RIMS-1755

Monoid structure on square matrices over a PID

By

Kyoji SAITO

July 2012

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

Monoid structure on square matrices over a PID

Kyoji Saito

[1]

Abstract

We consider the set $\mathrm{M}(n,R)^\times$ of all square matrices of size $n \in \mathbb{Z}_{\geq 1}$ with non-zero determinants and coefficients in a principal ideal domain R. It forms a cancellative monoid with the matrix product. We develop an *elementary theory of divisions* by irreducible elements in $\mathrm{M}(n,R)^\times$, and show that *any finite set of irreducible elements of* $\mathrm{M}(n,R)^\times$ *has the right/left least common multiple* up to a unit factor.

As an application, we calculate the growth function $P_{\mathrm{M}(n,R)^\times,\deg}(t)$ and the skew growth function $N_{\mathrm{M}(n,R)^\times,\deg}(t)$ of the monoid $\mathrm{M}(n,R)^\times$. We get expressions $P_{\mathrm{M}(n,R)^\times,\deg}(\exp(-s)) = \zeta_R(s)\zeta_R(s-1)\cdots\zeta_R(s-n+1)$ and $N_{\mathrm{M}(n,R)^\times,\deg}(\exp(-s)) = \prod_{p\in\{\text{primes}\}}(1-N(p)^s)(1-N(p)^{s-1})\cdots(1-N(p)^{s-n+1})$, where $\zeta_R(s)$ is Dedekind zeta-function and N is the absolute norm on R. The structure of least common multiples in the monoid $\mathrm{M}(n,R)^\times$ studied above gives an elementary and direct proof of these decompositions, that is distinct from proofs by classical machinary.

Contents

1. **Introduction** 1
2. **Monoid $\mathrm{M}(n,R)^\times$ and its irreducible elements** 3
3. **Normal form for the classes of $\mathrm{M}(n,R)/\sim_l$** 4
4. **Left division theory** 5
5. **Least common multiples** 9
6. **Growth function and skew-growth function** 12
7. **Appendix (irreducible decomposition)** 14
References 15

[2]

1. Introduction

Let R be a principal ideal domain. We study the division theory on the monoid $M(n,R)^\times$ of all square matrices of size $n \in \mathbb{Z}_{>0}$ with coefficients in R, non-zero determinants and the unit 1_n. When the size n of the matrix is equal to 1, then we obtain the classical theory of prime decompositions in the domain R, whose analytic counterpart is the study of the Dedekind zeta-function $\zeta_R(s)$. If the size n is at least 2, then the monoid is non-commutative. Even though the standard concepts of prime elements and prime decompositions lose their meaning, the concepts of left or right (least) common multiples make senses. However, such theory and its analytic counterpart have not been systematically studied. Motivated by a study of certain thermo-dynamical limit functions over cancellative monoids [S1,3], in the present paper, we study an elementary theory of left divisions by irreducible elements in $\mathrm{M}(n,R)^\times$. Using this division theory, we describe the growth and the skew-growth function for the monoid $\mathrm{M}(n,R)^\times$ as their analytic counterparts.

[1] 2000 Mathematics Subject Classification: Primary AL; Secondary GR.

[2] **Acknowledgement:** The author is grateful to professors Akio Fujii, Satoshi Kondo and Masatoshi Suzuki for discussions and for informing the author about some literatures. He also expresses his gratitude to Scott Carnahan for the careful reading of the manuscript.

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 $AC = B$. The division relation $A|_l B$ depends only on the right equivalence classes $[A], [B]$ in $M(n,R)^\times/\mathrm{GL}(n,R)$. Thus, a poset structure on $M(n,R)^\times/\mathrm{GL}(n,R)$ is defined as $[A] \leq [B] \Leftrightarrow_{def} A|_l B$. An element X in $\mathrm{M}(n,R)^\times$ is called irreducible if its class $[X]$ is minimal in the poset minus the lowest class $[1_n]$. Actually, irreduciblity of X is characterized by the fact that its determinant is a prime element, say p, in R (§2 Lemma2.1). We call such X a p-irreducible element. Then in §4, we formulate the key result of the division theory by irreducible elements in $M(n,R)^\times$ in the following form.[3]

Theorem 3. *Let $I_{0,p}$ be the set of right equivalence classes of all p-irreducible elements of the monoid $\mathrm{M}(n,R)^\times$. Then, for any element Z of the monoid $\mathrm{M}(n,R)^\times$, there exists a map $\sigma_Z : I_{0,p} \cup \{1_n\} \to I_{0,p} \cup \{1_n\}$ such that for any $X \in I_0 \cup \{1_n\}$ and for any element $Y \in \mathrm{M}(n,R)^\times$, we have the following equivalence:*

$$X \mid_l ZY \quad \Longleftrightarrow \quad \sigma_Z(X) \mid_l Y.$$

Applying this result recursively, we see immediately in §5 that there exists a unique, up to right equivalence, minimal common right-multiple, denoted by $\mathrm{LCM}(J)$, for any finite set J of irreducible elements. However, the behavior of the least common multiples among irreducible elements having the same determinant p is an intricate arithmetic process, caused by a phenomenon, called bridging[4].

If $\#R/(m) < \infty$ for all $m \in R \setminus \{0\}$ (e.g. $R = \mathbb{Z}$, see §6), using the absolute norm $N : R \setminus \{0\} \to \mathbb{Z}_{>0}, m \mapsto N(m) := \#R/(m)$, we introduce the degree map by

$$X \ \in \ \mathrm{M}(n,R)^\times \quad \mapsto \quad \deg(X) := \log(N(\det(X))) \ \in \ \mathbb{R}_{\geq 0}.$$

Actually, $\deg(X)$ depends only on the class $[X]$ of X. Then, in §6 we introduce the growth function and the skew-growth function ([S3]), respectively, by

$$\begin{array}{rcl} P_{\mathrm{M}(n,R)^\times,\deg}(t) & := & \sum_{[X] \in \mathrm{M}(n,R)^\times/\mathrm{GL}(n,R)} t^{\deg([X])} \\ N_{\mathrm{M}(n,R)^\times,\deg}(t) & := & \sum_{J\text{: finite subset of } I_0} (-1)^{\#J} t^{\deg(\mathrm{LCM}(J))} \end{array}$$

Then, by the change of variable $t = \exp(-s)$ to s, we get the expressions

$$\begin{array}{rcl} P_{\mathrm{M}(n,R)^\times,\deg}(\exp(-s)) & = & \zeta_R(s)\ \zeta_R(s-1)\ \cdots\ \zeta_R(s-n+1) \\ N_{\mathrm{M}(n,R)^\times,\deg}(\exp(-s)) & = & \prod_{p\text{: primes of } R} (1-N(p)^s)(1-N(p)^{s-1})\cdots(1-N(p)^{s-n+1}), \end{array}$$

where $\zeta_R(s)$ is the Dedekind zeta-function of R. The proofs of these formulae can be reduced to classical results (c.f. [Si][K]), however, we give direct elementary proofs, using the monoid structure on $\mathrm{M}(n,R)^\times$ studied above. Namely, n factors of the growth and the skew-growth functions corresponds to n levels on the monoid. However, in order to show the factorization of the skew-growth function $N_{\mathrm{M}(n,R)^\times}(t)$, we need to show a big cancellation of terms (§6, **7)**), and this cancellation is achieved by *bridging* among p-irreducible elements studied in §5.

