

On the equivalence of multivariate polynomial matrices with determinants in a principal ideal domain

Dong Lu^a, Dingkan Wang^{b,c}, Fanghui Xiao^d, Xiaopeng Zheng^{e,*}

^a*School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China*

^b*State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China*

^c*School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China*

^d*MOE-LCSM, School of Mathematics and Statistics, Hunan Normal University, Changsha 410081, China*

^e*College of Mathematics and Computer Science, Shantou University, Shantou 515821, China*

Abstract

Let A be a principal ideal domain. This paper addresses the equivalence problem for square matrices over the multivariate polynomial ring $A[x_1, \dots, x_n]$ whose determinants belong to A . A necessary and sufficient condition for such matrices to be equivalent to their Smith normal forms is established. This result is further extended to non-square and rank-deficient matrices via the Quillen-Suslin theorem. As the proofs provided are constructive, they naturally yield algorithms to reduce these matrices to their Smith normal forms.

Keywords: Multivariate polynomial matrix, Principal ideal domain, Matrix equivalence, Smith normal form, Quillen-Suslin theorem

MSC(2020): 68W30, 13P05

Contents

1	Introduction	2
2	Preliminaries	4
2.1	Notations and conventions	4
2.2	Basic concepts in matrix theory	5
2.3	Quillen-Suslin theorem	6
2.4	Resultants and homomorphisms	8
3	Equivalence of square matrices with irreducible power determinants in A	10
3.1	The special case $l = 2$ and $t_1 = 1$	11
3.2	The general case $l \geq 2$	13
3.3	Algorithm and example	18

*Corresponding author

Email addresses: donglu@swjtu.edu.cn (Dong Lu), dwang@mmrc.iss.ac.cn (Dingkan Wang), xiaofanghui@hunnu.edu.cn (Fanghui Xiao), xiaopengzheng@stu.edu.cn (Xiaopeng Zheng)

4	Equivalence of square matrices with determinants in A	20
4.1	Main theorem	20
4.2	Algorithm and example	23
5	Equivalence of non-square and rank-deficient matrices	26
6	Concluding remarks	27
	Acknowledgments	28
	References	28
Appendix A	ZLP matrix factorization theorem	29
Appendix B	Procedures	36

1. Introduction

Let A be a principal ideal domain (PID), and let $A[x_1, \dots, x_n]$ be the multivariate polynomial ring in variables $x_1, \dots, x_n$ over A . A square matrix over $A[x_1, \dots, x_n]$ is unimodular if its determinant is a unit in $A[x_1, \dots, x_n]$. Two matrices $\mathbf{M}, \mathbf{N} \in A[x_1, \dots, x_n]^{l \times m}$ are equivalent over $A[x_1, \dots, x_n]$ if there exist unimodular matrices $\mathbf{U} \in A[x_1, \dots, x_n]^{l \times l}$ and $\mathbf{V} \in A[x_1, \dots, x_n]^{m \times m}$ such that $\mathbf{N} = \mathbf{UMV}$. It is a classical result that any matrix with entries in a PID is equivalent to its Smith normal form. However, when the base ring is not a PID, the problem of matrix equivalence becomes significantly more challenging.

The study of multivariate polynomial matrices largely originates from multidimensional systems and signal processing (see [1, 2] and the references therein). Frost and Storey [3] were the first to study the equivalence of bivariate polynomial matrices over $K[x_1, x_2]$ to their Smith normal forms, where K is a field. For an arbitrary full-rank matrix $\mathbf{M} \in K[x_1, x_2]^{l \times l}$, they claimed that a necessary and sufficient condition for the equivalence is that for $i = 1, \dots, l$, all the $i \times i$ reduced minors of $\mathbf{M}$ generate the unit ideal $K[x_1, x_2]$. However, this claim was later shown to be false by a counterexample provided by Frost and Storey [4]. Since then, the problem of determining the equivalence of multivariate polynomial matrices (with $n \geq 2$ variables) to their Smith normal forms has remained open.

The Quillen-Suslin theorem originated from Serre's conjecture [5], which asks whether every finitely generated projective module over $K[x_1, \dots, x_n]$ is free. In 1976, Quillen [6] and Suslin [7] independently proved this conjecture and, more generally, established the corresponding result for the polynomial ring $A[x_1, \dots, x_n]$. From the perspective of matrix theory, the Quillen-Suslin theorem can be equivalently formulated as follows: if all $l \times l$ minors of a matrix $\mathbf{M} \in A[x_1, \dots, x_n]^{l \times m}$ ($l \leq m$) generate the unit ideal $A[x_1, \dots, x_n]$, then $\mathbf{M}$ is equivalent to its Smith normal form $(\mathbf{I}_l, \mathbf{0}_{l \times (m-l)})$, where $\mathbf{I}_l$ is the $l \times l$ identity matrix. Constructive and algorithmic aspects of the Quillen-Suslin theorem have also been extensively studied. Given a polynomial matrix over $\mathbb{C}[x_1, \dots, x_n]$ whose maximal minors generate the unit ideal, Logar and Sturmfels [8] gave a Gröbner basis algorithm that computes a free basis of the associated projective module, thereby providing a constructive proof of the Quillen-Suslin theorem. Using similar Gröbner basis techniques, Gago-Vargas [9] designed two algorithms that compute free bases of finitely generated projective modules over

$A[x_1, \dots, x_n]$, where A possesses suitable computational properties, with applications to algebraic K -theory. Subsequently, Fabiańska and Quadrat [10] developed the Maple package **QUILLENUSLIN**, which provides computer-algebra implementations of such constructive procedures for polynomial rings with coefficients in $\mathbb{Q}$ or $\mathbb{Z}$, and applies them to multidimensional systems theory. These algorithmic developments have made the Quillen-Suslin theorem an effective tool in the study of polynomial matrices and matrix equivalence.

The equivalence problem for multivariate polynomial matrices has been studied extensively. In particular, two classes of such matrices have received significant attention. The first class consists of square matrices $\mathbf{M} \in K[x_1, \dots, x_n]^{l \times l}$ with $\det(\mathbf{M}) = (x_1 - f(x_2, \dots, x_n))^t$, where t is a positive integer. For $t = 1$, Lin et al. [11] proved that $\mathbf{M}$ is always equivalent to its Smith normal form, without requiring any additional equivalence conditions. For $t \geq 2$, Liu et al. [12] verified that the claim of Frost and Storey holds true in this specific case. The second class comprises square matrices whose determinants belong to $K[x_1]$. For the bivariate case ($n = 2$), these matrices were studied in [13, 14, 15] by reducing the problem to matrices over a PID via homomorphic mappings, yielding equivalence criteria via the Euclidean algorithm. Recently, Guan et al. [16] extended the results of [14] to $K[x_1, \dots, x_n]$ for $l \geq 3$ by applying Suslin's stability theorem. It is worth noting that the Quillen-Suslin theorem provides a unified framework for addressing the matrix equivalence problem in a broader context. By utilizing this theorem, all the aforementioned conclusions for specific square matrices can be systematically extended to non-square and rank-deficient matrices.

To describe the main types of matrices studied in the literature, we clarify the notation used in Table 1 below. In this table, $\mathbf{M}$ denotes an $l \times l$ matrix over a base ring (specified in each row of the table), and $d_{l-1}(\mathbf{M})$ denotes the greatest common divisor (gcd) of all the $(l-1) \times (l-1)$ minors of $\mathbf{M}$. Furthermore, $\mathbb{Z}$ denotes the ring of integers, t, s are positive integers, $p(x_1)$ and $q(x_1)$ are two distinct irreducible polynomials in $K[x_1]$.

Table 1: Classification of matrix types studied in the literature on matrix equivalence

Ref.	Base ring	Type of $\mathbf{M}$
[17]	$\mathbb{Z}$	Arbitrary integer matrix
[6, 7]	$A[x_1, \dots, x_n]$	Maximal minors generate the unit ideal
[11]	$K[x_1, \dots, x_n]$	$\det(\mathbf{M}) = x_1 - f(x_2, \dots, x_n)$
[12]	$K[x_1, \dots, x_n]$	$\det(\mathbf{M}) = (x_1 - f(x_2, \dots, x_n))^t$
[13]	$K[x_1, x_2]$	$\det(\mathbf{M}) = p(x_1)^t$ and $d_{l-1}(\mathbf{M}) = 1$
[14]	$K[x_1, x_2]$	$\det(\mathbf{M}) = p(x_1)^t$
[15]	$K[x_1, x_2]$	$\det(\mathbf{M}) = p(x_1)^t \cdot q(x_1)^s$ and $d_{l-1}(\mathbf{M}) = 1$
[16]	$K[x_1, \dots, x_n]$	$\det(\mathbf{M}) = p(x_1)^t$ with $l \geq 3$
This paper	$A[x_1, \dots, x_n]$	$\det(\mathbf{M}) \in A$

In this paper, we will investigate the equivalence problem for square matrices over $A[x_1, \dots, x_n]$ whose determinants belong to A . As shown in Table 1, the classes of matrices studied in [13]–[17] can all be regarded as special cases of this type. We first prove that the Frost-Storey assertion holds for these matrices, and then extend this result to non-square and rank-deficient matrices. Based on our constructive proofs, we develop algorithms

for reducing these matrices to their Smith normal forms, explicitly constructing two unimodular matrices $\mathbf{U}, \mathbf{V} \in A[x_1, \dots, x_n]^{l \times l}$ satisfying $\text{SNF}(\mathbf{M}) = \mathbf{U}\mathbf{M}\mathbf{V}$, where $\text{SNF}(\mathbf{M})$ denotes the Smith normal form of $\mathbf{M}$. Moreover, we provide two concrete examples to illustrate the correctness of our equivalence theory and the effectiveness of the proposed algorithms.

The rest of the paper is organized as follows. Section 2 recalls some preliminary notions and results that will be used throughout. Section 3 establishes the equivalence criterion for square matrices whose determinant is a power of a single irreducible element of A , and includes an algorithm with an illustrative example. Section 4 extends this criterion to square matrices with arbitrary determinants in A , again accompanied by an algorithm. Section 5 generalizes the results to non-square and rank-deficient matrices. Section 6 offers some concluding remarks. Appendix A contains the detailed proof of the ZLP matrix factorization theorem over $A[x_1, \dots, x_n]$, and Appendix B collects the computational procedures of the main algorithms.

2. Preliminaries

2.1. Notations and conventions

Let A be a PID and let $R = A[x_1, \dots, x_n]$. All theoretical results in this paper are established for the polynomial ring R over an arbitrary PID A . Since our algorithms for Smith normal form reduction over R employ the second Quillen-Suslin algorithm of Gago-Vargas [9, Theorem 13] to construct the needed unimodular matrices, we impose the following effectiveness assumptions on A : it is an MC-PID (Definition 1 in [9]), i.e., linear equations are solvable in A and maximal ideals containing a given proper ideal are algorithmically constructible. Additionally, we assume the standard algorithmic capability of factoring univariate polynomials over $A/\langle p \rangle$ and $\text{Frac}(A)$, where $p \in A$ is a prime element, and $\text{Frac}(A)$ denotes the field of fractions of A .

Since A is a PID, it is a unique factorization domain (UFD). By Gauss' lemma and induction on n , R is also a UFD, and its units are precisely the units of A (see [18, Chapter II, Theorem 5.2 and Chapter IV, Corollary 2.4] for more details). Since R is a UFD, the gcd of any finite set of elements in R exists and is well-defined only up to multiplication by a unit. For clarity, we fix a unique representative for the gcd by requiring the unit factor to be 1 (i.e., by factoring out the unit part). This convention ensures the gcd is uniquely determined for our subsequent calculations.

Let l and m be positive integers, and let $R^{l \times m}$ denote the set of $l \times m$ matrices with entries in R . Throughout this paper, we assume without loss of generality that $l \leq m$, and denote matrices by bold uppercase letters. Let $\mathbf{M} \in R^{l \times m}$, and let $\text{Frac}(R)$ be the field of fractions of R . We define its rank by extending scalars from R to $\text{Frac}(R)$: $\text{rank}_R(\mathbf{M}) := \text{rank}_{\text{Frac}(R)}(\mathbf{M})$, where $\mathbf{M}$ is viewed as a matrix over $\text{Frac}(R)$. Equivalently, $\text{rank}_R(\mathbf{M})$ is the largest integer r such that $\mathbf{M}$ has at least one nonzero $r \times r$ minor in R . For convenience, we shall simply denote $\text{rank}_R(\mathbf{M})$ by $\text{rank}(\mathbf{M})$.

Let $\text{rank}(\mathbf{M}) = r$. For $i = 1, \dots, r$, let $I_i(\mathbf{M})$ be the ideal generated by all $i \times i$ minors of $\mathbf{M}$, and let $d_i(\mathbf{M})$ be the gcd of all $i \times i$ minors of $\mathbf{M}$. Here, we adopt the convention that

$d_0(\mathbf{M}) = 1$ and $d_i(\mathbf{M}) = 0$ for $i > r$. Let $f_1, \dots, f_l \in R$, we use $\text{diag}(f_1, \dots, f_l)$ to denote the diagonal matrix whose diagonal entries are $f_1, \dots, f_l$.

2.2. Basic concepts in matrix theory

Recall that a matrix $\mathbf{U} \in K^{l \times l}$ is invertible in linear algebra if and only if $\det(\mathbf{U}) \neq 0$. Similarly, in areas such as commutative algebra and multidimensional systems, there exists a comparable definition.

Definition 2.1. Let $\mathbf{U} \in R^{l \times l}$. Then $\mathbf{U}$ is said to be unimodular if $\det(\mathbf{U})$ is a unit in R .

The set of all $l \times l$ unimodular matrices over R is denoted by $\text{GL}_l(R)$. Based on Definition 2.1, we now introduce the concept of matrix equivalence over R .

Definition 2.2. Let $\mathbf{M}, \mathbf{N} \in R^{l \times m}$. We say that $\mathbf{M}$ is equivalent to $\mathbf{N}$ over R if there exist $\mathbf{U} \in \text{GL}_l(R)$ and $\mathbf{V} \in \text{GL}_m(R)$ such that $\mathbf{N} = \mathbf{U}\mathbf{M}\mathbf{V}$.

We write $\mathbf{M} \sim_R \mathbf{N}$ to denote that $\mathbf{M}$ and $\mathbf{N}$ are equivalent over R , and simply $\mathbf{M} \sim \mathbf{N}$ when no confusion can arise.

The Smith normal form for any matrix over R is defined as follows.

Definition 2.3 (Smith normal form). Let $\mathbf{M} \in R^{l \times m}$ with $\text{rank}(\mathbf{M}) = r$, where $1 \leq r \leq l$. For $i = 1, \dots, r$, define

$$\Phi_i := \frac{d_i(\mathbf{M})}{d_{i-1}(\mathbf{M})} \in R.$$

Then the Smith normal form of $\mathbf{M}$ is given by

$$\text{SNF}(\mathbf{M}) := \begin{pmatrix} \text{diag}(\Phi_1, \dots, \Phi_r) & \mathbf{0}_{r \times (m-r)} \\ \mathbf{0}_{(l-r) \times r} & \mathbf{0}_{(l-r) \times (m-r)} \end{pmatrix} \in R^{l \times m},$$

and its invariant factors $\Phi_1, \dots, \Phi_r$ satisfy $\Phi_1 \mid \dots \mid \Phi_r$.

Li et al. [19] proved that the divisibility chain $\Phi_1 \mid \dots \mid \Phi_r$ holds in any UFD. Since R is a UFD, Definition 2.3 is well-defined and is a natural generalization of the classical Smith normal form for λ -matrices in linear algebra.

The concept of reduced minors was introduced by Lin [20] over $K[x_1, \dots, x_n]$ in his study of multidimensional linear systems. We generalize this concept to R , where it plays a fundamental role in our investigation of the matrix equivalence problem.

Definition 2.4. Let $\mathbf{M} \in R^{l \times m}$ with $\text{rank}(\mathbf{M}) = r$, where $1 \leq r \leq l$. For any given integer i with $1 \leq i \leq r$, let $a_1, \dots, a_\beta$ be all the $i \times i$ minors of $\mathbf{M}$, where $\beta = \binom{l}{i} \binom{m}{i}$. Extracting $d_i(\mathbf{M})$ from $a_1, \dots, a_\beta$ yields

$$a_j = d_i(\mathbf{M}) \cdot b_j, \quad j = 1, \dots, \beta.$$

Then, $b_1, \dots, b_\beta$ are called the $i \times i$ reduced minors of $\mathbf{M}$. For convenience, we use $J_i(\mathbf{M})$ to denote the ideal in R generated by $b_1, \dots, b_\beta$. In addition, let $J_0(\mathbf{M}) = R$, and $J_i(\mathbf{M}) = 0$ for $i > r$.

Let $\mathbf{M} \in R^{l \times m}$. Given any two strictly increasing sequences of indices $\{i_1, \dots, i_s\}$ and $\{j_1, \dots, j_t\}$ with $1 \leq i_1 < \dots < i_s \leq l$ and $1 \leq j_1 < \dots < j_t \leq m$, denote by $\mathbf{M} \begin{pmatrix} i_1 & \dots & i_s \\ j_1 & \dots & j_t \end{pmatrix}$ the $s \times t$ submatrix of $\mathbf{M}$ formed by rows $i_1, \dots, i_s$ and columns $j_1, \dots, j_t$. The following formula holds for polynomial matrices over R .

Proposition 2.5 (Cauchy-Binet formula, [21]). *Let $\mathbf{M} = \mathbf{M}_1 \mathbf{M}_2$, where $\mathbf{M}_1 \in R^{l \times t}$ and $\mathbf{M}_2 \in R^{t \times m}$. Then every $r \times r$ minor of $\mathbf{M}$ is given by*

$$\det \left(\mathbf{M} \begin{pmatrix} i_1 & \dots & i_r \\ j_1 & \dots & j_r \end{pmatrix} \right) = \sum_{1 \leq s_1 < \dots < s_r \leq t} \det \left(\mathbf{M}_1 \begin{pmatrix} i_1 & \dots & i_r \\ s_1 & \dots & s_r \end{pmatrix} \right) \cdot \det \left(\mathbf{M}_2 \begin{pmatrix} s_1 & \dots & s_r \\ j_1 & \dots & j_r \end{pmatrix} \right),$$

where $1 \leq r \leq \min\{l, t\}$.

The following lemma shows that $d_i(\mathbf{M})$ and $J_i(\mathbf{M})$ are invariants under matrix equivalence. This lemma is straightforward to prove using the Cauchy-Binet formula.

Lemma 2.6. *Let $\mathbf{M}_1, \mathbf{M}_2 \in R^{l \times m}$. If $\mathbf{M}_1 \sim \mathbf{M}_2$, then $d_i(\mathbf{M}_1) = d_i(\mathbf{M}_2)$ and $J_i(\mathbf{M}_1) = J_i(\mathbf{M}_2)$ for all $i = 1, \dots, l$.*

The following lemma was originally established in [22] for matrices over $K[x_1, x_2]$. Since its proof relies only on the UFD property, which is also satisfied by R , the lemma holds for matrices over R . We present it here without proof.

Lemma 2.7. *Let $\mathbf{M} = \mathbf{F}\mathbf{G}$, where $\mathbf{F}, \mathbf{G} \in R^{l \times l}$ satisfy $\gcd(\det(\mathbf{F}), \det(\mathbf{G})) = 1$. Then*

- (1) $d_i(\mathbf{M}) = d_i(\mathbf{F}) \cdot d_i(\mathbf{G})$ for all $i = 1, \dots, l$;
- (2) for any integer i with $1 \leq i \leq l$, if $J_i(\mathbf{M}) = R$, then $J_i(\mathbf{F}) = J_i(\mathbf{G}) = R$.

2.3. Quillen-Suslin theorem

The notion of zero left coprimeness and the related zero left prime condition were introduced in [23] for polynomial matrices in n variables in the context of n -dimensional systems. In their setting, the zero prime condition is formulated by requiring that the maximal minors have no common zero. When the coefficients lie in a field and zeros are taken over its algebraic closure, this is equivalent, by Hilbert's Nullstellensatz, to the condition that the maximal minors generate the unit ideal. We adopt this latter algebraic condition as the definition of the ZLP property for matrices over R .

Definition 2.8. *Let $\mathbf{M} \in R^{l \times m}$ be of full row rank. Then $\mathbf{M}$ is said to be zero left prime (ZLP) if all the $l \times l$ minors of $\mathbf{M}$ generate the unit ideal R (i.e., $I_l(\mathbf{M}) = R$). Similarly, a matrix $\mathbf{M} \in R^{m \times l}$ is said to be zero right prime (ZRP) if $\mathbf{M}^T$ is ZLP.*

In 1976, Quillen [6] and Suslin [7] established a connection between ZLP matrices and unimodular matrices, a result now known as the Quillen-Suslin theorem. Specifically, a ZLP matrix can be embedded into a unimodular matrix. Equivalently, the Quillen-Suslin theorem asserts that any ZLP matrix is equivalent to its Smith normal form.

Theorem 2.9 (Quillen-Suslin theorem, [6, 7]). *Let $\mathbf{M} \in R^{l \times m}$ be a ZLP matrix. Then there exists $\mathbf{V} \in \mathrm{GL}_m(R)$ such that $\mathbf{M}\mathbf{V} = (\mathbf{I}_l, \mathbf{0}_{l \times (m-l)})$.*

The Lin-Bose conjecture, first proposed by Lin and Bose in [24] and later proved in [25, 26, 27, 28], is now known as the ZLP matrix factorization theorem over $K[x_1, \dots, x_n]$. We now generalize it to the following form.

