Czechoslovak Mathematical Journal

Juraj Kostra

Orders with a normal basis

Czechoslovak Mathematical Journal, Vol. 35 (1985), No. 3, 391–404

Persistent URL: http://dml.cz/dmlcz/102029

Czechoslovak Mathematical Journal, 35 (110) 1985, Praha

ORDERS WITH A NORMAL BASIS

JURAJ KOSTRA, Bratislava

(Received December 14, 1983)

Let K be a finite extension of the rational number field Q. Such a field will be called an *algebraic number field*. The integral closure Z_K of the ring Z of rational integers in an algebraic number field K will be called the *ring of integral numbers of the field K*.

In the present paper we shall show that if an Abelian algebraic number field K has no normal integral basis then there is no order of the field K with a normal basis, and if the field K has a normal integral basis then there are infinitely many orders of the field K with a normal basis. The former assertion follows from the known results while the latter is a corollary of two theorems about circulant matrices which will be proved in the sequel.

Definition 1. Let K be an algebraic number field and let the degree of the extension K/Q be equal to n. A Z-module $B \subset K$ is called an *order of the field K* if B satisfies the following three conditions:

1) $1 \in B$.
2) B has a basis over Z consisting of n elements.
3) B is a ring.

Remark 1. (Borevič, Šafarevič [1].) The ring Z_K is an order of the field K which contains all the other orders of the field K.

Definition 2. Let K be a normal algebraic number field. A basis of K over Q is called a *normal basis* if it consists of all conjugates of an element. A normal basis is called a *normal integral basis* of the field K if it is a basis of Z_K over Z. If B is an order of K then a normal basis is called a *normal basis* of B if it is a basis of B over Z.

Lemma 1. *Let R be an order with a normal basis of a normal algebraic number field K. Then the trace of any basis element in the field Q is equal to* ± 1.

Proof. Let $G(K/Q) = \{g_1, g_2, \ldots, g_n\}$ be the Galois group of the extension K/Q. Let

$$x^{g_1}, x^{g_2}, \ldots, x^{g_n}$$

be a normal basis of the order R. Remark 1 yields

$$\mathrm{Tr}_{K/Q}(x^{g_i}) = x^{g_1} + x^{g_2} + \dots + x^{g_n} = a$$

for $i = 1, 2, \dots, n$ and $a \in Z$. From the definition of an order we have $1 \in R$ and so

$$1 = \frac{1}{a} x^{g_1} + \frac{1}{a} x^{g_2} + \dots + \frac{1}{a} x^{g_n}$$

where $1/a \in Z$, hence $a = \pm 1$.

For the proof of Theorem 1 we shall need the following known results:

(1) Narkiewicz [5] (from the proof of Theorem 4.5): *Let K be a normal algebraic number field and let the degree of the extension K/Q be equal to n. If the homomorphism $\mathrm{Tr}_{K/Q}$ is surjective then the discriminant $D(K)$ cannot be divisible by the n-th power of a prime.*

(2) Narkiewicz [5]: *Let K be the same as in (1). If the discriminant $D(K)$ is not divisible by the n-th power of a prime then the extension K/Q is tamely ramified.*

(3) Leopold [3]: *An Abelian algebraic number field K has a normal integral basis if and only if the extension K/Q is tamely ramified.*

Theorem 1. *An Abelian algebraic number field K has a normal integral basis if and only if there is $x \in Z_K$ such that*

$$\mathrm{Tr}_{K/Q}(x) = 1 .$$

Proof. Let K be an Abelian algebraic number field. If K has a normal integral basis then Lemma 1 implies that there is an element $x \in Z_K$ such that $\mathrm{Tr}_{K/Q}(x) = 1$. Now let $[K : Q]$ be equal to n. If there is an element $x \in Z_K$ such that $\mathrm{Tr}_{K/Q}(x) = 1$ then the homomorphism $\mathrm{Tr}_{K/Q}$ is surjective and from (1) we have that the discriminant $D(K)$ is not divisible by the n-th power of a prime. From (2) it follows that the extension K/Q is tamely ramified and so (3) implies that the field K has a normal integral basis.

