

On number systems in algebraic number fields

By I. KÁTAI (Budapest) and I. KÖRNYEI (Budapest)

1. Let θ be an algebraic integer with minimal polynomial $p(x) = (x - \theta_1) \cdots (x - \theta_n)$, $\theta = \theta_1$ over $\mathbf{Q}$. Assume that $|\theta_i| > 1$ holds for every $i = 1, \dots, n$; let $\kappa = \max 1/|\theta_i|$. Let $\rho_j = \theta_j^{-1}$ ($j = 1, \dots, n$). Let $A = \{a_0 = 0, a_1, \dots, a_{t-1}\}$ be a full residue system mod θ , $A \subseteq \mathbf{Z}[\theta]$. Let $A^{(j)}$ be the conjugate sets, $A^{(j)} = \{a_0(\theta_j) = 0, a_1(\theta_j), \dots, a_{t-1}(\theta_j)\}$. Assume that $\theta_1, \dots, \theta_{2r} \in \mathbf{C} \setminus \mathbf{R}$; $\theta_{2r+1}, \dots, \theta_{2r+s} \in \mathbf{R}$, $n = 2r + s$, so ordered that $\theta_{r+l} = \bar{\theta}_l$ ($l = 1, \dots, r$). Let $K_n = K_n^{(r,s)}$ be the set of those vectorials $\tilde{z}$, the i th coordinate of which is denoted by z_i such that $z_1, \dots, z_{2r} \in \mathbf{C}$, $z_{r+l} = \bar{z}_l$ ($l = 1, \dots, r$), $z_{2r+1}, \dots, z_{2r+s} \in \mathbf{R}$. It is a linear normed space with $\|\tilde{z}\| = \max |z_j|$. λ will denote the Lebesgue measure in K_n , defined as $dx_1 dy_1 \cdots dx_r dy_r dz_{2r+1} \cdots dz_{2r+s}$. For an arbitrary $\alpha \in \mathbf{Z}[\theta]$ let $\tilde{\alpha} \in K_n$ the vectorial, the j th coordinate of which is $\alpha(\theta_j)$.

For every $\alpha \in \mathbf{Z}[\theta]$ there exists a unique $b_0 \in A$ and $\alpha_1 \in \mathbf{Z}[\theta]$ such that

$$(1.1) \quad \alpha = \alpha_1 \theta + b_0.$$

(1.1) implies the fulfilment of

$$(1.2) \quad \alpha(\theta_j) = \alpha_1(\theta_j)\theta_j + b_0(\theta_j) \quad (j = 1, \dots, n).$$

Let $J : \mathbf{Z}[\theta] \rightarrow \mathbf{Z}[\theta]$ be the function defined by $J(\alpha) = \alpha_1$. Let $T(\alpha) = \max_j |\alpha(\theta_j)|$, $K = \max_{b \in A} \max_{j=1, \dots, n} |b(\theta_j)|$. From (1.2) we have

$$(1.3) \quad T(\alpha_1) \leq \kappa T(\alpha) + \kappa K.$$

Since $T(\alpha) \leq C$ can be satisfied only for finitely many elements $\alpha \in \mathbf{Z}[\theta]$, and $\kappa < 1$, therefore the sequence $\alpha, \alpha_1, \alpha_2, \dots$ is ultimately periodic, where in general, α_{k+1} is defined as

$$\alpha_k = \alpha_{k+1}\theta + b_k, \quad b_k \in A.$$

An element $\beta \in \mathbf{Z}[\theta]$ is called to be (purely) periodic with respect to (θ, A) if the sequence $J^k(\beta)$ ($k = 0, 1, \dots$) is periodic, i.e. for some $l > 0$, $J^l(\beta) = \beta$. Let S be the set of all periodic elements.

One can see easily that S is a finite set, moreover that

$$(1.4) \quad (E :=) \max_{\beta \in S} T(\beta) \leq \frac{\kappa}{1 - \kappa} K.$$

Indeed, if $\beta \in S$ is such an element for which $E = T(\beta)$, and $J^l(\beta) = \beta$, by using (1.3) with $\alpha_1 = \beta_l = \beta$, $\alpha = \beta_{l-1}$, we have

$$E = T(\beta_l) \leq \kappa T(\beta_{l-1}) + \kappa K \leq \kappa E + \kappa K,$$

which implies (1.4) immediately.