Theorem 2.10 (ZLP matrix factorization theorem). *Let $\mathbf{M} \in R^{l \times m}$ with rank r , where $1 \leq r \leq l$. If $J_r(\mathbf{M}) = R$, then there exist $\mathbf{G}_1 \in R^{l \times r}$ and $\mathbf{F}_1 \in R^{r \times m}$ such that $\mathbf{M} = \mathbf{G}_1 \mathbf{F}_1$, where $d_r(\mathbf{G}_1) = d_r(\mathbf{M})$ and $\mathbf{F}_1$ is a ZLP matrix.*

Remark 2.11. In [28], the ZLP matrix factorization theorem is proved for full-rank matrices over $K[x_1, \dots, x_n]$. Theorem 2.10 extends this result to matrices of rank r over the base ring R , which are not assumed to be of full row rank. A complete proof in this generality is given in Appendix A.

By duality, the analogous factorization theorem for ZRP matrices can be stated as follows.

Theorem 2.12 (ZRP matrix factorization theorem). *Let $\mathbf{M} \in R^{m \times l}$ with rank r , where $1 \leq r \leq l$. If $J_r(\mathbf{M}) = R$, then there exist $\mathbf{F}_2 \in R^{m \times r}$ and $\mathbf{G}_2 \in R^{r \times l}$ such that $\mathbf{M} = \mathbf{F}_2 \mathbf{G}_2$, where $d_r(\mathbf{G}_2) = d_r(\mathbf{M})$ and $\mathbf{F}_2$ is a ZRP matrix.*

We construct the following set

$$\mathrm{SL}_l(K[x_1, \dots, x_n]) := \{\mathbf{U} \in K[x_1, \dots, x_n]^{l \times l} \mid \det(\mathbf{U}) = 1\}.$$

Let $\mathbf{e}_{ij}$ be the matrix in $K[x_1, \dots, x_n]^{l \times l}$ whose (i, j) -th entry is 1 and all other entries are zero. We use $\mathbf{E}_{i,j}(f)$ to denote the matrix $\mathbf{I}_l + f \cdot \mathbf{e}_{ij}$, where $f \in K[x_1, \dots, x_n]$. Then $\mathbf{E}_{i,j}(f)$ with $i \neq j$ is called an $l \times l$ third-class elementary matrix. Let $\mathrm{E}_l(K[x_1, \dots, x_n])$ denote the subgroup of $\mathrm{SL}_l(K[x_1, \dots, x_n])$ generated under multiplication by all $l \times l$ third-class elementary matrices over $K[x_1, \dots, x_n]$. When $l \geq 3$, Suslin [29] obtained the following important conclusion.

Theorem 2.13 (Suslin's stability theorem, [29]). *Let $l \geq 3$. Then*

$$\mathrm{SL}_l(K[x_1, \dots, x_n]) = \mathrm{E}_l(K[x_1, \dots, x_n]).$$

An algorithmic proof of Suslin's stability theorem can be found in [30].

Localization is a fundamental tool in commutative algebra and plays a crucial role in the proof of the Quillen–Suslin theorem. In the subsequent definition, the base ring applies to any commutative ring containing the unity 1. To prevent confusion from introducing excessive notation, we restrict the base ring in the definition to R .

Definition 2.14 (Definition 1.4.4, [31]). *Let S be a subset of $R \setminus \{0\}$.*

- (1) *S is called a multiplicative subset of R if $1 \in S$, and $f, g \in S$ implies $fg \in S$.*

(2) The localization of R with respect to the multiplicative subset S is defined as

$$S^{-1}R := \left\{ \frac{f}{g} \in \text{Frac}(R) \mid f \in R, g \in S \right\}.$$

Clearly, $S^{-1}R$ is a subring of $\text{Frac}(R)$.

(3) Let $S_1, \dots, S_t$ be multiplicative subsets of R . We say that $S_1, \dots, S_t$ are comaximal if for any $g_1 \in S_1, \dots, g_t \in S_t$, there exist $h_1, \dots, h_t \in R$ such that

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

Let x be a new variable over R , not an element of A and distinct from $x_1, \dots, x_n$. The following theorem is proposed by Vaserstein, which plays an important role in matrix equivalence.

Theorem 2.15 (Vaserstein). *Let $\mathbf{M} \in R[x]^{l \times l}$. Assume that $S_1, \dots, S_t$ are comaximal multiplicative subsets of R . Then $\mathbf{M}(x)$ and $\mathbf{M}(0)$ are equivalent over $R[x]$ if and only if they are equivalent over $(S_i^{-1}R)[x]$ for $i = 1, \dots, t$.*

For a constructive proof of Theorem 2.15, we refer to [32] or to Theorem 44 in [33] for more details. As shown in the proof, one can explicitly construct $\mathbf{U}, \mathbf{V} \in \text{GL}_l(R[x])$ such that $\mathbf{M}(0) = \mathbf{U} \cdot \mathbf{M}(x) \cdot \mathbf{V}$.

2.4. Resultants and homomorphisms

Let $h \in R[x] \setminus \{0\}$. We denote by $\deg_x(h)$ and $\text{lc}_x(h)$ the degree and the leading coefficient of h with respect to x , respectively. Clearly, $\text{lc}_x(h) \in R$.

Definition 2.16. *Let $f, g \in R[x]$ with $\deg_x(f) = s$ and $\deg_x(g) = t$, where s, t are nonnegative integers. We write*

$$\begin{cases} f = a_s x^s + \dots + a_0, & a_s \neq 0, \\ g = b_t x^t + \dots + b_0, & b_t \neq 0, \end{cases}$$

where $a_i, b_j \in R$ for $0 \leq i \leq s$ and $0 \leq j \leq t$. We define the resultant of f and g with respect to x as follows:

$$\text{res}_x(f, g) := \det \begin{pmatrix} a_s & a_{s-1} & \dots & a_0 & & & \\ & a_s & a_{s-1} & \dots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_s & a_{s-1} & \dots & a_0 \\ b_t & b_{t-1} & \dots & b_0 & & & \\ & b_t & b_{t-1} & \dots & b_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_t & b_{t-1} & \dots & b_0 \end{pmatrix},$$

where the numbers of row vectors $(a_s, \dots, a_0)$ and $(b_t, \dots, b_0)$ in the above matrix are t and s , respectively. Here, we adopt the convention that $\text{res}_x(f, g) = 1$ if $s = t = 0$.

Note that $\text{res}_x(f, g) \in R$; for further details we refer to Chapter 3.6 in [34]. With the notion of resultant now established, we can state the following lemma.

Lemma 2.17. *Let $g \in R \setminus \{0\}$ and $g_1, g_2 \in R[x]$ satisfy $\langle g, g_1, g_2 \rangle = R[x]$. If $\langle g, \text{lc}_x(g_1) \rangle = \langle g, \text{lc}_x(g_2) \rangle = R$, then $\langle g, \text{res}_x(g_1, g_2) \rangle = R$.*

Proof. Let $h = \text{lc}_x(g_1)$. Then $h \in R$. If $\deg_x(g_1) = 0$, then $\text{res}_x(g_1, g_2) = h^{\deg_x(g_2)}$. It follows from $\langle g, \text{lc}_x(g_1) \rangle = R$ that $\langle g, \text{res}_x(g_1, g_2) \rangle = R$. A similar argument holds if $\deg_x(g_2) = 0$.

We now consider the case of $\deg_x(g_1) > 0$ and $\deg_x(g_2) > 0$. Let

$$\psi : R[x] \longrightarrow (R/\langle g \rangle)[x]$$

be the canonical homomorphism induced by the natural projection $R \rightarrow R/\langle g \rangle$. More precisely, for any $f = \sum_{i=0}^s a_i x^i \in R[x]$, we have $\psi(f) = \sum_{i=0}^s \tilde{a}_i x^i$, where $\tilde{a}_i$ denotes the image of a_i in $R/\langle g \rangle$. By the fact that $\langle g, g_1, g_2 \rangle = R[x]$ and $\langle g, h \rangle = R$, we conclude that $\langle \psi(g_1), \psi(g_2) \rangle = (R/\langle g \rangle)[x]$ and $\psi(h)$ is a unit in $R/\langle g \rangle$. By Theorem 5.1 in [35], $\text{res}_x(\psi(g_1), \psi(g_2))$ is a unit in $R/\langle g \rangle$. Since $\deg_x(g_1) > 0$ and $\deg_x(g_2) > 0$, we have $\deg_x(\psi(g_1)) = \deg_x(g_1)$ and $\deg_x(\psi(g_2)) = \deg_x(g_2)$. It follows that

$$\text{res}_x(\psi(g_1), \psi(g_2)) = \psi(\text{res}_x(g_1, g_2)).$$

Therefore, $\psi(\text{res}_x(g_1, g_2))$ is a unit in $R/\langle g \rangle$. This implies that $\langle g, \text{res}_x(g_1, g_2) \rangle = R$. $\square$

Let $f \in R$ be a nontrivial element, and set $\deg_{x_n}(f) = s > 0$, where $\deg_{x_n}(f)$ denotes the degree of f with respect to x_n . Let $\text{lc}_{x_n}(f)$ be the leading coefficient of f with respect to x_n . Note that $\text{lc}_{x_n}(f) \in A[x_1, \dots, x_{n-1}]$; it may or may not belong to A . If $\text{lc}_{x_n}(f) \in A$, it will facilitate our treatment of the relevant problems. Now, we consider the following homomorphism ω defined by

$$\begin{aligned} \omega : R &\longrightarrow R \\ x_i &\longmapsto x_i + x_n^{d^{n-i}} \text{ for } i = 1, \dots, n-1, \\ x_n &\longmapsto x_n, \end{aligned}$$

where $d = \text{tdeg}(f) + 1$ and $\text{tdeg}(f)$ is the total degree of f . One checks that ω is an automorphism, with $\omega^{-1}(x_i) = x_i - x_n^{d^{n-i}}$ for $i = 1, \dots, n-1$, and $\omega^{-1}(x_n) = x_n$. Then $\text{lc}_{x_n}(\omega(f)) \in A$, and there exists a unique term in f whose coefficient equals $\text{lc}_{x_n}(\omega(f))$. Since the proof is similar to that of Lemma 4.58 in [36], we omit it.

Let $p_1 \in A$ be irreducible. It follows from A being a PID that $A/\langle p_1 \rangle$ is a field. We now introduce another homomorphism as follows:

$$\begin{aligned} \phi_{p_1} : \quad A[x_1, \dots, x_n] &\longrightarrow (A/\langle p_1 \rangle)[x_1, \dots, x_n] \\ \sum c_{i_1 \dots i_n} \cdot x_1^{i_1} \cdots x_n^{i_n} &\longmapsto \sum \overline{c_{i_1 \dots i_n}} \cdot x_1^{i_1} \cdots x_n^{i_n}, \end{aligned}$$

where $c_{i_1 \dots i_n} \in A$ and $\overline{c_{i_1 \dots i_n}} \in A/\langle p_1 \rangle$. We denote $(A/\langle p_1 \rangle)[x_1, \dots, x_n]$ by $\overline{R}$. This homomorphism can be extended canonically to the homomorphism $\phi_{p_1} : R^{l \times l} \rightarrow \overline{R}^{l \times l}$ by applying ϕ_{p_1} entry-wise. For convenience, we use $\overline{\mathbf{M}}$ to denote $\phi_{p_1}(\mathbf{M})$ in $\overline{R}^{l \times l}$, where $\mathbf{M} \in R^{l \times l}$.

Lemma 2.18. *Let $\mathbf{M} \in R^{l \times l}$, and let $p_1 \in A$ be irreducible. If there exists an integer r with $1 \leq r \leq l$ such that $J_r(\mathbf{M}) = R$ and $\text{rank}(\overline{\mathbf{M}}) = r$, then $J_r(\overline{\mathbf{M}}) = \overline{R}$.*

Proof. Let $a_1, \dots, a_\beta \in R$ be all the $r \times r$ minors of $\mathbf{M}$, and let $b_1, \dots, b_\beta \in R$ be all the $r \times r$ reduced minors of $\mathbf{M}$, where $\beta = \binom{l}{r}^2$. Then $a_j = d_r(\mathbf{M}) \cdot b_j$ for $j = 1, \dots, \beta$. Moreover, $\overline{a_1}, \dots, \overline{a_\beta} \in \overline{R}$ are all the $r \times r$ minors of $\overline{\mathbf{M}}$. Since $J_r(\mathbf{M}) = R$, there are $h_1, \dots, h_\beta \in R$ such that

$$d_r(\mathbf{M}) = a_1 h_1 + \dots + a_\beta h_\beta. \quad (1)$$

Since $\text{rank}(\overline{\mathbf{M}}) = r$, there exists at least one integer j_0 with $1 \leq j_0 \leq \beta$ such that $\overline{a_{j_0}} \neq 0$ in $\overline{R}$. It follows from $a_j = d_r(\mathbf{M}) \cdot b_j$ that

$$\overline{a_j} = \overline{d_r(\mathbf{M})} \cdot \overline{b_j}, \quad (2)$$

where $j = 1, \dots, \beta$. Then $\overline{d_r(\mathbf{M})} \neq 0$ and $\overline{b_{j_0}} \neq 0$ in $\overline{R}$. Combining Equations (1) and (2), we have

$$1 = \overline{b_1} \cdot \overline{h_1} + \dots + \overline{b_\beta} \cdot \overline{h_\beta}. \quad (3)$$

Equation (3) implies that $d_r(\overline{\mathbf{M}}) = \overline{d_r(\mathbf{M})}$ and $\overline{b_1}, \dots, \overline{b_\beta}$ are all $r \times r$ reduced minors of $\overline{\mathbf{M}}$. Therefore, $J_r(\overline{\mathbf{M}}) = \overline{R}$. $\square$

3. Equivalence of square matrices with irreducible power determinants in A

In this section, we consider the case where the determinant of a square matrix over R is a power of an irreducible element in A . The main result is stated as follows.

Theorem 3.1. *Let $\mathbf{M} \in R^{l \times l}$ with $\det(\mathbf{M}) = p_1^{t_1}$, where $p_1 \in A$ is irreducible, and t_1 is a positive integer. Then $\mathbf{M} \sim \text{SNF}(\mathbf{M})$ if and only if $J_i(\mathbf{M}) = R$ for all $i = 1, \dots, l$.*

The necessity of Theorem 3.1 follows directly from Lemma 2.6. In the following, we illustrate the three key steps in the sufficiency proof of Theorem 3.1 through an example.

Example 3.2. *Let $\mathbf{M} \in R^{3 \times 3}$ with $\det(\mathbf{M}) = p_1^3$, and let $\text{diag}(1, p_1, p_1^2)$ be the Smith normal form of $\mathbf{M}$, where $p_1 \in A$ is irreducible. Assume that $J_i(\mathbf{M}) = R$ for $i = 1, 2, 3$. Under this assumption, we proceed in three steps.*

First, we show that there exists $\mathbf{G}_1 \in R^{3 \times 3}$ such that

$$\mathbf{M} \sim \text{diag}(1, p_1, p_1) \cdot \mathbf{G}_1.$$

Second, we prove that there exists $\mathbf{G}_2 \in R^{3 \times 3}$ such that

$$\mathbf{G}_1 \sim \text{diag}(1, 1, p_1) \cdot \mathbf{G}_2,$$

and consequently, there exists $\mathbf{U} \in \text{GL}_3(R)$ such that

$$\mathbf{M} \sim \text{diag}(1, p_1, p_1) \cdot \mathbf{U} \cdot \text{diag}(1, 1, p_1) \cdot \mathbf{G}_2.$$

Third, we establish that

$$\text{diag}(1, p_1, p_1) \cdot \mathbf{U} \cdot \text{diag}(1, 1, p_1) \sim \text{diag}(1, p_1, p_1^2).$$

Combining these three steps yields $\mathbf{M} \sim \text{SNF}(\mathbf{M})$.

In Example 3.2, the first and second steps are closely related, and the third step is the most crucial part in the proof of Theorem 3.1. To overcome the difficulties that arise in verifying the correctness of these steps, the central theoretical tool is Suslin's stability theorem, which requires $l \geq 3$. To ensure Theorem 3.1 holds for an arbitrary positive integer l , we need to discuss the size of $\mathbf{M} \in R^{l \times l}$. Since the case $l = 1$ is trivial, we only need to consider $l \geq 2$.

Based on the above analysis, the structure of this section is as follows. First, we treat the special case $l = 2$ and $t_1 = 1$. Second, we consider the general case for $l \geq 2$, and provide a complete proof of Theorem 3.1. Finally, we present an algorithm derived from the constructive proof, and use an example to illustrate the effectiveness of the algorithm.

3.1. The special case $l = 2$ and $t_1 = 1$

We now handle the special case $l = 2$ and $t_1 = 1$ in Theorem 3.1.

Lemma 3.3. *Let $\mathbf{M} \in R^{2 \times 2}$ with $\det(\mathbf{M}) = p_1$, where $p_1 \in A$ is irreducible. If $J_1(\mathbf{M}) = R$, then $\mathbf{M} \sim \text{diag}(1, p_1)$.*

Proof. We prove the statement by induction on n , the number of variables. The case $n = 0$ holds because A is a PID. Assuming the statement is true for $n - 1$, we prove it for n .

It follows from $\det(\mathbf{M}) = p_1$ and the irreducibility of p_1 that $d_1(\mathbf{M}) = 1$. This implies that $\text{rank}(\overline{\mathbf{M}}) = 1$. By Lemma 2.18, we have $J_1(\overline{\mathbf{M}}) = \overline{R}$. According to Theorem 2.12, there exist $\overline{\mathbf{G}} \in \overline{R}^{2 \times 1}$ and $\overline{\mathbf{H}} \in \overline{R}^{1 \times 2}$ such that $\overline{\mathbf{M}} = \overline{\mathbf{G}} \cdot \overline{\mathbf{H}}$, where $\overline{\mathbf{G}}$ is a ZRP matrix over $\overline{R}$. Then there exist $g_1, g_2, h_1, h_2 \in R$ and $\mathbf{Q} \in R^{2 \times 2}$ such that

$$\mathbf{M} = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix} \begin{pmatrix} h_1 & h_2 \end{pmatrix} + p_1 \mathbf{Q},$$

where $\overline{\mathbf{G}} = \begin{pmatrix} \overline{g_1} \\ \overline{g_2} \end{pmatrix}$ and $\overline{\mathbf{H}} = (\overline{h_1} \quad \overline{h_2})$. If $g_1 = 0$ or $g_2 = 0$, then the conclusion holds trivially. Now suppose $g_1 \neq 0$ and $g_2 \neq 0$. If any term in g_1 or g_2 has a coefficient divisible by p_1 , we move that term into $p_1 \mathbf{Q}$. Hence we may further assume that no coefficient of any term in g_1 or g_2 is divisible by p_1 . Since $\overline{\mathbf{G}}$ is ZRP, we have $\langle p_1, g_1, g_2 \rangle = R$. Let $\text{tdeg}(g_j)$ denote the total degree of g_j for $j = 1, 2$. Consider the automorphism $\omega : R \rightarrow R$ defined by

$$\begin{cases} \omega(x_i) = x_i + x_n^{d^{n-i}}, & i = 1, \dots, n-1, \\ \omega(x_n) = x_n, \end{cases}$$

where $d = \max\{\text{tdeg}(g_1), \text{tdeg}(g_2)\} + 1$. Let $\mathbf{M}' = \omega(\mathbf{M})$, $\mathbf{Q}' = \omega(\mathbf{Q})$, $g'_j = \omega(g_j)$ and $h'_j = \omega(h_j)$, where $j = 1, 2$. Let $\text{lc}_{x_n}(g'_j)$ denote the leading coefficient of g'_j with respect to x_n , where $j = 1, 2$. Since ω is an automorphism, it follows from $\langle p_1, g_1, g_2 \rangle = R$ that $\langle p_1, g'_1, g'_2 \rangle = R$. Moreover, there exists a unique term in g_j such that its coefficient equals $\text{lc}_{x_n}(g'_j)$, where $j = 1, 2$. This implies that $\text{lc}_{x_n}(g'_j) \in A$ and $p_1 \nmid \text{lc}_{x_n}(g'_j)$, where $j = 1, 2$. Since A is a PID, we get $\langle p_1, \text{lc}_{x_n}(g'_j) \rangle = A$ for $j = 1, 2$. When considering $p_1, \text{lc}_{x_n}(g'_j)$ as

elements within $A[x_1, \dots, x_{n-1}]$, it follows that $\langle p_1, \text{lc}_{x_n}(g'_j) \rangle = A[x_1, \dots, x_{n-1}]$ for $j = 1, 2$. Define g_0 as

$$g_0 = \begin{cases} g'_1, & \text{if } \deg_{x_n}(g'_1) = \deg_{x_n}(g'_2) = 0; \\ \text{res}_{x_n}(g'_1, g'_2), & \text{otherwise.} \end{cases}$$

It follows that $g_0 \in A[x_1, \dots, x_{n-1}]$. By Lemma 2.17, we have $\langle p_1, g_0 \rangle = A[x_1, \dots, x_{n-1}]$. Furthermore, there exist $u, v \in R$ such that $ug'_1 + vg'_2 = g_0$. Let $\mathbf{U} = \begin{pmatrix} u & v \\ -g'_2 & g'_1 \end{pmatrix}$. Then we obtain

$$\mathbf{U}\mathbf{M}' = \begin{pmatrix} u & v \\ -g'_2 & g'_1 \end{pmatrix} \begin{pmatrix} g'_1 \\ g'_2 \end{pmatrix} \begin{pmatrix} h'_1 & h'_2 \end{pmatrix} + p_1 \mathbf{U}\mathbf{Q}' = \begin{pmatrix} g_0 h'_1 & g_0 h'_2 \\ 0 & 0 \end{pmatrix} + p_1 \mathbf{U}\mathbf{Q}' = \begin{pmatrix} 1 & 0 \\ 0 & p_1 \end{pmatrix} \mathbf{W},$$

where $\det(\mathbf{U}) = g_0$ and $\mathbf{W} \in R^{2 \times 2}$. It follows from $\det(\mathbf{M}) = p_1$ and $p_1 \in A$ that $\det(\mathbf{M}') = p_1$. This implies that $\det(\mathbf{W}) = g_0$. Let $S_1 = \{g_0^{\theta_1} \mid \theta_1 \in \mathbb{N}\}$, where $\mathbb{N}$ is the set of natural numbers that includes 0. It is straightforward to show that S_1 is a multiplicative subset of $A[x_1, \dots, x_{n-1}]$. Set $A[x_1, \dots, x_{n-1}]_{S_1} = S_1^{-1}(A[x_1, \dots, x_{n-1}])$. Then

$$\mathbf{M}' \sim_{A[x_1, \dots, x_{n-1}]_{S_1}[x_n]} \text{diag}(1, p_1).$$

Since $\mathbf{M}' = \omega(\mathbf{M})$, we have $\det(\mathbf{M}') = p_1$ and $J_1(\mathbf{M}') = R$. Applying the specialization homomorphism $x_n \mapsto 0$ gives

$$\det(\mathbf{M}'(x_1, \dots, x_{n-1}, 0)) = p_1 \text{ and } J_1(\mathbf{M}'(x_1, \dots, x_{n-1}, 0)) = A[x_1, \dots, x_{n-1}].$$