Remark 2. The previous theorem is not true for a general field K. A counterexample is found in Martinet [4].

Corollary 1. *If an Abelian algebraic number field K has no normal integral basis then there is no order of the field K with a normal basis.*

Proof follows from Remark 1 and Lemma 1.

Now let K be a cyclic algebraic number field with $[K : Q] = n$ and let $G = G(K/Q)$ be the Galois group of the extension K/Q. Let g be a generator of G and let

$$x, x^g, x^{g^2}, \dots, x^{g^{n-1}}$$

be a normal basis of the field K over Q. Let A be a regular rational circulant matrix which we shall write in the form

$$A = \mathrm{circ}_n(a_1, a_2, \dots, a_n)^{\mathrm{T}} .$$

The matrix A transforms the normal basis

$$x, x^g, \ldots, x^{g^{n-1}}$$

to the basis

$$y_1, y_2, \ldots, y_n,$$

where

$$y_1 = a_1 x + a_2 x^g + \ldots + a_n x^{g^{n-1}},$$
$$y_2 = a_n x + a_1 x^g + \ldots + a_{n-1} x^{g^{n-1}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$y_n = a_2 x + a_3 x^g + \ldots + a_1 x^{g^{n-1}}.$$

From the above we see that

$$y_{i+1} = y_1^{g^i}$$

for $i = 0, 1, \ldots, n - 1$ and so $y_1, y_2, \ldots, y_n$ is a normal basis of K over Q.

Let

$$x, x^g, \ldots, x^{g^{n-1}}$$

and

$$y, y^g, \ldots, y^{g^{n-1}}$$

be two normal bases of the field K over Q. Then there are rational numbers $c_1, c_2, \ldots$ $\ldots, c_n$ such that

$$y = c_1 x + c_2 x^g + \ldots + c_n x^{g^{n-1}}$$

and so

$$y^g = c_n x + c_1 x^g + \ldots + c_{n-1} x^{g^{n-1}},$$
$$y^{g^2} = c_{n-1} x + c_n x^g + \ldots + c_{n-2} x^{g^{n-1}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$y^{g^{n-1}} = c_2 x + c_3 x^g + \ldots + c_1 x^{g^{n-1}}.$$

Consequently, the transformation matrix from one normal basis to another is a regular rational circulant matrix.

In the following we shall need two propositions from [2].

Proposition 1. *Let A, B be rational circulant matrices and let the degree of each of them be n. Then the following matrices are circulant:*

1) $A + B$,
2) $a \, . \, A$ *where* $a \in Q$,
3) $A \, . \, B$,
4) A^{-1} *if* A^{-1} *exists,*
5) A^{T}.

Proposition 2. *Let* $C = \operatorname{circ}_n(c_1, c_2, \ldots, c_n)$ *and let* $\zeta = e^{2\pi i/n}$. *We denote* $\gamma =$

$= (c_1, c_2, \ldots, c_n)$ *and*

$$p_y(z) = c_1 + c_2 z + \ldots + c_n z^{n-1} .$$

Then we have

$$\det C = \prod_{j=1}^{n} p_y(\zeta^{j-1}) .$$

Theorem 2. *Let K be a cyclic algebraic number field and $[K : Q] = n$. Let*

$$A = \operatorname{circ}_n (a_1, a_2, \ldots, a_n)^{\mathrm{T}}$$

be a regular circulant matrix and $a_1, a_2, \ldots, a_n \in Z$. Let D be the determinant of the matrix A. By A_i, $i = 1, 2, \ldots, n$, we denote the algebraic complement of a_i in the matrix A. Let

$$\sum_{i=1}^{n} a_i = \pm 1$$

and

$$a_i \equiv a_j \pmod h$$

for $i, j \in \{1, 2, \ldots, n\}$, where $h = D/l$ and $l = (A_1, A_2, \ldots, A_n)$ is the greatest common divisor of the algebraic complements. Then the matrix A transforms a normal basis of any order B of the field K to a normal basis of an order C of the field K, where $C \subset B$.

