Integral domains with canonical number systems

By B. KOVÁCS* (Debrecen)

Dedicated to Professor Zoltán Daróczy on his 50th birthday

1. Introduction

Let R be an integral domain (with identity), $\alpha \in R$ and $\mathcal{N}_0 = \{0, 1, \ldots, m\}$ for some positive integer m. We shall say that $\{\alpha, \mathcal{N}_0\}$ is a *canonical number system,* if every $\gamma \in R$ can be uniquely represented as

(1.1)
$$\gamma = a_0 + a_1\alpha + \ldots + a_k\alpha^k, \quad \text{where} \quad a_i \in \mathcal{N}_0 \quad \text{for} \quad i = 0, 1, \ldots, k, \; a_k \neq 0 \quad \text{if} \quad k \neq 0.$$

(The unit element of R will be identified with 1.) The question of determining all the canonical number systems in the ring of Gaussian integers was raised by I. KÁTAI and J. SZABÓ and has been completely solved by them in [1]. The same question has been answered in [2], [3], [4] for the rings of integers of quadratic number fields. In [5], a necessary and sufficient condition has been given for the existence of a canonical number system in the ring of integers of an arbitrary algebraic number field.

The aim of this paper is to provide a complete description of integral domains having a canonical number system. Using some ideas of [5], we shall first give a complete characterization of integral domains R of characteristic 0 which have a canonical number system. Namely, we shall prove the following theorem:

Theorem 1. *Let R be an integral domain of characteristic* 0. *In R there exists a canonical number system if and only if*

$$R \cong \mathbf{Z}[\alpha]$$

for some element α which is algebraic over $\mathbf{Q}$[1]).

For integral domains of characteristic p (p prime) we have the following

Theorem 2. *Let R be an integral domain of characteristic $p > 0$. In R there exists a canonical number system if and only if*

$$R \cong (\mathbf{Z}/p \cdot \mathbf{Z})[x].$$

---

* Research supported in part by Grants 273 and 400 from the Hungarian National Foundation for Scientific Research.

[1]) $\mathbf{Z}$ and $\mathbf{Q}$ denote the ring of rational integers and the field of rational numbers, respectively.

Remark. Let R be a ring with unit element. Then the notion of canonical number system can be defined in a similar way. If R has a canonical number system, then R is commutative because it is generated by one element. One can show in the same way as in case of Theorem 1 that if the additive order of the unit element of R is infinite then the assertion of Theorem 1 remains valid for R.

2. Proofs

PROOF OF THEOREM 1.

1. First suppose that R has a canonical number system $\{\alpha, \mathcal{N}_0\}$ where $\alpha \in R$ and $\mathcal{N}_0 = \{0, 1, \ldots, m\}$ for some positive integer m. Then obviously $R = \mathbf{Z}[\alpha]$. Further we can write $m+1$ in the form

$$m+1 = a_0 + a_1\alpha + \ldots + a_t\alpha^t \quad \text{where} \quad a_i \in \mathcal{N}_0, \quad 0 \leqq i \leqq t.$$

This implies that α is a root of a polynomial with integral coefficients, i.e. α is an algebraic element over $\mathbf{Q}$.

2. Now assume that $R \cong \mathbf{Z}[\alpha]$ for some α which is algebraic over $\mathbf{Q}$. We shall show that there exists a canonical number system in $\mathbf{Z}[\alpha]$. Let $P(x) = a_n x^n + \ldots + a_1 x + a_0$ be an irreducible polynomial with integral coefficients such that $P(\alpha) = 0$ and $a_n > 0$.

Since $a_n > 0$, it is easy to see that there exists an integer $N_0 \geqq 0$ such that, for every integer $N > N_0$, the coefficients of the polynomial $P(x+N) = b_n x^n + \ldots + b_1 x + b_0$ satisfy

$$0 < b_n \leqq b_{n-1} \leqq \ldots \leqq b_1 \leqq b_0 \quad \text{and} \quad b_0 \geqq 2.$$

Let $\beta = \alpha - N$ where $N > N_0$ is a fixed integer. Then β is a root of the irreducible polynomial $P(x+N)$ and $\mathbf{Z}[\alpha] = \mathbf{Z}[\beta]$. Let us choose N such that $N > N_0$ and β is not a root of unity. We shall show that $\{\beta, \mathcal{N}_0\}$ is a canonical number system in $\mathbf{Z}[\alpha]$ where $\mathcal{N}_0 = \{0, 1, \ldots, b_0 - 1\}$.

