Acta Sci. Math., 50 (1986), 351—357

Canonical number systems in $Q(\sqrt[3]{2})$

S. KÖRMENDI

1. Let us given an algebraic number field $Q(\gamma)$ defined as a simple extension of the rational number field determined by γ. Let $S[\gamma]$ denote the ring of the integers in $Q(\gamma)$.

We shall say that an algebraic integer $\varrho\in S[\gamma]$ is the base of a full radix representation in $S[\gamma]$, if every $\alpha\in S[\gamma]$ can be written in the form

$$\alpha=\sum_{k=0}^{m} a_k\varrho^k, \tag{1.1}$$

where the digits a_k are nonnegative integers such that $0\leqq a_k<N=|\mathrm{Norm}(\varrho)|$.

The largest set that we could hope to represent in the form (1.1) is the ring $Z[\varrho]$, i.e. the polynomials in ϱ with rational integer coefficients. The reason that the norm N yields the correct number of digits is due to the fact that the quotient ring $Z[\varrho]/\varrho$ is isomorphic to Z_N by the map which takes a polynomial in ϱ to its constant term modulo N.

Any such radix representation is unique. Let $P(X)$ denote the minimum polynomial of ϱ. Since ϱ is an integer in $S[\gamma]$, therefore the coefficients of $P(X)$ are rational integers, the constant term of $P(X)$ is $\pm N$. Suppose $A(X)$, $B(X)\in Z[X]$ are polynomials whose coefficients are integers in the range from 0 to $N-1$. If $A(\varrho)$ and $B(\varrho)$ represent the same element of $Z[\varrho]$, then $A(X)-B(X)$ is in the ideal generated by $P(X)$ in $Z[X]$. Since the coefficients of $A(X)-B(X)$ are in the interval $[-N+1, N-1]$ and the constant term of $P(X)$ is $\pm N$, therefore $A(X)-B(X)$ must be the zero polynomial, i.e. $A(X)$ and $B(X)$ have the same coefficients.

I. KÁTAI and J. SZABÓ [1] proved that the only numbers which are suitable bases for all the Gaussian integers, using $0, 1, \dots, N-1$ as digits, are $-n\pm i$ where n is a positive integer, $N=n^2+1$ is the norm of $-n\pm i$. Their work was generalized by I. KÁTAI and B. KOVÁCS [2], [3], namely they determined all the bases for quad-

Received April 20, 1984.

ratic number fields, using natural numbers as digits. Similar results have been achieved by W. GILBERT [4], independently.

B. KOVÁCS [5] gave a necessary and sufficient condition for the existence of number base in algebraic number fields. Namely he proved: If $Q(\gamma)$ is an extension of degree n of Q, then there exists a number base in $S[\gamma]$ if and only if there exists a $\vartheta\in S[\gamma]$ such that $\{1, \vartheta, \dots, \vartheta^{n-1}\}$ is an integer-base in $S[\gamma]$.

However, the determination of all the number bases in algebraic number fields seems to be a quite hard problem. Our purpose in this paper is to determine all the number bases in $Q[\sqrt[3]{2}]$. This is the simplest case that has not been considered until now. We hope to extend our investigation for all cubic fields.

2. Let $\sigma=\sqrt[3]{2}$, and let $K(X)=X^3-2$ be the minimum polynomial of σ. We shall use some lemmas.

Lemma 1. *Let* $\alpha=a+b\sigma+c\sigma^2$ *with* $a, b, c\in Q$, *and let* $E_1=-3a$, $E_2=3(a^2-2bc)$, $E_3=-(a^3+2b^3+4c^3-6abc)$. *Then* α *is a root of the polynomial* $T(X)=X^3+E_1X^2+E_2X+E_3$.

