Annales Univ. Sci. Budapest., Sect. Comp. 18 (1999) 103-107

CONSTRUCTION OF NUMBER SYSTEMS IN ALGEBRAIC NUMBER FIELDS

I. Kátai (Budapest/Pécs, Hungary)

To the memory of Imre Környei
To the memory of Béla Kovács

1. Let Γ be an algebraic number of degree n, with conjugates $\Gamma^{(1)} = \Gamma, \Gamma^{(2)}, \dots, \Gamma^{(n)}$. Let $\mathcal{I}^{(j)}$ be the set of integers of $Q(\Gamma^{(j)})$, $\mathcal{I} = \mathcal{I}^{(1)}$.

Let $\alpha \in \mathcal{I}$, and $\mathcal{F}$ be a complete residue system *mod* α, such that $0 \in \mathcal{F}$.

Definition 1. We say that $(\mathcal{F}, \alpha)$ is a number system (NS) in $\mathcal{I}$, if each $\beta \in \mathcal{I}$ can be expanded as a finite sum of form

$$\beta = e_0 + e_1\alpha + \dots + e_k\alpha^k, \qquad e_j \in \mathcal{F} \quad (j = 0, \dots, k). \tag{1.1}$$

Remark. The uniqueness of the expansion is obvious, since e_0 is determined by β (mod α), etc.

2. For each $h \in Q(\Gamma)$ let $h^{(j)}$ be its jth conjugate, and for any $I \subseteq Q(\Gamma)$ let $I^{(j)} = \{h^{(j)} \mid h \in I\}$. For an arbitrary $\mathcal{F}$ complete residue system *mod* α let the mapping $J : I \to \mathcal{I}$ be defined as follows.

For each $\beta \in \mathcal{I}$ let e_0 be the coefficient (= element of $\mathcal{F}$) for which α is a divisor of $\beta - e_0$, and let $\beta_1 = \frac{\beta - e_0}{\alpha}$. Then $J(\beta) := \beta_1$.

From now on we shall assume that $|\alpha^{(j)}| > 1$ $(j = 1, \dots, n)$. Let

$$K_j = \max_{f^{(j)} \in \mathcal{F}^{(j)}} |f^{(j)}|, \qquad L_j = \frac{K_j}{|\alpha^{(j)}| - 1}.$$

Lemma 1. *We have*

$$(i) \qquad |J(\gamma)| < |\gamma| \quad \text{if} \quad |\gamma| > L_1.$$

$$(ii) \qquad \text{If} \quad |\gamma| \le L_1, \quad \text{then} \quad |J(\gamma)| \le L_1.$$

Proof. Clear.

We can extend the domain of J for $I^{(j)}$ defining it by $J(\beta^{(j)}) = \beta_1^{(j)}$ $(= J(\beta)^{(j)})$.

Lemma 2. *Let $\mathcal{K}$ $(\subseteq \mathcal{I})$ be the set of those $\gamma \in \mathcal{I}$ for which*

$$|\gamma^{(j)}| \le L_j \qquad (j = 1, \dots, n)$$

simultaneously holds. Then $\mathcal{K}$ is a finite set.

Proof. Well known.

For each $\beta \in \mathcal{I}$ let us consider the path

$$\beta,\ \ \beta_1 = J(\beta),\ \ \beta_2 = J^2(\beta),\ \ \beta_3 = J^3(\beta), \dots \tag{2.1}$$

generated by iterating the mapping J. If we iterate $\beta^{(j)}$ according to J, then obviously we obtain

$$\beta^{(j)},\ \ \beta_1^{(j)} = J(\beta^{(j)}),\ \ \beta_2^{(j)} = J^2(\beta^{(j)}), \dots \tag{2.1$_j$}$$

The sequence $\beta, \beta_1, \beta_2, \dots$ may contain only finitely many elements outside $\mathcal{K}$ (if any), (see Lemma 1), and so it is ultimately periodic (see Lemma 2).

Definition 2. The element $\pi \in \mathcal{I}$ is said to be periodic with respect to the expansion $(\mathcal{F}, \alpha)$ if there exists a positive integer k such that $J^{(k)}(\pi) = \pi$.

