mathematics

MDPI

Article

Multiplicative Structure and Hecke Rings of Generator Matrices for Codes over Quotient Rings of Euclidean Domains

Hajime Matsui

Toyota Technological Institute, 2–12–1 Hisakata, Tempaku, Nagoya, Aichi 468–8511, Japan; matsui@toyota-ti.ac.jp

Received: 30 June 2017; Accepted: 8 December 2017; Published: 15 December 2017

Abstract: In this study, we consider codes over Euclidean domains modulo their ideals. In the first half of the study, we deal with arbitrary Euclidean domains. We show that the product of generator matrices of codes over the rings mod a and mod b produces generator matrices of all codes over the ring mod ab, i.e., this correspondence is onto. Moreover, we show that if a and b are coprime, then this correspondence is one-to-one, i.e., there exist unique codes over the rings mod a and mod b that produce any given code over the ring mod ab through the product of their generator matrices. In the second half of the study, we focus on the typical Euclidean domains such as the rational integer ring, one-variable polynomial rings, rings of Gaussian and Eisenstein integers, p-adic integer rings and rings of one-variable formal power series. We define the reduced generator matrices of codes over Euclidean domains modulo their ideals and show their uniqueness. Finally, we apply our theory of reduced generator matrices to the Hecke rings of matrices over these Euclidean domains.

Keywords: error-correcting codes; quasi-cyclic codes; Euclidean division; Hermite normal form; Hecke algebras

1. Introduction

The structural properties of quasi-cyclic (QC) [1,2] and generalized quasi-cyclic (GQC) codes [3–5] have been reported. On the other hand, cyclic codes can be extended to pseudo-cyclic (PC) and generalized pseudo-cyclic (GPC) codes [6]. Similar constructions for the rational integer ring $\mathbb{Z}$ are known as integer codes and generalized integer codes [7]. We can summarize the module structure of these codes as follows:

$$\begin{aligned}
&\text{Cyclic codes: ideals in } \mathbb{F}_q[x]/\langle x^n-1\rangle\\
&\text{QC codes: submodules in } \textstyle\bigoplus_{i=1}^{l}\mathbb{F}_q[x]/\langle x^n-1\rangle\\
&\text{GQC codes: submodules in } \textstyle\bigoplus_{i=1}^{l}\mathbb{F}_q[x]/\langle x^{n_i}-1\rangle\\
&\text{PC codes: ideals in } \mathbb{F}_q[x]/\langle d\,\rangle\\
&\text{GPC codes: submodules in } \textstyle\bigoplus_{i=1}^{l}\mathbb{F}_q[x]/\langle d_i\rangle\\
&\text{Integer codes: submodules in } \textstyle\bigoplus_{i=1}^{l}\mathbb{Z}/d\mathbb{Z}\\
&\text{Generalized integer codes: submodules in } \textstyle\bigoplus_{i=1}^{l}\mathbb{Z}/d_i\mathbb{Z},
\end{aligned}$$

where $\mathbb{F}_q[x]$ is a one-variable polynomial ring over a q-element finite field $\mathbb{F}_q$ with a prime power q, $\langle f\rangle$ is the ideal of $\mathbb{F}_q[x]$ generated by $f\in\mathbb{F}_q[x]$, $\mathbb{F}_q[x]/\langle f\rangle$ is their quotient ring, $\bigoplus_{i=1}^{l}$ denotes the direct sum of the $\mathbb{F}_q[x]$- or $\mathbb{Z}$-modules and $\mathbb{Z}/d_i\mathbb{Z}$ is the integer residue ring modulo $d_i\in\mathbb{Z}$. Note that both

$\mathbb{F}_q[x]$ and $\mathbb{Z}$ are Euclidean domains [8,9]; we say that a commutative integral domain R is a Euclidean domain if there exists a function $\psi : R \setminus \{0\} \to \mathbb{N}_0$ such that, for any $a, b \in R$ with $b \neq 0$, $a = sb + r$ and $r = 0$ or $\psi(r) < \psi(b)$ are valid for some $s, r \in R$, where $\mathbb{N}_0$ denotes the set of non-negative integers. Finding s, r with $a = sb + r$ and $r = 0$ or $\psi(r) < \psi(b)$ is called Euclidean division, and s, r are called a quotient and a remainder of a by b, respectively. If $R = \mathbb{F}_q[x]$, then $\psi(\cdot) = \deg(\cdot)$ is the degree function, and if $R = \mathbb{Z}$, then $\psi(\cdot) = |\cdot|$ is the absolute value. However, no theory has yet been reported concerning the unified treatment of codes over the quotient rings of the general Euclidean domains.

In this study, we deal with the above codes uniformly, which can be constructed by any Euclidean domain R. Let $M_l(R)$ be the ring of l-by-l matrices with entries in R. We denote:

$$\mathbb{L} = R^l = \{(c_1\ c_2\ \ldots\ c_l) \mid c_1, c_2, \ldots, c_l \in R\},$$
$$\mathcal{M} = \mathbb{L}/\mathbb{L}\mathrm{diag}\,[d_1, \ldots, d_l]\,,$$

where $\mathrm{diag}\,[d_1, \ldots, d_l] \in M_l(R)$ denotes the diagonal matrix whose i-th entry is d_i for all $1 \leq i \leq l$; for $X \in M_l(R)$, $\mathbb{L}X$ denotes the R-module consisting of cX for all $c \in \mathbb{L}$; and for two R-modules $\mathbb{S} \supset \mathbb{T}$, $\mathbb{S}/\mathbb{T}$ denotes their quotient R-module. We investigate R-submodules of $\mathcal{M}$, and we denote one of them by $\mathcal{C}$. If $R = \mathbb{F}_q[x]$, then R-submodules are equivalent to the GPC codes, and if $R = \mathbb{Z}$, then R-submodules are equivalent to the generalized integer codes.

To indicate the R-modules explicitly, let us define their generator matrices. Let $F : \mathbb{L} \to \mathcal{M}$ be a natural surjective map of the R-modules and $F^{-1}(\mathcal{C})$ be the inverse image of an R-submodule $\mathcal{C} \subset \mathcal{M}$. If $G \in M_l(R)$ satisfies $F^{-1}(\mathcal{C}) = \mathbb{L}G$, then we say that G is a generator matrix of $\mathcal{C}$. For an arbitrary given $G \in M_l(R)$, there exists an R-module $\mathcal{C} \subset \mathcal{M}$ such that G is its generator matrix if and only if $\mathbb{L}G \supset \mathbb{L}\mathrm{diag}\,[d_1, \ldots, d_l]$, and this condition is equivalent to:

$$AG = \mathrm{diag}\,[d_1, \ldots, d_l]$$

for some $A \in M_l(R)$. Then, we have $\mathcal{C} = \mathbb{L}G/\mathbb{L}\mathrm{diag}\,[d_1, \ldots, d_l]$.

Under the above preparation, if $d_1 = \cdots = d_l$, then we can reveal the multiplicative structure of generator matrices of R-submodules in the following manner. Hereafter, we set $u = d_1 = \cdots = d_l$. Let $I \in M_l(R)$ be the identity matrix. In this case, we have $\mathrm{diag}\,[d_1, \ldots, d_l] = uI$ and:

$$\mathcal{C} = \mathbb{L}G/u\mathbb{L} \subset \mathcal{M} = \mathbb{L}/u\mathbb{L}.$$

For two R-modules $\mathcal{C}_1 = \mathbb{L}G_1/u_1\mathbb{L}$ and $\mathcal{C}_2 = \mathbb{L}G_2/u_2\mathbb{L}$, if $A_1G_1 = u_1I$ and $A_2G_2 = u_2I$, we have $A_2A_1G_1G_2 = u_1u_2I$. If we set $G = G_1G_2$ and $u = u_1u_2$, then $\mathcal{C} = \mathbb{L}G/u\mathbb{L}$ determines an R-module in $\mathcal{M} = \mathbb{L}/u\mathbb{L}$. Our results can be divided into two parts. The first result asserts that this correspondence $(\mathcal{C}_1, \mathcal{C}_2) \mapsto \mathcal{C}$ by the multiplication of generator matrices is surjective, i.e., all R-modules in $\mathcal{M} = \mathbb{L}/u\mathbb{L}$ can be obtained by this correspondence. The second result asserts that, if $\gcd(u_1, u_2) = 1$, then this correspondence is injective, i.e., $\mathcal{C}_1$ and $\mathcal{C}_2$ are both uniquely determined for each $\mathcal{C}$. The latter assertion corresponds to the explicit version of Chinese remainder theorem in our theory of R-submodules. Because we can express its composition and decomposition through the multiplication of generator matrices effectively, our results can be applied to the fast enumeration of the generator matrices of efficient R-modules in $\mathcal{M}$. The above results we obtain here are valid for the codes over the quotient rings of arbitrary Euclidean domains.

In general, the result of the Euclidean division is not unique; for $a, b \in R$ with $b \neq 0$, the quotient s and the remainder r are not always unique in $a = sb + r$ and $r = 0$ or $\psi(r) < \psi(b)$. For example, if $R = \mathbb{F}_q[x]$, the result is unique, but if $R = \mathbb{Z}$, $1 = 1 \cdot 2 - 1 = 0 \cdot 2 + 1$. One way to impose the uniqueness for the result of the Euclidean division in $R = \mathbb{Z}$ is to indicate $s = \lfloor a/b \rfloor$, where, for a real number x, $\lfloor x \rfloor$ denotes a unique $n \in \mathbb{Z}$ such that $n \leq x < n + 1$. It is shown that, if $a = sb + r$, then $s = \lfloor a/b \rfloor$ is equivalent to $\lfloor r/b \rfloor = 0$, and $r = 0$ or $\psi(r) < \psi(b)$ follows from $\lfloor r/b \rfloor = 0$. In this study, for the other cases of Euclidean domains R such as the ring of Gaussian integers $\mathbb{Z}[i]$,

the ring of Eisenstein integers $\mathbb{Z}[\omega]$, the p-adic integer ring $\mathbb{Z}_p$ and the ring of the formal power series $\mathbb{F}_q[[x]]$, namely,

$$R = \mathbb{Z},\ \mathbb{F}_q[x],\ \mathbb{Z}[i],\ \mathbb{Z}[\omega],\ \mathbb{Z}_p,\ \mathbb{F}_q[[x]],$$

where $i = \sqrt{-1}$, $\omega = (-1 + \sqrt{-3})/2$ and p denotes a rational prime, we determine a unique pair of the quotient and remainder similar to $s = \lfloor a/b \rfloor$ and $\lfloor r/b \rfloor = 0$ of $R = \mathbb{Z}$. We apply this uniqueness to show the uniqueness of the Euclidean division by a class of matrices over R.

Let $GL_l(R)$ be the group of invertible matrices in $M_l(R)$. Then, for two generator matrices $G, G' \in M_l(R)$ of an R-module $\mathcal{C} \subset \mathcal{M}$, there exists $E \in GL_l(R)$ such that $G' = EG$. Among these EG's, we can algorithmically find a simple form of G, which is called the reduced generator matrix, which generalizes the Hermite normal form [10,11] of $R = \mathbb{Z}$. Then, we apply the uniqueness of the Euclidean divisions to show that there exists a unique reduced generator matrix for each R-module in $\mathcal{M}$. This standard expression of the generator matrix is useful for enumerating and searching for efficient R-modules in $\mathcal{M}$.

Furthermore, we apply our theory of generator matrices to Hecke rings of matrices over the prescribed Euclidean domains. Hecke rings or Hecke algebras we consider here are the rings of the formal finite sums $\sum_{\alpha\in\Delta} c_\alpha \Gamma\alpha\Gamma$ of the double cosets $\Gamma\alpha\Gamma$ with $c_\alpha \in \mathbb{Z}$, where $\Delta = \{\alpha \in M_l(R) \mid \det(\alpha) \neq 0\}$, $\det(\alpha)$ denotes the matrix determinant, and $\Gamma = GL_l(R)$. Hecke rings are commonly used as Hecke operators to the number theory, especially, the theory of modular forms [12,13]. In this study, we show that the generator matrices of R-modules in $\mathcal{M}$ are deeply concerned with the theory of Hecke rings. We describe in terms of the generator matrices the definition of Hecke rings, the homomorphism "ind$(\cdot)$", the prime decompositions and a generating function of ind$(\cdot)$. Although these results on Hecke rings are not new (cf. [13]), the argument in this study shows that the concept of reduced generator matrices simplifies the theory of Hecke rings and makes it computable.

The rest of this paper is organized as follows. Section 2 gives the basic definitions and the one-to-one correspondence between R-modules in $\mathcal{M}$ and certain R-modules in $\mathbb{L}$. Section 3 gives a division algorithm, which is similar to the Euclidean division in R, for a class of matrices with a pair of quotient and remainder matrices. Section 4 defines generator matrices of R-modules in $\mathcal{M}$ and shows their existence constructively. Section 5 shows the multiplicative structure among the generator matrices in the case of $d_1 = \cdots = d_l$. Section 6 treats the cases where Euclidean divisions have a uniqueness property, which can deduce the uniqueness of the reduced generator matrix. Finally, Section 7 applies our theory of generator matrices to Hecke rings and shows a generating function which is useful for counting the reduced generator matrices with a fixed determinant. Section 8 concludes the study.

2. R-Modules in $\mathcal{M}$

Throughout this section, R is used to denote any commutative ring. The purposes of this section are to define R-modules in $\mathcal{M}$ and to show a one-to-one correspondence between R-modules in $\mathcal{M}$ and a class of lattices.

Let $l \in \mathbb{Z}$ be positive and $d_1, d_2, \ldots, d_l \in R$. Consider the quotient ring $R/\langle d_i \rangle$ for $1 \leq i \leq l$. For any $c \in R$, we denote the corresponding element in $R/\langle d_i \rangle$ by $c \bmod d_i \in R/\langle d_i \rangle$. If we define:

$$\begin{aligned} \mathcal{M} &= \bigoplus_{i=1}^{l} R/\langle d_i \rangle \\ &= \left\{ (c_1 \bmod d_1 \quad c_2 \bmod d_2 \quad \ldots \quad c_l \bmod d_l) \;\middle|\; \begin{array}{c} c_i \bmod d_i \in R/\langle d_i \rangle, \\ 1 \leq i \leq l \end{array} \right\}, \end{aligned} \tag{1}$$

then $\mathcal{M}$ has the natural structure of an R-module. If $d_1 = \cdots = d_l = 0$, then we write:

$$\mathbb{L} = \bigoplus_{i=1}^{l} R = \{(c_1 \ \ldots \ c_l) \,|\, c_i \in R,\ 1 \le i \le l\}\ .$$

We denote the projection map of the R-modules by:

$$\begin{aligned} F : \mathbb{L} &\to \mathcal{M} \\ (c_1 \ \ldots \ c_l) &\mapsto (c_1 \bmod d_1 \ \ \ldots \ \ c_l \bmod d_l)\,. \end{aligned}$$

Hereafter, if $\mathcal{M}$ is considered, then d_i is assumed to be $d_i \neq 0$ for all $1 \le i \le l$.

Let $\mathcal{C} \subset \mathcal{M}$ be a subset. In this study, we consider R-submodules of the form $\mathcal{C} \subset \mathcal{M}$.