Since $\mathbf{Z}[\alpha] = \mathbf{Z}[\beta]$, for every $\gamma \in \mathbf{Z}[\alpha]$ there exists a representation of the form

$$\gamma = u_0 + u_1\beta + \ldots + u_m\beta^m \tag{2.1}$$

where $u_0, u_1, \ldots, u_m$ are suitable rational integers. Since $\gamma = \gamma + d \cdot (b_0 + b_1\beta + \ldots + b_n\beta^n)$ with $b_i \cong 1$, $d \in \mathbf{Z}$, γ can be represented as

$$\gamma = v_0 + v_1\beta + \ldots + v_m\beta^m \tag{2.2}$$

where the v_j's are non-negative integers, and $m \geqq n$.

Consider a representation of γ with property (2.2). Let $T(\gamma, v) = v_0 + v_1 + \ldots + v_m$ and $l(\gamma) = m+1$ $(v_m \neq 0)$. It is obvious that $T(\gamma, v)$ is a positive integer if $\gamma \neq 0$. By $b_0 \geqq 2$ we have

$$v_0 = r_0 + t \cdot b_0 \quad \text{with} \quad t \geqq 0, \quad t \in \mathbf{Z}, \quad r_0 \in \mathcal{N}_0.$$

Then

$$\gamma = \gamma + t(\beta-1)(b_0+b_1\beta+\ldots+b_n\beta^n) =$$

$$= r_0(v_1-t\cdot b_1+t\cdot b_0)\beta+\ldots+(v_{n-1}-t\cdot b_{n-1}+t\cdot b_{n-2})\beta^{n-1}+(v_n-t\cdot b_n+t\cdot b_{n-1})\beta^n+$$

$$+(v_{n+1}+t\cdot b_n)\beta^{n+1}+v_{n+2}\beta^{n+2}+\ldots+v_m\beta^m = v_0^*+v_1^*\beta+\ldots+v_k^*\beta^k \quad \text{for some } k,$$

and in view of $b_i \geqq b_{i+1}$, we have $v_i^* \geqq 0$ for $i=0, \ldots, k$. Furthermore, we have

$$T(\gamma, v^*) = (v_0-t\cdot b_0)+(v_1-t\cdot b_1+t\cdot b_0)+\ldots+(v_n-t\cdot b_n+t\cdot b_{n-1})+(v_{n+1}+t\cdot b_n)+$$

$$+v_{n+2}+\ldots+v_m = T(\gamma, v).$$

Let $\gamma_1 = v_1^*+v_2^*\beta+\ldots+v_k^*\beta^{k-1}$ $(v_k \neq 0)$. Then $\gamma = r_0+\beta\cdot\gamma_1$ and $T(\gamma_1, v^*) = T(\gamma, v) - -r_0 \geqq 0$, because $v_0^* = r_0 \in \mathcal{N}_0$.

By repeating this argument we obtain the sequence $\gamma = r_0+\beta\cdot\gamma_1$, $\gamma_1 = r_1+ +\beta\cdot\gamma_2, \ldots$ where $r_i \in \mathcal{N}_0$ and $T(\gamma, v) \geqq T(\gamma_1, v) \geqq \ldots$ and $T(\gamma_i, v) = T(\gamma_{i+1}, v)$ only if $r_i = 0$. Since the sequence $T(\gamma_k, v)$ is a monotonically decreasing sequence of non-negative integers, for a suitable integer M we have $T(\gamma_k, v) = T(\gamma_{k+1}, v)$ for $k \geqq M$. Consequently, for $k \geqq M$ $r_k = 0$ and $\gamma_k = \beta\cdot\gamma_{k+1}$.

It is easy to see that for $k \geqq m$ either $\gamma_k = 0$ or $l(\gamma_k) \leqq n+1$. Let us assume that $\gamma_k \neq 0$ for all k with $k \geqq m$, $k \geqq M$, We have $T(\gamma_k, v) = T(\gamma_{k+1}, v)$ for $k \geqq M$ and $l(\gamma_k) \leqq n+1$, hence $\gamma_k, \gamma_{k+1}, \ldots$ are all different from zero and the number of different elements of the sequence $\gamma_k, \gamma_{k+1}, \ldots$ is finite. Hence there exist indices r, s such that $\gamma_r = \gamma_{r+s}$. But $\gamma_r = \beta^s\cdot\gamma_{r+s}$, hence

$$\gamma_r = \beta^s\cdot\gamma_r. \tag{2.3}$$

From (2.3) we see that β is a root of unity which contradicts the assumption made before. This shows that there exists an index k so that $\gamma_k = 0$. But this means that γ has a representation of form (1.1).