We define the directed graph $G(S)$ as follows: the nodes of it are the elements of S ; for every $\alpha \in S$ an edge is directed from α to $J(\alpha)$ and it is labelled by b , if $\alpha = \alpha_1\theta + b$, $b \in A$, $\alpha = J(\alpha)$.

It is clear that $G(S)$ is a union of disjoint directed circles. Furthermore, $\alpha \in S$ if there exists some $k \geq 0$ and $b_0, \dots, b_{k-1} \in A$ such that

$$\alpha = b_0 + b_1\theta + \dots + b_{k-1}\theta^{k-1} + \theta^k\alpha.$$

For some $\eta \in \mathbf{Z}[\theta]$ let $l(\eta)$ be the smallest integer k for which $J^k(\eta) \in S$.

Let $\alpha \in \mathbf{Z}[\theta]$, $\alpha_j = \alpha_{j+1}\theta + b_j$, $b_j \in A$ ($j = 0, \dots, k-1$), $\alpha_0 = \alpha$, and $l(\alpha) = k$. Then the sequence $b_0, \dots, b_{k-1}$, and $\alpha_k \in S$ allow to compute α ,

$$(1.5) \quad \alpha = b_0 + b_1\theta + \dots + b_{k-1}\theta^{k-1} + \theta^k\alpha_k.$$

We say that this is the regular expansion of α . Given $c_0, \dots, c_{s-1} \in A$, $\gamma \in S$, and consider the expansion

$$(1.6) \quad c_0 + c_1\theta + \dots + c_{s-1}\theta^{s-1} + \theta^s\gamma (= \eta).$$

It is the regular expansion of η , if and only if $c_{s-1} + \theta\gamma \notin S$.

For the regular expansion of (1.6) we shall use the notation $\eta = [c_0, \dots, c_{s-1} | \gamma]$. If $\eta \in S$, we shall write $\eta = [\emptyset | \eta]$.

Lemma 1. *There is a constant c depending only on θ and A such that*

$$(1.7) \quad \left| l(\alpha) - \max_{j=1, \dots, n} \frac{\log |\alpha(\theta_j)|}{\log |\theta_j|} \right| \leq c,$$

if $\alpha \neq 0$.

PROOF. By using (1.1), (1.2) and their iterates, we have

$$\alpha_k(\theta_j) = \alpha(\theta_j)\rho_j^k - \sum_{l=0}^{k-1} b_l(\theta_j)\rho_j^{k-l}.$$

Since the sum on the right hand side is bounded by $\frac{K\kappa}{1-\kappa}$, we get

$$(1.8) \quad |\alpha_k(\theta_j) - \alpha(\theta_j)\rho_j^k| \leq \frac{K\kappa}{1-\kappa}.$$

Let C be such a large constant for which

$$\max_{\beta \in S} T(\beta) < C, \quad C > 2K \frac{\kappa}{1-\kappa}$$

holds true. Then $l(\alpha)$ is at least so large as the least k for which $J^k(\alpha) < C$ is satisfied, consequently the lower estimate for $l(\alpha)$ given in (1.7) is true.

Let $k(\alpha)$ be the least integer k for which

$$\max_{j=1, \dots, n} |\alpha(\theta_j) \cdot \rho_j^k| < \frac{K\kappa}{1-\kappa}.$$

Thus

$$k(\alpha) \leq \max_j \frac{\log |\alpha(\theta_j)|}{\log |\theta_j|} + c_1$$

is true, with a suitable positive constant c_1 . Furthermore $T(\alpha_m) < C$ holds for every $m \geq k$. Let $N(C) = \text{card } \{\beta \in \mathbf{Z}[\theta], T(\beta) < C\}$. Then $l(\alpha) \leq k(\alpha) + N(C)$, and the upper estimate for $l(\alpha)$ in (1.7) is true.

If $\gamma \in S$,

$$\gamma = c_s + c_{s+1}\theta + \dots + c_{s+k-1}\theta^{k-1} + \theta^{k\gamma}$$

and

$$(1.9) \quad \begin{aligned} \eta &= c_0 + c_1\theta + \dots + c_{s-1}\theta^{s-1} + \theta^s (c_s + c_{s+1}\theta + \dots + c_{s+k-1}\theta^{k-1}) + \\ &\quad + \theta^{s+k} (c_s + c_{s+1}\theta + \dots + c_{s+k-1}\theta^{k-1}) + \theta^{s+2k}\gamma = \\ &= \dots \\ &= \xi_u + \eta_u, \end{aligned}$$

where $\xi_u = \sum_{s=0}^{u-1} c_s \theta^s$ and η_u is divisible by θ^u .