For example, let $R = \mathbb{F}_q[x]$. Then, $\mathcal{M}$ can be also viewed as a vector space of dimension $n = \sum_{i=1}^{l} \deg d_i$ over $\mathbb{F}_q$. If $\mathcal{C} \subset \mathcal{M}$ is an R-module, then $\mathcal{C}$ determines a linear code of length n over $\mathbb{F}_q$, whose dimension will be stated later in Proposition 5. If $l = 1$ and $d_1 = x^n - 1$, then $\mathcal{C}$ is called a cyclic code. If $l = 1$ and d_1 is arbitrary, then $\mathcal{C}$ is called a PC code. If $l \ge 1$, l divides n, and $d_1 = \cdots = d_l = x^{n/l} - 1$, then $\mathcal{C}$ is called a QC code. If $d_i = x^{n_i} - 1$ for all $1 \le i \le l$ and $\sum_{i=1}^{l} n_i = n$, then $\mathcal{C}$ is called a GQC code.

For the other example, let $R = \mathbb{Z}$. Then, an R-module $\mathcal{C} \subset \mathcal{M}$ is called a generalized integer code. If $d_1 = \cdots = d_l$, then $\mathcal{C}$ is called an integer code.

Let $\mathcal{C} \subset \mathcal{M}$ be an R-module. Consider R-module $F^{-1}(\mathcal{C}) \subset \mathbb{L}$. Then, $F^{-1}(\mathcal{C})$ includes l elements of the form:

$$(\underbrace{0 \ \ldots \ 0}_{i-1}\ d_i\ \underbrace{0 \ \ldots \ 0}_{l-i}), \tag{2}$$

where $1 \le i \le l$. Note that:

$$F^{-1}(\mathcal{C}) \supset \mathbb{L}\mathrm{diag}\,[d_1, \ldots, d_l]\,,$$

where:

$$\mathrm{diag}\,[d_1, \ldots, d_l] = \begin{pmatrix} d_1 & 0 & \ldots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & d_l \end{pmatrix} \in M_l(R)$$

and

$$\mathbb{L}G = \{(c_1 \ \ldots \ c_l)\, G \,|\, (c_1 \ \ldots \ c_l) \in \mathbb{L}\}$$

for $G \in M_l(R)$. Conversely, let $\mathbb{B} \subset \mathbb{L}$ be an R-module with $\mathbb{B} \supset \mathbb{L}\,\mathrm{diag}\,[d_1, \ldots, d_l]$. Then, $F(\mathbb{B}) \subset \mathcal{M}$ is an R-module. It is proven below that this correspondence between $\mathbb{B} \subset \mathbb{L}$ with $\mathbb{B} \supset \mathbb{L}\mathrm{diag}\,[d_1, \ldots, d_l]$ and $\mathcal{C} \subset \mathcal{M}$ is one-to-one and onto.

Proposition 1. *The set of R-modules $\mathbb{B} \subset \mathbb{L}$ with $\mathbb{B} \supset \mathbb{L}\mathrm{diag}\,[d_1, \ldots, d_l]$ and the set of R-modules $\mathcal{C} \subset \mathcal{M}$ are bijective through the correspondences $\mathbb{B} \mapsto F(\mathbb{B})$ and $\mathcal{C} \mapsto F^{-1}(\mathcal{C})$ which are the inverse maps of one another.*

Proof. $F(F^{-1}(\mathcal{C})) = \mathcal{C}$ follows from the surjectivity of F. Thus, we only need to show that $F^{-1}(F(\mathbb{B})) = \mathbb{B}$. For $b \in \mathbb{B}$, $F(b) \in F(\mathbb{B})$ implies that $F^{-1}(F(\mathbb{B})) \supset \mathbb{B}$. Conversely, from $x \in F^{-1}(F(\mathbb{B})) \iff F(x) \in F(\mathbb{B})$, there exists $b \in \mathbb{B}$ such that $F(x) = F(b)$. Then, $F(x - b) = 0$, and there exists $c \in \mathbb{L}$ such that $x - b = c\mathrm{diag}\,[d_1, \ldots, d_l]$. Thus, $x = b + c\mathrm{diag}\,[d_1, \ldots, d_l] \in \mathbb{B}$ and $F^{-1}(F(\mathbb{B})) = \mathbb{B}$. □

In [5], the author identified $\mathcal{C}$ with $F^{-1}(\mathcal{C})$ and expressed them using the same notation $\mathcal{C}$. In this study, we distinguish them and use the notation $\mathcal{C}$ only for an R-module in $\mathcal{M}$.

3. Euclidean Division

3.1. Euclidean Division in R

Hereafter, we will use R to denote a Euclidean domain; i.e., R is an integral domain and there exists a function $\psi : R \to \{-\infty\} \cup \mathbb{N}_0$ (where we consider $-\infty < n$ for all $n \in \mathbb{N}_0$), which is called a Euclidean function, that satisfies the following property.

$$\text{For } a, b \in R \text{ with } b \neq 0, \text{ there exist } s, r \in R \text{ such that } a = sb + r \text{ and } \psi(r) < \psi(b). \tag{3}$$

The case of $R = K[x]$. Let $R = K[x]$, the ring of one-variable polynomials over K, where K is a commutative field. For $f = \sum_{h=0}^{w} f_h x^h \in R$ with $f_w \neq 0$, we define $\deg(f) = w$ and $\deg(0) = -\infty$. If K has the infinite number of elements, then we adopt the Euclidean function $\psi : R \to \{-\infty\} \cup \mathbb{N}_0$ as $\psi(f) = \deg(f)$. If K is equal to a q-element finite field $\mathbb{F}_q$, where q denotes a rational prime power, then we adopt:

$$\psi(f) = \begin{cases} q^{\deg(f)} & f \neq 0 \\ 0 & f = 0 \end{cases}$$

for consistency with the case of $\mathbb{Z}$ and the cardinality formula in Proposition 5 later in the paper.

The case of $R = \mathbb{Z}$. Let $R = \mathbb{Z}$. Then, the Euclidean function $\psi : R \to \mathbb{N}_0$ is taken to be the absolute value $\psi(a) = |a|$ for all $a \in \mathbb{Z}$.

Hereafter, for a complex number z, $\mathrm{Re}(z)$ and $\mathrm{Im}(z)$ denote its real part and imaginary part, respectively.

The case of $R = \mathbb{Z}[i]$. Let $R = \mathbb{Z}[i] = \{a_1 + a_2 i \mid a_1, a_2 \in \mathbb{Z}\}$, where $i = \sqrt{-1}$, which is called Gaussian integers [9]. The Euclidean function $\psi : R \to \mathbb{N}_0$ is taken to be the square of the complex absolute value $\psi(a) = |a|^2 = a_1^2 + a_2^2$ for $a = a_1 + a_2 i \in \mathbb{Z}[i]$. Then, the property (3) is shown as follows. For $a, b \in R$ with $b \neq 0$, note that $\mathrm{Re}(a/b), \mathrm{Im}(a/b) \in \mathbb{Q}$ because $a/b = a\overline{b}/(b\overline{b})$. Let $s_1, s_2 \in \mathbb{Z}$ be any values such that:

$$|\mathrm{Re}(a/b) - s_1| \leq \frac{1}{2} \quad \text{and} \quad |\mathrm{Im}(a/b) - s_2| \leq \frac{1}{2}. \tag{4}$$

Then, $s = s_1 + s_2 i$ and $r = a - sb$ satisfies $a = sb + r$ and $\psi(r) < \psi(b)$ because:

$$\psi(r) = \psi(a - sb) = \left|\frac{a}{b} - s\right|^2 \psi(b) = \left(|\mathrm{Re}(a/b) - s_1|^2 + |\mathrm{Im}(a/b) - s_2|^2\right) \psi(b) \leq \frac{1}{2}\psi(b).$$

The case of $R = \mathbb{Z}[\omega]$. Let $R = \mathbb{Z}[\omega] = \{a_1 + a_2\omega \mid a_1, a_2 \in \mathbb{Z}\}$, where $\omega = \dfrac{-1 + \sqrt{-3}}{2}$, which is called Eisenstein integers [9]. Note that $\overline{\omega} = \omega^2 = -1 - \omega$. The Euclidean function $\psi : R \to \mathbb{N}_0$ is taken to be the square of the complex absolute value $\psi(a) = |a|^2 = a_1^2 - a_1 a_2 + a_2^2$ for $a = a_1 + a_2\omega \in \mathbb{Z}[\omega]$. Then, the property (3) is shown as follows. For $a, b \in R$ with $b \neq 0$, note that there exists $q_1, q_2 \in \mathbb{Q}$ such that $a/b = q_1 + q_2\omega$ because $a/b = a\overline{b}/(b\overline{b})$. Let $s_1, s_2 \in \mathbb{Z}$ be any values such that:

$$|q_1 - s_1| \leq \frac{1}{2} \quad \text{and} \quad |q_2 - s_2| \leq \frac{1}{2}. \tag{5}$$

Then, $s = s_1 + s_2\omega$ and $r = a - sb$ satisfies $a = sb + r$ and $\psi(r) < \psi(b)$ because:

$$\psi(r) = \left|\frac{a}{b} - s\right|^2 \psi(b) = \left(|q_1 - s_1|^2 - |q_1 - s_1|\,|q_2 - s_2| + |q_2 - s_2|^2\right) \psi(b) \leq \frac{3}{4}\psi(b).$$

The case of $R = \mathbb{Z}_p$. Let $R = \mathbb{Z}_p$, where p denotes a rational prime and $\mathbb{Z}_p$ denotes the p-adic integer ring:

$$\mathbb{Z}_p = \left\{ a = \sum_{h=0}^{\infty} a_h p^h \;\middle|\; a_h \in \{0, 1, \ldots, p-1\} \right\}.$$

For $a = \sum_{h=w}^{\infty} a_h p^h \in R$ with $a_w \neq 0$, we define $\mathrm{ord}(a) = w$ and $\mathrm{ord}(0) = \infty$. This ring $R = \mathbb{Z}_p$ has a metric called p-adic metric defined by $|a|_p = p^{-\mathrm{ord}(a)}$ for $a \in R$. Any infinite series $a = \sum_{h=0}^{\infty} a_h p^h \in R$ is convergent with respect to the p-adic distance $d_p(a,b) = |a-b|_p$ for $a, b \in R$, i.e., for any $\epsilon > 0$, there exists $N > 0$ such that, for all $m > n > N$,

$$d_p\left(\sum_{h=0}^{m} a_h p^h, \sum_{h=0}^{n} a_h p^h\right) = \left|\sum_{h=n+1}^{m} a_h p^h\right|_p \leq p^{-n-1} < \epsilon,$$

where the inequality $|a + a'|_p \leq \max\{|a|_p, |a'|_p\}$ is used. It is shown that $a = \sum_{h=0}^{\infty} a_h p^h \in R$ is invertible, i.e., there exists $a^{-1} \in R$ such that $aa^{-1} = 1$, if and only if $a_0 \neq 0$. We adopt the Euclidean function $\psi : R \to \mathbb{N}_0$ as:

$$\psi(a) = \begin{cases} |a|_p^{-1} = p^{\mathrm{ord}(a)} & a \neq 0 \\ 0 & a = 0. \end{cases}$$

Note that, for any $b \in R$ with $b \neq 0$, $b/\psi(b) \in R$ is invertible, i.e., $b^{-1}\psi(b) \in R$. Then, the property (3) is shown as follows. If $\psi(a) < \psi(b)$, then $s = 0$ and $r = a$. If $\psi(a) \geq \psi(b)$, then $s = b^{-1}a$ and $r = 0$ because $s = b^{-1}\psi(b) \cdot \psi(b)^{-1}a \in R$.

The case of $R = K[[x]]$. Let $R = K[[x]]$, the ring of one-variable formal power series over a commutative field K:

$$K[[x]] = \left\{ a = \sum_{h=0}^{\infty} a_h x^h \;\middle|\; a_h \in K \right\}.$$

For $a = \sum_{h=w}^{\infty} a_h x^h \in R$ with $a_w \neq 0$, we define $\mathrm{ord}(a) = w$ and $\mathrm{ord}(0) = -\infty$. It is shown that $a = \sum_{h=0}^{\infty} a_h x^h \in R$ is invertible, i.e., there exists $a^{-1} \in R$ such that $aa^{-1} = 1$, if and only if $\mathrm{ord}(a) = 0$. If K has the infinite number of elements, then we adopt the Euclidean function $\psi : R \to \{-\infty\} \cup \mathbb{N}_0$ as $\psi(a) = \mathrm{ord}(a)$. If $K = \mathbb{F}_q$, then we adopt:

$$\psi(a) = \begin{cases} q^{\mathrm{ord}(a)} & a \neq 0 \\ 0 & a = 0. \end{cases}$$

Note that, for any $b \in R$ with $b \neq 0$, $x^{-\mathrm{ord}(b)}b \in R$ is invertible, i.e., $x^{\mathrm{ord}(b)}b^{-1} \in R$. Then, the property (3) is shown as follows. If $\psi(a) < \psi(b)$, then $s = 0$ and $r = a$. If $\psi(a) \geq \psi(b)$, then $s = b^{-1}a$ and $r = 0$ because $s = b^{-1}x^{\mathrm{ord}(b)} \cdot x^{-\mathrm{ord}(b)}a \in R$.

Hereafter, for a finite set S, we use $|S|$ to denote the number of elements in S and we denote $|S| = \infty$ if and only if S is an infinite set. Summarizing the above, we take the Euclidean function $\psi : R \to \{-\infty\} \cup \mathbb{N}_0$ as, for $a \in R$,

$$\psi(a) = \begin{cases} \deg(a) \;\text{ or }\; \deg(0) = -\infty & R = K[x],\ |K| = \infty \\ q^{\deg(a)} \;\text{ or }\; \psi(0) = 0 & R = \mathbb{F}_q[x] \\ |a| & R = \mathbb{Z} \\ |a|^2 = a_1^2 + a_2^2 \;\text{ if }\; a = a_1 + a_2 i,\ a_1, a_2 \in \mathbb{Z} & R = \mathbb{Z}[i] \\ |a|^2 = a_1^2 - a_1 a_2 + a_2^2 \;\text{ if }\; a = a_1 + a_2\omega,\ a_1, a_2 \in \mathbb{Z} & R = \mathbb{Z}[\omega] \\ p^{\mathrm{ord}(a)} \;\text{ or }\; \psi(0) = 0 & R = \mathbb{Z}_p \\ \mathrm{ord}(a) \;\text{ or }\; \psi(0) = -\infty & R = K[[x]],\ |K| = \infty \\ q^{\mathrm{ord}(a)} \;\text{ or }\; \psi(0) = 0 & R = \mathbb{F}_q[[x]]. \end{cases} \tag{6}$$

Unless otherwise noted, the following argument is also valid for the other choices of the Euclidean function ψ and arbitrary Euclidean domains.

3.2. Euclidean Division by a Class of Matrices

Definition 1. *If* $G = \left(g_{i,j}\right) \in M_l(R)$ *satisfies* $g_{i,j} = 0$ *for all* $1 \leq j < i \leq l$*, i.e., G is of the form:*

$$G = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & g_{l,l} \end{pmatrix},$$

and $\det(G) \neq 0$*, then we say that G is upper triangular.*

Note that we impose $\det(G) \neq 0$ if we say that G is upper triangular.

In this study, we need the following division algorithm, which is described in [5] in the special case where $R = \mathbb{F}_q[x]$.

