JP Journal of Algebra, Number Theory and Applications
Volume 10, Number 2, 2008, Pages 203-236
Published Online: April 18, 2008
This paper is available online at http://www.pphmj.com

ON NORMAL BASES OF IDEALS IN EXTENSION OF DEGREE $2l$

VIKTOR DUBOVSKÝ and JURAJ KOSTRA

Department of Mathematics and Descriptive Geometry
Technical University of Ostrava
17. Listopadu 15, 708 33 Ostrava
Czech Republic

Department of Mathematics with Didactics
Pedagogical Faculty
University of Ostrava
Mlýnská 5, 701 03 Ostrava
Czech Republic
e-mail: juraj.kostra@osu.cz

Abstract

In the present paper a necessary and sufficient condition for a cyclic extension of the rationals of degree $2l$, with a prime l, to have a normal basis for any ambiguous ideal is given. Fields of the degree $2l$ are investigated by computational methods for primes l, with $h(\mathbb{Q}(\zeta_l)) = 1$.

Introduction

In 1969, Ullom [3, Theorem 1.10] gave a sufficient condition for all ambiguous ideals in cyclic extension of $\mathbb{Q}$ of a prime degree l to have a normal basis:

2000 Mathematics Subject Classification: 11R33, 11R18.

Keywords and phrases: normal basis, ambiguous ideal, circulant matrix.

Supported by grant GAČR 201/07/0191.

Communicated by Jannis A. Antoniadis

Received March 13, 2007

Let $K/\mathbb{Q}$ be a cyclic extension of a prime degree l in which the prime l is unramified. Suppose the class number of the cyclotomic field $\mathbb{Q}(\zeta_l)$ is one. Then every ambiguous ideal of K has a normal basis.

In 1992, Jakubec and Kostra extended the above result, namely they proved this theorem [2, Theorem 1].

Let $K/\mathbb{Q}$ be a cyclic extension of prime degree l in which the prime l is unramified. Let m be the conductor of the field K. Every ambiguous ideal of K has a normal basis if and only if for any prime p, $p \mid m$ there is an integer $\gamma \in \mathbb{Q}(\zeta_l)$ such that $|N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma)| = p$.

In the present paper we investigate existence of a normal basis for ambiguous ideals in field extensions $K/\mathbb{Q}$ of degree $2l$, where l is a prime and give a necessary and sufficient condition for any ambiguous ideal of K to have a normal basis and we will prove the following theorem.

Theorem 1. *Let l be a prime and $K/\mathbb{Q}$ be a cyclic tamely ramified extension of degree $2l$. Let m be the conductor of K. Every ambiguous ideal of K has a normal basis if and only if for any prime p, $p \mid m$ there is an integer $\gamma \in \mathbb{Q}(\zeta_l)$ such that $|N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma)| = p$ and a unit $\omega \in \mathbb{Q}(\zeta_l)$ such that $Tr_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\omega) = \pm 1$ and $\omega \equiv \gamma \pmod{2\,\mathbb{Z}_{\mathbb{Q}(\zeta_l)}}$.*

Before proving Theorem 1, let us first briefly recall some general properties of the ambiguous ideals according to Ullom [3]. 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

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

Let $\Psi(\mathfrak{P}) = \mathfrak{p}_1.\mathfrak{p}_2 \cdots \mathfrak{p}_g$. 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

$$U_O = \Psi(\mathfrak{P}_1)^{a_1} \cdots \Psi(\mathfrak{P}_t)^{a_t}, \quad 0 < a_i \leq e_i,$$

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 [3, 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 [3, Corollary 1.2] showed that $Tr_{K/F}(U) = U \cap F$ 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 $\mathbb{Z}$.

Theoretical Results

We will prove Theorem 1 as a consequence of two lemmas. First we prove it in the case $K \subseteq \mathbb{Q}(\zeta_p)$, where p is a prime.

Lemma 1. *Let $K/\mathbb{Q}$ be a cyclic extension with degree $[K : \mathbb{Q}] = 2l$ in which the prime l is unramified. Let $K \subseteq \mathbb{Q}(\zeta_p)$ for a prime p. Every ambiguous ideal of K has a normal basis if and only if for p there is an integer $\gamma \in \mathbb{Z}_{\mathbb{Q}(\zeta_l)}$ such that $|N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma)| = p$ and a unit $\omega \in \mathbb{Z}_{\mathbb{Q}(\zeta_l)}$ such that $Tr_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\omega) = \pm 1$ and $\omega \equiv \gamma (\mathrm{mod}\ 2\mathbb{Z}_{\mathbb{Q}(\zeta_l)})$.*

Proof. The existence of a normal basis for all ambiguous ideals is equivalent to the existence of circulant matrices $\mathbf{A}_i = \mathrm{circ}_{2l}(a_{i,1}, a_{i,2}, \ldots, a_{i,2l})$ transformating a normal basis of ideal (π^j) to a normal basis of

(π^{j+1}), i.e., matrices such that

$$\mathbb{Z}_K \overset{\mathbf{A}_0}{\to} (\pi) \overset{\mathbf{A}_1}{\to} (\pi^2) \overset{\mathbf{A}_2}{\to} (\pi^3) \cdots (\pi^{2l-1}) \overset{\mathbf{A}_{2l-1}}{\to} (\pi^{2l}) = p\mathbb{Z}_K.$$

Assume now that such matrices $\mathbf{A}_i$ exist, then since the index $[(\pi^i) : (\pi^{i+1})]$ is equal to p the determinant of each matrix $| \mathbf{A}_i | = \pm p$.

The formula for computing the determinant of circulant matrix $\mathbf{A}_i = \mathrm{circ}_{2l}(a_{i,1}, a_{i,2}, ..., a_{i,2l})$ is

$$| \mathbf{A}_i | = \prod_{j=0}^{2l-1} q_i(\zeta_{2l}^j), \tag{1}$$

where $q_i(z) = a_{i,1} + a_{i,2}z + a_{i,3}z^2 + \cdots + a_{i,2l}z^{2l-1}$.

Each term $q_i(\zeta_{2l}^k)$ represents an element of the field $\mathbb{Q}(\zeta_l)$, furthermore this element is an eigenvalue of the matrix $\mathbf{A}_i$, so we denote it by $\lambda_{i,k}$, i.e.,

$$\lambda_{i,k} = a_{i,1} + a_{i,2}\zeta_{2l}^k + a_{i,3}\zeta_{2l}^{2k} + \cdots + a_{i,2l}\zeta_{2l}^{(2l-1)k}. \tag{2}$$

The form of $\lambda_{i,k}$ can be simplified using the fact that

$$\zeta_{2l}^j = \begin{cases} \zeta_l^{\frac{j}{2}} & \text{for even } j, \\ -\zeta_l^{\frac{l+j}{2}} & \text{for odd } j. \end{cases}$$

So one gets

$$| \mathbf{A}_i | = \lambda_{i,0} N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\lambda_{i,1}) \lambda_{i,l+1} N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\lambda_{i,2}), \tag{3}$$

with

$$\lambda_{i,0} = \sum_{j=1}^{2l} a_{i,j}, \quad \lambda_{i,1} = \sum_{j=1}^{l} (-1)^{j-1}(a_{i,j} - a_{i,l+j})\zeta_l^{j-1},$$

$$\lambda_{i,l+1} = \sum_{j=1}^{2l} (-1)^{l-1} a_{i,j}, \quad \lambda_{i,2} = \sum_{j=1}^{l} (a_{i,j} + a_{i,l+j})\zeta_l^{j-1}.$$

Note that the basis of the ring of integers $\mathbb{Z}_K$ is transformated to a basis of the ideal $p\mathbb{Z}_K$ by the diagonal matrix $\mathbf{D} = \mathrm{diag}_{2l}(p, 0, ..., 0)$, i.e., $\mathbb{Z}_K \xrightarrow{\mathbf{D}} p\mathbb{Z}_K$. Thus we get following matrix equality:

$$\mathbf{A}_0 \cdot \mathbf{A}_1 \cdots \mathbf{A}_{2l-1} = \mathbf{D}.$$

Denote by $\mathbf{F}_n$ the Fourier transformation matrix, i.e., such a matrix that

$$\mathbf{F}_n^H = \mathbf{F}_n^{-1} = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \zeta_n & \zeta_n^2 & \cdots & \zeta_n^{n-1} \\ 1 & \zeta_n^2 & \zeta_n^4 & \cdots & \zeta_n^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_n^{n-1} & \zeta_n^{2(n-1)} & \cdots & \zeta_n^{(n-1)(n-1)} \end{pmatrix}, \tag{4}$$

then $\mathbf{F}_n \mathbf{A} \mathbf{F}_n^{-1}$ is a diagonal matrix with entries being eigenvalues of the circulant matrix $\mathbf{A}$.

Using the above facts, we get

$$\mathbf{A}_0 \cdot \mathbf{A}_1 \cdots \mathbf{A}_{2l-1} = \mathbf{D},$$

$$\mathbf{F}_{2l} \cdot \mathbf{A}_0 \cdot \mathbf{A}_1 \cdots \mathbf{A}_{2l-1} \cdot \mathbf{F}_{2l}^{-1} = \mathbf{F}_{2l} \mathbf{D} \mathbf{F}_{2l}^{-1},$$

$$\mathbf{F}_{2l} \cdot \mathbf{A}_0 \cdot \mathbf{F}_{2l}^{-1} \cdot \mathbf{F}_{2l} \cdot \mathbf{A}_1 \cdot \mathbf{F}_{2l}^{-1} \cdots \mathbf{F}_{2l} \cdot \mathbf{A}_{2l-1} \cdot \mathbf{F}_{2l}^{-1} = \mathbf{D},$$

$$\mathbf{D}_0 \cdot \mathbf{D}_1 \cdots \mathbf{D}_{2l-1} = \mathbf{D}$$

with diagonal matrices $\mathbf{D}_i = \mathrm{diag}_{2l}(\lambda_{i,0}, \lambda_{i,1}, ..., \lambda_{i,2l-1})$.