[3]The formulation of Theorem 3 here is, in its spirit, parallel to [B-S, Lemma3.1] of division theory in Artin monoids. Namely, we can make a dictionary: $X \in I_{0,p} \leftrightarrow a \in I = \{\text{generators}\}$, $\sigma_Z(X) \leftrightarrow b$, $Z \leftrightarrow C$, $Y \leftrightarrow D$ between them. However, they are not completely parallel, namely, Theorem 3 states an equivalence but Lemma 3.1 states only one implication $a|_l CD \Rightarrow b|_l D$. This was caused by the fact that the Artin braid relations may have length≥ 2.

[4]In §3, we introduce *level* of an irreducible element form 1 to n. If X and Z are p-irreducible elements of the same level i, then $\sigma_Z(X)$ is a p-irreducible element of level *strictly lower* than i. We call this phenomenon bridging of level (see §4 Proof of Theorem 1, 5.Case ii) and §6 Part II).

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:

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

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 $M(n,R)^\times$ 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

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

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 basic fact:

Lemma 1. *An element $X \in \mathrm{M}(n,R)^\times$ is irreducible if and only if $\det(X) \in R$ is irreducible, or, equivalent to say, prime in R.*

Proof. Suppose $\det(X)$ is irreducible 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 $\mathrm{GL}(n,R)$. Conversely assume that X is irreducible. Since, for a principal ideal domain R, any double coset in $\mathrm{GL}(n,R)\backslash M(n,R)/\mathrm{GL}(n,R)$ can be presented by a diagonal matrix, we may assume that X is diagonal. Then, except that one diagonal entry is an irreducible element in R, all the other diagonal entries of X are units in $\mathcal{E}$. Hence, $\det(X)$ is irreducible. □

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

Remark. We do not study irreducible decompositions of elements of $M(n,R)^\times$, but study the division relation between two right cosets in $\mathrm{M}(n,R)^\times/\mathrm{GL}(n,R)$, where, still, the concept of irreducible elements plays a crucial role (see §3,4).

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.

We define equivalences $X \sim_l Y \Leftrightarrow_{\mathrm{def}} X|_l Y \ \&\ Y|_l X$. Then, due to the cancellativity of $\mathrm{M}(n,R)^\times$, we have the coset expressions:

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

where RHS is the quotient set by the right action of $\mathrm{GL}(n,R)$. We sometimes denote by $[X]_l$ or by $[X]$ the left-equivalence class of an element $X \in \mathrm{M}(n,R)^\times$. 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: $[X]_l \leq_l [Y]_l \Leftrightarrow_{\mathrm{def}} X|_l Y$. 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 $\leq_l$,

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 $\mathrm{M}(n,R)^\times/\sim_r = \mathrm{GL}(nR)\backslash M(n,R)^\times$. One has a poset isomorphism: $\mathrm{M}(n,R)^\times/\sim_r \equiv \mathrm{M}(n,R)^\times/\sim_l$, $[X] \mapsto [{}^tX]$, and we study only $\mathrm{M}(n,R)^\times/\sim_l$.

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

We give normal forms for elements of the posets $\mathrm{M}(n,R)/\sim_l$ for all $n \in \mathbb{Z}_{\geq 1}$. To this end, we fix once and forall a subset $M \subset R \setminus \{0\}$ and subsets $R_m \subset R$ for all $m \in M$, for which the following natural projections are bijections:

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

where (m) is the principal ideal in R generated by m. Without a loss of generality, we assume that 1) the set M is multiplicative (i.e. the set M is closed under the products among its elements), and 2) the class $(m) \in R/(m)$ is presented by $0 \in R_m$.

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

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

Lemma 2. *Every right* $\mathrm{GL}(n,R)$*-orbit in* $\mathrm{M}(n,R)^\times$ *intersects with the set* M_n *at a single element. That is, the restriction to the subset* M_n *of 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 $\mathrm{M}(1,R)^\times/\sim = (R\setminus\{0\})/\mathcal{E} \simeq M = M_1$. 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 $\mathbf{x}=(x_1,\cdots,x_n) \in R^n$ be its first row vector, which is non-zero by the determinant condition $\det(X) \neq 0$. Then, there exists $m_1 \in M$, which generates the ideal $(x_1,\cdots,x_n)$, and $A \in \mathrm{GL}(n,R)$ such that $\mathbf{x}A = (m_1,0,\cdots,0)$. Hence, we may choose a representative of the class $[X]_l$ to be of the form: $\begin{bmatrix} m_1 & 0 \\ * & X' \end{bmatrix}$ for $X' \in M(n-1,\mathbb{Z})^\times$. By our induction hypothesis, there exists $A' \in \mathrm{GL}(n-1,R)$ such that $\begin{bmatrix} m_1 & 0 \\ * & X' \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & A' \end{bmatrix} = \begin{bmatrix} m_1 & 0 \\ * & X'' \end{bmatrix}$ where X'' is an element of M_{n-1} whose diagonal is $(m_j)_{j=2}^n \in M^{n-1}$. 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 $\begin{bmatrix} 1 & 0 \\ *' & 1_{n-1} \end{bmatrix}$ from the right, we get the normal form $\begin{bmatrix} m_1 & 0 \\ * & X'' \end{bmatrix} \begin{bmatrix} 1 & 0 \\ *' & 1_{n-1} \end{bmatrix} = \begin{bmatrix} m_1 & 0 \\ d' & X'' \end{bmatrix}$.

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 $\mathcal{Z}$. Since $m^{-1}m' \in \mathcal{Z}$ for $m, m' \in M$ 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 low or the last column and low, 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 $u_{n1} = 0$. $\square$

Definition. For an equivalence class $[X] \in \mathrm{M}(n,R)^\times/\sim_l$, we call the element $[X] \cap M_n \in M_n$ the *normal form* of $[X]$. We often identify the class $[X]$ with its normal form, when there is no possibility of confusion. By the *diagonal part of* the class $[X]$, denoted by $\mathrm{diag}([X])$, we mean the diagonal of the normal form of $[X]$, i.e. $\mathrm{diag}([X]\cap M_n) =$ the ordered sequence $(m_1,\cdots,m_n) \in M^n$, where each m_i $(1 \le i \le n)$ is called the diagonal entry of $[X]$ of ith *level*.

