BACHELOR THESIS

Linear Diophantine Equation Systems

in fulfillment of
the requirements for the degree of
Bachelor of Science (BSc)

submitted at the
Institute of Analysis and Number Theory

under supervision of
Roswitha Rissner, Dipl.-Ing. Dr.techn.

Martina Tscheckl

Graz, September 2016

AFFIDAVIT

I declare that I have authored this thesis independently, that I have not used other sources and resources than the ones declared, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used.

Date, September 14, 2016

Signature

Contents

1 Introduction

In this thesis we prove solvability conditions for Linear Diophantine Equation Systems over Euclidean rings. To receive such solvability conditions we introduce the Smith Normal Form. The Smith Normal Form is a diagonal matrix where each diagonal entry divides the following diagonal entry. We show that the Smith Normal Form exists and is unique for matrices over a Euclidian ring. In particular, representing a Linear Diophanine Equation System as Diophantine matrix equation system allows us to transform the system matrix into its Smith Normal Form. This simplifies our goal to determine solvability conditions.

Further, we present an algorithm to compute the Smith Normal Form for matrices over the Euclidean ring $\mathbb{Z}$. This algorithm takes advantage of the Hermite Normal Form. The Hermite Normal Form is a lower triangular matrix with restrictions on the size of its entries. Hence, the Hermite Normal Form ensures that matrix entries are bounded by a polynomial of the length of the input.

As an application for Linear Diophantine Equation Systems we solve the ideal membership question for rings of the form

$$R = \left\{ \sum_{\ell=0}^{n-1} v_\ell u^\ell \;\middle|\; v_0, \ldots, v_{n-1} \in \mathbb{Z} \right\}$$

where $u \in \mathbb{C} \setminus \mathbb{Z}$ is an element that satisfies a monic polynomial equation over the integers of degree n (with n minimal). We show how ideal membership can be reformulated as a Linear Diophantine Equation System.

We start with introducing notation and definitions in Section 2. Next, in Section 3, we show that for an matrix over a Euclidean ring there exists a Smith Normal Form. We also prove that the Smith Normal Form of such a matrix is uniquely determined (up to associates). Finally, we find conditions to determine whether a Linear Diophantine Equation System is solvable or not. And if a system is solvable, we additionally receive the integer solutions of the Linear Diophantine Equation system.

Section 4 describes algorithms to transform a matrix over $\mathbb{Z}$ into its Smith Normal Form. These algorithms are based on a paper from Kannan and Bachem [2] which describes algorithms for square matrices with full rank. In this thesis the algorithms are extended to work for matrices with full row rank. To ensure that entries of the matrix stay reasonable small during the computation, we make, like Kannan and Bachem [2], use of the so-called Hermite Normal Form. The Hermite Normal Form is a lower left triangular

matrix with conditions which keep its entries bounded by a polynomial of the length of the input.

In Section 5, we describe the ideal membership question in detail and show a formula to transform it into a Linear Diophantine Equation System. With the theory covered in the previous sections we are then able to answer the question algorithmically using the previous sections.

Finally, in Section 4, we give an example to demonstrate the approach of Section 5 together with the algorithm of Section 4.

2 Preliminaries

Notation. Let R be a commutative ring. Then

(a) $\mathrm{M}_{m,n}(R)$ denotes the set of all $m \times n$ matrices over R.

(b) the *general linear group* equipped with the usual matrix multiplication is denoted by

$$\mathrm{GL}_n(R) = \{A \in M_{n,n}(R) : A \text{ is invertible}\}.$$

Notation. Let $M \in \mathrm{M}_{m,n}(R)$ be a matrix.

1. m_{ij} denotes the entry of M in the i-th row and j-th column for $1 \leq i \leq m$ and $1 \leq j \leq n$.
2. M^t denotes M transposed.
3. M_j denotes the j-th column of M.
4. $M^{(i)}$ denotes the left upper submatrix of M with i rows and columns, as shown in Figure 1.
5. $M_{(i)}$ denotes the right lower submatrix of M with $(m - i + 1)$ rows and $(n - i + 1)$ columns, as shown in Figure 1.

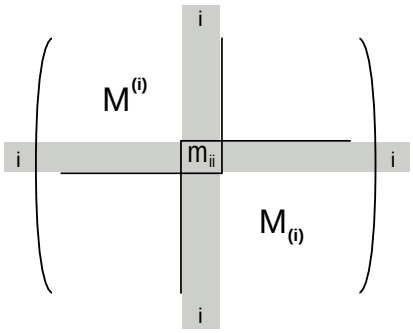


Figure 1: Submatrices $M^{(i)}$ and $M_{(i)}$ of M

Definition 1 (Elementary matrix)**.** *Let $I_n \in \mathrm{M}_{n,n}(R)$ be the unit matrix and $E_k^\ell \in \mathrm{M}_{n,n}(R)$ be defined as*

$$(e_k^\ell)_{ij} = \begin{cases} 1 & \text{if } i = k \text{ and } j = \ell \\ 0 & \text{otherwise} \end{cases}.$$

Further, we define

$$Q_i^j(\lambda) = I_n + \lambda \cdot E_i^j.$$

with $\lambda \in R$ *and* $\lambda \neq -1$ *in case* $i = j$. *Matrices* $Q_i^j(\lambda)$ *are called* elementary matrices.

Remark. (a) Let M be a matrix. Then $M' = MQ_i^j(\lambda)$ where $M'_j = M_j + \lambda M_i$ and $M'_k = M_k$ for $k \neq j$. This matrix multiplication equals the *elementary column operation* of adding the λ-fold of the i-th column to the j-th column. Analogously, $\hat{M} = Q_i^j(\lambda)M$ equals the corresponding *elementary row operation*, i.e. the i-th row of $\hat{M}$ is the λ-fold of the j-th row added to the i-th row of M.

(b) By definition of elementary column (row) operations, we can write the application of successive elementary column (row) operations $(V_i)_{1 \leq i \leq n}$ as a product from right (left) of according elementary matrices, i.e. for elementary column operations

$$(((A \cdot V_1) \cdot V_2) \cdots) \cdot V_n) = A \cdot (V_1 \cdots V_n) = A \cdot V.$$

(c) The inverse of $Q_i^j(\lambda)$ is

$$Q_i^j(\lambda)^{-1} = \begin{cases} Q_i^j(-\lambda) & \text{if } i \neq j \\ Q_i^j\left(\frac{-\lambda}{1+\lambda}\right) & \text{if } i = j \text{ and } 1 + \lambda \in R^\times \end{cases}$$

If $1 + \lambda \notin R^\times$, then there exists no inverse for $Q_i^i(\lambda)$.

(d) Multiplying the i-th column (row) of a matrix by -1 equals a matrix multiplication from right (left) with

$$Q_i^i(-2) = I_n - 2 \cdot E_i^i.$$

(e) Interchanging the i-th and j-th columns of a matrix equals a matrix multiplication from right with the following successive column operations

$$Q_j^i(1), Q_i^j(1), Q_j^i(-1), Q_i^j(2), Q_i^i(-2).$$

Multiplying this sequence to a matrix from left is the corresponding row operation.

Definition 2. *Let* $M \in \mathrm{M}_{m,n}(R)$ *be a matrix and* M_i, M_j *be two columns of* M. *Further, let* $r = p \cdot m_{ii} + q \cdot m_{ij}$ *be the greatest common divisor of* m_{ii} *and* m_{ij}. *Define the matrix* $T(M, i, j)$ *as an* $n \times n$ *matrix with*

$$t_{ii} = p \qquad t_{ij} = -\frac{m_{ij}}{r}$$

$$t_{ji} = q \qquad t_{jj} = \frac{m_{ii}}{r}$$

and $t_{kk} = 1$ *for* $k \neq i, j$*, and* $t_{kl} = 0$ *otherwise. Then* $T(M, i, j)$ *represents elementary column operations such that* $m'_{ii} = r$ *and* $m'_{ij} = 0$ *for* $M' = M \cdot T(M, i, j)$*. Analogously, we can define a* $m \times m$ *matrix* $\hat{T}(M, i, j)$ *for row operations such that* $\hat{M} = \hat{T}(M, i, j) \cdot M$ *results in* $\hat{m}_{ii} = \gcd(m_{ii}, m_{ji})$ *and* $\hat{m}_{ji} = 0$*.*

Remark. The matrix $T(M, i, j)$ is invertible. Let $T'(M, i, j)$ be defined as an $n \times n$ matrix with

$$t'_{ii} = \frac{m_{ii}}{r} \qquad t'_{ij} = \frac{m_{ij}}{r}$$
$$t'_{ji} = -q \qquad t'_{jj} = p$$

and $t'_{kk} = 1$ for $k \neq i, j$, and $t'_{kl} = 0$ otherwise. Multiplying those two matrices $T(M, i, j) \cdot T'(M, i, j) = S(M, i, j)$ will result in

$$s_{ii} = s_{jj} = p \cdot \frac{m_{ii}}{r} + q\frac{m_{ij}}{r} = \frac{p \cdot m_{ii} + q \cdot m_{ij}}{r} = \frac{r}{r} = 1$$

and

$$s_{ij} = p \cdot \frac{m_{ij}}{r} - p\frac{m_{ij}}{r} = 0$$
$$s_{ji} = q \cdot \frac{m_{ii}}{r} - q\frac{m_{ii}}{r} = 0$$

and $s_{kk} = 1$ for $k \neq i, j$ and $s_{kl} = 0$ otherwise. Thus, $S(M, i, j) = I_n$ equals the unit matrix and $T'(M, i, j)$ is the inverse of $T(M, i, j)$.

Definition 3. *Let* $M, M' \in \mathrm{M}_{m,n}(R)$*. We say* M *is equivalent to* M'*, written as* $M \sim M'$*, if and only if there exist two matrices* $U \in \mathrm{GL}_m(R)$ *and* $V \in \mathrm{GL}_n(R)$ *such that*

$$UMV = M'.$$

Remark. We refer to the matrices U and V as *transformation matrices*. Note, that the transformation matrices U and V are not uniquely determined.

3 Solving Linear Diophantine Equation Systems

3.1 Smith Normal Form

Solving equation systems with diagonal matrices is easier than with arbitrary matrices. Therefore, in this section we prove that we can transform any matrix A over an Euclidean ring R to a special diagonal matrix, the so-called Smith Normal Form, using elementary row and column operations. We denote the Euclidean distance as

$$\begin{aligned} |\cdot| : R \setminus \{0\} &\to \mathbb{N}_0 \\ x &\mapsto |x|. \end{aligned}$$

We show in two steps that every matrix A has a uniquely determined Smith Normal Form.