By the induction hypothesis, we obtain

$$\mathbf{M}'(x_1, \dots, x_{n-1}, 0) \sim_{A[x_1, \dots, x_{n-1}]} \text{diag}(1, p_1).$$

As $A[x_1, \dots, x_{n-1}] \subset A[x_1, \dots, x_{n-1}]_{S_1}[x_n]$, we get

$$\mathbf{M}' \sim_{A[x_1, \dots, x_{n-1}]_{S_1}[x_n]} \mathbf{M}'(x_1, \dots, x_{n-1}, 0).$$

Let $S_2 = \{p_1^{\theta_2} \mid \theta_2 \in \mathbb{N}\}$. As $p_1 \in A$ and $A \subset A[x_1, \dots, x_{n-1}]$, we may regard p_1 as an element of $A[x_1, \dots, x_{n-1}]$. Then S_2 is a multiplicative subset of $A[x_1, \dots, x_{n-1}]$. Set $A[x_1, \dots, x_{n-1}]_{S_2} = S_2^{-1}(A[x_1, \dots, x_{n-1}])$. By the fact that $\mathbf{M}' = \text{diag}(1, p_1) \cdot \text{diag}(1, p_1^{-1}) \cdot \mathbf{M}'$, we have

$$\mathbf{M}' \sim_{A[x_1, \dots, x_{n-1}]_{S_2}[x_n]} \text{diag}(1, p_1).$$

Therefore,

$$\mathbf{M}' \sim_{A[x_1, \dots, x_{n-1}]_{S_2}[x_n]} \mathbf{M}'(x_1, \dots, x_{n-1}, 0).$$

It follows from $\langle p_1, g_0 \rangle = A[x_1, \dots, x_{n-1}]$ that S_1 and S_2 are comaximal multiplicative subsets of $A[x_1, \dots, x_{n-1}]$. By Theorem 2.15, we conclude that

$$\mathbf{M}' \sim_{A[x_1, \dots, x_{n-1}][x_n]} \mathbf{M}'(x_1, \dots, x_{n-1}, 0).$$

This implies that

$$\mathbf{M}' \sim_{A[x_1, \dots, x_{n-1}][x_n]} \text{diag}(1, p_1).$$

Hence, there exist $\mathbf{U}', \mathbf{V}' \in \text{GL}_2(R)$ such that $\mathbf{U}'\mathbf{M}'\mathbf{V}' = \text{diag}(1, p_1)$. Let $\mathbf{U} = \omega^{-1}(\mathbf{U}')$ and $\mathbf{V} = \omega^{-1}(\mathbf{V}')$. Then $\mathbf{U}, \mathbf{V} \in R^{2 \times 2}$ are also unimodular matrices, and $\mathbf{U}\mathbf{M}\mathbf{V} = \text{diag}(1, p_1)$. Therefore, $\mathbf{M} \sim \text{diag}(1, p_1)$. $\square$

Remark 3.4. Since $\mathbf{M}$ in Lemma 3.3 is a 2×2 matrix, the condition $J_2(\mathbf{M}) = R$ is automatically satisfied.

The proof above is constructive; more precisely, it recursively reduces the number of variables while recording the associated left and right unimodular transformations. We formalize this construction as a procedure

$$(\mathbf{U}, \mathbf{V}) := \text{PrimeSmith}_{2,R}(\mathbf{M}, p_1),$$

whose details are given in [Appendix B.1](#).

3.2. The general case $l \geq 2$

For any matrix $\mathbf{M} \in R^{2 \times 2}$ with $p_1 \mid \det(\mathbf{M})$, the ZLP matrix factorization theorem allows us to extract p_1 from $\mathbf{M}$. This is made precise in the following lemma.

Lemma 3.5. Let $\mathbf{M} \in R^{2 \times 2}$ with $p_1 \mid \det(\mathbf{M})$, where $p_1 \in A$ is irreducible. If $J_1(\mathbf{M}) = R$, then there are $\mathbf{G}_1, \mathbf{F}_1 \in R^{2 \times 2}$ such that $\mathbf{M} = \mathbf{G}_1\mathbf{F}_1$ with $\det(\mathbf{G}_1) = p_1$.

Proof. If $d_1(\mathbf{M}) \neq 1$, then $d_1(\mathbf{M})$ can be factored out from $\mathbf{M}$, yielding a matrix $\mathbf{M}' \in R^{2 \times 2}$ of $d_1(\mathbf{M}') = 1$. Consequently, we may assume that $d_1(\mathbf{M}) = 1$. Let $\mathbf{M} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}$, where $f_i \in R$ for $i = 1, \dots, 4$. Then $\langle f_1, f_2, f_3, f_4 \rangle = R$ by the fact that $J_1(\mathbf{M}) = R$. Consider the following matrix

$$\mathbf{N} = (\mathbf{M}, p_1 \mathbf{I}_2) = \begin{pmatrix} f_1 & f_2 & p_1 & 0 \\ f_3 & f_4 & 0 & p_1 \end{pmatrix}.$$

It is straightforward to check that $d_2(\mathbf{N}) = p_1$ and $J_2(\mathbf{N}) = R$. By Theorem 2.10, there exist $\mathbf{G}_1 \in R^{2 \times 2}$ and $\mathbf{F} \in R^{2 \times 4}$ such that $\mathbf{N} = \mathbf{G}_1\mathbf{F}$, where $\det(\mathbf{G}_1) = p_1$ and $\mathbf{F}$ is a ZLP matrix. Let $\mathbf{F} = (\mathbf{F}_1, \mathbf{F}_2)$, where $\mathbf{F}_1, \mathbf{F}_2 \in R^{2 \times 2}$. Then, we obtain $\mathbf{M} = \mathbf{G}_1\mathbf{F}_1$. $\square$

We now introduce the following two results, which verify that the first and second steps in Example 3.2 are valid for every $l \geq 2$, not merely for $l = 3$.

Theorem 3.6. Let $\mathbf{M} \in R^{l \times l}$, and let $p_1 \in A$ be irreducible. If there is an integer r with $0 \leq r \leq l - 1$ such that $\text{rank}(\overline{\mathbf{M}}) = r$ and $J_r(\mathbf{M}) = R$, then there exist $\mathbf{U} \in \text{GL}_l(R)$ and $\mathbf{G} \in R^{l \times l}$ such that

$$\mathbf{U}\mathbf{M} = \text{diag}(\underbrace{1, \dots, 1}_r, p_1, \dots, p_1) \cdot \mathbf{G}.$$

Proof. If $r = 0$, then the conclusion holds trivially. Under the assumption that $1 \leq r \leq l-1$, we consider the following two cases.

We first address the case $l > 2$. It follows from Lemma 2.18 that $J_r(\overline{\mathbf{M}}) = \overline{R}$. According to Theorem 2.12, there exist $\overline{\mathbf{F}} \in \overline{R}^{l \times r}$ and $\overline{\mathbf{H}} \in \overline{R}^{r \times l}$ such that $\overline{\mathbf{M}} = \overline{\mathbf{F}} \cdot \overline{\mathbf{H}}$, where $\overline{\mathbf{F}}$ is a ZRP matrix over $\overline{R}$. Based on the Quillen-Suslin theorem, there exists $\overline{\mathbf{P}}' \in \text{GL}_l(\overline{R})$ such that

$$\overline{\mathbf{P}}' \cdot \overline{\mathbf{F}} = \begin{pmatrix} \overline{\mathbf{I}}_r \\ \mathbf{0}_{(l-r) \times r} \end{pmatrix}.$$

Let $\det(\overline{\mathbf{P}}') = \zeta$. Then ζ is a unit in $\overline{R}$. Set $\overline{\mathbf{P}} = \text{diag}(\underbrace{1, \dots, 1}_{l-1}, \zeta^{-1}) \cdot \overline{\mathbf{P}}'$. Then $\overline{\mathbf{P}} \in \text{SL}_l(\overline{R})$.

Moreover,

$$\overline{\mathbf{P}} \cdot \overline{\mathbf{F}} = \begin{pmatrix} \overline{\mathbf{I}}_r \\ \mathbf{0}_{(l-r) \times r} \end{pmatrix}.$$

By Theorem 2.13, we get $\text{SL}_l(\overline{R}) = \text{E}_l(\overline{R})$ for $l > 2$. This implies that there exist third-class elementary matrices $\overline{\mathbf{P}}_1, \dots, \overline{\mathbf{P}}_t \in \overline{R}^{l \times l}$ such that $\overline{\mathbf{P}} = \prod_{i=1}^t \overline{\mathbf{P}}_i$. For each matrix $\overline{\mathbf{P}}_i$, there is a third-class elementary matrix $\mathbf{U}_i \in R^{l \times l}$ such that $\mathbf{U}_i \equiv \overline{\mathbf{P}}_i \pmod{p_1}$. Let $\mathbf{U} = \prod_{i=1}^t \mathbf{U}_i$. Then $\mathbf{U} \in \text{GL}_l(R)$. In addition, we have

$$\mathbf{U}\mathbf{M} \equiv \mathbf{P}\mathbf{F}\mathbf{H} \equiv \begin{pmatrix} \mathbf{H} \\ \mathbf{0}_{(l-r) \times l} \end{pmatrix} \pmod{p_1}.$$

It follows that the last $l-r$ rows of $\mathbf{U}\mathbf{M}$ are divisible by p_1 . Consequently, there exists some matrix $\mathbf{G} \in R^{l \times l}$ such that

$$\mathbf{U}\mathbf{M} = \text{diag}(\underbrace{1, \dots, 1}_r, p_1, \dots, p_1) \cdot \mathbf{G}.$$

Now, for the case $l = 2$ we may assume that $d_1(\mathbf{M}) = 1$. Then $r = 1$ and $p_1 \mid \det(\mathbf{M})$. By Lemma 3.5, there exist $\mathbf{G}_1, \mathbf{F}_1 \in R^{2 \times 2}$ such that $\mathbf{M} = \mathbf{G}_1 \mathbf{F}_1$ and $\det(\mathbf{G}_1) = p_1$. According to the Cauchy-Binet formula and $J_1(\mathbf{M}) = R$, one checks that $J_1(\mathbf{G}_1) = R$. By Lemma 3.3, there exist $\mathbf{U}', \mathbf{V}' \in \text{GL}_2(R)$ such that $\mathbf{G}_1 = \mathbf{U}' \cdot \text{diag}(1, p_1) \cdot \mathbf{V}'$. Let $\mathbf{U} = (\mathbf{U}')^{-1}$. Then we have $\mathbf{U}\mathbf{M} = \text{diag}(1, p_1) \cdot \mathbf{G}$, where $\mathbf{G} = \mathbf{V}' \mathbf{F}_1$. $\square$

The proof of Theorem 3.6 yields an explicit procedure that extracts the diagonal factor $\text{diag}(\underbrace{1, \dots, 1}_r, p_1, \dots, p_1)$ from $\mathbf{M}$. We denote this procedure by

$$(\mathbf{U}, \mathbf{G}) := \text{DiagExtract}_{l,R}(\mathbf{M}, p_1, r),$$

and give its details in [Appendix B.2](#).

Lemma 3.7. *Let $\mathbf{M} \in R^{l \times l}$ with $\det(\mathbf{M}) = p_1^{t_1}$, where $p_1 \in A$ is irreducible, and t_1 is a positive integer. Assume that $\text{SNF}(\mathbf{M}) = \text{diag}(p_1^{s_1}, \dots, p_1^{s_l})$, where $0 = s_0 \leq s_1 \leq \dots \leq s_l$*

and $\sum_{i=1}^l s_i = t_1$. If there exist integers r, s (with $0 \leq r \leq l-1$ and $s_r \leq s < s_{r+1}$) and a matrix $\mathbf{G} \in R^{l \times l}$ such that

$$J_i(\mathbf{M}) = R \text{ for } i = 1, \dots, r, \text{ and } \mathbf{M} \sim \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^s, \dots, p_1^s) \cdot \mathbf{G},$$

then $J_i(\mathbf{G}) = R$ for $i = 1, \dots, r$, and $\text{rank}(\overline{\mathbf{G}}) = r$.

The proof of Lemma 3.7 is similar to that of Lemmas 3.5 and 3.7 in [14], and it is omitted here.

We next verify the correctness of the third step in Example 3.2.

Theorem 3.8. Let $\mathbf{M} \in R^{l \times l}$ with $\det(\mathbf{M}) = p_1^{t_1}$, where $p_1 \in A$ is irreducible. Assume that $J_i(\mathbf{M}) = R$ for $i = 1, \dots, l$, and $\text{SNF}(\mathbf{M}) = \text{diag}(p_1^{s_1}, \dots, p_1^{s_l})$, where $0 = s_0 \leq s_1 \leq \dots \leq s_l$ and $\sum_{i=1}^l s_i = t_1$. Let

$$\mathbf{W} = \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^s, \dots, p_1^s) \cdot \mathbf{U} \cdot \text{diag}(\underbrace{1, \dots, 1}_r, p_1, \dots, p_1),$$

where $\mathbf{U} \in \text{GL}_l(R)$, and r, s are integers satisfying $0 \leq r \leq l-1$ and $s_r \leq s < s_{r+1}$. If there is $\mathbf{G} \in R^{l \times l}$ such that $\mathbf{M} \sim \mathbf{W}\mathbf{G}$, then

- (1) $d_i(\mathbf{W}) = p_1^{s_1 + \dots + s_i}$ and $J_i(\mathbf{W}) = R$ for $i = 1, \dots, r$;
- (2) $\mathbf{W} \sim \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^{s+1}, \dots, p_1^{s+1})$.

Proof. If $r = 0$, then the conclusions hold trivially. Therefore, we only need to consider the case $1 \leq r \leq l-1$. Let $\mathbf{D}_1 = \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^s, \dots, p_1^s)$ and $\mathbf{D}_2 = \text{diag}(1, \dots, 1, p_1, \dots, p_1)$.

(1) It follows from $\mathbf{M} \sim \mathbf{W}\mathbf{G}$ that $d_i(\mathbf{W}\mathbf{G}) = d_i(\mathbf{M}) = p_1^{s_1 + \dots + s_i}$ for $i = 1, \dots, r$. On the one hand, one checks that $d_i(\mathbf{W}) \mid p_1^{s_1 + \dots + s_i}$. On the other hand, it follows from $\mathbf{W} = \mathbf{D}_1 \mathbf{U} \mathbf{D}_2$ and $d_i(\mathbf{D}_1) = p_1^{s_1 + \dots + s_i}$ that $p_1^{s_1 + \dots + s_i} \mid d_i(\mathbf{W})$. Therefore, $d_i(\mathbf{W}) = p_1^{s_1 + \dots + s_i}$ for $i = 1, \dots, r$. According to the Cauchy-Binet formula, for any $i \times i$ minor f of $\mathbf{M}$, we have $f = \sum_{j=1}^{\alpha} h_j g_j$, where $h_1, \dots, h_{\alpha} \in R$ are all the $i \times i$ minors of $\mathbf{W}$. This implies that

$$\frac{f}{d_i(\mathbf{M})} = \sum_{j=1}^{\alpha} \frac{h_j}{d_i(\mathbf{W})} g_j. \quad (4)$$

Clearly, the left side of Equation (4) is an $i \times i$ reduced minor of $\mathbf{M}$. It follows from Equation (4) that $J_i(\mathbf{M}) \subseteq J_i(\mathbf{W})$. Since $J_i(\mathbf{M}) = R$, we obtain $J_i(\mathbf{W}) = R$, where $i = 1, \dots, r$.

(2) If $s_1 = \dots = s_r = s$, then the conclusion is obvious. Suppose there exists a positive integer r_0 with $1 \leq r_0 < r$ such that $s_1 \leq \dots \leq s_{r_0} < s_{r_0+1} = s$.

Let $\mathbf{U} = \begin{pmatrix} \mathbf{U}_1 & \mathbf{U}_2 \\ \mathbf{U}_3 & \mathbf{U}_4 \end{pmatrix}$, where $\mathbf{U}_1 \in R^{r_0 \times r}$, $\mathbf{U}_2 \in R^{r_0 \times (l-r)}$, $\mathbf{U}_3 \in R^{(l-r_0) \times r}$, $\mathbf{U}_4 \in R^{(l-r_0) \times (l-r)}$. We claim that $(\mathbf{U}_1, p_1 \mathbf{U}_2)$ is a ZLP matrix. Let $a_1, \dots, a_{\beta} \in R$ be all the $r_0 \times r_0$ minors of $\mathbf{U}_1$, and $b_1, \dots, b_{\gamma} \in R$ be all the other $r_0 \times r_0$ minors of $(\mathbf{U}_1, \mathbf{U}_2)$. Then all the $r_0 \times r_0$ minors of $(\mathbf{U}_1, p_1 \mathbf{U}_2)$ are $a_1, \dots, a_{\beta}, b_1 p_1^{r_1}, \dots, b_{\gamma} p_1^{r_{\gamma}}$, where $r_1, \dots, r_{\gamma}$ are positive integers. Let $I = \langle a_1, \dots, a_{\beta}, b_1 p_1^{r_1}, \dots, b_{\gamma} p_1^{r_{\gamma}} \rangle$. If $I \neq R$, then there exists a maximal ideal

$\mathfrak{m} \subsetneq R$ containing I . Since $\mathbf{U}$ is unimodular, we get $\langle a_1, \dots, a_\beta, b_1, \dots, b_\gamma \rangle = R$. This implies that $p_1^{r_\eta} \in \mathfrak{m}$ for some positive integer $r_\eta \in \mathbb{N}$. As $\mathfrak{m}$ is maximal, it follows that $p_1 \in \mathfrak{m}$. By the fact that $d_{r_0}(\mathbf{W}) = p_1^{s_1 + \dots + s_{r_0}}$ and

$$\mathbf{W} = \begin{pmatrix} \text{diag}(p_1^{s_1}, \dots, p_1^{s_{r_0}}) \cdot \mathbf{U}_1 & \text{diag}(p_1^{s_1+1}, \dots, p_1^{s_{r_0}+1}) \cdot \mathbf{U}_2 \\ p_1^s \cdot \mathbf{U}_3 & p_1^{s+1} \cdot \mathbf{U}_4 \end{pmatrix}, \quad (5)$$

$a_1, \dots, a_\beta$ are some of all the $r_0 \times r_0$ reduced minors of $\mathbf{W}$, and all the other $r_0 \times r_0$ reduced minors of $\mathbf{W}$ are divisible by p_1 . This implies that all the $r_0 \times r_0$ reduced minors of $\mathbf{W}$ are contained in $\mathfrak{m}$. It follows from $J_{r_0}(\mathbf{W}) = R$ that $\mathfrak{m} = R$, which leads to a contradiction. Therefore, $(\mathbf{U}_1, p_1 \mathbf{U}_2)$ is a ZLP matrix.