Notation For a row vector $\mathbf{x} \in R^n$ and an integer $1 \le i \le n$, we set

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

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

If, further, the diagonal m of $M(i:\mathbf{x})$ is an irreducible 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 right equivalent to a unique irreducible normal form for a certain level i $(1 \le i \le n)$. We call i the *level of the irreducible element*. Thus, for any irreducible element $p \in R$, the set of right equivalence classes of all p-irreducible elements is naturally bijective to

$$I_{0,p} := \bigsqcup_{i=1}^{n} \{M(i:(d_1,\cdots,d_{i-1},p,0,\cdots,0)) \mid (d_1,\cdots,d_{i-1}) \in (R_p)^{i-1}\}.$$

4. Left division theory

We develop, in a style similar to the division theory for Artin monoids [BS,§3], a division theory of an element $\mathrm{M}(n,R)^\times$ by an irreducible element from left.

Theorem 3. *Let p be a prime of R, and let $I_{0,p}$ be the set of right equivalence classes of all p-irreducible elements of $\mathrm{M}(n,R)^\times$. Then, for any element $Z \in \mathrm{M}(n,R)^\times$, there exists a map σ_Z from $\{1_n\} \sqcup I_{0,p}$ to itself such that for any $X \in \{1_n\} \sqcup I_{0,p}$ and $Y \in \mathrm{M}(n,R)^\times$, one has the equivalence*

$$(*) \qquad X \mid_l ZY \quad \Longleftrightarrow \quad \sigma_Z(X) \mid_l Y$$

Proof. The proof is divided into the following six steps **1**. - **6**. i)-iv).

1. For a given pair of a p-irreducible element X and an element $Z \in \mathrm{M}(n,R)$, if there exists $\sigma_Z(X) \in M_n$ satisfying condition $(*)$, then it is unique.

Proof. Suppose that there are two elements $\sigma, \sigma' \in \mathrm{M}(n,R)$ such that $\sigma|_l Y \Leftrightarrow \sigma'|_l Y$ for any $Y \in \mathrm{M}(n,R)$. Then, by choosing Y to be σ and σ', we get $\sigma'|_l\sigma$ and $\sigma|_l\sigma'$. That is, σ and σ' are right equivalent, i.e. $[\sigma] = [\sigma']$. $\square$

2. Suppose that there exists σ_Z for a given $Z \in \mathrm{M}(n,R)$ satisfying the condition $(*)$. Then, for any $E \in \mathrm{GL}(n,R)$, there exists σ_{ZE} and

$$\sigma_{ZE} = E^{-1}\sigma_Z,$$

where E^{-1} is a self-map of $\{1_n\} \sqcup I_{0,p}$ induced from the left multiplication of E^{-1}.

Proof. We have: $X \mid_l ZEY \;\Leftrightarrow\; \sigma_Z(X) \mid_l EY \;\Leftrightarrow\; E^{-1}\sigma_Z(X) \mid_l Y$. $\square$

Corollary. In order to show the existence of σ_Z for all $Z \in \mathrm{M}(n,R)^\times$, it is sufficient to show its existence only for $Z \in M_n$.

3. Suppose that there exist σ_{Z_1} and σ_{Z_2} for Z_1 and $Z_2 \in \mathrm{M}(n,R)$ satisfying the condition $(*)$, respectively. Then, there exists $\sigma_{Z_2Z_1}$ and

$$\sigma_{Z_2Z_1} = \sigma_{Z_1} \circ \sigma_{Z_2}.$$

Proof. We have: $X \mid_l Z_2Z_1Y \quad \Leftrightarrow \quad \sigma_{Z_2}(X) \mid_l Z_1Y \quad \Leftrightarrow \quad \sigma_{Z_1}(\sigma_{Z_2}(X)) \mid_l Y$. □

Corollary. In order to show the existence of σ_Z for all $Z \in M_n$, it is sufficient to show the existence of σ_Z only for irreducible normal forms Z.

Proof. In §7, we shall see that any $Z \in M_n$ admits a decomposition $Z = Z_1 \cdot Z_2 \cdots Z_k$ into irreducible normal forms. Then, in view of the formula **3.**, we have $\sigma_Z = \sigma_{Z_k} \circ \cdots \circ \sigma_{Z_2} \circ \sigma_{Z_1}$. □

5. Let $Y \in \mathrm{M}(n,R)$ be a lower triangular matrix. Then, Y is divisible by a p-irreducible normal form X of level $1 \leq i \leq n$, i.e. $X \mid_l Y$, if and only if

$$p \mid v \qquad \text{and} \qquad \mathbf{y} \equiv \mathbf{d}Y' \mod p.$$

where $X = M(i : (\mathbf{d}, p, \mathbf{o}))$ for $\mathbf{d} \in (R_p)^{i-1}$ and the i-principal sub-matrix of Y is of the form $= \begin{bmatrix} Y' & 0 \\ \mathbf{y} & v \end{bmatrix} \in \mathbb{R})^{\times}$ with $Y' \in \mathrm{M}(i-1,R)$, $\mathbf{y} \in R^{i-1}$ and $v \in R$.

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

6. Let X be a p-irreducible element of level i and Z be a q-irreducible element of level j for primes $p, q \in M$ and $1 \leq i, j \leq n$. Then, there exists $\sigma_Z(X)$ satisfying condition $(*)$.

Proof. The proof is divided into 4 cases.

Case i) $i < j$.

Since Z is of level j, ZY is a lower triangular matrix, which coincides with Y from 1 to $j-1$ rows. On the other hand, the divisibility of ZY (resp. Y) by X from the left is determined by the low vectors of ZY (resp. Y) from 1 to ith. That is, we have the equivalence $X|_lZY \Leftrightarrow X|_lY$. That is, we have

$$\sigma_Z(X) = X.$$

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

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

This is the hardest and the most intricate case.

