On some Euclidean properties of matrix algebras

Pierre Lezowski

ON SOME EUCLIDEAN PROPERTIES OF MATRIX ALGEBRAS

PIERRE LEZOWSKI

Abstract. Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. We study some Euclidean properties of the algebra $\mathrm{M}_n(\mathfrak{R})$ of n by n matrices with coefficients in $\mathfrak{R}$. In particular, we prove that $\mathrm{M}_n(\mathfrak{R})$ is a left and right Euclidean ring if and only if $\mathfrak{R}$ is a principal ideal ring. We also study the Euclidean order type of $\mathrm{M}_n(\mathfrak{R})$. If $\mathfrak{R}$ is a K-Hermite ring, then $\mathrm{M}_n(\mathfrak{R})$ is $(4n-3)$-stage left and right Euclidean. We obtain shorter division chains when $\mathfrak{R}$ is an elementary divisor ring, and even shorter ones when $\mathfrak{R}$ is a principal ideal ring. If we assume that $\mathfrak{R}$ is an integral domain, $\mathfrak{R}$ is a Bézout ring if and only if $\mathrm{M}_n(\mathfrak{R})$ is ω-stage left and right Euclidean.

1. Introduction

In this paper, all rings are nonzero, with unity, but not necessarily commutative. An *integral domain* is a commutative ring with no nontrivial zero divisor. A *principal ideal ring* (or *PIR* for short) is a commutative ring in which every ideal is principal. A *principal ideal domain* (or *PID* for short) is an integral domain which is a PIR. Given a ring $\mathfrak{A}$, we denote by $\mathfrak{A}^\bullet$ the set $\mathfrak{A} \setminus \{0\}$ and by $\mathfrak{A}^\times$ the units of $\mathfrak{A}$.

Given a ring $\mathfrak{A}$ and integers $n, m > 0$, $\mathrm{M}_{m,n}(\mathfrak{A})$ is the set of matrices of elements of $\mathfrak{R}$ with m rows and n columns; $\mathrm{M}_n(\mathfrak{A}) = \mathrm{M}_{n,n}(\mathfrak{A})$; $\mathrm{GL}_n(\mathfrak{A})$ is the subset of $\mathrm{M}_n(\mathfrak{A})$ of units of $\mathrm{M}_n(\mathfrak{A})$.

Whenever $\mathfrak{R}$ is commutative, $\mathrm{M}_n(\mathfrak{R})$ is an algebra, and we are especially interested in its Euclidean properties. In the classical sense, we say that a ring $\mathfrak{A}$ is right Euclidean if there exists some function $\varphi : \mathfrak{A} \longrightarrow \mathbf{Z}_{>0}$ such that for all $a, b \in \mathfrak{A}$, $b \neq 0$, there exists $q \in \mathfrak{A}$ such that

$$a = bq \qquad \text{or} \qquad \varphi(a - bq) < \varphi(b).$$

However, with this definition, $\mathfrak{A} = \mathrm{M}_n(\mathbf{Z})$ cannot be right Euclidean when $n \in \mathbf{Z}_{>1}$(see [Kal85, Theorem 2]), so instead, we will use a broader definition, following Samuel [Sam71]. Let us denote by $\mathcal{O}$ the class of all ordinal numbers.

Definition 1.1. Let $\mathfrak{A}$ be a ring. We say that $\mathfrak{A}$ is *right Euclidean* if there exists a function $\varphi : \mathfrak{A}^\bullet \longrightarrow \mathcal{O}$ such that for all $a, b \in \mathfrak{A}$, $b \neq 0$, there exists $q \in \mathfrak{A}$ such that

$$a = bq \qquad \text{or} \qquad \varphi(a - bq) < \varphi(b). \tag{1}$$

Date: September 19, 2016.

2010 *Mathematics Subject Classification.* Primary: 13F07; Secondary: 11A05.

Key words and phrases. Euclidean rings, 2-stage Euclidean rings, Euclidean algorithm, Principal Ideal Rings, division chains, elementary divisor ring, K-Hermite ring.

Such a φ is then called a *right Euclidean stathm* (or a right Euclidean function).

Obviously, we may define similarly *left Euclidean* rings and *left Euclidean stathms* by replacing bq with qb in (1). With this definition, Brungs proved the following property.

Proposition 1.2 ([Bru73, Theorem 1])**.** *If $\mathfrak{A}$ is a (not necessarily commutative) left Euclidean ring without nontrivial zero divisors, then $\mathrm{M}_n(\mathfrak{A})$ is a left Euclidean ring for any $n \in \mathbf{Z}_{\geq 1}$.*

We will establish the following result.

Theorem 4.1. *Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. Then $\mathrm{M}_n(\mathfrak{R})$ is right and left Euclidean if and only if $\mathfrak{R}$ is a principal ideal ring.*

To prove it, we will use some technical tools and notations, introduced in Section 2, and proceed in two steps. We will rely on the fact that a PIR is a *K-Hermite ring*, that is to say that every matrix admits triangular reduction, and even an *elementary divisor ring*, that is to say that every matrix admits diagonal reduction[1]. First, we will prove Theorem 4.1 over PIDs in Section 3, which will allow us to extend it to PIRs in Section 4.

We will see in Section 5 under which conditions we can compute a quotient of the right Euclidean division (1) for the stathm that we build. As an application, we will see that we can compute continued fractions in a matrix algebra over a PID.

In Definition 1.1, the range of the Euclidean stathm may be arbitrary, but for a given right Euclidean ring $\mathfrak{A}$, we can try to find a right Euclidean stathm whose range is as "small" as possible. This is formalized by the notion of Euclidean order type of $\mathfrak{A}$. Section 6 will be devoted to the study of the Euclidean order type of $\mathrm{M}_n(\mathfrak{R})$ when $\mathfrak{R}$ is a PIR.

Finally, we will study another generalization of the Euclidean property in Section 7. Instead of allowing ordinals in the range of the stathm, we still consider $\varphi : \mathfrak{A}^\bullet \longrightarrow \mathbf{Z}_{>0}$, but we allow several divisions on the right: starting from the pair (a, b), we continue with a pair $(b, a - bq)$ for some $q \in \mathfrak{A}$, and so forth[2]. After k divisions, we want the remainder r_k to satisfy

$$r_k = 0 \qquad \text{or} \qquad \varphi(r_k) < \varphi(b). \tag{2}$$

If for all pair of elements of $\mathfrak{A}$, we can obtain a k-stage division chain with the k-th remainder r_k satisfying (2), we say that $\mathfrak{A}$ is *k-stage right Euclidean*. If $r_k = 0$, we say that the division chain is *terminating*. If for all $a, b \in \mathfrak{A}$, $b \neq 0$, there exists a terminating division chain starting from (a, b), we say that $\mathfrak{A}$ is *ω-stage right Euclidean*. A right Euclidean ring is necessarily ω-stage right Euclidean, but the converse is false in general since such a ring may have non-principal ideals. Alahmadi, Jain, Lam, and Leroy proved the following result about the ω-stage right Euclidean properties of matrix rings.

Proposition 1.3 ([AJLL14, Theorem 14])**.** *If $\mathfrak{A}$ is a (not necessarily commutative) ω-stage right Euclidean ring, then so is $\mathrm{M}_n(\mathfrak{A})$ for any $n \in \mathbf{Z}_{\geq 1}$.*

[1]See Section 2 for precise definitions.

[2]See Section 7 for precise definitions.

An immediate consequence of Theorem 4.1 is that $\mathrm{M}_n(\mathfrak{R})$ is ω-stage right Euclidean if $\mathfrak{R}$ is a PIR and $n \in \mathbf{Z}_{>1}$. But we will show the following more precise result in Section 7.

Theorem 7.3. *Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. Then we have the following properties.*

1. *If $\mathfrak{R}$ is a K-Hermite ring, then for every pair $(A, B) \in \mathrm{M}_n(\mathfrak{R}) \times \mathrm{M}_n(\mathfrak{R})^\bullet$, there exists a $(4n-3)$-stage terminating division chain in $\mathrm{M}_n(\mathfrak{R})$ starting from (A, B). In particular, $\mathrm{M}_n(\mathfrak{R})$ is ω-stage left and right Euclidean.*
2. *If $\mathfrak{R}$ is an elementary divisor ring (e.g. if $\mathfrak{R}$ is a PIR), then for every pair $(A, B) \in \mathrm{M}_n(\mathfrak{R}) \times \mathrm{M}_n(\mathfrak{R})^\bullet$, there exists a $(2n-1)$-stage terminating division chain in $\mathrm{M}_n(\mathfrak{R})$ starting from (A, B).*
3. *If $\mathfrak{R}$ is a PIR, then $\mathrm{M}_n(\mathfrak{R})$ is 2-stage right and left Euclidean.*

Therefore, when $\mathfrak{R}$ is an integral domain, we can characterize when $\mathrm{M}_n(\mathfrak{R})$ is ω-stage right and left Euclidean.

Corollary 7.4. *Let $\mathfrak{R}$ be an integral domain and $n \in \mathbf{Z}_{>1}$. Then $\mathrm{M}_n(\mathfrak{R})$ is ω-stage left and right Euclidean if and only if $\mathfrak{R}$ is a Bézout ring, that is to say for all a, $b \in \mathfrak{R}$, there exists $d \in \mathfrak{R}$ such that $a\mathfrak{R} + b\mathfrak{R} = d\mathfrak{R}$.*

2. Generalities and first remarks

2.1. **Notation and terminology.** Consider a ring $\mathfrak{A}$, a commutative ring $\mathfrak{R}$, and m, n, $p \in \mathbf{Z}_{\geq 1}$. In $\mathfrak{R}$, we say that a divides b, denoted by $a|b$, if $b\mathfrak{R} \subseteq a\mathfrak{R}$. Most of the definitions and the results in this paragraph are due to Kaplansky [Kap49][3].

We denote by $\mathrm{diag}(b_1, \ldots, b_n)_{m,p}$ the matrix in $\mathrm{M}_{m,p}(\mathfrak{A})$ with diagonal coefficients $b_1, \ldots, b_n$. For short, $\mathrm{diag}(b_1, \ldots, b_n) = \mathrm{diag}(b_1, \ldots, b_n)_{n,n}$. We write $\mathfrak{1}_n$ for the identity matrix of size n, $\mathfrak{o}_{m,n}$ for the zero matrix with m rows and n columns, $\mathfrak{o}_n = \mathfrak{o}_{n,n}$.

A ring $\mathfrak{A}$ is a *right Bézout ring* if for all a, $b \in \mathfrak{A}$, $a\mathfrak{A} + b\mathfrak{A} = d\mathfrak{A}$, for some $d \in \mathfrak{A}$. Such a d is called a greatest common left divisor of a and b, or *gcld* for short. We define similarly left Bézout rings and *gcrds* (i.e. greatest common right divisors).

The *stable rank* of a ring $\mathfrak{A}$ is the infimum of the positive integers n such that for all $a_0, \ldots, a_n \in \mathfrak{A}$,

$$\begin{aligned} &a_0\mathfrak{A} + \cdots + a_n\mathfrak{A} = \mathfrak{A} \Longrightarrow \exists b_1, \ldots, b_n \in \mathfrak{A}, \\ &\quad (a_1 + b_1 a_0)\mathfrak{A} + \cdots + (a_n + b_n a_0)\mathfrak{A} = \mathfrak{A}. \end{aligned} \tag{3}$$

We denote it by $\mathrm{sr}\,\mathfrak{A}$. If $\mathrm{sr}\,\mathfrak{A} = l$, then (3) holds for any $n \geq l$ [Vas71, Theorem 1]. The stable rank can be defined as in (3) using left ideals instead of right ideals; the value $\mathrm{sr}\,\mathfrak{A}$ coincides [Vas71, Theorem 2]. The stable rank of $\mathfrak{A}$ and matrix rings over $\mathfrak{A}$ are connected [Vas71, Theorem 3]:

$$\mathrm{sr}\,\mathrm{M}_n(\mathfrak{A}) = 1 + \left\lceil \frac{\mathrm{sr}\,\mathfrak{A} - 1}{n} \right\rceil.$$

In the formula above, $\lceil x \rceil$ is the least integer exceeding x. In particular, $\mathrm{M}_n(\mathfrak{A})$ has stable rank 1 if and only if $\mathfrak{A}$ has stable rank 1.

[3] We call "K-Hermite" what he calls "Hermite" to follow the current trend.

We say that $\mathfrak{A}$ is a *right K-Hermite ring* if for all a, $b \in \mathfrak{A}$, there exists $Q \in \mathrm{GL}_2(\mathfrak{A})$ and $d \in \mathfrak{A}$ such that $\begin{pmatrix} a & b \end{pmatrix} Q = \begin{pmatrix} d & 0 \end{pmatrix}$. Any right K-Hermite ring is a right Bézout ring. Besides, if $\mathfrak{A}$ is a right K-Hermite ring, then for all $M \in \mathrm{M}_n(\mathfrak{A})$, there exists $T \in \mathrm{GL}_n(\mathfrak{A})$ such that AT is lower triangular.

A left K-Hermite ring satisfies the following condition: for all a, $b \in \mathfrak{A}$, there exists $Q \in \mathrm{GL}_2(\mathfrak{A})$ and $d \in \mathfrak{A}$ such that $Q \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}$. A *K-Hermite ring* is a right and left K-Hermite ring. If $\mathfrak{A}$ is a K-Hermite ring, then $\mathrm{M}_n(\mathfrak{A})$ is a right K-Hermite ring ([Kap49, Theorem 3.6]). If $\mathfrak{A}$ is a K-Hermite ring with no nontrivial zero divisors, then for A, $B \in \mathrm{M}_n(\mathfrak{A})$, the gcld of A and B is unique up to multiplication by an element of $\mathrm{GL}_n(\mathfrak{A})$ on the right (see [Kap49, Theorem 3.8]). In commutative K-Hermite rings, we can simplify by a (good choice of a) gcd, and it is actually a characterization of these rings.

Lemma 2.1 ([GH56, Theorem 3])**.** *Let $\mathfrak{R}$ be a commutative ring. Then $\mathfrak{R}$ is a K-Hermite ring if and only if for all a, $b \in \mathfrak{R}$, there exist a', b', $d \in \mathfrak{R}$ such that $a = da'$, $b = db'$, and*

$$a'\mathfrak{R} + b'\mathfrak{R} = \mathfrak{R}.$$

We can clearly extend it to three elements, and we will especially use it in this form: Let $\mathfrak{R}$ be a commutative K-Hermite ring, a, b, $c \in \mathfrak{R}$. Then there exist a', b', c', $d \in \mathfrak{R}$ such that $a = da'$, $b = db'$, $c = dc'$ and

$$a'\mathfrak{R} + b'\mathfrak{R} + c'\mathfrak{R} = \mathfrak{R}.$$

Given A, $B \in \mathrm{M}_{m,p}(\mathfrak{R})$, we say that A and B are equivalent, which is denoted by $A \sim B$ if there exist $X \in \mathrm{GL}_p(\mathfrak{R})$, $Y \in \mathrm{GL}_m(\mathfrak{R})$ such that $B = YAX$. We say that $\mathfrak{R}$ is an *elementary divisor ring*[4] if for any m, $p \in \mathbf{Z}_{\geq 1}$, any $A \in \mathrm{M}_{m,p}(\mathfrak{R})$ is equivalent to a diagonal matrix $\mathrm{diag}(b_1, b_2, \ldots, b_n)_{m,p}$, where $b_1 | b_2 | \ldots | b_n$. In this case, b_1 divides every coefficient of the matrix A. Any elementary divisor ring is a K-Hermite ring. The following property will be a crucial tool.

Lemma 2.2 ([MM82, Proposition 8])**.** *Let $\mathfrak{A}$ be a right K-Hermite ring. Then the stable rank of $\mathfrak{A}$ satisfies* $\mathrm{sr}\,\mathfrak{A} \leq 2$.

If $\mathfrak{R}$ is a PID, then it is an elementary divisor ring, so a K-Hermite ring. You can refer to [Jac85, Section 3.7] for details. The reductions of matrices with coefficients in $\mathfrak{R}$ into triangular or diagonal ones can be computed, provided that for any a, $b \in \mathfrak{R}$, we know how to compute λ, μ, $d \in \mathfrak{R}$ such that

$$\begin{cases} a\mathfrak{R} + b\mathfrak{R} = d\mathfrak{R}, \\ a\lambda + b\mu = d. \end{cases}$$

Besides, recall that for any $M \in \mathrm{M}_n(\mathfrak{R})$, there exist $(b_i)_{1 \leq i \leq n} \in \mathfrak{R}^n$ such that $b_1 | b_2 | \ldots | b_n$ and

$$M \sim \mathrm{diag}(b_1, \ldots, b_n).$$

In this case, the elements $(b_i)_{1 \leq i \leq n}$ are unique up to multiplication by a unit of $\mathfrak{R}$ and are called the *invariant factors* of M. Such a reduction is called the

[4]Kaplansky's definition is not limited to a commutative context, but we will not need such a generality.

Smith normal form of M. The largest integer r such that $b_r \neq 0$ is the rank $\mathrm{rk}(M)$ of M. It corresponds to the classical notion of rank in vector spaces, because $\mathfrak{R}$ can be embedded into its field of fractions. In particular, a matrix $M \in \mathrm{M}_n(\mathfrak{R})$ has rank n if and only if $\det M \neq 0$, and more generally, the rank is equal to the maximal order of a nonzero minor.

Smith normal form has some further properties.

Lemma 2.3. *Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{\geq 1}$.*

(a) Let $M \in \mathrm{M}_n(\mathfrak{R})^\bullet$ and let $b_1, b_2, \ldots, b_r \in \mathfrak{R}$ be the invariant factors of M. For any $1 \leq l \leq r$, $\prod_{i=1}^{l} b_i$ is a gcd of the $l \times l$ minors of M. In particular, b_1 is a gcd of the coefficients of M.

(b) Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathfrak{R})$. If the greatest common divisor of a, b, c, d is 1, then

$$M \sim \mathrm{diag}(1, ad - bc).$$

Proof. Item (a) is a reformulation of [Jac85, Theorem 3.9]. For (b), write $M \sim \mathrm{diag}(b_1, b_2)$, for elements $b_1 | b_2$ in $\mathfrak{R}$. Thanks to (a), we can take $b_1 = 1$. Besides, $\det M$ and $b_1 b_2$ coincide up to multiplication by a unit, which completes the proof. □

2.2. **Basic remarks.** In Definition 1.1, we have distinguished right and left Euclidean rings, but such a care will be useless in our context.

Proposition 2.4. *Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. Then $\mathrm{M}_n(\mathfrak{R})$ is right Euclidean if and only if it is left Euclidean.*

Proof. Let f be any function $\mathrm{M}_n(\mathfrak{R})^\bullet \longrightarrow \mathcal{O}$. We define

$$f^{\mathsf{T}} : \left\{ \begin{array}{ccc} \mathrm{M}_n(\mathfrak{R})^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & f(M^{\mathsf{T}}) \end{array} \right. .$$

Then for any $A, B, Q \in \mathrm{M}_n(\mathfrak{R})$,

$$\Big(A = BQ \Longleftrightarrow A^{\mathsf{T}} = Q^{\mathsf{T}} B^{\mathsf{T}}\Big) \quad \text{and} \quad f^{\mathsf{T}}(A - BQ) = f(A^{\mathsf{T}} - Q^{\mathsf{T}} B^{\mathsf{T}}).$$

Hence, f is a right Euclidean stathm if and only f is a left Euclidean stathm. □

Therefore, to prove Theorem 4.1, we will only need to deal with right Euclidean stathms.

Proposition 2.5. *Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{\geq 1}$. If every right ideal of $\mathrm{M}_n(\mathfrak{R})$ is principal, then $\mathfrak{R}$ is a principal ideal ring.*

Proof. This is certainly very classical, but we include the proof to emphasize its simplicity. Let I be an ideal of $\mathfrak{R}$. We define

$$\mathfrak{I} = \{(a_{i,j})_{1 \leq i,j \leq n} \in \mathrm{M}_n(\mathfrak{R}), \text{ for any } 1 \leq j \leq n,\ a_{1,j} \in I\}.$$

It is clear that $\mathfrak{I}$ is a right ideal of $\mathrm{M}_n(\mathfrak{R})$. Let us consider $\det \mathfrak{I} = \{\det M,\ M \in \mathfrak{I}\}$. Then, the fact that I is an ideal and Leibniz formula for determinants imply that $\det \mathfrak{I} \subseteq I$. Besides, for any $a \in I$, define

$$A = \mathrm{diag}(a, 1, \ldots, 1) \in \mathrm{M}_n(\mathfrak{R}).$$

Then $A \in \mathfrak{I}$ and $a = \det A \in \det \mathfrak{I}$. Therefore, we also have $I \subseteq \det \mathfrak{I}$, which proves that $\det \mathfrak{I} = I$.