3.1.1 Existence

Lemma 1. *Let R be an Euclidean ring and $A \in M_{m,n}(R)$ a matrix with $a_{11} \neq 0$. Then there exists a matrix B such that $A \sim B$ with $b_{11} = a_{11}$ and all entries in the first row and column except b_{11} are strictly smaller than b_{11}, i.e. $0 \leq |b_{i1}| < |b_{11}|$ and $0 \leq |b_{1j}| < |b_{11}|$ for all $i, j \geq 2$. Moreover, $b_{i1} = 0 \iff a_{11}|a_{i1}$ for every $i \geq 2$; and $b_{1j} = 0 \iff a_{11}|a_{1j}$ for every $j \geq 2$. The corresponding transformation matrices are a product of elementary matrices.*

Proof. For any $j \geq 2$ we can write $a_{1j} = qa_{11} + r$ with $0 \leq |r| < |a_{11}|$. Then we transform A to $\hat{A}$ by subtracting the q-fold of the first column from the j-th column. Now $A \sim \hat{A}$ with $\hat{a}_{ij} = a_{ij} - qa_{i1}$ and $\hat{a}_{ik} = a_{ik}$ for all i and $k \neq j$. Since $\hat{a}_{1j} = r$, it follows that $0 \leq |\hat{a}_{1j}| < |\hat{a}_{11}|$ holds. In particular,

$$a_{11}|a_{1j} \iff a_{1j} = qa_{11} + 0 \iff \hat{a}_{1j} = a_{1j} - qa_{11} = 0.$$

Note that $\hat{a}_{11} = a_{11}$.

Analogously, we can transform for any $i \geq 2$ a matrix A to $\bar{A}$ with elementary row operations instead of elementary column operations. Then $A \sim \bar{A}$ with $\bar{a}_{11} = a_{11}$ and $0 \leq |\bar{a}_{i1}| < |\bar{a}_{11}|$. Again, $\bar{a}_{i1} = 0 \iff a_{11}|a_{i1}$.

If we perform these transformations for all $i, j \geq 2$, we receive a matrix B with $A \sim B$ where B has the desired properties. □

Proposition 1. *Let R be an Euclidean ring and $A \in \mathrm{M}_{m,n}(R)$. Then A is equivalent to a matrix B where $b_{11}|b_{ij}$ and entries of the first row and column*

except b_{11} equal 0, i.e. $0 = b_{i1} = b_{1j}$ for all $i, j \geq 2$, and the transformation matrices are a product of elementary matrices.

Proof. If A is the zero matrix the condition $a_{11}|a_{ij}$ holds for all i, j. Therefore, we assume that A is not the zero matrix. If $a_{11} = 0$, we can change the first row and first column with a row and a column which have an entry $a_{ij} \neq 0$ for $1 \leq i \leq m$ and $1 \leq j \leq n$.

A. *Let A be a matrix with $a_{11} \neq 0$. If there exists an $i \geq 2$ such that $a_{11} \nmid a_{i1}$ or a $j \geq 2$ such that $a_{11} \nmid a_{1j}$, then there exists a matrix A' such that $A \sim A'$ with $0 < |a'_{11}| < |a_{11}|$ and $a'_{i1} = a'_{1j} = 0$, for all $i, j \geq 2$.*

Proof of **A**. By Lemma 1, there exists a matrix $\hat{A}$ such that $A \sim \hat{A}$ with $\hat{a}_{11} = a_{11}$ and $0 \leq |\hat{a}_{k1}| < |\hat{a}_{11}|$ and $0 \leq |\hat{a}_{1\ell}| < |\hat{a}_{11}|$ for $k, \ell \geq 2$.

Now consider a_{1j} with $a_{11} \nmid a_{1j}$. By Lemma 1 follows that $0 < |\hat{a}_{1j}| < |\hat{a}_{11}|$ holds. We exchange the first and j-th column to get a matrix $\bar{A}$ such that $\hat{A} \sim \bar{A}$ with $|\bar{a}_{11}| < |\hat{a}_{11}|$.

We repeat the application of Lemma 1 and the exchange of columns as described above until we have found a matrix $\tilde{A}$ with $\tilde{a}_{1j} = 0$ for all $j \geq 2$.

Analogously, we do the same for all entries in the first column which are not divisible by the first entry of the first column.

Since we switch rows or columns for every element in the first column or row which is not divisible by the entry in the first row and column, the first row or column changes with every switch. Thus, we perform the steps described above alternatingly for the first row and the first column until we have found a matrix A' with $a'_{i1} = 0$ and $a'_{1j} = 0$ for all $i, j \geq 2$ and $0 < |a'_{11}| < |a_{11}|$. There are only finitely many steps since in each step either the absolute value of the entry in the first row and column gets strictly smaller than it was before or we have found a matrix with desired properties. □

B. *Let A be a matrix with $a_{11} \neq 0$ and $a_{i1} = a_{1j} = 0$ for all $i, j \geq 2$. If there exist $i, j \geq 2$ such that $a_{11} \nmid a_{ij}$, then there exists a matrix $A' \in \mathrm{M}_{m,n}(R)$ such that $A \sim A'$ with $0 < |a'_{11}| < |a_{11}|$ and $a'_{i1} = a'_{1j} = 0$ for all $i, j \geq 2$.*

Proof of **B**. Let $i, j \geq 2$ be two indices of A such that $a_{11} \nmid a_{ij}$. Then we transform A to $\bar{A}$ by adding the i-th row to the first row. Thus, $\bar{a}_{1j} = a_{1j} + a_{ij}$ and $\bar{a}_{kj} = a_{kj}$ for $k \geq 2$. Since $a_{i1} = a_{1j} = 0$ for $i, j \geq 2$, we have $\bar{a}_{11} = a_{11}$ and $\bar{a}_{1j} = a_{ij}$.

Now we have a matrix $\bar{A}$ with $\bar{a}_{11} \neq 0$ and $\bar{a}_{11} \nmid \bar{a}_{1j}$. By **A**, there exists a matrix A' such that $A \sim A'$ with $0 < |a'_{11}| < |a_{11}|$ and $a'_{i1} = a'_{1j} = 0$. □

So we transform matrix A by using Lemma 1 and if needed, we apply **A** once. In the following we iteratively apply **B** for every entry that is not divisible by the entry in the first row and column. Then we get a sequence of transformations

$$A = A(0), A(1), \ldots, A(k) = B$$

where B is a matrix with $A \sim B$ and $b_{11}|b_{ij}$ for all $i, j \geq 1$.

By **B** the entry in the first row and column gets replaced by a strictly smaller entry in each transformation, i.e.

$$|a(0)_{11}| \geq |a(1)_{11}| > |a(2)_{11}| > \cdots > |a(k)_{11}| > 0.$$

Thus we get matrix B after finitely many steps. □

Theorem 1. *Let $A \in M_{m,n}(R)$ be of rank r. Then there exist matrices $U \in \mathrm{GL}_m(R)$ and $V \in \mathrm{GL}_n(R)$ such that*

$$UAV = D = \mathrm{diag}(d_1, d_2, \ldots, d_r, 0, \ldots, 0)$$

where d_i are unique (up to associates) and $d_i|d_{i+1}$ for $i = 1, \ldots, r-1$.

Proof. We prove this by induction on $\max\{m, n\}$. If $\max\{m, n\} = 1$, the matrix has the desired form. Let A be a matrix with $\max\{m, n\} > 1$. By Proposition 1, there exists a matrix B such that $A \sim B$ with $b_{11}|b_{ij}$ and $b_{i1} = b_{1j} = 0$ for all $i, j \geq 2$.

Now consider a matrix C which equals B without its first row and column, i.e. $C = (c_{(i-1)(j-1)}) = (b_{ij})$ for $i > 1$ and $j > 1$. Then C has rank $l < r$. We apply the induction hypothesis on C and transform it with elementary row and column operations to a diagonal matrix

$$\mathrm{diag}(c_1, \ldots, c_l, 0, \ldots, 0)$$

such that $c_1|c_2|\ldots|c_l$. Actually, the same operations can be applied on B because they only affect entries of the first row or column which equal 0. Thus, we receive a diagonal matrix

$$\mathrm{diag}(b_{11}, c_1, \ldots, c_l).$$

Since b_{11} divides all entries of C, all those entries are multiples of b_{11}. So using elementary row and column operations, i.e. adding or subtracting multiples of other matrix entries to an entry, does not affect the divisibility by b_{11}. Thus b_{11} divides $c_1, \ldots, c_l$. So we have found a diagonal matrix with the desired properties. □

Definition 4 (Smith Normal Form)**.** *A matrix $S \in \mathrm{M}_{m,n}(R)$ of rank r is called* Smith Normal Form *if*

$$S = \mathrm{diag}(d_1, \dots, d_r, 0, \dots, 0)$$

with $d_i | d_{i+1}$ for all $i = 1, \dots, r-1$.

3.1.2 Uniqueness

Now we show that the Smith Normal Form of a matrix is uniquely determined (up to associates).

Definition 5 (Determinantal divisor)**.** *A $k \times k$* minor *of a matrix A is the determinant of a submatrix of A with k rows and k columns. The greatest common divisor of all $k \times k$ minors is called the k-th* determinantal divisor *g_k of A.*

Proposition 2. *Let A and A' be two equivalent matrices, $A \sim A'$, and let the transformation matrices be a product of successive elementary row and column operations, then A and A' have the same determinantal divisors.*

Proof. The determinant of a matrix A is linear with respect to rows and columns. Since $\det(A^t) = \det(A)$, we consider w.l.o.g. elementary column operations. For $c \in R$

$$\begin{aligned} \det(\dots, A_i + A_i', \dots) &= \det(\dots, A_i, \dots) + \det(\dots, A_i', \dots) \\ \det(\dots, c \cdot A_i, \dots) &= c \cdot \det(\dots, A_i, \dots). \end{aligned}$$

Let $B = A \cdot Q_i^j(\lambda)$ with $\lambda \in R$ if $i \neq j$ and $\lambda + 1 \in R^\times$ if $i = j$. If the j-th column is not part of a $k \times k$ minor of B, this minor is by definition a $k \times k$ minor of A. So assume the j-th column is part of the $k \times k$ minor of B. Then the linearity of the determinant gives us

$$\det(\dots, A_j + \lambda \cdot A_i, \dots) = \underbrace{\det(\dots, A_j, \dots)}_{\text{is a minor of } A} + \lambda \cdot \underbrace{\det(\dots, A_i, \dots)}_{\text{is a minor of } A}.$$

Since the determinantal divisor of A divides

$$\det(\dots, A_j, \dots) \text{ and } \det(\dots, A_i, \dots),$$

it also divides

$$\det(\dots, A_i + \lambda \cdot A_j, \dots).$$

And thus, the determinantal divisor of A divides the determinantal divisor of B.