If $X = Z$, we put $\sigma_Z(X) = 1_n$. Suppose $X \neq Z$, and let $X = M(i : (\mathbf{d}, p, \mathbf{0}))$ and $Z = M(i : (\mathbf{e}, p, \mathbf{0}))$ for $\mathbf{d}, \mathbf{e} \in (R_p)^{i-1}$ with $\mathbf{d} - \mathbf{e} \neq 0$. Let the i-principal sub-matrix of Y is of the form $= \begin{bmatrix} Y' & 0 \\ \mathbf{y} & v \end{bmatrix} \in \mathbb{R})^{\times}$ with $Y' \in \mathrm{M}(i-1,R)$, $\mathbf{y} \in R^{i-1}$ and $v \in R$. Then, the i-principal sub-matrix of ZY is of the form $\begin{bmatrix} Y' & 0 \\ \mathbf{e}Y' + p\mathbf{y} & pv \end{bmatrix} \in \mathbb{R})^{\times}$ with $Y' \in \mathrm{M}(i-1,R)$, $\mathbf{y} \in R^{i-1}$ and $v \in R$. Then the criterion in **5.** says that

$$\begin{aligned} X|_lZY \quad &\Leftrightarrow \quad p|pv \quad \text{and} \quad \mathbf{e}Y' + p\mathbf{y} \equiv \mathbf{d}Y' \bmod p \\ &\Leftrightarrow \quad (\mathbf{e} - \mathbf{d})Y' \equiv 0 \bmod p \end{aligned}$$

Let us give one particular solution W of a p-irreducible element, satisfying $X|_lZW$. Namely, put $v = 1$ and $\mathbf{y} = 0$. By the assumption, there is some $1 \leq k < i$ such that $e_k - d_k \not\equiv 0 \bmod p$. Let k be the largest such k. 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 follows. For $1 \le l < k$, we solve the following equation

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

on f_l. This is solvable since $e_k - d_k$ is prime to p in R. Clearly, if we substitute Y by W, then Y' is a $(i-1, i-1)$ matrix of the form $M(k : (\mathbf{f}, p, \mathbf{0}))$ with $\mathbf{0} \in R^{i-1-k}$ and satisfies the equation $(\mathbf{e}-\mathbf{d})M(k : (\mathbf{f}, p, \mathbf{0})) \equiv 0 \bmod p$. Thus, we have $X|_l ZW$. Therefore, any Y with $W|_l Y$ satisfies $X|_l ZW|_l ZY$.

On the other hand, let us consider any upper triangle matrix Y satisfying $X|_l ZY$. We want to show $W|_l Y$, where, according to **5.**, $W|_l Y$ if and only if

$$p \mid v'' \qquad \text{and} \qquad \mathbf{y}'' \equiv \mathbf{f}Y'' \bmod p,$$

where the k-principal sub-matrix of Y is of the form $\begin{bmatrix} Y'' & 0 \\ \mathbf{y}'' & v'' \end{bmatrix} \in \mathrm{M}(k, R)^\times$. Since $e_m - d_m \equiv 0 \bmod p$ for m with $k < m < i-1$, the condition $X|_l ZY$ on Y, i.e. $(\mathbf{e}-\mathbf{d})Y' \equiv 0 \bmod p$ on Y can be rewritten as $(\mathbf{e}''-\mathbf{d}'')\begin{bmatrix} Y'' & 0 \\ \mathbf{y}'' & v'' \end{bmatrix} \equiv 0 \bmod p$, where $(\mathbf{e}''-\mathbf{d}'')$ is the low 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 $X|_l ZY$ on Y can be further rewritten as $(e_k - d_k)(-\mathbf{f}, 1)\begin{bmatrix} Y'' & 0 \\ \mathbf{y}'' & v'' \end{bmatrix} \equiv 0 \bmod p$. 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 $\mathbf{y}'' \equiv \mathbf{f}Y'' \bmod p$. That is, the condition $X|_l ZY$ implies the condition $W|_l Y$ (in fact, they are equivalent). Then, we may put

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

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

Remark. We have shown that if X and Z are p-irreducible elements of the same level i, then $\sigma_Z(X)$ is also a p-irreducible element whose level $k := \max\{1 \le k \le n \mid d_k - e_k \not\equiv 0 \bmod p\}$ is *strictly smaller* than the level i of X and Z. We shall call this phenomenon the **bridging of levels** of p-irreducible elements.

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

Let $X = M(i : (\mathbf{d}, p, \mathbf{0}))$ and $Z = M(i : (\mathbf{e}, q, \mathbf{0}))$ for $\mathbf{d} \in (R_p)^{i-1}$ and $\mathbf{e} \in (R_q)^{i-1}$. Let the i-principal sub-matrix of Y is of the form $\begin{bmatrix} Y' & 0 \\ \mathbf{y} & v \end{bmatrix} \in \mathbb{R})^\times$ with $Y' \in \mathrm{M}(i-1, R)$, $\mathbf{y} \in R^{i-1}$ and $v \in R$. Then, the i-principal sub-matrix of ZY is of the form $= \begin{bmatrix} Y' & 0 \\ \mathbf{e}Y' + q\mathbf{y} & qv \end{bmatrix} \in \mathbb{R})^\times$ with $Y' \in \mathrm{M}(i-1, R)$, $\mathbf{y} \in R^{i-1}$ and $v \in R$. Then the criterion in **5.** says that

$$\begin{array}{lll} X|_l ZY & \Leftrightarrow & p|qv \quad \text{and} \quad \mathbf{e}Y' + q\mathbf{y} \equiv \mathbf{d}Y' \bmod p \\ & \Leftrightarrow & p|v \quad \text{and} \quad (\mathbf{e}-\mathbf{d})Y' + q\mathbf{y} \equiv 0 \bmod p \end{array}$$

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

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

$$p \mid v \qquad \text{and} \qquad \mathbf{y} \equiv \mathbf{f}Y' \mod p,$$

where the first condition $p|v$ is already satisfied. Furthermore, substituting the relation $\mathbf{e} - \mathbf{d} = -q\mathbf{f}$ in the condition $X|_l ZY$, we obtain $-q\mathbf{f}Y' + q\mathbf{y} \equiv 0 \mod p$. Since q is prime to p, we can divide this equality by q, and we obtain the condition for $W|_l Y$. That is, the condition $X|_l ZY$ implies the condition $W|_l Y$ (in fact, they are equivalent). Then, we may put

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

This complete 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 $Z = M(j : (\mathbf{e}, q, \mathbf{0}))$ 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 $Y \in \mathrm{M}(n, R)^\times$ be any lower triangular matrix, whose i-principal sub-matrix is of the form $\begin{bmatrix} Y' & 0 \\ \mathbf{y} & v \end{bmatrix} \in \mathbb{R})^\times$ with $Y' \in \mathrm{M}(i-1, R)$, $\mathbf{y} \in R^{i-1}$ and $v \in R$. Then, the i-principal sub-matrix of ZY is of the form $\left(I_i + \begin{bmatrix} \mathbf{0} \\ (\mathbf{e}, q-1, \mathbf{0}) \\ \mathbf{0} \end{bmatrix} \right) \begin{bmatrix} Y' & 0 \\ \mathbf{y} & v \end{bmatrix} = (Y + \begin{bmatrix} \mathbf{0} \\ (\mathbf{e}, q-1, \mathbf{0})Y \\ \mathbf{0} \end{bmatrix})$, 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 ZY is equal to that of Y and is $(\mathbf{y}, v, \mathbf{0})$.

