Stanislav Jakubec; Juraj Kostra

A note on normal bases of ideals

Mathematica Slovaca, Vol. 42 (1992), No. 5, 677--684

Persistent URL: http://dml.cz/dmlcz/133222

Math. Slovaca, 42 (1992), No. 5, 677–684

Mathematica Slovaca

A NOTE ON NORMAL BASES OF IDEALS

STANISLAV JAKUBEC*) — JURAJ KOSTRA**)[1])

ABSTRACT. Let $K/\mathbb{Q}$ be a cyclic tamely ramified extension of prime degree l, then any ambiguous ideal of K has a normal basis if and only if for any prime p dividing the conductor of K there is an integer γ of cyclotomic field $\mathbb{Q}(\zeta_l)$ such that $N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma) = p$.

Introduction

Let $K/\mathbb{Q}$ be a Galois extension of the rationals. The following necessary and sufficient condition for an Abelian extension of the rationals $\mathbb{Q}$ to have a normal integral basis consisting of all conjugates of an integer of K was given by H. W. Leopoldt [2]:

The field K should be contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$ generated by an m-th primitive root of unity with square-free m. This can be equivalently reformulated that $K/\mathbb{Q}$ is a tamely ramified extension.

S. Ullom [3] reduced the question of existence of normal bases of ambiguous ideals in a tamely ramified Abelian extension of the rationals $\mathbb{Q}$ to the corresponding question for ambiguous ideals of the cyclotomic fields over $\mathbb{Q}$. He gave a sufficient condition for all the ambiguous ideals in cyclic extension of $\mathbb{Q}$ of a prime degree l to have a normal basis: 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 the present paper we shall give a necessary and sufficient condition for the existence of a normal basis for all ambiguous ideals in a tamely ramified cyclic extension $K/\mathbb{Q}$ of a prime degree l. This result is a consequence of the following:

AMS Subject Classification (1991): Primary 11R33.
Key words: Galois extension, Normal bases, Ambiguous ideal.
[1]) Research supported by Slovak Academy of Sciences. Grant 363.

Let

$$\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_p), \quad [K:\mathbb{Q}] = l, \quad \zeta_p = e^{2\pi i/p},$$
$$G(\mathbb{Q}(\zeta_l)/\mathbb{Q}) = \{\sigma_1, \sigma_2, \dots, \sigma_{l-1}\} \quad \text{and} \quad \pi = N_{\mathbb{Q}(\zeta_p)/K}(1-\zeta_p).$$

For $\beta \in K$ and $\sigma \in G = G(K/\mathbb{Q})$ we denote by $\sigma\beta$ the action of σ on β. If there is an integer $\gamma' \in \mathbb{Q}(\zeta_l)$ with $N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma') = p$, then there is an integer $\gamma \in \mathbb{Q}(\zeta_l)$ with $N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma) = p$ such that each of $\sigma_i\gamma$ for $i = 1, 2, \dots, l-1$, uniquely determines a circulant matrix which transforms a normal basis of the ideal (π^i) to a normal basis of the ideal (π^{i+1}).

First we recall some general properties of ambiguous ideals according to Ullom [3]. Let K/F be a Galois extension of algebraic number field F with Galois group G, $\mathbb{Z}_K$ (resp. $\mathbb{Z}_F$) 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

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

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

(i) $\Psi(\mathfrak{P})$ 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.

(ii) An ambiguous ideal U of K may be written in the form $U_O \cdot T$ where T is an ideal of F and

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

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

We shall prove the following theorem:

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 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 $|N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma)| = p$.*

Remark. If $h(\mathbb{Q}(\zeta_l)) = 1$, then for any 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 so Theorem 1 is an extension of Theorem 1.10 of [3].

In the following example we show that in the case class number $h(\mathbb{Q}(\zeta_l)) \neq 1$ it is possible that an ambiguous ideal in a tamely ramified cyclic extension $K/\mathbb{Q}$ of a prime degree l has not a normal basis.

