Journal of Algebra 402 (2014) 294–318

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The skew-growth function on the monoid of square matrices

Kyoji Saito

Institute for Physics and Mathematics of Universe, University of Tokyo, Kashiwa, Chiba 277-8568, Japan

ARTICLE INFO

Article history:
Received 28 April 2013
Available online 11 January 2014
Communicated by Masaki Kashiwara

Keywords:
Square matrices over a principal ideal domain
Cancellative monoid
Least common multiple
Growth function
Skew-growth function
Zeta-function
Euler product

ABSTRACT

We study an elementary divisibility theory for the monoid $\mathrm{M}(n,R)^{\times} := \{X \in \mathrm{M}(n,R) \mid \det(X) \neq 0\}$, where R is a principal ideal domain and $\mathrm{M}(n,R)$ is the ring of n-by-n matrices with coefficients in R. We prove that *any finite subset of* $\mathrm{M}(n,R)^{\times}$ *has the right least common multiple* up to a left unit factor.

As an application, we consider the signed generating series, denoted by $N_{\mathrm{M}(n,R)^{\times},\deg}(t)$ and called the skew-growth function, of least common multiples of all finite sets of irreducible elements of $\mathrm{M}(n,R)^{\times}$, assuming R is residue finite. Then, using the above divisibility theory, we show the Euler product decomposition of the skew-growth function:

$$N_{\mathrm{M}(n,R)^{\times},\deg}\big(\exp(-s)\big) = \prod_{p\in\{\text{primes of } R\}} \big(1-N(p)^{-s}\big)\big(1-N(p)^{-s+1}\big)\cdots \big(1-N(p)^{-s+n-1}\big)$$

Here $N(p) := \#(R/(p))$ is the *absolute norm* of $p \in R$ (there is an unfortunate coincidence of notation "N" for the absolute norm and for the skew growth function [6]).

E-mail address: kyoji.saito@ipmu.ac.jp.

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2013.11.017

Contents

1. Introduction . . . 295
2. Monoid $\mathrm{M}(n,R)^\times$ and its irreducible elements . . . 297
3. Normal form for the classes of $\mathrm{M}(n,R)^\times/\sim_l$ . . . 298
4. Left divisibility theory . . . 300
5. Least common multiples . . . 308
6. Growth function and skew-growth function . . . 311
Acknowledgments . . . 316
Appendix A. Irreducible decomposition . . . 316
References . . . 318

1. Introduction

To any pair $(\mathcal{M}, \deg)$ of a cancellative monoid $\mathcal{M}$ and a degree map deg on $\mathcal{M}$, we associate the *skew growth function* $N_{\mathcal{M},\deg}(t)$ [6] in order to study certain thermodynamical limit functions [4,5]. In the present paper, we study a particular example of a monoid $\mathrm{M}(n,R)^\times := \{X \in \mathrm{M}(n,R) \mid \det(X) \neq 0\}$ of square matrices of size $n \in \mathbb{Z}_{>0}$ with coefficients in a residue finite principal ideal domain R.

For the purpose, we develop a divisibility theory of the monoid in a style similarly to Artin monoids [1], and show the existence of the right/left least common multiple for any finite subset of $\mathrm{M}(n,R)^\times$. Then the skew growth functions turns out to be a signed generating series of the least common multiples of irreducible elements [6]. Using further a phenomenon on the divisibility theory of $\mathrm{M}(n,R)^\times$, called the *jumps of levels of irreducible elements* in $\mathrm{M}(n,R)^\times$, we show that the skew-growth function $N_{\mathrm{M}(n,R)^\times}(\exp(-s))$ decomposes into an Euler product.

Let us explain this more precisely. For two elements $A, B \in \mathrm{M}(n,R)^\times$, we say, as usual, A *divides* B *from the left* or B *is a right-multiple of* A, denoted by $A|_l B$, if there exists $C \in \mathrm{M}(n,R)^\times$ such that $AC = B$. We say A is *left equivalent* to $A' \in \mathrm{M}(n,R)^\times$, denoted by $A \sim_l A'$, if $A|_l A'$ and $A'|_l A$ (which is equivalent to an existence of an invertible matrix $E \in \mathrm{GL}(n,R)$ such that $A' = AE$). Then the division relation $A|_l B$ depends only on their left equivalence classes of A and B, denoted by $[A], [B]$, in $\mathrm{M}(n,R)^\times/\sim_l$. In Section 3, we introduce a normal form for each equivalence class, and denote by M_n the set of all normal forms.

For a given finite subset of J of $\mathrm{M}(n,R)^\times$: i) we call an element $L \in \mathrm{M}(n,R)^\times$ a *left-common multiple* of J if $X|_l L$ for all $X \in J$ and ii) we call a left common multiple L of J a *least left-common multiple of* J if it divides any (other) left-common multiple of J (for simplicity, we shall omit "left"). The first main result of the present paper (Section 5 Theorem 4) is the following existence theorem.

Theorem 4. *Any finite subset of* $\mathrm{M}(n,R)$ *admits a least common multiple.*

We shall denoted by $\mathrm{LCM}(J)$ the normal form of the unique equivalence class of all least common multiples of J. The proof of Theorem 4 is reduced to the case when J consists of two elements, say X and Y. For that case, in Section 4, we prove:

Theorem 3. *There exists a unique map*

$$\sigma : \mathrm{M}(n,R)^{\times} \times M_n \to M_n, (Y,X) \mapsto \sigma_Y(X)$$

such that for any $X \in M_n$ *and* $Y, Z \in \mathrm{M}(n,R)^{\times}$*, one has the equivalence*

$$X|_l YZ \quad \Longleftrightarrow \quad \sigma_Y(X)|_l Z. \tag{$*$}$$

Then, $\mathrm{LCM}(X,Y)$ is given by the normal form of $Y\sigma_Y(X)$.[1] The proof in Section 4 of Theorem 3 is elementary but intricated using irreducible decompositions of X and Y.

We switch our attention to the growth and skew-growth functions of the monoid $\mathrm{M}(n,R)$, when R is residue finite, i.e. $\#(R/(m)) < \infty$ for all $m \in R \setminus \{0\}$. Namely, using the absolute norm given by $N : R \setminus \{0\} \to \mathbb{Z}_{>0}$, $m \mapsto N(m) := \#(R/(m))$, we define the degree map: $X \in \mathrm{M}(n,R)^{\times} \mapsto \deg(X) := \log(N(\det(X))) \in \mathbb{R}_{\geqslant 0}$. Then, the growth and the skew-growth functions (in simplified form [6]) are given by

$$P_{\mathrm{M}(n,R)^{\times},\deg}(t) := \sum_{[X] \in \mathrm{M}(n,R)^{\times}/\sim_l} t^{\deg([X])},$$

$$N_{\mathrm{M}(n,R)^{\times},\deg}(t) := \sum_{J:\text{finite subset of } I_0} (-1)^{\#J} t^{\deg(\mathrm{LCM}(J))}$$

where $I_0 := \{\text{left equivalence classes of all irreducible elements in } \mathrm{M}(n,R)^{\times}\}$. Using the level structure on $\mathrm{M}(n,R)^{\times}$ in Section 3, it is easy to get the expression $P_{\mathrm{M}(n,R)^{\times},\deg}(\exp(-s)) = \zeta_R(s)\zeta_R(s-1)\cdots\zeta_R(s-n+1)$, where $\zeta_R(s)$ is the Dedekind zeta-function for R (cf. [7,2]). Combining this with the inversion formula $P_{\mathrm{M}(n,R)^{\times},\deg}(t) \cdot N_{\mathrm{M}(n,R)^{\times},\deg}(t) = 1$ [6] and the Euler product of $\zeta_R(s)$, we get

$$N_{\mathrm{M}(n,R)^{\times},\deg}\big(\exp(-s)\big) = \prod_{p:\text{prime of } R/\text{units}} \big(1 - N(p)^{-s}\big)\big(1 - N(p)^{-s+1}\big)\cdots\big(1 - N(p)^{-s+n-1}\big).$$

However, as the second main result of the present paper, we prove in Section 6 this formula directly, using neither the inversion formula nor the Euler product of $\zeta_R(s)$, but using only the structure of the least common multiples on $\mathrm{M}(n,R)^{\times}$, where, in the proof, the jump of levels among p-irreducibles, introduced in Section 5, is used essentially to show some big cancellation of terms in $N_{\mathrm{M},\deg}(t)$ (see Section 6, **7**)).[2]

[1] We remark that Theorem 3 is formulated almost parallel with the key Lemma 3.1 in the divisibility theory in Artin monoids [1] with respect to a dictionary: $X \in M_n \leftrightarrow a \in I = \{\text{generators}\}$, $\sigma_Y(X) \leftrightarrow b$, $Y \leftrightarrow C$, $Z \leftrightarrow D$, except for the difference that Theorem 3 claims an equivalence "$\Leftrightarrow$" whereas Lemma 3.1 claims only one implication "$a|_l CD \Rightarrow b|_l D$".

[2] It is curious to compare the skew growth functions of this case with Artin monoid case, where they are, conjecturally, irreducible polynomials over $\mathbb{Z}$ up to a factor $1 - t$ [3].

2. Monoid $\mathrm{M}(n,R)^\times$ and its irreducible elements

Let R be a principal ideal domain. For any given positive integer $n \in \mathbb{Z}_{>0}$, consider the set of all square matrices of size n with non-zero determinant:

$$\mathrm{M}(n,R)^\times := \big\{X \in \mathrm{M}(n,R) \;\big|\; \det(X) \neq 0\big\}.$$

The set $\mathrm{M}(n,R)^\times$ forms a monoid (i.e. a semi-group with the unit 1_n) with respect to the matrix product. Since $\mathrm{M}(n,R)^\times$ is embedded into the group $\mathrm{GL}(n,\mathcal{F}(R))$ for $\mathcal{F}(R) =$ the fractional field of R, the monoid is cancellative, that is, $AXB = AYB$ implies $X = Y$ for all $A, B, X, Y \in \mathrm{M}(n,R)^\times$.

The set of all invertible elements in $\mathrm{M}(n,R)^\times$ is given by

$$\mathrm{GL}(n,R) := \big\{X \in \mathrm{M}(n,R) \mid \det(X) \in \mathcal{E}\big\},$$

where $\mathcal{E}$ is the unit group of R. An element $X \in \mathrm{M}(n,R)^\times$ is called *irreducible* if $X = YZ$ for $Y, Z \in \mathrm{M}(n,R)^\times$ implies either Y or Z belongs to $\mathrm{GL}(n,R)$.

Let us show an elementary fact, which we use constantly in the present paper.

Lemma 1. *An element $X \in \mathrm{M}(n,R)^\times$ is irreducible $\Leftrightarrow$ $\det(X) \in R$ is a prime.*

Proof. Suppose $\det(X)$ is prime in R. If $X = YZ$ then $\det(X) = \det(Y)\det(Z)$ and hence, either $\det(Y)$ or $\det(Z)$ belongs to $\mathcal{E}$, and either Y or Z belongs to $\mathrm{GL}(n,R)$. Let us show the converse. Since, for a principal ideal domain R, any double coset in $\mathrm{GL}(n,R)\backslash\mathrm{M}(n,R)/\mathrm{GL}(n,R)$ can be presented by a diagonal matrix. So, consider a diagonal matrix X. If, either more than two diagonal entries of X are non-unit, or a diagonal entry of X has more than two prime factors, then X is reducible. That is, if X is irreducible, then $\det(X)$ is a prime. □

Definition. Let p be a prime element of R. An element $X \in \mathrm{M}(n,R)^\times$ is called p-irreducible if $\det(X)$ is equal to p up to a unit factor.

Remark. Irreducible decompositions (nonunique) of elements of $\mathrm{M}(n,R)^\times$ are studied in Appendix A. We use them in the proof **7.** of main Theorem 3 in Section 4.