According to the Quillen-Suslin theorem, there exists $\mathbf{P} \in \text{GL}_l(R)$ such that

$$(\mathbf{U}_1, p_1 \mathbf{U}_2) \mathbf{P} = (\mathbf{I}_{r_0}, \mathbf{0}_{r_0 \times (l-r_0)}).$$

Then

$$\mathbf{W} \mathbf{P} = \mathbf{D}_1 \begin{pmatrix} \mathbf{U}_1 & p_1 \mathbf{U}_2 \\ \mathbf{U}_3 & p_1 \mathbf{U}_4 \end{pmatrix} \mathbf{P} = \begin{pmatrix} \text{diag}(p_1^{s_1}, \dots, p_1^{s_{r_0}}) & \mathbf{0}_{r_0 \times (l-r_0)} \\ p_1^s \cdot \mathbf{V}_1 & p_1^{s+1} \cdot \mathbf{V}_2 \end{pmatrix},$$

where $(\mathbf{V}_1, \mathbf{V}_2) = (\mathbf{U}_3, p_1 \mathbf{U}_4) \mathbf{P}$. Since $s > s_i$ for $i = 1, \dots, r_0$, there exists another unimodular matrix $\mathbf{Q}_1 \in \text{GL}_l(R)$ such that

$$\mathbf{Q}_1 \mathbf{W} \mathbf{P} = \begin{pmatrix} \text{diag}(p_1^{s_1}, \dots, p_1^{s_{r_0}}) & \mathbf{0}_{r_0 \times (l-r_0)} \\ \mathbf{0}_{(l-r_0) \times r_0} & p_1^s \cdot \mathbf{V}_2 \end{pmatrix},$$

where $\mathbf{V}_2 \in R^{(l-r_0) \times (l-r_0)}$. We claim that $p_1 \mid d_{r-r_0+1}(\mathbf{V}_2)$, $p_1 \nmid d_{r-r_0}(\mathbf{V}_2)$ and $J_{r-r_0}(\mathbf{V}_2) = R$. It follows from Equation (5) that $p_1^{s_1 + \dots + s_r + s + 1} \mid d_{r+1}(\mathbf{W})$. As $\det(\mathbf{W}) = p_1^{s_1 + \dots + s_r + (l-r)(s+1)}$ and $d_i(\mathbf{W}) = p_1^{s_1 + \dots + s_i}$ for $i = 1, \dots, r$, we have

$$\text{SNF}(\mathbf{W}) = \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^{s+1}, \dots, p_1^{s+1}),$$

where $s_{r_0+1} = \dots = s_r = s$. Let $\mathbf{C} = \mathbf{Q}_1 \mathbf{W} \mathbf{P}$. Since $\mathbf{Q}_1, \mathbf{P}$ are unimodular, we get

$$\text{SNF}(\mathbf{C}) = \text{SNF}(\mathbf{W}) \text{ and } J_i(\mathbf{C}) = J_i(\mathbf{W}) = R \text{ for } i = 1, \dots, r.$$

Let $\mathbf{G}' = \begin{pmatrix} \mathbf{I}_{r_0} & \mathbf{0}_{r_0 \times (l-r_0)} \\ \mathbf{0}_{(l-r_0) \times r_0} & \mathbf{V}_2 \end{pmatrix}$. Then

$$\mathbf{C} = \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^s, \dots, p_1^s) \cdot \mathbf{G}'.$$

Based on Lemma 3.7, we have $\text{rank}(\overline{\mathbf{G}'}) = r$ and $J_r(\mathbf{G}') = R$. It follows from $\text{rank}(\overline{\mathbf{G}'}) = r$ that $p_1 \mid d_{r-r_0+1}(\mathbf{V}_2)$ and $p_1 \nmid d_{r-r_0}(\mathbf{V}_2)$. Since $J_r(\mathbf{G}') = R$ and $d_r(\mathbf{G}') = 1$, we obtain $I_r(\mathbf{G}') = R$. Since $I_{l-r_0}(\mathbf{V}_2) \subset \dots \subset I_{r-r_0}(\mathbf{V}_2)$, we get

$$I_r(\mathbf{G}') = \sum_{i=r-r_0}^{\min\{r, l-r_0\}} I_i(\mathbf{V}_2) = I_{r-r_0}(\mathbf{V}_2).$$

Thus $J_{r-r_0}(\mathbf{V}_2) = R$. According to Theorem 3.6, there exists $\mathbf{Q}_2 \in \text{GL}_{l-r_0}(R)$ such that

$$\mathbf{V}_2 = \mathbf{Q}_2^{-1} \cdot \text{diag}(\underbrace{1, \dots, 1}_{r-r_0}, p_1, \dots, p_1) \cdot \mathbf{G}'',$$

where $\mathbf{G}'' \in R^{(l-r_0) \times (l-r_0)}$. Since $\det(\mathbf{V}_2) = \det(\mathbf{G}') = p_1^{l-r}$, we have $\det(\mathbf{G}'') = 1$. This implies that $\mathbf{G}''$ is unimodular. Furthermore,

$$\begin{aligned} \mathbf{Q}_1 \mathbf{W} \mathbf{P} &= \begin{pmatrix} \text{diag}(p_1^{s_1}, \dots, p_1^{s_{r_0}}) & \mathbf{0}_{r_0 \times (l-r_0)} \\ \mathbf{0}_{(l-r_0) \times r_0} & p_1^s \cdot \mathbf{Q}_2^{-1} \cdot \text{diag}(\underbrace{1, \dots, 1}_{r-r_0}, p_1, \dots, p_1) \cdot \mathbf{G}'' \end{pmatrix} \\ &= \begin{pmatrix} \text{diag}(p_1^{s_1}, \dots, p_1^{s_{r_0}}) & \mathbf{0}_{r_0 \times (l-r_0)} \\ \mathbf{0}_{(l-r_0) \times r_0} & \mathbf{Q}_2^{-1} \cdot \text{diag}(\underbrace{p_1^s, \dots, p_1^s}_{r-r_0}, p_1^{s+1}, \dots, p_1^{s+1}) \cdot \mathbf{G}'' \end{pmatrix}. \end{aligned}$$

As $s_{r_0+1} = \dots = s_r = s$, we have

$$\begin{pmatrix} \mathbf{I}_{r_0} & \mathbf{0}_{r_0 \times (l-r_0)} \\ \mathbf{0}_{(l-r_0) \times r_0} & \mathbf{Q}_2 \end{pmatrix} \cdot \mathbf{Q}_1 \mathbf{W} \mathbf{P} = \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^{s+1}, \dots, p_1^{s+1}) \cdot \begin{pmatrix} \mathbf{I}_{r_0} & \mathbf{0}_{r_0 \times (l-r_0)} \\ \mathbf{0}_{(l-r_0) \times r_0} & \mathbf{G}'' \end{pmatrix}.$$

Therefore, $\mathbf{W} \sim \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^{s+1}, \dots, p_1^{s+1})$.

If $s_1 \leq \dots \leq s_r < s$, then the same conclusion follows from the above method. $\square$

For the matrix $\mathbf{W}$ in Theorem 3.8, its proof produces unimodular matrices $\mathbf{L}, \mathbf{R} \in \text{GL}_l(R)$ that satisfy $\mathbf{LWR} = \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^{s+1}, \dots, p_1^{s+1})$. We write

$$(\mathbf{L}, \mathbf{R}) := \text{DiagMerge}_{l,R}(\mathbf{W}, \mathbf{U}, p_1, r, s_1, \dots, s_r, s)$$

for this construction, and outline the computational steps in Appendix B.3.

Based on Theorem 3.6, Lemma 3.7 and Theorem 3.8, we now present the complete proof of Theorem 3.1.

Proof of Theorem 3.1. Assume that $\text{SNF}(\mathbf{M}) = \text{diag}(p_1^{s_1}, \dots, p_1^{s_l})$, where $0 \leq s_1 \leq \dots \leq s_l$ and $\sum_{i=1}^l s_i = t_1$.

Necessity. If $\mathbf{M} \sim \text{SNF}(\mathbf{M})$, then by Lemma 2.6 we have $J_i(\mathbf{M}) = J_i(\text{SNF}(\mathbf{M})) = R$ for $i = 1, \dots, l$.

Sufficiency. Since $d_1(\mathbf{M}) = p_1^{s_1}$, we have $\mathbf{M} = \text{diag}(p_1^{s_1}, \dots, p_1^{s_1}) \cdot \mathbf{G}_1$, where $\mathbf{G}_1 \in R^{l \times l}$. If $s_2 = s_1$, then $\mathbf{M} = \text{diag}(p_1^{s_1}, p_1^{s_2}, \dots, p_1^{s_2}) \cdot \mathbf{G}_2$, where $\mathbf{G}_2 = \mathbf{G}_1$. If $s_2 > s_1$, then it follows from Lemma 3.7 and Theorem 3.6 that $\mathbf{G}_1 = \mathbf{U}_{21} \cdot \text{diag}(1, p_1, \dots, p_1) \cdot \mathbf{G}_{21}$, where $\mathbf{U}_{21} \in \text{GL}_l(R)$ and $\mathbf{G}_{21} \in R^{l \times l}$. Then, we get

$$\mathbf{M} \sim \text{diag}(p_1^{s_1}, p_1^{s_1}, \dots, p_1^{s_1}) \cdot \mathbf{U}_{21} \cdot \text{diag}(1, p_1, \dots, p_1) \cdot \mathbf{G}_{21}.$$

According to Theorem 3.8, we have

$$\text{diag}(p_1^{s_1}, p_1^{s_1}, \dots, p_1^{s_1}) \cdot \mathbf{U}_{21} \cdot \text{diag}(1, p_1, \dots, p_1) \sim \text{diag}(p_1^{s_1}, p_1^{s_1+1}, \dots, p_1^{s_1+1}).$$

Then $\mathbf{M} \sim \text{diag}(p_1^{s_1}, p_1^{s_1+1}, \dots, p_1^{s_1+1}) \cdot \mathbf{G}'_{21}$ for some matrix $\mathbf{G}'_{21} \in R^{l \times l}$. Repeating this process for $s_2 - s_1$ times, we obtain $\mathbf{M} \sim \text{diag}(p_1^{s_1}, p_1^{s_2}, \dots, p_1^{s_2}) \cdot \mathbf{G}_2$ for some matrix $\mathbf{G}_2 \in R^{l \times l}$. We can use the same method to get $\mathbf{M} \sim \text{diag}(p_1^{s_1}, p_1^{s_2}, \dots, p_1^{s_l}) \cdot \mathbf{G}_l$, where $\mathbf{G}_l \in R^{l \times l}$. It is easy to check that $\mathbf{G}_l$ is a unimodular matrix. Therefore, $\mathbf{M} \sim \text{diag}(p_1^{s_1}, p_1^{s_2}, \dots, p_1^{s_l})$. $\square$

3.3. Algorithm and example

According to Theorem 3.1, we can develop an algorithm to compute unimodular matrices $\mathbf{U}, \mathbf{V} \in \text{GL}_l(R)$ such that $\text{SNF}(\mathbf{M}) = \mathbf{UMV}$.

Algorithm 1: PrimePowerSmith($\mathbf{M}$)

Input : A matrix $\mathbf{M} \in R^{l \times l}$ such that $\det(\mathbf{M})$ is a power of an irreducible element of A .

Output: Either “ $\mathbf{M}$ is not equivalent to its Smith normal form”, or $\mathbf{S} \in R^{l \times l}$ and $\mathbf{U}, \mathbf{V} \in \text{GL}_l(R)$ such that $\mathbf{S} = \text{SNF}(\mathbf{M})$ and $\mathbf{S} = \mathbf{UMV}$.

```

1 begin
2   compute  $\det(\mathbf{M})$  and express it as  $p_1^{t_1}$ , where  $p_1 \in A$  is irreducible and  $t_1$  is a
   positive integer;
3   for  $i = 1$  to  $l$  do
4     compute the  $i$ -th invariant factor of  $\mathbf{M}$ , and determine  $s_i$  with  $\Phi_i = p_1^{s_i}$ ;
5     compute a Gröbner basis  $\mathcal{G}_i$  of  $J_i(\mathbf{M})$ ;
6     if  $1 \notin \mathcal{G}_i$  then
7       return “ $\mathbf{M}$  is not equivalent to its Smith normal form”;
8   set  $\mathbf{S} := \text{diag}(p_1^{s_1}, \dots, p_1^{s_l})$ ; //  $0 \leq s_1 \leq \dots \leq s_l$  and  $s_1 + \dots + s_l = t_1$ ;
9    $\mathbf{U}_0 \leftarrow \mathbf{I}_l$ ,  $\mathbf{D} \leftarrow \text{diag}(p_1^{s_1}, \dots, p_1^{s_l})$ ,  $\mathbf{G}_0 \leftarrow \mathbf{M}/p_1^{s_1}$ ; // extract  $p_1^{s_1}$  from  $\mathbf{M}$ 
10  for  $i = 2$  to  $l$  do
11     $r \leftarrow i - 1$ ;
12    for  $j = 1$  to  $s_i - s_{i-1}$  do
13       $s \leftarrow s_{i-1} + j - 1$ ;
14       $(\mathbf{U}_1, \mathbf{G}_1) \leftarrow \text{DiagExtract}_{l,R}(\mathbf{G}_0, p_1, r)$ ; // see Appendix B.2
15       $\mathbf{W} \leftarrow \mathbf{D} \cdot \mathbf{U}_1^{-1} \cdot \text{diag}(\underbrace{1, \dots, 1}_r, p_1, \dots, p_1)$ ;
16       $(\mathbf{L}, \mathbf{R}) \leftarrow \text{DiagMerge}_{l,R}(\mathbf{W}, \mathbf{U}_1^{-1}, p_1, r, s_1, \dots, s_r, s)$ ; // see Appendix B.3
17       $\mathbf{U}_0 \leftarrow \mathbf{U}_0 \mathbf{L}^{-1}$ ,  $\mathbf{G}_0 \leftarrow \mathbf{R}^{-1} \mathbf{G}_1$ ;
18       $\mathbf{D} \leftarrow \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, \underbrace{p_1^{s+1}, \dots, p_1^{s+1}}_{l-r})$ ;
19   $\mathbf{U} \leftarrow \mathbf{U}_0^{-1}$ ,  $\mathbf{V} \leftarrow \mathbf{G}_0^{-1}$ ;
20  return  $\mathbf{S}, \mathbf{U}, \mathbf{V}$ .
```

Theorem 3.9. Algorithm 1 outputs as specified within a finite number of steps.

Proof. The correctness follows directly from Theorem 3.1. For termination, note that Step 5 invokes the Gröbner basis algorithm (Theorem 10.14 in [37]); Steps 14 and 16 invoke subroutines whose termination is guaranteed by the second Quillen-Suslin algorithm of [9], Suslin’s stability algorithm of [30], and the Vaserstein patching procedure of [32, 33]. Since each of these subroutines is known to terminate, and Algorithm 1 makes only finitely many calls to them, it terminates in finitely many steps. $\square$

The following example illustrates Algorithm 1.

Example 3.10. Let $A = \mathbb{Q}[y]$, $R = A[x_1, x_2]$, and $p_1 = y + 1$. Consider

$$\mathbf{M} = \begin{pmatrix} y+1 & 0 & 0 \\ -(y+x_2)(y+x_1) & (y+1)^2 & -y-x_1 \\ 1+(2-x_2)y & 0 & 1 \end{pmatrix}.$$

A direct computation yields $\det(\mathbf{M}) = p_1^3$. For each $i = 1, 2, 3$, we compute the Gröbner basis $\mathcal{G}_i$ of the ideal generated by the $i \times i$ reduced minors of $\mathbf{M}$. In each case we obtain $\mathcal{G}_i = \{1\}$, and hence $J_i(\mathbf{M}) = R$. By Theorem 3.1, $\mathbf{M}$ is equivalent to its Smith normal form. By Definition 2.3, it follows that $d_1(\mathbf{M}) = 1$, $d_2(\mathbf{M}) = p_1$ and $d_3(\mathbf{M}) = p_1^3$. Thus

$$\text{SNF}(\mathbf{M}) = \text{diag}(1, p_1, p_1^2).$$

We now apply Algorithm 1 to compute explicit matrices $\mathbf{U}, \mathbf{V} \in \text{GL}_3(R)$ such that

$$\mathbf{UMV} = \text{diag}(1, p_1, p_1^2).$$

Step 1. We first apply the diagonal extraction procedure with $r = 1$:

$$(\mathbf{U}_1, \mathbf{G}_1) := \text{DiagExtract}_{3,R}(\mathbf{M}, y+1, 1),$$

where

$$\mathbf{U}_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & x_1 - 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \mathbf{G}_1 = \begin{pmatrix} 1+(2-x_2)y & 0 & 1 \\ -x_1x_2 - y + x_1 - 1 & y+1 & -1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Then $\mathbf{U}_1\mathbf{M} = \text{diag}(1, y+1, y+1)\mathbf{G}_1$.

Step 2. We next apply the diagonal extraction procedure with $r = 2$:

$$(\mathbf{U}_2, \mathbf{G}_2) := \text{DiagExtract}_{3,R}(\mathbf{G}_1, y+1, 2),$$

where

$$\mathbf{U}_2 = \begin{pmatrix} 0 & -1 & -x_1x_2 + x_1 \\ 0 & 0 & 1 \\ -1 & -1 & -x_1x_2 + x_1 + x_2 - 1 \end{pmatrix}, \quad \mathbf{G}_2 = \begin{pmatrix} y+1 & -y-1 & 1 \\ 1 & 0 & 0 \\ x_2-1 & -1 & 0 \end{pmatrix}.$$

Then $\mathbf{U}_2\mathbf{G}_1 = \text{diag}(1, 1, y+1)\mathbf{G}_2$.

Step 3. The matrix for the diagonal merging step is

$$\begin{aligned} \mathbf{W} &= \text{diag}(1, y+1, y+1) \mathbf{U}_2^{-1} \text{diag}(1, 1, y+1) \\ &= \begin{pmatrix} 1 & x_2-1 & -y-1 \\ -y-1 & -(y+1)(x_2-1)x_1 & 0 \\ 0 & y+1 & 0 \end{pmatrix}. \end{aligned}$$

Applying the diagonal merging procedure, we compute

$$(\mathbf{L}, \mathbf{R}) := \text{DiagMerge}_{3,R}(\mathbf{W}, \mathbf{U}_2^{-1}, y+1, 2, 0, 1, 1),$$

where

$$\mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ -y-1 & -1 & -(x_2-1)(x_1-1) \end{pmatrix}, \quad \mathbf{R} = \begin{pmatrix} 1 & 1-x_2 & y+1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then $\mathbf{LWR} = \text{diag}(1, y+1, (y+1)^2)$.

Step 4. Since $\mathbf{M} = \mathbf{U}_1^{-1}\mathbf{W}\mathbf{G}_2$ and $\mathbf{LWR} = \text{diag}(1, y+1, (y+1)^2)$, we get

$$(\mathbf{LU}_1)\mathbf{M}(\mathbf{G}_2^{-1}\mathbf{R}) = \text{diag}(1, y+1, (y+1)^2).$$

Thus take $\mathbf{U} = \mathbf{LU}_1$ and $\mathbf{V} = \mathbf{G}_2^{-1}\mathbf{R}$. A direct computation gives

$$\mathbf{U} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ (1-x_2)(x_1-1) & -1 & -y-x_1 \end{pmatrix}, \quad \mathbf{V} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & x_2-1 & -1 \\ 1 & yx_2-2y-1 & 0 \end{pmatrix}.$$

Therefore,

$$\mathbf{UMV} = \text{diag}(1, y+1, (y+1)^2).$$

4. Equivalence of square matrices with determinants in A

In this section, we focus on square matrices with entries in R whose determinants belong to $A \setminus \{0\}$.

4.1. Main theorem

The main theorem is stated as follows.

Theorem 4.1. *Let $\mathbf{M} \in R^{l \times l}$ with $\det(\mathbf{M}) \in A \setminus \{0\}$. Then $\mathbf{M} \sim \text{SNF}(\mathbf{M})$ if and only if $J_i(\mathbf{M}) = R$ for $i = 1, \dots, l$.*

If $\det(\mathbf{M})$ is a unit in A , then $\mathbf{M}$ is unimodular and the result is trivial. Thus we may assume that $\det(\mathbf{M})$ is not a unit. We factorize $\det(\mathbf{M})$ over A as $\det(\mathbf{M}) = p_1^{t_1} \cdots p_k^{t_k}$, where $p_1, \dots, p_k \in A$ are pairwise coprime and irreducible, $k, t_1, \dots, t_k$ are positive integers. In Section 3, we have considered the case $k = 1$. Now, we generalize the main result of Section 3 to the case where $k \geq 1$ using mathematical induction, thereby completing the proof of Theorem 4.1.

The following lemma shows that $\mathbf{M}$ can be factorized as $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2$ with $\det(\mathbf{M}_1) = p_1^{t_1}$, where $\mathbf{M}_1, \mathbf{M}_2 \in R^{l \times l}$.

Lemma 4.2. *Let $\mathbf{M} \in R^{l \times l}$ with $\det(\mathbf{M}) = p_1^{t_1}h \in A$, where $\gcd(p_1, h) = 1$ and p_1 is irreducible. Then there exist $\mathbf{M}_1, \mathbf{M}_2 \in R^{l \times l}$ such that $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2$ with $\det(\mathbf{M}_1) = p_1^{t_1}$.*

Proof. Consider the matrix

$$\mathbf{W} = (\mathbf{M}, p_1^{t_1} \mathbf{I}_l) \in R^{l \times 2l}.$$

A direct computation gives $d_l(\mathbf{W}) = p_1^{t_1}$. Moreover, $p_1^{(l-1)t_1}$ and $\det(\mathbf{M})/p_1^{t_1}$ are two $l \times l$ reduced minors of $\mathbf{W}$. Since A is a PID and $\gcd(p_1, h) = 1$, it follows that $J_l(\mathbf{W}) = R$. Based on Theorem 2.10, there exist $\mathbf{M}_1 \in R^{l \times l}$ and $\mathbf{G}_1 \in R^{l \times 2l}$ such that

$$\mathbf{W} = \mathbf{M}_1 \mathbf{G}_1, \text{ and } \det(\mathbf{M}_1) = d_l(\mathbf{W}) = p_1^{t_1}.$$

Let $\mathbf{G}_1 = (\mathbf{M}_2, \mathbf{G}_2)$, where $\mathbf{M}_2, \mathbf{G}_2 \in R^{l \times l}$. Then $\mathbf{M} = \mathbf{M}_1 \mathbf{M}_2$. □

From Lemma 4.2 we obtain the procedure

$$(\mathbf{M}_1, \mathbf{M}_2) := \text{PrimeSplit}_{l,R}(\mathbf{M}, p_1^{t_1}),$$

whose details are outlined in Appendix B.4.

Theorem 4.3. *Let $f_1, \dots, f_l, g_1, \dots, g_l \in A \setminus \{0\}$ satisfy $f_i \mid f_{i+1}$ and $g_i \mid g_{i+1}$, where $i = 1, \dots, l-1$. Assume that $\mathbf{U} \in \text{GL}_l(R)$ and $\gcd(f_l, g_l) = 1$. Then*

$$\text{diag}(f_1, \dots, f_l) \cdot \mathbf{U} \cdot \text{diag}(g_1, \dots, g_l) \sim \text{diag}(f_1 g_1, \dots, f_l g_l).$$

Proof. Let $\mathbf{F} = \text{diag}(f_1, \dots, f_l)$, $\mathbf{G} = \text{diag}(g_1, \dots, g_l)$, $\mathbf{M} = \mathbf{F} \mathbf{U} \mathbf{G}$ and $\mathbf{D} = \mathbf{F} \mathbf{G}$. Since $f_i \mid f_{i+1}$ and $g_i \mid g_{i+1}$ for $i = 1, \dots, l-1$, the Smith normal form of $\mathbf{D}$ coincides with itself.

We employ mathematical induction on the number of variables $x_1, \dots, x_n$ to prove the statement.