Example 1. Let $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_{47})$ and $[K : \mathbb{Q}] = 23$. Let

$$N_{\mathbb{Q}(\zeta_{47})/K}(1-\zeta_{47}) = (1-\zeta_{47})(1-\zeta_{47}^{-1}).$$

The element $1-\zeta_{47}$ generates a normal basis of the ideal $(1-\zeta_{47})$ and so

$$\beta_1 = \operatorname{Tr}_{\mathbb{Q}(\zeta_{47})/K}(1-\zeta_{47}) = 2 - (\zeta_{47} + \zeta_{47}^{-1})$$

generates a normal basis $\{\beta_1, \beta_2, \dots, \beta_{23}\}$ of the ideal $(\pi) = \operatorname{Tr}_{\mathbb{Q}(\zeta_{47})/K}(1-\zeta_{47})$. To see that the ambiguous ideal (π^2) has not a normal basis consider ideals as $\mathbb{Z}$-moduls. We then get that the index $[(\pi) : (\pi^2)] = 47$. If there would exist a normal basis $\{\alpha_1, \alpha_2, \dots, \alpha_{23}\}$ of (π^2), then there exist $a_1, a_2, \dots, a_{23} \in \mathbb{Z}$ such that $\alpha_1 = a_1\beta_1 + a_2\beta_2 + \dots + a_{23}\beta_{23}$.

We have

$$\operatorname{Tr}_{K/\mathbb{Q}}((\pi)) = \operatorname{Tr}_{K/\mathbb{Q}}((\pi^2)) = (p)$$

and so

$$\sum_{i=1}^{23} a_i = \pm 1.$$

Then

$$\begin{aligned}[(\pi) : (\pi^2)] = 47 &= |\det \operatorname{circ}_{23}(a_1, a_2, \dots, a_{23})| \\ &= |N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}}(a_1 + a_2\zeta_{23} + \dots + a_{23}\zeta_{23}^{22})|\end{aligned}$$

and this contradicts the well known fact that an integer element γ with $|N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}}(\gamma)| = 47$ does not exist in $\mathbb{Q}(\zeta_{23})$. □

Now let $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_p)$, $[K : \mathbb{Q}] = l$, where l, p are primes with $p \equiv 1 \pmod{l}$. The primitive ambiguous ideals of K are

$$(\pi), (\pi^2), \dots, (\pi^l), \qquad \text{where} \quad \pi = N_{\mathbb{Q}(\zeta_p)/K}(1-\zeta_p).$$

Considering ideals (π^i) as $\mathbb{Z}$-moduls, we have that index $[(\pi^i) : (\pi^{i+1})] = p$.

LEMMA 1. *Each of the ideals* (π^i), $i = 1,2,\dots,l$ *has a normal basis if and only if there is an integer* $\gamma \in \mathbb{Q}(\zeta_l)$, *such that* $|N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma)| = p$.

Proof. Similarly as in Example 1, the existence of an integer $\gamma \in \mathbb{Q}(\zeta_l)$, $|N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma)| = p$ is a necessary condition for the existence of a normal basis for ideals (π^i). Let γ be such a element. Then

$$\gamma = c_1 + c_2\zeta_l + \dots + c_{l-1}\zeta_l^{l-2}$$

and

$$\gamma \equiv c_1 + c_2 + \dots + c_{l-1} \pmod{1 - \zeta_l}.$$

Clearly, there is a unit $\varepsilon \in \mathbb{Q}(\zeta_l)$, such that

$$\varepsilon\gamma \equiv 1 \pmod{1 - \zeta_l}.$$

Then there is $k \in \mathbb{Z}$ that

$$\varepsilon\gamma + k\big(1 + \zeta_l + \dots + \zeta_l^{l-1}\big) = b_1 + b_2\zeta_l + \dots + b_l\zeta_l^{l-1}$$

and $b_1 + b_2 + \dots + b_l = \pm 1$.