From which it follows easily, thus we have

$$\prod_{j=0}^{2l-1} \lambda_{i,j} = p, \qquad \prod_{i=0}^{2l-1} \lambda_{i,j} = p, \tag{5}$$

for each $i, j = 0, 1, 2, ..., 2l - 1$. Notice that the first product represents the determinant of the matrix $\mathbf{A}_i$.

Since $\lambda_{i,0} = \sum_{j=1}^{2l} a_{i,j} \in \mathbb{Z}$, we have $\lambda_{i,0} = \pm p$ for some $i \in \{0, 1, ..., 2l-1\}$ and $\lambda_{k,0} = \pm 1$ for $k \neq i$. Similarly, $\lambda_{i,l+1} = \pm p$ for some $i \in \{0, 1, ..., 2l-1\}$ and $\lambda_{k,1} = \pm 1$ for $k \neq i$.

Particularly, in what follows we show that $\lambda_{0,0} = p$ and $\lambda_{l+1,l+1} = p$.

Finally, equality (3) shows that either $N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\lambda_{i,1}) = p$ and $\lambda_{i,2}$ is a unit of $\mathbb{Z}_K$ or $N_{\mathbb{Q}(\zeta_{i,l})/\mathbb{Q}}(\lambda_{i,2}) = p$ and $\lambda_{i,1}$ is a unit of $\mathbb{Z}_K$.

The circulant matrix $\mathbf{A}_i = \mathrm{circ}_{2l}(a_{i,1}, a_{i,2}, ..., a_{i,2l})$ is similar to the block matrix

$$\mathbf{A}_{i,\mathrm{block}} = \mathbf{X}\mathbf{A}_i\mathbf{X}^{-1} = \begin{pmatrix} \mathbf{A}_i^- & \mathbf{A}_i^* \\ \mathbf{O}_l & \mathbf{A}_i^+ \end{pmatrix}, \tag{6}$$

where $\mathbf{X}$ is unimodular matrix with entries x_{jk} defined as follows:

$$x_{jk} = \begin{cases} 1 & \text{for } j \leq l \text{ and } k \equiv 2j-1 \pmod{2l}, \\ 1 & \text{for } l < j \leq 2l \text{ and } k \equiv 2j-1 \pmod{l}, \\ 0 & \text{else.} \end{cases} \tag{7}$$

The blocks of $\mathbf{A}_{i,\mathrm{block}}$ are circulant matrices of this form

$$\mathbf{A}_i^- = \mathrm{circ}_l(a_{i,1} - a_{i,l+1}, a_{i,3} - a_{i,l+3}, ..., -a_{i,2} + a_{i,l+2}, ..., -a_{i,l-1} + a_{i,2l-1}),$$

$$\mathbf{A}_i^+ = \mathrm{circ}_l(a_{i,1} + a_{i,l+1}, a_{i,3} + a_{i,l+3}, ..., a_{i,2} + a_{i,l+2}, ..., a_{i,l-1} + a_{i,2l-1}),$$

$$\mathbf{A}_i^* = \mathrm{circ}_l(a_{i,l+1}, a_{i,l+3}, ..., a_{i,2}, ..., a_{i,l-1}), \tag{8}$$

and the block $\mathbf{O}_l$ is the zero matrix of degree l.

The determinant of $\mathbf{A}_{i,\mathrm{block}}$ depends only on the determinants of the blocks $\mathbf{A}_i^+$ and $\mathbf{A}_i^-$ and hence we have

$$|\mathbf{A}_i| = |\mathbf{X}\mathbf{A}_i\mathbf{X}^{-1}| = |\mathbf{A}_{i,\mathrm{block}}| = |\mathbf{A}_i^+||\mathbf{A}_i^-|.$$

Now let $\mathbf{B}$ be a circulant matrix of degree l, with the determinant

$$|\mathbf{B}| = (b_1 + b_2 + \cdots + b_l)\prod_{i=1}^{l} q_{\mathbf{B}}(\zeta_l^i),$$

$$|\mathbf{B}| = (b_1 + b_2 + \cdots + b_l)N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\beta), \tag{9}$$

where $\beta = b_1 + b_2\zeta_l + \cdots + b_l\zeta_l^{l-1}$ is an element of $\mathbb{Q}(\zeta_l)$.

Also let $\gamma = c_1 + c_2\zeta_l + \cdots + c_l\zeta_l^{l-1}$ be another element of $\mathbb{Q}(\zeta_l)$ and $\mathbf{C} = \mathrm{circ}_l(c_1, c_2, ..., c_l)$ be its circulant matrix.

Thus obviously in order to get $|\mathbf{A}_i| = \pm p$, one has to take the blocks $\mathbf{A}_i^- = \mathbf{B}$ and $\mathbf{A}_i^+ = \mathbf{C}$, as in one of the following four possibilities:

$$\sum_{i=1}^{l} b_i = \pm p, \quad N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\beta) = \pm 1, \quad \sum_{i=1}^{l} c_i = \pm 1, \quad N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma) = \pm 1, \tag{10}$$

$$\sum_{i=1}^{l} b_i = \pm 1, \quad N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\beta) = \pm p, \quad \sum_{i=1}^{l} c_i = \pm p, \quad N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma) = \pm 1, \tag{11}$$

$$\sum_{i=1}^{l} b_i = \pm 1, \quad N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\beta) = \pm 1, \quad \sum_{i=1}^{l} c_i = \pm p, \quad N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma) = \pm 1, \tag{12}$$

$$\sum_{i=1}^{l} b_i = \pm 1, \quad N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\beta) = \pm 1, \quad \sum_{i=1}^{l} c_i = \pm 1, \quad N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma) = \pm p. \tag{13}$$

Observe that in the cases of (10) and (12) both β and γ are units of $\mathbb{Z}_{\mathbb{Q}(\zeta_l)}$. In the cases (11) and (13) one has a unit and an element with norm equal to p.

From the form of blocks in (8) and matrices $\mathbf{B}$, $\mathbf{C}$ we get following system of linear equations:

$$\begin{aligned} a_{i,1} - a_{i,l+1} &= b_{k_1}, & a_{i,1} + a_{i,l+1} &= c_{k_1}, \\ a_{i,3} - a_{i,l+3} &= b_{k_3}, & a_{i,3} + a_{i,l+3} &= c_{k_3}, \\ &\cdots & &\cdots \\ a_{i,2l-1} - a_{i,l-1} &= b_{k_{2l-1}}, & a_{i,2l-1} + a_{i,l-1} &= c_{k_{2l-1}}, \end{aligned} \tag{14}$$

with the solutions

$$\begin{aligned} a_{i,1} &= (b_{k_1} + c_{k_1})/2, & a_{i,l+1} &= (b_{k_1} - c_{k_1})/2, \\ a_{i,3} &= (b_{k_3} + c_{k_3})/2, & a_{i,l+3} &= (b_{k_3} + c_{k_3})/2, \\ &\cdots & &\cdots \\ a_{i,2l-1} &= (b_{k_{2l-1}} + c_{k_{2l-1}})/2, & a_{i,l-1} &= (b_{k_{2l-1}} - c_{k_{2l-1}})/2. \end{aligned} \tag{15}$$

The indices k_j of b and c in (15) depend on j in $a_{i,j}$ and are equal to

$$k_j = \frac{j+1}{2}, \tag{16}$$

for odd j. For even j, particularly, for $a_{i,j+l \pmod{2l}}$ they are the same.

From the above it is also easy to see that in order to get $a_{i,j} \in \mathbb{Z}$ for $j \in \{1, 2, ..., 2l\}$ the

$$b_{k_j} \equiv c_{k_j} \pmod 2$$

must hold for all $k_j \in \{1, 2, ..., l\}$.

Finally, observe that one has

$$\sum_{j=1}^{2l} a_{i,j} = \sum_{k=1}^{l} b_k.$$

By the proof of [2, Lemma 1] for a matrix $\mathbf{A}_i$ to transform a normal basis of the ideal (π^i) to a normal basis of the ideal (π^{i+1}) it is now sufficient to show that i solves the following congruence:

$$a_{i,1} + a_{i,2}\tilde{g}^i + \cdots + a_{i,2l}(\tilde{g}^i)^{2l-1} \equiv 0 \pmod p, \tag{17}$$

where $\tilde{g} = r^{\frac{p-1}{2l}}$, with r primitive root modulo p.

