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 $M_n(\mathfrak{R})$ of n by n matrices with coefficients in $\mathfrak{R}$. In particular, we prove that $M_n(\mathfrak{R})$ 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 $M_n(\mathfrak{R})$. If $\mathfrak{R}$ is a principal ideal ring, we prove that $M_n(\mathfrak{R})$ is 2-stage Euclidean and every pair of matrices in $M_n(\mathfrak{R})$ admits a terminating division chain whose length is at most $3n-1$.

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 $\mathfrak{R}$ and integers $n, m > 0$, $M_{m,n}(\mathfrak{R})$ is the set of matrices of elements of $\mathfrak{R}$ with m rows and n columns; $M_n(\mathfrak{R}) = M_{n,n}(\mathfrak{R})$; $GL_n(\mathfrak{R})$ is the subset of $M_n(\mathfrak{R})$ of invertible matrices.

Whenever $\mathfrak{R}$ is commutative, $M_n(\mathfrak{R})$ 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, $\mathfrak{A} = M_n(\mathbf{Z})$ 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

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

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

Date: March 24, 2015.

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.

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])**.** *If $\mathfrak{R}$ is a (not necessarily commutative) left-Euclidean ring, then $M_n(\mathfrak{R})$ 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 $M_n(\mathfrak{R})$ 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 notation, introduced in Section 2, and proceed in two steps. 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 $M_n(\mathfrak{R})$ when $\mathfrak{R}$ is a PIR.

Finally, we will study another generalization of the Euclidean property. 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[1]. After k divisions, we want the remainder r_k to satisfy

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

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 Euclidean. A Euclidean ring is necessarily ω-stage Euclidean, but the converse if 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 Euclidean properties of matrix rings.

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

An immediate consequence of Theorem 4.1 is that $M_n(\mathfrak{R})$ is ω-stage 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 PIR and $n \in \mathbf{Z}_{>1}$. Then we have the following properties.*

1. *$M_n(\mathfrak{R})$ is 2-stage right-Euclidean and left-Euclidean.*
2. *For any pair $(a, b) \in M_n(\mathfrak{R}) \times M_n(\mathfrak{R})^\bullet$, there exists a $(3n-1)$-stage terminating division chain in $M_n(\mathfrak{R})$ starting from (a, b).*

[1] See Section 7 for precise definitions.

2. Generalities and first remarks

2.1. **Notation.** Let $n, m \in \mathbf{Z}_{\geq 1}$. We denote by $\mathrm{diag}(b_1, \ldots, b_n)$ the diagonal matrix of size n by n with entries $b_1, \ldots, b_n$. 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, $\mathfrak{o}_n = \mathfrak{o}_{n,n}$.

In a PID $\mathfrak{R}$, for $a, b \in \mathfrak{R}$, we say that a divides b, which is denoted by $a|b$, if $\mathfrak{R}b \subseteq \mathfrak{R}a$. For $a, b \in \mathfrak{R}$, the greatest common divisor (gcd for short) of a and b is only defined up to multiplication by a unit, we will write $\gcd(a, b)$ for any choice of a gcd.

2.2. **Decomposition of matrices in a PID.** In this paragraph, $n \in \mathbf{Z}_{\geq 1}$, and $\mathfrak{R}$ is a PID.

Lemma 2.1. *Let $M \in M_n(\mathfrak{R})$. Then there exists $X \in GL_n(\mathfrak{R})$ such that MX is lower triangular, that is $MX = (a_{i,j})_{1 \leq i,j \leq n}$ satisfies $a_{i,j} = 0$ if $j > i$.*

Proof. This is simply a transformation of M to column echelon form, which can be obtained through Gaussian elimination. □

Definition 2.2. Given two matrices $A, B \in M_n(\mathfrak{R})$, we say that A and B are equivalent if there exist $X, Y \in GL_n(\mathfrak{R})$ such that

$$A = YBX.$$

We will denote it by $A \sim B$.

The relation $\sim$ is an equivalence relation on $M_n(\mathfrak{R})$ and given any matrix $M \in M_n(\mathfrak{R})$, M admits a normal form given by its invariant factors.

Lemma 2.3 (Smith normal form)**.** *Let $M \in M_n(\mathfrak{R})$. Then there exist $(b_i)_{1 \leq i \leq n} \in \mathfrak{R}^n$ such that $b_1|b_2|\ldots|b_n$ and*

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

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. The largest integer r such that $b_r \neq 0$ is the rank $\mathrm{rk}(M)$ of M.

Proof. See for instance [Jac85, Theorem 3.8]. □

Remark that the rank corresponds to the classical notion of rank in vector spaces, because $\mathfrak{R}$ can be embedded into its fraction field. In particular, a matrix $M \in M_n(\mathfrak{R})$ has rank n if and only if $\det M \neq 0$.

Lemma 2.4. (a) *Let $M \in M_n(\mathfrak{R})^\bullet$ 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 greatest common divisor of the $l \times l$ minors of M. In particular, b_1 is a gcd of the coefficients of M.*
(b) *Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathfrak{R})$. If the greatest common divisor of a, b, c, d is 1, then*

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

Proof. (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. □

2.3. **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 2.5. *Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{>1}$. Then $M_n(\mathfrak{R})$ is right-Euclidean if and only if it is left-Euclidean.*

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

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

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

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

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 2.6. *Let $\mathfrak{R}$ be a commutative ring and $n \in \mathbf{Z}_{\geq 1}$. If every right ideal of $M_n(\mathfrak{R})$ 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

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

It is straightforward that $\mathfrak{I}$ is a right ideal of $M_n(\mathfrak{R})$. We also 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

$$A = \operatorname{diag}(a, 1, \ldots, 1) \in M_n(\mathfrak{R}).$$

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 $\alpha \in M_n(\mathfrak{R})$ such that $\mathfrak{I} = \alpha M_n(\mathfrak{R})$. Then $I = \det \mathfrak{I} = (\det \alpha)\, R$, which completes the proof. □

Remark. If we do not assume $\mathfrak{R}$ to be commutative, the validity of this result is unknown.

2.4. **Length in a PID.** Let $\mathfrak{R}$ be a PID and $x \in \mathfrak{R}^\bullet$. For $\mathfrak{R}$ 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 associates, that is to say there exists $u \in \mathfrak{R}^\times$ such that $b = au$.

2.5. **A classical lemma.** The following lemma will be very useful.

Lemma 2.7. *Let $\mathfrak{R}$ be a PID.*

a. *Take a, b, $c \in \mathfrak{R}$ such that $b \neq 0$ and $\gcd(a, b, c) = 1$. Then there exists $z \in \mathfrak{R}$ such that $\gcd(a + cz, b) = 1$.*
b. *Take a, b, $c \in \mathfrak{R}$ which are not all equal to 0. Then there exists $z, t \in \mathfrak{R}$, such that $\gcd(a + cz, b + ct) = gcd(a, b, c)$, which is nonzero and divides c.*

Proof. *a.* If a and b are coprime, we can take $z = 0$. If not, write a decomposition of $b \neq 0$ as follows:

$$b = \prod_{i=1}^{l} d_i^{\alpha_i} z, \tag{2}$$

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. If $c = 0$, take $z = t = 0$, then $a \neq 0$ or $b \neq 0$, thus $\gcd(a, b) \neq 0$ and certainly divides $c = 0$. From now on, assume $c \neq 0$. 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 $\gcd(a + cz, b + ct) = d$, which divides c. □

Remark 2.8. In the proof above, we can compute z in (2) 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. □

2.6. **Conventions and notation for ordinals.** We follow the notation used by Clark [Cla14], 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 $a \in \mathfrak{A}^\bullet$,

$$\varphi(a) < \alpha. \tag{3}$$

Now, we associate to $\mathfrak{A}$ the following ordinal number, called *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

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

it is a right-Euclidean stathm.

