Annales Univ. Sci. Budapest., Sect. Comp. 22 (2008) 83-94

DIGITAL EXPANSION IN $\mathbb{Q}(\sqrt{2})$

G. Farkas and A. Kovács (Budapest, Hungary)

Dedicated to Prof. K.-H. Indlekofer on his 60th birthday

Abstract. One objective of our research is to extend the concept of number system to various algebraic structures. A study of the quadratic fields automatically raises the question: for what algebraic integers α can we find such a digit set E_α where (α, E_α) is a number system.

1. Introduction

Let D be a square free (positive or negative) integer, or $D = -1$. The quadratic fields $\mathbb{Q}\left(\sqrt{D}\right)$ are classified: we say that it is an imaginary extension of $\mathbb{Q}$, if $D < 0$, while in the case $D > 0$ we say that it is a real extension field. For some fixed D, let I denote the set of algebraic integers in $\mathbb{Q}\left(\sqrt{D}\right)$.

Definition. Let $\alpha \in I$ and E_α $(\subseteq I)$ be a complete residue system mod α containing 0.

We say that (α, E_α) is a *coefficient system* in I, the elements of E_α are digits and α is the base (number) of (α, E_α).

Definition. (α, E_α) is a *number system* in I if each $\gamma \in I$ can be written in a finite sum

$$\gamma = e_0 + e_1\alpha + \ldots + e_k\alpha^k, \tag{1.1}$$

where $e_i \in E_\alpha,\ i = 0, 1, \ldots, k$.

Then α is the *base (number)* of the number system (α, E_α).

Since E_α is a complete residue system mod α, therefore the uniqueness of the representation (1.1) is clear. Furthermore, it is obvious that for every $\gamma \in I$ there exists a unique $f \in E_\alpha$ for which

$$\gamma = \alpha \cdot \gamma_1 + f \tag{1.2}$$

holds with a suitable $\gamma_1 \in I$.

Let $J : I \to I$ be the function defined by $J(\gamma) = \gamma_1$, if γ, γ_1 are related by (1.2). Then we can define a directed graph over I, by drawing an edge from γ to γ_1, labeling it with f:

$$\gamma \xrightarrow{(f)} \gamma_1. \tag{1.3}$$

We say that $\pi \in I$ is a periodic element, if $J^k(\pi) = \pi$ holds for some positive integer k. Let $\mathcal{P}$ be the set of periodic elements.

It is clear that (α, E_α) is a number system, if $\mathcal{P} = \{0\}$.

The question we are interested in is the following: what are those $\alpha \in I$ in some $\mathbb{Q}\left(\sqrt{D}\right)$ for which (α, E_α) is a number system with an appropriate digit set E_α.

The question was completely solved by G. Steidl for $D = -1$ [5], for arbitrary imaginary quadratic fields by I. Kátai. Namely they proved that α is a base of a number system, if and only if $\alpha \neq 0$ and $\alpha,\ 1-\alpha$ are not units. The explicit construction of E_α is given.

The case of real quadratic extension field seems to be harder due to the fact that the module of α and its conjugate $\overline{\alpha}$ are not the same in general.

Assume that $D > 0$. If α is a base of a number system then clearly

$$\begin{cases} \alpha \neq 0, \\ \alpha, 1-\alpha \quad \text{are not units}, \\ |\alpha| > 1,\ |\overline{\alpha}| > 1 \end{cases} \tag{1.4}$$

should be satisfied.

It is true that α is a base of a number system if (1.4) holds?

The first named author proved it [4] if (1.4) holds in a stronger form:

$$|\alpha| \geq 2, \quad |\overline{\alpha}| \geq 2.$$

We shall improve this in the case $D = 2$.

2. The formulation of our results

2.1. A previous achievement

The starting point of our investigation is a theorem published by I. Kátai in [1]. He proved for imaginary quadratic fields that $\alpha \in I$ is a base of a number system with an appropriate digit set E_α if and only if

$$\alpha \neq 0,$$
$$\alpha,\ 1-\alpha \quad \text{are not units and}$$
$$|\alpha|, |\overline{\alpha}| > 1,$$

where $\overline{\alpha}$ is the algebraic conjugate of α. In that paper the explicit construction of digit set E_α was given. The digit sets constructed in this way are called *K-type digit sets*.

