MATHEMATICS OF COMPUTATION
VOLUME 56, NUMBER 194
APRIL 1991, PAGES 809-815

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 $K \subset Q(m)$, where $Q(m)$ is the cyclotomic field of mth 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 ± 1. We will determine a necessary condition which a positive integer m has to fulfill under the suppositions that $K \subset Q(m)$, and in the field K there exists a unit ε such that

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

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 computational and based on the isomorphism between a subgroup $E \subseteq Q(\omega)$, where $\omega = \sqrt[l]{1}$,

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

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 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 $K \subset Q(m)$. Since m is squarefree, there exist distinct primes $p_1, p_2, \dots, p_s$ such that

$$m = p_1 \cdot p_2 \cdots p_s. \tag{1}$$

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

$$l^l \equiv 1 \pmod{p_i} \quad \textit{for all } i = 1, 2, \dots, s, \tag{2}$$

or

$$l^l \equiv -1 \pmod{p_i} \quad \textit{for all } i = 1, 2, \dots, s, \tag{3}$$

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/Q for all $i = 1, 2, \dots, s$. So, $\varepsilon \equiv a \pmod{\wp_i}$ for some rational integer a, where $\wp_i$ is the prime above p_i in K. Therefore, $\pm 1 = \mathrm{Tr}_{K/Q}(\varepsilon) \equiv la \pmod{p_i}$ and $\pm 1 = N_{K/Q}(\varepsilon) \equiv a^l \pmod{p_i}$. It follows that

$$\mathrm{Tr}_{K/Q}(\varepsilon)^l \equiv l^l a^l \equiv N_{K/Q}(\varepsilon) l^l \pmod{p_i}$$

for all $i = 1, 2, \dots, s$. Therefore, either $l^l \equiv +1 \pmod{p_i}$ for all i, or $l^l \equiv -1 \pmod{p_i}$ for all i. □

Our aim is to find all fields of given prime degree l over 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 Q, then $\mathrm{Tr}_{K/Q}(\varepsilon) = \pm 1$. 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

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

We need some further notation. For $i \in \{1, 2, \dots, s\}$, let $m_i = \frac{m}{p_i}$ and define the projection

$$\mathrm{pr}_i\colon G \to (Z/m_i Z)^*,$$

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

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

Proof. (a) First we show that if $x \in K \cap Q(m_i)$, 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 $\mathrm{pr}_i(\psi') = \psi$. Thus, $\psi(x) = \mathrm{pr}_i(\psi')(x) = x$.

(b) Conversely, let $x \in L$. We have to prove that $x \in K \cap Q(m_i)$. Since $L \subset Q(m_i)$, it is sufficient to show that $x \in K$. Let $\psi' \in G$. Then $\psi'(x) = \mathrm{pr}_i(\psi')(x) = x$. 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 $\mathrm{pr}_s : G \to (Z/m_sZ)^*$ is surjective by Corollary 1. Hence,

$$|(Z/m_sZ)^*| \mid |G|.$$

It follows that

$$\prod_{i=1}^{s-1}(p_i - 1) \mid \frac{\prod_{i=1}^{s}(p_i-1)}{l},$$

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 $K \subset Q(m)$ 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,

$$5^5 \equiv 1 \pmod{p} \quad \text{or} \quad 5^5 \equiv -1 \pmod{p}.$$

We obtained the following four values of m:

$$m = 11, \qquad m = 71, \qquad m = 521, \qquad m = 11 \cdot 71.$$

Let ξ denote the primitive mth 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 ξ^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* $a \in (Z/mZ)^* - G$,

$$\alpha_1 = \sum_{x\in G} \xi^x, \ \alpha_2 = \sum_{x\in G} \xi^{ax}, \ \ldots, \ \alpha_l = \sum_{x\in G} \xi^{a^{l-1}x} \tag{4}$$

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 $\{N(\beta_1)\}$ for all integral normal bases $(\beta_1, \beta_2, \ldots, \beta_l) = (\alpha_1, \alpha_2, \ldots, \alpha_l)\cdot A$, $A \in C_l$, 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 $\omega = \sqrt[l]{1}$. 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 $\gamma \equiv -\operatorname{Tr}_{Q(l)/Q}(\gamma) \pmod{1-\omega}$, 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 Φ, from E into a set of circulant matrices of rank l: for $\gamma \in E$, let

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

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

Lemma 2. *The mapping Φ is an isomorphism of groups E and C_l.*

Proof. Since the number c is determined uniquely, the mapping Φ is correctly defined. Φ 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,

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

implies that Φ is into the group C_l. Directly from the definition of Φ, it follows that Φ 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