Proposition 2. *Let* $G = \left(g_{i,j}\right) \in M_l(R)$ *be upper triangular. Then, for any* $a = (a_1 \ \ldots \ a_l) \in \mathbb{L}$*, there exist* $s = (s_1 \ \ldots \ s_l), r = (r_1 \ \ldots \ r_l) \in \mathbb{L}$ *such that* $a = sG + r$*, i.e.,*

$$(a_1 \ \ldots \ a_l) = (s_1 \ \ldots \ s_l)\, G + (r_1 \ \ldots \ r_l), \tag{7}$$

with $\psi(r_i) < \psi(g_{i,i})$ *for all* $1 \leq i \leq l$*.*

Proof. To prove Proposition 2 constructively, consider the following $(l+1)$-by-l matrix:

$$\left(\frac{G}{a}\right) = \left(\begin{array}{c} g_1 \\ g_2 \\ \vdots \\ \hline g_l \\ a \end{array}\right) = \left(\begin{array}{cccc} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ \hline 0 & \ldots & 0 & g_{l,l} \\ a_1 & \ldots & a_{l-1} & a_l \end{array}\right), \tag{8}$$

where g_i denotes the i-th row of G for all $1 \leq i \leq l$. Then, the following row operations for the matrix (8) are performed:

⟨1⟩ Set $i = 1$.
⟨2⟩ Compute $s_i, r_i \in R$ such that $a_i = s_i g_{i,i} + r_i$ with $\psi(r_i) < \psi(g_{i,i})$ and replace a with $a - s_i g_i$ in (8).
⟨3⟩ If $i = l$, stop. Otherwise, set i to $i + 1$ and return to ⟨2⟩.

Thus, $s = (s_1 \ \ldots \ s_l), r = (r_1 \ \ldots \ r_l) \in \mathbb{L}$ are determined and (7) holds because the initial a is converted into r in (8), and the result of these row operations can be represented by $r = a - \sum_{i=1}^{l} s_i g_i = a - sG$. □

4. Generator Matrices of R-Modules in $\mathcal{M}$

In this section, we define the generator matrices of $\mathcal{C}$, which are useful to generate code words in $\mathcal{C}$.

Definition 2. *We call* $G \in M_l(R)$ *a generator matrix of* $\mathcal{C}$ *if and only if* $F^{-1}(\mathcal{C}) = \mathbb{L}G$*.*

If such a generator matrix G of $\mathcal{C}$ is constructed, we have $\mathcal{C} = F(\mathbb{L}G)$ because of $F\left(F^{-1}(\mathcal{C})\right) = \mathcal{C}$. We now show the construction of a generator matrix G of $\mathcal{C}$.

Proposition 3. *For all* $1 \leq i \leq l$*, let:*

$$g_i = (g_{i,1} \ \ldots \ g_{i,l}) \in F^{-1}(\mathcal{C}) \tag{9}$$

be an element of $\mathbb{L}$ *satisfying the following two conditions:*

1. $g_{i,i} \neq 0$ *and, if* $i \neq 1$, $g_{i,1} = \cdots = g_{i,i-1} = 0$.
2. $\psi(g_{i,i})$ *has the minimum value among* $\psi(c_i)$ *for all* $(c_1 \ \ldots \ c_l) \in F^{-1}(\mathcal{C})$ *with* $c_i \neq 0$ *and, if* $i \neq 1$, *with* $c_1 = \cdots = c_{i-1} = 0$.

Let $G \in M_l(R)$ *have an i-th row equal to* (9) *that satisfies Conditions 1 and 2 for all* $1 \leq i \leq l$. *Then, G is a generator matrix of* $\mathcal{C}$, *i.e., we have* $F^{-1}(\mathcal{C}) = \mathbb{L}G$. *Conversely, if* G' *is another generator matrix of* $\mathcal{C}$, *then there exists* $E \in GL_l(R)$ *such that* $G' = EG$.

Proof. Such a $g_i \in \mathbb{L}$ with $g_{i,i} \neq 0$ exists because $F^{-1}(\mathcal{C})$ includes (2). For any $c \in F^{-1}(\mathcal{C})$, let $s, r \in \mathbb{L}$ be such that $c = sG + r$ and $\psi(r_i) < \psi(g_{i,i})$ for all $1 \leq i \leq l$ by Proposition 2. Because $F^{-1}(\mathcal{C})$ is an R-module, $r = c - sG \in F^{-1}(\mathcal{C})$ implies that $r = (0 \ \ldots \ 0)$, which completes the first half of the proof. If $\mathbb{L}G = \mathbb{L}G'$, then $\mathbb{L} = \mathbb{L}G'G^{-1}$. Because:

$$\mathbb{L} \ni (1\,0\,0 \ \ldots \ 0)G'G^{-1},\ (0\,1\,0 \ \ldots \ 0)G'G^{-1}, \ldots, (0\,0 \ \ldots \ 0\,1)G'G^{-1},$$

we have $G'G^{-1} \in M_l(R)$. Because:

$$(1\,0\,0 \ \ldots \ 0),\ (0\,1\,0 \ \ldots \ 0), \ldots, (0\,0 \ \ldots \ 0\,1) \in \mathbb{L}G'G^{-1},$$

we have $G'G^{-1} \in GL_l(R)$, which completes the proof. □

Let $\mathcal{C} \subset \mathcal{M}$ be an R-module. Because $F^{-1}(\mathcal{C}) = \mathbb{L}G$ implies that $\mathbb{L}G \supset \mathbb{L}\mathrm{diag}\,[d_1, \ldots, d_l]$, the generator matrix $G \in M_l(R)$ of $\mathcal{C}$ satisfies the following matrix equation:

$$AG = \mathrm{diag}\,[d_1, \ldots, d_l]\,, \tag{10}$$

for some $A \in M_l(R)$. Conversely, if $G \in M_l(R)$ satisfies (10) for some $A \in M_l(R)$, then G determines an R-module $\mathcal{C} = \mathbb{L}G/\mathbb{L}\mathrm{diag}\,[d_1, \ldots, d_l]$. We summarize these facts.

Proposition 4. *Let* $G \in M_l(R)$. *Then, G is equal to a generator matrix for some* $\mathcal{C}$ *if and only if G satisfies* (10) *for some* $A \in M_l(R)$.

Note that if upper triangular G satisfies (10), then A is also upper triangular. Note also that, if $u = d_1 = \cdots = d_l$, then $AG = GA = \mathrm{diag}\,[u, \ldots, u]$, cf. [5,7].

Example 1. *Let* $R = \mathbb{Z}[i]$. *If* $l = 1$ *and* $d_1 = 5$, *then* $F : R \to R/\langle 5 \rangle \supset \mathcal{C} = gR/\langle 5 \rangle$ *is satisfied by* $g = 1, 2 \pm i, 5$ *up to units. Although the general R-submodule R is equal to* αR *for some* $\alpha \in R$, $F^{-1}\left(gR/\langle 5 \rangle\right) = gR$ *is valid for* $g = 1, 2 \pm i, 5$ *up to units. This fact corresponds to the equation* $Ag = 5$ *of* (10). *Next, if* $l = 2$ *and* $d_1 = d_2 = 5$, *then consider:*

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (4+2i, 2+i), \\ (3+4i, 4+2i), \\ (2+i, 1+3i), \\ (1+3i, 3+4i), \\ (0,0) \end{array} \right\} \subset \mathcal{M} = (R/\langle 5 \rangle)^2.$$

Because $\mathcal{C}_2$ *forms an R-submodule,* $\mathcal{C}_2$ *is a code over Gaussian integers. We note that the generator matrix of* $\mathcal{C}_2$ *is equal to:*

$$G_2 = \begin{pmatrix} 2+i & 1+3i \\ 0 & 5 \end{pmatrix}.$$

Then, G_2 satisfies:

$$\begin{pmatrix} 2-i & -1-i \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2+i & 1+3i \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}.$$

Cardinality Formulae

In this subsection, we focus on the Euclidean domain R described above. We denote $|K| = \infty$ to mean the case where the coefficient field K of $R = K[x]$ or $K[[x]]$ contains infinitely many elements.

Then, for any $a, b \in R$, the Euclidean function of (6) satisfies:

$$\psi(ab) = \begin{cases} \psi(a) + \psi(b) & \text{if } |K| = \infty \\ \psi(a)\psi(b) & \text{otherwise.} \end{cases}$$

Moreover, for any $b \in R$ with $b \neq 0$, we have:

$$\psi(b) = \begin{cases} \dim_K R/\langle b \rangle & \text{if } |K| = \infty \\ |R/\langle b \rangle| & \text{otherwise,} \end{cases}$$

where, for a finite dimensional K-vector space V, $\dim_K V$ denotes its dimension. Let G be a generator matrix of an R-module $\mathcal{C} \subset \mathcal{M}$. Consider the following composition map:

$$\begin{aligned} \mathbb{L} &\to \mathcal{M} \\ (c_1 \ \dots \ c_l) &\mapsto F\left((c_1 \ \dots \ c_l)\, G\right). \end{aligned}$$

Note that $F(\cdot)G$ is not well-defined in general because $\mathbb{L}\mathrm{diag}\,[d_1, \dots, d_l]\, G \not\subset \mathbb{L}\mathrm{diag}\,[d_1, \dots, d_l]$ in general, e.g., $\begin{pmatrix} 2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \notin \mathbb{Z}^2\mathrm{diag}[2,4]$ for $\begin{pmatrix} 2 & -1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$. Then, the image of this composition map is equal to $\mathcal{C}$. Moreover, the kernel of this composition map is equal to $\mathbb{L}A$ because:

$$\begin{aligned} F\left((c_1 \ \dots \ c_l)\, G\right) = 0 &\iff (c_1 \ \dots \ c_l)\, G \in \mathbb{L}\mathrm{diag}\,[d_1, \dots, d_l] \\ &\iff (c_1 \ \dots \ c_l)\, G \in \mathbb{L}AG \quad (\because (10)) \\ &\iff (c_1 \ \dots \ c_l) \in \mathbb{L}A. \end{aligned}$$

Thus, the R-modules $\mathbb{L}/\mathbb{L}A$ and $\mathcal{C}$ are isomorphic. On the other hand, it follows from the theory of elementary divisors [14] that there exist $U, V \in GL_l(R)$ such that $UAV = \mathrm{diag}\,[b_1, \dots, b_l]$ and $\langle b_1 \rangle \supset \cdots \supset \langle b_l \rangle$. Then, $\mathbb{L}/\mathbb{L}A$ is isomorphic to $\bigoplus_{i=1}^{l} R/\langle b_i \rangle$ as R-modules and:

$$\psi(\det(A)) = \begin{cases} \sum_{i=1}^{l} \psi(b_i) = \dim_K \mathbb{L}/\mathbb{L}A & \text{if } |K| = \infty \\ \prod_{i=1}^{l} \psi(b_i) = |\mathbb{L}/\mathbb{L}A| & \text{otherwise.} \end{cases}$$

We also note that:

$$\psi(\det(A)\det(G)) = \begin{cases} \sum_{i=1}^{l} \psi(d_i) = \dim_K \mathcal{M} & \text{if } |K| = \infty \\ \prod_{i=1}^{l} \psi(d_i) = |\mathcal{M}| & \text{otherwise.} \end{cases}$$

Hence, we obtain the following cardinality formula for $\mathcal{C}$ and all G.

Proposition 5. *Let $\mathcal{C} \subset \mathcal{M}$ be an R-module and G be its generator matrix. Then, we have:*

$$\begin{cases} \dim_K \mathcal{C} = n - \psi(\det(G)) & \text{if } |K| = \infty \\ |\mathcal{C}| = |\mathcal{M}|/\psi(\det(G)) & \text{otherwise.} \end{cases}$$

In the case where $R = \mathbb{F}_q[x]$, we denote $k_i = \deg d_i - \deg g_{i,i}$ and $k = \sum_{i=1}^{l} k_i$ if the generator matrix $G = (g_{i,j})$ is upper triangular. Then, k is equal to the dimension of $\mathcal{C}$ over $\mathbb{F}_q$. As an application of Proposition 5, we see that a generator matrix of $\mathcal{C}$ viewed as a linear code is composed of the following linearly independent k code words from the rows of G for $1 \leq i \leq l$ and $0 \leq m < k_i$:

$$\left(x^m g_{i,1} \bmod d_1 \quad x^m g_{i,2} \bmod d_2 \quad \dots \quad x^m g_{i,l} \bmod d_l\right). \tag{11}$$

Example 2. *In the case of $R = \mathbb{F}_q[x]$, $q = 2$, and $l = 3$, we set $d_1 = d_2 = d_3 = (1 + x + x^3)^2 = 1 + x^2 + x^6$. Consider:*

$$A = \begin{pmatrix} 1 + x^2 + x^6 & 1 + x^4 + x^5 & x^2 + x^3 + x^4 + x^5 \\ 0 & 1 + x + x^3 & x + x^2 \\ 0 & 0 & 1 \end{pmatrix},$$

$$G = \begin{pmatrix} 1 & 1 + x + x^2 & x + x^2 + x^3 + x^5 \\ 0 & 1 + x + x^3 & x + x^3 + x^4 + x^5 \\ 0 & 0 & 1 + x^2 + x^6 \end{pmatrix}.$$

Then, we have:

$$AG = \left(1 + x^2 + x^6\right) I.$$

Let $\mathcal{C}$ be the R-module in $\mathcal{M}$ defined by G. Then, the length n of $\mathcal{C}$ is equal to 18 and the dimension k of $\mathcal{C}$ is equal to 9. From G and (11), we can derive a binary generator matrix:

$$\left(\begin{array}{c|c|c} 100000 & 111000 & 011101 \\ 010000 & 011100 & 100110 \\ 001000 & 001110 & 010011 \\ 000100 & 000111 & 100001 \\ 000010 & 101011 & 111000 \\ 000001 & 111101 & 011100 \\ \hline 000000 & 110100 & 010111 \\ 000000 & 011010 & 100011 \\ 000000 & 001101 & 111001 \end{array}\right).$$

By applying the division algorithm to G in Proposition 2, we obtain the systematic encoding of $\mathcal{C}$, which is similar to that in the case of GQC codes [5].

5. Multiplicative Structure

In this section, we again consider the R-modules in $\mathcal{M}$ for the general Euclidean domain R. Hereafter, we mainly consider the case of $d_1 = \cdots = d_l$ in (1). If $u = d_1 = \cdots = d_l$, then we have $\operatorname{diag}[u, \dots, u] = uI$ and $\mathcal{M} = \mathbb{L}/\mathbb{L}\operatorname{diag}[d_1, \dots, d_l] = \mathbb{L}/u\mathbb{L}$.

Let $G_1, G_2 \in M_l(R)$ satisfy the relations:

$$A_1 G_1 = u_1 I, \quad A_2 G_2 = u_2 I$$

for some $A_1, A_2 \in M_l(R)$ with $u_1, u_2 \in R$ and $u_1 u_2 \neq 0$. Then, we have:

$$A_2 A_1 G_1 G_2 = u_1 u_2 I.$$

This argument shows that $\mathcal{C}_1 = \mathbb{L}G_1/u_1\mathbb{L}$ and $\mathcal{C}_2 = \mathbb{L}G_2/u_2\mathbb{L}$ produce $\mathcal{C} = \mathbb{L}G_1G_2/u_1u_2\mathbb{L}$.

Remark 1. *If $d_1 = \cdots = d_l$ does not hold, then in general $\mathbb{L}G_1G_2$ does not include $u_1u_2\mathbb{L}$. For example, consider $G_1 = \begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix}$ and $G_2 = \begin{pmatrix} 1 & 3 \\ 0 & 9 \end{pmatrix}$. Then, we have:*

$$A_1G_1 = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix},$$
$$A_2G_2 = \begin{pmatrix} 3 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 0 & 9 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 9 \end{pmatrix},$$

$G_1G_2 = \begin{pmatrix} 1 & 21 \\ 0 & 36 \end{pmatrix}$, *and* $G_2G_1 = \begin{pmatrix} 1 & 14 \\ 0 & 36 \end{pmatrix}$. *If there exists $a, g \in \mathbb{Z}$ such that:*

$$\begin{pmatrix} 6 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & g \\ 0 & 36 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 36 \end{pmatrix},$$

then we have $6g + 36a = 0$ and $g \in 6\mathbb{Z}$. Thus, for $G = G_1G_2$ and $G = G_2G_1$, there does not exist A such that $AG = \begin{pmatrix} 6 & 0 \\ 0 & 36 \end{pmatrix}$.