Our prospective purpose is to prove the same result in real quadratic fields. In this paper we concentrate on the quadratic field $\mathbb{Q}\left(\sqrt{2}\right)$.

2.2. The construction of the K-type digit sets

Let $\alpha = a + b\sqrt{2}$ be an arbitrary algebraic integer in $\mathbb{Q}\left(\sqrt{2}\right)$, that is $a, b \in \mathbb{Z}$, and $d = \alpha \cdot \overline{\alpha}$, where $\overline{\alpha} = a - b\sqrt{2}$ is the conjugate of α. Then $E_\alpha^{(\varepsilon,\delta)}$ are the sets of those $f = k + l\sqrt{2}$ $(k, l \in \mathbb{Z})$ for which

$$f \cdot \overline{\alpha} = \left(k + l\sqrt{2}\right)\left(a - b\sqrt{2}\right) = (ka - bl2) + (la - kb) = r + s\sqrt{2}$$

satisfy the following conditions:

- if $(\varepsilon, \delta) = (1, 1)$, then $r, s \in \left(\frac{-|d|}{2}, \frac{|d|}{2}\right]$,
- if $(\varepsilon, \delta) = (-1, -1)$, then $r, s \in \left[\frac{-|d|}{2}, \frac{|d|}{2}\right)$,
- if $(\varepsilon, \delta) = (-1, 1)$, then $r \in \left[\frac{-|d|}{2}, \frac{|d|}{2}\right)$, $s \in \left(\frac{-|d|}{2}, \frac{|d|}{2}\right]$,
- if $(\varepsilon, \delta) = (1, -1)$, then $r \in \left(\frac{-|d|}{2}, \frac{|d|}{2}\right]$, $s \in \left[\frac{-|d|}{2}, \frac{|d|}{2}\right)$.

We call the above constructed digit sets K-type digit sets. If we do not specify the value of (ε, δ), then we denote with E_α an arbitrary element of the set $\left\{E_\alpha^{(1,1)}, E_\alpha^{(1,-1)}, E_\alpha^{(-1,1)}, E_\alpha^{(-1,-1)}\right\}$.

2.3. The construction of the F-type digit sets

For an arbitrary $\alpha \in I\left(\subseteq \mathbb{Q}(\sqrt{2}\right)$ let E_α be a K-type digit set. We proved in [2] that if $P\backslash\{0\}$ is not empty, then either $G\left(P\backslash\{0\}\right)$ is a disjoint union of loops, or a disjoint union of circles of length 2, which take the form: $\pi \xrightarrow{f} (-\pi) \xrightarrow{-f} \pi$.

We shall construct the appropriate F-type digit set A_α by modifying E_α as follows.

1) If (α, E_α) is a number system, then $A_\alpha = E_\alpha$.

2) If $f \in E_\alpha$ and either

a) $\pi \xrightarrow{f} \pi$ holds for some $\pi \in \mathcal{P}$

or

b) $\pi \xrightarrow{f} (\pi) \xrightarrow{-f} \pi$ holds for some $\pi \in \mathcal{P}$,

then let $f^* \in \mathcal{A}_\alpha$, where f^* is one of $f+\alpha,\ f-\alpha$, so that

$$|\overline{f^*}| = \big||\overline{\alpha}| - |\overline{f}|\big|$$

holds.

Let the other elemenets of E_α belong to A_α.

2.4. The formulation of our Theorem

Theorem. *Let $\alpha \in \mathbb{Q}\left(\sqrt{2}\right)$ be an arbitrary algebraic integer and*

$$\begin{aligned} &\alpha \neq 0, \\ &\alpha,\ 1-\alpha \quad \textit{not units and} \\ &|\alpha|, |\overline{\alpha}| > \sqrt{2} \end{aligned}$$

hold. Then α is a base of a number system.