When $n = 0$, by the fact that A is a PID, $\mathbf{M}$ is equivalent to its Smith normal form. Since $\mathbf{U}$ is unimodular, we have $d_i(\mathbf{F}) = d_i(\mathbf{F} \mathbf{U})$ by Lemma 2.6, where $i = 1, \dots, l$. It follows from $\gcd(f_l, g_l) = 1$ that $\gcd(\det(\mathbf{F} \mathbf{U}), \det(\mathbf{G})) = 1$. According to Lemma 2.7, we obtain

$$d_i(\mathbf{M}) = d_i(\mathbf{F} \mathbf{U}) \cdot d_i(\mathbf{G}) = d_i(\mathbf{F}) \cdot d_i(\mathbf{G}) = d_i(\mathbf{D}),$$

where $i = 1, \dots, l$. This implies that the Smith normal form of $\mathbf{M}$ is $\mathbf{D}$. Therefore, $\mathbf{M} \sim_R \mathbf{D}$. Hence, the statement holds for $n = 0$.

Assuming the statement is true for $n-1$, we now show it also holds for n .

We construct the following two sets

$$S_1 = \{f_l^{\theta_1} \mid \theta_1 \in \mathbb{N}\} \text{ and } S_2 = \{g_l^{\theta_2} \mid \theta_2 \in \mathbb{N}\}.$$

It is straightforward to show that $S_1, S_2 \subset A[x_1, \dots, x_{n-1}]$ are multiplicative sets. Moreover, it follows from $\gcd(f_l, g_l) = 1$ that S_1, S_2 are comaximal. Set $A[x_1, \dots, x_{n-1}]_{S_i} = S_i^{-1}(A[x_1, \dots, x_{n-1}])$ for $i = 1, 2$. Let

$$\mathbf{H}_1 = \text{diag}(f_1, \dots, f_l) \cdot \mathbf{U} \cdot \text{diag}(f_1^{-1}, \dots, f_l^{-1}).$$

Then, $\det(\mathbf{H}_1) = \det(\mathbf{U})$ is a unit in $A[x_1, \dots, x_{n-1}]_{S_1}[x_n]$. Since $\mathbf{M} = \mathbf{F} \mathbf{U} \mathbf{G}$, we have $\mathbf{M} = \mathbf{H}_1 \mathbf{D}$. This implies that

$$\mathbf{M} \sim_{A[x_1, \dots, x_{n-1}]_{S_1}[x_n]} \mathbf{D}. \tag{6}$$

Since the specialization homomorphism $x_n \mapsto 0$ preserves the unimodularity of $\mathbf{U}$, the Smith normal form of $\mathbf{M}(x_1, \dots, x_{n-1}, 0) = \mathbf{F} \cdot \mathbf{U}(x_1, \dots, x_{n-1}, 0) \cdot \mathbf{G}$ is still $\mathbf{D}$. By the induction hypothesis, we get

$$\mathbf{M}(x_1, \dots, x_{n-1}, 0) \sim_{A[x_1, \dots, x_{n-1}]} \mathbf{D}. \quad (7)$$

Combining Equations (6) and (7), we have

$$\mathbf{M} \sim_{A[x_1, \dots, x_{n-1}]_{S_1}[x_n]} \mathbf{M}(x_1, \dots, x_{n-1}, 0). \quad (8)$$

Let

$$\mathbf{H}_2 = \text{diag}(g_1^{-1}, \dots, g_l^{-1}) \cdot \mathbf{U} \cdot \text{diag}(g_1, \dots, g_l).$$

Then, $\det(\mathbf{H}_2) = \det(\mathbf{U})$ is a unit in $A[x_1, \dots, x_{n-1}]_{S_2}[x_n]$. It follows from $\mathbf{M} = \mathbf{FUG}$ that $\mathbf{M} = \mathbf{DH}_2$. This implies that

$$\mathbf{M} \sim_{A[x_1, \dots, x_{n-1}]_{S_2}[x_n]} \mathbf{D}. \quad (9)$$

It follows from Equations (7) and (9) that

$$\mathbf{M} \sim_{A[x_1, \dots, x_{n-1}]_{S_2}[x_n]} \mathbf{M}(x_1, \dots, x_{n-1}, 0). \quad (10)$$

Since $\mathbf{S}_1$ and $\mathbf{S}_2$ are comaximal, by Theorem 2.15 we obtain

$$\mathbf{M} \sim_{A[x_1, \dots, x_{n-1}][x_n]} \mathbf{M}(x_1, \dots, x_{n-1}, 0). \quad (11)$$

Combining Equations (7) and (11), we get

$$\mathbf{M} \sim_R \mathbf{D}.$$

Therefore, the statement holds for n . □

The inductive proof of Theorem 4.3 gives rise to the following recursive procedure: starting from $(n, \mathbf{F}, \mathbf{U}, \mathbf{G})$, it sets $x_n = 0$, recursively processes the resulting matrix over $A[x_1, \dots, x_{n-1}]$, and then lifts the equivalence back via Vaserstein patching. We denote this procedure by

$$(\mathbf{P}, \mathbf{Q}) := \text{CoprimeMerge}_{l,A}(n, \mathbf{F}, \mathbf{U}, \mathbf{G}),$$

with $\mathbf{P}, \mathbf{Q} \in \text{GL}_l(R)$ and $\mathbf{P}(\mathbf{FUG})\mathbf{Q} = \mathbf{FG}$. A description of the steps is given in Appendix B.5.

Proof of Theorem 4.1. The necessity follows directly from Lemma 2.6. We now proceed to prove the sufficiency. If $\det(\mathbf{M})$ is a unit in A , then the result is trivial. Suppose that $\det(\mathbf{M}) = p_1^{t_1} \cdots p_k^{t_k}$, where $p_1, \dots, p_k \in A$ are pairwise coprime and irreducible. We employ induction on k to prove the statement.

If $k = 1$, then the statement holds by Theorem 3.1. Assuming the statement is true for $k - 1$, we now show it also holds for k . According to Lemma 4.2, there exist $\mathbf{M}_1, \mathbf{M}_2 \in R^{l \times l}$ such that $\mathbf{M} = \mathbf{M}_1 \mathbf{M}_2$, where $\det(\mathbf{M}_1) = p_1^{t_1}$ and $\det(\mathbf{M}_2) = p_2^{t_2} \cdots p_k^{t_k}$. It follows that $\gcd(\det(\mathbf{M}_1), \det(\mathbf{M}_2)) = 1$. Based on Lemma 2.7, we have $J_i(\mathbf{M}_1) = J_i(\mathbf{M}_2) = R$, where $i = 1, \dots, l$. Assume that the Smith normal forms of $\mathbf{M}_1$ and $\mathbf{M}_2$ are $\text{diag}(f_1, \dots, f_l)$ and

$\text{diag}(g_1, \dots, g_l)$, respectively, where $f_i \mid f_{i+1}$ and $g_i \mid g_{i+1}$ for $i = 1, \dots, l-1$. By the induction hypothesis, we get $\mathbf{M}_1 \sim \text{diag}(f_1, \dots, f_l)$ and $\mathbf{M}_2 \sim \text{diag}(g_1, \dots, g_l)$. Then there exist unimodular matrices $\mathbf{U}_1, \mathbf{V}_1, \mathbf{U}_2, \mathbf{V}_2 \in \text{GL}_l(R)$ such that $\mathbf{U}_1 \mathbf{M}_1 \mathbf{V}_1 = \text{diag}(f_1, \dots, f_l)$ and $\mathbf{U}_2 \mathbf{M}_2 \mathbf{V}_2 = \text{diag}(g_1, \dots, g_l)$. It follows from $\mathbf{M} = \mathbf{M}_1 \mathbf{M}_2$ that

$$\mathbf{M} = \mathbf{U}_1^{-1} \cdot \text{diag}(f_1, \dots, f_l) \cdot \mathbf{V}_1^{-1} \mathbf{U}_2^{-1} \cdot \text{diag}(g_1, \dots, g_l) \cdot \mathbf{V}_2^{-1}.$$

Since $\mathbf{V}_1^{-1} \mathbf{U}_2^{-1} \in \text{GL}_l(R)$, it follows from Theorem 4.3 that

$$\text{diag}(f_1, \dots, f_l) \cdot \mathbf{V}_1^{-1} \mathbf{U}_2^{-1} \cdot \text{diag}(g_1, \dots, g_l) \sim \text{diag}(f_1 g_1, \dots, f_l g_l).$$

Therefore, $\mathbf{M} \sim \text{diag}(f_1 g_1, \dots, f_l g_l)$. It follows that $\mathbf{M} \sim \text{SNF}(\mathbf{M})$. $\square$

4.2. Algorithm and example

Based on the proof of Theorem 4.1, we design the following algorithm to compute unimodular matrices $\mathbf{U}, \mathbf{V} \in \text{GL}_l(R)$ such that $\text{SNF}(\mathbf{M}) = \mathbf{U} \mathbf{M} \mathbf{V}$, where $\det(\mathbf{M}) = p_1^{t_1} \cdots p_k^{t_k}$.

Algorithm 2: SquareSmithForm($\mathbf{M}$)

Input : A matrix $\mathbf{M} \in R^{l \times l}$ such that $\det(\mathbf{M})$ is a nonzero element of A .

Output: Either “ $\mathbf{M}$ is not equivalent to its Smith normal form”, or $\mathbf{S} \in R^{l \times l}$ and $\mathbf{U}, \mathbf{V} \in \text{GL}_l(R)$ such that $\mathbf{S} = \text{SNF}(\mathbf{M})$ and $\mathbf{S} = \mathbf{U} \mathbf{M} \mathbf{V}$.

```

1 begin
2   compute  $\det(\mathbf{M})$ ;
3   if  $\det(\mathbf{M})$  is a unit in  $A$  then
4      $\mathbf{S} \leftarrow \mathbf{I}_l$ ,  $\mathbf{U} \leftarrow \mathbf{I}_l$ , and  $\mathbf{V} \leftarrow \mathbf{M}^{-1}$ ;
5     return  $\mathbf{S}, \mathbf{U}, \mathbf{V}$ ;
6   express  $\det(\mathbf{M})$  as  $p_1^{t_1} \cdots p_k^{t_k}$ , where  $p_1, \dots, p_k \in A$  are pairwise coprime and
   irreducible;
7   if  $k = 1$  then
8     return PrimePowerSmith( $\mathbf{M}$ ) by Algorithm 1;
9   for  $i = 1$  to  $l$  do
10    compute a Gröbner basis  $\mathcal{G}_i$  of  $J_i(\mathbf{M})$ ;
11    if  $1 \notin \mathcal{G}_i$  then
12      return “ $\mathbf{M}$  is not equivalent to its Smith normal form”;
13   $(\mathbf{M}_1, \mathbf{M}_2) \leftarrow \text{PrimeSplit}_{l,R}(\mathbf{M}, p_1^{t_1})$ ; // see Appendix B.4
14   $(\mathbf{S}_1, \mathbf{U}_1, \mathbf{V}_1) \leftarrow \text{PrimePowerSmith}(\mathbf{M}_1)$ ,  $(\mathbf{S}_2, \mathbf{U}_2, \mathbf{V}_2) \leftarrow \text{SquareSmithForm}(\mathbf{M}_2)$ ;
15   $\mathbf{T} \leftarrow \mathbf{V}_1^{-1} \mathbf{U}_2^{-1}$ ;
16   $(\mathbf{P}, \mathbf{Q}) \leftarrow \text{CoprimeMerge}_{l,A}(n, \mathbf{S}_1, \mathbf{T}, \mathbf{S}_2)$ ; // see Appendix B.5
17   $\mathbf{S} \leftarrow \mathbf{S}_1 \mathbf{S}_2$ ,  $\mathbf{U} \leftarrow \mathbf{P} \mathbf{U}_1$ , and  $\mathbf{V} \leftarrow \mathbf{V}_2 \mathbf{Q}$ ;
18  return  $\mathbf{S}, \mathbf{U}, \mathbf{V}$ .
```

Theorem 4.4. Algorithm 2 outputs as specified within a finite number of steps.

Proof. The correctness follows directly from Theorem 4.1. For termination, observe that Algorithm 2 invokes the Gröbner basis algorithm and Algorithm 1; the former terminates by [37], and the latter by Theorem 3.9. The subroutines called in Steps 13 and 16 rely on the same constructive procedures (the Quillen-Suslin algorithm, Suslin's stability algorithm, and Vaserstein patching) as those in Algorithm 1, all of which are known to terminate. Since Algorithm 2 comprises only finitely many calls to these terminating subroutines, together with elementary operations, it terminates in finitely many steps. $\square$

We now illustrate Algorithm 2 with an example.

Example 4.5. Let $A = \mathbb{Q}[y]$ and $R = A[x_1, x_2] = \mathbb{Q}[y, x_1, x_2]$. Consider the matrix

$$\mathbf{M} = \begin{pmatrix} 0 & y+1 & 0 \\ -y-x_1 & -(y+x_2)(y+x_1) & y^3+3y^2+x_1^2+5y+2 \\ 1 & 1+(2-x_2)y & y-x_1 \end{pmatrix}.$$

A direct computation gives $\det(\mathbf{M}) = (y+1)^3(y+2)$. By Definition 2.3, we compute the determinantal divisors of $\mathbf{M}$:

$$d_1(\mathbf{M}) = 1, \quad d_2(\mathbf{M}) = y+1, \quad d_3(\mathbf{M}) = \det(\mathbf{M}) = (y+1)^3(y+2).$$

Hence $\text{SNF}(\mathbf{M}) = \text{diag}(1, y+1, (y+1)^2(y+2))$. As shown by computation, the Gröbner basis of the ideal generated by the $i \times i$ reduced minors of $\mathbf{M}$ is $\{1\}$ for each $i = 1, 2, 3$. Hence

$$J_i(\mathbf{M}) = R, \quad i = 1, 2, 3.$$

Therefore, by Theorem 4.1, $\mathbf{M}$ is equivalent to its Smith normal form. We now apply Algorithm 2 to compute matrices $\mathbf{U}, \mathbf{V} \in \text{GL}_3(R)$ such that

$$\text{SNF}(\mathbf{M}) = \mathbf{U}\mathbf{M}\mathbf{V}.$$

Step 1. We first separate $(y+1)^3$ from $\det(\mathbf{M})$. Applying the splitting procedure in Lemma 4.2, namely $(\mathbf{M}_1, \mathbf{M}_2) := \text{PrimeSplit}_{3,R}(\mathbf{M}, (y+1)^3)$, we obtain $\mathbf{M} = \mathbf{M}_1\mathbf{M}_2$, where

$$\mathbf{M}_1 = \begin{pmatrix} y+1 & 0 & 0 \\ -(y+x_2)(y+x_1) & (y+1)^2 & -y-x_1 \\ 1+(2-x_2)y & 0 & 1 \end{pmatrix}, \quad \mathbf{M}_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & y+2 \\ 1 & 0 & y-x_1 \end{pmatrix}.$$

Moreover, $\det(\mathbf{M}_1) = (y+1)^3$ and $\det(\mathbf{M}_2) = y+2$.

Step 2. We reduce the two factors $\mathbf{M}_1, \mathbf{M}_2$ separately. By Example 3.10 we have

$$\mathbf{U}_1\mathbf{M}_1\mathbf{V}_1 = \mathbf{S}_1 \quad \text{and} \quad \mathbf{S}_1 = \text{diag}(1, y+1, (y+1)^2),$$

where

$$\mathbf{U}_1 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ (1-x_2)(x_1-1) & -1 & -y-x_1 \end{pmatrix}, \quad \mathbf{V}_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & x_2-1 & -1 \\ 1 & yx_2-2y-1 & 0 \end{pmatrix}.$$

For the second factor $\mathbf{M}_2$, we directly take

$$\mathbf{S}_2 = \text{diag}(1, 1, y+2), \quad \mathbf{U}_2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathbf{V}_2 = \begin{pmatrix} 1 & 0 & x_1 - y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then $\mathbf{U}_2 \mathbf{M}_2 \mathbf{V}_2 = \mathbf{S}_2$.

Step 3. Set $\mathbf{T} := \mathbf{V}_1^{-1} \mathbf{U}_2^{-1}$. Then

$$\mathbf{T} = \begin{pmatrix} 1 & -yx_2 + 2y + 1 & 0 \\ 0 & 1 & 0 \\ 0 & x_2 - 1 & -1 \end{pmatrix}.$$

Thus

$$\mathbf{S}_1 \mathbf{T} \mathbf{S}_2 = \begin{pmatrix} 1 & -yx_2 + 2y + 1 & 0 \\ 0 & y + 1 & 0 \\ 0 & (y+1)^2(x_2 - 1) & -(y+1)^2(y+2) \end{pmatrix}.$$

Applying the coprime merging procedure, we compute

$$(\mathbf{P}, \mathbf{Q}) := \text{CoprimeMerge}_{3,A}(2, \mathbf{S}_1, \mathbf{T}, \mathbf{S}_2),$$

where

$$\mathbf{P} = \begin{pmatrix} 1 & (y+1)yx_2 & 0 \\ 0 & 1 & 0 \\ 0 & (y+1)(y^2x_2 + 2yx_2 - y + x_2 - 3) & -1 \end{pmatrix}$$

and

$$\mathbf{Q} = \begin{pmatrix} 1 & -x_2y^3 - 2x_2y^2 - 2y - 1 & 0 \\ 0 & 1 & 0 \\ 0 & -yx_2 + 1 & 1 \end{pmatrix}.$$

Then

$$\mathbf{P}(\mathbf{S}_1 \mathbf{T} \mathbf{S}_2) \mathbf{Q} = \mathbf{S}_1 \mathbf{S}_2 = \text{diag}(1, y+1, (y+1)^2(y+2)).$$

Step 4. Combining the above steps, Algorithm 2 returns $\mathbf{U} = \mathbf{P} \mathbf{U}_1$ and $\mathbf{V} = \mathbf{V}_2 \mathbf{Q}$. A direct computation gives

$$\mathbf{U} = \begin{pmatrix} yx_2(y+1) & 0 & 1 \\ 1 & 0 & 0 \\ (y+1)(y^2x_2 + 2yx_2 - y + x_2 - 3) + (x_1 - 1)(x_2 - 1) & 1 & y + x_1 \end{pmatrix},$$

and

$$\mathbf{V} = \begin{pmatrix} 1 & -y^3x_2 - y^2x_2 - yx_1x_2 - 3y + x_1 - 1 & x_1 - y \\ 0 & 1 & 0 \\ 0 & -yx_2 + 1 & 1 \end{pmatrix}.$$

Therefore,

$$\mathbf{U} \mathbf{M} \mathbf{V} = \text{diag}(1, y+1, (y+1)^2(y+2)) = \text{SNF}(\mathbf{M}).$$

5. Equivalence of non-square and rank-deficient matrices

Based on the Quillen-Suslin theorem, we now extend Theorem 4.1 to the non-square and rank-deficient cases.

Theorem 5.1. *Let $\mathbf{M} \in R^{l \times m}$ with $\text{rank}(\mathbf{M}) = r$, and $d_r(\mathbf{M}) \in A$, where $1 \leq r \leq l$. Then $\mathbf{M} \sim \text{SNF}(\mathbf{M})$ if and only if $J_i(\mathbf{M}) = R$ for $i = 1, \dots, r$.*

Proof. The necessity follows directly from Lemma 2.6. We now proceed to prove the sufficiency. Since $J_r(\mathbf{M}) = R$, by Theorem 2.10 there exist $\mathbf{G}_1 \in R^{l \times r}$ and $\mathbf{F}_1 \in R^{r \times m}$ such that $\mathbf{M} = \mathbf{G}_1 \mathbf{F}_1$ and $\mathbf{F}_1$ is a ZLP matrix. According to the Quillen-Suslin theorem, there exists $\mathbf{Q}_1 \in \text{GL}_m(R)$ such that $\mathbf{F}_1 \cdot \mathbf{Q}_1 = (\mathbf{I}_r, \mathbf{0}_{r \times (m-r)})$. Therefore, we have

$$\mathbf{M} \cdot \mathbf{Q}_1 = \mathbf{G}_1 \cdot (\mathbf{I}_r, \mathbf{0}_{r \times (m-r)}) = (\mathbf{G}_1, \mathbf{0}_{l \times (m-r)}).$$

Based on Lemma 2.6, $J_r(\mathbf{G}_1) = J_r(\mathbf{M}) = R$. It follows from Theorem 2.12 that there exist $\mathbf{F}_2 \in R^{l \times r}$ and $\mathbf{G}_2 \in R^{r \times r}$ such that $\mathbf{G}_1 = \mathbf{F}_2 \mathbf{G}_2$ and $\mathbf{F}_2$ is a ZRP matrix. By the Quillen-Suslin theorem again, there exists $\mathbf{P}_1 \in \text{GL}_l(R)$ such that

$$\mathbf{P}_1 \cdot \mathbf{F}_2 = \begin{pmatrix} \mathbf{I}_r \\ \mathbf{0}_{(l-r) \times r} \end{pmatrix}.$$

Therefore,

$$\mathbf{P}_1 \cdot \mathbf{M} \cdot \mathbf{Q}_1 = (\mathbf{P}_1 \mathbf{F}_2 \mathbf{G}_2, \mathbf{0}_{l \times (m-r)}) = \begin{pmatrix} \mathbf{G}_2 & \mathbf{0}_{r \times (m-r)} \\ \mathbf{0}_{(l-r) \times r} & \mathbf{0}_{(l-r) \times (m-r)} \end{pmatrix}.$$

By Lemma 2.6, $d_r(\mathbf{G}_2) = d_r(\mathbf{M}) \in A$ and $J_i(\mathbf{G}_2) = J_i(\mathbf{M}) = R$ for $i = 1, \dots, r$. According to Theorem 4.1, there exist $\mathbf{P}_2, \mathbf{Q}_2 \in \text{GL}_r(R)$ such that $\mathbf{P}_2 \cdot \mathbf{G}_2 \cdot \mathbf{Q}_2 = \text{SNF}(\mathbf{G}_2)$. It follows that

$$\begin{pmatrix} \mathbf{P}_2 & \mathbf{0}_{r \times (l-r)} \\ \mathbf{0}_{(l-r) \times r} & \mathbf{I}_{(l-r)} \end{pmatrix} \mathbf{P}_1 \mathbf{M} \mathbf{Q}_1 \begin{pmatrix} \mathbf{Q}_2 & \mathbf{0}_{r \times (m-r)} \\ \mathbf{0}_{(m-r) \times r} & \mathbf{I}_{(m-r)} \end{pmatrix} = \begin{pmatrix} \text{SNF}(\mathbf{G}_2) & \mathbf{0}_{r \times (m-r)} \\ \mathbf{0}_{(l-r) \times r} & \mathbf{0}_{(l-r) \times (m-r)} \end{pmatrix}.$$

Therefore, $\mathbf{M} \sim \text{SNF}(\mathbf{M})$. □

Let $\mathbf{M} \in R^{l \times m}$ with $\text{rank}(\mathbf{M}) = r$, where $1 \leq r \leq l$. If $d_r(\mathbf{M}) \in A$, then by Theorem 5.1 we can design an algorithm to determine whether $\mathbf{M}$ is equivalent to its Smith normal form $\text{SNF}(\mathbf{M})$. Furthermore, if $\mathbf{M} \sim \text{SNF}(\mathbf{M})$, then the algorithm explicitly computes unimodular matrices $\mathbf{U} \in \text{GL}_l(R)$ and $\mathbf{V} \in \text{GL}_m(R)$ such that $\text{SNF}(\mathbf{M}) = \mathbf{U} \mathbf{M} \mathbf{V}$.