Proof. Let $\xi=\exp(2\pi i/3)$ be one of the cubic roots of unity, and let $\alpha_1=\alpha$, $\alpha_2=a+b\xi\sigma+c\xi^2\sigma^2$, $\alpha_3=a+b\xi^2\sigma+c(\xi^2\sigma)^2$ be the conjugates of α. Expanding the product $(X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$ we get immediately that this is $T(X)$.

Lemma 2. $\{1, \sigma, \sigma^2\}$ *is an integer base, i.e.* $\alpha=a+b\sigma+c\sigma^2$ *is an integer in* $Q(\sigma)$ *if and only if* a, b, c *are rational integers.*

Proof. This is well known.

Lemma 3. *Let* $\alpha\in S[\sigma]$ $\{1, \alpha, \alpha^2\}$ *is an integer basis if and only if* $\alpha=M\pm\sigma$, *or* $\alpha=M\pm(\sigma+\sigma^2)$ *with a rational integer* M.

Proof. Let $\alpha=a+b\sigma+c\sigma^2$. Then $\alpha^2=(a^2+4bc)+(2ab+2c^2)\sigma+(2ac+b^2)\sigma^2$. The matrix A of the basis transformation $[1, \sigma, \sigma^2]\to[1, \alpha, \alpha^2]$ has the form

$$A=\begin{bmatrix} 1 & 0 & 0 \\ a & b & c \\ a^2+4bc & 2ab+2c^2 & 2ac+b^2 \end{bmatrix}.$$

$\det A=\pm 1$ if and only $b^3-2c^3=\pm 1$. It is well known, see e.g. [6], that all the solutions of this Diophantine equation are:

$$(b, c) = (1,0), (-1,0), (1,1), (-1,1). \tag{2.1}$$

Let B denote the set of the number bases in $Q(\sigma)$.

Lemma 4. *If* $\alpha\in B$, *then* $\{1, \alpha, \alpha^2\}$ *is an integer base.*

Proof. Obvious.

Lemma 5. *Let $\vartheta \in S[\sigma]$ be such that $\{1, \vartheta, \vartheta^2\}$ is an integer basis. Let the minimum polynomial $T(X)=X^3+E_1X^2+E_2X+E_3$ of ϑ satisfy the conditions $1 \leqq E_1 \leqq E_2 \leqq E_3$, $E_3 \geqq 2$. Then $\vartheta \in B$.*

Proof. See [4].

Lemma 6. *If $\vartheta \geqq -1$, $\vartheta \in S[\sigma]$, then $\vartheta \notin B$.*

Proof. Let H_ϑ denote the set of those numbers α that can be written in the form

$$\alpha = a_0+a_1\vartheta+\ldots+a_k\vartheta^k$$

with suitable digits $a_j \in [0, |N(\vartheta)|-1]$. If $\vartheta \geqq 0$, then $H_\vartheta \subseteqq [0, \infty)$, and so -1 cannot be represented. If $\vartheta=-1$, then $|N(\vartheta)|=1$, $a_j=0$, and so $H_\vartheta=\{0\}$. If $|\vartheta|<1$ and $\alpha \in H_\vartheta$, then

$$|\alpha| \leqq a_0+a_1|\vartheta|+\ldots+a_k|\vartheta|^k \leqq (|N(\vartheta)|-1)\,|\vartheta|/(|\vartheta|-1),$$

consequently H_ϑ is a bounded subset of the real numbers. Since $Z[\vartheta]$ is not bounded, the proof is finished.