Remark 2.9. Let $\mathfrak{R}$ be a commutative ring, $n \in \mathbf{Z}_{\geq 1}$ so that $M_n(\mathfrak{R})$ is right-Euclidean. Let θ be the smallest right-Euclidean stathm for $M_n(\mathfrak{R})$. Then for any $m, m' \in M_n(\mathfrak{R})$ such that $m \sim m'$, we have $\theta(m) = \theta(m')$. In particular, if $\mathfrak{R}$ is a PID, $\theta^{\mathsf{T}} = \theta$ and θ is the smallest left-Euclidean stathm for $M_n(\mathfrak{R})$.

Proof. It follows immediately from the fact that the function

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

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 [Cla14][2])

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

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 $M_n(\mathfrak{R})$ is a left and right-Euclidean ring.*

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

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

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

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

Notice that if $A,\, B \in M_n(\mathfrak{R})^\bullet$ 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 2.5 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:

$$\psi_2 : \begin{cases} M_2(\mathbf{Z})^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & \begin{cases} |\det M| \text{ if } \det m \neq 0, \\ \omega + |\alpha| \text{ if } M \sim \begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}. \end{cases} \end{cases}$$

See Proposition 6.5 for a more general construction.

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

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 $A = \left(\begin{smallmatrix} a & 0 \\ b & c \end{smallmatrix}\right), B = \mathrm{diag}(b_1, b_2) \in M_2(\mathfrak{R})$, 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 $Q \in M_2(\mathfrak{R})$ 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.

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

$$\lambda(b + b_2 t) + \mu(c + b_2 z) = e. \tag{4}$$

Set $Q = \begin{pmatrix} a/b_1 - \mu & \lambda \\ -t & -z \end{pmatrix}$. 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, (4) implies that $\det(A - BQ) = b_1 e$. As a result, thanks to Lemma 2.4,

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

□

Lemma 3.5. *Let $A \in M_2(\mathfrak{R})$ and $B = \mathrm{diag}(b_1, b_2) \in M_2(\mathfrak{R})$, where $b_1 | b_2$ and $b_2 \neq 0$. Then there exists $Q \in M_2(\mathfrak{R})$ such that*

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

Proof of Lemma 3.5. Thanks to Lemma 2.1, there exists $T \in GL_2(\mathfrak{R})$ 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 $Q_{\lambda,\mu} = \begin{pmatrix} \lambda & -1 \\ 0 & \mu \end{pmatrix}$ 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

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

so, thanks to Lemma 2.4,

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

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 $Q = (B^{-1}AT)T^{-1} \in M_2(\mathfrak{R})$ satifisfies $A = BQ$, or b_2 does not divide b or c, and then we apply Lemma 3.4 to find $Q \in M_2(\mathfrak{R})$ 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. 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 $n \in \mathbf{Z}_{>1}$, $A \in M_n(\mathfrak{R})$, and $B = \operatorname{diag}(b_1, \dots, b_n) \in M_n(\mathfrak{R})$, where*

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

Then there exists $Q \in M_n(\mathfrak{R})$ such that

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

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

Take $A \in M_n(\mathfrak{R})$. Thanks to Lemma 2.1, there exists $T \in GL_n(\mathfrak{R})$ 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

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

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 2.4). 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 $A' \in M_{n-1}(R)$ 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 $Q' \in M_{n-1}(R)$ 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 2.4). There exist $X, Y \in GL_{n-1}(\mathfrak{R})$ such that $YR'X = \operatorname{diag}(b'_2, \dots, b'_n)$. Then

$$\left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_{2,1} \\ \vdots \\ a_{n,1} \end{matrix} & A' \end{array}\right) - B \left(\begin{array}{c|c} 0 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q' \end{array}\right)$$

$$= \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Y \end{array}\right)^{-1} \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_{2,1} \\ \vdots \\ a_{n,1} \end{matrix} & YR'X \end{array}\right) \left(\begin{array}{c|c} 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & X \end{array}\right)^{-1}$$

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

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

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

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

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

$$Q''_\epsilon = \left(\begin{array}{c|c|cc|c} 1 & & -1 & 0 & \\ a_{2,1}/b_2 & & & & \\ \vdots & \mathfrak{o}_{l,l-2} & & \mathfrak{o}_{l-2,2} & \mathfrak{o}_{l,n-l-1} \\ a_{l-1,1}/b_{l-1} & & & & \\ \epsilon & & 1 & -1 & \\ \hline & \multicolumn{3}{c}{\mathfrak{o}_{n-l,n}} & \end{array}\right) \in M_n(\mathfrak{R}).$$

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

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

where

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

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 $b'_l | \ldots | b'_n \neq 0$. Furthermore, b_{l-1} divides all coefficients of A'''_ϵ, so thanks to Lemma 2.4, b_{l-1} divides b'_l. It follows that the invariant factors of $A'' - BQ''_\epsilon$ are $(b_1, \ldots, b_{l-1}, b'_l, \ldots, b'_n)$. 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 $Q \in M_n(\mathfrak{R})$ such that $AT - BQT = A'' - BQ''_\epsilon$, we have $A - BQ \sim \mathrm{diag}(b_1, \ldots, b_{l-1}, b'_l, \ldots, b'_n)$, which implies $\mathrm{rk}(A - BQ) = n$ 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

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

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

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

where

$$A''' = \begin{pmatrix} \mu b_{n-1} & -\lambda b_{n-1} \\ b_n & a_{n,1} \end{pmatrix} \in M_2(\mathfrak{R}).$$

Thanks to Lemma 2.4, the invariant factors of A''' are $(b_{n-1}, b_{n-1} \cdot g)$. As there exists some $Q \in M_n(\mathfrak{R})$ 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 $n > 1$, $A = \operatorname{diag}(a, 0, \dots, 0), B = \operatorname{diag}(b, 0, \dots, 0) \in M_n(\mathfrak{R})$, where $b \neq 0$. Then there exists $Q \in M_n(\mathfrak{R})$ such that*

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

Proof of Lemma 3.7. If b divides a, set $Q = \operatorname{diag}(a/b, 0, \dots, 0) \in M_n(\mathfrak{R})$. 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 $Q = (q_{i,j})_{1 \leq i,j \leq n}$ 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 $A, B \in M_n(\mathfrak{R})$, $B \neq 0$. We want to find $Q \in M_n(\mathfrak{R})$ such that $A = BQ$ or $\varphi_n(A - BQ) < \varphi_n(B)$.