We have shown that if we receive B from A with elementary column operations, then the determinantal divisor of A divides the determinantal divisor of B. Furthermore, if we can receive B from A with elementary column operations, then we can also receive A from B with elementary column operations (see Section 2), i.e.

$$\begin{aligned} i \neq j: &\qquad B = A \cdot Q_i^j(\lambda) \iff A = B \cdot Q_i^j(-\lambda), \\ i = j: &\qquad B = A \cdot Q_i^i(\lambda) \iff A = B \cdot Q_i^i\left(-\frac{\lambda}{1+\lambda}\right). \end{aligned}$$

Thus, the determinantal divisors of B divide the determinantal divisors of A. Therefore, the determinantal divisors of a matrix do not change, if elementary column operations are applied to the matrix. □

Theorem 2. *Two matrices have the same Smith Normal Form if and only if they have the same determinantal divisors (up to multiplication with associates). In particular, the Smith Normal Form is uniquely determined (up to associates).*

Proof. Let $A, \tilde{A} \in \mathrm{M}_{m,n}(R)$.

($\Rightarrow$) Let A and $\tilde{A}$ have the same Smith Normal Form D. The Smith Normal Form is computed by elementary row and column operations. By Proposition 2, elementary row and column operations do not change the determinantal divisors up to multiplication with associates. Therefore, we consider the determinantal divisors of the Smith Normal Forms of A and $\tilde{A}$. Since A and $\tilde{A}$ have the same Smith Normal Form, their determinantal divisors are the same.

($\Leftarrow$) Conversely, let A have rank r and $\tilde{A}$ have rank s. Let D and $\tilde{D}$ with $D \neq \tilde{D}$ be their Smith Normal Forms. By Proposition 2, elementary row and column operations do not change determinantal divisors of a matrix. Thus, we consider the determinantal divisors of D and $\tilde{D}$. Because D and $\tilde{D}$ are diagonal matrices where each diagonal entry is divisible by its previous diagonal entry, the determinantal divisors g_k of D and $\tilde{g}_l$ of $\tilde{D}$ are

$$g_k = \begin{cases} \prod_{i=1}^{k} d_i & k \leq r \\ 0 & k > r \end{cases}, \qquad \tilde{g}_l = \begin{cases} \prod_{i=1}^{l} \tilde{d}_i & l \leq s \\ 0 & l > s \end{cases}.$$

Since $D \neq \tilde{D}$, there exists a $j \in \{1, \ldots, \max(r,s)\}$ with $d_j \neq \tilde{d}_j$ and $d_i = \tilde{d}_i$ for $1 \leq i < j$. Thus,

$$g_j = d_j \prod_{i=1}^{j-1} d_i \neq \tilde{d}_j \prod_{i=1}^{j-1} d_i = \tilde{g}_j.$$

Therefore, A does not have the same determinantal divisors as $\tilde{A}$.

□

3.2 Solvability of LDE

In this section we want to show conditions such that a system of linear diophantine equations $Ax = b$ is solvable over an Euclidean ring R. Solving equation systems with diagonal matrices is easier than with arbitrary matrices. Thus, we use Theorem 1, which states that existences of matrices D, U and V such that $D = UAV$ with D in Smith Normal Form are given.

Theorem 3 (cf. [3] Exercise 12.3)**.** *Let R be an Euclidean ring and $A \in \mathrm{M}_{m,n}(R)$ be a matrix of rank r with Smith Normal Form*

$$D = \mathrm{diag}(d_1, \ldots, d_r, 0, \ldots, 0).$$

Further, let $U \in \mathrm{GL}_m(R)$ and $V \in \mathrm{GL}_n(R)$ such that $UAV = D$. For $b \in R^m$ the linear equation system

$$Ax = b$$

is solvable in $x \in R^n$ if and only if, for $c = Ub$, there exist $y_1, \ldots, y_r \in R$ such that

$$\begin{aligned} d_i \cdot y_i &= c_i && (i = 1, \ldots, r), \\ 0 &= c_j && (j = r+1, \ldots, m). \end{aligned}$$

In this case, all solutions to the system are of the form $x = Vy$ with $y_i = \frac{c_i}{d_i}$ for $1 \leq i \leq r$ and $y_{r+1}, \ldots, y_n$ arbitrary.

Proof. First, we transform $Ax = b$ to an equation system of the form $Dy = c$:

$$\begin{aligned} Ax = b &\iff UAx = Ub \\ &\iff UAVV^{-1}x = c \\ &\iff Dy = c \end{aligned}$$

with $y = V^{-1}x$.

Let $r \leq \min\{m, n\}$ be the rank of the matrix A. Then, the entries d_i of D with $i > r$ are 0. So we write

$$\begin{array}{c} \\ r \\ m-r \end{array} \begin{array}{c} \begin{array}{cc} r & n-r \end{array} \\ \begin{pmatrix} D' & 0 \\ 0 & 0 \end{pmatrix} \end{array} = D$$

where $D' = \operatorname{diag}(d_1, \ldots, d_r)$ is the submatrix of D with rank r. Furthermore, we write

$$\begin{matrix} r \\ n-r \end{matrix} \begin{pmatrix} y' \\ \tilde{y} \end{pmatrix} = y, \qquad \begin{matrix} r \\ m-r \end{matrix} \begin{pmatrix} c' \\ \tilde{c} \end{pmatrix} = c.$$

Then we split the equation system

$$Dy = c \iff \begin{pmatrix} D' & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y' \\ \tilde{y} \end{pmatrix} = \begin{pmatrix} c' \\ \tilde{c} \end{pmatrix}$$

into two subsystems

$$D'y' + 0\tilde{y} = c' \tag{1}$$

$$0y' + 0\tilde{y} = \tilde{c} \tag{2}$$

Subsystem (2) is solvable if and only if $\tilde{c} = 0$. Then all y' and $\tilde{y}$ are solutions for this subsystem.

Now consider subsystem (1). Clearly,

$$D'y' + 0\tilde{y} = c' \iff D'y' = c'.$$

Since all entries except the diagonal entries of D' are 0, we can write $D'y' = c'$ as $d_i y_i = c_i$ for $i = 1, \ldots, r$. Then, this subsystem is solvable if and only if there exist $y_i \in R$ for $i = 1, \ldots, r$ such that $d_i y_i = c_i$. Solutions to this subsystem are $y' = (D')^{-1}c'$ and all $\tilde{y}$.

Thus, the equation system $Dy = c$ is solvable if and only if there exist $y_1, \ldots, y_r \in R$ such that

$$\begin{aligned} d_i \cdot y_i &= c_i && (i = 1, \ldots, r), \\ 0 &= c_j && (j = r+1, \ldots, m). \end{aligned}$$

If this is the case, we can determine y_i from $d_i y_i = c_i$ for $i = 1, \ldots, r$ and choose y_j for $j = r+1, \ldots, m$ arbitrarily. Then, we retrieve x from the equation system $y = V^{-1}x \iff Vy = x$. □

4 Algorithmic computation of SNF over $\mathbb{Z}$

In this section we consider the algorithmic computation of the Smith Normal Form of a matrix with entries in $\mathbb{Z}$. Although the proofs in Section 3.1 are constructive, a straight-forward implementation (by the author) demonstrated that the entries of a matrix can grow very large during the computation. This causes already problems for 12×12 matrices.

Therefore, we describe a different approach to transform a matrix M into its Smith Normal Form. In this transformation the number of digits of all intermediate results and the number of elementary row and column operations are bounded by a polynomial of the length of the input. This approach is due to Kannan and Bachem [2] and exploits properties of the so-called Hermite Normal Form (and Left Hermite Normal Form) to compute the Smith Normal Form of a matrix. The Hermite Normal Form is a lower left triangular matrix with restrictions on its entries. These restrictions guarantee that the entries of a transformed matrix are bounded in the number of digits by a polynomial of the length of the input. Analogously, the Left Hermite Form is defined as an upper right triangular matrix with restrictions on its entries. Since a diagonal matrix is a special triangular matrix, these forms are well suited to compute the Smith Normal Form of a matrix.

Note that the algorithmic computation of Hermite Normal Form and Smith Normal Form of a matrix are described for matrices with full row rank only.

4.1 Hermite Normal Form

In this section we will describe an algorithm to compute the Hermite Normal Form of a $m \times n$ matrix with full row rank m.

Definition 6 (Hermite Normal Form)**.** *Let $H \in \mathrm{M}_{m,n}(\mathbb{Z})$ be a matrix of rank r. If H is a lower triangular matrix with*

$$0 < h_{ii} \text{ and} \tag{3}$$

$$-h_{ii} < h_{ij} \leq 0 \tag{4}$$

for all $i \in [1, r]$ and $j \leq i$, then H is called Hermite Normal Form.

Remark.

1. Using the Hermite Normal Form guarantees that the matrix entries will not grow unreasonably large and make further computations easy.
2. The literature provides slightly different definitions of Hermite Normal Form. We follow the definition of Kannan and Bachem [2].

Definition 7 (Left Hermite Normal Form)**.** *The Left Hermite Normal Form of a matrix M is defined as* $\mathrm{LHNF}(M) = \mathrm{HNF}(M^t)^t$.

Algorithm. We use an iterative algorithm to compute the Hermite Normal Form of a matrix M. We only deal with square matrices with full rank m as it is always possible to reduce the computation to this case. Recall that $M^{(i)}$ denotes the upper left submatrix of M with i rows and columns; and that M_j denotes the j-th column of M; cf. Section 2. $M^{(1)}$ is already in Hermite Normal Form since either $m_{11}^{(1)} > 0$ or we replace the first column $M_1^{(1)}$ by $-M_1^{(1)}$ such that $m_{11}^{(1)} < 0$ becomes $-m_{11}^{(1)} > 0$. So let $i > 1$. Further, let $M^{(i-1)}$ be already in Hermite Normal Form. Then consider $M^{(i)}$.

As shown in Figure 2, $M^{(i)}$ is, in general, not in Hermite Normal Form because entries above $m_{ii}^{(i)}$ may not equal 0 and entries to the left of $m_{ii}^{(i)}$ may not satisfy Equation (4). So first, we transform the entries above the diagonal entry m_{ii} into 0.

