cdot \overline{\mathbf{a}}^m = (\overline{t} \cdot \overline{a_1}, \ldots, \overline{t} \cdot \overline{a_m}) = (\overline{t \cdot a_1}, \ldots, \overline{t \cdot a_m}) = \overline{t \cdot \mathbf{a}}^m.$$

Furthermore, $^{-m}$ is clearly surjective since $^-$ is, so a module epimorhism.

Claim 40. Let $\mathcal{C} = \bigoplus_{i=1}^{l} p^{e_i}\mathbf{v}_i\mathbf{R}$ be a $[m, l]_\mathbf{R}$-code for $e_1, \ldots, e_m \in \{0, \ldots, n-1\}$ and a free basis $V = (\mathbf{v}_1, \ldots, \mathbf{v}_l)$. Consider a free linear code $\mathcal{D}$ over $\mathbf{R}$ generated by V. Then, $\mathrm{Soc}(\mathcal{C})$ has a basis $W = (p^{n-1}\mathbf{v}_1, \ldots, p^{n-1}\mathbf{v}_l)$ and is isomorphic to the linear code $\overline{\mathcal{D}}^m$ over the residue field $\overline{\mathbf{R}}$.

Proof. **Theorem 30** affirms that a free basis V satisfying hypothesis exists. The socle of $\mathcal{D}$ has a basis W over $\mathcal{T}_r$ according to **Lemma 28** as $\mathcal{D}$ has a free basis V. Moreover, $W \subseteq \mathcal{C}$ and the code $\mathcal{C}$ is certainly a submodule of $\mathcal{D}$. Hence, W is also a basis of $\mathrm{Soc}(\mathcal{C})$.

Consider a map $\varphi : \mathcal{D} \to \mathbf{R}^m, \mathbf{d} \mapsto p^{n-1}\mathbf{d}$. Choose some codewords $\mathbf{a}, \mathbf{b} \in \mathcal{D}$ and $r \in \mathbf{R}$. Then, $\varphi(\mathbf{a}) + \varphi(\mathbf{b}) = p^{n-1}\mathbf{a} + p^{n-1}\mathbf{b} = p^{n-1}(\mathbf{a} + \mathbf{b}) = \varphi(\mathbf{a} + \mathbf{b})$ and $\varphi(r \cdot \mathbf{a}) = p^{n-1} \cdot r \cdot \mathbf{a} = r \cdot \varphi(\mathbf{a})$, so φ is a module homomorphism. Furthermore, $\ker(\varphi) = p\mathcal{D}$ as $p^{n-1}\mathbf{d} = \mathbf{o}$ if and only if p divides $d_1, \ldots, d_m$, and $\mathrm{Im}(\varphi) = \mathrm{Soc}(\mathcal{C})$ follows from $\varphi(V) = W$. Hence, $\mathrm{Soc}(C) \simeq {}^{\mathcal{D}}\!/_{p\mathcal{D}}$ based on the first isomorphism theorem.

On the other hand, let ω be a restriction of the module epimorphism $^{-m}$ to $\mathcal{D}$. Then, $\ker(\omega) = p\mathcal{D}$ and $\mathrm{Im}(\omega) = \overline{\mathcal{D}}^m$. Again by using the first isomorphism theorem, ${}^{\mathcal{D}}\!/_{p\mathcal{D}} \simeq \overline{\mathcal{D}}^m$. In conclusion, $\mathrm{Soc}(C) \simeq_\varphi {}^{\mathcal{D}}\!/_{p\mathcal{D}} \simeq_\omega \overline{\mathcal{D}}^m$.

□

2.4 Permutation Equivalent Linear Codes

Equipped with the necessary module theory and code terminology, it is now possible to describe linear codes over the Galois ring $\mathbf{R}$ and determine their equivalence classes.

Definition 41. Let $m \in \mathbb{N}$, $S = \{i \in \mathbb{N}, i \leq m\}$ and $\mathcal{C}$, $\mathcal{C}'$ be $[m, l]$-codes over $\mathbf{R}$. The codes $\mathcal{C}$ and $\mathcal{C}'$ are said to be *permutation equivalent* provided there exists a permutation $\sigma : S \to S$ such that a codeword $(c_1, \ldots, c_m) \in \mathcal{C}$ if and only if $(c_{\sigma(1)}, \ldots, c_{\sigma(m)}) \in \mathcal{C}'$, written as $\mathcal{C}' = \sigma(\mathcal{C})$.

The primary intent of this section is to find a "well-behaved" representative of every equivalence class under the permutation equivalence. The subsequent definition clarifies which codes are "well-behaved".

Definition 42. Let $m, l \in \mathbb{N}$ and $\mathcal{C}$ be an $[m, l]$-code over $\mathbf{R}$ with a generator matrix $G \in \mathbf{R}^{l \times m}$. Then, G is in the *systematic form* provided

$$G = \begin{pmatrix} I_{k_0} & G_{0,1} & G_{0,2} & \dots & G_{0,n-1} & G_{0,n} \\ 0 & p \cdot I_{k_1} & p \cdot G_{1,2} & \dots & p \cdot G_{1,n-1} & p \cdot G_{1,n} \\ 0 & 0 & p^2 \cdot I_{k_2} & \dots & p^2 \cdot G_{2,n-1} & p^2 \cdot G_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & p^{n-2} \cdot G_{n-2,n-1} & p^{n-2} \cdot G_{n-2,n} \\ 0 & 0 & 0 & \dots & p^{n-1} \cdot I_{k_{n-1}} & p^{n-1} \cdot G_{n-1,n} \end{pmatrix}, \tag{2.5}$$

where $k_0, k_1, \dots, k_n \in \mathbb{N} \cup \{0\}$, $\sum\limits_{i=0}^{n} k_i = m$, and $G_{i,j} \in \mathbf{R}^{k_i \times k_j}$ for every i, j such that $0 \leq i < j < n$. We shall write $G \sim (1)^{k_0}(p)^{k_1}(p^2)^{k_2} \dots (p^{n-1})^{k_{n-1}}(0)^{k_n}$, where terms $(p^i)^{k_i}$ for $k_i = 0$ are omitted.

Consider a linear $[m, l]$-code $\mathcal{C}$ over $\mathbf{R}$. **Theorem 30** asserts that a free basis $B = (\mathbf{b}_1, \dots, \mathbf{b}_m)$ of $\mathbf{R}^m$ exists, which fulfills $\mathcal{C} = \bigoplus\limits_{i=1}^{m} p^{e_i}\mathbf{b}_i\mathbf{R}$, where every $e_i \in \mathbb{Z}$ satisfies $0 \leq e_i \leq n$. Now, let us propose a relation between rows of a generator matrix of $\mathcal{C}$ in the systematic form and the free basis B.

Lemma 43. Let $m, l \in \mathbb{N}$, $\mathbf{v}_1, \dots, \mathbf{v}_l \in \mathbf{R}^m$ be of height n and $e_1, \dots, e_l \in \mathbb{N} \cup \{0\}$ be less than n. If a matrix $G = (p^{e_i} \cdot \mathbf{v}_i)_{i=1}^{l} \in \mathbf{R}^{l \times m}$ is in the systematic form then $(\mathbf{v}_, \dots, \mathbf{v}_l)$ is a free basis of some submodule of $\mathbf{R}^m$.

Proof. Suppose that G is in the systematic form and let $\mathcal{C}$ be the code generated by G. For any $i, j \in \mathbb{N}$, $j < i \leq l$, we have $v_{ii} = 1$ and $v_{ij} = 0$. If it is shown that $\operatorname{Soc}(\mathcal{C})$ has a free basis $(p^{n-1}\mathbf{v}_1, \dots, p^{n-1}\mathbf{v}_l)$ then, in line with **Lemma 28**, $\mathbf{v}_1, \dots, \mathbf{v}_l$ constitute a free basis.

Let $z_1, \dots, z_l \in \mathcal{T}_r$ satisfy $\sum\limits_{i=1}^{l} z_i p^{n-1}\mathbf{v}_i = \mathbf{o}$. Notice that $v_{kk} = 1$ and $v_{kj} = 0$ for any $j, k \in \mathbb{N}$, $j < k \leq l$. Express the sum over every coordinate for $i = 1, \dots, l$:

- $i = 1 : 0 = \sum\limits_{j=1}^{l} z_j p^{n-1} v_{j1} = z_1 p^{n-1} \overset{z_1 \in \mathcal{T}_r}{\Longrightarrow} z_1 = 0,$

- $i = 2 : 0 = \sum\limits_{j=1}^{l} z_j p^{n-1} v_{j2} = z_1 p^{n-1} v_{12} + z_2 p^{n-1} = z_2 p^{n-1} \overset{z_2 \in \mathcal{T}_r}{\Longrightarrow} z_2 = 0,$

- $i > 2 :$ Suppose that $z_j = 0$ for each $j < i$. Then, $0 = \sum\limits_{j=1}^{l} z_j p^{n-1} v_{ji} = z_i p^{n-1}$, and it is possible to conclude that $z_i = 0$.

Thus, there exists only a trivial zero combination of $p^{n-1}\mathbf{v}_1, \dots, p^{n-1}\mathbf{v}_l$ and these codewords form a free basis of $\operatorname{Soc}(\mathcal{C})$.

□

Now, we formulate an algorithm for finding a generator matrix $G \in \mathbf{R}^{l \times m}$ in the systematic form (2.5) of some permutation equivalent code to the given

Algorithm 5 Finding systematic form of a generator matrix

```
Require: alinear code $\mathcal{C}$ over $\mathbf{R}$ given by a basis $(\mathbf{u}_1, \ldots, \mathbf{u}_l) \subset \mathbf{R}^m$
Ensure: a generator matrix $G$ of $\sigma(\mathcal{C})$ in the form (2.5), a permutation $\sigma$
  $i \leftarrow 1$
  while $i \leq l$ do
      $(h_i, \mathbf{v}_i) \leftarrow$ Algorithm 4$(\mathbf{u}_i)$
      $e_i \leftarrow n - h_i$
      $i \leftarrow i + 1$
  end while
  sort $\mathbf{v}_1, \ldots, \mathbf{v}_l$ by their corresponding exponents $e_i$ in non-decreasing order
  $G \leftarrow (p^{e_i}\mathbf{v}_i)_{i=1}^{l} \in \mathbf{R}^{l \times m}, \sigma \leftarrow \mathrm{id}_{\mathbf{S}_m}$
  $e \leftarrow 0$
  while $e < n$ do
      $m_e \leftarrow \sum_{i=0}^{e-1} k_i + 1$
      $i \leftarrow m_e$
      $k_e \leftarrow |\{m_e \leq j \leq l \mid e_i = e\}|$
      while $i < m_e + k_e$ do
          find $j \in \{i, \ldots, m\}$ such that $x = \frac{g_{ij}}{p^e} \in \mathbf{R}^*$
          $\mathbf{G}^c_i \leftrightarrow \mathbf{G}^c_j, \sigma \leftarrow \sigma \circ (i, j)$
          $\mathbf{G}^r_i \leftarrow x^{-1} \cdot \mathbf{G}^r_i$
          $j \leftarrow 1$
          while $j \leq l$ do
              if $j \neq i$ then
                  $\mathbf{G}^r_j \leftarrow \mathbf{G}^r_j - g_{ji} \cdot \mathbf{G}^r_i$
                  if $j > i$ then
                      $(h_j, \mathbf{v}_j) \leftarrow$ Algorithm 4$(\mathbf{G}^r_j)$
                      $e_j \leftarrow n - h_j$
                  end if
                  if $\mathbf{G}^r_j = \mathbf{o}$ then
                      $G \leftarrow (\mathbf{G}^r_t)_{t=1, t \neq j}^{l}$ (omit the $j^{\text{th}}$ row $\mathbf{G}^r_j$ from the matrix $G$)
                      $l \leftarrow l - 1$
                      $j \leftarrow j - 1$
                      if $m_e \leq j + 1 < m_e + k_e$ then
                          $k_e \leftarrow k_e - 1$
                      end if
                  end if
              end if
              $j \leftarrow j + 1$
          end while
          $i \leftarrow i + 1$
          $k_e \leftarrow |\{m_e \leq j \leq l \mid e_i = e\}|$
          sort $\mathbf{G}^r_i, \ldots, \mathbf{G}^r_l$ by their corresponding $e_j$ in non-decreasing order
      end while
      $e \leftarrow e + 1$
  end while
```

$[m, l]$-code. In the algorithm, we use the notation from **Definition 31**: $\mathbf{G}_i^c$ denotes the i^{th} column of G, $\mathbf{G}_i^r$ is the i^{th} row of G, g_{ij} is the entry of G at position (i, j), and $\mathbf{G}_i^c \leftrightarrow \mathbf{G}_j^c$ means swapping the i^{th} and j^{th} row of G.

Claim 44. **Algorithm 5** is correct and on input $\mathbf{u}_1, \ldots, \mathbf{u}_l \in \mathbf{R}^m$ has the time complexity $\mathcal{O}\left(l^2(m \cdot s^2 + \log(l))\right)$, $s = n \cdot r \cdot \log(p)$.

Proof. Based on **Theorem 30**, there exists a free basis $(\mathbf{b}_1, \ldots, \mathbf{b}_m)$ of $\mathbf{R}^m$ for every linear code $\mathcal{C} \subseteq \mathbf{R}^m$ such that $\mathcal{C} = \bigoplus_{i=1}^{m} p^{f_i}\mathbf{b}_i\mathbf{R}$, $f_1, \ldots, f_m \in \{0, \ldots, n\}$. Then, **Algorithm 5** is trying to find some modified codewords $\mathbf{b}_1^*, \ldots, \mathbf{b}_l^*$, where each $\mathbf{b}_j^*$ is obtained by permutating the coordinates of some linear combination of $\mathbf{b}_i$ with $e_i < n$, where $i = 1, \ldots, m$ and $j = 1, \ldots, l$.

Let $\mathbf{u}_1, \ldots, \mathbf{u}_t \in \mathbf{R}^m$ be given. For each $i \in \mathbb{N}$, $i \leq t$, perform **Algorithm 4** on $\mathbf{u}_i$ to get the height h_i of $\mathbf{u}_i$ and a codeword $\mathbf{v}_i \in \mathbb{R}^m$ of height n meeting the condition $\mathbf{u}_i = p^{e_i} \cdot \mathbf{v}_i$ for $e_i = n - h_i$. Assume, WLOG, $e_1 \leq e_2 \leq \cdots \leq e_t < n$. Denote by k_e the number of exponents $e_i = e$ and by m_e the index of the first $\mathbf{u}_i$ with the exponent e for every integer e, $0 \leq e < n$. Now, define a matrix $G_0 = (\mathbf{u}_i)_{i=1}^t \in \mathbf{R}^{t \times m}$, and let $\mathcal{C}$ be a code generated by G_0. Notice that the matrix G_0 corresponds to the initialised matrix G in **Algorithm 5**.

Choose $e \in \mathbb{Z}, 0 \leq e < n$. Note, for every integer i satisfying $m_e \leq i < m_e + k_e$, the row $\mathbf{G}_i^r$ has the height $n - e$. Therefore, the codeword $\frac{\mathbf{G}_i^r}{p^e}$ has at least one invertible coordinate $x \in \mathbf{R}^*$ based on **Claim 26**, and the "normalisation" $x^{-1} \cdot \mathbf{G}_i^r$ is possible. The process of row elimination can only reduce the heights of rows since $\mathcal{C} \cap (p^e\mathbf{R})^m$ is, derived from **Claim 26**, a submodule of the code $\mathcal{C}$ containing all $\mathbf{c} \in \mathcal{C}$ with height at most $n - e$. Thus, every operation applied to the matrix $G \in \mathbf{R}^{l \times m}$ is well-defined. Moreover, for obtained $G = (p^{e_i}\mathbf{v}_i)_{i=1}^l$, we have $e_j \leq e_i < n$ (sorting and omitting), $v_{ij} = 0 = v_{ik}$ (reduction) and $v_{ii} = 1$ (normalisation), where $i, j, k \in \mathbb{N}$ satisfying $j < i \leq k < m_e + k_e$. As a result, the matrix G is in the systematic form.

Observe that the only transformations applied to G_0 in order to obtain G were elementary row operations, permutation σ of the indices of the columns and omitting of zero rows. Subsequently, there exist a matrix $E \in \mathbf{R}^{t \times t}$, which is the product of elementary matrices corresponding to the applied elementary row operations, a permutation matrix $P \in \mathbf{R}^{m \times m}$ representing the permutation σ acting on the indices of the columns of G_0 and a zero matrix $O \in \mathbf{R}^{(t-l) \times m}$ satisfying $\left(\begin{smallmatrix} G \\ O \end{smallmatrix}\right) = E \cdot G_0 \cdot P$. Additionally, E and P are invertible matrices according to *Example* 9 and **Lemma 33** maintaining that the product of invertible matrices is invertible. Let $\mathcal{C}'$ be the code generated by G and $\mathbf{c} \in \mathcal{C}'$. Then, $\mathbf{x} \in \mathbf{R}^l$ exists such as $\mathbf{c} = \mathbf{x} \cdot G$, which is equivalent to that there exists $\mathbf{x} \in \mathbf{R}^t$, for which $\mathbf{c} = \mathbf{x} \cdot \left(\begin{smallmatrix} G \\ O \end{smallmatrix}\right)$. This can happen if and only if $\mathbf{y} \in \mathbf{R}^t$ exists satisfying $\mathbf{c} = \mathbf{y} \cdot G_0 \cdot P$. Equivalently, $\mathbf{c} \cdot P^{-1} \in \mathcal{C}$, and it confirms that the codes $\mathcal{C}$ and $\mathcal{C}'$ are permutation equivalent.

Remark that every element of $\mathbf{R}$ can be stored using $s = n \cdot r \cdot \log(p)$ bits and every codeword of $\mathbf{R}^m$ using $m \cdot s$ bits. **Lemma 27** proposes that computing $\mathbf{v}_1, \ldots, \mathbf{v}_l$ can be done in time $\mathcal{O}\left(l \cdot m \cdot \frac{s^2}{r}\right)$. Clearly, sorting them is possible in time $\mathcal{O}(l \cdot \log(l))$. The cycles over e and i give l iterations of:

1. Finding $\frac{G_{i,j}}{p^e} \in \mathbf{R}^*$ using trial division: $\mathcal{O}\left(m \cdot \frac{s^2}{r}\right)$, $\frac{s}{r}$ bits needed for $p^e \leq p^n$,

2. $\mathbf{G}^c_i \leftrightarrow \mathbf{G}^c_j : \mathcal{O}(m \cdot s)$,
3. $x^{-1} \cdot \mathbf{G}^r_i : \mathcal{O}(m \cdot s^2)$,
4. While $j \leq l$ give l iterations of:
    (a) $\mathbf{G}^r_j - \mathbf{G}_{j,i} \cdot \mathbf{G}^r_i : \mathcal{O}(m \cdot s^2)$,
    (b) **Algorithm 4**: $\mathcal{O}\left(m \cdot \frac{s^2}{r}\right)$,

    $\Longrightarrow \mathcal{O}(l \cdot m \cdot s^2)$
5. sorting $\mathbf{G}^r_i, \ldots, \mathbf{G}^r_l$: $\mathcal{O}(l \cdot \log(l))$.

Altogether, the algorithm's time complexity is $\mathcal{O}\left(l^2(m \cdot s^2 + \log(l))\right)$.

□

Corollary 45. Every linear code $\mathcal{C}$ of the length $m \in \mathbb{N}$ over $\mathbf{R}$ is permutation equivalent to some linear code generated by $G \sim (1)^{k_0}(p)^{k_1} \ldots (p^{n-1})^{k_{n-1}}(0)^{k_n}$, where $k_0, k_1, \ldots, k_n \in \mathbb{N} \cup \{0\}$, $\sum\limits_{i=0}^{n} k_i = m$.

Demonstrating **Algorithm 5** to find the systematic form of some code $\mathcal{C}$ can be only beneficial for broadening insight into the algorithm's functioning and codes in general.

Example 11. Let $\mathbf{R}$ be the Galois ring $\mathrm{GR}(3^2, 2) = \mathbb{Z}_{3^2}[\xi]$ with operations defined modulo polynomial $G_{3,2}(x) = x^2 + x + 2 \in \mathbb{Z}_{3^2}[x]$. Consider codewords

$$\mathbf{v}_1 = \begin{pmatrix} 30 \\ 05 \\ 33 \\ 00 \\ 10 \end{pmatrix}^{\top}, \mathbf{v}_2 = \begin{pmatrix} 10 \\ 11 \\ 12 \\ 20 \\ 00 \end{pmatrix}^{\top}, \mathbf{v}_3 = \begin{pmatrix} 03 \\ 06 \\ 00 \\ 00 \\ 11 \end{pmatrix}^{\top}, \mathbf{v}_4 = \begin{pmatrix} 20 \\ 21 \\ 22 \\ 00 \\ 01 \end{pmatrix}^{\top} \in \mathbf{R}^5.$$

Let $\mathcal{C}$ be a linear code generated by $\mathbf{v}_1, 3 \cdot \mathbf{v}_2, \mathbf{v}_3$ and $3 \cdot \mathbf{v}_4$.

Emulate **Algorithm 5**:

1. swap $\mathbf{v}_2$ and $\mathbf{v}_3$ to achieve $e_1 = 0 = e_2 \leq e_3 = 1 = e_4$ in $\mathcal{C} = \bigoplus\limits_{i=1}^{4} p^{e_i} \cdot \mathbf{v}_i \cdot \mathbf{R}$,
2. $G \leftarrow \begin{pmatrix} 3^{e_1}\mathbf{v}_1 \\ 3^{e_2}\mathbf{v}_2 \\ 3^{e_3}\mathbf{v}_3 \\ 3^{e_4}\mathbf{v}_4 \end{pmatrix} = \begin{pmatrix} 30 & 05 & 33 & 00 & 10 \\ 03 & 06 & 00 & 00 & 11 \\ 30 & 33 & 36 & 60 & 00 \\ 60 & 63 & 66 & 00 & 03 \end{pmatrix}$
3. $e \leftarrow 0:$

    $k_0 \leftarrow 2$, $m_0 \leftarrow 1$, $M_0 \leftarrow 2$

    $i \leftarrow 1$: $G \overset{\mathbf{G}^c_1 \leftrightarrow \mathbf{G}^c_2}{\longleftarrow} \begin{pmatrix} 05 & 30 & 33 & 00 & 10 \\ 06 & 03 & 00 & 00 & 11 \\ 33 & 30 & 36 & 60 & 00 \\ 63 & 60 & 66 & 00 & 03 \end{pmatrix} \overset{\mathbf{G}^r_1 \leftarrow 02 \cdot \mathbf{G}^r_1}{\longleftarrow} \begin{pmatrix} 01 & 60 & 66 & 00 & 20 \\ 06 & 03 & 00 & 00 & 11 \\ 33 & 30 & 36 & 60 & 00 \\ 63 & 60 & 66 & 00 & 03 \end{pmatrix} \leftarrow \begin{pmatrix} 01 & 60 & 66 & 00 & 20 \\ 00 & 03 & 00 & 00 & 11 \\ 00 & 30 & 36 & 60 & 00 \\ 00 & 60 & 66 & 00 & 03 \end{pmatrix}$

    $i \leftarrow 2$: $G \overset{\mathbf{G}^c_2 \leftrightarrow \mathbf{G}^c_5}{\longleftarrow} \begin{pmatrix} 01 & 20 & 66 & 00 & 60 \\ 00 & 11 & 00 & 00 & 03 \\ 00 & 00 & 36 & 60 & 30 \\ 00 & 03 & 66 & 00 & 60 \end{pmatrix} \overset{\mathbf{G}^r_2 \leftarrow 40 \cdot \mathbf{G}^r_2}{\longleftarrow} \begin{pmatrix} 01 & 20 & 66 & 00 & 60 \\ 00 & 01 & 00 & 00 & 30 \\ 00 & 00 & 36 & 60 & 30 \\ 00 & 03 & 66 & 00 & 60 \end{pmatrix} \leftarrow \begin{pmatrix} 01 & 00 & 66 & 00 & 60 \\ 00 & 01 & 00 & 00 & 30 \\ 00 & 00 & 36 & 60 & 30 \\ 00 & 00 & 66 & 00 & 60 \end{pmatrix}$
4. $e \leftarrow 1:$

    $k_1 \leftarrow 2$, $m_1 \leftarrow 3$, $M_1 \leftarrow 4$

    $i \leftarrow 3$: $G \overset{\mathbf{G}^c_3 \leftrightarrow \mathbf{G}^c_3}{\longleftarrow} \begin{pmatrix} 01 & 00 & 66 & 00 & 60 \\ 00 & 01 & 00 & 00 & 30 \\ 00 & 00 & 36 & 60 & 30 \\ 00 & 00 & 66 & 00 & 60 \end{pmatrix} \overset{\mathbf{G}^r_3 \leftarrow 27 \cdot \mathbf{G}^r_2}{\longleftarrow} \begin{pmatrix} 01 & 00 & 66 & 00 & 60 \\ 00 & 01 & 00 & 00 & 30 \\ 00 & 00 & 03 & 33 & 66 \\ 00 & 00 & 66 & 00 & 60 \end{pmatrix} \leftarrow \begin{pmatrix} 01 & 00 & 00 & 00 & 60 \\ 00 & 01 & 00 & 00 & 30 \\ 00 & 00 & 03 & 33 & 66 \\ 00 & 00 & 00 & 00 & 60 \end{pmatrix}$

    $i \leftarrow 4$: $G \overset{\mathbf{G}^c_4 \leftrightarrow \mathbf{G}^c_5}{\longleftarrow} \begin{pmatrix} 01 & 00 & 00 & 60 & 00 \\ 00 & 01 & 00 & 30 & 00 \\ 00 & 00 & 03 & 66 & 33 \\ 00 & 00 & 00 & 60 & 00 \end{pmatrix} \overset{\mathbf{G}^r_4 \leftarrow 22 \cdot \mathbf{G}^r_4}{\longleftarrow} \begin{pmatrix} 01 & 00 & 00 & 60 & 00 \\ 00 & 01 & 00 & 30 & 00 \\ 00 & 00 & 03 & 66 & 33 \\ 00 & 00 & 00 & 03 & 00 \end{pmatrix} \leftarrow \begin{pmatrix} 01 & 00 & 00 & 00 & 00 \\ 00 & 01 & 00 & 00 & 00 \\ 00 & 00 & 03 & 00 & 33 \\ 00 & 00 & 00 & 03 & 00 \end{pmatrix}$

Denote the matrices $G_{0,1} = 0_2$, $G_{0,2} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $G_{1,2} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. Thus, the output of the algorithm is indeed the matrix $G = \left(\begin{smallmatrix} I_2 & G_{0,1} & G_{0,2} \\ 0_2 & 3\cdot I_2 & 3\cdot G_{1,2} \end{smallmatrix}\right)$ in the systematic form, which generates some code permutation equivalent to $\mathcal{C}$.

Consider some matrix A over $\mathbf{R}$. Let G be the output of **Algorithm 5** applied to A. Execute **Algorithm 5** a second time, now on the $G^\top$, and denote by D the result. Then, D is a diagonal matrix with elements p^e on diagonal, where $e \in \{0, 1, \dots, n-1\}$. Extend D into D' of the same type as A by zero rows and columns. Clearly, A is similar to D'.