Set $r = \operatorname{rk} B$. Thanks to Lemma 2.3 and Lemma 2.1, there exist $X, Y, T \in GL_n(\mathfrak{R})$, and $b_1 | b_2 | \dots | b_r \in \mathfrak{R}^\bullet$ such that

$$YBX = \operatorname{diag}(b_1, \dots, b_r, 0, \dots, 0) \in M_n(\mathfrak{R}),$$

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 $Q' \in M_n(\mathfrak{R})$ 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 $D = \operatorname{diag}(\mu_1, \dots, \mu_r, 0, \dots, 0) \in M_n(\mathfrak{R})$ 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 $A_1 \in M_r(\mathfrak{R})$ is lower triangular, $A_2 \in M_{n-r,r}(\mathfrak{R})$, $A_3 \in M_{n-r}(\mathfrak{R})$. 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 $1 \leq r < n$, $M^{(1)} \in M_r(\mathfrak{R})$, $M^{(k)} = \left(m_{i,j}^{(k)}\right)$. for $1 \leq k \leq 4$. Take $1 \leq i_0, j_0 \leq n-r$, we write $\mathrm{Extr}_r(M; i_0, j_0)$ for the matrix

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

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

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 $\mathrm{Extr}_r(YAT - YBXD; i_0, j_0)$ is lower triangular and all its diagonal coefficients are nonzero. Therefore,

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

Consequently, by setting $Q = XDT^{-1}$, we obtain $\mathrm{rk}(A - BQ) > \mathrm{rk}(B) > 0$, 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 $v = (v_j)_{1 \leq j \leq r} \in M_{r,1}(\mathfrak{R})$ such that $v_{j_0} = -1$ and all other coefficients are equal to 0. Then define

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

so that the matrix $\mathrm{Extr}_r(YAT - YBXQ'; i_0, 1)$ has rank $r+1$. Indeed, by exchanging the j_0-th and the $(r+1)$-th row of $\mathrm{Extr}_r(YAT - YBXQ'; i_0, 1)$, we obtain a lower triangular matrix whose diagonal coefficients are all nonzero. In particular,

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

It follows that $\mathrm{rk}(A - BQ) > r = \mathrm{rk}\,B$, 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 $Q' \in M_n(\mathfrak{R})$ 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 $B_1 = \mathrm{diag}(b_1, \ldots, b_r) \in M_r(\mathfrak{R})$. Thanks to Lemma 3.6, there exists $Q_1 \in M_r(\mathfrak{R})$ such that for $R_1 = A_1 - B_1 Q_1$, we have

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

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 $M_n(\mathfrak{R})$ 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.*

We have studied PIDs in Section 3, but this actually provides information about special PIRs.

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

Proof. As noted by Samuel ([Sam71]), by denoting by $\mathfrak{p} = p\mathfrak{S}$ the prime ideal of $\mathfrak{S}$ ($p \in \mathfrak{S}$), the function $\varphi : \left\{ \begin{array}{ccc} \mathfrak{S}^\bullet & \longrightarrow & \mathbf{Z}_{\geq 0} \\ x & \longmapsto & v_{\mathfrak{p}}(x) \end{array} \right.$ (which coincides with ℓ) is a Euclidean stathm. Indeed, for any $a, b \in \mathfrak{S}$, $b \neq 0$, either $v_{\mathfrak{p}}(a) < v_{\mathfrak{p}}(b)$, or $a \in b\mathfrak{S}$. The image of φ is finite for $\mathfrak{p}$ is nilpotent.

Fix now $n \in \mathbf{Z}_{>1}$ Using Proposition 1.2, we can conclude that $M_n(\mathfrak{S})$ is Euclidean, but it remains to see that it admits a right-Euclidean stathm whose image is finite.

It is known that $\mathfrak{S}$, as a special PIR, is the homomorphic image of a PID $\mathfrak{R}$ (see [Hun68]). We extend the surjective ring homomorphism $\pi : \mathfrak{R} \longrightarrow \mathfrak{S}$ to a surjective ring homomorphism $\pi : M_n(\mathfrak{R}) \longrightarrow M_n(\mathfrak{S})$. Remark in particular that $\pi(GL_n(\mathfrak{R})) \subseteq GL_n(\mathfrak{S})$. Define the function

$$\psi_n : \left\{ \begin{array}{ccc} M_n(\mathfrak{S})^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & \min\{\varphi_n(\hat{M}), \hat{M} \in M_n(\mathfrak{R}), \pi(\hat{M}) \sim M\}. \end{array} \right.$$

Then ψ_n is a right-Euclidean stathm.

Indeed, take A, $B \in M_n(\mathfrak{S})$, $B \neq \mathfrak{o}_n$. There exist $\hat{B} \in M_n(\mathfrak{R})$, X, $Y \in GL_n(\mathfrak{S})$ such that $\pi(\hat{B}) = YBX$ and $\psi_n(B) = \varphi_n(\hat{B})$. Take $\hat{A} \in M_n(\mathfrak{R})$ such that $YA = \pi(\hat{A})$. Then, we can divide $\hat{A}$ by $\hat{B}$, i.e. there exists $\hat{Q} \in M_n(\mathfrak{R})$ such that

$$\varphi_n\left(\hat{A} - \hat{B}\hat{Q}\right) < \varphi_n(\hat{B}) = \psi_n(B).$$

Set $Q = X\pi(\hat{Q})$, then $\pi\left(\hat{A} - \hat{B}\hat{Q}\right) = Y(A - BQ) \sim A - BQ$. It follows that

$$\psi_n(A - MQ) \leq \varphi_n\left(\hat{A} - \hat{B}\hat{Q}\right) < \psi_n(B).$$

Besides, as π is a ring homomorphism, every element M of $M_n(\mathfrak{R})$ is equivalent to a diagonal matrix, i.e.

$$M \sim \mathrm{diag}(m_1, \ldots, m_r, 0, \ldots, 0),$$

where $m_1 | \ldots | m_r \neq 0$. But every nonzero element h of $\mathfrak{R}$ can be written as $h = up^a$, where $u \in \mathfrak{R}^\times$ and $a \in \mathbf{Z}$ is such that $0 \leq a < t$, where t is such that $\mathfrak{p}^t = (0)$ and is independent of h.

Therefore, every element M of $M_n(\mathfrak{R})$ satisfies

$$M \sim \mathrm{diag}(p^{a_1}, \ldots, p^{a_r}, 0, \ldots, 0),$$

where $0 \leq r \leq n$, $a_1 \leq a_2 \leq \cdots \leq a_r < t$. We take a prime $\hat{p} \in \hat{\mathfrak{R}}$ such that $\pi(\hat{p}) = p$, and then define $\hat{D} = \mathrm{diag}(\hat{p}^{a_1}, \ldots, \hat{p}^{a_r}, 0, \ldots, 0)$. If follows that $\pi(\hat{D}) \sim M$. Consequently, if $M \neq \mathfrak{o}_n$, then

$$\psi_n(M) \leq \varphi_n(D) = (n - r)\omega^n + \sum_{i=1}^{r} a_i \omega^{r-i}.$$

As $r \leq n$ and for any $1 \leq i \leq r$, $0 \leq a_i < t$, $\psi_n(M)$ can only take finitely many values. Therefore, $e(M_n(\mathfrak{R})) < \omega$, which completes the proof. □

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 [Cla14, Theorem 3.13], where the commutativity hypothesis is not used. We give some details for 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 (3), 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 ([Cla14, Theorem 3.40[3]]). 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 $e\left(\prod_{i=1}^{l} \mathfrak{A}_i\right) < \omega$.