Proof. Let $x_1, x_2, \ldots, x_n$ be a normal basis of an order B of the field K. Let

$$(y_1, y_2, \ldots, y_n) = (x_1, x_2, \ldots, x_n) . A ,$$

so that $y_1, y_2, \ldots, y_n$ is a normal basis of a Z-module $C \subset B$ which contains n linearly independent elements over Z. By Lemma 1

$$\sum_{i=1}^{n} x_i = \pm 1$$

and we have

$$\mathrm{Tr}_{K/Q}(y_1) = \mathrm{Tr}_{K/Q}(a_1 x_1 + a_2 x_2 + \ldots + a_n x_n) = \sum_{i=1}^{n} a_i . \sum_{j=1}^{n} x_j = \pm 1$$

and so $1 \in C$. Now it is sufficient to prove that C is a ring.

Since

$$A^{-1} = \operatorname{circ}_n \left(\frac{A_1}{D}, \frac{A_2}{D}, \ldots, \frac{A_n}{D} \right)$$

we have

$$x_i = \frac{1}{h} (t_{1,i} y_1 + t_{2,i} y_2 + \ldots + t_{n,i} y_n)$$

for $i = 1, 2, \ldots, n$, where $t_{1,i}, t_{2,i}, \ldots, t_{n,i} \in Z$. Hence

$$h . B \subset C .$$

Now we choose arbitrary y_i, y_j from the basis elements of C and we shall prove that $y_i y_j \in C$. Let

$$y_i = b_1 x_1 + b_2 x_2 + \ldots + b_n x_n ,$$

$$y_j = c_1 x_1 + c_2 x_2 + \ldots + c_n x_n$$

where $(b_1, b_2, \ldots, b_n)^{\mathrm{T}}$ and $(c_1, c_2, \ldots, c_n)^{\mathrm{T}}$ are the i-th and the j-th column, respectively, of the matrix A. Then

$$y_i y_j = \sum_{k=1}^{n} b_k c_k x_k^2 + \sum_{k \neq l} (b_k c_l + b_l c_k)\, x_k x_l =$$

$$= b_1 c_1 \sum_{k=1}^{n} x_k^2 + (b_1 c_2 + b_2 c_1) \sum_{k \neq 1} x_k x_l + \sum_{k=1}^{n} (b_k c_k - b_1 c_1)\, x_k^2 +$$

$$+ \sum_{k \neq 1} (b_k c_l + b_l c_k - b_1 c_2 - b_2 c_1)\, x_k x_l .$$

For any automorphism $g \in G(K/Q)$ we have

$$g\Big(\sum_{k=1}^{n} x_k^2\Big) = \sum_{k=1}^{n} x_k^2 ,$$

$$g\Big(\sum_{k \neq l} x_k x_l\Big) = \sum_{k \neq l} x_k x_l$$

and so

$$b_1 c_1 \sum_{k=1}^{n} x_k^2 = L_1 ,$$

$$(b_1 c_2 + b_2 c_1) \sum_{k \neq l} x_k x_l = L_2 ,$$

where $L_1, L_2 \in Z$. From

$$a_i \equiv a_j \pmod{h}$$

for $i, j \in \{1, 2, \ldots, n\}$ we have

$$b_k c_k - b_1 c_1 \equiv 0 \pmod{h}$$

and

$$b_k c_l + b_l c_k - b_1 c_2 - b_2 c_1 \equiv 0 \pmod{h} .$$

Now we can write

$$y_i y_j = L_1 + L_2 + h \,.\, z_1 + h \,.\, z_2$$

where $z_1, z_2 \in B$ and so

$$y_i y_j \in C .$$

The theorem is proved.

