

A p-adic phenomenon related to certain integer matrices, and p-adic values of a multidimensional continued fraction

Jun-ichi TAMURA

3-3-7-307 AZAMINO AOBA-KU YOKOHAMA 225-0011 JAPAN

ABSTRACT: All the components of the first row of the hermitian canonical form of the n-th power of the adjugate matrix of the companion matrix of a monic polynomial $f \in \mathbb{Z}[x]$ converge to numbers ($\neq 0$) in the p-adic sense, as n tends to infinity, for some prime numbers p under a minor condition on f, cf. Theorem 1. Using this fact, for any given monic polynomial $f \in \mathbb{Z}[x]$ of degree $s+1$ ($s \geq 1$) satisfying $|f(0)| > 1$, and $\text{GCD}(f(0), f'(0)) = 1$, we can construct a periodic continued fraction of dimension s that converges, with respect to the p-adic topology for all the prime factors p of $f(0)$, to a vector consisting of s numbers belonging to a field $\mathbb{Q}(\lambda_p)$, where $\lambda_p \in \mathbb{Z}_p$ is a root of f, cf. Theorem 2.

§0. Introduction. Throughout the paper, s denotes a fixed positive integer, $|*|_p$ the p-adic absolute value for prime $p < \infty$, $|*|$ the ordinal absolute value $|*|_\infty$. For a given monic polynomial

$$f := x^{s+1} - c_s x^s - \cdots - c_1 x - c_0 \in \mathbb{Z}[x],$$

we mean by C the matrix

$$C = C(f) := \begin{bmatrix} {}^t \underline{0} & c_0 \\ E_s & \underline{c} \end{bmatrix}, \quad \underline{c} = {}^t(c_1, \dots, c_s),$$

where E_s is the $s \times s$ unit matrix, “ t ” indicates the transpose of a matrix. The matrix C, the so called companion matrix of f, which is one of the matrices having f as its characteristic polynomial. Let us suppose

$$d := |c_0| > 1, \quad \text{GCD}(c_0, c_1) = 1. \tag{1}$$

Then, Hensel's lemma (cf., e.g., [1]) tells us that there exists a unique p-adic number $\lambda_p \in \mathbb{Z}_p$ satisfying:

$$f(\lambda_p) = 0, \quad |\lambda_p|_p < 1, \quad p \in \text{Prime}(d),$$

where $\text{Prime}(d)$ denotes the set of the prime factors of d, see any standard text for p-adic numbers, cf., e.g., [1]. In what follows, we assume (1) unless otherwise mentioned.

In Section 1, we give a theorem which disclose a link between the numbers λ_p ($p \in \text{Prime}(d)$) and the hermitian canonical forms of the powers of the adjugate matrix

$$\tilde{C} := (\det C) C^{-1}$$

of the companion matrix C of f , cf. Theorem 1. We give the proof of Theorem 1 in Section 2. In Sections 3-4, we construct a continued fraction of dimension s that converges in $\mathbb{Q}_p$ with respect to the p -adic metric, for any $p \in \text{Prime}(d)$, to a vector consisting of s components belonging to the field $\mathbb{Q}(\lambda_p) \subset \mathbb{Q}_p$, cf. Theorem 2. We give some p -adic results related to a homogeneous form coming from Theorem 1 in connection with a certain partition of the lattice $\mathbb{Z}^s$ in Section 5. In Section 6, we refer to something more about p -adic phenomena taking place around Theorem 1.

Some of the results can be extended to matrices with entries in $\mathbb{Z}_p$ by taking $f \in \mathbb{Z}_p[x] \supset \mathbb{Z}[x]$, but we do not extend them, since we are mainly interested in matrices with integer entries.

§1. Hermitian canonical forms. We denote by $M(s; \mathbb{Q})$ (resp. $M(s; \mathbb{Z})$) the set of $s \times s$ matrices with rational entries (resp. integer entries), and by $M_0(s; \mathbb{Q})$ (resp. $M_0(s; \mathbb{Z})$) the set of matrices $X \in M(s; \mathbb{Q})$ (resp. $X \in M(s; \mathbb{Z})$) such that $\det X \neq 0$. $GL(s; \mathbb{Z})$ is the set of matrices $X \in M(s; \mathbb{Z})$ with $|\det X| = 1$, which are the units of $M(s; \mathbb{Z})$. For two matrices $A, B \in M(s+1; \mathbb{Q})$, we write

$$A \sim B$$

iff there exists a matrix $P \in GL(s+1; \mathbb{Z})$ such that $A = PB$. The relation $\sim$ is an equivalence relation on $M(s+1; \mathbb{Q})$, in particular, so is on $M_0(s+1; \mathbb{Z})$. For a given matrix $X \in M_0(s+1; \mathbb{Z})$, there exists a unique upper triangular matrix $H(X)$ satisfying

$$\begin{aligned} X \sim H(X) &= (h_{ij})_{0 \leq i, j \leq s} \in M_0(s+1; \mathbb{Z}), \\ h_{00} &> 0, \quad 0 \leq h_{ij} < h_{jj} \quad (0 \leq i < j \leq s), \quad h_{ij} = 0 \quad (0 \leq j < i \leq s). \end{aligned}$$

$H(X)$ is the so called hermitian canonical form of X , which can be obtained by elementary transformations, i.e., it can be found by multiplying X by elementary matrices $\in GL(s+1; \mathbb{Z})$ from the left.

We denote by $H_n(X)$ the hermitian canonical form of $\tilde{X}^n$

$$H_n(X) := H(\tilde{X}^n) = H((\det X \cdot X^{-1})^n), \quad X \in M_0(s+1; \mathbb{Z}).$$

Theorem 1. Let $f := x^{s+1} - c_s x^s - \dots - c_1 x - c_0 \in \mathbb{Z}[x]$ be a polynomial satisfying (1), and let $C = C(f)$ be its companion matrix. Let $e(p)$ be numbers determined by

$$d := |c_0| = \prod_{p \in \text{Prime}(d)} p^{e(p)}, \quad e(p) \geq 1 \quad (p \in \text{Prime}(d)),$$

and $\lambda_p \in \mathbb{Z}_p$ the number satisfying

$$f(\lambda_p) = 0, \quad |\lambda_p|_p < 1 \quad (p \in \text{Prime}(d))$$

Then the following statements (i, ii) hold.

(i) The hermitian canonical forms $H_n(C)$ are of the shape

$$H_n(C) = \begin{bmatrix} 1 & {}^t \underline{h}_n \\ \underline{0} & d^n E \end{bmatrix} \in M_0(s+1; \mathbb{Z}), \quad \underline{h}_n = {}^t(h_n^{(1)}, \dots, h_n^{(s)}), \quad 0 \leq h_n^{(j)} < d^n$$

for all $n \geq 1, 1 \leq j \leq s$.

(ii) $|\lambda_p^j - h_n^{(j)}| \leq p^{-e(p)n}$ holds for all $n \geq 1, 1 \leq j \leq s, p \in \text{Prime}(d)$.

We denote by $a_0.a_1a_2\dots(p)$ the p -adic expansion of a number in $\mathbb{Z}_p$ with canonical representatives for the residue field of the valuation:

$$a_0.a_1a_2\dots(p) := \sum_{n \geq 0} a_n p^n, \quad a_n \in \{0, 1, \dots, p-1\}.$$

Remark 1. When $|f(0)| = d = p^e$ (p : prime, $e \geq 1$), then $h_n^{(j)}$ coincides with an integer coming from the truncation of the p -adic expansion of λ_p^j , i.e., $\lambda_p^j = a_0.a_1a_2\dots a_{en-1}\dots(p)$ implies $h_n^{(j)} = a_0.a_1a_2\dots a_{en-1}(p)$, and vice versa. Note that $a_0 = 0$ since $|\lambda_p|_p < 1$. In particular, if $\lambda_p^j \notin \mathbb{Z}_{>0}$, then $a_n \neq 0$ for infinitely many $n \geq 1$, so that in the statement (ii), the equality holds infinitely often. In this sense, the approximation (ii) is best possible.

Remark 2. Since $f \in \mathbb{Z}[x]$ is monic, $\lambda_p \notin \mathbb{Z}$ implies $\lambda_p \notin \mathbb{Q}$, so that the p -adic expansion of $\lambda_p^j \notin \mathbb{Z}$ can not be periodic, and in particular, the expansion diverges with respect to the archimedian norm $|\cdot|_\infty$. Hence, the sequence $\{h_n^{(j)}\}_{n=1,2,\dots}$ is unbounded for all $1 \leq j \leq s$ (with respect to the usual metric) if there exists a prime $p \in \text{Prime}(d)$ such that $\lambda_p \notin \mathbb{Z}$. (Note that the converse is not valid.) In particular, if f has no linear factors in $\mathbb{Z}[x]$, then $\{h_n^{(1)}\}_{n=1,2,\dots}$ is unbounded; if f is irreducible over $\mathbb{Q}[x]$, then $\{h_n^{(j)}\}_{n=1,2,\dots}$ is unbounded for all $1 \leq j \leq s$.

Remark 3. In general, the minimal polynomial f_p in $\mathbb{Z}[x]$ of λ_p depends on

p. If $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}[x]$, and $\#\text{Prime}(d) > 1$ then the assertion (ii) with $j=1$ gives simultaneous diophantine approximations by a rational integer $h_n^{(1)}$ for roots λ_p ($p \in \text{Prime}(d)$) having an identical minimal polynomial.

Remark 4. (cf. the Chinese remainder theorem) Let $f(0)$ be an integer having $s+1$ distinct prime factors, and let

$$f = \prod_{p \in \text{Prime}(f(0))} (x - p^{e(p)}).$$

Then $\text{GCD}(f(0), f'(0)) = 1$, i.e., (1) is valid. In this case, $\lambda_p = p^{e(p)}$ holds, so that for any fixed $n \geq 1$ and $1 \leq j \leq s$, Theorem 1 gives a unique solution

$0 \leq h_n^{(j)} < |f(0)|^n$ independent of p satisfying the system of congruences

$$x_n^{(j)} \equiv p^{e(p)j} \pmod{p^{e(p)n}} \text{ for all } p \in \text{Prime}(f(0)).$$

Remark 5. In general, the assertion (i) does not hold even for the case where f is irreducible over $\mathbb{Q}[x]$ if the condition (1) does not hold. For instance, take an irreducible polynomial $f = x^5 - 13x^4 - 7x^3 + 5x^2 - 3x - 3$ with its companion matrix C . Then the $(2,4)$ -entry of $H_4(C) = 54 \neq 0$, and the $(1,2)$ -entry of $H_n(C)$ is identically zero for $1 \leq n \leq 16$. Consequently, the assertions (i) is not valid.

§2. Proof of Theorem 1. Instead of showing Theorem 1, (i), we prove the following assertion (i)*:

Lemma 1. For $C = C(f)$ satisfying (1),

$$(i)^* \quad H_n(C) = \begin{bmatrix} 1 & {}^t \underline{h}_n \\ \underline{0} & d^n E_s \end{bmatrix} \in M(s+1; \mathbb{Z}), \quad \underline{h}_n = {}^t(h_n^{(1)}, \dots, h_n^{(s)})$$

with $0 \leq h_n^{(j)} < d^n$, $h_n^{(j)} \in d^j \mathbb{Z}$ ($1 \leq j \leq s$) holds for all $n \geq 1$.

It is clear that Lemma 1 implies Theorem 1, (i). Notice that (i) and (ii) in Theorem 1 imply (i)*.

Proof of Lemma 1. (Induction on n .) We have

$$\det C \cdot C^{-1} = (-1)^s \begin{bmatrix} -\underline{c} & c_0 E_s \\ 1 & {}^t \underline{0} \end{bmatrix} \sim \begin{bmatrix} 1 & {}^t \underline{0} \\ \underline{0} & d E_s \end{bmatrix},$$

so that (i)* is valid for $n=1$. Suppose that (i)* holds for an integer $n \geq 1$. Then, we get

$$\begin{aligned}
H_{n+1}(C) &\sim (\det C \cdot C^{-1})^n \det C \cdot C^{-1} \sim H_n(C) \cdot \det C \cdot C^{-1} \\
&= (-1)^s \begin{bmatrix} 1 & {}^T \underline{h}_n \\ \underline{0} & d^n E_s \end{bmatrix} \begin{bmatrix} -\underline{c} & c_0 E_s \\ 1 & {}^T \underline{0} \end{bmatrix} \\
&= (-1)^s \left[\begin{array}{c|c|c} -d_n & c_0 & c_0 h_n^{(1)} \quad c_0 h_n^{(2)} \quad \dots \quad c_0 h_n^{(s-1)} \\ -c_2 d^n & & \\ \vdots & \underline{0} & c_0 d^n E_{s-1} \\ -c_s d^n & & \\ d^n & & {}^T \underline{0} \end{array} \right],
\end{aligned}$$

where

$$d_n := c_1 + c_2 h_n^{(1)} + \dots + c_{s-1} h_n^{(s-1)} - h_n^{(s)}. \quad (2)$$

Hence, we obtain

$$H_{n+1}(C) \sim \left[\begin{array}{c|c|c} d^n & 0 & 0 \quad 0 \quad \dots \quad 0 \\ -d_n & c_0 & c_0 h_n^{(1)} \quad c_0 h_n^{(2)} \quad \dots \quad c_0 h_n^{(s-1)} \\ -c_2 d^n & & \\ \vdots & \underline{0} & c_0 d^n E_{s-1} \\ -c_s d^n & & \end{array} \right]. \quad (3)$$

By the induction hypothesis, we have $h_n^{(j)} \in d^j \mathbb{Z} \subset d\mathbb{Z}$ for all $1 \leq j \leq s$, so that (2) implies $d_n \equiv c_1 \pmod{d}$. Thus, we get $\text{GCD}(d^n, d_n) = 1$ by (1). Therefore, there exist integers u_n, v_n satisfying $d^n u_n - d_n v_n = 1$, which together with (3) implies

$$H_{n+1}(C) \sim \left[\begin{array}{c|c} \begin{bmatrix} u_n & v_n \\ d_n & d^n \end{bmatrix} & \begin{bmatrix} \underline{0} \\ E_{s-1} \end{bmatrix} \end{array} \right] \left[\begin{array}{c|c|c} d^n & 0 & 0 \quad 0 \quad \dots \quad 0 \\ -d_n & c_0 & (d^2) \quad (d^3) \quad \dots \quad (d^s) \\ (d^n) & & \\ \vdots & \underline{0} & c_0 d^n E_{s-1} \\ (d^n) & & \end{array} \right]$$

$$\sim \left[\begin{array}{cc|cccc} 1 & (d) & (d^2) & (d^3) & \cdots & (d^s) \\ 0 & c_0 d^n & (d^{n+1}) & (d^{n+1}) & \cdots & (d^{n+1}) \\ \hline (d^n) & & & & & \\ \vdots & \underline{0} & & & & \\ (d^n) & & c_0 d^n E_{s-2} & & & \end{array} \right],$$

where we mean by (d^m) an integer divisible by d^m . Note that integers indicated by the identical symbols (d^m) are not necessarily the same numbers. Hence, we get

$$H_{n+1}(C) \sim \left[\begin{array}{cc} 1 & {}^T \underline{k}_n \\ \underline{0} & d^{n+1} P \end{array} \right], \quad \underline{k}_n = {}^T (k_n^{(1)}, \dots, k_n^{(s)}), \quad (4)$$

$$k_n^{(j)} \in d^j \mathbb{Z} \quad (1 \leq j \leq s), \quad P \in M(s; \mathbb{Z}). \quad (5)$$

Since

$$|\det(H_{n+1}(C))| = |\det((\det C \cdot C^{-1}))^{n+1}| = d^{s(n+1)},$$

(4) together with (5) yields $P \in GL(s; \mathbb{Z})$, so that we obtain

$$H_{n+1}(C) \sim \left[\begin{array}{cc} 1 & {}^T \underline{k}_n \\ \underline{0} & d^{n+1} E_s \end{array} \right].$$

Thus, noting (5), we get (i)* with $n+1$ in place of n , which completes the proof of (i)*. ■

Theorem 1, (i) follows from Lemma 1 as we have mentioned. We need the following Lemmas 2-4 for the proof of Theorem (ii). We denote by $\underline{e}_j$ ($1 \leq j \leq s$) the j -th fundamental vector $(0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{Z}^s$.