But there exists $\alpha \in \mathrm{M}_n(\mathfrak{R})$ such that $\mathfrak{I} = \alpha \mathrm{M}_n(\mathfrak{R})$. Then $I = \det \mathfrak{I} = (\det \alpha) R$, which completes the proof. □

Remark 2.6. If we do not assume $\mathfrak{R}$ to be commutative, this property is false in general: consider the Weyl algebra A_1 in characteristic 0. Then A_1 admits non-principal right ideals, but for any $n \geq 2$, every right ideal of $\mathrm{M}_n(A_1)$ is principal, see [MR01, 7.11.7 and 7.11.8, p. 293].

2.3. **Length in a PID.** Let $\mathfrak{R}$ be a PID and $x \in \mathfrak{R}^\bullet$. Since $\mathfrak{R}$ is a unique factorization domain, x may be decomposed into a finite product of prime elements

$$x = u \prod_{i=1}^{n} {p_i}^{e_i},$$

where $n \in \mathbf{Z}_{\geq 0}$, $u \in \mathfrak{R}^\times$, for any $1 \leq i \leq n$, $p_i \in \mathfrak{R}$ is prime and $e_i \in \mathbf{Z}_{>0}$. The decomposition is unique up to multiplication by units and order. We set $\ell(x) = \sum_{i=1}^{n} e_i$, which defines a function

$$\ell : \left\{ \begin{array}{ccc} \mathfrak{R}^\bullet & \longrightarrow & \mathbf{Z}_{\geq 0} \\ x & \longmapsto & \ell(x) \end{array} \right. .$$

Remark that ℓ is invariant under multiplication by a unit. Besides, if a, b are elements of $\mathfrak{R}$ such that a divides b and $b \neq 0$, then $\ell(a) \leq \ell(b)$ and the equality holds if and only if a and b are associate, that is to say there exists $u \in \mathfrak{R}^\times$ such that $b = au$.

2.4. **Explicit stable rank 2 in a PID.** The following classical lemma will be very useful. It can be seen as an easy consequence of Lemma 2.2, but we give its proof to see how explicit it is; this will prove useful for Section 5.

Lemma 2.7. *Let $\mathfrak{R}$ be a PID. Then $\operatorname{sr} \mathfrak{R} \leq 2$. More precisely, for any a, b, $c \in \mathfrak{R}$ which are not all equal to 0, there exist $z, t \in \mathfrak{R}$, such that $\gcd(a + cz, b + ct) = gcd(a, b, c)$, which is nonzero and divides c.*

Proof. We will proceed in two steps.
(a) First, consider a, b, $c \in \mathfrak{R}$ such that $b \neq 0$ and $\gcd(a, b, c) = 1$, we will prove that there exists $z \in \mathfrak{R}$ such that $\gcd(a + cz, b) = 1$. If a and b are coprime, we can take $z = 0$. If not, write a decomposition of $b \neq 0$ as follows:

$$b = \prod_{i=1}^{l} d_i^{\alpha_i} z, \tag{4}$$

where $l \in \mathbf{Z}_{>0}$, $(d_i)_{1 \leq i \leq l}$ is a family of distinct and non-associated primes in $\mathfrak{R}$, for any $1 \leq i \leq l$, $\alpha_i \in \mathbf{Z}_{>0}$, d_i divides a, but d_i does not divide z. Take a prime $p \in \mathfrak{R}$ such that p divides b. If p divides a, then p is associated to some d_i, for $1 \leq i \leq l$, and p does not divide z. Therefore, if p divides $a + cz$, then it necessarily divides $a + cz - a = cz$, so it divides c. Then p divides a, b, and c, which are coprime. This is impossible, so p does not divide $a + cz$. If p does not divide a, then p divides z. Thus, p does not divide $a + cz$ in this case either. Consequently, $\gcd(a + cz, b) = 1$.
(b) Now, we consider a, b, $c \in \mathfrak{R}$ which are not all equal to 0. If $c = 0$, take $z = t = 0$. From now on, assume that $c \neq 0$. Take $t \in \{0, 1\}$ such that $b + ct \neq 0$. Set $d = \gcd(a, b, c)$, consider $a' = \frac{a}{d}$, $b' = \frac{b+tc}{d}$, $c' = \frac{c}{d}$

and apply (a): there exists $z \in \mathfrak{R}$ such that $\gcd(a' + c'z, b') = 1$. Then $\gcd(a + cz, b + ct) = d$. □

Remark 2.8. In the proof above, we can compute z in (4) without actually computing a decomposition of b into a product of primes, it is enough to compute some gcds.

Proof. For $a, b \in \mathfrak{R}$, $b \neq 0$, we want to find a pair $(d, z) \in \mathfrak{R}^2$ such that $b = dz$, $\gcd(d, z) = 1$, and for any prime p dividing b, p divides a if and only if p divides d.

We build inductively a pair (d_m, z_m) of elements of $\mathfrak{R}$. Write $d_1 = \gcd(b, a)$ and $b = d_1 z_1$ for some $z_1 \in \mathfrak{R}$. If d_1 and z_1 are coprime, then $m = 1$ and we are done. If not, assume that we have (d_i, z_i) such that $b = d_i z_i$. If $\gcd(d_i, z_i)$, we are done, set $m = i$. If not, set $d_{i+1} = d_i \gcd(d_i, z_i)$ and write $z = d_{i+1} z_{i+1}$.

As at each step d_i is a divisor of b and a strict divisor of d_{i+1}, we are done in a finite number of steps: we obtain

$$z = d_m z_m,$$

where $\gcd(d_m, z_m) = 1$. Besides, it is straightforward that $\gcd(b, a) = d_1$ divides d_m. Notice that for any $i \geq 1$, $d_{i+1} = d_i \gcd(d_i, z_i)$, so any prime divisor of d_{i+1} is a prime divisor of d_i. Consequently, any prime divisor of d_m is a prime divisor of $d_1 = \gcd(b, a)$.

Take a prime p dividing b. If p divides a, then it divides $\gcd(b, a)$, so p divides d_m. Conversely, if p divides d_m, then it divides $d_1 = \gcd(b, a)$, so p divides a.

Hence the pair $(d, z) = (d_m, z_m)$ is convenient. □

2.5. **Conventions and notations for ordinals.** We follow the notation used by Clark [Cla15], that is to say we denote by ω the least infinite ordinal, and for ordinal arithmetic, we fix the ordinal addition so that $\omega + 1 > \omega = 1 + \omega$, and for the multiplication $2\omega = \omega + \omega > \omega 2 = \omega$. For short, for $r \in \mathbf{Z}_{>0}$, $a_i, b_i \in \mathcal{O}$, $1 \leq i \leq r$, we write $\sum_{i=1}^{r} a_i \omega^{b_i} = a_1 \omega^{b_1} + a_2 \omega^{b_2} + \cdots + a_r \omega^{b_r}$.

We denote by $\oplus$ the Hessenberg sum of ordinals, that is to say for $k \in \mathbf{Z}_{>0}$, $(a_i)_{0 \leq i \leq k}$, $(b_i)_{0 \leq i \leq k}$ finite sequences of nonnegative integers,

$$\left(\sum_{i=0}^{k} a_i \omega^{k-i} \right) \oplus \left(\sum_{i=0}^{k} b_i \omega^{k-i} \right) = \left(\sum_{i=0}^{k} (a_i + b_i) \omega^{k-i} \right).$$

For $n \in \mathbf{Z}_{>0}$, $\alpha \in \mathcal{O}$, we write $n \otimes \alpha = \underbrace{\alpha \oplus \alpha \oplus \cdots \oplus \alpha}_{n \text{ times}}$.

Consider a right Euclidean ring $\mathfrak{A}$. In Definition 1.1, the right Euclidean stathm φ is not defined at 0. Following Clark, we define $\varphi(0)$ to be the smallest $\alpha \in \mathcal{O}$ such that for all $a \in \mathfrak{A}^\bullet$,

$$\varphi(a) < \alpha. \tag{5}$$

Now, we associate to $\mathfrak{A}$ the following ordinal number, called *(right) Euclidean order type*:

$$e(\mathfrak{A}) = \inf\{\varphi(0),\ \varphi : \mathfrak{A} \longrightarrow \mathcal{O},\ \varphi \text{ right Euclidean stathm}\}.$$

In other words, $e(\mathfrak{A}) = \theta(0)$, where θ is the smallest right Euclidean stathm for A, as defined by Samuel [Sam71] (or "bottom Euclidean function", with Clark's terminology): it is the function defined by

$$\theta : \left\{ \begin{array}{ccl} \mathfrak{A}^\bullet & \longrightarrow & \mathcal{O} \\ x & \longmapsto & \inf\left\{\phi(x),\, \phi : \mathfrak{A}^\bullet \longrightarrow \mathcal{O},\, \phi \text{ right Euclidean stathm}\right\}; \end{array} \right.$$

it is a right Euclidean stathm.

Remark 2.9. Let $\mathfrak{R}$ be a commutative ring, $n \in \mathbf{Z}_{\geq 1}$ so that $\mathrm{M}_n(\mathfrak{R})$ is right Euclidean. Let θ be the smallest right Euclidean stathm for $\mathrm{M}_n(\mathfrak{R})$. Then for any $m, m' \in \mathrm{M}_n(\mathfrak{R})$ such that $m \sim m'$, we have $\theta(m) = \theta(m')$. In particular, if $\mathfrak{R}$ is an elementary divisor ring, $\theta^{\mathsf{T}} = \theta$ and θ is the smallest left Euclidean stathm for $\mathrm{M}_n(\mathfrak{R})$. For this reason, we will write *Euclidean order type* instead of *right Euclidean order* type in what follows.

Proof. It follows immediately from the fact that the function

$$\tilde{\theta} : \left\{ \begin{array}{ccl} \mathrm{M}_n(\mathfrak{R})^\bullet & \longrightarrow & \mathcal{O} \\ m & \longmapsto & \inf\{\theta(m'),\, m' \sim m\} \end{array} \right.$$

is a right Euclidean stathm verifying $\tilde{\theta} \leq \theta$. Therefore, $\tilde{\theta} = \theta$. □

Lemma 2.10. *Let $\mathfrak{A}$ be a right Euclidean ring and $\theta : \mathfrak{A}^\bullet \longrightarrow \mathcal{O}$ be the smallest right Euclidean stathm. Take $x \in \mathfrak{A}^\bullet$ and $\mathcal{S} \subseteq \mathfrak{A} \setminus x\mathfrak{A}$ such that $\mathcal{S} \cup \{0\}$ is a system of representatives of $\mathfrak{A}/x\mathfrak{A}$. Then*

$$\theta(x) \leq \sup_{y \in \mathcal{S}} \inf_{a \in \mathfrak{A}} \theta(y + xa) + 1.$$

Proof. This is a consequence of Motzkin's construction. For $\alpha \in \mathcal{O}$, define $\mathfrak{A}_\alpha = \{z \in \mathfrak{A},\, \theta(z) \leq \alpha\}$ and $\mathfrak{A}^0_\alpha = \cup_{\beta<\alpha} \mathfrak{A}_\beta$. Then we have (see [Sam71] or [Cla15][5])

$$\mathfrak{A}_\alpha = \left\{ b \in \mathfrak{A},\, \text{the composite map } \mathfrak{A}^0_\alpha \cup \{0\} \hookrightarrow \mathfrak{A} \twoheadrightarrow \mathfrak{A}/x\mathfrak{A} \text{ is onto} \right\}.$$

Fix $\alpha = \sup_{y \in \mathcal{S}} \inf_{a \in \mathfrak{A}} \theta(y + xa) + 1$, we will prove that $x \in \mathfrak{A}_\alpha$. Let $\hat{y} + x\mathfrak{A} \in \mathfrak{A}/x\mathfrak{A} \setminus \{x\mathfrak{A}\}$, there exists $y \in \mathcal{S}$ such that $\hat{y} + x\mathfrak{A} = y + x\mathfrak{A}$. By definition of α, there exists $a \in \mathfrak{A}$ such that $\theta(y + xa) < \alpha$, therefore $y + xa \in \mathfrak{A}^0_\alpha$, which concludes the proof as $y + xa + x\mathfrak{A} = \hat{y} + x\mathfrak{A}$. □

3. A left and right Euclidean stathm for matrix algebras over a PID

3.1. **Statement and first remarks.** The purpose of this section will be to establish the following result.

Theorem 3.1. *Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$. Then $\mathrm{M}_n(\mathfrak{R})$ is a left and right Euclidean ring.*

Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$. We define

$$\rho_n : \left\{ \begin{array}{ccl} \mathrm{M}_n(\mathfrak{R})^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & \sum_{i=1}^{\mathrm{rk}\, M} \ell(b_i)\omega^{\mathrm{rk}\, M - i} \text{ if} \\ & & b_1, b_2, \ldots, b_{\mathrm{rk}\, M} \text{ are the invariant factors of } M. \end{array} \right.$$

[5] They deal with the commutative case but never use the commutativity hypothesis in this context.

The function ρ_n is well-defined because the function ℓ is invariant under multiplication by a unit. Now define

$$\varphi_n : \begin{cases} \mathrm{M}_n(\mathfrak{R})^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & (n - \operatorname{rk} M)\omega^n + \rho_n(M). \end{cases}$$

Notice that if A, $B \in \mathrm{M}_n(\mathfrak{R})^\bullet$ satisfy $A \sim B$, then $\rho_n(A) = \rho_n(B)$ and $\varphi_n(A) = \varphi_n(B)$.

Proposition 3.2. *The function φ_n is a right and left Euclidean stathm.*

The remainder of this section will be devoted to the proof of Proposition 3.2. This will imply Theorem 3.1.

Remark 3.3. For any $n > 1$, $\varphi_n^{\mathsf{T}} = \varphi_n$, so the proof of Proposition 2.4 implies that φ_n is a left Euclidean stathm if and only if it is a right Euclidean stathm.

Remark. The Euclidean stathm is in no way unique. For instance, the following function is a left and right Euclidean stathm:

$$\psi_2 : \begin{cases} \mathrm{M}_2(\mathbf{Z})^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & \begin{cases} |\det M| \text{ if } \det m \neq 0, \\ \omega + |\alpha| \text{ if } M \sim \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}. \end{cases} \end{cases}$$

See Proposition 6.5 for a more general construction.

3.2. **Case of size** 2 **matrices.** To prove Proposition 3.2, we will first deal with 2 by 2 matrices.

Lemma 3.4. *Let $A = \left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right), B = \operatorname{diag}(b_1, b_2) \in \mathrm{M}_2(\mathfrak{R})$, where b_1 divides $b_2 \neq 0$. If b_1 divides a, b and c, but b_2 does not divide b or b_2 does not divide c, then there exists $Q \in \mathrm{M}_2(\mathfrak{R})$ such that*

$$A - BQ \sim \operatorname{diag}(b_1, e),$$

where $e \in \mathfrak{R}^\bullet$ is such that $b_1 | e$ and e is a strict divisor of b_2.

Proof of Lemma 3.4. Set $e = \gcd(b, c, b_2) \neq 0$, which is a multiple of b_1 and a strict divisor of b_2. Lemma 2.7 implies that there exists $z, t \in \mathfrak{R}$ such that

$$\gcd(c + b_2 z, b + b_2 t) = e.$$

Therefore, there exist λ, $\mu \in \mathfrak{R}$ which are coprime and satisfy

$$\lambda(b + b_2 t) + \mu(c + b_2 z) = e. \tag{6}$$

Set $Q = \left(\begin{smallmatrix} a/b_1 - \mu & \lambda \\ -t & -z \end{smallmatrix}\right)$. Then

$$A - BQ = \begin{pmatrix} \mu b_1 & -\lambda b_1 \\ b + b_2 t & c + b_2 z \end{pmatrix}.$$

Since λ and μ are coprime, the gcd of the coefficients of $A - BQ$ is b_1. Besides, (6) implies that $\det(A - BQ) = b_1 e$. As a result, thanks to Lemma 2.3(b),

$$A - BQ \sim \operatorname{diag}(b_1, e).$$

□

Lemma 3.5. *Let $A \in \mathrm{M}_2(\mathfrak{R})$ and $B = \mathrm{diag}(b_1, b_2) \in \mathrm{M}_2(\mathfrak{R})$, where $b_1|b_2$ and $b_2 \neq 0$. Then there exists $Q \in \mathrm{M}_2(\mathfrak{R})$ such that*

$$A = BQ \qquad or \qquad (\mathrm{rk}(A - BQ) = 2 \quad and \quad \rho_2(A - BQ) < \rho_2(B)).$$

Proof of Lemma 3.5. Take $T \in \mathrm{GL}_2(\mathfrak{R})$ such that $AT = \left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right)$. We distinguish two cases.
a. Assume that b_1 does not divide a, b or c. Fix $\lambda, \mu \in \{0, 1\}$ such that $Q_{\lambda,\mu} = \left(\begin{smallmatrix} \lambda & -1 \\ 0 & \mu \end{smallmatrix}\right)$ satisfies

$$\det(AT - BQ_{\lambda,\mu}) = \begin{vmatrix} a - b_1\lambda & b_1 \\ b & c \end{vmatrix} - \mu b_2(a - b_1\lambda) \neq 0.$$

Therefore, $AT - BQ_{\lambda,\mu} \sim \mathrm{diag}(\alpha, \beta)$ for $\alpha|\beta \in \mathfrak{R}$, $\beta \neq 0$. But

$$AT - BQ_{\lambda,\mu} = \begin{pmatrix} a - b_1\lambda & b_1 \\ b & c - \mu b_2 \end{pmatrix}, \tag{7}$$

so, thanks to Lemma 2.3(a),

$$\alpha = \gcd(a - b_1\lambda, b_1, b, c - \mu b_2) = \gcd(a, b_1, b, c),$$

since b_1 divides b_2. Then α is a strict divisor of b_1. In particular, $\ell(\alpha) < \ell(b_1)$. Consequently, by setting $Q = Q_{\lambda,\mu}T^{-1}$, we have $\mathrm{rk}(A - BQ) = 2$ and

$$\rho_2(A - BQ) = \ell(\alpha)\omega + \ell(\beta) < \ell(b_1)\omega + \ell(b_2) = \rho_2(B).$$

b. If b_1 divides a, b, and c, we have two sub-cases. Either b_2 divides b and c and then $Q = (B^{-1}AT)T^{-1} \in \mathrm{M}_2(\mathfrak{R})$ satisfies $A = BQ$, or b_2 does not divide b or c, and then we apply Lemma 3.4 to find $Q \in \mathrm{M}_2(\mathfrak{R})$ such that

$$A - BQ \sim \mathrm{diag}(b_1, e),$$

where $e \in \mathfrak{R}^\bullet$ is such that $b_1|e$ and e is a strict divisor of b_2. Then

$$\rho_2(A - BQ) = \ell(b_1)\omega + \ell(e) < \ell(b_1)\omega + \ell(b_2) = \rho_2(B).$$

□

3.3. **Case of size n full-rank matrices.** Now, we extend Lemma 3.5 to n by n matrices, where $n \in \mathbf{Z}_{>1}$.

Lemma 3.6. *Let $n \in \mathbf{Z}_{>1}$, $A \in \mathrm{M}_n(\mathfrak{R})$, and $B = \mathrm{diag}(b_1, \ldots, b_n) \in \mathrm{M}_n(\mathfrak{R})$, where*

$$b_1|b_2|\ldots|b_n \neq 0.$$

Then there exists $Q \in \mathrm{M}_n(\mathfrak{R})$ such that

$$A = BQ \qquad or \qquad (\mathrm{rk}(A - BQ) = n \quad and \quad \rho_n(A - BQ) < \rho_n(B)).$$

Proof of Lemma 3.6. We prove it by induction on $n \geq 2$. The case $n = 2$ is Lemma 3.5. Set $n \geq 3$ and assume that Lemma 3.6 holds for all strictly smaller dimensions.