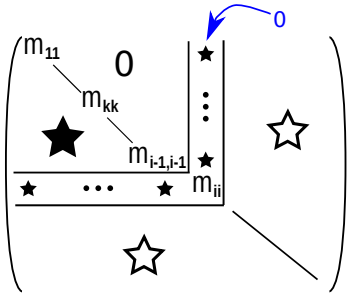


Figure 2: Transforming $M^{(i)}$ into Hermite Normal Form

We fix $1 \leq k < i$ and show that it is possible to transform the matrix M to get $m_{ki}^{(i)} = 0$. Assume that this is already done for all rows from 1 to $k-1$ in $M^{(i)}$, that is, $m_{li}^{(i)} = 0$ for $l < k$. We compute the greatest common divisor r of $m_{kk}^{(i)}$ and $m_{ki}^{(i)}$. All entries above them equal 0 and thus the following computations do not affect any entry above the k-th row. When $r = \gcd(m_{kk}^{(i)}, m_{ki}^{(i)})$, then there exist $p, q \in \mathbb{Z}$ such that $r = pm_{kk}^{(i)} + qm_{ki}^{(i)}$. Then we transform the k-th column of M by $M_k = pM_k + qM_i$ such that $m_{kk}^{(i)} = r$. Simultaneously, we transform the i-th column by $M_i = \frac{(m^{(i)})_{kk}}{r} M_i - \frac{(m^{(i)})_{ki}}{r} M_k$. Since $\frac{(m^{(i)})_{kk}}{r}(m^{(i)})_{ki} - \frac{(m^{(i)})_{ki}}{r}(m^{(i)})_{kk} = 0$, this results in $(m^{(i)})_{ki} = 0$. This simultaneous transformation can be written as $M = M \cdot T(M, i, j)$ where $T(M, i, j)$ is defined as in Section 2.

Notice that the value of $m_{kk}^{(i)}$ gets replaced by $r > 0$ where $|r| \leq |m_{kk}^{(i)}|$. Hence the k-th row might not satisfy the condition in Equation (4) anymore. So

as a second step we need to transform all entries to the left of the diagonal entry such that Equation (4) holds.

Now we consider the entries to the left of the diagonal entry, i.e. $m_{kj}^{(i)}$ with $j < k$. For $M^{(i)}$ to be in Hermite Normal Form, they need to fulfill Equation (4), i.e. $-m_{kk}^{(i)} < m_{kj}^{(i)} \leq 0$. Therefore, we compute for every $1 \leq j < i$ some t_j such that $m_{kj}^{(i)} = t_j m_{kk}^{(i)} + r_j$ with $0 \leq r_j < m_{kk}^{(i)}$. Then we transform M such that $M_j = M_j - (t_j + 1)M_k$ for every j. No entries above the k-th row change since entries $m_{lk}^{(i)} = 0$ for $l < k$. This results in the first k rows of $M^{(i)}$ being in Hermite Normal Form.

Repeat these two steps for every row $1 \leq k < i$. In order to have $M^{(i)}$ in HNF, it remains to ensure that the i-th row satisfies Equation (3) and Equation (4). This is achieved by replacing the column $M_i^{(i)}$ by $-M_i^{(i)}$ if $m_{ii}^{(i)} < 0$ and repeating the second step for the i-th row as well.

In each of the k rows at most $k + 1$ entries change their values. These are the diagonal entry, the entry of the last column and at most all $k - 1$ entries to the left of the diagonal entry. Each of the k rows is considered at most m times.

Theorem 4. *Every square matrix M of full rank has a Hermite Normal Form.*

Algorithm 1 Hermite Normal Form

Input: $M \in \mathrm{M}_{m,n}(\mathbb{Z})$

Output: $H = \mathrm{HNF}(M)$, K such that $MK = H$

Set $H = M$ and $K = I_n$.

for all $1 < i \leq n$ **do**

for all rows $1 \leq k < \min(i, m)$ **do**

if $h_{kk} < 0$ **then**

Turn h_{kk} into $|h_{kk}|$

$$H_k = -H_k, \qquad K_k = -K_k$$

end if

Compute $p, q \in \mathbb{Z}$ such that

$$r = \gcd(h_{kk}, h_{ki}) = ph_{kk} + qh_{ki}.$$

Turn h_{kk} into r by computing

$$H_k = pH_k + qH_i, \qquad K_k = pK_k + qK_i.$$

Simultaneously, turn h_{ki} into 0 by computing

$$H_i = \frac{h_{kk}}{r} \cdot H_i - \frac{h_{ki}}{r} \cdot H_k, \qquad K_i = \frac{h_{kk}}{r} \cdot K_i - \frac{h_{ki}}{r} \cdot K_k.$$

for all $1 \leq j < k$ **do**

$$H_j = H_j - \left\lceil \frac{h_{kj}}{h_{kk}} \right\rceil H_k, \qquad K_j = K_j - \left\lceil \frac{h_{kj}}{h_{kk}} \right\rceil K_k.$$

end for

end for

if $h_{ii} < 0$ **then**

Turn h_{ii} into $|h_{ii}|$

$$H_i = -H_i, \qquad K_i = -K_i$$

end if

for all $1 \leq j < i \leq m$ **do**

$$H_j = H_j - \left\lceil \frac{h_{ij}}{h_{ii}} \right\rceil H_i, \qquad K_j = K_j - \left\lceil \frac{h_{ij}}{h_{ii}} \right\rceil K_i.$$

end for

end for

4.2 Smith Normal Form

In this section we describe an algorithm to transform $M \in \mathrm{M}_{m,n}(\mathbb{Z})$ with full row rank m into its Smith Normal Form, i.e. a diagonal matrix D with $d_i | d_{i+1}$ for all $1 \leq i < \mathrm{rank}(D)$. Recall that $M_{(i)}$ denotes the lower right submatrix of M with $(m-i+1)$ rows and $(n-i+1)$ columns; further, that M_j denotes the j-th column of M; cf. Section 2.

We look at i from 1 to m. The algorithmic idea is to start with the upper left entry of $M_{(i)}$ and transform $M_{(i)}$ such that all entries of its first row and first column except $(m_{(i)})_{11}$ equal 0 and $(m_{(i)})_{11}$ divides all other entries of $\mathrm{M}_{(i)}$, i.e. $(m_{(i)})_{k1} = (m_{(i)})_{1j} = 0$ and $(m_{(i)})_{11} | (m_{(i)})_{kj}$ for all $k, j \geq 2$.
Assume we have already transformed the first $(i-1)$ rows and columns of M such that $m_{11} | m_{22} | \ldots | m_{(i-1)(i-1)} | m_{kj}$ for all $k, j \geq i$ and all other entries $m_{kj} = 0$ for $k, j < i$ and $k \neq j$.

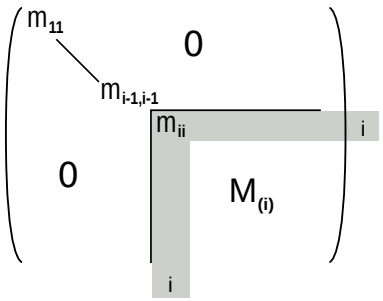
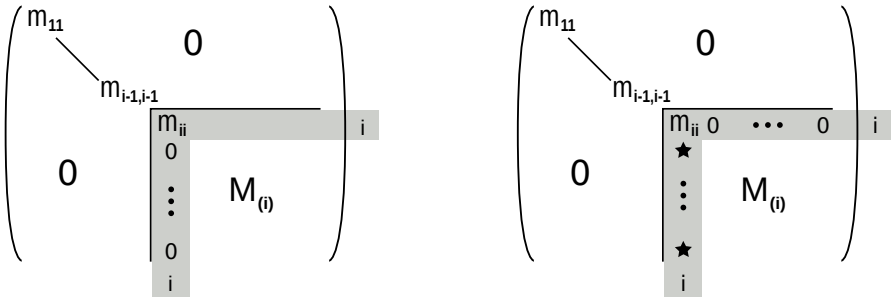


Figure 3: The first $i-1$ rows and columns of M are already in SNF

Consider $M_{(i)}$. All entries above $M_{(i)}$ and to the left of $M_{(i)}$ equal 0. So all elementary row and column operations applied to $M_{(i)}$ can be applied to M and yield the same result.

For better readability let A stand for $M_{(i)}$. Transform the first column A_1 of A into Left Hermite Normal Form. Then all entries but the first of A_1 equal 0, as shown in Figure 4a. Next we transform A into Hermite Normal Form. Then $a_{kj} = 0$ for $k < j$. In particular, all entries of the first row except the first equal 0, as shown in Figure 4b.

The computation of the Hermite Normal Form of A may again cause non-zero entries in the first column of A. To understand what causes such a change, consider A before it is transformed into Hermite Normal Form. Then a_{k1} of the first column equals 0 for all $k \geq 2$. In Section 4.1 we explained that the transformation into Hermite Normal Form of an entry



(a) Application of LHNF (b) Application of HNF

Figure 4: LHNF of $(M_(i))_1$, HNF of $M_{(i)}$

a_{kj}, k fixed and $j > k$, which is not divisible by a_{kk} affects only the columns A_k and A_j. Thus, the only case in which entries of the first column can change from value zero to a non-zero value is when $k = 1$. Assume in the first row is an a_{1j} which is not divisible by a_{11}. Since we want a_{1j} to equal 0, we first replace a_{11} by its proper divisor $\gcd(a_{11}, a_{1j}) = pa_{11} + qa_{1j}$ by transforming $A_1 = pA_1 + qA_j$. Now there might be non-zero entries in the first column. At the same time, we transform a_{1j} into 0. This step does not affect the first column, so we can neglect it.

Furthermore, entries of the first column can change when they do not fulfill Equation (4). Though this only holds for non-zero entries.

All in all, first column entries with value zero change if and only if a_{11} gets replaced by one of its proper divisors. Since $a_{11} = \left(m_{(i)}\right)_{ii} \in \mathbb{Z}$, there exist only finitely many proper divisors of a_{11}. And hence, we apply Left Hermite Normal Form and Hermite Normal Form finitely often to A until $a_{k1} = a_{1j} = 0$ for all $k, j \geq 2$.

To ensure the condition $a_{11} | a_{kj}$ holds for all k, j, we add for an a_{kj} with $a_{11} \nmid a_{kj}$ the j-th column to the first column, i.e. $A_1 = A_1 + A_j$. It suffices to do this for $j \leq m$, since the transformation into Hermite Normal Form turns the values of all entries of columns M_j with $m < j \leq n$ into 0. Then we apply again the Left Hermite Normal Form and Hermite Normal Form until $a_{k1} = a_{1j} = 0$ for all $k, j \geq 2$. Repeat this until $a_{11} | a_{kj}$ for all $k, j \geq 2$.

Every entry that is divisible by a_{11} is also divisible by its proper divisors. Thus, after applying Left Hermite Normal Form and Hermite Normal Form, there are at least as many entries divisible by a_{11} as before the transformation.

We do not need to consider the case where entries of the first row turn into

non-zero entries when the Left Hermite Normal Form is applied because after the Left Hermite Normal Form always the Hermite Normal Form is applied.