Lemma 2. For $1 \leq j \leq s$

$$d^{-n} H_n(C) \begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix} = \begin{bmatrix} (h_{n+1}^{(j)} - h_n^{(j)})/d^n \\ -\underline{e}_j \end{bmatrix} \in \mathbb{Z}^{s+1}.$$

Proof. The assertion (i) in Theorem 1 implies

$$d^{-n-1}H_{n+1}(C) \begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix} = \begin{bmatrix} 0 \\ -\underline{e}_j \end{bmatrix} \in \mathbb{Z}^{s+1}$$

for all $n \geq 0$, $1 \leq j \leq s-1$, so that

$$C^{-n-1} \begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix} \in \mathbb{Z}^{s+1}$$

follows from $d^{-n-1}H_{n+1}(C) \sim C^{-n-1}$. Hence we get

$$C^{-n} \begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix} \in C(\mathbb{Z}^{s+1}) \subset \mathbb{Z}^{s+1},$$

so that

$$d^{-n}H_n(C) \begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix} = \begin{bmatrix} (h_{n+1}^{(j)} - h_n^{(j)})/d^n \\ -\underline{e}_j \end{bmatrix} \in \mathbb{Z}^{s+1}. \blacksquare$$

Lemma 3.

$$\begin{aligned} \mathbb{Z}^{s+1} \ni d^{-n} \begin{bmatrix} 1 & {}^T \underline{h}_n \\ \underline{0} & d^n E_s \end{bmatrix} \begin{bmatrix} -\underline{c} & c_0 E_s \\ 1 & {}^T \underline{0} \end{bmatrix} \begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix} \\ = d^{-n} \left[\begin{array}{c|c} \begin{matrix} -d_n \\ -c_2 d^n \\ \vdots \\ -c_s d^n \\ d^n \end{matrix} & \begin{matrix} c_0 \\ \underline{0} \end{matrix} \\ \hline \begin{matrix} c_0 h_n^{(1)} & c_0 h_n^{(2)} & \dots & c_0 h_n^{(s-1)} \\ \hline c_0 d^n E_{s-1} \\ \hline {}^T \underline{0} \end{matrix} \end{array} \right] \begin{bmatrix} h_{n+1}^{(j)} \\ -\underline{e}_j \end{bmatrix} \end{aligned}$$

for all $n \geq 1$, $1 \leq j \leq s$, where d_n is the integer (2).

Proof. Noting $d^{-n-1}H_{n+1}(C) {}^T(h_{n+1}^{(j)}, -{}^T \underline{e}_j) \in \mathbb{Z}^{s+1}$, and

$d^{-n-1}H_{n+1}(C) \sim d^{-n}H_n(C)\tilde{C}$, we get $d^{-n}H_n(C)\tilde{C} {}^T(h_{n+1}^{(j)}, -{}^T \underline{e}_j) \in \mathbb{Z}^{s+1}$, which implies

the lemma. ■

Lemma 4. $|\lambda_p - h|_p = |f(h)|_p$ for any $h \in p\mathbb{Z}_p$, $p \in \text{Prime}(f(0))$.

Proof. Since $f = x^{s+1} - c_s x^s - \dots - c_1 x - c_0 \in \mathbb{Z}[x] \subset \mathbb{Z}_p[x]$, $|c_0|_p < 1$, $|c_1|_p = 1$ for $p \in \text{Prime}(f(0))$, since f satisfies (1). Noting $|\lambda_p|_p < 1$, we have $|f'(\lambda_p)|_p = 1$. We can set $f(x + \lambda_p) = \gamma_1 x + \dots + \gamma_{s+1} x^{s+1} \in \mathbb{Z}_p[x]$, so that

$$f(x) = \gamma_1 (x - \lambda_p) + \dots + \gamma_{s+1} (x - \lambda_p)^{s+1}, \quad \gamma_j \in \mathbb{Z}_p \quad (1 \leq j \leq s), \quad \gamma_1 = f'(\lambda_p), \quad |\gamma_1|_p = 1.$$

We put $g(x) = f(x)/(x - \lambda_p)$. Then $g(x) = \gamma_1 + \gamma_2 (x - \lambda_p) + \dots + \gamma_{s+1} (x - \lambda_p)^s$. Hence, for $h \in p\mathbb{Z}_p$, we get

$$|g(h)|_p = |\gamma_1 + \gamma_2 (h - \lambda_p) + \dots + \gamma_{s+1} (h - \lambda_p)^s|_p = |\gamma_1|_p = 1,$$

which implies

$$|h - \lambda_p|_p = |h - \lambda_p|_p \cdot |g(h)|_p = |(h - \lambda_p)g(h)|_p = |f(h)|_p. \quad \blacksquare$$

Proof of Theorem 1, (ii). Lemma 2 yields

$$h_{n+1}^{(j)} \equiv h_n^{(j)} \pmod{d^n}, \quad n \geq 1, \quad 1 \leq j \leq s. \quad (6)$$

By Lemma 3, we obtain

$$d_n h_{n+1}^{(1)} + c_0 \equiv 0 \pmod{d^n}, \quad (7)$$

$$d_n h_{n+1}^{(j)} + c_0 h_n^{(j-1)} \equiv 0 \pmod{d^n}, \quad 2 \leq j \leq s \quad (8)$$

In view of (6)-(8), we have

$$d_n h_n^{(1)} + c_0 \equiv 0 \pmod{d^n}, \quad (9)$$

$$d_n h_n^{(j)} + c_0 h_n^{(j-1)} \equiv 0 \pmod{d^n} \quad (10)$$

for all $n \geq 1$, $2 \leq j \leq s$. The assertion (i) in Theorem 1 implies

$$h_n^{(j)} / |c_0| = h_n^{(j)} / d \in \mathbb{Z}, \quad 1 \leq j \leq s.$$

Therefore, we obtain by (9), (10)

$$d_n h_n^{(1)} h_n^{(j)} / c_0 + h_n^{(j)} \equiv 0 \pmod{d^n}, \quad (11)$$

$$d_n h_n^{(1)} h_n^{(j)} / c_0 + h_n^{(1)} h_n^{(j-1)} \equiv 0 \pmod{d^n}. \quad (12)$$

Comparing (11) with (12), we obtain

$$h_n^{(j)} \equiv h_n^{(1)} h_n^{(j-1)} \pmod{d^n}, \quad 2 \leq j \leq s,$$

namely,

$$h_n^{(j)} \equiv (h_n^{(1)})^j \pmod{d^n}, \quad 2 \leq j \leq s. \quad (13)$$

Combining (13) and (7) with (2), we get

$$(h_n^{(1)})^s - c_{s-1} (h_n^{(1)})^{s-1} - \dots - c_1 h_n^{(1)} - c_0 \equiv 0 \pmod{d^n},$$

i.e.,

$$f(h_n^{(1)}) \equiv 0 \pmod{p^{e(p)}}$$

for all $n \geq 1$, $p \in \text{Prime}(d)$.

Therefore, from Lemma 4, it follows

$$|\lambda_p - h_n^{(1)}| \leq p^{-e(p)n} \quad (n \geq 1, p \in \text{Prime}(d)) \quad (14)$$

holds. In view of (13), (14), we get the assertion (ii). ■

§3. A continued fraction of dimension s . Let K be any field. By $K(\underline{x})$, we denote the field of rational functions, over K , of s variables $\underline{x} := {}^T(x_1, \dots, x_s)$, and by $T(\underline{x})$ the s -tuple of rational functions defined by

$$T(\underline{x}) := {}^T(1/x_s, x_1/x_s, \dots, x_{s-1}/x_s) \in K(\underline{x})^s.$$

We write

$$\frac{x_0^{-1}}{\underline{x}} := x_0^{-1} T(\underline{x}) \in K(x_0, \underline{x})^s = K(\underline{x}), \quad \underline{x} = {}^T(x_0, \dots, x_s).$$

Then, we can consider a continued fraction

$$\begin{aligned} \underline{\Xi}(\underline{x}_0, \dots, \underline{x}_n) &= {}^T(\xi_1(\underline{x}_0, \dots, \underline{x}_n), \dots, \xi_s(\underline{x}_0, \dots, \underline{x}_n)) \\ &:= (x_0^{(0)})^{-1} \underline{x}_0 + \frac{(x_0^{(0)})^{-1}}{(x_1^{(0)})^{-1} \underline{x}_1 + \frac{(x_1^{(0)})^{-1}}{(x_2^{(0)})^{-1} \underline{x}_2 + \dots + \frac{(x_{n-1}^{(0)})^{-1}}{(x_n^{(0)})^{-1} \underline{x}_n}}}} \\ &\in K(\underline{x}_0, \dots, \underline{x}_n)^s, \quad \underline{x}_m = {}^T(x_m^{(1)}, \dots, x_m^{(s)}), \quad \underline{x}_m = {}^T(x_m^{(0)}, \dots, x_m^{(s)}) \quad (0 \leq m \leq n). \end{aligned}$$

If the denominators of ξ_j do not vanish at $\underline{x}_0 = \underline{c}_0, \dots, \underline{x}_n = \underline{c}_n \in K^{s+1}$, then we can consider the value $\underline{\Xi}(\underline{c}_0, \dots, \underline{c}_n) \in K^s$. In such a case, we say that the continued fraction $\underline{\Xi}(\underline{c}_0, \dots, \underline{c}_n)$ is well-defined. Setting $K = \mathbb{Q}_p$, we may consider an infinite continued fraction $\underline{\Xi}(\underline{c}_0, \dots, \underline{c}_n, \dots)$, which is defined to be the limit of its n -th convergent $\underline{\Xi}(\underline{c}_0, \dots, \underline{c}_n)$ with respect the p -adic topology provided that $\underline{\Xi}(\underline{c}_0, \dots, \underline{c}_n)$ is well-defined for all sufficiently large n , and the limit exists. In particular, if $c_m^{(0)} = 1$ for all m , then the continued fraction $\underline{\Xi}(\underline{c}_0, \dots, \underline{c}_n, \dots)$ turns out to be of the form of a "simple continued fraction" of dimension s , which is denoted by

$$[\underline{c}_0; \underline{c}_1, \underline{c}_2, \underline{c}_3, \dots] =$$

$$\begin{bmatrix} C_0^{(1)}; C_1^{(1)}, C_2^{(1)}, C_3^{(1)}, \dots \\ C_0^{(2)}; C_1^{(2)}, C_2^{(2)}, C_3^{(2)}, \dots \\ \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \quad \quad \quad \vdots \\ C_0^{(s)}; C_1^{(s)}, C_2^{(s)}, C_3^{(s)}, \dots \end{bmatrix},$$

$$\underline{C}_n = {}^T(C_n^{(1)}, C_n^{(2)}, \dots, C_n^{(s)}), \quad n \geq 0.$$

If we take $s=1$, then

$$\begin{aligned} & \underline{E}(\underline{C}_0, \dots, \underline{C}_n, \dots) \\ &= (C_0^{(0)})^{-1} C_0^{(1)} + \frac{(C_0^{(0)})^{-1}}{(C_1^{(0)})^{-1} C_1^{(1)} + \frac{(C_1^{(0)})^{-1}}{(C_2^{(0)})^{-1} C_2^{(1)} + \frac{(C_2^{(0)})^{-1}}{(C_3^{(0)})^{-1} C_3^{(1)} + \dots}}}, \end{aligned}$$

and $T(\underline{x})=T(x_1)=1/x_1$ turns out to be the usual reciprocal of x_1 . Hence we have

$$C_0^{(0)} \underline{E}(\underline{C}_0, \dots, \underline{C}_n, \dots) = C_0^{(1)} + \frac{C_1^{(0)}}{C_1^{(1)} + \frac{C_2^{(0)}}{C_2^{(1)} + \frac{C_3^{(0)}}{C_3^{(1)} + \dots}}.$$

Theorem 2. Let $f:=x^{s+1}-c_s x^s-\dots-c_1 x-c_0 \in \mathbb{Z}[x]$, $\lambda_p \in \mathbb{Z}_p$, $e(p)$ ($p \in \text{Prime}(d)$) be as in Theorem 1. Let $\underline{\theta}_n = {}^T(\theta_n^{(1)}, \dots, \theta_n^{(s)}) \in \mathbb{Q}^s (\subset \mathbb{Q}_p^s)$ be the n -th convergent of the following periodic continued fraction:

$$\begin{aligned} & \frac{C_0^{-s}}{-C_0^{-s} \underline{C}_1^* + \frac{C_0^{-s}}{-C_0^{-s} \underline{C}_2^* + \dots + \frac{C_0^{-s}}{-C_0^{-s} \underline{C}_{s-1}^* + \frac{C_0^{-s}}{-C_0^{-s} \underline{C}^* + \dots + \frac{C_0^{-s}}{-C_0^{-s} \underline{C}^* + \dots}}}}, \end{aligned}$$

$$\underline{c}_m^* := {}^T(0, \dots, 0, c_0^{m-1}c_m, c_0^{m-2}c_{m-1}, \dots, c_0c_2, c_1) \in \mathbb{Z}^s \quad (1 \leq m \leq s),$$

$$\underline{c}^* := \underline{c}_s^*.$$
$$J_m := \begin{bmatrix} \tau \underline{0} & C_0^s \\ E_s & -\underline{C}_m^* \end{bmatrix} \quad (0 \leq m \leq s), \quad J_m := J_s \quad (m > s),$$

- 11 -

Remark 6. Lemma 9, (i) given below implies that $r_n^{(0)} \neq 0$ for all $n \geq 0$, so that any convergent θ_n ($n \geq 0$) of the continued fraction given in Theorem 2 is well-defined.

Remark 7. In general, the continued fractions in Theorem 2, and Corollary 1 do not converge in R with respect to the metric coming from $|\ast| = |\ast|_\infty$. These continued fractions always diverge when $f \in \mathbb{Z}[x]$ is of totally imaginary.

§4. Proof of Theorem 2. We need some lemmas for the proof of Theorem 2, and its Corollary.

Let $A \in (a_{ij})_{0 \leq i \leq s, 0 \leq j \leq s} \in M_0(s+1; K)$. Then A defines a linear map on K^{s+1} , which will be also denoted by A . For elements $\underline{v}, \underline{w} \in K^{s+1} \setminus \{\underline{0}\}$, iff there exists $c \in K$ such that $c\underline{v} = \underline{w}$, we write $\underline{v} \sim \underline{w}$, which defines an equivalence relation on $K^{s+1} \setminus \{\underline{0}\}$. We denote by κ the map

$$\begin{aligned} \kappa: K^{s+1} &\longrightarrow P^s(K) := (K^{s+1} \setminus \{\underline{0}\}) / \sim, \\ \kappa(\underline{v}) &:= \{\underline{w} \in K^{s+1} \setminus \{\underline{0}\}; \underline{w} \sim \underline{v}\} \quad (\underline{v} \neq \underline{0}), \end{aligned}$$

where the broken arrow $\longrightarrow$ indicates a "map" with some exceptional elements for which the map is not defined. Since $\kappa(\underline{v}) = \kappa(\underline{w})$ implies $\kappa A\underline{v} = \kappa A\underline{w}$, so that the linear map A induces a map $A_\ast: P^s(K) \dashrightarrow P^s(K)$. We define a projection π , and an injection ι by

$$\begin{aligned} \pi: P^s(K) &\dashrightarrow K^s, \\ \pi(\kappa(\underline{v})) &:= (v_1/v_0, v_2/v_0, \dots, v_s/v_0), \quad \underline{v} = {}^T(v_0, v_1, \dots, v_s) \in K^{s+1}; \\ \iota: K^s &\dashrightarrow P^s(K), \\ \iota(\underline{v}) &:= \kappa(1, v_1, v_2, \dots, v_s), \quad \underline{v} = {}^T(v_1, v_2, \dots, v_s) \in K^s. \end{aligned}$$

We set $A_\# = \pi \circ A_\ast \circ \iota$. Then, Lemma 5 given below can be easily seen.