Lemma 7. *Let $T(X)=X^3+E_1X^2E_2X+E_3$ be the minimum polinomial of α, and let $\gamma=(E_2+E_1+1)+(E_1+1)+\alpha^2$. Then $(1-\alpha)\gamma=T(1)$. Consequently, if $|T(1)|<$ <1, then γ or $-\gamma$ cannot be represented in the form $r_0+r_1\alpha+\ldots+r_k\alpha^k$, $r_i \in \{0, 1, \ldots,$ $\ldots, |N(\alpha)|-1\}$, i.e. $\alpha \notin B$.*

Proof. The assertion $T(1)=(1-\alpha)\gamma$ is obvious. Let $c=\operatorname{sgn} T(1)$. Then

$$c\gamma = cT(1)+(c\gamma)\alpha, \quad cT(1) \in \{0, \ldots, |N(\alpha)|-1\}.$$

Let us assume in contrary that c has a representation in the form

$$c\gamma = r_0+r_1\alpha+\ldots+r_k\alpha^k.$$

Then $r_0=cT(1)$, $c\gamma=r_1+r_2\alpha+\ldots+r_k\alpha^{k-1}$. Repeating this procedure we get that $cT(1)=r_0=r_1\ldots=r_k$, $c\gamma=0$, which does not hold.

3. From Lemmas 3 and 4 it follows that if $\alpha \in B$, then $\alpha=M\pm\sigma$ or $\alpha=$ $=M\pm(\sigma+\sigma^2)$. Let $T(X)=X^3+E_1X^2+E_2X+E_3$ be the minimum polynomial of α. Let us consider the table below.

α	E_1	E_2	E_3	Conditions of Lemma 5 are satisfied if
$M+\sigma$	$-3M$	$3M^2$	M^3+2	$M \leqq -4$
$M-\sigma$	$-3M$	$3M^2$	M^3-2	$M \leqq -3$ or $M=-1$
$M+\sigma+\sigma^2$	$-3M$	$3(M^2-2)$	M^3-6M+6	$M \leqq -5$
$M-\sigma-\sigma^2$	$-3M$	$3(M^2-2)$	M^3-6M-6	$M \leqq -4$

The numbers α satisfying the conditions stated in the last column belong to B.

From Lemma 7 we get that $\alpha \notin B$ if $\alpha \geqq -1$, i.e. if

$$\begin{aligned}
\alpha &= M+\sigma && \text{and} \quad M \geqq -2, \\
\alpha &= M-\sigma && \text{and} \quad M \geqq 1, \\
\alpha &= M+\sigma+\sigma^2 && \text{and} \quad M \geqq -3, \\
\alpha &= M-\sigma-\sigma^2 && \text{and} \quad M \geqq 2.
\end{aligned}$$

It remains to consider the following set of integers $\alpha_1, \ldots, \alpha_9$, the minimum polynomials of which are denoted by $T_1(X), \ldots, T_9(X)$, resp.

	α	$T(X)$	$N(\alpha)$
1	$-3+\sigma$	$X^3+9X^2+27X+25$	25
2	$-2-\sigma$	$X^3+6X^2+12X+10$	10
3	$-\sigma$	X^3+2	2
4	$-4+\sigma+\sigma^2$	$X^3+12X^2+42X+34$	34
5	$-3-\sigma-\sigma^2$	$X^3+9X^2+21X+15$	15
6	$-2-\sigma-\sigma^2$	X^3+6X^2-6X+2	2
7	$-1-\sigma-\sigma^2$	X^3+3X^2-3X+1	1
8	$-\sigma-\sigma^2$	X^3-6X+6	6
9	$1-\sigma-\sigma^2$	$X^3-3X^2-3X+11$	11

Lemma 8. *We have* $\alpha_6, \alpha_7, \alpha_8, \alpha_9 \notin B$.

Proof. The conditions of Lemma 7 hold for $\alpha_6, \alpha_8, \alpha_9$. α_7 is a unit, the set of the digits contains only one element, the zero, so $\alpha_7 \notin B$.

Lemma 9. $\alpha_3 = -\sigma \in B$.

Proof. The set of the allowable digits are $\{0, 1\}$. Let $\alpha_3 = \alpha$. First we observe that $-1 = 1+\alpha^3$, $2 = \alpha^3+\alpha^6$. The general form of the integers in $Q(\sigma)$ is $Z = X_0+X_1\alpha+X_2\alpha^2$, $X_i \in Z$. By the relation $-1 = 1+\alpha^3$, each Z can be written in the form

$$Z = Y_0+Y_1\alpha+\ldots+Y_5\alpha^5 \tag{3.1}$$

with nonnegative integers $Y_0, \ldots, Y_5$.