5.1. Surjectivity

We fix a nonzero $u \in R$. Because $GL_l(R)$ acts from the left on the set of $G \in M_l(R)$ with $AG = uI$ for some $A \in M_l(R)$, we can consider a quotient set:

$$GL_l(R)\backslash\{G \in M_l(R) \mid AG = uI \text{ for some } A \in M_l(R)\}. \tag{12}$$

Let $\{G\}_u$ denote a complete system of representatives of generator matrices of R-modules in $\mathcal{M} = \mathbb{L}/u\mathbb{L}$. In other words, $\{G\}_u$ corresponds one-to-one and onto to R-modules $\mathcal{C} = \mathbb{L}G/u\mathbb{L}$ in $\mathcal{M}$. In Section 6, we will define a standard form of $G \in \{G\}_u$, which will be called reduced, in order to indicate a unique representative of generator matrices of an R-module in $\mathcal{M}$ for specified R's.

Theorem 1. *Suppose that $u = u_1u_2$ with $u_1, u_2 \in R$. Consider the map:*

$$\varpi : \{G_1\}_{u_1} \times \{G_2\}_{u_2} \to \{G\}_u$$
$$(G_1, G_2) \mapsto G,$$

where $\mathbb{L}G_1G_2 = \mathbb{L}G$. Then, ϖ is surjective.

Proof. For each $G \in \{G\}_u$, let $\mathcal{C} = \mathbb{L}G/u\mathbb{L}$. We consider an R-module in $\mathbb{L}/u_2\mathbb{L}$:

$$\mathcal{C}_2 = \frac{u_2\mathbb{L} + \mathbb{L}G}{u_2\mathbb{L}}. \tag{13}$$

Then, there exists $G_2 \in \{G_2\}_{u_2}$ such that $\mathcal{C}_2 = \mathbb{L}G_2/u_2\mathbb{L}$. By Proposition 1, we have:

$$u_2\mathbb{L} + \mathbb{L}G = \mathbb{L}G_2, \tag{14}$$

which leads to $\mathbb{L}G \subset \mathbb{L}G_2$. Then, there exists some $G_1 \in M_l(R)$ such that $G = G_1G_2$. If we can show that $\mathbb{L}G_1 \supset u_1\mathbb{L}$, then the proof is completed. From $AG = uI = u_1u_2I$ and $A_2G_2 = u_2I$, we have:

$$AG_1G_2 = u_1A_2G_2, \quad AG_1 = u_1A_2 = A_2u_1I,$$

and $A_2^{-1}AG_1 = u_1I$. Thus, we may show $A_2^{-1}A \in M_l(R)$. Because, for some $M \in M_l(R)$,

$$M = A_2^{-1}A \Longleftrightarrow A_2M = A \Longleftrightarrow u_2IM = G_2A_2M = G_2A,$$

where we note $u_2I = A_2G_2 = G_2A_2$, we may show $u_2\mathbb{L} \supset \mathbb{L}G_2A$. It follows from $\mathbb{L}G_2 = \mathbb{L}G + u_2\mathbb{L}$ that $G_2 = PG + u_2Q$ for some $P, Q \in M_l(R)$. Hence we have, noting that $uI = AG = GA$,

$$\mathbb{L}G_2A = \mathbb{L}\left(PG + u_2Q\right)A = u_2\mathbb{L}\left(u_1P + QA\right) \subset u_2\mathbb{L}.$$

□

Example 3. *(Continued from Example 2.) For $u_1 = u_2 = 1 + x + x^3$, G is equal to G_1G_2, where:*

$$G_1 = \begin{pmatrix} 1 & 0 & x^2 \\ 0 & 1 & x + x^2 \\ 0 & 0 & 1 + x + x^3 \end{pmatrix} \in \{G_1\}_{u_1},\ G_2 = \begin{pmatrix} 1 & 1 + x + x^2 & x \\ 0 & 1 + x + x^3 & 0 \\ 0 & 0 & 1 + x + x^3 \end{pmatrix} \in \{G_2\}_{u_2}.$$

As for this G, there exists another pair of representatives G_1, G_2 with $G = G_1G_2$, i.e.,

$$G_1 = \begin{pmatrix} 1 & 1 + x + x^2 & x + x^2 \\ 0 & 1 + x + x^3 & 0 \\ 0 & 0 & 1 + x + x^3 \end{pmatrix} \in \{G_1\}_{u_1},\ G_2 = \begin{pmatrix} 1 & 0 & x + x^2 \\ 0 & 1 & x + x^2 \\ 0 & 0 & 1 + x + x^3 \end{pmatrix} \in \{G_2\}_{u_2}.$$

5.2. Injectivity

Theorem 2. *Let the notation be as in Theorem 1. If* $\gcd(u_1, u_2) = 1$, *then ϖ is bijective.*

To prove Theorem 2, we must first prove a lemma.

Lemma 1. *Let the notation be the same as that in Theorem 1. If* $\gcd(u_1, u_2) = 1$, *then:*

$$\frac{u_2\mathbb{L} + \mathbb{L}G_1G_2}{u_2\mathbb{L}} = \frac{\mathbb{L}G_2}{u_2\mathbb{L}}.$$

If $\gcd(u_1, u_2) \neq 1$, then Lemma 1 is not correct in general. For example, if $u_1 = u_2 = 2$, $G_1 = 2$, and $G_2 = 1$, then $\left(u_2\mathbb{L} + \mathbb{L}G_1G_2\right)/u_2\mathbb{L} = \{0\}$ but $\mathbb{L}G_2/u_2\mathbb{L} = \mathbb{F}_2$. Note that this fact does not contradict (13) in the proof of Theorem 1.

Proof of Lemma 1. We may show that $u_2\mathbb{L} + \mathbb{L}G_1G_2 \supset \mathbb{L}G_2$. Because there exists $E \in GL_l(R)$ such that EG_1 is upper triangular, we may assume without loss of generality that G_1 is upper triangular. For $A_1 = \left(a_{i,j}^{(1)}\right)$ and $G_1 = \left(g_{i,j}^{(1)}\right)$ with $A_1G_1 = u_1I$, we have $a_{i,i}^{(1)}g_{i,i}^{(1)} = u_1$ for all $1 \leq i \leq l$. Then, $\gcd\left(g_{i,i}^{(1)}, u_2\right) = 1$ and there exist $s_i, t_i \in R$ such that $s_ig_{i,i}^{(1)} - t_iu_2 = 1$ for all $1 \leq i \leq l$. Thus,

$$\operatorname{diag}\left[s_1, \ldots, s_l\right]G_1 = \begin{pmatrix} s_1g_{1,1}^{(1)} & & * \\ & \ddots & \\ 0 & & s_lg_{l,l}^{(1)} \end{pmatrix} = \begin{pmatrix} t_1u_2 & & 0 \\ & \ddots & \\ 0 & & t_lu_2 \end{pmatrix} + \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

and:

$$u_2\mathbb{L}+\mathbb{L}G_1G_2 \supset u_2\mathbb{L}+\mathbb{L}\mathrm{diag}\,[s_1,\ldots,s_l]\,G_1G_2 \supset u_2\mathbb{L}+\mathbb{L}\begin{pmatrix}1 & & *\\ & \ddots & \\ 0 & & 1\end{pmatrix}G_2=\mathbb{L}G_2.$$

□

Proof of Theorem 2. For a given $G \in \{G\}_u$, there exists $(G_1, G_2) \in \{G_1\}_{u_1} \times \{G_2\}_{u_2}$ such that $\mathbb{L}G_1G_2 = \mathbb{L}G$ by Theorem 1. We may prove only the uniqueness of G_2, which leads the uniqueness of G_1 by the relation $\mathbb{L}G_1 = \mathbb{L}GG_2^{-1}$. Again, we consider an R-module in $\mathbb{L}/u_2\mathbb{L}$

$$\mathcal{C}_2 = \frac{u_2\mathbb{L}+\mathbb{L}G}{u_2\mathbb{L}}.$$

By Lemma 1, we have $\mathcal{C}_2 = \mathbb{L}G_2/u_2\mathbb{L}$. If there exists $(G_1', G_2') \in \{G_1\}_{u_1} \times \{G_2\}_{u_2}$ such that $\mathbb{L}G_1'G_2' = \mathbb{L}G$, it again follows from Lemma 1 that $\mathcal{C}_2 = \mathbb{L}G_2'/u_2\mathbb{L}$. By Proposition 1, we have $\mathbb{L}G_2 = \mathbb{L}G_2'$, which completes the proof. □

Remark 2. *Because Lemma 1 is true only for G_2 in general, $\mathcal{C}_1 = (u_1\mathbb{L}+\mathbb{L}G)/u_1\mathbb{L}$ does not agree with $\mathbb{L}G_1/u_1\mathbb{L}$ in general. For example, consider the case where $R = \mathbb{Z}$, $l = 2$, $u = 6$, $u_1 = 2$, $u_2 = 3$, and $G = \begin{pmatrix}1 & 4\\ 0 & 6\end{pmatrix}$. Then, we have:*

$$AG = \begin{pmatrix}6 & -4\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 4\\ 0 & 6\end{pmatrix} = \begin{pmatrix}6 & 0\\ 0 & 6\end{pmatrix},$$
$$\mathcal{C} = \frac{\mathbb{L}G}{u\mathbb{L}} = \{(0\,0), (1\,4), (2\,2), (3\,0), (4\,4), (5\,2)\},$$
$$\mathcal{C}_2 = \frac{u_2\mathbb{L}+\mathbb{L}G}{u_2\mathbb{L}} = \{(0\,0), (1\,1), (2\,2)\}.$$

Then, $\mathcal{C}_2 = \mathbb{L}G_2/u_2\mathbb{L}$ with $G_2 = \begin{pmatrix}1 & 1\\ 0 & 3\end{pmatrix}$ and $A_2G_2 = \begin{pmatrix}3 & -1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 3\end{pmatrix} = \begin{pmatrix}3 & 0\\ 0 & 3\end{pmatrix}$. On the other hand, we have:

$$\mathcal{C}_1 = \frac{u_1\mathbb{L}+\mathbb{L}G}{u_1\mathbb{L}} = \{(0\,0), (1\,0)\}$$

and $\mathcal{C}_1 = \mathbb{L}G_1'/u_1\mathbb{L}$ with $G_1' = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$. In fact, $G = G_1G_2$ with $G_1 = \begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix} \neq G_1'$ and $A_1G_1 = \begin{pmatrix}2 & -1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix} = \begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$.

Example 4. *Consider the case of $R = \mathbb{F}_2[x]$, $u = x + x^2$, $u_1 = x$, and $u_2 = 1 + x$. Because $\mathbb{L}/u_1\mathbb{L} = (\mathbb{F}_2)^l$ for any positive $l \in \mathbb{Z}$, the number of $\mathcal{C}_1 \subset \mathbb{L}/u_1\mathbb{L}$ is equal to $\sum_{k=0}^{l} c_k^{(l)}(2)$, where $c_k^{(l)}(q)$ denotes the number of k-dimensional $\mathbb{F}_q$-vector subspaces in $\left(\mathbb{F}_q\right)^l$,*

$$c_k^{(l)}(q) = c_{l-k}^{(l)}(q) = \frac{(q^l-1)(q^l-q)\ldots(q^l-q^{k-1})}{(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})}, \tag{15}$$

cf. [13], e.g., $\sum_{k=0}^{l} c_k^{(l)}(2) = 2, 5, 16, 67, 374, 2825, 29212$ for $l = 1, \ldots, 7$. Because $\mathbb{L}/u_2\mathbb{L} = (\mathbb{F}_2)^l$, the number of $\mathcal{C}_2 \subset \mathbb{L}/u_2\mathbb{L}$ is equal to that of $\mathcal{C}_1 \subset \mathbb{L}/u_1\mathbb{L}$. Then, Theorem 2 asserts that

$|\{G\}_u| = |\{G_1\}_{u_1}| \cdot |\{G_2\}_{u_2}|$, *and that any* $G \in \{G\}_u$ *can be uniquely obtained from* G_1G_2 *for some* $G_1 \in \{G_1\}_{u_1}$ *and* $G_2 \in \{G_2\}_{u_2}$. *For example, let:*

$$G = \begin{pmatrix} 1 & 1 & 1 & 1+x \\ 0 & x & 1 & 1 \\ 0 & 0 & 1+x & 1+x \\ 0 & 0 & 0 & x+x^2 \end{pmatrix} \in \{G\}_u.$$

Then, we can find:

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & x & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & x \end{pmatrix}, \; G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1+x & 0 \\ 0 & 0 & 0 & 1+x \end{pmatrix}, \; G_1G_2 = \begin{pmatrix} 1 & 1 & 1 & 1+x \\ 0 & x & x & x \\ 0 & 0 & 1+x & 1+x \\ 0 & 0 & 0 & x+x^2 \end{pmatrix}.$$

There exists $E \in GL_l(R)$ *such that* $EG_1G_2 = G$.

6. Unique Euclidean Division Cases

In this section, we focus on the Euclidean domain R described above specifically. First, we will show that the Euclidean division in R satisfies the following condition.

- For $a, b \in R$ with $b \neq 0$, there exist unique $s, r \in R$ such that:
  - $a = sb + r$ with $\psi(r) < \psi(b)$,
  - (if necessary,) the additional property on s, r, which is described below, specified on each R.

To validate this condition for the Euclidean division by a nonzero $b \in R$, one may choose a complete system $S_b \subset R$ of representatives of $R/\langle b \rangle$ such that $\psi(r) < \psi(b)$ for all $r \in S_b$. Then, the above condition is valid because $a = sb + r = s'b + r'$ with $s, s' \in R$ and $r, r' \in S_b$ implies $r + \langle b \rangle = r' + \langle b \rangle \in R/\langle b \rangle$ and $r = r'$. However, for each b, it is not always easy to choose S_b. Thus, in this section, we show that a convenient S_b can be taken in each case of R's.

The case of $R = K[x]$. The Euclidean function ψ has the uniqueness properties, i.e., s, r are uniquely determined in $a = sb + r$ with $b \neq 0$ and $\psi(r) < \psi(b)$ because, if $a = sb + r = s'b + r'$, then $0 = (s - s')b + (r - r')$, and it follows from $\psi(r - r') = \psi((s' - s)b)$ and $\psi(r - r') \leq \max\{\psi(r), \psi(r')\}$ that $s - s' = r - r' = 0$.

