VERSITA

Mathematica Slovaca

DOI: 10.2478/s12175-008-0064-5
Math. Slovaca **58** (2008), No. 2, 165–172

A NOTE ON NORMAL BASES OF IDEALS IN SEXTIC ALGEBRAIC NUMBER FIELD

Viktor Dubovský* — Juraj Kostra** — Vladimír Lazar***

(*Communicated by Stanislav Jakubec*)

ABSTRACT. Let K/Q be a cyclic tamely ramified extension of degree 6, then any ambiguous ideal of K has a normal basis.

In the present paper we will prove that any ambiguous ideal of cyclic algebraic field with squarefree conductor m of degree 6 over the rationals $\mathbb{Q}$ has a normal basis.

First we recall some general properties of ambiguous ideals according to Ullom [2]. Let K/F be a Galois extension of algebraic number field F with Galois group G, let $\mathbb{Z}_K$ (resp. $\mathbb{Z}_F$) be the ring of integers of K (resp. F).

Definition. An ideal U (possibly fractional) of K is *G-ambiguous* or simply ambiguous if U is invariant under the action of the Galois group G.

Let $\mathfrak{P}$ be a prime ideal of F whose decomposition into prime ideals in K is

$$\mathfrak{P}\mathbb{Z}_K = (\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_g)^e.$$

Let $\Psi(\mathfrak{P}) = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_g$. It is known that

- $\Psi(\mathfrak{P})$ is ambiguous and the set of the all $\Psi(\mathfrak{P})$ with $\mathfrak{P}$ prime in F, is a free basis for the group of ambiguous ideals of K
- An ambiguous ideal U of K may be written in the form $U_O T$, where T is an ideal of F and

$$U_O = \Psi(\mathfrak{P}_1)^{a_1} \dots \Psi(\mathfrak{P}_t)^{a_t}, \qquad 0 < a_i \le e_i,$$

2000 Mathematics Subject Classification: Primary 11R33.
Keywords: normal basis, ambiguous ideal, circulant matrix.
Supported by grants GAČR 201/07/0191, VEGA 2/4138/04, VEGA 1/0084/08.

where $e_i > 1$ is the ramification index of a prime ideal of K dividing $\mathfrak{P}_i$. The ideal U determines U_O and T uniquely. The ambiguous ideal U_O is called a *primitive ambiguous ideal.* By [2, Remark 1.7] for $K/\mathbb{Q}$ the problem of showing that an ambiguous ideal of K has a normal basis is reduced to the corresponding problem for primitive ambiguous ideals.

Ullom [2, Corollary 1.2] showed that $\mathrm{Tr}_{K/F}(U) = U \cap F$ for K/F is tamely ramified. Consequently, if F is a Galois extension of $\mathbb{Q}$ and ideal U of K has a normal basis over the rational integers $\mathbb{Z}$ then $U \cap F$ has a normal basis over $\mathbb{Z}$.

We will prove the following theorem:

Theorem 1. *Let $K/\mathbb{Q}$ be a cyclic tamely ramified extension of degree 6, then any ambiguous ideal of K has a normal basis.*

First we will prove the following lemma:

Lemma 1. *Let K be cyclic extension of rationals with $[K:\mathbb{Q}] = 6$ and $K \subseteq \mathbb{Q}(\zeta_p)$ with prime p, then any ambiguous ideal of $\mathbb{Z}_K$ has a normal basis.*

Proof. Let $\alpha \in \mathbb{Z}_{\mathbb{Q}(\zeta_3)}$ then it could be expressed as $\alpha = a_1 + a_2\,\zeta_6 + a_3\,\zeta_6^2 + a_4\,\zeta_6^3 + a_5\,\zeta_6^4 + a_6\,\zeta_6^5$, with $a_i \in \mathbb{Z}$, $i = 1, 2, \ldots, 6$.