Theorem 3. *For any natural number $n \geqq 2$ there is a circulant matrix A of degree n such that the assumptions of Theorem 2 are satisfied and $|\det A| \neq 1$.*

Proof. First we shall prove the case $n = 2$. Let $A = \operatorname{circ}_2(a_1, a_2)$ be a circulant matrix such that $a_1 + a_2 = 1$, $a_1, a_2 \in Z$ and $a_1 > 1$. We have

$$D = \det A = \det(\operatorname{circ}_2(a_1, 1 - a_1)) = 2a_1 - 1 > 1 .$$

For the algebraic complements we have

$$A_1 = a_1 , \quad A_2 = a_1 - 1$$

and so

$$(A_1, A_2) = 1$$

and

$$h = \frac{D}{(A_1, A_2)} = 2a_1 - 1 .$$

Then

$$a_1 \equiv a_1 - (2a_1 - 1) = 1 - a_1 = a_2 \pmod h$$

and for $n = 2$ the theorem is proved.

Now let $n > 2$ and let m be a natural number greater than 1 sich that $(m, n) = 1$. Then there is an integral rational number x such that

$$n \,.\, x \equiv 1 \pmod m$$

and $x \neq 1$. We put

$$z = 1 - (n - 1)\, x ,$$

then

$$z = (1 - nx) + x \equiv x \pmod m$$

and so there is an integral rational number t such that

$$z - x = t \,.\, m .$$

Now we shall prove that the matrix $A = \operatorname{circ}_n(z, x, x, \ldots, x)$ satisfies the assumptions of Theorem 2. From the definition we have

$$1 = z + (n - 1)\, x .$$

Clearly

$$z \equiv x \pmod{t \,.\, m}$$

and so it is sufficient to prove that $h = t \,.\, m$. By Proposition 2

$$D = \det A = \prod_{j=1}^{n} p_\gamma(\zeta^{j-1})$$

where $\gamma = (z, x, x, \ldots, x)$ is n-dimensional. We have

1) $p_\gamma(1) = z + (n - 1)\, x = 1,$

2) $p_\gamma(\zeta^{j-1}) = z + x\zeta^{j-1} + x\zeta^{2(j-1)} + \ldots + x\zeta^{(n-1)(j-1)} = z - x = t \,.\, m$
for $j > 1$.

Hence $D = (t \,.\, m)^{n-1}$ and $|D| > 1$.

For the algebraic complements we have

$$A_1 = \det(\mathrm{circ}_{n-1}(z, x, x, \ldots, x)) = (1 - x)(t \,.\, m)^{n-2}$$

and

$$|A_i| = |A_j|$$

for $i, j > 1$, because if we leave out the first row and the i-th column in the matrix A for $i > 1$ we get matrices transferable one to the other by means of an exchange of the rows. If we leave out the first row and the second column in the matrix A we get a matrix H which can be obtained also by replacing the first row of the matrix $\mathrm{circ}_{n-1}(z, x, x, \ldots, x)$ by the $(n-1)$-dimensional vector $(x, x, \ldots, x)$. If we multiply the first row of the matrix H by

$$\frac{1 - x}{x}$$

and subtract all the other rows from the first one we get the matrix $\mathrm{circ}_{n-1}(z, x, x, \ldots \ldots, x)$ by virtue of

$$z + (n - 1)\,x = 1 \,.$$

From the above we have

$$A_2 = -\frac{x}{1 - x}\det(\mathrm{circ}_{n-1}(z, x, x, \ldots, x)) = -x \,.\, (t \,.\, m)^{n-2} \,.$$

Then

$$(A_1, A_2, \ldots, A_n) = (t \,.\, m)^{n-2}$$

and so

$$h = t \,.\, m \,.$$

Theorem 3 is proved.

Corollary 2. *Let K be a cyclic algebraic number field with a normal integral basis. Then there are infinitely many orders of the field K with a normal basis.*

In the proof of Theorem 4 we shall need the following proposition.

