ON THE EXISTENCE OF AN INTEGRAL NORMAL BASIS
GENERATED BY A UNIT IN PRIME EXTENSIONS
OF RATIONAL NUMBERS

STANISLAV JAKUBEC, JURAJ KOSTRA, AND KAROL NEMOGA

Abstract. In the present paper a necessary condition for a cyclic extension
of the rationals of prime degree \( l \) to have an integral normal basis generated
by a unit is given. For a fixed \( l \), this condition implies that there exists at
most a finite number of such fields. A computational method for verifying the
existence of an integral normal basis generated by a unit is given. For \( l = 5 \),
all such fields are found.

Let the field \( K \) be a Galois extension of the rational numbers of prime degree
\( l \). According to the Kronecker-Weber theorem there exists a positive integer \( m \)
such that \( K \subseteq Q(m) \), where \( Q(m) \) is the cyclotomic field of \( m \)th roots of unity
over \( Q \). Let \( m \) be the least such integer. In the field \( K \) there exists an integral
normal basis if and only if \( m \) is squarefree (Leopoldt [1]).

In the present paper the existence of an integral normal basis generated by
a unit in a prime extension of rational numbers \( Q \) will be investigated. The
procedure for solving this problem will be the following.

1. It is obvious that if an element generates an integral normal basis over
\( Q \), then its trace in \( Q \) is \( \pm 1 \). We will determine a necessary condition which
a positive integer \( m \) has to fulfill under the suppositions that \( K \subseteq Q(m) \), and
in the field \( K \) there exists a unit \( \varepsilon \) such that

\[
\text{Tr}_{K/Q}(\varepsilon) = \pm 1.
\]

We shall prove that for each prime \( l \) there exists only a finite number of positive
integers \( m \) fulfilling this condition. So there is at most a finite number of fields
\( K \) of prime degree \( l \) over \( Q \) in which an integral normal basis is generated by
a unit.

2. For each field \( K \) of degree \( l \) over \( Q \) the problem of the existence of a
normal basis generated by a unit will be solved. This solution will be computa-
tional and based on the isomorphism between a subgroup \( E \subseteq Q(\omega) \), where
\( \omega = \sqrt{l} \),

\[
E\{\gamma \in Q(\omega), N(\gamma) = \pm 1, \gamma \equiv \pm 1 \pmod{l - \omega}\},
\]

and the group \( C_l \) of all circulant unimodular matrices of degree \( l \).

Received June 12, 1989; revised December 7, 1989.
1980 Mathematics Subject Classification (1985 Revision). Primary 11R33.
Let the field \( K \) be an extension of \( \mathbb{Q} \) of prime degree \( l \). Let there be an integral normal basis in the field \( K \). Let \( m \) be the least positive integer such that \( K \subset \mathbb{Q}(m) \). Since \( m \) is squarefree, there exist distinct primes \( p_1, p_2, \ldots, p_s \) such that

\[
m = p_1 \cdot p_2 \cdots p_s.
\]

**Theorem 1.** Let \( \varepsilon \) be a unit in the field \( K \) and \( \text{Tr}_{K/\mathbb{Q}}(\varepsilon) = \pm 1 \). Then

\[
(2) \quad l^i \equiv 1 \pmod{p_i} \quad \text{for all } i = 1, 2, \ldots, s,
\]

or

\[
(3) \quad l^i \equiv -1 \pmod{p_i} \quad \text{for all } i = 1, 2, \ldots, s,
\]

where the \( p_i \) are the factors of \( m \) given by (1).