Let now $Z^0 \neq 0$ be an arbitrary integer, written in the form (3.1). We shall define the following algorithm:

$$t(Z^0) := Y_0+Y_1+\ldots+Y_5; \quad h = [Y_0/2], \quad l = Y_0-2[Y_0/2] \in \{0, 1\}.$$

$$Z^{(1)} = Y_1+Y_2\alpha+(Y_3+h)\alpha^2+Y_4\alpha^3+Y_5\alpha^4+h\alpha^5.$$

Then $Z^{(0)} = l+\alpha Z^{(1)}$, furthermore

$$t(Z^{(1)}) = Y_1+Y_2+(Y_3+h)+Y_4+Y_5+h = t(Z^{(0)})-l. \tag{3.2}$$

Let us continue this procedure with $Z^{(1)}$ instead of $Z^{(0)}$, and so on. We get a sequence $Z^{(1)}, Z^{(2)}, \dots$. We say that the procedure *terminates* if $Z^{(N)}=0$ for a suitable N. It is obvious that $\alpha\in B$, if the procedure terminates for every Z. Let us assume in contrary that there exists a Z for which it does not terminate. Since the sequence $t(Z^{(\nu)})$ the values of the members of which are positive integers, is monotonically decreasing, we get that $t(Z^{(N)})=t(Z^{(N+1)})=\dots=m>0$. From (3.2) we get that $\alpha Z^{(N+j+1)}=$ $=Z^{(N+j)}$ $(j=0, 1, 2, \dots)$, i.e. α^k divides $Z^{(N)}$ for every positive integer k, which implies that $Z^{(N)}=0$, contrary to our assumption.

4. It remains to consider the cases $\alpha_1, \alpha_2, \alpha_4, \alpha_5$. We shall prove that the question whether they belong to B can be decided by a finite amount of computations.

Let $\alpha\in Q[\sigma]$, $\alpha=a+b\sigma+c\sigma^2$, $A=\{0, 1, \dots, |N(\alpha)|-1\}$. For $\gamma\in Q[\sigma]$ the algorithm

(4.1) $$\gamma_i=\alpha\gamma_{i+1}+r_i,\quad r_i\in A,\quad \gamma_0=\gamma$$

is well defined. Let

$$\gamma_i=\xi^{(i)}+\eta^{(i)}\sigma+\zeta^{(i)}\sigma^2,\quad \Gamma_i=\begin{bmatrix}\xi^{(i)}\\ \eta^{(i)}\\ \zeta^{(i)}\end{bmatrix},\quad \mathbf{e}=\begin{bmatrix}1\\0\\0\end{bmatrix}.$$

Let A denote the matrix that describes the multiplication by α in the base $1, \sigma, \sigma^2$, i.e. for which

(4.2) $$\Gamma_i=A\Gamma_{i+1}+r_i\mathbf{e}$$

holds.

From (4.2) we get that

(4.3) $$\Gamma_{i+1}=A^{-1}\Gamma_i-r_iA^{-1}\mathbf{e}\quad (i=0, 1, 2, \dots),$$

where A^{-1} has the following explicit form:

(4.4) $$A^{-1}=\frac{1}{N(\alpha)}\begin{bmatrix}a^2-2bc & 2b^2-2ac & 4c^2-2ab\\ 2c^2-ab & a^2-2bc & 2b^2-2ac\\ b^2-ac & 2c^2-ab & a^2-2bc\end{bmatrix}.$$

The algorithm $\gamma_i\to\gamma_{i+1}$ terminates if $\gamma_N=0$ for a suitable N, i.e. if $\Gamma_N=0$ in (4.3). Let $\|\cdot\|$ be a vector norm for which, with the corresponding matrix norm,