Proposition 3 (Leopold [3]). *Let K be an Abelian algebraic number field. Then K has a normal integral basis if and only if K is contained in a cyclotomic field generated by the m-th primitive root of unity with a square-free m.*

Theorem 4. *Let K be an Abelian algebraic number field with a normal integral basis. Then there are infinitely many orders of the field K with a normal basis.*

Proof. Let $[K : Q] = n$. The Galois group $G = G(K/Q)$ is a finite Abelian group which contains n elements. The main theorem about Abelian groups yields that the group G can be decomposed into a direct sum of cyclic groups

$$G = \operatorname{dir} \sum_{j=1}^{k} C_j .$$

For $j = 1, 2, \ldots, k$ we put

$$l_j = \operatorname{card} C_j ;$$

then

$$n = \operatorname{card} G = \prod_{j=1}^{k} l_j .$$

By G_i, for $i = 1, 2, \ldots, k$, we denote the following subgroup of G:

$$G_i = \operatorname{dir} \sum_{\substack{j=1 \\ j \neq i}}^{k} C_j .$$

It follows from the Galois theory that for each of the groups G_i there is a subfield K_i of the field K such that the action of G_i on K_i is identical and

$$G(K_i/Q) \simeq G/G_i \simeq C_i .$$

The group $G(K_i/Q)$ can be identified with the group C_i because the restrictions of the automorphisms from C_i to K_i generate the group $G(K_i/Q)$.

The field K has a normal integral basis. Proposition 3 implies that each of the fields K_i has a normal integral basis. By Corollary 2, for $i = 1, 2, \ldots, k$, there are infinitely many orders of the field K_i with a normal basis. From the field K_i, for $i = 1, 2, \ldots, k$, we choose an order B_i with a normal basis.

$$\beta_i = \{x_{i,1}, x_{i,2}, \ldots, x_{i,l_i}\} .$$

No we shall show that the set

$$\beta(B_1, B_2, \ldots, B_k) = \{ \prod_{j=1}^{k} y_j \mid y_j \in \beta_j \}$$

is a normal basis of an order B of the field K.

Denote the least field generated by the fields K_i, K_j by

$$K_i \vee K_j .$$

Clearly

$$\bigvee_{j=1}^{k} K_j \subset K .$$

By e we denote the identical automorphism. Let $g \in G$ and $g \neq e$. Then

$$g = g_1 + g_2 + \ldots + g_k$$

where $g_i \in C_i$ and there is $g_j \neq e$. It means that there is $z_j \in K_j$ such that

$$g(z_j) = g_j(z_j) \neq z_j .$$

Now it follows from the Galois theory that

$$\bigvee_{j=1}^{k} K_j = K .$$

Consequently, any $z \in K$ can be written in the form

$$z = \sum_{j=1}^{m} \prod_{i=1}^{k} d_{i,j}$$

for $m \in Z$ and

$$d_{i,j} = \sum_{s=1}^{l_i} a_{s,j} \,.\, x_{i,s}$$

where $a_{s,j} \in Q$, $x_{i,s} \in \beta_i$. If we denote $\beta(B_1, B_2, \ldots, B_k) = \{t_1, t_2, \ldots, t_n\}$ we have

$$z = \sum_{r=1}^{n} a_r t_r$$

where $a_r \in Q$. So, from the above and from the fact that all elements from $\beta(B_1, B_2, \ldots, B_k)$ belong to Z_K (Remark 1) we conclude that the set $\beta(B_1, B_2, \ldots, B_k)$ is a basis of an n-dimensional Z-module $B \subset Z_K$. Now we shall prove that this basis is normal. Let t_u, t_v be elements from $\beta(B_1, B_2, \ldots, B_k)$, then

$$t_u = \prod_{i=1}^{k} x_{i,s_u} , \quad t_v = \prod_{i=1}^{k} x_{i,s_v}$$

where x_{i,s_u}, $x_{i,s_v} \in \beta_i$. Since each of the bases β_i is a normal basis of the corresponding K_i we have that for any i there is an automorphism $g_i \in C_i$ such that

$$g_i(x_{i,s_u}) = x_{i,s_v}$$

and so

$$(g_1 + g_2 + \ldots + g_k) \colon t_u \mapsto t_v .$$

This implies that $\beta(B_1, B_2, \ldots, B_k)$ is normal.