Summing up, we get a matrix $M_{(i)}$ with $(m_{(i)})_{k1} = (m_{(i)})_{1j} = 0$ and $(m_{(i)})_{11} | (m_{(i)})_{kj}$ for all $k, j \geq 2$ after finitely many steps. Furthermore, $m_{(i-1)(i-1)} | m_{ii}$ because $m_{(i-1)(i-1)} | (m_{(i)})_{kj}$ for all $k, j \geq 1$. Thus, the greatest common divisor of any two elements of $M_{(i)}$ is still divisible by $m_{(i-1)(i-1)}$. Since m_{ii} gets only replaced by its proper divisors which are the greatest common divisor of m_{ii} and an entry of $M_{(i)}$, $m_{(i-1)(i-1)} | m_{ii}$ holds.

Remark. According to Kannan and Bachem [2], Left Hermite Normal Form and Hermite Normal Form are called at most $n^2(\log n \cdot ||M^{(0)}||) + 2n$ times each which is a polynomial upper bound.

Algorithm 2 Smith Normal Form

Input: $M \in \mathrm{M}_{m,n}(\mathbb{Z})$
Output: $S = \mathrm{SNF}(M)$, U, K such that $S = UMK$
  Set $S = M$ and $U = I_m$ and $K = I_n$.
  for all $1 \leq i < m$ **do**
    Compute LHNF of S_i

$$(S, U') = \mathrm{LHNF}(S_{(i)}), \qquad U = U' \cdot U.$$

    Compute HNF of $S_{(i)}$

$$(S, K') = \mathrm{HNF}(S_{(i)}), \qquad K = K \cdot K'.$$

    if $\exists k \neq i$ such that $s_{ki} \neq 0$ **then**
      $i = i - 1$
      continue
    end if
    if $\exists i \leq j \leq k \leq m$ such that $s_{ii} \nmid s_{kj}$ **then**
      Compute

$$S_i = S_i + S_j, \qquad K_i = K_i + K_j.$$

      $i = i - 1$
      continue
    end if
  end for

---

5 Ideal Membership

Let $u \in \mathbb{C} \setminus \mathbb{Z}$ be an element such that there exist $f_0, \ldots, f_{n-1} \in \mathbb{Z}$ with $u^n = \sum_{\ell=0}^{n-1} f_\ell u^\ell$. Moreover, assume n to be minimal. Then,

$$R = \left\{ \sum_{\ell=0}^{n-1} v_\ell u^\ell \;\middle|\; v_0, \ldots, v_{n-1} \in \mathbb{Z} \right\}$$

is a ring. A straight-forward proof that R is a ring can be found in Appendix A.

Given an element b and an ideal I of R, the aim of this section is to determine whether b is contained in I. If $a_1, \ldots, a_m$ denote the generators of I, then an element $b \in R$ is contained in I if and only if there exist $r_1, \ldots, r_m \in R$ such that

$$b = \sum_{j=1}^{m} r_j a_j. \tag{5}$$

In particular, there exist integers $a_{\ell j}$, b_ℓ and $r_{\ell j}$ such that $a_j = \sum_{\ell=0}^{n-1} a_{\ell j} u^\ell$, $b = \sum_{\ell=0}^{n-1} b_\ell u^\ell$ and $r_j = \sum_{\ell=0}^{n-1} r_{\ell j} u^\ell$. Hence Equation (5) can be rewritten as

$$\sum_{j=1}^{m} \left(\sum_{\ell=0}^{n-1} r_{\ell j} u^\ell \right) \left(\sum_{\ell=0}^{n-1} a_{\ell j} u^\ell \right) = \sum_{\ell=0}^{n-1} b_\ell u^\ell. \tag{6}$$

Therefore $b \in I$ if and only if there exist integers $r_{\ell j}$ such that Equation (6) holds. However, according to Lemma 2 every element of R has a unique representation in terms of 1, u, $\ldots$, u^{n-1}. We rewrite the left hand side of Equation (6) in order to express the coefficients of the u^ℓ as R-linear combinations of the elements $a_{\ell j}$. This further allows us to set up an equation system in the indeterminates $r_{\ell j}$. Then b is contained in I if and only if this linear equation system over $\mathbb{Z}$ is solvable. Moreover, if a solution exists, we can use it to determine the elements r_i in Equation (5) explicitly.

Remark. A straightforward multiplication of the left hand side of Equation (6) yields a polynomial in u of degree $2n-2$. We need to ensure that the degree of a polynomial is at most $n-1$. Therefore, we determine $w_{\ell h} \in \mathbb{Z}$ such that

$$u^{n+h} = \sum_{\ell=0}^{n-1} w_{\ell h} u^\ell$$

for $1 \leq h \leq n-2$. Consider

$$\begin{aligned} u^{n+h} &= u \cdot u^{n+h-1} = \sum_{\ell=0}^{n-1} w_{\ell(h-1)} u^{\ell+1} \\ &= w_{(n-1)(h-1)} u^n + \sum_{\ell=1}^{n-1} w_{(\ell-1)(h-1)} u^\ell \\ &= \sum_{\ell=0}^{n-1} w_{(n-1)(h-1)} \cdot w_{\ell 0} \cdot u^\ell + \sum_{\ell=1}^{n-1} w_{(\ell-1)(h-1)} \cdot u^\ell. \end{aligned}$$

Thus, we can determine $w_{\ell h}$ recursively as

$$w_{\ell h} = \begin{cases} 0 & \text{if } \ell < 0 \\ f_\ell & \text{if } h = 0 \\ w_{(n-1)(h-1)} w_{\ell 0} + w_{(\ell-1)(h-1)} & \text{if } 1 \leq h \leq n-2 \end{cases}. \tag{7}$$

Lemma 2. *Let R be a ring as defined above. Then every $r \in R$ has a unique representation in terms of $1, u, \ldots, u^{n-1}$.*

Proof. Let $f = X^n - \sum_{\ell=0}^{n-1} f_\ell X^\ell \in \mathbb{Z}[X] \in \mathbb{Q}[X]$ with $f(u) = 0$. Then u has a minimal polynomial over $\mathbb{Q}[X]$. Further, let

$$J = \{\, g \in \mathbb{Q}[X] \mid g(u) = 0 \,\} \lhd \mathbb{Q}[X]$$

where $J \neq \langle 0 \rangle$ because $f \in J$.

Claim. *The polynomial f is the minimal polynomial of u in $\mathbb{Q}[X]$.*

Proof. Since $J \neq \langle 0 \rangle$, there exists a monic and irreducible polynomial $h \in \mathbb{Q}[X] \setminus \mathbb{Q}[X]^\times$ such that $J = \langle h \rangle$. Then h is the minimal polynomial of u in $\mathbb{Q}[X]$ and $h | g$ for all g with $g(u) = 0$. In particular, $h | f$. We want to show that $h = f$ by showing that f is irreducible in $\mathbb{Q}[X]$ and therefore the minimal polynomial.

We know the polynomial f is irreducible and primitive in $\mathbb{Z}[X]$ because n is minimal and $f_n = 1$.

Assume f is reducible in $\mathbb{Q}[X]$. Since $h | f$, there exists a $g \in \mathbb{Q}[X] \setminus \mathbb{Q}[X]^\times$ such that $f = gh$. Note that $\deg(g), \deg(h) \geq 1$.

Let $a, b \in \mathbb{Z}$ such that $ag = g_1 \in \mathbb{Z}[X]$ and $bh = h_1 \in \mathbb{Z}[X]$. Let $\operatorname{cont}(p)$ denote the content of a polynomial p. Then there exist primitive polynomials g_2 and h_2 such that $g_1 = \operatorname{cont}(g_1) g_2$ and $h_1 = \operatorname{cont}(h_1) h_2$. Further note that $\deg(a) = \deg(b) = \deg(\operatorname{cont}(g_1)) = \deg(\operatorname{cont}(h_1)) = 0$ for $a, b, \operatorname{cont}(g_1), \operatorname{cont}(h_1) \in \mathbb{Z}[X]$. Hence, $\deg(g) = \deg(g_1) = \deg(g_2)$ and

$\deg(h) = \deg(h_1) = \deg(h_2)$. Now we have in $\mathbb{Z}[X]$ the equation $abf = g_1 h_1$. Thus, there exists a unit e such that

$$eab = \operatorname{cont}(abf) = \operatorname{cont}(g_1 h_1) = \operatorname{cont}(g_1)\operatorname{cont}(h_1).$$

Then, $abf = g_1 h_1 = eabg_2 h_2$ where $g_2, h_2 \in \mathbb{Z}[X]$ with $\deg(g_2), \deg(h_2) \geq 1$. Therefore, $f = eg_2 h_2$ and g_2 and h_2 are no units which contradicts f being irreducible in $\mathbb{Z}[X]$. Thus, f is irreducible in $\mathbb{Q}[X]$ as well and $f = h$ is the minimal polynomial of u in $\mathbb{Q}[X]$. □

Let $r \in R$ be ambiguous, i.e. $r = \sum_{\ell=0}^{n-1} r_\ell X^\ell$ and $r = \sum_{\ell=0}^{n-1} s_\ell X^\ell$. Then

$$\sum_{\ell=0}^{n-1} r_\ell u^\ell = \sum_{\ell=0}^{n-1} s_\ell u^\ell \implies \sum_{\ell=0}^{n-1} (r_\ell - s_\ell) u^\ell = 0.$$

Hence, define the polynomial p as

$$p = \sum_{\ell=0}^{n-1} (r_\ell - s_\ell) X^\ell.$$

Since $p(u) = 0$, it is an ideal element $p \in J$. Thus, the minimal polynomial f divides p. From $f|p$ and $\deg(f) = n > n-1 = \deg(p)$ follows $p = 0$ because f is the minimal polynomial. Further, $p = 0$ holds if and only if $r_i = s_i$ for every $0 \leq i \leq n-1$. Therefore, $r \in R$ is uniquely determined. □