Claim 46 (Smith normal form)**.** Let $X \in \mathbf{R}^{l\times m}$ for some $m, l \in \mathbb{N}$. Then, there exists invertible matrices $Q \in \mathbf{R}^{l\times l}$, $P \in \mathbf{R}^{m\times m}$ and the diagonal matrix $Y = \operatorname{diag}(1, \dots, 1, p, \dots, p^{n-1}, 0, \dots, 0) \in \mathbf{R}^{l\times m}$ satisfying $Y = Q \cdot X \cdot P$, which is called the *Smith normal form* of X.

Proof. Let X be a matrix of type $l \times m$ over $\mathbf{R}$. Consider a code $\mathcal{C}$ generated by X. **Corollary 45** states that a matrix $G \in \mathbf{R}^{t\times m}$ in the systematic form exists, which generates code $\mathcal{D}$ permutation equivalent to $\mathcal{C}$. **Lemma 43** suggests that $t \le l$. It is possible to compute an invertible matrix $Q \in \mathbf{R}^{l\times l}$, a permutation matrix $P_1 \in \mathbf{R}^{m\times m}$ and a zero matrix $O \in \mathbf{R}^{(l-t)\times m}$ subject to $\left(\begin{smallmatrix} G \\ O \end{smallmatrix}\right) = Q \cdot X \cdot P_1$ (executing **Algorithm 5** on X). Thence, it suffices to perform column reduction without interchanging the columns as i^{th} pivot has value p^{e_i} and $\mathbf{G}_i^r = p^{e_i}\mathbf{v}_i$, where $e_i = 0, 1, \dots, n$ and $\mathbf{v}_i$ is of height n for each $i \in \mathbb{N}, i \le l$. Denote by $E \in \mathbf{R}^{m\times m}$ the matrix representing the applied elementary column operations. The matrix E appears to be invertible as the product of elementary matrices by combination of *Example* 9 and **Lemma 33**. In consequence, $Y = \left(\begin{smallmatrix} G\cdot E \\ O \end{smallmatrix}\right) = Q\cdot X\cdot P_1\cdot E = Q\cdot X\cdot P$ for $P = P_1 \cdot E$.

□

Grounded on the described approach, we outline the algorithm for computing the Smith normal form Y of a given matrix X. Since invertible matrices indicating the similarity between X and Y are neglected in **Section 3.1**, the algorithm disregards them.

Algorithm 6 Determining the Smith normal form

```
Require: matrix $X$ of type $k \times l$ over $\mathbf{R}$
Ensure: matrix $Y$ of type $k \times l$ over $\mathbf{R}$, which is Smith normal form of $X$
  $(Y, \sigma) \leftarrow$ Lemma 43$(\mathbf{X}_1^r, \dots, \mathbf{X}_k^r)$, where $Y$ is of type $s \times l$
  $i \leftarrow 1$
  while $i \le s$ do
      $j \leftarrow i + 1$
      while $j \le l$ do
          $\mathbf{Y}_j^c \leftarrow \mathbf{Y}_j^c - \frac{y_{ij}}{y_{ii}} \cdot \mathbf{Y}_i^c$; $j \leftarrow j + 1$
      end while
      $i \leftarrow i + 1$
  end while
  while $i \le k$ do
      $\mathbf{Y}_i^r \leftarrow \mathbf{o}$ (add zero rows at the bottom of $Y$ until it is of type $k \times l$)
      $i \leftarrow i + 1$
  end while
  return $Y$
```

3. Maximum Cardinal Rank Distance Codes

This chapter presents the definition of a different metric from the usually used Hamming distance. The metric is essential for generalising maximum rank metric codes over finite fields. Readers who are not familiar with rank metric codes, especially Gabidulin codes, can find more in [12], [13] or [14].

Let $n, r \in \mathbb{N}$, p be a prime, $\mathbf{R} = \mathrm{GR}(p^n, r)$ and $\mathbf{S} = \mathrm{GR}(p^n, 1) = \mathbb{Z}_{p^n}$ be Galois rings, which remain fixed henceforth.

3.1 Cardinal Rank Metric of Matrices

Consider a matrix A of type $k \times l$ over the ring $\mathbf{S}$, then an $\mathbf{S}$-module generated by the columns $\mathbf{A}_1^c, \dots, \mathbf{A}_k^c$ of A is exactly $\mathrm{Im}(A) = \sum\limits_{i=1}^{k} \mathbf{A}_i^c \cdot \mathbf{S}$. The notation utilised in this thesis is slightly different from the one used in [6, Chapter 3], where the cardinal rank metric was introduced.

Definition 47. Let $k, l \in \mathbb{N}$ and $A \in \mathbf{S}^{k \times l}$. The number $\log_{p^n}(|\mathrm{Im}(A)|)$ is defined to be *the cardinal rank* of the matrix A and is denoted by $\mathrm{rk}\,(A)$.

Let us look at the basic properties of the cardinal rank metric of any matrix over the ring $\mathbf{S}$.

Theorem 48. Let $k, l \in \mathbb{N}$ and $A, B \in \mathbf{S}^{k \times l}$.

1. $\forall C \in \mathbf{S}^{k \times l} : \mathrm{rk}\,(C) \geq 0$, specially $\mathrm{rk}\,(C) = 0 \iff C = 0_{k \times l}$,
2. If $\mathrm{Im}(A) \subseteq \mathrm{Im}(B)$ then $\mathrm{rk}\,(A) \leq \mathrm{rk}\,(B)$,
3. If $\exists Q \in \mathbf{S}^{k \times k}\, \exists P \in \mathbf{S}^{l \times l}$, both of them invertible, such that $A = Q^{-1}BP$, then $\mathrm{rk}\,(A) = \mathrm{rk}\,(B)$,
4. $\mathrm{rk}\,(A) = \mathrm{rk}\left(A^\top\right)$,
5. $\mathrm{rk}\,(A + B) \leq \mathrm{rk}\,(A) + \mathrm{rk}\,(B)$,
6. If there exist matrices $C \in \mathbf{S}^{k_1 \times l_1}$ and $D \in \mathbf{S}^{k_2 \times l_2}$, for which $k_1 + k_2 = k$, $l_1 + l_2 = l$ and $A = \left(\begin{smallmatrix} C & 0 \\ 0 & D \end{smallmatrix}\right)$, then $\mathrm{rk}\,(A) = \mathrm{rk}\,(C) + \mathrm{rk}\,(D)$,
7. $\mathrm{rk}\,(A) \leq \mathrm{rank}(A)$, where the equality is achieved if and only if an $\mathbf{S}$-module $\mathrm{Im}(A)$ is free.

Proof. 1. and 2. follow directly from the definition. To address 3., it suffices to remark that a map $\omega : \mathrm{Im}(B) \to \mathrm{Im}(A), \mathbf{x} \mapsto Q^{-1}\mathbf{x}P$ appears to be a module homomorphism based on the distributive property of matrix multiplication, which is bijective as $\omega^{-1}(\mathbf{y}) = Q\mathbf{y}P^{-1}$. Hence, $\mathrm{Im}(A) \simeq \mathrm{Im}(B)$ and $|\mathrm{Im}(A)| = |\mathrm{Im}(B)|$.

4. Let the matrix $B = Q^{-1}AP$ be the Smith normal form of A for some invertible matrices $Q \in \mathbf{S}^{k \times k}$ and $\mathbf{S}^{l \times l}$ as in **Claim 46**. Since the diagonal

elements of B are the only non-zero entries, it is evident that $|\mathrm{Im}(B)| = |\mathrm{Im}(B^\top)|$. Thus, $\mathrm{rk}\,(A) = \mathrm{rk}\,(QBP^{-1}) \overset{3.}{=} \mathrm{rk}\,(B) = \mathrm{rk}\left(B^\top\right) \overset{3.}{=} \mathrm{rk}\left((QBP^{-1})^\top\right) = \mathrm{rk}\left(A^\top\right)$.

5. Firstly, given that $\mathrm{Im}(A+B)$ is generated by the columns of $A+B$, which certainly lie in $\mathrm{Im}(A)+\mathrm{Im}(B)$, $\mathrm{Im}(A+B)$ is an $\mathbf{S}$-submodule of $\mathrm{Im}(A)+\mathrm{Im}(B)$. Secondly, let $\rho : \mathrm{Im}(A)\times\mathrm{Im}(B) \to \mathrm{Im}(A)+\mathrm{Im}(B)$ be defined as $\rho(\mathbf{a},\mathbf{b}) = \mathbf{a}+\mathbf{b}$, where $(\mathbf{a},\mathbf{b}) \in \mathrm{Im}(A)\times\mathrm{Im}(B)$. Then, ρ seems to be a module epimorphism. It directly results in

$$|\mathrm{Im}(A+B)| \leq |\mathrm{Im}(A)+\mathrm{Im}(B)| \leq |\mathrm{Im}(A)\times\mathrm{Im}(B)| = |\mathrm{Im}(A)|\cdot|\mathrm{Im}(B)|.$$

By taking the logarithm, $\mathrm{rk}\,(A+B) \leq \mathrm{rk}\,(A) + \mathrm{rk}\,(B)$.

6. Since the matrix A is block diagonal with blocks C and D on the main diagonal, it can be expressed as $\mathrm{Im}(A) \simeq \mathrm{Im}(C)\times\mathrm{Im}(D)$. For this reason, $\log_{p^n}(|\mathrm{Im}(A)|) = \log_{p^n}(|\mathrm{Im}(C)|\cdot|\mathrm{Im}(D)|) = \log_{p^n}(|\mathrm{Im}(C)|) + \log_{p^n}(|\mathrm{Im}(D)|)$.

7. Let $(\mathbf{g}_1,\ldots,\mathbf{g}_t)$ be a basis of $\mathrm{Im}(A)$ over $\mathbf{S}$ and $\mathbf{b}_1,\ldots,\mathbf{b}_t \in \mathbf{S}^t$ form a free basis of $\mathbf{S}^t$. Then, a map $\rho : \mathbf{S}^t \to \mathrm{Im}(A)$ defined as $\sum\limits_{i=1}^{t} z_i\mathbf{b}_i \mapsto \sum\limits_{i=1}^{t} z_i\mathbf{g}_i$ appears to be a module homomorphism. Additionally, ρ is surjective since it maps the free basis of $\mathbf{S}^t$ to the basis of $\mathrm{Im}(A)$. As a result, $|\mathrm{Im}(A)| = |\rho(\mathbf{S}^t)| \leq |\mathbf{S}|^t = p^{nt}$. If $\mathrm{Im}(A)$ is free then certainly $|\mathrm{Im}(A)| = p^{nt}$. On the other hand, ρ is bijective provided $|\mathrm{Im}(A)| = p^{nt}$. In consequence, ρ in an module isomorphism, and $\mathrm{Im}(A)$ is free according to **Theorem 24**.

□

Let $Y \in \mathbf{S}^{k\times l}$ be the Smith normal form of a matrix X, which exists thanks to **Corollary 46**. An explicit formula for computing the cardinal rank of X is founded on the prior theorem.

Corollary 49. Let $k, l \in \mathbb{N}$ and $X \in \mathbf{S}^{k\times l}$. Let $Y \in \mathbf{R}^{r\times m}$ be the Smith normal form of X and define t_i as the number of pivots of Y equal to p^i, $i = 0,\ldots,n$. Then, $\mathrm{rk}(X) = \sum\limits_{i=0}^{n-1} \frac{(n-i)\cdot t_i}{n}$.

Proof. Execute **Algorithm 6** on X to obtain the Smith normal form $Y \in \mathbf{S}^{k\times l}$ of X with diagonal blocks $I_{t_0}, pI_{t_1}, \ldots, p^{n-1}I_{t_{n-1}}$ and a zero block O. Doubtless, $\mathrm{rk}(O) = 0$. Choose $i \in \mathbb{Z}, i < n$. Notice that $\mathrm{Im}\left(p^iI_{t_i}\right) = (p^i\mathbf{S})^{t_i}$ as $p^{n-i}\cdot s = \mathbf{o}$ for every $s \in p^i\mathbf{S}$, and only $z \in \mathbf{S}$, $z < p^{n-i}$, defines a unique $z\cdot s$. Thus, $\log_{p^n}\left(\left|\mathrm{Im}\left(p^iI_{t_i}\right)\right|\right) = \log_{p^n}\left(p^{(n-i)\cdot t_i}\right) = \frac{(n-i)\cdot t_i}{n}$. Concluded from **Theorem 48**, $\mathrm{rk}(X) \overset{3.}{=} \mathrm{rk}(Y) \overset{6.}{=} \sum\limits_{i=0}^{n-1} \mathrm{rk}(p^iI_{t_i}) = \sum\limits_{i=0}^{n-1} \frac{(n-i)\cdot t_i}{n}$.

□

Algorithm 7 Computing the cardinal rank

```
Require: matrix $X$ of type $k \times l$ over $\mathbf{S}$
Ensure: $\mathrm{rk}(X)$
  $Y \leftarrow$ Algorithm 6$(X)$
  $c \leftarrow 0$; $i \leftarrow 1$
  while $i \leq k$ do
    $(h, \mathbf{v}) \leftarrow$ Algorithm 4$(\mathbf{Y}_i^r)$, where $\mathbf{v}$ of height $n$ satisfy $\mathbf{Y}_i^r = p^{n-h}\cdot\mathbf{v}$
    $c \leftarrow c + \frac{h}{n}$; $i \leftarrow i + 1$
  end while
  return $c$
```

Let A and B be two matrices over $\mathbf{S}$ of the same type and C be their difference. The cardinal rank of C may be used as a metric between A and B, but the metric axioms must be verified first.

Corollary 50. Let $k, l \in \mathbb{N}$. A map d, which associates a pair of matrices A, B of the same type $k \times l$ over $\mathbf{S}$ with a value $\operatorname{rk}(A - B) \in \mathbb{Q}$, is a metric over $\mathbf{S}^{k\times l}$.

Proof. Choose $A, B, C \in \mathbf{S}^{k\times l}$ and regard **Theorem 48**.

1. Non-negativity: According to the theorem's first assertion, $\operatorname{rk}(A - B) \geq 0$ and $\operatorname{rk}(A - B) = 0$ if and only if $A = B$.

2. Symmetry: $\operatorname{rk}(A - B) = \operatorname{rk}((-I_k)(B - A)) \overset{\mathbf{48.3}}{=} \operatorname{rk}(B - A)$.

3. The triangle inequality:

$$\operatorname{rk}(A - C) = \operatorname{rk}((A - B) + (B - C)) \overset{\mathbf{48.5}}{\leq} \operatorname{rk}(A - B) + \operatorname{rk}(B - C)$$

Hence, $(\mathbf{S}^{k\times l}, d)$ is a metric space.

□

Before providing the codeword version of the cardinal rank used in the code theory, the cardinal rank of matrices is illustrated on three simple but non-trivial examples without figuring out the Smith normal form.

Example 12. Let $\mathbf{S} = \mathbb{Z}_{3^2}$. Compute $\operatorname{rk}(A), \operatorname{rk}(B)$ and $d(A, B)$ for the matrices $A = \left(\begin{smallmatrix} 0&8&2&2\\ 0&0&6&3\\ 3&0&0&6 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 1&0&6&0\\ 0&4&3&3\\ 8&0&0&6 \end{smallmatrix}\right) \in \mathbf{S}^{3\times 4}$.

Rewind the notation: $\mathbf{G}^c_i$ is the i^{th} column of a matrix G, $\mathbf{G}^r_i$ is the i^{th} row of G, g_{ij} is the entry of G at the position (i, j).

1. $A = \left(\begin{smallmatrix} 0&8&2&2\\ 0&0&6&3\\ 3&0&0&6 \end{smallmatrix}\right) \overset{8\mathbf{A}^c_2}{\sim} \left(\begin{smallmatrix} 0&1&2&2\\ 0&0&6&3\\ 3&0&0&6 \end{smallmatrix}\right) \underset{\mathbf{A}^c_4+7\mathbf{A}^c_2}{\overset{\mathbf{A}^c_3+7\mathbf{A}^c_2}{\sim}} \left(\begin{smallmatrix} 0&1&0&0\\ 0&0&6&3\\ 3&0&0&6 \end{smallmatrix}\right) \underset{\mathbf{A}^c_4+\mathbf{A}^c_1}{\overset{\mathbf{A}^c_4+\mathbf{A}^c_3}{\sim}} \left(\begin{smallmatrix} 0&1&0&0\\ 0&0&6&0\\ 3&0&0&0 \end{smallmatrix}\right)$

   We have an $\mathbf{S}$-module $\operatorname{Im}(A) = \left\{ \left(\begin{smallmatrix} x_1\\ 6x_2\\ 3x_3 \end{smallmatrix}\right) \middle| x_1, x_2, x_3 \in \mathbf{S} \right\}$, where the second and the third coordinate seems to lie in the maximal ideal $3\mathbf{S} = \{0, 3, 6\}$. Therefore, $|\operatorname{Im}(A)| = 9 \cdot 3 \cdot 3 = 81$ and the cardinal rank of the matrix A is $\operatorname{rk}(A) = \log_9(|\operatorname{Im}(A)|) = \log_9(81) = 2$.

2. $B = \left(\begin{smallmatrix} 1&0&6&0\\ 0&4&3&3\\ 8&0&0&6 \end{smallmatrix}\right) \overset{7\mathbf{B}^c_2}{\sim} \left(\begin{smallmatrix} 1&0&6&0\\ 0&1&3&3\\ 8&0&0&6 \end{smallmatrix}\right) \overset{\mathbf{B}^c_3+3\mathbf{B}^c_1}{\sim} \left(\begin{smallmatrix} 1&0&0&0\\ 0&1&3&3\\ 8&0&6&6 \end{smallmatrix}\right) \underset{\mathbf{B}^c_3+6\mathbf{B}^c_2}{\overset{\mathbf{B}^c_4+1\mathbf{B}^c_3}{\sim}} \left(\begin{smallmatrix} 1&0&0&0\\ 0&1&0&0\\ 8&0&6&0 \end{smallmatrix}\right)$

   Now, it is clear that $\operatorname{Im}(B^\top) = \left\{ \left(\begin{smallmatrix} x_1-x_3\\ x_2\\ 6x_3\\ 0 \end{smallmatrix}\right) \middle| x_1, x_2, x_3 \in \mathbf{S} \right\}$ has cardinality $|\operatorname{Im}(B^\top)| = 9 \cdot 9 \cdot 3 = 243$ as the third coordinate can be only from $3\mathbf{S}$. Consequently, $\operatorname{rk}(B) \overset{\mathbf{48.4}}{=} \operatorname{rk}\left(B^\top\right) = \log_9(|\operatorname{Im}(B^\top)|) = \log_9(81 \cdot 3) = \frac{5}{2}$.

3. $C = A - B = \left(\begin{smallmatrix} 8&8&5&2\\ 0&5&3&0\\ 4&0&0&0 \end{smallmatrix}\right) \underset{7\mathbf{C}^c_1,5\mathbf{C}^c_4}{\overset{\mathbf{C}^c_1\leftrightarrow\mathbf{C}^c_4}{\sim}} \left(\begin{smallmatrix} 1&8&5&2\\ 0&5&3&0\\ 0&0&0&1 \end{smallmatrix}\right) \underset{\mathbf{C}^c_3+3\mathbf{C}^c_1}{\overset{\mathbf{C}^c_2+\mathbf{C}^c_1}{\sim}} \left(\begin{smallmatrix} 1&0&0&2\\ 0&5&3&0\\ 0&0&0&1 \end{smallmatrix}\right) \underset{2\mathbf{C}^c_2}{\overset{\mathbf{C}^c_4+7\mathbf{C}^c_1}{\sim}} \left(\begin{smallmatrix} 1&0&0&0\\ 0&1&3&0\\ 0&0&0&1 \end{smallmatrix}\right)$

   $$\overset{\mathbf{C}^c_3+6\mathbf{C}^c_2}{\sim} \left(\begin{smallmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1 \end{smallmatrix}\right) \implies \operatorname{Im}(C) = \left\{ \left(\begin{smallmatrix} x_1\\ x_2\\ x_3 \end{smallmatrix}\right) \middle| x_1, x_2, x_3 \in \mathbf{S} \right\}$$

   Hence, the module generated by the columns of C is free and has cardinality $|\operatorname{Im}(C)| = 9^3$. Thus, $d(A, B) = \operatorname{rk}(A - B) = \operatorname{rk}(C) = \log_9(|\operatorname{Im}(C)|) = 3$.

3.2 Cardinal Rank Metric of Codewords

Let $B = \{\xi_1, \dots, \xi_r\}$ be a free basis of $\mathbf{R}$ over $\mathbf{S}$. The coordinate vector of $a \in \mathbf{R}$ relative to the basis B, denoted by $[a]_B$, is a codeword $(\alpha_1, \alpha_2, \dots, \alpha_r)^\top$ over $\mathbf{S}$ provided $a = \sum\limits_{i=1}^{r} \alpha_i \cdot \xi_i$. Similarly, $[\mathbf{a}]_B = ([a_1]_B \mid \dots \mid [a_m]_B) \in \mathbf{S}^{r \times m}$ is said to be the coordinate matrix of $\mathbf{a} = (a_1, \dots, a_m) \in \mathbf{R}^m$ relative to B, where $m \in \mathbb{N}$. Straightforwardly, $[\cdot]_B : \mathbf{R}^m \to \mathbf{S}^{r \times m}$ is a module isomorphism since $\ker([\cdot]_B) = \{\mathbf{o}\}$, $[\mathbf{a}]_B + [\mathbf{b}]_B = [\mathbf{a} + \mathbf{b}]_B$ and $[s \cdot \mathbf{a}]_B = s \cdot [\mathbf{a}]_B$ for any $\mathbf{a}, \mathbf{b} \in \mathbf{R}^m$ and $s \in \mathbf{S}$.

Lemma 51. The cardinal rank of the coordinate matrix of $\mathbf{a}$ and the induced cardinal rank distance between the coordinate matrices of $\mathbf{a}$ and $\mathbf{b}$ are basis invariant for any $m \in \mathbb{N}$ and $\mathbf{a}, \mathbf{b} \in \mathbf{R}^m$.

Proof. Let $m \in \mathbb{N}$ and $B = \{\xi_1, \dots, \xi_r\}, C = \{\zeta_1, \dots, \zeta_r\}$ be two free bases of $\mathbf{R}$ over $\mathbf{S}$. Set $Q = ([\zeta_1]_B \mid \dots \mid [\zeta_r]_B) \in \mathbf{S}^{r \times r}$. Due to both B and C being the free bases, the matrix Q is invertible by **Lemma 34** applied to the trasposed Q. Observe that $[\mathbf{c}]_B = Q \cdot [\mathbf{c}]_C$ for all $\mathbf{c} \in \mathbf{R}^m$. Choose any $\mathbf{a}, \mathbf{b} \in \mathbf{R}^m$. Compute the cardinal rank of $\mathbf{a}$ $\operatorname{rk}([\mathbf{a}]_C) = \operatorname{rk}(Q^{-1} \cdot [\mathbf{a}]_C) \overset{\mathbf{48.3}}{=} \operatorname{rk}([\mathbf{a}]_B)$ and the distance between $\mathbf{a}$ and $\mathbf{b}$

$$d([\mathbf{a}]_C, [\mathbf{b}]_C) = \operatorname{rk}([\mathbf{a}]_C - [\mathbf{b}]_C) = \operatorname{rk}([\mathbf{a} - \mathbf{b}]_C) = \operatorname{rk}([\mathbf{a} - \mathbf{b}]_B) = d([\mathbf{a}]_B, [\mathbf{b}]_B).$$

□

Let $\mathbf{a} \in \mathbf{R}^m$ for a positive integer m. **Lemma 51** justifies defining the cardinal rank of $\mathbf{a}$ as the cardinal rank of its coordinate matrix relative to any free basis of $\mathbf{R}$ over $\mathbf{S}$.

Definition 52. Let $m \in \mathbb{N}$ and B be a free basis of $\mathbf{R}$ over $\mathbf{S}$. The *cardinal rank* of $\mathbf{a} \in \mathbf{R}^m$ is $\operatorname{rk}(\mathbf{a}) = \operatorname{rk}([\mathbf{a}])_B$ and the *cardinal rank distance* between $\mathbf{a}, \mathbf{b} \in \mathbf{R}^m$ is $\mathrm{d}_{\mathcal{R}}(\mathbf{a}, \mathbf{b}) = \operatorname{rk}(\mathbf{a} - \mathbf{b})$.

Remark. $(\mathbf{R}^m, \mathrm{d}_{\mathcal{R}})$ is a metric space in accordance with **Corollary 50**.

Let $\xi \in \mathbf{R}$ have order $p^r - 1$. Due to **Section 1.2**, $\Xi = (1, \xi, \dots, \xi^{r-1})$ is a free basis of $\mathbf{R}$ over $\mathbf{S}$. Choose $a \in \mathbf{R}$. Let $a_0, a_1, \dots, a_{r-1} \in \mathbf{S}$ satisfy $a = \sum\limits_{i=0}^{r-1} a_i \xi^i$. Denote by $a_{r-1}{:}\dots{:}a_1{:}a_0$ the aditive representation of a. Notice that this representation of a almost coincides with $[a]_\Xi$. Now, we depict the cardinal rank of codewords and the induced distance between them utilising *Example* 12.

Example 13. Let $\mathbf{S} = \mathrm{GR}(3^2, 1) = \mathbb{Z}_{3^2}$ and $\mathbf{R} = \mathrm{GR}(3^2, 3) = \mathbf{S}[\xi]$ with operations defined modulo polynomial $G_{3,3}(x) = x^3 + 2x + 1 \in \mathbf{S}[x]$, where ξ is the formal root of $G_{3,3}$ of the order $3^3 - 1 = 26$. Consider a free basis $B = \{1, \xi, \xi^2\}$ of the ring $\mathbf{R}$ over $\mathbf{S}$. Compute the cardinal ranks $\operatorname{rk}(\mathbf{a}), \operatorname{rk}(\mathbf{b})$ and the cardinal rank distance $\mathrm{d}_{\mathcal{R}}(\mathbf{a}, \mathbf{b})$ for $\mathbf{a} = (3{:}0{:}0, 0{:}0{:}8, 0{:}6{:}2, 6{:}3{:}2)$, $\mathbf{b} = (8{:}0{:}1, 0{:}4{:}0, 0{:}3{:}6, 6{:}3{:}0) \in \mathbf{R}^4$.

1. $[\mathbf{a}]_B = \left(\begin{smallmatrix} 0 & 8 & 2 & 2 \\ 0 & 0 & 6 & 3 \\ 3 & 0 & 0 & 6 \end{smallmatrix}\right) \implies \operatorname{rk}(\mathbf{a}) = \operatorname{rk}([\mathbf{a}]_B) \overset{\mathit{Ex}\ 12.1}{=} 2,$

2. $[\mathbf{b}]_B = \left(\begin{smallmatrix} 1 & 0 & 6 & 0 \\ 0 & 4 & 3 & 3 \\ 8 & 0 & 0 & 6 \end{smallmatrix}\right) \implies \operatorname{rk}(\mathbf{b}) = \operatorname{rk}([\mathbf{b}]_B) \overset{\mathit{Ex}\ 12.2}{=} \frac{5}{2},$

3. $\mathbf{c} = \mathbf{a} - \mathbf{b} = (4{:}0{:}8, 0{:}5{:}8, 0{:}3{:}5, 0{:}0{:}2) \implies [\mathbf{c}]_B = \left(\begin{smallmatrix} 8 & 8 & 5 & 2 \\ 0 & 5 & 3 & 0 \\ 4 & 0 & 0 & 0 \end{smallmatrix}\right)$
$\implies \mathrm{d}_{\mathcal{R}}\left(\mathbf{a}, \mathbf{b}\right) = \mathrm{rk}\left(\mathbf{a} - \mathbf{b}\right) = \mathrm{rk}\left(\mathbf{c}\right) = \mathrm{rk}\left([\mathbf{c}]_B\right) \overset{Ex\ 12.3}{=} 3.$

Theorem 48 proposes that multiplying any matrix A by an invertible matrix B, for which the product $A \cdot B$ is defined, does not change the cardinal rank of A. We generalise this property to the cardinal rank of a codeword.