Since relations among ζ_6 and ζ_3 are

$$\zeta_6 = -\zeta_3^2, \quad \zeta_6^2 = \zeta_3, \quad \zeta_6^3 = -1,$$
$$\zeta_6^4 = \zeta_3^2, \quad \zeta_6^5 = -\zeta_3, \quad \zeta_6^6 = 1,$$

one can rewrite α as

$$\begin{aligned} \alpha &= a_1 - a_2\,\zeta_3^2 + a_3\,\zeta_3 - a_4 + a_5\,\zeta_3^2 + a_6\,\zeta_3 \\ &= (a_1 - a_4) + (a_3 - a_6)\,\zeta_3 + (a_5 - a_2)\,\zeta_3^2. \end{aligned}$$

Denote by $\mathbf{A}_\alpha$ the circulant matrix of the element α coefficients, i.e.

$$\mathbf{A}_\alpha = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_6 & a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_6 & a_1 & a_2 & a_3 & a_4 \\ a_4 & a_5 & a_6 & a_1 & a_2 & a_3 \\ a_3 & a_4 & a_5 & a_6 & a_1 & a_2 \\ a_2 & a_3 & a_4 & a_5 & a_6 & a_1 \end{pmatrix}.$$

Also denote by $\mathbf{X}$ following unimodular matrix

$$\mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

The matrix $\mathbf{A}_\alpha$ is similar to the block matrix

$$\mathbf{A}_{\alpha,\,\text{block}} = \mathbf{X}\,\mathbf{A}_\alpha\,\mathbf{X}^{-1}$$

$$= \left(\begin{array}{ccc|ccc} a_1-a_4 & a_3-a_6 & a_5-a_2 & a_4 & a_6 & a_2 \\ a_5-a_2 & a_1-a_4 & a_3-a_6 & a_2 & a_4 & a_6 \\ a_3-a_6 & a_5-a_2 & a_1-a_4 & a_6 & a_2 & a_4 \\ \hline 0 & 0 & 0 & a_1+a_4 & a_3+a_6 & a_5+a_2 \\ 0 & 0 & 0 & a_5+a_2 & a_1+a_4 & a_3+a_6 \\ 0 & 0 & 0 & a_3+a_6 & a_5+a_2 & a_1+a_4 \end{array}\right)$$

$$\mathbf{A}_{\alpha,\,\text{block}} = \left(\begin{array}{c|c} \mathbf{A}_\alpha^- & \mathbf{B}_\alpha \\ \hline \mathbf{0} & \mathbf{A}_\alpha^+ \end{array}\right). \tag{1}$$

Note that each of blocks is circulant and, because of the zero matrix block, the determinant of $\mathbf{A}_\alpha$ depends only on blocks $\mathbf{A}_\alpha^+$ and $\mathbf{A}_\alpha^-$. Particularly is

$$|\mathbf{A}_\alpha| = |\mathbf{A}_{\alpha,\,\text{block}}| = |\mathbf{A}_\alpha^+|\,|\mathbf{A}_\alpha^-|.$$

Let $\gamma \in \mathbb{Q}(\zeta_3)$, be of the form $\gamma = c_1 + c_2\,\zeta_3 + c_3\,\zeta_3^2$, with $c_1 + c_2 + c_3 = \pm 1$, then such element γ is representable by circulant matrix $\mathbf{A}_\gamma = \text{circ}_3(c_1, c_2, c_3)$, and its determinant is

$$\begin{aligned} |\mathbf{A}_\gamma| &= (c_1 + c_2 + c_3)\,(c_1 + c_2\,\zeta_3 + c_3\,\zeta_3^2)\,(c_1 + c_2\,\zeta_3^2 + c_3\,\zeta_3) \\ &= \pm N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\gamma). \end{aligned}$$

Consider now element γ with norm equal to p, such element exists in $\mathbb{Q}(\zeta_3)$ for all p. It is easy to see that if we replace $\mathbf{A}_\alpha^+$ by $\mathbf{A}_\gamma$ and $\mathbf{A}_\alpha^-$ by the identity matrix, then the resulting matrix will have determinant p as we demanded.

