Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

LINEAR SYSTEMS OF DIOPHANTINE EQUATIONS*

FERNANDO SZECHTMAN†

Abstract. Given free modules $M \subseteq L$ of finite rank $f \geq 1$ over a principal ideal domain R, we give a procedure to construct a basis of L from a basis of M assuming the invariant factors or elementary divisors of L/M are known. Given a matrix $A \in M_{m,n}(R)$ of rank r, its nullspace L in R^n is a free R-module of rank $f = n - r$. We construct a free submodule M of L of rank f naturally associated with A and whose basis is easily computable, we determine the invariant factors of the quotient module L/M and then indicate how to apply the previous procedure to build a basis of L from one of M.

Key words. Linear system, Diophantine equation, Smith normal form.

AMS subject classifications. 11D04, 15A06.

1. Introduction.

Let R be a principal ideal domain. Given $f \in \mathbb{N}$, by a lattice of rank f we understand a free R-module L of rank f. By a sublattice of L, we mean a submodule M of L, necessarily free, also of rank f. In this case, L/M is a finitely generated torsion R-module.

In different settings, we may face the problem of having to construct a basis of L from a known basis $\{u_1, \dots, u_f\}$ of M. A prime example occurs when $R = \mathbb{Z}$, $L = \mathcal{O}_K$, the ring of integers of an algebraic number field K of degree f over $\mathbb{Q}$, $M = \mathbb{Z}[\theta]$, and $\{u_1, \dots, u_f\} = \{1, \theta, \dots, \theta^{f-1}\}$, where $\theta \in \mathcal{O}_K$ is chosen so that $\mathbb{Q}[\theta] = K$.

A general procedure to construct a basis of L from a known basis $\{u_1, \dots, u_f\}$ of M is available to us, provided we know the index $i(M, L)$ of M in L, which is the determinant of the matrix whose columns are the coordinates of any basis of M relative to any basis of L. This is determined up to multiplication by units only. Note that if $R = \mathbb{Z}$, then $|i(M, L)|$ is the order of the finite abelian group L/M.

If $i(M, L) = 1$, then $L = M$ has basis $\{u_1, \dots, u_f\}$. Suppose next $i(M, L) \neq 1$ and let $p \in R$ be a prime factor of $i(M, L)$. Then, L/M has a cyclic submodule isomorphic to R/Rp, so there exist $a_1, \dots, a_f \in \mathbb{Z}$, such that

$$v = \frac{a_1 u_1 + \cdots + a_f u_f}{p} \in L \setminus M. \tag{1.1}$$

Since $v \notin M$, we have $p \nmid a_i$ for some i and we assume for notational convenience that $i = 1$. Since $\gcd(p, a_1) = 1$, we can find $x, y \in R$ such that $xa_1 + yp = 1$. Here $ypv \in M$, so

$$xa_1 v = (1 - yp)v = v - ypv \notin M,$$

whence $xv \notin M$ and a fortiori $v' = xv + yu_1 \in L \setminus M$, where

$$v' = \frac{x(a_1 u_1 + \cdots + a_f u_f) + pyu_1}{p} = \frac{u_1 + xa_2 u_2 + \cdots + xa_f u_f}{p}.$$

*Received by the editors on October 23, 2021. Accepted for publication on January 21, 2022. Handling Editor: João Filipe Queiró.

†Department of Mathematics and Statistics, University of Regina, Canada (fernando.szechtman@gmail.com). Supported in part by an NSERC discovery grant.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

Thus, replacing v by a suitable R-linear combination of itself and u_1, namely v', we may suppose that $a_1 = 1$ in (1.1). Then, $\{v, u_2, \ldots, u_f\}$ is a basis for a sublattice, say P, of L such that $M \subset P$ and $i(M, P) = p$, so $i(P, L) = i(M, L)/p$. Repeating this process, we eventually arrive at a basis of L.

In this paper, we modify and improve this procedure, provided the invariant factors or elementary divisors of L/M are known, and we illustrate the use of this method with a concrete problem.

Indeed, let F be the field of fractions of R. Given a matrix $A \in M_{m,n}(R)$, we write T for the nullspace of A in F^n so that $S = T \cap R^n$ is the nullspace of A in R^n. We note that $L = S$ is a lattice of rank $f = n - r$, where r is the rank of A.