Lemma 5. The following diagram is commutative:

$$\begin{array}{ccccc} K^{s+1} & \xrightarrow{\kappa} & P^s(K) & \xleftarrow{\pi} \xrightarrow{\quad} & K^s \\ \downarrow A & & \downarrow A_\ast & \downarrow \iota & \downarrow A_\# \\ K^{s+1} & \xrightarrow{\kappa} & P^s(K) & \xleftarrow{\pi} \xrightarrow{\quad} & K^s \end{array}$$

Using Lemma 5, we get the following

Lemma 6. Let X_m be a matrix with $s+1$ variables $\underline{x}_m = {}^T(x_m^{(0)}, \dots, x_m^{(s)})$:

$$X_m := \begin{bmatrix} {}^T 0 & x_m^{(0)} \\ E_s & \underline{x}_m \end{bmatrix}, \quad \underline{x}_m := {}^T(x_m^{(1)}, \dots, x_m^{(s)}), \quad 0 \leq m \leq n.$$

and let $p_i^{(j)}$ be polynomials

$$p_i^{(j)} = p_i^{(j)}(\underline{x}_0, \dots, \underline{x}_n) \in \mathbb{Z}[\underline{x}_0, \dots, \underline{x}_n] \quad (-s-1 \leq i \leq n, \quad 0 \leq j \leq s)$$

defined by $s+1$ recurrences

$$p_m^{(j)} = x_m^{(0)} p_{m-s-1}^{(j)} + x_m^{(1)} p_{m-s}^{(j)} + \dots + x_m^{(s)} p_{m-1}^{(j)} \quad (0 \leq m \leq n, \quad 0 \leq j \leq s)$$

with an initial condition

$$P_{-1} = E_{s+1},$$

where

$$P_m := (p_{m-s+i}^{(j)})_{0 \leq i \leq s, \quad 0 \leq j \leq s} \quad (0 \leq m \leq n).$$

Then the continued fractions $\underline{\Xi}(\underline{x}_0, \dots, \underline{x}_m)$ are written by the following formulae:

- (i) $P_m = X_0 X_1 \cdots X_m \in M(s+1; \mathbb{Z}[\underline{x}_0, \dots, \underline{x}_m]) \quad (0 \leq m \leq n).$
- (ii) $\underline{\Xi}(\underline{x}_0, \dots, \underline{x}_m) = (p_m^{(0)})^{-1} {}^T(p_m^{(1)}, \dots, p_m^{(s)}) \in \mathbb{Q}(\underline{x}_0, \dots, \underline{x}_m)^s \quad (0 \leq m \leq n).$

Proof. The assertion (i) can be easily seen by induction on n . Let

$\underline{\xi} := {}^T(\xi_1, \dots, \xi_s)$ be a vector with s indeterminates. Lemma 5 implies

$$\begin{aligned} (X_m)_\#(\underline{\xi}) &= (\pi \circ (X_m)_* \circ \iota)(\underline{\xi}) = (\pi \circ (X_m)_*)(\kappa({}^T(1, \xi_1, \dots, \xi_s))) \\ &= \pi(\kappa({}^T(x_m^{(0)} \xi_s, 1 + x_m^{(1)} \xi_s, y_1 + x_m^{(2)} \xi_s, \dots, y_{s-1} + x_m^{(s)} \xi_s))) \\ &= (x_m^{(0)})^{-1} \underline{x}_m + (x_m^{(0)})^{-1} (1/\xi_s, \xi_1/\xi_s, \dots, \xi_{s-1}/\xi_s) \\ &= (x_m^{(0)})^{-1} \underline{x}_m + \frac{(x_m^{(0)})^{-1}}{\underline{\xi}}. \end{aligned}$$

Lemma 5 implies $(AB)_\# = A_\# B_\#$ for any $A, B \in M(s+1; K)$ ($K \in \mathbb{Q}(\underline{x}_0, \dots, \underline{x}_m)$), since

$(AB)_* = A_* B_*$. Hence, taking $\underline{\xi} := {}^T(0, \dots, 0, \xi^{-1})$, we get

$$\begin{aligned} \pi((P_m)_*(\kappa({}^T(\xi, 0, \dots, 0, 1)))) &= (P_m)_\#(\underline{\xi}) = ((X_0)_\# \circ (X_1)_\# \circ \dots \circ (X_m)_\#)(\underline{\xi}) \\ &= (x_0^{(0)})^{-1} \underline{x}_0 + \frac{(x_0^{(0)})^{-1}}{(x_1^{(0)})^{-1} \underline{x}_1 + \frac{(x_1^{(0)})^{-1}}{(x_2^{(0)})^{-1} \underline{x}_2 + \dots + \frac{(x_{m-1}^{(0)})^{-1}}{(x_m^{(0)})^{-1} \underline{x}_m + \frac{(x_m^{(0)})^{-1}}{\underline{\xi}}}}}. \end{aligned}$$

which can be considered as an element of $\mathbb{Q}(\underline{x}_0, \dots, \underline{x}_m, \xi)$. Since

$T(\underline{\xi}) = \xi \cdot {}^T(1, 0, \dots, 0)$, we get, by setting $\xi=0$, the following identity

$$\pi(P_m \underline{e}_s) = \pi(\tau(P_m^{(0)}, P_m^{(1)}, \dots, P_m^{(s)})) = \underline{\Xi}(\underline{x}_0, \dots, \underline{x}_m) \in Q(\underline{x}_0, \dots, \underline{x}_m)^s,$$

which is the formula (ii). Since $p_m^{(0)}$ is a polynomial in $Z[\underline{x}_0, \dots, \underline{x}_m]$ which exactly has $x_0^{(0)} x_1^{(0)} \dots x_m^{(0)}$ as one of its terms (i.e., the coefficient equals one), it is not the zero polynomial, so that the s -tuple of rational functions $\underline{\Xi}(\underline{x}_0, \dots, \underline{x}_m) \in Q(\underline{x}_0, \dots, \underline{x}_m, \underline{y})^s$ is well-defined. ■

Remark 8. In general, the formula (ii) holds for $\underline{x}_0, \dots, \underline{x}_m \in L^{s+1}$ for any field L even for the case of $\text{char}(L) \neq 0$ provided that $p_m^{(0)}(\underline{x}_0, \dots, \underline{x}_m)$ differs from 0 as an element of L .

In what follows, we mean by $H_n = H_n(C)$ ($n \geq 0$), and by J_m ($0 \leq m \leq s$) the matrices in Theorem 2. Recall that we are assuming (1).

We put

$$K_n := \begin{bmatrix} d^n & -\tau \underline{h}_n \\ \underline{0} & E_s \end{bmatrix} \quad (n \geq 0), \quad J := J_s = \begin{bmatrix} \tau \underline{0} & c_0^s \\ E_s & -\underline{c}^* \end{bmatrix},$$

$$\underline{c}^* := \tau(c_0^{s-1} c_s, c_0^{s-2} c_{s-1}, \dots, c_0 c_2, c_1),$$

where $\underline{h}_n \in \mathbb{Z}^s$ is the vector in Theorem 1, (i). We define integers $q_n^{(j, i)}$ by

$$Q^n =: (q_n^{(j, i)})_{0 \leq i \leq s, 0 \leq j \leq s} \quad (n \geq 0), \quad (15)$$

where

$$Q := \begin{bmatrix} -\underline{c} & c_0 E_s \\ 1 & \tau \underline{0} \end{bmatrix}.$$

Note that

$$Q = c_0 C^{-1} = (-1)^s \tilde{C}, \quad C = C(f).$$

We mean by $X \equiv Y \pmod{m}$ that all the entries of $X - Y$ are divisible by $m \in \mathbb{Z}$.

Lemma 7. $q_n^{(0, i)} h_n^{(j)} \equiv q_n^{(j, i)} \pmod{d^n}$ for all $0 \leq i \leq s, 1 \leq j \leq s, n \geq 0$.

Proof. Since $c^n C^{-n} = U_n H_n$ ($c := (-1)^s c_0 = \det C, U_n \in GL(s+1; \mathbb{Z})$),

we have

$$c^n H_n^{-1} = C^n U_n. \quad (16)$$

Theorem 1, (i) implies $K_n H_n = d^n E_{s+1}$, i.e., $K_n = d^n H_n^{-1}$, so that

$$K_n F_n = c^n H_n^{-1} (F_n := |c^n|^{-1} c^n E_{s+1} (= \pm E_{s+1})). \quad (17)$$

From (16), (17), it follows $K_n F_n = C^n U_n$, so that $K_n = C^n V_n$ ($V_n = U_n F_n^{-1} \in GL(s+1; \mathbb{Z})$).

Hence we obtain $\tilde{C}^n K_n = \tilde{C}^n C^n V_n = c^n V_n$, which together with $Q = (-1)^s \tilde{C}$ implies

$$Q^n K_n \equiv 0 \pmod{d^n}, \quad n \geq 0,$$

where $0 \in M(s+1; \mathbb{Z})$ is the zero matrix. Considering the (i, j) -component of the matrices on both sides of the congruence given above for $0 \leq i \leq s$, $1 \leq j \leq s$, we get

$$-q_n^{(0, i)} h_n^{(j)} + q_n^{(j, i)} \equiv 0 \pmod{d^n},$$

which implies the lemma. ■

We set

$$Q_n := (q_{n-s+j}^{(i, 0)})_{0 \leq i \leq s, 0 \leq j \leq s} \quad (n \geq s).$$

Lemma 8. $Q_n = Q_s J^{n-s}$ for all $n \geq s$.

Proof. In view of (15), we have

$$\begin{aligned} & (q_n^{(j, i)})_{0 \leq i \leq s, 0 \leq j \leq s} \\ &= Q \cdot (q_{n-1}^{(j, i)})_{0 \leq i \leq s, 0 \leq j \leq s} \\ &= \begin{bmatrix} -c_1 q_{n-1}^{(0, 0)} + c_0 q_{n-1}^{(0, 1)} & \dots & -c_1 q_{n-1}^{(s, 0)} + c_0 q_{n-1}^{(s, 1)} \\ -c_2 q_{n-1}^{(0, 0)} + c_0 q_{n-1}^{(0, 2)} & \dots & -c_2 q_{n-1}^{(s, 0)} + c_0 q_{n-1}^{(s, 2)} \\ \vdots & & \vdots \\ -c_s q_{n-1}^{(0, 0)} + c_0 q_{n-1}^{(0, s)} & \dots & -c_s q_{n-1}^{(s, 0)} + c_0 q_{n-1}^{(s, s)} \\ q_{n-1}^{(0, 0)} & \dots & q_{n-1}^{(s, 0)} \end{bmatrix}. \end{aligned}$$

Hence, we get

$$\begin{aligned} q_n^{(j, 0)} &= -c_1 q_{n-1}^{(j, 0)} + c_0 q_{n-1}^{(j, 1)} \\ &= -c_1 q_{n-1}^{(j, 0)} + c_0 (-c_2 q_{n-2}^{(j, 0)} + c_0 q_{n-2}^{(j, 2)}) \\ &= -c_1 q_{n-1}^{(j, 0)} - c_0 c_2 q_{n-2}^{(j, 0)} + c_0^2 q_{n-2}^{(j, 2)} \\ &= -c_1 q_{n-1}^{(j, 0)} - c_0 c_2 q_{n-2}^{(j, 0)} + c_0^2 (-c_3 q_{n-3}^{(j, 0)} + c_0 q_{n-3}^{(j, 3)}) \\ &= -c_1 q_{n-1}^{(j, 0)} - c_0 c_2 q_{n-2}^{(j, 0)} - c_0^2 c_3 q_{n-3}^{(j, 0)} + c_0^3 q_{n-3}^{(j, 3)} \\ &\quad \dots \quad \dots \quad \dots \quad \dots \\ &= -c_1 q_{n-1}^{(j, 0)} - c_0 c_2 q_{n-2}^{(j, 0)} - c_0^2 c_3 q_{n-3}^{(j, 0)} - \dots - c_0^{s-1} c_s q_{n-s}^{(j, 0)} + c_0^s q_{n-s}^{(j, s)} \\ &= -c_1 q_{n-1}^{(j, 0)} - c_0 c_2 q_{n-2}^{(j, 0)} - c_0^2 c_3 q_{n-3}^{(j, 0)} - \dots - c_0^{s-1} c_s q_{n-s}^{(j, 0)} + c_0^s q_{n-s-1}^{(j, 0)} \end{aligned}$$

for each $0 \leq j \leq s$, i.e.,

$$q_n^{(j, 0)} = (q_{n-s-1}^{(j, 0)}, q_{n-s-2}^{(j, 0)}, \dots, q_{n-1}^{(j, 0)})^T (c_0^s, -c_0^{s-1}c_s, \dots, -c_0c_2, -c_1). \quad (18)$$

Therefore, we obtain

$$Q_n = Q_{n-1}J \quad (n \geq s+1),$$

which implies the lemma. ■

Lemma 9. (i) $q_n^{(0)} \equiv (-c_1)^n \pmod{d}$,

(ii) $|h_n^{(j)} - q_n^{(j, 0)} / q_n^{(0, 0)}|_p \leq p^{-e(p)n}$ for all $n \geq 0$, $1 \leq j \leq s$, and $p \in \text{Prime}(d)$.

Proof. By Lemma 7 we get

$$q_n^{(0, 0)} h_n^{(j)} \equiv q_n^{(j, 0)} \pmod{d^n} \quad (1 \leq j \leq s, n \geq 0). \quad (19)$$

From (18), it follows

$$q_n^{(0, 0)} \equiv -c_1 q_{n-1}^{(0, 0)} \equiv c_1^2 q_{n-2}^{(0, 0)} \equiv \dots \equiv (-c_1)^n q_0^{(0, 0)} \equiv (-c_1)^n \pmod{d}.$$

Hence, recalling $\text{GCD}(c_0, c_1) = 1$, we get

$$\text{GCD}(q_n^{(0, 0)}, d) = 1 \quad (n \geq 0). \quad (20)$$

Therefore, we obtain by (20), (19)

$$\begin{aligned} |h_n^{(j)} - q_n^{(j, 0)} / q_n^{(0, 0)}|_p &= |q_n^{(0, 0)} h_n^{(j)} - q_n^{(j, 0)}|_p \\ &\leq p^{-e(p)n} \quad (1 \leq j \leq s, n \geq 0). \quad \blacksquare \end{aligned}$$

Let J_m be as in Theorem 2. We denote by $0_{t, u}$ the zero matrix of size $t \times u$, by $\underline{0}_m$ the matrix $0_{m, 1}$, and by $D(a_0, a_2, \dots, a_s)$ the diagonal matrix with $a_0, a_2, \dots, a_s$ as its diagonal components. For $m \geq 0$, we put

$$\begin{aligned} Q_m^* &:= GJ_0J_1 \cdots J_m, \\ G_{m+1} &:= D(c_0^{-m}, c_0^{-m+1}, \dots, c_0^{-1}, 1), \\ G &:= G_{s+1}, \end{aligned} \quad (21)$$

$$\Delta_{m+1} := \begin{bmatrix} q_0^{(0)} & q_1^{(0)} & \dots & q_m^{(0)} \\ & q_1^{(1)} & \dots & q_m^{(1)} \\ & & \ddots & \vdots \\ 0 & & & q_m^{(m)} \end{bmatrix},$$

where

$$q_n^{(i)} := q_n^{(i, 0)} \quad (0 \leq i \leq s, n \geq 0)$$

with $q_n^{(j, 0)}$ defined by (15). We put

$$\underline{q}_n := {}^T(q_n^{(0)}, \dots, q_n^{(s)}) \in \mathbb{Z}^{s+1} \quad (n \geq 0).$$

Then we can prove the following

Lemma 10.

$$\begin{aligned} (i) \quad & \underline{q}_0 = {}^T(1, 0, \dots, 0), \\ & \underline{q}_n = {}^T(-C_1 q_{n-1}^{(0)} - C_2 q_{n-1}^{(1)} - \dots - C_n q_{n-1}^{(n-1)}, \\ & \quad C_0 q_{n-1}^{(0)}, C_0 q_{n-1}^{(1)}, \dots, C_0 q_{n-1}^{(n-1)}, {}^T \underline{0}_{s-n}) \quad (1 \leq n \leq s). \end{aligned} \quad (22)$$

$$(ii) \quad Q_n^* = \begin{bmatrix} 0_{n+1, s-n} & \Delta_{n+1} \\ D_{s-n} & 0_{s-n, n+1} \end{bmatrix} \quad (0 \leq n < s), \quad Q_s^* = Q_s.$$

Proof. We prove (i), and (ii) by induction on n. We put

$$\underline{e}_0 := {}^T(1, 0, \dots, 0), \dots, \underline{e}_s := {}^T(0, 0, \dots, 1) \in \mathbb{Z}^{s+1}.$$

Note that, this time, $\underline{e}_i$ is the (i+1)-th fundamental vector of dimension s+1.