We denote $X|_l Y$ for $X, Y \in \mathrm{M}(n,R)^\times$, if there exists $Z \in \mathrm{M}(n,R)^\times$ such that $XZ = Y$, and we say that X divides Y from the left or Y is a right multiple of X.

Define the *left-equivalence* $X \sim_l Y \Leftrightarrow_{\mathrm{def}} X|_l Y \;\&\; Y|_l X$ ($\Leftrightarrow X = YE$ for an $E \in \mathrm{GL}(n,R)$ due to cancellativity of $\mathrm{M}(n,R)^\times$), and denote by $[X]_l$ or by $[X]$ the left-equivalence class of an element $X \in \mathrm{M}(n,R)^\times$. That is, $[X]_l = X \cdot \mathrm{GL}(n,R)$, and

$$\mathrm{M}(n,R)^\times/\!\sim_l \;= \mathrm{M}(n,R)^\times/\mathrm{GL}(n,R),$$

where RHS is the quotient set by the right action of $\mathrm{GL}(n,R)$. Since the left-equivalence preserves the left-division relation (i.e. $X \sim_l X'$, $Y \sim_l Y'$ and $X|_l Y$ implies $X'|_l Y'$), the quotient set $\mathrm{M}(n,R)^\times/\sim_l$ naturally carries *poset structure* induced from the left-division relation: $[X]_l \leqslant_l [Y]_l \Leftrightarrow_{\mathrm{def}} X|_l Y$. Using the poset structures, irreducible elements are characterized as follows.

Fact. *An element $X \in \mathrm{M}(n,R)^\times$ is irreducible if and only if $[X]_l$ is a minimal element in $(\mathrm{M}(n,R)^\times/\sim_l) \setminus \{[1_n]_l\}$ with respect to the poset structure $\leqslant_l$.*

Remark. Similar to the above, we can introduce the right division relation, the right equivalence relation on $\mathrm{M}(n,R)^\times$ and the poset structure on $\mathrm{M}(n,R)^\times/\sim_r = \mathrm{GL}(n,R)\setminus \mathrm{M}(n,R)^\times$. But, in the present paper, we study only $\mathrm{M}(n,R)^\times/\sim_l$, since one has a poset isomorphism: $\mathrm{M}(n,R)^\times/\sim_r \equiv \mathrm{M}(n,R)^\times/\sim_l, [X] \mapsto [{}^tX]$.

3. Normal form for the classes of $\mathrm{M}(n,R)^\times/\sim_l$

We keep notation in Section 2 so that R is a principal ideal domain and $\mathcal{E}$ is the unit group of R. We define normal forms for elements of the posets $\mathrm{M}(n,R)^\times/\sim_l$ for $n \in \mathbb{Z}_{\geqslant 1}$. To this end, we fix, once and for all, a subset $|R| \subset R\setminus\{0\}$ and subsets $R(m) \subset R$ for each $m \in |R|$, for which the following natural bijections hold:

$$|R| \simeq \big(R\setminus\{0\}\big)/\mathcal{E} \quad \text{and} \quad R(m) \simeq R/(m) \quad \text{for } m \in |R|,$$

where (m) is the ideal in R generated by m. Without loss of generality, we assume that 1) $|R|$ is multiplicative by choosing the representatives for prime elements first, and 2) the class of 0 (resp. 1) in $R/(m)$ is presented by 0 (resp. 1) in $R(m)$.

Eg. Let $R=\mathbb{Z}$. Then, we choose $|R| = \mathbb{Z}_{>0}$ and $R(m) = [0,|m|-1]\cap\mathbb{Z}$.

Depending on the choices of $|R|$ and $R(m)$, we introduce a subset of $\mathrm{M}(n,R)^\times$:

$$M_n := \left\{ \begin{bmatrix} m_1 & 0 & 0 & \cdots & 0 \\ d_{21} & m_2 & 0 & \cdots & 0 \\ d_{31} & d_{32} & m_3 & \cdots & 0 \\ * & * & * & \cdots & 0 \\ d_{n1} & d_{n2} & d_{n3} & \cdots & m_n \end{bmatrix} \;\middle|\; \begin{array}{l} m_1,m_2,\ldots,m_n \in |R|, \\ d_{i1},d_{i2},\ldots,d_{i(i-1)} \in R(m_i) \\ \text{for } i=2,\ldots,n \end{array} \right\}.$$

Lemma 2. *Every right $\mathrm{GL}(n,R)$-orbit (= a left equivalent class) in $\mathrm{M}(n,R)^\times$ intersects with the set M_n at a single element. That is, the projection $\mathrm{M}(n,R)^\times \to \mathrm{M}(n,R)^\times/\mathrm{GL}(n,R)$ induces a bijection*

$$M_n \simeq \mathrm{M}(n,R)^\times/\sim_l.$$

Proof. This is shown by an induction on $n \in \mathbb{Z}_{>0}$.

Case $n = 1$ is shown by $\mathrm{M}(1,R)^\times/\sim = (R \setminus \{0\})/\mathcal{E} \simeq |R| = M_1$. Let $n > 1$ and assume lemma for $n-1$. We first show that the projection from M_n is surjective. Let $X \in \mathrm{M}(n,R)^\times$ and let $\mathbf{x} = (x_1, \dots, x_n) \in R^n$ be its first row vector, which is non-zero by the determinant condition $\det(X) \neq 0$. Then, there exists $m_1 \in |R|$, which generates the ideal $(x_1, \dots, x_n)$, and $A \in \mathrm{GL}(n,R)$ such that $\mathbf{x}A = (m_1, 0, \dots, 0)$. Hence, we may choose a representative of the class $[X]_l$ to be of the form: $\left[\begin{smallmatrix} m_1 & 0 \\ * & X' \end{smallmatrix}\right]$ for $X' \in \mathrm{M}(n-1,R)^\times$. By our induction hypothesis, there exists $A' \in \mathrm{GL}(n-1,R)$ such that $\left[\begin{smallmatrix} m_1 & 0 \\ * & X' \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 0 \\ 0 & A' \end{smallmatrix}\right] = \left[\begin{smallmatrix} m_1 & 0 \\ * & X'' \end{smallmatrix}\right]$ where X'' is an element of M_{n-1} whose diagonal is $(m_j)_{j=2}^n \in |R|^{n-1}$. Then we find a column vector $[*'] \in R^{n-1}$ such that $[*] + X''[*'] =: [d']$ is a vector in $\prod_{i=2}^n R(m_i)$. Applying a matrix of the form $\left[\begin{smallmatrix} 1 & 0 \\ *' & 1_{n-1} \end{smallmatrix}\right]$ from the right, we get the normal form $\left[\begin{smallmatrix} m_1 & 0 \\ * & X'' \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 0 \\ *' & 1_{n-1} \end{smallmatrix}\right] = \left[\begin{smallmatrix} m_1 & 0 \\ d' & X'' \end{smallmatrix}\right]$.

Next we show the injectivity of the correspondence. Let $X, Y \in M_n$ such that $X \sim_l Y$. Then $U := X^{-1}Y$ is a lower triangular matrix in $\mathrm{GL}(n,R)$, whose diagonal entries are of $\mathcal{E}$. Since $m^{-1}m' \in \mathcal{E}$ for $m, m' \in |R|$ implies $m^{-1}m' = 1$, diagonals of U are 1. This proves, in particular, the case for $n = 1$.

For $n > 1$, restricting the equality $XU = Y$ to the two $(n-1) \times (n-1)$ principal sub-matrices forgetting either the first column and row or the last column and row, respectively, we see that parts of X and Y are left-equivalent. By the induction hypothesis, the corresponding $(n-1) \times (n-1)$ principal sub-matrices of U are equal to the identity matrix. Thus, U is equal to the identity matrix 1_n of size n up to the $(n,1)$-entry u_{n1}. Then the equality $XU = Y$ implies $x_{n1} + u_{n1}m_n = y_{n1}$. Since we have the normalization $x_{n1}, y_{n1} \in R(m_n)$, we get $x_{n1} = y_{n1}$ and $u_{n1} = 0$. □

Definition. 1. For a left equivalence class $[X] \in \mathrm{M}(n,R)^\times/\sim_l$, we call the element in $X\mathrm{GL}(n,R) \cap M_n$ the *normal form* of $[X]$. *We shall often identify the class* $[X]$ *with its normal form, when there is no possibility of confusions.*

2. By the *diagonal part of* a class $[X]$, denoted by $\mathrm{diag}([X])$, we mean the diagonal part of its normal form which is an ordered sequence $(m_1, \dots, m_n) \in |R|^n$, where m_i $(1 \leqslant i \leqslant n)$ is called the diagonal entry of $[X]$ of ith *level*.

Notation. For a row vector $\mathbf{x} \in R^n$, we define an element of *pure of level* $1 \leqslant i \leqslant n$ by

$$M(i : \mathbf{x}) := \begin{array}{l}\text{the matrix obtained by substituting the} \\ i\text{th row of the identity matrix } 1_n \text{ by } \mathbf{x}.\end{array}$$

Definition. 3. If $M(i : \mathbf{x}) \in M_n$, i.e. $\mathbf{x} = (d_1, \dots, d_{i-1}, m, 0, \dots, 0)$ for some $m \in |R|$ and $d_j \in R(m)$ $(1 \leqslant j < i)$, we call it a *normal form of level* i *with diagonal* m.

4. If the diagonal m of a normal form $M(i : \mathbf{x})$ is a prime element, say p, in R, we call $M(i : \mathbf{x})$ a *p-irreducible* (*normal form*) of level i.

It is clear that any irreducible element of $\mathrm{M}(n,R)^\times$ is left equivalent to a unique irreducible normal form for a certain level i $(1 \leqslant i \leqslant n)$. We call i the *level of the*

irreducible element. For any prime element $p \in R$, the set of left equivalence classes of all p-irreducible elements is naturally bijective to the set

$$I_{0,p} := \bigsqcup_{i=1}^{n} \{ M\big(i : (\mathbf{d}, p, 0, \dots, 0)\big) \mid \mathbf{d} = (d_1, \dots, d_{i-1}) \in \big(R(p)\big)^{i-1} \}$$

of all p-irreducible normal forms. We shall sometimes confuse them.

4. Left divisibility theory

We develop an *elementary divisibility theory for* $\mathrm{M}(n,R)^\times$ in a style similar to the divisibility theory for Artin monoids ([1, §3], see footnote 1). The main result is formulated in Theorem 3. In order to state the result, let us recall notations: R is a principal ideal domain, $|R|$ is a subset of R s.t. $|R| \simeq (R \setminus \{0\})/\{\text{units}\}$, and M_n is the set of normal forms in $\mathrm{M}(n,R)^\times$ s.t. $M_n \simeq \mathrm{M}(n,R)^\times/\mathrm{GL}(n,R)$ (Section 3).

Theorem 3. *There exists a unique map*

$$\sigma : \mathrm{M}(n,R)^\times \times M_n \to M_n,\ (Y, X) \mapsto \sigma_Y(X)$$

such that for any $X \in M_n$ *and* $Y, Z \in \mathrm{M}(n,R)^\times$, *one has the equivalence*

$$X|_l YZ \quad \Longleftrightarrow \quad \sigma_Y(X)|_l Z. \tag{$*$}$$

The map σ *satisfies further the following* **1)**–**4)**.

1) $\mathrm{M}(n,R)^\times$**-action on** M_n**.** *The map* σ *defines an opposite left action* σ_Y *of* $Y \in \mathrm{M}(n,R)^\times$ *on the set* M_n *with the fixed point* 1_n. *That is,*

$$\sigma_{1_n} = id_{M_n}, \qquad \sigma_{Y_2 Y_1} = \sigma_{Y_1} \circ \sigma_{Y_2} \quad \text{and} \quad \sigma_Y(1_n) = 1_n$$

for any $Y, Y_1, Y_2 \in \mathrm{M}(n,R)^\times$.