We recall here that in the proof of [2, Lemma 1] the congruences

$$b_1 + b_2 g^i + \cdots + b_l (g^i)^{l-1} \equiv 0 \pmod p, \tag{18}$$

with $g = r^{\frac{p-1}{l}}$ are solved. Our goal is to transform congruences (17) to the above form. To do it, observe that directly from the definitions of g

and $\widetilde{g}$ one sees relations among them

$$\widetilde{g}^2 = g, \qquad \widetilde{g}^l \equiv -1 \pmod{p},$$
$$\widetilde{g} \equiv g^{\frac{l}{2}} \pmod{p}, \qquad \widetilde{g}^{2l} \equiv 1 \pmod{p}. \tag{19}$$

We start with dividing the congruence $\sum_{j=1}^{2l} a_{i,j}(\widetilde{g}^i)^{j-1} \equiv 0 \pmod{p}$ into two parts. One with even exponents, one with odd. Then we replace coefficients $a_{i,j}$ by b_{k_j} resp. c_{k_j} as in solutions of (15) and divide once again

$$\sum_{x=1}^{l} \frac{b_{k_{2x-1}} + c_{k_{2x-1}}}{2} (\widetilde{g}^i)^{2x-2} + \sum_{y=1}^{l} \frac{b_{k_{2y}} - c_{k_{2y}}}{2} (\widetilde{g}^i)^{2y-1}$$
$$= \frac{1}{2} \sum_{x=1}^{l} b_{k_{2x-1}} (\widetilde{g}^i)^{2x-2} + \frac{1}{2} \sum_{y=1}^{l} b_{k_{2y}} (\widetilde{g}^i)^{2y-1}$$
$$+ \frac{1}{2} \sum_{x=1}^{l} c_{k_{2x-1}} (\widetilde{g}^i)^{2x-2} - \frac{1}{2} \sum_{y=1}^{l} c_{k_{2y}} (\widetilde{g}^i)^{2y-1}.$$

Observe that in order to have $b_{k_{2y}} = b_{k_{2x-1}}$ (resp., $c_{k_{2y}} = c_{k_{2x-1}}$) the following must hold $2y \equiv 2x - 1 \pmod{l}$, i.e., $2y = 2x - 1 \pm l$, and thus we get

$$\frac{1}{2} \sum_{x=1}^{l} b_{k_{2x-1}} (\widetilde{g}^i)^{2x-2} + \frac{1}{2} \sum_{x=1}^{l} b_{k_{2x-1}} (\widetilde{g}^i)^{(2x-1\pm l)-1}$$
$$+ \frac{1}{2} \sum_{x=1}^{l} c_{k_{2x-1}} (\widetilde{g}^i)^{2x-2} - \frac{1}{2} \sum_{x=1}^{l} c_{k_{2x-1}} (\widetilde{g}^i)^{(2x-1\pm l)-1}.$$

All exponents are even now so, we can replace $\widetilde{g}$ by g, i.e.,

$$\frac{1}{2} \sum_{x=1}^{l} b_{k_{2x-1}} (g^i)^{x-1} + \frac{1}{2} \sum_{x=1}^{l} b_{k_{2x-1}} (g^i)^{x-1} (g^i)^{\frac{l}{2}}$$
$$+ \frac{1}{2} \sum_{x=1}^{l} c_{k_{2x-1}} (g^i)^{x-1} - \frac{1}{2} \sum_{x=1}^{l} c_{k_{2x-1}} (g^i)^{x-1} (g^i)^{\frac{l}{2}}.$$

Finally, since $k_{2x-1} = x$ and $(g^i)^{\frac{l}{2}} = (\tilde{g}^i)^l = (-1)^l$ we get

$$\frac{1}{2}\sum_{x=1}^{l} b_x (g^i)^{x-1} + (-1)^i \frac{1}{2}\sum_{x=1}^{l} b_x (g^i)^{x-1}$$

$$+ \frac{1}{2}\sum_{x=1}^{l} c_x (g^i)^{x-1} - (-1)^i \frac{1}{2}\sum_{x=1}^{l} c_x (g^i)^{x-1}.$$

From the above we see that if i is even solution of the congruence (17), then it also solves the congruence $\sum_{x=1}^{l} b_x (g^i)^{x-1} \equiv 0 \pmod{p}$. Odd solutions of (17) are solutions of the congruence $\sum_{x=1}^{l} c_x (g^i)^{x-1} \equiv 0 \pmod{p}$.

Thus this way we may obtain solutions of (17) for all $i \in \{1, 2, ..., 2l-1\}$, since obviously if i solves the congruence (18), then $i + l$ solves it too and the change of i to $i + l$ corresponds to the change of positions of the blocks in matrix $\mathbf{A}_{i,\,\mathrm{block}}$ or interchanging roles of **B** and **C**.

Now let β and γ be as in the case (10). We shall show that the circulant matrix $\mathbf{A}_i$ reached from (15), transforms a normal basis of the $\mathbb{Z}_K$ to the normal basis of the ideal (π).

Notice first that a pair with the same parities of b_i and c_i always exists. Since $p \equiv 1 \pmod{l}$ and hence one can take the unit β with the representing circulant matrix in the form

$$\mathbf{B} = \mathrm{circ}_l(b+1,\, b,\, b,\, ...,\, b),$$

with $b = \frac{p-1}{l}$. To verify that such β is a unit observe that each term in (9) can be reduced to 1 by subtraction $0 = b + b\zeta_l + \cdots + b\zeta_l^{l-1}$ and thus it follows that β has the norm equal to 1. Furthermore, b is even, since $lb + 1 = p$ with l and p being odd primes, so we can take matrix **C** to be the identity matrix, i.e., $\mathrm{circ}_l(1,\, 0,\, 0,\, ...,\, 0)$.

As a solution of (14) we get matrix

$$\mathbf{A}_0 = \mathrm{circ}_{2l}(a+1,\ a,\ a,\ \ldots,\ a),$$

with $a = \dfrac{p-1}{2l}$ and sum of its entries equal to p.

To verify that the index $i = 0$, one has to solve these congruences

$$(b+1) + bg^i + b(g^i)^2 + \cdots + b(g^i)^{l-1} \equiv 0 \pmod{p},$$

$$b\sum_{j=0}^{l-1}(g^i)^j \equiv -1 \pmod{p}$$

and thus from $lb + 1 = p$ it follows easily that $i = 0$.

Thus the matrix $\mathbf{A}_0$ transforms normal basis of the ring of integers in the field K to the normal basis of ideal (π).

The case (12) is similar to the above construction, so let $\mathbf{B} = \mathrm{circ}_l(1,\ 0,\ 0,\ \ldots,\ 0)$ be the identity matrix, $c = \dfrac{p-1}{l}$ and

$$\mathbf{C} = \mathrm{circ}_l(c+1,\ c,\ c,\ \ldots,\ c).$$

Then we get the circulant matrix

$$\mathbf{A}_i = \mathrm{circ}_{2l}(a+1,\ -a,\ a,\ -a,\ \ldots,\ a,\ a),$$

again with $a = \dfrac{p-1}{2l}$ and sum of its entries equal to 1.

We show that Theorem 1 holds in the case with prime conductor p. To prove in the case of the squarefree conductor $m = p_1p_2\cdots p_s$ we will need the following lemma.

Lemma 2. *Let K be as in Theorem 1 with the squarefree conductor $m = p_1p_2\cdots p_s$, where p_i is a prime for $i = 1, 2, \ldots, s$. Let $\mathbb{Q} \subset L_{p_i} \subset \mathbb{Q}(\zeta_{p_i})$, $[L_{p_i} : \mathbb{Q}] = 2l$. Then*

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

Proof. The proof is by the same way as the proof of [2, Lemma 2] for field extension of prime degree l. The situation in case of extension of degree $2l$ is similar.

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

with

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

and the index

$$[(\mathbb{Z}/p_i\,\mathbb{Z})^* : H_i] = 2l.$$

Clearly $H = [(\mathbb{Z}/m\mathbb{Z})^*]^{2l}$. 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 $(\mathbb{Z}/p_i\mathbb{Z})^*/G$ equals $2l$ and so $x^{2l} \in G$. Thus we have $H \subset G$.

Remark. From the above it is easy to see that also in the case of non-cyclic extension $K \subset \mathbb{Q}(\zeta_m)$ with $[K : \mathbb{Q}] = 4$ any ambiguous ideal has a normal basis, since

$$K \subset \bigvee_{i=1}^{s} K_i,$$

where $K_i \subseteq \mathbb{Q}(\zeta_{p_i})$ and $[K_i : \mathbb{Q}] = 4$ for $p_i \equiv 1 \pmod 4$ and $[K_i : \mathbb{Q}] = 2$ for $p_i \equiv 3 \pmod 4$.

Now we are in position to complete the proof of Theorem 1.

Proof. By Lemma 1 any ambiguous ideal of L_{p_i}, $i = 1, 2, ..., s$, has a normal basis. By [3, Proposition 1.8] any ambiguous ideal of $\bigvee_{i=1}^{s} L_{p_i}$ has a normal basis and so by [3, Corollary 1.2] any ideal of K has a normal basis. Which proves Theorem 1.

Computational Results

Methods. In the next part of this paper we shall discuss existence or

non-existence of pairs of an element γ and a unit $\omega \in \mathbb{Q}(\zeta_l)$ such that

$$\gamma \equiv \omega \pmod{2\mathbb{Z}[\mathbb{Q}(\zeta_l)]}$$

which by Lemma 1 ensures existence of normal basis for ambiguous ideals. Especially the cases with prime $l \leq 19$, i.e., those for which $h(\mathbb{Q}(\zeta_l)) = 1$, are solved and also examples will be given.

We start with some simple observations. As the elements $\gamma, \omega \in \mathbb{Q}(\zeta_l)$ can be represented as $\gamma = \sum_{i=1}^{l} c_i \zeta_l^{i-1}$ or by circulant matrix $\mathbf{A}_\gamma = \mathrm{circ}_l(c_1, c_2, ..., c_l)$, resp. by $\mathbf{A}_\omega$ with the coefficients ω_i of the unit ω.

We are mainly interested in comparing parity of pairs c_i, ω_i and hence to each $\mathbf{A}_\gamma$ we attach "parity" matrix $\overline{\mathbf{A}}_\gamma = \mathrm{circ}_l(\bar{c}_i)$, where by $\bar{c}_i$ we denote the residue class modulo 2.

In what follows, since there is no risk of confusion, we will use the term parity for both, integers in usual meaning and for matrices and vectors in the way it is defined above, i.e., parity term by term.