2. If $S = \{0\}$, then (θ, A) is said to be a number system (NS). If $A = A_0 = \{0, 1, \dots, |N(\theta)| - 1\}$ in additionally then (θ, A_0) is said to be a canonical number system (CNS). All the possible CNS were given for Gaussian integers by I. KÁTAI and J. SZABÓ [2], for quadratic extension field by I. KÁTAI and B. KOVÁCS [3], [4], and independently by W. GILBERT [1], for $\mathbf{Q}(\sqrt[3]{2})$ by S. KÖRMENDI [5].

W. GILBERT observed some nice geometric properties of the sets

$$H = \{Z \mid Z = \sum_{j=1}^{\infty} b_j \theta^{-j}; \quad b_j \in A_0\}$$

in imaginary quadratic extensions.

3. Theorem 1. Assume that the conditions stated for (θ, A) in section 1 are satisfied. Let $H \subseteq K_n$ be the set of those z , for which there exists an infinite sequence of elements $b_1(\theta), b_2(\theta), \dots \in A$, such that

$$(3.2) \quad z_j = \sum_{m=1}^{\infty} b_m(\theta_j) \rho_j^m \quad (j = 1, \dots, n)$$

hold.

Then

- (i) H is a compact set,
- (ii) $\bigcup_{\alpha \in Z[\theta]} \{H + \alpha\} = K_n$,

furthermore, if (θ, A) is a number system, then

$$(iii) \quad \lambda((H + \gamma_1) \cap (H + \gamma_2)) = 0$$

for every $\gamma_1, \gamma_2 \in Z[0]$, $\gamma_1 \neq \gamma_2$, and if A denotes the linear mapping $K_n \rightarrow K_n$ acting as $z_j \rightarrow \theta_j z_j$ ($j = 1, \dots, n$), then

$$(iv) \quad A^l H = \bigcup_{\gamma} (H + \gamma)$$

where γ runs over those elements of $Z[\theta]$ which have the form $\gamma = \sum_{m=0}^{l-1} b_m \theta^m$, $b_m \in A$.

PROOF. Assertion (i) is clear. A detailed proof is given in [2] in the case of Gaussian integers.

Let $e = 1$. Then $\theta^j = A^j e$ ($j = 0, 1, \dots, n-1$). These vectorials are independent in K_n , since the matrix composed from them is of a Vandermonde type with distinct generating elements, $\theta_1, \dots, \theta_n$.

Since every integer $\alpha \in \mathbf{Z}[\theta]$ can be uniquely written as $\alpha = d_0 + d_1\theta + \dots + d_{n-1}\theta^{n-1}$, $d_\nu \in \mathbf{Z}$, therefore $M = \{\alpha \mid \alpha \in \mathbf{Z}[\theta]\}$ form a lattice with the basis vectors θ^j ($j = 0, \dots, n-1$) in K_n .

Let $z \in K_n$, $z \neq 0$. We let T to run over the set of positive integers. Consider $A^T z$. Then it can be approximated with a suitable $\alpha_T \in M$ such that $|A^T z - \alpha_T| < c$, i.e.

$$(3.3) \quad |\theta_j^T z_j - \alpha_T(\theta_j)| < c \quad (j = 1, \dots, n)$$

Then $\alpha_T(\theta)$ has a regular expansion,

$$(3.4) \quad \alpha_T(\theta) = c_0^{(T)} + c_1^{(T)}\theta + \dots + c_{s-1}^{(T)}\theta^{s-1} + \theta^s \gamma_T,$$

where $c_j^{(T)} \in A$, $\gamma_T \in S$ and s depends on T . From Lemma 1 we have that $l(\alpha) \leq T + R$, where R is a suitable integer which does not depend on T . It may depend on z . Applying the algorithm (1.1) ($\alpha \rightarrow \alpha_1$) $T + R - s$ times,

$$\gamma_T = c_s^{(T)} + c_{s+1}^{(T)}\theta + \dots + c_{T+R}^{(T)}\theta^{T+R-s-1} + \theta^{T+R-s+1}\gamma_T^*,$$

where $\gamma_T^* \in S$, $c_\nu^{(T)} \in A$ ($\nu = s, \dots, T + R$).