**Proof.** By definition of \( m \) it follows that \( p_i \) is totally ramified in \( K/\mathbb{Q} \) for all \( i = 1, 2, \ldots, s \). So, \( \varepsilon \equiv a \pmod{\varphi_i} \) for some rational integer \( a \), where \( \varphi_i \) is the prime above \( p_i \) in \( K \). Therefore, \( \pm 1 = \text{Tr}_{K/\mathbb{Q}}(\varepsilon) \equiv la \pmod{p_i} \) and \( \pm 1 = N_{K/\mathbb{Q}}(\varepsilon) \equiv a^l \pmod{p_i} \). It follows that

\[
\text{Tr}_{K/\mathbb{Q}}(\varepsilon)^l \equiv l^ia^l \equiv N_{K/\mathbb{Q}}(\varepsilon)/l^i \pmod{p_i}
\]

for all \( i = 1, 2, \ldots, s \). Therefore, either \( l^i \equiv +1 \pmod{p_i} \) for all \( i \), or \( l^i \equiv -1 \pmod{p_i} \) for all \( i \). \( \Box \)

Our aim is to find all fields of given prime degree \( l \) over \( \mathbb{Q} \) in which there exists an integral normal basis generated by a unit. If a unit \( \varepsilon \in K \) generates an integral normal basis over \( \mathbb{Q} \), then \( \text{Tr}_{K/\mathbb{Q}}(\varepsilon) = \pm 1 \). Hence, by Theorem 1, congruences (2) or congruences (3) hold. We shall give a computational method for verifying the existence of an integral normal basis generated by a unit.

For \( l = 2 \), the solution of the problem is trivial. In the following, \( l \) is an odd prime.

The field \( K \) will be determined by the Galois group

\[
G = \Gamma(\mathbb{Q}(m)/K) \subset (\mathbb{Z}/m\mathbb{Z})^*.
\]

We need some further notation. For \( i \in \{1, 2, \ldots, s\} \), let \( m_i = m/p_i \) and define the projection

\[
\text{pr}_i: G \to (\mathbb{Z}/m_i\mathbb{Z})^*,
\]

where for \( \sigma \in G \), \( \text{pr}_i(\sigma) \) is the restriction of \( \sigma \) on \( \mathbb{Q}(m_i) \). By the symbol \( H_i \) we denote the image \( \text{pr}_i(G) \).

**Lemma 1.** Let \( L \) be the fixed field of the group \( H_i \). Then \( K \cap \mathbb{Q}(m_i) = L \).

**Proof.** (a) First we show that if \( x \in K \cap \mathbb{Q}(m_i) \), then \( x \in L \), i.e., \( \psi(x) = x \) for all \( \psi \in H_i \). Let \( \psi \in H_i \). Then there exists \( \psi' \in G \) such that \( \text{pr}_i(\psi') = \psi \). Thus, \( \psi(x) = \text{pr}_i(\psi')(x) = x \).
(b) Conversely, let \( x \in L \). We have to prove that \( x \in K \cap Q(m_i) \). Since \( L \subseteq Q(m_i) \), it is sufficient to show that \( x \in K \). Let \( \psi' \in G \). Then \( \psi'(x) = pr_i(\psi')(x) = x \). Hence \( x \in K \). □

**Corollary 1.** For \( i = 1, 2, \ldots, s \), \( H_i = (Z/m_iZ)^* \).

*Proof.* Since \( [K : Q] = l \) is a prime, the field extension \( K/Q \) has no nontrivial intermediary field. □

**Corollary 2.** For all \( p_1, p_2, \ldots, p_s \),

\[
p_1 \equiv p_2 \equiv \cdots \equiv p_s \equiv 1 \pmod{l}.
\]

*Proof.* Let, for instance, \( p_s \not\equiv 1 \pmod{l} \). The homomorphism \( pr_z : G \rightarrow (Z/m_zZ)^* \) is surjective by Corollary 1. Hence,

\[
\frac{|(Z/m_zZ)^*|}{|G|}.
\]

It follows that

\[
\prod_{i=1}^{s-1} (p_i - 1) \cdot \prod_{i=1}^{l} \frac{p_i - 1}{l},
\]

which contradicts \( p_s - 1 \not\equiv 0 \pmod{l} \). □

**Example 1.** Let \( [K : Q] = 5 \). If in the field \( K \) there exists a unit of trace 1, then Theorem 1 determines all possible values of \( m \) such that \( K \subseteq Q(m) \) and \( m \) is the least such positive integer. We have to find all primes \( p \), \( p \equiv 1 \pmod{5} \), fulfilling the congruences of Theorem 1,

\[
5 \equiv 1 \pmod{p} \quad \text{or} \quad 5 \equiv -1 \pmod{p}.
\]