This together with form of blocks in (1) yields the following system of linear equations

$$\begin{aligned} a_1 - a_4 &= c_1, & a_1 + a_4 &= 1, \\ a_3 - a_6 &= c_2, & a_3 + a_6 &= 0, \\ a_5 - a_2 &= c_3, & a_5 + a_2 &= 0, \end{aligned}$$

with solutions

$$\begin{aligned} a_1 &= \frac{1+c_1}{2}, & a_2 &= \frac{-c_3}{2}, & a_3 &= \frac{c_2}{2}, \\ a_4 &= \frac{1-c_1}{2}, & a_5 &= \frac{c_3}{2}, & a_6 &= \frac{-c_2}{2}. \end{aligned} \tag{2}$$

From this it follows directly that in order to get solutions from $\mathbb{Z}$ the coefficient c_1 has to be odd and c_2, c_3 even. Because we demanded $\sum_{i=1}^{3} c_i = \pm 1$ we are forced to have odd number of odd coefficients in expression of γ, but determinant of $\text{circ}_3(2\,k+1, 2\,l+1, 2\,m+1)$ equals to $4\,z$ with $z \in \mathbb{Z}$ and hence could not be prime, so exactly one of c_i is odd. We may always assume c_1 to be odd one, since in case of c_2 resp. c_3 one could multiply such $\tilde{\gamma}$ by ζ_3 resp. ζ_3^2 and get γ with c_1 odd.

This way we obtained element $\alpha_1 \in \mathbb{Q}(\zeta_6)$

$$\begin{aligned}
\alpha_1 &= a_1 + a_2\,\zeta_6 + a_3\,\zeta_6^2 + a_4\,\zeta_6^3 + a_5\,\zeta_6^4 + a_6\,\zeta_6^5 \\
&= \frac{1+c_1}{2} + \frac{-c_3}{2}\,\zeta_6 + \frac{c_2}{2}\,\zeta_6^2 + \frac{1-c_1}{2}\,\zeta_6^3 + \frac{c_3}{2}\,\zeta_6^4 + \frac{-c_2}{2}\,\zeta_6^5 \\
&= \left(\frac{1+c_1}{2} - \frac{1-c_1}{2}\right) + \left(\frac{c_2}{2} - \frac{-c_2}{2}\right)\zeta_3 + \left(\frac{c_3}{2} - \frac{-c_3}{2}\right)\zeta_3^2 \\
&= c_1 + c_2\,\zeta_3 + c_3\,\zeta_3^2 = \gamma
\end{aligned}$$

The element α_1 matrix $\mathbf{A}_{\alpha_1} = \operatorname{circ}_6(a_1, a_2, \ldots, a_6)$ could be also obtained from the matrix identity

$$\mathbf{A}_{\alpha_1} = \mathbf{X}^{-1}\,\mathbf{S}_1\,\mathbf{X},$$

where

$$\mathbf{S}_1 = \left(\begin{array}{c|c} \mathbf{A}_\gamma & \mathbf{C}_1 \\ \hline \mathbf{0} & \mathbf{E} \end{array}\right),$$

with blocks $\mathbf{A}_\gamma$ is the circulant matrix representing γ, $\mathbf{0}$ is the zero matrix, $\mathbf{E}$ is the unit matrix and $\mathbf{C}_1 = \operatorname{circ}_3((1-c_1)/2, -c_3/2, -c_2/2) = \frac{1}{2}(\mathbf{E} - \mathbf{A}_\gamma)$.