Take $A \in \mathrm{M}_n(\mathfrak{R})$. Consider $T \in \mathrm{GL}_n(\mathfrak{R})$ such that $AT = (a_{i,j})_{1 \leq i,j \leq n}$ is lower triangular.
1st step. Assume that there exist $1 \leq i_0, j_0 \leq n$ such that b_1 does not divide a_{i_0,j_0}. For any $1 \leq i \leq n$, take $\mu_i \in \{0, 1\}$ such that $a_{i,i} - \mu_i b_i \neq 0$. Then take $\lambda \in \{0, 1\}$ such that

$$(a_{1,1} - \mu_1 b_1)(a_{2,2} - \mu_2 b_2) - b_1(a_{2,1} - \lambda b_2) \neq 0.$$

Now consider

$$Q' = \left(\begin{array}{cc|c} \mu_1 & -1 & \\ \lambda & \mu_2 & \mathfrak{o}_{2,n-2} \\ \hline \mathfrak{o}_{n-2,2} & & \operatorname{diag}(\mu_3,\dots,\mu_n) \end{array}\right) \in \mathrm{M}_n(\mathfrak{R}),$$

then $AT - BQ'$ has rank n, its invariant factors are $b'_1|\dots|b'_n \neq 0$, and b'_1 divides all coefficients of $AT - BQ'$ (cf. Lemma 2.3(a)). In particular, b'_1 divides b_1 and a_{i_0,j_0}, so it is a strict divisor of b_1. Therefore, $\ell(b'_1) < \ell(b_1)$. Taking $Q = Q'T^{-1}$, we find $\operatorname{rk}(A - BQ) = n$ and

$$\rho_n(A - BQ) = \rho_n(AT - BQ') = \sum_{i=1}^{n} \omega^{n-i}\ell(b'_i) < \sum_{i=1}^{n} \omega^{n-i}\ell(b_i) = \rho_n(B).$$

2nd step. From now on, we assume that b_1 divides all coefficients of AT. Take $A' \in \mathrm{M}_{n-1}(R)$ such that

$$AT - B\left(\begin{array}{c|c} \frac{a_{1,1}}{b_1} - 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & \mathfrak{o}_{n-1} \end{array}\right) = \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline a_{2,1} & \\ \vdots & A' \\ a_{n,1} & \end{array}\right).$$

Set $B' = \operatorname{diag}(b_2,\dots,b_n)$. By the induction hypothesis, there exists $Q' \in \mathrm{M}_{n-1}(R)$ such that $R' = A' - B'Q'$ satisfies

$$R' = \mathfrak{o}_{n-1} \qquad \text{or} \qquad \left(\operatorname{rk} R' = n-1 \quad \text{and} \quad \rho_{n-1}(R') < \rho_{n-1}(B')\right).$$

1. Assume that $R' \neq \mathfrak{o}_{n-1}$. Its invariant factors $(b'_2,\dots,b'_n)$ are all divisible by b_1, as all coefficients of A' and B' are divisible by b_1 (see Lemma 2.3(a)). There exist $X, Y \in \mathrm{GL}_{n-1}(\mathfrak{R})$ such that $YR'X = \operatorname{diag}(b'_2,\dots,b'_n)$. Then

$$\begin{aligned} &\left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline a_{2,1} & \\ \vdots & A' \\ a_{n,1} & \end{array}\right) - B\left(\begin{array}{c|c} 0 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q' \end{array}\right) \\ &= \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Y \end{array}\right)^{-1} \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline a_{2,1} & \\ \vdots & YR'X \\ a_{n,1} & \end{array}\right) \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & X \end{array}\right)^{-1} \\ &\sim \operatorname{diag}(b_1, b'_2,\dots,b'_n). \end{aligned}$$

Thus, there exists $Q'' \in \mathrm{M}_n(\mathfrak{R})$ such that $AT - BQ'' \sim \operatorname{diag}(b_1, b'_2,\dots,b'_n)$. Taking $Q = Q''T^{-1} \in \mathrm{M}_n(\mathfrak{R})$, we obtain

$$A - BQ \sim \operatorname{diag}(b_1, b'_2,\dots,b'_n).$$

Since $b_1|b'_2|\dots|b'_n \neq 0$, $\operatorname{rk}(A - BQ) = n$ and they are the invariant factors of $A - BQ$. Hence

$$\rho_n(A - BQ) = \ell(b_1)\omega^{n-1} + \rho_{n-1}(R') < \ell(b_1)\omega^{n-1} + \rho_{n-1}(B') = \rho_n(B).$$

2. Assume now that $R' = \mathfrak{o}_{n-1}$. We distinguish two subcases.
2.*a*. First, assume that for all $l > 1$, b_l divides $a_{l,1}$, then

$$\left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_{2,1} \\ \vdots \\ a_{n,1} \end{matrix} & A' \end{array}\right) - B \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_{2,1}/b_2 \\ \vdots \\ a_{n,1}/b_n \end{matrix} & Q' \end{array}\right) = \mathfrak{o}_n.$$

Therefore, there exists $Q'' \in \mathrm{M}_n(\mathfrak{R})$ such that $AT - BQ'' = \mathfrak{o}_n$. Take $Q = Q''T^{-1}$, then

$$A - BQ = \mathfrak{o}_n.$$

2.*b*. Now assume that there exists $l > 1$ such that b_l does not divide $a_{l,1}$. Define

$$\begin{aligned} A'' &= \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_{2,1} \\ \vdots \\ a_{n,1} \end{matrix} & A' \end{array}\right) - B \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q' \end{array}\right) + B \\ &= \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_{2,1} \\ \vdots \\ a_{n,1} \end{matrix} & \mathrm{diag}(b_2, \dots, b_n) \end{array}\right). \end{aligned}$$

Take $l > 1$ to be the smallest integer such that there exists $m \geq l$ such that b_l does not divide $a_{m,1}$.
2.*b*.*i*. If $l < n$, take $\epsilon \in \{0, 1\}$ to be chosen later to define

$$Q''_\epsilon = \left(\begin{array}{c|c|c|c} \begin{matrix} 1 \\ a_{2,1}/b_2 \\ \vdots \\ a_{l-1,1}/b_{l-1} \\ \epsilon \end{matrix} & \mathfrak{o}_{l,l-2} & \begin{array}{cc} -1 & 0 \\ \hline & \\ & \mathfrak{o}_{l-2,2} \\ & \\ \hline 1 & -1 \end{array} & \mathfrak{o}_{l,n-l-1} \\ \hline \multicolumn{4}{c}{\mathfrak{o}_{n-l,n}} \end{array}\right) \in \mathrm{M}_n(\mathfrak{R}).$$

Exchanging the first and l-th columns of $A'' - BQ''_\epsilon$, we obtain

$$A'' - BQ''_\epsilon \sim \left(\begin{array}{c|c} \mathrm{diag}(b_1, \dots, b_{l-1}) & \mathfrak{o}_{l-1,n-l+1} \\ \hline \mathfrak{o}_{n-l+1,l-1} & A'''_\epsilon \end{array}\right),$$

where

$$A'''_\epsilon = \left(\begin{array}{c|c|c} a_{l,1} - b_l\epsilon & b_l & \mathfrak{o}_{1,n-l-1} \\ \hline \begin{matrix} a_{l+1,1} \\ \vdots \\ a_{n,1} \end{matrix} & \multicolumn{2}{c}{\mathrm{diag}(b_{l+1}, \dots, b_n)} \end{array}\right) \in \mathrm{M}_{n-l+1}(\mathfrak{R}).$$

We have $\det A'''_\epsilon = \det A'''_0 - \epsilon b_l b_{l+1} \cdots b_n$. As $b_l b_{l+1} \cdots b_n \neq 0$, we can choose $\epsilon \in \{0, 1\}$ such that $\det A'''_\epsilon \neq 0$. Then $\mathrm{rk}\, A'''_\epsilon = n - l + 1$, and the invariant factors of A'''_ϵ are $b'_l | \dots | b'_n \neq 0$. Furthermore, b_{l-1} divides all coefficients of A'''_ϵ, so thanks to Lemma 2.3(a), b_{l-1} divides b'_l. It follows that the invariant factors of $A'' - BQ''_\epsilon$ are $(b_1, \dots, b_{l-1}, b'_l, \dots, b'_n)$. Besides, there exists $m \geq l$ such that b_l does not divide $a_{m,1}$. As b'_l divides b_l and $a_{m,1}$, it is a strict divisor of b_l. Consequently, $\ell(b'_l) < \ell(b_l)$. As there exists $Q \in \mathrm{M}_n(\mathfrak{R})$ such

that $AT-BQT = A''-BQ''_\epsilon$, we have $A-BQ \sim \operatorname{diag}(b_1,\dots,b_{l-1},b'_l,\dots,b'_n)$, which implies $\operatorname{rk}(A-BQ)=n$ and

$$\rho_n(A-BQ) = \sum_{i=1}^{l-1}\ell(b_i)\omega^{n-i} + \sum_{i=l}^{n}\ell(b'_i)\omega^{n-i} < \sum_{i=1}^{n}\ell(b_i)\omega^{n-i} = \rho_n(B).$$

2.*b*.*ii*. If $l=n$, set $g=\gcd\left(\frac{b_n}{b_{n-1}},\frac{a_n}{b_{n-1}}\right)$ and take $\lambda,\mu\in\mathfrak{R}$ coprime such that

$$\lambda\frac{b_n}{b_{n-1}}+\mu\frac{a_n}{b_{n-1}}=g.$$

Fix

$$Q''=\left(\begin{array}{c|c|c} 1 & \mathfrak{o}_{n,n-3} & \begin{array}{cc} 0 & -1 \\ \hline & \\ & \mathfrak{o}_{n-3,2} \\ & \\ \hline 1-\mu & 0 \\ -1 & 1 \end{array} \\ a_{2,1}/b_2 & & \\ \vdots & & \\ a_{n-2,1}/b_{n-2} & & \\ a_{n-1,1}/b_{n-1}+\lambda & & \\ 0 & & \end{array}\right) \in \mathrm{M}_n(\mathfrak{R}).$$

By exchanging the first and last columns of $A''-BQ''$, we obtain

$$A''-BQ'' \sim \left(\begin{array}{c|c} \operatorname{diag}(b_1,\dots,b_{n-2}) & \mathfrak{o}_{n-2,2} \\ \hline \mathfrak{o}_{2,n-2} & A''' \end{array}\right),$$

where

$$A'''=\begin{pmatrix}\mu b_{n-1} & -\lambda b_{n-1}\\ b_n & a_{n,1}\end{pmatrix}\in\mathrm{M}_2(\mathfrak{R}).$$

Thanks to Lemma 2.3(b), the invariant factors of A''' are $(b_{n-1}, b_{n-1}\cdot g)$. As there exists some $Q\in\mathrm{M}_n(\mathfrak{R})$ such that $AT-BQ\sim A''-BQ''$, the invariant factors of $A-BQ$ are $(b_1,\dots,b_{n-1},b_{n-1}\cdot g)$ too. In particular, $\operatorname{rk}(A-BQ)=n$. Furthermore, $b_{n-1}g$ is the gcd of a_n and b_n, so it is a strict divisor of b_n. Then $\ell(b_{n-1}\cdot g)<\ell(b_n)$. Consequently,

$$\rho_n(A-BQ) = \sum_{i=1}^{n-1}\ell(b_i)\omega^{n-i} + \ell(b_{n-1}\cdot g) < \sum_{i=1}^{n}\ell(b_i)\omega^{n-i} = \rho_n(B).$$

That completes the proof of Lemma 3.6. □

3.4. **Case of matrices with rank 1.**

Lemma 3.7. *Let $n>1$, $A=\operatorname{diag}(a,0,\dots,0), B=\operatorname{diag}(b,0,\dots,0)\in\mathrm{M}_n(\mathfrak{R})$, where $b\neq 0$. Then there exists $Q\in\mathrm{M}_n(\mathfrak{R})$ such that*

$$A=BQ \qquad or \qquad \varphi_n(A-BQ)<\varphi_n(B).$$

Proof of Lemma 3.7. If b divides a, set $Q=\operatorname{diag}(a/b,0,\dots,0)\in\mathrm{M}_n(\mathfrak{R})$. Then $A=BQ$.

Now, assume that b does not divide a. Then $e=\gcd(a,b)$ is a strict divisor of b and $\ell(e)<\ell(b)$. Set $Q=(q_{i,j})_{1\le i,j\le n}$ where $q_{1,2}=1$ and all other coefficients are equal to 0. Then $A-BQ\sim\operatorname{diag}(e,0,\dots,0)$. Consequently,

$$\varphi_n(A-BQ)=(n-1)\omega^n+\ell(e)<(n-1)\omega^n+\ell(b)=\varphi_n(B).$$

□

Now, we have all the tools required to prove Proposition 3.2.

3.5. **Proof of Proposition 3.2.** Recall that $\mathfrak{R}$ is a PID and $n \in \mathbf{Z}_{>1}$. Thanks to Remark 3.3, if suffices to prove that φ_n is a right Euclidean stathm. Let $A, B \in \mathrm{M}_n(\mathfrak{R})$, $B \neq 0$. We want to find $Q \in \mathrm{M}_n(\mathfrak{R})$ such that $A = BQ$ or $\varphi_n(A - BQ) < \varphi_n(B)$.

Set $r = \operatorname{rk} B$. We take $X, Y, T \in \mathrm{GL}_n(\mathfrak{R})$, and $b_1|b_2|\ldots|b_r \in \mathfrak{R}^\bullet$ such that

$$YBX = \operatorname{diag}(b_1, \ldots, b_r, 0, \ldots, 0) \in \mathrm{M}_n(\mathfrak{R}),$$

and $YAT = (a_{i,j})_{1 \leq i,j \leq n}$ is lower triangular.

1. If $r = n$, then, thanks to Lemma 3.6, there exists $Q' \in \mathrm{M}_n(\mathfrak{R})$ such that $YAT = YBXQ'$, or $\operatorname{rk}(YAT - YBXQ') = n$ and $\rho_n(YAT - YBXQ') < \rho_n(YBX)$. Setting $Q = XQ'$, we have as required

$$A = BQ \qquad \text{or} \qquad \varphi_n(A - BQ) < \varphi_n(B).$$

2. From now on, we assume that $r < n$. For any $1 \leq i \leq r$, there exists $\mu_i \in \{0, 1\}$ such that $a_{i,i} - b_i\mu_i \neq 0$. Write $D = \operatorname{diag}(\mu_1, \ldots, \mu_r, 0, \ldots, 0) \in \mathrm{M}_n(\mathfrak{R})$ and then

$$YAT - YBXD = \left(\begin{array}{c|c} A_1 & \mathfrak{o}_{r,n-r} \\ \hline A_2 & A_3 \end{array}\right)$$

where $A_1 \in \mathrm{M}_r(\mathfrak{R})$ is lower triangular, $A_2 \in \mathrm{M}_{n-r,r}(\mathfrak{R})$, $A_3 \in \mathrm{M}_{n-r}(\mathfrak{R})$. By construction, $\operatorname{rk} A_1 = r$.

Notation. Let $M = \left(\begin{array}{c|c} M^{(1)} & M^{(2)} \\ \hline M^{(3)} & M^{(4)} \end{array}\right)$, where $1 \leq r < n$, $M^{(1)} \in \mathrm{M}_r(\mathfrak{R})$, $M^{(k)} = \left(m_{i,j}^{(k)}\right)$. for $1 \leq k \leq 4$. Take $1 \leq i_0, j_0 \leq n - r$, we write $\operatorname{Extr}_r(M; i_0, j_0)$ for the matrix

$$\operatorname{Extr}_r(M; i_0, j_0) = \left(\begin{array}{c|c} M^{(1)} & v \\ \hline w & m_{i_0,j_0}^{(4)} \end{array}\right) \in \mathrm{M}_{r+1}(\mathfrak{R}),$$

where $v = (m_{i,j_0}^{(2)})_{1 \leq i \leq r} \in \mathrm{M}_{r,1}(\mathfrak{R})$, $w = (m_{i_0,j}^{(3)})_{1 \leq j \leq r} \in \mathrm{M}_{1,r}(\mathfrak{R})$.

If $A_3 = (a_{i,j}^{(3)}) \neq \mathfrak{o}_r$, then there exist coordinates $1 \leq i_0, j_0 \leq n - r$ such that $a_{i_0,j_0}^{(3)} \neq 0$. But $\operatorname{Extr}_r(YAT - YBXD; i_0, j_0)$ is lower triangular and all its diagonal coefficients are nonzero. Therefore,

$$\operatorname{rk}(YAT - YBXD) \geq \operatorname{rk} \operatorname{Extr}_r(A; i_0, j_0) > r.$$

Consequently, by setting $Q = XDT^{-1}$, we obtain $\operatorname{rk}(A - BQ) > \operatorname{rk}(B) > 0$, which implies

$$\varphi_n(A - BQ) < \varphi_n(B).$$

From now on, we assume that $A_3 = \mathfrak{o}_r$. If $A_2 = (a_{i,j}^{(2)}) \neq \mathfrak{o}_{n-r,r}$, there exist some $1 \leq i_0 \leq n - r$ and $1 \leq j_0 \leq r$ such that $a_{i_0,j_0}^{(2)} \neq 0$. Take such a coefficient with the greatest column index j_0. Set $v = (v_j)_{1 \leq j \leq r} \in \mathrm{M}_{r,1}(\mathfrak{R})$ such that $v_{j_0} = -1$ and all other coefficients are equal to 0. Then define

$$Q' = \left(\begin{array}{c|c|c} \operatorname{diag}(\mu_1, \ldots, \mu_r) & v & \mathfrak{o}_{r,n-r-1} \\ \hline \multicolumn{3}{c}{\mathfrak{o}_{n-r,n}} \end{array}\right) \in \mathrm{M}_n(\mathfrak{R}),$$

so that the matrix $\operatorname{Extr}_r(YAT - YBXQ'; i_0, 1)$ has rank $r + 1$. Indeed, by exchanging the j_0-th and the $(r+1)$-th row of $\operatorname{Extr}_r(YAT - YBXQ'; i_0, 1)$, we

obtain a lower triangular matrix whose diagonal coefficients are all nonzero. In particular,

$$\operatorname{rk}(YAT - YBXQ') \geq \operatorname{rk}\operatorname{Extr}_r(YAT - YBXQ'; i_0, 1) > r.$$

It follows that $\operatorname{rk}(A - BQ) > r = \operatorname{rk} B$, for $Q = XQ'T^{-1}$, which implies

$$\varphi_n(A - BQ) < \varphi_n(B).$$

3. Now we can assume that $A_2 = \mathfrak{o}_{n-r,r}$ and $A_3 = \mathfrak{o}_r$. If $r = 1$, then we can apply Lemma 3.7 to find $Q' \in \mathrm{M}_n(\mathfrak{R})$ such that $YAT = YBXQ'$ or $\varphi_n(YAT - YBXQ') < \varphi_n(YBX)$. Set $Q = XQ'T^{-1}$, then

$$A = BQ \qquad \text{or} \qquad \varphi_n(A - BQ) < \varphi_n(B).$$

It remains to consider $r > 1$. We set $B_1 = \operatorname{diag}(b_1, \ldots, b_r) \in \mathrm{M}_r(\mathfrak{R})$. Thanks to Lemma 3.6, there exists $Q_1 \in \mathrm{M}_r(\mathfrak{R})$ such that for $R_1 = A_1 - B_1Q_1$, we have

$$R_1 = \mathfrak{o}_r \qquad \text{or} \qquad (\operatorname{rk} R_1 = r \quad \text{and} \quad \rho_r(R_1) < \rho_r(B_1)).$$

In any case, set

$$Q = X\left[\left(\begin{array}{c|c} Q_1 & \mathfrak{o}_{r,n-r} \\ \hline \mathfrak{o}_{n-r,r} & \mathfrak{o}_{n-r} \end{array}\right) + D\right] T^{-1},$$

then

$$A - BQ = Y^{-1}\left(\begin{array}{c|c} R_1 & \mathfrak{o}_{r,n-r} \\ \hline \mathfrak{o}_{n-r,r} & \mathfrak{o}_{n-r} \end{array}\right) T^{-1}.$$

If $R_1 = \mathfrak{o}_r$, then $A = BQ$. If $R_1 \neq \mathfrak{o}_r$, then $\operatorname{rk} R_1 = r$, so

$$\varphi_n(A - BQ) = (n - r)\omega^n + \rho_r(R_1) < (n - r)\omega^n + \rho_r(B_1) = \varphi_n(B).$$

□

4. The Euclidean property for matrix algebras over a PIR

The aim of this section will be to prove the following property.

Theorem 4.1. *Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. Then $\mathrm{M}_n(\mathfrak{R})$ is right and left Euclidean if and only if $\mathfrak{R}$ is a principal ideal ring.*

4.1. Some general properties of Euclidean and principal ideal rings.

A PIR $\mathfrak{R}$ is said to be *special* if $\mathfrak{R}$ has a unique prime ideal and this ideal is nilpotent. To infer Theorem 4.1 from Theorem 3.1, we will use the following property due to Samuel and Zariski.

Proposition 4.2 ([ZS75, Theorem 33, p. 245])**.** *Let $\mathfrak{R}$ be a PIR, then it can be written as a direct product $\mathfrak{R} = \prod_{i=1}^{l} \mathfrak{R}_i$, where each $\mathfrak{R}_i$ is a PID or a special PIR.*

Special PIRs can be easily dealt with.