5.1 Representation of an ideal element

Let $a_1, \ldots, a_m \in R$ such that $\langle a_1, \ldots, a_m \rangle = I \triangleleft R$. Then any element $v \in I$ is of form

$$v = \sum_{j=1}^{m} x_j a_j \tag{8}$$

with $x_1, \ldots, x_m \in R$. Further, let $x_{0j}, \ldots, x_{(n-1)j} \in \mathbb{Z}$ and $a_{0j}, \ldots, a_{(n-1)j} \in \mathbb{Z}$ such that $x_j = \sum_{\ell=0}^{n-1} x_{\ell j} u^\ell$ and $a_j = \sum_{\ell=0}^{n-1} a_{\ell j} u^\ell$. Since $v \in R$, there exist $v_1, \ldots, v_{n-1} \in \mathbb{Z}$ such that

$$v = \sum_{\ell=0}^{n-1} v_\ell u^\ell. \tag{9}$$

Consider

$$x_j \cdot a_j = \left(\sum_{\ell=0}^{n-1} x_{\ell j} u^\ell \right) \cdot \left(\sum_{\ell=0}^{n-1} a_{\ell j} u^\ell \right) = \sum_{h=0}^{2n-2} \left(\sum_{i=0}^{h} x_{ij} a_{(h-i)j} \right) u^h, \tag{10}$$

where $x_{ij} = a_{ij} = 0$ for $i \geq n$. We can split this sum into two parts,

$$x_j a_j = \sum_{h=0}^{n-1} \left(\sum_{i=0}^{h} x_{ij} \cdot a_{(h-i)j} \right) u^h + \sum_{h=n}^{2n-2} \left(\sum_{i=0}^{h} x_{ij} \cdot a_{(h-i)j} \right) u^h \tag{11}$$

where the first part has already the form of Equation (9). So we have to work on the second part. First, simplify the summation

$$\sum_{i=0}^{h} x_{ij} \cdot a_{(h-i)j} \tag{12}$$

by removing zero-value terms. As stated above, $x_{ij} = 0$ for every $i \geq n$. Hence, it is sufficient to sum over all $x_{ij}a_{(h-i)j}$ with i from 0 to $n-1$. Values of $a_{(h-i)j}$ equal 0 for all $h - i \geq n \iff i \leq h - n$. Thus, we consider only $x_{ij}a_{(h-i)j}$ with i from $h - n + 1$ to $n - 1$, i.e.

$$\sum_{i=h-n+1}^{n-1} x_{ij} \cdot a_{(h-i)j} \tag{13}$$

Now replace Equation (12) by Equation (13) to get a simpler second part

$$\sum_{h=n}^{2n-2} \left(\sum_{i=h-n+1}^{n-1} x_{ij} \cdot a_{(h-i)j} \right) u^h.$$

Next, we perform an index shift to get

$$\sum_{h=0}^{n-2} \left(\sum_{i=h+1}^{n-1} x_{ij} \cdot a_{(h+n-i)j} \right) u^{h+n}. \tag{14}$$

The elements u^{h+n} are elements of R and therefore there exist $w_{\ell h} \in \mathbb{Z}$ such that

$$u^{n+h} = \sum_{\ell=0}^{n-1} w_{\ell h} u^{\ell}. \tag{15}$$

We fix h and use Equation (15) in the inner sum of Equation (14) to receive

$$\left(\sum_{i=h+1}^{n-1} x_{ij} \cdot a_{(h+n-i)j} \right) \left(\sum_{\ell=0}^{n-1} w_{\ell h} \cdot u^{\ell} \right) = \sum_{i=h+1}^{n-1} \sum_{\ell=0}^{n-1} x_{ij} \cdot a_{(h+n-i)j} \cdot w_{\ell h} \cdot u^{\ell}.$$

Now, we can insert this into Equation (14) and change the summation order to get

$$\begin{aligned}&\sum_{h=0}^{n-2}\sum_{i=h+1}^{n-1}\left(\sum_{\ell=0}^{n-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h}\cdot u^{\ell}\right)\\ =&\sum_{\ell=0}^{n-1}\left(\sum_{h=0}^{n-2}\sum_{i=h+1}^{n-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h}\right)u^{\ell}\end{aligned}$$

Finally, the second part of Equation (11) has also the desired representation and we can merge the two parts and receive

$$\begin{aligned}x_j a_j &= \sum_{h=0}^{n-1}\left(\sum_{i=0}^{h} x_{ij}\cdot a_{(h-i)j}\right)u^h + \sum_{\ell=0}^{n-1}\left(\sum_{h=0}^{n-2}\sum_{i=h+1}^{n-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h}\right)u^{\ell}\\ &= \sum_{\ell=0}^{n-1}\left(\sum_{i=0}^{\ell} x_{ij}\cdot a_{(\ell-i)j} + \sum_{h=0}^{n-2}\sum_{i=h+1}^{n-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h}\right)u^{\ell}.\end{aligned}$$

Inserting this into Equation (8) and changing the summation order gives us a representation for any element $v \in I$

$$\begin{aligned}v &= \sum_{j=1}^{m} x_j a_j\\ &= \sum_{j=1}^{m}\sum_{\ell=0}^{n-1}\left(\sum_{i=0}^{\ell} x_{ij}\cdot a_{(\ell-i)j} + \sum_{h=0}^{n-2}\sum_{i=h+1}^{n-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h}\right)u^{\ell}\\ &= \sum_{\ell=0}^{n-1}\sum_{j=1}^{m}\left(\sum_{i=0}^{\ell} x_{ij}\cdot a_{(\ell-i)j} + \sum_{h=0}^{n-2}\sum_{i=h+1}^{n-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h}\right)u^{\ell} \qquad (16)\\ &= \sum_{\ell=0}^{n-1} v_{\ell} u^{\ell}.\end{aligned}$$

Hence, we have an explicit form for v_ℓ depending on x_{ij} and a_{ij}, i.e.

$$v_{\ell} = \sum_{j=1}^{m}\left(\sum_{i=0}^{\ell} x_{ij}\cdot a_{(\ell-i)j} + \sum_{h=0}^{n-2}\sum_{i=h+1}^{n-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h}\right) \qquad (17)$$

5.2 Solving the Ideal Membership question as a Linear Diophantine Equation System

Our goal is to determine whether an element $b \in R$ lies in $I = \langle a_1, \dots a_m\rangle$ with $a_j \in R$ for all $1 \leq j \leq m$. Moreover, let $a_{\ell j}$, $b_j \in \mathbb{Z}$ such that $a_j = \sum_{\ell=0}^{n-1} a_{\ell j} u^{\ell}$ and $b = \sum_{\ell=0}^{n-1} b_{\ell} u^{\ell}$.

According to Section 5.1, if $b \in I$, then there exist $x_{ij} \in \mathbb{Z}$ such that

$$b_\ell = \sum_{j=1}^{m} \left(\sum_{i=0}^{\ell} x_{ij} \cdot a_{(\ell-i)j} + \sum_{h=0}^{n-2} \sum_{i=h+1}^{n-1} x_{ij} \cdot a_{(h+n-i)j} \cdot w_{\ell h} \right) \tag{18}$$

for $1 \leq \ell \leq n-1$.

On the other hand the elements b_ℓ are uniquely determined according to Lemma 2. Hence $b \in I$ if and only if the elements $x_{ij} \in \mathbb{Z}$ exist.

In order to decide whether b is an element of I, it suffices to decide whether the equation system (18) in the unknowns x_{ij} has a solution. If this is the case, we are even capable to determine $x_j \in R$ with $b = \sum_{j=1}^{m} x_j a_j$, see Section 5.1.

We want to translate this explicit form into an equation system of form $M\mathbf{x} = \mathbf{b}$ where M is a matrix and

$$\mathbf{x} = (x_{01}, \ldots, x_{(n-1)1}, x_{02}, \ldots, x_{(n-1)(m-1)}, x_{0m}, \ldots, x_{(n-1)m})^t$$

and $\mathbf{b} = (b_0, \ldots, b_{n-1})^t$.

In order to determine M we need to rewrite

$$\sum_{h=0}^{n-2} \sum_{i=h+1}^{n-1} x_{ij} \cdot a_{(h+n-i)j} \cdot w_{\ell h}$$

in Equation (18). The following lemma turns out to be useful.

Lemma 3. *Let $k \in \mathbb{N}$ and $a_{ij} \in \mathbb{Z}$ for $0 \leq i, j \leq k$. Then*

$$\sum_{i=0}^{k} \sum_{j=i}^{k} a_{ji} = \sum_{j=0}^{k} \sum_{i=0}^{j} a_{ji}.$$

Proof.

$$\begin{aligned}
\sum_{i=0}^{k} \sum_{j=i}^{k} a_{ji} &= \sum_{i=0}^{k} (a_{ii} + a_{(i+1)i} + \cdots + a_{(k-1)i} + a_{ki}) \\
&= \sum_{i=0}^{k} a_{ki} + \sum_{i=0}^{k-1} a_{(k-1)i} + \cdots + \sum_{i=0}^{1} a_{1i} + \sum_{i=0}^{0} a_{0i} \\
&= \sum_{j=0}^{k} \sum_{i=0}^{j} a_{ji}
\end{aligned}$$

□

Using Lemma 3 and two index shifts we get

$$\begin{aligned}
&\sum_{h=0}^{n-2}\sum_{i=h+1}^{n-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h}\\
=&\sum_{h=0}^{n-2}\sum_{i=h}^{n-2} x_{(i+1)j}\cdot a_{(h+n-i-1)j}\cdot w_{\ell h}\\
=&\sum_{i=0}^{n-2}\sum_{h=0}^{i} x_{(i+1)j}\cdot a_{(h+n-i-1)j}\cdot w_{\ell h}\\
=&\sum_{i=1}^{n-1}\sum_{h=0}^{i-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h} \qquad (19)
\end{aligned}$$

Now we can insert Equation (19) into the equation system (18) to receive

$$b_\ell = \sum_{j=1}^{m}\left(\sum_{i=0}^{\ell} x_{ij}\cdot a_{(\ell-i)j} + \sum_{i=1}^{n-1}\sum_{h=0}^{i-1} x_{ij}\cdot a_{(h+n-i)j}\cdot w_{\ell h}\right)$$

It follows now that $b \in I$ if and only if the equation system $M\mathbf{x} = \mathbf{b}$ is solvable where M is defined for $0 \le \ell < n$ as

$$m_{(\ell+1)(\nu+1)} = \begin{cases} a_{\ell j} & \text{if } \nu = n(j-1) \\ a_{(\ell-i)j} + \sum_{h=0}^{i-1} a_{(h+n-i)j} w_{\ell h} & \text{if } \nu = n(j-1)+i \text{ for } 1 \le i \le \ell \\ \sum_{h=0}^{i-1} a_{(h+n-i)j} w_{\ell h} & \text{if } \nu = n(j-1)+i \text{ for } \ell < i < n \end{cases}. \qquad (20)$$

We can now answer the question using the results of Section 3. We transform the matrix M with the Smith Normal Form algorithm into the diagonal matrix D. Since M is an $n \times mn$ matrix, we need to expand the Hermite Normal Form algorithm for matrices with more columns than rows. First, we perform the Hermite Normal Form algorithm as described in Section 4 for the first n rows and columns. Then, if $m > 1$, we need to additionally transform all entries of the remaining $mn - m$ columns into 0. For every column $m < j \le n$ and for every row $1 \le k \le m$, replace m_{kk} by the greatest common divisor of m_{kk} and m_{kj}, and transform m_{kj} into 0.