Lemma 53. Let $m \in \mathbb{N}$, $\mathbf{x} \in \mathbf{R}^m$ and $T \in \mathbf{S}^{m \times m}$ be a invertible matrix. Then, $\mathrm{rk}(\mathbf{x}) = \mathrm{rk}(\mathbf{x} \cdot T)$.

Proof. Let B be a free basis of $\mathbf{R}$ over $\mathbf{S}$. If we show that $[\mathbf{x} \cdot T]_B = [\mathbf{x}]_B \cdot T$ then the conclusion follows from **Theorem 48**. Choose $i \in \mathbb{N}$ such that $i \leq m$ and compute $[\mathbf{x} \cdot \mathbf{T}^c_i]_B = \left[\sum\limits_{j=1}^{m} x_j \cdot T_{ji}\right]_B = \sum\limits_{j=1}^{m} [x_j \cdot T_{ji}]_B = \sum\limits_{j=1}^{m} [x_j]_B \cdot T_{ji} = [\mathbf{x}]_B \cdot \mathbf{T}^c_i$. Hence,
$[\mathbf{x} \cdot T]_B = \left([\mathbf{x} \cdot \mathbf{T}^c_1]_B \,\middle|\, \ldots \,\middle|\, [\mathbf{x} \cdot \mathbf{T}^c_m]_B\right) = \left([\mathbf{x}]_B \cdot \mathbf{T}^c_1 \,\middle|\, \ldots \,\middle|\, [\mathbf{x}]_B \cdot \mathbf{T}^c_m\right) = [\mathbf{x}]_B \cdot T.$ □

Let $\mathbb{K} = \mathbf{R}/_{p\mathbf{R}}$ and $\mathbb{L} = \mathbf{S}/_{p\mathbf{S}}$ be the residue fields of $\mathbf{R}$ and $\mathbf{S}$ respectively. Apparently, $\mathbb{L}$ is a subfield of $\mathbb{K}$ since $\mathbf{S}$ is the subring of $\mathbf{R}$. Recall the Teichmuller sets $\mathcal{T}_r$ of $\mathbf{R}$ and $\mathcal{T}$ of $\mathbf{S}$ from **Definition 16**. Then, the field isomorphisms $\mathcal{T}_r \simeq \mathbb{K} \simeq \mathbb{F}_{p^r}$ and $\mathcal{T} \simeq \mathbb{L} \simeq \mathbb{F}_p$ are derived from the remark in **Section 1.2** and the paragraph above **Corollary 17**. Let $B = \{\xi_1, \ldots, \xi_r\}$ be a free basis of $\mathbf{R}$ over $\mathbf{S}$. If possible, we aim to propose a more direct way of computing the cardinal rank. Let this notation be established henceforth.

Theorem 54. Let $m \in \mathbb{N}$ and $\mathbf{x} \in \mathbf{R}^m$ of the height i for $i \in \mathbb{N}, i \leq n$. Then, $\mathrm{rk}(\mathbf{x}) \geq i \cdot \mathrm{rk}\left(p^{i-1} \cdot \mathbf{x}\right) = i \cdot \frac{c}{n}$, where $c = \dim_{\mathcal{T}}\left(\mathrm{Im}([p^{i-1}\mathbf{x}]_B)\right)$. Furthermore, the equality $\mathrm{rk}(\mathbf{x}) = i \cdot \mathrm{rk}(p^{i-1} \cdot x)$ is achieved for non-zero $\mathbf{x}$ if and only if there is no coordinate of $\mathbf{x}$ divisible by p^{n-i+1}.

Proof. Let $m \in \mathbb{N}$ and $x \in \mathbf{R}^m$ be of the height $i \in \mathbb{N}, i \leq n$. Define a matrix $X = [\mathbf{x}]_B \in \mathbf{S}^{r \times m}$. Set $\mathbf{y} = p^{i-1} \cdot \mathbf{x} \in \mathrm{Soc}(\mathbf{R}^m)$ and $Y = [\mathbf{y}]_B \in \mathbf{S}^{r \times m}$. It results in $Y = p^{i-1} \cdot X$ and $\mathrm{Im}(Y) \subseteq \mathrm{Soc}(\mathrm{Im}(X))$, which implies

$$\mathrm{rk}(\mathbf{y}) = \log_{p^n}(|\mathrm{Im}(Y)|) = \log_{p^n}(p^c) = \frac{c}{n}, \tag{3.1}$$

where c is the dimension of the vector space $\mathrm{Im}(Y)$ over $\mathcal{T}$.

Let $(p^{n-1}\beta_1, \ldots, p^{n-1}\beta_c)$ be a free basis of $\mathrm{Im}(Y)$ over $\mathcal{T}$ and M be a module generated by $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_c)$ over $\mathbf{S}$, which is free in light of **Lemma 28**. Compute $\mathbf{v} \in \mathbf{R}^m$ of height n satisfying $\mathbf{x} = p^{n-i} \cdot \mathbf{v}$ by **Algorithm 4**. Firstly, assume that no coordinate of $\mathbf{v}$ is divisible by p, which implies $\mathrm{Im}(V)$ is free, where $V = [\mathbf{v}]_B$. However, $\mathrm{Soc}(\mathrm{Im}(V)) = p^{n-1} \cdot \mathrm{Im}(V) = \mathrm{Im}(Y) = \mathrm{Soc}(M)$ and both $\mathrm{Im}(V)$ and M are free $\mathbf{S}$-submodules of $\mathbf{S}^l$. Thus, $\mathrm{Im}(V) = M$ and

$$\mathrm{rk}(\mathbf{v}) = \log_{p^n}(|M|) = \log_{p^n}\left(p^{n \cdot c}\right) = c = n \cdot \mathrm{rk}(\mathbf{y}). \tag{3.2}$$

Return attention to $\mathbf{x} = p^{n-i} \cdot \mathbf{v}$ and the $\mathbf{S}$-module $\mathrm{Im}(X) = p^{n-i} \cdot M = \langle \boldsymbol{\beta}' \rangle$ for $\boldsymbol{\beta}' = (p^{n-i}\beta_1, \ldots, p^{n-i}\beta_c)$. Note that $\boldsymbol{\beta}'$ is already a minimal basis of $\mathrm{Im}(X)$

as $\boldsymbol{\beta}$ is the free basis of M. As a consequence,

$$\begin{aligned}\operatorname{rk}(\mathbf{x}) = \log_{p^n}(|\operatorname{Im}(X)|) &= \log_{p^n}\left(\left|\left\{\sum_{l=1}^{c} s_l \cdot p^{n-i} \cdot \beta_l \,\middle|\, s_1, \ldots, s_l \in \mathbf{S}\right\}\right|\right) \\ &= \log_{p^n}\left(\left|\left\{\sum_{l=1}^{c} s_l \cdot \beta_l \,\middle|\, s_1, \ldots, s_l \in p^{n-i} \cdot \mathbf{S}\right\}\right|\right) = \log_{p^n}(p^{i \cdot c}) = \frac{i \cdot c}{n}\end{aligned} \tag{3.3}$$

where p^i is the cardinality of $p^{n-i} \cdot \mathbf{S}$.

Secondly, assume a coordinate of $\mathbf{v}$ divisible by p exists. Compute $\mathbf{u}, \mathbf{w} \in \mathbf{R}^m$, which satisfies $\mathbf{v} = \mathbf{u} + \mathbf{w}$, no coordinate of $\mathbf{u}$ is divisible by p and $\mathbf{w}$ has height $h \in \mathbb{N}, h < n$. Since $p^{n-1} \cdot \mathbf{u} = p^{n-1} \cdot \mathbf{v} - p^{n-1}\mathbf{w} = p^{n-1} \cdot \mathbf{v}$, then $\operatorname{rk}(\mathbf{u}) \overset{(3.2)}{=} c$ and $\operatorname{rk}(p^{n-i}\mathbf{u}) \overset{(3.3)}{=} \frac{i \cdot c}{n}$ by the already proven part. Clearly, $p^l \cdot \operatorname{Im}(U) \subset p^l \cdot \operatorname{Im}(V)$, where $U = [\mathbf{u}]_B$ and $l, 0 \leq l < h$. Finally, $\operatorname{rk}\left(p^l \mathbf{u}\right) < \operatorname{rk}\left(p^l \mathbf{v}\right)$.

□

The previous theorem states the lower bound for the cardinal rank of element $\mathbf{x}$ with height $h \in \mathbb{N}, h \leq n$. However, the equality within the bound is achieved if and only if the coordinates of $\frac{\mathbf{x}}{p^{n-h}}$ generates a free $\mathbf{S}$-module. On the other hand, it is always possible to use **Algorithm 7** grounded on **Corollary 49**.

Rewind the ring epimorhism $^{-} : \mathbf{R} \to \mathbb{K}, a \mapsto a + p\mathbf{R}$, and the induced module epimorphism $^{-m} : \mathbf{R}^m \to \mathbb{K}^m$, $\mathbf{a} \mapsto (\overline{a_1}, \ldots, \overline{a_m})$ for some $m \in \mathbb{N}$. **Theorem 15** about the p-adic representation implies that $\overline{\mathcal{T}_r} = \mathbb{K}$ and $\overline{\mathcal{T}} = \mathbb{L}$. Remark that the operations on $\mathcal{T}_r$ were determined utilising the ring epimorphism $^{-}$. Then, $\overline{B} = \left\{\overline{\xi}_1, \ldots, \overline{\xi}_r\right\}$ is a basis of the field $\mathbb{K}$ over $\mathbb{L}$. To clarify over which ring is the cardinal rank and the induced distance meant, denote for each $\mathbf{a}, \mathbf{b} \in \mathbf{R}^m$

$$\operatorname{rk}_{\mathbf{S}}(\mathbf{a}) = \log_{p^n}\left(|\operatorname{Im}_{\mathbf{S}}([\mathbf{a}]_B)|\right) \quad \text{and} \quad \mathrm{d}_{\mathbf{S}}(\mathbf{a}, \mathbf{b}) = \operatorname{rk}_{\mathbf{S}}(\mathbf{a} - \mathbf{b}), \tag{3.4}$$

$$\operatorname{rk}_{\mathbb{L}}\left(\overline{\mathbf{a}}^m\right) = \log_p\left(|\operatorname{Im}_{\mathbb{L}}([\overline{\mathbf{a}}^m]_{\overline{B}})|\right) \quad \text{and} \quad \mathrm{d}_{\mathbb{L}}\left(\overline{\mathbf{a}}^{\mathbf{m}}, \overline{\mathbf{b}}^{\mathbf{m}}\right) = \operatorname{rk}_{\mathbb{L}}\left(\overline{\mathbf{a}}^{\mathbf{m}} - \overline{\mathbf{b}}^{\mathbf{m}}\right). \tag{3.5}$$

Let $\mathcal{C}$ be an $[m, l]_{\mathbf{R}}$-code and $\mathbf{a}, \mathbf{b}$ be codewords of $\mathcal{C}$. Thus, using the proposed notation, the cardinal rank of $\mathbf{a} \in \mathbf{R}^m$ over $\mathbf{S}$ is $\operatorname{rk}(\mathbf{a}) = rk_{\mathbf{S}}(\mathbf{a})$, and the cardinal rank distance between $\mathbf{a}, \mathbf{b} \in \mathbf{R}^m$ over $\mathbf{S}$ is $\mathrm{d}_{\mathcal{R}}(\mathbf{a}, \mathbf{b}) = \mathrm{d}_{\mathbf{S}}(\mathbf{a}, \mathbf{b})$. In the same manner, the minimal cardinal distance of $\mathcal{C}$ over $\mathbf{S}$ is $\mathrm{d}_{\mathcal{R}}(\mathcal{C}) = \mathrm{d}_{\mathbf{S}}(\mathcal{C})$. Denote by $\mathcal{E} = \overline{\mathcal{C}}^m$ the code of length m over $\mathbb{K}$ and by $\mathbf{d} = \overline{\mathbf{a}}^m, \mathbf{e} = \overline{\mathbf{b}}^m$ its codewords. Hence, the cardinal rank of $\mathbf{d} \in \mathbb{K}^m$ over $\mathbb{L}$ is $\operatorname{rk}(\mathbf{d}) = \operatorname{rk}_{\mathbb{L}}(\mathbf{d})$, the cardinal rank distance between $\mathbf{d}, \mathbf{e} \in \mathbb{K}^m$ over $\mathbb{L}$ is $\mathrm{d}_{\mathcal{R}}(\mathbf{d}, \mathbf{e}) = \mathrm{d}_{\mathbb{L}}(\mathbf{d}, \mathbf{e})$, and the minimal cardinal distance of $\mathcal{E}$ over $\mathbb{L}$ is $\mathrm{d}_{\mathcal{R}}(\mathcal{E}) = \mathrm{d}_{\mathbb{L}}(\mathcal{E})$. Hopefully, the reason why rk and $\mathrm{d}_{\mathcal{R}}$ are distinguished based on the ring over which they are taken is clear now.

Claim 55. Let $m \in \mathbb{N}$, $\mathbf{a} \in \mathbf{R}^m$. Then $\operatorname{rk}_{\mathbf{S}}(\mathbf{a}) > \operatorname{rk}_{\mathbf{S}}(p^{n-1}\mathbf{a}) = \frac{\operatorname{rk}_{\mathbb{L}}(\overline{\mathbf{a}}^m)}{n}$.

Proof. Let $m \in \mathbb{N}$ and $\mathbf{a} \in \mathbf{R}^m$ be given. Compute $\mathbf{d} \in \mathbf{R}^m$ with all coordinates from $\mathcal{T}_r$ and $\mathbf{e} \in (p\mathbf{R})^m$ such that $\mathbf{a} = \mathbf{d} + \mathbf{e}$, which is possible due to **Theorem 15** being used for each entry of $\mathbf{a}$. Denote the matrices $A = [\mathbf{a}]_B$, $D = [\mathbf{d}]_B \in \mathbf{S}^{r \times m}$ and $C = [\overline{\mathbf{a}}^m]_{\overline{B}} \in \mathbb{L}^{r \times m}$. It can be directly derived that $p^{n-1}\mathbf{a} = p^{n-1}\mathbf{d}$ and $p^{n-1}A = [p^{n-1}\mathbf{a}]_B = [p^{n-1}\mathbf{d}]_B = p^{n-1}D$.

Define a map $\varpi = \operatorname{Soc}(\mathbf{S}^r) \to \mathbb{L}^r$ for any $\mathbf{x} \in \mathbf{S}^r$ by $\varpi(p^{n-1} \cdot \mathbf{x}) = \overline{\mathbf{x}}^r$. Drawn from the proof of **Claim 40**, ϖ is a module isomorphism. Observe that

$\varpi(p^{n-1}\mathbf{A}_i^c) = \varpi(p^{n-1}\mathbf{D}_i^c) = \overline{[d_i]_B}^r = \left[\overline{d_i}\right]_{\overline{B}} = [\overline{a_i}]_{\overline{B}} = \mathbf{C}_i^c$ for any $i = 1, \dots, m$, where it was used that $\overline{\mathbf{a}}^m = \overline{\mathbf{d}}^m$, and the basis $\overline{B}$ of $\mathbb{K}$ over $\mathbb{L}$ is the projection of the basis B of $\mathbf{R}$ over $\mathbf{S}$. Furthermore, $\varpi(\mathrm{Im}_{\mathbf{S}}(p^{n-1}A)) = \mathrm{Im}_{\mathbb{L}}(C)$ since for any $\mathbf{x} \in \mathrm{Im}_{\mathbf{S}}(p^{n-1}A)$ there exist coefficients $t_1, \dots, t_m \in \mathcal{T}$ such that $\mathbf{x} = \sum_{i=1}^{m} t_i p^{n-1}\mathbf{A}_i^c$ and $\varpi(\mathbf{x}) = \sum_{i=1}^{m} \varpi(t_i p^{n-1}\mathbf{A}_i^c) = \sum_{i=1}^{m} \overline{t_i \mathbf{D}_i^c}^r = \sum_{i=1}^{m} \overline{t_i}\mathbf{C}_i^c$. Conclude from **Theorem 54** that $\mathrm{rk}_{\mathbf{S}}(\mathbf{a}) \geq n \cdot \mathrm{rk}_{\mathbf{S}}(p^{n-1}\mathbf{a}) > \mathrm{rk}_{\mathbf{S}}(p^{n-1}\mathbf{a})$ and

$$\mathrm{rk}_{\mathbf{S}}(p^{n-1}\mathbf{a}) = \log_{p^n}(|\mathrm{Im}_{\mathbf{S}}(p^{n-1}A)|) = \frac{\log_p(|\mathrm{Im}_{\mathbb{L}}(C)|)}{\log_p(p^n)} = \frac{\mathrm{rk}_{\mathbb{L}}(\overline{\mathbf{a}}^m)}{n},$$

which finalises the proof.

□

Let $\mathbf{a} \in \mathbf{R}^m$. Regard two $\mathbf{S}$-modules $M = \mathrm{Im}([\mathbf{a}]_B)$ and $N = \langle a_1, \dots, a_m \rangle_{\mathbf{S}}$. Clearly, both of them are fully determined by the codeword $\mathbf{a}$. Denote by $\boldsymbol{\beta} \in \mathbf{R}^m$ the codeword composed of the basis B elements. Consider a map $\nu : M \to N$ defined as $\nu(\mathbf{x}) = \boldsymbol{\beta} \cdot \mathbf{x}^\top$ for $\mathbf{x} \in M$, which appears to be a module homomorphism. In addition, ν is bijective since $\nu^{-1}\left(\sum_{i=1}^{m} z_i a_i\right) = \sum_{i=1}^{m} z_i [a_i]_B$ for $z_1, \dots, z_m \in \mathbf{S}$ as $\boldsymbol{\beta} \cdot [\mathbf{a}]_B = \mathbf{a}$. Consequently, we have $\mathrm{rank}(M) = \mathrm{rank}(N)$. We finish this section by relating the rank of N to the cardinal rank of $\mathbf{a}$.

Corollary 56. Let $A = \langle a_1, \dots, a_m \rangle_{\mathbf{S}}$ be the $\mathbf{S}$-submodule of $\mathbf{R}$ for some $m \in \mathbb{N}$ and $\mathbf{a} \in \mathbf{R}^m$. Then $\mathrm{rk}(\mathbf{a}) \leq \mathrm{rank}(A)$ and $\mathrm{rank}(A) \leq \lfloor n \cdot \mathrm{rk}(\mathbf{a}) \rfloor$.

Proof. Choose $m \in \mathbb{N}$ and $\mathbf{a} \in \mathbf{R}^m$. Put $A = \langle a_1, \dots, a_m \rangle_{\mathbf{S}}$ and $c = \mathrm{rk}(\mathbf{a})$. The first inequality $c \leq \mathrm{rank}(A)$ is derived from **Theorem 48**. Next, based on **Claim 55**, $\mathrm{rk}_{\mathbb{L}}(\overline{\mathbf{a}}^m) < n \cdot c$, which can be rewritten as $\dim_{\mathbb{L}}\left(\overline{A}\right) \leq \lfloor n \cdot c \rfloor$. According to **Claim 40**, $\mathrm{Soc}(A) \simeq \overline{A}$ and therefore $\dim_{\mathcal{T}}(\mathrm{Soc}(A)) = \dim_{\mathbb{L}}\left(\overline{A}\right)$. The rest follows from $\mathrm{rank}(A) = \mathrm{rank}(\mathrm{Soc}(A)) = \dim_{\mathcal{T}}(\mathrm{Soc}(A))$.

□

3.3 Cardinal Rank Metric Codes

When linear code $\mathcal{C}$ of length $m \in \mathbb{N}$ over $\mathbf{R} = \mathrm{GR}(p^n, r)$ uses the cardinal rank metric $\mathrm{d}_{\mathcal{R}}$ as the distance of its two codewords, $\mathcal{C}$ is called a *cardinal rank metric code*. Additionally, $\mathrm{d}_{\mathcal{R}}(\mathcal{C}) = \min\{\mathrm{d}_{\mathcal{R}}(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathcal{C}; \mathbf{a} \neq \mathbf{b}\}$ is the *minimum (cardinal rank) distance* of $\mathcal{C}$ instead of $\mathrm{d}_{\mathcal{H}}(\mathcal{C})$.

Briefly turn to the standard theory of error-correcting codes over finite fields, which has among its main goals finding the largest possible code for the given minimal distance. Definitely, the most known upper bound for the size of a code $\mathcal{C}$ of the length $n \in \mathbb{N}$ over $\mathbb{F}_q$ with the minimal Hamming distance $d \in \mathbb{N}$ is the Singleton bound which states that $|\mathcal{C}| \leq q^{n-d+1}$. Moreover, the Singleton bound can be restated as $\mathrm{d}_{\mathcal{H}}(\mathcal{C}) \leq n - k + 1$ for a linear code $\mathcal{C}$ of the dimension $k \in \mathbb{N}$. Lastly, linear codes that achieve equality in the bound are called maximum distance separable (MDS) codes. Analogically, the same inequality holds also for the rank distance defined as $\mathrm{d}_{\mathcal{R}}(\mathbf{c}_1, \mathbf{c}_2) = \mathrm{rank}([\mathbf{c}_1 - \mathbf{c}_2]_B)$ for codewords

$\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$, where B is some basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ for prime $p, p \mid q$. Maximum rank distance (MRD) codes are linear codes which reach the upper bound with the rank distance. Additional information concerning linear codes over finite fields can be found in the book by Bruen et al. [15].

Remark. It is not difficult to notice that the cardinal rank distance equals the rank distance for linear codes over a finite field.

Theorem 57 (Singleton-like bound)**.** Let $l, m \in \mathbb{N}$ and $\mathcal{C}$ be a cardinal rank metric $[m, l]_{\mathbf{R}}$-code. There exist integers $e_1, \ldots, e_m \in \{0, \ldots, n-1\}$ and a free basis $V = (\mathbf{v}_1, \ldots, \mathbf{v}_l)$ fulfilling $\mathcal{C} = \langle p^{e_1}\mathbf{v}_1, \ldots, p^{e_l}\mathbf{v}_l \rangle_{\mathbf{R}}$. Let $\mathcal{D} = \langle V \rangle_{\mathbf{R}}$. Then,

$$\mathrm{d}_{\mathbf{S}}(\mathcal{C}) = \mathrm{d}_{\mathbf{S}}(\mathrm{Soc}(\mathcal{C})) = \frac{\mathrm{d}_{\mathbb{L}}\left(\overline{\mathcal{D}}^m\right)}{n} \leq \frac{m-l+1}{n}. \tag{3.6}$$

Proof. **Theorem 30** states that there exist a free basis $V = (\mathbf{v}_1, \ldots, \mathbf{v}_l)$ of an-$\mathbf{R}$-submodule of $\mathbf{R}^m$ and exponents $e_1, \ldots, e_l \in \{0, 1, \ldots, n-1\}$, which satisfy $\mathcal{C} = \bigoplus_{i=1}^{l} p^{e_i}\mathbf{v}_i\mathbf{R}$. Consider a free linear code $\mathcal{D}$ generated by V. According to the Singleton bound for the $[m, l]_{\mathbb{K}}$-code $\overline{\mathcal{D}}^m$, we have $\mathrm{d}_{\mathcal{H}}(\overline{\mathcal{D}}^m) \leq m-l+1$. If we manage to prove that $\mathrm{d}_{\mathbf{S}}(\mathcal{C}) = \frac{\mathrm{d}_{\mathbb{L}}(\overline{\mathcal{D}}^m)}{n}$ and $\mathrm{d}_{\mathbb{L}}\left(\overline{\mathcal{D}}^m\right) \leq \mathrm{d}_{\mathcal{H}}(\overline{\mathcal{D}}^m)$ then the minimal cardinal rank distance of $\mathcal{C}$ is $\mathrm{d}_{\mathcal{R}}(\mathcal{C}) = \mathrm{d}_{\mathbf{S}}(\mathcal{C}) = \frac{\mathrm{d}_{\mathbb{L}}(\overline{\mathcal{D}}^m)}{n} \leq \frac{\mathrm{d}_{\mathcal{H}}(\overline{\mathcal{D}}^m)}{n} \leq \frac{m-l+1}{n}$.

Let B be a free basis of $\mathbf{R}$ over $\mathbf{S}$. Thus, $\overline{B}$ is a basis of the field $\mathbb{K}$ over $\mathbb{L}$. Choose any $\mathbf{a}, \mathbf{b} \in \overline{\mathcal{D}}^m$ and denote by $M \in \mathbb{L}^{r \times m}$ the coordinate matrix $[\mathbf{a} - \mathbf{b}]_{\overline{B}}$. Let us direct attention to the cardinal rank distance between $\mathbf{a}$ and $\mathbf{b}$:

$$\begin{aligned}\mathrm{d}_{\mathbb{L}}(\mathbf{a}, \mathbf{b}) = \mathrm{rk}_{\mathbb{L}}(\mathbf{a} - \mathbf{b}) = \log_p\left(|\mathrm{Im}_{\mathbb{L}}(M)|\right) = \mathrm{rank}(M) = \dim_{\mathbb{L}}\left(\sum_{i=1}^{m} \mathbf{M}_i^c \cdot \mathbb{L}\right)\\ \leq |\{\mathbf{M}_i^c \mid i \in \mathbb{N}, i \leq m : \mathbf{M}_i^c \neq \mathbf{o}\}| = \mathrm{w}_{\mathcal{H}}(\mathbf{a} - \mathbf{b}) = \mathrm{d}_{\mathcal{H}}(\mathbf{a}, \mathbf{b})\end{aligned}$$

Next, find $\mathbf{c} \in \mathcal{C}$ meeting the condition $\mathrm{rk}_{\mathbf{S}}(\mathbf{c}) = \mathrm{d}_{\mathbf{S}}(\mathcal{C})$, which may be done as $\mathrm{d}_{\mathbf{S}}(\mathcal{C}) = \min\{\mathrm{rk}_{\mathbf{S}}(\mathbf{a} - \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathcal{C}; \mathbf{a} \neq \mathbf{b}\} = \min\{\mathrm{rk}_{\mathbf{S}}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C} \setminus \{\mathbf{o}\}\}$. Since $\mathrm{Im}_{\mathbf{S}}\left([p \cdot \mathbf{c}]_B\right) \subset \mathrm{Im}_{\mathbf{S}}\left([\mathbf{c}]_B\right)$ and $\mathrm{rk}_{\mathbf{S}}(p \cdot \mathbf{c}) < \mathrm{rk}_{\mathbf{S}}(\mathbf{c})$, it is now evident that $p \cdot \mathbf{c} = \mathbf{o}$ and $\mathbf{c} \in \mathrm{Soc}(\mathcal{C})$. Hence, $\mathrm{d}_{\mathbf{S}}(\mathcal{C}) = \mathrm{d}_{\mathbf{S}}(\mathrm{Soc}(\mathcal{C}))$. Execute **Algorithm 4** on $\mathbf{c}$ to obtain $\mathbf{d} \in \mathcal{D}$ of height n satisfying $\mathbf{c} = p^{n-1} \cdot \mathbf{d}$. Additionally, **Claim 55** asserts that $\mathrm{rk}_{\mathbf{S}}(p^{n-1}\mathbf{d}) = \frac{\mathrm{rk}_{\mathbb{L}}\left(\overline{\mathbf{d}}^m\right)}{n}$. Assume, for a contradiction, there exists $\mathbf{f} \in \mathcal{D}$ such as $0 < \mathrm{rk}_{\mathbb{L}}\left(\overline{\mathbf{f}}^m\right) < \mathrm{rk}_{\mathbb{L}}\left(\overline{\mathbf{d}}^m\right)$. In this scenario, $p^{n-1}\mathbf{f}$ must remain non-zero, because if $p^{n-1}\mathbf{f} = \mathbf{o}$ then $\mathbf{f} \in p\mathcal{D}$ and $\overline{\mathbf{f}}^m = \mathbf{o}$, which contradicts $\mathrm{rk}_{\mathbb{L}}\left(\overline{\mathbf{f}}^m\right) > 0$. Moreover, $p^{n-1}\mathbf{f} \in \mathrm{Soc}(\mathcal{C}) \setminus \{\mathbf{o}\}$ and $\mathrm{rk}_{\mathbf{S}}(p^{n-1} \cdot \mathbf{f}) < \mathrm{rk}_{\mathbf{S}}(p^{n-1} \cdot \mathbf{d})$, a contradiction with the minimality of $\mathrm{rk}(\mathbf{c})$. Finally, it is possible to conclude $\mathrm{d}_{\mathbf{S}}(\mathcal{C}) = \mathrm{d}_{\mathbf{S}}(\mathrm{Soc}(\mathcal{C})) = \mathrm{rk}_{\mathbf{S}}(\mathbf{c}) = \frac{\mathrm{rk}_{\mathbb{L}}\left(\overline{\mathbf{d}}^m\right)}{n} = \frac{\mathrm{d}_{\mathbb{L}}(\overline{\mathcal{D}}^m)}{n}$.