2) $\mathrm{GL}(n,R)$**-action on** M_n**.** *The map* σ *is compatible with the actions of* $\mathrm{GL}(n,R)$ *on* $\mathrm{M}(n,R)^\times$ *from right and on* M_n *from left. That is, for any* $Y \in \mathrm{M}(n,R)^\times$ *and* $E \in \mathrm{GL}(n,R)$, *we have*

$$\sigma_{YE} = \big[E^{-1}\big]\sigma_Y$$

where $[E^{-1}]$ *denotes the left action on the set* M_n *induced from the left action of* E^{-1} *on the set of left equivalence classes through the identification* **Lemma 2**.

3) Reciprocity. *There exists a map* $u : M_n \times M_n \to \mathrm{U}(n,R) := \{$*lower triangular matrices in* $\mathrm{M}(n,R)$ *whose diagonals are* $1\}$ *such that, for* $X, Y \in M_n$, *we have*

$$X\sigma_X(Y) = Y\sigma_Y(X) \cdot u(X,Y).$$

Here $u(X,Y)$ *is of pure of level equal to the maximum of levels of* X *and* Y.

4) Monotonicity. *For any $X \in M_n$ and $Y \in \mathrm{M}(n,R)^\times$, one has*

$$\frac{\det(X)}{\det(\sigma_Y(X))} \in |R| \quad \big(\simeq (R \setminus \{0\})/\mathcal{E}\big).$$

In particular, if X is a p-irreducible element, then $\sigma_Y(X)$ is equal either to 1 or to a p-irreducible element. Precisely, $\sigma_Y(X)$ is a p-irreducible of the same level as X if and only if an irreducible decomposition of Y does not contain a p-irreducible element of the same level as X. More over, let $X = M(i : (\mathbf{d}, p, \mathbf{0}))$ (resp. $Y = M(j : (\mathbf{e}, q, \mathbf{0}))$ be normal forms of p- (resp. q-) irreducible elements of level i (resp. j) with $X \neq Y$. Then, $\sigma_Y(X)$ is p-irreducible such that

$$\textit{level of } \sigma_Y(X) = \begin{cases} i & \text{if } i \neq j \text{ or } p \neq q, \\ \max\{k \mid d_k \not\equiv e_k \bmod p,\ 1 \leqslant k < i\} & \text{if } i = j \text{ and } p = q. \end{cases}$$

Proof. Let us, first, give an overview of the proof.

The proof is divided into nine steps **1**–**9.** In **1.**, we show the uniqueness of the map σ satisfying (∗) (if it exists). Then in **2.**–**4.**, using the uniqueness property, we show that the properties **1)**, **2)** and **3)** of σ are deduced from (∗). In **5.**, we show a criterion for a lower triangular matrix to be divisible from left by a p-irreducible element. Then, using the criterion **5.**, we show in **6.**, the existence of $\sigma_Y(X)$ when X and Y are irreducible normal forms. Then, in **7.**, applying the composition rule in **1)** to **6.** repeatedly for an irreducible decomposition of Y, we show the existence of $\sigma_Y(X)$ for general $Y \in \mathrm{M}(n,R)^\times$. Then, using **3)** Reciprocity, we exchange the role of X and Y. To the general Y, we again apply the rule in **1)** for an irreducible decomposition of X, and we obtain $\sigma_X(Y)$ for all $(X,Y) \in M_n \times M_n$. Finally, the property **4)** is shown in **8.** and **9.** by induction on the number of irreducible factors of X and Y, where the essential case is when X and Y are irreducible, discussed in **6.**

The core of the proof is **5.**, **6.** where we use matrix expression of the monoid $\mathrm{M}(n,R)^\times$, whereas the other parts **1.**, **2.**, **3.**, **4.** and **7.** of the proof are general properties for any cancellative monoids, and **8.** and **9.** are applications of **6.**

1. *For a given pair $(X,Y) \in M_n \times \mathrm{M}(n,R)$, if there exists $\sigma_Y(X) \in M_n$ satisfying the condition (∗), then it is unique.*

Proof. Suppose there are two elements $\sigma, \sigma' \in \mathrm{M}(n,R)$ satisfying (∗). It implies, in particular, $\sigma|_l Z \Leftrightarrow \sigma'|_l Z$ for any $Z \in \mathrm{M}(n,R)$. Then, by choosing Z to be σ and σ', we get $\sigma'|_l \sigma$ and $\sigma|_l \sigma'$. That is, σ and σ' are left equivalent, i.e. $[\sigma] = [\sigma']$. □

2. *Let a map $\sigma_Y : M_n \to M_n$ satisfy the condition (∗) for $Y \in \mathrm{M}(n,R)^\times$. Then for any $E \in \mathrm{GL}(n,R)$, the map $[E^{-1}]\sigma_Y : X \in M_n \mapsto [E^{-1}]\sigma_Y(X) \in M_n$ satisfies the condition (∗) for YE. That is, σ_{YE} exists and is equal to $[E^{-1}]\sigma_Y$.*

Proof. We have: $X|_l YEZ \Leftrightarrow \sigma_Y(X)|_l EZ \Leftrightarrow E^{-1}\sigma_Y(X)|_l Z$. This means that $[E^{-1}]\sigma_Y$ satisfies the condition (∗) for σ_{YE}. Then, the uniqueness **1.** implies the result. □

3. *Suppose that there exist the maps σ_{Y_1} and σ_{Y_2} for Y_1 and $Y_2 \in \mathrm{M}(n,R)$ satisfying the condition (∗), respectively. Then, the composition $\sigma_{Y_1} \circ \sigma_{Y_2}$ satisfies the condition (∗) for Y_2Y_1. That is, $\sigma_{Y_2Y_1}$ exists, and is equal to $\sigma_{Y_1} \circ \sigma_{Y_2}$.*

Proof. We have: $X|_l Y_2Y_1Z \Leftrightarrow \sigma_{Y_2}(X)|_l Y_1Z \Leftrightarrow \sigma_{Y_1}(\sigma_{Y_2}(X))|_l Z$. □

4. *If there exists $\sigma_Y(X)$ satisfying (∗) for $X, Y \in M_n$, then there exists $\sigma_X(Y)$ satisfying (∗) for Y, X, and an element $u(X,Y) \in \mathrm{U}(n,R)$ satisfying the equation*

$$X\sigma_X(Y) = Y\sigma_Y(X)u(X,Y).$$

Proof. That $\sigma_Y(X)$ satisfies the condition (∗) for the pair (X,Y) implies, in particular (by choosing $Z = \sigma_Y(X)$), $X|_l(Y\sigma_Y(X))$. So, put $Y\sigma_Y(X) = XW$ for a $W =$ a lower triangular matrix in $\mathrm{M}(n,R)^\times$. Let us show that the class $\sigma := [W] \in M_n$ (recall Lemma 2) satisfies the condition (∗) for the pair (Y,X). That is, we need to show the equivalence $Y|_l XZ \Leftrightarrow \sigma|_l Z$ for any $Z \in \mathrm{M}(n,R)^\times$. The implication "⇒" follows, since $Y|_l XZ$ implies an existence of $V \in \mathrm{M}(n,R)^\times$ with $XZ = YV$. Then, $X|_l YV$ and (∗) for (X,Y) implies $\sigma_Y(X)|_l V$. So, put $V = \sigma_Y(X)U$ for $U \in \mathrm{M}(n,R)^\times$. Then, $XZ = Y\sigma_Y(X)U = XWU$. Cancelling X from left, we obtain $Z = WU$. That is, Z is left divisible by the class of W, i.e. by σ. The opposite implication "⇐" follows, since $\sigma|_l Z$ implies an existence of $T \in \mathrm{M}(n,R)^\times$ such that $Z = \sigma T$, and, hence $XZ = X\sigma T = XWET = Y\sigma_Y(X)ET$ for some $E \in \mathrm{GL}(n,R)$. That is, XZ is left-divisible by Y. □

5. *A lower triangular matrix $Z = \begin{bmatrix} Z' & 0 & 0 \\ \mathbf{z} & v & 0 \\ * & * & * \end{bmatrix}$ with $Z' \in \mathrm{M}(i-1,R)$, $\mathbf{z} \in R^{i-1}$ and $v \in R$, is divisible by a p-irreducible element $X = M(i : (\mathbf{d}, p, \mathbf{0}))$ for $\mathbf{d} \in R^{i-1}$ of level $1 \leqslant i \leqslant n$ from left, if and only if they satisfy*

$$p|v \quad \textit{and} \quad \mathbf{z} \equiv \mathbf{d}Z' \bmod p.$$

Proof. Since $X^{-1} = M(i : (-\frac{\mathbf{d}}{p}, \frac{1}{p}, \mathbf{0}))$, we observe that $X^{-1}Z$ is equal to Z except for the ith row, where the ith row is given by $(\frac{1}{p}(\mathbf{z} - \mathbf{d}Z'), \frac{v}{p}, \mathbf{0})$. □

6. We study the case when X and Y are irreducible in $\mathrm{M}(n,R)^\times$. This part is the essential part of the whole proof of Theorem 3.

Assertion. *Let X and Y be a p-irreducible element of level i and a q-irreducible element of level j for primes $p, q \in |R|$ and $1 \leqslant i, j \leqslant n$. Then, either $X = Y$ and $\sigma_Y(X) = 1_n$, or there exists a p-irreducible element $\sigma_Y(X)$ satisfying condition (∗) whose level is unchanged from that of X except for the case $p = q$ and $i = j$.*

Proof. The proof is divided into 4 cases.

Case i) $i < j$.

Since Y is of level j, YZ for any $Z \in \mathrm{M}(n,R)$ is a matrix which coincides with Z from 1 to $j-1$ rows. On the other hand, the divisibility of YZ (resp. Z) by X from the left is determined by the row vectors of YZ (resp. Z) from 1 to ith. That is, we have the equivalence $X|_l YZ \Leftrightarrow X|_l Z$. That is, we have

$$\sigma_Y(X) = X.$$

This completes the proof for the case when $i < j$.

Case ii) $i = j$ and $p = q$.

This is the most intricate and subtle case.

If $X = Y$, we have $\sigma_Y(X) = 1_n$. Suppose $X \neq Y$, and let $X = M(i : (\mathbf{d}, p, \mathbf{0}))$ and $Y = M(i : (\mathbf{e}, p, \mathbf{0}))$ for $\mathbf{d}, \mathbf{e} \in (R(p))^{i-1}$ with $\mathbf{d} - \mathbf{e} \neq 0$. Let the i-principal sub-matrix of Z is of the form $= \left[\begin{smallmatrix} Z' & 0 \\ \mathbf{z} & v \end{smallmatrix}\right]$ with $Z' \in \mathrm{M}(i-1,R)$, $\mathbf{z} \in R^{i-1}$ and $v \in R$. Then, the i-principal sub-matrix of YZ is of the form $\left[\begin{smallmatrix} Z' & 0 \\ \mathbf{e}Z' + p\mathbf{z} & pv \end{smallmatrix}\right]$. Then the criterion in **5.** says that

$$\begin{aligned} X|_l YZ \quad &\Leftrightarrow \quad p|pv \quad \text{and} \quad \mathbf{e}Z' + p\mathbf{z} \equiv \mathbf{d}Z' \bmod p \\ &\Leftrightarrow \quad (\mathbf{e} - \mathbf{d})Z' \equiv 0 \bmod p. \end{aligned}$$

Let us find one particular solution of the equations, satisfying $v = 1$ and $\mathbf{z} = 0$. By the assumption $X \neq Y$, there is some

$$k := \max\{1 \leqslant l < i \mid e_l - d_l \not\equiv 0 \bmod p\}.$$

Then, we consider a p-irreducible element $W := M(k : (\mathbf{f}, p, \mathbf{0}))$ with $\mathbf{0} \in R^{n-k}$, where $\mathbf{f} \in R(p)^{k-1}$ is defined as: for $1 \leqslant l < k$, we solve the following equation

$$e_l - d_l + f_l(e_k - d_k) \equiv 0 \bmod p$$

on $f_l \in R(p)$. This is solvable since $e_k - d_k$ is prime to p in R. The i-principal sub matrix of W is of the form $M(k : (\mathbf{f}, p, \mathbf{0}))$ with $\mathbf{0} \in R^{i-1-k}$ and satisfies the equation $(\mathbf{e} - \mathbf{d})M(k : (\mathbf{f}, p, \mathbf{0})) \equiv 0 \bmod p$. This means that W is a solution of $X|_l YW$. Then, any Z with $W|_l Z$ satisfies $X|_l YW|_l YZ$.