It is easy to find an F-basis of T from the reduced row echelon form, say E, of A. It is not clear at all how to use E to produce an R-basis of S. To achieve this, we first identify a sublattice M of L as well as a basis of M, naturally, in terms of E; we then compute the complete structure of the R-module L/M, namely its invariant factors, whose product is equal to $i(M, L)$; we finally indicate how to build a basis of L from the given basis of M by making use of the full structure of L/M.

Now if $r = n$, then E consists of the first n canonical vectors of R^m, and $L = 0$. On the other hand, if $r = 0$ then $E = 0$ and $L = R^n$. None of these cases is of any interest, so we assume throughout that $0 < r < n$.

In Sections 2, 3, 4, and 5, we use E to naturally produce a lattice U of rank f, a basis of U, and a nonzero scalar $d \in R$ such that $M = dU$ is a sublattice of L, and L is a sublattice of U. Moreover, we compute the full structures of L/M and U/L. Furthermore, in Section 6, we indicate how to use either the invariant factors or the elementary divisors of L/M to construct a basis of L from one of M (this is done for arbitrary L and M). In addition, if $d = p$ is a prime, we indicate in Section 7 how to produce a basis of L more or less directly from one of U. Examples can be found in Section 8.

We may summarize our study of S as follows: given the lattice S of all solutions of $AX = 0$ in R^n, we approximate S from below by a naturally occurring lattice of solutions M in R^n, we determine how far M is from S, and we describe how to bridge the gap between them. A like approach was recently utilized in [9] in the special case of a single linear homogeneous equation, that is, when $m = 1$, except that in [9] the approximation was taken from above, by means of U. The case $m = 1$ is necessarily simpler than the general case addressed here, as much in the computation of the structures of U/S and S/M as in the passage from a basis of a lattice to a basis of S, where the material from Section 6 not required.

As is well known (see the note at the end of [9, Section 4] in the special case $m = 1$), we may also find a basis of S by appealing to the Smith normal form D of A. There are $P \in \mathrm{GL}_m(R)$ and $Q \in \mathrm{GL}_n(R)$ such that $D = PAQ$. It is then trivial to find a basis, say $\mathcal{B}$, of the nullspace of D, whence $Q\mathcal{B}$ is a basis of the nullspace of A. This approach gives no information whatsoever on how far naturally occurring lattices of solutions of $AX = 0$ are from S, as provided in Theorem 5.1, or how to expand or shrink these lattices to reach S, as expounded in Section 6 or [9, Theorem 4.5].

Most of the literature on systems of linear diophantine equations is naturally focused on the case $R = Z$. One significant body of work is focused on nonnegative solutions, with applications to linear programming and combinatorial optimization. See [1], [2], [3], [4], [7], [10], and references therein.

Regarding lattices over the integers and their bases, a large body of literature is concerned with lattice basis reduction, which takes as input a basis of a lattice and aims at producing as output a new basis of

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

the same lattice with vectors that are short and nearly orthogonal. A celebrated algorithm of this kind is the LLL algorithm [6], which has a wide range of applications, such as in cryptanalysis, algorithmic number theory, factorization of polynomials with rational coefficients, integer linear programming, and many more. See the reference book [8] for comprehensive information on this subject.

2. Reduced matrices. A matrix $Z \in M_{m,n}(R)$ of rank r is said to be *reduced* if there are $0 \neq d \in R$ and $K \in M_{r,f}(R)$ such that

$$Z = \begin{pmatrix} dI_r & K \\ 0 & 0 \end{pmatrix}. \tag{2.2}$$

Two matrices $B, C \in M_{m,n}$ are *associated* if there are $L \in \mathrm{GL}_m(F)$ and $\Sigma \in \mathrm{GL}_n(F)$ such that Σ is a permutation matrix and $LB\Sigma = C$. This is clearly an equivalence relation.

LEMMA 2.1. *The given matrix A is associated with a reduced matrix.*

Proof. Let $Y \in M_{m,n}(F)$ be the reduced row echelon form of A. Multiplying Y by suitable element of R and permuting the columns of resulting matrix yields a reduced matrix associated with A. ∎

For the remainder of the paper, we fix a reduced matrix Z associated with A, say via that $LA\Sigma = Z$, and write $J = (dI_r\, K) \in M_{r,n}(R)$ for the matrix obtained from Z by eliminating its last $m-r$ rows. We let N stand for the nullspace of J in R^n so that $S = \Sigma N$ (thus, up to permutation of the variables $X_1, \dots, X_n$, our linear system is $JX = 0$).