Interchanging the roles of $\mathbf{A}_\gamma$ and $\mathbf{E}$ we obtain

$$\mathbf{S}_2 = \left(\begin{array}{c|c} \mathbf{E} & \mathbf{C}_2 \\ \hline \mathbf{0} & \mathbf{A}_\gamma \end{array}\right)$$

with block $\mathbf{C}_2 = \frac{1}{2}(\mathbf{A}_\gamma - \mathbf{E})$, which is yielding matrix

$$\mathbf{A}_{\alpha_2} = \mathbf{X}^{-1}\,\mathbf{S}_2\,\mathbf{X},$$

and henceforth element $\alpha_2 \in \mathbb{Q}(\zeta_6)$

$$\begin{aligned}
\alpha_2 &= \frac{1+c_1}{2} + \frac{c_3}{2}\,\zeta_6 + \frac{c_2}{2}\,\zeta_6^2 + \frac{-1+c_1}{2}\,\zeta_6^3 + \frac{c_3}{2}\,\zeta_6^4 + \frac{c_2}{2}\,\zeta_6^5 \\
&= \left(\frac{1+c_1}{2} - \frac{-1+c_1}{2}\right) + \left(\frac{c_2}{2} - \frac{c_2}{2}\right)\zeta_3 + \left(\frac{c_3}{2} - \frac{c_3}{2}\right)\zeta_3^2 = 1.
\end{aligned}$$

Note that we get elements γ and 1 from $\mathbb{Q}(\zeta_3)$, but this time via α_1 resp. α_2 as elements $\mathbb{Q}(\zeta_6)$, so obviously for both α_1, α_2 the sum $\sum\limits_{i=1}^{6} a_i = \pm 1$ and furthermore determinants of $\mathbf{A}_{\alpha_1}$, $\mathbf{A}_{\alpha_2}$ are equal to p.

Let us now recall some facts proven in the article of Ullom [2], namely that if K is subfield of $\mathbb{Q}(\zeta_p)$ with degree $[K:\mathbb{Q}] = l$, and (Π) is ideal with normal basis generated by element $1-\zeta_p$, then ideal $(\pi) = (\Pi) \cap K$ has normal basis generated by $\operatorname{Tr}_{\mathbb{Q}(\zeta_p)/K}(1-\zeta_p)$.

By [1], normal basis of the ideal (π^t) could be transformed to the normal basis of (π^{t+1}), for $t = 1, 2, \ldots, l$, by circulant matrix $\mathrm{circ}_l(c_1, c_2, \ldots, c_{l-1})$, where c_i are such that $\sum_{i=1}^{l} c_i = \pm 1$ and

$$\begin{aligned} |N_{K/\mathbb{Q}}(c_1 + c_2\,\zeta_l + \cdots + c_l\,\zeta_l^{l-1})| &= p, && (3)\\ c_1 + c_2\,g^t + \cdots + c_l (g^t)^{l-1} &\equiv 0 \pmod p && (4)\end{aligned}$$

with $g = a^{\frac{p-1}{l}}$, where a is such a positive integer that the automorphism

$$\sigma\colon \zeta_p \longmapsto \zeta_p^a,$$

restricted to the field K is nontrivial.

Let $\gamma = c_1 + c_2\,\zeta_3 + c_3\,\zeta_3^2$ be such that it satisfies these conditions for $g = a^{\frac{p-1}{3}}$ with suitable a, especially that the congruence (4) holds. We shall prove that for elements α_1, α_2 the same is true.

Let us consider $\tilde{g} = a^{\frac{p-1}{6}}$ with a as above. It is easy to see, that

$$\begin{aligned} g^3 &\equiv 1 \pmod p, & \tilde{g}^3 &\equiv -1 \pmod p,\\ g &\equiv \tilde{g}^2 \pmod p, & \tilde{g}^6 &\equiv 1 \pmod p,\end{aligned}$$

and as an easy consequence of that $-\tilde{g} \equiv g^2 \pmod p$.

Now we are in position to solve congruences

$$a_1 + a_2\,\tilde{g}^k + a_3\,(\tilde{g}^k)^2 + a_4\,(\tilde{g}^k)^3 + a_5\,(\tilde{g}^k)^4 + a_6\,(\tilde{g}^k)^5 \equiv 0 \pmod p. \qquad (5)$$

But using the relations among g and $\tilde{g}$, together with fact that a_i depend on c_j as a solutions of equations above, we get tables with dependence of k solving congruences (5) and solution t of congruence (4).