On the other hand, let us consider any lower triangular matrix Z satisfying $X|_l YZ$. We want to show $W|_l Z$, where, according to **5.**, $W|_l Z$ if and only if

$$p|v'' \quad \text{and} \quad \mathbf{z}'' \equiv \mathbf{f}Z'' \bmod p,$$

where the k-principal sub-matrix of Z is of the form $\left[\begin{smallmatrix} Z'' & 0 \\ \mathbf{z}'' & v'' \end{smallmatrix}\right] \in \mathrm{M}(k,R)^\times$. Since $e_m - d_m \equiv 0 \bmod p$ for m with $k < m \leqslant i-1$, the condition $X|_l YZ$ on Z, i.e. $(\mathbf{e} - \mathbf{d})Z' \equiv 0 \bmod p$

on Z can be rewritten as $(\mathbf{e}'' - \mathbf{d}'')\left[\begin{smallmatrix} Z'' & 0 \\ \mathbf{z}'' & v'' \end{smallmatrix}\right] \equiv 0 \bmod p$, where $(\mathbf{e}'' - \mathbf{d}'')$ is the row vector consisting of the first k entries of $(\mathbf{e} - \mathbf{d})$. Since, by the definition of $\mathbf{f}$, we have $(\mathbf{e}'' - \mathbf{d}'') \equiv (e_k - d_k)(-\mathbf{f}, 1) \bmod p$. Then the condition $X|_l YZ$ on Z can be further rewritten as $(e_k - d_k)(-\mathbf{f}, 1)\left[\begin{smallmatrix} Z'' & 0 \\ \mathbf{z}'' & v'' \end{smallmatrix}\right] \equiv 0 \bmod p$. Since by the choice of k, $e_k - d_k$ is prime to p so that we can divide the equality by $d_k - e_k$. Then, this condition exactly implies $p \mid v''$ and $\mathbf{z}'' \equiv \mathbf{f}Z'' \bmod p$. That is, the condition $X|_l YZ$ implies the condition $W|_l Z$ (in fact, they are equivalent). Then, W satisfies the property $(*)$, and we put

$$\sigma_Y(X) := W = M\big(k : (\mathbf{f}, p, \mathbf{0})\big).$$

This completes the proof for the case when $p = q$ and $i = j$.

Remark. We have shown the latter half of **4)** for the case $i = j$ and $p = q$. In particular, the level k of $\sigma_Y(X)$ is *strictly smaller* than the level i of X and Y. We shall call this phenomenon the **jump of levels** of p-irreducible elements.

Case iii) $i = j$ and $p \neq q$.

Let $X = M(i : (\mathbf{d}, p, \mathbf{0}))$ and $Y = M(i : (\mathbf{e}, q, \mathbf{0}))$ for $\mathbf{d} \in R(p)^{i-1}$ and $\mathbf{e} \in R(q)^{i-1}$. Let the i-principal sub-matrix of Z be of the form $\left[\begin{smallmatrix} Z' & 0 \\ \mathbf{z} & v \end{smallmatrix}\right]$ with $Z' \in \mathrm{M}(i-1, R)$, $\mathbf{z} \in R^{i-1}$ and $v \in R$. Then, the i-principal sub-matrix of YZ is of the form $= \left[\begin{smallmatrix} Z' & 0 \\ \mathbf{e}Z' + q\mathbf{z} & qv \end{smallmatrix}\right]$ with $Z' \in \mathrm{M}(i-1, R)$. The criterion in **5.** says that

$$\begin{aligned} X|_l YZ \quad &\Leftrightarrow \quad p|qv \quad \text{and} \quad \mathbf{e}Z' + q\mathbf{z} \equiv \mathbf{d}Z' \bmod p \\ &\Leftrightarrow \quad p|v \quad \text{and} \quad (\mathbf{e} - \mathbf{d})Z' + q\mathbf{z} \equiv 0 \bmod p. \end{aligned}$$

Let us give one particular solution $W = M(i : (\mathbf{f}, p, \mathbf{0}))$, satisfying $X|_l YW$. Namely, we put $v = p$ and $Z' = 1_{i-1}$, then, since p and q are prime, the equation $q\mathbf{z} \equiv \mathbf{d} - \mathbf{e} \bmod p$ on $\mathbf{z}$ has a unique solution $\mathbf{f} \in R(p)^{i-1}$. Then, obviously, for any $Z \in \mathrm{M}(n, R)^\times$ with $W|_l Z$, we get $X|_l YW|_l YZ$.

On the other hand, let us consider any lower-triangular matrix Z satisfying $X|_l YZ$. We want to show $W|_l Z$, where, according to **5.**, $W|_l Z$ if and only if

$$p|v \quad \text{and} \quad \mathbf{z} \equiv \mathbf{f}Z' \bmod p,$$

where the first condition $p|v$ is already satisfied. Furthermore, substituting the relation $\mathbf{e} - \mathbf{d} \equiv -q\mathbf{f}$ in the condition $X|_l YZ$, we obtain $-q\mathbf{f}Z' + q\mathbf{z} \equiv 0 \bmod p$. Since q is prime to p, we can divide this equality by q, and we obtain the condition for $W|_l Z$. That is, the condition $X|_l YZ$ implies the condition $W|_l Z$ (in fact, they are equivalent). Thus, W satisfies the property $(*)$, and we put

$$\sigma_Y(X) := W = M\big(i : (\mathbf{f}, p, \mathbf{0})\big).$$

This completes the proof for the case when $p \neq q$ and $i = j$.

Case iv) $i > j$.

Let $X = M(i : (\mathbf{d}, p, \mathbf{0}))$ and $Y = M(j : (\mathbf{e}, q, \mathbf{0}))$ for $\mathbf{d} \in R(p)^{i-1}$ and $\mathbf{e} \in R(q)^{j-1}$, where p may or may not be equal to q. Let $Z \in \mathrm{M}(n, R)^\times$ be any lower triangular matrix, whose i-principal sub-matrix is of the form $\left[\begin{smallmatrix} Z' & 0 \\ \mathbf{z} & v \end{smallmatrix}\right] \in \mathrm{M}(i, R)^\times$ with $Z' \in \mathrm{M}(i-1, R)$, $\mathbf{z} \in R^{i-1}$ and $v \in R$. Then, the i-principal sub-matrix of YZ is of the form $(1_i + \left[\begin{smallmatrix} \mathbf{0} \\ (\mathbf{e}, q-1, \mathbf{0}) \\ \mathbf{0} \end{smallmatrix}\right])\left[\begin{smallmatrix} Z' & 0 \\ \mathbf{z} & v \end{smallmatrix}\right] = \left[\begin{smallmatrix} Z' & 0 \\ \mathbf{z} & v \end{smallmatrix}\right] + \left[\begin{smallmatrix} \mathbf{0} \\ (\mathbf{e}, q-1, \mathbf{0})Z' \\ \mathbf{0} \end{smallmatrix}\right]$, where

1) $(\mathbf{e}, q-1, \mathbf{0})$ is a row vector located in the jth row. Since $i > j$, the size j of the vector $(\mathbf{e}, q-1)$ is strictly smaller than the size i of the matrix.

2) $\mathbf{0}$'s are zero matrices or zero vectors whose size depends on the place where they are located. In particular, due to the inequality $i > j$, the $\mathbf{0}$'s in the bottom row are non-empty. This implies that the ith row vector of YZ is equal to that of Z and is $(\mathbf{z}, v, \mathbf{0})$.

Then the criterion in **5.** says that

$$X|_l YZ \quad \Leftrightarrow \quad p|v \quad \text{and} \quad \mathbf{z} \equiv \big(\mathbf{d} + d_j(\mathbf{e}, q-1, \mathbf{0})\big)Z' \bmod p.$$

Reversing the criterion **5.**, the last condition is equivalent to that Z is divisible by $W := M(i : (\mathbf{d} + d_j(\mathbf{e}, q-1, \mathbf{0}), p, \mathbf{0}))$. Clearly, W is a p-irreducible element (even if it is not yet a normal form because of the term $d_j(\mathbf{e}, q-1, \mathbf{0})$).

Thus, we put

$$\sigma_Y(X) := \text{the normal form of } W.$$

This completes the proof of the case $i > j$, and, hence, that of **6.** □

7. In Appendix A Lemma 10, we show that for any element $Y \in \mathrm{M}(n, R)^\times$ with $\mathrm{diag}([Y]) = (m_1, \dots, m_n)$ and irreducible decompositions $m_i = \prod_{k=1}^{k_i} p_{i,k}$ $(i = 1, \dots, n)$, there exists a unique decomposition $Y = (\prod_{i=1}^{n} \prod_{k=1}^{k_i} P_{i,k})E$ where $P_{i,k}$ is a $p_{i,k}$-irreducible normal form of level i and $E \in \mathrm{GL}(n, R)$. Then, for any p-irreducible normal form X, applying the composition rule in **1)** and **2)** of Theorem 3, we see that $\sigma_Y(X)$ is given by

$$\sigma_Y(X) := \left([E^{-1}] \prod_{i=n}^{1} \prod_{k=k_i}^{1} \sigma_{P_{i,k}} \right)(X)$$

where RHS means 1) act $\sigma_{P_{i,k}}$ on X successively in the lexicographic order, 2) left act of $[E^{-1}]$ (use **1.**, **2.**, **3.** and **6.**). The result is either a p-irreducible element or 1_n.

So far, we constructed $\sigma_Y(X)$ for a p-irreducible X. We want to construct it for arbitrary $X \in M_n$ and $Y \in \mathrm{M}(n, R)^\times$. Due to **2)** or **2.**, it is sufficient to show the existence for the case when $Y \in M_n$. Then, due to **3)** Reciprocity or **4.**, this is equivalent to show the existence of $\sigma_X(Y)$. For general $X \in \mathrm{M}(n, R)^\times$, taking an irreducible decomposition

$X = (\prod_{i=1}^{n}\prod_{k'=1}^{k'_i} P'_{i,k'})E'$ in Appendix A, and applying again the composition rule in **1)** and **2)**, we get

$$\sigma_X(Y) := \left(\left[(E')^{-1} \right] \prod_{i=n}^{1} \prod_{k'=k'_i}^{1} \sigma_{P'_{i,k'}} \right)(Y)$$

where RHS is similarly defined as before.

This completes a proof of existence of the map σ for all X and Y.

8. Before we show **4)**, let us show its weaker (numerical) version:

$$\#(X) \geqslant \#\big(\sigma_Y(X)\big),$$

where we mean by $\#(A)$ for $A \in \mathrm{M}(n,R)^\times$ the number of irreducible factors in the irreducible decomposition of A (= # of prime factors in $\det(A)$). If X is irreducible (i.e. $\#(X) = 1$), then $\sigma_Y(X)$ is either irreducible or 1_n so that the inequality holds. Then, using **4.**, $\#(Y) - \#(\sigma_X(Y)) = \#(X) - \#(\sigma_Y(X)) \geqslant 0$ for an irreducible X. Then for an irreducible decomposition $X = X_1 \cdots X_N$, we obtain $\#(Y) \geqslant \#(\sigma_{X_1}(Y)) \geqslant \#(\sigma_{X_2}(\sigma_{X_1}(Y))) = \#(\sigma_{X_1X_2}(Y)) \geqslant \cdots \geqslant \#(\sigma_{X_1\cdots X_N}(Y)) = \#(\sigma_X(Y))$. Again using **4.**, we obtain $\#(X) - \#(\sigma_Y(X)) = \#(Y) - \#(\sigma_X(Y)) \geqslant 0$.