First, we prove (i). Recalling (15), we have

$${}^T Q^n =: (q_n^{(i, j)})_{0 \leq i \leq s, 0 \leq j \leq s} \quad (n \geq 0),$$

where

$${}^T Q := \begin{bmatrix} -{}^T \underline{C} & 1 \\ C_0 E_s & \underline{0}_s \end{bmatrix}.$$

It is trivial that $\underline{q}_0 = \underline{e}_0$, and $\underline{q}_1 = {}^T(-C_1, C_0, {}^T \underline{0}_{s-1})$ are valid. Suppose that (22) holds for an integer satisfying $1 \leq n \leq s-1$. Then

$$\begin{aligned} \underline{q}_{n+1} &= {}^T C^{n+1} \underline{e}_0 = {}^T C \cdot {}^T C^n \underline{e}_0 = {}^T C \underline{q}_n \\ &= {}^T(-C_1 q_n^{(0)} - C_2 q_n^{(1)} - \dots - C_{n+1} q_n^{(n)}, C_0 q_n^{(0)}, C_0 q_n^{(1)}, \dots, C_0 q_n^{(n)}, {}^T \underline{0}_{s-n-1}), \end{aligned}$$

so that (22) holds with n+1 in place of n.

Secondly, we prove (ii). (ii) with n=0 follows from

$$Q_0^* = G J_0 = \begin{bmatrix} 0_{1, s} & \Delta_1 \\ D_s & 0_{s, 1} \end{bmatrix}.$$

Suppose (ii) holds for an integer $0 \leq n < s-1$. Then

$$Q_{n+1}^* = Q_n^* J_{n+1}$$

$$\begin{aligned}
&= \begin{bmatrix} O_{n+1, s-n} & \Lambda_{n+1} \\ G_{s-n} & O_{s-n, n+1} \end{bmatrix} \begin{bmatrix} {}^T \underline{O} & C_0^s \\ E_s & -\underline{C}_{n+1}^* \end{bmatrix} \\
&= \begin{bmatrix} & \Lambda_{n+1} & \begin{matrix} -C_1 q_n^{(0)} - C_0 C_2 q_n^{(0)} - \dots - C_0^n C_{n+1} q_0^{(0)} \\ -C_1 q_n^{(1)} - C_0 C_2 q_n^{(1)} - \dots - C_0^{n-1} C_n q_1^{(1)} \\ \vdots \\ -C_1 q_n^{(n)} \end{matrix} \\ O_{n+2, s-n-1} & & \\ & {}^T \underline{O}_{n+1} & C_0^{n+1} \\ G_{s-n-1} & O_{s-n-1, n+1} & \underline{O}_{s-n-1} \end{bmatrix}. \quad (23)
\end{aligned}$$

On the other hand, (i) implies $q_{n+1}^{(n+1)} = C_0^{n+1}$ ($0 \leq n < s-1$), and

$$\begin{aligned}
q_{n+1}^{(m)} &= C_0 q_n^{(m-1)} = C_0^2 q_{n-1}^{(m-2)} = \dots = C_0^m q_{n-m+1}^{(0)} \\
&= C_0^m (-C_1 q_{n-m}^{(0)} - C_2 q_{n-m}^{(1)} - \dots - C_{n-m+1} q_{n-m}^{(n-m)}) \\
&= C_0^m (-C_1 q_{n-m}^{(0)} - C_0 C_2 q_{n-m-1}^{(0)} - \dots - C_0^{n-m} C_{n-m+1} q_0^{(0)}) \\
&= -C_0^m C_1 q_{n-m}^{(0)} - C_0^{m+1} C_2 q_{n-m-1}^{(0)} - \dots - C_0^n C_{n-m+1} q_0^{(0)} \\
&= -C_1 q_n^{(m)} - C_0 C_2 q_{n-1}^{(m)} - \dots - C_0^{n-m} C_{n-m+1} q_m^{(m)}. \quad (24)
\end{aligned}$$

Therefore, we get by (23), (24),

$$Q_{n+1}^* = \begin{bmatrix} O_{n+2, s-n-1} & \Lambda_{n+2} \\ G_{s-n-1} & O_{s-n-1, n+2} \end{bmatrix},$$

which says that (ii) holds with $n+1$ in place of n for $0 \leq n < s-1$. In particular,

$$Q_{s-1}^* = \begin{bmatrix} O_s & \Lambda_s \\ 1 & {}^T \underline{O}_s \end{bmatrix}.$$

Hence,

$$Q_s^* = Q_{s-1}^* J_s =$$

$$= \left[\begin{array}{c|c} \Lambda_s & \begin{matrix} -C_1 q_{s-1}^{(0)} - C_0 C_2 q_{s-2}^{(0)} - \dots - C_0^{s-1} C_s q_0^{(0)} \\ -C_1 q_{s-1}^{(1)} - C_0 C_2 q_{s-2}^{(1)} - \dots - C_0^{s-2} C_{s-1} q_1^{(1)} \\ \vdots \\ -C_1 q_{s-1}^{(s-1)} \end{matrix} \\ \hline {}^T \underline{Q}_s & C_0^s \end{array} \right]. \quad (25)$$

On the other hand, we have

$$\begin{aligned} \underline{q}_s &= {}^T C^s \underline{e}_0 = {}^T C {}^T C^{s-1} \underline{e}_0 = {}^T C \underline{q}_{s-1} \\ &= {}^T (-C_1 q_{s-1}^{(0)} - C_2 q_{s-1}^{(1)} - \dots - C_s q_{s-1}^{(s-1)}, C_0 q_{s-1}^{(0)}, \dots, C_0 q_{s-1}^{(s-1)}). \end{aligned} \quad (26)$$

Using (i), for $0 \leq m \leq s-1$, we get

$$\begin{aligned} & -C_1 q_{s-1}^{(m)} - C_0 C_2 q_{s-2}^{(m)} - \dots - C_0^{s-m-1} C_{s-m} q_m^{(m)} \\ &= C_0^m (-C_1 q_{s-m-1}^{(0)} - C_2 q_{s-m-1}^{(1)} - \dots - C_{s-m} q_{s-m-1}^{(s-m-1)}) \\ &= C_0^m q_{s-m}^{(0)} \\ &= q_s^{(m)}, \end{aligned} \quad (27)$$

and

$$\begin{aligned} & -C_1 q_{s-1}^{(0)} - C_0 C_2 q_{s-2}^{(0)} - \dots - C_0^{s-1} C_s q_0^{(0)} \\ &= q_s^{(0)} = -C_1 q_{s-1}^{(0)} - C_2 q_{s-1}^{(1)} - \dots - C_s q_{s-1}^{(s-1)}. \end{aligned} \quad (28)$$

From (26) and (i), it follows

$$q_s^{(s)} = C_0 q_{s-1}^{(s-1)} = C_0^s q_0^{(0)} = C_0^s. \quad (29)$$

In view of (25-29), we obtain $Q_s^* = \Lambda_{s+1}$. Since (i) implies

$$q_n^{(m)} = 0 \quad (0 \leq n < m \leq s),$$

we get $Q_s^* = Q_s$, which completes the proof of Lemma 10. ■

Proof of Theorem 2. We consider the vector $\underline{r}_n \in \mathbb{Z}^{s+1}$ ($n \geq 0$) in Theorem 2.

Then $\underline{r}_n = J_0 J_1 \cdots J_n \underline{e}_s$. We define $\underline{q}_n^* = (q_n^{*(0)}, \dots, q_n^{*(s)}) \in \mathbb{Q}^s$ by

$$\underline{q}_n^* = (q_n^{*(0)}, \dots, q_n^{*(s)}) := \begin{cases} G J_0 J_1 \cdots J_n \underline{e}_s & (0 \leq n \leq s-1) \\ G J_0 J_1 \cdots J_{s-1} J^{n-s+1} \underline{e}_s & (n \geq s). \end{cases}$$

Then

$$\underline{r}_n = G^{-1} \underline{q}_n^* = (C_0^s q_n^{*(0)}, C_0^{s-1} q_n^{*(1)}, \dots, q_n^{*(s)}).$$

Lemmas 8, 10 imply

$$\begin{aligned} \underline{q}_n^* &= (q_n^{(0)}, \dots, q_n^{(n)}, 0, \dots, 0) \quad (0 \leq n \leq s), \\ \underline{q}_n^* &= Q_s J^{n-s} \underline{e}_s = Q_n \underline{e}_s = (q_n^{(0)}, \dots, q_n^{(s)}) = \underline{q}_n \quad (n > s). \end{aligned}$$

Recalling $q_n^{(m)} = 0$ ($n < m \leq s$), we get

$$q_n^{*(m)} = q_n^{(m)} \quad (0 \leq m \leq s, n \geq 0),$$

which together with Lemma 6 implies

$$\theta_n^{(j)} = r_n^{(j)} / r_n^{(0)} = c_0^{-j} q_n^{(j)} / q_n^{(0)} \quad (n \geq 0, 1 \leq j \leq s),$$

Lemma 9, (i) implies $|q_n^{(0)}|_p = 1$, so that Lemma 9, (ii), which together with Theorem 1 implies

$$\begin{aligned} |\theta_n^{(j)} - c_0^{-j} \lambda_p^j|_p &= |c_0^{-j}|_p |q_n^{(j)} / q_n^{(0)} - \lambda_p^j|_p, \\ &\leq |c_0^{-j}|_p \cdot \max\{|q_n^{(j)} / q_n^{(0)} - h_n^{(j)}|_p, |h_n^{(j)} - \lambda_p^j|_p\} \\ &\leq p^{-e(p)n+j} \end{aligned}$$

for all $n \geq 0$, $1 \leq j \leq s$, and $p \in \text{Prime}(d)$. ■

Proof of Corollary 1. We denote by $[r]$ ($r \in \mathbb{R}$, $[\infty] := \infty$) the largest integer not exceeding r . We put

$$t(n) := [n/(s+1)], \quad r(n) := n - (s+1)t(n) \quad (n \in \mathbb{Z}).$$

It is clear that $n = (s+1)t(n) + r(n)$, $0 \leq r(n) \leq s$ holds. In view of the following lemma, we get Corollary 1 from Theorem 2. ■

Lemma 11. Let $X_m \in M(s+1; \mathbb{Z}[\underline{x}_m])$, $\underline{x}_m = {}^T(x_m^{(0)}, x_m^{(1)}, \dots, x_m^{(s)})$, $0 \leq m \leq n$ be as in Lemma 6. Let

$$\begin{aligned} X_m^\# &:= X_m X_{m-s-1} X_{m-2(s+1)} \cdots X_{r(m)} \quad (0 \leq m \leq n), \quad X_m^\# := 1 \quad (m < 0); \\ \underline{x}_m^* &= {}^T(x_m^{*(0)}, x_m^{*(1)}, \dots, x_m^{*(s)}) \\ &:= (X_m^\#)^{-1} \cdot {}^T(X_{m-s}^\# \cdot X_m^{(1)}, X_{m-s+1}^\# \cdot X_m^{(2)}, \dots, X_{m-1}^\# \cdot X_m^{(s)}), \end{aligned}$$

where $x_m = x_m^{(0)}$. Then the following formula holds:

$$\begin{aligned} (x_0^{(0)})^{-1} \underline{x}_0 &+ \frac{(x_0^{(0)})^{-1}}{(x_1^{(0)})^{-1} \underline{x}_1 + \frac{(x_1^{(0)})^{-1}}{(x_2^{(0)})^{-1} \underline{x}_2 + \cdots + \frac{(x_{m-2}^{(0)})^{-1}}{(x_{m-1}^{(0)})^{-1} \underline{x}_n + \frac{(x_{m-1}^{(0)})^{-1}}{(x_m^{(0)})^{-1} \underline{x}_m}}}} \\ &= [\underline{x}_0^*; \underline{x}_1^*, \dots, \underline{x}_m^*] \in (Q[\underline{x}_0, \underline{x}_1, \dots, \underline{x}_m])^s, \quad 0 \leq m \leq n. \end{aligned}$$

Proof. Let $D_m \in M(s+1; \mathbb{Z}[\underline{x}_0, \underline{x}_1, \dots, \underline{x}_m])$ be diagonal matrices

$$D_m := D(x_{m-s}^\#, \dots, x_{m-1}^\#, x_m^\#) \quad (-1 \leq m \leq n).$$

and X_m^* the matrices defined by

$$X_m^* := D_{m-1} X_m D_m^{-1} \in M(s+1; Q[\underline{x}_0, \dots, \underline{x}_m]) \quad (0 \leq m \leq n).$$

Then

$$X_m^* = \begin{bmatrix} {}^T \underline{0} & 1 \\ E_s & \underline{x}_m^* \end{bmatrix}$$

with

$$\underline{x}_m^* = (X_m^\#)^{-1} \cdot {}^T (X_{m-s}^\# \cdot X_m^{(1)}, X_{m-s+1}^\# \cdot X_m^{(2)}, \dots, X_{m-1}^\# \cdot X_m^{(s)})$$

holds. Noting $X_0 X_1 \cdots X_m D_m^{-1} = X_0^* X_1^* \cdots X_m^*$, we get

$$\begin{aligned} & ((X_0)_\# \circ (X_1)_\# \circ \cdots \circ (X_m)_\#)((D_m^{-1})_\#(\underline{\xi})) \\ &= (X_0^{(0)})^{-1} \underline{x}_0 + \frac{(X_0^{(0)})^{-1}}{(X_1^{(0)})^{-1} \underline{x}_1 + \frac{(X_1^{(0)})^{-1}}{(X_2^{(0)})^{-1} \underline{x}_2 + \cdots + \frac{(X_{m-1}^{(0)})^{-1}}{(X_m^{(0)})^{-1} \underline{x}_m + \frac{(X_m^{(0)})^{-1}}{D_m^{-1} * (\underline{\xi})}}} \\ &= ((X_0^*)_\# \circ (X_1^*)_\# \circ \cdots \circ (X_m^*)_\#)(\underline{\xi}) \\ &= \underline{x}_0^* + \frac{1}{\underline{x}_1^* + \frac{1}{\underline{x}_2^* + \cdots + \frac{1}{\underline{x}_n^* + \frac{1}{\underline{\xi}}}}} \end{aligned}$$

We set $\underline{\xi} = {}^T(0, \dots, 0, \xi^{-1})$ as in the proof of Lemma 6. Taking $\xi=0$, we have

$$T(\underline{\xi}) = T((D_m^{-1})_\#(\underline{\xi})) = \underline{0} \in Q(\underline{x}_0, \underline{x}_1, \dots, \underline{x}_m)^s$$

as rational functions, and we get Lemma 11. ■

§5. A form $\Psi(\underline{x}; f)$. We denote by $Q^{a_1 s} \supset Q$ (resp., $Q_p^{a_1 s} \supset Q_p$) the algebraic closure of Q (resp., Q_p). Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree $s+1$, $C = C(f) \in M_0(s+1; \mathbb{Z})$ the companion matrix of f , $e(p)$ ($p \in \text{Prime}(|f(0)|)$) the number as in Section 0. We denote by $\Phi(x; A)$ the characteristic polynomial of a matrix $A \in M(s+1; Q)$.