We obtained the following four values of \( m \):

\[
m = 11, \quad m = 71, \quad m = 521, \quad m = 11 \cdot 71.
\]

Let \( \xi \) denote the primitive \( m \)th root of unity. By \( G \) we will denote the Galois group

\[
G = \Gamma(Q(m)/K) \subset (Z/mZ)^*.
\]

It is known that the numbers \( \xi^b, \ b \in (Z/mZ)^* \), form an integral normal basis of the field \( Q(m) \). So the following proposition holds.

**Proposition 1.** For a fixed \( a \in (Z/mZ)^* - G \),

\[
\alpha_1 = \sum_{x \in G} \xi^x, \quad \alpha_2 = \sum_{x \in G} \xi^{ax}, \ldots, \quad \alpha_l = \sum_{x \in G} \xi^{a^{l-1}x}
\]

form an integral normal basis of the field \( K \) over \( Q \).

Let \( C_l \) be the group of all unimodular circulant matrices of rank \( l \). Let \( \alpha_1, \alpha_2, \ldots, \alpha_l \) be an integral normal basis of the field \( K \) defined by (4). Let \( \beta_1, \beta_2, \ldots, \beta_l \) be an integral normal basis of the field \( K \). Then we have

\[
(\beta_1, \beta_2, \ldots, \beta_l) = (\alpha_1, \alpha_2, \ldots, \alpha_l) \cdot A,
\]

where \( A \in C_l \).
We shall investigate the set of norms $\{N(\beta_i)\}$ for all integral normal bases $(\beta_1, \beta_2, \ldots, \beta_l) = (\alpha_1, \alpha_2, \ldots, \alpha_l) \cdot A$, $A \in C_1$, for a fixed prime modulus $p$.

Let $E$ be a subgroup of $Q(l)$,

$$E = \{ \gamma \in Q(l) ; \gamma \text{ is a unit, } \gamma \equiv \pm 1 \pmod{1 - \omega} \},$$

where $\omega = \sqrt{-1}$. An element $\gamma \in E$ can be expressed in the form

$$\gamma = b_1 \omega + b_2 \omega^2 + \cdots + b_{l-1} \omega^{l-1}.$$ 

Since $\gamma \equiv \pm 1 \pmod{1 - \omega}$ and $\gamma \equiv -Tr_{Q(l)/Q}(\gamma) \pmod{1 - \omega}$, the following congruence holds:

$$b_1 + b_2 + \cdots + b_{l-1} \equiv \pm 1 \pmod{l}.$$ 

Hence, for $l \neq 2$, there exists a unique integer $c$ such that

$$b_1 + b_2 + \cdots + b_{l-1} + l \cdot c = \pm 1.$$ 

We define a mapping $\Phi$, from $E$ into a set of circulant matrices of rank $l$:

For $\gamma \in E$, let

$$\Phi(\gamma) = \text{Circ}_l(a_1, a_2, \ldots, a_l),$$

where $a_1 = c$, $a_2 = b_1 + c$, $\ldots$, $a_l = b_{l-1} + c$.

**Lemma 2.** The mapping $\Phi$ is an isomorphism of groups $E$ and $C_l$.

**Proof.** Since the number $c$ is determined uniquely, the mapping $\Phi$ is correctly defined. $\Phi$ is clearly a homomorphism, i.e.,

$$\Phi(\gamma_1 \cdot \gamma_2) = \Phi(\gamma_1) \cdot \Phi(\gamma_2)$$

for all $\gamma_1, \gamma_2 \in E$. The formula for a determinant of a circulant matrix,

$$\det \text{Circ}_l(a_1, a_2, \ldots, a_l) = (a_1 + \cdots + a_l) \cdot N_{Q(l)/Q}(a_1 + a_2 \omega + \cdots + a_l \omega^{l-1}),$$

implies that $\Phi$ is into the group $C_l$. Directly from the definition of $\Phi$, it follows that $\Phi$ is a surjection and an injection. 