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

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

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

Let $p \equiv 1 \pmod{l}$. Let $Z(\omega)$ be the ring of integers of the field $Q(l)$. Let ε 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:

$$\begin{aligned}\varepsilon^p &= (b_1\omega + b_2\omega^2 + \cdots + b_{l-1}\omega^{l-1})^p \\ &\equiv b_1^p\omega^p + b_2^p\omega^{2p} + \cdots + b_{l-1}^p\omega^{p(l-1)} \equiv \varepsilon \pmod{p}.\end{aligned}$$

Denote by d the least positive integer such that $\varepsilon^d \equiv 1 \pmod{p}$. Hence, $d \mid (p-1)$. The integer d can be determined exactly.

Lemma 3. *Let $\varepsilon = b_1\omega + b_2\omega^2 + \cdots + b_{l-1}\omega^{l-1}$ be a unit of the ring $Z(\omega)$ and $f(x) = b_1x + b_2x^2 + \cdots + b_{l-1}x^{l-1}$. Let g be a primitive root modulo p and $g_1 = g^{(p-1)/l}$. 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 $\wp_k$ in $Z(\omega)$ such that $\wp_k \mid p$ and $\omega \equiv g_1^k \pmod{\wp_k}$. Therefore,

$$\varepsilon = f(\omega) \equiv f(g_1^k) \pmod{\wp_k}.$$

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

$$1 \equiv f(g_1^k)^d \pmod{p} \tag{5}$$

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 $\varepsilon^{d^*} \equiv 1 \pmod{\wp_k}$ for all $k = 1, 2, \ldots, l-1$, we have that $\varepsilon^{d^*} - 1$ is divisible by $p = \prod_{k=1}^{l-1} \wp_k$. Therefore, $\varepsilon^{d^*} \equiv 1 \pmod{p}$ 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 $A \in C_l$, we have

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

As was shown above, when the set

$$\{N(\beta_1); (\beta_1, \beta_2, \ldots, \beta_l) = (\alpha_1, \alpha_2, \ldots, \alpha_l) \cdot A,\ A \in C_l\}$$

is investigated modulo p, it is sufficient to investigate a finite set of norms $\{N(\beta_1); (\beta_1, \ldots, \beta_l) = (\alpha_1, \ldots, \alpha_l) \cdot A\}$, $A = A_0^{n_0} \cdot A_1^{n_1} \cdots A_t^{n_t}$, $n_0 \leq 2l$, $n_1 \leq d_1, \ldots, n_t \leq d_t$, 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) $m = 11$, (b) $m = 71$, (c) $m = 521$, (d) $m = 11 \cdot 71$.

(a) $m = 11$. The element α 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 α.

(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 α.

(c) $m = 521$. In this case, the element α 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 $A_1 = \Phi(\eta_1) = \mathrm{Circ}_5(1, 0, 0, 1, -1)$. Define the sequence of norms

$$u_n = N_{K/Q}(\beta_1),$$

where $(\beta_1, \dots, \beta_5) = (\alpha_1, \dots, \alpha_5) \cdot A_1^n$, $n \in Z$.

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:

$$(u_1, \dots, u_{10}) = (9, 4, 8, 4, 7, 10, 2, 9, 4, 7).$$

Hence, the numbers $N_{K/Q}(\beta_1)$, where $(\beta_1, \dots, \beta_5) = (\alpha_1, \dots, \alpha_5) \cdot A$, $A \in C_l$, assume the values $\pm 9, \pm 4, \dots, \pm 7$. (Since $A = A_0^a \cdot A_1^n$, $n \in Z$, $A_0 = \mathrm{Circ}_5(0, -1, 0, 0, 0) = \Phi(-\omega)$.)

It follows from above that β_1, for $(\beta_1, \dots, \beta_5) = (\alpha_1, \dots, \alpha_5) \cdot A^a \cdot A_1^n$, can be a unit if $n \equiv 6 \pmod{10}$.

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 $u_1 \equiv 50$, $u_6 \equiv 54$, $u_{11} \equiv 26 \pmod{61}$, which are all different from $\pm 1 \pmod{61}$.

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 $(Z/11 \cdot 71Z)^*$ 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:

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

In case 1, for $n = 4$ we have $u_n \equiv -1 \pmod{61}$. 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 ± 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

1. H.-W. Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern*, J. Reine Angew. Math. **209** (1962), 54–71.
2. P. J. Davis, *Circulant matrices*, Wiley, New York, 1979.

Slovak Academy of Sciences, Institute of Mathematics, Štefánikova 49, 814 73 Bratislava, Czechoslovakia