One can easily determine that the number of all possible distributions of odd and even numbers in the vector $(c_1, c_2, ..., c_l)$ is 2^l.

Since to get $\sum_{i=1}^{l} c_i = \pm 1$ one has to have odd number of odd c_i's, we may decrease this number to 2^{l-1}.

Finally the determinant of the circulant matrix with all entries being odd, i.e., $\mathrm{circ}_l(2k_1 + 1, 2k_2 + 1, ..., 2k_l + 1)$, is divisible by 2^{l-1} and hence is not a prime, so we may discard this possibility and conclude that there is only $2^{l-1} - 1$ of distributions of odd and even entries in $\mathrm{circ}_l(c_1, c_2, ..., c_l)$, such that they can represent the elements of $\mathbb{Q}(\zeta_l)$ with prime norm.

On the other hand, since the group of units in $\mathbb{Q}(\zeta_l)$, for l prime and $l \leq 19$, is generated by the fundamental units, one can determine the number of all units distinct from the parity point of view.

The fundamental units can be computed by the formula

$$\varepsilon_a = \zeta_l^{\frac{1-a}{2}} \left(\frac{1-\zeta_l^a}{1-\zeta_l} \right), \tag{20}$$

with $a = 2, 3, \ldots, (l-1)/2$. Next we use ε_1 for the unit ζ_l.

Notice that nonzero coefficients in (20) are all equal to ± 1 and that there is even number of them, but this can be changed by adding resp. subtracting element $1 + \zeta_l + \zeta_l^2 + \cdots + \zeta_l^{l-1}$, i.e., zero, to ε_a, so we may always assume to have fundamental units in the form

$$\varepsilon_a = e_{a,1} + e_{a,2}\zeta_l + \cdots + e_{a,l}\zeta_l^{l-1}$$

with odd number of odd coefficients $e_{a,i}$.

Once we determine fundamental units ε_a, their representation matrices $\mathbf{E}_{\varepsilon_a}$ and the parity matrices $\overline{\mathbf{E}}_{\varepsilon_a}$ belonging to them, we compute the power of $\mathbf{E}_{\varepsilon_a}^m$, and $\mathbf{E}_{\varepsilon_b}^n$, with $a, b \in \{2, 3, \ldots, (p-1)/2\}$, $m, n \in \mathbb{N}$ to find a pair m, n such that

$$\overline{\mathbf{E}}_{\varepsilon_a}^m = \overline{\mathbf{E}}_{\varepsilon_b}^n.$$

From the last section of tables we can see that all possible parity matrices can be written as a power of only one suitably chosen fundamental unit ε_i and power of ζ_l. Only one exception appears in case of $l = 17$, where we have to choose two fundamental units ε_i, ε_j and the unit ζ_l to produce all possible parity matrices.

For the fundamental units $\sum_{i=1}^{l} e_{a,i} = s(\varepsilon_a) = \pm 1$ is not valid, to put them in this form compute $s(\varepsilon_a)$ for each $a = 2, 3, \ldots, (l-1)/2$ and fix ε_a, such that $s(\varepsilon_a)$ is primitive root modulo l, then for $i = 2, 3, \ldots, (l-1)/2$, $i \neq a$ one can find $k \in \mathbb{N}$ such that

$$s(\varepsilon_i)s(\varepsilon_a)^k \equiv \pm 1 \pmod{l}.$$

Thus the units $\varepsilon_i\varepsilon_a^k$ can be put in the form with sum of coefficients equal to ± 1. Particularly this is done by adding the term

$$\frac{s(\varepsilon_i\varepsilon_a^k) \pm 1}{l}(1 + \zeta_l + \zeta_l^2 + \cdots + \zeta_l^{l-1})$$

we denote the yielding units by ω_i.

This way we obtain the new set

$$\{\omega_i;\ i = 2, 3, ..., (l-1)/2\},$$

with ω_i from product $\varepsilon_i\varepsilon_a^k$. In what follows we denote this relation by $\varepsilon_i\varepsilon_a^k \approx \omega_i$. Notice that this set is not the set of fundamental units, in fact it generates subgroup of rank $(l-1)/2$ in the unit group.

Computational investigation of the parity cycles for units ω_i, the dependence between them and the dependence between parities of ω_i and the fundamental units ε_j, resp. their powers, shows that both sets $\{\varepsilon_i;\ i = 2, 3, ..., (l-1)/2\}$ and $\{\omega_i;\ i = 2, 3, ..., (l-1)/2\}$ produce the same parity matrices and for both it is enough to choose just one generator, except for $l = 17$.

To get all possible parity matrices one has to multiply those we get by $\mathbf{E}_{\varepsilon_1}^i$, with $i = 0, 1, ..., l-1$, since l is obviously length of ε_1 cycle.

Hence this way we are able to computationally determine the number of all distinct parity matrices for each l. Thus to decide whether there is such a pair γ, ω as Lemma 1 demands us to find, it just left to compare this number with $2^{l-1} - 1$.

Prime $l = 2$**.** Let the circulant matrix $\mathbf{C} = \mathrm{circ}_2(a, b)$ represent an element γ. One immediately sees that if $a + b = \pm 1$, then $b = \pm 1 - a$, so a and b have opposite parities. Obviously one of the units 1, resp. i with matrices $\mathrm{circ}_2(1, 0)$ resp. $\mathrm{circ}_2(0, 1)$ have the same parity matrix as the element γ.

Prime $l = 3$ [1]**.** Since in this case $2^{l-1} - 1 = 3$, i.e., there are 3 possibilities to get an element with prime norm, namely with the representing matrices $\mathrm{circ}_3(2k_1 + 1, 2k_2, 2k_3)$, $\mathrm{circ}_3(2k_1, 2k_2 + 1, 2k_3)$ and $\mathrm{circ}_3(2k_1, 2k_2, 2k_3 + 1)$.

On the other hand the units $1, \zeta_3, \zeta_3^2$ have the matrices $\mathrm{circ}_3(1, 0, 0)$, $\mathrm{circ}_3(0, 1, 0)$ and $\mathrm{circ}_3(0, 0, 1)$.

Thus we can always choose a unit with the same parity as an arbitrary element of $\mathbb{Q}(\zeta_3)$.

Prime $l = 5$**.** Let us illustrate the use of computational results, which are summarized in Appendix B.

The fundamental units ε_i resp. ω_i, $i = 1, 2$ are equal to

$$\varepsilon_1 = \zeta_5, \qquad \omega_1 = \varepsilon_1,$$

$$\varepsilon_2 = -1 - \zeta_5 - \zeta_5^4, \qquad \varepsilon_1^2 \approx \omega_2 = 1 - \zeta_5^2 - \zeta_5^3$$

resp. written as circulant matrices

$$\mathbf{E}_{\varepsilon_1} = \mathrm{circ}_5(0, 1, 0, 0, 0), \qquad \mathbf{W}_{\omega_1} = \mathrm{circ}_5(0, 1, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2} = \mathrm{circ}_5(-1, -1, 0, 0, -1), \qquad \mathbf{E}_{\varepsilon_1^2} \approx \mathbf{W}_{\omega_2} = \mathrm{circ}_5(1, 0, -1, -1, 0).$$

Computing the powers of the fundamental units and the units ω_i we get Table 1, where the input k at i, j-th place means that $\overline{\mathbf{E}}_{\varepsilon_i}^k = \overline{\mathbf{E}}_{\varepsilon_j}$, or the same for matrices belonging to ω_i's.

Table 1. Parity dependence of the units in $\mathbb{Q}(\zeta_5)$

	ε_1	ε_2
ε_1	6	-
ε_2	3	4

	ω_1	ω_2
ω_1	6	-
ω_2	3	4

From Table 1 we also see that ω_1 has parity cycle is of length 5, and ω_2 has cycle length 3, so there is $5 \cdot 3 = 15$ possible distributions of odd and even numbers in representation of any unit in $\mathbb{Q}(\zeta_5)$.

The number of all possible distributions of odd and even coefficients in representation matrices of elements with prime norm is $2^{l-1} = 16 - 1 = 15$.

So for any γ with $|N_{\mathbb{Q}(\zeta_5)/\mathbb{Q}}(\gamma)| = p$ the condition of Lemma 1 is always fulfilled and so for the fields tamely ramified cyclic extensions K with $[K : \mathbb{Q}]$ there exists a normal basis for all ambiguous ideals.

Prime $l = 7$. From the tables of fundamental units ε_i and the units ω_i of $\mathbb{Q}(\zeta_7)$, resp. tables with their parity dependence (Appendix B, Subsection $l = 7$) we see that the units ω_2, ω_3 produce the same cycle with length 7. The parity cycle of the unit ω_1 is also 7.

Thus the number of all parity distinct units is $7 \cdot 7 = 49 < 2^{l-1} - 1 = 2^6 - 1 = 63$, so there are 14 possibilities, which can yield element with prime norm and are different from those we get as units ω_i powers.

Now denote by $\overline{\mathbf{A}}_i$ these three parity matrices

$$\overline{\mathbf{A}}_1 = \mathrm{circ}_7(0, 0, 0, 1, 0, 1, 1),$$

$$\overline{\mathbf{A}}_2 = \mathrm{circ}_7(0, 0, 0, 1, 1, 0, 1),$$

$$\overline{\mathbf{A}}_3 = \mathrm{circ}_7(1, 0, 0, 0, 1, 0, 1),$$

counting them together with their conjugates we get the rest 14 possibilities, since elements with parity $\overline{\mathbf{A}}_1$ have only two conjugates, watching them from parity point of view.