The group $E$ is a subgroup of the group of all units of the field $Q(l)$. Let $t = (l - 1)/2 - 1$ and $\eta_1, \eta_2, \ldots, \eta_t$ be fundamental units of the field $Q(l)$. Clearly, there is a positive integer $a$ such that

$$\eta_1^a, \eta_2^a, \ldots, \eta_t^a \in E.$$ 

And so there exist $t$ fundamental units $\eta_1, \eta_2, \ldots, \eta_t$ of the group $E$. (Every finitely generated torsionfree module has a basis.) Hence, for any $\gamma \in E$, we have

$$\gamma = (-\omega)^n \cdot \eta_1^{c_1} \cdot \eta_2^{c_2} \cdots \eta_t^{c_t}, \quad n, c_1, c_2, \ldots, c_t \in \mathbb{Z}.$$ 

Let $p \equiv 1 \pmod{l}$. Let $Z(\omega)$ be the ring of integers of the field $Q(l)$. Let $\varepsilon$ be a unit of $Z(\omega)$. Hence, $(\varepsilon, p) = 1$ in $Z(\omega)$ and $\varepsilon = b_1 \omega + b_2 \omega^2 + \cdots + b_{l-1} \omega^{l-1}$. The following congruence holds:

$$\varepsilon^p = (b_1 \omega + b_2 \omega^2 + \cdots + b_{l-1} \omega^{l-1})^p$$

$\equiv b_1^p \omega^p + b_2^p \omega^{2p} + \cdots + b_{l-1}^p \omega^{p(l-1)} \equiv \varepsilon \pmod{p}.$
Denote by $d$ the least positive integer such that $e^d \equiv 1 \pmod{p}$. Hence, $d \mid (p-1)$. The integer $d$ can be determined exactly.

**Lemma 3.** Let $e = b_1 \omega + b_2 \omega^2 + \cdots + b_{l-1} \omega^{l-1}$ be a unit of the ring $\mathbb{Z}(\omega)$ and $f(x) = b_1 x + b_2 x^2 + \cdots + b_{l-1} x^{l-1}$. Let $\varphi$ be a primitive root modulo $p$ and $g_1 = \varphi^{(p-1)/l}$. Denote by $a_k$, $k = 1, 2, \ldots, l-1$, the least positive integer such that $f(g_1^{k})^{a_k} \equiv 1 \pmod{p}$. Then $d$ is the least common multiple of the numbers $a_k$.

**Proof.** For each $k = 1, 2, \ldots, l-1$ there exists exactly one prime divisor $\varphi_k$ in $\mathbb{Z}(\omega)$ such that $\varphi_k \mid p$ and $\omega \equiv g_1^k \pmod{\varphi_k}$. Therefore,

$$\varphi = f(\omega) \equiv f(g_1^k) \pmod{\varphi_k}.$$

Since $1 \equiv e^d \equiv f(g_1^k)^d \pmod{\varphi_k}$, we have

$$1 \equiv f(g_1^k)^d \pmod{p}$$

for all $k = 1, 2, \ldots, l-1$.

Denote by the symbol $d^*$ the least common multiple of the numbers $a_1$, $a_2$, $\ldots$, $a_{l-1}$. From (5) we have $d^* \mid d$.