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

$$X|_l ZY \qquad \Leftrightarrow \qquad p|v \quad \text{and} \quad \mathbf{y} \equiv (\mathbf{d} + d_j(\mathbf{e}, q-1, \mathbf{0}))Y' \bmod p$$

Reversing the criterion **5.**, the last condition is equivalent to that Y 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 normalized because of the term $d_j(\mathbf{e}, \mathbf{0})$),

Thus, by normalizing W, we put

$$\sigma_Z(X) := [W] = [M(i : (\mathbf{d} + d_j(\mathbf{e}, q-1, \mathbf{0}), p, \mathbf{0}))].$$

This completes the proof of the case $i > j$ and that of Theorem 3. □

Combining **6. i)-iv)** of proof with irreducible decompositions of normal forms in **Appendix**, we can determine $\sigma_Z(X)$ algorithmically. The following criterion on divisibility by irreducible elements is a consequence of Theorem 3.

Corollary 4. *An element $Z \in \mathrm{M}(n, R)^\times$ is left-divisible by (an equivalence class of) an irreducible element X if and only if $\sigma_Z(X) = 1_n$.*

Proof. This follows from the equivalence: $X|_l Z \Leftrightarrow \sigma_Z(X)|_l 1_n \Leftrightarrow \sigma_Z(X) = 1_n$. □

Remark. Using above Corollary, we rewrite Theorem 3 into following Theorem 3', which may make it evident that an irreducible element in $\mathrm{M}(n, R)^\times$ is a non-commutative analogue, in a suitable sense, of a prime element.

Theorem 3'. *Let X be a p-irreducible element in $\mathrm{M}(n,R)^\times$. Then for any two elements $Z, Y \in \mathrm{M}(n,R)^\times$, the following 1) and 2) are equivalent:*

1) ZY is divisible by X from the left, 2) either Z is divisible by X from the left, or Y is divisible by a p-irreducible element $\sigma_Z(X)$ from the left.

5. Least common multiples

Definition. An element $Z \in \mathrm{M}(n,R)^\times$ is called a *least common multiple* of $J \subset \mathrm{M}(n,R)^\times$, 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 $Z \,|_l\, Z'$. Any element left equivalent to Z is again a least common multiple of J. Thus least common multiples of J form a left equivalence class (if it exists), whose normal form, denoted by $\mathrm{LCM}(J)$, is called *the least common multiple* of J.

A consequence of the division theory in the previous section is the following.

Theorem 5. *Any finite set J of irreducible elements of $\mathrm{M}(n,R)^\times$ admits the least common multiple $\mathrm{LCM}(J)$.*

Proof. In the following, we give two different Proofs 1 and 2 of Theorem 5.

Proof 1. We apply recursively Theorem 3 on the cardinality of J, where the case $\#J = 1$ is trivial. 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 $\mathrm{LCM}(J')\sigma_{\mathrm{LCM}(J')}(X)$. □

We give an alternative Proof 2 of Theorem 5, which give some insights on least common multiples, and which we shall use in a later application in §6.

Proof 2. This proof is divided in two parts.

Part 1. We consider least common multiples for a pair of elements in $\mathrm{M}(n,R)^\times$ whose normal forms have relatively prime diagonals.

Lemma 6. *Let $X, Y \in M(n,R)^\times$ with $\mathrm{diag}([X]) = (l_1, \cdots, l_n)$ and $\mathrm{diag}([Y]) = (m_1, \cdots, m_n)$. Assume that l_i and m_i are relatively prime in R for $i = 1, \cdots, n$. Then, there exists the least common multiple $\mathrm{LCM}(X,Y) \in M_n$ such that $\mathrm{diag}(\mathrm{LCM}(X,Y)) = (l_1 m_1, \cdots, l_n m_n)$. In particular, $\det(X)\det(Y) = \det(\mathrm{LCM}(X,Y))$.*

Proof. We perform an induction on $n \in \mathbb{Z}_{\geq 1}$. The case $n = 1$ is trivial. Assume $n \geq 2$. We may assume that X and Y are in M_n: $X = \begin{bmatrix} X' & 0 \\ \mathbf{x} & l_n \end{bmatrix}$ and $Y = \begin{bmatrix} Y' & 0 \\ \mathbf{y} & m_n \end{bmatrix}$ for $X', Y' \in M_{n-1}$, $\mathbf{x}, \mathbf{y} \in R^{n-1}$ and $l_n, m_n \in R$. By our induction hypothesis, we have the least common multiple $Z' \in M_{n-1}$ of X' and Y'. Let us consider a matrix $Z = \begin{bmatrix} Z' & 0 \\ \mathbf{z} & l_n m_n \end{bmatrix}$ for some $\mathbf{z} \in (R_{l_n m_n})^{n-1}$. Then, we calculate as $X^{-1}Z = \begin{bmatrix} X'^{-1} & 0 \\ -l_n^{-1}\mathbf{x}X'^{-1} & l_n^{-1} \end{bmatrix} \begin{bmatrix} Z' & 0 \\ \mathbf{z} & l_n m_n \end{bmatrix} = \begin{bmatrix} X'^{-1}Z' & 0 \\ l_n^{-1}(\mathbf{z} - \mathbf{x}X'^{-1}Z') & m_n \end{bmatrix}$, where $X'^{-1}Z' \in M(n-1,R)^\times$ by the assumption on Z'. Thus, we have $X|_l Z \Leftrightarrow \mathbf{z} \equiv \mathbf{x}X'^{-1}Z' \bmod l_n$. Similarly, we have $Y|_l Z \Leftrightarrow \mathbf{z} \equiv \mathbf{y}Y'^{-1}Z' \bmod m_n$. Since l_n and m_n are relatively prime in R, we have the unique solution $\mathbf{z} \in (R_{l_n m_n})^{n-1}$ to these two constraints.