$k=1$	$c_1 + c_2\,\tilde{g}^2 - c_3\,\tilde{g}$	$\equiv$	$c_1 + c_2\,g + c_3\,g^2 \pmod p$	$t=1$
$k=2$	1	$\equiv$	$1 \pmod p$	
$k=3$	$c_1 + c_2 + c_3$	$\equiv$	$1 \pmod p$	
$k=4$	1	$\equiv$	$1 \pmod p$	
$k=5$	$c_1 - c_2\,\tilde{g} + c_3\,\tilde{g}^2$	$\equiv$	$c_1 + c_2\,g^2 + c_3\,g \pmod p$	$t=2$

$k=1$	1	$\equiv$	$1 \pmod p$	
$k=2$	$c_1 - c_2\,\tilde{g} + c_3\,\tilde{g}^2$	$\equiv$	$c_1 + c_2\,g^2 + c_3\,g \pmod p$	$t=2$
$k=3$	1	$\equiv$	$1 \pmod p$	
$k=4$	$c_1 + c_2\,\tilde{g}^2 - c_3\,\tilde{g}$	$\equiv$	$c_1 + c_2\,g + c_3\,g^2 \pmod p$	$t=1$
$k=5$	1	$\equiv$	$1 \pmod p$	

This way we obtained solutions of (5) for $k = 1, 2, 4, 5$, i.e. two for each solution of (4). Particularly from this tables it is easy to see that if congruence corresponding to γ is solved by t, then the congruence corresponding to α has solutions $k \equiv t \pmod 3$.

Since one could get only two solutions from each γ and γ', it is impossible to obtain the solution with $k = 3$ same way as those for $k = 1, 2, 4, 5$.

To get such solution construct now following circulant matrix

$$\mathbf{A}_3 = \operatorname{circ}_6\left(\frac{p-1}{6}+1, -\frac{p-1}{6}, \frac{p-1}{6}, -\frac{p-1}{6}, \frac{p-1}{6}, -\frac{p-1}{6}\right).$$

The determinant of $\mathbf{A}_3$ is equal to p and

$$\begin{aligned} &\frac{p-1}{6}+1-\frac{(p-1)\tilde{g}^3}{6}+\frac{(p-1)(\tilde{g}^3)^2}{6} \\ -&\frac{(p-1)(\tilde{g}^3)^3}{6}+\frac{(p-1)(\tilde{g}^3)^4}{6}-\frac{(p-1)(\tilde{g}^3)^5}{6} &= \\ \frac{p-1}{6}+1+&\frac{p-1}{6}+\frac{p-1}{6}+\frac{p-1}{6}+\frac{p-1}{6}+\frac{p-1}{6} &\equiv \quad 0 \pmod p \end{aligned}$$

Thus we have five circulant matrices $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4, \mathbf{A}_5$ which transform normal basis of ambiguous ideals, i.e.

$$(\pi) \xrightarrow{\mathbf{A}_1} (\pi^2) \xrightarrow{\mathbf{A}_2} (\pi^3) \xrightarrow{\mathbf{A}_3} (\pi^4) \xrightarrow{\mathbf{A}_4} (\pi^5) \xrightarrow{\mathbf{A}_5} (\pi^6),$$

and the lemma is proved. □

LEMMA 2. *Let K be as in* Theorem 1 *with squarefree conductor $m = p_1 p_2 \cdots p_s$, where p_i is a prime for $i = 1, 2, \dots, s$. Let $\mathbb{Q} \subset L_{p_i} \subset \mathbb{Q}(\zeta_{p_i})$, $[L_{p_i} : \mathbb{Q}] = 6$. Then*

$$K \subset \bigvee_{i=1}^{s} L_{p_i}.$$

P r o o f. The proof is by the same way as the proof of [1, Lemma 2] for field extension of prime degree l.