□

Corollary 58. If $\mathrm{Soc}(\mathcal{C}_1) = \mathrm{Soc}(\mathcal{C}_2)$, where $\mathcal{C}_1, \mathcal{C}_2$ are cardinal rank metric codes of the same length over $\mathbf{R}$, then $\mathrm{d}_{\mathcal{R}}(\mathcal{C}_1) = \mathrm{d}_{\mathcal{R}}(\mathcal{C}_2)$.

Proof. Absolutely, $\mathrm{d}_{\mathcal{R}}(\mathcal{C}_1) \overset{(3.6)}{=} \mathrm{d}_{\mathcal{R}}(\mathrm{Soc}(\mathcal{C}_1)) = \mathrm{d}_{\mathcal{R}}(\mathrm{Soc}(\mathcal{C}_2)) \overset{(3.6)}{=} \mathrm{d}_{\mathcal{R}}(\mathcal{C}_2)$.

□

3.4 Maximum Cardinal Rank Distance Codes

A class of cardinal rank metric codes which achieve the Singleton-like bound (3.6) is studied in this part. The class clearly generalises MRD codes over finite fields.

Definition 59. *Maximum cardinal rank distance (MCRD) codes* are cardinal rank metric codes, which reach equality in the Singleton-like bound (3.6).

Let $\mathcal{C}, \mathcal{D}$ be $[m,l]_{\mathbf{R}}$-codes such that $\mathcal{D}$ is free and $\operatorname{Soc}(\mathcal{C}) = \operatorname{Soc}(\mathcal{D})$. Thanks to the Singleton-like bound, $\mathrm{d}_{\mathbf{S}}(\mathcal{C}) = \frac{\mathrm{d}_{\mathbb{L}}(\overline{\mathcal{D}}^m)}{n}$. If $\mathcal{C}$ is MCRD then clearly $\overline{\mathcal{D}}^m$ is MRD and $\mathcal{D}$ is MCRD since $\mathrm{d}_{\mathbf{S}}(\mathcal{D}) = \frac{\mathrm{d}_{\mathbb{L}}(\overline{\mathcal{D}}^m)}{n}$. Remark that we know almost nothing about the code $\overline{\mathcal{C}}^m$ over $\mathbb{K}$.

Corollary 60. Let $l, m \in \mathbb{N}$ and $\mathcal{C}$ be a free cardinal rank metric $[m,l]_{\mathbf{R}}$-code. Then, $\mathrm{d}_{\mathbf{S}}(\mathcal{C}) = \frac{\mathrm{d}_{\mathbb{L}}(\overline{\mathcal{C}}^m)}{n}$, and $\mathcal{C}$ is MCRD if and only if $\overline{\mathcal{C}}^m$ is MRD.

Proof. According to **Claim 40**, it suffices to state $\operatorname{Soc}(\mathcal{C})$ is isomorphic to $\overline{\mathcal{C}}^m$ as $\mathcal{D}$ in **Claim 40** is exactly our code $\mathcal{C}$. Hence, we have $\mathrm{d}_{\mathbf{S}}(\mathcal{C}) \overset{(3.6)}{=} \frac{\mathrm{d}_{\mathbb{L}}(\overline{\mathcal{C}}^m)}{n}$ and the equivalence is the direct consequence of this equality.

□

Note that in the preceding proof, $\mathcal{C}$ equals the free code $\mathcal{D}$ only when $\mathcal{C}$ is also free. It may sound trivial, but it is vital to keep it in mind as for a codeword $\mathbf{c} \in \operatorname{Soc}(\mathcal{C})$, which satisfies $\operatorname{rk}(\mathbf{c}) = \mathrm{d}_{\mathcal{R}}(\mathcal{C})$, the codeword $p^{1-n} \cdot \mathbf{c}$ does not have to be located in a non-free MCRD $\mathcal{C}$. Accordingly, the projection $\overline{\mathbf{c}}^m$ does not have to be in $\overline{\mathcal{C}}^m$, i.e. $\overline{\mathcal{C}}^m$ is not required to be MRD. Let us introduce some necessary conditions for codes to be MCRD.

Theorem 61. Let $l, m \in \mathbb{N}$ satisfy $2l < m \leq \min(n, r)$, and $\mathcal{C}$ be a MCRD $[m,l]_{\mathbf{R}}$-code with a generator matrix $G \in \mathbf{R}^{l \times m}$ in the systematic form, i.e.

$$G = \begin{pmatrix} I_{k_0} & G_{0,1} & G_{0,2} & \dots & G_{0,n-1} & G_{0,n} \\ 0 & p \cdot I_{k_1} & p \cdot G_{1,2} & \dots & p \cdot G_{1,n-1} & p \cdot G_{1,n} \\ 0 & 0 & p^2 \cdot I_{k_2} & \dots & p^2 \cdot G_{2,n-1} & p^2 \cdot G_{2,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & p^{n-2} \cdot G_{n-2,n-1} & p^{n-2} \cdot G_{n-2,n} \\ 0 & 0 & 0 & \dots & p^{n-1} \cdot I_{k_{n-1}} & p^{n-1} \cdot G_{n-1,n} \end{pmatrix},$$

where $k_0, k_1, \dots, k_n \in \mathbb{N} \cup \{0\}$ satisfy $\sum_{i=0}^{n} k_i = m$, and $G_{i,j} \in \mathbf{R}^{k_i \times k_j}$, where $i, j \in \mathbb{Z}$, $0 \leq i < j < n$. Denote $d = \mathrm{d}_{\mathcal{R}}(\mathcal{C}) = \frac{m-l+1}{n}$, $m_i = \sum_{j=0}^{i-1} k_j$ and $M_i = \sum_{j=0}^{i} k_j - 1$ for every $i \in \{0, \dots, n\}$. Put $F = (p^i G_{i,n})_{i=0}^{n-1} \in \mathbf{R}^{l \times (m-l)}$.

1. The $[m-l, l]_{\mathbf{R}}$-code $\mathcal{D}$ generated by F is MCRD.
2. Every row of F may have maximally $l-1$ coordinates of height less than the height of the whole row.
3. $\forall i \in \{0, \dots, n-1\} \forall j \in \{m_i, \dots, M_i\} : (n-i)d \leq \operatorname{rk}\left(\mathbf{G}_j^r\right) \leq \frac{(n-i)(m-m_{i+1}+1)}{n}$.

Proof. 1. Assume, for a contradiction, that $\mathcal{D}$ is not MCRD. So, there exists a non-zero $\mathbf{f} \in \mathcal{D}$, which satisfies $\operatorname{rk}(\mathbf{f}) < \frac{m-2l+1}{n}$. Find $\mathbf{x} \in \mathbf{R}^l$ such that $\mathbf{f} = \mathbf{x} \cdot F$, and compute $\mathbf{c} = \mathbf{x} \cdot G = \begin{pmatrix} \mathbf{e} & \mathbf{f} \end{pmatrix} \in \mathcal{C}$ for appropriate $\mathbf{e} \in \mathbf{R}^l$. Obtain minimal $i = 0, 1, \dots, n$ fulfilling $p^i \cdot \mathbf{c} \in \operatorname{Soc}(\mathcal{C})$, and figure the upper bound $\operatorname{rk}(p^i\mathbf{e}) \leq \log_{p^n}(p^l) = \frac{l}{n}$ as for every coordinate of $p^i\mathbf{e}$, there is maximally p possible coefficients from $\mathbf{S}$. Thence,

$$\begin{aligned}\operatorname{rk}(p^i\mathbf{c}) &= \operatorname{rk}\left(\begin{pmatrix} p^i\mathbf{e} & \mathbf{o}_{m-l} \end{pmatrix} + \begin{pmatrix} \mathbf{o}_l & p^i\mathbf{f} \end{pmatrix}\right) \overset{\mathbf{48.5}}{\leq} \operatorname{rk}\left(\begin{pmatrix} p^i\mathbf{e} & \mathbf{o}_{m-l} \end{pmatrix}\right) + \operatorname{rk}\left(\begin{pmatrix} \mathbf{o}_l & p^i\mathbf{f} \end{pmatrix}\right) \\ &= \operatorname{rk}(p^i\mathbf{e}) + \operatorname{rk}(p^i\mathbf{f}) < \frac{l}{n} + \frac{m-2l+1}{n} = d,\end{aligned}$$

a contradiction with $\mathcal{C}$ being MCRD.

2. Let $\Delta = (\boldsymbol{\delta}_1, \dots, \boldsymbol{\delta}_m)$ be the standard basis of $\mathbf{R}^m$ over $\mathbf{R}$, which is free. Denote $e = \mathrm{d}_{\mathcal{R}}(\mathcal{D}) = \frac{m-2l+1}{n}$ as $\mathcal{D}$ is MCRD by 1. Assume, for a contradiction, that $i \in \mathbb{N}, i \leq l$, exists, for which the row $\mathbf{F}_i^r$ of height h_i has at least l coordinates of the height less than h_i. On other hand, $\mathbf{f} = p^{h_i-1} \cdot \delta_i \cdot F = p^{h_i-1} \cdot \mathbf{F}_i^r \in \operatorname{Soc}(\mathcal{D})$ must have the cardinal rank $\operatorname{rk}(\mathbf{f}) > e$ since $\mathbf{f} \neq \mathbf{o}$ and $\mathcal{D}$ is MCRD. At the same time, there is at least l coordinates of $\mathbf{f}$ equal to 0. It may be deduced that $\operatorname{rk}(\mathbf{f}) \leq \log_{p^n}(p^{m-2l}) = \frac{m-2l}{n} = e - \frac{1}{n}$, which cannot happen.

3. Let Δ be as before. Choose any non-negative integers i and j meeting the conditions $i < n$ and $m_i \leq j \leq M_i$. Set $h_i = n - i$ and consider a codeword $\mathbf{c} = p^{h_i-1} \cdot \delta_j \cdot G = p^{h_i-1} \cdot \mathbf{G}_j^r \in \mathcal{C}$. Then, $\mathbf{c} \in \operatorname{Soc}(\mathcal{C})$ as $\mathbf{G}_j^r \in (p^i\mathbf{R})^m$, and $\mathbf{c}$ has $\operatorname{rk}(\mathbf{c}) \geq d$, because $\mathcal{C}$ is MCRD. In accordance with **Theorem 54** applied to $\mathbf{G}_j^r$ of the height h_i, $\operatorname{rk}(\mathbf{G}_j^r) \geq h_i \cdot d$. Moreover, $\mathbf{G}_j^r = \begin{pmatrix} \mathbf{o}_{j-1} & p^{n-i} & \mathbf{o}_{M_i-j} & \mathbf{y} \end{pmatrix}$, where $j-1$ zeros from the row-echelon form of G are followed by the pivot p^{n-i} and other $M_i - j$ zeros of the current block $p^{n-i}I_{k_i}$. Specially, $\mathbf{y} = p^{n-i}(g_{jm_{i+1}}, \dots, g_{jm})$ is the last part of $\mathbf{G}_j^r$ as $m_{i+1} = M_i + 1$. Hence, the j^{th} row of G has the cardinal rank $\operatorname{rk}(\mathbf{G}_j^r) \leq \log_{p^n}\left(p^{h_i \cdot (m-m_{i+1}+1)}\right) = \frac{h_i \cdot (m-m_{i+1}+1)}{n}$, because $\mathbf{G}_j^r$ of the height h_i has at most $(m - m_{i+1} + 1)$ non-zero coordinates.

□

Now, let us focus on only free MCRD codes over Galois rings. We can state the necessary conditions for generator matrices in the systematic form and codes themselves much more clearly.

Corollary 62. Let $l, m \in \mathbb{N}$ satisfy $2l < m \leq \min(n, r)$, and $\mathcal{C}$ be a free MCRD $[m, l]_{\mathbf{R}}$-code with a generator matrix $G = \begin{pmatrix} I_l & F \end{pmatrix} \in \mathbf{R}^{l \times m}$. Denote $d = \frac{n-l+1}{n}$.

1. Every row of G has the cardinal rank $n \cdot d$.
2. No entry of F is divisible by p and the code generated by F over $\mathbf{R}$ is free.
3. The number of codewords in $\mathcal{C}$ of the cardinal rank d is at least $l(p^r - 1)$.
4. A tuple $(1, f_{1j}, f_{2j}, \dots, f_{lj})$ is a free basis of some $\mathbf{S}$-submodule of $\mathbf{R}$ for every $j \in \mathbb{N}, j \leq m - l$.

Proof. 1. In the case of $\mathcal{C}$ being free, we have $k_0 = l$ and $k_i = 0$ for all $i \in \mathbb{N}, i \leq n$, where $k_0, \dots, k_n$ are from the systematic form (2.5). **Theorem 61** implies $n \cdot d \leq \mathrm{rk}(\mathbf{G}_j^r) \leq \frac{n\cdot(m-l+1)}{n}$ for $j \in \mathbb{N}, j \leq l$. Subsequently, $\mathrm{rk}(\mathbf{G}_j^r) = n \cdot d$ by simplifying the inequalities.

2. Choose any $i \in \mathbb{N}, i \leq n$. Then, we have $\mathrm{rk}(\mathbf{G}_i^r) = n \cdot d$ as a result of 1. **Theorem 54** proposes that $\mathrm{rk}(\mathbf{G}_i^r) \geq n \cdot \mathrm{rk}(p^{n-1}\mathbf{G}_i^r)$ and the equality is achieved if and only if no coordinate of $\mathbf{G}_i^r$ is divisible by p. Since $\mathcal{C}$ is MCRD, we have $\mathrm{rk}(p^{n-1}\mathbf{G}_i^r) = d$. Hence, no coordinate of $\mathbf{G}_i^r$ is divisible by p, so neither is any coordinate of $\mathbf{F}_i^r$.

3. Let $B = (1, \xi, \ldots, \xi^{r-1})$ be a free basis of $\mathbf{R}$ over $\mathbf{S}$ for $\xi \in \mathbf{R}$ of order $p^r - 1$. Choose some $x \in \mathcal{T}_r \setminus \{0\}$ and $i \in \mathbb{N}, i \leq l$. Abbreviate $p^{n-1} \cdot \mathbf{G}_i^r \in \mathrm{Soc}(C)$ to $\mathbf{g}$. Remark that $\mathbf{g} \neq \mathbf{o}$ based on the previous point, from what $x \cdot \mathbf{g} \in \mathrm{Soc}(C) \setminus \{\mathbf{o}\}$ follows directly. Set $X = ([x]_B \mid [x \cdot \xi]_B \mid \cdots \mid [x \cdot \xi^{r-1}]_B) \in \mathbf{S}^{r \times r}$. Then, X seems to be the matrix of a module homomorphism $\chi : \mathbf{R}^m \to \mathbf{R}^m, \mathbf{a} \mapsto x \cdot \mathbf{a}$ relative to the basis B, because

$$[x \cdot \mathbf{a}]_B = ([x \cdot a_1]_B \mid \cdots \mid [x \cdot a_m]_B) = (X \cdot [a_1]_B \mid \cdots \mid X \cdot [a_m]_B) = X \cdot [\mathbf{a}]_B.$$

Especially, χ is bijective since $\chi^{-1}(\mathbf{y}) = x^{-1} \cdot \mathbf{y}$ for any $\mathbf{y} \in \mathbf{R}^m$ as $x \in \mathcal{T}_r$, $x \neq 0$. Hence, the matrix X is invertible. Consequently, it is derived from **Theorem 48** that $\mathrm{rk}(x \cdot \mathbf{g}) = \mathrm{rk}(X \cdot [\mathbf{g}]_B) = \mathrm{rk}([\mathbf{g}]_B) = \mathrm{rk}(\mathbf{g}) = d$. As a result, there exists at least $l \cdot (p^r - 1)$ codewords in $\mathcal{C}$ of the cardinal rank d, where l is the number of possible rows of G and $(p^r - 1)$ is the number of appropriate $x \in \mathcal{T}_r \setminus \{0\}$.

4. Assume, for contradiction, that $j \in \mathbb{N}, j \leq m - l$, and $s_0, s_1, \ldots, s_l \in \mathbf{S}$ exist, which fulfill $\sum\limits_{t=0}^{l} s_t \cdot F_{t,j} = 0$, where $F_{0,j} = 1$, and $s_i \cdot f_{ij} \neq 0$ for some $i \in \{0, 1, \ldots, l\}$. Grounded the second point, $s_i \cdot f_{ij} \neq 0$ if and only if $s_{ij} \neq 0$. Define a codeword $\mathbf{c} = \mathbf{s} \cdot G \in \mathcal{C}$ for $\mathbf{s} = (s_1, \ldots, s_l)$. In this situation, $c_t = s_t$ for all $t \in \mathbb{N}$, $t \leq l$, and $c_{l+j} = \mathbf{s} \cdot \mathbf{F}_j^c = \sum\limits_{t=1}^{l} s_t \cdot f_{tj} = -s_0$. Let B be a free basis of $\mathbf{R}$ over $\mathbf{S}$ as above and $e \in \{0, 1, \ldots, n-1\}$ be minimal such that $p^e \cdot \mathbf{c} \in \mathrm{Soc}(\mathcal{C})$. Set $\mathbf{a} = p^e \cdot (c_1, \ldots, c_l, c_{l+j})$, so $[\mathbf{a}]_B = p^e \cdot \begin{pmatrix} s_1 & s_2 & \ldots & s_l & -s_0 \\ 0 & 0 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & 0 \end{pmatrix}$ and $\mathrm{rk}(\mathbf{a}) = \frac{1}{n}$ based on **Claim 49**. It is a direct consequence that $\mathrm{rk}(p^e\mathbf{c}) \leq \frac{m-l}{n} < d$ since the other $(m - l - 1)$ columns of $[p^e\mathbf{c}]_B$ may generate an $\mathbf{S}$-module of cardinality at most p^{m-l-1}, a contradiction with $\mathcal{C}$ being MCRD.

□

4. Gabidulin Codes

Gabidulin codes over finite fields, firstly introduced by Gabidulin [12], are one of the most well-known MRD codes. Construction of these codes relies entirely on the Frobenius automorphism and its iterations. Abbreviate the i^{th} power of p to $[i]$ for $i \in \mathbb{N}$. Any Gabidulin $[n,k]_{\mathbb{F}_{q^m}}$-code is generated by some matrix $\left(g_j^{[i-1]}\right)_{i=1,j=1}^{k,n}$, where the vector $\mathbf{g} \in \mathbb{F}_{q^m}^n$ has $\mathbb{F}_q$-linearly independent coordinates.

4.1 Gabidulin Codes over Galois Rings

Let $\mathbf{R}, \mathbf{S}$ be Galois rings $\mathrm{GR}(p^n, r)$, $\mathrm{GR}(p^n, 1)$ and $\mathcal{T}_r, \mathcal{T}$ be theirs Teichmüller sets in the given order, where p is a prime and n, r are positive integers. Denote by $\mathbb{K}$ the residue field of $\mathbf{R}$ and by $\mathbb{L}$ the residue field of $\mathbf{S}$. Continue by recalling the generalised Frobenius automorphism τ of $\mathbf{R}$ (**Theorem 18**) defined for $\xi \in \mathbf{R}$ of order $k = p^r - 1$ as $\tau(\xi) = \xi^p$. Deduced from **Theorem 21**, τ generates the Galois group $\mathrm{Gal}(\mathbf{R}/\mathbf{S})$. Furthermore, for every $\zeta \in \mathcal{T}_r$ and $e \in \mathbb{N}$, it holds that $\tau^e(\zeta) = \zeta^{p^e} = \zeta^{[e]}$.

This section aims to define Gabidulin codes over Galois rings, consistent with the definition over finite fields, and provide their fundamental properties. Gabidulin codes, utilising the cardinal rank metric, are introduced in the article by Epelde and Rúa [6]. However, here, we commence with the matrix approach rather than the linearised polynomials'.

Theorem 63. Let $m \in \mathbb{N}$ satisfy $m \leq \min(n, r)$ and $\mathbf{g} \in \mathbf{R}^m$. Let G be a matrix of order m over $\mathbf{R}$ with entries $\tau^{i-1}(g_j)$ for $i, j \in \mathbb{N}, i, j \leq m$. Then, $\mathrm{Im}(G^\top)$ is a free $\mathbf{R}$-module with a free basis $(\mathbf{G}_1^r, \ldots, \mathbf{G}_m^r)$ if and only if $\mathrm{rk}(\mathbf{g}) = m$.

Proof. "$\implies$": If there exists coordinate of $\mathbf{g}$ divisible by p, then there is entire column of G divisible by p and also pivot of the Smith normal form of G divisible by p. Now, assume there is no coordinate of $\mathbf{g}$ divisible by p and $\mathrm{rk}(\mathbf{g}) < m$, i.e. $\sum_{i=1}^{m} s_i \cdot g_i = 0$ for some $s_1, \ldots, s_m \in \mathbf{S}$ and at least one $s_i \neq 0$. Then for every $i = 0, \ldots, l-1$ also $\tau^i\left(\sum_{j=1}^{m} s_j \cdot g_j\right) = \sum_{j=1}^{m} s_j \cdot \tau^i(g_j) = 0$. Hence, at least one column of G can be eliminated and the number of pivots of the Smith normal form of G is less than m. Rows of G cannot form a free basis in both cases.

"$\impliedby$": Let X be the coordinate matrix of $\mathbf{g}$ relative to some basis of $\mathbf{R}$ over $\mathbf{S}$. Since $m = \mathrm{rk}(\mathbf{g}) = \log_{p^n}(|\mathrm{Im}(X)|)$, it needs to be true that columns of X form a free basis of $\mathrm{Im}(X)$ over $\mathbf{S}$ as there is m of them. Specially, no coordinate of $\mathbf{g}$ can be divisible by p, which means that $p \nmid \tau^{i-1}(g_j)$ for every $i, j \in \mathbb{N}$, $j \leq m$, since **Theorem 18** affirms that τ is the $\mathbf{S}$-automorhism. It directly results in $p^{n-1} \cdot \tau^{i-1}(g_j) \in \mathrm{Soc}(\mathbf{R}) \setminus \{0\}$. Derived from **Theorem 15**, the unique non-zero $b_{ji} \in \mathcal{T}_r$, which satisfies $p^{n-1} \cdot b_{ji} = p^{n-1} \cdot \tau^{i-1}(g_j)$, exists for each $i, j \in \mathbb{N}, j \leq m$.

Suppose that there exist $z_1, \ldots, z_m \in \mathcal{T}_r$ for which $\sum_{i=1}^{m} z_i(p^{n-1} \cdot \mathbf{G}_i^r) = \mathbf{o}$ and at least one of the coefficients is non-zero. Choose $j \in \mathbb{N}$ satisfying $j \leq m$.

In the given situation,

$$0 = \sum_{i=1}^{m} z_i \cdot p^{n-1} \cdot \tau^{i-1}(g_j) = \sum_{i=1}^{m} z_i \cdot p^{n-1} \cdot b_{ji} = p^{n-1} \sum_{i=1}^{m} z_i \cdot b_{ji} = p^{n-1} \sum_{i=1}^{m} z_i \cdot b_{j1}^{[i-1]}.$$

Define a polynomial $L(X) = \sum_{i=1}^{m} z_i \cdot X^{[i-1]} \in \mathcal{T}_r[X]$ and the evaluation map $\lambda : \mathcal{T}_r \to \mathcal{T}_r$ as $a \mapsto L(a)$. The map λ seems to be a field homomorphism as the characteristic of $\mathcal{T}_r$ equals p. Besides, $a \in \mathcal{T}_r$ is a root of L if and only if $a \in \ker(\lambda)$, and $\ker(\lambda) = \{0\}$, because $\ker(\lambda)$ is an ideal of the field $\mathcal{T}_r$ and $1 \notin \ker(\lambda)$. Now, $p^{n-1} \cdot L(b_{j1}) = 0$ can occur if and only if $L(b_{j1}) = 0$, but $b_{j1} \neq 0$, a contradiction.

It is shown that $\sum_{i=1}^{m} a_i \left(p^{n-1} \cdot \mathbf{G}_i^r\right) = \mathbf{o}$ over $\mathcal{T}_r$ if and only if all $a_1, \dots, a_m$ equal 0. Therefore, $(p^{n-1}\mathbf{G}_1^r, \dots, p^{n-1}\mathbf{G}_m^r)$ is a basis of a vector space $\mathrm{Soc}(\mathrm{Im}(G^\top))$ over $\mathcal{T}_r$. **Lemma 28** implies that $(\mathbf{G}_1^r, \dots, \mathbf{G}_m^r)$ is a free basis of $\mathrm{Im}(G^\top) \leq \mathbf{R}^m$.

□

Consider $\mathbf{g} \in \mathbf{R}^m$ of cardinal rank $m \in \mathbb{N}$. Denote by $\mathbf{g}_i$ the codeword $(\tau^{i-1}(g_1), \dots, \tau^{i-1}(g_m))$ for each $i \in \mathbb{N}, i \leq m$. It can be deduced from the last theorem combined with **Theorem 24** that $(\mathbf{g}_1, \dots, \mathbf{g}_l)$ is a free basis of some $\mathbf{R}$-module isomorphic to $\mathbf{R}^l$ for every positive integer $l, l \leq m$.