9. Let us show **4)** by the double induction on $(u,v) = (\#(X), \#(Y)) \in \mathbb{Z}_{\geqslant 0} \times \mathbb{Z}_{\geqslant 0}$. The cases for $(u,0)$ or $(0,v)$ (i.e. the cases when $Y = 1_n$ or $X = 1_n$) are trivially true. The construction in **6.** shows that $\sigma_Y(X)$ for a p-irreducible element X and a q-irreducible element Y is a p-irreducible element, except for the case $X = Y$ and $\sigma_Y(X) = 1$, and its level is unchanged except $p = q$ and levels of X and Y coincide. This implies the statement **4)** for the case $(u,v) = (1,1)$. Let us show that our construction of σ using **1.**, **2.** and **3.** preserves the property **4)**, respectively.

Let $X \in M_n$ and $Y \in \mathrm{M}(n,R)^\times$ such that $\frac{\det(X)}{\det(\sigma_Y(X))} \in |R|$.

1. For any $Y' \in \mathrm{M}(n,R)^\times$, one has

$$\frac{\det(X)}{\det(\sigma_{YY'}(X))} = \frac{\det(\sigma_Y(X))}{\det(\sigma_{Y'}(\sigma_Y(X)))} \frac{\det(X)}{\det(\sigma_Y(X))} \in |R|.$$

2. For any $E \in \mathrm{GL}(n,R)$, one has

$$\frac{\det(X)}{\det(\sigma_{YE}(X))} = \frac{\det(X)}{\det(E^{-1}(\sigma_Y(X)))} = \frac{\det(X)}{\det(\sigma_Y(X))} \in |R|.$$

3. If $X, Y \in M_n$

$$\frac{\det(Y)}{\det(\sigma_X(Y))} = \frac{1}{\det(u(X,Y))} \frac{\det(X)}{\det(\sigma_Y(X))} = \frac{\det(X)}{\det(\sigma_Y(X))} \in |R|.$$

This completes a proof of **4)** and, hence, that of Theorem 3. □

Corollary. *For $X \in M_n$ and $Y \in \mathrm{M}(n,R)^\times$, $X|_l Y \Leftrightarrow \sigma_Y(X) = 1$.*

Explicit formula of $u(X,Y)$ for irreducible X and Y. Let X and Y be irreducible normal forms $M(i : (\mathbf{d}, p, \mathbf{0}))$ and $M(j : (\mathbf{e}, q, \mathbf{0}))$, respectively. Using **6.** of the proof of Theorem 3, we obtain:

Case i) If $i < j$, then $u(X,Y) = M(j : (-[\frac{\mathbf{e}+e_i(\mathbf{d},p-1,\mathbf{0})}{q}], 1, \mathbf{0})) \in \mathrm{U}(n,R)$, where we denote by $[\frac{a}{q}]$ for $a \in R$ the unique element $r \in R$ such that $a - rq \in R(q)$.

Case ii) If $i = j$ and $p \neq q$, then $u(X,Y) = M(i : (\mathbf{h}, 1, \mathbf{0})) \in \mathrm{U}(n,R)$. where $\mathbf{h} \in R^{i-1}$ is the unique solution of the equation: $\mathbf{d} - \mathbf{e} = q\mathbf{f} - p\mathbf{g} + pq\mathbf{h}$ for some unknown $\mathbf{f} \in R(p)^{i-1}$, $\mathbf{g} \in R(q)^{i-1}$ (this equation has a unique solution, since p and q are distinct primes).

Case iii) Let $i = j$, $p = q$. If $X = Y$, then $\sigma(X,Y) = 1_n$. If $X \neq Y$, then $u(X,Y) = M(i : (g_1, \ldots, g_{k-1}, d_k - e_k, \frac{d_{k+1}-e_{k+1}}{p}, \ldots, \frac{d_{i-1}-e_{i-1}}{p}, 1, \mathbf{0})) \in \mathrm{U}(n,R)$, where $k := \max\{1 \leqslant m < i \mid d_m - e_m \not\equiv 0 \bmod p\}$ and $\mathbf{g} \in R^{k-1}$ is the unique solution of the equation: $d_l - e_l + f_l(d_k - e_k) = g_l p$ $(1 \leqslant l \leqslant k-1)$ for some unknown $\mathbf{f} \in R(p)^{k-1}$ (this equation has a unique solution since $d_k - e_k$ is prime to p).

Case iv) If $i > j$, we reduce this case to i) by $u(X,Y) = u(Y,X)^{-1}$.

Note. As stated in the proof of Theorem 3, the steps **1.**, **2.**, **3.**, **4.** and **7.** are general properties valid for any cancellative monoids. Therefore, we formulate below the result. As we shall see in the proof of Section 5 Theorem 4, Corollary below holds also.

Theorem. *Let $\mathcal{M}$ be a cancellative monoid. Let $\mathbf{M}$ be a subset of $\mathcal{M}$ which represents all left equivalence classes in $\mathcal{M}$ uniquely. Set $I_0 := \mathbf{M} \cap \{\text{irreducible elements}\}$.*

Suppose that there exists a map $\sigma : I_0 \times I_0 \to I_0$, $(Y,X) \mapsto \sigma_Y(X)$ such that for any $Z \in \mathcal{M}$ one has the equivalence:

$$X|_l YZ \quad \Longleftrightarrow \quad \sigma_Y(X)|_l Z. \tag{$*$}$$

Then the map σ uniquely extends to a map $\sigma : \mathcal{M} \times \mathbf{M} \to \mathbf{M}$ so that ($*$) holds for any $X \in \mathbf{M}$ and $Y, Z \in \mathcal{M}$. The map σ satisfies further the following **1)**–**4)**.

1) *The map σ defines an opposite left action σ_Y of $Y \in \mathcal{M}$ on the set $\mathbf{M}$ with the fixed point 1_n. That is,*

$$\sigma_{1_n} = id_{M_n}, \qquad \sigma_{Y_2 Y_1} = \sigma_{Y_1} \circ \sigma_{Y_2} \quad \text{and} \quad \sigma_Y(1_n) = 1_n$$

for any $Y, Y_1, Y_2 \in \mathcal{M}$.

2) *The map σ is compatible with the unit group action on $\mathcal{M}$ from right and that on $\mathbf{M}$ from left. That is, for any $Y \in \mathcal{M}$ and an invertible $E \in \mathcal{M}$, we have*

$$\sigma_{YE} = \left[E^{-1}\right]\sigma_Y$$

where $[E^{-1}]$ *denotes the left action on the set* $\mathbf{M}$ *induced from the left action of* E^{-1} *on the set of all left equivalence classes.*

3) *There exists a map* $u : \mathbf{M} \times \mathbf{M} \to \mathrm{U}(\mathcal{M}) :=$ *the unit group of* $\mathcal{M}$ *preserving* $\mathbf{M}$ *such that, for* $X, Y \in \mathbf{M}$*, we have*

$$X\sigma_X(Y) = Y\sigma_Y(X) \cdot u(X, Y).$$

4) *If there exists a degree map on* $|R|$ (*cf. Section 6*) *such that* $\deg(X) \geqslant \deg(\sigma_Y(X))$ *for* $X, Y \in I_0$*, then the inequality holds for all* $X, Y \in \mathbf{M}$*.*

Corollary. *Under the setting of theorem, any finite subset* J *of* $\mathcal{M}$ *admits a unique least common multiple* $\mathrm{LCM}(J) \in \mathbf{M}$ (*up to the right unit factor*)*.*

5. Least common multiples

As a consequence of the divisibility theory in the previous section, we describe the least common multiple for a given finite set in $\mathrm{M}(n, R)^\times$ and its basic nature.

Definition. An element $Z \in \mathrm{M}(n, R)^\times$ is called a *least common multiple* of a set $J \subset \mathrm{M}(n, R)^\times$, if 1) $X|_l Z\ \forall X \in J$ and 2) if $X|_l Z'\ \forall X \in J$ for some $Z' \in \mathrm{M}(n, R)^\times$ then $Z|_l Z'$. By the definition, least common multiples of J form either an empty set or a single left equivalence class. In the latter case, we shall denote by $\mathrm{LCM}(J)$ the normal form of the class and call it *the left least common multiple* of J.

Theorem 4. *Any finite* $J \subset \mathrm{M}(n, R)^\times$ *has the least common multiple* $\mathrm{LCM}(J)$*.*

Proof. We apply recursively Theorem 3 on the cardinality of J, where the case $\#J = 1$ is trivially true. Let $\#J > 1$ and put $J = J' \sqcup \{X\}$. By our induction hypothesis, there exists $\mathrm{LCM}(J')$. Then, $\mathrm{LCM}(J') \cdot \sigma_{\mathrm{LCM}(J')}(X)$ is a least common multiple of the set J, since 1) it is divisible by any $X' \in J'$, and divisible by X ($\Leftrightarrow \sigma_{Z \cdot \sigma_Z(X)}(X) = \sigma_{\sigma_Z(X)}(\sigma_Z(X)) = 1_n$), and 2) if an element $Z \in \mathrm{M}(n, R)^\times$ is divisible by the elements of $J' \sqcup \{X\}$ then Z should be divisible by $\mathrm{LCM}(J')$ and by X, implying that Z is divisible by $\mathrm{LCM}(J')\sigma_{\mathrm{LCM}(J')}(X)$. □

Combining the description $\mathrm{LCM}(X, Y) = [Y\sigma_Y(X)]$ with **4)** the monotonicity of Theorem 3, we obtain the following "upper and lower bound" of $\mathrm{LCM}(X, Y)$.

Corollary 5. *For any* $X, Y \in \mathrm{M}(n, R)^\times$*, we have*

$$\mathrm{LCM}\big(\det(X), \det(Y)\big) \,\big|\, \det\big(\mathrm{LCM}(X, Y)\big) \,\big|\, \det(X)\det(Y).$$

Proof. The first division relation follows from: $X|_l Y\sigma_Y(X)$ and $Y|_l X\sigma_X(Y)$, and the second division relation follows from $\det(X)\det(Y)/\det(\mathrm{LCM}(X, Y)) = \det(X)\det(Y)/\det(X\sigma_X(Y)) = \det(Y)/\det(\sigma_X(Y)) \in |R| \subset R$. □

In the following Parts I and II of the present section, we describe two basic properties of LCM, which will be used in Section 6 to analyze the skew growth function.

Part I. We first study the behavior of LCM of elements whose diagonals are co-prime to each other at each level $i = 1, \dots, n$. Then we get "multiplicativity" of the diagonals at each level. The result is used to show the weak Euler product decomposition of the skew growth function.

Lemma 6. *Let* $X, Y \in \mathrm{M}(n,R)^{\times}$ *be with* $\mathrm{diag}([X]) = (l_1, \dots, l_n)$ *and* $\mathrm{diag}([Y]) = (m_1, \dots, m_n)$. *If* l_i *and* m_i *are relatively prime in* R *for* $1 \leqslant i \leqslant n$ (*we shall say that* $\mathrm{diag}([X])$ *and* $\mathrm{diag}([Y])$ *are componentwisely co-prime*), *then* $\mathrm{diag}(\mathrm{LCM}(X,Y)) = (l_1 m_1, \dots, l_n m_n)$. *In particular, we have*: $\det(X)\det(Y) = \det(\mathrm{LCM}(X,Y))$.