Consequently

$$\alpha_T(\theta_j) = \sum_{m=0}^{T+R} c_m^{(T)}(\theta_j)\theta_j^m + \gamma_T^*(\theta_j)\theta_j^{T+R+1} \quad (j = 1, \dots, n).$$

Thus, from (3.3) we have

$$(3.5) \quad z_j = \rho_j^T \alpha_T(\theta_j) + \omega_j^{(T)} \quad (j = 1, \dots, n),$$

where $\omega_j^{(T)} \rightarrow 0$ as $T \rightarrow \infty$, furthermore from (1.9)

$$(3.6) \quad \rho_j^T \alpha_T(\theta_j) = \sum_{h=-T}^{-1} c_{T+h}^{(T)}(\theta_j)\theta_j^h + \eta_T^*(\theta_j)\theta_j^{-T}.$$

Since

$$(3.7) \quad \eta_T^*(\theta_j)\rho_j^T \in Z(\theta_j)$$

may take only on finitely many values, therefore there exists an $\alpha(\theta_j)$ which occurs as the value of (3.7) for infinitely many values of T .

Let us keep only those T for which

$$(3.8) \quad Z_j = \sum_{h=-T}^{-1} c_{T+h}^{(T)}(\theta_j) \theta_j^h + \alpha(\theta_j)$$

holds. Then there is an infinite subsequence of these T values for which some $d_{-1} \in A$ occurs as $c_{T-1}^{(T)}$ infinitely often. Continuing this process ad infinitum, we obtain that

$$z_j = \alpha(\theta_j) + \sum_{l=1}^{\infty} d_{-l}(\theta_j) \cdot \rho_j^l \quad (j = 1, \dots, n)$$

holds with some $\alpha \in \mathbf{Z}[\theta]$, $d_{-l} \in A$ ($l = 1, 2, \dots$). This proves (ii).

Assume now that (θ, A) is a NS. The fulfilment of (iv) is clear. From (ii) we have $\lambda(H) = \lambda(H + \alpha) > 0$. We have $\text{card}(A) = |\theta_1 \dots \theta_n| = |N(\theta)|$, furthermore that $\lambda(A^l H) = |N(\theta)|^l \lambda(H)$. There exist exactly $|N(\theta)|^l$ distinct γ occuring on the right hand side of (iv). Thus

$$(3.9) \quad |N(\theta)|^l \lambda(H) = \lambda(A^l H) = \lambda(\cup(H + \gamma)) \leq \sum \lambda(H + \gamma)$$

and equality holds if and only if

$$(3.10) \quad \lambda((H + \gamma_1) \cap (H + \gamma_2)) = 0$$

is satisfied for all pairs of $\gamma_1 \neq \gamma_2$ occuring in (iv). Since the right most side of (3.9) equals $|N(\theta)|^l \lambda(H)$, and l can be chosen to be arbitrarily large, therefore (3.10) is true for all $\gamma_1, \gamma_2 \in \mathbf{Z}[\theta] \mid \gamma_1 \neq \gamma_2$. This completes the proof of our theorem.

References

- [1] W. GILBERT, Radix representations of quadratic fields, *J. Math. Anal. and Appl.* **83** (1981), 264–274.
- [2] I. KÁTAI AND J. SZABÓ, Canonical number systems for complex integers, *Acta Sci. Math. (Szeged)* **37** (1975), 255–260.
- [3] I. KÁTAI AND B. KOVÁCS, Canonical number systems in imaginary quadratic field, *Acta Math. Acad. Sci. Hung.* **37** (1981), 159–164.
- [4] I. KÁTAI AND B. KOVÁCS, Kanonische Zahlensysteme in der Theorie der quadratischen Zahlen, *Acta Sci. Math. (Szeged)* **42** (1980), 99–107.
- [5] J. KÖRMENDI, Canonical number systems in $\mathbf{Q}(\sqrt[3]{2})$, *Acta Sci. Math.* **37** (1975), 255–260.

I. KÁTAI AND I. KÖRNYEI
 EÖTVÖS LORÁND UNIVERSITY
 COMPUTER CENTER
 H-1117 BUDAPEST
 BOGDÁNFY ÚT 10/B.

(Received September 20, 1991)