The case of $R = \mathbb{Z}$. For $a, b \in R$ with $b \neq 0$, the results s, r of Euclidean division $a = sb + r$ with $\psi(r) < \psi(b)$ and $\psi(\cdot) = |\cdot|$ are not unique as stated in Introduction. Hence, we decide s, r by $a = sb + r$ with $s = \lfloor a/b \rfloor$. In other words, we have $a = sb + r$ with $0 \leq r/b < 1$, or equivalently, with $\lfloor r/b \rfloor = 0$, because:

$$s = \left\lfloor \frac{a}{b} \right\rfloor \Longleftrightarrow s \leq \frac{a}{b} < s + 1 \Longleftrightarrow 0 \leq \frac{r}{b} < 1 \Longleftrightarrow \left\lfloor \frac{r}{b} \right\rfloor = 0.$$

Then, s, r are unique because of the expression $s = \lfloor a/b \rfloor$. (Alternatively, if $a = sb + r = s'b + r'$, then $0 = (s - s')b + (r - r')$ and it follows from $0 \leq r/b < 1$ and $0 \leq r'/b < 1$ that $|(r - r')/b| < 1$ and $s - s' = 0$.) There are some choices to indicate unique s, r, e.g.,

$$s = \lfloor a/b \rfloor \Longleftrightarrow \lfloor r/b \rfloor = 0, \qquad s = \lceil a/b \rfloor \Longleftrightarrow \lceil r/b \rfloor = 0,$$
$$s = \lfloor a/b + 1/2 \rfloor \Longleftrightarrow \lfloor r/b + 1/2 \rfloor = 0, \qquad s = \lceil a/b - 1/2 \rfloor \Longleftrightarrow \lceil r/b - 1/2 \rfloor = 0,$$

where, for $x \in \mathbb{R}$, $\lceil x \rfloor$ denotes a unique $n \in \mathbb{Z}$ such that $n - 1 < x \leq n$. We adopt $s = \lfloor a/b \rfloor$ for simplicity.

The case of $R = \mathbb{Z}[i]$. For $a, b \in R$ with $b \neq 0$, the results s, r of Euclidean division $a = sb + r$ with $\psi(r) < \psi(b)$ and $\psi(\cdot) = |\cdot|^2$ are not unique because $1 = 1 \cdot 2 - 1 = 0 \cdot 2 + 1$. We decide s, r with $a = sb + r$ and $\psi(r) < \psi(b)$ by

$$s = \left\lfloor \mathrm{Re}\left(\frac{a}{b}\right) + \frac{1}{2} \right\rfloor + \left\lfloor \mathrm{Im}\left(\frac{a}{b}\right) + \frac{1}{2} \right\rfloor i. \tag{16}$$

(Similarly, $s = \lceil \mathrm{Re}\,(a/b) - 1/2 \rceil + \lceil \mathrm{Im}\,(a/b) - 1/2 \rceil\, i$ is also satisfactory. On the other hand, $s = \lfloor \mathrm{Re}\,(a/b) \rfloor + \lfloor \mathrm{Im}\,(a/b) \rfloor\, i$ dose not satisfy $\psi(a - sb) < \psi(b)$ in general, e.g., $a = 3 + 3i$ and $b = 4$.)

Because:

$$\mathrm{Re}(s) \leq \mathrm{Re}\left(\frac{a}{b}\right) + \frac{1}{2} < \mathrm{Re}(s) + 1 \quad \text{and} \quad \mathrm{Im}(s) \leq \mathrm{Im}\left(\frac{a}{b}\right) + \frac{1}{2} < \mathrm{Im}(s) + 1,$$

(16) deduces $|\mathrm{Re}(a/b) - \mathrm{Re}(s)| \leq 1/2$ and $|\mathrm{Im}(a/b) - \mathrm{Im}(s)| \leq 1/2$ of (4). Moreover, (16) is equivalent to the property on r, through the equation $a = sb + r$,

$$\left\lfloor \mathrm{Re}\left(\frac{r}{b}\right) + \frac{1}{2} \right\rfloor = \left\lfloor \mathrm{Im}\left(\frac{r}{b}\right) + \frac{1}{2} \right\rfloor = 0. \tag{17}$$

Then, s, r are unique because of the expression (16) on s. Alternatively, if $a = sb + r = s'b + r'$, then $0 = (s - s')b + (r - r')$ and it follows from $\left\lfloor \mathrm{Re}\left(\frac{r}{b}\right) + \frac{1}{2} \right\rfloor = \left\lfloor \mathrm{Re}\left(\frac{r'}{b}\right) + \frac{1}{2} \right\rfloor = 0$ that:

$$0 \leq \mathrm{Re}\left(\frac{r}{b}\right) + \frac{1}{2} < 1 \quad \text{and} \quad 0 \leq \mathrm{Re}\left(\frac{r'}{b}\right) + \frac{1}{2} < 1$$

and $-1 < \mathrm{Re}\left(\frac{r}{b}\right) - \mathrm{Re}\left(\frac{r'}{b}\right) = \mathrm{Re}(s' - s) < 1$ deduces $\mathrm{Re}(s' - s) = 0$, and similarly, $\mathrm{Im}(s' - s) = 0$.

Thus, we take (16) or (17) as "the additional property" to indicate unique quotient and remainder in Euclidean division in R. A numerical example is shown in Figure 1.

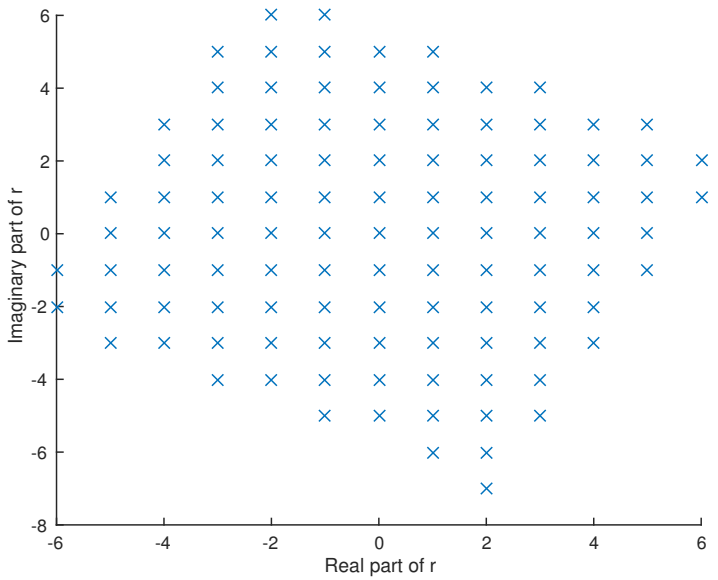

Figure 1. The remainders r of Euclidean division by $b = 5 + 9i$ in $\mathbb{Z}[i]$. There are $5^2 + 9^2 = 106 = |b|^2$ crosses, which can be all representatives of $\mathbb{Z}[i]/\langle b \rangle$, satisfying (17). If we adopt s with the ceiling function, then $r = -2 + 7i$ is included instead of $r = 2 - 7i$.

The case of $R = \mathbb{Z}[\omega]$. For $a, b \in R$ with $b \neq 0$, the results s, r of Euclidean division $a = sb + r$ with $\psi(r) < \psi(b)$ and $\psi(\cdot) = |\cdot|^2$ are not unique because $1 = 1 \cdot 2 - 1 = 0 \cdot 2 + 1$. Similarly to $\mathbb{Z}[i]$, we may decide s, r with $a = sb + r$ and $\psi(r) < \psi(b)$ by $s = \lfloor q_1 + 1/2 \rfloor + \lfloor q_2 + 1/2 \rfloor \omega$ if $a/b = q_1 + q_2\omega$, which is equivalent to $\lfloor t_1 + 1/2 \rfloor = \lfloor t_2 + 1/2 \rfloor = 0$ if $r/b = t_1 + t_2\omega$. (Similarly, $s = \lceil q_1 - 1/2 \rceil + \lceil q_2 - 1/2 \rceil \omega$ is also satisfactory.) However, unlike $\mathbb{Z}[i]$, we can decide s, r with $a = sb + r$ and $\psi(r) < \psi(b)$ by:

$$s = \lfloor q_1 \rfloor + \lfloor q_2 \rfloor \omega \quad \text{if} \quad \frac{a}{b} = q_1 + q_2\omega,\ q_1, q_2 \in \mathbb{Q}. \tag{18}$$

Because (18) deduces $0 \leq q_1 - \lfloor q_1 \rfloor < 1$ and $0 \leq q_2 - \lfloor q_2 \rfloor < 1$,

$$\psi(a - sb) = \left|\frac{a}{b} - s\right|^2 \psi(b) = \left\{(q_1 - \lfloor q_1 \rfloor)^2 - (q_1 - \lfloor q_1 \rfloor)(q_2 - \lfloor q_2 \rfloor) + (q_2 - \lfloor q_2 \rfloor)^2\right\} \psi(b) < \psi(b),$$

where the last inequality follows from the fact that $x^2 - xy + y^2$ takes the maximum on $0 \leq x, y \leq 1$ only at $(x, y) = (1, 0), (0, 1), (1, 1)$ and that, for $0 \leq x, y < 1$, $x^2 - xy + y^2 < 1$. Moreover, (18) is equivalent to the property on r, through the equation $a = sb + r$,

$$\lfloor t_1 \rfloor = \lfloor t_2 \rfloor = 0 \quad \text{if} \quad \frac{r}{b} = t_1 + t_2\omega,\ t_1, t_2 \in \mathbb{Q}. \tag{19}$$

Then, s, r are unique because of the expression (18) on s. Thus, we take (18) or (19) as "the additional property" to indicate unique quotient and remainder in Euclidean division in R. A numerical example is shown in Figure 2.

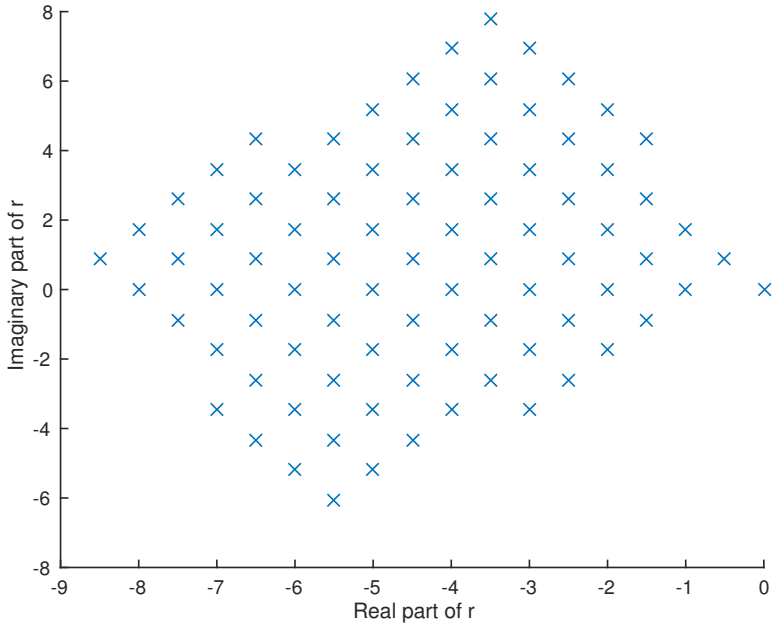

Figure 2. The remainders r of Euclidean division by $b = 2 + 10\omega$ in $\mathbb{Z}[\omega]$. There are $2^2 - 2 \cdot 10 + 10^2 = 84 = |b|^2$ crosses, which can be all representatives of $\mathbb{Z}[\omega]/\langle b \rangle$, satisfying (19).

The case of $R = \mathbb{Z}_p$. For $a, b \in R$ with $b \neq 0$, the results s, r of Euclidean division $a = sb + r$ with $\psi(r) < \psi(b)$ and $\psi(\cdot) = p^{\mathrm{ord}(\cdot)}$ or $\psi(0) = 0$ are not unique because $3 = 0 \cdot 2 + 3 = 1 \cdot 2 + 1$ for $p = 2$. Let $\mathbb{Q}_p$ be the field of fractions of R. For $c \in \mathbb{Q}_p$, there exists $w \in \mathbb{Z}$ such that $c = \sum_{h=w}^{\infty} c_h p^h$ with $c_h \in \{0, 1, \ldots, p-1\}$. For $c = \sum_{h=w}^{\infty} c_h p^h \in \mathbb{Q}_p$, we uniquely define $\{c\}_p = \sum_{h<0} c_h p^h \in \mathbb{Q}_p$ and

$\lfloor c \rceil_p = \sum_{h=0}^{\infty} c_h p^h \in \mathbb{Z}_p$ such that $c = \{c\}_p + \lfloor c \rceil_p$. Then, for $a, b \in R$ with $b \neq 0$, we decide $s, r \in R$ by $a = sb + r$ with $s = \lfloor a/b \rceil_p$. In other words, we have $a = sb + r$ with $\lfloor r/b \rceil_p = 0$ because:

$$s = \left\lfloor \frac{a}{b} \right\rceil_p \Longleftrightarrow \frac{r}{b} = \frac{a}{b} - s = \left\{ \frac{a}{b} \right\}_p \Longleftrightarrow \left\lfloor \frac{r}{b} \right\rceil_p = 0.$$

Moreover, $\lfloor r/b \rceil_p = 0$ implies $\psi(r) < \psi(b)$ because $r = b \{a/b\}_p$. Finally, we show the uniqueness of such s, r. Suppose that, for $a, b \in R$ with $b \neq 0$, $a = sb + r = s'b + r'$ and $\lfloor r/b \rceil_p = \lfloor r'/b \rceil_p = 0$. Then, from $0 = (s - s')b + (r - r')$, we say $c = (r - r')/b \in R$. In view of $r/b = \{r/b\}_p + \lfloor r/b \rceil_p = r'/b + c$, the uniqueness of $\{r/b\}_p$ and $\lfloor r/b \rceil_p$ implies that $\{r/b\}_p = r'/b$ and $\lfloor r/b \rceil_p = c = 0$.

The case of $R = K[[x]]$. For $a, b \in R$ with $b \neq 0$, the results s, r of Euclidean division $a = sb + r$ with $\psi(r) < \psi(b)$ are not unique because $1 = 0 \cdot x + 1 = 1 \cdot x + x + 1$ for $K = \mathbb{F}_2$ and $\psi(\cdot) = 2^{\mathrm{ord}(\cdot)}$ or $\psi(0) = 0$. Let $K((x))$ be the field of fractions of R. For $c \in K((x))$, there exists $w \in \mathbb{Z}$ such that $c = \sum_{h=w}^{\infty} c_h x^h$ with $c_h \in K$. For $c = \sum_{h=w}^{\infty} c_h x^h \in K((x))$, we uniquely define $\{c\}_K = \sum_{h<0} c_h x^h \in K((x))$ and $\lfloor c \rceil_K = \sum_{h=0}^{\infty} c_h x^h \in R$ such that $c = \{c\}_K + \lfloor c \rceil_K$. Then, for $a, b \in R$ with $b \neq 0$, we decide $s, r \in R$ by $a = sb + r$ with $s = \lfloor a/b \rceil_K$. In other words, we have $a = sb + r$ with $\lfloor r/b \rceil_K = 0$ because:

$$s = \left\lfloor \frac{a}{b} \right\rceil_K \Longleftrightarrow \frac{r}{b} = \frac{a}{b} - s = \left\{ \frac{a}{b} \right\}_K \Longleftrightarrow \left\lfloor \frac{r}{b} \right\rceil_K = 0.$$

Moreover, $\lfloor r/b \rceil_K = 0$ implies $\psi(r) < \psi(b)$ because $r = b \{a/b\}_K$. The uniqueness of such s, r can be shown similarly to the case of $R = \mathbb{Z}_p$.

Hereafter, we denote the quotient field of R by $Q(R) = \{a/b \mid a, b \in R, b \neq 0\}$. For any $a/b \in Q(R)$, $a, b \in R$ with $\gcd(a, b) = 1$ are uniquely determined up to units because $0 = a/b - a'/b' = (ab' - a'b)/bb'$ implies $\langle a \rangle = \langle a' \rangle$ and $\langle b \rangle = \langle b' \rangle$.