[3]As in 2, 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 $M_n(\mathfrak{R})$ is right-Euclidean, then every right ideal of $M_n(\mathfrak{R})$ is principal. Therefore, thanks to Proposition 2.6, $\mathfrak{R}$ 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, $M_n(\mathfrak{R})$ is isomorphic to $\prod_{i=1}^{l} M_n(\mathfrak{R}_i)$. Thanks to Theorem 3.1 and Remark 4.3, for any $1 \leq i \leq l$, $M_n(\mathfrak{R}_i)$ is Euclidean. Using Lemma 4.4, we can conclude that $\prod_{i=1}^{l} M_n(\mathfrak{R}_i)$ 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 $\mathfrak{A} = M_n(\mathfrak{R})$, 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, $B \in M_n(\mathfrak{R})$, we can compute some $Q \in M_n(\mathfrak{R})$ 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 explicitely computed assuming (a).

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

Algorithm 5.2. Input: $A, B \in M_n(\mathfrak{R})$.
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 $Q, R \in M_n(\mathfrak{R})$ 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, $V \in M_n(\mathfrak{R})$ such that

$$AU + BV = D, \tag{5}$$

where D is a greatest common left-divisor[4] (or glcd for short) of A and B in $M_n(\mathfrak{R})$.

[4] D is not unique, it is defined up to multiplication by an element of $GL_n(\mathfrak{R})$ on the right.

If $B = 0$, then Algorithm 5.2 returns $D = A$, so in this case $D = \operatorname{diag}(1, \dots, 1, a)$. If $B \neq 0$, by construction, at each further step of the execution of Algorithm 5.2, $\varphi_n(D) \leq \varphi_n(B) = \ell(b)$. Therefore, $\operatorname{rk} D = n$ and $D \sim \operatorname{diag}(1, \dots, 1, \lambda)$ for some $\lambda \in \mathfrak{R}$.

This λ is defined up to multiplication by a unit, we choose $\lambda = \det D$. Then, denoting by C the cofactor matrix of D, (5) implies that

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

Identifying the coefficients in position (n, n), we obtain $au + bv = \lambda$ for some $u, v \in \mathfrak{R}$. It remains to see that λ is actually the gcd of a and b. To see this, observe that D is a left-divisor of A and B, so $\lambda = \det D$ divides $a = \det A$ and $b = \det B$. □

5.2. **Computation of gcd of matrices, an example.** It is straightforward to remark that Algorithm 5.2 above will return a glcd of A and B in a finite number of steps. We can similarly compute greatest common right divisors (grcd).

The following example illustrates such computations, and the fact that grcd and glcd may be unconnected.

Example 5.3. In $M_3(\mathbf{Z})$, 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 glcd 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 grcd 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 glcds and grcds of matrices in $M_n(\mathfrak{R})$. Indeed, given $A, B \in M_n(\mathfrak{R})$, we can proceed as follows. Consider the matrix $\left(A \,\middle|\, B\right) \in M_{n,2n}(\mathfrak{R})$ and compute $R \in M_n(\mathfrak{R})$, $U \in GL_{2n}(\mathfrak{R})$ such that

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

Then R is a glcd of A and B.

Likewise, we can compute $V \in GL_{2n}(\mathfrak{R})$, $S \in M_n(\mathfrak{R})$ such that

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

then S^{T} is a grcd of A and B.

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

$$\begin{aligned} [Q_1] &= Q_1, \\ [Q_1, Q_2, \dots, Q_k] &= Q_1 + [Q_2, \dots, Q_k]^{-1}, \quad \text{if } [Q_2, \dots, Q_k] \in GL_n(\mathfrak{F}). \end{aligned}$$

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

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

Proposition 5.5. *Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$, set $\mathfrak{F}$ to be the fraction field of $\mathfrak{R}$. Then for any $X \in M_n(\mathfrak{F})$, there exist $k \in \mathbf{Z}_{>0}$ and $Q_1, \dots, Q_k \in M_n(\mathfrak{R})$ 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 7.10).

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 $B = b \cdot \mathfrak{1}_n \in M_n(\mathfrak{R})$, $A = BX \in M_n(\mathfrak{R})$.

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

$$\text{(6)} \qquad \begin{cases} A - BQ_1 = R_1, \\ B - R_1Q_2 = R_2, \\ \qquad\vdots \\ R_{k-2} - R_{k-1}Q_k = R_k, \end{cases}$$

$$\text{(7)} \qquad \begin{gathered} \text{with } R_k = \mathfrak{o}_n, \text{ for all } 1 \leq i < k,\ R_i \neq 0, \text{ and} \\ \varphi_n(R_{k-1}) < \varphi_n(R_{k-2}) < \cdots < \varphi_n(R_1) < \varphi_n(B). \end{gathered}$$

But B has rank n, so (7) implies that for all $1 \leq i < k$, R_i has also rank n, i.e.

$$\text{(8)} \qquad R_k = 0 \qquad \text{and} \qquad R_i \in GL_n(\mathfrak{F}), \qquad \text{for all } 1 \leq i < k.$$

We prove by induction on k that for any division chain satisfying conditions (6) and (8), 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 (6) and (8) starting from B, R_1. So, by induction hypothesis, $B = R_1[Q_2, \dots, Q_k]$. But $R_1, B \in GL_n(\mathfrak{F})$, so

$[Q_2, \dots, Q_k] \in GL_n(\mathfrak{F})$ 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 $X = \begin{pmatrix} 1/x & 0 \\ 2/(x+3) & 3 \end{pmatrix} \in M_2(\mathbf{Q}(x))$.

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 7.6 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

$$e(M_n(\mathfrak{R})) \leq (n-1)\omega^n + \omega. \tag{9}$$

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

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 $e(M_n(\mathfrak{R})) > \omega$ (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 $\chi : M_n(\mathfrak{R})^\bullet \longrightarrow \mathcal{O}$. Then, for any $\alpha \in \mathbf{Z}_{>0}$, there exists $M_\alpha \in M_n(\mathfrak{R})$ such that $\chi(M_\alpha) \geq (n-1)\omega + \alpha$. In particular, $e(M_n(\mathfrak{R})) \geq n\omega$.*

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

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

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 $Q \in M_n(\mathfrak{R})$ 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 $Q' \in M_n(\mathfrak{R})$ 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

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

is a left and right-Euclidean stathm[5], so $e(M_n(\mathfrak{F})) < \omega$.

(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 $n > 1$, $e(M_n(\mathfrak{R})) < \omega$ (see Remark 4.3).

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

[5]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].

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 $1 \leq i \leq l$, $e\left(M_n\left(\mathfrak{R}_i\right)\right) < \omega$ (see Remark 6.2 (3) and Remark 4.3). So, thanks to Remark 4.5, $e\left(M_n\left(\mathfrak{R}\right)\right) < \omega$.

Conversely, assume that $M_n\left(\mathfrak{R}\right)$ admits the right-Euclidean stathm $\varphi : \begin{cases} M_n\left(\mathfrak{R}\right)^\bullet & \longrightarrow & \mathcal{O} \\ M & \longmapsto & \varphi(M) \end{cases}$. First remark that $\mathfrak{R}$ is a PIR thanks to Proposition 2.6. Then, thanks to Proposition 4.2, $\mathfrak{R}$ 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 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

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

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

In passing, we proved that for any $n \in \mathbf{Z}_{>1}$, there exists no commutative ring $\mathfrak{R}$ such that $\omega \leq e\left(M_n\left(\mathfrak{R}\right)\right) < n\omega$.