We define a form $\Psi(\underline{x}; f)$ with $s+1$ indeterminates by

$$\Psi(\underline{x}; f) = \Psi(x_0, x_1, \dots, x_s; f) := \det \left(\sum_{0 \leq j \leq s} x_j C(f)^j \right) \in \mathbb{Z}[x_0, \dots, x_s].$$

We remark that

$$\begin{aligned}\Psi(\underline{x}; f) &= \prod_{f(a)=0} \prod_{(a \in \mathbb{Q}^{s+1})} \left(\sum_{0 \leq j \leq s} a^j x_j \right) \\ &= \prod_{f(a)=0} \prod_{(a \in \mathbb{Q}_p^{s+1})} \left(\sum_{0 \leq j \leq s} a^j x_j \right)\end{aligned}$$

holds, where the former (resp. the latter) product is taken over all the roots a of f in the field $\mathbb{Q}^{s+1}$ (resp. $\mathbb{Q}_p^{s+1}$) with their multiplicity. For f being irreducible over $\mathbb{Z}[x]$, $\Psi(\underline{x}; f)$ becomes a norm form in the usual sense.

For a given matrix $A \in M_0(s+1; \mathbb{Z})$, we write $A \in (\text{Bdd})$ if A satisfies the following condition (Bdd):

(Bdd) The set $\{n \geq 0; A^{-n} \underline{x} \in \mathbb{Z}^{s+1}\}$ is bounded for any $\underline{x} \in \mathbb{Z}^{s+1} \setminus \{\underline{0}\}$.

We can show that if $A \in (\text{Bdd})$, then $A \in M(s+1; \mathbb{Z})$ has no units ($\in \mathbb{Q}^{s+1}$) as its eigenvalues in $\mathbb{Q}^{s+1}$; and if

$$A = U^{-1} \begin{bmatrix} A_1 & * \\ & \ddots \\ \circ & A_t \end{bmatrix} U \quad (\text{or} \quad U^{-1} \begin{bmatrix} A_1 & \circ \\ & \ddots \\ * & A_t \end{bmatrix} U), \quad U \in GL(s+1; \mathbb{Z})$$

such that $|\det A_k| > 1$, and $\Phi(x; A_k)$ is irreducible over $\mathbb{Z}[x]$ for all $1 \leq k \leq t$, then $C(f) \in (\text{Bdd})$. In particular, if $f \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}[x]$, and $|f(0)| > 1$, then $C(f) \in (\text{Bdd})$, cf. Theorem 2 in [3], see also [2].

Let us suppose $A \in (\text{Bdd})$, and consider a map ind_A defined by

$$\text{ind}_A: \mathbb{Z}^{s+1} \longrightarrow \mathbb{N} \cup \{\infty\}$$

$$\text{ind}_A(\underline{x}) := \max\{n \geq 0; A^{-n} \underline{x} \in \mathbb{Z}^{s+1}\} \quad (\underline{x} \neq \underline{0}), \quad \text{ind}_A(\underline{0}) := \infty,$$

where $\mathbb{N} := \{0, 1, 2, \dots\}$. We remark that there exists a unique partition

$$\bigcup_{0 \leq j < c} A^j \Gamma = \mathbb{Z}^{s+1} \setminus \{\underline{0}\} \quad (\text{disjoint})$$

of the set $\mathbb{Z}^{s+1} \setminus \{\underline{0}\}$ into c ($2 \leq c \leq \infty$) parts iff $A \in (\text{Bdd})$, and

$$\Gamma = \{\underline{x} \in \mathbb{Z}^{s+1} \setminus \{\underline{0}\}; \text{ind}_A(\underline{x}) \equiv 0 \pmod{c}\} \quad (c \neq \infty),$$

$$\Gamma = \{\underline{x} \in \mathbb{Z}^{s+1} \setminus \{\underline{0}\}; \text{ind}_A(\underline{x}) = 0\} \quad (c = \infty)$$

holds, cf. Theorem 1 in [3].

We mean by $v_p = \text{ord}_p$ the p -adic valuation, i.e., the additive version of $|\cdot|_p$.

Then Theorem 1 implies the following

Corollary 2. Let $f \in \mathbb{Z}[x]$ be a monic polynomial satisfying (1) such that $C(f) \in (\text{Bdd})$. Let $\lambda_p \in \mathbb{Z}_p$ ($p \in \text{Prime}(f(0))$) be as in Theorem 1. Then

$$\text{ind}_{C(f)}(\underline{x}) = \min_{p \in \text{Prime}(f(0))} \left(\lfloor v_p \left(\sum_{0 \leq j \leq s} \lambda_p^j x_j \right) / v_p(f(0)) \rfloor \right)$$

holds for all $\underline{x} = {}^T(x_0, x_1, \dots, x_s) \in \mathbb{Z}^{s+1}$.

Proof. For any $\underline{x} \in \mathbb{Z}^{s+1} \setminus \{0\}$, we have the following equivalences:

$$\begin{aligned} \text{ind}_{C(f)}(\underline{x}) = m &\iff C(f)^{-m} \underline{x} \in \mathbb{Z}^{s+1} \text{ \& } C(f)^{-m-1} \underline{x} \notin \mathbb{Z}^{s+1} \\ &\iff d^m C(f)^{-m} \underline{x} \in d^m \mathbb{Z}^{s+1} \text{ \& } d^{m+1} C(f)^{-m} \underline{x} \notin d^{m+1} \mathbb{Z}^{s+1} \\ &\iff H_m(C) \underline{x} \in d^m \mathbb{Z}^{s+1} \text{ \& } H_{m+1}(C) \underline{x} \notin d^{m+1} \mathbb{Z}^{s+1} \\ &\iff d^{-m} H_m(C) \underline{x} \in \mathbb{Z}^{s+1} \text{ \& } d^{-m-1} H_{m+1}(C) \underline{x} \notin \mathbb{Z}^{s+1} \end{aligned}$$

Thus, in view of Theorem 1, we have

$$\begin{aligned} \text{ind}_{C(f)}(\underline{x}) = m &\iff \\ x_0 + h_m^{(1)} x_1 + \dots + h_m^{(s)} x_s &\in d^m \mathbb{Z}^{s+1} \text{ \& } x_0 + h_{m+1}^{(1)} x_1 + \dots + h_{m+1}^{(s)} x_s \notin d^{m+1} \mathbb{Z}^{s+1} \\ &\iff e(p)m \leq v_p\left(\sum_{0 \leq j \leq s} \lambda_p^j x_j\right) \text{ for all } p \in \text{Prime}(d), \text{ and} \\ &\quad v_p\left(\sum_{0 \leq j \leq s} \lambda_p^j x_j\right) < e(p)(m+1) \text{ for some } p \in \text{Prime}(d) \\ &\iff e(p)m \leq \min_{p \in \text{Prime}(f(0))} v_p\left(\sum_{0 \leq j \leq s} \lambda_p^j x_j\right) < e(p)(m+1) \end{aligned}$$

so that Corollary 2 follows. ■

Recalling

$$\Psi(\underline{x}; f) = \prod_{f(a)=0} \prod_{(a \in \mathbb{Q}_{p^{s+1}})} \left(\sum_{0 \leq j \leq s} a^j x_j \right),$$

we see

$$|\Psi(\underline{x}; f)|_p \leq \left| \sum_{0 \leq j \leq s} \lambda_p^j x_j \right|_p \quad (\underline{x} \in \mathbb{Z}^{s+1})$$

since $\left| \sum_{0 \leq j \leq s} a^j x_j \right|_p \leq 1$ ($\underline{x} \in \mathbb{Z}^{s+1}$) holds for any root $a \in \mathbb{Q}_{p^{s+1}}$ of monic polynomial $f \in \mathbb{Z}[x]$. Noting $|a|_p = 1$ for any root $a \neq \lambda_p$ ($a \in \mathbb{Q}_{p^{s+1}}$) of f satisfying (1), we see that Corollary 2 immediately implies the following corollary.

Corollary 3. Let f be as in Corollary 2. Then

$$\min_{p \in \text{Prime}(|f(0)|)} (|v_p(\Psi(\underline{x}; f)) / v_p(f(0))|) \leq \text{ind}_{C(f)}(\underline{x}), \quad \underline{x} \in \mathbb{Z}^{s+1}.$$

In particular, the equality holds if $x_j \not\equiv 0 \pmod{p}$ for exactly one $0 \leq j \leq s$.

Corollary 3 is of somewhat trivial, but it may be of interest by two reasons: first, the assertion is stated within the set $\mathbb{Z}$; secondly, the form $\Psi(\underline{x}; f)$ is not so simple when s is large. We give some examples, using a, b, c, d (resp. x, y, z, w) instead of c_0, c_1, c_2, c_3 (resp. x_0, x_1, x_2, x_3):

$$(i) \quad s=1, \quad f=x^2-bx-a,$$

$$\Psi(x, y; f) = x^2 + bxy - ay^2.$$

$$(ii) \quad s=2, \quad f=x^3-cx^2-bx-a,$$

$$\Psi(x, y, z; f) = x^3 + cx^2y + (2b+c^2)x^2z - bxy^2 - (3a+bc)xyz + (b^2-2ac)xz^2 + ay^3 + acy^2z - abyz^2 + a^2z^3$$

$$(iii) \quad s=3, \quad f=x^4-dx^3-cx^2-bx-a,$$

$$\begin{aligned} \Psi(x, y, z, w; f) = & x^4 + dx^3y + (2c+d^2)x^3z + (3b+3cd+d^3)x^3w - cx^2y^2 - (3b+cd)x^2yz \\ & - (4a+bd+2c^2+cd^2)x^2yw - (2a+2bd-c^2)x^2z^2 - (5ad-bc+2bd^2-c^2d)x^2zw \\ & - (3ac+3ad^2-3b^2-3bcd+c^3)x^2w^2 + bxy^3 + (4a+bd)xy^2z + (ad+bd^2+2bc)xy^2w + (3ad-bc)xyz^2 \\ & + (4ac+3ad^2-3b^2-bcd)xyzw - (5ab+acd+2b^2d-bc^2)xyw^2 - (2ac-b^2)xz^3 + (ab-2acd+b^2d)xz^2w \\ & + (4a^2+2ac^2+abd-b^2c)xzw^2 + (3a^2d-3abc+b^3)xw^3 - ay^4 - ady^3z - (2ac+ad^2)y^3w + acy^2z^2 \\ & + (3ab+acd)y^2zw + (2a^2+2abd-ac^2)y^2w^2 - abyz^3 - (4a^2+abd)yz^2w - (3a^2d-abc)yzw^2 \\ & + (2a^2c-ab^2)yw^3 + a^2z^4 + a^2dz^3w - a^2cz^2w^2 + a^2bzw^3 - a^3w^4 \end{aligned}$$

In general, $\Psi(x_0, x_1, \dots, x_s; f)$ consists of $(2s+1)!/((s+1)!s!)$ terms as a polynomial in $x_0, x_1, \dots, x_s$.

§6. Something more about p-adic phenomena. We can get something more related to Theorem 1. For simplicity, we take a matrix $A = [2, 2//2, 3] \in M(2; \mathbb{Z})$, and consider hermitian canonical forms $H_n(A) = H(B^n)$ for $B = \tilde{A} = (\det A) \cdot A^{-1}$, where we mean by $[a, b//c, d]$ the matrix having (a, b) (resp. (c, d)) as its first (resp. second) row. We can find a matrix $U \in GL(2; \mathbb{Z})$ satisfying $A = U^{-1}CU$, where C is a companion matrix of the characteristic polynomial f of A . In fact, we have

$$U = [-1, 0//1, 1], \quad C = UAU^{-1} = [0, -2//1, 5], \quad f = x^2 - 5x + 2,$$

so that

$$H_n(C) \sim 2^n UA^{-n}U^{-1} \sim 2^n A^{-n}U^{-1}.$$

Since $\text{GCD}(f(0), f'(0)) = 1$, we can set

$$H_n(C) = [1, x_n//0, 2^n], \quad 0 \leq x_n < 2^n$$

by virtue of Theorem 1, and so, we get

$$H_n(A) \sim 2^n A^{-n} \sim H_n(C)U = [x_n - 1, x_n//2^n, 2^n].$$

Since $x_n \equiv 0 \pmod{2}$ follows from $x_{n+1} \equiv x_n \pmod{2^n}$, so that $\text{GCD}(x_n - 1, 2^n) = 1$. Hence

$$(x_n - 1)u_n + 2^n v_n = 1 \tag{30}$$

holds for some integers u_n, v_n , we obtain

$$\begin{aligned} 2^n A^{-n} & \sim [u_n, v_n// -2^n, x_n - 1][x_n - 1, x_n//2^n, 2^n] \\ & = [1, u_n x_n + 2^n v_n//0, -2^n] \sim [1, u_n + 1//0, 2^n]. \end{aligned}$$

Setting $y_n := u_n + 1$, we get by (30)

$$(x_n - 1)(y_n - 1) \equiv 1 \pmod{2^n}. \tag{31}$$

Since $\{x_n\}_{n=1, 2, \dots}$ is a coherent sequence, it becomes a Cauchy sequence with

respect to the ultrametric in $\mathbb{Z}_p$. Therefore, from (31) x_n (resp. y_n) converges to an 2-adic integer λ (resp. μ), and we get $(\lambda-1)(\mu-1)=1$, which yields

$$g(\mu)=0, \quad g=2x^2-5x+2 \in \mathbb{Z}[x].$$

Thus, one can show that

$$|g(y_n)|_2 \leq 2^{-n}, \quad |\mu - y_n|_2 \leq 2^{-n}, \quad n \geq 1,$$

as well as

$$|f(x_n)|_2 \leq 2^{-n}, \quad |\lambda - x_n|_2 \leq 2^{-n}, \quad n \geq 1,$$

where $\lambda, \mu \in 2\mathbb{Z}_2$. In addition, there occurs an additional phenomenon. Noting

$$g(\mu)=0 \iff (2\mu+2)^2-5(2\mu+2)+2=0 \iff f(2\mu+2)=0,$$

we see that the 2-adic expansion of μ coincides with that of λ except for the head of the expansions:

$$\lambda = 0.1110001001101100110100001100110011000001 \dots (2),$$

$$\mu = 0.110001001101100110100001100110011000001 \dots (2),$$

where we mean by $d_k d_{k+1} \dots d_0 . d_1 d_2 \dots (p)$ the p -adic expansion $\sum_{n \geq k} d_n p^n$ of a number belonging to $\mathbb{Z}_p$ with respect to the canonical representatives.

Such a phenomenon is an accidental one, but we can find such examples, applying a conjecture/observation ($\dagger$) given below.

Obsevation ($\dagger$): In the example given above, we can find a relation

$$\mu = \lambda / (\lambda - 1) = ({}^t U)_\#(\lambda) = (\pi \circ {}^t U_* \circ \iota)(\lambda). \quad (32)$$

Such a relation does not always hold, but we can show (32) under some conditions on $f \in \mathbb{Z}[x]$, and $U \in \text{GL}(s+1; \mathbb{Z})$. For instance, let $f = x^{s+1} - c_s x^s - \dots - c_1 x - c_0 \in \mathbb{Z}[x]$ such that

$$|c_0| = p \text{ is a prime, and } v_p(c_1) = 0. \quad (33)$$

Then, we can show (32) in a general situation, if $U = (u_{ij})_{0 \leq i \leq s, 0 \leq j \leq s} \in \text{GL}(s+1; \mathbb{Z})$ satisfies a condition

$$\begin{aligned} \text{GCD}(u_{10}, u_{20}, \dots, u_{s0}) &= p^e, \quad e \geq 0, \\ u_{00} &\notin p\mathbb{Z}, \quad u_{0j} \in p\mathbb{Z} \quad (1 \leq j \leq s). \end{aligned} \quad (34)$$

Namely, under the hypotheses (33), (34), can show that

$$H_n(U^{-1}C(f)U) = \begin{bmatrix} 1 & \underline{h}_n^\# \\ \underline{0} & p^n E_s \end{bmatrix} \quad \text{for all } n \geq 1, \quad (35)$$

and

$$\lim_{n \rightarrow \infty} \underline{h}_n^* = (\tau U)_*(\underline{\lambda}_p), \quad \underline{\lambda}_p := {}^\tau(\lambda_p, \lambda_p^2, \dots, \lambda_p^s) \quad (36)$$

holds, where the limit is taken with respect to the p-adic metric, cf.