3. The proof of our Theorem

Remark 1. We saw in [3] that we can assume, without injuring the generality that $|\alpha| > |\overline{\alpha}|$. In case $|\alpha| < |\overline{\alpha}|$ we can prove the same assertion in the same way.

Remark 2. In [4] we proved that if $|\alpha|, |\overline{\alpha}| \geq 2$ and the conditions of our Theorem hold then (α, E_α) is a number system, where E_α is the appropriate K-type digit set.

Remark 3. If $|\alpha|, |\overline{\alpha}| < 2$ then $1 - \alpha$ is a unit. Thus we have to prove our Theorem when the inequalities

$$\min(|\alpha|, |\overline{\alpha}|) < 2 \quad \text{and} \quad \max(|\alpha|, |\overline{\alpha}|) > 2$$

are simultaneously valid.

Remark 4. Relying on the data included in the appendix of [3], the validity of our Theorem can be easily verified for case $\max(|\alpha|, |\overline{\alpha}|) \leq 6 + 3\sqrt{2}$.

In line with the Remarks we have made so far, in the following we assume that

$$|\alpha| > 6 + 3\sqrt{2} \quad \text{and}$$

$$\sqrt{2} < |\overline{\alpha}| < 2$$

inequalities hold true.

In [3], [4] we proved some useful assertions assuming that $1 + \alpha$ is not a unit. In order to use these results in this paper we present the following lemma:

Lemma 1. *If* $1 + \alpha$ *is a unit in* I *then*

$$|\overline{\alpha}| < \sqrt{2}.$$

Proof. It is a well-known fact in number theory that a number β is a unit in an arbitrary quadratic field if and only if either $\beta \cdot \overline{\beta} = 1$ or $\beta \cdot \overline{\beta} = -1$. Let us consider the following product. Assume that $1 + \alpha$ is a unit. Then $M = (1+\alpha)(1 + \overline{\alpha}) = \pm 1$, that is $M = 1 + 2a + d$, where naturally $\alpha = a + b\sqrt{2}$ and $\alpha \cdot \overline{\alpha} = d$.

There are four cases:

1. If $\alpha, \overline{\alpha} > 0$ then $M = 1$.
2. If $\alpha < 0$, $\overline{\alpha} > 0$ then $M = -1$, that is $2a + d = -2$.

It is clear that both cases yield a contradiction.

3. If $\alpha > 0,\ \overline{\alpha} < 0$ then $M = -1$, that is $a = -\dfrac{d}{2} - 1$.

Since $|\overline{\alpha}| = |b|\sqrt{2} - |a|$, therefore $|\alpha| = |a| + |b|\sqrt{2} = 2|a| + |\overline{\alpha}|$. Thus $|\alpha| = |\alpha| - 2 + |\overline{\alpha}|$. We get from $|d| = |\alpha||\overline{\alpha}|$ that

$$|\alpha| + 2 - |\overline{\alpha}| = |\alpha||\overline{\alpha}|, \quad \text{that is}$$

$$|\overline{\alpha}| = 1 + \frac{2 - |\overline{\alpha}|}{|\alpha|} < \sqrt{2}.$$

4. If $\alpha, \overline{\alpha} < 0$ then $M = 1$, that is $a = \dfrac{-d}{2}$. We get that $|\alpha| = |d| - |\overline{\alpha}|$ and from this

$$|\alpha| + |\overline{\alpha}| = |\alpha||\overline{\alpha}|.$$

Then

$$|\overline{\alpha}| = 1 + \frac{|\overline{\alpha}|}{|\alpha|} < \sqrt{2}$$

is true completing the proof of the Lemma 1. Thus, we can use the results of our previous papers, without losing the generality, because $1 + \alpha$ never is unit.

The following assertions are related to the estimation of the modulus of the digits and their conjugates.