Definition 3. *For $a \in Q(R)$, we define $[\![a]\!] \in R$ by*

$$[\![a]\!] = \begin{cases} s \text{ if } a = r/b + s \text{ and } \deg(r) < \deg(b) & R = K[x] \\ \lfloor a \rceil & R = \mathbb{Z} \\ \lfloor \mathrm{Re}\,(a) + 1/2 \rfloor + \lfloor \mathrm{Im}\,(a) + 1/2 \rfloor\, i & R = \mathbb{Z}[i] \\ \lfloor q_1 \rfloor + \lfloor q_2 \rfloor\, \omega \text{ if } a = q_1 + q_2\omega,\ q_1, q_2 \in \mathbb{Q} & R = \mathbb{Z}[\omega] \\ \lfloor a \rceil_p & R = \mathbb{Z}_p \\ \lfloor a \rceil_K & R = K[[x]]. \end{cases}$$

In the case of $R = K[x]$, this definition is well-defined because, if $a = r/b + s = r'/b' + s'$ with $r, b, s, r', b', s' \in R$, $b, b' \neq 0$, $\deg(r) < \deg(b)$, and $\deg(r') < \deg(b')$, then $(rb' - r'b)/bb' + s - s' = 0$ and $\deg(rb' - r'b) \leq \max\{\deg(rb'), \deg(r'b)\} < \deg(bb')$ deduce $s = s'$.

Lemma 2. *For any $a, a' \in Q(R)$, if $[\![a]\!] = [\![a']\!] = 0$ and $a - a' \in R$, then $a = a'$.*

Proof. In the case of $R = K[x]$, let $a = r/b$ and $a' = r'/b'$ with $r, b, r', b' \in R$, $b, b' \neq 0$, $\deg(r) < \deg(b)$, and $\deg(r') < \deg(b')$. Then, $a - a' = (rb' - r'b)/bb' \in R$ deduces $a = a'$. The other cases follow from the argument in each case. □

Hereafter, for $a, b \in R$ with $b \neq 0$, the quotient s and the remainder r of the Euclidean division $a = sb + r$ with $\psi(r) < \psi(b)$ are determined uniquely such that $s = [\![a/b]\!]$, or equivalently, $[\![r/b]\!] = 0$. Note that $\psi(r) < \psi(b)$ follows from $[\![r/b]\!] = 0$.

Proposition 6. *Let $G = (g_{i,j}) \in M_l(R)$ be upper triangular. Then, for any $a = (a_1 \ \dots \ a_l) \in \mathbb{L}$, there exist unique $s = (s_1 \ \dots \ s_l), r = (r_1 \ \dots \ r_l) \in \mathbb{L}$ such that $a = sG + r$, i.e.,*

$$(a_1 \ \dots \ a_l) = (s_1 \ \dots \ s_l)\, G + (r_1 \ \dots \ r_l),$$

with $[\![r_i/g_{i,i}]\!] = 0$ for all $1 \le i \le l$. In other words, the result of the division in Proposition 2 is unique.

Proof. Suppose that $s, s', r, r' \in \mathbb{L}$ satisfy $a = sG + r = s'G + r'$ and $[\![r_i/g_{i,i}]\!] = [\![r'_i/g_{i,i}]\!] = 0$ for all $1 \le i \le l$. Then, subtracting one expression for a from the other, we obtain $(0 \ \dots \ 0) = (s - s')G + (r - r')$, which is equivalent to $0 = \sum_{h=1}^{i}(s_h - s'_h)g_{h,i} + (r_i - r'_i)$ for all $1 \le i \le l$. For $i = 1$, we have $0 = (s_1 - s'_1)g_{1,1} + (r_1 - r'_1)$, which deduces $s_1 - s'_1 = r_1 - r'_1 = 0$ by Lemma 2. Supposing $s_h - s'_h = r_h - r'_h = 0$ for all $h = 1, \dots, i-1$, we have $0 = (s_i - s'_i)g_{i,i} + (r_i - r'_i)$, which deduces $s_i - s'_i = r_i - r'_i = 0$ by Lemma 2. By induction on i, we obtain $s - s' = r - r' = (0 \ \dots \ 0)$, which completes the proof. □

*Reduced Generator Matrices of **R**-Modules in $\mathcal{M}$*

Definition 4. *For $a \in R$, we say that a is monic if and only if $a \neq 0$ and a satisfies the following condition:*

$$\begin{cases} a_w = 1 \ \text{ if } \ a = \sum_{h=0}^{w} a_h x^h, \ \deg(a) = w & R = K[x] \\ a > 0 & R = \mathbb{Z} \\ \mathrm{Re}(a) > 0, \ \mathrm{Im}(a) \ge 0 & R = \mathbb{Z}[i] \\ a_1 > 0, \ a_2 \ge 0 \ \text{ if } \ a = a_1 + a_2\omega, \ a_1, a_2 \in \mathbb{Z} & R = \mathbb{Z}[\omega] \\ a_w = 1 \ \text{ if } \ a = \sum_{h=w}^{\infty} a_h p^h, \ \mathrm{ord}(a) = w & R = \mathbb{Z}_p \\ a_w = 1 \ \text{ if } \ a = \sum_{h=w}^{\infty} a_h x^h, \ \mathrm{ord}(a) = w & R = K[[x]]. \end{cases}$$

If $ea = a'$ for $e, a, a' \in R$ with monic a, a' and invertible e, then we have $e = 1$ and $a = a'$.

Definition 5. *We say that $G = (g_{i,j}) \in M_l(R)$ is reduced if and only if G is upper triangular, $g_{i,i}$ is monic for all $1 \le i \le l$ and $[\![g_{i,j}/g_{j,j}]\!] = 0$ for all $1 \le i < j \le l$.*

If a generator matrix G of $\mathcal{C}$ is given, then the reduced generator matrix $\widetilde{G}$ with $\mathbb{L}G = \mathbb{L}\widetilde{G}$ is obtained through the row operations for G, cf. [14]. In fact, the result of the row operations is written as $\widetilde{G} = EG$ for some $E \in GL_l(R)$.

Example 5. *(Continued from Example 1.)* $G_2 = \begin{pmatrix} 2+i & 1+3i \\ 0 & 5 \end{pmatrix}$ *is not reduced because* $\lfloor \mathrm{Re}\,((1+3i)/5) + 1/2 \rfloor = 0$ *and* $\lfloor \mathrm{Im}\,((1+3i)/5) + 1/2 \rfloor = 1$. *From* $1 + 3i - i \cdot 5 = 1 - 2i$, $\begin{pmatrix} 1 & -i \\ 0 & 1 \end{pmatrix} G_2 = \begin{pmatrix} 2+i & 1-2i \\ 0 & 5 \end{pmatrix}$ *is reduced.*

In the case where $R = \mathbb{Z}$, the reduced $\widetilde{G}$ of G is called the Hermite normal form of G, which is unique for each R-module $\mathbb{L}G$, according to Theorem 4.2 in [11]. Here, we prove the uniqueness of the reduced generator matrix in the cases of Euclidean domains with unique Euclidean division.

Proposition 7. *There exists a unique reduced generator matrix of each $\mathcal{C}$.*

Proof. Let $G = (g_{i,j}), G' = (g'_{i,j})$ be two reduced generator matrices of $\mathcal{C}$. Then, it follows from $\mathbb{L}G = \mathbb{L}G'$ that there exists an upper triangular $E = (e_{i,j}) \in GL_l(R)$ such that $EG = G'$. Note that:

$$EG = G' \Longleftrightarrow \sum_{i \le k \le j} e_{i,k} g_{k,j} = g'_{i,j} \text{ for all } 1 \le i \le j \le l.$$

Then, $e_{i,i}$ is invertible in R for all $1 \le i \le l$ because $\det(E) = \prod_{i=1}^{l} e_{i,i}$ is invertible in R. If $i = j$, then $e_{i,i} g_{i,i} = g'_{i,i}$ implies that $e_{i,i} = 1$ and $g_{i,i} = g'_{i,i}$ because $g_{i,i}$ and $g'_{i,i}$ are monic. If $i + 1 = j$, then:

$$g_{i,i+1} + e_{i,i+1} g_{i+1,i+1} = g'_{i,i+1}.$$

Because of $g_{i+1,i+1} = g'_{i+1,i+1}$, $[\![g_{i,i+1} / g_{i+1,i+1}]\!] = [\![g'_{i,i+1} / g'_{i+1,i+1}]\!] = 0$, and Lemma 2, we have $e_{i,i+1} = 0$ and $g_{i,i+1} = g'_{i,i+1}$. If $e_{i,i+1} = \cdots = e_{i,j-1} = 0$, then:

$$\sum_{i \le k \le j} e_{i,k} g_{k,j} = g_{i,j} + e_{i,j} g_{j,j} = g'_{i,j}.$$

Because of $g_{j,j} = g'_{j,j}$, $[\![g_{i,j} / g_{j,j}]\!] = [\![g'_{i,j} / g'_{j,j}]\!] = 0$, and Lemma 2, we have $e_{i,j} = 0$ and $g_{i,j} = g'_{i,j}$. It follows from induction on j that $G = G'$, which completes the proof. □

Example 6. *(Continued from Remark 2.) Let $R = \mathbb{Z}$, $l = 2$, $u = 6$, $u_1 = 2$, and $u_2 = 3$. Then, $|\{G_1\}_2| = 5$ and $|\{G_2\}_3| = 6$ are explicitly given as:*

$$\{G_1\}_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\},$$

$$\{G_2\}_3 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \right\}.$$

Thus, all G with $|\{G\}_6| = 30$ can be obtained by $G_1 G_2$. Although $G_1 G_2$ is not always reduced, e.g., $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix}$, we can find $E \in GL_l(R)$ such that $E G_1 G_2$ is reduced.

Example 7. *In [15], an ideal generated by $g(x) = x^3 + \lambda x^2 + (\lambda - 1)x - 1$ in a ring $\mathbb{Z}_2[x]/(x^7 - 1)$ is considered, where $g(x)$ divides $x^7 - 1$ in $\mathbb{Z}_2[x]$ and $\lambda = 2 + 2^2 + 2^5 + 2^7 + 2^8 + \cdots \in \mathbb{Z}_2$ is a root of $\lambda^2 - \lambda + 2 = 0$. This ideal is called the two-adic lift of the binary [7,4] Hamming code because $g(x) \equiv x^3 + x + 1 \bmod 2$ agrees with its generator polynomial. Moreover, it is pointed out that $\mathbb{Z}_2$-module $(\mathbb{Z}_2)^4 U \subset (\mathbb{Z}_2)^8$, where:*

$$U = \begin{pmatrix} 1 & \lambda & \lambda - 1 & -1 & 0 & 0 & 0 & 1 \\ 0 & 1 & \lambda & \lambda - 1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 1 & \lambda & \lambda - 1 & -1 & 0 & 1 \\ 0 & 0 & 0 & 1 & \lambda & \lambda - 1 & -1 & 1 \end{pmatrix},$$

can be called a self-dual code over $\mathbb{Z}_2$ because $U\,({}^t U)$ is all-zero, where ${}^t U$ denotes the transpose matrix of U. Then, there exists $E_1 \in GL_4(\mathbb{Z}_2)$ such that:

$$E_1 U = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & -\lambda & 1 - \lambda & -1 \\ 0 & 1 & 0 & 0 & 1 - \lambda & 1 & 1 & -\lambda \\ 0 & 0 & 1 & 0 & 1 & 1 & \lambda & 1 - \lambda \\ 0 & 0 & 0 & 1 & \lambda & \lambda - 1 & -1 & 1 \end{pmatrix}.$$

We say $E_1U = [I \mid V]$ *for* $V \in M_4(\mathbb{Z}_2)$. *Note that* $A_1G_1 = \mathrm{diag}\left[2^b, \ldots, 2^b\right]$ *holds for any positive* $b \in \mathbb{Z}$, *where* $A_1 = \left(\begin{array}{c|c} 2^bI & -V \\ \hline 0 & I \end{array}\right)$ *and* $G_1 = \left(\begin{array}{c|c} I & V \\ \hline 0 & 2^bI \end{array}\right)$. *Then, various notable codes appear as the image of* $(\mathbb{Z}_2)^4 U$ *by* $F : (\mathbb{Z}_2)^8 \to \left(\mathbb{Z}_2/2^b\mathbb{Z}_2\right)^8$, *where* $\mathbb{Z}_2/2^b\mathbb{Z}_2 = \mathbb{Z}/2^b\mathbb{Z}$, *and Proposition 7 assures that their unique reduced generator matrices can be computed from* E_2G_1 *for some* $E_2 \in GL_8(\mathbb{Z}_2)$. *For example, If* $b = 1$, *then* $\mathcal{C} = F\left((\mathbb{Z}_2)^4 U\right)$ *is equal to the binary [8,4] extended Hamming code and there exists* $A_2 \in M_8(\mathbb{Z})$ *such that its unique reduced generator matrix* G_2 *satisfies* $A_2G_2 = \mathrm{diag}[2, \ldots, 2]$, *where:*

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

If $b = 2$, *then* $\mathcal{C} = F\left((\mathbb{Z}_2)^4 U\right)$ *is equal to the octacode, cf. [15], and there exists* $A_3 \in M_8(\mathbb{Z})$ *such that its unique reduced generator matrix* G_3 *satisfies* $A_3G_3 = \mathrm{diag}[4, \ldots, 4]$, *where:*

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 2 & 3 & 3 \\ 0 & 1 & 0 & 0 & 3 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 2 & 1 & 3 & 1 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}.$$

7. Application to Hecke Rings

In this section, we continue to focus on the Euclidean domain R described above. Furthermore, if $R = K[x]$ or $R = K[[x]]$, then we take $K = \mathbb{F}_q$. Under these assumptions, for all $b \in R$ with $b \neq 0$, $\psi(b) = |R/\langle b\rangle|$ has a positive finite value in $\mathbb{Z}$.

7.1. Preliminaries on Hecke Rings

We define:

$$H(\Gamma, \Delta) = \left\{ \sum_{\alpha \in \Delta} c_\alpha \Gamma \alpha \Gamma \;\middle|\; c_\alpha \in \mathbb{Z},\ c_\alpha \neq 0 \text{ for finite number of } \alpha \in \Delta \right\},$$

where $\Gamma = GL_l(R)$ and $\Delta = \{\alpha \in M_l(R) \mid \det(\alpha) \neq 0\}$. We call $H(\Gamma, \Delta)$ a Hecke ring [12,13] with respect to Γ and Δ with a commutative multiplication (cf. the next subsection) and a unit $\Gamma I \Gamma = \Gamma$.