Proposition 1 given below.

The condition (33) on f may be too special, and (34) on U does not seem to be beautiful. As we shall see in Lemma 12, the behavior of the sequence

$$\{H_n(U^{-1}C(f)U)\}_{n=1, 2, 3, \dots}$$

turns out to be simple under a condition (37) given below, which is slightly weaker (33). We remark that, in general, the behavior of the sequence is somewhat chaotic. For instance, some of the entries ${}^\tau \underline{e}_i H_n(U^{-1}C(f)U) \underline{e}_j$ ($0 \leq i < j \leq s$) are not monotone increasing. Even for the diagonal entries, the behavior seems to be somewhat complicated.

Nevertheless, it seems very likely that, under a suitable normalization, the identity (36) can be generalized for any $U \in GL(s+1; \mathbb{Z})$ even for $f \in \mathbb{Z}[x]$ not satisfying (1), cf. Observation (§) given below.

For convenience' sake, we introduce the following:

Definition: Let $f \in \mathbb{Z}[x]$ be a monic polynomial, and p be a prime number. We say that f is singular at p iff there exists a root $\lambda_p^* \in \mathbb{Z}_p$ of f satisfying

$$|\lambda_p^*|_p < 1, \text{ and } |\lambda_p^*|_p < |\lambda_p|_p,$$

for all the roots $\lambda_p \neq \lambda_p^*$ of f in $\mathbb{Z}_p$. The number λ_p^* will be referred to as the singular root of f in $\mathbb{Z}_p$.

Notice that f is singular at p if it has a unique root $\alpha \in p\mathbb{Z}_p$, so that any monic $f \in \mathbb{Z}[x]$ satisfying (1) is singular at $p \in \text{Prime}(f(0))$. We put

$$\text{Prime}^*(f) := \{p; f \text{ is singular at } p\}.$$

Obsevation (§): Let $A \in M_0(s+1; \mathbb{Z})$ be any matrix given by

$$A = U^{-1}CU \text{ with } U \in GL(s+1; \mathbb{Z})$$

for the companion matrix $C = C(f) \in M_0(s+1; \mathbb{Z})$ of a monic polynomial $f \in \mathbb{Z}[x]$, which possibly does not satisfy (1). Let

$$H_n(U^{-1}CU) = (h_n^{(i, j)})_{0 \leq i \leq s, 0 \leq j \leq s, n \geq 0}.$$

Then the limits

$$\lim_{n \rightarrow \infty} h_n^{(0, j)} / h_n^{(0, 0)} \quad (1 \leq j \leq s) \quad \text{in } \mathbb{Z}_p$$

exist for all $p \in \text{Prime}^*(f)$. Furthermore, a formula

$$\begin{aligned}
& \lim_{n \rightarrow \infty} (h_n^{(0,0)})^{-1} \cdot \underline{h}_n (= \lim_{n \rightarrow \infty} \pi(\underline{h}_n)) = ({}^T U)_\#(\underline{\lambda}_p^\#), \\
& \underline{h}_n := {}^T(h_n^{(0,1)}, \dots, h_n^{(0,s)}), \quad \underline{h}_n := {}^T(h_n^{(0,0)}, \dots, h_n^{(0,s)}), \\
& \underline{\lambda}_p^\# := {}^T(\lambda_p^\#, \lambda_p^{2\#}, \dots, \lambda_p^{s\#}), \\
& p \in \text{Prime}^*(f)
\end{aligned}$$

holds, where $\lambda_p^\# \in p\mathbb{Z}_p$ is the singular root of f .

Warning At the moment, ($\dagger$) is an observation in exact sense; so, it has not proved yet. While, it seems very likely to work well as far as a few experiments by computers tell us.

The following proposition is a special case of ($\dagger$).

Proposition 1. Let $f \in \mathbb{Z}[x]$ be a polynomial as in Lemma 1 satisfying (33), and $C = C(f)$ its companion matrix. Let $U = (u_{ij})_{0 \leq i \leq s, 0 \leq j \leq s} \in GL(s+1; \mathbb{Z})$ satisfying (34). Then

$$(i) \quad H_n(U^{-1}CU) = \begin{bmatrix} 1 & {}^T \underline{h}_n^\# \\ \underline{0} & p^n E_s \end{bmatrix} \in M(s+1; \mathbb{Z}),$$

(ii) $\underline{h}_n$ converges in $\mathbb{Q}_p$ as n tends to infinity.

(iii) $\lim_{n \rightarrow \infty} \underline{h}_n^\# = ({}^T U)_\#(\underline{\lambda}_p)$, $\underline{\lambda}_p = {}^T(\lambda_p, \dots, \lambda_p^s)$, where $\lambda_p \in \mathbb{Z}_p$ is the number determined by $f(\lambda_p) = 0$, $\lambda_p \in p\mathbb{Z}_p$.

We mean by $\langle S \rangle$ ($S \subset \mathbb{Z}_{>0} := \{1, 2, 3, \dots\}$) the multiplicative monoid generated by S . We need three lemmas:

Lemma 12. Let $f = x^{s+1} - c_s x^s - \dots - c_1 x - c_0 \in \mathbb{Z}[x]$ be a polynomial satisfying (1). Let $C = C(f)$, and

$$H_n(C) = \begin{bmatrix} 1 & {}^T \underline{h}_n \\ \underline{0} & d^n E_s \end{bmatrix} \in M(s+1; \mathbb{Z}), \quad \underline{h}_n = {}^T(h_n^{(1)}, \dots, h_n^{(s)}), \quad d = |c_0|$$

as in Theorem 1. Let $U=(u_{ij})_{0 \leq i \leq s, 0 \leq j \leq s} \in GL(s+1; \mathbb{Z})$ be a matrix satisfying

$$\begin{aligned} \text{GCD}(u_{10}, u_{20}, \dots, u_{s0}) &\in \langle \text{Prime}(d) \rangle \\ \text{GCD}(u_{00}, d) &= 1, \quad u_{0j} \in d\mathbb{Z} \quad (1 \leq j \leq s). \end{aligned} \quad (37)$$

Then

$$(i)^* \quad H_n^* := H_n(U^{-1}CU) = H(H_n(C)U) = \begin{bmatrix} 1 & {}^T \underline{h}_n^* \\ \underline{0} & d^n E_s \end{bmatrix} \in M(s+1; \mathbb{Z})$$

with

$$\begin{aligned} {}^T \underline{h}_n^* &= (h_n^{*(1)}, \dots, h_n^{*(s)}) \in (d\mathbb{Z})^s, \\ 0 \leq h_n^{*(j)} &< d^n \quad (1 \leq j \leq s, n \geq 1). \end{aligned}$$

Lemma 12, $(i)^*$ corresponds to Lemma 1, $(i)^*$.

Proof of Lemma 12. We prove $(i)^*$ by induction on n . Using Lemma 1,

$$H_1(U^{-1}CU) \sim \det C \cdot U^{-1}C^{-1}U \sim H_1(C)U,$$

$$\sim \begin{bmatrix} 1 & {}^T \underline{h}_1 \\ \underline{0} & dE_s \end{bmatrix} \begin{bmatrix} u_{00} & {}^T \underline{u}_{0*} \\ \underline{u}_{*0} & U_1 \end{bmatrix} \sim \begin{bmatrix} u_{00} + {}^T \underline{h}_1 \underline{u}_{*0} & {}^T \underline{u}_{0*} + {}^T \underline{h}_1 U_1 \\ d\underline{u}_{*0} & dU_1 \end{bmatrix},$$

where

$$\begin{aligned} \underline{u}_{*0} &:= {}^T(u_{10}, u_{20}, \dots, u_{s0}), \quad \underline{u}_{0*} := {}^T(u_{01}, u_{02}, \dots, u_{0s}), \\ U_1 &:= (u_{ij})_{1 \leq i \leq s, 1 \leq j \leq s}. \end{aligned}$$

Recalling ${}^T \underline{h}_n \in (d\mathbb{Z})^s$, we get $u_{00} + {}^T \underline{h}_1 \underline{u}_{*0} \equiv u_{00} \not\equiv 0 \pmod{d}$; and by (37), we see that any common prime factor of $du_{10}, du_{20}, \dots, du_{s0}$ should be a prime factor of d .

Hence, we get

$$\text{GCD}(u_{00} + {}^T \underline{h}_1 \underline{u}_{*0}, du_{10}, du_{20}, \dots, du_{s0}) = 1.$$

On the other hand, we have

$${}^T({}^T \underline{u}_{0*} + {}^T \underline{h}_1 U_1) \in (d\mathbb{Z})^s$$

by (37) and Lemma 1. Hence, we get

$$H_1(U^{-1}CU) = H(H_1(C)U) \sim \begin{bmatrix} 1 & {}^T \underline{k}_1 \\ * & dU_1 \end{bmatrix} \sim$$

$$\sim \begin{bmatrix} 1 & {}^t \underline{k}_1 \\ \underline{0} & dU_1 \end{bmatrix} \in M(s+1; \mathbb{Z}), \quad \underline{k}_1 \in (d\mathbb{Z})^s,$$

cf. Proposition 2, in Supplement (b), Section 7. Here, $|\det(dU_1)| = |\det C \cdot C^{-1}| = d^s$, so that $U_1 \in GL(s; \mathbb{Z})$. Hence (i)* is valid for $n=1$.

Assume that (i)* holds for some integer $n \geq 1$. It is clear that

$$H_{n+1}(U^{-1}CU) \sim d^{n+1}U^{-1}C^{-n-1}U \sim H(H_{n+1}(C)U).$$

By the induction hypothesis, we get

$$H_{n+1}(U^{-1}CU) \sim d^n C^{-n} \cdot dC^{-1}U \sim H_n^\# \cdot dC^{-1}U$$

$$\sim \begin{bmatrix} 1 & {}^t \underline{h}_n^\# \\ \underline{0} & d^n E_s \end{bmatrix} \begin{bmatrix} -\underline{c} & c_0 E_s \\ 1 & {}^t \underline{0} \end{bmatrix} U$$

$$\sim \left[\begin{array}{c|c|c} -d_n^\# & \underline{c}_0 & c_0 h_n^{\#(1)} \quad c_0 h_n^{\#(2)} \quad \dots \quad c_0 h_n^{\#(s-1)} \\ -c_2 d^n & & \\ \vdots & \underline{0} & \\ -c_s d^n & & c_0 d^n E_{s-1} \\ d^n & & \hline & & {}^t \underline{0} \end{array} \right] U,$$

where

$$d_n^\# := c_1 + c_2 h_n^{\#(1)} + \dots + c_{s-1} h_n^{\#(s-1)} - h_n^{\#(s)}. \quad (38)$$

Hence, we obtain

$$H_{n+1}(U^{-1}CU) \sim \left[\begin{array}{c|c|c} d^n & 0 & 0 \quad 0 \quad \dots \quad 0 \\ -d_n & \underline{c}_0 & c_0 h_n^{\#(1)} \quad c_0 h_n^{\#(2)} \quad \dots \quad c_0 h_n^{\#(s-1)} \\ -c_2 d^n & & \\ \vdots & \underline{0} & \\ -c_s d^n & & c_0 d^n E_{s-1} \\ & & \hline & & {}^t \underline{0} \end{array} \right] U \quad (39)$$

By the induction hypothesis, we have $h_n^{\#(j)} \in d\mathbb{Z}$ for all $1 \leq j \leq s$, so that (38) implies $d_n \equiv c_1 \pmod{d}$. Thus, we get $\text{GCD}(d^n, d_n^\#) = 1$ by (1). Therefore, there exist integers u_n, v_n satisfying $d^n u_n - d_n^\# v_n = 1$. Hence, (39) implies

$$\begin{aligned}
H_{n+1}(U^{-1}CU) &\sim \left[\begin{array}{c|c} \begin{array}{cc} u_n & v_n \\ \hline d_n & d^n \end{array} & \begin{array}{c} \bigcirc \\ \hline E_{s-1} \end{array} \end{array} \right] \left[\begin{array}{c|c|c} \begin{array}{c} d^n \\ \hline -d_n \\ (d^n) \\ \vdots \\ (d^n) \end{array} & \begin{array}{c} 0 \\ \hline c_0 \\ \hline \underline{0} \end{array} & \begin{array}{cccc} 0 & 0 & \cdots & 0 \\ \hline (d) & (d) & \cdots & (d) \\ \hline & & c_0 d^n E_{s-1} & \end{array} \end{array} \right] U \\
&\sim \left[\begin{array}{c|c} \begin{array}{cc} 1 & (d) \\ \hline 0 & c_0 d^n \end{array} & \begin{array}{ccc} (d) & (d) & \cdots (d) \\ \hline (d^{n+1}) & (d^{n+1}) & \cdots (d^{n+1}) \\ \hline & & c_0 d^n E_{s-2} \end{array} \end{array} \right] U,
\end{aligned}$$

Hence, we get

$$H_{n+1}(U^{-1}CU) \sim \left[\begin{array}{c|c} 1 & {}^T \underline{k}_n \\ \hline \underline{0} & d^{n+1} P \end{array} \right] U, \quad \underline{k}_n \in (dZ)^s, \quad P \in M(s; Z). \quad (40)$$

Since $|\det(H_{n+1}(C))| = |\det((\det C \cdot C^{-1})^n)| = d^{s(n+1)}$, which together with (40) yields $P \in GL(s; Z)$, so that we obtain

$$\begin{aligned}
H_{n+1}(U^{-1}CU) &\sim \left[\begin{array}{c|c} 1 & {}^T \underline{k}_n \\ \hline \underline{0} & d^{n+1} E_s \end{array} \right] \left[\begin{array}{c|c} u_{00} & {}^T \underline{u}_{0*} \\ \hline \underline{u}_{*0} & U_1 \end{array} \right] \\
&= \left[\begin{array}{cc} u_{00} + {}^T \underline{k}_n \underline{u}_{*0} & {}^T \underline{u}_{0*} + {}^T \underline{k}_n U_1 \\ \hline d^{n+1} \underline{u}_{*0} & d^{n+1} U_1 \end{array} \right], \text{ say } = K_n.
\end{aligned}$$

Here, (40), respectively (37), implies $\text{GCD}(u_{00} + {}^T \underline{k}_n \underline{u}_{*0}, d) = \text{GCD}(u_{00}, d) = 1$, and $\text{GCD}(d^{n+1} u_{10}, \dots, d^{n+1} u_{s0}) \in \langle \text{Prime}(d) \rangle$, so that

$$\text{GCD}(u_{00} + {}^T \underline{k}_n \underline{u}_{*0}, d^{n+1} u_{10}, \dots, d^{n+1} u_{s0}) = 1.$$

Hence, we can find a matrix $V \in GL(s+1; Z)$ such that

$$\begin{aligned}
VK_n &= \begin{bmatrix} v_{00} & {}^T\underline{v}_{0*} \\ \underline{v}_{*0} & V_1 \end{bmatrix} \begin{bmatrix} u_{00} + {}^T\underline{k}_n \underline{u}_{*0} & {}^T\underline{u}_{0*} + {}^T\underline{k}_n U_1 \\ d^{n+1} \underline{u}_{*0} & d^{n+1} U_1 \end{bmatrix} \\
&= \begin{bmatrix} v_{00} \cdot (u_{00} + {}^T\underline{k}_n \underline{u}_{*0}) + d^{n+1} \cdot {}^T\underline{v}_{0*} \underline{u}_{*0} & v_{00} \cdot ({}^T\underline{u}_{0*} + {}^T\underline{k}_n U_1) + d^{n+1} \cdot {}^T\underline{v}_{0*} U_1 \\ (u_{00} + {}^T\underline{k}_n \underline{u}_{*0}) \cdot \underline{v}_{*0} + d^{n+1} V_1 \underline{u}_{*0} & \underline{v}_{*0} ({}^T\underline{u}_{0*} + {}^T\underline{k}_n U_1) + d^{n+1} \cdot V_1 U_1 \end{bmatrix} \quad (41) \\
&= \begin{bmatrix} 1 & | & \\ \underline{0} & | & \end{bmatrix} * ,
\end{aligned}$$

cf. Propositions 2, 3 in Supplement (b), Section 7. Therefore we obtain

$$(u_{00} + {}^T\underline{k}_n \underline{u}_{*0}) \cdot \underline{v}_{*0} + d^{n+1} V_1 \underline{u}_{*0} = \underline{0},$$

so that

$$(u_{00} + {}^T\underline{k}_n \underline{u}_{*0}) \cdot \underline{v}_{*0} \equiv \underline{0} \pmod{d^{n+1}}. \quad (42)$$

On the other hand, it follows from (37) and the induction hypothesis that

$$\text{GCD}(u_{00} + {}^T\underline{k}_n \underline{u}_{*0}, d) = \text{GCD}(u_{00}, d) = 1,$$

which together with (42) implies

$$\underline{v}_{*0} \equiv \underline{0} \pmod{d^{n+1}}. \quad (43)$$

Hence, in view of (41), (43), and

$${}^T(v_{00} \cdot ({}^T\underline{u}_{0*} + {}^T\underline{k}_n U_1) + d^{n+1} \cdot {}^T\underline{v}_{0*} U_1) \in (d\mathbb{Z})^s,$$

we get

$$H_{n+1}(U^{-1}CU) = H(H_{n+1}(C)U) \sim \begin{bmatrix} 1 & {}^T\underline{k}_{n+1} \\ \underline{0} & d^{n+1}W \end{bmatrix}, \quad \underline{k}_{n+1} \in (d\mathbb{Z})^s.$$

Since $|\det(H_{n+1}(U^{-1}CU))| = d^{s(n+1)}$, we have $W \in \text{GL}(s+1; \mathbb{Z})$, which implies (i)[#] with $n+1$ in place of n , which completes the proof of (i)[#]. ■

Lemma 13. Let $f = x^{s+1} - c_s x^s - \cdots - c_1 x - c_0 \in \mathbb{Z}[x]$ be a polynomial satisfying (33).