3. Choice of a lattice. The linear system $JX = 0$ reads as follows:

$$\begin{aligned} dX_1 &= -(K_{1,1}X_{r+1} + \cdots + K_{1,f}X_n), \\ dX_2 &= -(K_{2,1}X_{r+1} + \cdots + K_{2,f}X_n), \\ &\vdots \\ dX_r &= -(K_{r,1}X_{r+1} + \cdots + K_{r,f}X_n). \end{aligned}$$

Consider the f vectors $V(1), \dots, V(f) \in F^n$ and defined as follows:

$$V(1) = \begin{pmatrix} -\frac{K_{1,1}}{d} \\ \vdots \\ -\frac{K_{r,1}}{d} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, V(f) = \begin{pmatrix} -\frac{K_{1,f}}{d} \\ \vdots \\ -\frac{K_{r,f}}{d} \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{3.3}$$

It is clear that $\{V(1), \dots, V(f)\}$ is an F-basis of the nullspace of J in F^n. We set

$$W = \mathrm{span}_R\{V(1), \dots, V(f)\},$$

so that $\{V(1), \dots, V(f)\}$ is an R-basis of W. We thus have

$$dW \subseteq N \subseteq W, \tag{3.4}$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

and we aim to determine the structure of the factors:

$$N/dW \text{ and } W/N,$$

where

$$W/dW \cong (R/Rd)^f.$$

Given $\alpha_1, \ldots, \alpha_f \in F$, we have

$$\alpha_1 V(1) + \cdots + \alpha_f V(f) \in N \Leftrightarrow \alpha_1, \ldots, \alpha_f \in R \text{ and } \alpha_1 K_{i,1} + \cdots + \alpha_f K_{i,f} \equiv 0 \mod d,\ 1 \le i \le r. \tag{3.5}$$

Thus, we have an isomorphism $R^f \to W$ given by:

$$(\alpha_1, \ldots, \alpha_f) \mapsto \alpha_1 V(1) + \cdots + \alpha_f V(f),$$

and N corresponds to the submodule, say Y, of R^f of all $(\alpha_1, \ldots, \alpha_f)$ such that the right-hand side of (3.5) holds. In particular, $W/N \cong R^f/Y$.

4. Each of N/dW and W/N determines the other. By the theory of finitely generated modules over a principal ideal domain, there is a basis $\{u_1, \ldots, u_f\}$ of W and nonzero elements $a_1, \ldots, a_f \in R$ such that

$$a_1 | \cdots | a_f | d,$$

and $\{a_1 u_1, \ldots, a_f u_f\}$ is a basis of N. Since $\{du_1, \ldots, du_f\}$ is a basis of dW, we see that

$$W/N \cong (R/Ra_1) \oplus \cdots \oplus (R/Ra_f) \text{ and } N/dW \cong (R/Rb_f) \oplus \cdots \oplus (R/Rb_1),$$

where

$$b_i = d/a_i, \quad 1 \le i \le f,$$

and

$$b_f | \cdots | b_1.$$

As d is fixed, we see that N/dW and W/N determine each other.

5. Structures of W/N and N/dW. Set $\overline{R} = R/Rd$ and consider the homomorphism of R-modules:

$$\Delta : R^f \to R^r \to \overline{R}^r,$$

given by:

$$\alpha \mapsto \overline{K}\overline{\alpha},$$

where $\alpha = (\alpha_1, \ldots, \alpha_f)$, and $\overline{K}$ and $\overline{\alpha}$ are the reductions of K and α modulo Rd. Then, (3.5) shows that the kernel of Δ is Y. Thus,

$$W/N \cong R^f/Y \cong \Delta(R^f) \cong C(\overline{K}),$$

where $C(\overline{K})$ is the column space of $\overline{K}$, namely the $\overline{R}$-span of the columns of $\overline{K}$.

Consider the natural epimorphism of R-modules $\Lambda : R^r \to \overline{R}^r$ with kernel $(Rd)^r$. Then, Λ restricts to an epimorphism of R-modules $\Omega : C(K) \to C(\overline{K})$ with kernel $C(K) \cap (Rd)^r$.