Use the matrix U from $D = UMV$ to compute $c = Ub$. Then we can check the conditions for solvability. There have to exist $y_1, \ldots, y_r \in \mathbb{Z}$ such that

$$\begin{aligned} d_i y_i &= c_i && (i = 1, \ldots, r) \\ 0 &= c_j && (j = r+1, \ldots, mn). \end{aligned}$$

If the conditions do not hold, b is not an element in I. If the conditions hold, we can easily compute $x_1, \ldots, x_m$ by the equations system $x = Vy$. Recall that as stated in Theorem 3, y, and therefore x, are not necessarily unique.

6 Example

In this section we demonstrate how the Ideal Membership problem can be solved by transforming it into a Linear Diophantine Equation System.

Let $u = \sqrt{-5} \in \mathbb{C} \setminus \mathbb{Z}$ and $f(X) = 1 \cdot X^2 - 0 \cdot X^1 - 5 \cdot X^0$. Then $f(u) = 0$ and

$$R = \{\, v_0 + v_1 u \,|\, v_0, v_1 \in \mathbb{Z} \,\}$$

is a commutative ring with unique elements. Further, let $I = \langle 2, 1 + \sqrt{-5} \rangle$ be an ideal of R. Then we have

$$\begin{aligned} f_0 &= -5 & a_{01} &= 2 & a_{02} &= 1 \\ f_1 &= 0 & a_{11} &= 0 & a_{12} &= 1 \end{aligned}$$

and compute recursively the integers $w_{\ell h}$ which we defined in Equation (7)

$$\begin{aligned} w_{00} &= -5 \\ w_{10} &= 0. \end{aligned}$$

Now we use Equation (20) to construct the matrix M

$$M = \begin{pmatrix} a_{01} & a_{11} \cdot w_{00} & a_{02} & a_{12} \cdot w_{00} \\ a_{11} & a_{01} + a_{11} \cdot w_{10} & a_{12} & a_{02} + a_{12} \cdot w_{10} \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 & -5 \\ 0 & 2 & 1 & 1 \end{pmatrix}.$$

6.1 Compute the Smith Normal Form

Compute the Left Hermite Normal Form of the first column

$$M_1 = \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \qquad U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Since this vector is already in Left Hermite Normal Form, we will skip the process of transforming it into Left Hermite Normal Form. Next, we need to compute the Hermite Normal form of

$$A = M_{(1)} = \begin{pmatrix} 2 & 0 & 1 & -5 \\ 0 & 2 & 1 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since $A^{(1)} = \begin{pmatrix} 2 \end{pmatrix}$ and $A^{(2)} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$ are already in Hermite Normal Form, we consider

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

The greatest common divisor r of a_{11} and a_{13} is $\gcd(2,1) = 1 = 0 \cdot 2 + 1 \cdot 1$. Hence,

$$r = 1 \qquad p = 0 \qquad q = 1.$$

Next we transform the first and third column such that a_{11} becomes the greatest common divisor of a_{11} and a_{13}, and a_{13} becomes 0.

$$\begin{aligned} M_1 &= p \cdot M_1 + q \cdot M_3 \\ &= \frac{0}{1} \cdot \begin{pmatrix} 2 \\ 0 \end{pmatrix} + \frac{1}{1} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad V_1 = 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} M_3 &= \frac{m_{11}}{r} M_3 - \frac{m_{13}}{r} M_1 \\ &= \frac{2}{1} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \frac{1}{1} \cdot \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \quad V_3 = 2 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} - 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix} \end{aligned}$$

Then we receive

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 2 \end{pmatrix}, \qquad V = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now we repeat this for the second row with a_{22} and a_{23}. The greatest common divisor of those two entries is $r = \gcd(a_{22}, a_{23}) = 2 = 0 \cdot 2 + 1 \cdot 2$. Hence,

$$r = 2 \qquad p = 0 \qquad q = 1.$$

We transform the second and third column

$$M_2 = 0 \cdot \begin{pmatrix} 0 \\ 2 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \quad V_2 = 0 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix}$$

$$M_3 = \frac{2}{2} \cdot \begin{pmatrix} 0 \\ 2 \end{pmatrix} - \frac{2}{2} \cdot \begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad V_3 = 1 \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix} - 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ 2 \\ 0 \end{pmatrix}$$

and receive

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \end{pmatrix}, \qquad V = \begin{pmatrix} 0 & -1 & -1 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

This time we have entries to the left of the diagonal entry. Therefore, we need to subtract the diagonal entry of the entries to its left until the fulfill Equation (4). This concerns the second entry of the first column $a_{21} = 1 \geq 0$.

$$\begin{aligned} A_1 &= A_1 - \left\lceil \frac{a_{21}}{a_{22}} \right\rceil \cdot A_2 \\ &= \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \underbrace{\left\lceil \frac{1}{2} \right\rceil}_{=1} \cdot \begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad V_1 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} - 1 \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} \end{aligned}$$

Now we have $\begin{pmatrix} 1 & 0 & 0 \\ -1 & 2 & 0 \end{pmatrix}$ in Hermite Normal Form and

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

Add the last column and repeat the previous process for $\begin{pmatrix} 1 & 0 & 0 & -5 \\ -1 & 2 & 0 & 1 \end{pmatrix}$.
For the first and fourth column we get

$$r = 1 \qquad p = 1 \qquad q = 0.$$

and

$$M_1 = 1 \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} + 0 \cdot \begin{pmatrix} -5 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \quad V_1 = 1 \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}$$

$$M_4 = \frac{1}{1} \cdot \begin{pmatrix} -5 \\ 1 \end{pmatrix} + \frac{5}{1} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ -4 \end{pmatrix}, \quad V_4 = 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} + 5 \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} +5 \\ 0 \\ -5 \\ 1 \end{pmatrix}.$$

Thus, we have

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 2 & 0 & -4 \end{pmatrix}, \qquad V = \begin{pmatrix} 1 & -1 & -1 & 5 \\ 0 & 0 & -1 & 0 \\ -1 & 2 & 2 & -5 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and proceed with the second and fourth column. This time we have

$$r = 2 \qquad p = 1 \qquad q = 0.$$

and

$$M_2 = 1 \cdot \begin{pmatrix} 0 \\ 2 \end{pmatrix} + 0 \cdot \begin{pmatrix} 0 \\ -4 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \quad V_2 = 1 \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} 5 \\ 0 \\ -5 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix}$$

$$M_4 = \frac{2}{2} \cdot \begin{pmatrix} 0 \\ -4 \end{pmatrix} + \frac{4}{2} \cdot \begin{pmatrix} 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \quad V_4 = 1 \cdot \begin{pmatrix} 5 \\ 0 \\ -5 \\ 1 \end{pmatrix} + 2 \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ -1 \\ 1 \end{pmatrix}.$$

Finally, matrix $M_{(1)}$ is in Hermite Normal Form.

$$M_{(1)} = A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 2 & 0 & 0 \end{pmatrix}, \qquad V = \begin{pmatrix} 1 & -1 & -1 & 3 \\ 0 & 0 & -1 & 0 \\ -1 & 2 & 2 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Still, there is a non-zero entry other than a_{11} in the first column. And because we want to compute the Smith Normal Form of M, we have to

apply the algorithms of Left Hermite Normal Form and Hermite Normal Form again.

Compute the Left Hermite Normal Form of the first column

$$M_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

We know $\mathrm{LHNF}(A') = \mathrm{HNF}((A')^t)^t$. Hence, compute the Hermite Normal Form of $A' = M_1^t = \begin{pmatrix} 1 & -1 \end{pmatrix}$. The greatest common divisor of 1 and -1 is

$$r = 1 \qquad p = 0 \qquad q = -1.$$

And thus,

$$A'_1 = 0 \cdot \begin{pmatrix} 1 \end{pmatrix} - 1 \cdot \begin{pmatrix} -1 \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix}, \qquad U_1^t = 0 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} - 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$$

$$A'_2 = \frac{1}{1} \cdot \begin{pmatrix} -1 \end{pmatrix} + \frac{1}{1} \cdot \begin{pmatrix} 1 \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}, \qquad U_2^t = 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} + 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix},$$

which gives

$$M_1^t = A' = \begin{pmatrix} 1 & 0 \end{pmatrix}, \qquad U^t = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Note that we need to apply the elementary row operations, which we used for the Left Hermite Normal Form of the first column, to all other columns as well. Therefore, we take the computation of M which we got before performing the Left Hermite Normal Form algorithm and multiply it from left with U where U represents the elementary row operations,

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

Then we apply one more time the Hermite Normal Form algorithm to M,

$$r = 1, \qquad p = 1, \qquad q = 0.$$

Next compute

$$M_1 = 1 \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} -2 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad V_1 = 1 \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + 0 \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}$$

$$M_2 = \frac{1}{1} \cdot \begin{pmatrix} -2 \\ 2 \end{pmatrix} + \frac{2}{1} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \quad V_2 = 1 \cdot \begin{pmatrix} -1 \\ 0 \\ 2 \\ 0 \end{pmatrix} + 2 \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

So, in the end we have determined the Smith Normal Form D of the given matrix M

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}, \qquad U = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \qquad V = \begin{pmatrix} 1 & 1 & -1 & 3 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

6.2 How to determine whether b is an ideal element

Let $b_1 = 6 + \sqrt{-5}$ and $b_2 = 6 + 2\sqrt{-5}$. Then

$$b_1 = \begin{pmatrix} 6 \\ 1 \end{pmatrix} \qquad\qquad b_2 = \begin{pmatrix} 6 \\ 2 \end{pmatrix}.$$

Now transform b_1, b_2 to c_1, c_2, respectively.

$$c_1 = U \cdot b_1 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 7 \end{pmatrix}$$

$$c_2 = U \cdot b_2 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 6 \\ 2 \end{pmatrix} = \begin{pmatrix} -2 \\ 8 \end{pmatrix}$$

Check whether the Linear Diophantine Equation System is solvable for b_1 and b_2. Since

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} -1 \\ 7 \end{pmatrix} \iff 1 \cdot y_1 = -1 \ \wedge \ 2 \cdot y_2 = 7$$

has no integer solution for y_2, we conclude that $6 + \sqrt{-5} \notin \langle 2, 1 + \sqrt{-5} \rangle$, i.e. b_1 is not an ideal element.