Lemma 4.3. *Let $\mathfrak{S}$ be a special PIR. Then for any $n \in \mathbf{Z}_{\geq 1}$, $\mathrm{M}_n(\mathfrak{S})$ is Euclidean, and $e(\mathrm{M}_n(\mathfrak{S})) < \omega$.*

Proof. Let $\mathfrak{p}$ be the prime ideal of $\mathfrak{S}$. Take $m \in \mathbf{Z}_{>0}$ such that $\mathfrak{p}^m = 0$. We prove that the function $\psi_n : \left\{ \begin{array}{ccc} \mathrm{M}_n(\mathfrak{S})^\bullet & \longrightarrow & \{0, 1, \ldots, m-1\} \\ M & \longmapsto & v_\mathfrak{p} \circ \det(M) \end{array} \right.$ is a right Euclidean stathm.

We know that $\mathfrak{S}$ is the homomorphic image of a PID $\mathfrak{R}$ (see [Hun68]). Consider a surjective homomorphism $\pi : \mathfrak{R} \longrightarrow \mathfrak{S}$, which we extend to a surjective homomorphism $\pi : \mathrm{M}_n(\mathfrak{R}) \longrightarrow \mathrm{M}_n(\mathfrak{S})$.

Take A, $B \in \mathrm{M}_n(\mathfrak{S})$, $B \neq \mathfrak{o}_n$. There exist $\hat{A}$, $\hat{B} \in \mathrm{M}_n(\mathfrak{R})$ such that $\pi(\hat{A}) = A$ and $\pi(\hat{B}) = B$. Besides, there exist $\hat{D}$, $\hat{A}'$, $\hat{B}' \in \mathrm{M}_n(\mathfrak{R})$ such that $\hat{A} = \hat{D}\hat{A}'$, $\hat{B} = \hat{D}\hat{B}'$, and $\hat{A}'\mathrm{M}_n(\mathfrak{R}) + \hat{B}'\mathrm{M}_n(\mathfrak{R}) = \mathrm{M}_n(\mathfrak{R})$. Set $D = \pi(\hat{D})$, $A' = \pi(\hat{A}')$, and $B' = \pi(\hat{B}')$. Then we have

$$A = DA', \quad B = DB', \quad \text{and } A'\mathrm{M}_n(\mathfrak{S}) + B'\mathrm{M}_n(\mathfrak{S}) = \mathrm{M}_n(\mathfrak{S}).$$

But $\mathrm{sr}\,\mathfrak{S} = 1$, so $\mathrm{sr}\,\mathrm{M}_n(\mathfrak{S}) = 1$, and there exists $Q' \in \mathrm{M}_n(\mathfrak{S})$ such that $U = A' - B'Q' \in \mathrm{GL}_n(\mathfrak{S})$.

If $v_\mathfrak{p} \circ \det(B') > 0$, set $Q = Q'$, then

$$v_\mathfrak{p} \circ \det(A - BQ) = v_\mathfrak{p} \circ \det(DU) = v_\mathfrak{p} \circ \det D < v_\mathfrak{p} \circ \det(DB') = v_\mathfrak{p} \circ \det B.$$

If $v_\mathfrak{p} \circ \det(B') = 0$, then $B' \in \mathrm{GL}_n(\mathfrak{S})$. Set $Q = B'^{-1}A'$, we have $A - BQ = \mathfrak{o}_n$. □

Lemma 4.4. *Let $l \in \mathbf{Z}_{\geq 1}$ and $\mathfrak{A}_i$, $1 \leq i \leq l$ be right Euclidean rings. Then the product ring $\prod_{i=1}^{l} \mathfrak{A}_i$ is a right Euclidean ring.*

Proof. You can refer to [Sam71, Proposition 6] or [Cla15, Theorem 3.13], where the commutativity hypothesis is not used. We give some details to get some insight into Remark 4.5. Note that an immediate induction shows that it is enough to consider the product of two right Euclidean rings $\mathfrak{A}_1$ and $\mathfrak{A}_2$. In that case, we consider two right Euclidean stathms $\varphi_i : \mathfrak{A}_i^\bullet \longrightarrow \mathcal{O}$, extended at 0 as in (5), for $i = 1, 2$, and we can prove that

$$\varphi : \left\{ \begin{array}{ccc} (\mathfrak{A}_1 \times \mathfrak{A}_2)^\bullet & \longrightarrow & \mathcal{O} \\ (r_1, r_2) & \longmapsto & \varphi_1(r_1) \oplus \varphi_2(r_2) \end{array} \right.$$

is a right Euclidean stathm. □

In fact, we also have the following property.

Remark 4.5 ([Cla15, Theorem 3.40[6]]). With the above hypotheses,

$$\sum_{i=1}^{l} e(\mathfrak{A}_i) \leq e\left(\prod_{i=1}^{l} \mathfrak{A}_i\right) \leq \bigoplus_{i=1}^{l} e(\mathfrak{A}_i).$$

The upper bound, which is easily implied by the proof of Lemma 4.4 above, has the following consequence: if for any i, $\mathfrak{A}_i$ is right Euclidean and $e(\mathfrak{A}_i) < \omega$), then $\prod_{i=1}^{l} \mathfrak{A}_i$ is also right Euclidean and $e\left(\prod_{i=1}^{l} \mathfrak{A}_i\right) < \omega$.

[6]As in Footnote 5, Clark sets himself in a commutative context, but this property does not rely on the commutative hypothesis.

4.2. **Proof of Theorem 4.1.** Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. If $\mathrm{M}_n(\mathfrak{R})$ is right Euclidean, then every right ideal of $\mathrm{M}_n(\mathfrak{R})$ is principal. Therefore, thanks to Proposition 2.5, $\mathfrak{R}$ is a PIR.

Conversely, assume that $\mathfrak{R}$ is a PIR. Thanks to Proposition 4.2, $\mathfrak{R}$ can be written as $\mathfrak{R} = \prod_{i=1}^{l} \mathfrak{R}_i$, such that for any $1 \leq i \leq l$, $\mathfrak{R}_i$ is either a PID or a special PIR. But now, $\mathrm{M}_n(\mathfrak{R})$ is isomorphic to $\prod_{i=1}^{l} \mathrm{M}_n(\mathfrak{R}_i)$. Thanks to Theorem 3.1 and Lemma 4.3, for any $1 \leq i \leq l$, $\mathrm{M}_n(\mathfrak{R}_i)$ is Euclidean. Using Lemma 4.4, we can conclude that $\prod_{i=1}^{l} \mathrm{M}_n(\mathfrak{R}_i)$ is Euclidean. □

5. Effectivity

5.1. **General result.** The fact that a ring $\mathfrak{A}$ is right Euclidean for some right Euclidean stathm $\varphi : \mathfrak{A}^\bullet \longrightarrow \mathcal{O}$ does not mean that we know how to compute a quotient (or equivalently a remainder) for each pair $(a, b) \in \mathfrak{A} \times \mathfrak{A}^\bullet$, that is to say an element $q \in \mathfrak{A}$ such that

$$a = bq \quad \text{or} \quad \varphi(a - bq) < \varphi(b).$$

Nevertheless, in the case when $\mathfrak{A} = \mathrm{M}_n(\mathfrak{R})$, with a further condition on $\mathfrak{R}$, we can effectively compute it. More precisely, we have the following property.

Proposition 5.1. *Let $n > 1$ and $\mathfrak{R}$ be a PID. The following statements are equivalent.*

(a) For any a, $b \in \mathfrak{R}$, we can compute $d = \gcd(a, b)$, and elements u, $v \in \mathfrak{R}$ such that $au + bv = d$.
(b) For any A, $B \in \mathrm{M}_n(\mathfrak{R})$, we can compute some $Q \in \mathrm{M}_n(\mathfrak{R})$ such that $\varphi_n(A - BQ) < \varphi_n(B)$.

Proof. Assuming (a), a careful reading of the proof in Section 3 shows that we may compute (b). Indeed, all constructions rely on gcds (see Remark 2.8), and reduction of matrices into echelon form or Smith normal form. These reductions can be explicitly computed assuming (a).

Conversely, take a, $b \in \mathfrak{R}$. Set $A = \mathrm{diag}(1, \ldots, 1, a) \in \mathrm{M}_n(\mathfrak{R})$ and $B = \mathrm{diag}(1, \ldots, 1, b) \in \mathrm{M}_n(\mathfrak{R})$. As we can compute quotients (and remainders) of Euclidean divisions in $\mathrm{M}_n(\mathfrak{R})$, we can apply the Euclidean algorithm to A and B:

Algorithm 5.2. Input: $A, B \in \mathrm{M}_n(\mathfrak{R})$.
Set $D = A$, $U = \mathbf{1}_n$, $V = \mathfrak{o}_n$, $D_1 = B$, $U_1 = \mathfrak{o}_n$, $V_1 = \mathfrak{1}_n$.

(i) If $D_1 = \mathfrak{o}_n$, return $[U, V, D]$.
(ii) Compute $Q, R \in \mathrm{M}_n(\mathfrak{R})$ such that $D = D_1 Q + R$. Set

$$(D, U, V, D_1, U_1, V_1) = (D_1, U_1, V_1, R, U - U_1 Q, V - V_1 Q)$$

and go to Step (i).

We obtain U, $V \in \mathrm{M}_n(\mathfrak{R})$ such that

$$AU + BV = D, \tag{8}$$

where D is a gcld of A and B in $\mathrm{M}_n(\mathfrak{R})$. But a gcld of A and B is $\mathrm{diag}(1, \ldots, 1, d)$ where d is a gcd of a and b. Therefore, there exists $T \in \mathrm{GL}_n(\mathfrak{R})$ such that $D = \mathrm{diag}(1, \ldots, 1, d)T$. In particular, $\det D = d\varepsilon$ for

some $\epsilon \in \mathfrak{R}^\times$. We replace d by $d\varepsilon$ such that $\det D = d$. Then, denoting by C the cofactor matrix of D, (8) implies that

$$AUC^\mathsf{T} + BVC^\mathsf{T} = dI_n.$$

Identifying the coefficients in position (n, n), we obtain $au + bv = d$. □

5.2. **Computation of gcd of matrices, an example.** It is straightforward to remark that Algorithm 5.2 above will return a gcld of A and B in a finite number of steps. We can similarly compute gcrds.

The following example illustrates such computations, and the fact that gcrd and gcld may be unconnected.

Example 5.3. In $\mathrm{M}_3(\mathbf{Z})$, consider the matrices

$$A = \begin{pmatrix} -1 & 1 & 0 \\ 2 & -2 & 0 \\ -1 & -1 & 2 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} -1 & -1 & -1 \\ 2 & 2 & 2 \\ 2 & 1 & 0 \end{pmatrix}.$$

Then $A = B \begin{pmatrix} -2 & 0 & 2 \\ 3 & -1 & -2 \\ 0 & 0 & 0 \end{pmatrix}$, therefore a gcld for A and B is B, which has rank 2. Besides,

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{pmatrix} B + \begin{pmatrix} -1 & 1 & 0 \\ 4 & -1 & 0 \\ -1 & -1 & 2 \end{pmatrix},$$

$$B = \begin{pmatrix} 2 & 1 & 1 \\ -7 & -3 & -4 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 & 0 \\ 4 & -1 & 0 \\ -1 & -1 & 2 \end{pmatrix} + \begin{pmatrix} -2 & -1 & -3 \\ 3 & 2 & 10 \\ 2 & 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} -1 & 1 & 0 \\ 4 & -1 & 0 \\ -1 & -1 & 2 \end{pmatrix} = \begin{pmatrix} 10 & 3 & 5 \\ -20 & -6 & -9 \\ -4 & -1 & -3 \end{pmatrix} \begin{pmatrix} -2 & -1 & -3 \\ 3 & 2 & 10 \\ 2 & 1 & 0 \end{pmatrix}.$$

Consequently, a gcrd of A and B is $\begin{pmatrix} -2 & -1 & -3 \\ 3 & 2 & 10 \\ 2 & 1 & 0 \end{pmatrix}$, which has rank 3.

Remark 5.4. In a PID $\mathfrak{R}$, under the effectivity conditions of Proposition 5.1, there is a more direct way to compute gclds and gcrds of matrices in $\mathrm{M}_n(\mathfrak{R})$. Indeed, given $A, B \in \mathrm{M}_n(\mathfrak{R})$, we can proceed as follows. Consider the matrix $\left(A \,\middle|\, B\right) \in \mathrm{M}_{n,2n}(\mathfrak{R})$ and compute $R \in \mathrm{M}_n(\mathfrak{R})$, $U \in \mathrm{GL}_{2n}(\mathfrak{R})$ such that

$$\left(A \,\middle|\, B\right) U = \left(\mathfrak{o}_n \,\middle|\, R\right).$$

Then R is a gcld of A and B.

Likewise, we can compute $V \in \mathrm{GL}_{2n}(\mathfrak{R})$, $S \in \mathrm{M}_n(\mathfrak{R})$ such that

$$\left(A^\mathsf{T} \,\middle|\, B^\mathsf{T}\right) V = \left(\mathfrak{o}_n \,\middle|\, S\right),$$

then S^T is a gcrd of A and B.

5.3. **Continued fractions.** Let $\mathfrak{R}$ be an integral domain, set $\mathfrak{F}$ to be the field of fractions of $\mathfrak{R}$. For $k \in \mathbf{Z}_{>0}$ and given $Q_1, \dots, Q_k \in \mathrm{M}_n(\mathfrak{R})$, we define the continued fraction $[Q_1, \dots, Q_k]$ as follows:

$$[Q_1] = Q_1,$$
$$[Q_1, Q_2, \dots, Q_k] = Q_1 + [Q_2, \dots, Q_k]^{-1}, \quad \text{if } [Q_2, \dots, Q_k] \in \mathrm{GL}_n(\mathfrak{F}).$$

Remark that $[Q_1, \dots, Q_k]$ is defined if and only if $Q_k \in \mathrm{GL}_n(\mathfrak{F})$, $[Q_{k-1}, Q_k] \in \mathrm{GL}_n(\mathfrak{F})$, ..., and $[Q_2, \dots, Q_k] \in \mathrm{GL}_n(\mathfrak{F})$.

It is clear that any continued fraction $[Q_1, \dots, Q_k]$ is an element of $\mathrm{M}_n(\mathfrak{F})$, actually the converse holds in a PID.

Proposition 5.5. *Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$, set $\mathfrak{F}$ to be the field of fractions of $\mathfrak{R}$. Then for any $X \in \mathrm{M}_n(\mathfrak{F})$, there exist $k \in \mathbf{Z}_{>0}$ and $Q_1, \dots, Q_k \in \mathrm{M}_n(\mathfrak{R})$ such that $X = [Q_1, \dots, Q_k]$.*

Remark. This result is false for $n = 1$, take for instance $\mathfrak{R} = \mathbf{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, see [Coo76, Proposition 1 and Example p. 139]. Besides, we will obtain a more precise result (Corollary 7.14).

Proof of Proposition 5.5. If $X = \mathfrak{o}_n$, then $X = [\mathfrak{o}_n]$. From now on, assume $X \neq \mathfrak{o}_n$. Each coefficient of X can be written as $\frac{a_{i,j}}{b_{i,j}}$, with $a_{i,j}, b_{i,j} \in \mathfrak{R}$. Take b to be a lowest common multiple of the family of denominators $\{b_{i,j},\ 1 \leq i, j \leq n\}$. Then set $B = b \cdot \mathfrak{1}_n \in \mathrm{M}_n(\mathfrak{R})$, $A = BX \in \mathrm{M}_n(\mathfrak{R})$.

$\mathrm{M}_n(\mathfrak{R})$ is a Euclidean ring with respect to the Euclidean stathm φ_n, $B \neq \mathfrak{o}_n$, so by repeating divisions, we find $k \in \mathbf{Z}_{>0}$, $Q_1, \dots, Q_k, R_1, \dots, R_k \in \mathrm{M}_n(\mathfrak{R})$ such that we have the following division chain:

$$\text{(9)} \qquad \begin{cases} A - BQ_1 = R_1, \\ B - R_1Q_2 = R_2, \\ \vdots \\ R_{k-2} - R_{k-1}Q_k = R_k, \end{cases}$$

$$\text{(10)} \qquad \begin{gathered} \text{with } R_k = \mathfrak{o}_n, \text{ for all } 1 \leq i < k,\ R_i \neq 0, \text{ and} \\ \varphi_n(R_{k-1}) < \varphi_n(R_{k-2}) < \cdots < \varphi_n(R_1) < \varphi_n(B). \end{gathered}$$

But B has rank n, so (10) implies that for all $1 \leq i < k$, R_i has also rank n, i.e.

$$\text{(11)} \qquad R_k = 0 \qquad \text{and} \qquad R_i \in \mathrm{GL}_n(\mathfrak{F}), \qquad \text{for all } 1 \leq i < k.$$

We prove by induction on k that for any division chain satisfying conditions (9) and (11), we have

$$A = B[Q_1, \dots, Q_k].$$

If $k = 1$, then $A = B[Q_1]$. If $k > 1$, then $Q_2, \dots, Q_k$, $R_2, \dots, R_k$ provide a division chain satisfying conditions (9) and (11) starting from B, R_1. So, by induction hypothesis, $B = R_1[Q_2, \dots, Q_k]$. But $R_1, B \in \mathrm{GL}_n(\mathfrak{F})$, so $[Q_2, \dots, Q_k] \in \mathrm{GL}_n(\mathfrak{F})$ and $R_1 = B[Q_2, \dots, Q_k]^{-1}$. Then $R_1 = A - BQ_1$, therefore $A = B(Q_1 + [Q_2, \dots, Q_k]^{-1})$, and we obtain $A = B[Q_1, \dots, Q_k]$ as expected.

If follows that $X = B^{-1}A = [Q_1, \dots, Q_k]$, which completes the proof. □

If we suppose that the effectivity conditions of Proposition 5.1 hold, then every step in the proof above is explicit.

Example 5.6. Take $\mathfrak{R} = \mathbf{Q}[x]$, consider $X = \begin{pmatrix} 1/x & 0 \\ 2/(x+3) & 3 \end{pmatrix} \in \mathrm{M}_2(\mathbf{Q}(x))$.

Then write $B = x(x+3) \cdot \mathtt{1}_2$, $A = \begin{pmatrix} x+3 & 0 \\ 2x & 3x(x+3) \end{pmatrix}$. We have the following division chain

$$\begin{cases} A - BQ_1 = \begin{pmatrix} x+3 & x^2+3x \\ 2x & 3x^2+9x \end{pmatrix}, \\ B - \begin{pmatrix} x+3 & x^2+3x \\ 2x & 3x^2+9x \end{pmatrix} Q_2 = \begin{pmatrix} \frac{-x^3}{3} - x^2 + x + 3 & \frac{x^3}{6} + x^2 + x - \frac{3}{2} \\ \frac{-2x^3}{3} - 2x^2 + 2x & \frac{x^3}{3} + 2x^2 + 2x \end{pmatrix}, \\ \begin{pmatrix} x+3 & x^2+3x \\ 2x & 3x^2+9x \end{pmatrix} - \begin{pmatrix} \frac{-x^3}{3} - x^2 + x + 3 & \frac{x^3}{6} + x^2 + x - \frac{3}{2} \\ \frac{-2x^3}{3} - 2x^2 + 2x & \frac{x^3}{3} + 2x^2 + 2x \end{pmatrix} Q_3 = \mathtt{0}_2, \end{cases}$$

$$\text{where } Q_1 = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} \frac{x^2}{2} + x - 1 & -\frac{x^2}{6} - \frac{x}{2} + \frac{1}{2} \\ 0 & 0 \end{pmatrix},$$

$$Q_3 = \begin{pmatrix} \frac{x}{3} + 1 & -\frac{x^3}{18} - \frac{x^2}{3} - \frac{x}{3} + \frac{3}{2} \\ \frac{2x}{3} & \frac{-x^3}{9} - \frac{x^2}{3} + \frac{x}{3} + 3 \end{pmatrix}.$$

Therefore, $X = [Q_1, Q_2, Q_3]$. It may seem that such a short continued fraction decomposition was obtained by sheer luck, but Remark 7.12 will explain this behavior.

6. Euclidean order type of matrix algebras

Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$. The Euclidean stathm φ_n built for the proof of Theorem 3.1 satisfies $\varphi_n(0) \leq (n-1)\omega^n + \omega$. Therefore, we have

$$e(\mathrm{M}_n(\mathfrak{R})) \leq (n-1)\omega^n + \omega. \tag{12}$$

The purpose of this section will be to obtain other information on the Euclidean order type $e(\mathrm{M}_n(\mathfrak{R}))$.