Let $Q = \operatorname{diag}(q_1, \ldots, q_s)$ be the Smith normal form of K, where $q_1 | \cdots | q_s$ and $s = \min\{r, n-r\}$, and let t be the rank of K, so that $t = 0$ if and only if $K = 0$.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

If $K = 0$, then (3.5) implies that $W = N$ and a fortiori:

$$N/dW \cong W/dW \cong \overline{R}^f.$$

Suppose next $K \neq 0$. Then, t is the last index such that $q_t \neq 0$ and from the theory of finitely generated modules over a principal ideal domain, there is a basis $\{u_1, \dots, u_r\}$ of R^r such that $\{q_1u_1, \dots, q_tu_t\}$ is a basis for $C(K)$. Notice that

$$C(K) \cap (Rd)^r = (Rq_1u_1 \oplus \cdots \oplus Rq_tu_t) \cap (Rdu_1 \oplus \cdots \oplus Rdu_r) = R\,\mathrm{lcm}(d, q_1)u_1 \oplus \cdots \oplus R\,\mathrm{lcm}(d, q_t)u_t,$$

so that

$$W/N \cong C(\overline{K}) \cong C(K)/(C(K) \cap (Rd)^r) \cong (Rq_1u_1 \oplus \cdots \oplus Rq_tu_t)/(R\,\mathrm{lcm}(d, q_1)u_1 \oplus \cdots \oplus R\,\mathrm{lcm}(d, q_t)u_t).$$

Since

$$\mathrm{lcm}(d, q_i)/q_i = d/\gcd(d, q_i), \quad 1 \leq i \leq t,$$

setting

$$m_i = \mathrm{lcm}(d, q_i)/q_i,\ d_i = d/\gcd(d, q_i), \quad 1 \leq i \leq t,$$

we infer

$$W/N \cong R/Rm_t \oplus \cdots \oplus R/Rm_1 \cong R/Rd_t \oplus \cdots \oplus R/Rd_1. \tag{5.6}$$

Adding $f - t$ zero summands to the right-hand side of (5.6), we may write

$$W/N \cong (R/R \cdot 1)^{f-t} \oplus R/Rd_t \oplus \cdots \oplus R/Rd_1.$$

We finally deduce from Section 4 the sought formula:

$$N/Wd \cong R/R\gcd(d, q_1) \oplus \cdots \oplus R/R\gcd(d, q_t) \oplus (R/Rd)^{f-t}. \tag{5.7}$$

Dividing every entry of Z by $g = \gcd\{d, K_{ij} \,|\, 1 \leq i \leq r, 1 \leq j \leq f\}$, we may assume that $g = 1$, which translates into $\gcd(d, q_1) = 1$. In this case, if $r = 1$ then (5.6) and (5.7) reduce to the corresponding formulas from [9, Theorems 4.1 and 3.2], respectively.

Notice that (5.6) and (5.7) remain valid when $K = 0$.

Set $U = \Sigma W$, with Σ as in Section 2, and let $M = dU$. We have an isomorphism $W \to U$, given by $X \mapsto \Sigma X$, yielding isomorphisms $W/N \to U/S$ and $N/dW \to S/M$. We have thus proved the following result.

Theorem 5.1. *Let $A \in M_{m,n}(R)$, with rank $0 < r < n$ and nullspace S in R^n. Let Z be a reduced matrix associated with A, as in (2.2), say via $LA\Sigma = Z$. Let W be the free R-module of rank $n - r$ corresponding to Z as defined in Section 3 and set $U = \Sigma W$ and $M = dU$. Then, $M \subseteq S \subseteq U$, where $U/S \cong W/N$ and $S/M \cong N/dW$ are as described in (5.6) and (5.7), respectively.*

Corollary 5.2. *We have $U = S$ if and only if d divides every entry of K, and $S = M$ if and only if $\gcd(d, q_i) = 1$, $1 \leq i \leq t$, and either d is a unit or K has rank f.*

Proof. This follows immediately from (5.6) and (5.7). ∎

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

6. An improved procedure to construct a basis of L. Here, we go back to the general case and suppose that L is an arbitrary lattice of rank f with a proper sublattice M. We assume that the list of invariant factors or elementary divisors of L/M is known, and we wish to use one list or the other to improve the process indicated in the Introduction to obtain a basis of L from a given basis $\{u_1, \dots, u_f\}$ of M.

Let $g_1, \dots, g_s \in R$ be the unique elements, up to multiplication by units, such that g_1 is not a unit, g_s is not zero, $g_1 | \cdots | g_s$, and

$$L/M \cong R/Rg_1 \oplus \cdots \oplus R/Rg_s. \tag{6.8}$$

Here, $i(M, L) = g_1 \cdots g_s$, and we will use all of $g_1, \dots, g_s$ instead of $i(M, L)$ to obtain a basis of L. The idea is to advance one invariant factor of L/M at a time, rather than one prime factor of $i(M, L)$ at a time.