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 $M_n\left(\mathfrak{R}\right)$ is right-Euclidean and*

$$ln\omega \leq e\left(M_n\left(\mathfrak{R}\right)\right) < l(n-1)\omega^n + (l+1)\omega.$$

Proof. Just apply (9), 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 $e(M_n\left(\mathfrak{R}\right))$.

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

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

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

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 $e(M_n\left(\mathfrak{R}\right)) \leq n \otimes e(\mathfrak{R})$.

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 $A, B \in M_n\left(\mathfrak{R}\right)$,

$B \neq 0$. Write $r = \operatorname{rk} B \geq 1$. Take $X, Y \in GL_n(\mathfrak{R})$ such that $YBX = \operatorname{diag}(b_1, \ldots, b_r, 0, \ldots, 0)$. 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 paragraph 3.5 that there exists $Q \in M_n(\mathfrak{R})$ 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 $A' = (a_{i,j})_{1 \leq i,j \leq r}, B' = \operatorname{diag}(b_1, \ldots, b_r) \in M_r(\mathfrak{R})$. By the induction hypothesis, there exists $Q' \in M_r(\mathfrak{R})$ such that $A' = B'Q'$ or $\psi_r(A' - B'Q') < \psi_r(B')$. Setting $Q \in M_n(\mathfrak{R})$ 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 $T \in GL_n(\mathfrak{R})$ such that YAT is lower triangular (Lemma 2.1) 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 $A' = (a'_{i,j})_{1 \leq i,j < n} \in M_{n-1}(\mathfrak{R})$. 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 $\hat{A} = \operatorname{diag}(a_1 - \lambda^\star b_1, 1, \ldots, 1) \cdot A'$ and $\hat{B} = \operatorname{diag}(b_2(a_1 - \lambda^\star b_1), b_3, \ldots, b_n) \in M_{n-1}(\mathfrak{R})^\bullet$, with $\operatorname{rk} \hat{B} = n - 1$. By the induction hypothesis, we may perform the Euclidean division of $\hat{A}$ by $\hat{B}$: there exists $\hat{Q} \in M_{n-1}(\mathfrak{R})$ 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 $\det(\hat{A} - \hat{B}\hat{Q}) = (a_1 - \lambda^\star b_1) \det(A' - \operatorname{diag}(b_2, \ldots, b_n)\hat{Q})$, and setting $Q \in M_n(\mathfrak{R})$ 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

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

Consequently,

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

Suppose now that $\hat{A} = \hat{B}\hat{Q}$. Then we also have $A' = \operatorname{diag}(b_2, \ldots, b_n)\hat{Q}$. We distinguish two cases. First, assume that $a_1 - b_1\lambda \neq 0$. Setting $Q \in M_n(\mathfrak{R})$ 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 $Q', T' \in M_n(\mathfrak{R})$ such that

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

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 $\hat{Q}' \in M_{n-1}(\mathfrak{R})$ such that

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

or we find some $Q'' \in M_n(\mathfrak{R})$ 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 $n \in \mathbf{Z}_{>0}$, $e(M_n(\mathfrak{R})) = n\omega$.*

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

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

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 $n \in \mathbf{Z}_{>1}$, $M_n(\mathfrak{R})$ is Euclidean and $e(M_n(\mathfrak{R})) \leq n\omega$. If besides $\mathfrak{R}$ is not a field, then $e(M_n(\mathfrak{R})) = n\omega$.*

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

(10) 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 $A \in M_n(\mathfrak{R})$, there exists $Q(A,D) \in M_n(\mathfrak{R})$ 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 $D' \in M_n(\mathfrak{R})$ such that $\varphi_n(D') < \varphi_n(D)$. Therefore, $\theta(A - DQ(A,D)) = \theta(D') < \omega$. Let $\mathcal{S} \subseteq M_n(\mathfrak{R}) \setminus DM_n(\mathfrak{R})$ such that $\mathcal{S} \cup \{0\}$ is a system of representatives of $M_n(\mathfrak{R})/DM_n(\mathfrak{R})$, 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 (10) holds for $r = n$. We will prove (10) for $r = r_0 - 1$.

Now let us assume that we have some $1 < r_0 \leq n$, such that for all $r_0 \leq r \leq n$, (10) 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 $A \in M_n(\mathfrak{R})$. There exists $T \in GL_n(\mathfrak{R})$ 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. 12) that there exists $Q'(A,D) \in M_n(\mathfrak{R})$ 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 $Q'(A,D) \in M_n(\mathfrak{R})$ 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 $\mathcal{S} \subseteq M_n(\mathfrak{R}) \setminus DM_n(\mathfrak{R})$ such that $\mathcal{S} \cup \{0\}$ is a system of representatives of $M_n(\mathfrak{R})/DM_n(\mathfrak{R})$. Then, thanks to Lemma 2.10, we have $\theta(D) \leq \sup_{a \in \mathcal{S}} \inf_{Q \in M_n(\mathfrak{R})} \theta(A + DQ) + 1$. But for all $A \in \mathcal{S}$, there exists $T \in GL_n(\mathfrak{R})$ such that $AT \in \mathcal{S}_1$ or $AT \in \mathcal{S}_2$, thus

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

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

(11)
$$\theta(D) \leq \sup\left(\sup_{A' \in \mathcal{S}_1} \inf_{Q \in M_n(\mathfrak{R})} \theta(A' + DQ), \sup_{A' \in \mathcal{S}_2} \inf_{Q \in M_n(\mathfrak{R})} \theta(A' + DQ) \right) + 1.$$

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

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

Thus

$$\sup_{A' \in \mathcal{S}_1} \inf_{Q \in M_n(\mathfrak{R})} \theta(A' + DQ) < (n - r_0 + 2)\omega. \tag{12}$$

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

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

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

$$\sup_{A' \in \mathcal{S}_1} \inf_{Q \in M_n(\mathfrak{R})} \theta(A' + DQ) < (n - r_0 + 2)\omega. \tag{13}$$

So, by combining (11), (12), and (13), we obtain $\theta(D) < (n - r_0 + 2)\omega$ as expected.

Finally, consider any matrix $A \in M_n(\mathfrak{R})^\bullet$. Thanks to Lemma 2.3, A is equivalent to some diagonal matrix D. Thanks to (10), $\theta(D) < n\omega$, and Remark 2.9 implies that $\theta(A) = \theta(D)$. We conclude that $e(M_n(\mathfrak{R})) = \theta(0) \leq n\omega$.

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

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

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

7. k-stage Euclidean property

In this section, we will 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 $(q_i)_{1 \leq i \leq k} \in \mathfrak{A}^k$ and $(r_i)_{1 \leq i \leq k} \in \mathfrak{A}^k$ such that

$$\begin{cases} a - bq_1 = r_1, \\ b - r_1 q_2 = r_2, \\ r_1 - r_2 q_3 = r_3, \\ \vdots \\ r_{k-2} - r_{k-1} q_k = r_k, \end{cases} \tag{14}$$

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.
- 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 it admits a terminating l-stage division chain whose set of remainders is preserved for any $l \geq k$.