Definition 64. Let $l, m \in \mathbb{N}$ be such that $l \leq m \leq \min(n, r)$ and a codeword $\mathbf{g} \in \mathbf{R}^m$ satisfy $\mathrm{rk}(\mathbf{g}) = m$. The *Gabidulin code* of length m and rank l over $\mathbf{R}$ *generated* by $\mathbf{g}$, denoted by $\mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$, is a cardinal rank metric $[m, l]_{\mathbf{R}}$-code with a generator matrix

$$G = \begin{pmatrix} g_1 & \cdots & g_m \\ \tau(g_1) & \cdots & \tau(g_m) \\ \vdots & \ddots & \vdots \\ \tau^{l-1}(g_1) & \cdots & \tau^{l-1}(g_m) \end{pmatrix} \tag{4.1}$$

It is beyond any doubt, if the field $\mathbb{F}_{p^r}$ and the Frobenius automorphism σ of $\mathbb{F}_{p^r}$ are taken instead of the Galois ring $\mathbf{R}$ and τ, then $\mathrm{Gab}_{\mathbb{F}_{p^r}}(m, l, \mathbf{g})$ is a correctly defined Gabidulin $[m, l]_{p^r}$-code. Significantly, the projection of a Gabidulin code over the Galois ring is a Gabidulin code over its residue field, written as $\overline{\mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})}^m = \mathrm{Gab}_{\mathbb{K}}(m, l, \overline{\mathbf{g}}^m)$.

Corollary 65. Any Gabidulin code over $\mathbf{R}$ is free.

Immediate result of the preceding corollary and **Lemma 40** is that the socle of $\mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$ is isomorphic to $\mathrm{Gab}_{\mathbb{K}}(m, l, \overline{\mathbf{g}}^m)$ for any $m, l \in \mathbb{N}$ satisfying $l \leq m$, and $\mathbf{g} \in \mathbb{R}^m$ fulfilling $\mathrm{rk}(\mathbf{g}) = m$.

Corollary 66. Any Gabidulin code over $\mathbf{R}$ is MCRD.

Proof. It is a combination of **Corollary 65** and **Corollary 60** as a Gabidulin code over a finite field is MRD.

□

Example 14. Let $p = 5$, $n = 5$, $r = 4$ and $\mathbf{R}$ be the Galois rings of characteristic 5^5 and cardinality 5^{20}. Denote by $G_{5,4}(x) = x^4+450x^3+830x^2+1892x+3124$ a basic primitive polynomial over $\mathbb{Z}_{5^5}$, which divides $x^k - 1$ for $k = 5^4 - 1$, computed by the Hensel's lift (**Algorithm 3**) of $(x^4 + 2x + 4) \in \mathbb{Z}_5[x]$. Set $\xi = x + (G_{5,4})$. Based on **Section 1.2**, ξ is of order k and $B = (1, \xi, \xi^2, \xi^3)$ is a basis of $\mathbf{R}$ over $\mathbf{S} \simeq \mathbb{Z}_{p^n}$. Any element $\sum\limits_{i=0}^{3} a_i\xi^i \in \mathbf{R}$ is represented by the tuple $a_3{:}a_2{:}a_1{:}a_0$.

Consider $\mathbf{g} = (0{:}11{:}9{:}0, 0{:}0{:}31{:}124, 19{:}0{:}934{:}0, 87{:}0{:}21{:}0) \in \mathbf{R}^4$. If the cardinal rank of $\mathbf{g}$ equals 4, the $\mathbf{g}$ generates a Gabidulin code of length 4 over $\mathbf{R}$. Let us compute the Smith normal form of $X = [\mathbf{g}]_B$:

$$\begin{gathered} X = \begin{pmatrix} 0 & 124 & 0 & 0 \\ 9 & 31 & 934 & 21 \\ 11 & 0 & 0 & 0 \\ 0 & 0 & 19 & 87 \end{pmatrix} \underset{2999\mathbf{X}_1^r}{\overset{\mathbf{X}_1^c \leftrightarrow \mathbf{X}_2^c}{\sim}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 31 & 9 & 934 & 21 \\ 0 & 11 & 0 & 0 \\ 0 & 0 & 19 & 87 \end{pmatrix} \underset{1389\mathbf{X}_2^r}{\overset{\mathbf{X}_2^r+3094\mathbf{X}_1^r}{\sim}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 451 & 1044 \\ 0 & 11 & 0 & 0 \\ 0 & 0 & 19 & 87 \end{pmatrix} \\ \underset{1234\mathbf{X}_2^r}{\overset{\mathbf{X}_3^r+3114\mathbf{X}_2^r}{\sim}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 451 & 1044 \\ 0 & 0 & 1 & 619 \\ 0 & 0 & 19 & 87 \end{pmatrix} \underset{\mathbf{X}_4^r+3106\mathbf{X}_3^r}{\overset{\mathbf{X}_2^r+2674\mathbf{X}_3^r}{\sim}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 619 \\ 0 & 0 & 0 & 826 \end{pmatrix} \underset{\mathbf{X}_3^r+2506\mathbf{X}_4^r}{\overset{1676\mathbf{X}_4^r}{\sim}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{gathered} \tag{4.2}$$

Thence, $\operatorname{rk}(\mathbf{g}) = \operatorname{rk}(X) = \operatorname{rk}(I_4) = 4$ and $\mathbf{g}$ is a generator of $\operatorname{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$ with a generator matrix

$$\begin{aligned} G &= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 \\ \tau(g_1) & \tau(g_2) & \tau(g_3) & \tau(g_4) \end{pmatrix} = \begin{pmatrix} 0{:}11{:}9{:}0 & 0{:}0{:}31{:}124 & 19{:}0{:}934{:}0 & 87{:}0{:}21{:}0 \\ \tau(0{:}11{:}9{:}0) & \tau(0{:}0{:}31{:}124) & \tau(19{:}0{:}934{:}0) & \tau(87{:}0{:}21{:}0) \end{pmatrix} \\ &= \begin{pmatrix} 0{:}11{:}9{:}0 & 0{:}0{:}31{:}124 & 19{:}0{:}934{:}0 & 87{:}0{:}21{:}0 \\ 481{:}948{:}631{:}3119 & 1770{:}1098{:}2806{:}1799 & 2638{:}1089{:}2965{:}1596 & 229{:}1959{:}2934{:}1008 \end{pmatrix}. \end{aligned} \tag{4.3}$$

Prior to concluding this section, a way for computing a parity-check matrix of Gabidulin codes, which are in the form (4.1), is presented as in the section III.D of Kamche and Mouaha's work [16].

Theorem 67. Let $l, m \in \mathbb{N}$ satisfy $l \le m \le \min(n, r)$, and $\mathbf{g} \in \mathbf{R}^m$ fulfill $\operatorname{rk}(\mathbf{g}) = m$. Consider $\mathbf{h} \in \mathbf{R}^m$ with coordinates $h_i = \tau^{l+1-m}(f_{im})$ for each i, $1 \le i \le m$, where $F = (f_{ij})_{i,j=1}^m$ is the inverse of a matrix $G = (\tau^{i-1}(g_j))_{i,j=1}^m$. Then, the cardinal rank of $\mathbf{h}$ is m and $H = (\tau^{i-1}(h_j))_{i=1,j=1}^{m-l,m}$ is a parity-check matrix of $\operatorname{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$.

Proof. **Theorem 63** proposes that $(\mathbf{G}_1^r, \dots, \mathbf{G}_m^r)$ is free basis of $\operatorname{Im}(G^\top)$, so G is invertible by **Theorem 37**. Hence, the entries $f_{11}, \dots, f_{mm} \in \mathbf{R}$ of the matrix $F = G^{-1}$ are correctly introduced, and for every $i \in \mathbb{N}$ such that $i \le m$, we have $\delta_{im} = \mathbf{G}_i^r \cdot \mathbf{F}_m^c = \sum\limits_{t=1}^{m} \tau^{i-1}(g_t) \cdot f_{tj}$. Denote by F' the matrix of order m over $\mathbf{R}$ with entries $f'_{ij} = (\tau^{j-m}(f_{im}))$ for $i, j \in \{1, \dots, m\}$. Compute the entry l_{ij} of $L = G \cdot F'$ at the position (i, j):

$$\begin{aligned} \sum_{t=1}^{m} \tau^{i-1}(g_t) \cdot f'_{tj} &= \sum_{t=1}^{m} \tau^{i-1}(g_t) \cdot \tau^{j-m}(f_{tm}) = \sum_{t=1}^{m} \tau^{j-m}\left(\tau^{i-1-j+m}(g_t) \cdot f_{tm}\right) \\ &= \tau^{j-m}\left(\sum_{t=1}^{m} \tau^{i-1-j+m}(g_t) \cdot f_{tm}\right) = \begin{cases} \delta_{(i-j+m)m} & \text{, if } 1 - m \le i - j \le 0, \\ l_{ij} \in \mathbf{R} & \text{, otherwise.} \end{cases} \end{aligned}$$

Thus, the product L is a lower triangular matrix with units on the main diagonal, so L is invertible as shown in *Example* 9. Moreover, $F' = F \cdot L$ is also invertible due to **Lemma 33**. Deduced from **Theorem 37**, the columns of F' constitute a free basis of $\operatorname{Im}(F')$. In this case, **Theorem 63** dictates that $\operatorname{rk}(\mathbf{F'}_1^c) = m$.

Since τ is the $\mathbf{S}$-automorphism of $\mathbf{R}$, applying τ to the coordinates of $\mathbf{F'}^c_1$ cannot change its cardinal rank, and we have $\mathrm{rk}(\mathbf{h}) = m$ as $\mathbf{h} = \mathbf{F'}^c_{l+1}$. Consequently,

$$H = \begin{pmatrix} h_1 & \dots & h_m \\ \tau(h_1) & \dots & \tau(h_m) \\ \vdots & \ddots & \vdots \\ \tau^{m-l}(h_1) & \dots & \tau^{m-l}(h_m) \end{pmatrix} \overset{\mathbf{h}=\mathbf{F'}^c_{l+1}}{=} \begin{pmatrix} \mathbf{F'}^c_{l+1} \\ \mathbf{F'}^c_{l+2} \\ \vdots \\ \mathbf{F'}^c_m \end{pmatrix} \tag{4.4}$$

is a generator matrix of the Gabidulin $[m, m-l]_{\mathbf{R}}$-code $\mathrm{Gab}_{\mathbf{R}}(m, m-l, \mathbf{h})$.

It remains to verify $\mathbf{c} \cdot H^\top = \mathbf{o}$ if and only if $\mathbf{c} \in \mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$ is valid for any codeword $\mathbf{c} \in \mathbf{R}^m$. Denote by G_l the matrix created from G by omitting the last $(m-l)$ rows. Choose $\mathbf{c} \in \mathbf{R}^m$. Express the homogeneous system $\mathbf{c} \cdot H^\top = \mathbf{o}$ using the equations (4.4)

$$\begin{aligned} \mathbf{c} \cdot H^\top = \mathbf{o} \overset{(4.4)}{\iff} & \exists \mathbf{x} \in \mathbf{R}^l : \mathbf{c} \cdot F' = (\mathbf{x}, \mathbf{o}) \overset{F'=F\cdot L}{\iff} \exists \mathbf{x} \in \mathbf{R}^l : \mathbf{c} = (\mathbf{x}, \mathbf{o}) \cdot L^{-1} \cdot F^{-1} \\ \overset{F=G^{-1}}{\iff} & \exists \mathbf{x} \in \mathbf{R}^l : \mathbf{c} = (\mathbf{x}, \mathbf{o}) \cdot L^{-1} \cdot G \\ \iff & \exists \mathbf{x} \in \mathbf{R}^l : \mathbf{y} = (\mathbf{x}, \mathbf{o}) \cdot L^{-1} \wedge \mathbf{c} = \mathbf{y} \cdot G. \end{aligned}$$

Remark that L^{-1} is also lower triangular, which is displayed in *Example* 9. Then, necessary, $\mathbf{z} \in \mathbf{R}^l$ exists and satisfies $\mathbf{y} = (\mathbf{x}, \mathbf{o}) \cdot L^{-1} = (\mathbf{z}, \mathbf{o})$. In conclusion, $\mathbf{c} \cdot H^\top = \mathbf{o}$ if and only if $\mathbf{c} = (\mathbf{z}, \mathbf{o}) \cdot G = \mathbf{z} \cdot G_l$ for some $\mathbf{z} \in \mathbf{R}^l$.

□

Corollary 68. Let $l, m \in \mathbb{N}$ satisfy $l \leq m \leq \min(n, r)$, and $\mathbf{g} \in \mathbf{R}^m$ fulfill $\mathrm{rk}(\mathbf{g}) = m$. Then, $\mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})^\perp$ is a free $[m, m-l]$-code, which is MCRD.

4.2 Linearised Polynomials

Gabidulin codes are usually represented by linearised polynomials, which get evaluated at each coordinate of the generating codeword. Linearised polynomials over $\mathbf{R}$ have to be introduced and their properties understood to formalise this approach. Linearised polynomials in this thesis are applications of more general Skew polynomials over Galois rings studied in multiple publications, for example, by Kamche and Mouaha [16].

Definition 69. A *linearised polynomial over* $\mathbf{R}$ *of degree* d is any polynomial of the form $F(X) = \sum\limits_{i=0}^{d} f_i \cdot \tau^i(X)$ with the coefficients from $\mathbf{R}$ and $f_d \neq 0$. Let $\mathcal{P}(\mathbf{R})$ be the set of all linearised polynomials over $\mathbf{R}$. The *degree* of $F \in \mathcal{P}(\mathbf{R})$ is denoted by $\deg(F)$ and $\deg(0)$ is defined as $-\infty$. Define, for every $d \in \mathbb{N}$, the set $\mathcal{P}_d(\mathbf{R})$, which contains linearised polynomials of degree less than d, and the set $\mathcal{P}^*_d(\mathbf{R})$ composed of monic linearised polynomials of degree exactly $(d-1)$, i.e. $F(X) = \tau^{d-1}(X) + G(X)$ for $G \in \mathcal{P}_{d-1}(\mathbf{R})$.

The main idea behind the definition of linearised polynomials is that they should represent module endomorphisms of the ring $\mathbf{R}$ viewed as the $\mathbf{S}$-module, denoted by $\mathbf{R}_{\mathbf{S}}$. The addition and subtraction of linearised polynomials defined in the same way as in $\mathbf{R}[x]$ are consistent with module endomorphisms' addition and subtraction. To have the multiplication of linearised polynomials consistent with the composition of module endomorphisms, a different multiplication than the one used in $\mathbf{R}[x]$ must be established.

Theorem 70. $(\mathcal{P}(\mathbf{R}), +, -, \circ, 0, \varepsilon)$ is a non-commutative ring, where $\varepsilon(X) = X$ and $\circ$ is defined for $F, G \in \mathcal{P}(\mathbf{R})$ as $(F \circ G)(X) = F(G(X))$.

Proof. Commence by observing that $(\mathcal{P}(\mathbf{R}), +, -, 0)$ is truly an abelian group, because $\mathbf{R}$ is. Choose $F = \sum_{i=0}^{d_f} f_i \tau^{i-1}(X), G = \sum_{i=0}^{d_g} g_i \tau^{i-1}(X), H = \sum_{i=0}^{d_h} h_i \tau^{i-1}(X)$ from $\mathcal{P}(\mathbf{R})$. Let p_i equal zero for every $P = \sum_{i=0}^{d_p} p_i \tau^{i-1}(X) \in \mathcal{P}(\mathbf{R})$ and $i \in \mathbb{Z}$ such that $i < 0$ or $i > d_p$. Denote the sums $d_1 = d_f + d_g, d_2 = d_f + d_h$, $d_3 = d_g + d_h$, and the maximums $d_{12} = \max(d_1, d_2), d_{23} = \max(d_2, d_3)$. Firstly, verify that $(\mathcal{P}(\mathbf{R}), \circ, \varepsilon)$ is a monoid, i.e. the operation $\circ$ is associative and ε is an identity:

$$\begin{aligned}
&((F \circ G) \circ H)(X) = (F \circ G)(H(X)) = F(G(H(X))) = F((G \circ H)(X)) \\
&\quad = (F \circ (G \circ H))(X), \\
&(\varepsilon \circ F)(X) = \varepsilon(F(X)) = F(X) = F(\varepsilon(X)) = (F \circ \varepsilon)(X)
\end{aligned}$$

Secondly, it has to be shown that the operation $\circ$ is distributive with respect to the addition:

$$\begin{aligned}
&(F \circ (G + H))(X) = F((G + H)(X)) = \sum_{i=0}^{d_{12}} \sum_{j=0}^{i} f_j \tau^j (g_{i-j} + h_{i-j}) \tau^{i-1}(X) \\
&\quad = \sum_{i=0}^{d_1} \sum_{j=0}^{i} f_j \tau^j (g_{i-j}) \tau^{i-1}(X) + \sum_{i=0}^{d_2} \sum_{j=0}^{i} f_j \tau^j (h_{i-j}) \tau^{i-1}(X) = (F(G) + F(H))(X) \\
&\quad = (F \circ G)(X) + (F \circ H)(X), \\
&((F + G) \circ H)(X) = (F + G)(H(X)) = \sum_{i=0}^{d_{23}} \sum_{j=0}^{i} (f_j + g_j) \tau^j (h_{i-j}) \tau^{i-1}(X) \\
&\quad = \sum_{i=0}^{d_2} \sum_{j=0}^{i} f_j \tau^j (h_{j-i}) \tau^{i-1}(X) + \sum_{i=0}^{d_3} \sum_{j=0}^{i} g_j \tau^j (h_{j-i}) \tau^{i-1}(X) = (F(H) + G(H))(X) \\
&\quad = (F \circ H)(X) + (G \circ H)(X).
\end{aligned}$$

Let $\xi \in \mathbf{R}$ be of order $p^r - 1$. Consider $P(X) = \xi \cdot X$, $Q(X) = \tau(X) \in \mathcal{P}(\mathbf{R})$. Then, $(P \circ Q)(X) = \xi \cdot \tau(X)$ and $(Q \circ P)(X) = \tau(\xi \cdot X) = \tau(\xi) \cdot \tau(X)$ are not equal. Thence, $(\mathcal{P}(\mathbf{R}), +, -, \circ, 0, \varepsilon)$ is a non-commutative ring. □

Remark. **Theorem 70** can be also proven by providing an isomorphism between $(\mathcal{P}(\mathbf{R}), +, -, \circ, 0, \varepsilon)$ and $\mathrm{End}_{\mathbf{S}}(\mathbf{R}_{\mathbf{S}})$, where $\mathrm{End}_{\mathbf{S}}(\mathbf{R}_{\mathbf{S}})$ is a non-commutative ring consisting of all $\mathbf{S}$-module endomorphisms of the ring $\mathbf{R}$ viewed as an $\mathbf{S}$-module.

Consider $F, G \in \mathcal{P}(\mathbf{R})$ and set $d_f = \deg(F)$ and $d_g = \deg(G)$. It is apparent that $\deg(F + G) \leq \max(d_F, d_G)$ and $\deg(F \circ G) \leq d_F + d_G$. Let G be monic and $d_Q = d_F - d_G$. Therefore, the product $F \circ G$ is exactly of degree d_Q. Now, we demonstrate that in this situation, $Q_l, Q_r \in \mathcal{P}_{d_Q+1}(\mathbf{R})$ and $R_l, R_r \in \mathcal{P}_{d_G}(\mathbf{R})$ meeting the condition $F = G \circ Q_l + R_l = Q_r \circ G + R_r$ exist.

Definition 71. Let $F, G \in \mathcal{P}(\mathbf{R})$. One shall say that G is the *left (right) divisor* of F and F is *left (right) divisible* by G provided there exists a non-zero $Q \in \mathcal{P}(\mathbf{R})$ satisfying $F = G \circ Q$ $(F = Q \circ G)$.

Algorithm 8 Left and right division with remainder

```
Require: $F = \sum_{i=0}^{d_F} f_i\tau^i(X) \in \mathcal{P}_{d_F+1}(\mathbf{R}), G = \sum_{i=0}^{d_G} g_i\tau^i(X) \in \mathcal{P}^*_{d_G+1}(\mathbf{R})$
Ensure: $Q_l, Q_r \in \mathcal{P}_{d_F-d_G+1}(\mathbf{R}), R_l, R_r \in \mathcal{P}_{d_G}(\mathbf{R}) : F = G \circ Q_l + R_l = Q_r \circ G + R_r$
  $d_Q \leftarrow d_F - d_G$, $i \leftarrow d_F$
  while $i \geq d_G$ do
    $a_{i-d_G} \leftarrow \tau^{r-d_G}\left(f_i - \sum_{j=i-d_G+1}^{\min(d_Q,i)} g_{i-j}\tau^{i-j}(a_j)\right)$
    $b_{i-d_G} \leftarrow f_i - \sum_{j=i-d_G+1}^{\min(d_Q,i)} b_j\tau^j(g_{i-j})$
    $i \leftarrow i - 1$
  end while
  $Q_l \leftarrow \sum_{i=0}^{d_Q} a_i\tau^i(X)$, $R_l \leftarrow F - G \circ Q_l$
  $Q_r \leftarrow \sum_{i=0}^{d_Q} b_i\tau^i(X)$, $R_r \leftarrow F - Q_r \circ G$
  return $(Q_l, Q_r, R_l, R_r)$
```

Theorem 72. Let $d_F, d_G \in \mathbb{N}$, $F \in \mathcal{P}_{d_F}(\mathbf{R})$ and $G \in \mathcal{P}^*_{d_G}(\mathbf{R})$. Set $d_Q = d_F - d_G$. Then, there exist left and right quotient $Q_l, Q_r \in \mathcal{P}_{d_Q+1}(\mathbf{R})$ and left and right remainder $R_l, R_r \in \mathcal{P}_{d_G}(\mathbf{R})$ such that $F = G \circ Q_l + R_l = Q_r \circ G + R_r$.

Proof. It is enough to display that **Algorithm 8** is correct. Let $F \in \mathcal{P}_{d_F+1}(\mathbf{R})$ and $G \in \mathcal{P}^*_{d_G+1}(\mathbf{R})$ be given. Denote $d_Q = d_F - d_G$ and $m_i = \min(d_Q, i)$ for $i \in \mathbb{Z}$, $0 \leq i \leq d_F$. Let $Q_r \in \mathcal{P}_{d_Q+1}(\mathbf{R})$ be the right quotient of division with remainder, computed as in the algorithm on inputs F, G. Firstly, determine boundaries for indices i, j such that i iterates over coefficients of F, j iterates over coefficients of Q_R, and $(i - j)$ iterates over coefficients of G. Clearly, we have $0 \leq i \leq d_F$, $0 \leq j \leq d_Q$ and $0 \leq i - j \leq d_G$. The third pair of inequalities can be rewritten as $j \leq i \leq d_G + j$, which, combined with the second pair of inequalities, gives that $\max(0, i - d_G) \leq j \leq \min(d_Q, i) = m_i$. Next, express the product $Q_r \circ G$:

$$Q_r \circ G = \sum_{i=0}^{d_F} \left(\sum_{j=\max(0,i-d_G)}^{m_i} b_j\tau^j(g_{i-j}) \right) \tau^i(X) \tag{4.5}$$

$$= \sum_{i=d_G}^{d_F} \left(\sum_{j=i-d_G}^{m_i} b_j\tau^j(g_{i-j}) \right) \tau^i(X) + \sum_{i=0}^{d_G-1} \left(\sum_{j=0}^{m_i} b_j\tau^j(g_{i-j}) \right) \tau^i(X). \tag{4.6}$$

Observe that $f_i = \sum_{j=i-d_G}^{m_i} b_j\tau^j(g_{i-j}) = b_{i-d_G} + \sum_{j=i-d_G+1}^{m_i} b_j\tau^j(g_{i-j})$ since $g_{d_G} = 1$, where $i \in \mathbb{N}, d_G \leq i \leq d_F$. By integrating the equation 4.6 with the observation,

$$\begin{aligned} R_r = F - Q_r \circ G &= \sum_{i=0}^{d_F} f_i\tau^i(X) - \sum_{i=d_G}^{d_F} f_i\tau^i(X) - \sum_{i=0}^{d_G-1} \left(\sum_{j=0}^{m_i} b_j\tau^j(g_{i-j}) \right) \tau^i(X) \\ &= \sum_{i=0}^{d_G-1} \left(f_i - \sum_{j=0}^{m_i} b_j\tau^j(g_{i-j}) \right) \tau^i(X) \in \mathcal{P}_{d_G}(\mathbf{R}). \end{aligned}$$

Thus, the requirements for the right division are fulfilled. The left division may be proven analogically using that $\tau^{-d_G} = \tau^{r-d_G}$ as τ is fully defined by the image of $\xi \in \mathcal{T}_r$ of order $p^r - 1$, and $\tau^r(\xi) = \xi^{[r]} = \xi$.

□

Example 15. Let $\mathbf{R} = \mathrm{GR}(5^5, 4)$, $G_{5,4}(x) = x^4 + 450x^3 + 830x^2 + 1892x + 3124$ over $\mathbb{Z}_{5^5}[x]$, $\xi = x + (G_{5,4})$ and $B = (1, \xi, \xi^2, \xi^3)$ be as in *Example* 14. The left division with the remainder for the ensuing linearised polynomials U and V is provided:

$$U(X) = \big(\text{1646:2004:1497:825}\big)\tau^2(X) + \big(\text{2018:1595:473:3039}\big)\tau(X) + \big(\text{1824:1381:2671:2340}\big)X$$
$$V(X) = \tau(X) + \big(\text{2:4:2:1}\big)X$$

Let us simulate **Algorithm 8** on U and V instead of F and G, where all arithmetic is done in Wolfram Mathematica.

$$
\begin{aligned}
d_Q &= 2 - 1 = 1 \\
i = 2 : a_1 &= \tau^{4-1}\left(u_2 - \sum_{j=1}^{1} v_{i-j}\tau^{i-j}(a_j)\right) = \tau^3\left(u_2\right) = \tau^3\big(\text{1646:2004:1497:825}\big) \\
&= \text{28:0:0:1123} \\
i = 1 : a_0 &= \tau^{4-1}\left(u_1 - \sum_{j=1}^{1} v_{i-j}\tau^{i-j}(a_j)\right) = \tau^3\left(u_1 - v_0\tau^0(a_1)\right) \\
&= \tau^3\big((\text{2018:1595:473:3039}) - (\text{2:4:2:1}) \cdot (\text{28:0:0:1123})\big) \\
&= \tau^3\big((\text{2018:1595:473:3039}) - (\text{2662:589:666:549})\big) \\
&= \tau^3\big((\text{2481:1006:2932:2490})\big) = \text{0:91:2875:1} \\
Q(X) &= \sum_{j=0}^{1} a_j\tau^j(X) = Q(X) = \big(\text{28:0:0:1123}\big)\tau(X) + \big(\text{0:91:2875:1}\big)X \\
V \circ Q(X) &= v_1\tau(a_1)\tau^2(X) + (v_0a_1 + v_1\tau(a_0))\tau(X) + v_0a_0X \\
&= \tau\big(\text{28:0:0:1123}\big)\tau^2(X) + \big((\text{2:4:2:1})(\text{28:0:0:1123}) + \tau\big(\text{0:91:2875:1}\big)\big)\tau(X) + \\
&\quad + \big((\text{2:4:2:1})(\text{0:91:2875:1})\big)X \\
&= \big(\text{1646:2004:1497:825}\big)\tau^2(X) + \big(\text{2018:1595:473:3039}\big)\tau(X) + \\
&\quad + \big(\text{1824:1381:2671:2340}\big)X = U(X) \\
R(X) &= U - V \circ Q = 0
\end{aligned}
$$

Hence, V is the left divisor of U.

Let F be a linearised polynomial over $\mathbf{R}$. We shall say that $a \in \mathbf{R}$ is a root of F over $\mathbf{R}$ provided $F(a) = 0$. One of the most essential properties of linearised polynomials is that the set of all roots of F over $\mathbf{R}$ forms an $\mathbf{S}$-module. Let us focus on proving that.