6.1. Lower bound on the Euclidean order type of matrix algebras.

Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$. If $\mathfrak{R}$ is not a field, we know that $e(\mathrm{M}_n(\mathfrak{R})) > \omega$ (see [Kal85, Theorem 2]), but we can improve this lower bound.

Proposition 6.1. *Let $\mathfrak{R}$ be a PID which is not a field, and $n \in \mathbf{Z}_{>1}$. Take any right Euclidean stathm $\chi : \mathrm{M}_n(\mathfrak{R})^\bullet \longrightarrow \mathcal{O}$. Then, for any $\alpha \in \mathbf{Z}_{>0}$, there exists $M_\alpha \in \mathrm{M}_n(\mathfrak{R})$ such that $\chi(M_\alpha) \geq (n-1)\omega + \alpha$. In particular, $e(\mathrm{M}_n(\mathfrak{R})) \geq n\omega$.*

Proof. Fix some $r \in \mathfrak{R}$, which is neither 0 nor a unit. Such an element exists because $\mathfrak{R}$ is not a field. Take $1 \leq i_0 \leq n$. For $\alpha \in \mathbf{Z}_{\geq 0}$, $r^{\alpha+1}\mathfrak{R} \subsetneq r^\alpha \mathfrak{R}$, which allows us to define the nonempty set

$$E_\alpha^{i_0} = \left\{ (m_{i,j})_{1 \leq i,j \leq n} \in \mathrm{M}_n(\mathfrak{R}), \begin{array}{l} \text{for any } 1 \leq i < i_0, 1 \leq j \leq n, \\ m_{i,j} = 0, \text{ and } m_{i_0,j} \in r^\alpha \mathfrak{R} \setminus r^{\alpha+1}\mathfrak{R} \end{array} \right\}.$$

For any i_0 and α, there exists some $T_{i_0,\alpha} \in E_\alpha^{i_0}$ such that

$$\chi(T_{i_0,\alpha}) = \min\left\{ \chi(X), X \in E_\alpha^{i_0} \right\}.$$

Fix i_0 and take $\alpha, \beta \in \mathbf{Z}_{\geq 0}$ such that $\alpha < \beta$. As $T_{i_0,\beta} \neq \mathfrak{o}_n$, there exists $Q \in \mathrm{M}_n(\mathfrak{R})$ such that

$$\chi(T_{i_0,\alpha} - T_{i_0,\beta}Q) < \chi(T_{i_0,\beta}).$$

But $T_{i_0,\alpha} - T_{i_0,\beta}Q \in E_\alpha^{i_0}$, therefore

$$\chi(T_{i_0,\alpha}) \leq \chi(T_{i_0,\alpha} - T_{i_0,\beta}Q) < \chi(T_{i_0,\beta}).$$

Thus, $(\chi(T_{i_0,\alpha}))_{\alpha \in \mathbf{Z}_{\geq 0}}$ is a strictly increasing sequence.

Take now $\alpha \in \mathbf{Z}_{\geq 0}$ and take $1 \leq i_0 < n$. As $T_{i_0+1,0} \neq \mathfrak{o}_n$, there exists $Q' \in \mathrm{M}_n(\mathfrak{R})$ such that

$$\chi(T_{i_0,\alpha} - T_{i_0+1,0}Q') < \chi(T_{i_0+1,0}).$$

But $T_{i_0,\alpha} - T_{i_0+1,0}Q' \in E_\alpha^{i_0}$, therefore

$$\chi(T_{i_0,\alpha}) \leq \chi(T_{i_0,\alpha} - T_{i_0+1,0}Q') < \chi(T_{i_0+1,0}).$$

In other words, $\chi(T_{i_0+1,0})$ is an upper-bound to $(\chi(T_{i_0,\alpha}))_{\alpha \in \mathbf{Z}_{\geq 0}}$.

A straightforward induction on i_0 proves that for any $1 \leq i_0 \leq n$ and for any $\alpha \in \mathbf{Z}_{\geq 0}$,

$$\chi(T_{i_0,\alpha}) \geq (i_0 - 1)\omega + \alpha.$$

Taking $M_\alpha = T_{n,\alpha}$ grants the result. □

Remark 6.2.
(1) The proof of Proposition 6.1 above relies on the existence of r which is neither a unit, nor a zero divisor. Therefore, the conclusion of Proposition 6.1 holds for any commutative ring $\mathfrak{R}$ which is not equal to its total quotient ring.
(2) The proof of Proposition 6.1 above is still valid if $\mathfrak{R}$ is a (not necessarily commutative) ring with no nontrivial zero divisors which is not a skew field.
(3) If $\mathfrak{F}$ is a (skew) field, then for any $n \in \mathbf{Z}_{\geq 1}$, the function

$$\chi_n : \left\{ \begin{array}{ccc} \mathrm{M}_n(\mathfrak{F})^\bullet & \longrightarrow & \{0, 1, \ldots, n\} \\ M & \longmapsto & n + 1 - \operatorname{rk} M \end{array} \right.$$

is a left and right Euclidean stathm[7], so $e(\mathrm{M}_n(\mathfrak{F})) < \omega$.
(4) If $\mathfrak{R}$ is a special PIR (e.g. $\mathfrak{R} = \mathbf{Z}/4\mathbf{Z}$, $\mathfrak{R} = \mathbf{R}[X]/(X^2+1)^3$), then for any $n > 1$, $e(\mathrm{M}_n(\mathfrak{R})) < \omega$ (see Lemma 4.3).

Proposition 6.3. *Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. Then $\mathrm{M}_n(\mathfrak{R})$ is right Euclidean and satisfies $e(\mathrm{M}_n(\mathfrak{R})) < \omega$ if and only if $\mathfrak{R}$ is a direct product of fields and of special PIRs.*

Proof. Assume that $\mathfrak{R} = \prod_{i=1}^l \mathfrak{R}_i$ where for any i, $\mathfrak{R}_i$ is a field or a special PIR. For any $1 \leq i \leq l$, $e(\mathrm{M}_n(\mathfrak{R}_i)) < \omega$ (see Remark 6.2(3) and Lemma 4.3). So, thanks to Remark 4.5, $e(\mathrm{M}_n(\mathfrak{R})) < \omega$.

Conversely, assume that $\mathrm{M}_n(\mathfrak{R})$ admits the right Euclidean stathm $\varphi : \left\{ \begin{array}{ccc} \mathrm{M}_n(\mathfrak{R})^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & \varphi(M) \end{array} \right.$. First remark that $\mathfrak{R}$ is a PIR thanks to Proposition 2.5. Then, we apply Proposition 4.2, so that $\mathfrak{R}$ can be written as a product $\mathfrak{R} = \prod_{i=1}^l \mathfrak{R}_i \times \prod_{i=1}^m \mathfrak{S}_i$, where for any i, $\mathfrak{R}_i$ is a PID and $\mathfrak{S}_i$ is

[7]When $\mathfrak{R} = \mathfrak{F}$ is a field, ℓ takes only the values 0 and 1 and the invariant factors are trivial: Smith normal form is uniquely determined by the rank. In the noncommutative case, you can adapt the proof or see [Bru73, Corollary to Theorem 1].

a special PIR. If there exists some $1 \leq i_0 \leq l$ such that $\mathfrak{R}_{i_0}$ is not a field, then define the ring $\mathfrak{S}$ such that $\mathfrak{R} = \mathfrak{R}_{i_0} \times \mathfrak{S}$, and we can prove that the following function

$$\psi : \left\{ \begin{array}{ccc} \mathrm{M}_n(\mathfrak{R}_{i_0})^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & \inf_{S \in \mathrm{M}_n(\mathfrak{S})} \varphi(M,S) \end{array} \right.$$

is a right Euclidean stathm. It follows that $e(\mathrm{M}_n(\mathfrak{R}_{i_0})) \leq e(\mathrm{M}_n(\mathfrak{R}))$. If $e(\mathrm{M}_n(\mathfrak{R})) < n\omega$, it contradicts Proposition 6.1. □

Let us notice that we have proved that for any $n \in \mathbf{Z}_{>1}$, there exists no commutative ring $\mathfrak{R}$ such that $\omega \leq e(\mathrm{M}_n(\mathfrak{R})) < n\omega$.

6.2. **General bounds for the Euclidean order type of matrix algebras.** We combine the above results to obtain.

Proposition 6.4. *Let $\mathfrak{R}$ be a PIR, $n \in \mathbf{Z}_{>1}$, and $l, m \in \mathbf{Z}_{\geq 0}$ such that $\mathfrak{R} = \prod_{i=1}^{l} \mathfrak{R}_i \times \prod_{i=1}^{m} \mathfrak{S}_i$, where for each i, $\mathfrak{R}_i$ is a PID but not a field, and $\mathfrak{S}_i$ is a special PIR or a field. Then $\mathrm{M}_n(\mathfrak{R})$ is right Euclidean and*

$$ln\omega \leq e(\mathrm{M}_n(\mathfrak{R})) < l(n-1)\omega^n + (l+1)\omega.$$

Proof. Just apply Equation (12), Remark 4.5 and Proposition 6.1. □

Notice that the bounds still hold for $l = 0$, but the upper bound is false in general for $n = 1$ (even with the assumption that $\mathfrak{R}$ is Euclidean).

6.3. **Euclidean order type of matrix algebras over Euclidean rings.** We will build another Euclidean stathm, which provides another upper bound on $e(\mathrm{M}_n(\mathfrak{R}))$.

Proposition 6.5. *Let $\mathfrak{R}$ be a integral domain which is Euclidean and $n \in \mathbf{Z}_{\geq 1}$. Then $\mathrm{M}_n(\mathfrak{R})$ is a Euclidean ring and $e(\mathrm{M}_n(\mathfrak{R})) \leq n \otimes e(\mathfrak{R})$.*

Proof. Let $\varphi : \mathfrak{R}^\bullet \longrightarrow \mathcal{O}$ be a Euclidean stathm. If required, we replace φ by $\hat{\varphi} : \left\{ \begin{array}{ccc} \mathfrak{R}^\bullet & \longrightarrow & \mathcal{O} \\ r & \longmapsto & \inf\{\varphi(ru), u \in \mathfrak{R}^\times\} \end{array} \right.$ so that φ is invariant under multiplication by units. Then, for any $n \geq 1$, the following function is well-defined:

$$\psi_n : \left\{ \begin{array}{ccc} \mathrm{M}_n(\mathfrak{R})^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & [(n - \operatorname{rk} M) \otimes \varphi(0)] \oplus \varphi\left(\prod_{i=1}^{\operatorname{rk} M} b_i\right) \text{ if} \\ & & b_1, b_2, \ldots, b_{\operatorname{rk} M} \text{ are the invariant factors of } M. \end{array} \right.$$

We will prove by induction on $n \geq 1$ that ψ_n is a Euclidean stathm. Since $\psi_n(0) \leq n \otimes \varphi(0)$, this will imply that $e(\mathrm{M}_n(\mathfrak{R})) \leq n \otimes e(\mathfrak{R})$.

First, $\psi_1 = \varphi$ is a Euclidean stathm. Fix now $n > 1$, and assume that for all $1 \leq l < n$, ψ_l is a Euclidean stathm. Consider $A, B \in \mathrm{M}_n(\mathfrak{R})$, $B \neq 0$. Write $r = \operatorname{rk} B \geq 1$. Take $X, Y \in \mathrm{GL}_n(\mathfrak{R})$ such that $YBX = \operatorname{diag}(b_1, \ldots, b_r, 0, \ldots, 0)$, such that $b_1 | b_2 | \ldots | b_r \neq 0$. Set $YA = (a_{i,j})_{1 \leq i,j \leq n}$.

Assume that $r < n$. If there exists $1 \leq i, j \leq n$ such that $i > r$ or $j > r$, then we saw in the proof of Proposition 3.2, in Section 3.5 that there exists $Q \in \mathrm{M}_n(\mathfrak{R})$ such that $\operatorname{rk}(A - BQ) > \operatorname{rk} B$. Therefore, $\psi_n(A - BQ) < \psi_n(B)$. Consequently, we may assume that for all $1 \leq i, j \leq n$, such that $i > r$ or $j > r$, we have $a_{i,j} = 0$. Let $A' = (a_{i,j})_{1 \leq i,j \leq r}, B' = \operatorname{diag}(b_1, \ldots, b_r) \in \mathrm{M}_r(\mathfrak{R})$. By the induction hypothesis, there exists $Q' \in$

$\mathrm{M}_r(\mathfrak{R})$ such that $A' = B'Q'$ or $\psi_r(A' - B'Q') < \psi_r(B')$. Set $Q \in \mathrm{M}_n(\mathfrak{R})$ such that $XQ = \left(\begin{array}{c|c} Q' & \mathfrak{o}_{r,n-r} \\ \hline \mathfrak{o}_{n-r,r} & \mathfrak{o}_{n-r} \end{array}\right)$, we obtain

$$A = BQ \text{ or } \psi_n(A - BQ) < \psi_n(B).$$

Now, we can assume that $r = n$. Take $T \in \mathrm{GL}_n(\mathfrak{R})$ such that YAT is lower triangular and write $YAT = \left(\begin{array}{c|c} a_1 & \mathfrak{o}_{1,n-1} \\ \hline a_2 & \\ \vdots & A' \\ a_n & \end{array}\right)$, where $A' = (a'_{i,j})_{1 \leq i,j < n} \in \mathrm{M}_{n-1}(\mathfrak{R})$. Now we perform the Euclidean division of $a_1 \prod_{i=2}^n b_i$ by $\prod_{i=1}^n b_i$: there exists $\lambda \in \mathfrak{R}$ such that

$$a_1 = \lambda b_1 \text{ or } \varphi\left((a_1 - \lambda b_1)\prod_{i=2}^n b_i\right) < \varphi\left(\prod_{i=1}^n b_i\right) = \psi_n(B).$$

Define $\lambda^\star = \lambda$ if $a_1 \neq \lambda b_1$, and $\lambda^\star = \lambda - 1$ else. Set the lower triangular matrix $\hat{A} = \mathrm{diag}(a_1 - \lambda^\star b_1, 1, \ldots, 1) \cdot A'$ and $\hat{B} = \mathrm{diag}\,(b_2(a_1 - \lambda^\star b_1), b_3, \ldots, b_n) \in \mathrm{M}_{n-1}(\mathfrak{R})^\bullet$, with $\mathrm{rk}\,\hat{B} = n-1$. By the induction hypothesis, we may perform the Euclidean division of $\hat{A}$ by $\hat{B}$: there exists $\hat{Q} \in \mathrm{M}_{n-1}(\mathfrak{R})$ such that

$$\hat{A} = \hat{B}\hat{Q} \text{ or } \psi_{n-1}(\hat{A} - \hat{B}\hat{Q}) < \psi_{n-1}(\hat{B}).$$

Assume first that $\hat{A} \neq \hat{B}\hat{Q}$. Then $\psi_{n-1}(\hat{A} - \hat{B}\hat{Q}) < \varphi(0)$, so that $\hat{A} - \hat{B}\hat{Q}$ has rank $n-1$. Besides,

$$\varphi(\det(\hat{A} - \hat{B}\hat{Q})) = \psi_{n-1}(\hat{A} - \hat{B}\hat{Q}) < \psi_{n-1}(\hat{B}) = \varphi(\det \hat{B}) \leq \psi_n(B).$$

But $\det(\hat{A} - \hat{B}\hat{Q}) = (a_1 - \lambda^\star b_1)\det(A' - \mathrm{diag}(b_2, \ldots, b_n)\hat{Q})$, and setting $Q \in \mathrm{M}_n(\mathfrak{R})$ such that $X^{-1}QT = \left(\begin{array}{c|c} \lambda^\star & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & \hat{Q} \end{array}\right)$, we have

$$\begin{aligned} \det(YAT - YBQT) &= (a_1 - \lambda^\star b_1)\det(A' - \mathrm{diag}(b_2, \ldots, b_n)\hat{Q}), \\ &= \det(\hat{A} - \hat{B}\hat{Q}) \neq 0. \end{aligned}$$

Consequently,

$$\psi_n(A - BQ) = \varphi\left((a_1 - \lambda^\star b_1)\det(A' - \mathrm{diag}(b_2, \ldots, b_n)\hat{Q})\right) < \psi_n(B).$$

Suppose now that $\hat{A} = \hat{B}\hat{Q}$. Then we also have $A' = \mathrm{diag}(b_2, \ldots, b_n)\hat{Q}$. We distinguish two cases. First, assume that $a_1 - b_1\lambda \neq 0$. Setting $Q \in \mathrm{M}_n(\mathfrak{R})$ such that

$$X^{-1}QT = \left(\begin{array}{c|c} \lambda^\star & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & \hat{Q} - \mathfrak{1}_{n-1} \end{array}\right),$$

we obtain $\det(YAT - YBQT) = (a_1 - \lambda b_1)\prod_{i=2}^n b_i$. Then

$$\psi_n(A - BQ) = \varphi(\det(A - BQ)) < \psi_n(B).$$

Now, assume that $a_1 = b_1\lambda$, i.e. $a_1 - \lambda^\star b_1 = b_1$, set $Q', T' \in \mathrm{M}_n(\mathfrak{R})$ such that

$$T' = \left(\begin{array}{cc|c} 1 & 1 & \mathfrak{o}_{2,n-2} \\ 0 & 1 & \\ \hline \mathfrak{o}_{n-2,2} & & \mathfrak{1}_{n-2} \end{array}\right) \quad \text{and} \quad X^{-1}Q'T = \left(\begin{array}{c|c|c} \lambda^\star & 1 & \mathfrak{o}_{1,n-2} \\ \hline \mathfrak{o}_{n-1,1} & & \hat{Q} \end{array}\right),$$

which allows us to define

$$\tilde{A} = YATT' - YBQ'TT' = \left(\begin{array}{cc|c} b_1 & 0 & \\ a_2 & a_2 & \\ \vdots & \vdots & \mathfrak{o}_{n,n-2} \\ a_n & a_n & \end{array}\right).$$

Then we apply what we did above to $\tilde{A}$ and YBX: either we find some $\hat{Q}' \in \mathrm{M}_{n-1}(\mathfrak{R})$ such that

$$\left(\begin{array}{c|c} a_2 & \\ a_3 & \\ \vdots & \mathfrak{o}_{n-1,n-2} \\ a_n & \end{array}\right) = \mathrm{diag}(b_2, \ldots, b_n)\hat{Q}',$$

or we find some $Q'' \in \mathrm{M}_n(\mathfrak{R})$ such that $\psi_n(\tilde{A} - YBXQ'') < \psi_n(B)$.

In the first case, write q' for the first column of $\hat{Q}'$ and set

$$Q = Q' + X\left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline q' & \hat{Q}' \end{array}\right) T'^{-1}T^{-1}.$$

Then $A = BQ$.

In the latter case, set $Q = Q' + XQ''T'^{-1}T^{-1}$, then $\psi_n(A - BQ) = \psi_n(\tilde{A} - YBXQ'') < \psi_n(B)$. □

Combining the above result with Proposition 6.1, we obtain immediately the following result.

Corollary 6.6. *Let $\mathfrak{R}$ be a integral domain which is Euclidean such that $e(\mathfrak{R}) = \omega$. Then for any $n \in \mathbf{Z}_{>0}$, $e(\mathrm{M}_n(\mathfrak{R})) = n\omega$.*

Actually, Samuel ([Sam71]) proved that if $\mathfrak{R}$ is a integral domain which is Euclidean and for any $x \in \mathfrak{R}^\bullet$, $\mathfrak{R}/\mathfrak{R}x$ is finite, then $e(\mathfrak{R}) \leq \omega$. We have an equality except when $\mathfrak{R}$ is a field ([Fle71]).

Example. Let $n \in \mathbf{Z}_{\geq 1}$,

$$e(\mathrm{M}_n(\mathbf{Z})) = e(\mathrm{M}_n(\mathbf{Q}[x])) = e(\mathrm{M}_n(\mathbf{Z}[i])) = n\omega.$$

6.4. **Euclidean order type of matrix algebras over a PID with finite residues.** Imitating Samuel, we can prove Corollary 6.6 without assuming $\mathfrak{R}$ to be Euclidean.

Proposition 6.7. *Let $\mathfrak{R}$ be a PID. If for any $x \in \mathfrak{R}^\bullet$, $\mathfrak{R}/x\mathfrak{R}$ is finite, then for any $n \in \mathbf{Z}_{>1}$, $\mathrm{M}_n(\mathfrak{R})$ is Euclidean and $e(\mathrm{M}_n(\mathfrak{R})) \leq n\omega$. If besides $\mathfrak{R}$ is not a field, then $e(\mathrm{M}_n(\mathfrak{R})) = n\omega$.*

Proof. Let us consider the smallest right Euclidean stathm $\theta : \mathrm{M}_n(\mathfrak{R})^\bullet \longrightarrow \mathcal{O}$. We prove by induction on $1 \leq r \leq n$ that

(13) if $x_1, \ldots, x_r \in \mathfrak{R}^\bullet$, then $\theta(\mathrm{diag}(x_1, \ldots, x_r, 0, \ldots, 0)) < (n - r + 1)\omega$.