According to (6.8), S/M has a vector with annihilating ideal Rg_s. This means that there are $a_1, \dots, a_f$ in R such that the following extension of (1.1) holds

$$v = \frac{a_1 u_1 + \cdots + a_f u_f}{g_s} \in L \text{ but } hv \notin M \text{ for any proper factor } h \text{ of } g_s. \tag{6.9}$$

In particular, $Rv \cap M = Rg_s v$, and we set $P = Rv + M$. Thus,

$$P/M \cong Rv/(Rv \cap M) \cong R/Rg_s,$$

is a submodule of L/M. On the other hand, it is well known [5, Lemma 6.8 and Theorem 6.7] that any cyclic submodule of L/M with annihilating ideal Rg_s is complemented in L/M. The uniqueness of the invariant factors of L/M implies that

$$S/P \cong R/Rg_1 \oplus \cdots \oplus R/Rg_{s-1}.$$

Thus, if we can provide a way to produce a basis of P from a basis of M, then successively applying the above procedure with $g_s, g_{s-1}, \dots, g_1$ will yield a basis of L. We next indicate two ways to construct a basis of P from $\{u_1, \dots, u_f\}$ and v. Set $v = u_{f+1}$ and $a_{f+1} = -g_s$. Then from the first condition in (6.9), we have

$$a_1 u_1 + \cdots + a_f u_f + a_{f+1} u_{f+1} = 0, \tag{6.10}$$

while the second condition in (6.9) implies

$$\gcd(a_1, \dots, a_f, a_{f+1}) = 1. \tag{6.11}$$

In the first way, set $a = (a_1, \dots, a_{f+1})$ and let u be the column vector with vector entries $(u_1, \dots, u_{f+1})$. Using an obvious notation, (6.10) means $au = 0$. Moreover, from (6.11), we infer the existence of Q in $\mathrm{GL}_{f+1}(R)$ such that $aQ = (1, 0, \dots, 0)$. Setting $v = Q^{-1}u$, we have

$$0 = au = aQQ^{-1}u = (1, 0, \dots, 0)v.$$

Now v is a column vector, say with vector entries $(v_1, \dots, v_{f+1})$, where $v_1 = 0$. But $v = Q^{-1}u$ ensures that the entries of u and v have the same span. Since P is a lattice of rank f, it follows that the f spanning vectors $v_2, \dots, v_{f+1}$ must form a basis of P.

For the second way, we assume that R is an Euclidean domain. Thus, R is an integral domain endowed with a function $\delta : R \to \mathbb{Z}_{\geq 0}$ such that given any $a, b \in R$ with $b \neq 0$, there are $q, r \in R$ such that $a = bq + r$, with $r = 0$ or $\delta(r) < \delta(b)$. We may then use (6.11) and the Euclidean algorithm to transform (6.10) into

$$b_1 v_1 + \cdots + b_f v_f + v_{f+1} = 0, \tag{6.12}$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

where $u_1,\dots,u_{f+1}$ and $v_1,\dots,v_f$ span the same module. As above, this implies that $\{v_1,\dots,v_f\}$ is a basis of P. We briefly describe the foregoing transformation. Choose $1\le i\le f+1$ such that $a_i\neq 0$ with $\delta(a_i)$ is as small as possible. For notational convenience, let us assume that $i=f+1$. Dividing every other a_j by a_{f+1}, we obtain $a_j=q_ja_{f+1}+r_j$, where $r_j=0$ or $\delta(r_j)<\delta(a_j)$, $1\le j\le f$. If every $r_j=0$, then (6.11) forces a_{f+1} to be a unit, so dividing (6.10) by a_{f+1} we obtain (6.12). Suppose at least one $r_j\neq 0$. We can rewrite (6.10) in the form:

$$r_1u_1+\cdots+r_fu_f+a_{f+1}(q_1u_1+\cdots+q_fu_f+u_{f+1})=0,$$

where $u_1,\dots,u_f,u_{f+1}$ and $u_1,\dots,u_f,q_1u_1+\cdots+q_fu_f+u_{f+1}$ span the same module, $r_j\neq 0$, $\delta(r_j)<\delta(a_{f+1})$, and $\gcd(r_1,\dots,r_f,a_{f+1})=1$. Since δ takes only nonnegative values, repeating this process we must eventually arrive to a unit remainder, as required for (6.12).