$$G\Big(\mathbb{Q}(\zeta_m)/\bigvee_{i=1}^{s} L_{p_i}\Big) \cong H_1 \times H_2 \times \cdots \times H_s = H$$

with

$$H_i \subset (\mathbb{Z}/p_i\mathbb{Z})^* \qquad \text{for} \quad i = 1, 2 \dots, s$$

and the index

$$[(\mathbb{Z}/p_i\mathbb{Z})^* : H_i] = 6.$$

Clearly $H = [(\mathbb{Z}/m\mathbb{Z})^*]^6$. Let $G = G(\mathbb{Q}(\zeta_m)/K)$. It is sufficient to show that $H \subset G$. Let $x \in (\mathbb{Z}/m\mathbb{Z})^*$. The order of the group $(\mathbb{Z}/m\mathbb{Z})^*/G$ equals 6 and so $x^6 \in G$. Thus we have $H \subset G$. □

P r o o f o f t h e T h e o r e m 1. By Lemma 1, any ambiguous ideal of L_{p_i}, $i = 1, 2, \dots, s$, has a normal basis. By [2, Proposition 1.8], any ambiguous ideal of $\bigvee_{i=1}^{s} L_{p_i}$ has a normal basis and so by [2, Corollary 1.2], any ideal of K has a normal basis. This proves Theorem 1. $\square$

Example. We shall illustrate the above results in field $K \subset \mathbb{Q}(\zeta_{13})$ with $[K : \mathbb{Q}] = 6$. By U l l o m [2, Corollary 1.2], a normal basis of ideal $\Pi \subset \mathbb{Z}[\zeta_{13}]$ is generated by element $1 - \zeta_{13}$ and hence the normal basis of ideal $\pi \subset \mathbb{Z}_K$ is generated by $\mathrm{Tr}_{\mathbb{Q}(\zeta_{13})/K}(1 - \zeta_{13}) = 2 - \zeta_{13} - \zeta_{13}^{12}$.

Since $a = 2$ is primitive root modulo $p = 13$, we have got

$$g = a^{\frac{p-1}{3}} = 2^{\frac{12}{3}} = 16, \qquad \tilde{g} = a^{\frac{p-1}{6}} = 2^{\frac{12}{6}} = 4.$$

Element $\gamma = 1 - 2\,\zeta_3 + 2\,\zeta_3^2 \in \mathbb{Q}(\zeta_3)$ is represented by circulant matrix $\mathbf{A}_\gamma = \mathrm{circ}_3(1, -2, 2)$ and has norm equal to 13 and sum of its coefficients 1, henceforth it satisfies condition of [1].

It is easy to find that solutions of (4) are

$$\begin{aligned} 1 - 2\,g + 2\,g^2 &= 1 - 2 \cdot 16 + 2 \cdot 256 \\ &= 481 \equiv 0 \pmod{13}, \\ 1 + 2\,g^2 - 2\,(g^2)^2 &= 1 + 2 \cdot 256 - 2 \cdot 65536 \\ &= -130559 \equiv 0 \pmod{13}, \end{aligned}$$

where the second equalities are obtained from element $\gamma' = 1 + 2\,\zeta_3 - 2\,\zeta_3^2$ i.e. conjugate of γ. From this we see that matrix $\mathrm{circ}_3(1, -2, 2)$ transforms basis of ideal Π to the basis of Π^2 and $\mathrm{circ}_3(1, 2, -2)$ transforms basis of Π^2 to the basis of Π^3.

Using the methods described above one could obtain this five elements of $\mathbb{Q}(\zeta_6)$ and henceforth transformating circulant matrices. They are written in following tables, with indices such that α_i resp. $\mathbf{A}_i$ transforms normal basis of π^i to the normal basis of ideal π^{i+1}.