(4.5) $$\|A^{-1}\|=\varkappa<1$$

is satisfied. From (4.3) we get that

(4.6) $$\Gamma_{i+N}=(A^{-1})^N\Gamma_i-\sum_{k=0}^{N-1}r_{i+k}(A^{-1})^{N-k+1}(A^{-1}\mathbf{e}),$$

and hence that

$$\|\Gamma_{i+N}\| \leqq \varkappa^N \|\Gamma_i\| + (|N(\alpha)|-1)\|A^{-1}e\|(\varkappa/(1-\varkappa)). \tag{4.7}$$

From (4.7) we get immediately that the sequence $\Gamma_0, \Gamma_1, \ldots$ is bounded for every Γ_0.

Let us assume that there exists a γ which cannot be represented in the base α. Then (4.3) does not terminate. Since any bounded domain contains only a finite number of vectors with integer entries, we get that (4.3) is cyclic. From (4.7) we get that

$$\limsup_N \|\Gamma_N\| \leqq (|N(\alpha)|-1)\|A^{-1}e\|(\varkappa/(1-\varkappa)). \tag{4.8}$$

Furthermore, the integer γ_N corresponding to Γ_N cannot be represented in the base α.

So we have proved the following assertion. Let $\varepsilon>0$, and let S_ε be the set of those γ for which

$$\|\Gamma\| \leqq (|N(\alpha)|-1)\|A^{-1}e\|(\varkappa/(1-\varkappa))+\varepsilon =: L+\varepsilon,$$

$\Gamma=\Gamma(\gamma)$ holds. If $\alpha\notin B$, then there exists a $\gamma\in K_\varepsilon$ which cannot be written in the base α.

Furthermore, if $\|\Gamma_i\|\leqq L/(1-\varkappa)$, then $\|\Gamma_{i+1}\|\leqq L/(1-\varkappa)$, which is an obvious consequence of (4.7). This implies that the number of arithmetical operations that needs to be executed to determine the whole periodic sequence $\Gamma_0, \Gamma_1, \ldots$ is finite.

By using the spectral norm for the matrices A_i corresponding to α_i, we get by an easy computation that

$$\|A_1^{-1}\|_S \approx 0{,}63, \quad \|A_2^{-1}\|_S \approx 0{,}75, \quad \|A_4^{-1}\|_S \approx 0{,}97, \quad \|A_5^{-1}\|_S \approx 0{,}75,$$

i.e. the condition (4.5) holds.

5. So we have proved the following

Theorem. *The question whether the integers $\alpha_1=-3\sigma$, $\alpha_2=-2-\sigma$, $\alpha_4=-4+\sigma+\sigma^2$, $\alpha_5=-3-\sigma-\sigma^2$ do or do not belong to B can be decided by executing a finite number of arithmetical operations. All the remaining elements of B are the following integers:*

(a) $\alpha = M+\sigma, \quad M\leqq -4,$

(b) $\alpha = M-\sigma, \quad M\leqq -3$ *or* $M=-1$ *or* $M=0,$

(c) $\alpha = M+\sigma+\sigma^2, \quad M\leqq -5,$

(d) $\alpha = M-\sigma-\sigma^2, \quad M\leqq -4.$

References

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

[2] I. KÁTAI, B. KOVÁCS, Canonical number systems in imaginary quadratic fields, *Acta Math. Hung.*, **37** (1981), 159—164.

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

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

[5] W. GILBERT, Radix representations of quadratic fields, *J. Math. Anal. Appl.*, **83** (1981), 264—274.

[6] W. SIERPINSKI, *Elementary theory of numbers* (Warsawa, 1964).

DEPARTMENT OF COMPUTER SCIENCE
EÖTVÖS LORÁND UNIVERSITY
BOGDÁNFY ÚT 10/B
1117 BUDAPEST, HUNGARY