We next indicate how to use the elementary divisors of L/M instead of its invariant factors to construct a basis of L. There are more of the former than of the latter, but this is be balanced by the fact that each intermediate basis is more easily found. Let $p\in R$ be a prime, $1\le e_1\le\cdots\le e_k$, and suppose that $p^{e_1},\dots,p^{e_k}$ are the p-elementary divisors of L/M. Set $e=e_k$. Then, L/M has a vector with annihilating ideal Rp^e, which translates as follows. There are $a_1,\dots,a_f\in R$ such that the following extension of (1.1) holds

$$v=\frac{a_1u_1+\cdots+a_fu_f}{p^e}\in L \text{ but } p^{e-1}v\notin M. \tag{6.13}$$

By [5, Lemma 6.8], any vector of L/M with annihilating ideal Rp^e has a complement in L/M. Thus, the preceding procedure applies, except that now we advance one p-elementary divisor of L/M at a time. In this case, however, it is easier to pass from a basis to the next one. Indeed, since $p^{e-1}v\notin M$, we must have $p\nmid a_i$ for some i, and the same argument given in the Introduction produces a basis of the span of $v,u_1,\dots,u_f$ from the basis $\{u_1,\dots,u_f\}$ of M.

We finally indicate how to apply the above procedure when $L=S$, $M=dU$, and we take $\{u_1,\dots,u_f\}=\Sigma\{dV(1),\dots,dV(f)\}$. The invariant factors of $S/M\cong N/dW$ are given in Theorem 5.1, and we can obtain from these corresponding the elementary divisors. Furthermore, Corollary 5.2 makes it clear when $S=M$. Observe that we can replace L in (6.9) and (6.13) by R^n, for in that case $v\in F^n\cap T=S$.

7. The case when d is a prime. We assume throughout this section that $d=p$ is a prime and set $\overline{R}=R/Rp$. In this case, a sharpening of (5.6) and (5.7) is available, and we can obtain a basis of N, and hence of $S=\Sigma N$, directly, without having to resort to the procedure outlined in Section 6. It follows from (3.4) that all of W/pW, W/N, and N/pW are $\overline{R}$-vector spaces, and hence completely determined by their dimensions. Let $\overline{K}$ be the reduction of K modulo p. Then, $W/pW\cong\overline{R}^f$; N/pW is isomorphic to the nullspace of $\overline{K}$ by Section 3; and W/N is isomorphic to the column space of $\overline{K}$ by Section 5. Thus,

$$\dim W/N=\operatorname{rank}\overline{K},\ \dim N/pW=f-\operatorname{rank}\overline{K}. \tag{7.14}$$

This formula is compatible with the isomorphism:

$$W/N\cong (W/pW)/(N/pW).$$

Moreover, a careful examination of (7.14) reveals that, as expected, it is in agreement with (5.6) and (5.7).

Next, we show how to obtain a basis of N directly from the basis $\{V(1),\dots,V(f)\}$ of W. Let $H\in M_{r,f}(R)$ be such that $\overline{H}$ is the reduced row echelon form of $\overline{K}$. For simplicity of notation, let us assume that the leading columns of $\overline{H}$ are columns $1,\dots,s$.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

THEOREM 7.1. *Consider the vectors:*

$$z_1 = pV(1), \dots, z_s = pV(s),$$

and if $s < f$ *also the vectors:*

$$z_{s+i} = -(H_{1,s+i}V(1) + \cdots + H_{s,s+i}V(s)) + V(s+i), \quad 1 \le i \le f-s.$$

Then, $\{z_1, \dots, z_f\}$ *is a basis of* N *(if* $s = 0$ $\{z_1, \dots, z_f\}$ *is simply* $\{V(1), \dots, V(f)\}$*).*

Proof. Given $\alpha = (\alpha_1, \dots, \alpha_f) \in R^f$, we have

$$\overline{K}\overline{\alpha} = 0 \Leftrightarrow \overline{H}\overline{\alpha} = 0,$$

and therefore (3.5) gives

$$\alpha_1 V(1) + \cdots + \alpha_f V(f) \in N \Leftrightarrow \overline{H}\overline{\alpha} = 0.$$

Our choice of H ensures that $z_1, \dots, z_f \in N$. Let $G \in M_f(R)$ be the matrix whose columns are the coefficients of $z_1, \dots, z_f$ relative to the basis $V(1), \dots, V(f)$ of W. Then, $|G| = p^s$. On the other hand, $W/N \cong C(\overline{K})$ is a vector space over $\overline{R}$ of dimension s, so there is a basis $\{u_1, \dots, u_f\}$ of W such that $\{pu_1, \dots, pu_s, u_{s+1}, \dots, u_f\}$ is a basis of N. It follows from [9, Lemma 4.3] that $\{z_1, \dots, z_f\}$ is a basis of N. □