For $r = n$, if such elements exist, consider $x_1, \ldots, x_n \in \mathfrak{R}^\bullet$ such that $D = \mathrm{diag}(x_1, \ldots, x_n)$ satisfies $\theta(D) \geq \omega$ and $\varphi_n(D)$ minimal. Then for any $A \in \mathrm{M}_n(\mathfrak{R})$, there exists $Q(A, D) \in \mathrm{M}_n(\mathfrak{R})$ such that $\varphi_n(A - DQ(A, D)) < \varphi_n(d)$. By definition of φ_n, we have $\mathrm{rk}(A - DQ(A, D)) = n$, so $A - DQ(A, D)$ is equivalent to a full-rank diagonal matrix $D' \in \mathrm{M}_n(\mathfrak{R})$ such

that $\varphi_n(D') < \varphi_n(D)$. Therefore, $\theta(A - DQ(A,D)) = \theta(D') < \omega$. Let $\mathcal{S} \subseteq \mathrm{M}_n(\mathfrak{R}) \setminus D\mathrm{M}_n(\mathfrak{R})$ such that $\mathcal{S} \cup \{0\}$ is a system of representatives of $\mathrm{M}_n(\mathfrak{R})/D\mathrm{M}_n(\mathfrak{R})$, then Lemma 2.10 implies that

$$\theta(D) \leq \sup_{A \in \mathcal{S}} \theta(A - DQ(A,D)) + 1.$$

As $\mathcal{S}$ is finite, this implies that $\theta(D) < \omega$. This contradicts our hypothesis. Therefore (13) holds for $r = n$. We will prove (13) for $r = r_0 - 1$.

Now let us assume that we have some $1 < r_0 \leq n$, such that for all $r_0 \leq r \leq n$, (13) holds. Similarly, if such elements exist, consider $x_1, \ldots, x_{r_0-1} \in \mathfrak{R}^\bullet$ such that $D = \mathrm{diag}(x_1, \ldots, x_{r_0-1}, 0, \ldots, 0)$ satisfies $\theta(D) \geq (n - r_0 + 2)\omega$ and $\varphi_n(D)$ minimal. Consider now $A \in \mathrm{M}_n(\mathfrak{R})$. There exists $T \in \mathrm{GL}_n(\mathfrak{R})$ such that $A' = AT$ is lower triangular. If $A' = (a_{i,j})_{1 \leq i,j \leq n}$ admits a nonzero coefficient $a_{i,j}$ such that $i \geq r_0$ or $j \geq r_0$, we say that $A' \in \mathcal{S}_1$. We saw in the proof of Proposition 3.2 (on p. 14) that there exists $Q'(A,D) \in \mathrm{M}_n(\mathfrak{R})$ such that $A' - DQ'(A,D)$ has rank at least r_0. Therefore, by the induction hypothesis, $\theta(A' - DQ'(A,D)) < (n - r_0 + 1)\omega$.

If for all $1 \leq i,j \leq n$, $a'_{i,j} \neq 0$ implies $i,j < r_0$, then we say that $A' \in \mathcal{S}_2$. There exists $Q'(A,D) \in \mathrm{M}_n(\mathfrak{R})$ such that $A' = DQ'(A,D)$ or $\varphi_n(A' - DQ'(A,D)) < \varphi_n(d)$ and then $\mathrm{rk}(A' - DQ'(A,D)) \geq r_0 - 1$. Consequently, $\theta(A' - DQ'(A,D)) < (n - r_0 + 2)\omega$.

Let $\mathcal{S} \subseteq \mathrm{M}_n(\mathfrak{R}) \setminus D\mathrm{M}_n(\mathfrak{R})$ such that $\mathcal{S} \cup \{0\}$ is a system of representatives of $\mathrm{M}_n(\mathfrak{R})/D\mathrm{M}_n(\mathfrak{R})$. Then, thanks to Lemma 2.10, we have $\theta(D) \leq \sup_{a \in \mathcal{S}} \inf_{Q \in \mathrm{M}_n(\mathfrak{R})} \theta(A + DQ) + 1$. But for all $A \in \mathcal{S}$, there exists $T \in \mathrm{GL}_n(\mathfrak{R})$ such that $AT \in \mathcal{S}_1$ or $AT \in \mathcal{S}_2$, thus

$$\theta(D) \leq \sup_{\substack{A' \in \mathcal{S}_1 \cup \mathcal{S}_2 \\ T \in \mathrm{GL}_n(\mathfrak{R})}} \inf_{Q \in \mathrm{M}_n(\mathfrak{R})} \theta(A'T^{-1} + DQ) + 1.$$

But for all $A', Q \in \mathrm{M}_n(\mathfrak{R})$, $T \in \mathrm{GL}_n(\mathfrak{R})$, $\theta(A'T^{-1} + DQ) = \theta(A' + DQT)$ (see Remark 2.9) and then

(14)
$$\theta(D) \leq \sup\left(\sup_{A' \in \mathcal{S}_1} \inf_{Q \in \mathrm{M}_n(\mathfrak{R})} \theta(A' + DQ), \sup_{A' \in \mathcal{S}_2} \inf_{Q \in \mathrm{M}_n(\mathfrak{R})} \theta(A' + DQ) \right) + 1.$$

For all $A' \in \mathcal{S}_1$, we have

$$\inf_{Q \in \mathrm{M}_n(\mathfrak{R})} \theta(A' + DQ) \leq \theta(A' + DQ'(A,D)) < (n - r_0 + 1)\omega.$$

Thus

$$\sup_{A' \in \mathcal{S}_1} \inf_{Q \in \mathrm{M}_n(\mathfrak{R})} \theta(A' + DQ) < (n - r_0 + 2)\omega. \tag{15}$$

For all $A' \in \mathcal{S}_2$, we have

$$\inf_{Q \in \mathrm{M}_n(\mathfrak{R})} \theta(A' + DQ) \leq \theta(A' + DQ'(A,D)) < (n - r_0 + 2)\omega.$$

But there are only finitely many cosets $A' + D\mathrm{M}_n(\mathfrak{R})$ with $A' \in \mathcal{S}_2$, therefore

$$\sup_{A' \in \mathcal{S}_1} \inf_{Q \in \mathrm{M}_n(\mathfrak{R})} \theta(A' + DQ) < (n - r_0 + 2)\omega. \tag{16}$$

So, by combining (14), (15), and (16), we obtain $\theta(D) < (n - r_0 + 2)\omega$ as expected.

Finally, consider any $A \in \mathrm{M}_n(\mathfrak{R})^\bullet$. The matrix A is equivalent to some diagonal matrix D. Thanks to (13), $\theta(D) < n\omega$, and Remark 2.9 implies that $\theta(A) = \theta(D)$. We conclude that $e(\mathrm{M}_n(\mathfrak{R})) = \theta(0) \leq n\omega$.

If $\mathfrak{R}$ is not a field, Proposition 6.1 proves that $e(\mathrm{M}_n(\mathfrak{R})) \geq n\omega$. □

Example. Let $n \in \mathbf{Z}_{>1}$. Then

$$e\left(\mathrm{M}_n\left(\mathbf{Z}\left[\frac{1+\sqrt{-19}}{2}\right]\right)\right) = n\omega.$$

7. k-stage Euclidean properties

In this section, we will study the Euclidean properties of matrix algebras for another generalization of the Euclidean notion, introduced by Cooke [Coo76].

7.1. **Definition and basic remarks.** Let $\mathfrak{A}$ be a ring. Let $f : \mathfrak{A} \longrightarrow \mathbf{Z}_{\geq 0}$ be a function such that for $\alpha \in \mathfrak{A}$, $f(\alpha) = 0$ if, and only if $\alpha = 0$.

Given a pair $(a, b) \in \mathfrak{A} \times \mathfrak{A}^\bullet$, and a positive integer k, we say that (a, b) is a *k-stage right Euclidean pair* with respect to f if there exists a *k-stage division chain* starting from (a, b), that is to say there exist $(q_i)_{1\leq i\leq k} \in \mathfrak{A}^k$ (the *quotients*) and $(r_i)_{1\leq i\leq k} \in \mathfrak{A}^k$ (the *remainders*) such that

$$\text{(17)} \qquad \begin{cases} a - bq_1 = r_1, \\ b - r_1q_2 = r_2, \\ r_1 - r_2q_3 = r_3, \\ \vdots \\ r_{k-2} - r_{k-1}q_k = r_k, \end{cases}$$

and $f(r_k) < f(b)$.

If $r_k = 0$, we say that (1) is a *terminating* k-stage division chain starting from (a, b).

Remark 7.1. Any division $r_{k-2} - r_{k-1}q_k = r_k$ can be turned into a 2-stage division $\begin{cases} r_{k-2} - r_{k-1}(q_k + 1) = -r_{k-1} + r_k, \\ r_{k-1} - (-r_{k-1} + r_k) \cdot (-1) = r_k. \end{cases}$ Consequently,

- If (a, b) is a k-stage right Euclidean pair with respect to f, it is a l-stage right Euclidean pair with respect to f for any $l \geq k$.
- If (a, b) admits a k-stage terminating division chain, then for any $l \geq k$, the pair (a, b) admits admits a terminating l-stage division chain.

Definition 7.2. We say that $\mathfrak{A}$ is *ω-stage right Euclidean* if there exists a function $f : \mathfrak{A} \longrightarrow \mathbf{Z}_{\geq 0}$ whose zero set is exactly $\{0\}$ such that for every pair $(a, b) \in \mathfrak{A} \times \mathfrak{A}^\bullet$, there exists $k \in \mathbf{Z}_{>0}$ such that (a, b) is a k-stage Euclidean pair with respect to f. If for all pairs, we can take $k \leq k_0$, we say that A is a *k_0-stage right Euclidean* ring. If for all pairs $(a, b) \in \mathfrak{A} \times \mathfrak{A}^\bullet$, there exists a k-stage terminating division chain starting from (a, b), we say that $\mathfrak{A}$ is a *k-stage terminating right Euclidean* ring.

In light of Remark 7.1, to prove that $\mathfrak{A}$ is k-stage right Euclidean, it is enough to prove that every pair $(a, b) \in \mathfrak{A} \times \mathfrak{A}^\bullet$ is a l-stage right Euclidean pair for some $l \leq k$.

If $\mathfrak{A}$ is right Euclidean, then the Euclidean algorithm provides division chains and shows that $\mathfrak{A}$ is ω-stage right Euclidean. However, the converse is false in general, since an ω-stage right Euclidean ring may have non-principal right ideals.

If $\mathfrak{A}$ is ω-stage right Euclidean, then $\mathfrak{A}$ is a right K-Hermite ring. But the converse is false in general: $\mathfrak{R} = \mathbf{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID, but $\mathfrak{R}$ is not ω-stage Euclidean.

Let $\mathfrak{R}$ be a commutative ring, we consider $\mathfrak{A} = \mathrm{M}_n(\mathfrak{R})$. We can also define k-stage left Euclidean pairs, by replacing bq_1 by $q_1 b$ and $r_i q_{i+1}$ by $q_{i+1} r_i$ in (17), which leads to define ω-stage left Euclidean rings and k-stage left Euclidean rings. But for $(a, b) \in \mathrm{M}_n(\mathfrak{R})$, $b \neq \mathfrak{o}_n$, (a, b) is a k-stage right Euclidean pair with respect to f if and only if $(a^{\mathsf{T}}, b^{\mathsf{T}})$ is a k-stage left Euclidean pair with respect to f^{T}. Consequently, $\mathrm{M}_n(\mathfrak{R})$ is k-stage right Euclidean if and only if it is k-stage left Euclidean, and likewise, $\mathrm{M}_n(\mathfrak{R})$ is ω-stage right Euclidean if and only if it is ω-stage left Euclidean.

Let us immediately indicate a corollary. Let $\mathfrak{R}$ be a PIR and $n \in \mathbf{Z}_{>1}$. Theorem 4.1 implies that $\mathrm{M}_n(\mathfrak{R})$ is ω-stage right Euclidean, but we can improve this property.

Theorem 7.3. *Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. Then we have the following properties.*

(1) If $\mathfrak{R}$ is a K-Hermite ring, then $\mathrm{M}_n(\mathfrak{R})$ is $(4n-3)$-stage terminating right and left Euclidean.
(2) If $\mathfrak{R}$ is an elementary divisor ring, then $\mathrm{M}_n(\mathfrak{R})$ is $(2n-1)$-stage terminating right and left Euclidean.
(3) If $\mathfrak{R}$ is a PIR, then $\mathrm{M}_n(\mathfrak{R})$ is 2-stage right and left Euclidean.

If $\mathfrak{R}$ is an integral domain, then Amitsur [Ami63, Theorem 1.4] proved that $\mathfrak{R}$ is Bézout if and only if $\mathfrak{R}$ is K-Hermite. Consequently, Theorem 7.3(1) implies the following result.

Corollary 7.4. *Let $\mathfrak{R}$ be an integral domain and $n \in \mathbf{Z}_{>1}$, then the following statements are equivalent.*

(1) $\mathfrak{R}$ is Bézout.
(2) $\mathfrak{R}$ is K-Hermite.
(3) $\mathrm{M}_n(\mathfrak{R})$ is $(4n-3)$-stage terminating right Euclidean.
(4) $\mathrm{M}_n(\mathfrak{R})$ is ω-stage right Euclidean.
(5) $\mathrm{M}_n(\mathfrak{R})$ is right Bézout.

Proof. We have (1) $\iff$ (2) because $\mathfrak{R}$ is an integral domain; (2) $\Longrightarrow$ (3) is Theorem 7.3(1); (3) $\Longrightarrow$ (4) and (4) $\Longrightarrow$ (5) are clear; let us explain (5) $\Longrightarrow$ (1).

Take a, $b \in \mathfrak{R}$. Consider the matrices

$$A = \mathrm{diag}(1, \ldots, 1, a) \quad \text{and} \quad B = \mathrm{diag}(1, \ldots, 1, b) \in \mathrm{M}_n(\mathfrak{R}).$$

Since $\mathrm{M}_n(\mathfrak{R})$ is right Bézout, there exists $D \in \mathrm{M}_n(\mathfrak{R})$ such that

$$A\mathrm{M}_n(\mathfrak{R}) + B\mathrm{M}_n(\mathfrak{R}) = D\mathrm{M}_n(\mathfrak{R}). \tag{18}$$

Thanks to (18), there exists M, $N \in \mathrm{M}_n(\mathfrak{R})$ such that $A = DM$, $B = DN$. Therefore $a = \det A \in (\det D)\mathfrak{R}$, and $b = \det B \in (\det D)\mathfrak{R}$, which implies $a\mathfrak{R} + b\mathfrak{R} \subseteq (\det D)\mathfrak{R}$.

But (18) also implies that there exist U, $V \in \mathrm{M}_n(\mathfrak{R})$ such that $AU+BV = D$. The elements of the last row of $AU + BV$ are elements of $a\mathfrak{R}+b\mathfrak{R}$. Since $a\mathfrak{R} + b\mathfrak{R}$ is an ideal of $\mathfrak{R}$, Leibniz formula shows that $\det D \in a\mathfrak{R} + b\mathfrak{R}$, and we can conclude that $a\mathfrak{R} + b\mathfrak{R} = (\det D)\mathfrak{R}$. □

The remainder of this section will be devoted to the proof of Theorem 7.3. Since $\mathfrak{R}$ is commutative left and right Euclidean properties are equivalent, so we will only be concerned with right Euclidean properties. We will first deal with special PIRs, where the situation is even simpler.

7.2. **2-stage Euclidean property over a special PIR.** If $\mathfrak{S}$ is a special PIR, then for any $n \in \mathbf{Z}_{\geq 1}$, $\mathrm{M}_n(\mathfrak{S})$ is right Euclidean and $e(\mathrm{M}_n(\mathfrak{S})) < \omega$, but we can also find a terminating 2-stage division for any pair of elements of $\mathrm{M}_n(\mathfrak{S})$.

Proposition 7.5. *Let $\mathfrak{S}$ be a special PIR and $n \in \mathbf{Z}_{\geq 1}$. Then $\mathrm{M}_n(\mathfrak{S})$ is 2-stage terminating left and right Euclidean.*

Proof. Let A, $B \in \mathrm{M}_n(\mathfrak{S})$, $B \neq \mathfrak{o}_n$. Thanks to [Hun68], there exist a PID $\mathfrak{R}$ and a surjective ring homomorphism $\pi : \mathfrak{R} \longrightarrow \mathfrak{S}$. We extend π to a surjective ring homomorphism $\pi : \mathrm{M}_n(\mathfrak{R}) \longrightarrow \mathrm{M}_n(\mathfrak{S})$. Take A', $B' \neq \mathfrak{o}_n \in \mathrm{M}_n(\mathfrak{R})$ such that $A = \pi(A')$, $B = \pi(B')$.

Since $\mathfrak{R}$ is a PID, it is a K-Hermite ring with no nontrivial zero divisors, so there exists A'_1, B'_1, and $D' \in \mathrm{M}_n(\mathfrak{R})$, such that $A' = D'A'_1$, $B' = D'B'_1$ and $A'_1\mathrm{M}_n(\mathfrak{R}) + B'_1\mathrm{M}_n(\mathfrak{R}) = \mathrm{M}_n(\mathfrak{R})$. By writing $A_1 = \pi(A'_1)$, $B_1 = \pi(B'_1)$, $D = \pi(D') \in \mathrm{M}_n(\mathfrak{S})$, we obtain

$$A = DA_1, \quad B = DB_1, \quad \text{and} \quad A_1\mathrm{M}_n(\mathfrak{S}) + B_1\mathrm{M}_n(\mathfrak{S}) = \mathrm{M}_n(\mathfrak{S}). \tag{19}$$

But $\operatorname{sr}\mathfrak{S} = 1$, so $\operatorname{sr}\mathrm{M}_n(\mathfrak{S}) = 1$ too. Consequently, there exists a matrix $Q' \in \mathrm{M}_n(\mathfrak{S})$ such that $(A_1 + B_1Q')\mathrm{M}_n(\mathfrak{S}) = \mathrm{M}_n(\mathfrak{S})$, i.e. $A_1 + B_1Q' = U \in \mathrm{GL}_n(\mathfrak{S})$. This provides the following terminating 2-stage division for (A, B):

$$\begin{cases} A - B(-Q') = DU, \\ B - DUU^{-1}B_1 = \mathfrak{o}_n. \end{cases}$$

□

Remark 7.6. The conclusion of Proposition 7.5 above still holds if we assume $\mathfrak{S}$ to be an integral domain, which is also a Bézout ring and has stable rank 1, because we can directly obtain (19) and the end of the proof can be applied without changes.

For example, the ring of all algebraic integers $\mathfrak{R} = \overline{\mathbf{Z}}$ satisfies this property. As $\mathfrak{R}$ is not a PID, this shows that the converse of Theorem 7.3(3) is false.

7.3. **The K-Hermite case.** For technical reasons, we will deal with non-square matrices, starting with 2 rows.