Definition 73. The *kernel* of a linearised polynomial $F \in \mathcal{P}(\mathbf{R})$ is the set of all its roots over $\mathbf{R}$ and is denoted by $\ker(F)$.

Lemma 74. The kernel of any $F \in \mathcal{P}(\mathbf{R})$ is an $\mathbf{S}$-submodule of $\mathbf{R}$. Additionally, $\ker(F)$ is free, if $F \in \mathcal{P}_t^*(\mathbf{R})$ for $t \in \mathbb{N}$.

Proof. Choose $F = \sum\limits_{i=0}^{t} f_i \tau^i(X) \in \mathcal{P}(\mathbf{R})$. Suppose that $\zeta_1, \zeta_2 \in \ker(F)$ and $s \in \mathbf{S}$. Then, $\zeta_1 + \zeta_2, s \cdot \zeta_1 \in \ker(F)$ since

$$\sum_{i=0}^{t} f_i \tau^i(\zeta_1 + \zeta_2) = \sum_{i=0}^{t} f_i(\tau^i(\zeta_1) + \tau^i(\zeta_2)) = \sum_{i=0}^{t} f_i \tau^i(\zeta_1) + \sum_{i=0}^{t} f_i \tau^i(\zeta_2) = 0,$$
$$F(s \cdot \zeta_1) = \sum_{i=0}^{t} f_i \cdot s \cdot \tau^i(\zeta_1) = s \sum_{i=0}^{t} f_i \tau^i(\zeta_1) = 0.$$

Suppose that $f_t = 1$ and find minimal basis $\boldsymbol{\chi} = (\chi_1, \ldots, \chi_l)$ of $\ker(F)$. Assume there exists $i \in \mathbb{N}, i \leq l$, for which $\chi_i \in p\mathbf{R}$. Find maximal exponent $e \in \mathbb{N}$ and a unit $\upsilon \in \mathbf{R}^*$ satisfying $\chi_i = p^e \cdot \upsilon$. It results in $\tau^t(\upsilon) \in \mathbf{R}^*$ and $F(\chi_i) = p^e \cdot F(\upsilon) = p^e \left(\tau^t(\upsilon) + \sum\limits_{i=0}^{t-1} f_i \tau^i(\upsilon)\right)$. Hence, $F(\chi_i) = 0$ if and only if $F(\upsilon) \in p^{n-e}\mathbf{R}$. This can happen if and only if $F(\upsilon) = 0$, and $\boldsymbol{\chi}$ is not minimal in that case.

Now, there is no element of $\boldsymbol{\chi}$ divisible by p. Let $z_1, \ldots, z_l \in \mathbf{S}$ satisfy $\sum\limits_{i=1}^{l} z_i \chi_i = 0$ and at least one of them is non-zero. Find $e = 0, \ldots, n-1$ and $y_1, \ldots, y_l \in \mathbf{R}$ such that $z_i = p^e \cdot y_i$ for each $i \in \mathbb{N}, i \leq l$, and $y_j \in \mathbf{R}^*$ for some $j \in \mathbb{N}$ non-greater l. In the given situation,

$$\sum_{i=1}^{l} z_i \chi_i = 0 \iff p^n \mid \sum_{i=1}^{l} z_i \chi_i \iff p^{n-e} \mid \sum_{i=1}^{l} y_i \chi_i \iff \sum_{i=1}^{l} y_i \chi_i = 0.$$

Consequently, $\chi_j = -\sum\limits_{\substack{i=1 \\ i \neq j}}^{l} \frac{y_i}{y_j} \chi_i$, which contradicts that $\boldsymbol{\chi}$ is the minimal basis. It may be concluded that $\boldsymbol{\chi}$ is a free basis of $\ker(F)$.

□

Thanks to the preceding lemma, we know that roots of a monic linearised polynomial F over $\mathbf{R}$ form a free $\mathbf{S}$-module. This statement may be generalised for linearised polynomials with the leading coefficient being a unit. At first sight, it may not be clear how large the rank of $\ker(F)$ is, even though the intuition likely advises that the rank is connected to degree. Before providing the relation, introduce a useful notation. Consider $F \in \mathcal{P}(\mathbf{R})$ and $\mathbf{x} \in \mathbf{R}^m$ for some $m \in \mathbb{N}$. The codeword $(F(x_1), \ldots, F(x_m)) \in \mathbf{R}^m$ is referred to as $F(\mathbf{x})$.

Claim 75. Let $m \in \mathbb{N}$ and $F \in \mathcal{P}^*_{m+1}(\mathbf{R})$. Then $\operatorname{rank}(\ker(F)) \leq m$.

Proof. Denote $l = \operatorname{rank}(\ker(F))$. **Lemma 74** asserts that the kernel of F is a free $\mathbf{S}$-module, and therefore there exists a free basis $\boldsymbol{\chi} = (\chi_1, \ldots, \chi_l)$ of $\ker(F)$ over $\mathbf{S}$. Set $A = (\tau^{i-1}(\chi_j))_{i,j=1}^{l} \in \mathbf{R}^{l \times l}$, which columns compose a free basis of $\operatorname{Im}(A)$ over $\mathbf{R}$ by applying **Theorem 63**. Grounded on **Theorem 37**, the matrix A is invertible, so $\mathbf{g} \in \mathbf{R}^l$ exists unique such as $A \cdot \mathbf{g}^\top = (-\tau^l(\chi_i))_{i=1}^{l}$. Define $G(X) = \tau^l(X) + \sum\limits_{i=1}^{l} g_i \cdot \tau^{i-1}(X) \in \mathcal{P}^*_{l+1}(\mathbf{R})$. Then, for every $i = 1, \ldots, l$, we have $G(\chi_i) = \tau^l(\chi_i) + \sum\limits_{i=1}^{l} g_i \cdot \tau^{i-1}(\chi_i) = \tau^l(\chi_i) + \sum\limits_{i=1}^{l} \mathbf{A}^c_i \cdot g_i = \tau^l(\chi_i) - \tau^l(\chi_i) = 0$, which means that $\langle \chi_1, \ldots, \chi_l \rangle_{\mathbf{S}} \subseteq \ker(G)$.

Suppose $y \in \ker(G) \setminus \langle \chi_1, \ldots, \chi_l \rangle_{\mathbf{S}}$ exists. Find $e = 0, \ldots n-1$ and $\chi_{l+1} \in \mathbf{R}^*$ such that $y = p^e \cdot \chi_{l+1}$. Note that $0 = G(y) = p^e \cdot G(\chi_{l+1})$ can happen if and only if $p^{n-e} \mid G(\chi_{l+1})$, which is equivalent to $G(\chi_{l+1}) = 0$ as G is monic and $p \nmid \chi_{l+1}$. Thus, $\chi_{l+1} \in \ker(F)$. Set $\mathbf{z} = (\chi_1, \ldots, \chi_{l+1}) \in \mathbf{R}^{l+1}$. **Theorem 48** implies $\operatorname{rk}(\mathbf{z}) = l + 1$. Consider $B = (\tau^{i-1}(\chi_j))_{i,j=1}^{l+1}$ with the columns forming a free basis of $\operatorname{Im}(B)$ over $\mathbf{R}$ as stated by **Theorem 63**. On the other hand, $G(\mathbf{z}) = \mathbf{o}$ if and only if $\sum\limits_{i=1}^{l} \mathbf{B}_i^c \cdot g_i = (-\tau^l(\chi_j))_{j=1}^{l+1} = -\mathbf{B}_{l+1}^c$, which contradicts $(\mathbf{B}_1^c, \ldots, \mathbf{B}_{l+1}^c)$ being the free basis. Hence, $\ker(G) = \langle \chi_1, \ldots, \chi_l \rangle_{\mathbf{S}}$ and $l \leq m$.

□

Let $\mathbf{g} \in \mathbf{R}^m$ has cardinal rank m. Proof of the prior claim provides a way to construct a linearised polynomial F, whose kernel is precisely $\langle g_1, \ldots, g_m \rangle_{\mathbf{S}}$. Now, we show that there is exactly one such F.

Lemma 76. Let $m \in \mathbb{N}$, $\mathbf{x} \in \mathbf{R}^m$ satisfy $\operatorname{rk}(\mathbf{x}) = m$ and $G \in \mathcal{P}(\mathbf{R})$. There exists the unique $F \in \mathcal{P}_{m+1}^*(\mathbf{R})$ such that $\ker(F) = \langle x_1, \ldots, x_m \rangle_{\mathbf{S}}$. Furthermore, $G(\mathbf{x}) = \mathbf{o}$ if and only if $G = H \circ F$ for some $H \in \mathcal{P}(\mathbf{R})$.

Proof. The existence of F follows directly from the construction of linearised polynomial G in **Claim 75**'s proof. Assume that we already have $F \in \mathcal{P}_{m+1}^*(\mathbf{R})$ with $\ker(f) = \langle x_1, \ldots, x_m \rangle_{\mathbf{S}}$. Choose $d \in \mathbb{N}$ and $G \in \mathcal{P}_d(\mathbf{R})$. Put $d_Q = d - m$. Compute the right quotient $Q \in \mathcal{P}_{d_Q+1}(\mathbf{R})$ and the right remainder $R \in \mathcal{P}_m(\mathbf{R})$ fulfilling $G = Q \circ F + R$ performing **Algorithm 8**. If $R = 0$ then, undoubtedly, $G(\mathbf{x}) = \mathbf{o}$.

Let $R = \sum\limits_{i=1}^{d_R} r_i \tau^{i-1}(X)$ for $d_R = \deg(R) \in \mathbb{N}$. Assume, for contradiction, that $R(\mathbf{x}) = \mathbf{o}$. Define codewords $\mathbf{b}_i = (\tau^{i-1}(x_j))_{j=1}^m \in \mathbf{R}^m$, where $i = 1, \ldots, m$. Then $B = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$ is a free basis over $\mathbf{R}$ due to **Theorem 63**. Express the codeword $R(\mathbf{x}) = \sum\limits_{i=1}^{d_R} r_i \tau^{i-1}(\mathbf{x}) = \sum\limits_{i=1}^{d_R} r_i \mathbf{b}_i = \mathbf{o}$, so B cannot be free as $d_R < m$ and $r_{d_R} \neq 0$, a contradiction. It may be concluded that $G(\mathbf{x}) = R(\mathbf{x}) \neq \mathbf{o}$.

Finally, let $G \in \mathcal{P}_{m+1}^*(\mathbf{R})$ satisfy $\ker(G) = \langle x_1, \ldots, x_m \rangle_{\mathbf{S}}$. Then, by already proven part, there exists $H \in \mathcal{P}(\mathbf{R})$ such that $G = H \circ F$. Since both F and G are monic of degree m, H must equal ε and F must equal G.

□

Before concluding this part about linearised polynomials, we extend the prior lemma to address the general case in which there is no requirement on the cardinal rank.

Theorem 77. Let $m \in \mathbb{N}$ and $\mathbf{x} \in \mathbf{R}^m$ be non-zero. Denote $t = \lfloor n \cdot \operatorname{rk}(\mathbf{x}) \rfloor$. Then, there exists $F \in \mathcal{P}_{t+1}^*(\mathbf{R})$ satisfying $F(\mathbf{x}) = \mathbf{o}$.

Proof. Let $d \in \mathbb{N}$ be the rank of an $\mathbf{S}$-module $A = \langle x_1, \ldots, x_m \rangle_{\mathbf{S}}$. Denote by $B = (p^{n-1}v_1, \ldots, p^{n-1}v_d)$ a free basis of $\operatorname{Soc}(A)$ over $\mathcal{T}$. Clearly, $v_1, \ldots, v_d$ are units of $\mathbf{R}$, or otherwise there exists $i \in \mathbb{N}$ meeting the conditions $i \leq d$ and $p^{n-1}v_i = 0$, which implies B is not the free basis. Set $\mathbf{v} = (v_1, \ldots, v_d) \in \mathbf{R}^d$. In line with **Theorem 54**, $\operatorname{rk}(\mathbf{v}) = n \cdot \frac{d}{n} = d$.

Derived from **Lemma 76**, the unique $G \in \mathcal{P}_{d+1}^*(\mathbf{R})$ exists which satisfies $\ker(G) = \langle v_1, \ldots, v_d \rangle_{\mathbf{S}}$. Thence, A seems to be a submodule of $\ker(G)$, because

$\mathrm{Soc}(A) = \langle B\rangle_{\mathbf{S}} = \mathrm{Soc}(\ker(G))$ and $\ker(G)$ is free. Consequently, $G(\mathbf{x}) = \mathbf{o}$. To finalise the proof, define $F(X) = \tau^{t-d}(X) \circ G(X)$, which seems to be monic of degree t.

□

4.3 Decoding Gabidulin Codes

Any Gabidulin $[m, l]_{\mathbf{R}}$-code can be viewed as the set of linearised polynomials of degree less than l evaluated on the generating codeword, i.e.

$$\mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g}) = \{F(\mathbf{g}) \mid F \in \mathcal{P}_l(\mathbf{R})\} \tag{4.7}$$

for any $\mathbf{g} \in \mathbf{R}^m$ of cardinal rank m. Numerous publications, between them the one by Epelde and Rúa [6], prefer to define Gabidulin codes using the equation 4.7. The lemma 78 validates this equation.

Lemma 78. *Let $l, m \in \mathbb{N}$ such that $l \le m \le \min(n, r)$ and $\mathbf{g} \in \mathbf{R}^m$ satisfy $\mathrm{rk}(\mathbf{g}) = m$. Then, for every $\mathbf{c} \in \mathbf{R}^m$, a linearised polynomial $F \in \mathcal{P}_l(\mathbf{R})$, which fulfills $\mathbf{c} = F(\mathbf{g})$, exists if and only if $\mathbf{c} \in \mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$.*

Proof. Suppose that $G = (\tau^{i-1}(g_j))_{i=1,j=1}^{l,m}$ is a generator matrix of $\mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$. Assume that $\mathbf{c} \in \mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$, so $\mathbf{c} = \mathbf{z} \cdot G$ for $\mathbf{z} \in \mathbf{R}^l$. Define a linearised polynomial $F = \sum_{i=1}^{l} z_i \cdot \tau^{i-1}(X)$. Then $F \in \mathcal{P}_l(\mathbf{R})$ and

$$\forall i \in \mathbb{N}, i \le m : F(g_i) = \sum_{j=1}^{l} z_j \cdot \tau^{j-1}(g_i) = \mathbf{z} \cdot \mathbf{G}_i^c = c_i \tag{4.8}$$

Now, let $F(X) = \sum_{i=1}^{l} z_i \cdot \tau^{i-1}(X) \in \mathcal{P}_l(\mathbf{R})$. Hence, $F(\mathbf{g}) \in \mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$ follows from the equations (4.8).

□

Consider positive integers m and l satisfying $l \le m \le \min(n, r)$. Choose $\mathbf{g} \in \mathbf{R}^m$ with the full cardinal rank and abbreviate $\mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$ to $\mathcal{G}$. Let $\mathbf{c} \in \mathcal{G}$ be a sent codeword over some channel and $\mathbf{e} \in \mathbf{R}^m$ be the received codeword. In theory, if $\mathrm{d}_{\mathcal{R}}(\mathbf{c}, \mathbf{e}) < \mathrm{d}_{\mathcal{R}}(\mathcal{G})$ then the code $\mathcal{G}$ is able to detect errors, and if $\mathrm{d}_{\mathcal{R}}(\mathbf{c}, \mathbf{e}) < \frac{\mathrm{d}_{\mathcal{R}}(\mathcal{G})}{2}$ then $\mathcal{G}$ is even capable of correcting errors and recovering the original $\mathbf{c}$.

A decoding algorithm for Gabidulin codes over Galois rings can be grounded on a division of linearised polynomials as proposed in Kamche and Mouaha's work [16, Chapter 3]. The lemma 79 encompasses the principal idea of decoding.

Lemma 79. *Let $l, m \in \mathbb{N}$ be such that $l \le m \le \min(n, r)$ and $\mathbf{g} \in \mathbf{R}^m$ have full cardinal rank. Set $\mathcal{G} = \mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$, $k = \frac{m-l}{2n}$ and $t = \lfloor nk \rfloor$. Assume that there exist codewords $\mathbf{c} \in \mathcal{G}$ and $\mathbf{y} \in \mathbf{R}^m$ such that $\mathrm{d}_{\mathcal{R}}(\mathbf{c}, \mathbf{y}) \le k$. Let $F \in \mathcal{P}_l^*(\mathbf{R})$ meet the condition $F(\mathbf{g}) = \mathbf{c}$. Define $\mathbf{b} = (\tau^t(y_i))_{i=1}^m \in \mathbf{R}^m$ and a block matrix $A = \begin{pmatrix} G & Y \end{pmatrix}$ of type $m \times (l + 2t)$ over $\mathbf{R}$, where*

$$G = \begin{pmatrix} g_1 & \tau(g_1) & \dots & \tau^{l+t-1}(g_1) \\ \vdots & \vdots & \ddots & \vdots \\ g_m & \tau(g_m) & \dots & \tau^{l+t-1}(g_m) \end{pmatrix}, Y = -\begin{pmatrix} y_1 & \tau(y_1) & \dots & \tau^{t-1}(y_1) \\ \vdots & \vdots & \ddots & \vdots \\ y_m & \tau(y_m) & \dots & \tau^{t-1}(y_m) \end{pmatrix}.$$

Then, $\mathbf{u} \in \mathbf{R}^{l+t}$, $\mathbf{v} \in \mathbf{R}^{t}$, which solve the linear system $A \cdot \left(\begin{smallmatrix}\mathbf{u}^\top \\ \mathbf{v}^\top\end{smallmatrix}\right) = \mathbf{b}^\top$, exist. Especially, $U = \sum_{i=1}^{l+t} u_i\tau^{i-1}(X)$ and $V = \tau^{t}(X) + \sum_{i=1}^{t} v_i\tau^{i-1}(X)$ satisfy $U = V \circ F$ and $U(\mathbf{g}) = V(\mathbf{c})$.

Proof. Begin by proving the existence of solutions. Set $d = \mathrm{d}_{\mathcal{R}}(\mathbf{c}, \mathbf{y})$, $f_d = \lfloor nd \rfloor$ and $f_k = \lfloor nk \rfloor$. Due to **Theorem 77**, there exists $W \in \mathcal{P}^*_{f_d}(\mathbf{R})$ such that $W(\mathbf{y} - \mathbf{c}) = \mathbf{o}$, which implies $W(\mathbf{y}) = W(\mathbf{c}) = W \circ F(\mathbf{g})$. Define $\mathbf{u} \in \mathbf{R}^{l+f_k}$ and $\mathbf{v} \in \mathbf{R}^{f_k}$ by the subsequent formulas

$$U = \tau^{f_k - f_d}(W \circ F(X)) = \sum_{i=1}^{l+f_k} u_i \cdot \tau^{i-1}(X) \in \mathcal{P}_{l+f_k}(\mathbf{R}), \tag{4.9}$$

$$V = \tau^{f_k - f_d}(W(X)) = \tau^{f_k}(X) + \sum_{i=1}^{f_k} v_i \cdot \tau^{i-1}(X) \in \mathcal{P}^*_{f_k+1}(\mathbf{R}). \tag{4.10}$$

Choose $i \in \mathbb{N}, i \leq m$, and verify that the i^{th} coordinate of $A \cdot \left(\begin{smallmatrix}\mathbf{u}^\top \\ \mathbf{v}^\top\end{smallmatrix}\right)$ equals $\tau^{f_k}(y_i)$:

$$\begin{aligned}\left(A \cdot \left(\begin{smallmatrix}\mathbf{u}^\top \\ \mathbf{v}^\top\end{smallmatrix}\right)\right)_i &= \sum_{j=1}^{l+f_k} \tau^{j-1}(g_i)u_j - \sum_{j=1}^{f_k} \tau^{j-1}(y_i)v_j = U(g_i) - V(y_i) + \tau^{f_k}(y_i) \\ &\underset{(4.10)}{\overset{(4.9)}{=}} \tau^{f_k - f_d}(\underbrace{W \circ F(g_i) - W(y_i)}_{=0 \text{ since } W\circ F(g_i) = W(y_i)}) + \tau^{f_k}(y_i) = \tau^{f_k}(y_i).\end{aligned} \tag{4.11}$$

Suppose that solutions $\mathbf{u} \in \mathbf{R}^{l+f_k}$ and $\mathbf{v} \in \mathbf{R}^{f_k}$ of the linear system are given. Set $U = \sum_{i=1}^{l+f_k} u_i \cdot \tau^{i-1}(X) \in \mathcal{P}_{l+f_k}(\mathbf{R})$ and $V = \tau^{f_k}(X) + \sum_{i=1}^{f_k} v_i \cdot \tau^{i-1}(X) \in \mathcal{P}^*_{f_k+1}(\mathbf{R})$. Derived from the first line of (4.11), $\mathbf{b} = U(\mathbf{g}) - V(\mathbf{y}) + \mathbf{b}$ and so $U(\mathbf{g}) = V(\mathbf{y})$. Observe that $(U - V \circ F)(\mathbf{g}) = U(\mathbf{g}) - V \circ F(\mathbf{g}) = V(\mathbf{y}) - V(F(\mathbf{g})) = V(\mathbf{y} - F(\mathbf{g}))$ and $\mathrm{rk}((U - V \circ F)(\mathbf{g})) = \mathrm{rk}(V(\mathbf{y} - F(\mathbf{g}))) \leq \mathrm{rk}(\mathbf{y} - F(\mathbf{g})) \leq k$. Once again using **Theorem 77**, a monic linearised polynomial H of degree at most f_k exists, which satisfies $H(U - V \circ F)(\mathbf{g})) = \mathbf{o}$. So the degree of $H' = H((U - V \circ F)$ is

$$\begin{aligned}\deg(H') &\leq \deg(H) + \max(\deg(U), \deg(V \circ F)) \leq f_k + f_k + l - 1 \\ &= 2 \cdot \left\lfloor n \cdot \frac{m - l}{2n} \right\rfloor + l - 1 \leq m - l + l - 1 = m - 1.\end{aligned}$$

In accordance with **Theorem 76**, there exist $G' \in \mathcal{P}^*_{m+1}(\mathbf{R})$ and $Q \in \mathcal{P}(\mathbf{R})$ such that $\ker(G') = \langle g_1, \ldots, g_m \rangle_{\mathbf{S}}$ and $H' = Q \circ G'$. Since $\deg(H') < \deg(G')$, both Q and H' must be constant zeros. In conclusion, $U = V \circ F$, because H is monic and non-zero.

□

Let $\mathbf{g}, \mathbf{y} \in \mathbf{R}^m$ and $U, V \in \mathcal{P}(\mathbf{R})$ be given as in **Lemma 79**. In this scenario, $F \in \mathcal{P}_l(\mathbf{R})$, which satisfies $F(\mathbf{g}) \in \mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$ and $\mathrm{d}_{\mathcal{R}}F(\mathbf{c}), \mathbf{y} \leq \frac{m-l}{2n}$, can be computed by the left division of U by V. As a result, the decoding algorithm is described below.

Theorem 80. Let $m, l \in \mathbb{N}$ be such that $l \leq m \leq \min(r, n)$ and $\mathbf{g} \in \mathbf{R}^m$ satisfy $\mathrm{rk}(\mathbf{g}) = m$. Let $\mathbf{y} \in \mathbf{R}^m$ and $\mathbf{c} \in \mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$. Then, **Algorithm 9** outputs $\mathbf{c}$ on the input $m, l, \mathbf{g}, \mathbf{y}$ if and only if $\mathrm{d}_{\mathcal{R}}(\mathbf{y}, \mathbf{c}) \leq \frac{m-l}{2n}$.

Algorithm 9 Decoding for Gabidulin codes

```
Require: $m, l \in \mathbb{N}, \mathbf{g}, \mathbf{y} \in \mathbf{R}^m$ such that $\mathrm{rk}(\mathbf{g}) = m$
Ensure: $\mathbf{c} \in \mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$ such that $\mathrm{d}_{\mathcal{R}}(\mathbf{c}, \mathbf{y}) \leq \frac{m-l}{2n}$, or $\perp$
  $k \leftarrow \left\lfloor \frac{m-l}{2} \right\rfloor$
  $G \leftarrow (\tau^{j-1}(g_i))_{i=1,j=1}^{m,l+k}$, $Y \leftarrow (-\tau^{j-1}(y_i))_{i=1,j=1}^{m,k}$, $\mathbf{b} \leftarrow (\tau^k(y_i))_{i=1}^m$
  $\mathcal{Z} \leftarrow \left\{(\mathbf{u}, \mathbf{v}) \mid \mathbf{u} \in \mathbf{R}^{k+l}, \mathbf{v} \in \mathbf{R}^k : G \cdot \mathbf{u}^\top + Y \cdot \mathbf{v}^\top = \mathbf{b}^\top\right\} = \{(\mathbf{u}_j, \mathbf{v}_j)\}_{j=1}^t$
  $j \leftarrow 1$
  while $j \leq t$ do
      $U \leftarrow \sum_{i=1}^{l+k} u_{ji} \cdot \tau^{i-1}(X)$, $V \leftarrow \tau^k(X) + \sum_{i=1}^{k} v_{ji} \cdot \tau^{i-1}(X)$
      $(Q, -, R, -) \leftarrow$ Algorithm 8$(U, V)$
      if $((R = 0) \wedge (\mathrm{d}_{\mathcal{R}}(\mathbf{y}, Q(\mathbf{g})) \leq \frac{m-l}{2n}))$ then
          return $Q(\mathbf{g})$
      end if
      $j \leftarrow j + 1$
  end while
  return $\perp$
```

Proof. If $\mathrm{d}_{\mathcal{R}}(\mathbf{y}, \mathbf{c}) \leq \frac{m-l}{2n}$ then it is clear using **Lemma 79**. Assume that $Q(\mathbf{g})$ is the output of **Algorithm 9** applied to $m, l, \mathbf{g}, \mathbf{y}$. It is evident that $Q \in \mathcal{P}_l(\mathbf{R})$ since $U = V \circ Q$ for $U \in \mathcal{P}_{l+\left\lfloor \frac{m-l}{2} \right\rfloor}(\mathbf{R})$ and $V \in \mathcal{P}^*_{\left\lfloor \frac{m-l}{2} \right\rfloor + 1}(\mathbf{R})$. Set $\mathbf{c} = Q(\mathbf{g})$, so $\mathbf{c} \in \mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$ in line with **Lemma 78**. In conclusion, $\mathrm{d}_{\mathcal{R}}(\mathbf{y}, \mathbf{c}) \leq \frac{m-l}{2n}$ as the algorithm returned $\mathbf{c}$, i.e. the conditions $R = 0$ and $\mathrm{d}_{\mathcal{R}}(\mathbf{y}, \mathbf{c}) \leq \frac{m-l}{2n}$ were met.