Proof. The first point is clear. As for the second one, simply notice that $r_{k-2} - r_{k-1}q_k = 0$ can be turned into

$$\begin{cases} r_{k-2} - r_{k-1}(q_k - 1) = r_{k-1}, \\ r_{k-1} - r_{k-1} \cdot 1 = 0. \end{cases}$$

□

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 for an ω-stage right-Euclidean ring may have non-principal right ideals.

Let $\mathfrak{R}$ be a commutative ring. Let us also notice that we can 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 (14), which leads to define ω-stage left-Euclidean rings and k-stage left-Euclidean rings. But for $(a, b) \in M_n(\mathfrak{R})$, $b \neq \mathfrak{o}_n$, (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, $M_n(\mathfrak{R})$ is k-stage right-Euclidean if and only if it is k-stage left-Euclidean, and likewise, $M_n(\mathfrak{R})$ is ω-stage right-Euclidean if and only if it is ω-stage left-Euclidean.

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

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

(1) $M_n(\mathfrak{R})$ is 2-stage right-Euclidean and left-Euclidean.
(2) $M_n(\mathfrak{R})$ is $(3n-1)$-stage terminating right and left-Euclidean.

The remainder of this section will be devoted to the proof of this statement. We will first deal with PIDs, then extend properties to PIRs.

7.2. **2-stage Euclidean property over a PID.** Consider first the case $n = 2$.

Proposition 7.4. *Let $\mathfrak{R}$ be a PID. Then $M_2(\mathfrak{R})$ is 2-stage right-Euclidean.*

Proof. Let us define

$$f : \begin{cases} M_2(\mathfrak{R}) & \longrightarrow & \mathbf{Z}_{\geq 0} \\ \mathfrak{o}_2 & \longmapsto & 0 \\ M \sim \operatorname{diag}(b_1, b_2), b_1 | b_2, b_1 \neq 0 & \longmapsto & \ell(b_1) + 1. \end{cases}$$

We will prove that $M_2(\mathfrak{R})$ is 2-stage Euclidean with respect to f. Take $A, B \in M_2(\mathfrak{R})$, $B \neq \mathfrak{o}_2$. There exist $X, Y, T \in GL_2(\mathfrak{R})$, $a, b, c, b_1 | b_2 \in \mathfrak{R}$ such that

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

If b_1 does not divide a, then

$$A - BX \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} T^{-1} = Y^{-1} \begin{pmatrix} a & -b_1 \\ b & c \end{pmatrix} T^{-1}, \tag{15}$$

whose first invariant factor is a strict divisor of b_1 (see Lemma 2.4).

If b_1 divides a, we distinguish two sub-cases. First, if $b = c = 0$, then we have

$$A - BX \begin{pmatrix} a/b_1 & 0 \\ 0 & 0 \end{pmatrix} T^{-1} = \mathfrak{o}_2. \tag{16}$$

Then, if $b \neq 0$ or $c \neq 0$, there exist $t, z \in \mathfrak{R}$ such that $\gcd(b + b_2 t, c + b_2 z) = e$ is nonzero and divides b_2 (see Lemma 2.7). Take $\lambda, \mu \in \mathfrak{R}$ such that $\lambda(b + b_2 t) + \mu(c + b_2 z) = e$. We obtain the following 2-stage division.

$$\begin{cases} A - BX \begin{pmatrix} a/b_1 - \mu & \lambda \\ -t & -z \end{pmatrix} T^{-1} = Y^{-1} \begin{pmatrix} b_1\mu & -b_1\lambda \\ b + b_2 t & c + b_2 z \end{pmatrix} T^{-1} \\ B - Y^{-1} \begin{pmatrix} b_1\mu & -b_1\lambda \\ b + b_2 t & c + b_2 z \end{pmatrix} T^{-1} T \begin{pmatrix} (c + b_2 z)/e & \lambda b_2/e \\ -(b + b_2 t)/e & \mu b_2/e \end{pmatrix} X^{-1} \\ \qquad\qquad = \mathfrak{o}_2. \end{cases} \tag{17}$$

In each case, (15), (16), and (17) provide a 2-stage Euclidean division for the pair (a, b) with respect to f. □

Remark 7.5. With the notation of the proof above, if the first invariant factor b_1 of B divides a_1, we obtain a terminating 2-stage right-Euclidean division starting from the pair (a, b). If b_1 does not divide a_1, then with a single division, we obtain the pair (B, R_1) where

$$R_1 = Y^{-1} \begin{pmatrix} a_1 & b_1 \\ a_2 & a_3 \end{pmatrix} X^{-1}.$$

But the first invariant factor of R_1 is a (strict) divisor of b_1, which divides all coefficients of B, so it divides the coefficient in position $(1, 1)$ of BT' for any $T' \in GL_n(\mathfrak{R})$. Consequently, we can obtain a terminating 3-stage division chain starting from (a, b).

Remark 7.6. *1.* In the proof of Proposition 7.4 above, when we obtain a suitable remainder with a 1-stage division, it is exactly the remainder that we built in Section 3 to prove Proposition 3.2. If we obtain a suitable remainder with a 2-stage division, then each division also corresponds to the division used in Section 3. Consequently, applying Euclid's algorithm with φ_2 terminates in at most 3 divisions.

2. If we assume that B has rank 2, then thanks to the definition of φ_2, each remainder in the 3-stage division chain built above is either equal to $\mathfrak{o}_2$, or has full rank. The following corollary immediately follows.

Corollary 7.7. *Let $\mathfrak{R}$ be a PID and $\mathfrak{F}$ its fraction field. Then for every $X \in M_2(\mathfrak{F})$, there exist $Q_1, Q_2, Q_3 \in M_2(\mathfrak{R})$ such that*

$$X = [Q_1, Q_2, Q_3].$$

This explains why we obtained such a decomposition in continued fractions in Example 5.6.

Now, we consider arbitrary size $n > 1$.

Proposition 7.8. *Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$. Then $M_n(\mathfrak{R})$ is 2-stage right-Euclidean.*

Proof. Let us define

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

We will prove by induction on $n \geq 2$ that $M_n(\mathfrak{R})$ is 2-stage right-Euclidean with respect to f_n. For $n = 2$, it is Proposition 7.4.

Take $n > 2$, $A, B \in M_n(\mathfrak{R})$, $B \neq \mathfrak{o}_n$. There exist $X, Y, T \in GL_n(\mathfrak{R})$ such that $YBX = \operatorname{diag}(b_1, b_2, \ldots, b_r, 0, \ldots, 0)$ 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 $E = (e_{i,j})_{1 \leq i \leq n-1, 1 \leq j \leq n} \in M_{n-1,n}(\mathfrak{R})$, 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 $v = (v_i)_{1 \leq i \leq n} \in M_{n,1}(\mathfrak{R})^\bullet$ such that $v \in \ker E$ and the coordinates of v are coprime, i.e.