Proof. Let $m_i = \prod_{k=1}^{k_i} p_{i,k}$ be the prime decomposition of the diagonal entities of Y, and let $Y = (\prod_{i=1}^{n}\prod_{k=1}^{k_i} P_{i,k})E$, where $P_{i,k}$ is a $p_{i,k}$-irreducible normal form of level i, $E \in \mathrm{GL}(n,R)$ and the order of the product is lexicographic, be the irreducible decomposition of Y given in Appendix A Lemma 10. Then, we have $Y\sigma_Y(X) \simeq (\prod_{i=1}^{n}\prod_{k=1}^{k_i} P_{i,k})(\prod_{i=n}^{1}\prod_{k=k_i}^{1} \sigma_{P_{i,k}}(X))$, where, inside in each big parenthesis of RHS, product is lexicographic or anti-lexico-graphic order. Considering each action of $\sigma_{P_{i,k}}$ inductively, it is sufficient to prove the case when Y is irreducible. Namely, we have only to prove the following special case.

Assertion. *Let* Y *be a* p*-irreducible element of level* i. *Suppose the* i*th component* l_i *of* $\mathrm{diag}([X])$ *is prime to* p. *Then, we have* $\mathrm{diag}([X]) = \mathrm{diag}(\sigma_Y(X))$.

Proof. The statement is equivalent to that $\mathrm{diag}([X\sigma_X(Y)]) = \mathrm{diag}([Y\sigma_Y(X)])$ is equal to $\mathrm{diag}([X])$ except at the ith place, where the values is pl_i, and, then, it is equivalent to that $\sigma_X(Y)$ is p-irreducible of level i if Y is so and X is lower triangular matrix whose ith diagonal element l_i is prime to p. This can be reduced again to the case when X is irreducible, by considering the decomposition $X = (\prod_{i=1}^{n}\prod_{k'=1}^{k'_i} P'_{i,k})E'$ and considering the action of $\sigma_{P'_{i,k}}$ in the expression $X\sigma_X(Y) \simeq (\prod_{i=1}^{n}\prod_{k'=1}^{k'_i} P'_{i,k})(\prod_{i=n}^{1}\prod_{k'=k'_i}^{1} \sigma_{P'_{i,k}})(Y)$ inductively. However, in **6.** of the proof of Theorem 3, it was shown that if X and Y are irreducibles, then $\sigma_X(Y)$ is an irreducible element such that i) $\det(Y) = \det(\sigma_X(Y))$ and ii) levels of Y and $\sigma_X(Y)$ coincide each other except the case $\det(X) = \det(Y)$ and levels of X and Y coincide (when the jump of level occurs in Case ii) of the proof). □

This completes a proof of Lemma 6. □

Part II. We next study the behavior of LCM for a set of p-irreducibles for a fixed prime $p \in R$. We will observe that the diagonals are no-longer multiplicative but the levels may go down or disappear (jumping of the level), that is, the data of levels of the input J alone cannot determine the levels of the output $\mathrm{LCM}(J)$.

Lemma 7. *Let $X = M(i : \mathbf{x})$ and $Y = M(i : \mathbf{y})$ be two distinct p-irreducible normal forms of the same level i. Set $k := \max\{1 \leqslant l < i \mid x_l - y_l \not\equiv 0 \bmod p\}$. Then*

$$\mathrm{LCM}(X, Y) = M(k : \mathbf{u})M(i : \mathbf{v}),$$

where $M(k : \mathbf{u})$ and $M(i : \mathbf{v})$ are mutually commutative p-irreducible normal forms of levels k and i, where the row vectors $\mathbf{u} = (u_i)$ and $\mathbf{v} = (v_i)$ are given as follows.

$$u_l \equiv (x_l - y_l)/(y_k - x_k) \bmod p \quad \text{for } 1 \leqslant l < k,\ u_k = p,\ u_l = 0 \text{ for } k < l \leqslant n,$$
$$v_l \equiv (x_l y_k - y_l x_k)/(y_k - x_k) \bmod p \quad \text{for } 1 \leqslant l < k,\ v_k = 0,\ v_l = x_l = y_l \text{ for } k < l \leqslant n.$$

Here we use the bijection $R/(p) \simeq R(p)$ for the reason given in **Lemma 9**.

Proof. Recall the proof of **6.**ii) of Theorem 3. Details are left to the reader. □

For a set J of p-irreducibles elements, $\mathrm{LCM}(J)$ can be calculated by applying Lemmas 6 and 7 successively. Its final form is characterized in the following lemma.

Lemma 8. *The following conditions* i)–v) *on $X \in M_n$ are equivalent.*

i) *There exists a set J of p-irreducibles such that $X = \mathrm{LCM}(J)$.*
ii) *X divides $p1_n$.*
iii) *X satisfies the following* 1) *and* 2).
   1) *Diagonal entries of X are either equal to* 1 *or to p.*
   2) *If the ith diagonal entry of X is equal to* 1*, then the (i, j)-entry of X for all j with $1 \leqslant j < i$ is equal to* 0*. If jth diagonal entry of X is equal to p, then the (i, j)-entry of X for all i with $j < i \leqslant n$ is equal to* 0*.*
iv) *Let $\mathbf{x}_i$ be the ith row-vectors of X $(1 \leqslant i \leqslant n)$, and set $J(X) := \{M(M : \mathbf{x}_i)\}_{i=1}^n$. Then,* 1) *$J(X)$ consists of mutually commutative p-irreducibles and possibly 1_n,* 2) *$X = \mathrm{LCM}(J(X)) = \prod_{i\in\{1,\dots,n\}} M(i : \mathbf{x}_i)$.*
v) *X is a product of p-irreducible normal forms which are mutually commutative and mutually of different levels.*

Proof. i) ⇒ ii). For a p-irreducible element X, $\det(X) = \varepsilon p$ $(\varepsilon \in \mathcal{E})$ implies $X|_l p1_n$. Then, any least common multiple of p-irreducible elements should divide $p1_n$.

ii) ⇒ iii). 1) follows since $p \cdot X^{-1}$ is integral. The first half of 2) follows from the definition of a normal form and $R(1) = \{0\}$. Let jth diagonal entry of X is equal to p. Put $\bar{i} := \min\{j < i \leqslant n \mid (i, j)\text{-entry of } X \text{ is not equal to } 0\}$. Due to 1) and the first half of 2), the $\bar{i}$th diagonal entry of X is equal to p. Then the $(\bar{i}, j)$-entry of X^{-1} is of a form c/p^2 for non-zero c, which contradicts to $pX^{-1} \in \mathrm{M}(n, R)$.

iii) ⇒ iv). Since the diagonals of X are either 1 or p, $J(X)$ consists of identity matrices 1_n and some p-irreducible normal forms of different levels. The commutativity of the elements of $J(X)$ follows from a general fact that *two normal forms $M(i:\mathbf{x})$ and $M(j:\mathbf{y})$ of levels i and j, respectively, for $i<j$ are commutative if and only if ith entry of $\mathbf{y}$ is equal to* 0. The commutativity implies $\mathrm{LCM}(J(X))|_l \prod_{i=1}^n M(i:\mathbf{x}_i)$. On the other hand, **Lemma 6** implies that $\det(\mathrm{LCM}(J(X)))$ is equal to $p^k = \det(\prod_{i=1}^n M(i:\mathbf{x}_i)) = \det(X)$ where $k := \#$ of p's in the diagonal of X. Thus, the equalities are shown.

iv) ⇒ v). Clear.

v) ⇒ i). If $X = X_1 \cdot \cdots \cdot X_m$ where $X_1, \ldots, X_m$ are mutually commutative, then $\mathrm{LCM}(X_1, \ldots, X_m)|X$. If $X_1, \ldots, X_m$ are mutually of different level, then applying Lemma 6, we get $\det(\mathrm{LCM}(X_1, \ldots, X_m)) = \det(X)$. This implies that $\mathrm{LCM}(X_1, \ldots, X_m)$ and X are equivalent normal forms, implying the equality. □

Note. The "commutativity" used in iv) and v) are not a property of the classes in $\mathrm{M}(n,R)^\times/\sim_l$ but a property of the matrices of normal forms themselves.

Example. 1. A matrix like $\left[\begin{smallmatrix} p & 0 \\ 1 & p \end{smallmatrix}\right] = \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 0 \\ 1 & p \end{smallmatrix}\right]$, which violates the condition iii), cannot be a least common multiple of some irreducible elements.

2. If $A := \left[\begin{smallmatrix} p & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right]$, $B := \left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ i & k & p \end{smallmatrix}\right]$, $C := \left[\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ j & k & p \end{smallmatrix}\right]$ for $i \neq j, k \in R(p)$, then $\mathrm{LCM}(B,C) = \left[\begin{smallmatrix} p & 0 & 0 \\ 0 & 1 & 0 \\ 0 & k & p \end{smallmatrix}\right]$ is divisible by A. Then we have: $\mathrm{LCM}(A,B) = \mathrm{LCM}(B,C) = \mathrm{LCM}(C,A) = \mathrm{LCM}(A,B,C)$.

We give a useful criterion to be divisible by a p-irreducible element.

Lemma 9. *A p-irreducible element $X \in \mathrm{M}(n,R)^\times$ divides an element $Y \in \mathrm{M}(n,R)^\times$ from the left, if and only if the mod p reduction of X divides that of Y in $\mathrm{M}(n,R/(p))$ (here "division relation in $\mathrm{M}(n,R/(p))$" is used in the sense given in the proof since $\det(X \bmod p) \equiv \det(X) \equiv 0 \bmod p$).*

Proof. Suppose there exists $Z \in \mathrm{M}(n,R)$ such that $Y \equiv XZ \bmod p$. Then, there exists $W \in \mathrm{M}(n,R)$ such that $XZ = Y + pW$. Using X^* (= adjoint of X, i.e. an element $X^* \in \mathrm{M}(n,R)$ s.t. $XX^* = p1_n$), we get the expression $X(Z - X^*W) = Y$. Since $\det(Y) \neq 0$, we get $\det(Z - X^*W) \neq 0$, and hence $X|_l Y$ in $\mathrm{M}(n,R)^\times$. Conversely, if there exists $Z \in \mathrm{M}(n,R)^\times$ with $Y = XZ$, then $Y \equiv XZ \bmod p$. □

6. Growth function and skew-growth function

As an application of the divisibility theory of $\mathrm{M}(n,R)^\times$, we study the growth and skew-growth function of the monoid $\mathrm{M}(n,R)^\times$. When R is residue finite, we give a direct proof of their Euler product formula.

We recall the definition of the skew-growth functions [6]. Let $\mathcal{M}$ be a cancellative monoid with the unit group G, which admits least common multiples.[3]

A map $\deg : \mathcal{M} \longrightarrow \mathbb{R}_{\geqslant 0}$ is called a *degree map* if it satisfies

i) $\deg(X) = 0$ if and only if $X \in G$,
ii) $\deg(XY) = \deg(X) + \deg(Y)$ for all $X, Y \in \mathcal{M}$,
iii) $\#(\{X \in \mathcal{M} \mid \deg(X) \leqslant r\}/G) < \infty$ for all $r \in \mathbb{R}_{>0}$.

For a given degree map, the growth function $P_{\mathcal{M},\deg}(t)$ and the skew growth function $N_{\mathcal{M},\deg}(t)$ are defined as formal Dirichlet series:

$$P_{\mathcal{M},\deg}(t) := \sum_{[X]\in\mathcal{M}/G} t^{\deg([X])},$$

$$N_{\mathcal{M},\deg}(t) := \sum_{J:\text{finite subset of } I_0} (-1)^{\#J} \sum t^{\deg(\mathrm{LCM}(J))},$$

where $I_0 :=$ left equivalence classes of irreducible elements of $\mathcal{M}$. As formal Dirichlet series, they satisfy the inversion formula [6, Section 5]

$$P_{\mathcal{M},\deg}(t) N_{\mathcal{M},\deg}(t) = 1.$$

Let us call a domain R to be *residue finite*, if $\#(R/mR) < \infty$ for all $m \in R \setminus \{0\}$.[4] The map $N : R \setminus \{0\} \to \mathbb{Z}_{\geqslant 1}$, $m \mapsto \#(R/mR)$ is called the *absolute norm*. We define the degree map on $\mathrm{M}(n, R)^{\times}$ by the composition:

$$\deg := \log \circ N \circ \det : \mathrm{M}(n, R)^{\times} \longrightarrow \mathbb{R}_{\geqslant 0}$$

where log is the logarithmic function taking the branch: $\mathbb{R}_{\geqslant 1} \to \mathbb{R}_{\geqslant 0}$. The fact that this map satisfies the condition iii) follows from the following fact.