Lemma 2. *If $f^* \in A_\alpha$ and $f^* \notin E_\alpha$ then*

$$|f^*| < \left(3 - \sqrt{2}\right)|\alpha| + 1$$

and

$$|\overline{f^*}| < |\overline{\alpha}| - 1.$$

Proof. If $f^* \notin E_\alpha$, then there exists a digit f in E_α for which either $f^* = f + \alpha$ or $f^* = f - \alpha$ holds, thus

$$|f^*| \le |f| + |\alpha|.. \tag{3.1}$$

$f^* \notin E_\alpha$ implies further that there exists a $\pi = p + q\sqrt{2}$ in (α, E_α), for which either

$$f = \pi(1 - \alpha) \quad \text{or} \quad f = \pi(1 + \alpha) \tag{3.2}$$

is true. From this follows that

$$|\pi| \le \frac{|f|}{|\alpha| - 1} \quad \text{and} \quad |\overline{\pi}| \le \frac{|\overline{f}|}{|\overline{\alpha}| - 1}. \tag{3.3}$$

Let

$$S := \frac{|f|}{|\alpha|-1} + \frac{|\overline{f}|}{|\overline{\alpha}|-1}.$$

(3.3) implies that

$$|\pi - \overline{\pi}| = 2|q|\sqrt{2} \leq |\pi| + |\overline{\pi}| \leq S.$$

The construction of E_α leads to

$$|f \cdot \overline{\alpha}| = |r + s\sqrt{2}|, \quad |\overline{f} \cdot \alpha| = |r - s\sqrt{2}| \quad \text{and} \quad |r|, |s| \leq \frac{|d|}{2}.$$

Now we can compute easily that

$$\text{if } sgn(r) = sgn(s) \text{ then } S \leq \frac{1+\sqrt{2}}{2}\frac{|\alpha|}{|\alpha|-1} + \frac{\sqrt{2}}{2}\frac{|\overline{\alpha}|}{|\overline{\alpha}|-1} \quad \text{and,}$$

$$\text{if } sgn(r) \neq sgn(s) \text{ then } S \leq \frac{\sqrt{2}}{2}\frac{|\alpha|}{|\alpha|-1} + \frac{\sqrt{2}+1}{2}\frac{|\overline{\alpha}|}{|\overline{\alpha}|-1}.$$

Since $|q| \leq \dfrac{S}{2\sqrt{2}}$ we get that

$$|q| < 2.$$

In [3] we saw that $|\pi| = |p + q\sqrt{2}| < 2$ and $\pm 1 \notin \mathcal{P}$, thus either

$$|\pi| = \sqrt{2} - 1 \quad \text{or} \quad |\pi| = 2 - \sqrt{2}$$

can be valid. Then, it follows from (3.1) and (3.2) that

$$|f^*| \leq \left(2 - \sqrt{2}\right)(|\alpha| + 1) + |\alpha| = \left(3 - \sqrt{2}\right)|\alpha| + 2 - \sqrt{2},$$

that is

$$|f^*| < \left(3 - \sqrt{2}\right)|\alpha| + 1$$

holds.

What can we say about $|\overline{f^*}|$? We have to consider two cases. If $|\pi| = \sqrt{2}-1$ then $|\overline{\pi}| = \sqrt{2} + 1$ and

$$|\overline{f}| = \left(1 + \sqrt{2}\right)(|\overline{\alpha}| - 1) > \left(1 + \sqrt{2}\right)\left(\sqrt{2} - 1\right) = 1.$$

If $|\pi| = 2-\sqrt{2}$ then $|\overline{\pi}| = 2+\sqrt{2}$ and

$$|\overline{f}| = \left(2+\sqrt{2}\right)(|\overline{\alpha}|-1) > \left(2+\sqrt{2}\right)\left(\sqrt{2}-1\right) = \sqrt{2}.$$

Thus we get that if $|\overline{f}| > |\overline{\alpha}|$ then

$$|\overline{f^*}| = |\overline{f}| - |\overline{\alpha}| \geq \frac{1+\sqrt{2}}{2}|\overline{\alpha}| - |\overline{\alpha}|,$$

that is

$$|\overline{f^*}| < \sqrt{2}-1,$$

and if $|\overline{f}| < |\overline{\alpha}|$ then

$$|\overline{f^*}| = |\overline{\alpha}| - |\overline{f}| < |\overline{\alpha}| - 1.$$

We can see that in both cases $|\overline{f^*}| < |\overline{\alpha}| - 1$, therefore we proved Lemma 2.