Let us show that the Z which we just constructed is the least common multiple of X and Y. Suppose $\overline{Z} \in M_n$ is a common multiple of X and Y. Then, by induction

hypothesis, $\overline{Z}$ up to a unit factor from the right has the form $\overline{Z}=\begin{bmatrix} Z'U' & 0 \\ \overline{\mathbf{z}} & l_n m_n v \end{bmatrix}$ for some $U'\in M(n-1,R)^\times$, $\overline{\mathbf{z}}\in (R_{l_n m_n v})^{n-1}$ and $v\in R$. The left-divisibility by X and Y of $\overline{Z}$, as in the previous paragraph, imply $\overline{\mathbf{z}}\equiv \mathbf{x}X'^{-1}Z'U' \bmod l_n$ and $\overline{\mathbf{z}}\equiv \mathbf{y}Y'^{-1}Z'U' \bmod m_n$. On the other hand, in the construction of Z, we already have some $\mathbf{z}\in R^{n-1}$ satisfying $\mathbf{z}\equiv \mathbf{x}X'^{-1}Z' \bmod l_n$ and $\mathbf{z}\equiv \mathbf{y}Y'^{-1}Z' \bmod m_n$. So, we also have $\mathbf{z}U'\equiv \mathbf{x}X'^{-1}Z'U' \bmod l_n$ and $\mathbf{z}U'\equiv \mathbf{y}Y'^{-1}Z'U' \bmod m_n$. Consequently, we have $\overline{\mathbf{z}}\equiv \mathbf{z}U' \bmod l_n$ and $\overline{\mathbf{z}}\equiv \mathbf{z}U' \bmod m_n$. Then, by the assumption that l_n and m_n are relatively prime, we finally get $\overline{\mathbf{z}}\equiv \mathbf{z}U' \bmod l_n m_n$.

On the other hand, since $Z^{-1}\overline{Z} = \begin{bmatrix} Z'^{-1} & 0 \\ -(l_n m_n)^{-1}\mathbf{z}Z'^{-1} & (l_n m_n)^{-1} \end{bmatrix}\begin{bmatrix} Z'U' & 0 \\ \overline{\mathbf{z}} & l_n m_n v \end{bmatrix}$ $= \begin{bmatrix} U' & 0 \\ (l_n m_n)^{-1}(\overline{\mathbf{z}}-\mathbf{z}U') & v \end{bmatrix}$, we see that the divisibility condition $Z|_l Z' \Leftrightarrow \overline{\mathbf{z}}\equiv \mathbf{z}U' \bmod l_n m_n$ is already shown in the above calculation. That is, Z is the minimal element among all common multiples of X and Y.

This completes the proof of Lemma 6. □

Part II. Next, we consider least common multiples of a set of p-irreducible elements for a fixed irreducible $p\in R$. In this case, as we shall see below, the data of levels of the input J alone cannot determine the diagonals of $\mathrm{LCM}(J)$. Such jumping (down) of the levels shall be called *bridging*, which plays a role when we calculate skew-growth function of the monoid $\mathrm{M}(n,R)^\times$ in the next section.

Lemma 7. *Let $X=M(n,\mathbf{x})$ and $Y=M(n,\mathbf{y})$ be two p-irreducible normal forms of level n. Set $k:=\max\{k \mid k\text{th entry of } \mathbf{x}-\mathbf{y} \text{ is not equal to zero}\}$. Then*

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

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

$$\begin{array}{ll} u_i\equiv (x_i-y_i)/(x_k-y_k) \mod p \text{ for } 1\le i<k, & u_k=p,\ u_i=0 \text{ for } k<i\le n \\ v_i\equiv (x_i y_k - y_i x_k)/(x_k-y_k) \mod p \text{ for } 1\le i<k, & v_k=0,\ v_i=x_i=y_i \text{ for } k<i\le n. \end{array}$$

Here we use the bijection $R/(p)\simeq R_p$ for the reason given in the following **5***).*

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

We refer to the descend of the level $n\to k$ the *bridging of levels.*

Corollary. *Any finite set of p-irreducible elements has the least common multiple.*

Proof. Let $J=J'\sqcup J_n$ where J' consists of p-primes of level $<n$ and J_n consists of p-primes of level n. We perform the proof by induction on n and $\#(J_n)$, where the case $n=1$ is trivial. Suppose $n>1$ and $J_n\neq\emptyset$.

Case 1: J_n consists of a single element, say X. By induction hypothesis, there exists $\mathrm{LCM}(J')$ such that the pair X and $Y:=\mathrm{LCM}(J')$ satisfies the condition of Lemma 6 so that $\mathrm{LCM}(J)=\mathrm{LCM}(X,\mathrm{LCM}(J'))$ exists.

Case 2: $J_n=J"\sqcup\{X,Y\}$ for distinct p-irreducibles X,Y of level n. According to Lemma 7, $\mathrm{LCM}(X,Y)$ decomposes into a product of mutually commuting p-irreducibles of level k and n with $k<n$. Then, put $\tilde{J}=J'\cup J"\cup\{M(k,\mathbf{u}),M(n,\mathbf{v})\}$ so that 1) new $\tilde{J}$ satisfies the induction hypothesis, 2) $\mathrm{LCM}(J)=\mathrm{LCM}(\tilde{J})$. □

We characterize elements which are least common multiples of some p-irreducibles.

Lemma 8. *The following conditions i) - v) on $X \in M_n$ are equivalent.*
i) There exists a set 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 $1 \le j < i$ is equal to 0. If jth diagonal entry of X is equal to p, then the (i,j)-entry of X for all $j < i \le n$ is equal to 0.
iv) Let $\mathbf{x}_i$ be the ith row-vectors of X $(1 \le i \le n)$, and set $J(X) := \{M(i, \mathbf{x}_i)\}_{i=1}^n$. Then, 1) $J(X)$ consists of mutually commutative p-irreducibles and possibly 1_n,
2) $X = \mathrm{LCM}(J(X)) = \prod_{i \in \{1,\cdots,n\}} M(i, \mathbf{x}_i)$.
v) X is a product of mutually commutative p-irreducible normal forms.

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

ii) $\Rightarrow$ iii). 1) follows since $p \cdot \mathrm{LCM}(J)^{-1}$ is integral. The first half of 2) follows from the fact $R_1 = \{0\}$. The latter half follows by induction on $i - j$ from the fact that $p \cdot \mathrm{LCM}(J)^{-1}$ is integral (details are left to the reader).

iii) $\Rightarrow$ iv). Since the diagonals of X are either 1or 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 $\mathrm{LCM}(J(X)) \big|_l \prod_{i=1}^n M(i, \mathbf{x}_i)$. 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 ps in the diagonal of X. Thus, the equalities are shown.

iv) $\Rightarrow$ v). Clear. v) $\Rightarrow$ i). Clear. □

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

Example. 1. A matrix like $\begin{bmatrix} p & 0 \\ 1 & p \end{bmatrix}$, which violate the condition iii), cannot be a least common multiple of some irreducible elements.
2. If $A := \begin{bmatrix} p & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, B := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ i & k & p \end{bmatrix}, C := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ j & k & p \end{bmatrix}$ for $i \neq j, k \in R_p$, then $\mathrm{LCM}(B, C) = \begin{bmatrix} p & 0 & 0 \\ 0 & 1 & 0 \\ 0 & k & p \end{bmatrix}$ is divisible by A. Then we have: $\mathrm{LCM}(A, B) = \mathrm{LCM}(B, C) = \mathrm{LCM}(C, A) = \mathrm{LCM}(A, B, C)$.