Analyse the determinant of the matrix $\mathrm{circ}_7(2k_1, 2k_2, 2k_3, 2k_4 + 1, 2k_5, 2k_6 + 1, 2k_7 + 1)$ with $k_i \in \mathbb{Z}$, i.e., matrix of element with the same parity as $\overline{\mathbf{A}}_1$, is equal to $4z$, $z \in \mathbb{Z}$. Determinants of matrices with the same parity as $\overline{\mathbf{A}}_i$, $i = 2, 3$, are also divisible by 4.

Hence for any γ with prime norm, one can find unit with corresponding coefficient parity in the case of $l = 7$.

Prime $l = 11$. The computation (Appendix B, Subsection 11) shows

that there are $11 \cdot 31 = 341$ of units different from parity point of view. Notice that 11 is length of parity cycle of ω_1 and 31 length of parity cycle of the unit ω_5.

Since $341 < 2^{l-1} - 1 = 2^{10} - 1 = 1027$ and as this difference grows the probability of non-existence of pair γ, ω with $c_i \equiv \omega_i \pmod 2$ grows as well, also checking determinants, like it was done in the case of $l = 7$, become at least tedious.

So we produce a counter-example. Computing the determinant of matrix $\mathrm{circ}_{11}(1, 1, -1, 0, 0, 0, 0, 0, 0, 0, 0)$, and matrices received by all permutations of its coefficients we get 495 elements of $\mathbb{Q}(\zeta_{11})$, out of which there are 55 units, i.e., with determinant equal to 1, 220 of them have determinant 23 and 110 with 67 resp. 199.

Thus we obtained 440 non-units, with prime norm congruent to 1 modulo 11 and each distinct with respect to the parities of coefficients, and since the number of distinct units is 341 there must be γ with no corresponding ω.

The element $\gamma = 1 + \zeta_{11} - \zeta_{11}^3$ has the norm 23 and there is no unit with the same parity as γ, and hence can serve us as a counter-example. And all of its conjugates, resp. all of those 220 permutations with this determinant are counterexamples as well.

Of course one could ask a question, whether there could be another element with norm 23, which satisfied condition of Lemma 1. Answer is no, because the elements of the same norm differs only by multiple of unit, then by taking parity matrices received as multiples of element γ_{23} and each of units in form $\varepsilon_1^{i_1}\varepsilon_2^{i_2}$ with $i_1 = 1, 2, ..., 11$, $i_2 = 1, 2, ..., 31$, we get set of all parities for elements with norm equal to 23. Comparing this with set of unit parity matrices one can see that there is nothing common, hence there is no pair γ, ω with $|N_{\mathbb{Q}(\zeta_{11})/\mathbb{Q}}(\gamma)| = 23$.

On the other hand element $\gamma = 1 + \zeta_{11}^3 - \zeta_{11}^8$, with $|N_{\mathbb{Q}(\zeta_{11})/\mathbb{Q}}(\gamma)| = 199$ and unit $v = \omega_5^{19}$ have the same coefficient parities

$$\upsilon = \mathrm{circ}_{11}(-1015495487978067, -854289166836692, -421852071343190,$$
$$144520076139427, 665008120576992, 974360785452496,$$
$$974360785452496, 665008120576992, 144520076139427,$$
$$-421852071343190, -854289166836692),$$

which is really awkward to carry through the computation, but using parity tables once again one can get unit with the same parity as follows:

$$\upsilon = \omega_5^{19} = \omega_5^{18}\omega_5 \neq \omega_3\omega_5 = \upsilon',$$

with

$$\upsilon' = \mathrm{circ}_{11}(-11, -10, -6, 1, 8, 12, 12, 8, 1, -6, -10),$$

which is much more comfortable.

Prime $l = 13$**.** The situation in $\mathbb{Q}(\zeta_{13})$ is similar to the case of $l = 11$, namely after computing fundamental units and determining their parity dependence, we find that there are only $13 \cdot 63 = 819$ parity distinct units and against $2^{13} - 1 = 8191$ possible odd-even distributions, as follows from the results and the tables in Appendix B, Subsection $l = 13$.

Permuting 13-tuple (1, 1, −1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) and computing the determinants of all corresponding circulant matrices one finds 78 units and elements with norms 27, 53, 79, 131, 521 each occurring 156-times, that is, 780 non-units, which is less than total number of parity distinct units, however it is enough to produce the counter-example.

For the element $\gamma = 1 - \zeta_{13} + \zeta_{13}^3$ with the norm equal to 53 there is no matching unit and there is no such unit even for $\gamma\upsilon$, where υ is any of those 819 parity distinct units.

On the other hand, let now be $\gamma = \zeta_{13} + \zeta_{13}^3 - \zeta_{13}^{12}$ with $N_{\mathbb{Q}(\zeta_{13})/\mathbb{Q}}(\gamma) = 521$, and let the unit υ be $\omega_1\omega_6^{60}$, then γ and υ have the same parities.

Multiplying γ by $\omega_1^{12}\omega_6^3$, one can get another pair

$$\gamma' = -79 - 132\zeta_{13} - 156\zeta_{13}^2 - 142\zeta_{13}^3 - 94\zeta_{13}^4 - 26\zeta_{13}^5 + 46\zeta_{13}^6 + 108\zeta_{13}^7 + 148\zeta_{13}^8 + 154\zeta_{13}^9 + 122\zeta_{13}^{10} + 62\zeta_{13}^{11} - 10\zeta_{13}^{12},$$

$$v' = \omega_0 = 1.$$

Prime $l = 17$**.** In the case of the field $\mathbb{Q}(\zeta_{17})$ a counter-example will be produced once again. But first of all notice that the tables in Appendix B, Subsection $l = 17$, show that all possible parity different units are given as product $\omega_1^{i_1}\omega_5^{i_5}\omega_6^{i_6}$ with $1 \le i_1 \le 17$ and $1 \le i_5,\ i_6 \le 16$, implying that its number is $4352 < 2^{l-1} - 1 = 2^{16} - 1 = 65535$.

To produce the counter-example, check the determinants of circulant matrices with entries being permutation of 17-tuple $(1, 1, -1, 0, 0, 0, 0\ 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$, one gets 136 units and elements with the norms 103, 137, 307, 409, 613, 3571.

Let γ be an element of $\mathbb{Q}(\zeta_{17})$ with the norm equal to 103, namely $\gamma = 1 + \zeta_{17} - \zeta_{17}^6$. Then to such element there is no unit satisfying conditions of Theorem 1 with the same parity.

The same is true for those elements of norms 137, 307, 409, 613, so in the fields satisfying conditions of Theorem 1 with these conductors, there are ambiguous ideals without a normal basis.

On the other hand, if we let the field K be as in Theorem 1 with the conductor $p = 3571$, then as shows the example of the element γ with the norm equal to $p = 3571$ and the unit v from the cyclotomic field $\mathbb{Q}(\zeta_{17})$,

$$\gamma = 1 + \zeta_{17} - \zeta_{17}^{16},$$

$$v = 3 + 3\zeta_{17} + 2\zeta_{17}^2 + 2\zeta_{17}^3 + 2\zeta_{17}^4 - 2\zeta_{17}^6 - 4\zeta_{17}^7 - 4\zeta_{17}^8 - 4\zeta_{17}^9 - 4\zeta_{17}^{10} - 2\zeta_{17}^{11} + 2\zeta_{17}^{13} + 2\zeta_{17}^{14} + 2\zeta_{17}^{15} + 3\zeta_{17}^{16}$$

there is a pair with matching parities, and one may construct

transformation matrices $\mathbf{A}_i$. Henceforth one may obtain normal bases of all ambiguous ideals of such field K.

Prime $l = 19$**.** All parity different units are products of powers of ω_1 and ω_9, see Appendix B, Subsection $l = 19$, and their number $19 \cdot 511 = 9709$, while $2^{l-1} - 1 = 2^{18} - 1 = 262143$. So counter-example must be shown once again.

Permutations of $(1, 1, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$ give us 171 units and the elements having norms equal to 191, 229, 419, 647, 761, 1483, 9349.

For the elements with the norms equal to 191, 229, 419, 647, 761, 1483, resp. for the fields as in Theorem 1 there are ambiguous ideals without a normal basis. As an example of such element take $\gamma = 1 + \zeta_{19} - \zeta_{19}^7$ with the $N_{\mathbb{Q}(\zeta_{19})/\mathbb{Q}}(\gamma) = 191$.

Now let γ to be the element of $\mathbb{Q}(\zeta_{19})$ with the norm equal to 9349 and the unit v with the same parity, namely

$$\gamma = 1 + \zeta_{19}^9 - \zeta_{19}^{10},$$

$$\begin{aligned} v = {} & 27 + 26\zeta_{19} + 18\zeta_{19}^2 - 6\zeta_{19}^3 - 38\zeta_{19}^4 - 48\zeta_{19}^5 - 24\zeta_{19}^6 \\ & + 8\zeta_{19}^7 + 24\zeta_{19}^8 + 27\zeta_{19}^9 + 27\zeta_{19}^{10} + 24\zeta_{19}^{11} + 8\zeta_{19}^{12} \\ & - 24\zeta_{19}^{13} - 48\zeta_{19}^{14} - 38\zeta_{19}^{15} - 6\zeta_{19}^{16} + 18\zeta_{19}^{17} + 26\zeta_{19}^{18}, \end{aligned}$$

then one gets the elements α_{13} resp. α_{32} with the corresponding matrices

$$\begin{aligned} \mathbf{A}_{13} = \operatorname{circ}_{38}(&14, 14, 13, 12, 9, 4, -3, -12, -19, -24, -24, \\ &-19, -12, -3, 4, 9, 12, 13, 14, 13, 13, 13, 12, 9, 4, -3, \\ &-12, -19, -24, -24, -19, -12, -3, 4, 9, 12, 13, 13) \end{aligned}$$

$$\begin{aligned} \mathbf{A}_{32} = \operatorname{circ}_{38}(&14, -14, 13, -12, 9, -4, -3, 12, -19, 24, -24, \\ &19, -12, 3, 4, -9, 12, -13, 14, -13, 13, -13, 12, -9, 4, 3, \\ &-12, 19, -24, 24, -19, 12, -3, -4, 9, -12, 13, -13). \end{aligned}$$

The matrix $\mathbf{A}_{13}$ transforms a normal basis of ideal $(\prod^{13})$ to a normal basis of ideal $(\prod^{14})$ and $\mathbf{A}_{32}$ transforms basis of $(\prod^{32})$ to the basis $(\prod^{33})$. The rest of transformation matrices can be obtained as above and so for every ambiguous ideal in the cyclic tamely ramified extension there exists normal basis.