□

Refer to the matrices $G \in \mathbf{R}^{m \times (l+k)}$, $Y \in \mathbf{R}^{m \times k}$ of types $m \times (l+k)$ and $m \times k$ over $\mathbf{R}$, respectively, and the codeword $\mathbf{b} \in \mathbf{R}^m$ from **Algorithm 9**. Similarly, as described in Epelde and Rúa's work [6, Section 5.2], the system of linear equations $G \cdot \mathbf{u}^\top + Y \cdot \mathbf{v}^\top = \mathbf{b}^\top$ may be partially precomputed since the matrix G is fixed given the Gabidulin code. Divide the matrices G, Y and the codeword $\mathbf{b}$ into two blocks: $G = \left(\begin{smallmatrix} G_1 \\ G_2 \end{smallmatrix}\right)$ and $Y = \left(\begin{smallmatrix} Y_1 \\ Y_2 \end{smallmatrix}\right)$, where the first blocks consist of first $l + k$ rows, and $\mathbf{b} = \begin{pmatrix} \mathbf{b}_1 & \mathbf{b}_2 \end{pmatrix}$ is divided accordingly. Thence, the matrix G_1 is invertible by applying **Theorem 63** to $G^\top$ and following **Theorem 37**. Consequently, $G \cdot \mathbf{u}^\top + Y \cdot \mathbf{v}^\top = \mathbf{b}^\top$ if and only if $G_i \cdot \mathbf{u}_i^\top + Y_i \cdot \mathbf{v}_i^\top = \mathbf{b}_i^\top$ for both $i \in \{1, 2\}$. This is equivalent to

$$(Y_2 - G_2 G_1^{-1} Y_1) \cdot \mathbf{v}^\top = \mathbf{b}_2^\top - G_2 G_1^{-1} \mathbf{b}_1^\top \ \wedge \ \mathbf{u}^\top = G_1^{-1}(\mathbf{b}_1^\top - Y_1 \mathbf{v}^\top),$$

where matrices G_1^{-1} and $G_2 \cdot G_1^{-1}$ can be computed beforehand.

We illustrate the decoding for Gabidulin codes in an example, by which we end this section. A good understanding of decoding is essential as a PKC is grounded on it.

Example 16. Let $\mathbf{R} = \mathrm{GR}(5^5, 4)$, $\mathbf{S} = \mathrm{GR}(5^5, 1)$, the basic primitive polynomial $G_{5,4}(x) = x^4 + 450x^3 + 830x^2 + 1892x + 3124$ over $\mathbb{Z}_{5^5}[x]$, $\xi = x + (G_{5,4})$ and the free basis $B = (1, \xi, \xi^2, \xi^3)$ of $\mathbf{R}$ over $\mathbf{S}$ all be such as in *Example* 14. Consider $\mathbf{g} = (0{:}11{:}9{:}0, 0{:}0{:}31{:}124, 19{:}0{:}934{:}0, 87{:}0{:}21{:}0) \in \mathbf{R}^4$, which satisfy $\mathrm{rk}(\mathbf{g}) = 4$ by (4.2). Thus, the Gabidulin code $\mathcal{G} = \mathrm{Gab}_{\mathbf{R}}(4, 2, \mathbf{g})$ has the generator matrix $G \in \mathbf{R}^{2 \times 4}$

from (4.3)

$$G = \begin{pmatrix} 0{:}11{:}9{:}0 & 0{:}0{:}31{:}124 & 19{:}0{:}934{:}0 & 87{:}0{:}21{:}0 \\ 481{:}948{:}631{:}3119 & 1770{:}1098{:}2806{:}1799 & 2638{:}1089{:}2965{:}1596 & 229{:}1959{:}2934{:}1008 \end{pmatrix}.$$

Set $\mathbf{z} = \left(0{:}91{:}2875{:}1,\ 28{:}0{:}0{:}1123\right) \in \mathbf{R}^2$ and the codeword $\mathbf{c} \in \mathcal{G}$ determined by $\mathbf{z}$, i.e. $\mathbf{c} = \mathbf{z} \cdot G = \begin{pmatrix} 1913{:}590{:}1648{:}2441 \\ 2138{:}2810{:}207{:}1244 \\ 2682{:}2904{:}775{:}2133 \\ 715{:}2361{:}358{:}1251 \end{pmatrix}^\top$. Let $\mathbf{e} = \begin{pmatrix} 2500{:}1875{:}2500{:}1250 \\ 625{:}1250{:}625{:}1875 \\ 1250{:}2500{:}1250{:}625 \\ 625{:}1250{:}625{:}1875 \end{pmatrix}^\top$ be an error codeword. We have to verify that $\operatorname{rk}(\mathbf{e}) \leq \frac{4-2}{2\cdot 5} = \frac{1}{5}$. Thus,

$$[\mathbf{e}]_B = \begin{pmatrix} 1250 & 1875 & 625 & 1875 \\ 2500 & 625 & 1250 & 625 \\ 1875 & 1250 & 2500 & 1250 \\ 2500 & 625 & 1250 & 625 \end{pmatrix} \sim \begin{pmatrix} 625 & 2500 & 1875 & 2500 \\ 2500 & 625 & 1250 & 625 \\ 1875 & 1250 & 2500 & 1250 \\ 2500 & 625 & 1250 & 625 \end{pmatrix} \sim \begin{pmatrix} 625 & 2500 & 1875 & 2500 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (4.12)$$

where the first row of $[\mathbf{e}]_B$ is multiplied by an integer 1563, and afterwards, an 3121-multiple of the first row is added to the second and the fourth row and an 3122-multiple to the third row. Using **Claim 48**, the cardinal rank of $\mathbf{e}$ is $\operatorname{rk}(\mathbf{e}) = \operatorname{rk}([\mathbf{e}]_B) = \operatorname{rk}([\mathbf{e}]_B^\top) = \log_{5^5}(|\operatorname{Im}[\mathbf{e}]_B^\top|) = \log_{5^5}(5) = \frac{1}{5}$. Therefore, the code $\mathcal{G}$ is able to correct a codeword $\mathbf{y} \in \mathbf{R}^4$ corrupted by the error $\mathbf{e}$, i.e.

$$\begin{aligned} \mathbf{y} &= \mathbf{c} + \mathbf{e} \\ &= \left(1288{:}2465{:}1023{:}566, 2763{:}935{:}832{:}3119, 807{:}2279{:}2025{:}2758, 1340{:}486{:}983{:}1\right). \end{aligned} \quad (4.13)$$

Now, we perform **Algorithm 9** to decode corrupted $\mathbf{y}$. Note that $\left\lfloor \frac{4-2}{2} \right\rfloor = 1$. Let $A = \left(G_1 \ \ -\mathbf{y}^\top \middle| \ \mathbf{b}^\top\right)$ be an augmented matrix representing the linear system $G_1 \cdot \mathbf{u}^\top - v \cdot \mathbf{y}^\top = \mathbf{b}^\top$ for $G_1 = (\tau^{j-1}(g_i))_{i=1,j=1}^{4,3}$ and $\mathbf{b} = (\tau(y_i))_{i=1}^{4}$. In the described scenario,

$$A = \left(\begin{array}{cccc|c} 0{:}11{:}9{:}0 & \tau(0{:}11{:}9{:}0) & \tau^2(0{:}11{:}9{:}0) & -y_1 & \tau(1288{:}2465{:}1023{:}566) \\ 0{:}0{:}31{:}124 & \tau(0{:}0{:}31{:}124) & \tau^2(0{:}0{:}31{:}124) & -y_2 & \tau(2763{:}935{:}832{:}3119) \\ 19{:}0{:}934{:}0 & \tau(19{:}0{:}934{:}0) & \tau^2(19{:}0{:}934{:}0) & -y_3 & \tau(807{:}2279{:}2025{:}2758) \\ 87{:}0{:}21{:}0 & \tau(87{:}0{:}21{:}0) & \tau^2(87{:}0{:}21{:}0) & -y_4 & \tau(1340{:}486{:}983{:}1) \end{array}\right),$$

which equals

$$\left(\begin{array}{cccc|c} 0{:}11{:}9{:}0 & 481{:}948{:}631{:}3119 & 2030{:}2999{:}3121{:}2565 & 1837{:}660{:}2102{:}2559 & 816{:}2358{:}2015{:}2618 \\ 0{:}0{:}31{:}124 & 1770{:}1098{:}2806{:}1799 & 803{:}3001{:}2882{:}671 & 362{:}2190{:}2293{:}6 & 691{:}175{:}1139{:}2651 \\ 19{:}0{:}934{:}0 & 2638{:}1089{:}2965{:}1596 & 1990{:}328{:}30{:}3019 & 2318{:}846{:}1100{:}367 & 2138{:}2015{:}3001{:}937 \\ 87{:}0{:}21{:}0 & 229{:}1959{:}2934{:}1008 & 302{:}1913{:}3048{:}2955 & 1785{:}2639{:}2142{:}3124 & 2541{:}735{:}1190{:}2905 \end{array}\right)$$

Multiply the first row by $\left(1496{:}2942{:}2382{:}1854\right)$ and after that, add the first row multiplied by $\left(0{:}0{:}3094{:}3001\right)$, $\left(3106{:}0{:}2191{:}0\right)$ and $\left(3038{:}0{:}3104{:}0\right)$ to the second row, the third row and the fourth row in the specified order:

$$\left(\begin{array}{cccc|c} 0{:}0{:}0{:}1 & 819{:}1118{:}1949{:}1280 & 1955{:}1395{:}1625{:}719 & 1862{:}1666{:}1223{:}847 & 1216{:}2409{:}1415{:}1530 \\ 0{:}0{:}0{:}0 & 3106{:}3042{:}1188{:}2065 & 3013{:}546{:}3{:}910 & 2103{:}1328{:}33{:}2881 & 928{:}1524{:}2206{:}235 \\ 0{:}0{:}0{:}0 & 2153{:}636{:}1502{:}2899 & 14{:}743{:}1269{:}649 & 1802{:}254{:}2258{:}1062 & 2685{:}278{:}2863{:}1578 \\ 0{:}0{:}0{:}0 & 3122{:}1359{:}2862{:}811 & 99{:}2933{:}2044{:}2200 & 343{:}1891{:}499{:}1541 & 646{:}194{:}829{:}224 \end{array}\right).$$

Now, normalise the second row by multiplying it by $\left(2206{:}1228{:}1982{:}2394\right)$. Then, reduce the first, the third and the fourth row by adding the second row multiplied by $\left(2306{:}2007{:}1176{:}1845\right)$, $\left(972{:}2489{:}1623{:}226\right)$ and $\left(3{:}1766{:}263{:}2314\right)$, respectively:

$$\left(\begin{array}{cccc|c} 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 & 367{:}420{:}1492{:}1940 & 625{:}3034{:}250{:}3124 & 964{:}2940{:}201{:}1626 \\ 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 & 1937{:}1388{:}23{:}422 & 1222{:}1875{:}1875{:}2002 & 2432{:}2100{:}1949{:}879 \\ 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 1448{:}2994{:}3029{:}315 & 2500{:}1250{:}1875{:}2500 & 1433{:}179{:}729{:}2401 \\ 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 1878{:}2010{:}1407{:}1711 & 2500{:}1250{:}625{:}2500 & 698{:}2197{:}1793{:}2213 \end{array}\right).$$

Finally, multiply the third row by a scalar $(\text{1996:2689:1247:1124})$. Subsequently, add $(\text{2758:2705:1633:1185})$, $(\text{1188:1737:3102:2703})$ and $(\text{1247:1115:1718:1414})$-multiple of the third row to the first, the second and the fourth row in the given order:

$$\left(\begin{array}{cccc|c} \text{0:0:0:1} & \text{0:0:0:0} & \text{0:0:0:0} & \text{1250:534:875:2499} & \text{1875:1875:2500:2500} \\ \text{0:0:0:0} & \text{0:0:0:1} & \text{0:0:0:0} & \text{2472:625:2500:127} & \text{2481:381:432:615} \\ \text{0:0:0:0} & \text{0:0:0:0} & \text{0:0:0:1} & \text{1875:1875:0:0} & \text{2896:754:2747:2700} \\ \text{0:0:0:0} & \text{0:0:0:0} & \text{0:0:0:0} & \text{1875:1875:2500:1875} & \text{2500:1875:625:2500} \end{array}\right).$$

Thence, it is possible to straightforwardly compute $v_1 \in \mathbf{R}$ and $\mathbf{u} \in \mathbf{R}^3$, which satisfy $G_1 \cdot \mathbf{u}^\top - v_1 \cdot \mathbf{y}^\top = \mathbf{b}^\top$:

$$\begin{aligned} v_1 &= (\text{2:4:2:1}) \\ \mathbf{u} &= (\text{1824:1381:2671:2340}, \text{2018:1595:473:3039}, \text{1646:2004:1497:825}) \end{aligned} \tag{4.14}$$

Define linearised polynomials

$$\begin{aligned} U(X) &= (\text{1646:2004:1497:825})\tau^2(X) + (\text{2018:1595:473:3039})\tau(X) + (\text{1824:1381:2671:2340})X \\ V(X) &= \tau(X) + (\text{2:4:2:1})X. \end{aligned}$$

Conclude from *Example* 15, $Q(X) = (\text{28:0:0:1123})\tau(X) + (\text{0:91:2875:1})X$ satisfies $U(X) = V \circ Q(X)$. Undoubtedly, the coefficients of Q are the coordinates of $\mathbf{z}$ in the reversed order, so truly $Q(\mathbf{g}) = \mathbf{z} \cdot G = \mathbf{c}$. Since the left remainder is zero and $\mathrm{d}_{\mathcal{R}}(\mathbf{y}, Q(\mathbf{g})) = \mathrm{rk}(\mathbf{e}) \leq \frac{1}{5}$, Algorithm 9 would output $Q(\mathbf{g}) \in \mathcal{G}$.

4.4 GPT Cryptosystem

Gabidulin et al. [2] presented a modification of the McEliece cryptosystem, known as the GPT cryptosystem, to effectively utilise the Gabidulin codes. In this section, a version of the GPT PKC over Galois rings is derived from the Smart approach for GPT Cryptosystem [4].

Let $\mathbf{x} \in \mathbf{R}^m$, $A \in \mathbf{R}^m$ and $I \subseteq \{1, \ldots, m\}$ be given. Then, the codeword composed of the $\mathbf{x}$'s coordinates with the indices from I shall be denoted by $\mathbf{x}_I$. Similarly, the matrices created by omitting the rows and the columns of A, which indices are not contained in I, shall be written as $A_{I\cdot}$ and $A_{\cdot I}$, respectively. Now, let us depict the GPT cryptosystem over a Galois ring by its building blocks: key generation, encryption, and decryption algorithms.

Algorithm 10 GPT Cryptosystem Key Generation

```
Require: $p$ prime, $a, l, m, n, r, t \in \mathbb{N}$, $l \leq m \leq \min(r, n)$ and $2 \leq a \leq t$
Ensure: a public key $\mathcal{K}_{\text{pub}} = (G_{\text{pub}}, e)$, a private key $\mathcal{K}_{\text{priv}} = (\mathbf{g}, G_{\text{priv}}, T^{-1}, t)$
  $\mathbf{R} \leftarrow \mathrm{GR}(p^n, r)$
  choose a random $\mathbf{g} \in \mathbf{R}^m$ such that $\mathrm{rk}(\mathbf{g}) = m$, $G \leftarrow (\tau^{i-1}(g_j))_{i=1,j=1}^{l,m}$
  compute $F \in \mathbf{R}^{m \times l}$ satisfying $G \cdot F = I_l$
  choose $\mathbf{x} \in \mathbf{R}^a$ for which $\mathrm{rank}(\mathrm{Im}(\mathbf{x})_{\mathbf{S}}) = a$ and $\mathrm{rk}(\mathbf{x}) < a$
  $X_1 \leftarrow (\tau^{i-1}(x_j))_{i=1,j=1}^{l,a}$
  choose $X_2 \in \mathbf{R}^{l \times (t-a)}$ such that $\mathrm{rank}(\mathrm{Im}(X_1)_{\mathbf{S}} + \mathrm{Im}(X_2)_{\mathbf{S}}) = t$
  $X \leftarrow \begin{pmatrix} X_1 & X_2 \end{pmatrix}$
  choose invertible matrices $S \in \mathbf{R}^{l \times l}$ and $T \in \mathbf{S}^{(m+t) \times (m+t)}$, compute $T^{-1}$
  $G_{\text{pub}} \leftarrow S \cdot \begin{pmatrix} X & G \end{pmatrix} \cdot T$; $G_{\text{priv}} \leftarrow F \cdot S^{-1}$
  choose $e \in \mathbb{N}$, $e \leq \frac{m-l}{2n}$
  return $(G_{\text{pub}}, e), (\mathbf{g}, G_{\text{priv}}, T^{-1}, t)$
```

Algorithm 11 GPT Cryptosystem Encryption

```
Require: $\mathbf{x} \in \mathbf{R}^l, \mathcal{K}_{\text{pub}} = (G_{\text{pub}}, e)$
Ensure: $\mathbf{c} = \text{Enc}_{\mathcal{K}_{\text{pub}}}(\mathbf{x})$
  choose $\mathbf{z} \in \mathbf{R}^{m+t}$ such that $\text{rk}(\mathbf{z}) \leq e$
  return $\mathbf{x} \cdot G_{\text{pub}} + \mathbf{z}$
```

Algorithm 12 GPT Cryptosystem Decryption

```
Require: $\mathbf{c} \in \mathbf{R}^{m+t}, \mathcal{K}_{\text{priv}} = (\mathbf{g}, G_{\text{priv}}, T^{-1}, t)$
Ensure: $\mathbf{x} = \text{Dec}_{\mathcal{K}_{\text{priv}}}(\mathbf{c})$, or $\perp$
  $d \leftarrow (\mathbf{c} \cdot T^{-1})_{\{t+1,\ldots,m+t\}}$
  $\mathbf{y} \leftarrow$ Algorithm 9$(m, l, \mathbf{g}, \mathbf{d})$
  if $\mathbf{y} \neq \perp$ then
      return $\mathbf{y} \cdot G_{\text{priv}}$
  else
      return $\perp$
  end if
```

Lemma 81. The decryption of the GPT cryptosystem is correct.

Proof. Suppose that $\mathcal{K}_{\text{pub}}, \mathcal{K}_{\text{priv}}$ and $\mathbf{c} = \mathbf{x} \cdot G_{\text{pub}} + \mathbf{z}$ are given, where $\mathbf{x} \in \mathbf{R}^l$ and $\mathbf{z} \in \mathbf{R}^{m+t}$ satisfying $\text{rk}(\mathbf{z}) \leq e$. Denote $I = \{t+1, \ldots, t+m\}$. Begin by computing $\mathbf{c} \cdot T^{-1} = (\mathbf{x} \cdot G_{\text{pub}} + z) \cdot T^{-1} = \mathbf{x} \cdot S \cdot \begin{pmatrix} X & G \end{pmatrix} + z \cdot T^{-1}$. Thus,

$$\begin{aligned}\mathbf{d} = \left(\mathbf{c} \cdot T^{-1}\right)_I = \left(\mathbf{x} \cdot S \cdot \begin{pmatrix} X & G \end{pmatrix} + z \cdot T^{-1}\right)_I &= \left(\mathbf{x} \cdot S \cdot \begin{pmatrix} X & G \end{pmatrix}\right)_I + \left(z \cdot T^{-1}\right)_I \\ = (\mathbf{x} \cdot S) \cdot \begin{pmatrix} X & G \end{pmatrix}_{.I} + \left(z \cdot T^{-1}\right)_I &= (\mathbf{x} \cdot S) \cdot G + \left(z \cdot T^{-1}\right)_I .\end{aligned}$$

According to **Lemma 53**, $\text{rk}(\mathbf{z} \cdot T^{-1}) = \text{rk}(\mathbf{z})$. Observe that omitting coordinates cannot increase the cardinal rank, so $\text{rk}((\mathbf{z} \cdot T^{-1})_I) \leq \text{rk}(\mathbf{z} \cdot T^{-1})$. It directly results in $\text{rk}((\mathbf{z} \cdot T^{-1})_I) \leq e \leq \frac{m-l}{2n}$. Therefore, **Algorithm 9** applied to $\mathbf{d}$ returns the codeword $\mathbf{y} = \mathbf{x} \cdot S \cdot G$ due to **Theorem 80**. Finally, it is possible to obtain the original message $\mathbf{x}$ as

$$\mathbf{y} \cdot G_{\text{priv}} = \mathbf{x} \cdot S \cdot G \cdot F \cdot S^{-1} = \mathbf{x} \cdot S \cdot S^{-1} = \mathbf{x},$$

where the existence of the right inverse F of the generator matrix G is deduced from **Theorem 63** and **Theorem 37**.

□

Note that the matrix G_{priv} can be omitted from the private key $\mathcal{K}_{\text{priv}}$ to create a more memory-efficient version. In this scenario, the message $\mathbf{x}$ can be obtained from the decoded message $\mathbf{y} = \mathbf{x} \cdot A$ by solving the system of linear equalities with the matrix A, where $A = (G_{\text{pub}} \cdot T^{-1})_{.\{t+1,\ldots,t+m\}} = S \cdot G$.

The final stage in this thesis is to display a specific instance of the described GPT cryptosystem. Although the ensuing example is straightforward, performing the decryption is non-trivial. However, some preparations have already been made in the previous examples. We remark here that computations were made partially in Wolfram Mathematica and partially in SageMath.

Example 17. Setup is the same as in *Example* 16. Let $\mathbf{R} = \mathrm{GR}(5^5, 4)$, $\mathbf{S}_{\mathrm{GR}}(5^5, 1)$, $G_{5,4}(x) = x^4 + 450x^3 + 830x^2 + 1892x + 3124$ be basic primitive over $\mathbb{Z}_{5^5}[x]$. Consider $\xi = x + (G_{5,4})$ of order $(5^4 - 1) = 624$ and the basis $B = (1, \xi, \xi^2, \xi^3)$ of $\mathbf{R}$ over $\mathbf{S}$.

Key generation: Let $a = l = t = 2$ and $m = 4$. The equation (4.2) implies that the codeword $\mathbf{g} = (0{:}11{:}9{:}0, 0{:}0{:}31{:}124, 19{:}0{:}934{:}0, 87{:}0{:}21{:}0) \in \mathbf{R}^4$ has cardinal rank $\mathrm{rk}(\mathbf{g}) = 4$. Recall the generator matrix $G \in \mathbf{R}^{2\times 4}$ from (4.3)

$$G = \begin{pmatrix} 0{:}11{:}9{:}0 & 0{:}0{:}31{:}124 & 19{:}0{:}934{:}0 & 87{:}0{:}21{:}0 \\ 481{:}948{:}631{:}3119 & 1770{:}1098{:}2806{:}1799 & 2638{:}1089{:}2965{:}1596 & 229{:}1959{:}2934{:}1008 \end{pmatrix},$$

we have to compute its right inverse:

$$\begin{aligned} \left(G^\top \,\middle|\, I_4 \right) &= \left(\begin{array}{cc|cccc} 0{:}11{:}9{:}0 & 481{:}948{:}631{:}3119 & 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 \\ 0{:}0{:}31{:}124 & 1770{:}1098{:}2806{:}1799 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 \\ 19{:}0{:}934{:}0 & 2638{:}1089{:}2965{:}1596 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 \\ 87{:}0{:}21{:}0 & 229{:}1959{:}2934{:}1008 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 \end{array}\right) \\ &\sim \left(\begin{array}{cc|cccc} 0{:}0{:}0{:}1 & 819{:}1118{:}1949{:}1280 & 1496{:}2942{:}2382{:}1854 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 \\ 0{:}0{:}0{:}0 & 3106{:}3042{:}1188{:}2065 & 1869{:}305{:}3050{:}1853 & 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 \\ 0{:}0{:}0{:}0 & 2153{:}636{:}1502{:}2899 & 2394{:}2614{:}1925{:}2873 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 \\ 0{:}0{:}0{:}0 & 3122{:}1359{:}2863{:}811 & 1699{:}944{:}867{:}2435 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 \end{array}\right) \\ &\sim \left(\begin{array}{cc|cccc} 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 & 2237{:}638{:}681{:}600 & 2174{:}2621{:}756{:}1894 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 \\ 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 & 591{:}2149{:}2982{:}10 & 2206{:}1228{:}1982{:}2394 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 \\ 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 2761{:}1067{:}48{:}2506 & 1772{:}1892{:}811{:}1818 & 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 \\ 0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 & 1846{:}2063{:}1907{:}2148 & 236{:}2635{:}1956{:}2423 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 \end{array}\right) \\ &= \left(\begin{array}{c|c} I_2 & F^\top \\ 0_2 & 0_{2\times 4} \end{array}\right). \end{aligned}$$

Thus, $G \cdot F = I_2$. Next, take $\mathbf{x} = (0{:}1{:}111{:}11, 125{:}0{:}0{:}0) \in \mathbf{R}^2$. The rank of the matrix $[\mathbf{x}]_B$ appears to be 2. It is not difficult to see that $\mathrm{rk}(\mathbf{x}) \le 2$ since the second coordinate is divisible by 5. Define matrices

$$\begin{aligned} X &= \begin{pmatrix} 0{:}1{:}111{:}11 & 125{:}0{:}0{:}0 \\ \tau(0{:}1{:}111{:}11) & \tau(125{:}0{:}0{:}0) \end{pmatrix} = \begin{pmatrix} 0{:}1{:}111{:}11 & 125{:}0{:}0{:}0 \\ 1661{:}3054{:}1013{:}1565 & 875{:}2250{:}3000{:}1125 \end{pmatrix} \in \mathbf{R}^{2\times 2}, \\ S &= \begin{pmatrix} 1{:}13{:}12{:}10 & 0{:}189{:}1294{:}0 \\ 0{:}1{:}0{:}2549 & 19{:}0{:}178{:}0 \end{pmatrix} \in \mathbf{R}^{2\times 2}, \\ T &= \begin{pmatrix} 1138 & 1209 & 363 & 2795 & 1683 & 1205 \\ 2949 & 2635 & 2331 & 680 & 2663 & 1598 \\ 532 & 1463 & 263 & 2996 & 1523 & 835 \\ 2350 & 271 & 1016 & 43 & 567 & 2755 \\ 2483 & 396 & 1817 & 3097 & 1976 & 2000 \\ 890 & 673 & 2213 & 448 & 419 & 3012 \end{pmatrix} \in \mathbf{S}^{6\times 6}. \end{aligned} \tag{4.15}$$

Next, find the inverse of $\mathbf{S}$ since it is required that S be invertible:

$$\begin{aligned} \left(S \,\middle|\, I_2 \right) &= \left(\begin{array}{cc|cc} 1{:}13{:}12{:}10 & 0{:}189{:}1294{:}0 & 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 \\ 0{:}1{:}0{:}2549 & 19{:}0{:}178{:}0 & 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 \end{array}\right) \\ &\sim \left(\begin{array}{cc|cc} 0{:}0{:}0{:}1 & 871{:}3058{:}409{:}1939 & 1077{:}1599{:}1085{:}1601 & 0{:}0{:}0{:}0 \\ 0{:}0{:}0{:}0 & 961{:}2041{:}1227{:}2631 & 352{:}2912{:}86{:}2142 & 0{:}0{:}0{:}1 \end{array}\right) \\ &\sim \left(\begin{array}{cc|cc} 0{:}0{:}0{:}1 & 0{:}0{:}0{:}0 & 3028{:}1288{:}10{:}2462 & 2247{:}1784{:}1515{:}603 \\ 0{:}0{:}0{:}0 & 0{:}0{:}0{:}1 & 1211{:}2298{:}1769{:}1333 & 33{:}1463{:}1474{:}1313 \end{array}\right) = \left(I_2 \,\middle|\, S^{-1} \right). \end{aligned}$$