Lemma 7.7. *Let $\mathfrak{R}$ be a commutative K-Hermite ring. Let $m \in \mathbf{Z}_{>1}$, $A \in \mathrm{M}_{2,m}(\mathfrak{R})$, $B \in \mathrm{M}_{2,m}(\mathfrak{R})$, then there exist $Q_i \in \mathrm{M}_m(\mathfrak{R})$, $R_i \in \mathrm{M}_{2,m}(\mathfrak{R})$,*

$1 \leq i \leq 5$, *such that*

$$\begin{cases} A - BQ_1 = R_1, \\ B - R_1Q_2 = R_2, \\ R_1 - R_2Q_3 = R_3, \\ R_2 - R_3Q_4 = R_4, \\ R_3 - R_4Q_5 = \mathfrak{o}_{2,m}. \end{cases}$$

Proof. Write $A = (a_{i,j})_{1\leq i\leq 2,\, 1\leq j\leq m}$. Since $\mathfrak{R}$ is K-Hermite, there exists some $V \in \mathrm{GL}_m(\mathfrak{R})$ such that BV is lower triangular. Denote by $b \in \mathfrak{R}$ the coefficient $(1,1)$ of BV. There exist d, b', $a'_i \in \mathfrak{R}$, $1 \leq i \leq m$ such that $b = db'$, $a_{1,i} = da'_i$, and satisfying

$$a'_1\mathfrak{R} + \cdots + a'_m\mathfrak{R} + b'\mathfrak{R} = \mathfrak{R}.$$

But $\operatorname{sr}\mathfrak{R} \leq m$, so there exist $x_i \in \mathfrak{R}$, $1 \leq i \leq m$ such that

$$(a'_1 + b'x_1)\mathfrak{R} + \cdots + (a'_m + b'x_m)\mathfrak{R} = \mathfrak{R}.$$

Therefore, there exist $\lambda_i \in \mathfrak{R}$, $1 \leq i \leq m$, satisfying $\sum_{i=1}^m (a'_i + b'x_i)\lambda_i = b'$. Set $R_1 = A - BV\begin{pmatrix} -x_1 & \cdots & -x_m \\ \hline \multicolumn{3}{c}{\mathfrak{o}_{m-1,m}} \end{pmatrix}$, whose first row is

$$\begin{pmatrix} a_{1,1} + bx_1 & \cdots & a_{1,m} + bx_m \end{pmatrix}.$$

Then we have the following "division chain":

$$\begin{cases} A - BV\begin{pmatrix} -x_1 & \cdots & -x_m \\ \hline \multicolumn{3}{c}{\mathfrak{o}_{m-1,m}} \end{pmatrix} = R_1, \\ B - R_1\left(\begin{array}{c|c} \lambda_1 & \\ \vdots & \mathfrak{o}_{m,m-1} \\ \lambda_m & \end{array}\right)V^{-1} = \begin{pmatrix} \mathfrak{o}_{1,m-1} \\ \hline R'_2 \end{pmatrix}, \\ R_1 - \begin{pmatrix} \mathfrak{o}_{1,m-1} \\ \hline R'_2 \end{pmatrix}\mathfrak{o}_n = R_1. \end{cases} \tag{20}$$

Set $R_2 = \begin{pmatrix} \mathfrak{o}_{1,m-1} \\ \hline R'_2 \end{pmatrix}$ and $R_3 = R_1$. Write $R'_2 = \begin{pmatrix} \alpha_1 & \cdots & \alpha_m \end{pmatrix} \in \mathrm{M}_{1,m}(\mathfrak{R})$. Since $\mathfrak{R}$ is K-Hermite, there exists $V_1 \in \mathrm{GL}_m(\mathfrak{R})$ such that

$$R_3V_1 = \left(\begin{array}{cc|c} b_1 & 0 & \\ b_2 & c & \mathfrak{o}_{2,m-2} \end{array}\right)$$

Besides, there exist d, c', $\alpha'_i \in \mathfrak{R}$, $1 \leq i \leq m$, such that $c = dc'$, $\alpha_i = d\alpha'_i$, and

$$\alpha'_1\mathfrak{R} + \alpha'_2\mathfrak{R} + \cdots + \alpha'_m\mathfrak{R} + c'\mathfrak{R} = \mathfrak{R}.$$

But $\operatorname{sr}\mathfrak{R} \leq m$, so there exist $x_i \in \mathfrak{R}$, $1 \leq i \leq m$ satisfying

$$(\alpha'_1 + c'x_1)\mathfrak{R} + (\alpha'_2 + c'x_2)\mathfrak{R} + \cdots + (\alpha'_m + c'x_m)\mathfrak{R} = \mathfrak{R}.$$

Thanks to [Kap49, Theorem 3.7], we can find an invertible matrix $U \in \mathrm{GL}_m(\mathfrak{R})$ whose second row is

$$\begin{pmatrix} \alpha'_1 + c'x_1 & \alpha'_2 + c'x_2 & \cdots & \alpha'_m + c'x_m \end{pmatrix}.$$

Let us denote by $\begin{pmatrix}\lambda_1 & \cdots & \lambda_m\end{pmatrix}$ the first row of U. Set $M = \begin{pmatrix} b_1 & 0 \\ b_2 & d\end{pmatrix}$. Notice that $R_2 = M\begin{pmatrix}\mathfrak{o}_{1,m} \\ \hline \alpha'_1 & \cdots & \alpha'_m\end{pmatrix}$, and $R_3V_1 = M\left(\begin{array}{cc|c} 1 & 0 & \\ 0 & c' & \mathfrak{o}_{2,m-2}\end{array}\right)$. Then set $R_4 = M\begin{pmatrix}\lambda_1 & \cdots & \lambda_m \\ \alpha'_1 + c'x_1 & \cdots & \alpha'_m + c'x_m\end{pmatrix}$, we obtain the following "division chain":

$$\left\{\begin{array}{l} R_2 - R_3V_1\left(\begin{array}{c}\begin{pmatrix}-\lambda_1 & \cdots & -\lambda_m \\ -x_1 & \cdots & -x_m\end{pmatrix} \\ \hline \mathfrak{o}_{m-2,m}\end{array}\right) = R_4, \\ R_3 - R_4U^{-1}\left(\begin{array}{cc|c} 1 & 0 & \\ 0 & c' & \mathfrak{o}_{2,m-2} \\ \hline & \mathfrak{o}_{m-2,m} & \end{array}\right)V_1^{-1} = \mathfrak{o}_{2,m}. \end{array}\right. \tag{21}$$

Combining Equations (20) and (21) provides a 5-stage terminating division chain. □

Now, we can exhibit a terminating division chain in the general case.

Proposition 7.8. *Let $\mathfrak{R}$ be a commutative K-Hermite ring. Then $\mathrm{M}_n(\mathfrak{R})$ is $(4n-3)$-stage terminating right Euclidean.*

Proof. We will prove a little more to facilitate the induction. Namely, we will prove by induction on $n \in \mathbf{Z}_{>1}$ that for any $m \geq n$, $A \in \mathrm{M}_{n,m}(\mathfrak{R})$, $B \in \mathrm{M}_{n,m}(\mathfrak{R})$, there exist matrices $Q_i \in \mathrm{M}_m(\mathfrak{R})$, $R_i \in \mathrm{M}_{n,m}(\mathfrak{R})$, $1 \leq i \leq 4n-3$ such that

$$\left\{\begin{array}{r} A - BQ_1 = R_1, \\ B - R_1Q_2 = R_2, \\ R_1 - R_2Q_3 = R_3, \\ \vdots \\ R_{4n-5} - R_{4n-4}Q_{4n-3} = \mathfrak{o}_{n,m}. \end{array}\right.$$

For $n = 2$, it is Lemma 7.7. Take $n > 2$ and assume that the property holds for $n-1$. Fix $m \geq n$. Denote by A', $B' \in \mathrm{M}_{n-1,m}(\mathfrak{R})$ the $(n-1)$ first rows of A and B. Then by the induction hypothesis, there exists a $(4n-7)$-stage terminating division chain starting from (A', B'). Denoting by $Q_i \in \mathrm{M}_m(\mathfrak{R})$, $1 \leq i \leq 4n-7$ the quotients of this chain, we can apply them starting from (A, B) and we construct $R_i \in \mathrm{M}_{n,m}(\mathfrak{R})$, satisfying

$$R_{4n-7} = \begin{pmatrix}\mathfrak{o}_{n-1,m} \\ \hline \alpha_1 & \cdots & \alpha_m\end{pmatrix}.$$

We apply the trivial division $R_{4n-8} - R_{4n-7} \cdot \mathfrak{o}_m = R_{4n-8}$, so that $R_{4n-6} = R_{4n-8}$. Since $\mathfrak{R}$ is K-Hermite, there exists $V \in \mathrm{GL}_m(\mathfrak{R})$ such that $R_{4n-6}V$ is lower triangular. Denote by b the coefficient of $R_{4n-6}V$ with coordinates (n, n).

There exist d, b', $\alpha'_i \in \mathfrak{R}$, $1 \leq i \leq m$ satisfying $\alpha_i = d\alpha'_i$, $b = db'$, and

$$\alpha'_1\mathfrak{R} + \cdots + \alpha'_m\mathfrak{R} + b'\mathfrak{R} = \mathfrak{R}.$$

Since $\operatorname{sr}\mathfrak{R} \leq m$, there exists $x_i \in \mathfrak{R}$, $1 \leq i \leq m$ such that

$$(\alpha'_1 + b'x_1)\mathfrak{R} + \cdots + (\alpha'_m + b'x_m)\mathfrak{R} = \mathfrak{R}.$$

Take $\lambda_i \in \mathfrak{R}$, $1 \leq i \leq m$ such that $\sum_{i=1}^{m}(\alpha'_i + b'x_i)\lambda_i = 1$. Then set

$$R_{4n-5} = \left(\begin{array}{c} \mathfrak{o}_{n-1,m} \\ \hline \alpha_1 + bx_1 \quad \cdots \quad \alpha_m + bx_m \end{array}\right),$$

$$\text{and } R_{4n-4} = R_{4n-6} + \left(\mathfrak{o}_{n,n-1} \left|\begin{array}{c} \mathfrak{o}_{n-1,1} \\ \hline d-b \end{array}\right| \mathfrak{o}_{n,m-n}\right) V^{-1},$$

so that we obtain

$$\left\{\begin{array}{c} R_{4n-7} - R_{4n-6}V \left(\begin{array}{c} \mathfrak{o}_{n-1,m} \\ \hline -x_1 \quad \cdots \quad -x_m \\ \hline \mathfrak{o}_{m-n,m} \end{array}\right) = R_{4n-5}, \\ R_{4n-6} - R_{4n-5}\left(\mathfrak{o}_{m,n-1} \left|\begin{array}{c} \lambda_1(b'-1) \\ \vdots \\ \lambda_m(b'-1) \end{array}\right| \mathfrak{o}_{m,m-n}\right) V^{-1} = R_{4n-4}, \\ R_{4n-5} - R_{4n-4}V \left(\begin{array}{c} \mathfrak{o}_{n-1,m} \\ \hline \alpha'_1 + b'x_1 \quad \cdots \quad \alpha'_m + b'x_m \\ \hline \mathfrak{o}_{m-n,m} \end{array}\right) = \mathfrak{o}_{n,m}. \end{array}\right.$$

□

7.4. **The elementary divisor ring case.** A commutative elementary divisor ring $\mathfrak{R}$ is a K-Hermite ring, so we know already that for any $n \in \mathbf{Z}_{>1}$, $\mathrm{M}_n(\mathfrak{R})$ is $(4n-3)$-stage terminating right Euclidean, but we want to obtain shorter terminating division chains. Let us first deal with a special case.

Lemma 7.9. *Let $\mathfrak{R}$ be an elementary divisor ring. Take A, $B \in \mathrm{M}_2(\mathfrak{R})$. Assume that $B \sim \mathrm{diag}(b_1, b_2)$ and that b_1 divides the coefficients of A. Then there exists a 2-stage terminating division chain starting from (A, B).*

Proof. Take X, $Y \in \mathrm{GL}_2(\mathfrak{R})$ such that

$$YA = \begin{pmatrix} b_1 a & b_1 b \\ c & d \end{pmatrix} \quad \text{and} \quad YBX = \mathrm{diag}(b_1, b_2).$$

As $\mathfrak{R}$ is a K-Hermite ring, thanks to Lemma 2.1, there exist c', d', b'_2, $e \in \mathfrak{R}$ such that $c = ec'$, $d = ed'$, $b_2 = eb'_2$, and

$$c'\mathfrak{R} + d'\mathfrak{R} + b'_2\mathfrak{R} = \mathfrak{R}.$$

But the stable rank of $\mathfrak{R}$ is at most 2 (see Lemma 2.2), so there exist t, $z \in \mathfrak{R}$ such that

$$(c' + b'_2 t)\mathfrak{R} + (d' + b'_2 z)\mathfrak{R} = \mathfrak{R}.$$

Hence there exist λ, $\mu \in \mathfrak{R}$ such that

$$(c' + b'_2 t)\lambda + (d' + b'_2 z)\mu = 1.$$

Now, we have the following 2-stage division chain:

$$\left\{\begin{array}{c} A - BX \begin{pmatrix} a-\mu & b+\lambda \\ -t & -z \end{pmatrix} = Y^{-1} \begin{pmatrix} b_1\mu & -b_1\lambda \\ c + b_2 t & d + b_2 z \end{pmatrix} \\ B - Y^{-1} \begin{pmatrix} b_1\mu & -b_1\lambda \\ c + b_2 t & d + b_2 z \end{pmatrix} \begin{pmatrix} d' + b'_2 z & \lambda b'_2 \\ -(c' + b'_2 t) & \mu b'_2 \end{pmatrix} X^{-1} = \mathfrak{o}_2. \end{array}\right. \tag{22}$$

□

Proposition 7.10. *Let $\mathfrak{R}$ be a commutative ring.*

(1) If $\mathfrak{R}$ is an elementary divisor ring, then $\mathrm{M}_2(\mathfrak{R})$ is 3-stage terminating right Euclidean.

(2) If $\mathfrak{R}$ is a PID, then $\mathrm{M}_2(\mathfrak{R})$ is 2-stage right Euclidean.

Proof. Notice that $\mathfrak{R}$ is an elementary divisor ring in any case. Take A, $B \in \mathrm{M}_2(\mathfrak{R})$, $B \neq \mathfrak{o}_2$. There exist X, Y, $T \in \mathrm{GL}_2(\mathfrak{R})$, a, b, c, $b_1|b_2 \in \mathfrak{R}$ such that

$$YBX = \mathrm{diag}(b_1, b_2), \qquad YAT = \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}.$$

(i) If b_1 divides a, b, and c, then Lemma 7.9 implies the existence of a 2-stage terminating division starting from (A, B).

(ii) If b_1 does not divide a, b or c, then set $Q = X \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} T^{-1}$, so that

$$A - BQ = Y^{-1} \begin{pmatrix} a & b_1 \\ b & c \end{pmatrix} T^{-1}, \tag{23}$$

To prove (1), simply notice that there is a 2-stage terminating division chain starting from $(B, A - BQ)$ thanks to case (i) above.

If $\mathfrak{R}$ is a PID, then the first invariant factor of $A - BQ$ is a strict divisor of b_1 (see Lemma 2.3(a)). Consequently, we have $f(A-BQ) < f(B)$ for the function

$$f : \begin{cases} \mathrm{M}_2(\mathfrak{R}) & \longrightarrow \quad \mathbf{Z}_{\geq 0} \\ \mathfrak{o}_2 & \longmapsto \quad 0 \\ M \sim \mathrm{diag}(b_1, b_2), b_1|b_2, b_1 \neq 0 & \longmapsto \quad \ell(b_1) + 1. \end{cases}$$

It proves that $\mathrm{M}_2(\mathfrak{R})$ is 2-stage right Euclidean with respect to f.

□

Remark 7.11. Let $\mathfrak{R}$ be an elementary divisor ring which is an integral domain. Then for any A, $B \in \mathrm{M}_2(\mathfrak{R})$, with $\mathrm{rk}\, B = 2$, there exists a 3-stage terminating division chain whose (nonzero) remainders have rank 2.

Indeed, instead of (23), we can apply division (7), which grants the same properties for the remainder, and the additional condition that the remainder has full rank.

Besides, we see that the nonzero remainder in (22) has full rank (by computing its determinant for instance).

This explains why we have obtained a short division chain in Example 5.6. Indeed,

Remark 7.12. Divisions (7) and (22) are exactly the divisions prescribed to define φ_2 in Section 3. So, if $\mathfrak{R}$ is a PID, and if we start from a pair (A, B) of elements of $\mathrm{M}_2(\mathfrak{R})$, with $\mathrm{rk}\, B = 2$, applying successive divisions by φ_2 as constructed in Section 3 will terminate in at most 3 steps.

We can extend the terminating division chain that we have obtained in size 2 to arbitrary size n.

Proposition 7.13. *Let $\mathfrak{R}$ be a (commutative) elementary divisor ring and $n \in \mathbf{Z}_{>1}$.*

(1) $\mathrm{M}_n(\mathfrak{R})$ is $(2n-1)$-stage terminating right Euclidean.

(2) If moreover $\mathfrak{R}$ is an integral domain, then for all A, $B \in \mathrm{M}_n(\mathfrak{R})$, with $\operatorname{rk} B = n$, there exists a $(2n-1)$-stage terminating division chain such that all nonzero remainders have rank n.

Proof. (1) Thanks to Remark 7.1, it suffices to prove the existence of division chains with length at most $(2n-1)$. We will prove it by induction on n. For $n = 2$, this is Proposition 7.10(1).

Take $n > 2$, and A, $B \in \mathrm{M}_n(\mathfrak{R})$, $B \neq \mathfrak{o}_n$. Then there exist X, Y, $T \in \mathrm{GL}_n(\mathfrak{R})$, $(a_i)_{1\leq i\leq n} \in \mathfrak{R}^n$, A' $B' \in \mathrm{M}_{n-1}(\mathfrak{R})$, such that

$$YAT = \left(\begin{array}{c|c} a_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_2 \\ \vdots \\ a_n \end{matrix} & A' \end{array}\right) \qquad \text{and} \qquad YBX = \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & B' \end{array}\right), \tag{24}$$

and b_1 divides all coefficients of B'. If b_1 does not divide a_1, take $Q = \left(\begin{array}{cc|c} 0 & -1 & \mathfrak{o}_{1,n-2} \\ \hline & \mathfrak{o}_{n-1,n} & \end{array}\right)$. Then $A - BQ \sim \operatorname{diag}(b'_1, \dots, b'_n)$ where b'_1 divides b_1, so b'_1 divides all coefficients of B.

In other words, after at most 1 division, we can assume that we have (24), with the further assumption that b_1 divides all coefficients of A', and in particular, b_1 divides a_1. Write $a_1 = b_1 a'_1$

By the induction hypothesis, there exists a $(2n-2)$-stage[8] terminating division chain in $\mathrm{M}_{n-1}(\mathfrak{R})$. Let us denote by Q'_k its quotients and R'_k its remainders, for $1 \leq k \leq 2n-2$.

Set $Q_1 = \left(\begin{array}{c|c} a'_1 - 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q'_1 \end{array}\right)$, $Q_i = \left(\begin{array}{c|c} 0 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q'_i \end{array}\right)$, for $1 < i < 2n-2$, and $Q_{2n-2} = \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q'_{2n-2} \end{array}\right)$. Then we obtain a $(2n-2)$-stage terminating division stage with the following remainders:

$$\text{for } 1 \leq i \leq n-1,\ R_{2i-1} = \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_2 \\ \vdots \\ a_n \end{matrix} & R'_{2i-1} \end{array}\right),$$

$$\text{for } 1 \leq i < n-1,\ R_{2i} = \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & R'_{2i} \end{array}\right).$$

(2) We prove it by induction on $n \geq 2$. The case $n = 2$ is Remark 7.11. In the induction hypothesis, we include the fact that the nonzero remainders have full rank. We perform the same divisions as in the proof of (1) with the following modifications. First, we replace the first division by the division performed in the 1st step of the proof of Lemma 3.6: we obtain $Q \in \mathrm{M}_n(\mathfrak{R})$ such that $A - BQ$ has rank n, and the first invariant factor of $A - BQ$ divides the first invariant factor of B. With the construction above, the nonzero remainders R_k have full rank. This completes the proof.

[8]The induction hypothesis ensures the existence of the $(2n-3)$-stage division chain with the required properties, but we can turn it into a $(2n-2)$-stage division chain with Remark 7.1.

□

Corollary 7.14. *Let $\mathfrak{R}$ be an integral domain which is an elementary divisor ring and $n \in \mathbf{Z}_{>1}$. Denote by $\mathfrak{F}$ the field fractions of $\mathfrak{R}$. Then for all $X \in \mathrm{M}_n(\mathfrak{F})$, there exist Q_1, Q_2, …, $Q_{2n-1} \in \mathrm{M}_n(\mathfrak{R})$ satisfying*

$$X = [Q_1, Q_2, \ldots, Q_{2n-1}].$$

Proof. We can apply the same technique as in the proof of Proposition 5.5. Proposition 7.13(2) implies that we can obtain a $(2n-1)$-stage terminating division chain satisfying (11). □

7.5. 2-stage Euclidean property over a PID.

Proposition 7.15. *Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$. Then $\mathrm{M}_n(\mathfrak{R})$ is 2-stage right Euclidean.*

Proof. Let us define

$$f_n : \begin{cases} \mathrm{M}_n(\mathfrak{R}) & \longrightarrow \mathbf{Z}_{\geq 0} \\ \mathfrak{o}_n & \longmapsto 0 \\ M \sim \mathrm{diag}(b_1, b_2, \ldots, b_r, 0, \ldots, 0), \\ b_1 | b_2 | \ldots | b_r, b_r \neq 0 & \longmapsto \ell\left(\prod_{i=1}^{\min(r,n-1)} b_i\right) + 1. \end{cases}$$

We will prove by induction on $n \geq 2$ that $\mathrm{M}_n(\mathfrak{R})$ is 2-stage right Euclidean with respect to f_n. For $n = 2$, it is Proposition 7.10(2) (or rather its proof).