Then

$$\text{ind}_{U^{-1}CU}(\underline{x}) = v_p({}^T \underline{h}_n \# \underline{x}) = v_p({}^T \underline{\lambda}_p U \underline{x})$$

holds for all $\underline{x} := {}^T(x_0, x_1, \dots, x_s) \in \mathbb{Z}^{s+1}$, where

$$\begin{aligned} \underline{h}_n &= {}^T(h_n^{(0)}, h_n^{(1)}, \dots, h_n^{(s)}) := H_n \underline{e}_0, \\ \underline{\lambda}_p &:= (1, \lambda_p, \dots, \lambda_p^s) \end{aligned}$$

with λ_p as in Theorem 1.

Proof. Note that (33) implies (1). For any $\underline{x} \in \mathbb{Z}^{s+1}$, we have the following equivalences:

$$\begin{aligned} \text{ind}_{U^{-1}CU}(\underline{x}) = m &\iff U^{-1}C^{-m}U\underline{x} \in \mathbb{Z}^{s+1} \text{ \& } U^{-1}C^{-m-1}U\underline{x} \notin \mathbb{Z}^{s+1} \\ &\iff p^m U^{-1}C^{-m}U\underline{x} \in p^m \mathbb{Z}^{s+1} \text{ \& } p^{m+1} U^{-1}C^{-m-1}U\underline{x} \notin p^{m+1} \mathbb{Z}^{s+1} \\ &\iff H_m U\underline{x} \in p^m \mathbb{Z}^{s+1} \text{ \& } H_{m+1} U\underline{x} \notin p^{m+1} \mathbb{Z}^{s+1}. \end{aligned}$$

In view of Theorem 1, and Lemma 12, we get

$$\begin{aligned} H_n \# &= \begin{bmatrix} 1 & {}^T \underline{h}_n \# \\ \underline{0} & p^n E_s \end{bmatrix} \sim H_n U = \begin{bmatrix} u_{00} + {}^T \underline{h}_n \underline{u}_{*0} & {}^T \underline{u}_{0*} + {}^T \underline{h}_n U_1 \\ p^n \underline{u}_{*0} & p^n U_1 \end{bmatrix}. \\ &\equiv \begin{bmatrix} \underline{\lambda}_p \\ O_{s, s+1} \end{bmatrix} U \pmod{p^n}, \end{aligned}$$

where, for $\alpha, \beta \in \mathbb{Z}_p$, we mean by $\alpha \equiv \beta \pmod{p^n}$ that $v_p(\alpha - \beta) \geq n$. Thus, we get

$$\text{ind}_{U^{-1}CU}(\underline{x}) = n \iff v_p({}^T \underline{h}_n \# \underline{x}) = n \iff v_p({}^T \underline{\lambda}_p U \underline{x}) = n. \blacksquare$$

Lemma 14. Let $\underline{a} = {}^T(1, a_1, \dots, a_s)$, $\underline{\beta} = {}^T(\beta_0, \dots, \beta_s) \in \mathbb{Z}_p^{s+1}$. Suppose that $v_p({}^T \underline{a} \cdot \underline{x}) = v_p({}^T \underline{\beta} \cdot \underline{x})$ holds for all $\underline{x} \in \mathbb{Z}^{s+1}$. Then

$$(a_1, \dots, a_s) = \pi({}^T(\beta_0, \dots, \beta_s)) = \beta_0^{-1} \cdot {}^T(\beta_1, \dots, \beta_s).$$

Proof. Setting $\underline{x} = \underline{e}_j$ in $v_p({}^T \underline{a} \cdot \underline{x}) = v_p({}^T \underline{\beta} \cdot \underline{x})$, we get

$$a_j = \varepsilon_j \beta_j \quad (\varepsilon_j \in \mathbb{Z}_p^\times := \{\varepsilon \in \mathbb{Z}_p; |\varepsilon|_p = 1\}, 0 \leq j \leq s, a_0 := 1).$$

Hence, setting $x_0 := -a_k$, $x_k := 1$ ($k \neq 0$), $x_j := 0$ ($j \neq 0, k$), we obtain

$$0 = -\beta_0 a_k + \beta_k = (-\beta_0 \varepsilon_k + 1) \beta_k,$$

so that $\varepsilon_k = \beta_0^{-1}$. We can choose any $1 \leq k \leq s$, we get the lemma. $\blacksquare$

Proof of Proposition 1. The statements (i–iii) in Proposition 1 are clear

from Lemmas 12-14. ■

§7. Supplements and an Appendix. We give two supplements (a), (b), and an appendix (c). The supplement (a) gives a structure to the set $\mathbb{Z}^{s+1}$ not only as a $\mathbb{Z}$ -module, but also a ring with respect to a given polynomial $f \in \mathbb{Z}[x]$ satisfying (1), and a given prime factor p of $f(0)$. We give an algorithm of a kind of multidimensional continued fraction expansion, and a Proposition 2 in the supplement (b).

(a) Let $f \in \mathbb{Z}[x]$ be a monic polynomial satisfying (1), and λ_p ($p \in \text{Prime}(f(0))$) be as in Section 0. We put

$$F := \mathbb{Q}(\lambda_p) \subset \mathbb{Q}_p.$$

Let μ be a map defined by

$$\begin{aligned} \mu: \mathbb{Z}^{s+1} &\longrightarrow F, \\ \mu(\underline{x}) &:= \sum_{0 \leq j \leq s} x_j \lambda_p^j, \quad \underline{x} = {}^T(x_0, \dots, x_s) \in \mathbb{Z}^{s+1}. \end{aligned}$$

It is clear that $\text{Im } \mu = \mathbb{Z}[\lambda_p]$, which is a subring of the valuation ring $O(F) := \{\alpha \in F; |\alpha|_p \leq 1\}$ of F . Notice that $0(F) \ni \lambda_p/p \notin \text{Im } \mu$, and $\text{Im } \mu$ is not a ideal of $O(F)$. We have the following exact sequence:

$$\{0\} \longrightarrow \text{Ker } \mu \longrightarrow \mathbb{Z}^{s+1} \xrightarrow{\mu} \text{Im } \mu \longrightarrow \{0\}.$$

If $f \in \mathbb{Z}[x]$ is irreducible, then $\text{Ker } \mu = \{0\}$. Hence, we can identify $\mathbb{Z}^{s+1}$ with $\mathbb{Z}[\lambda_p]$ not only as a $\mathbb{Z}$ -module, but also as a commutative ring with a unit. Namely, the lattice $\mathbb{Z}^{s+1}$ becomes a commutative ring, with respect to the multiplication

$$\underline{x} \cdot \underline{y} := \mu^{-1}(\mu(\underline{x})\mu(\underline{y})) \in \mathbb{Z}^{s+1} \quad (\underline{x}, \underline{y} \in \mathbb{Z}^{s+1}),$$

with $\underline{e}_0$ as its unit.

In the proof of Lemma 12, we used the fact that for any given vector $\underline{a} = {}^T(a_0, a_1, \dots, a_s) \in \mathbb{Z}^{s+1}$ with $\text{GCD}(a_0, a_1, \dots, a_s) = 1$, there exists a vector $\underline{b} \in \mathbb{Z}^{s+1}$ satisfying ${}^T \underline{a} \cdot \underline{b} = 1$. This fact is a direct conclusion of that $\mathbb{Z}$ is a principal ideal ring. We can find $\underline{b}$ by applying the Euclidean algorithm among integers $a_0, a_1, \dots, a_s$. The problem is that the bigger is the number s , the harder is the practical calculation to find $\underline{b}$. The following continued fraction algorithm can resolve such a problem.

(b) Let $\mathcal{Q} := [0, 1]^s$ be the unit cube of dimension s , and $\mathcal{Q}_i$ ($0 \leq i \leq s-1$) be its subsets defined by

$$\mathcal{Q}_i := \{^T(x_1, \dots, x_s) \in \mathcal{Q}; x_1 = \dots = x_{i-1} = 0, x_i \neq 0\}, \quad 1 \leq i \leq s.$$

Then

$$\mathcal{Q} \setminus \{\underline{0}\} = \bigcup_{1 \leq i \leq s} \mathcal{Q}_i$$

is a disjoint union, so that we can define a map

$$\begin{aligned} \tau: \mathcal{Q} \setminus \{\underline{0}\} &\longrightarrow \mathbb{R}^s, \\ \tau(\underline{x}) &:= T_i(\underline{x}) \text{ iff } \underline{x} \in \mathcal{Q}_i \quad (1 \leq i \leq s) \end{aligned}$$

where

$$T_i: \mathcal{Q}_i \longrightarrow \mathbb{R}^s, \quad T_i(\underline{x}) := (R^i)_\#(\underline{x}),$$

$$R := \begin{bmatrix} 0 & E_s \\ 1 & \underline{0} \end{bmatrix} \in GL(s+1; \mathbb{Z}).$$

Recalling the definition of T in Section 3, we see that $T = (R^{-1})_\#$, and $T^{-1}(\underline{x}) = T_i(\underline{x})$ ($\underline{x} \in \mathcal{Q}_i$). Hence, we have

$$T^{-1}(\underline{x}) = T_i(\underline{x}) \quad (\underline{x} \in \mathcal{Q}_i, \quad 1 \leq i \leq s).$$

We write

$$T^i(\underline{x}) := \frac{1}{\underline{x}}(i$$

as far as $T^i(\underline{x})$ is well-defined. Then, for any $\underline{x} \in \mathcal{Q} \setminus \{\underline{0}\}$, we may assume that $\underline{x} \in \mathcal{Q}_i$ for a number $1 \leq i \leq s$, and then, we can write

$$\underline{x} = T^i(T^{-i}(\underline{x})) = T^i(T_i(\underline{x})) = \frac{1}{T_i(\underline{x})}(i.$$

We set

$$\begin{aligned} [\underline{x}] &:= ^T([x_1], \dots, [x_s]) \in \mathbb{Z}^s, \\ \langle \underline{x} \rangle &:= \underline{x} - [\underline{x}] \in \mathcal{Q} \cup \{\underline{0}\}, \\ \sigma(\underline{x}) &:= \tau(\langle \underline{x} \rangle). \end{aligned}$$

for $\underline{x} = ^T(x_1, \dots, x_s) \in \mathbb{R}^s$. Now, we can define an algorithm of a continued fraction expansion for $\underline{x} \in \mathbb{R}^s$.

(Algorithm) For a given vector $\underline{x} \in \mathbb{R}^s$, we define $\underline{a}_n \in \mathbb{Z}^s$ by the following procedure:

*) $\underline{a}_n := [\sigma^n(\underline{x})]$ ($n \geq 0$) if $\langle \sigma^m(\underline{x}) \rangle \neq \underline{0}$ for all $0 \leq m < n$,
namely,

- 0) $\underline{a}_0 := \lfloor \underline{x} \rfloor$, $\underline{x}_0 := \langle \underline{x} \rangle (= \langle \sigma^0(\underline{x}) \rangle)$,
- 1) if $\underline{x}_0 \neq \underline{0}$, then choose $1 \leq \varepsilon_1 \leq s$ such that $\underline{x}_0 \in \mathbb{Q}_{\varepsilon_1}$,
and set $\underline{a}_1 := \lfloor T_{\varepsilon_1}(\underline{x}_0) \rfloor$, $\underline{x}_1 := \langle T_{\varepsilon_1}(\underline{x}_0) \rangle (= \langle \sigma^1(\underline{x}) \rangle)$,
- 2) if $\underline{x}_1 \neq \underline{0}$, then choose $1 \leq \varepsilon_2 \leq s$ such that $\underline{x}_1 \in \mathbb{Q}_{\varepsilon_2}$,
and set $\underline{a}_2 := \lfloor T_{\varepsilon_2}(\underline{x}_1) \rfloor$, $\underline{x}_2 := \langle T_{\varepsilon_2}(\underline{x}_1) \rangle (= \langle \sigma^2(\underline{x}) \rangle)$,
- ...
- n) if $\underline{x}_{n-1} \neq \underline{0}$, then choose $1 \leq \varepsilon_n \leq s$ such that $\underline{x}_{n-1} \in \mathbb{Q}_{\varepsilon_n}$,
and set $\underline{a}_n := \lfloor T_{\varepsilon_n}(\underline{x}_{n-1}) \rfloor$, $\underline{x}_n := \langle T_{\varepsilon_n}(\underline{x}_{n-1}) \rangle (= \langle \sigma^n(\underline{x}) \rangle)$,
- ...

We denote by $\varepsilon_n(\underline{x})$ the number determined above by the algorithm for a given $\underline{x} \in \mathbb{R}^s$. We say that the algorithm terminates iff there exists a number $n \geq 0$ such that $\langle \sigma^n(\underline{x}) \rangle = \underline{0}$. We can show the following

Proposition 2. (i) The algorithm terminates if and only if $\underline{x} \in \mathbb{Q}^s$.

(ii) Let $\underline{x} \in \mathbb{Q}^s$, and suppose

$$\langle \sigma^m(\underline{x}) \rangle \neq \underline{0} \text{ for all } 0 \leq m < n, \text{ and } \langle \sigma^n(\underline{x}) \rangle = \underline{0}.$$

Then

$$\underline{x} = {}^t(P_n \underline{e}_s) = (p_n^{(0)})^{-1} \cdot {}^t(p_n^{(1)}, \dots, p_n^{(s)}),$$

where

$$P_n = (p_{n-s+j}^{(i)})_{0 \leq i \leq s, 0 \leq j \leq s} \in GL(s+1; \mathbb{Z}),$$

$$P_n := A_0 S^{\varepsilon_1-1} A_1 S^{\varepsilon_2-1} A_2 \cdots S^{\varepsilon_n-1} A_n, \quad \varepsilon_n = \varepsilon_n(\underline{x}), \quad S := R^{-1},$$

$$A_m := \begin{bmatrix} {}^t \underline{0} & 1 \\ E_s & \underline{a}_m \end{bmatrix}, \quad \underline{a}_m := \lfloor \sigma^m(\underline{x}) \rfloor \quad (0 \leq m \leq n, \quad P_0 := A_0).$$

Proof. It is clear that $\underline{x} \in \mathbb{Q}^s$, if the algorithm terminates. We prove that the algorithm terminates for any $\underline{x} \in \mathbb{Q}^s$. Since the assertion is clear when $\langle \underline{x} \rangle = \underline{0}$, we suppose $\underline{x}_0 = \langle \underline{x} \rangle \in \mathbb{Q}^s \setminus \{\underline{0}\}$. Then we can set

$$\underline{x}_0 = (r_0^{(0)})^{-1} \cdot {}^t(r_0^{(1)}, \dots, r_0^{(s)}),$$

$$r_0^{(0)} \in \mathbb{Z}_{>0}, \quad {}^t(r_0^{(1)}, \dots, r_0^{(s)}) \in \mathbb{N}^s \setminus \{\underline{0}\},$$

$$\text{GCM}(r_0^{(0)}, r_0^{(1)}, \dots, r_0^{(s)}) = 1,$$

$$0 \leq r_0^{(i)} < r_0^{(0)} \quad (1 \leq i \leq s),$$

where $N := \{0, 1, 2, \dots\}$, $Z_{>0} := N \setminus \{0\}$. The number $r_0^{(0)}$ is referred to as the denominator of $\underline{x}_0 = \langle \underline{x} \rangle$, and denoted by $\text{den}(\underline{x}_0)$. We may suppose $\langle \underline{x} \rangle \in \mathcal{Q}_{\varepsilon_1}(1 \leq \varepsilon_1 \leq s)$.