Let a be a positive integer such that the automorphism

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

restricted to the field K is nontrivial. Let $\pi' = \sigma\pi$ and ε_1 be such a unit of K that $\pi' = \varepsilon_1\pi$. Then

$$\varepsilon_1 = \frac{\pi'}{\pi} = \frac{\sigma N_{\mathbb{Q}(\zeta_p)/K}(1-\zeta_p)}{N_{\mathbb{Q}(\zeta_p)/K}(1-\zeta_p)} = N_{\mathbb{Q}(\zeta_p)/K}\big(1 + \zeta_p + \dots + \zeta_p^{a-1}\big)$$

and so

$$\varepsilon_1 \equiv a^{\frac{p-1}{l}} \pmod{1 - \zeta_p}.$$

Denote $g = a^{\frac{p-1}{l}}$. Then $g^l \equiv 1 \pmod{p}$. Consider all conjugates of

$$\varepsilon\gamma = b_1 + b_2\zeta_l + \dots + b_l\zeta_l^{l-1} \in \mathbb{Q}(\zeta_l).$$

We have $|N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\varepsilon\gamma)| = p$ and $g^l \equiv 1 \pmod{p}$ and so there exists for each $i = 1,2,\dots,l-1$ a unique conjugate $r_1 + r_2\zeta_l + \dots + r_l\zeta_l^{l-1}$ of $\varepsilon\gamma$, where $(r_1, r_2, \dots, r_l)$ is a permutation of $(b_1, b_2, \dots, b_l)$, such that

$$r_1 + r_2 g^i + \dots + r_l (g^i)^{l-1} \equiv 0 \pmod{p}.$$

Now we prove that if the ideal (π^i) has a normal basis, then the circulant matrix

$$\mathrm{circ}(r_1, r_2, \dots, r_l)^T$$

transforms a normal basis of the ideal (π^i) to a normal basis of the ideal (π^{i+1}).

Here it follows from previous ideas and the fact that the ideal (π) has a normal basis generated by $\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(1-\zeta)$ that each of the ideals (π^i), $i = 1, 2, \dots, l$, has a normal basis. Let $r_1 + r_2\zeta_l + \cdots + r_l\zeta_l^{l-1}$ be such a conjugate of $\varepsilon\gamma$ that $r_1 + r_2 g^i + \cdots + r_l(g^i)^{l-1} \equiv 0 \pmod{p}$.

Let the ideal (π^i) have a normal basis $\beta_1, \beta_2, \dots, \beta_l$, where $\beta_{j+1} = \sigma\beta_j$. We show that $\alpha = r_1\beta_1 + r_2\beta_2 + \cdots + r_l\beta_l$ generates a normal basis of the ideal (π^{i+1}). To prove this it is sufficient to show that

$$\mathrm{Index}\big[(\pi^i) : \mathbb{Z}_{G(K/\mathbb{Q})}[\alpha]\big] = p$$

and $\pi^{i+1} \mid \alpha$. We have

$$\begin{aligned}\mathrm{Index}\big[(\pi^i) : \mathbb{Z}_{G(K/\mathbb{Q})}[\alpha]\big] &= |\det \mathrm{circ}(r_1, r_2, \dots, r_l)| \\ = |(r_1 + r_2 + \cdots + r_l)\, N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}&(r_1 + r_2\zeta_l + \cdots + r_l\zeta_l^{l-1})| = p.\end{aligned}$$

Let

$$\begin{aligned}\beta_1 &= \pi^i\tau_1, \\ \beta_2 &= \varepsilon^i\pi^i\tau_2, \\ &\vdots \\ \beta_l &= (\varepsilon_1\varepsilon_2\dots\varepsilon_{l-1})^i\pi^i\tau_l,\end{aligned}$$

where $\varepsilon_{j+1} = \sigma\varepsilon_j$ and $\tau_{j+1} = \sigma\tau_j$. We have

$$\alpha = \pi^i\big(r_1\tau_1 + r_2\varepsilon_1^i\tau_2 + \cdots + r_l(\varepsilon_1\varepsilon_2\dots\varepsilon_{l-1})^i\tau_l\big).$$