Fact. *If R is residue finite, then $\#(\{(m) \subset R \mid \#R/(m) \leqslant r\}) < \infty$ for any $r \in \mathbb{R}_{>0}$.*

Proof. (Kurano.) Suppose the contrary. Then there are infinitely many distinct ideals $I_i \subset R$ such that all quotients R/I_i are isomorphic to a fixed finite field of order, say, f. The natural map $R \to \prod R/I_i$ is injective since for any $x \neq 0 \in R$, the ideal (x) is contained in only finite many of I_i's. For any element $x \neq 0 \in R$, the image of x^{f-1} in R/I_i is equal to either 0 or 1 so that we have $x^{f-1}(x^{f-1} - 1) = 0$. Since $x \neq 0$, the fact that R is a domain implies $x^{f-1} - 1 = 0$. Since R is infinite, taking mutually distinct

[3] The skew-growth function [6, Section 4] is defined for arbitrary cancellative monoid without assuming the existence of l.c.m. but using towers of common multiple sets. However, the existence of l.c.m.'s implies that the height of the towers is 1 and we get the present simple formulation.

[4] This condition is satisfied by 1) the principal order R of an algebraic number field of class number 1, e.g. $R = \mathbb{Z}$, and 2) the coordinate ring of a smooth affine curve over a finite field.

elements $x_1, \dots, x_f \in R \setminus \{0\}$, we get $x_i^{f-1} - 1 = 0$ $(i = 1, \dots, f)$. This contradicts again to the fact that R is a domain. □

In the rest of the present paper, we consider only the case when the principal ideal domain R is residue finite, and consider only the growth and skew-growth functions associated with the degree map induced from the absolute norm.

Formulae. Let R be residue finite. Then, by a change $t = \exp(-s)$ of variables from t to s, the associated growth and skew-growth functions are absolutely convergent on some right half s-plane and are given as analytic functions as follows.

1) $P_{\mathrm{M}(n,R)^\times,\deg}(\exp(-s)) = \zeta_R(s)\zeta_R(s-1)\cdots\zeta_R(s-n+1)$,
2) $N_{\mathrm{M}(n,R)^\times,\deg}(\exp(-s)) = \prod_{p\in\{\text{primes of } R\}/\mathcal{E}}(1 - N(p)^{-s})(1 - N(p)^{-s+1})\cdots(1 - N(p)^{-s+n-1})$

where $\zeta_R(s) := \sum_{a\in(R\setminus\{0\})/\mathcal{E}} N(a)^{-s}$ is the Dedekind zeta-function, which is well-known to be absolutely convergent on a region $\Re(s) > \exists\sigma_a$ and has the Euler product expression on $\prod_{p\in\{\text{primes of } R\}/\mathcal{E}}(1 - N(p)^{-s})^{-1}$ on the same domain.

Proof. 1) By the change of the variable, we rewrite the growth function

1)′ $P_{\mathrm{M}(n,R)^\times,\deg}(\exp(-s)) = \sum_{[X]\in\mathrm{M}(n,R)^\times/\mathrm{GL}(n,R)} N(\det(X))^{-s}$.

There are two proofs of the zeta function expression **1)**. The first one is to regard the expression **1)′** as a generalized Epstein zeta function $\zeta_n(1_n, s)$ for the quadratic form $X \in \mathrm{M}(n,R) \mapsto \det({}^tX 1_n X) = \det(X)^2$ (up to a factor of 2), then the formula **1)** follows from classical results (K.L. Siegel [7], M. Koecher [2]).

Let us give an alternative elementary proof of **1)** using the normal forms M_n. Let $X \in M_n$ be a normal form (Section 3) with $\mathrm{diag}(X) = (m_1, \dots, m_n)$. Then by the definition of the degree map, we have

$$t^{\deg(X)} = t^{\log(N(m_1))+\cdots+\log(N(m_n))} = N(m_1)^{\log(t)}\cdots N(m_n)^{\log(t)}.$$

Then, due to Lemma 2 and in view of $N(m) = \#(R(m))$ for $m \in |R|$, we have

$$\begin{aligned} P_{\mathrm{M}(n,R)^\times,\deg}(t) &= \sum_{X\in M_n} t^{\deg(X)} \\ &= \Big(\sum_{m_1\in|R|} N(m_1)^{\log(t)}\Big)\Big(\sum_{m_2\in|R|}\Big(\sum_{d_{21}\in R(m_2)} N(m_2)^{\log(t)}\Big)\Big) \\ &\quad \cdots \\ &\quad \times\Big(\sum_{m_n\in|R|}\Big(\sum_{d_{n1}\in R(m_n)}\cdots\sum_{d_{n,n-1}\in R(m_n)} N(m_n)^{\log(t)}\Big)\Big) \end{aligned}$$

$$= \sum_{m_1 \in |R|} N(m_1)^{\log(t)} \sum_{m_2 \in |R|} N(m_2)^{\log(t)+1} \cdots \sum_{m_n \in |R|} N(m_n)^{\log(t)+n-1},$$

where we use a fact $\#(R(m)) = N(m)$ for $m \in |R|$. Recalling the fact $|R| \simeq (R \setminus \{0\})/\mathcal{E}$, we have $\sum_{m \in |R|} N(m)^{\log(t)} = \zeta_R(-\log(t))$ and, hence, the formula **1)**.

2) There are two proofs of the Euler product formula **2)**.

The first proof is, as explained in Introduction, to rewrite the formula **1)** by the well-known Euler product formula of the Dedekind zeta-function, and to apply the inversion formula [6].

In the following, we present another proof of **2)**, which uses the structure of common multiples studied in Section 5 but does not use the inversion formula.

Let us, first, show a partial Euler product expansion of skew-growth functions in the sense of the following formula **4)** in next assertion.

Assertion 1. *For any finite subset $J \subset I_0$, one has an addition formula*:

3) $\deg(\mathrm{LCM}(J)) = \sum_{p:\text{primes of } R} \deg(\mathrm{LCM}(J \cap I_{0,p}))$.

where $I_{0,p} := \{$left equivalence classes of all p-irreducible elements$\}$. Then we get

4) $N_{\mathrm{M}(n,R)^\times,\deg}(t) = \prod_{p:\text{primes of } R} (\sum_{J \subset I_{0,p}} (-1)^{\#(J)} t^{\deg(\mathrm{LCM}(J))})$.

Proof. Obviously, $\mathrm{LCM}(J) = \mathrm{LCM}(\{\mathrm{LCM}(J \cap I_{0,p}) \mid p : \text{primes of } R\})$, where, except for finite primes p, the intersection $J \cap I_{0,p}$ is empty and $\mathrm{LCM}(J \cap I_{0,p}) = 1_n$. Then, the diagonal part $\mathrm{diag}(\mathrm{LCM}(J))$ of LHS is equal to that of RHS, which is given by the componentwise product of diagonal part of $\mathrm{diag}(\mathrm{LCM}(J \cap I_{0,p}))$ for primes p of R, since they are mutually componentwisely co-prime and we can apply Lemma 6. Thus, we have $\det(\mathrm{LCM}(J)) = \prod_{p:\text{primes}} \det(\mathrm{LCM}(J \cap I_{0,p}))$ and **3)**. Then applying **3)** to the definition of $N_{M,\deg}(t)$, we obtain **4)**. □

To get the finer decomposition **2)**, it remains to show the decomposition

5) $\sum_{J \subset I_{0,p}} (-1)^{\#(J)} t^{\deg(\mathrm{LCM}(J))} = \prod_{i=1}^{n} (1 - N(p)^{-s+i-1})$

for each prime p of R, where $-s = \log(t)$.

Set $I_{0,p} = \bigsqcup_{i=1}^{n} I_{0,p}^{(i)}$ where $I_{0,p}^{(i)} := \{X \in I_{0,p} \mid X \text{ is of level } i\}$ and $J^{(i)} := J \cap I_{0,p}^{(i)}$ for $J \subset I_{0,p}$. We decompose the summation index set of **5)** as $2^{I_{0,p}} = A \sqcup B$, where $A := \{J \subset I_{0,p} \mid \#(J^{(i)}) \leqslant 1 \ (1 \leqslant \forall i \leqslant n)\}$ and $B := 2^{I_{0,p}} \setminus A$.[5] Then the proof of the formula **5)** is achieved if we show the following two formulae.

[5] The decomposition $2^{I_{0,p}} = A \cup B$ is "suggested" by Lemma 8, where $\mathrm{LCM}(J)$ for any $J \in 2^{I_{0,p}}$ is given by another $\mathrm{LCM}(J')$ for $J \in A$.

6) $\sum_{J\in A}(-1)^{\#(J)}t^{\deg(\mathrm{LCM}(J))} = \prod_{i=1}^{n}(1-N(p)^{-s+i-1})$,
7) $\sum_{J\in B}(-1)^{\#(J)}t^{\deg(\mathrm{LCM}(J))} = 0$.

Proof of 6). Since for any $J \in A$, elements in J consist of p-irreducibles elements of different levels, we can apply Lemma 6 repeatedly. Then, we get

3)′ $\deg(\mathrm{LCM}(J)) = \deg(p^{\#(J)}) = \log(N(p)^{\#(J)}) = \sum_{i=1}^{n}\log(N(p)^{\#(J^{(i)})})$,

so that, similarly to the formula **4)**, we get

4)′ $\sum_{J\in A}(-1)^{\#(J)}t^{\deg(\mathrm{LCM}(J))} = \prod_{i=1}^{n}(1-\sum_{X\in I_{0,p}^{(i)}}N(p)^{-s}) = \prod_{i=1}^{n}(1-N(p)^{-s+i-1})$,

where, in the last step, we use the fact $\#(I_{0,p}^{(i)}) = \#(R(p))^{i-1} = N(p)^{i-1}$. □

Proof of 7). It is sufficient to show an existence of an involution map $\tau : B \to B$ satisfying the following conditions:

i) $\mathrm{LCM}(J) = \mathrm{LCM}(\tau(J))$ and ii) $\#(J)+\#(\tau(J)) \equiv 1 \bmod 2$ for all $J \in B$, since then

$$\begin{aligned} 2\sum_{J\in B}(-1)^{\#(J)}t^{\deg(\mathrm{LCM}(J))} &= \sum_{J\in B}\left((-1)^{\#(J)}t^{\deg(\mathrm{LCM}(J))} + (-1)^{\#(\tau(J))}t^{\deg(\mathrm{LCM}(\tau(J)))}\right) \\ &= 0. \end{aligned}$$

If $n = 1$, then $B = \emptyset$. Assume $n \geqslant 2$. We construct the involution τ by a use of the jump (Section 5 Part II). For $J \in B$, set $m := \max\{2 \leqslant m \leqslant n \mid \#(J^{(m)}) \geqslant 2\}$. According to Section 5 Part II, Lemmas 7 and 8, we have a decomposition $\mathrm{LCM}(J^{(m)}) = \prod_{i\in\{1,\dots,r\}} M(k_i : \mathbf{x}_{k_i})$, where $M(k_i : \mathbf{x}_{k_i})$ $(1 \leqslant i \leqslant r)$ are mutually commutative p-irreducible normal forms of levels k_i. By the jump phenomenon, we know that $r \geqslant 2$ and $1 \leqslant k_1 < \cdots < k_r = m$, and, in particular, $k_1 < m$. Then we define

$$\tau(J) := \begin{cases} J \sqcup \{M(k_1 : \mathbf{x}_{k_1})\} & \text{if } M(k_1 : \mathbf{x}_{k_1}) \notin J, \\ J \setminus \{M(k_1 : \mathbf{x}_{k_1})\} & \text{if } M(k_1 : \mathbf{x}_{k_1}) \in J. \end{cases}$$

It is clear that τ defines an involution of B. Let us show the properties i) and ii) of τ, where ii) is apparent by definition. To see i), let us decompose $J = J^{(m)} \cup J'$ and $\tau(J) = J^{(m)} \cup J''$ with $J' := J \setminus J^{(m)}$ and $J'' := \tau(J) \setminus J^{(m)}$ for $J \in B$. Then,

$$\begin{aligned} \mathrm{LCM}(J) &= \mathrm{LCM}\big(\{\mathrm{LCM}(J^{(m)}), J'\}\big) = \mathrm{LCM}\big(\{M(k_i : \mathbf{x}_{k_i})\ (i = 1, \dots, r), J'\}\big), \\ \mathrm{LCM}\big(\tau(J)\big) &= \mathrm{LCM}\big(\{\mathrm{LCM}(J^{(m)}), J''\}\big) = \mathrm{LCM}\big(\{M(k_i : \mathbf{x}_{k_i})\ (i = 1, \dots, r), J''\}\big) \end{aligned}$$

where RHS's of both lines coincide to each other, since only difference between J' and J'' is that one contains the element $M(k_1 : \mathbf{x}_{k_1})$ and the other does not.