Lemma 3. *In* (α, A_α) *for an aribtrary* $\pi\left(= p + q\sqrt{2}\right) \in \mathcal{P}$

$$|p| \leq 2 \quad and \quad |q| \leq 1$$

hold.

Proof. Let π_1 be a periodic element of maximal modulus. There exists a transition

$$\pi = \pi_1\alpha + f^*$$

with suitable $\pi \in \mathcal{P}$ and $p^* \in A_\alpha$.

Consequently, we can carry out the following deduction:

$$\begin{aligned}
&\pi_1\alpha = \pi - f^*,\\
&|\pi_1| \leq \frac{|\pi| + |f^*|}{|\alpha|} \leq \frac{|\pi_1| + |f^*|}{|\alpha|},\\
&|\pi_1|\left(1 - \frac{1}{|\alpha|}\right) \leq \frac{|f^*|}{|\alpha|},\\
&|\pi_1| \leq \frac{|f^*|}{|\alpha|-1}.
\end{aligned}$$

In the same way we get that

$$|\overline{\pi}_1| \leq \frac{|\overline{f^*}|}{|\overline{\alpha}|-1}.$$

In order to estimate the value of $|p|$ and $|q|$, we use the method described in the proof of the Lemma 2. Thus let

$$S_{\max} = \max_{f^* \in A_\alpha} \left(\frac{|f^*|}{|\alpha| - 1} + \frac{|\overline{f^*}|}{|\overline{\alpha}| - 1} \right).$$

We know that

$$|\pi + \overline{\pi}| = 2|p| \leq S_{\max}$$

and

$$|\pi - \overline{\pi}| = 2|q\sqrt{2}| \leq S_{\max}.$$

If $f^* \in E_\alpha$, then we have already proved that $|p| \leq 2$, $|q| \leq 1$, since $|\overline{\alpha}| > \sqrt{2}$ and $|\alpha| > 10$.

If $f^* \notin E_\alpha$, then we get from Lemma 2 that

$$S_{\max} < \frac{\left(3 - \sqrt{2}\right) |\alpha| + 1}{|\alpha| - 1} + \frac{|\overline{\alpha}| - 1}{|\overline{\alpha}| - 1} < 3.$$

The proof is completed.

The next assertion helps to describe the structure of $G\left(\mathcal{P} \backslash \{0\}\right)$.

Lemma 4. In (α, A_α) $G\left(\mathcal{P} \backslash \{0\}\right)$ does not contain loops, and circles of the form $\pi \xrightarrow{f^*} (-\pi) \xrightarrow{-f^*} \pi$, or in case $\overline{\alpha} > 0$ a transition with form $-\pi \xrightarrow{f^*} \pi$.

Proof. Assume first that for same $\pi \in \mathcal{P}$ and $f^* \in A_\alpha$

$$\pi = \pi \cdot \alpha + f^*$$

holds, i.e. there exists a loop in $G\left(\mathcal{P} \backslash \{0\}\right)$. Thus we get

$$f^* = \pi(1 - \alpha).$$

If $\overline{\alpha} > 0$ then $1 - \alpha \mid f^*$, which implies that either

$$1 - \alpha \mid f + \alpha \quad \text{or} \quad 1 - \alpha \mid f - \alpha$$

for the appropriate $f \in E_\alpha$. Let us observe that this is a contradiction because in this case $1 - \alpha$ is a unit.

If $\overline{\alpha} < 0$, then the inequality

$$|\overline{f^*}| = |\overline{\pi}| \left(|\overline{\alpha}| + 1\right) \geq \sqrt{2} \left(|\overline{\alpha}| + 1\right)$$

is true, which yields a contradiction, since $|\overline{f^*}| < |\overline{\alpha}| - 1$. Thus we have proved that there dose not exist a loop.

Now let us assume that the equation

$$-\pi = \pi \cdot \alpha + f^*$$

holds for some $f^* \in A_\alpha$, and also $-f^* \in A_\alpha$. It is obvious that

if $\overline{\alpha} > 0$, then $|f^*| = |\overline{\pi}| \left(|\overline{\alpha}| + 1\right)$, and

if $\overline{\alpha} < 0$, then $1 + \alpha$ is a unit, which can be proved in the above mentioned way.