Analogously, perform elementary row operations on an augmented matrix $(\, T \mid I_6 \,)$ over the ring $\mathbf{S}$ to yield $T^{-1} \in \mathbf{S}^{6\times 6}$:

$$\left(\begin{array}{cccccc|cccccc} 1138 & 1209 & 363 & 2795 & 1683 & 1205 & 1 & 0 & 0 & 0 & 0 & 0 \\ 2949 & 2635 & 2331 & 680 & 2663 & 1598 & 0 & 1 & 0 & 0 & 0 & 0 \\ 532 & 1463 & 263 & 2996 & 1523 & 835 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2350 & 271 & 1016 & 43 & 567 & 2755 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2483 & 396 & 1817 & 3097 & 1976 & 2000 & 0 & 0 & 0 & 0 & 1 & 0 \\ 890 & 673 & 2213 & 448 & 419 & 3012 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccccc|cccccc} 1 & 218 & 2826 & 840 & 2591 & 910 & 2952 & 0 & 0 & 0 & 0 & 0 \\ 0 & 378 & 2832 & 1645 & 2429 & 2383 & 802 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1112 & 3081 & 2991 & 1236 & 1090 & 1411 & 0 & 1 & 0 & 0 & 0 \\ 0 & 471 & 541 & 1043 & 2342 & 1755 & 300 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2852 & 484 & 1752 & 2898 & 1845 & 1434 & 0 & 0 & 0 & 1 & 0 \\ 0 & 403 & 2698 & 2848 & 679 & 2487 & 845 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\sim \left(\begin{array}{cccccc|cccccc} 1 & 0 & 2284 & 470 & 3042 & 412 & 340 & 1719 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1694 & 2840 & 643 & 461 & 184 & 2042 & 0 & 0 & 0 & 0 \\ 0 & 0 & 603 & 1161 & 1845 & 958 & 3053 & 1171 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2667 & 903 & 2614 & 249 & 1136 & 718 & 0 & 1 & 0 & 0 \\ 0 & 0 & 446 & 2072 & 312 & 2698 & 1666 & 1216 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1266 & 2078 & 925 & 1079 & 1693 & 2074 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 37 & 2257 & 2313 & 706 & 1756 & 1297 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2237 & 2083 & 1102 & 2765 & 2209 & 702 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2987 & 2615 & 411 & 1026 & 1282 & 767 & 0 & 0 & 0 \\ 0 & 0 & 0 & 199 & 284 & 987 & 2294 & 374 & 1286 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1120 & 2772 & 642 & 320 & 1319 & 1668 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1786 & 2835 & 2628 & 2777 & 937 & 853 & 0 & 0 & 1 \end{array}\right)$$

$$
\sim \left(\begin{array}{cccccc|cccccc}
1 & 0 & 0 & 0 & 3115 & 2632 & 3059 & 69 & 1529 & 3062 & 0 & 0 \\
0 & 1 & 0 & 0 & 241 & 2821 & 2543 & 2072 & 1384 & 1512 & 0 & 0 \\
0 & 0 & 1 & 0 & 1273 & 1755 & 2554 & 395 & 324 & 2262 & 0 & 0 \\
0 & 0 & 0 & 1 & 1666 & 2863 & 781 & 2326 & 1514 & 424 & 0 & 0 \\
0 & 0 & 0 & 0 & 2477 & 332 & 600 & 2449 & 2863 & 120 & 1 & 0 \\
0 & 0 & 0 & 0 & 2359 & 1810 & 1661 & 2951 & 3099 & 2111 & 0 & 1
\end{array}\right)
\sim \left(\begin{array}{cccccc|cccccc}
1 & 0 & 0 & 0 & 0 & 42 & 2934 & 1314 & 2594 & 1787 & 1630 & 0 \\
0 & 1 & 0 & 0 & 0 & 2115 & 1493 & 2380 & 2280 & 52 & 92 & 0 \\
0 & 0 & 1 & 0 & 0 & 1462 & 29 & 1594 & 687 & 2382 & 1251 & 0 \\
0 & 0 & 0 & 1 & 0 & 2482 & 356 & 1784 & 2210 & 964 & 2192 & 0 \\
0 & 0 & 0 & 0 & 1 & 366 & 925 & 1062 & 1669 & 810 & 1413 & 0 \\
0 & 0 & 0 & 0 & 0 & 916 & 836 & 818 & 303 & 696 & 1108 & 1
\end{array}\right)
$$

$$
\sim \left(\begin{array}{cccccc|cccccc}
1 & 0 & 0 & 0 & 0 & 0 & 2227 & 2723 & 308 & 2260 & 1934 & 2313 \\
0 & 1 & 0 & 0 & 0 & 0 & 1828 & 1235 & 110 & 3112 & 222 & 2860 \\
0 & 0 & 1 & 0 & 0 & 0 & 2502 & 343 & 1916 & 1585 & 970 & 1943 \\
0 & 0 & 0 & 1 & 0 & 0 & 1284 & 823 & 154 & 47 & 2151 & 973 \\
0 & 0 & 0 & 0 & 1 & 0 & 1014 & 394 & 1391 & 914 & 1830 & 2299 \\
0 & 0 & 0 & 0 & 0 & 1 & 2621 & 2273 & 2733 & 956 & 588 & 1061
\end{array}\right)
= \Big(I_6 \quad \Big| \quad T^{-1}\Big).
$$

Finally, the public and the private matrix can be determined

$$
\begin{aligned}
G_{\text{pub}} = S \cdot \Big(X \quad G\Big) \cdot T &= \begin{pmatrix}
2537{:}106{:}906{:}213 & 2683{:}2453{:}2340{:}2018 \\
872{:}1963{:}1177{:}2439 & 924{:}1871{:}1075{:}1537 \\
708{:}459{:}3096{:}2135 & 656{:}397{:}2388{:}2676 \\
2617{:}200{:}1915{:}2323 & 101{:}1941{:}1296{:}2110 \\
52{:}1103{:}336{:}2350 & 2851{:}2615{:}427{:}1975 \\
2047{:}3106{:}2745{:}2649 & 2337{:}2739{:}2250{:}641
\end{pmatrix}^{\top}, \\
G_{\text{priv}} = \qquad F \cdot S^{-1} \qquad &= \begin{pmatrix}
2918{:}2474{:}2460{:}1810 & 256{:}428{:}2711{:}1876 \\
3057{:}1079{:}1808{:}2431 & 2135{:}2694{:}200{:}1519 \\
0{:}0{:}0{:}0 & 0{:}0{:}0{:}0 \\
0{:}0{:}0{:}0 & 0{:}0{:}0{:}0
\end{pmatrix}.
\end{aligned} \tag{4.16}
$$

We have successfully generated the public key $\mathcal{K}_{\text{pub}} = (G_{\text{pub}}, \frac{1}{5})$ and the private key $\mathcal{K}_{\text{priv}} = (\mathbf{g}, G_{\text{priv}}, T^{-1}, t)$.

Encryption: Let $\mathbf{z} = \left(\begin{smallmatrix} 419{:}678{:}3114{:}2871 \\ 747{:}2453{:}901{:}2223 \end{smallmatrix}\right)^{\top} \in \mathbf{R}^2$ be a message. We must choose an codeword from $\mathbf{R}^6$ and verify that it has cardinal rank at most $\frac{1}{5}$

$$
\mathbf{e} = \begin{pmatrix}
2500{:}1875{:}2500{:}1250 \\
1875{:}625{:}1875{:}2500 \\
0{:}0{:}0{:}0 \\
2500{:}1875{:}2500{:}1250 \\
0{:}0{:}0{:}0 \\
1250{:}2500{:}1250{:}625
\end{pmatrix}^{\top}
$$

$$
[\mathbf{e}]_B = \begin{pmatrix}
1250 & 2500 & 0 & 1250 & 0 & 625 \\
2500 & 1875 & 0 & 2500 & 0 & 1250 \\
1875 & 625 & 0 & 1875 & 0 & 2500 \\
2500 & 1875 & 0 & 2500 & 0 & 1250
\end{pmatrix} = \begin{pmatrix}
625 & 1250 & 0 & 625 & 0 & 1875 \\
2500 & 1875 & 0 & 2500 & 0 & 1250 \\
1875 & 625 & 0 & 1875 & 0 & 2500 \\
2500 & 1875 & 0 & 2500 & 0 & 1250
\end{pmatrix} = \begin{pmatrix}
625 & 1250 & 0 & 625 & 0 & 1875 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix},
$$

where the first row of $[\mathbf{e}]_B$ is multiplied by an integer 1563. Then, the first row multiplied by 3121, 3122 and 3121 is added to the second, third, and fourth rows in the specified order. Refer to **Claim 48** to calculate the cardinal rank of the error codeword $\operatorname{rk}(\mathbf{e}) = \operatorname{rk}([\mathbf{e}]_B) = \operatorname{rk}([\mathbf{e}]_B^{\top}) = \log_{5^5}(|\operatorname{Im}[\mathbf{e}]_B^{\top}|) = \log_{5^5}(5) = \frac{1}{5}$. Thus, $\mathbf{e}$ is correctable. Let $\mathbf{c} = \operatorname{Enc}_{\mathcal{K}_{\text{pub}}}(\mathbf{z})$ be obscured by $\mathbf{e}$, i.e.

$$
\begin{aligned}
\mathbf{c} &= \left(\begin{pmatrix}
2537{:}106{:}906{:}213 & 2683{:}2453{:}2340{:}2018 \\
872{:}1963{:}1177{:}2439 & 924{:}1871{:}1075{:}1537 \\
708{:}459{:}3096{:}2135 & 656{:}397{:}2388{:}2676 \\
2617{:}200{:}1915{:}2323 & 101{:}1941{:}1296{:}2110 \\
52{:}1103{:}336{:}2350 & 2851{:}2615{:}427{:}1975 \\
2047{:}3106{:}2745{:}2649 & 2337{:}2739{:}2250{:}641
\end{pmatrix} \left(\begin{smallmatrix} 419{:}678{:}3114{:}2871 \\ 747{:}2453{:}901{:}2223 \end{smallmatrix}\right) + \begin{pmatrix}
2500{:}1875{:}2500{:}1250 \\
1875{:}625{:}1875{:}2500 \\
0{:}0{:}0{:}0 \\
2500{:}1875{:}2500{:}1250 \\
0{:}0{:}0{:}0 \\
1250{:}2500{:}1250{:}625
\end{pmatrix}\right)^{\top} \\
&= \begin{pmatrix}
1686{:}751{:}2752{:}1989 \\
1636{:}749{:}708{:}1012 \\
2280{:}2090{:}2736{:}1334 \\
1266{:}2671{:}383{:}2272 \\
2136{:}12{:}2061{:}636 \\
115{:}247{:}2771{:}147
\end{pmatrix}^{\top}.
\end{aligned}
$$

The ciphertext $\mathbf{c}$ in now ready to be transmitted to the recipient whose public key was utilised in the encryption.

Decryption: Denote by I the set of indices $\{3, \dots, 6\}$. Then,

$$
\begin{aligned}
\mathbf{d} = \mathbf{c} \cdot T^{-1} &= \begin{pmatrix}
1686{:}751{:}2752{:}1989 \\
1636{:}749{:}708{:}1012 \\
2280{:}2090{:}2736{:}1334 \\
1266{:}2671{:}383{:}2272 \\
2136{:}12{:}2061{:}636 \\
115{:}247{:}2771{:}147
\end{pmatrix}^{\top} \cdot \begin{pmatrix}
2227 & 2723 & 308 & 2260 & 1934 & 2313 \\
1828 & 1235 & 110 & 3112 & 222 & 2860 \\
2502 & 343 & 1916 & 1585 & 970 & 1943 \\
1284 & 823 & 154 & 47 & 2151 & 973 \\
1014 & 394 & 1391 & 914 & 1830 & 2299 \\
2621 & 2273 & 2733 & 956 & 588 & 1061
\end{pmatrix} \\
&= \begin{pmatrix}
2128{:}573{:}317{:}2046 \\
875{:}1250{:}1000{:}3000 \\
1288{:}2465{:}1023{:}566 \\
2763{:}953{:}832{:}3119 \\
807{:}2279{:}2025{:}2758 \\
1340{:}486{:}983{:}1
\end{pmatrix}^{\top},
\end{aligned}
$$

$$
\mathbf{d}_I = \big(1288{:}2465{:}1023{:}566, 2763{:}953{:}832{:}3119, 807{:}2279{:}2025{:}2758, 1340{:}486{:}983{:}1\big).
$$

Note that $\mathbf{d}_I$ corresponds to $\mathbf{y}$ in *Example* 16, so **Algorithm 9** executed on input $(4, 2, \mathbf{g}, \mathbf{d}_I)$ outputs $\mathbf{y} = \begin{pmatrix} \text{1913:590:1648:2441} \\ \text{2138:2810:207:1244} \\ \text{2682:2904:775:2133} \\ \text{715:2361:358:1251} \end{pmatrix}^\top$. It remains to multiply the decoded codeword $\mathbf{y}$ by the matrix G_{priv} from the left

$$\begin{aligned} \mathbf{z}' = \mathbf{y} \cdot G_{\text{priv}} &= \begin{pmatrix} \text{1913:590:1648:2441} \\ \text{2138:2810:207:1244} \\ \text{2682:2904:775:2133} \\ \text{715:2361:358:1251} \end{pmatrix}^\top \cdot \begin{pmatrix} \text{2918:2474:2460:1810} & \text{256:428:2711:1876} \\ \text{3057:1079:1808:2431} & \text{2135:2694:200:1519} \\ \text{0:0:0:0} & \text{0:0:0:0} \\ \text{0:0:0:0} & \text{0:0:0:0} \end{pmatrix} \\ &= \big(\text{419:678:3114:2871}, \text{747:2453:901:2223}\big), \end{aligned}$$

which, clearly, equals the original message $\mathbf{z}$.

Conclusion

The thesis objective is to describe error-correcting codes over Galois rings instead of finite fields as a potential strengthening of code-based cryptography. The main focus is on the class of codes utilising the cardinal rank metric, which is a natural generalisation of the rank metric introduced by Gabidulin. Throughout the work, the constructive rather than the existential approach is chosen. The immediate benefit is the possibility to formulate algorithms. **Algorithms 4** to **8** are our own contribution; the rest is slightly modified to use the cardinal rank metric. Essential notions are even illustrated in examples, none of which is borrowed.

Chapter One establishes the construction of Galois rings and studies their fundamental properties. This is necessary to comprehend the concept of codes and their distinctions from the standard code theory. The subsequent chapter introduces modules over Galois rings and explains the decomposition into powers of p. Our additions here are namely **Theorem 24**, **Claim 26**, **Lemma 28**, **Theorem 37**, **Claim 40** and **Claim 44**.

The central point of the third chapter is to characterise the cardinal rank together with its induced metric and demonstrate them. A connection between the cardinal rank metric over the Galois ring and the rank metric over its residue field is presented, which clarifies the relation between MCRD and MRD codes. The significance lies in **Corollary 49** providing formula for the cardinal rank metric, **Theorem 54** with **Claim 55** is advantageous for proving the generalised version of Singleton bound (**Theorem 57**), and necessary conditions for codes to be MCRD are asserted in **Theorem 61** and **Corollary 62**.

The final chapter discusses Gabidulin codes as representants of MCRD codes, grounded on matrices and linear polynomials. Linear polynomials are examined thoroughly as the efficient decoding algorithm is based on them. The version of the GPT cryptosystem over Galois rings is a direct cryptographic application of Gabidulin codes. In this part, we contribute with the proof of **Theorem 63**, **Theorem 70**, **Theorem 72**, **Claim 75** and **Lemma 81**.

Bibliography

[1] R. J. McEliece. A Public-Key Cryptosystem Based on Algebraic Coding Theory. *JPL DSN Progress Report*, 42-44:114–116, 1978.

[2] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a Non--Commutative Ring and their Application in Cryptology. In D. W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, pages 482–489, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[3] R. Overbeck. Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes. *Journal of cryptology*, 21(2):280–301, 2008.

[4] H. Rashwan, E. M. Gabidulin, and B. Honary. A Smart Approach for GPT Cryptosystem Based on Rank Codes. *2010 IEEE International Symposium on Information Theory*, page 5, 2010.

[5] H. T. Kalachi. On the failure of the smart approach of the GPT cryptosystem. *Cryptologia*, 46(2):167–182, 2022.

[6] M. Epelde and I. F. Rúa. Cardinal rank metric codes over Galois rings. *Finite Fields and Their Applications*, 77, 2022.

[7] G. Bini and F. Flamini. *Finite Commutative Rings and Their Applications.* The Springer International Series in Engineering and Computer Science 680. Springer US, 1 edition, 2002.

[8] L. C. Grove. *Algebra.* Academic Press, New York, 1st edition, 1983.

[9] Z.-X. Wan. *Lectures on Finite Fields and Galois Rings.* World Scientific, Singapore, 1 edition, 2003.

[10] A. Drápal. Commutative rings. `https://www.karlin.mff.cuni.cz/~zemlicka/11-12/komalg.pdf`, 2006. Accessed: 2024-02-23.

[11] S. T. Dougherty, J. l. Kim, and H. Kulosman. MDS codes over finite principal ideal rings. *Designs, codes, and cryptography*, 50(1):77–92, 2008.

[12] E. M. Gabidulin. Theory of Codes with Maximum Rank Distance. *Problems of Information Transmission*, 21(1):12, 1985.

[13] C. H. Tan, T. F. Prabowo, and T. S. Chien Lau. Rank Metric Code-based Signature. *2018 International Symposium on Information Theory and Its Applications (ISITA), Information Theory and Its Applications (ISITA), 2018 International Symposium on*, pages 70–74, 2018.

[14] M. Marko. Cryptosystems based on codes with rank metrics. Bachelor thesis, Charles University, Faculty of Mathematics and Physics, Department of Algebra, Prague, 2021.

[15] A. A. Bruen, M. A. Forcinito, and J. M. McQuillan. *Cryptography, Information Theory, and Error-Correction.* John Wiley & Sons, Incorporated, Newark, 2 edition, 2021.

[16] H. T. Kamche and Ch. Mouaha. Rank-Metric Codes Over Finite Principal Ideal Rings and Applications. *IEEE transactions on information theory*, 65(12):7718–7735, 2019.

List of Algorithms

List of Abbreviations

EEA Extended Euclidean Algorithm providing the greatest common divisor and the coefficients of Bezout's identity

MDS Maximum Distance Separable, in terms of codes over finite fields, codes that achieve the equality in Singleton bound for the Hamming distance

MRD Maximum Rank Distance, in terms of codes over finite fields, codes that achieve the equality in Singleton bound for the rank distance

MCRD Maximum Cardinal Rank Distance, in terms of codes over Galois rings, codes that achieve the equality in Singleton-like bound for the cardinal rank distance

PKC Public Key Cryptosystem

WLOG Without Loss Of Generality

Notation

$\mathrm{GR}(p^n, r)$ Galois ring of characteristic p^n and cardinality p^{nr}

$\mathcal{T}_r$ Teichmüller set $\{0, 1, \xi, \xi^2, \dots, \xi^{p^r-1}\} \subseteq \mathrm{GR}(p^n, r)$, where ξ has order $p^r - 1$

$\mathcal{T}$ Teichmüller set $\mathcal{T}_1$

$a_{r-1}{:}a_{r-2}{:}\dots{:}a_0$ The additive representation of an element $\sum\limits_{i=0}^{r-1} a_i \xi^i$, where ξ has order $p^r - 1$

$[i]$ The i^{th} power of a prime p modulo p^r

τ The generalised Frobenius automorphism of $\mathrm{GR}(p^n, r)$ defined using the aditive representation as $\tau\left(\sum\limits_{i=0}^{r-1} z_i \xi^i\right) = \sum\limits_{i=0}^{r-1} z_i \xi^{i[1]}$, where ξ has order $p^r - 1$

Modules

Let $\mathbf{R} = \mathrm{GR}(p^n, r)$, $\mathbf{S} = \mathrm{GR}(p^n, 1)$ and M, N be $\mathbf{R}$-modules.

$M \leq N$ M is a submodule of N

$M_{\mathbf{S}}$ The module M viewed as an $\mathbf{S}$-module

$\langle \mathbf{x}_1, \dots, \mathbf{x}_k \rangle_{\mathbf{R}}$ The $\mathbf{R}$-module generated by $\mathbf{x}_1, \dots, \mathbf{x}_k$; $\mathbf{R}$ can be omitted

$\mathrm{rank}(M)$ The rank of a module M, the minimal number of M's generators

$\mathrm{Soc}(M)$ The submodule of a module M composed of elements with height ≤ 1

δ_{ij} The Kronecker delta; $\delta_{ii} = 1$ and $\delta_{ij} = 0$ provided $i \neq j$

$\boldsymbol{\delta}_i$ The element $(\delta_{i1}, \dots, \delta_{ik})$ of an $\mathbf{R}$-module $\mathbf{R}^k$

$\mathbf{x}_I$ The codewords composed of coordinates of $\mathbf{x} \in \mathbf{R}^m$ which indices lies in the set $I \subseteq \{1, \dots, m\}$

$\overline{}$ The projection $\mathbf{R} \to {}^{\mathbf{R}}\!/_{p\mathbf{R}}$ defined by $a \mapsto a + p\mathbf{R}$; a ring epimorphism

$\overline{}^m$ The induced projection $\mathbf{R}^m \to \left({}^{\mathbf{R}}\!/_{p\mathbf{R}}\right)^m$; $\overline{(a_1, \dots, a_m)}^m = (\overline{a_1}, \dots, \overline{a_m})$; a module epimorphism

Matrices

Let A be a matrix over $\mathbf{R} = \mathrm{GR}(p^n, r)$ of type $k \times l$, $\mathbf{S} = \mathrm{GR}(p^n, 1)$ be a subring of $\mathbf{R}$ and $B = (\beta_1, \dots, \beta_r)$ be a free basis of $\mathbf{R}$ over $\mathbf{S}$.

$\mathbf{A}_i^c$ The i^{th} column of A

$\mathbf{A}_i^r$ The i^{th} column of A

a_{ij} The entry of a matrix A at position (i, j)

$A_{I\cdot}$ The matrix composed of the rows $\mathbf{A}_i^r$, $i \in I \subseteq \{1, \dots, k\}$

$A_{\cdot I}$ The matrix composed of the columns $\mathbf{A}_i^c$, $i \in I \subseteq \{1, \dots, l\}$

I_k The identity matrix of order k

$0_{k \times l}$ The zero matrix of type $k \times l$

0_k The zero matrix $0_{k \times k}$

$\mathrm{Im}_{\mathbf{S}}(A)$ The image of A; the $\mathbf{S}$-module generated by the columns $\mathbf{A}_1^c, \dots, \mathbf{A}_l^c$, where $\mathbf{S}$ is a subring of $\mathbf{R}$ and can be omitted

$\ker(A)$ The kernel of A; the set of $\mathbf{x} \in \mathbf{R}^l$ such that $A \cdot \mathbf{x}^\top = \mathbf{o}$

$\mathrm{rank}(A)$ The rank of $\mathrm{Im}(A)$

$\mathrm{rk}(A)$ The cardinal rank of A defined as $\log_{p^n}(|\mathrm{Im}(A)|)$

$[x]_B$ A coordinate vector $(z_1, \dots, z_r) \in \mathbf{S}^r$ of $x \in \mathbf{R}$ relative to the free basis B such that $x = z_1\beta_1 + \dots + z_r\beta_r$

$[\mathbf{x}]_B$ A coordinate matrix $([x_1]_B \mid \dots \mid [x_k]_B) \in \mathbf{S}^{r \times k}$ of $\mathbf{x} = (x_1, \dots, x_k) \in \mathbf{R}^k$

$\mathrm{rk}_{\mathbf{S}}(\mathbf{x})$ The cardinal rank of $\mathbf{x} \in \mathbf{R}^k$ defined as $\mathrm{rk}([\mathbf{x}]_B)$; $\mathbf{S}$ can be omitted

Linear codes

Let $\mathcal{C}$ be a linear code of length m over $\mathbf{R}$ and $\mathbf{c}, \mathbf{d} \in \mathcal{C}$.

$[m, l]_{\mathbf{R}}$**-code** A linear code of length m and rank l over $\mathbf{R}$; $\mathbf{R}$ can be omitted

$\mathrm{w}_{\mathcal{H}}(\mathbf{c})$ The Hamming weight of $\mathbf{c}$; the number of non-zero coordinates of $\mathbf{c}$

$\mathrm{d}_{\mathcal{H}}(\mathbf{c}, \mathbf{d})$ The Hamming distance between $\mathbf{c}$ and $\mathbf{d}$ defined as $\mathrm{w}_{\mathcal{H}}(\mathbf{c} - \mathbf{d})$

$\mathrm{d}_{\mathcal{H}}(\mathcal{C})$ The minimum Hamming distance of $\mathcal{C}$; $\min\{\mathrm{d}_{\mathcal{H}}(\mathbf{e}, \mathbf{f}) \mid \mathbf{e}, \mathbf{f} \in \mathcal{C} : \mathbf{e} \neq \mathbf{f}\}$

$\mathrm{d}_{\mathcal{R}}(\mathbf{c}, \mathbf{d})$ The cardinal rank distance between $\mathbf{c}$ and $\mathbf{d}$ defined as $\mathrm{rk}(\mathbf{c} - \mathbf{d})$

$\mathrm{d}_{\mathcal{R}}(\mathcal{C})$ The minimum cardinal rank distance of $\mathcal{C}$; $\min\{\mathrm{d}_{\mathcal{R}}(\mathbf{e}, \mathbf{f}) \mid \mathbf{e}, \mathbf{f} \in \mathcal{C} : \mathbf{e} \neq \mathbf{f}\}$

$\mathrm{d}_{\mathbf{S}}(\mathbf{c}, \mathbf{d})$ The cardinal rank distance between $\mathbf{c}$ and $\mathbf{d}$ over $\mathbf{S}$

$\mathrm{d}_{\mathbf{S}}(\mathcal{C})$ The minimum cardinal rank distance of $\mathcal{C}$ over $\mathbf{S}$

$\mathrm{Gab}_{\mathbf{R}}(m, l, \mathbf{g})$ The Gabidulin $[m, l]_{\mathbf{R}}$-code with a generator matrix $G \in \mathbf{R}^{m \times l}$ such that $g_{ij} = \tau^{i-1}(g_j)$, $i = 1, \ldots, l, j = 1, \ldots, m$, provided $\mathrm{rk}(\mathbf{g}) = m$

Linearised polynomials

$\mathcal{P}(\mathbf{R})$ The set of all linearised polynomials $\sum\limits_{i=0}^{d} a_i \cdot \tau^i(X)$ with coefficients from $\mathbf{R}$

$\deg(F)$ The degree of a linearised polynomial $F \in \mathcal{P}(\mathbf{R})$ defined as the minimal non-negative integer d for $F \neq 0$ such that $F = \sum\limits_{i=0}^{d} f_i \cdot \tau^i(X)$ and $f_d \neq 0$, and $-\infty$ for $F = 0$

$\mathcal{P}_d(\mathbf{R})$ The set of $F \in \mathcal{P}(\mathbf{R})$ such that $\deg(F) < d$

$\mathcal{P}_d^*(\mathbf{R})$ The set of $F \in \mathcal{P}(\mathbf{R})$ such that $\deg(F) = d - 1$ and $f_{d-1} = 1$

ε The linearised polynomial $\varepsilon(X) = X$; the identity of $\mathcal{P}(\mathbf{R})$

$F \circ G$ The product of $F, G \in \mathcal{P}(\mathbf{R})$ defined as the evaluation $F(G(X))$

$\ker(F)$ The kernel of $F \in \mathcal{P}(\mathbf{R})$; the set of all its roots over $\mathbf{R}$

$F(\mathbf{x})$ The codeword $(F(x_1), \ldots, F(x_k))$, where $F \in \mathcal{P}(\mathbf{R})$ and $\mathbf{x} \in \mathbf{R}^k$