Lemma 1 yields that

$$\sum_{r=1}^{n} t_r = \prod_{i=1}^{k} \sum_{j=1}^{l_i} x_{i,j} = \pm 1$$

and so $1 \in B$.

Now we shall prove that B is a ring. To this end it is sufficient to show that $t_i \,.\, t_j \in B$ for $i, j \in \{1, 2, \ldots, n\}$. Let

$$t_i = \prod_{s=1}^{k} x_{s,i_s} , \quad t_j = \prod_{s=1}^{k} x_{s,j_s}$$

where $i_s, j_s \in \{1, 2, \ldots, l_s\}$. Then

$$t_i t_j = \prod_{s=1}^{k} x_{s,i_s} \cdot x_{s,j_s}$$

and from the fact that each of

$$x_{s,i_s} \cdot x_{s,j_s}$$

can be expressed as a linear combination of elements from β_s with integral rational coefficients we have that $t_i t_j$ is a linear combination of elements from $\beta(B_1, B_2, \ldots, B_k)$ with integral rational coefficients. Hence it follows that B is a ring and thus an order of the field K with a normal basis.

Now if B_i' is an order of the field K_i with a normal basis and $B_i' \neq B_i$ we get a normal basis

$$\beta(B_1, B_2, \ldots, B_{i-1}, B_i', B_{i+1}, \ldots, B_k)$$

of an order B' of the field K. The set

$$\beta(B_1, B_2, \ldots, B_{i-1}, B_{i+1}, \ldots, B_k)$$

is a basis of the field K over the field K_i and we get B and B' as all linear combinations of elements from this basis with coefficients from B_i and B_i', respectively. The fact that an expression in a basis is unique yields that $B \neq B'$.

The proof of the theorem now follows by Corollary 2.

Now we shall show, in the quadratic field of algebraic numbers K with the integral normal basis, an example of an order invariant with respect to the Galois group $G(K/Q)$, which has no normal basis.

Example 1. Let $K = Q(\sqrt{d})$, where

1. $d \neq 1$,
2. $d \equiv 1 \pmod 4$,
3. $p^2 \nmid d$ for all primes p.

By ([1], p. 154) the numbers

$$1, \quad \frac{1 + \sqrt{d}}{2}$$

form a basis of the ring Z_K over the ring of integral rational numbers Z, hence an integral basis of the field K. Now we show that the numbers

$$\frac{1 - \sqrt{d}}{2}, \quad \frac{1 + \sqrt{d}}{2}$$

form a normal integral basis of the field K. The property of being integral follows from the fact that this basis is obtained from the basis

$$1, \quad \frac{1 + \sqrt{d}}{2}$$

by the transformation with the unimodular matrix

$$\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}.$$

The fact that these elements are the roots of the polynomial

$$x^2 - x + \frac{1-d}{4}$$

which is irreducible over Q implies that this basis is also normal.

Now it is easy to see that the generating automorphism g of the group $G(K/Q)$ can be represented as

$$g: \frac{1-\sqrt{d}}{2} \mapsto \frac{1+\sqrt{d}}{2}.$$

It is clear that the Z-module $B = Z[1, \sqrt{d}]$ is an order in the field K, which is invariant with respect to $G(K/Q)$. Further,

$$\mathrm{Tr}_{K/Q}(\sqrt{d}) = \sqrt{d} - \sqrt{d} = 0$$

and

$$\mathrm{Tr}_{K/Q}(1) = 2,$$

hence the order B contains no element of the trace 1. By Lemma 1 the order B has no normal basis.

In the following example we shall show a ring A with a normal basis, which is a complete module in the cubic field of algebraic numbers K without an integral normal basis. This example does not contradict Corollary 1, because the ring A does not contain the unit element.