Theorem 5.2. *Algorithm 3 outputs as specified within a finite number of steps.*

Proof. The correctness follows directly from Theorem 5.1. For termination, compared with Algorithm 2, Algorithm 3 has additional Steps 7-10, which invoke the second Quillen-Suslin algorithm of [9] and are therefore terminating. The remaining operations (Gröbner basis computations, polynomial factorization, etc.) are also finite. Hence Algorithm 3 terminates in finitely many steps. □

Algorithm 3: SmithForm($\mathbf{M}$)

Input : A matrix $\mathbf{M} \in R^{l \times m}$ such that $d_r(\mathbf{M})$ is a nonzero element of A , where r is the rank of $\mathbf{M}$ with $1 \leq r \leq l$.

Output: Either “ $\mathbf{M}$ is not equivalent to its Smith normal form”, or $\mathbf{S} \in R^{l \times m}$, $\mathbf{U} \in \text{GL}_l(R)$, and $\mathbf{V} \in \text{GL}_m(R)$, such that $\mathbf{S} = \text{SNF}(\mathbf{M})$ and $\mathbf{S} = \mathbf{UMV}$.

```
1 begin
2   compute the rank of  $\mathbf{M}$  and set  $\text{rank}(\mathbf{M}) := r$ ;
3   for  $i = 1$  to  $r$  do
4     compute a Gröbner basis  $\mathcal{G}_i$  of  $J_i(\mathbf{M})$ ;
5     if  $1 \notin \mathcal{G}_i$  then
6       return “ $\mathbf{M}$  is not equivalent to its Smith normal form”;
7    $(\mathbf{G}_1, \mathbf{F}_1) \leftarrow \text{ZLPFact}_R(\mathbf{M}, r)$ ; // see Appendix A.3
8   compute  $\mathbf{Q}_1 \in \text{GL}_m(R)$  such that  $\mathbf{F}_1 \mathbf{Q}_1 = (\mathbf{I}_r, \mathbf{0}_{r \times (m-r)})$  by using the second
   Quillen-Suslin algorithm of Gago-Vargas [9];
9    $(\mathbf{G}_2^T, \mathbf{F}_2^T) \leftarrow \text{ZLPFact}_R(\mathbf{G}_1^T, r)$ ; // see Appendix A.3
10  compute  $\mathbf{P}_1 \in \text{GL}_l(R)$  such that  $\mathbf{P}_1 \mathbf{F}_2 = (\mathbf{I}_r, \mathbf{0}_{r \times (l-r)})^T$  by using the second
   Quillen-Suslin algorithm of Gago-Vargas [9];
11   $(\mathbf{S}_2, \mathbf{P}_2, \mathbf{Q}_2) \leftarrow \text{SquareSmithForm}(\mathbf{G}_2)$ ;
12   $\mathbf{S} \leftarrow \begin{pmatrix} \mathbf{S}_2 & \mathbf{0}_{r \times (m-r)} \\ \mathbf{0}_{(l-r) \times r} & \mathbf{0}_{(l-r) \times (m-r)} \end{pmatrix}$ ,  $\mathbf{U} \leftarrow \begin{pmatrix} \mathbf{P}_2 & \mathbf{0}_{r \times (l-r)} \\ \mathbf{0}_{(l-r) \times r} & \mathbf{I}_{(l-r)} \end{pmatrix} \mathbf{P}_1$ ,  $\mathbf{V} \leftarrow \mathbf{Q}_1 \begin{pmatrix} \mathbf{Q}_2 & \mathbf{0}_{r \times (m-r)} \\ \mathbf{0}_{(m-r) \times r} & \mathbf{I}_{(m-r)} \end{pmatrix}$ ;
13  return  $\mathbf{S}, \mathbf{U}, \mathbf{V}$ .
```

6. Concluding remarks

Let $\mathbf{M} \in A[x_1, \dots, x_n]^{l \times m}$ with rank r , and assume $d_r(\mathbf{M}) \in A$. In this paper, we have investigated the equivalence problem between such a matrix $\mathbf{M}$ and its Smith normal form. With the aid of the Quillen-Suslin theorem over $A[x_1, \dots, x_n]$ and the technique of localization, we prove that the Frost-Storey assertion holds true for this class of matrices: namely, $\mathbf{M}$ is equivalent to $\text{SNF}(\mathbf{M})$ if and only if all the $i \times i$ reduced minors of $\mathbf{M}$ generate the unit ideal $A[x_1, \dots, x_n]$ for every $i = 1, \dots, r$. This criterion extends and unifies several known results in the literature.

Since the proofs of our main theorems (Theorems 3.1, 4.1 and 5.1) are constructive, we have developed corresponding algorithms (Algorithms 1, 2 and 3) for computing unimodular matrices $\mathbf{U} \in \text{GL}_l(R)$ and $\mathbf{V} \in \text{GL}_m(R)$ such that $\text{SNF}(\mathbf{M}) = \mathbf{UMV}$. The effectiveness of these algorithms is demonstrated through two illustrative examples (Examples 3.10 and 4.5).

Compared with previous works, the present paper enlarges the class of multivariate polynomial matrices for which the equivalence to the Smith normal form is fully characterized. Nevertheless, the general equivalence problem still leaves many open questions. For instance, when $\mathbf{M}$ is a square matrix with $\det(\mathbf{M}) \in A[x_1]$ (i.e., depending on a single variable), does the Frost-Storey assertion remain valid? If not, what alternative criteria can be established?

We hope that the techniques developed herein will stimulate further investigations in this direction.

Acknowledgments

We are grateful to the anonymous referees for their constructive comments and suggestions, which have significantly improved the presentation of this paper. This research was supported by the Key Project of the National Natural Science Foundation of China under Grant No. 12494550&12494551, the National Natural Science Foundation of China under Grant No. 12201210, the Sichuan Science and Technology Program under Grant No. 2024NSFSC0418, and the STU Scientific Research Initiation under Grant No. NTF24023T.

References

- [1] B. Buchberger, Gröbner bases and systems theory, *Multidimensional systems and signal processing* 12 (2001) 223–251.
- [2] N. Bose, *Applied Multidimensional Systems Theory*, Second Edition, Springer, New York, 2017.
- [3] M. Frost, C. Storey, Equivalence of a matrix over $\mathbb{R}[s, z]$ with its Smith form, *International Journal of Control* 28 (1978) 665–671.
- [4] M. Frost, C. Storey, Equivalence of matrices over $\mathbb{R}[s, z]$: a counter-example, *International Journal of Control* 34 (1981) 1225–1226.
- [5] J. Serre, Faisceaux algébriques cohérents, *Annals of Mathematics* 61 (1955) 197–278.
- [6] D. Quillen, Projective modules over polynomial rings, *Inventiones Mathematicae* 36 (1976) 167–171.
- [7] A. Suslin, Projective modules over polynomial rings are free, *Soviet Mathematics-Doklady* 17 (1976) 1160–1164.
- [8] A. Logar, B. Sturmfels, Algorithms for the Quillen-Suslin theorem, *Journal of Algebra* 145 (1992) 231–239.
- [9] J. Gago-Vargas, Constructions in $R[x_1, \dots, x_n]$: applications to K-theory, *Journal of Pure and Applied Algebra* 171 (2002) 185–196.
- [10] A. Fabiańska, A. Quadrat, Applications of the Quillen-Suslin theorem to multidimensional systems theory, *Radon Series on Computational and Applied Mathematics* 3 (2007) 23–106.
- [11] Z. Lin, M. Boudelloua, L. Xu, On the equivalence and factorization of multivariate polynomial matrices, in: *Proceedings of ISCAS*, Kos, Greece, 2006, pp. 4911–4914.
- [12] J. Liu, D. Li, T. Wu, The Smith normal form and reduction of weakly linear matrices, *Journal of Symbolic Computation* 120 (2024) 1–14.
- [13] D. Li, R. Liang, J. Liu, Some further results on the Smith form of bivariate polynomial matrices, *Journal of System Science and Mathematical Sciences (Chinese Series)* 39 (2019) 1983–1997.
- [14] X. Zheng, D. Lu, D. Wang, F. Xiao, New results on the equivalence of bivariate polynomial matrices, *Journal of Systems Science and Complexity* 36 (2023) 77–95.
- [15] D. Lu, D. Wang, F. Xiao, X. Zheng, Equivalence and reduction of bivariate polynomial matrices to their Smith forms, *Journal of Symbolic Computation* 118 (2023) 1–16.
- [16] J. Guan, J. Liu, L. Zheng, T. Wu, J. Liu, New results on equivalence of multivariate polynomial matrices, *Journal of Systems Science and Complexity* 38 (2025) 1823–1832.
- [17] H. Smith, On systems of linear indeterminate equations and congruences, *Philosophical Transactions of the Royal Society of London* 151 (1861) 293–326.
- [18] S. Lang, *Algebra*, volume 211 of *Graduate Texts in Mathematics*, revised third ed., Springer, 2002.
- [19] D. Li, Z. Chen, J. Liu, Smith form of the matrix over the unique factorization domain (in Chinese), *Scientia Sinica Mathematica* 55 (2025) 919–926.
- [20] Z. Lin, On matrix fraction descriptions of multivariable linear n-D systems, *IEEE Transactions on Circuits and Systems* 35 (1988) 1317–1322.

- [21] G. Strang, *Linear Algebra and Its Applications*, Academic Press, New York, 2010.
- [22] D. Lu, D. Wang, F. Xiao, X. Zheng, Smith normal forms of bivariate polynomial matrices, *Linear Algebra and its Applications* 737 (2026) 308–330.
- [23] D. Youla, G. Gnani, Notes on n -dimensional system theory, *IEEE Transactions on Circuits and Systems* 26 (1979) 105–111.
- [24] Z. Lin, N. Bose, A generalization of Serre’s conjecture and some related issues, *Linear Algebra and Its Applications* 338 (2001) 125–138.
- [25] J. Pommaret, Solving Bose conjecture on linear multidimensional systems, in: *Proceedings of the 2001 European Control Conference*, 2001, pp. 1653–1655.
- [26] V. Srinivas, A generalized Serre problem, *Journal of Algebra* 278 (2004) 621–627.
- [27] M. Wang, D. Feng, On Lin-Bose problem, *Linear Algebra and its Applications* 390 (2004) 279–285.
- [28] J. Liu, D. Li, L. Zheng, The Lin-Bose problem, *IEEE Transactions on Circuits and Systems II: Express Briefs* 61 (2014) 41–43.
- [29] A. Suslin, On the structure of the special linear group over polynomial rings, *Mathematics of the USSR-Izvestiya* 11 (1977) 221–238.
- [30] C. Woodburn, An algorithm for Suslin’s stability theorem, Ph.D. thesis, USA, 1994.
- [31] G.-M. Greuel, G. Pfister, *A Singular Introduction to Commutative Algebra*, Second Extended Edition, Springer, New York, 2008.
- [32] S. Barhoumi, H. Lombardi, I. Yengui, Projective modules over polynomial rings: a constructive approach, *Mathematische Nachrichten* 282 (2009) 792–799.
- [33] I. Yengui, Constructive Commutative Algebra: Projective Modules over Polynomial Rings and Dynamical Gröbner Bases, volume 2138 of *Lecture Notes in Mathematics*, Springer, Berlin, 2015.
- [34] D. Cox, J. Little, D. O’Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics (Third Edition), Springer, New York, 2007.
- [35] R. Lubarsky, F. Richman, Zero sets of univariate polynomials, *Transactions of the American Mathematical Society* 362 (2010) 6619–6632.
- [36] J. Rotman, *An Introduction to Homological Algebra*, Academic Press, New York, 1979.
- [37] T. Becker, V. Weispfenning, *Gröbner Bases: A Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*, Springer-Verlag, 1993. In cooperation with Heinz Kredel.
- [38] M. Atiyah, I. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.
- [39] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*, Springer, 1995.
- [40] M. Wang, C. Kwong, On multivariate polynomial matrix factorization problems, *Mathematics of Control, Signals, and Systems* 17 (2005) 297–311.

Appendix A. ZLP matrix factorization theorem

In this appendix, we give a detailed proof of Theorem 2.10. Throughout, we retain the notation of Section 2; in particular, $R = A[x_1, \dots, x_n]$, where A is a PID, and hence R is a UFD.

Appendix A.1. Basic facts and auxiliary results

We first recall some basic facts that will be used in the proof.

Since A is a PID, it is Noetherian. By Hilbert’s basis theorem, R is Noetherian. Hence R^m is a Noetherian R -module, and every submodule of R^m is finitely generated. For more details, see Propositions 6.2 and 6.5, and Corollary 7.6 in [38].

Unless otherwise specified, let $\mathfrak{p}$ denote a maximal ideal of R . Since every maximal ideal is prime, the set $S = R \setminus \mathfrak{p}$ is a multiplicative subset of R . We denote the localization of R

at $\mathfrak{p}$ by $R_{\mathfrak{p}} := S^{-1}R$. The canonical localization map is

$$\begin{aligned} \varphi: R &\longrightarrow R_{\mathfrak{p}}, \\ h &\longmapsto \frac{h}{1}. \end{aligned}$$

Since R is a domain and $0 \notin S$, the map φ is injective. Thus, whenever no confusion can arise, we identify an element $h \in R$ with its image $\varphi(h) = h/1 \in R_{\mathfrak{p}}$. For an ideal $I \subseteq R$, its extension to $R_{\mathfrak{p}}$ is denoted by $IR_{\mathfrak{p}} = S^{-1}I$. In particular, $\mathfrak{p}R_{\mathfrak{p}} = S^{-1}\mathfrak{p}$ is the unique maximal ideal of $R_{\mathfrak{p}}$, so $R_{\mathfrak{p}}$ is a local ring. Moreover, since any localization of a UFD is again a UFD, $R_{\mathfrak{p}}$ is a local UFD; see, for example, Lang [18, Ch. II, p. 115, Ex. 5]. Because $R \subseteq R_{\mathfrak{p}} \subseteq \text{Frac}(R)$, we have $\text{Frac}(R_{\mathfrak{p}}) = \text{Frac}(R)$. Consequently, for any matrix $\mathbf{F} \in R_{\mathfrak{p}}^{l \times m}$, the rank $\text{rank}_{R_{\mathfrak{p}}}(\mathbf{F})$ can be computed by extending scalars from $R_{\mathfrak{p}}$ to $\text{Frac}(R)$. Hence we omit the subscript and simply write $\text{rank}(\mathbf{F})$.

Let $\mathcal{K}$ be an R -submodule of R^m . The rank of $\mathcal{K}$ over R is defined by

$$\text{rank}_R(\mathcal{K}) := \dim_{\text{Frac}(R)}(\text{Frac}(R) \otimes_R \mathcal{K});$$

see, for example, Eisenbud [39, Ch. 11.6, p. 265]. We write $\mathcal{K}_{\mathfrak{p}} := S^{-1}\mathcal{K} \subseteq R_{\mathfrak{p}}^m$ for its localization at $\mathfrak{p}$. Then the equality

$$\text{rank}_R(\mathcal{K}) = \text{rank}_{R_{\mathfrak{p}}}(\mathcal{K}_{\mathfrak{p}})$$

holds because $\text{Frac}(R) \otimes_{R_{\mathfrak{p}}} \mathcal{K}_{\mathfrak{p}} \cong \text{Frac}(R) \otimes_R \mathcal{K}$. In what follows, the rank of a submodule over R or $R_{\mathfrak{p}}$ is always understood in this sense.

For $d \in R \setminus \{0\}$, we write

$$\mathcal{K} : d := \{\vec{u} \in R^m \mid d\vec{u} \in \mathcal{K}\}.$$

After localization at $\mathfrak{p}$, the corresponding colon submodule is

$$\mathcal{K}_{\mathfrak{p}} : \frac{d}{1} := \left\{ \vec{v} \in R_{\mathfrak{p}}^m \mid \frac{d}{1}\vec{v} \in \mathcal{K}_{\mathfrak{p}} \right\}.$$

If $q \in R_{\mathfrak{p}}$ is associated to $d/1$ (i.e., $q = u \cdot (d/1)$ for some unit $u \in R_{\mathfrak{p}}$), then $\mathcal{K}_{\mathfrak{p}} : \frac{d}{1} = \mathcal{K}_{\mathfrak{p}} : q$. Indeed, multiplication by a unit does not affect membership in $\mathcal{K}_{\mathfrak{p}}$.

Let $\mathbf{M} \in R^{l \times m}$, and let $\mathbf{M}_{\mathfrak{p}} \in R_{\mathfrak{p}}^{l \times m}$ denote the image of $\mathbf{M}$ under the entry-wise extension of φ . We use $\rho(\mathbf{M})$ to denote the submodule of R^m generated by the rows of $\mathbf{M}$. The row module $\rho(\mathbf{M}_{\mathfrak{p}}) \subseteq R_{\mathfrak{p}}^m$ is always understood to be generated over $R_{\mathfrak{p}}$. With this convention, we have the natural identification $\rho(\mathbf{M}_{\mathfrak{p}}) = \rho(\mathbf{M})_{\mathfrak{p}}$.

We next record several auxiliary results that will be used in the sequel. The following results are direct specializations of Lemmas 3.4-3.6 (over an arbitrary UFD) and Theorem 3.1 (over a local UFD) in [28]. Since R is a UFD and $R_{\mathfrak{p}}$ is a local UFD, they apply in the present setting.

Lemma A.1. *Let $\mathbf{M} \in R^{l \times m}$ be of full row rank. If $\rho(\mathbf{M}) : d_l(\mathbf{M}) = \rho(\mathbf{M})$, then $d_l(\mathbf{M})$ is a unit in R .*

Lemma A.2. Let $\mathcal{K}$ be a submodule of R^m and let $d \in R \setminus \{0\}$. Then $\mathcal{K}_{\mathfrak{p}} : \frac{d}{1} = (\mathcal{K} : d)_{\mathfrak{p}}$.

Lemma A.3. Let $\mathbf{F} \in R_{\mathfrak{p}}^{l \times m}$ be of full row rank. Then for every $q \in R_{\mathfrak{p}} \setminus \{0\}$, we have $\rho(\mathbf{F}) : q \subseteq \rho(\mathbf{F}) : d_l(\mathbf{F})$.

Theorem A.4. Let $\mathbf{F} \in R_{\mathfrak{p}}^{l \times m}$ be of full row rank. If $J_l(\mathbf{F}) = R_{\mathfrak{p}}$, then $\rho(\mathbf{F}) : d_l(\mathbf{F})$ is a free $R_{\mathfrak{p}}$ -module of rank l .

To globalize the preceding local freeness result, we use the following standard local criterion for projectivity.

Lemma A.5 (Characterization of Projectives, Theorem 19.2 in [39]). Let $\mathcal{N}$ be a finitely generated module over the Noetherian ring R . The following statements are equivalent:

1. $\mathcal{N}$ is a projective R -module.
2. $\mathcal{N}_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$ -module for every maximal ideal $\mathfrak{p}$ of R .

Together with this local criterion, we shall use the module-theoretic form of the Quillen-Suslin theorem, which is equivalent to the matrix formulation given in Theorem 2.9.

Theorem A.6 (Quillen-Suslin theorem). Every finitely generated projective R -module is free.

Appendix A.2. Proof of Theorem 2.10

We now turn to the proof of Theorem 2.10. We begin with a lemma showing that, under suitable assumptions, the row module of a rank-deficient matrix over $R_{\mathfrak{p}}$ is generated by the rows of a full-row-rank submatrix.

Lemma A.7. Let $\mathbf{W} \in R_{\mathfrak{p}}^{l \times m}$ satisfy $\text{rank}(\mathbf{W}) = r$ and $d \mid d_r(\mathbf{W})$, where $1 \leq r \leq l$ and $d \in R_{\mathfrak{p}} \setminus \{0\}$. Let $\mathbf{B} \in R_{\mathfrak{p}}^{r \times m}$ be a submatrix consisting of r rows of $\mathbf{W}$, and suppose that $\mathbf{B}$ has an $r \times r$ minor $\Delta = ud$ for some unit $u \in R_{\mathfrak{p}}$. Then $\rho(\mathbf{W}) = \rho(\mathbf{B})$.

Proof. The inclusion $\rho(\mathbf{B}) \subseteq \rho(\mathbf{W})$ is clear. We prove the reverse inclusion.