We have to show that

$$\pi \mid r_1\tau_1 + r_2\varepsilon_1^i\tau_2 + \cdots + r_l(\varepsilon_1\varepsilon_2\dots\varepsilon_{l-1})^i\tau_l = T.$$

It is sufficient to show that

$$(1 - \zeta_p) \mid T.$$

From the fact that $\zeta_p \equiv 1 \pmod{1-\zeta_p}$ we have

$$\tau_1 \equiv \tau_2 \equiv \cdots \equiv \tau_l \equiv t \pmod{1-\zeta_p}$$

and

$$\varepsilon_1 \equiv \varepsilon_2 \equiv \cdots \equiv \varepsilon_{l-1} \equiv g \pmod{1-\zeta_p}.$$

Now it is sufficient to show that

$$r_1 + r_2 g^i + \cdots + r_l g^{i(l-1)} \equiv 0 \pmod{1-\zeta_p}.$$

But

$$r_1 + r_2 g^i + \cdots + r_l g^{i(l-1)} \equiv 0 \pmod{p}$$

and so

$$r_1 + r_2 g^i + \cdots + r_l g^{i(l-1)} \equiv 0 \pmod{1-\zeta_p}$$

and Lemma 1 is proved. □

Now we shall illustrate Lemma 1 for $p = 23$ and $l = 11$.

Example 2. Let $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_{23})$ and $[K : \mathbb{Q}] = 11$. As in the proof of Lemma 1 let $\pi = N_{\mathbb{Q}(\zeta_{23})/K}(1-\zeta_{23})$. The ideal (π) has a normal basis generated by $\mathrm{Tr}_{\mathbb{Q}(\zeta_{23})/K}(1-\zeta_{23})$. Let σ be the automorphism that $\sigma\colon \zeta_{23} \longmapsto \zeta_{23}^5$. Then

$$\varepsilon_1 = \frac{\sigma\pi}{\pi} \equiv 2 \pmod{23}.$$

If $\gamma = 1 + \zeta_{11}^4 + \zeta_{11}^9$, then $\gamma \in \mathbb{Q}(\zeta_{11})$ and $N_{\mathbb{Q}(\zeta_{11})/\mathbb{Q}}(\gamma) = 23$. The unit $\varepsilon = 1 + \zeta_{11} + \zeta_{11}^2 + \zeta_{11}^3$ satisfies $\varepsilon\gamma \equiv 1 \pmod{1-\zeta_{11}}$.

The element $\varepsilon\gamma$ can be expressed in such a form that the sum of coefficients is equal to one:

$$\varepsilon\gamma = (1 + \zeta_{11} + \zeta_{11}^2 + \zeta_{11}^3)(1 + \zeta_{11}^4 + \zeta_{11}^9) - (1 + \zeta_{11} + \cdots + \zeta_{11}^{10}) = 1 + \zeta_{11} - \zeta_{11}^8.$$

Let $f(\zeta_{11})$ be such a conjugate of $1 + \zeta_{11} - \zeta_{11}^8$ that $f(2^i) \equiv 0 \pmod{23}$. Then $f(\zeta_{11})$ determines the circulant matrix A_i, which transforms a normal basis of the ideal (π^i) to a normal basis of the ideal (π^{i+1}). In such a way we get:

$$\begin{aligned}
1+\zeta_{11}-\zeta_{11}^{8} &\longmapsto A_1 = \mathrm{circ}\,(1,1,0,0,0,0,0,0,-1,0,0)^T\\
1-\zeta_{11}^{4}+\zeta_{11}^{6} &\longmapsto A_2 = \mathrm{circ}\,(1,0,0,0,-1,0,1,0,0,0,0)^T\\
1+\zeta_{11}^{4}-\zeta_{11}^{10} &\longmapsto A_3 = \mathrm{circ}\,(1,0,0,0,1,0,0,0,0,0,-1)^T\\
1+\zeta_{11}^{2}+\zeta_{11}^{3} &\longmapsto A_4 = \mathrm{circ}\,(1,0,-1,1,0,0,0,0,0,0,0)^T\\
1-\zeta_{11}^{6}+\zeta_{11}^{9} &\longmapsto A_5 = \mathrm{circ}\,(1,0,0,0,0,0,-1,0,0,1,0)^T\\
1+\zeta_{11}^{2}-\zeta_{11}^{5} &\longmapsto A_6 = \mathrm{circ}\,(1,0,1,0,0,-1,0,0,0,0,0)^T\\
1+\zeta_{11}^{8}-\zeta_{11}^{9} &\longmapsto A_7 = \mathrm{circ}\,(1,0,0,0,0,0,0,0,1,-1,0)^T\\
1-\zeta_{11}+\zeta_{11}^{7} &\longmapsto A_8 = \mathrm{circ}\,(1,-1,0,0,0,0,0,1,0,0,0)^T\\
1+\zeta_{11}^{5}-\zeta_{11}^{7} &\longmapsto A_9 = \mathrm{circ}\,(1,0,0,0,0,1,0,-1,0,0,0)^T\\
1-\zeta_{11}^{3}+\zeta_{11}^{10} &\longmapsto A_{10} = \mathrm{circ}\,(1,0,0,-1,0,0,0,0,0,0,1)^T\,.
\end{aligned}$$

□

P r o o f o f T h e o r e m 1. Now consider the general situation.

Let $[K:\mathbb{Q}]=l$, $K\subset\mathbb{Q}(\zeta_m)$, where m is the smallest number for which $K\subset\mathbb{Q}(\zeta_m)$. Let $m=p_1p_2p_3\dots p_s$ be the factorization of m into the product of distinct primes. Each p_i is totally ramified in K:

$$p_i\,\mathbb{Z}_K=P_i^e\,.$$

By [3, Theorem 1.9] the ideals P_i, $i=1,2\dots,s$ have a normal basis. If for some i and for all integers $\gamma\in\mathbf{Q}(\zeta_l)$ we have $|N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma)|\neq p_i$, then by the same reason as in Example 1 the ambiguous ideal P_i^2 has not a normal basis.

To prove the converse statement we need the following Lemma.

LEMMA 2. *Let $\mathbb{Q}\subset L_{p_i}\subset\mathbb{Q}(\zeta_{p_i})$, $[L_{p_i}:\mathbb{Q}]=l$, for $i=1,2,\dots s$. Then*

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

P r o o f . We have

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

with

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

and the index

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

Clearly $H = \left[(\mathbb{Z}/m\mathbb{Z})^*\right]^l$. Let $G = G\left(\mathbb{Q}^*(\zeta_m)/K\right)$. 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 l and so $x^l \in G$. We have $H \subset G$. □

Suppose now that for any p_i, $i = 1, 2, \dots, s$, there is an integer $\gamma_i \in \mathbb{Q}(\zeta_l)$ such that $N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\gamma_i) = p_i$. By Lemma 1 any ambiguous ideal of L_{p_i}, $i = 1, 2 \dots, s$, 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 ambiguous ideal of K has a normal basis. This proves Theorem 1.

REFERENCES

[1] DAVIS, P. J.: *Circulant Matrices*, Wiley-Interscience publishers, John Wiley and sons, New York-Chichester-Brisbane-Toronto, 1979.

[2] LEOPOLDT, H. W.: *Zur Arithmetic in abelschen Zahlkörpern*, J. Reine Angew. Math. **209** (1962), 54–71.

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

Received April 9, 1990

Revised October 27, 1992

*) *Mathematical Institute*
Slovak Academy of Sciences
Štefánikova 49
814 73 Bratislava
Czecho-Slovakia

**) *Department of Mathematics*
Faculty of Civil Engineering
Radlinského 11
813 68 Bratislava
Czecho-Slovakia