The elements with norms 191, 229, 419, 647, 761, 1483, obtained above, can serve us as a counter-example, since there is no unit with the same parity and hence in the fields K, as in Theorem 1, with these conductors, there exist ambiguous ideals without normal integral basis.

Conclusion

From the above computations we have that any ambiguous ideal of a cyclic tamely ramified algebraic number field K has a normal basis for $[K : \mathbb{Q}] = 2l$ with $l = 2, 3, 5, 7$ and for $l = 11, 13, 17, 19$ there exist ambiguous ideals without normal basis.

Appendix A. Example

We shall illustrate the results on example of element $\gamma = 1 + \zeta_7 - \zeta_7^2 \in \mathbb{Q}(\zeta_7)$,

$$N_{\mathbb{Q}(\zeta_7)/\mathbb{Q}}(\gamma) = 29.$$

So let the prime p be equal to 29 and L be an extension of rationals of degree 14, i.e., $l = 7$. Also denote by $K \subset \mathbb{Q}(\zeta_{29})$ with $[K : \mathbb{Q}] = 7$. Primitive root modulo 29 is $r = 2$, hence

$$g = r^{\frac{p-1}{l}} = 16, \qquad \widetilde{g} = r^{\frac{p-1}{2l}} = 4.$$

Element γ can be represented by the circulant matrix

$$\mathbf{C} = \mathrm{circ}_7(1, 1, -1, 0, 0, 0, 0),$$

and hence its parity matrix is $\overline{\mathbf{C}} = \mathrm{circ}_7(1, 1, 1, 0, 0, 0, 0)$.

Solution of the congruence

$$1 + g^i - (g^i)^2 \equiv 0 \pmod{p},$$

is $i = 2$ and so the matrix $\mathbf{C}$ transforms normal basis of ideal (π^2) in K to the normal basis of ideal (π^3).

In order to find matrices transformating ideal basis in L, one have to find unit $\omega \in \mathbb{Q}(\zeta_7)$ with the same parity as γ. All possible parities are represented by $\omega_1^i\omega_3^j$, with $i, j = 1, 2, ..., 7$ so we search through them and find

$$\begin{aligned} v &= \omega_1\omega_3^6 \\ &= 785 + 1259\zeta_7 + 785\zeta_7^2 - 280\zeta_7^3 - 1134\zeta_7^4 - 1134\zeta_7^5 - 280\zeta_7^6, \end{aligned}$$

this is quite awkward to carry through all computations, but using the fact that ω_3^6 has the same parity as ω_2, we may replace the unit v by v',

$$v' = \omega_1\omega_2 = -1 - \zeta_7 - \zeta_7^2 + 2\zeta_7^4 + 2\zeta_7^5,$$

with the same parity.

Having γ and v' according to the proof of Lemma 1 we get two elements of $\mathbb{Q}(\zeta_{14})$ as a solution of equations (14). Denote them by α_2 and α_9, particularly they are

$$\alpha_2 = -\zeta_{14} - \zeta_{14}^3 - \zeta_{14}^4 + \zeta_{14}^7 + \zeta_{14}^8 + \zeta_{14}^9 + \zeta_{14}^{10},$$

$$\alpha_9 = \zeta_{14} + \zeta_{14}^3 - \zeta_{14}^4 - \zeta_{14}^7 + \zeta_{14}^8 - \zeta_{14}^9 + \zeta_{14}^{10}.$$

Notice that one can obtain matrices corresponding to the element α_2, resp. α_9 using the transformation matrix $\mathbf{X}$ defined in (7), i.e.,

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

From norm two block matrices

$$\mathbf{R} = \begin{pmatrix} \mathbf{C} & \mathbf{R}^* \\ \mathbf{O}_l & \mathbf{U} \end{pmatrix}, \qquad \mathbf{S} = \begin{pmatrix} \mathbf{U} & \mathbf{S}^* \\ \mathbf{O}_l & \mathbf{C} \end{pmatrix},$$

where $\mathbf{C}$ resp. $\mathbf{U}$ are circulant matrices representing γ resp. v'. Matrices $\mathbf{R}^* = (-\mathbf{C} + \mathbf{U})/2$ and $\mathbf{S}^* = (\mathbf{C} - \mathbf{U})/2$, thus matrices $\mathbf{A}_2$ and $\mathbf{A}_9$ can be obtained by

$$\mathbf{A}_2 = \mathbf{X}^{-1}\mathbf{R}\mathbf{X},$$

$$\mathbf{A}_9 = \mathbf{X}^{-1}\mathbf{S}\mathbf{X}. \tag{21}$$

Solving congruences (17) one finds that

$$\widetilde{g}^9 + (\widetilde{g}^9)^3 - (\widetilde{g}^9)^4 - (\widetilde{g}^9)^7 + (\widetilde{g}^9)^8 - (\widetilde{g}^9)^9 + (\widetilde{g}^9)^{10} \equiv 0 \pmod{29},$$

$$-\widetilde{g}^2 - (\widetilde{g}^2)^3 - (\widetilde{g}^2)^4 + (\widetilde{g}^2)^7 + (\widetilde{g}^2)^8 + (\widetilde{g}^2)^9 + (\widetilde{g}^2)^{10} \equiv 0 \pmod{29}$$

and hence the matrix $\mathbf{A}_2 = \mathrm{circ}_{14}(0, -1, 0, -1, -1, 0, 0, 1, 1, 1, 1, 0, 0, 0)$ transforms a normal basis of L ideal $(\prod^2)$ to a normal basis of ideal $(\prod^3)$ and the matrix $\mathbf{A}_9 = \mathrm{circ}_{14}(0, 1, 0, 1, -1, 0, 0, -1, 1, -1, 1, 0, 0, 0)$ a normal basis of $(\prod^9)$ to a normal basis of $(\prod^{10})$.

To find the rest of transformation matrices one just takes all conjugates of the element α_2 and solves corresponding congruences. This way we obtained matrices $\mathbf{A}_i$ for $0 < i < 14$, $i \neq 7$.

The matrices $\mathbf{A}_0$ and $\mathbf{A}_7$ are as in the proof of Lemma 1, i.e., with entries computed from the term $\frac{p-1}{2l}$, particularly

$$\mathbf{A}_0 = \mathrm{circ}_{2l}\left(\frac{p-1}{2l}+1, \frac{p-1}{2l}, \frac{p-1}{2l}, ..., \frac{p-1}{2l}\right),$$

$$\mathbf{A}_0 = \mathrm{circ}_{14}(3, 2, 2, ..., 2).$$

$$\mathbf{A}_0 = \mathrm{circ}_{14}(3, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2) \quad : \quad (\mathbb{Z}_L) \to (\Pi)$$

$$\mathbf{A}_1 = \mathrm{circ}_{14}(0, 0, 1, 0, 0, 0, 1, -1, -1, 1, 0, -1, 0, 1) \quad : \quad (\Pi) \to (\Pi^2)$$

$$\mathbf{A}_2 = \mathrm{circ}_{14}(0, -1, 0, -1, -1, 0, 0, 1, 1, 1, 1, 0, 0, 0) \quad : \quad (\Pi^2) \to (\Pi^3)$$

$$\mathbf{A}_3 = \mathrm{circ}_{14}(0, 0, 1, 1, 0, 0, 0, -1, 0, 1, 1, 0, -1, -1) \quad : \quad (\Pi^3) \to (\Pi^4)$$

$$\mathbf{A}_4 = \mathrm{circ}_{14}(0, 1, -1, 0, -1, 0, 1, 0, 0, 0, -1, 1, 0) \quad : \quad (\Pi^4) \to (\Pi^5)$$

$$\mathbf{A}_5 = \mathrm{circ}_{14}(0, 0, 0, 0, 1, -1, 1, -1, 0, 0, -1, 1, 0, 1) \quad : \quad (\Pi^5) \to (\Pi^6)$$

$$\mathbf{A}_6 = \mathrm{circ}_{14}(0, -1, 0, 1, 0, -1, -1, 1, 1, 0, 0, 0, 1, 0) \quad : \quad (\Pi^6) \to (\Pi^7)$$

$$\mathbf{A}_7 = \mathrm{circ}_{14}(3, -2, 2, -2, 2, -2, 2, -2, 2, -2, 2, -2, 2, -2) \quad : \quad (\Pi^7) \to (\Pi^8)$$

$$\mathbf{A}_8 = \mathrm{circ}_{14}(0, 0, 1, 0, 0, 0, 1, 1, -1, -1, 0, 1, 0, -1) \quad : \quad (\Pi^8) \to (\Pi^9)$$

$$\mathbf{A}_9 = \mathrm{circ}_{14}(0, 1, 0, 1, -1, 0, 0, -1, 1, -1, 1, 0, 0, 0) \quad : \quad (\Pi^9) \to (\Pi^{10})$$

$$\mathbf{A}_{10} = \mathrm{circ}_{14}(0, 0, 1, -1, 0, 0, 0, 1, 0, -1, 1, 0, -1, 1) \quad : \quad (\Pi^{10}) \to (\Pi^{11})$$

$$\mathbf{A}_{11} = \mathrm{circ}_{14}(0, -1, -1, 0, 1, 1, 0, -1, 0, 0, 0, 1, 1, 0) \quad : \quad (\Pi^{11}) \to (\Pi^{12})$$

$$\mathbf{A}_{12} = \mathrm{circ}_{14}(0, 0, 0, 0, 1, 1, 1, 1, 0, 0, -1, -1, 0, -1) \quad : \quad (\Pi^{12}) \to (\Pi^{13})$$

$$\mathbf{A}_{13} = \mathrm{circ}_{14}(0, 1, 0, -1, 0, 1, -1, -1, 1, 0, 0, 0, 1, 0) \quad : \quad (\Pi^{13}) \to (\Pi^{14})$$

The above table summarizes all the transformation matrices and also shows that each ideal of the field L has a normal basis.