This completes the proof of the formula **7)** and, hence, of the formula **2)**. □

Acknowledgments

The author is grateful to professors Akio Fujii, Masatoshi Suzuki, Satochi Kondo and Keiich Watanabe for informing the author some references and to Kazuhiko Kurano for a proof of Fact in Section 6. He also expresses his gratitude to Scott Carnahan and to the referee for the careful reading of the manuscript and valuable suggestions.

Appendix A. Irreducible decomposition

Any element of $\mathrm{M}(n,R)^\times$ is decomposable into a product of irreducible elements. However the decomposition is not unique and has a big variety. In the present appendix, we give a decomposition, which is used in the proof **7.** of Theorem 3.

Lemma 10. *Let $X \in \mathrm{M}(n,R)^\times$ and let $\mathrm{diag}([X]) = (m_1,\dots,m_n)$ be the diagonal of its normal form. Let us fix an ordered irreducible decomposition $m_i = \prod_{k=1}^{k_i} p_{i,k}$ for each m_i $(i = 1,\dots,n)$. Then, there exist a unique $p_{i,k}$-irreducible normal form $P_{i,k}$ of level i for $1 \leqslant i \leqslant n$ and $1 \leqslant k \leqslant k_i$, and a unit element $E \in \mathrm{GL}(n,R)$ such that*

$$X = \left(\prod_{i=1}^{n} \prod_{k=1}^{k_i} P_{i,k} \right) E.$$

Here the product order is the lexicographic order of the running indexes i and k.

Proof. We fix a notation: for $1 \leqslant i \leqslant n$ and $p \in |R| \subset R$, we set

$$M(i:p) := \text{the set of normal forms of level } i \text{ with diagonal } p.$$

According to the ordered product of m_i, we consider the ordered product set

$$P := \prod_{k=1}^{k_1} M(1:p_{1,k}) \prod_{k=1}^{k_2} M(2:p_{2,k}) \cdots \prod_{k=1}^{k_n} M(n:p_{n,k})$$

and consider a product map $\pi : P \to \mathrm{M}(n,R)^\times$ according to the order. Then, in view of Lemma 2 and the identification $[X]_l = X \cdot \mathrm{GL}(n,R)$, Lemma 10 is equivalent to say that *the map π induces a bijection to a subset of $\mathrm{M}(n,R)^\times$ which is in one-to-one correspondence (by the left equivalence) with the set*

$$M_n(m_1,\dots,m_n) := \left\{ X \in M_n \;\middle|\; \mathrm{diag}(X) = (m_1,\dots,m_n) \right\}.$$

We prove the statement by induction on the number of factors in P. So, consider the product set $\tilde{P}$ by forgetting the last factor from P, i.e. $P = \tilde{P} \times M(n : p_{n,k_n})$, and put $m_n = \tilde{m}_n p_{n,k_n}$. The induction hypothesis says that the image $\pi(\tilde{P})$ is bijective to

a set which is in one-to-one correspondence with $M_n(m_1,\dots,m_{n-1},\tilde{m}_n)$. Precisely, this means that $\pi(\tilde{P})$ consists of elements of the form $X=(\prod_{i=1}^{n-1}M(i:(\mathbf{x}_i,m_i,\mathbf{0})))M(n:(\mathbf{y},\tilde{m}_n))$ for $\mathbf{x}_i\in R^{i-1}$ and $\mathbf{y}\in R^{n-1}$ such that the set of their left-equivalence class $\{[X]_l \mid X\in\pi(\tilde{P})\}$ is bijective to $M_n(m_1,\dots,m_{n-1},\tilde{m})$. That is, $\mathbf{x}_i$ runs over the set which is (by taking mod m_i) bijective to $R(m_i)^{i-1}$ for $1\leqslant i\leqslant n-1$ and $\mathbf{y}$ runs over the set $S\subset R^{n-1}$ which is (by taking mod $\tilde{m}_n$) bijective to $R(\tilde{m}_n)^{n-1}$. We have to show that the set $\pi(P)=\pi(\tilde{P})M(n:p_{n,k_n})=\{XZ \mid X\in\pi(\tilde{P}),Z\in M(n:p_{n,k_n})\}\subset \mathrm{M}(n,R)^\times$ is (by the left-equivalence) bijective to $M_n(m_1,\dots,m_n)$. Actually, $Z\in M(n:p_{n,k_n})$ is of the form $M(n:(\mathbf{z},p_{n,k_n}))$ where $\mathbf{z}$ is running over the set $R(p_{n,k_n})^{n-1}$. Then the product XZ is of the form

$$XZ=\left(\prod_{i=1}^{n-1}M\big(i:(\mathbf{x}_i,m_i,\mathbf{0})\big)\right)M\big(n:(\mathbf{y}+\tilde{m}_n\mathbf{z},m_n)\big).$$

Then, we need to show that the set $T:=\{\mathbf{y}+\tilde{m}_n\mathbf{z}\mid \mathbf{y}\in S,\mathbf{z}\in R(p_{n,k_n})^{n-1}\}$ is (by taking mod m_n) bijective to $R(m_n)^{n-1}$. But, this is trivial, since, for each $\mathbf{w}\in R(\tilde{m}_n)^{n-1}$, there exist a unique element $\mathbf{y}\in S$ and $\mathbf{v}_{\mathbf{w}}\in R^{n-1}$ such that $\mathbf{y}=\mathbf{w}+\tilde{m}_n\mathbf{v}_{\mathbf{w}}$. Then, changing the index from $\mathbf{y}$ to $\mathbf{w}$, we have an expression

$$T=\big\{\mathbf{w}+\tilde{m}_n(\mathbf{v}_{\mathbf{w}}+\mathbf{z})\;\big|\;\mathbf{w}\in R(\tilde{m}_n)^{n-1},\ \mathbf{z}\in R(p_{n,k_n})^{n-1}\big\}.$$

In view of the exact sequence $0\to(\tilde{m}_n)/(m_n)\to R/(m_n)\to R/(\tilde{m}_n)\to 0$, we get $T \bmod m_n=\{\mathbf{w}+\tilde{m}_n\mathbf{z}\mid \mathbf{w}\in R(\tilde{m}_n)^{n-1},\mathbf{z}\in R(p_{n,k_n})^{n-1}\}\bmod m_n=R(m_n)^{n-1}\bmod m_n$.

This completes a proof of Lemma 10. □

Remark. 1. In **Lemma 10** for the case $R=\mathbb{Z}$ (Section 3 **Eg.**), if $X\in M_n$, then $E=1_n$.

2. The irreducible factors $P_{i,k}$ depend strongly on the order of the product.

Here are some examples of different irreducible normal forms decomposition.

$$\begin{bmatrix}1&0\\1&6\end{bmatrix}=\begin{bmatrix}1&0\\1&3\end{bmatrix}\begin{bmatrix}1&0\\0&2\end{bmatrix}=\begin{bmatrix}1&0\\1&2\end{bmatrix}\begin{bmatrix}1&0\\0&3\end{bmatrix},$$
$$\begin{bmatrix}1&0\\4&6\end{bmatrix}=\begin{bmatrix}1&0\\1&3\end{bmatrix}\begin{bmatrix}1&0\\1&2\end{bmatrix}=\begin{bmatrix}1&0\\0&2\end{bmatrix}\begin{bmatrix}1&0\\2&3\end{bmatrix}$$

3. The product map: $M_n(m_1,\dots,m_n)\times M_n(l_1,\dots,l_n)\to M_n(m_1l_1,\dots,m_nl_n)$, where the target set is considered as a subset of the quotient set $\mathrm{M}(n,R)/\mathrm{GL}(n,R)$, for general $m_i,l_i\in|R|$ is neither injective nor surjective. Eg. for $(m_1,m_2)=(a,2)$ and $(l_1,l_2)=(2,b)$, we have two decompositions $\left[\begin{smallmatrix}2a&0\\2c&2b\end{smallmatrix}\right]=\left[\begin{smallmatrix}a&0\\0&2\end{smallmatrix}\right]\left[\begin{smallmatrix}2&0\\c&b\end{smallmatrix}\right]=\left[\begin{smallmatrix}a&0\\1&2\end{smallmatrix}\right]\left[\begin{smallmatrix}2&0\\c-1&b\end{smallmatrix}\right]$. However $\left[\begin{smallmatrix}2a&0\\2c+1&2b\end{smallmatrix}\right]$ has no decomposition $\left[\begin{smallmatrix}a&0\\*&2\end{smallmatrix}\right]\left[\begin{smallmatrix}2&0\\*&b\end{smallmatrix}\right]E\equiv 0 \bmod 2$. *A sufficient condition for the map to be bijective is that there exists* $1\leqslant i_0\leqslant n$ *such that* $m_i=1$ *for* $i>i_0$ *and* $l_i=1$ *for* $i<i_0$ (the proof is the same as Lemma 10). These examples show that the

lexicographic order using levels in Lemma 10 is necessary. Once one violates the ordering of levels, then one loses the uniqueness or existence of the decompositions.

References

[1] Egbert Brieskorn, Kyoji Saito, Artin-Gruppen und Coxeter-Gruppen, Invent. Math. 17 (1972) 245–271, English translation by C. Coleman, R. Corran, J. Crisp, D. Easdown, R. Howlett, D. Jackson and A. Ram at the University of Sydney, 1996.
[2] Max Koecher, Über Dirichlet-Reihen mit Funktionalgleichung, J. Reine Angew. Math. 192 (1953) 1–23.
[3] Kyoji Saito, Growth functions associated with Artin monoids of finite type, Proc. Japan Acad. Ser. A Math. Sci. 84 (10) (2008) 179–183.
[4] Kyoji Saito, Limit elements in the configuration algebra for a cancellative monoid, Publ. Res. Inst. Math. Sci. 46 (2010) 37–113, http://dx.doi.org/10.2977/PRIMS/2.
[5] Kyoji Saito, Growth partition functions for cancellative infinite monoids, preprint RIMS-1705, 2010.
[6] Kyoji Saito, Inversion formula for the growth function of a cancellative monoid, J. Algebra 385 (2013) 314–332, http://dx.doi.org/10.1016/j.jalgebra.2013.01.037, arXiv:1201.5496.
[7] Carl Ludwig Siegel, Über die Zetafunktionen indefiniter quadratischer Formen I, Math. Z. 43 (1938) 682–708;
Carl Ludwig Siegel, Über die Zetafunktionen indefiniter quadratischer Formen II, Math. Z. 44 (1939) 398–426.