$$\sum_{i=1}^{n} \mathfrak{R} v_i = \mathfrak{R}. \tag{18}$$

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

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

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 $\operatorname{diag}(e, 0, \ldots, 0)$, 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 (18), take $\lambda = (\lambda_i)_{1 \leq i \leq n} \in M_{1,n}(\mathfrak{R})$ such that $\sum_{i=1}^{n} \lambda_i v_i = -\frac{a_{1,1} v_1}{b_1} + 1$. Consider the following 2-stage division chain:

$$\begin{cases} A - BX \left(\begin{array}{c} -\lambda \\ \hline \mathfrak{o}_{n-1,n} \end{array}\right) T^{-1} = Y^{-1} \left(\begin{array}{ccccc} a_{1,1} + \lambda_1 b_1 & \lambda_2 b_1 & \cdots & \lambda_n b_1 \\ \hline \multicolumn{5}{c}{E} \end{array}\right) T^{-1}, \\ B - Y^{-1} \left(\begin{array}{ccccc} a_{1,1} + \lambda_1 b_1 & \lambda_2 b_1 & \cdots & \lambda_n b_1 \\ \hline \multicolumn{5}{c}{E} \end{array}\right) T^{-1} T \left(v \;\middle|\; \mathfrak{o}_{n,n-1}\right) X^{-1} = \mathfrak{o}_n. \end{cases}$$

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 $M \in M_{r,n}(\mathfrak{R})$ and $M^{(0)} \in M_{n-r,n}(\mathfrak{R})$ such that

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

We build inductively $v^{(i)} \in M_{n,1}(\mathfrak{R})$ and $\lambda^{(i)} \in M_{1,n}(\mathfrak{R})$ for $1 \leq i \leq r$ as follows. The kernel of $M^{(0)}$ is nontrivial, so there exists $v^{(1)} = \left(v_i^{(1)}\right)_{1 \leq i \leq n} \in M_{n,1}(\mathfrak{R})$ 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 $\lambda^{(1)} \in M_{1,n}(\mathfrak{R})$ 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 $M^{(i_0)} \in M_n(\mathfrak{R})$ 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 $v^{(i_0+1)} \in M_{n,1}(\mathfrak{R})$ 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 $\lambda^{(i_0+1)} \in M_{1,n}(\mathfrak{R})$ satisfying $\lambda^{(i_0+1)}v^{(i_0+1)} = (1)$. Now, we can exhibit the following 2-stage division chain.

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

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

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

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 $Q_1', Q_2', R_1', R_2' \in M_{n-1}(\mathfrak{R})$ such that

$$\begin{cases} A' - B'Q_1' = R_1', \\ B' - R_1'Q_2' = R_2', \end{cases} \tag{19}$$

and $f_{n-1}(R'_2) < f_{n-1}(B')$.
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 (19), we get

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

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 (19) to size n:

$$(20) \qquad \begin{cases} A - BX \left(\begin{array}{c|c} 0 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q'_1 \end{array}\right) T^{-1} = Y^{-1} \left(\begin{array}{c|c} a_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{array}{c} a_2 \\ \vdots \\ a_n \end{array} & R'_1 \end{array}\right) T^{-1}, \\ B - Y^{-1} \left(\begin{array}{c|c} a_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{array}{c} a_2 \\ \vdots \\ a_n \end{array} & R'_1 \end{array}\right) T^{-1} T \left(\begin{array}{c|c} 0 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q'_2 \end{array}\right) X^{-1} = R_2, \end{cases}$$

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 (20) 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 $b'_2 | b'_3 | \ldots | b'_{r'} \neq 0$ (Lemma 2.1). By construction, these invariant factors satisfy

$$(21) \quad \ell \left(\prod_{i=2}^{\min(r',n-1)} b'_i \right) = f_{n-1}(R'_2) - 1 < f_{n-1}(B') - 1 = \ell \left(\prod_{i=2}^{\min(r,n-1)} b_i \right).$$

Besides, we can still extend (19) to size n as in (20). Then R_2 has rank r', and $R_2 \sim \operatorname{diag}(b''_1, b''_2, \ldots, b''_{r'}, 0, \ldots, 0)$, with $b''_1 | b''_2 | \ldots | b''_{r'} \neq 0$ (Lemma 2.3). But, thanks to Lemma 2.4, $\prod_{i=1}^{\min(r',n-1)} b''_i$ divides $b_1 \prod_{i=2}^{\min(r',n-1)} b'_i$, so (21)

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 (20) 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.

7.3. **Terminating division chains.**

Proposition 7.9. *Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$. Then for all A, $B \in M_n(\mathfrak{R})$, with $\operatorname{rk} B = n$, there exists a $(2n-1)$-stage terminating division chain starting from (A, B) and such that all the intermediate remainders R_i have rank n, for $1 \leq i < k$.*

Proof. 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 was observed in Remark 7.6.

Take $n > 2$, and A, $B \in M_n(\mathfrak{R})$, then there exist X, Y, $T \in GL_n(\mathfrak{R})$, $(a_i)_{1\leq i\leq n} \in \mathfrak{R}^n$, $A' \in M_{n-1}(\mathfrak{R})$ lower triangular, $B' \in M_{n-1}(\mathfrak{R})$ diagonal with rank $n-1$ such that

$$YAT = \left(\begin{array}{c|c} a_1 & \mathfrak{o}_{1,n-1} \\ \hline \begin{matrix} a_2 \\ \vdots \\ a_n \end{matrix} & A' \end{array}\right) \qquad \text{and} \qquad YBX = \left(\begin{array}{c|c} b_1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & B' \end{array}\right). \tag{22}$$

If b_1 does not divide a_1, thanks to the 1st step of proof of Lemma 3.6, there exists $Q \in M_n(\mathfrak{R})$ such that

$$A - BQ \sim \operatorname{diag}(b_1', \ldots, b_n'),$$

where $b_1' | \ldots | b_n' \neq 0$, and $b_1' | b_1$. In other words, after at most 1 division, we can assume that we have (22), with the further assumption that b_1 divides all coefficients of A', and in particular, b_1 divides a_1.

By the induction hypothesis, there exists a $(2n-2)$-stage[6] terminating division chain in $M_{n-1}(\mathfrak{R})$. Let us denote by Q_k' its quotients and R_k' its remainders, for $1 \leq k \leq 2n-2$.

Set $Q_1 = \left(\begin{array}{c|c} a_1/b_1 - 1 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q_1' \end{array}\right)$, $Q_i = \left(\begin{array}{c|c} 0 & \mathfrak{o}_{1,n-1} \\ \hline \mathfrak{o}_{n-1,1} & Q_i' \end{array}\right)$, 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

[6]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.

terminating division stage with the following remainders:

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

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

These remainders have rank n. All in all, we obtain a $2n-1$-stage terminating division chain starting from (A, B) with the required properties. □

Corollary 7.10. *Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$. Denote by $\mathfrak{F}$ the fraction field of $\mathfrak{R}$. Then for all $X \in M_n(\mathfrak{F})$, there exist Q_1, Q_2, …, $Q_{2n-1} \in M_n(\mathfrak{R})$ 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 7.9 implies that we can obtain a $(2n-1)$-stage terminating division chain satisfying (8). □

Corollary 7.11. *Let $\mathfrak{R}$ be a PID and $n \in \mathbf{Z}_{>1}$. Then $M_n(\mathfrak{R})$ is a $(3n-2)$-stage terminating right-Euclidean ring.*

Proof. Let A, $B \in M_n(\mathfrak{R})$, with $B \neq \mathfrak{o}_n$. Set $r = \operatorname{rk} B$. In the proof of Proposition 3.2, in paragraph 3.5, we saw that either there exists some $Q \in M_n(\mathfrak{R})$ such that $\operatorname{rk}(A - BQ) > r$, or there exist $X, Y, T \in GL_n(\mathfrak{R})$ such that

$$YBX = \operatorname{diag}(b_1, \ldots, b_r, 0, \ldots, 0) \quad \text{and} \quad YAT = \left(\begin{array}{c|c} A' & \mathfrak{o}_{r,n-r} \\ \hline \mathfrak{o}_{n-r,r} & \mathfrak{o}_{n-r} \end{array}\right). \tag{23}$$

So, after at most $n - r \leq n - 1$ divisions, we can consider a pair (A, B) satisfying (23). Thanks to Proposition 7.9, with $2n-1$ further divisions, we obtain a terminating division chain. In total, we apply at most $2n-1+n-1 = 3n-2$ divisions. □

7.4. **k-stage Euclidean properties over a PIR.** The purpose of this paragraph will be to prove Theorem 7.3. First, let us consider special PIRs.