Appendix B. Tables

Prime $l = 5$.

: The fundamental units ε_i and the ω_i units

$\mathbf{E}_{\varepsilon_1} = \mathrm{circ}_5(0, 1, 0, 0, 0)$, $\mathbf{W}_{\omega_1} = \mathrm{circ}_5(0, 1, 0, 0, 0)$,

$\mathbf{E}_{\varepsilon_2} = \mathrm{circ}_5(-1, -1, 0, 0, -1)$, $\mathbf{E}_{\varepsilon_1^2} \approx \mathbf{W}_{\omega_2} = \mathrm{circ}_5(1, 0, -1, -1, 0)$.

: Parity dependence of the units in $\mathbb{Q}(\zeta_5)$

	ε_1	ε_2
ε_1	6	-
ε_2	3	4

	ω_1	ω_2
ω_1	6	-
ω_2	3	4

Prime $l = 7$.

: The fundamental units ε_i

$$\mathbf{E}_{\varepsilon_1} = \mathrm{circ}_7(0, 1, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2} = \mathrm{circ}_7(-1, -1, -1, 0, 0, -1, -1),$$

$$\mathbf{E}_{\varepsilon_3} = \mathrm{circ}_7(1, 1, 0, 0, 0, 0, 1).$$

: The units ω_i

$$\mathbf{E}_{\varepsilon_1} = \mathbf{W}_{\omega_1} = \mathrm{circ}_7(0, 1, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2}^3 \approx \mathbf{W}_{\omega_2} = \mathrm{circ}_7(-1, -1, 0, 2, 2, 0, -1),$$

$$\mathbf{E}_{\varepsilon_2}\mathbf{E}_{\varepsilon_3} \approx \mathbf{W}_{\omega_3} = \mathrm{circ}_7(-1, -1, 0, 1, 1, 0, -1).$$

: Parity dependence of the units in $\mathbb{Q}(\zeta_7)$

	ε_1	ε_2	ε_3
ε_1	8	-	-
ε_2	7	8	3
ε_3	7	5	8

	ω_1	ω_2	ω_3
ω_1	8	-	-
ω_2	7	8	6
ω_3	7	6	8

Prime $l = 11$**.**

: The fundamental units ε_i

$$\mathbf{E}_{\varepsilon_1} = \mathrm{circ}_{11}(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2} = \mathrm{circ}_{11}(-1, -1, -1, -1, -1, 0, 0, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_3} = \mathrm{circ}_{11}(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1),$$

$$\mathbf{E}_{\varepsilon_4} = \mathrm{circ}_{11}(-1, -1, -1, -1, 0, 0, 0, 0, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_5} = \mathrm{circ}_{11}(1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1).$$

: The units ω_i

$$\mathbf{E}_{\varepsilon_1} = \mathbf{W}_{\omega_1} = \mathrm{circ}_{11}(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2}^5 \approx \mathbf{W}_{\omega_2} = \mathrm{circ}_{11}(-3, -3, -3, -2, 2, 7, 7, 2, -2, -3, -3),$$

$$\mathbf{E}_{\varepsilon_2}^2 \mathbf{E}_{\varepsilon_3} \approx \mathbf{W}_{\omega_3} = \mathrm{circ}_{11}(3, 2, 0, -1, -1, -1, -1, -1, -1, 0, 2),$$

$$\mathbf{E}_{\varepsilon_2}^3 \mathbf{E}_{\varepsilon_4} \approx \mathbf{W}_{\omega_4} = \mathrm{circ}_{11}(5, 4, 1, -2, -3, -3, -3, -3, -2, 1, 4),$$

$$\mathbf{E}_{\varepsilon_2} \mathbf{E}_{\varepsilon_5} \approx \mathbf{W}_{\omega_5} = \mathrm{circ}_{11}(-1, -1, -1, 0, 1, 1, 1, 1, 0, -1, -1).$$

: Parity dependence of the units in $\mathbb{Q}(\zeta_{11})$

	ε_1	ε_2	ε_3	ε_4	ε_5
ε_1	12	-	-	-	-
ε_2	31	32	7	3	15
ε_3	31	9	32	27	11
ε_4	31	21	23	32	5
ε_5	31	29	17	25	32

	ω_1	ω_2	ω_3	ω_4	ω_5
ω_1	12	-	-	-	-
ω_2	31	32	8	26	28
ω_3	31	4	32	11	19
ω_4	31	6	17	32	13
ω_5	31	10	18	12	32

Prime $l = 13$**.**

: The fundamental units ε_i

$$\mathbf{E}_{\varepsilon_1} = \mathrm{circ}_{13}(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2} = \mathrm{circ}_{13}(-1, -1, -1, -1, -1, -1, 0, 0, -1, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_3} = \mathrm{circ}_{13}(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1),$$

$$\mathbf{E}_{\varepsilon_4} = \mathrm{circ}_{13}(-1, -1, -1, -1, -1, 0, 0, 0, 0, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_5} = \mathrm{circ}_{13}(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1),$$

$$\mathbf{E}_{\varepsilon_6} = \mathrm{circ}_{13}(-1, -1, -1, -1, 0, 0, 0, 0, 0, 0, -1, -1, -1).$$

: The units ω_i

$$\mathbf{E}_{\varepsilon_1} = \mathbf{W}_{\omega_1} = \mathrm{circ}_{13}(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2}^6 \approx \mathbf{W}_{\omega_2} = \mathrm{circ}_{13}(15, 10, 1, -4, -5, -5, -5, -5, -5, -5, -4, 1, 10),$$

$$\mathbf{E}_{\varepsilon_2}^2 \mathbf{E}_{\varepsilon_3} \approx \mathbf{W}_{\omega_3} = \mathrm{circ}_{13}(3, 2, 0, -1, -1, -1, -1, -1, -1, -1, -1, 0, 2),$$

$$\mathbf{E}_{\varepsilon_2}^4 \mathbf{E}_{\varepsilon_4} \approx \mathbf{W}_{\omega_4} = \mathrm{circ}_{13}(-5, -5, -5, -4, 0, 6, 10, 10, 6, 0, -4, -5, -5),$$

$$\mathbf{E}_{\varepsilon_2}^3 \mathbf{E}_{\varepsilon_5} \approx \mathbf{W}_{\omega_5} = \mathrm{circ}_{13}(-3, -3, -3, -2, 1, 4, 5, 5, 4, 1, -2, -3, -3),$$

$$\mathbf{E}_{\varepsilon_2} \mathbf{E}_{\varepsilon_6} \approx \mathbf{W}_{\omega_6} = \mathrm{circ}_{13}(1, 1, 1, 0, -1, -1, -1, -1, -1, -1, 0, 1, 1).$$

: Parity dependence of the units in $\mathbb{Q}(\zeta_{13})$

	ε_1	ε_2	ε_3	ε_4	ε_5	ε_6
ε_1	14	-	-	-	-	-
ε_2	63	64	15	3	7	31
ε_3	21	-	22	17	-	-
ε_4	21	-	5	22	-	-
ε_5	9	-	-	-	10	-
ε_6	63	61	33	57	49	64

	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6
ω_1	14	-	-	-	-	-
ω_2	21	22	-	-	-	-
ω_3	63	30	64	56	8	13
ω_4	9	-	-	10	-	-
ω_5	63	51	8	7	64	41
ω_6	63	12	34	14	20	64

Prime $l = 17$**.**

: The fundamental units ε_i

$$\mathbf{E}_{\varepsilon_1} = \mathrm{circ}_{17}(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2} = \mathrm{circ}_{17}(-1, -1, -1, -1, -1, -1, -1, -1, 0, 0, -1, -1, -1, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_3} = \mathrm{circ}_{17}(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1),$$

$$\mathbf{E}_{\varepsilon_4} = \mathrm{circ}_{17}(-1, -1, -1, -1, -1, -1, -1, 0, 0, 0, 0, -1, -1, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_5} = \mathrm{circ}_{17}(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1),$$

$$\mathbf{E}_{\varepsilon_6} = \mathrm{circ}_{17}(-1, -1, -1, -1, -1, -1, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_7} = \mathrm{circ}_{17}(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1),$$

$$\mathbf{E}_{\varepsilon_8} = \mathrm{circ}_{17}(-1, -1, -1, -1, -1, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1).$$