Since $e^{d^*} \equiv 1 \pmod{\varphi_k}$ for all $k = 1, 2, \ldots, l-1$, we have that $e^{d^*} - 1$ is divisible by $p = \prod_{k=1}^{l-1} \varphi_k$. Therefore, $e^{d^*} \equiv 1 \pmod{p}$ and $d \mid d^*$. This concludes the proof of Lemma 3. \(\square\)

We define matrices $A_0 = \Phi(-\omega)$, $A_1 = \Phi(\eta_1)$, $A_2 = \Phi(\eta_2)$, $\ldots$, $A_t = \Phi(\eta_t)$. And so for $A \in C_i$, we have

$$A = A_0^{n_0} \cdot A_1^{n_1} \cdot A_2^{n_2} \cdots A_t^{n_t}, \quad n_0, n_1, \ldots, n_t \in \mathbb{Z}.$$

As was shown above, when the set

$$\{N(\beta_i); (\beta_1, \beta_2, \ldots, \beta_i) = (\alpha_1, \alpha_2, \ldots, \alpha_i) \cdot A, \ A \in C_i\}$$

is investigated modulo $p$, it is sufficient to investigate a finite set of norms $\{N(\beta_i); (\beta_1, \ldots, \beta_i) = (\alpha_1, \ldots, \alpha_i) \cdot A\}$, $A = A_0^{n_0} \cdot A_1^{n_1} \cdots A_t^{n_t}$, $n_0 \leq 2l$, $n_1 \leq d_1$, $\ldots$, $n_t \leq d_t$, where $d_1, \ldots, d_t$ are corresponding periods computable by Lemma 3.

**Example 2.** In this example, all fields $K$ of degree 5 over $Q$ in which an integral normal basis generated by a unit exists will be determined.

Let $K$ be such a field. Then by Example 1, $K \subset Q(m)$, where

(a) $m = 11$, \quad (b) $m = 71$, \quad (c) $m = 521$, \quad (d) $m = 11 \cdot 71$.

(b) $m = 11$. The element $\alpha$ defined by (4) is a unit. Hence, the field $K \subset Q(11)$ of degree 5 over $Q$ has an integral normal basis generated by the unit $\alpha$.

(b) $m = 71$. This is the same case as in part (a). $K \subset Q(71)$, $K$ is of degree 5 over $Q$ and has an integral normal basis generated by the unit $\alpha$. 

(c) \( m = 521 \). In this case, the element \( \alpha \) has the norm \( N_{K/Q}(\alpha) = -2083 \).
In the field \( Q(5) \), \( t = (l - 1)/2 - 1 = (5 - 1)/2 - 1 = 1 \). (\( t \) is the number of fundamental units of the field \( Q(5) \).) By computation it can be verified that \( \eta_1 = 1 + \omega^3 - \omega^4 \) is a fundamental unit of the group \( E \). Put \( A_1 = \Phi(\eta_1) = \text{Circ}_2(1, 0, 0, 1, -1) \). Define the sequence of norms
\[
u_n = N_{K/Q}(\beta_1),
\]
where \( (\beta_1, \ldots, \beta_5) = (\alpha_1, \ldots, \alpha_5) \cdot A^n, \; n \in \mathbb{Z} \).

Let \( p = 11 \). By a direct computation we have that the period \( d_1 = 10 \).
Thus, the sequence \( u_n \) is periodic, with the period 10 modulo 11. By means of a computer it has been found that the sequence \( u_n \) assumes these values modulo 11:
\[
(u_1, \ldots, u_{10}) = (9, 4, 8, 4, 7, 10, 2, 9, 4, 7).
\]

Hence, the numbers \( N_{K/Q}(\beta_1) \), where \( (\beta_1, \ldots, \beta_5) = (\alpha_1, \ldots, \alpha_5) \cdot A, \; A \in C_1 \), assume the values \( \pm 9, \pm 4, \ldots, \pm 7 \). (Since \( A = A_0 \cdot A_1^n, \; n \in \mathbb{Z} \), \( A_0 = \text{Circ}_2(0, -1, 0, 0, 0) = \Phi(-\omega) \).

It follows from above that \( \beta_1 \), for \( (\beta_1, \ldots, \beta_5) = (\alpha_1, \ldots, \alpha_5) \cdot A^a \cdot A_1^n \), can be a unit if \( n \equiv 6 \) (mod 10).

Now the sequence \( u_n \) will be investigated modulo 61. In this case, the period \( d_1 = 15 \). Clearly, it is sufficient to investigate the numbers \( u_n \), \( n = 1, 6, 11 \).
We have that \( u_1 \equiv 50, \; u_6 \equiv 54, \; u_{11} \equiv 26 \) (mod 61), which are all different from \( \pm 1 \) (mod 61).