Let $\mathcal{P}$ be the set of periodic elements, and let $G(\mathcal{P})$ be the directed graph getting by directing an edge from π to $J(\pi)$, for each $\pi \in \mathcal{P}$.

Lemma 3. *(1) $\mathcal{P}$ is a finite set. If $\pi \in \mathcal{P}$, then*

$$|\pi^{(j)}| \le L_j \qquad (j = 1, \dots, n). \tag{2.2}$$

(2) $G(\mathcal{P})$ is the union of disjoint directed circles (loops are allowed).
(3) $(\mathcal{F}, \alpha)$ is a number system in I, if and only if $\mathcal{P} = \{0\}$.

Proof. (1) is a direct consequence of Lemma 1, (2), (3) are obvious.

3. Let us fix an integer basis $\omega_1, \dots, \omega_n$ in $Q(\Gamma)$. Let

$$\Delta_j := |\omega_1^{(j)}| + \dots + |\omega_n^{(j)}|. \tag{3.1}$$

Let $\tau = \alpha_1 \alpha_2 \dots \alpha_n$, $t = |\tau|$. Then $O(I/\alpha I) = t$, thus the size of a complete residue system *mod* α is t. Let $H = \{h_0, h_1, \dots, h_{t-1}\}$ be a complete residue system *mod* α. Then for arbitrary choice of $g_j \in I$, the set $\mathcal{F} = \{f_0, \dots, f_{t-1}\}$

defined by $f_j = h_j + \alpha g_j$ $(j = 0, \dots, t-1)$ is a complete residue system as well. Then

$$\alpha^{(2)} \dots \alpha^{(2)} f_j = \alpha^{(2)} \dots \alpha^{(n)} h_j + \tau g_j. \tag{3.2}$$

Since g_j can be chosen from the set $k_1\omega_1 + \dots + k_n\omega_n$, $k_j \in \mathbb{Z}$, therefore we can always find such an f_j for which

$$\alpha^{(2)} \dots \alpha^{(n)} f_j = T_{1,j}\omega_1 + \dots + T_{n,j}\omega_n \tag{3.3}$$

satisfies

$$-\frac{t}{2} < T_{i,j} \leq \frac{t}{2}, \qquad i = 1, \dots, n; \quad j = 0, \dots, t-1.$$

Let $\mathcal{F}_0$ be the so constructed set of digits. Observe that $f_0 = 0$. Hence we deduce that

$$|\alpha^{(2)} \dots \alpha^{(n)}||f_j| \leq \frac{t}{2}\Delta_1,$$

i.e.

$$|f_j| \leq \frac{|\alpha^{(1)}|}{2}\Delta_1.$$

Observing that the "conjugate equations"

$$\frac{\tau}{\alpha^{(\ell)}} f_j^{(\ell)} = T_{1,j}\omega_1^{(\ell)} + \dots + T_{n,j}\omega_n^{(\ell)}$$

lead to

$$|f_j^{(\ell)}| \leq \frac{|\alpha^{(\ell)}|}{2}\Delta_\ell \qquad (\ell = 1, \dots, n) \tag{3.4}$$

we can get a good estimation for the elements of $\mathcal{P}$ corresponding to the expansion defined by $(\mathcal{F}_0, \alpha)$, at least in the case if $|\alpha^{(\ell)}|$ are all large enough.

Let $\pi \in \mathcal{P}$. Then

$$\pi = e_0 + e_1\alpha + \dots + e_{k-1}\alpha^{k-1} + \alpha^k\pi, \qquad e_j \in \mathcal{F}_0 \tag{3.5}$$

and

$$\pi^{(\ell)} = e_0^{(\ell)} + e_1^{(\ell)}\alpha^{(\ell)} + \dots + e_{k-1}^{(\ell)}(\alpha^{(\ell)})^{k-1} + (\alpha^{(\ell)})^k\pi^{(\ell)}. \tag{3.6}$$

From (3.6), (3.4) we obtain that

$$|\pi^{(\ell)}| \leq \frac{\Delta_\ell}{2\left(1 - \frac{1}{|\alpha^{(\ell)}|}\right)} \qquad (\ell = 1, \dots, n). \tag{3.7}$$