Example 5.2. Let $L = Q(\zeta)$, where ζ is a primitive root of degree 9 from 1. By [5], L is a normal extension of degree 6 over the field Q. The numbers

$$1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5$$

form a basis of the ring of integral numbers Z_L over Z and the Galois group $G(L/Q)$ is isomorphic to the multiplicative group of residual classes (mod 9) prime to 9. In our case $G(L/Q)$ is a cyclic group of order 6. The elements of the group $G(L/Q)$ map the primitive roots of degree 9 from 1 onto the primitive roots of degree 9 from 1. If ζ is a primitive root, then

$$\zeta, \zeta^2, \zeta^4, \zeta^5, \zeta^7, \zeta^8$$

are all the primitive roots. The element $g \in G(L/Q)$ which maps

$$\zeta \mapsto \zeta^8$$

has order 2 and hence forms a cyclic subgroup of order 2, under which by the main theorem of the Galois theory the cyclic extension K of the field Q of degree 3, $L \supset K \supset Q$ remain fixed.

Now we shall show that the submodule $A = Z[\alpha_1, \alpha_2, \alpha_3]$ of the ring of integral numbers Z_K of the field K, where

$$\alpha_1 = 1 + \zeta + \zeta^8 , \quad \alpha_2 = 1 + \zeta^2 + \zeta^7 , \quad \alpha_3 = 1 + \zeta^4 + \zeta^5 ,$$

is a complete Z-module with the normal basis $\alpha_1, \alpha_2, \alpha_3$, and simultaneously a subring of the ring Z_K. We shall also show that Z_K contains no element of the trace 1 and hence the field K has no normal integral basis.

To show that $\alpha_1, \alpha_2, \alpha_3$ form a normal basis of a complete submodule of the ring Z_K we need to show that

(1) $\alpha_1, \alpha_2, \alpha_3$ belong to Z_K;

(2) $\alpha_1, \alpha_2, \alpha_3$ are linearly independent over Q;

(3) $\alpha_1, \alpha_2, \alpha_3$ are mapped onto each other under automorphisms of the group $G(K/Q)$.

(1) follows from the fact that these elements belong to Z_L and remain fixed under the automorphism $g \in G(L/Q)$, under which the field K remains fixed.

Now we prove (2). Let

$$a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 = 0$$

where $a_1, a_2, a_3 \in Q$. Using

$$\zeta^6 + \zeta^3 + 1 = 0 ,$$

which means that the sum of all roots from 1 of degree 3 is equal to 0, we lower the exponents in the expressions for α_i. In this way we get

$$0 = 1 . (a_1 + a_2 + a_3) + \zeta(a_1 - a_2) + \zeta^2(a_2 - a_1) + \\ + \zeta^4(a_3 - a_2) + \zeta^5(a_3 - a_1) .$$

As

$$1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5$$

form an integral basis of the field L over Q we get that all coefficients in the last expression are equal to 0. From this it can be easily shown that

$$a_1 = a_2 = a_3 = 0$$

This proves (2).

(3) follows from the fact that the generating automorphism h of the group $G(L/Q)$

$$h\colon \zeta \mapsto \zeta^2$$

restricted to the field K is a generating automorphism h of the group $G(K/Q)$, which maps α_1 on α_2, α_2 on α_3 and α_3 on α_1.

Thus we have proved that A is a complete submodule of the ring Z_K.

It is easy to show that

$$\alpha_1^2 = 2\alpha_1 + \alpha_2\,, \quad \alpha_2^2 = 2\alpha_2 + \alpha_3\,, \quad \alpha_3^2 = 2\alpha_3 + \alpha_1\,,$$

$$\alpha_1\alpha_2 = \alpha_1 - \alpha_3\,, \quad \alpha_2\alpha_3 = \alpha_2 - \alpha_1\,, \quad \alpha_3\alpha_1 = \alpha_3 - \alpha_2\,.$$

Hence we see that A is a subring of Z_K.