It remains to prove that the representation of form (1.1) is unique. Suppose on the contrary that for some γ there exist two representations

$$r_0+r_1\beta+\ldots+r_k\beta^k = s_0+s_1\beta+\ldots+s_t\beta^t, \quad r_i \in \mathcal{N}_0, \tag{2.4}$$

$s_j \in \mathcal{N}_0$. We may assume that $k=t$ and $r_0 \geqq s_0$. Then

$$0 = (r_0-s_0)+(r_1-s_1)\beta+\ldots+(r_k-s_k)\beta^k. \tag{2.5}$$

Hence $0 \leqq r_0-s_0 < b_0$. But $P(x+N)$ is an irreducible polynomial and β is a root of $P(x+N)$. Thus the polynomial $P(x+N)$ divides $(r_0-s_0)+(r_1-s_1)x+\ldots$ $\ldots+(r_k-s_k)x^k$ in the polynomial ring $\mathbf{Q}[x]$. Using Gauss' lemma and the fact that $0 \leqq r_0-s_0 < b_0$ we get that $r_0-s_0=0$. After dividing (2.5) by β we obtain

$$0 = (r_1-s_1)+(r_2-s_2)\beta+\ldots+(r_k-s_k)\beta^{k-1}$$

and we can deduce in the same way as above that $r_1 = s_1$. Repeating this argument we obtain

$$r_0 = s_0, \quad r_1 = s_1, \ldots, r_k = s_k$$

which contradicts our assumption. This proves that the representation (1.1) is unique for every $\gamma \in \mathbf{Z}[\alpha]$.

PROOF OF THEOREM 2.

a) Suppose that in R there is a canonical number system $\{\alpha, \mathcal{N}_0\}$ where $\alpha \in R$ and $\mathcal{N}_0 = \{0, 1, \ldots, m\}$ for some $m \geqq 1$. First assume that α is an algebraic element over the field $\mathbf{Z}/p \cdot \mathbf{Z}$. Then the field $(\mathbf{Z}/p \cdot \mathbf{Z})(\alpha)$ is finite. But we can take infinitely many sums of the form (1.1) and these elements are all contained in R. Since every $\gamma \in R$ can be written in the form (1.1), $\gamma \in (\mathbf{Z}/p \cdot \mathbf{Z})(\alpha)$ and so R is finite. Therefore there exists at least one $\gamma \in R$ which has at least two different representations in the form (1.1). But this is impossible because $\{\alpha, \mathcal{N}_0\}$ is a canonical number system in R.

Now assume that α is a transcendental element over $\mathbf{Z}/p \cdot \mathbf{Z}$. Then $m \leqq p-1$. If $m < p-1$ then

$$p-1 = a_0 + a_1\alpha + \ldots + a_r\alpha^r \quad \text{where} \quad a_i \in \mathcal{N}_0 \quad \text{for} \quad i = 0, \ldots, r.$$

This would imply that α is an algebraic element over $\mathbf{Z}/p \cdot \mathbf{Z}$. Consequently, $m = p-1$ and $R \cong (\mathbf{Z}/p \cdot \mathbf{Z})[x]$.

b) Suppose now that $R = (\mathbf{Z}/p \cdot \mathbf{Z})[x]$. Putting $\alpha = x$ and $\mathcal{N}_0 = \{0, 1, \ldots, p-1\}$, it is evident that $\{\alpha, \mathcal{N}_0\}$ is a canonical number system in $(\mathbf{Z}/p \cdot \mathbf{Z})[x]$ and so the proof of our Theorem 2 is complete.

References

[1] I. KÁTAI and J. SZABÓ, Canonical number systems for complex integers, *Acta Sci. Math. Szeged*, **37** (1975), 255—260.

[2] I. KÁTAI und B. KOVÁCS, Kanonische Zahlensysteme in der Theorie der quadratischen Zahlen, *Acta Sci. Math. Szeged*, **42** (1980), 99—107.

[3] I. KÁTAI and B. KOVÁCS, Canonical number systems in imaginary quadratic fields, *Acta Math. Acad. Sci. Hungar.*, **37** (1981), 159—164.

[4] E. H. GROSSMAN, Number bases in quadratic fields, *Studia Sci. Math. Hungar.*, **20** (1985), 55—58.

[5] B. KOVÁCS, Canonical number systems in algebraic number fields, *Acta Math. Acad. Sci. Hungar.*, **37** (4), 1981), 405—407.

KOSSUTH LAJOS UNIVERSITY
MATHEMATICAL INSTITUTE
4010 DEBRECEN
HUNGARY

(Received June 5, 1988)