4. **Theorem.** *Assume that* $|\alpha^{(\ell)}| > \max(2, 2\Delta_\ell)$ $(\ell = 1, \dots, n)$. *Let* $\mathcal{F}(\subseteq \mathcal{I})$ *be the set of those integers* γ *in* I *for which*

$$|\gamma^{(\ell)}| \le \Delta_\ell \qquad (\ell = 1, \dots, n) \tag{4.1}$$

holds. Then the elements of $\mathcal{F}$ *are incongruent mod* α. *Let* $\mathcal{F}_1$ *be the coefficient set getting from* $\mathcal{F}_0$ *by substituting* $f \in \mathcal{F}_0$ *with that* $\gamma \in I$, *for which* $f \equiv \gamma$ *(mod* α*), if such an element exists. Then* $(\mathcal{F}_1, \alpha)$ *is a NS.*

Proof. Assume that there exists $\gamma_1, \gamma_2 \in I$, $\gamma_1 \ne \gamma_2$ for which $\gamma_1 - \gamma_2 \equiv$ $\equiv 0 \pmod{\alpha}$. Then $\gamma_1 - \gamma_2 = \alpha\eta$, $\eta \in I$, furthermore $\gamma_1^{(\ell)} - \gamma_2^{(\ell)} = \alpha^{(\ell)}\eta^{(\ell)}$. Since $|\gamma_1^{(\ell)} - \gamma_2^{(\ell)}| \le 2\Delta_\ell$, therefore $|\eta^{(\ell)}| < \frac{2\Delta_\ell}{|\alpha^{(\ell)}|} < 1$, consequently $|\prod \eta^{(\ell)}| < 1$. Since η is an algebraic integer, therefore its norm is a rational integer, it cannot be satisfied.

Thus $\mathcal{F}^{(1)}$ is a complete residue system *mod* α, for the elements $\tilde{f}$ of which

$$|\tilde{f}^{(\ell)}| \le \frac{|\alpha^{(\ell)}|\Delta_\ell}{2} \tag{4.3}$$

holds.

Let $\tilde{\mathcal{P}}$ be the set of periodic elements with respect to the expansion $(\mathcal{F}_1, \alpha)$. Repeating the estimations which were done in Section 3, for $\tilde{\pi} \in \tilde{\mathcal{P}}$ we obtain that

$$|\tilde{\pi}^{(\ell)}| \le \Delta_\ell \qquad (\ell = 1, \dots, n), \tag{4.4}$$

i.e. $\tilde{\pi} \in I$. But $\tilde{\pi} \in I$ implies that $\tilde{\pi}$ is a digit, $J(\tilde{\pi}) = 0$, consequently $\mathcal{P} = \{0\}$. The proof is completed.

5. The exact characterization of those α algebraic integers for which $(\mathcal{F}, \alpha)$ is a NS with a suitable digit set $\mathcal{T}$ seems to be hard.

It is clear that both of the conditions

$$1) \quad |\alpha^{(j)}| > 1 \qquad (j = 1, \dots, n),$$
$$2) \quad 1 - \alpha^{(j)} \ne \text{unit}$$

are necessary.

G.Steidl [1] for $\mathbb{Q}(i)$, I.Kátai [2] for imaginary quadratic extension fields proved that 1) and 2) are also sufficient. G.Farkas [3] proved that if α belongs to a real quadratic extension field such that $|\alpha^{(1)}| > 2$, $|\alpha^{(2)}| > 2$, then $(\mathcal{F}, \alpha)$ is a NS with a suitable $\mathcal{F}$.

References

[1] **Steidl G.**, On symmetric representation of Gaussian integers, *BIT*, **29** (1989), 563-571.

[2] **Kátai I.**, Number systems in imaginary quadratic fields, *Annales Univ. Sci. Bud. Sect. Comp.*, **14** (1994), 91-103.

[3] **Farkas G.**, Number systems in real quadratic fields, *Annales Univ. Sci. Bud. Sect. Comp.*, **18** (1999), 47-59.

I. Kátai
Department of Computer Algebra
Eötvös Loránd University
P.O.B. 32
H-1518 Budapest, Hungary

Department of Applied Mathematics
Janus Pannonius University
Ifjúság u. 6.
H-7624 Pécs, Hungary