Thus, in the field \( K \subset Q(521) \), \( [K : Q] = 5 \), an integral normal basis generated by a unit does not exist.

(d) \( m = 11 \cdot 71 \). In the field \( Q(11 \cdot 71) \) there exist four subfields \( K \) of degree 5 over \( Q \), corresponding to subgroups of the group \( (\mathbb{Z}/11 \cdot 71\mathbb{Z})^* \) of index 5, the projections of which are surjective:

1. the field \( K_1 \) corresponding to the subgroup generated by 122, 717;
2. the field \( K_2 \) corresponding to the subgroup generated by 122, 475;
3. the field \( K_3 \) corresponding to the subgroup generated by 122, 343;
4. the field \( K_4 \) corresponding to the subgroup generated by 122, 200.

In all four cases 1–4, the sequence \( u_n \) modulo 61 was investigated. The following values were obtained:

<table>
<thead>
<tr>
<th>( u_n )</th>
<th>1.</th>
<th>2.</th>
<th>3.</th>
<th>4.</th>
<th>5.</th>
<th>6.</th>
<th>7.</th>
<th>8.</th>
<th>9.</th>
<th>10.</th>
<th>11.</th>
<th>12.</th>
<th>13.</th>
<th>14.</th>
<th>15.</th>
</tr>
</thead>
<tbody>
<tr>
<td>( K_1 )</td>
<td>20</td>
<td>14</td>
<td>36</td>
<td>60</td>
<td>20</td>
<td>0</td>
<td>19</td>
<td>24</td>
<td>42</td>
<td>21</td>
<td>40</td>
<td>52</td>
<td>44</td>
<td>36</td>
<td>17</td>
</tr>
<tr>
<td>( K_2 )</td>
<td>7</td>
<td>13</td>
<td>46</td>
<td>53</td>
<td>20</td>
<td>41</td>
<td>47</td>
<td>39</td>
<td>38</td>
<td>30</td>
<td>27</td>
<td>35</td>
<td>7</td>
<td>34</td>
<td>49</td>
</tr>
<tr>
<td>( K_3 )</td>
<td>23</td>
<td>51</td>
<td>43</td>
<td>41</td>
<td>14</td>
<td>36</td>
<td>41</td>
<td>52</td>
<td>55</td>
<td>25</td>
<td>57</td>
<td>21</td>
<td>59</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>( K_4 )</td>
<td>32</td>
<td>41</td>
<td>31</td>
<td>24</td>
<td>18</td>
<td>45</td>
<td>27</td>
<td>34</td>
<td>34</td>
<td>1</td>
<td>50</td>
<td>6</td>
<td>48</td>
<td>30</td>
<td>31</td>
</tr>
</tbody>
</table>

In case 1, for \( n = 4 \) we have \( u_n \equiv -1 \) (mod 61). Using computations modulo 31, where the period of the sequence \( u_n \) is \( d_1 = 30 \), the following
values were obtained:

$$u_4 \equiv 14, \quad u_{19} \equiv 26 \pmod{31},$$

different from $\pm 1$.

In case 4, for $n = 10$ we have $u_n \equiv 1 \pmod{61}$. In the same manner,

$$u_{10} \equiv 11, \quad u_{25} \equiv 11 \pmod{31}.$$

It follows from above that in the field $K, K \subset Q(11 \cdot 71)$, of degree 5 over $Q$ an integral normal basis generated by a unit does not exist. ($11 \cdot 71$ is the least number $m$ such that $K \subset Q(m)$.)

ACKNOWLEDGMENT

We would like to thank the referee for simplifying the proof of Theorem 1.

BIBLIOGRAPHY


SLOVAK ACADEMY OF SCIENCES, INSTITUTE OF MATHEMATICS, ŠTEFÁNIKOVA 49, 814 73 BRATISLAVA, CZECHOSLOVAKIA