Hereafter, for two R-modules $\mathcal{A}$ and $\mathcal{B}$, we write $\mathcal{A} \simeq \mathcal{B}$ if $\mathcal{A}$ is isomorphic to $\mathcal{B}$ as R-modules. The theory of elementary divisors [14] asserts that, for $\alpha \in \Delta$, $\Gamma\alpha\Gamma = \Gamma\mathrm{diag}[a_1, \ldots, a_l]\Gamma$ for unique $\langle a_1\rangle \supset \cdots \supset \langle a_l\rangle$ with $a_1, \ldots, a_l \in R$. Then, we denote $T(a_1, \ldots, a_l) = \Gamma\alpha\Gamma$. Let $\beta \in \Delta$ and $T(b_1, \ldots, b_l) = \Gamma\beta\Gamma$. We note that:

$$\begin{aligned}\Gamma\alpha\Gamma = \Gamma\beta\Gamma &\Longleftrightarrow \mathbb{L}\alpha = \mathbb{L}\beta\gamma \text{ for some } \gamma \in \Gamma \\ &\Longleftrightarrow \langle a_1\rangle = \langle b_1\rangle, \ldots, \langle a_l\rangle = \langle b_l\rangle \\ &\Longleftrightarrow \mathbb{L}/\mathbb{L}\alpha \simeq \mathbb{L}/\mathbb{L}\beta \end{aligned} \tag{20}$$

because $\Gamma\alpha\Gamma = T(a_1, \ldots, a_l) \Longleftrightarrow \mathbb{L}/\mathbb{L}\alpha \simeq \bigoplus_{i=1}^{l} R/\langle a_i\rangle$. On the other hand, so far, we have frequently used the fact that:

$$\Gamma\alpha = \Gamma\beta \Longleftrightarrow \mathbb{L}\alpha = \mathbb{L}\beta. \tag{21}$$

Remark 3. *Let $\mathcal{C}, \mathcal{D} \subset \mathbb{L}/u\mathbb{L}$ be R-modules. Then, $\mathcal{C} \simeq \mathcal{D}$ as R-modules does not in general mean $\mathcal{C} = \mathcal{D}$ as sets. For example, in the case of $\mathbb{L} = \mathbb{F}_2[x]^2$, consider three different G of $\{G\}_x$, i.e.,*

$$AG = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} x & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} = xI.$$

Because these three A are in $\Gamma\mathrm{diag}[1, x]\Gamma$, and we have:

$$\frac{\mathbb{L}G}{u\mathbb{L}} = \frac{\mathbb{L}G}{\mathbb{L}AG} \simeq \frac{\mathbb{L}}{\mathbb{L}A},$$

it follows from (20) that three R-modules $\mathbb{L}G/x\mathbb{L}$ are all isomorphic R-modules. On the other hand, because $\mathbb{L}/x\mathbb{L} = (\mathbb{F}_2)^2$, three R-modules $\mathbb{L}G/x\mathbb{L}$ have two elements and equal:

$$\{(0\,0), (1\,0)\},\ \{(0\,0), (1\,1)\},\ \{(0\,0), (0\,1)\},$$

respectively. Note that their values of the minimum Hamming distance are 1, 2 and 1, respectively.

This example shows that isomorphic R-modules could have distinct values of the minimum Hamming distance.

Lemma 3. *For all $\alpha \in \Delta$, if $\Gamma\alpha\Gamma = T(a_1, \ldots, a_l)$, then we have $\mathbb{L}\alpha \supset a_l\mathbb{L} \supset \det(\alpha)\mathbb{L}$.*

Proof. Let $\iota : \mathbb{L}/\mathbb{L}\alpha \to \bigoplus_{i=1}^{l} R/\langle a_i\rangle$ be the isomorphism of R-modules. Because $\iota(a_l r) = a_l\iota(r) = (0 \ldots 0) \in \bigoplus_{i=1}^{l} R/\langle a_i\rangle$, $a_l r \in \mathbb{L}\alpha$ for all $r \in \mathbb{L}$. Thus, we have $\mathbb{L}\alpha \supset a_l\mathbb{L}$. On the other hand, $\Gamma\alpha\Gamma = T(a_1, \ldots, a_l)$ implies that $\gamma_1\alpha\gamma_2 = \mathrm{diag}[a_1, \ldots, a_l]$ for some $\gamma_1, \gamma_2 \in \Gamma$. Then, $\det(\alpha) = \epsilon\prod_{i=1}^{l} a_i$ with a unit ϵ implies $a_l\mathbb{L} \supset \det(\alpha)\mathbb{L}$. □

Because Γ acts from the left on Δ, we can consider a quotient set $\Gamma\backslash\Delta$ similarly to (12). Let T_l denote a complete system of representatives of $\Gamma\backslash\Delta$. As one choice of T_l, we can take:

$$T_l = \{G \in M_l(R) \mid G \text{ is reduced}\}.$$

Let $\Gamma\alpha\Gamma = \biguplus_k \Gamma\alpha_k$ be the disjoint decomposition into the left cosets, where the number of the left cosets is actually finite as shown now. In view of (20) and (21), there exists a one-to-one correspondence:

$$\left\{\alpha_k \,\middle|\, \Gamma\alpha\Gamma = \biguplus_k \Gamma\alpha_k\right\} \longrightarrow \{G \in T_l \mid \mathbb{L}/\mathbb{L}G \simeq \mathbb{L}/\mathbb{L}\alpha\}$$

by $\alpha_k \mapsto \gamma\alpha_k \in T_l$ for some $\gamma \in \Gamma$. Thus, the disjoint decomposition $\Gamma\alpha\Gamma = \biguplus_k \Gamma\alpha_k$ has a finite number of cosets because Lemma 3 deduces that $AG = a_l I$ for some $A \in M_l(R)$ and there exists a finite number of $G \in T_l$ such that $AG = a_l I$. Hereafter, we denote:

$$T_l(\alpha) = \{G \in T_l \mid \mathbb{L}/\mathbb{L}G \simeq \mathbb{L}/\mathbb{L}\alpha\},$$

which is equivalent to, in the notation of Section 5,

$$T_l(\alpha) = \{G \in \{G\}_{a_l} \mid \mathbb{L}/\mathbb{L}G \simeq \mathbb{L}/\mathbb{L}\alpha\} = \left\{G \in \{G\}_{\det(\alpha)} \,\middle|\, \mathbb{L}/\mathbb{L}G \simeq \mathbb{L}/\mathbb{L}\alpha\right\}.$$

Hereafter, for a finite set S, we also use $\#S = |S|$ to denote the number of elements in S. Then, we define:

$$\mathrm{ind}\,(\Gamma\alpha\Gamma) = \#T_l(\alpha) \quad \text{and} \quad \mathrm{ind}\left(\sum_{\alpha\in\Delta} c_\alpha \Gamma\alpha\Gamma\right) = \sum_{\alpha\in\Delta} c_\alpha \mathrm{ind}\,(\Gamma\alpha\Gamma)$$

for all $\sum_{\alpha\in\Delta} c_\alpha\Gamma\alpha\Gamma \in H(\Gamma,\Delta)$. It is shown (cf. the next subsection) that $\mathrm{ind}(\cdot)$ ($\deg(\cdot)$ in [13]) is a ring homomorphism of $H(\Gamma,\Delta)$.

7.2. Multiplication in Hecke Rings

There exists finite disjoint decomposition $\Gamma\alpha\Gamma\beta\Gamma = \biguplus_\xi \Gamma\xi\Gamma$ because we have:

$$\Gamma\alpha\Gamma = \biguplus_i \Gamma\alpha_i, \qquad \Gamma\beta\Gamma = \biguplus_j \Gamma\beta_j,$$

and moreover:

$$\Gamma\alpha\Gamma\beta\Gamma = \bigcup_j \Gamma\alpha\Gamma\beta_j = \bigcup_{i,j} \Gamma\alpha_i\beta_j.$$

Then, we define the multiplication $\cdot$ in $H(\Gamma,\Delta)$ by:

$$\Gamma\alpha\Gamma\cdot\Gamma\beta\Gamma = \sum_\xi m_\xi(\alpha,\beta)\,\Gamma\xi\Gamma \in H(\Gamma,\Delta)$$

where:

$$m_\xi(\alpha,\beta) = \#\left\{(i,j) \mid \Gamma\alpha_i\beta_j = \Gamma\xi\right\} = \#\left\{(G_1,G_2) \in T_l(\alpha)\times T_l(\beta) \mid \mathbb{L}G_1G_2 = \mathbb{L}\xi\right\}. \tag{22}$$

We note:

$$\begin{aligned} m_\xi(\alpha,\beta) &= \#\left\{G_2 \in T_l(\beta) \mid \mathbb{L}G_2/\mathbb{L}\xi \simeq \mathbb{L}/\mathbb{L}\alpha\right\} &(23)\\ &= \#\left\{G \in T_l \mid \mathbb{L}/\mathbb{L}G \simeq \mathbb{L}/\mathbb{L}\beta,\ \mathbb{L}G/\mathbb{L}\xi \simeq \mathbb{L}/\mathbb{L}\alpha\right\} &(24)\end{aligned}$$

because $\mathbb{L}G_1G_2 = \mathbb{L}\xi$ deduces $\mathbb{L}G_2/\mathbb{L}\xi = \mathbb{L}G_2/\mathbb{L}G_1G_2 \simeq \mathbb{L}/\mathbb{L}G_1 \simeq \mathbb{L}/\mathbb{L}\alpha$ and $(G_1,G_2) \mapsto G_2$ and $G_2 \mapsto (\xi G_2^{-1}, G_2)$ determine the bijections between the sets in (22) and (23). Then, $m_\xi(\alpha,\beta)$ does not depend on the choices of $\{\alpha_i\}$, $\{\beta_j\}$, and $\{\xi\}$ and the operation $\cdot$ defines the multiplication; moreover, this multiplication is commutative, cf. [13].

There is another formula $\#\left\{(i,j) \mid \Gamma\alpha_i\beta_j\Gamma = \Gamma\xi\Gamma\right\} = m_\xi(\alpha,\beta)\,\mathrm{ind}\,(\Gamma\xi\Gamma)$ because:

$$\begin{aligned}
&\#\left\{(i,j) \mid \Gamma\alpha_i\beta_j\Gamma = \Gamma\xi\Gamma\right\} = \#\left\{(G_1,G_2) \in T_l(\alpha)\times T_l(\beta) \mid \mathbb{L}/\mathbb{L}G_1G_2 \simeq \mathbb{L}/\mathbb{L}\xi\right\}\\
&= \#\left\{(G_1,G_2) \in T_l(\alpha)\times T_l(\beta) \mid \mathbb{L}G_1G_2 = \mathbb{L}\xi\gamma \text{ for some } \gamma\in\Gamma\right\}\\
&= \sum_{k=1}^m \#\left\{(G_1,G_2) \in T_l(\alpha)\times T_l(\beta) \mid \mathbb{L}G_1G_2 = \mathbb{L}\xi_k\right\} \quad \text{if} \quad \Gamma\xi\Gamma = \biguplus_{k=1}^m \Gamma\xi_k\\
&= \#\left\{(G_1,G_2) \in T_l(\alpha)\times T_l(\beta) \mid \mathbb{L}G_1G_2 = \mathbb{L}\xi\right\} \sum_{k=1}^m 1 = m_\xi(\alpha,\beta)\,\mathrm{ind}\,(\Gamma\xi\Gamma).
\end{aligned}$$

Then, the fact that $\mathrm{ind}(\cdot)$ is a ring homomorphism of $H(\Gamma,\Delta)$ follows from:

$$\mathrm{ind}\,(\Gamma\alpha\Gamma\cdot\Gamma\beta\Gamma)=\sum_{\xi}m_{\xi}(\alpha,\beta)\,\mathrm{ind}\,(\Gamma\xi\Gamma)=\#\{\text{all }(i,j)\}=\mathrm{ind}\,(\Gamma\alpha\Gamma)\cdot\mathrm{ind}\,(\Gamma\beta\Gamma)\,.$$

Note that, if $\xi\in\Gamma\alpha\Gamma\beta\Gamma$, then we have $\mathrm{ind}\,(\Gamma\xi\Gamma)>0$ and:

$$\mathrm{ind}\,(\Gamma\xi\Gamma)\le\mathrm{ind}\,(\Gamma\alpha\Gamma\cdot\Gamma\beta\Gamma)=\mathrm{ind}\,(\Gamma\alpha\Gamma)\cdot\mathrm{ind}\,(\Gamma\beta\Gamma)\,. \tag{25}$$

Proposition 8. *For $\alpha,\beta\in\Delta$, suppose that $\gcd(\det(\alpha),\det(\beta))=1$. Then, we have $\Gamma\alpha\Gamma\cdot\Gamma\beta\Gamma=\Gamma\alpha\beta\Gamma$, in other words,*

$$T(a_1,\ldots,a_l)T(b_1,\ldots,b_l)=T(a_1b_1,\ldots,a_lb_l)$$

if $\Gamma\alpha\Gamma=T(a_1,\ldots,a_l)$ and $\Gamma\beta\Gamma=T(b_1,\ldots,b_l)$.

Proof. For $(G_1,G_2)\in T_l(\alpha)\times T_l(\beta)$, there exists an exact sequence:

$$0\to\frac{\mathbb{L}G_2}{\mathbb{L}G_1G_2}\to\frac{\mathbb{L}}{\mathbb{L}G_1G_2}\to\frac{\mathbb{L}}{\mathbb{L}G_2}\to 0.$$

Moreover, we have $\frac{\mathbb{L}G_2}{\mathbb{L}G_1G_2}\simeq\frac{\mathbb{L}}{\mathbb{L}G_1}\simeq\bigoplus_{i=1}^{l}R/\langle a_i\rangle$ and $\frac{\mathbb{L}}{\mathbb{L}G_2}\simeq\bigoplus_{i=1}^{l}R/\langle b_i\rangle$, and we say $\frac{\mathbb{L}}{\mathbb{L}G_1G_2}\simeq\bigoplus_{i=1}^{l}R/\langle c_i\rangle$. Then, there exist exact sequences $0\to R/\langle a_i\rangle\to R/\langle c_i\rangle\to R/\langle b_i\rangle\to 0$ for all $1\le i\le l$. It follows from the uniqueness of elementary divisors that $\langle c_i\rangle=\langle a_ib_i\rangle$ for all $1\le i\le l$. Thus, we deduce $\frac{\mathbb{L}}{\mathbb{L}G_1G_2}\simeq\bigoplus_{i=1}^{l}R/\langle a_ib_i\rangle$. In particular, if $(G_1,G_2)=(\alpha,\beta)$, then $\frac{\mathbb{L}}{\mathbb{L}\alpha\beta}\simeq\bigoplus_{i=1}^{l}R/\langle a_ib_i\rangle$. Hence, $G_1G_2\in T_l(\alpha\beta)$. Moreover, it follows from Theorem 2 that $(G_1,G_2)\mapsto G_1G_2$ is an injective map $T_l(\alpha)\times T_l(\beta)\to T_l(\alpha\beta)$. Thus, $\mathrm{ind}(\Gamma\alpha\Gamma)\cdot\mathrm{ind}(\Gamma\beta\Gamma)=\#T_l(\alpha)\times\#T_l(\beta)\le\#T_l(\alpha\beta)=\mathrm{ind}(\Gamma\alpha\beta\Gamma)$. Together with (25), we have $\mathrm{ind}(\Gamma\alpha\Gamma)\cdot\mathrm{ind}(\Gamma\beta\Gamma)=\mathrm{ind}(\Gamma\alpha\beta\Gamma)$, which shows that $m_{\alpha\beta}(\alpha,\beta)=1$ and $\Gamma\alpha\Gamma\cdot\Gamma\beta\Gamma=\Gamma\alpha\beta\Gamma$. □

7.3. A Generating Function of ind $(T(f))$

For a nonzero $f\in R$, define:

$$T(f)=\sum_{\alpha\in\Delta,\,\det(\alpha)=f}\Gamma\alpha\Gamma\in H(\Gamma,\Delta),$$

where the sum runs over all distinct $\Gamma\alpha\Gamma$ with $\alpha\in\Delta$ and $\det(\alpha)=f$. Let $\mathcal{M}=(R/\langle f\rangle)^l=\mathbb{L}/f\mathbb{L}$.