Finally, we give a useful criterion to be divisible by a p-irreducible element.

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

Proof. The "only if" part is trivial. Suppose the converse, i.e. there exists $Z' \in \mathrm{M}(n, R/(p))$ such that $(Y \bmod p) = (X \bmod p)Z'$. Let $Z \in \mathrm{M}(n, R)$ be any lifting of Z'. Then, there exists $W \in \mathrm{M}(n, R)$ such that $XZ = Y + pW$. Using Step 1., we get the expression $X(Z - \varepsilon^{-1} X^* W) = Y$. Since $\det(Y) \neq 0$, we get $\det(Z - \varepsilon^{-1} X^* W) \neq 0$, and hence $X \mid_l Y$ in $M(n, R)^\times$. □

6. Growth function and skew-growth function

As an application of the division theory on the monoid $\mathrm{M}(n,R)^{\times}$ developed in §2 - 5, we determine its growth function and skew-growth function (c.f. [S3]). For this purpose, we first recall a discrete degree map. A map:

$$\deg : M(n,R)^{\times} \longrightarrow \mathbb{R}_{\geq 0}$$

is called a *discrete degree map* if it satisfies

i) $\deg(X) = 0$ if and only if $X \in \mathrm{GL}(n,R)$,
ii) $\deg(XY) = \deg(X) + \deg(Y)$ for all $X, Y \in M(n,R)^{\times}$,
iii) $\#(\{X \in M_n \mid \deg(X) \leq r\}) < \infty$ for all $r \in \mathbb{R}_{>0}$.

For a given discrete degree map, the growth function $P_{M(n,R)^{\times},\deg}(t)$ and the skew growth function $N_{M(n,r)^{\times},\deg}(t)$ are defined as formal Dirichlet series: [5]

$$\begin{aligned} P_{M(n,R)^{\times},\deg}(t) &:= \textstyle\sum_{[X]\in M(n,R)^{\times}/\mathrm{GL}(n,R)} t^{\deg([X])}, \\ N_{M(n,R)^{\times},\deg}(t) &:= \textstyle\sum_{J:\text{ finite subset of } I_0} (-1)^{\#J} \sum t^{\deg(\mathrm{LCM}(J))}, \end{aligned}$$

where $I_0 := \sqcup_{p:\text{primes of } R} I_{0,p}$ is the set of all right equivalence classes of irreducible elements of $\mathrm{M}(n,R)^{\times}$. As formal series, they satisfy the inversion formula ([S3,§5])

$$P_{M(n,R)^{\times},\deg}(t)\ N_{M(n,R)^{\times},\deg}(t) = 1.$$

If $\#(R/mR) < \infty$ for all $m \in R \setminus \{0\}$ and $\#(\{(m) \subset R \mid \#R/(m) \leq r\}) < \infty$ for all $r \in \mathbb{R}_{>0}$, [6] then we can define a discrete degree map deg on $M(n,R)^{\times}$ from the absolute norm $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 1}, m \mapsto \#(R/mR)$ by the composition:

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

where log is the logarithmic function taking the branch: $\mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 0}$.

Formulae. Let R be as above. 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 plane and are given as analytic functions as follows.

1) $P_{M(n,R)^{\times},\deg}(\exp(-s)) = \zeta_R(s)\ \zeta_R(s-1)\ \cdots\ \zeta_R(s-n+1)$

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

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

This can be regarded 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) (K.L. Siegel [Si] and M. Koecher [K]), and then the formula **1)** follows. We give here an elementary proof of **1)** using the normal forms M_n of $M(n,r)^{\times}/\sim$ studied in §3.

[5] The original definition of the skew-growth function [S3, §4] using towers of common multiple sets is much complicated than the present one. Due to the existence of the minimal common multiples for the monoid $\mathrm{M}(n,R)^{\times}$ (§5 Theorem 5), we employ the present simple formulation.

[6] 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.

Let $X \in M_n$ be a normal form (§3) with $\mathrm{diag}(X) = (m_1, \cdots, m_n)$. Then

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

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

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

Recalling the fact $M \simeq (R\setminus\{0\})/\mathcal{E}$ so that $\sum_{m\in M} N(m)^{\log(t)} = \zeta_R(-\log(t))$, and the fact $\#(R_m) = N(m)$, we obtain the formula 1).

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

The first proof is to rewrite the formula 1) by the Euler product formula of the Dedekind zeta-function, and, then, we apply the inversion formula.

The second proof, which we present below, is a direct elementary proof using the structure of common multiples in $M(n,R)^\times$ studied in §5.

We, first, describe a partial Euler product expansion of skew-growth functions.

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

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

Then the skew growth function decomposes as

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

Proof. Lemma 1 and Lemma 6 imply the addition formula **3)**. Then the partial factorization **4)** is an immediate consequence of **3)**. □

It remains to show a decomposition

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

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

Set $I_{0,p} = \sqcup_{i=1}^n I_{0,p}^{(i)}$ 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 $J \subset I_0$. We decompose the summation index set of **5)** as $2^{I_{0,p}} = A \sqcup B$, where $A := \{J \subset I_{0,p} \mid \#(J^{(i)}) \le 1\ (1 \le \forall i \le n)\}$ and $B := 2^{I_{0,p}} \setminus A$. Then the proof of the formula **5)** is achieved if we show the following two formulae.

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

7) $$\textstyle\sum_{J\in B} (-1)^{\#(J)}\ t^{\deg(\mathrm{LCM}(J))} = 0.$$

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′) $$\deg\big(\mathrm{LCM}(J)\big) = \deg\big(p^{\#(J)}\big) = \log(N(p)^{\#(J)}).$$

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

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

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 $\sigma : B \to B$ satisfying the conditions:

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

$$2\sum_{J\in B}(-1)^{\#(J)}t^{\deg(\mathrm{LCM}(J))}=\sum_{J\in B}\big((-1)^{\#(J)}t^{\deg(\mathrm{LCM}(J))}+(-1)^{\#(\sigma(J))}t^{\deg(\mathrm{LCM}(\sigma(J)))}\big)=0.$$

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

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

It is clear that σ defines an involution of B and satisfies the properties i) and ii).