Take $n > 2$, $A, B \in \mathrm{M}_n(\mathfrak{R})$, $B \neq \mathfrak{o}_n$. There exist $X, Y, T \in \mathrm{GL}_n(\mathfrak{R})$ such that $YBX = \mathrm{diag}(b_1, b_2, \ldots, b_r, 0, \ldots, 0)$ with $b_1 | b_2 | \ldots | b_r \neq 0$ and YAT is lower triangular.

1. First consider the case $r = 1$. Write $(a_{i,j})_{1 \leq i,j \leq n} = YAT$ and set $E = (e_{i,j})_{1 \leq i \leq n-1, 1 \leq j \leq n} \in \mathrm{M}_{n-1,n}(\mathfrak{R})$, where

$$\text{for all } 1 \leq i \leq n-1, 1 \leq j \leq n,\ e_{i,j} = a_{i+1,j},$$

that is to say

$$YAT = \left(\begin{array}{c|c} a_{1,1} & \mathfrak{o}_{1,n-1} \\ \hline E & \end{array}\right).$$

The kernel of E is nontrivial. Take $v = (v_i)_{1 \leq i \leq n} \in \mathrm{M}_{n,1}(\mathfrak{R})^\bullet$ such that $v \in \ker E$ and the coordinates of v are coprime, i.e.

$$\sum_{i=1}^{n} \mathfrak{R} v_i = \mathfrak{R}. \tag{25}$$

1.***a***. If $a_{1,1} v_1 \notin \mathfrak{R} b_1$, then we have the following 2-stage right Euclidean division:

$$\begin{cases} A - B\,\mathfrak{o}_n = A, \\ B - AT\left(\mathfrak{o}_{n,1} \mid -v \mid \mathfrak{o}_{n,n-2}\right) X^{-1} = Y^{-1} \left(\begin{array}{cc|c} b_1 & a_{1,1} v_1 & \mathfrak{o}_{1,n-2} \\ \hline \multicolumn{2}{c|}{\mathfrak{o}_{n-1,2}} & \mathfrak{o}_{n-1,n-2} \end{array}\right) X^{-1}. \end{cases}$$

Notice that this latter matrix $\left(\begin{array}{cc|c} b_1 & a_{1,1} v_1 & \mathfrak{o}_{1,n-2} \\ \hline \multicolumn{2}{c|}{\mathfrak{o}_{n-1,2}} & \mathfrak{o}_{n-1,n-2} \end{array}\right)$ is equivalent to the matrix $\mathrm{diag}(e, 0, \ldots, 0)$, where $e = \gcd(b_1, a_{1,1} v_1)$ is a strict divisor of b_1, so $\ell(e) < \ell(b_1)$.

1*.*b. If $a_{1,1}v_1 \in \mathfrak{R}b_1$, thanks to (25), take $\lambda = (\lambda_i)_{1\leq i\leq n} \in \mathrm{M}_{1,n}(\mathfrak{R})$ such that $\sum_{i=1}^n \lambda_i v_i = -\frac{a_{1,1}v_1}{b_1} + 1$. Hence we have the following 2-stage division chain:

$$\begin{cases} A - BX \left(\begin{array}{c} -\lambda \\ \hline \mathfrak{o}_{n-1,n} \end{array}\right) T^{-1} = Y^{-1} \left(\begin{array}{cccc} a_{1,1}+\lambda_1 b_1 & \lambda_2 b_1 & \cdots & \lambda_n b_1 \\ \hline & & E & \end{array}\right) T^{-1}, \\ B - Y^{-1} \left(\begin{array}{cccc} a_{1,1}+\lambda_1 b_1 & \lambda_2 b_1 & \cdots & \lambda_n b_1 \\ \hline & & E & \end{array}\right) T^{-1} T \left(v \;\middle|\; \mathfrak{o}_{n,n-1}\right) X^{-1} = \mathfrak{o}_n. \end{cases}$$

2. Assume now that $r > 1$ and that $b_r \in \mathfrak{R}^\times$, in which case we may suppose that $b_1 = \cdots = b_r = 1$. Define $M \in \mathrm{M}_{r,n}(\mathfrak{R})$ and $M^{(0)} \in \mathrm{M}_{n-r,n}(\mathfrak{R})$ such that

$$YAT = \left(\begin{array}{c} M \\ \hline M^{(0)} \end{array}\right).$$

We build inductively $v^{(i)} \in \mathrm{M}_{n,1}(\mathfrak{R})$ and $\lambda^{(i)} \in \mathrm{M}_{1,n}(\mathfrak{R})$ for $1 \leq i \leq r$ as follows. The kernel of $M^{(0)}$ is nontrivial, so there exists $v^{(1)} = \left(v_i^{(1)}\right)_{1\leq i\leq n} \in \mathrm{M}_{n,1}(\mathfrak{R})$ such that $M^{(0)}v^{(1)} = \mathfrak{o}_{n,1}$. We choose $v^{(1)}$ whose coordinates are coprime, i.e. they satisfy $\sum_{i=1}^n \mathfrak{R}v_i^{(1)} = \mathfrak{R}$, which allows us to take $\lambda^{(1)} \in \mathrm{M}_{1,n}(\mathfrak{R})$ such that $\lambda^{(1)}v^{(1)} = (1)$. Having built $v^{(i)}$ and $\lambda^{(i)}$ for $1 \leq i \leq i_0 < r$, we build $v^{(i_0+1)}$ and $\lambda^{(i_0+1)}$. Define $M^{(i_0)} \in \mathrm{M}_n(\mathfrak{R})$ by

$$M^{(i_0)} = \left(\begin{array}{c} \lambda^{(1)} \\ \vdots \\ \lambda^{(i_0)} \\ \hline \mathfrak{o}_{r-i_0,n} \\ \hline M^{(0)} \end{array}\right).$$

The kernel of $M^{(i_0)}$ is nontrivial, so there exists $v^{(i_0+1)} \in \mathrm{M}_{n,1}(\mathfrak{R})$ such that $M^{(i_0+1)}v^{(i_0+1)} = \mathfrak{o}_{n,1}$. We can choose $v^{(i_0+1)}$ such that its coordinates are coprime, which allows us to define $\lambda^{(i_0+1)} \in \mathrm{M}_{1,n}(\mathfrak{R})$ satisfying $\lambda^{(i_0+1)}v^{(i_0+1)} = (1)$. Now, we can exhibit the following 2-stage division chain.

$$\begin{cases} A - BX \left(\begin{array}{c} M - \left(\begin{array}{c} \lambda^{(1)} \\ \vdots \\ \lambda^{(r)} \end{array}\right) \\ \hline \mathfrak{o}_{n-r,n} \end{array}\right) T^{-1} = Y^{-1} \left(\begin{array}{c} \lambda^{(1)} \\ \vdots \\ \lambda^{(r)} \\ \hline M^{(0)} \end{array}\right) T^{-1}, \\ B - Y^{-1} \left(\begin{array}{c} \lambda^{(1)} \\ \vdots \\ \lambda^{(r)} \\ \hline M^{(0)} \end{array}\right) T^{-1} T \left(v^{(1)} \;\middle|\; \cdots \;\middle|\; v^{(r)} \;\middle|\; \mathfrak{o}_{n,n-r}\right) X^{-1} = \mathfrak{o}_n. \end{cases}$$

3. Assume now that $r > 1$ and that $b_r \notin \mathfrak{R}^\times$. Consider $A' \in \mathrm{M}_{n-1}(\mathfrak{R})$ such that

$$YAT = \left(\begin{array}{c|c} a_1 & \mathfrak{o}_{1,n-1} \\ \hline a_2 & \\ \vdots & A' \\ a_n & \end{array}\right), \qquad B' = \mathrm{diag}(b_2, \ldots, b_r).$$

Then, by induction hypothesis, we can write a 2-stage right Euclidean division of A' by B' with respect to f_{n-1}, that is to say that there exist $Q'_1, Q'_2, R'_1, R'_2 \in \mathrm{M}_{n-1}(\mathfrak{R})$ such that

$$\begin{cases} A' - B'Q'_1 = R'_1, \\ B' - R'_1 Q'_2 = R'_2, \\ \text{and } f_{n-1}(R'_2) < f_{n-1}(B'). \end{cases} \tag{26}$$

3.a. If $r = n$, and $b_{n-1} \in \mathfrak{R}^\times$, then $f_{n-1}(B') = 1$, so $f_{n-1}(R'_2) = 0$ and then $R'_2 = \mathfrak{o}_{n-1}$. As for all $1 \leq i < n-1$, b_i divides b_{n-1}, $b_i \in \mathfrak{R}^\times$ and we may suppose that $b_1 = \cdots = b_{n-1} = 1$. Using (26), we get

$$\begin{cases} A - BX \left(\begin{array}{c|c} a_1 - 1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_2 \\ \vdots \\ a_n \end{matrix} & Q'_1 \end{array}\right) T^{-1} = Y^{-1} \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & R'_1 \end{array}\right) T^{-1} \\ B - Y^{-1} \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & R'_1 \end{array}\right) T^{-1} T \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q'_2 \end{array}\right) X^{-1} = \mathfrak{o}_n. \end{cases}$$

From now, we can assume that $r < n$ or $b_{n-1} \notin \mathfrak{R}^\times$. In both cases, since $b_r \notin \mathfrak{R}^\times$, $b_{\min(r,n-1)} \notin \mathfrak{R}^\times$.

3.b. Suppose that $R'_2 = \mathfrak{o}_{n-1}$. Let us extend (26) to size n:

$$\begin{cases} A - BX \left(\begin{array}{c|c} 0 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q'_1 \end{array}\right) T^{-1} = Y^{-1} \left(\begin{array}{c|c} a_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_2 \\ \vdots \\ a_n \end{matrix} & R'_1 \end{array}\right) T^{-1}, \\ B - Y^{-1} \left(\begin{array}{c|c} a_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_2 \\ \vdots \\ a_n \end{matrix} & R'_1 \end{array}\right) T^{-1} T \left(\begin{array}{c|c} 0 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q'_2 \end{array}\right) X^{-1} = R_2, \end{cases} \tag{27}$$

where $R_2 = Y^{-1} \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & R'_2 \end{array}\right) X^{-1}$. Then

$$f_n(B) = \ell \left(\prod_{i=1}^{\min(r,n-1)} b_i \right) \geq \ell(b_1 b_{\min(r,n-1)}) + 1 > \ell(b_1) + 1,$$

and $f_n(R_2) = \ell(b_1) + 1$, so

$$f_n(R_2) < f_n(B),$$

which proves that (27) is a 2-stage right Euclidean division for (A, B).

3.c. Assume that $R'_2 \neq \mathfrak{o}_{n-1}$. Set $r' = \operatorname{rk} R'_2 + 1$, write

$$R'_2 \sim \operatorname{diag}(b'_2, \ldots, b'_{r'}, 0, \ldots, 0),$$

with $b'_2 | b'_3 | \ldots | b'_{r'} \neq 0$. By construction, these invariant factors satisfy

$$\ell \left(\prod_{i=2}^{\min(r',n-1)} b'_i \right) = f_{n-1}(R'_2) - 1 < f_{n-1}(B') - 1 = \ell \left(\prod_{i=2}^{\min(r,n-1)} b_i \right). \tag{28}$$

Besides, we can still extend (26) to size n as in (27). Then R_2 has rank r', and $R_2 \sim \operatorname{diag}(b_1'', b_2'', \dots, b_{r'}'', 0, \dots, 0)$, with $b_1''|b_2''|\dots|b_{r'}'' \neq 0$. But, thanks to Lemma 2.3(a), $\prod_{i=1}^{\min(r',n-1)} b_i''$ divides $b_1 \prod_{i=2}^{\min(r',n-1)} b_i'$, so (28) implies

$$f_n(R_2) = \ell \left(\prod_{i=1}^{\min(r',n-1)} b_i'' \right) + 1 < \ell \left(\prod_{i=1}^{\min(r,n-1)} b_i \right) + 1 = f_n(B).$$

This implies that (27) is a 2-stage right Euclidean division for the pair (A, B). □

Remark. This division does not necessarily correspond to taking successively the quotient and remainder of the division with respect to φ_n.

7.6. **Proof of Theorem 7.3.** We will combine the above results to prove Theorem 7.3. Notice that 2-stage right Euclidean rings are preserved by products.

Lemma 7.16. *The direct product of finitely many 2-stage right Euclidean rings is a 2-stage right Euclidean ring.*

Proof. By a clear induction, it is enough to prove it for the product of two rings. Let $\mathfrak{A}_1$, $\mathfrak{A}_2$ be 2-stage right Euclidean rings with respect to f_1 and f_2. Then we will prove that $\mathfrak{A}_1 \times \mathfrak{A}_2$ is 2-stage right Euclidean with respect to

$$f : \left\{ \begin{array}{ccc} \mathfrak{A}_1 \times \mathfrak{A}_2 & \longrightarrow & \mathbf{Z}_{\geq 0} \\ \left(a^{(1)}, a^{(2)}\right) & \longmapsto & f_1\left(a^{(1)}\right) + f_2\left(a^{(2)}\right). \end{array} \right.$$

Take $a^{(i)}, b^{(i)} \in \mathfrak{A}_i$, for $i = 1, 2$, with $(b^{(1)}, b^{(2)}) \neq (0, 0)$.

a. First, assume that $b^{(1)} \neq 0$ and $b^{(2)} \neq 0$. Then for $i = 1, 2$, we have some 2-stage right Euclidean divisions

$$\left\{ \begin{array}{l} a^{(i)} - b^{(i)} q_1^{(i)} = r_1^{(i)}, \\ b^{(i)} - r_1^{(i)} q_2(i) = r_2^{(i)}, \\ \text{and } f_i\left(r_2^{(i)}\right) < f_i\left(b^{(i)}\right). \end{array} \right. \tag{29}$$

These divisions can be naturally combined into

$$\left\{ \begin{array}{l} \left(a^{(1)}, a^{(2)}\right) - \left(b^{(1)}, b^{(2)}\right)\left(q_1^{(1)}, q_1^{(2)}\right) = \left(r_1^{(1)}, r_1^{(2)}\right), \\ \left(b^{(1)}, b^{(2)}\right) - \left(r_1^{(1)}, r_1^{(2)}\right)\left(q_2^{(1)}, q_2^{(2)}\right) = \left(r_2^{(1)}, r_2^{(2)}\right), \end{array} \right.$$

with

$$f\left(r_2^{(1)}, r_2^{(2)}\right) = f_1\left(r_2^{(1)}\right) + f_2\left(r_2^{(2)}\right) < f_1\left(b_2^{(1)}\right) + f_2\left(b_2^{(2)}\right) = f\left(b^{(1)}, b^{(2)}\right).$$

b. Now, assume that $b^{(1)} = 0$ and $b^{(2)} \neq 0$. Then (29) still holds for $i = 2$, and we have the following 2-stage right Euclidean division:

$$\left\{ \begin{array}{l} \left(a^{(1)}, a^{(2)}\right) - \left(0, b^{(2)}\right)\left(0, q_1^{(2)}\right) = \left(a^{(1)}, r_1^{(2)}\right), \\ \left(0, b^{(2)}\right) - \left(a^{(1)}, r_1^{(2)}\right)\left(0, q_2^{(2)}\right) = \left(0, r_2^{(2)}\right), \end{array} \right.$$

with

$$f\left(0, r_2^{(2)}\right) = f_2\left(r_2^{(2)}\right) < f_2\left(b_2^{(2)}\right) = f\left(0, b^{(2)}\right).$$

c. The proof is similar for $b^{(1)} \neq 0$ and $b^{(2)} = 0$. □

Proof of Theorem 7.3. (1) See Proposition 7.8.
(2) See Proposition 7.13(1).
(3) Let $\mathfrak{R}$ be a PIR and $n \in \mathbf{Z}_{>1}$. Thanks to Proposition 4.2, $\mathfrak{R} = \prod_{i=1}^{l} \mathfrak{R}_i$, where each $\mathfrak{R}_i$ is a PID or a special PIR. Then $\mathrm{M}_n(\mathfrak{R})$ can be identified with $\prod_{i=1}^{l} \mathrm{M}_n(\mathfrak{R}_i)$. Each $\mathrm{M}_n(\mathfrak{R}_i)$ is 2-stage right Euclidean, cf. Propositions 7.5 and 7.15. Lemma 7.16 completes the proof.

□

7.7. **Final remarks.** Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. If $\mathrm{M}_n(\mathfrak{R})$ is ω-stage right Euclidean, then $\mathrm{M}_n(\mathfrak{R})$ is right K-Hermite, it follows that $\operatorname{sr} \mathrm{M}_n(\mathfrak{R}) \leq 2$ (Lemma 2.2). Consequently, $\operatorname{sr} \mathfrak{R} \leq n+1$. As $\mathfrak{R}$ is a Bézout ring, $\mathfrak{R}$ is K-Hermite if and only if $\operatorname{sr} \mathfrak{R} \leq 2$ [Zab03, Theorem 1]. I do not know of any commutative Bézout ring $\mathfrak{R}$ satisfying $2 < \operatorname{sr} \mathfrak{R} < \infty$.

Let $\mathfrak{R}$ be an integral domain. If $\mathfrak{R}$ is a Bézout ring, then $\mathrm{M}_2(\mathfrak{R})$ is 5-stage right Euclidean. If we can find such a ring $\mathfrak{R}$ which is not 3-stage right Euclidean, then it cannot be an elementary divisor ring.

Acknowledgements

The research of the author was funded by ERC Starting Grant ANTICS 278537, and by a "nouveau chercheur" grant by Région Auvergne. He would like to thank the anonymous referee for her/his insightful comments and corrections, in particular for indicating Remark 2.6. He also would like to thank Jean-Paul Cerri for his constant and invaluable help, and especially for his patience for reading the technical details of the article.

References

[AJLL14] Adel Alahmadi, Surender K. Jain, Tsit Yuen Lam, and André Leroy, *Euclidean pairs and quasi-Euclidean rings*, Journal of Algebra **406** (2014), 154–170.
[Ami63] Shimshon A. Amitsur, *Remarks on Principal Ideal Rings*, Osaka Mathematical Journal **15** (1963), 59–69.
[Bru73] Hans-Heinrich Brungs, *Left Euclidean rings*, Pacific Journal of Mathematics **45** (1973), 27–33.
[Cla15] Pete L. Clark, *A note on Euclidean order types*, Order **32** (2015), no. 2, 157–178.
[Coo76] George E. Cooke, *A weakening of the Euclidean property for integral domains and applications to algebraic number theory. I.*, Journal für die reine und angewandte Mathematik **282** (1976), 133–156.
[Fle71] Colin R. Fletcher, *Euclidean Rings*, Journal of the London Mathematical Society **4** (1971), 79–82.
[GH56] Leonard Gillman and Melvin Henriksen, *Some remarks about elementary divisor rings*, Transactions of the American Mathematical Society **82** (1956), 362–365.
[Hun68] Thomas W. Hungerford, *On the structure of principal ideal rings*, Pacific Journal of Mathematics **25** (1968), no. 3, 543–547.
[Jac85] Nathan Jacobson, *Basic Algebra I: Second Edition*, W. H. Freeman and Company, 1985.
[Kal85] Gojko V. Kalajdžić, *Euclidean algorithm in matrix modules over a given Euclidean ring*, Siberian Mathematical Journal **26** (1985), no. 6, 818–822.
[Kap49] Irving Kaplansky, *Elementary divisors and modules*, Transactions of the American Mathematical Society **66** (1949), 464–491.

[MM82] Pere Menal and Jaume Moncasi, *On regular rings with stable range* 2, Journal of Pure and Applied Algebra **24** (1982), no. 1, 25–40.

[MR01] John C. McConnell and J. Chris Robson, *Noncommutative Noetherian rings*, revised ed., Graduate Studies in Mathematics, vol. 30, American Mathematical Society, Providence, RI, 2001, With the cooperation of L. W. Small.

[Sam71] Pierre Samuel, *About Euclidean Rings*, Journal of Algebra **19** (1971), 282–301.

[Vas71] Leonid N. Vaserštein, *Stable rank of rings and dimensionality of topological spaces*, Functional Analysis and Its Applications **5** (1971), no. 2, 102–110.

[Zab03] Bogdan V. Zabavs'kyi, *Reduction of matrices over Bezout rings of stable rank not higher than* 2, Ukrainian Mathematical Journal **55** (2003), no. 4, 665–670.

[ZS75] Oscar Zariski and Pierre Samuel, *Commutative algebra. Vol. 1*, Graduate Texts in Mathematics, vol. 28, Springer-Verlag, 1975.

Université Clermont Auvergne, F-63000 Clermont-Ferrand, France, e-mail: pierre.lezowski@uca.fr