8. Examples.

(1) Consider the case $R = \mathbb{Z}$, $n = 4$, and

$$A = \begin{pmatrix} 2 & 3 & 5 & 4 \\ 3 & -5 & 2 & -7 \end{pmatrix}.$$

Let B (resp. C) be the 2×2 submatrix formed by the first (resp. last) two columns of A and let D be the adjoint of B. Then $|B| = -19$, which implies $|D| = -19$ and $|DC| \equiv |D||C| \equiv 0 \mod 19$. Multiplying A on the left by C, we obtain the the following reduced matrix Z associated with A:

$$Z = \begin{pmatrix} dI_2 & K \end{pmatrix} = \begin{pmatrix} -19 & 0 & -31 & 1 \\ 0 & -19 & -11 & -26 \end{pmatrix}.$$

The reduction of K modulo 19 has rank $s = 1$, since $|K| \equiv 0 \mod 19$ and not all entries of K are divisible by 19. In this case, the formulas from Section 7 give $S/19W \cong \mathbb{Z}/19\mathbb{Z}$ and $W/S \cong \mathbb{Z}/19\mathbb{Z}$. We can use this information to obtain a $\mathbb{Z}$-basis of S. Indeed, by Section 3 the vectors:

$$V(1) = (-31/19, -11/19, 1, 0),\ V(2) = (1/19, -26/19, 0, 1),$$

form a $\mathbb{Q}$-basis of T. Moreover, it is clear that if $\alpha_1, \alpha_2 \in \mathbb{Q}$, then $\alpha_1 V(2) + \alpha_2 V(2) \in S$ if and only if $\alpha_1, \alpha_2 \in \mathbb{Z}$ and

$$-31\alpha_1 + \alpha_2 \equiv 0 \mod 19,\ 11\alpha_1 + 26\alpha_2 \equiv 0 \mod 19.$$

The second equation is redundant since $|K| \equiv 0 \mod 19$, and the first equation is equivalent to

$$\alpha_2 \equiv 12\alpha_1 \mod 19.$$

This yields the following vectors from S:

$$z_1 = 19V(2) = (1, -26, 0, 19),\ z_2 = V(1) + 12V(2) = (-1, -17, 1, 12).$$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

The 2×2 matrix formed by coordinates of z_1, z_2 relative to $V(1), V(2)$ is

$$\begin{pmatrix} 0 & 1 \\ 19 & 12 \end{pmatrix}.$$

This implies $W/(Rz_1 \oplus Rz_2) \cong \mathbb{Z}/19\mathbb{Z}$, whence $\{z_1, z_2\}$ is a basis of S.

(2) Consider the case $R = \mathbb{Z}$, $r = 3$, $n = 6$, and

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 2 & 3 \\ 1 & 3 & 7 & 4 & 5 & 6 \\ 1 & 9 & 49 & 7 & 8 & 9 \end{pmatrix}.$$

Let B be the 3×3 submatrix formed by the first three columns of A. Then B is a Vandermonde matrix with determinant 48. Let C be the adjoint of B. Then,

$$C = \begin{pmatrix} 84 & -40 & 4 \\ -42 & 48 & -6 \\ 6 & -8 & 2 \end{pmatrix}.$$

Multiplying A on the left by C, we obtain the matrix:

$$\begin{pmatrix} 48 & 0 & 0 & -48 & 0 & 48 \\ 0 & 48 & 0 & 108 & 108 & 108 \\ 0 & 0 & 48 & -12 & -12 & -12 \end{pmatrix}.$$

Dividing every entry by 12, we obtain the following reduced matrix Z associated with A:

$$Z = \begin{pmatrix} dI_3 & K \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 & -4 & 0 & 4 \\ 0 & 4 & 0 & 9 & 9 & 9 \\ 0 & 0 & 4 & -1 & -1 & -1 \end{pmatrix}.$$

Thus, (3.3) produces a free submodule M of S of rank 3 with basis:

$$u_1 = (4, -9, 1, 4, 0, 0), u_2 = (0, -9, 1, 0, 4, 0), u_3 = (-4, -9, 1, 0, 0, 4).$$