Then, we have:

$$\begin{aligned}\mathrm{ind}(T(f))&=\#\left\{G\in T_l\;\middle|\;\mathbb{L}/\mathbb{L}G\simeq\bigoplus_{i=1}^{l}R/\langle b_i\rangle\text{ for some }\langle b_1\rangle\supset\cdots\supset\langle b_l\rangle\text{ with }\prod_{i=1}^{l}b_i=f\right\}\\&=\#\{G\in T_l\mid\deg(G)=f\}.\end{aligned} \tag{26}$$

By Proposition 8 and (26), for nonzero $f,g\in R$ with $\gcd(f,g)=1$, we have $T(fg)=T(f)T(g)$. We say that $\pi\in R$ is a prime element if $\langle ab\rangle\subset\langle\pi\rangle$ implies $\langle a\rangle\subset\langle\pi\rangle$ or $\langle b\rangle\subset\langle\pi\rangle$ for all $a,b\in R$. Because a Euclidean domain R is a principal ideal domain, π is a prime element if and only if $\langle\pi\rangle$ is a maximal ideal. Moreover, all nonzero $f\in R$ has a prime factorization $f=\epsilon\prod_{i=1}^{s}\pi_i^{e_i}$, where ϵ denotes a unit, π_i is a prime element, and $e_i\in\mathbb{Z}$ is positive and unique for all $1\le i\le s$.

Thus, we can compute ind $(T(f))$ by calculating ind $(T(\pi^e))$ for each prime power factor $\pi^e \,||\, f$, where $\pi^e \,||\, f$ means $\langle f\rangle \subset \langle \pi^e\rangle$ but $\langle f\rangle \not\subset \langle \pi^{e+1}\rangle$ for a positive $e \in \mathbb{Z}$. For $\pi^e \,||\, f$, we have:

$$T(\pi^e) = \sum_{\substack{0\le d_1\le\cdots\le d_l\\ d_1+\cdots+d_l=e}} T\left(\pi^{d_1},\ldots,\pi^{d_l}\right).$$

Lemma 4. *Let $\pi \in R$ be a nonzero prime element. For $A=(a_{i,j})$, $G=(g_{i,j}) \in M_l(R)$, if $AG=\pi I$ with the reduced G, then $g_{i,i}=\pi$ implies $a_{i,j}=g_{i,j}=0$ for all $1\le i\ne j\le l$. Conversely, if a reduced $G=(g_{i,j})\in M_l(R)$ satisfies $g_{i,i}=1$ or π for all $1\le i\le l$ and $g_{i,i}=\pi$ implies $g_{i,j}=0$ for all $1\le i\ne j\le l$, then there exists $A\in M_l(R)$ such that $AG=\pi I$.*

Proof. By the assumption, A and G are upper triangular. If $g_{i,i}=\pi$ and $i<j$, then $AG=\pi I$ implies $\sum_{h=i}^{j} a_{i,h}g_{h,j}=0$, $a_{i,i}=1$, and $g_{j,j}=1$ or π. Supposing $j=i+1$, we have $g_{i,j}+a_{i,j}g_{j,j}=0$. In both cases of $g_{j,j}=1$ and π, the reduced condition implies $g_{i,j}=0$ and $a_{i,j}=0$. Suppose the induction hypothesis $a_{i,h}=g_{i,h}=0$ for all $i<h<j$. Then, we have $g_{i,j}+a_{i,j}g_{j,j}=0$. In both cases of $g_{j,j}=1$ and π, the reduced condition implies $g_{i,j}=a_{i,j}=0$.

On the other hand, from the assumption of G, there exists $E\in GL_l(R)$ such that GE is diagonal. Then, we put $A'=(GE)^{-1}\pi I \in M_l(R)$. Thus, $(GE)A'=G(EA')=(EA')G=\pi I$ with $EA'\in M_l(R)$. □

We denote $T_k^{(l)}=T(\overbrace{1,\ldots,1}^{l-k},\overbrace{\pi,\ldots,\pi}^{k})\in H(\Gamma,\Delta)$.

Remark 4. *Let the notation be as in Lemma 4. Let $r=|R/\langle\pi\rangle|=\psi(\pi)$. We will show:*

$$\text{ind}\left(T_k^{(l)}\right)=\sum_{1\le j_1<\cdots<j_k\le l} r^{(j_1-1)+\cdots+(j_k-k)}=r^{-k(k-1)/2}\sum_{0\le i_1<\cdots<i_k\le l-1} r^{i_1+\cdots+i_k}. \tag{27}$$

Note that:

$$\text{ind}\left(T_k^{(l)}\right)=\#\left\{G\in T_l \,\middle|\, \det(G)=\pi^k,\ AG=\pi I \text{ for some } A\in M_l(R)\right\}.$$

We count such $G=\left(g_{i,j}\right)$ by Lemma 4. Let $j(1),\ldots,j(k)\in\mathbb{Z}$ such that $1\le j(1)<\cdots<j(k)\le l$. If $g_{j(1),j(1)}=\cdots=g_{j(k),j(k)}=\pi$, then $\left\{g_{i,j(h)} \,\middle|\, 1\le i<j(h),\ 1\le h\le k\right\}$ may be nonzero and the total number of these $g_{i,j(h)}$ is equal to $\sum_{h=1}^{k}(j(h)-1)=\sum_{h=1}^{k}j(h)-k$. By Lemma 4, we have $g_{j(h),j}=0$ for $j=j(h+1),\ldots,j(k)$ and the total number of these $g_{j(h),j}=0$ is equal to $\sum_{h=1}^{k}(k-h)=k(k-1)/2$. Thus, G has nonzero entries at most:

$$\sum_{h=1}^{k} j(h)-k-\frac{k(k-1)}{2}=\sum_{h=1}^{k} j(h)-\frac{k(k+1)}{2}=\sum_{h=1}^{k}(j(h)-h),$$

which proves (27). There is another expression $\text{ind}\left(T_k^{(l)}\right)=c_k^{(l)}(r)$ *of (15), cf. [13].*

It follows from (27) that:

$$\sum_{k=0}^{l}(-1)^k r^{k(k-1)/2}\text{ind}\left(T_k^{(l)}\right)X^k=\sum_{k=0}^{l}(-1)^k\left(\sum_{0\le i_1<\cdots<i_k\le l-1} r^{i_1+\cdots+i_k}\right)X^k=\prod_{i=0}^{l-1}\left(1-r^iX\right).$$

On the other hand, we have:

$$\prod_{i=0}^{l-1}\frac{1}{1-r^iX}=\prod_{i=0}^{l-1}\sum_{d_i=0}^{\infty}r^{id_i}X^{d_i}=\sum_{e=0}^{\infty}\left\{\sum_{\substack{0\le d_1,d_2,\ldots,d_l\\ d_1+d_2+\cdots+d_l=e}}r^{d_2}\ldots r^{(l-1)d_l}\right\}X^e=\sum_{e=0}^{\infty}\mathrm{ind}\left(T(\pi^e)\right)X^e,$$

where the last equality follows from (26) and the fact that any reduced $G\in M_l(R)$ with $\det(G)=\pi^e$ is of the form:

$$\begin{pmatrix}\pi^{d_1} & g_{1,2} & \cdots & g_{1,l}\\ 0 & \pi^{d_2} & \ddots & \vdots\\ \vdots & \ddots & \ddots & g_{l-1,l}\\ 0 & \ldots & 0 & \pi^{d_l}\end{pmatrix},$$

where $d_1+\cdots+d_l=e$ and $[\![g_{i,j}/\pi^{d_j}]\!]=0$ for all $i<j$. Thus, $\mathrm{ind}\left(T(\pi^e)\right)$ can be computed by:

$$\sum_{e=0}^{\infty}\mathrm{ind}\left(T(\pi^e)\right)X^e=\left[\sum_{k=0}^{l}(-1)^kr^{k(k-1)/2}\mathrm{ind}\left(T_k^{(l)}\right)X^k\right]^{-1}=\prod_{i=0}^{l-1}\frac{1}{1-r^iX}.$$

Actually, $T(\pi^e)$ has the generating function [13]:

$$\sum_{e=0}^{\infty}T(\pi^e)X^e=\left[\sum_{k=0}^{l}(-1)^kr^{k(k-1)/2}T_k^{(l)}X^k\right]^{-1}.$$

Summarizing the above results, for a nonzero $f=\epsilon\prod_{i=1}^{s}\pi_i^{e_i}\in R$, we decompose $T(f)=\prod_{i=1}^{s}T\left(\pi_i^{e_i}\right)$ and, by the multiplication, obtain all G of $\mathcal{C}\subset\left(R/\langle f\rangle\right)^l$ with $\deg(G)=f$.

Example 8. *In case of $R=\mathbb{Z}[i]$ and $l=3$, $\mathrm{ind}\left(T\left(\pi^e\right)\right)$ with $\pi=2+i$ is computed by:*

$$\begin{aligned}\sum_{e=0}^{\infty}\mathrm{ind}\left(T\left(\pi^e\right)\right)X^e&=\frac{1}{1-31X+155X^2-125X^3}\\&=1+31x+806X^2+20306X^3+508431X^4+\ldots.\end{aligned}$$

For example, we have $\mathrm{ind}\left(T(\pi^2)\right)=806$. *On the other hand, because we have* $T(\pi^2)=T(1,\pi,\pi)+T(1,1,\pi^2)$, *all reduced generator matrices are:*

$$\begin{pmatrix}1 & * & *\\ & \pi & *\\ & & \pi\end{pmatrix}\ (5^3)\qquad\begin{pmatrix}\pi & 0 & *\\ & 1 & *\\ & & \pi\end{pmatrix}\ (5^2)\qquad\begin{pmatrix}\pi & * & 0\\ & \pi & 0\\ & & 1\end{pmatrix}\ (5)$$

$$\begin{pmatrix}1 & 0 & *\\ & 1 & *\\ & & \pi^2\end{pmatrix}\ (25^2)\qquad\begin{pmatrix}1 & * & 0\\ & \pi^2 & 0\\ & & 1\end{pmatrix}\ (25)\qquad\begin{pmatrix}\pi^2 & 0 & 0\\ & 1 & 0\\ & & 1\end{pmatrix}\ (1),$$

where $(\cdot)$ indicates the number of reduced generator matrices of each type. Thus, we can list all 806 reduced G for $\mathcal{C}\subset(R/\pi^2R)^3$ with $|\mathcal{C}|=\psi(\pi)^4=5^4$.

8. Conclusions

In this study, we have found various useful properties of the codes over some Euclidean residue rings and proven that many characteristics of the generator matrices of GQC codes (in particular,

the uniqueness of the reduced generator matrices) remain valid for the case analyzed here. If the moduli of the codes are equal among all symbols, i.e., $\mathcal{C} \subset \mathbb{L}/u\mathbb{L}$ for some nonzero $u \in R$, then we have shown that the product of the generator matrices constructs all generator matrices. In addition, if the moduli of the codes are relatively prime, then this construction has been shown to be a one-to-one correspondence among the classes of generator matrices.

In the case of QC and GQC codes, the results in [2,3] have a similarity with ours in the sense of producing codes of a modulus from those of factored moduli. We compare these results as follows.

Table 1 is supplementally explained as follows. For the classes of codes, we have treated the codes $\mathcal{C} \subset (R/\langle u \rangle)^l$ with Euclidean domain R, which generalize the case of QC codes with $R = \mathbb{F}_q[x]$. Whereas, in [2,3], the producing methods is the concatenation which is represented by, e.g., Turyn's $(x+a, x+b, x+a+b)$-method, our producing method is the multiplication $G = G_1 G_2$ of generator matrices in Theorems 1,2. In [2,3], the self-duality is preserving, i.e., roughly speaking, if codes mod u_1 and mod u_2 are self-dual in a sense, then the produced code mod $u = u_1 u_2$ is also self-dual. Unfortunately, our producing method does not have this preserving property of self-duality. From the viewpoint of computational complexity, our method can have an advantage over those of [2,3] because, whereas Turyn-type methods require overall combination of codewords in the worst case, our method requires only multiplying two l-by-l matrices. Consequently, it is important to use different methods according to the desired types of codes. For example, for GQC or self-dual codes, the methods of [2,3] should be chosen, and for high-rate QC codes, where "high-rate" means that the ratio k/n of dimension k and length n is greater than $1/2$, our method is appropriate because of its less computational complexity.

Table 1. Comparison of various methods which produce a code mod $u = u_1 u_2$ from codes mod u_1 and mod u_2.

Papers	[2]	[3]	**Ours**
classes of codes	$\mathcal{C} \subset \left(\frac{\mathbb{F}_q[x]}{\langle x^m-1\rangle}\right)^l$ QC codes	$\mathcal{C} \subset \bigoplus_{i=1}^{l} \frac{\mathbb{F}_q[x]}{\langle x^{m_i}-1\rangle}$ GQC codes	$\mathcal{C} \subset (R/\langle u \rangle)^l$ R: Euclidean domain
producing methods	concatenation	concatenation	multiplication of generator matrices
self-duality	preserving	preserving	not preserving
computational complexity	generally large	generally large	approximately $O(l^3)$

As an application, for specified standard Euclidean domains, we have applied the theory of reduced generator matrices to Hecke rings, and we have shown the enumeration formulae of the number of a certain types of generator matrices. Future work will focus on developing a method for the efficient enumeration of general GPC codes. Another area of research will involve the establishment of the theory of parity-check matrices for these codes, especially a formula for extracting them from the equalities such as in [5,7].

Acknowledgments: The author would like to thank the anonymous referees for their comments which helped improve the presentation of the paper. This work was supported in part by a grant of JSPS KAKENHI Grant Number 15K13994 and in part by a grant of the Strategic Research Foundation Grant-aided Project for Private Universities from MEXT (S1311034).

Conflicts of Interest: The author declares no conflict of interest.

References

1. Lally, K.; Fitzpatrick, P. Algebraic structure of quasi-cyclic codes. *Discret. Appl. Math.* **2001**, *111*, 157–175.
2. Ling, S.; Solé, P. On the algebraic structure of quasi-cyclic codes I: Finite fields. *IEEE Trans. Inf. Theory* **2001**, *47*, 2751–2760.

3. Güneri, C.; Özbudak, F.; Özkaya, B.; Saçıkara, E.; Sepasdar, Z.; Solé, P. Structure and performance of generalized quasi-cyclic codes. *Finite Fields Appl.* **2017**, *47*, 183–202.
4. Heegard, C.; Little, J.; Saints, K. Systematic encoding via Gröbner bases for a class of algebraic geometric Goppa codes. *IEEE Trans. Inf. Theory.* **1995**, *41*, 1752–1761.
5. Matsui, H. On generator and parity-check polynomial matrices of generalized quasi-cyclic codes. *Finite Fields Appl.* **2015**, *34*, 280–304.
6. Matsui, H. On generator polynomial matrices of generalized pseudo-cyclic codes. In Proceedings of the International Symposium on Information Theory and Its Applications (ISITA2014), Melbourne, Australia, 26–29 October 2014; pp. 366–370
7. Matsui, H. On generator matrices and parity check matrices of generalized integer codes. *Des. Codes Cryptogr.* **2015**, *74*, 681–701.
8. Becker, T.; Weispfenning, V. *Gröbner Bases: A Computational Approach to Commutative Algebra;* Springer: New York, NY, USA, 1993.
9. Ireland, K.; Rosen, M. *A Classical Introduction to Modern Number Theory;* Springer: Berlin, Germany, 1990.
10. Cohen, H. *A Course in Computational Algebraic Number Theory;* Springer-Verlag: Berlin, Germany, 1993.
11. Schrijver, A. *Theory of Linear and Integer Programming*; John Wiley & Sons: Hoboken, NJ, USA, 1986.
12. Serre, J.-P. *A Course in Arithmetic;* Springer-Verlag: New York, NY, USA, 1973.
13. Shimura, G. *Introduction to the Arithmetic Theory of Automorphic Functions*; Princeton University Press: Princeton, NJ, USA, 1971.
14. Lang, S. *Algebra,* 3rd ed.; Springer: Berlin, Germany, 2002.
15. Calderbank, A.R.; Sloane, N.J.A. Modular and *p*-adic cyclic codes. *Des. Codes Cryptogr.* **1995**, *6*, 21–35.