Let $\vec{h}_1, \dots, \vec{h}_r \in R_{\mathfrak{p}}^m$ be the rows of $\mathbf{B}$. Since $\mathbf{B}$ has a nonzero $r \times r$ minor, the rows $\vec{h}_1, \dots, \vec{h}_r$ are linearly independent over $\text{Frac}(R_{\mathfrak{p}})$. Since $\text{rank}(\mathbf{W}) = r$, every row $\vec{w} \in R_{\mathfrak{p}}^m$ of $\mathbf{W}$ can be written uniquely in the form

$$\vec{w} = \lambda_1 \vec{h}_1 + \dots + \lambda_r \vec{h}_r, \quad (\text{A.1})$$

where $\lambda_1, \dots, \lambda_r \in \text{Frac}(R_{\mathfrak{p}})$. Let $\mathfrak{J}$ be the index set of columns corresponding to Δ , so that

$$\det(\mathbf{B}_{\mathfrak{J}}) = \Delta. \quad (\text{A.2})$$

Restricting Equation (A.1) to the columns in $\mathfrak{J}$, we obtain

$$\vec{w}_{\mathfrak{J}} = (\lambda_1, \dots, \lambda_r) \mathbf{B}_{\mathfrak{J}}. \quad (\text{A.3})$$

By Cramer's rule, we have

$$\lambda_i = \frac{\Delta_i}{\Delta}, \quad (\text{A.4})$$

where Δ_i is the determinant of the matrix obtained from $\mathbf{B}_J$ by replacing its i -th row by $\vec{w}_J$, and $i = 1, \dots, r$. Since $\vec{w}, \vec{h}_1, \dots, \vec{h}_r$ are rows of $\mathbf{W}$, each Δ_i is an $r \times r$ minor of $\mathbf{W}$. Since $d \mid d_r(\mathbf{W})$, we have $\Delta_i = dv_i$ for some $v_i \in R_{\mathfrak{p}}$, where $i = 1, \dots, r$. Then

$$\lambda_i = \frac{\Delta_i}{\Delta} = \frac{dv_i}{ud} = \frac{v_i}{u} \in R_{\mathfrak{p}}, \quad i = 1, \dots, r. \quad (\text{A.5})$$

Combining Equations (A.1) and (A.5), every row $\vec{w}$ of $\mathbf{W}$ belongs to $\rho(\mathbf{B})$. Therefore, $\rho(\mathbf{W}) \subseteq \rho(\mathbf{B})$. Combining the two inclusions gives $\rho(\mathbf{W}) = \rho(\mathbf{B})$. $\square$

Lemma A.7 is formulated over $R_{\mathfrak{p}}$. We now apply it to a matrix over R . More precisely, for a rank-deficient matrix over R , we show that one can choose a full-row-rank submatrix, formed by some of its rows, whose localization at $\mathfrak{p}$ satisfies the conclusion of Lemma A.7. This gives the following lemma.

Lemma A.8. *Let $\mathbf{M} \in R^{l \times m}$ satisfy $\text{rank}(\mathbf{M}) = r$ and $J_r(\mathbf{M}) = R$, where $1 \leq r \leq l$. Then for every maximal ideal $\mathfrak{p}$ of R , there exists a submatrix $\mathbf{C} \in R^{r \times m}$ consisting of r rows of $\mathbf{M}$ such that $\rho(\mathbf{C}_{\mathfrak{p}}) = \rho(\mathbf{M}_{\mathfrak{p}})$. Moreover, $d_r(\mathbf{C}_{\mathfrak{p}})$ is associated to $d_r(\mathbf{M}_{\mathfrak{p}})$ in $R_{\mathfrak{p}}$, and $J_r(\mathbf{C}_{\mathfrak{p}}) = R_{\mathfrak{p}}$.*

Proof. Let $a_1, \dots, a_{\eta} \in R$ be all the $r \times r$ minors of $\mathbf{M}$, and let $b_1, \dots, b_{\eta} \in R$ be the corresponding $r \times r$ reduced minors of $\mathbf{M}$, where $\eta = \binom{l}{r} \binom{m}{r}$. Thus $a_i = d_r(\mathbf{M}) \cdot b_i$ for $i = 1, \dots, \eta$. By assumption, $\langle b_1, \dots, b_{\eta} \rangle = R$. After localizing at $\mathfrak{p}$, we have

$$\frac{a_i}{1} = \frac{d_r(\mathbf{M})}{1} \cdot \frac{b_i}{1} \text{ for } i = 1, \dots, \eta, \text{ and } \left\langle \frac{b_1}{1}, \dots, \frac{b_{\eta}}{1} \right\rangle = R_{\mathfrak{p}}.$$

Then all $r \times r$ minors of $\mathbf{M}_{\mathfrak{p}}$ are $a_1/1, \dots, a_{\eta}/1$. Moreover, $d_r(\mathbf{M})/1$ is a gcd of these minors, up to multiplication by a unit in $R_{\mathfrak{p}}$. Equivalently, $d_r(\mathbf{M}_{\mathfrak{p}})$ is associated to $d_r(\mathbf{M})/1$ in $R_{\mathfrak{p}}$.

Since $R_{\mathfrak{p}}$ is a local ring with the unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$, every nonunit of $R_{\mathfrak{p}}$ belongs to $\mathfrak{p}R_{\mathfrak{p}}$. Hence at least one of the elements $b_1/1, \dots, b_{\eta}/1$ must be a unit in $R_{\mathfrak{p}}$. Therefore, there exists an index i_0 with $1 \leq i_0 \leq \eta$ such that $b_{i_0}/1$ is a unit in $R_{\mathfrak{p}}$. The corresponding $r \times r$ minor satisfies $a_{i_0}/1 = (d_r(\mathbf{M})/1) \cdot (b_{i_0}/1)$. Choose $\mathbf{C} \in R^{r \times m}$ to be the submatrix consisting of the r rows of $\mathbf{M}$ involved in the minor a_{i_0} . Then $\mathbf{C}_{\mathfrak{p}}$ has an $r \times r$ minor $(d_r(\mathbf{M})/1) \cdot (b_{i_0}/1)$. Since $d_r(\mathbf{M})/1$ divides all $r \times r$ minors of $\mathbf{M}_{\mathfrak{p}}$, by Lemma A.7 we have $\rho(\mathbf{M}_{\mathfrak{p}}) = \rho(\mathbf{C}_{\mathfrak{p}})$. Moreover, it is straightforward to verify that $d_r(\mathbf{C}_{\mathfrak{p}})$ is associated to $d_r(\mathbf{M}_{\mathfrak{p}})$ in $R_{\mathfrak{p}}$ and $J_r(\mathbf{C}_{\mathfrak{p}}) = R_{\mathfrak{p}}$. $\square$

Lemma A.8 now allows us to prove the first main step in the proof of Theorem 2.10.

Theorem A.9. *Let $\mathbf{M} \in R^{l \times m}$ satisfy $\text{rank}(\mathbf{M}) = r$ and $J_r(\mathbf{M}) = R$, where $1 \leq r \leq l$. Then $\rho(\mathbf{M}) : d_r(\mathbf{M})$ is a free R -module of rank r .*

Proof. Let $\mathfrak{p}$ be an arbitrary maximal ideal of R . According to Lemma A.8, there exists a submatrix $\mathbf{C} \in R^{r \times m}$ consisting of r rows of $\mathbf{M}$ such that $\rho(\mathbf{C}_{\mathfrak{p}}) = \rho(\mathbf{M}_{\mathfrak{p}})$. Moreover, $d_r(\mathbf{C}_{\mathfrak{p}})$ is associated to $d_r(\mathbf{M}_{\mathfrak{p}})$ in $R_{\mathfrak{p}}$, and $J_r(\mathbf{C}_{\mathfrak{p}}) = R_{\mathfrak{p}}$. By Theorem A.4, $\rho(\mathbf{C}_{\mathfrak{p}}) : d_r(\mathbf{C}_{\mathfrak{p}})$ is a free $R_{\mathfrak{p}}$ -module of rank r . Then

$$\rho(\mathbf{M}_{\mathfrak{p}}) : d_r(\mathbf{M}_{\mathfrak{p}}) = \rho(\mathbf{C}_{\mathfrak{p}}) : d_r(\mathbf{C}_{\mathfrak{p}}),$$

and it is a free $R_{\mathfrak{p}}$ -module of rank r . Since $d_r(\mathbf{M}_{\mathfrak{p}})$ is associated to $d_r(\mathbf{M})/1$, by Lemma A.2 we have

$$(\rho(\mathbf{M}) : d_r(\mathbf{M}))_{\mathfrak{p}} = \rho(\mathbf{M})_{\mathfrak{p}} : \frac{d_r(\mathbf{M})}{1} = \rho(\mathbf{M}_{\mathfrak{p}}) : d_r(\mathbf{M}_{\mathfrak{p}}).$$

Based on Lemma A.5 and the Quillen-Suslin theorem (Theorem A.6), $\rho(\mathbf{M}) : d_r(\mathbf{M})$ is a free R -module of rank r . $\square$

To proceed with the proof of Theorem 2.10, we need some further auxiliary lemmas. The following lemma provides a localization criterion for membership in a submodule.

Lemma A.10. *Let $\mathcal{N}$ be a submodule of R^m . Then for any vector $\vec{u} \in R^m$, one has $\vec{u} \in \mathcal{N}$ if and only if $\vec{u}/1 \in \mathcal{N}_{\mathfrak{p}}$ for every maximal ideal $\mathfrak{p}$ of R .*

Proof. Consider $\mathcal{W} = R^m/\mathcal{N}$, and let $\bar{u} = \vec{u} + \mathcal{N}$ denote the image of $\vec{u}$ in $\mathcal{W}$. Then $\vec{u} \in \mathcal{N}$ if and only if $\bar{u} = 0$ in $\mathcal{W}$. According to Proposition 3.8 in [38], $\bar{u} = 0$ in $\mathcal{W}$ if and only if $\bar{u}/1 = 0$ in $\mathcal{W}_{\mathfrak{p}}$ for every maximal ideal $\mathfrak{p}$ of R . Since localization is exact, there is a natural isomorphism

$$\mathcal{W}_{\mathfrak{p}} = (R^m/\mathcal{N})_{\mathfrak{p}} \cong (R_{\mathfrak{p}}^m)/\mathcal{N}_{\mathfrak{p}}.$$

Under this isomorphism, we have $\bar{u}/1 = 0$ in $\mathcal{W}_{\mathfrak{p}}$ if and only if $\vec{u}/1 \in \mathcal{N}_{\mathfrak{p}}$. Combining these equivalences gives

$$\vec{u} \in \mathcal{N} \Leftrightarrow \vec{u}/1 \in \mathcal{N}_{\mathfrak{p}} \text{ for every maximal ideal } \mathfrak{p} \subset R.$$

$\square$

Using Lemma A.10, we now establish a useful containment for colon submodules associated with matrices over R .

Lemma A.11. *Let $\mathbf{M} \in R^{l \times m}$ satisfy $\text{rank}(\mathbf{M}) = r$ and $J_r(\mathbf{M}) = R$, where $1 \leq r \leq l$. Then for every $h \in R \setminus \{0\}$, we have $\rho(\mathbf{M}) : h \subseteq \rho(\mathbf{M}) : d_r(\mathbf{M})$.*

Proof. Let $\vec{u} \in \rho(\mathbf{M}) : h$. Then $h\vec{u} \in \rho(\mathbf{M})$. For every maximal ideal $\mathfrak{p}$ of R , localizing $h\vec{u} \in \rho(\mathbf{M})$ gives

$$\frac{\vec{u}}{1} \in \rho(\mathbf{M})_{\mathfrak{p}} : \frac{h}{1}.$$

By Lemma A.8, there exists a submatrix $\mathbf{C} \in R^{r \times m}$ consisting of r rows of $\mathbf{M}$ such that $\rho(\mathbf{C}_{\mathfrak{p}}) = \rho(\mathbf{M}_{\mathfrak{p}})$ and $d_r(\mathbf{C}_{\mathfrak{p}})$ is associated to $d_r(\mathbf{M}_{\mathfrak{p}})$ in $R_{\mathfrak{p}}$. Then

$$\frac{\vec{u}}{1} \in \rho(\mathbf{C}_{\mathfrak{p}}) : \frac{h}{1}.$$

According to Lemma A.3, we have

$$\rho(\mathbf{C}_{\mathfrak{p}}) : \frac{h}{1} \subseteq \rho(\mathbf{C}_{\mathfrak{p}}) : d_r(\mathbf{C}_{\mathfrak{p}}) = \rho(\mathbf{M}_{\mathfrak{p}}) : d_r(\mathbf{M}_{\mathfrak{p}}).$$

Then $\vec{u}/1 \in (\rho(\mathbf{M}) : d_r(\mathbf{M}))_{\mathfrak{p}}$ for every maximal ideal $\mathfrak{p}$. It follows from Lemma A.10 that $\vec{u} \in \rho(\mathbf{M}) : d_r(\mathbf{M})$. Therefore, $\rho(\mathbf{M}) : h \subseteq \rho(\mathbf{M}) : d_r(\mathbf{M})$. $\square$

The next lemma concerns a basic property of greatest common divisors in R .

Lemma A.12. *Let $\{f_1, \dots, f_s\}$ and $\{g_1, \dots, g_t\}$ be two finite subsets of R , each containing at least one nonzero element. Then $\gcd(f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq t)$ is associated to $\gcd(f_1, \dots, f_s) \cdot \gcd(g_1, \dots, g_t)$ in R .*

Proof. Let $f = \gcd(f_1, \dots, f_s)$ and $g = \gcd(g_1, \dots, g_t)$. It is enough to compare the exponent of each irreducible element of R in $\gcd(f_i g_j \mid i, j)$ and fg . Let π be an irreducible element of R . For any nonzero $h \in R$, set

$$\mu_{\pi}(h) := \max\{e \in \mathbb{Z}_{\geq 0} \mid \pi^e \text{ divides } h\}.$$

Here, we adopt the convention that $\mu_{\pi}(0) = +\infty$. Then

$$\mu_{\pi}(f) = \min_{1 \leq i \leq s} \{\mu_{\pi}(f_i)\} \text{ and } \mu_{\pi}(g) = \min_{1 \leq j \leq t} \{\mu_{\pi}(g_j)\}.$$

By assumption, $\mu_{\pi}(f), \mu_{\pi}(g)$ are finite. Clearly, for each i, j we have

$$\mu_{\pi}(f_i g_j) = \mu_{\pi}(f_i) + \mu_{\pi}(g_j).$$

Therefore,

$$\begin{aligned} \mu_{\pi}(\gcd(f_i g_j \mid i, j)) &= \min_{i,j} \{\mu_{\pi}(f_i) + \mu_{\pi}(g_j)\} \\ &= \min_i \{\mu_{\pi}(f_i)\} + \min_j \{\mu_{\pi}(g_j)\} \\ &= \mu_{\pi}(f) + \mu_{\pi}(g) \\ &= \mu_{\pi}(fg). \end{aligned}$$

Since this holds for every irreducible element $\pi \in R$, $\gcd(f_i g_j \mid i, j)$ is associated to fg . $\square$

Having established the necessary auxiliary lemmas, we now give the full proof of Theorem 2.10. To keep this appendix self-contained, we restate Theorem 2.10 as the following theorem.

Theorem A.13. *Let $\mathbf{M} \in R^{l \times m}$ with $\text{rank}(\mathbf{M}) = r$, where $1 \leq r \leq l$. If $J_r(\mathbf{M}) = R$, then there exist $\mathbf{G}_1 \in R^{l \times r}$ and $\mathbf{F}_1 \in R^{r \times m}$ such that $\mathbf{M} = \mathbf{G}_1 \mathbf{F}_1$, where $d_r(\mathbf{G}_1) = d_r(\mathbf{M})$ and $\mathbf{F}_1$ is a ZLP matrix.*

Proof. By Theorem A.9, $\rho(\mathbf{M}) : d_r(\mathbf{M})$ is a free R -module of rank r . Choose a free basis $\{\vec{u}_1, \dots, \vec{u}_r\} \subseteq R^m$ of $\rho(\mathbf{M}) : d_r(\mathbf{M})$, and let $\mathbf{F}'_1 \in R^{r \times m}$ be the matrix whose rows are $\vec{u}_1, \dots, \vec{u}_r$. Then

$$\rho(\mathbf{F}'_1) = \rho(\mathbf{M}) : d_r(\mathbf{M}).$$

Because $\rho(\mathbf{F}'_1) : d_r(\mathbf{F}'_1) = (\rho(\mathbf{M}) : d_r(\mathbf{M})) : d_r(\mathbf{F}'_1)$, by Lemma A.11 we have

$$\rho(\mathbf{F}'_1) : d_r(\mathbf{F}'_1) \subseteq \rho(\mathbf{M}) : d_r(\mathbf{M}) = \rho(\mathbf{F}'_1).$$

Clearly, $\rho(\mathbf{F}'_1) \subseteq \rho(\mathbf{F}'_1) : d_r(\mathbf{F}'_1)$. Therefore,

$$\rho(\mathbf{F}'_1) = \rho(\mathbf{F}'_1) : d_r(\mathbf{F}'_1).$$

According to Lemma A.1, $d_r(\mathbf{F}'_1)$ is a unit in R .

Since $\rho(\mathbf{M}) \subseteq \rho(\mathbf{M}) : d_r(\mathbf{M})$, there exists $\mathbf{G}'_1 \in R^{l \times r}$ such that

$$\mathbf{M} = \mathbf{G}'_1 \mathbf{F}'_1.$$

Let $f_1, \dots, f_s \in R$ be all $r \times r$ minors of $\mathbf{F}'_1$, and $g_1, \dots, g_t \in R$ be all $r \times r$ minors of $\mathbf{G}'_1$, where $s = \binom{m}{r}$ and $t = \binom{l}{r}$. According to the Cauchy-Binet formula,

$$\{f_i g_j \mid 1 \leq i \leq s, 1 \leq j \leq t\}$$

are all $r \times r$ minors of $\mathbf{M}$. Based on Lemma A.12, $d_r(\mathbf{M})$ is associated to $d_r(\mathbf{G}'_1) \cdot d_r(\mathbf{F}'_1)$ in R . Since $d_r(\mathbf{F}'_1)$ is a unit in R , there exists a unit $\alpha \in R$ such that $d_r(\mathbf{M}) = \alpha \cdot d_r(\mathbf{G}'_1)$. Then

$$\left\{ f_i \cdot \frac{g_j}{d_r(\mathbf{M})} \mid 1 \leq i \leq s, 1 \leq j \leq t \right\}$$

are all $r \times r$ reduced minors of $\mathbf{M}$. Since $J_r(\mathbf{M}) = R$, we have

$$R = \left\langle f_i \cdot \frac{g_j}{d_r(\mathbf{M})} \mid 1 \leq i \leq s, 1 \leq j \leq t \right\rangle \subseteq \langle f_1, \dots, f_s \rangle.$$

Therefore, $\mathbf{F}'_1$ is a ZLP matrix. Let $\mathbf{\Lambda} = \text{diag}(1, \dots, 1, \alpha) \in R^{r \times r}$. Then $\mathbf{\Lambda} \in \text{GL}_r(R)$. Set

$$\mathbf{G}_1 = \mathbf{G}'_1 \mathbf{\Lambda} \text{ and } \mathbf{F}_1 = \mathbf{\Lambda}^{-1} \mathbf{F}'_1.$$

Then $\mathbf{M} = \mathbf{G}_1 \mathbf{F}_1$, where $d_r(\mathbf{G}_1) = d_r(\mathbf{M})$ and $\mathbf{F}_1$ is a ZLP matrix. □

Appendix A.3. ZLP Algorithm

The constructive proof of Theorem A.13 gives the following procedure, denoted by ZLPFact_R .

$$(\mathbf{G}_1, \mathbf{F}_1) := \text{ZLPFact}_R(\mathbf{M}, r)$$

Input: A matrix $\mathbf{M} \in R^{l \times m}$ with $\text{rank}(\mathbf{M}) = r$ and $J_r(\mathbf{M}) = R$, where $1 \leq r \leq l$.

Output: A pair $(\mathbf{G}_1, \mathbf{F}_1) \in R^{l \times r} \times R^{r \times m}$ such that $\mathbf{M} = \mathbf{G}_1 \mathbf{F}_1$ and $\mathbf{F}_1$ is ZLP.

Step 1. Compute $d = d_r(\mathbf{M})$.

Step 2. Compute a generating set $\{(\mathbf{a}_i, \mathbf{b}_i) \in R^{1 \times l} \times R^{1 \times m} \mid i = 1, \dots, s\}$ of the row syzygy module

$$\text{Syz}_R \left(\begin{pmatrix} \mathbf{M} \\ -d \cdot \mathbf{I}_m \end{pmatrix} \right).$$

Let $\mathcal{N} \subseteq R^{1 \times m}$ be the submodule generated by $\mathbf{b}_1, \dots, \mathbf{b}_s$. Then $\mathcal{N} = \rho(\mathbf{M}) : d$. By Theorem A.9, $\mathcal{N}$ is a free R -module of rank r .

Step 3. Compute a free basis $\mathbf{f}_1, \dots, \mathbf{f}_r$ of $\mathcal{N}$ by using the second Quillen-Suslin algorithm of Gago-Vargas [9] (which computes free bases of finitely generated projective modules over polynomial rings over a PID). Let $\mathbf{F}_1$ be the matrix whose rows are $\mathbf{f}_1, \dots, \mathbf{f}_r$.

Step 4. Choose r columns of $\mathbf{F}_1$ that are linearly independent over $\text{Frac}(R)$, and let $\mathbf{H}$ be the $r \times r$ matrix formed by these columns. Let $\mathbf{M}_0$ denote the corresponding columns of $\mathbf{M}$, and compute $\mathbf{G}_1 := \mathbf{M}_0 \mathbf{H}^{-1}$. Since $\rho(\mathbf{M}) \subseteq \rho(\mathbf{F}_1)$, we have $\mathbf{G}_1 \in R^{l \times r}$ and $\mathbf{M} = \mathbf{G}_1 \mathbf{F}_1$. Return $(\mathbf{G}_1, \mathbf{F}_1)$.