$\alpha_1 = 1 - 1\,\zeta_6 - 1\,\zeta_6^2 + 1\,\zeta_6^4 + 1\,\zeta_6^5$	$\mathbf{A}_1 = \mathrm{circ}_6(1, -1, -1, 0, 1, 1)$
$\alpha_2 = 1 - 1\,\zeta_6 + 1\,\zeta_6^2 - 1\,\zeta_6^4 + 1\,\zeta_6^5$	$\mathbf{A}_2 = \mathrm{circ}_6(1, -1, 1, 0, -1, 1)$
$\alpha_3 = 3 - 2\,\zeta_6 + 2\,\zeta_6^2 - 2\,\zeta_6^3 + 2\,\zeta_6^4 - 2\,\zeta_6^5$	$\mathbf{A}_3 = \mathrm{circ}_6(3, -2, 2, -2, 2, -2)$
$\alpha_4 = 1 + 1\,\zeta_6 - 1\,\zeta_6^2 + 1\,\zeta_6^4 - 1\,\zeta_6^5$	$\mathbf{A}_4 = \mathrm{circ}_6(1, 1, -1, 0, 1, -1)$
$\alpha_5 = 1 + 1\,\zeta_6 + 1\,\zeta_6^2 - 1\,\zeta_6^4 - 1\,\zeta_6^5$	$\mathbf{A}_5 = \mathrm{circ}_6(1, 1, 1, 0, -1, -1)$

TABLE 1. Elements α_i and transformation matrices

Thus we get following table of ideals together with generators of their normal bases

Ideal	Normal basis generator
(π)	$2-\zeta_{13}-\zeta_{13}^{12}$
(π^2)	$2-\zeta_{13}+\zeta_{13}^2-\zeta_{13}^3+\zeta_{13}^4-\zeta_{13}^6$ $-\zeta_{13}^{12}+\zeta_{13}^{11}-\zeta_{13}^{10}+\zeta_{13}^9-\zeta_{13}^7$
(π^3)	$2-\zeta_{13}+2\,\zeta_{13}^2-2\,\zeta_{13}^6$ $-\zeta_{13}^{12}+2\,\zeta_{13}^{11}-2\,\zeta_{13}^7$
(π^4)	$2-3\zeta_{13}+4\,\zeta_{13}^2-2\,\zeta_{13}^3-2\,\zeta_{13}^4+2\,\zeta_{13}^5$ $-3\,\zeta_{13}^{12}+4\,\zeta_{13}^{11}-2\,\zeta_{13}^{10}-2\,\zeta_{13}^9+2\,\zeta_{13}^8$
(π^5)	$2-7\zeta_{13}+5\,\zeta_{13}^2-\zeta_{13}^3+\zeta_{13}^4-2\,\zeta_{13}^5+3\,\zeta_{13}^6$ $-7\,\zeta_{13}^{12}+5\,\zeta_{13}^{11}-\zeta_{13}^{10}+\zeta_{13}^9-2\,\zeta_{13}^8+3\,\zeta_{13}^7$
(π^6)	$2-11\,\zeta_{13}+2\,\zeta_{13}^2+2\,\zeta_{13}^3+2\,\zeta_{13}^4+2\,\zeta_{13}^5+2\,\zeta_{13}^6$ $-11\,\zeta_{13}^{12}+2\,\zeta_{13}^{11}+2\,\zeta_{13}^{10}+2\,\zeta_{13}^9+2\,\zeta_{13}^8+2\,\zeta_{13}^7$

REFERENCES

[1] JAKUBEC, S.—KOSTRA, J.: *A note on normal bases of ideals*, Math. Slovaca, **42** (1992), 677–684.

[2] ULLOM, S.: *Normal bases in Galois extensions of number fields*, Nagoya Math. J. **34** (1969), 153–167.

Received 21. 5. 2006

* *Department of Mathematics and Geometry*
Technical University of Ostrava
17. listopadu 15
CZ–708 33 Ostrava
CZECH REPUBLIC
E-mail: viktor.dubovsky@vsb.cz

** *Department of Mathematics*
Padagogical faculty
University of Ostrava
Mlýnská 5
CZ–701 03 Ostrava
CZECH REPUBLIC
E-mail: juraj.kostra@osu.cz

** *** *Department of Mathematics*
Faculty of Wood sciences and Technology
Technical University of Zvolen
T. G. Masaryka 24
SK–960 53 Zvolen
SLOVAK REPUBLIC
E-mail: kostra@vsld.tuzvo.sk
lazar@vsld.tuzvo.sk