Now we shall show that Z_K contains no element of the trace 1. The proof proceeds by way of contradiction.

Let $\alpha \in Z_K$ be such that

$$\mathrm{Tr}_{K/Q}(\alpha) = 1\,.$$

As $\alpha_1, \alpha_2, \alpha_3$ is a basis of the field K over Q we can express α using rational coefficients:

$$\alpha = a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3\,.$$

Now we shall evaluate the trace of the element α by using the last expression:

$$\mathrm{Tr}_{K/Q}(\alpha) = a_1\,\mathrm{Tr}_{K/Q}(\alpha_1) + a_2\,\mathrm{Tr}_{K/Q}(\alpha_2) + a_3\,\mathrm{Tr}_{K/Q}(\alpha_3) = (a_1 + a_2 + a_3)\,.\,3\,.$$

Hence

$$a_1 + a_2 + a_3 = \tfrac{1}{3}\,.$$

Now, similarly as in the proof of linear independence of the basis $\alpha_1, \alpha_2, \alpha_3$, we express α in the integral basis of the field L as

$$\alpha = 1\,.\,(a_1 + a_2 + a_3) + \zeta(a_1 - a_2) + \zeta^2(a_2 - a_1) + \\ + \zeta^4(a_3 - a_2) + \zeta^5(a_3 - a_1)\,.$$

The fact that the coefficient at 1 is not an integral rational number yields that $\alpha \notin Z_L$ and hence $\alpha \notin Z_K$ which contradicts the assumption.

Thus we have proved that Z_K does not contain any element of the trace 1 and hence we conclude from Theorem 1 that the field K has no integral normal basis.

Lemma 1 together with the fact that the trace of the basis elements $\alpha_1, \alpha_2, \alpha_3$ is equal to 3 imply that A is not an order of the field K.

From the preceding it could appear that if an Abelian field of algebraic numbers contains an integral element with a trace h, then there is a ring $A \subset Z_K$ with a normal basis, whose elements have the trace h. The following example shows that this need not be true.

Example 3. Let $K = Q(\sqrt{2})$. By ([1], p. 154) the integral basis of the field K is

$$1,\ \sqrt{2}\,.$$

Hence

$$\mathrm{Tr}_{K/Q}(1) = 2\,, \quad \mathrm{Tr}_{K/Q}(\sqrt{2}) = 0\,.$$

Consequently, if there exists a ring $A \subset Z_K$ with a normal basis x_1, x_2 where

$\mathrm{Tr}_{K/Q}(x_1) = 2$ then

$$x_1 = 1 + l \cdot \sqrt{2}$$

where $l \in Z$. Then

$$x_1 \cdot x_2 = (1 + l \cdot \sqrt{2})(1 - l\sqrt{2}) = 1 - 2l .$$

It means that $x_1 x_2$ can not be expressed in the basis x_1, x_2 with integral rational coefficients, because $1 - 2l$ is odd.

Hence we have shown that though the field K contains an integral element of the trace 2, it does not contain any subring $A \subset Z_K$ with a normal basis, whose elements have the trace 2.

References

[1] *Z. Borevič; I. R. Šafarevič:* Elements of the number theory (Russian) Nauka, Moscow 1972.

[2] *Davis, P. J.:* Circulant matrices. A. Wiley-Interscience publishers, John Wiley and sons, New York—Chichester—Brisbane—Toronto, 1979.

[3] *Leopold, H. W.:* Zur Arithmetic in abelschen Zahlkörpern, J. Reine Angew. Math. *209*, 1962.

[4] *Martinet, J.:* Modules sur l'algebre du groupe quaternionien. Ann. Sci. École. Norm. Sup *4*, 1971.

[5] *Narkiewicz, W.:* Elementary and analytic theory of algebraic numbers, PWN, Warszawa 1974.

Author's address: 814 73 Bratislava, Obrancov mieru 49, Czechoslovakia (Matematický ústav SAV).