Then

$$\begin{aligned} \sigma(\underline{x}) &= \tau(\langle \underline{x} \rangle) = T_{\varepsilon_1}(\langle \underline{x} \rangle) = T_{\varepsilon_1}(\underline{x}_0) \\ &= (r_0^{(\varepsilon_1)})^{-1} \cdot (r_0^{(\varepsilon_1+1)}, r_0^{(\varepsilon_1+2)}, \dots, r_0^{(s)}, r_0^{(0)}, r_0^{(1)}, \dots, r_0^{(\varepsilon_1-1)}). \end{aligned}$$

Hence, we get

$$\text{den}(\underline{x}_1) = \text{den}(\langle T_{\varepsilon_1}(\underline{x}_0) \rangle) \leq r_0^{(\varepsilon_1)} < \text{den}(\underline{x}_0).$$

Repeating the argument, we have

$$\text{den}(\underline{x}_0) > \text{den}(\underline{x}_1) > \dots > \text{den}(\underline{x}_n) \geq 1,$$

as far as $\langle \sigma^m(\underline{x}) \rangle \neq \underline{0}$ for all $0 \leq m < n$. Hence, $\text{den}(\underline{x}_n) = 1$ for a number n , i.e., $\underline{x}_n = \underline{0}$, which implies (i).

We prove (ii). We suppose $\langle \sigma^m(\underline{x}) \rangle \neq \underline{0}$ for all $0 \leq m < n$, and $\langle \sigma^n(\underline{x}) \rangle = \underline{0}$. Then, by the algorithm, we have

$$\underline{x} = \underline{a}_0 + \frac{1}{\underline{a}_1 + \frac{1}{\underline{a}_2 + \dots + \frac{1}{\underline{a}_n}}(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)} \quad (44)$$

On the other hand, for an s -tuple variables $\underline{\xi} = {}^T(\xi_1, \dots, \xi_s)$, we have

$$(A_m)_\#(S^{\varepsilon_m-1})_\#(\underline{\xi}) = \underline{a}_m + \frac{1}{\underline{\xi}}(\varepsilon_m,$$

which is an s -tuple of rational functions $\in \mathcal{Q}(\underline{\xi})^s$. Taking $\underline{\xi} := {}^T(0, \dots, 0, \xi^{-1})$ as in the proof of Lemma 6, we get by Lemma 5

$$\begin{aligned} \pi((P_n)_*(\kappa({}^T(\xi, 0, \dots, 0, 1)))) &= (\pi(P_n)_*\kappa)(1, 0, \dots, 0, \xi^{-1}) \\ &= (P_n)_\#(\underline{\xi}) = (A_0 S^{\varepsilon_1-1})_\#(A_1 S^{\varepsilon_2-1})_\# \dots (A_{n-1} S^{\varepsilon_n-1})_\#(A_n)_\#(\underline{\xi}). \end{aligned}$$

Hence, we get

$$\begin{aligned} &\pi((P_n)_*(\kappa({}^T(\xi, 0, \dots, 0, 1)))) \\ &= \underline{a}_0 + \frac{1}{\underline{a}_1 + \frac{1}{\underline{a}_2 + \dots + \frac{1}{\underline{a}_n + \frac{1}{\underline{\xi}}}}(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n)} \quad (45) \end{aligned}$$

Since $1/\underline{\xi} = T(\underline{\xi}) = \underline{\xi} \underline{e}_0$, setting $\xi=0$, we get by (44), (45) the identity

$$\underline{x} = \pi(P_n \underline{e}_s),$$

which implies the formula (ii). ■

Proposition 2 gives an algorithm to find a vector $\underline{b} \in \mathbb{Z}^s$ for any given vector $\underline{a} = {}^T(a_0, a_1, \dots, a_s) \in \mathbb{Z}^{s+1}$ with $\text{GCD}(a_0, a_1, \dots, a_s) = 1$. In fact, suppose such a vector $\underline{a}$ is given. Then, since $\underline{a} \neq \underline{0}$, we may suppose $a_0 \neq 0$, changing the order of $a_0, a_1, \dots, a_s$ if necessary. We put $\underline{x} := (a_0)^{-1} \cdot {}^T(a_1, \dots, a_s)$. Apply the algorithm of our continued fraction expansion for $\underline{x}$. Then it terminates. So, let P_n be as in Proposition 2. Then we have

$$(p_n^{(0)})^{-1} \cdot {}^T(p_n^{(1)}, \dots, p_n^{(s)}) = \pi(P_n \underline{e}_s) = \underline{x} = (a_0)^{-1} \cdot {}^T(a_1, \dots, a_s).$$

Since $P_n \in \text{GL}(s+1; \mathbb{Z})$, $\text{GCD}(p_n^{(0)}, p_n^{(1)}, \dots, p_n^{(s)}) = 1$, so that

$${}^T(p_n^{(0)}, p_n^{(1)}, \dots, p_n^{(s)}) = \varepsilon \cdot {}^T(a_0, a_1, \dots, a_s), \quad \varepsilon = \pm 1.$$

Hence, setting $\underline{b} = \varepsilon \delta \cdot {}^T(\tilde{p}_{0s}, \tilde{p}_{1s}, \dots, \tilde{p}_{ss})$ ($\delta := \det(P_n) = \pm 1$), we get ${}^T \underline{a} \cdot \underline{b} = 1$, where we mean by $\tilde{p}_{ij}$ the (i, j) -cofactor of the matrix P_n .

Using the fact mentioned above, we can show the following

Proposition 3. For any matrix $A = (a_{ij})_{0 \leq i \leq s, 0 \leq j \leq s} \in M(s+1; \mathbb{Z})$ such that $\text{GCD}(a_{0j}, \dots, a_{sj}) = 1$, we can construct a matrix $U = U(i) \in \text{GL}(s+1; \mathbb{Z})$ such that

$$U \underline{a}_{\underline{j}} = \underline{e}_i$$

for any $0 \leq i \leq s$. In particular, we can construct a matrix $U \in \text{GL}(s+1; \mathbb{Z})$ such that 1 is an eigenvalue of UA , and the vector $\underline{e}_i$ becomes an eigenvector with respect to the eigenvalue 1.

Proof. If necessary, we can exchange some of the row vectors of A , and we may assume that $a_{0j} \neq 0$. To be precise, we rewrite the vector $M \underline{e}_j$ ($M \in \text{GL}(s+1; \mathbb{Z})$) to be ${}^T(a_{0j}, \dots, a_{sj})$ so that $a_{0j} \neq 0$, and $\text{GCD}(a_{0j}, \dots, a_{sj}) = 1$. We can construct a matrix $P = P_n \in \text{GL}(s+1; \mathbb{Z})$ such that

$$P \underline{e}_s = {}^T(a_{0j}, \dots, a_{sj})$$

by applying the continued fraction algorithm for $(a_{0j})^{-1}(a_{1j}, \dots, a_{sj})$. We put

$$\underline{g} = {}^T(g_0, \dots, g_s) := \delta \cdot {}^T(\tilde{p}_{0s}, \dots, \tilde{p}_{ss}), \quad \delta := \det P,$$

where $P = (p_{ij})_{0 \leq i \leq s, 0 \leq j \leq s}$, and $\tilde{p}_{ij}$ is the (i, j) -cofactor of P . Then ${}^T \underline{g} \cdot \underline{a} = 1$. Now, we can construct a matrix $W \in \text{GL}(s+1; \mathbb{Z})$ such that

$$W_{\underline{e}_s} = \delta \cdot {}^T(\tilde{p}_{0s}, \dots, \tilde{p}_{ss}),$$

by applying the continued fraction algorithm for $(\tilde{p}_{0s})^{-1} \cdot {}^T(\tilde{p}_{1s}, \dots, \tilde{p}_{ss})$. Let L be the matrix obtained from TW by exchanging the final row (i.e., the s -th row) with the i -th row. Then ${}^T\underline{e}_i L M A \underline{e}_j = 1$. Hence, by sweeping out the j -th column of LMA with the (i, j) -component as a pivot, we get

$$KLMA \underline{e}_j = \underline{e}_i, \quad K \in GL(s+1; \mathbb{Z}),$$

which implies Proposition 2. ■

We remark that, in the proof given above, all the matrices K , L , and $M \in GL(s+1; \mathbb{Z})$ are effectively constructive for any given $A \in M(s+1; \mathbb{Z})$.

(c) For $a, \beta \in \mathbb{Q}_p$, we write

$$a \equiv \beta \pmod{p^e}$$

iff $|a - \beta|_p \leq p^{-e}$ ($e \in \mathbb{Z}$). We denote by $M(v, w; S)$ the set of matrices of size $v \times w$ with entries $\in S$, by $O^\times(F) := \{\varepsilon \in O(F); |\varepsilon|_p = 1\}$, the set of units in $O(F)$. We write

$$A \equiv B \pmod{p^e} \text{ for } A = (a_{ij}), B = (\beta_{ij}) \in M(v, w; O(F))$$

iff

$$a_{ij} \equiv \beta_{ij} \pmod{p^e} \text{ for all } 1 \leq i \leq v, 0 \leq j \leq w.$$

We note that, for $\underline{a}, \underline{\beta} \in \mathbb{Q}_p^{s+1}$,

$$\begin{aligned} \underline{a} \equiv \underline{\beta} \pmod{p^e} &\iff U\underline{a} \equiv U\underline{\beta} \pmod{p^e} \text{ for a matrix } U \in GL(s+1; O(F)) \\ &\iff {}^T\underline{a}V \equiv {}^T\underline{\beta}V \pmod{p^e} \text{ for a matrix } V \in GL(s+1; O(F)); \end{aligned}$$

and for $A, B \in M(s+1; \mathbb{Q}_p)$,

$$\begin{aligned} A \equiv B \pmod{p^e} &\iff UA \equiv UB \pmod{p^e} \text{ for a matrix } U \in GL(s+1; O(F)), \\ &\iff AV \equiv BV \pmod{p^e} \text{ for a matrix } V \in GL(s+1; O(F)), \end{aligned}$$

where $GL(s+1; O(F)) = \{U \in M(s+1; O(F)); \det U \in O^\times(F)\}$. We set

$$\Lambda_p := \begin{bmatrix} \underline{\lambda}_p \\ O_{s, s+1} \end{bmatrix} \in M(s+1; \mathbb{Z}[\lambda_p]),$$

where

$$\underline{\lambda}_p := {}^T(1, \lambda_p, \lambda_p^2, \dots, \lambda_p^s)$$

with λ_p as in Section 0. Then, we can write by Theorem 1

$$H(d^n C^{-n}) \equiv \Lambda_p \pmod{p^{e(p)n}} \text{ for } n \geq 0, p \in \text{Prime}(f(0)),$$

so that

$$d^n V_n C^{-n} \equiv \Lambda_p (p^{e(p)^n}),$$

where V_n is a matrix determined by

$$d^n V_n C^{-n} = H(d^n C^{-n}), \quad V_n \in GL(s+1; O(F)).$$

Hence,

$$d^n V_n C^{-n} U \equiv \Lambda_p U (p^{e(p)^n})$$

for any $U \in GL(s+1; O(F))$, namely

$$d^n W_n (U^{-1} C^{-1} U)^n \equiv \Lambda_p U (p^{e(p)^n}), \quad W_n := V_n U \in GL(s+1; O(F)). \quad (46)$$

Let $H_n^* \in M_0(s+1; \mathbb{Z})$ be the hermitian canonical form of the n -th power of the adjugate matrix of $U^{-1} C U$ for $C = C(f) \in M_0(s+1; \mathbb{Z})$. Then

$$H_n^* = d^n V_n^* (U^{-1} C U)^{-n} = d^n V_n^* (U^{-1} C^{-1} U)^n, \quad (47)$$

where $V_n^* \in GL(s+1; O(F))$ is a matrix determined by n . In view of (46), (47), we get

$$\begin{aligned} V_n^* &= d^{-n} H_n^* (U^{-1} C U)^n \equiv d^{-n} H_n^* (d^n U^{-1} \Lambda_p^{-1} W_n) = H_n^* U^{-1} \Lambda_p^{-1} W_n, \\ H_n^* &\equiv V_n^* W_n^{-1} \Lambda_p U (p^{e(p)^n}). \end{aligned}$$

Can we show (‡) by using (a), (c), and some of the arguments in the proofs of Lemmas 12-14?

Related to the continued fractions given in Theorem 2, and in Corollary 1, we have seen that they converge to

$$\underline{\theta}(p) = {}^T (c_0^{-1} \lambda_p, c_0^{-2} \lambda_p^2, \dots, c_0^{-s} \lambda_p^s) \in \mathbb{Q}_p^s \quad (48)$$

with respect to p -adic topology for all $p \in \text{Prime}(f(0))$; but, in general, they do not converge in $\mathbb{R}$, as we have mentioned in Remark 7. The convergence in $\mathbb{R}$ depends on the distribution of the zeros of the polynomial f on the complex plane $\mathbb{C}$. We can show that the continued fractions converge to

$$\underline{\theta}(\infty) = {}^T (c_0^{-1} a, c_0^{-2} a^2, \dots, c_0^{-s} a^s) \in \mathbb{R}^s,$$

which is obtained by taking $\lambda_\infty := a \in \mathbb{R}$ instead of λ_p in $\underline{\theta}(p)$ given by (48), for f possibly not satisfying (1) but satisfying the following condition (¶):

(¶) f is irreducible, has a real root a , and $|a| < |\beta|$ for all the roots $\beta \in \mathbb{C}$ of f different from a .

Such a result may be given in a forthcoming paper. Notice that if a^{-1} is a Perron number and if f is its minimal polynomial then (¶) follows. Probably the

irreducibility in (¶) is not essential, but the primitivity of $C(f)$ may be essential. Recall that the irreducibility of f in $\mathbb{Z}[x]$ is independent of the convergence of the p -adic values of our continued fractions.

References

- [1] N. Koblitz, p -adic Numbers, p -adic Analysis, and Zeta-functions, Springer-Verlag, New York, Heidelberg, Berlin, 1977.
- [2] J.-I. Tamura, Certain partition of a lattice, J.-M. Gambaudo (ed.) et al., Dynamical Systems, From crystal to chaos, Proceedings of the conference in honor of Gérard Rauzy on his 60-th birthday (Luminy Marseille, France, July 6-10, 1998), World Scientific, Singapore, 2000, 199-219.
- [3] _____, Certain words, tilings, their nonperiodicity, and substitutions of high dimension, Ch. Jia (ed.) et al., Analytic Number Theory, the joint Proceedings of the China-Japan Number Theory Conference (Beijing/Kyoto, 1999), Dev. Math., 6, Kluwer Acad. Publ., Dordrecht, 2002, 303-348.
- [4] _____, Certain word and tiling of high dimension, p -adic phenomenon, Analytic number theory and related topics (Kyoto, 1999), (Japanese) *Surikaiseikikenkyūsho Kōkyūroku* No. 1160 (2000), 40-60.