: The units ω_i

$$\mathbf{E}_{\varepsilon_1} = \mathbf{W}_{\omega_1}$$

$$= \mathrm{circ}_{17}(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2}\mathbf{E}_{\varepsilon_3}^2 \approx \mathbf{W}_{\omega_2}$$

$$= \mathrm{circ}_{17}(-1, -1, -1, -1, -1, -1, 0, 2, 4, 4, 2, 0, -1, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon 3}^8 \approx \mathbf{W}_{\omega_3}$$

$$= \mathrm{circ}_{17}(721, 630, 398, 118, -120, -274, -350, -378, -385,$$

$$-385, -378, -350, -274, -120, 118, 398, 630),$$

$$\mathbf{E}_{\varepsilon_3}^4\mathbf{E}_{\varepsilon_4} \approx \mathbf{W}_{\omega_4}$$

$$= \mathrm{circ}_{17}(-19, -19, -19, -18, -14, -4, 12, 30, 42,$$

$$42, 30, 12, -4, -14, -18, -19, -19),$$

$$\mathbf{E}_{\varepsilon_3}^3\mathbf{E}_{\varepsilon_5} \approx \mathbf{W}_{\omega_5}$$

$$= \mathrm{circ}_{17}(17, 15, 9, 2, -4, -7, -8, -8, -8, -8, -8, -8, -7, -4, 2, 9, 15),$$

$$\mathbf{E}_{\varepsilon_3}\mathbf{E}_{\varepsilon_6} \approx \mathbf{W}_{\omega_6}$$

$$= \mathrm{circ}_{17}(-1, -1, -1, -1, -1, 0, 1, 2, 2, 2, 2, 1, 0, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_3}^5\mathbf{E}_{\varepsilon_7} \approx \mathbf{W}_{\omega_7}$$

$$= \mathrm{circ}_{17}(131, 121, 92, 47, -4, -49, -79, -94, -99,$$

$$-99, -94, -79, -49, -4, 47, 92, 121),$$

$$\mathbf{E}_{\varepsilon_3}^6\mathbf{E}_{\varepsilon_8} \approx \mathbf{W}_{\omega_8}$$

$$= \mathrm{circ}_{17}(-329, -314, -265, -175, -49, 92, 218, 307, 351,$$

$$351, 307, 218, 92, -49, -175, -265, -314).$$

: Parity dependence of the fundamental units ε_i in $\mathbb{Q}(\zeta_{17})$

	ε_1	ε_2	ε_3	ε_4	ε_5	ε_6	ε_7	ε_8
ε_1	18	-	-	-	-	-	-	-
ε_2	15	16	-	3	-	-	-	7
ε_3	15	-	16	-	-	-	-	-
ε_4	15	-	-	16	-	-	-	-
ε_5	15	-	-	-	6	-	-	-
ε_6	15	-	-	-	-	16	-	-
ε_7	15	-	-	-	-	-	16	-
ε_8	15	13	-	9	-	-	-	16

: Parity dependence of the units ω_i in $\mathbb{Q}(\zeta_{17})$

	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6	ω_7	ω_8
ω_1	18	-	-	-	-	-	-	-
ω_2	15	16	-	-	-	-	-	-
ω_3	15	-	16	-	-	-	-	-
ω_4	15	-	-	16	-	-	-	-
ω_5	15	-	-	-	16	-	-	-
ω_6	15	-	-	-	-	16	-	7
ω_7	15	-	-	-	-	-	16	-
ω_8	15	-	-	-	-	13	-	16

: Parity dependence among ω_i's

$$\omega_2 \approx \omega_5^8\omega_6^7, \qquad \omega_3 \approx \omega_5^{11}\omega_6^{12}, \qquad \omega_4 \approx \omega_5^{10}\omega_6^3,$$

$$\omega_7 \approx \omega_5^4\omega_6^{10}, \qquad \omega_8 \approx \omega_6^7.$$

Prime $l = 19$**.**

: The fundamental units ε_i

$$\mathbf{E}_{\varepsilon_1} = \mathrm{circ}_{19}(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2} = \mathrm{circ}_{19}(-1, -1, -1, -1, -1, -1, -1, -1, -1, 0,$$
$$0, -1, -1, -1, -1, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_3} = \mathrm{circ}_{19}(1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1),$$

$$\mathbf{E}_{\varepsilon_4} = \mathrm{circ}_{19}(-1, -1, -1, -1, -1, -1, -1, -1, 0, 0,$$
$$0, 0, -1, -1, -1, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_5} = \mathrm{circ}_{19}(1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1),$$

$$\mathbf{E}_{\varepsilon_6} = \mathrm{circ}_{19}(-1, -1, -1, -1, -1, -1, -1, 0, 0, 0,$$
$$0, 0, 0, -1, -1, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_7} = \mathrm{circ}_{19}(1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1),$$

$$\mathbf{E}_{\varepsilon_8} = \mathrm{circ}_{19}(-1, -1, -1, -1, -1, -1, 0, 0, 0, 0$$
$$0, 0, 0, 0, -1, -1, -1, -1, -1),$$

$$\mathbf{E}_{\varepsilon_9} = \mathrm{circ}_{19}(1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1).$$

: The units ω_i

$$\mathbf{E}_{\varepsilon_1} = \mathbf{W}_{\omega_1} = \mathrm{circ}_{19}(0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0),$$

$$\mathbf{E}_{\varepsilon_2}^{9} \approx \mathbf{W}_{\omega_2}$$

$$= \mathrm{circ}_{19}(-27, -27, -27, -27, -27, -26, -18, 9, 57, 99,$$
$$99, 57, 9, -18, -26, -27, -27, -27, -27),$$

$$\mathbf{E}_{\varepsilon_2}^{5}\mathbf{E}_{\varepsilon_3} \approx \mathbf{W}_{\omega_3}$$

$$= \mathrm{circ}_{19}(-5, -5, -5, -5, -5, -5, -4, 9, 11, 20,$$
$$20, 11, 9, -4, -5, -5, -5, -5, -5),$$

$$\mathbf{E}_{\varepsilon_2}^{7}\mathbf{E}_{\varepsilon_4} \approx \mathbf{W}_{\omega_4}$$

$$= \mathrm{circ}_{19}(85, 71, 37, 2, -19, -26, -27, -27, -27, -27,$$
$$-27, -27, -27, -27, -26, -19, 2, 37, 71),$$

$$\mathbf{E}_{\varepsilon_2}^{2}\mathbf{E}_{\varepsilon_5} \approx \mathbf{W}_{\omega_5}$$

$$= \mathrm{circ}_{19}(3, 3, 2, 0, -1, -1, -1, -1, -1, -1,$$
$$-1, -1, -1, -1, -1, -1, 0, 2, 3),$$

$$\mathbf{E}_{\varepsilon_2}^{4}\mathbf{E}_{\varepsilon_6} \approx \mathbf{W}_{\omega_6}$$

$$= \mathrm{circ}_{19}(-5, -5, -5, -5, -5, -4, 0, 6, 10, 11,$$
$$11, 10, 6, 0, -4, -5, -5, -5, -5),$$

$$\mathbf{E}_{\varepsilon_2}^{3}\mathbf{E}_{\varepsilon_7} \approx \mathbf{W}_{\omega_7}$$

$$= \mathrm{circ}_{19}(-3, -3, -3, -3, -3, -2, 1, 4, 5, 5,$$
$$5, 5, 4, 1, -2, -3, -3, -3, -3),$$

$$\mathbf{E}_{\varepsilon_2}^{6}\mathbf{E}_{\varepsilon_8} \approx \mathbf{W}_{\omega_8}$$

$$= \mathrm{circ}_{19}(-27, -27, -27, -26, -20, -5, 15, 30, 36, 37$$
$$37, 36, 30, 15, -5, -20, -26, -27, -27),$$

$$\mathbf{E}_{\varepsilon_2}\mathbf{E}_{\varepsilon_9} \approx \mathbf{W}_{\omega_9}$$

$$= \mathrm{circ}_{19}(-1, -1, -1, -1, -1, 0, 1, 1, 1, 1$$

$$1, 1, 1, 1, 0, -1, -1, -1, -1).$$

: Parity dependence of the fundamental units ε_i in $\mathbb{Q}(\zeta_{19})$

	ε_1	ε_2	ε_3	ε_4	ε_5	ε_6	ε_7	ε_8	ε_9
ε_1	20	-	-	-	-	-	-	-	
ε_2	511	512	15	3	127	31	63	7	255
ε_3	511	477	512	409	281	479	413	273	17
ε_4	511	341	5	512	383	351	21	343	85
ε_5	511	169	491	507	512	129	427	161	171
ε_6	511	33	495	99	103	512	35	231	239
ε_7	73	-	-	-	-	-	74	65	-
ε_8	73	-	-	-	-	-	9	74	-
ε_9	511	509	481	505	257	449	385	497	512

: Parity dependence of the units ω_i in $\mathbb{Q}(\zeta_{19})$

	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6	ω_7	ω_8	ω_9
ω_1	20	-	-	-	-	-	-	-	
ω_2	511	512	59	285	355	231	348	115	142
ω_3	511	26	512	256	32	385	361	435	115
ω_4	511	52	2	512	64	259	211	359	230
ω_5	511	416	16	8	512	28	155	317	307
ω_6	73	-	-	-	-	74	-	-	-
ω_7	511	395	310	155	211	287	512	457	391
ω_8	511	40	316	158	403	42	123	512	59
ω_9	511	18	40	20	258	70	132	26	512

References

[1] V. Dubovský, J. Kostra and V. Lazar, A note on normal bases of ideals in sextic algebraic number field, Mathematica Slovaca (to appear).

[2] S. Jakubec and J. Kostra, A note on normal bases of ideals, Mathematica Slovaca 42(5) (1992), 677-684.

[3] S. Ullom, Normal bases in Galois extensions of number fields, Nagoya Math. J. 34 (1969), 153-167.