Lemma 7.12. *Let $\mathfrak{S}$ be a special PIR and $n \in \mathbf{Z}_{>1}$. Then $M_n(\mathfrak{S})$ is a $(3n-2)$-stage terminating right-Euclidean ring.*

Proof. Take $(A, B) \in M_n(\mathfrak{S}) \times M_n(\mathfrak{S})^\bullet$. There exists a PID $\mathfrak{R}$ and a surjective ring homomorphism $\pi : \mathfrak{R} \longrightarrow \mathfrak{S}$ (see [Hun68]). We extend π to a surjective ring homomorphism $\pi : M_n(\mathfrak{R}) \longrightarrow M_n(\mathfrak{S})$. Then there exist $\hat{A}, \hat{B} \in M_n(\mathfrak{R})$ such that $\pi(\hat{A}) = A$ and $\pi(\hat{B}) = B$, with $\hat{B} \neq \mathfrak{o}_n$. Thanks to Corollary 7.11, there exists a terminating $(3n-2)$-stage division chain in $M_n(\mathfrak{R})$ starting from $(\hat{A}, \hat{B})$. The ring homomorphism π converts it into a terminating $(3n-2)$-stage division chain in $M_n(\mathfrak{S})$ starting from (A, B). □

Let us notice then that 2-stage right-Euclidean rings and terminating division chains are preserved by products.

Lemma 7.13. *1. The direct product of finitely many 2-stage right-Euclidean rings is a 2-stage right-Euclidean ring.*
2. Let $k \in 2\mathbf{Z}_{>1}$. The direct product of finitely many k-stage terminating right-Euclidean rings is a k-stage terminating right-Euclidean ring.

Proof. By a clear induction, it is enough to prove it for the product of two rings.

1. 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 $(b^{(1)}, b^{(2)}) \neq (0, 0)$.
1.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

$$\left\{ \begin{array}{l} a^{(i)} - b^{(i)} q_1^{(i)} = r_1^{(i)}, \\ b^{(i)} - r_1^{(i)} q_2(i) = r_2^{(i)}, \\ \text{and } f_i\left(r_2^{(i)}\right) < f_i\left(b^{(i)}\right). \end{array} \right. \tag{24}$$

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

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

1.b. Now, assume that $b^{(1)} = 0$ and $b^{(2)} \neq 0$. Then (24) 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

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

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

2. Let $\mathfrak{A}_1$, $\mathfrak{A}_2$ be two k-stage terminating right-Euclidean rings. Take $a^{(i)}, b^{(i)} \in \mathfrak{A}_i$, for $i = 1, 2$, with $(b^{(1)}, b^{(2)}) \neq (0, 0)$.
2.a. First, assume that $b^{(1)} \neq 0$ and $b^{(2)} \neq 0$. Then for $i = 1, 2$, we have k-stage a terminating divisions chain, which we describe with the quotients $(q_j^{(i)})_{1 \leq j \leq k}$ and the remainders $(r_j^{(i)})_{1 \leq j \leq k}$, $r_k^{(i)} = 0$. Then we have a terminating k-stage division chain starting from $\left((a^{(1)}, a^{(2)}), (b^{(1)}, b^{(2)})\right)$ obtained with the following quotients q_j and remainders r_j, where for $1 \leq j \leq k$,

$$q_j = \left(q_j^{(1)}, q_j^{(2)}\right) \qquad \text{and} \qquad r_j = \left(r_j^{(1)}, r_j^{(2)}\right).$$

2.b. If $b^{(1)} \neq 0$ and $b^{(2)} \neq 0$, let $(q_j^{(1)})_{1\leq j\leq k}$ and $(r_j^{(1)})_{1\leq j\leq k}$ be the quotients and the remainders of a terminating division chain in $\mathfrak{A}_1$ starting from $(a^{(1)}, b^{(1)})$. Then we have the following terminating k-stage division chain starting from $\big((a^{(1)}, a^{(2)}), (b^{(1)}, 0)\big)$ and defined by the quotients q_j and the remainders r_j, where for $1 \leq j \leq k$,

$$q_j = (q_j^{(1)}, 0) \qquad \text{and} \qquad r_j = \begin{cases} (r_j^{(1)}, a_j^{(2)}) & \text{if } j \text{ is odd,} \\ (r_j^{(1)}, 0) & \text{if } j \text{ is even.} \end{cases}$$

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

Proof of Theorem 7.3. 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 $M_n(\mathfrak{R})$ can be identified with $\prod_{i=1}^{l} M_n(\mathfrak{R}_i)$.

(1) If $\mathfrak{R}_i$ is a PID, then $M_n(\mathfrak{R}_i)$ is 2-stage right-Euclidean (Proposition 7.8). If $\mathfrak{R}_i$ is a special PIR, then $M_n(\mathfrak{R}_i)$ is right-Euclidean with $e(M_n(\mathfrak{R}_i)) < \omega$ (Remark 4.3), therefore $M_n(\mathfrak{R}_i)$ is also 2-stage right-Euclidean. Thus, we can conclude with Lemma 7.13 that $M_n(\mathfrak{R})$ is indeed 2-stage right-Euclidean.

(2) If $\mathfrak{R}_i$ is a PID, then $M_n(\mathfrak{R}_i)$ is a $(3n-2)$-stage terminating right-Euclidean ring (Corollary 7.11). If $\mathfrak{R}_i$ is a special PIR, then $M_n(\mathfrak{R}_i)$ is also $(3n-2)$-stage terminating right-Euclidean (see Lemma 7.12). Either $3n-2$ or $3n-1$ is even, so we can conclude with Lemma 7.13 that $M_n(\mathfrak{R})$ is $(3n-1)$-stage terminating right-Euclidean.

□

Acknowledgements

The research of the author was funded by ERC Starting Grant ANTICS 278537. 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.

[Bru73] Hans-Heinrich Brungs, *Left Euclidean rings*, Pacific Journal of Mathematics **45** (1973), 27–33.

[Cla14] Pete L. Clark, *A Note on Euclidean Order Types*, Order (2014), to appear, doi:10.1007/s11083-014-9323-y.

[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.

[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. Kalaĭdzhich, *Euclidean algorithm in matrix modules over a given Euclidean ring*, Siberian Mathematical Journal **26** (1985), no. 6, 818–822.

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

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

INRIA LFANT, F-33400 Talence, France, CNRS, IMB, UMR 5251, F-33400 Talence, France, Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France,
e-mail: pierre.lezowski@math.u-bordeaux.fr