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

7. **Appendix (irreducible decomposition)**

We show the following irreducible decomposition of elements in M_n.

Lemma 10. *Let X be a normal form in M_n with $\mathrm{diag}(X) = (m_1, \cdots, m_n)$. Let us fix an ordered irreducible decomposition $m_i = \prod_{k=1}^{k_i} p_{i,k}$ for each m_i $(i = 1, \cdots, n)$. Then, there exist a unique system $\cup_{i=1}^{n} \cup_{k=1}^{k_i} \{P_{i,k}\}$ where $P_{i,k}$ is a $p_{i,k}$-irreducible normal form of level i such that $X = \prod_{i=1}^{n} \prod_{k=1}^{k_i} P_{i,k}$ where the product order is the lexicographic order order of the running index i and k.*

Proof. Let $\mathbf{x_i}$ $(1 \leq i \leq n)$ be the ith row vector of X, i.e. $X = {}^t\big[{}^t\mathbf{x_1}, {}^t\mathbf{x_2}, \cdots, {}^t\mathbf{x_n}\big]$. Then, X decomposes into a product of pure normal forms of level 1 to n.

$$(*) \qquad M(1 : \mathbf{x_1}) \cdot M(2 : \mathbf{x_2}) \cdots M(n : \mathbf{x_n}).$$

In order to show the decomposition $M(i, \mathbf{x_i}) = \prod_k P_{i,k}$, we prepare a lemma.

Lemma 11. *For a positive integer $1 \leq i \leq n$ and $w \in M$, we set*
$M_n(i; w) := \{$ *all normal forms pure of level i with the diagonal w*$\}$.
1) For any $u, v \in M$ and $1 \leq i \leq n$, the natural product of matrices:
$M_n(i; u) \times M_n(i; v) \to M_n(i; uv)$ *induces a bijection.*
2) For any $u, v \in M$ and $1 \leq i < j \leq n$, the natural product of matrices:
$M_n(i; u) \times M_n(j; v) \to M_n$ *is commutative.*

Proof. Let $M(i : \mathbf{x}) \in M_n(i; u)$ and $M(i : \mathbf{y}) \in M_n(i; v)$ for row vectors $\mathbf{x} = (x_1, \cdots, x_{i-1}, u, \mathbf{0})$ and $\mathbf{y} = (y_1, \cdots, y_{i-1}, v, \mathbf{0})$. Then, their product $M(i:\mathbf{x})M(i:\mathbf{y})$ has the form $M(i:\mathbf{z})$ for $\mathbf{z} = (z_1, \cdots, z_{i-1}, uv, \mathbf{0})$ such that $z_j = uy_j + x_j$ $(1 \leq j < i \leq n)$. Since $0 \leq x_j < u$ and $0 \leq y_j < v$, we have $0 \leq z_j \leq uv$ so that the product is a pure normal form of the diagonal entry uv and of level i. More precisely, the correspondence $(x_j, y_j) \in (\mathbb{Z} \cap [0, u[) \times (\mathbb{Z} \cap [0, v[) \mapsto z_j \in \mathbb{Z} \cap [0, uv[$ is a bijection. □

Applying Lemma 11 $(k-1)$-times repeatedly, we obtain a bijection

$$(**) \qquad M_n(i;p_1) \times M_n(i;p_2) \times \cdots \times M_n(i;p_k) \longrightarrow \quad M_n(i;p_1p_2\cdots p_k).$$

The uniqueness of the decomposition in Lemma 10 is a consequence of the uniqueness of the decomposition $(*)$ and the bijectivity of $(**)$.

This completes a proof of Lemma 10. □

Remark. The product decomposition in Lemma 10 is not commutative, in the sense that the natural transposition $M_n(i;u) \times M_n(i;v) \simeq M_n(i;v) \times M_n(i;u)$ may not commute with the matrix product maps to $M_n(i;uv) = M_n(i;vu)$. That is, in Lemma 10, if we change the order of the irreducible decomposition of m_i, or if we mix up the levels of irreducible normal forms, we obtain different irreducible decompositions (in the latter case, with a possible $\mathrm{GL}(n,R)$ factor from right).

Here are some examples of different irreducible normal forms decomposition.

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

We remark further that *if X is a normal form which is not of pure level, then, associated to the decompositions $m_i = u_iv_i$ $(1 \le i \le n)$ of its diagonal* $\mathrm{diag}(X) = (m_1,\cdots,m_n)$*, the decomposition $X \sim U\cdot V$ by normal forms U and V with* $\mathrm{diag}(U) = (u_1,\cdots,u_n)$ *and* $\mathrm{diag}(V) = (v_1,\cdots,v_n)$ *may either exist non-uniquely or not exist at all* (that is, an analogy of the bijection in Lemma 11 does not hold). Here we have an example of multiple solutions: $\begin{bmatrix}2a&0\\2c&2b\end{bmatrix} = \begin{bmatrix}a&0\\0&2\end{bmatrix}\begin{bmatrix}2&0\\c&b\end{bmatrix} = \begin{bmatrix}a&0\\1&2\end{bmatrix}\begin{bmatrix}2&0\\c-1&b\end{bmatrix}$.

However, if we replace $2c$ in the $(2,1)$-entry of the matrix in LHS by an odd number, then there does not exists its decomposition into a product (up to a unit factor from right) of two normal forms whose diagonals are $(a,2)$ and $(2,b)$.

References

[B-S] Brieskorn, Egbert & Saito, Kyoji: Artin-Gruppen und Coxeter-Gruppen, *Inventiones 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..

[K] Koecher, Max: Über Dirichlet-Reihen mit Funktionalgleichung. Jour. für Mathem. **192** (195*), 1-23.

[S1] Saito, Kyoji: Limit elements in the Configuration Algebra for a Cancellative Monoid, Publ. RIMS Kyoto Univ. **46** (2010), 37-113. DOI 10.2977/PRIMS/2

[S2] Saito, Kyoji: Growth partition functions for cancellative infinite monoids, preprint RIMS-1705 (2010).

[S3] Saito, Kyoji: Inversion formula for the growth function of a cancellative monoid, arXive:1201.5496

[Si] Siegel, Carl Ludwig: Über die Zetafunktionen indefiniter quadratischer Formen. I., II., Math. Zeitshrift **43** (1938), 682-708, and **44** (1939), 398-426.

Iinstitute for Physics and Mathematics of Universe,
University of Tokyo, Kashiwa, Chiba, 277-8568 JAPAN
e-mail address : kyoji.saito@ipmu.ac.jp