Remark A.14. In Step 2, the equality $\mathcal{N} = \rho(\mathbf{M}) : d$ follows directly from the projection of the syzygy module onto its last m coordinates: $\mathbf{b} \in \rho(\mathbf{M}) : d$ if and only if there exists $\mathbf{a} \in R^{1 \times l}$ such that $\mathbf{a}\mathbf{M} - d\mathbf{b} = \mathbf{0}$, i.e., $(\mathbf{a}, \mathbf{b})$ is a syzygy of $\begin{pmatrix} \mathbf{M} \\ -d \cdot \mathbf{I}_m \end{pmatrix}$. This projection is valid for any rank r , without requiring $\mathbf{M}$ to be full row rank. We emphasize that Lemma 1 in [40] states a stronger one-to-one correspondence and allows the inverse reconstruction of syzygy generators from a generating set of the colon module; that stronger assertion relies crucially on the full row rank assumption and is not employed in our algorithm. Our Step 2 only uses the forward projection, which holds unconditionally.

Appendix B. Procedures

This appendix collects the procedures corresponding to several key conclusions in the main text. These auxiliary procedures are intended to facilitate understanding of the computational details of the primary algorithms (Algorithms 1 and 2).

Appendix B.1. Procedure PrimeSmith_{2,R} derived from Lemma 3.3

$(\mathbf{U}, \mathbf{V}) := \text{PrimeSmith}_{2,R}(\mathbf{M}, p_1)$

Input: A pair $(\mathbf{M}, p_1)$, where $\mathbf{M} \in R^{2 \times 2}$, $p_1 \in A$ is irreducible, $\det(\mathbf{M}) = p_1$ and $J_1(\mathbf{M}) = R$.

Output: A pair $(\mathbf{U}, \mathbf{V}) \in \text{GL}_2(R)^2$ such that $\mathbf{U}\mathbf{M}\mathbf{V} = \text{diag}(1, p_1)$.

Step 1. If $n = 0$, then compute $(\mathbf{U}, \mathbf{V}) \in \text{GL}_2(A)^2$ such that $\mathbf{U}\mathbf{M}\mathbf{V} = \text{diag}(1, p_1)$ by the standard Smith reduction over the PID A , and return $(\mathbf{U}, \mathbf{V})$.

Step 2. Assume $n > 0$, set $\bar{R} := (A/\langle p_1 \rangle)[x_1, \dots, x_n]$ and $\bar{\mathbf{M}} := \mathbf{M} \pmod{p_1}$. Compute $(\bar{\mathbf{H}}^T, \bar{\mathbf{G}}^T) := \text{ZLPFact}_{\bar{R}}(\bar{\mathbf{M}}^T, 1)$. Then $\bar{\mathbf{M}} = \bar{\mathbf{G}} \cdot \bar{\mathbf{H}}$ and $\bar{\mathbf{G}} \in \bar{R}^{2 \times 1}$ is ZRP. There exist $g_1, g_2, h_1, h_2 \in R$ and $\mathbf{Q} \in R^{2 \times 2}$ such that

$$\mathbf{M} = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix} \begin{pmatrix} h_1 & h_2 \end{pmatrix} + p_1 \mathbf{Q}.$$

Terms in g_1, g_2 whose coefficients are divisible by p_1 are absorbed into $p_1 \mathbf{Q}$. If one of g_1, g_2 is zero, extract p_1 from the corresponding row and return the resulting transformation matrices.

Step 3. Let $d = \max\{\text{tdeg}(g_1), \text{tdeg}(g_2)\} + 1$. Apply the automorphism $\omega : R \rightarrow R$ defined by $\omega(x_i) = x_i + x_n^{d^{n-i}}$ for $i = 1, \dots, n-1$, and $\omega(x_n) = x_n$. Set $\mathbf{M}' := \omega(\mathbf{M})$ and $\mathbf{Q}' := \omega(\mathbf{Q})$, $g'_j := \omega(g_j)$ and $h'_j := \omega(h_j)$ for $j = 1, 2$. Set $R' := A[x_1, \dots, x_{n-1}]$, and define

$$g_0 = \begin{cases} g'_1, & \text{if } \deg_{x_n}(g'_1) = \deg_{x_n}(g'_2) = 0; \\ \text{res}_{x_n}(g'_1, g'_2), & \text{otherwise.} \end{cases}$$

Then $g_0 \in R'$ and $\langle p_1, g_0 \rangle = R'$. Compute $u, v \in R$ such that $ug'_1 + vg'_2 = g_0$, where u, v are obtained from the Bézout identity for the resultant.

Step 4. Set $S_1 := \{g_0^{\theta_1} \mid \theta_1 \in \mathbb{N}\}$, $S_2 := \{p_1^{\theta_2} \mid \theta_2 \in \mathbb{N}\}$, and $R'_{S_i} := S_i^{-1}R'$ for $i = 1, 2$. Let

$$\mathbf{D} := \text{diag}(1, p_1) \text{ and } \mathbf{X} := \begin{pmatrix} u & v \\ -g'_2 & g'_1 \end{pmatrix}.$$

Then $\det(\mathbf{X}) = g_0$. Compute $\mathbf{W}_1$ from $\mathbf{X}\mathbf{M}' = \mathbf{D}\mathbf{W}_1$, equivalently by dividing the second row of $\mathbf{X}\mathbf{M}'$ by p_1 . Over $R'_{S_1}[x_n]$, set $\mathbf{L}_1 := \mathbf{X}$ and $\mathbf{R}_1 := \mathbf{W}_1^{-1}$. Then $\mathbf{L}_1\mathbf{M}'\mathbf{R}_1 = \mathbf{D}$. Over $R'_{S_2}[x_n]$, set $\mathbf{W}_2 := \text{diag}(1, p_1^{-1})\mathbf{M}'$, $\mathbf{L}_2 := \mathbf{I}_2$ and $\mathbf{R}_2 := \mathbf{W}_2^{-1}$. Since $\det(\mathbf{W}_2) = 1$, we have $\mathbf{L}_2\mathbf{M}'\mathbf{R}_2 = \mathbf{D}$.

Step 5. Set $\mathbf{M}'_0 := \mathbf{M}'(x_1, \dots, x_{n-1}, 0)$. Since $\det(\mathbf{M}'_0) = p_1$ and $J_1(\mathbf{M}'_0) = R'$, recursively compute $(\mathbf{U}_0, \mathbf{V}_0) := \text{PrimeSmith}_{2, R'}(\mathbf{M}'_0, p_1)$. Thus $\mathbf{U}_0, \mathbf{V}_0 \in \text{GL}_2(R')$ and $\mathbf{U}_0\mathbf{M}'_0\mathbf{V}_0 = \mathbf{D}$. Combining this equality with *Step 4*, we obtain

$$(\mathbf{U}_0^{-1}\mathbf{L}_i)\mathbf{M}'(\mathbf{R}_i\mathbf{V}_0^{-1}) = \mathbf{M}'_0 \text{ over } R'_{S_i}[x_n] \text{ for } i = 1, 2.$$

Step 6. Since S_1 and S_2 are comaximal, Vaserstein patching [32, 33] applied to the equivalences in *Step 5* returns $\mathbf{U}_1, \mathbf{V}_1 \in \text{GL}_2(R'[x_n])$ such that $\mathbf{U}_1\mathbf{M}'\mathbf{V}_1 = \mathbf{M}'_0$.

Step 7. Composing *Step 6* with $\mathbf{U}_0\mathbf{M}'_0\mathbf{V}_0 = \mathbf{D}$, we get $(\mathbf{U}_0\mathbf{U}_1)\mathbf{M}'(\mathbf{V}_1\mathbf{V}_0) = \mathbf{D}$.

Step 8. Set $\mathbf{U} := \omega^{-1}(\mathbf{U}_0\mathbf{U}_1)$ and $\mathbf{V} := \omega^{-1}(\mathbf{V}_1\mathbf{V}_0)$. Then $\mathbf{U}, \mathbf{V} \in \text{GL}_2(R)$ and $\mathbf{U}\mathbf{M}\mathbf{V} = \text{diag}(1, p_1)$. Return $(\mathbf{U}, \mathbf{V})$.

Appendix B.2. Procedure $\text{DiagExtract}_{l,R}$ derived from Theorem 3.6

$(\mathbf{U}, \mathbf{G}) := \text{DiagExtract}_{l,R}(\mathbf{M}, p_1, r)$

Input: A triple $(\mathbf{M}, p_1, r)$, where $\mathbf{M} \in R^{l \times l}$, $p_1 \in A$ is irreducible, $0 \leq r \leq l - 1$, $\text{rank}(\overline{\mathbf{M}}) = r$ and $J_r(\mathbf{M}) = R$.

Output: A pair $(\mathbf{U}, \mathbf{G}) \in \text{GL}_l(R) \times R^{l \times l}$, such that $\mathbf{U}\mathbf{M} = \text{diag}(\underbrace{1, \dots, 1}_r, p_1, \dots, p_1) \cdot \mathbf{G}$.

Step 1. If $r = 0$, then $\overline{\mathbf{M}} = 0$. Hence all entries of $\mathbf{M}$ are divisible by p_1 . Set $\mathbf{U} := \mathbf{I}_l$ and $\mathbf{G} := p_1^{-1}\mathbf{M}$. Return $(\mathbf{U}, \mathbf{G})$.

Step 2. If $l = 2$ and $r = 1$, set $\mathbf{N} := (\mathbf{M}, p_1 \mathbf{I}_2)$. Compute $(\mathbf{G}_1, \mathbf{F}) := \text{ZLPFact}_R(\mathbf{N}, 2)$. Set $(\mathbf{F}_1, \mathbf{F}_2) := \mathbf{F}$, where $\mathbf{F}_1 \in R^{2 \times 2}$. Then $\mathbf{M} = \mathbf{G}_1 \mathbf{F}_1$ and $\det(\mathbf{G}_1) = p_1$. Compute $(\mathbf{P}, \mathbf{Q}) := \text{PrimeSmith}_{2,R}(\mathbf{G}_1, p_1)$, so that $\mathbf{P}\mathbf{G}_1\mathbf{Q} = \text{diag}(1, p_1)$. Return $(\mathbf{P}, \mathbf{Q}^{-1}\mathbf{F}_1)$.

Step 3. Assume $l > 2$ and $r > 0$. Set $\overline{R} := (A/\langle p_1 \rangle)[x_1, \dots, x_n]$. Compute $(\overline{\mathbf{H}}^T, \overline{\mathbf{F}}^T) := \text{ZLPFact}_{\overline{R}}(\overline{\mathbf{M}}^T, r)$. Then $\overline{\mathbf{M}} = \overline{\mathbf{F}}\overline{\mathbf{H}}$ and $\overline{\mathbf{F}} \in \overline{R}^{l \times r}$ is ZRP. Use the second Quillen-Suslin algorithm of Gago-Vargas [9] to compute $\overline{\mathbf{P}} \in \text{SL}_l(\overline{R})$ such that

$$\overline{\mathbf{P}}\overline{\mathbf{F}} = \begin{pmatrix} \overline{\mathbf{I}}_r \\ \mathbf{0}_{(l-r) \times r} \end{pmatrix}.$$

Step 4. Decompose $\overline{\mathbf{P}}$ into elementary matrices by Suslin's stability algorithm [30], lift them to R , and let their product be $\mathbf{U} \in \text{GL}_l(R)$. Then

$$\mathbf{U}\mathbf{M} \equiv \begin{pmatrix} \mathbf{H} \\ \mathbf{0}_{(l-r) \times l} \end{pmatrix} \pmod{p_1}.$$

Hence the last $l - r$ rows of $\mathbf{U}\mathbf{M}$ are divisible by p_1 . Let $\mathbf{G}$ be obtained from $\mathbf{U}\mathbf{M}$ by dividing these last $l - r$ rows by p_1 . Return $(\mathbf{U}, \mathbf{G})$.

Appendix B.3. Procedure $\text{DiagMerge}_{l,R}$ derived from Theorem 3.8

$(\mathbf{L}, \mathbf{R}) := \text{DiagMerge}_{l,R}(\mathbf{W}, \mathbf{U}, p_1, r, s_1, \dots, s_r, s)$

Input: $(\mathbf{W}, \mathbf{U}, p_1, r, s_1, \dots, s_r, s)$ satisfying the hypotheses of Theorem 3.8, where $\mathbf{W} \in R^{l \times l}$, $\mathbf{U} \in \text{GL}_l(R)$, $p_1 \in A$ is irreducible, and

$$\mathbf{W} = \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^s, \dots, p_1^s) \cdot \mathbf{U} \cdot \text{diag}(\underbrace{1, \dots, 1}_r, p_1, \dots, p_1).$$

Output: A pair $(\mathbf{L}, \mathbf{R}) \in \text{GL}_l(R)^2$ such that $\mathbf{L}\mathbf{W}\mathbf{R} = \text{diag}(p_1^{s_1}, \dots, p_1^{s_r}, p_1^{s+1}, \dots, p_1^{s+1})$.

Step 1. Set $r_0 := \#\{i \in \{1, \dots, r\} \mid s_i < s\}$, where $\#$ denotes the number of elements in a set. If $r_0 = 0$, return $(\mathbf{U}^{-1}, \mathbf{I}_l)$.

Step 2. Partition

$$\mathbf{U} = \begin{pmatrix} \mathbf{U}_1 & \mathbf{U}_2 \\ \mathbf{U}_3 & \mathbf{U}_4 \end{pmatrix},$$

where $\mathbf{U}_1 \in R^{r_0 \times r}$, $\mathbf{U}_2 \in R^{r_0 \times (l-r)}$, $\mathbf{U}_3 \in R^{(l-r_0) \times r}$ and $\mathbf{U}_4 \in R^{(l-r_0) \times (l-r)}$. Compute $\mathbf{P} \in \text{GL}_l(R)$ such that $(\mathbf{U}_1, p_1 \mathbf{U}_2) \mathbf{P} = (\mathbf{I}_{r_0}, \mathbf{0}_{r_0 \times (l-r_0)})$ by using the second Quillen-Suslin algorithm of Gago-Vargas [9].

Step 3. Write $(\mathbf{V}_1, \mathbf{V}_2) := (\mathbf{U}_3, p_1 \mathbf{U}_4) \mathbf{P}$, where $\mathbf{V}_1 \in R^{(l-r_0) \times r_0}$ and $\mathbf{V}_2 \in R^{(l-r_0) \times (l-r_0)}$. Set

$$\mathbf{Q}_1 := \begin{pmatrix} \mathbf{I}_{r_0} & \mathbf{0}_{r_0 \times (l-r_0)} \\ -\mathbf{V}_1 \text{diag}(p_1^{s-s_1}, \dots, p_1^{s-s_{r_0}}) & \mathbf{I}_{(l-r_0)} \end{pmatrix}.$$

Then

$$\mathbf{Q}_1 \mathbf{W} \mathbf{P} = \begin{pmatrix} \text{diag}(p_1^{s_1}, \dots, p_1^{s_{r_0}}) & \mathbf{0}_{r_0 \times (l-r_0)} \\ \mathbf{0}_{(l-r_0) \times r_0} & p_1^s \mathbf{V}_2 \end{pmatrix}.$$

Step 4. Set $k := r - r_0$, and compute

$$(\mathbf{Q}_2, \mathbf{G}'') := \text{DiagExtract}_{l-r_0, R}(\mathbf{V}_2, p_1, k),$$

so that $\mathbf{Q}_2 \mathbf{V}_2 = \text{diag}(\underbrace{1, \dots, 1}_k, p_1, \dots, p_1) \mathbf{G}''$, where $\mathbf{Q}_2, \mathbf{G}'' \in \text{GL}_{l-r_0}(R)$. Set

$$\mathbf{L} := \begin{pmatrix} \mathbf{I}_{r_0} & \mathbf{0}_{r_0 \times (l-r_0)} \\ \mathbf{0}_{(l-r_0) \times r_0} & \mathbf{Q}_2 \end{pmatrix} \mathbf{Q}_1 \text{ and } \mathbf{R} := \mathbf{P} \begin{pmatrix} \mathbf{I}_{r_0} & \mathbf{0}_{r_0 \times (l-r_0)} \\ \mathbf{0}_{(l-r_0) \times r_0} & (\mathbf{G}'')^{-1} \end{pmatrix}.$$

Return $(\mathbf{L}, \mathbf{R})$.

Appendix B.4. Procedure PrimeSplit_{l,R} derived from Lemma 4.2

$$(\mathbf{M}_1, \mathbf{M}_2) := \text{PrimeSplit}_{l,R}(\mathbf{M}, p_1^{t_1})$$

Input: A matrix $\mathbf{M} \in R^{l \times l}$ with $\det(\mathbf{M}) = p_1^{t_1} h \in A$, where $p_1 \in A$ is irreducible and $\gcd(p_1, h) = 1$.

Output: A pair $(\mathbf{M}_1, \mathbf{M}_2) \in R^{l \times l} \times R^{l \times l}$ such that $\mathbf{M} = \mathbf{M}_1 \mathbf{M}_2$ and $\det(\mathbf{M}_1) = p_1^{t_1}$.

Step 1. Set $\mathbf{W} := (\mathbf{M}, p_1^{t_1} \mathbf{I}_l) \in R^{l \times 2l}$.

Step 2. Compute $(\mathbf{M}_1, \mathbf{G}_1) := \text{ZLPFact}_R(\mathbf{W}, l)$.

Step 3. Set $(\mathbf{M}_2, \mathbf{G}_2) := \mathbf{G}_1$, where $\mathbf{M}_2, \mathbf{G}_2 \in R^{l \times l}$. Return $(\mathbf{M}_1, \mathbf{M}_2)$.

Appendix B.5. Procedure $\text{CoprimeMerge}_{l,A}$ derived from Theorem 4.3

$(\mathbf{P}, \mathbf{Q}) := \text{CoprimeMerge}_{l,A}(n, \mathbf{F}, \mathbf{U}, \mathbf{G})$

Input: An integer $n \geq 0$, diagonal matrices $\mathbf{F} = \text{diag}(f_1, \dots, f_l)$ and $\mathbf{G} = \text{diag}(g_1, \dots, g_l)$ with $f_i, g_i \in A \setminus \{0\}$, and $\mathbf{U} \in \text{GL}_l(R)$, such that $f_i \mid f_{i+1}$, $g_i \mid g_{i+1}$ for $i = 1, \dots, l-1$, and $\gcd(f_l, g_l) = 1$.

Output: A pair $(\mathbf{P}, \mathbf{Q}) \in \text{GL}_l(R)^2$ such that $\mathbf{P}(\mathbf{F}\mathbf{U}\mathbf{G})\mathbf{Q} = \mathbf{F}\mathbf{G}$.

Step 1. For $n = 0$, compute $(\mathbf{P}, \mathbf{Q}) \in \text{GL}_l(A)^2$ such that $\mathbf{P}(\mathbf{F}\mathbf{U}\mathbf{G})\mathbf{Q} = \mathbf{F}\mathbf{G}$ by the standard Smith reduction over the PID A , and return $(\mathbf{P}, \mathbf{Q})$.

Step 2. Assume $n > 0$. Set $R' := A[x_1, \dots, x_{n-1}]$, $\mathbf{M} := \mathbf{F}\mathbf{U}\mathbf{G}$ and $\mathbf{D} := \mathbf{F}\mathbf{G}$. Let $S_1 := \{f_l^{\theta_1} \mid \theta_1 \in \mathbb{N}\}$ and $S_2 := \{g_l^{\theta_2} \mid \theta_2 \in \mathbb{N}\}$. Write $R'_{S_i} := S_i^{-1}R'$ for $i = 1, 2$.

Step 3. Set $\mathbf{U}_0 := \mathbf{U}(x_1, \dots, x_{n-1}, 0)$ and $\mathbf{M}_0 := \mathbf{F}\mathbf{U}_0\mathbf{G}$. Recursively compute

$$(\mathbf{P}_0, \mathbf{Q}_0) := \text{CoprimeMerge}_{l,A}(n-1, \mathbf{F}, \mathbf{U}_0, \mathbf{G}),$$

so that $\mathbf{P}_0\mathbf{M}_0\mathbf{Q}_0 = \mathbf{D}$, where $\mathbf{P}_0, \mathbf{Q}_0 \in \text{GL}_l(R')$.

Step 4. Over $R'_{S_1}[x_n]$, set $\mathbf{H}_1 := \mathbf{F}\mathbf{U}\mathbf{F}^{-1}$, so that $\mathbf{M} = \mathbf{H}_1\mathbf{D}$. Over $R'_{S_2}[x_n]$, set $\mathbf{H}_2 := \mathbf{G}^{-1}\mathbf{U}\mathbf{G}$, so that $\mathbf{M} = \mathbf{D}\mathbf{H}_2$. Combining these two local reductions with $\mathbf{P}_0\mathbf{M}_0\mathbf{Q}_0 = \mathbf{D}$, we obtain

$$\mathbf{P}_0^{-1}\mathbf{H}_1^{-1}\mathbf{M}\mathbf{Q}_0^{-1} = \mathbf{M}_0 \text{ over } R'_{S_1}[x_n], \quad \mathbf{P}_0^{-1}\mathbf{M}\mathbf{H}_2^{-1}\mathbf{Q}_0^{-1} = \mathbf{M}_0 \text{ over } R'_{S_2}[x_n].$$

Step 5. Since S_1 and S_2 are comaximal, Vaserstein patching [32, 33] applied to the equivalences in *Step 4* returns $\mathbf{P}_1, \mathbf{Q}_1 \in \text{GL}_l(R'[x_n])$ such that $\mathbf{P}_1\mathbf{M}\mathbf{Q}_1 = \mathbf{M}_0$.

Step 6. Set $\mathbf{P} := \mathbf{P}_0\mathbf{P}_1$ and $\mathbf{Q} := \mathbf{Q}_1\mathbf{Q}_0$. Then $\mathbf{P}\mathbf{F}\mathbf{U}\mathbf{G}\mathbf{Q} = \mathbf{F}\mathbf{G}$. Return $(\mathbf{P}, \mathbf{Q})$.