Although we have proved Lemma 4, in case $\overline{\alpha} < 0$ there may exist transition with form $-\pi \xrightarrow{f^*} \pi$.

Summing up the results we have reached so far, and taking into account that $\pm 1 \notin \mathcal{P}$, we can include the possible elements of $\mathcal{P}$ in this table:

(3.4)

$\|p\|$	$\|q\|$	$\|\pi\|$	$\|\overline{\pi}\|$
0	1	$\sqrt{2}$	$\sqrt{2}$
1	1	$\sqrt{2} - 1$	$\sqrt{2} + 1$
2	0	2	2
2	1	$2 - \sqrt{2}$	$2 + \sqrt{2}$

As a matter of fact our last assertion completes the proof of the Theorem, namely:

Lemma 5. $\mathcal{P} = \{0\}$.

Proof. Let us observe that $\pm 2 \notin \mathcal{P}$, otherwise the equation

$$|\pi_1| = 2|\alpha| - |f^*|$$

would be valid, but this means that

$$|\pi_1| > 2|\alpha| - \left(3 - \sqrt{2}\right) |\alpha| - 1,$$

and we would get that

$$|\pi_1| > \left(\sqrt{2} - 1\right) |\alpha| - 1 > 2,$$

which is a contradiction.

Now let us assume that $\pi_1 \in \mathcal{P}$ such that $|\pi_1| = \sqrt{2}$. According to Lemma 4 it must be a transition

$$\pi_1 = \pi \cdot \alpha + f^*,$$

where $|\pi| \neq \sqrt{2}$, that is $|\overline{\pi}| \geq \sqrt{2}+1$. Then we get that the inequalities

$$\frac{\sqrt{2}+1}{2}|\overline{\alpha}| \geq |\overline{f^*}| \geq (\sqrt{2}+1)|\overline{\alpha}| - \sqrt{2}$$

hold and these imply that

$$\sqrt{2} \geq \frac{\sqrt{2}+1}{2}|\overline{\alpha}| > \frac{\sqrt{2}+1}{2}\sqrt{2},$$

which is impossible, thus $\pm\sqrt{2} \notin \mathcal{P}$.

Now, we only have to concentrate on the 2nd and 4th rows of the table (3.4). In accordance with Lemma 4 there must exist a transition

$$\pi_1 = \pi \cdot \alpha + f^*,$$

where $|\overline{\pi}_1| = 1+\sqrt{2}$ and $|\overline{\pi}| = 2+\sqrt{2}$, but then

$$\frac{\sqrt{2}+1}{2}|\overline{\alpha}| \geq |\overline{f^*}| = \left(2+\sqrt{2}\right)|\overline{\alpha}| - \sqrt{2} - 1$$

is true and we get from this that

$$1+\sqrt{2} \geq \frac{3+\sqrt{2}}{2}|\overline{\alpha}| > \frac{3+\sqrt{2}}{2}\sqrt{2}.$$

Obviously, this is a contradiction, therefore $\mathcal{P} = \{0\}$.

This concludes the proof of Lemma 5 as well as that of our Theorem.

References

[1] **Kátai I.,** Number systems in imaginary quadratic fields, *Annales Univ. Sci. Budapest. Sect. Comp.,* **14** (1994), 159-164.

[2] **Farkas G.,** Digital expansion in real algebraic quadratic fields, *Mathematica Pannonica,* **10** (2) (1999), 235-248.

[3] **Farkas G.,** Location and number of periodic elements in $\mathbb{Q}(\sqrt{2})$, *Annales Univ. Sci. Budapest. Sect. Comp.,* **20** (2001), 133-146.

[4] **Farkas G.,** Number systems in real quadratic fields, *Annales Univ. Sci. Budapest. Sect. Comp.,* **18** (1999), 47-60.

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

G. Farkas and A. Kovács
Department of Computer Algebra
Eötvös Loránd University
XI. Pázmány P. sét. 1/C.
H-1117 Budapest, Hungary