But because

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} -2 \\ 8 \end{pmatrix} \iff 1 \cdot y_1 = -2 \ \wedge \ 2 \cdot y_2 = 8$$

yields integer solutions for y_1 and y_2, we conclude that $6+2\sqrt{-5} \in \langle 2, 1 + \sqrt{-5} \rangle$, i.e. b_2 is an ideal element. Furthermore, we can determine the linear combination of b_2 in terms of the ideal generators. Take the unique solutions $y_1 = -2$ and $y_2 = 4$, and choose y_3 and y_4 arbitrarily. Let $y_3 = y_4 = 1$. Then compute $x = V \cdot y$

$$\begin{pmatrix} x_{01} \\ x_{11} \\ x_{02} \\ x_{12} \end{pmatrix} = \begin{pmatrix} 1 & 1 & -1 & 3 \\ 0 & 0 & -1 & 0 \\ -1 & 0 & 2 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 \\ 4 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 4 \\ -1 \\ 3 \\ 1 \end{pmatrix}.$$

This results in $x_1 = 4 - \sqrt{-5}$ and $x_2 = 3 + \sqrt{-5}$ for $b_2 = x_1 \cdot a_1 + x_2 \cdot a_2$. Now write b_2 as linear combination of ideal generators, i.e.

$$\begin{aligned} (4 - \sqrt{-5}) \cdot 2 + (3 + \sqrt{-5})(1 + \sqrt{-5}) &= 8 - 2\sqrt{-5} + 3 + 3\sqrt{-5} + \sqrt{-5} - 5 \\ &= 6 + 2\sqrt{-5} = b_2. \end{aligned}$$

We determined that $b_2 \in I$ and received solutions x_1, x_2 such that we can represent b_2 as linear combination of ideal generators.

References

[1] William A. Adkins and Steven H. Weintraub. *Algebra*. Vol. 136. Graduate Texts in Mathematics. An approach via module theory. Springer-Verlag, New York, 1992. ISBN: 0-387-97839-9.

[2] "Polynomial algorithms for computing Smith and Hermite normal forms of an integer matrix". In: *SIAM J. Computing* 8.4 (1979).

[3] B.L. van der Waerden. *Algebra*. 5th ed. Vol. 2. Springer-Verlag, New York, 2003. ISBN: 978-0-387-40625-5.

A Proof that R is a ring

Let $u \in \mathbb{C} \setminus \mathbb{Z}$ be an element such that there exist $f_0, \dots, f_{n-1} \in \mathbb{Z}$ with $u^n = \sum_{\ell=0}^{n-1} f_\ell u^\ell$. Moreover, assume n to be minimal. Then,

$$R = \left\{ \sum_{\ell=0}^{n-1} v_\ell u^\ell \,\middle|\, v_0, \dots, v_{n-1} \in \mathbb{Z} \right\}$$

is a ring. For $r \in R$ we write $r = \sum_{\ell=0}^{n-1} r_\ell u^\ell$, $r_0, \dots, r_{n-1} \in \mathbb{Z}$.

$(R, +)$ is an Abelian group

We show that $(R, +)$ is an Abelian group.

closed For every $a, b \in R$

$$a + b = \sum_{\ell=0}^{n-1} a_\ell u^\ell + \sum_{\ell=0}^{n-1} b_\ell u^\ell = \sum_{\ell=0}^{n-1} (a_\ell + b_\ell) u^\ell \in R$$

Note that $a_\ell + b_\ell \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under the operation $+$.

associative For every $a, b, c \in R$

$$a + (b + c) = \sum_{\ell=0}^{n-1} a_\ell u^\ell + \left(\sum_{\ell=0}^{n-1} b_\ell u^\ell + \sum_{\ell=0}^{n-1} c_\ell u^\ell \right) = \sum_{\ell=0}^{n-1} \underbrace{(a_\ell + (b_\ell + c_\ell))}_{\in \mathbb{Z}} u^\ell \tag{21}$$

Since $(\mathbb{Z}, +)$ is a commutative group, $a_\ell + (b_\ell + c_\ell) = (a_\ell + b_\ell) + c_\ell$. Thus, also $(R, +)$ is associative.

commutative For every $a, b \in R$

$$a + b = \sum_{\ell=0}^{n-1} a_\ell u^\ell + \sum_{\ell=0}^{n-1} b_\ell u^\ell = \sum_{\ell=0}^{n-1} \underbrace{(a_\ell + b_\ell)}_{\in \mathbb{Z}} u^\ell$$

Again by $(\mathbb{Z}, +)$ being a commutative group, $(R, +)$ is commutative.

neutral element There exists an $e^+ \in R$ with $e_0^+ = \dots = e_{n-1}^+ = 0 \in \mathbb{Z}$ such that for all $a \in R$

$$a + e^+ = \sum_{\ell=0}^{n-1} a_\ell u^\ell + \sum_{\ell=0}^{n-1} e_\ell^+ u^\ell = \sum_{\ell=0}^{n-1} \underbrace{(a_\ell + e_\ell^+)}_{=a_\ell} u^\ell = a$$

We already know that $(R, +)$ is commutative. Thus, $e + a = a + e = a$ and $(R, +)$ has a neutral element e^+.

inverse element For every $a \in R$ exists an $-a \in R$ such that

$$a + (-a) = \sum_{\ell=0}^{n-1} a_\ell u^\ell + \sum_{\ell=0}^{n-1} (-a_\ell) u^\ell = \sum_{\ell=0}^{n-1} \underbrace{(a_\ell - a_\ell)}_{=0=e_\ell} u^\ell = e$$

We use again that $(R, +)$ is commutative to get $(-a)+a = a+(-a) = e$, i.e. every element in $(R, +)$ has an inverse element.

$(R, \cdot)$ is a commutative monoid

Now we show that $(R, \cdot)$ is a commutative monoid.

closed Define $w_{\ell h}$ from $u^{h+n} = \sum_{\ell=0}^{n-1} w_{\ell h} u^\ell$ as described in the Remark in Section 5,

$$w_{\ell h} = \begin{cases} 0 & \text{if } \ell < 0 \\ f_\ell & \text{if } h = 0 \\ w_{(n-1)(h-1)} w_{\ell 0} + w_{(\ell-1)(h-1)} & \text{if } 1 \le h \le n-2 \end{cases}.$$

For every $a, b \in R$

$$\begin{aligned} a \cdot b &= \sum_{\ell=0}^{n-1} a_\ell u^\ell \cdot \sum_{\ell=0}^{n-1} a_\ell u^\ell = \sum_{h=0}^{2n-2} \left(\sum_{i+j=h} a_i b_j \right) u^h \\ &= \sum_{h=0}^{n-1} \left(\sum_{i+j=h} a_i b_j \right) u^h + \sum_{h=n}^{2n-2} \left(\sum_{i+j=h} a_i b_j \right) u^h \\ &= \sum_{h=0}^{n-1} \left(\sum_{i+j=h} a_i b_j \right) u^h + \sum_{h=0}^{n-2} \left(\sum_{i+j=h+n} a_i b_j \right) u^{h+n} \\ &= \sum_{h=0}^{n-1} \left(\sum_{i+j=h} a_i b_j \right) u^h + \sum_{h=0}^{2n-2} \left(\sum_{i+j=h+n} a_i b_j \right) \left(\sum_{\ell=0}^{n-1} w_{\ell h} u^\ell \right) \\ &= \sum_{h=0}^{n-1} \left(\sum_{i+j=h} a_i b_j \right) u^h + \sum_{\ell=0}^{n-1} \left(\sum_{h=0}^{2n-2} \sum_{i+j=h+n} a_i b_j w_{\ell h} \right) u^\ell \end{aligned}$$

From $(\mathbb{Z}, +, \cdot)$ being a commutative ring with 1 follows that $a \cdot b \in R$.

associative For every $a, b, c \in R$

$$a(b \cdot c) = \sum_{\ell=0}^{n-1} a_\ell u^\ell \left(\sum_{\ell=0}^{n-1} b_\ell u^\ell \cdot \sum_{\ell=0}^{n-1} c_\ell u^\ell \right) = \sum_{\ell=0}^{n-1} a_\ell u^\ell \cdot \sum_{\ell=0}^{2n-n} \left(\sum_{j+k=\ell} b_j c_k \right) u^\ell$$
$$= \sum_{\ell=0}^{3n-3} \left(\sum_{i+j+k=\ell} a_i b_j c_k \right) u^\ell \tag{22}$$

We do the same for $(a \cdot b)c$ and see that both result in Equation (22). Therefore, $(R, \cdot)$ is associative.

commutative For every $a, b \in R$

$$a \cdot b = \sum_{\ell=0}^{n-1} a_\ell u^\ell \cdot \sum_{\ell=0}^{n-1} b_\ell u^\ell = \sum_{\ell=0}^{2n-2} \left(\sum_{i+j=\ell} a_i b_j \right) u^\ell$$

Since $(\mathbb{Z}, \cdot)$ is commutative, $(R, \cdot)$ is also commutative.

neutral element There exists an $e \in R$ with $v_0 = 1$ and $v_1 = \cdots = v_{n-1} = 0$ such that for every $a \in R$

$$a \cdot e = \sum_{\ell=0}^{n-1} a_\ell u^\ell \cdot \sum_{\ell=0}^{n-1} e_\ell u^\ell = \sum_{\ell=0}^{2n-2} \left(\sum_{i+j=\ell} a_i e_j \right) u^\ell \tag{23}$$

Since $e_j = 0$ for $j \neq 0$, we only need to consider the case $j = 0$. So the only values that contribute to the sum are a_i for $i = \ell$. Thus, Equation (23) equals a. By $(R, \cdot)$ being commutative, also $e \cdot a = a \cdot e = a$ and $(R, \cdot)$ has a neutral element e.

$(R, +, \cdot)$ fulfills the distributive law

We show that $(R, +, \cdot)$ is distributive.

$$a(b + c) = \sum_{\ell=0}^{n-1} a_\ell u^\ell \cdot \sum_{\ell=0}^{n-1} (b_\ell + c_\ell) u^\ell = \sum_{\ell=0}^{2n-2} \left(\sum_{i+j=\ell} a_i (b_j + c_j) \right) u^\ell$$

equals

$$a \cdot b + a \cdot c = \sum_{\ell=0}^{2n-2} \left(\sum_{i+j=\ell} a_i b_j \right) u^\ell + \sum_{\ell=0}^{2n-2} \left(\sum_{i+j=\ell} a_i c_j \right) u^\ell = \sum_{\ell=0}^{2n-2} \left(\sum_{i+j=\ell} a_i b_j + a_i c_j \right) u^\ell$$

because $(\mathbb{Z}, +, \cdot)$ fulfills the distributive law. Also, $(a + b)c = ac + bc$ can be shown analogously. Thus, $(R, +, \cdot)$ is a commutative ring with 1.