The Smith normal form of K is $\mathrm{diag}(1, 4, 0)$. Here, $d = 4$, $f = 3$, and $t = 2$, so according to (5.7), we have

$$S/M \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

We look for $a, b, c \in \mathbb{Z}$ such that

$$v = \frac{au_1 + bu_2 + cu_3}{4} \in \mathbb{Z}^3 \text{ but } 2v \notin M.$$

This translates into

$$a + b + c \equiv 0 \mod 4 \text{ and } (a, b, c) \notin (2\mathbb{Z})^3.$$

Taking $(a, b, c) = (1, -1, 1)$, we find the following vectors from S:

$$z_1 = (u_1 - u_2)/4,\ z_2 = (u_2 - u_3)/4,\ u_3.$$

We clearly have

$$(\mathbb{Z}z_1 \oplus \mathbb{Z}z_2 \oplus \mathbb{Z}z_3)/M \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},$$

which implies that $\{z_1, z_2, z_3\}$ is a basis of S.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 38, pp. 160-169, February 2022.

(3) Consider the case $R = \mathbb{Z}$, $r = 3$, $n = 6$, and

$$A = \begin{pmatrix} 12 & 24 & 36 & -4 & 12 & 44 \\ 24 & 36 & 12 & -2 & 10 & 20 \\ 36 & 12 & 24 & 0 & 20 & 44 \end{pmatrix}.$$

Multiplying A on the left by a suitable matrix from $\mathrm{GL}_3(\mathbb{Q})$ yields the the following reduced matrix associated with A:

$$Z = \begin{pmatrix} dI_3 & K \end{pmatrix} = \begin{pmatrix} 12 & 0 & 0 & 1 & 5 & 6 \\ 0 & 12 & 0 & -1 & -1 & -2 \\ 0 & 0 & 12 & -1 & 3 & 14 \end{pmatrix}.$$

Following (3.3), we obtain a free submodule M of S of rank 3 having basis:

$$u_1 = (-1, 1, 1, 12, 0, 0), u_2 = (-5, 1, -3, 0, 12, 0), u_3 = (-6, 2, -14, 0, 0, 12).$$

The Smith normal form of K is $\mathrm{diag}(1, 4, 12)$. We have $d = 12$, $f = 3$ and $t = 3$, so (5.7) yields

$$S/M \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}.$$

We use (6.9) to obtain the vector:

$$v = \frac{-u_1 - u_2 + u_3}{12} = (0, 0, -1, -1, -1, 1) \in S.$$

Then, $\{v, u_2, u_3\}$ is a basis of a module P containing M such that $S/P \cong \mathbb{Z}/4\mathbb{Z}$. Applying (6.9) once again yields the vector:

$$w = \frac{4v + 2u_2 + u_3}{4} = (-4, 1, -6, -1, 5, 4) \in S,$$

and the basis $\{w, v, u_2\}$ of S.

REFERENCES

[1] E. Contejean and H. Devie. An efficient incremental algorithm for solving systems of linear Diophantine equations. *Inform. and Comput.*, 113:143–173, 1994.

[2] M. Clausen and A. Fortenbacher. Efficient solution of linear Diophantine equations. *J. Symbolic Comput.*, 8:201–216, 1989.

[3] S. Chapman, U. Krause, and E. Oeljeklaus. Monoids determined by a homogeneous linear Diophantine equation and the half-factorial property. *J. Pure Appl. Algebra*, 151:107–133, 2000.

[4] R.N. Greenwell and S. Kertzner. Solving linear Diophantine matrix equations using the Smith normal form (more or less). *Int. J. Pure Appl. Math.*, 55:49—60, 2009.

[5] T.W. Hungerford. *Algebra*. Graduate Texts in Mathematics, Vol. 73, Springer-Verlag, New York, 1980.

[6] A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[7] P. Pisón-Casares and A. Vigneron-Tenorio. $\mathbb{N}$-solutions to linear systems over $\mathbb{Z}$. *Linear Algebra Appl.*, 384:135–154, 2004.

[8] Q.N. Phong and B. Vallée (Editors). *The LLL Algorithm: Survey and Applications*. Springer, 2009.

[9] R. Quinlan, M. Shau and F. Szechtman. Linear diophantine equations in several variables. *Linear Algebra Appl.*, 640:67–90, 2022.

[10] R.P. Stanley. *Combinatorics and Commutative Algebra*. Progress in Mathematics, Vol. 41, 2nd edition, Birkhäuser, Boston, MA, 1996.