Juraj Kostra

A note on normal and power bases

Mathematica Slovaca, Vol. 37 (1987), No. 4, 357--362

Persistent URL: http://dml.cz/dmlcz/128828

Math. Slovaca 37, 1987, No. 4, 357—362

A NOTE ON NORMAL AND POWER BASES

JURAJ KOSTRA

Let K/Q be a normal field of algebraic numbers of prime degree p over the field of rational numbers Q with the Galois group

$$G(K/Q) = \{1, g, g^2, \ldots, g^{p-1}\}.$$

In this paper we show: Let $\{\varepsilon, \varepsilon^g, \ldots, \varepsilon^{g^{p-1}}\}$ be an integral normal basis of K over Q. Let l be a prime and Q_l be the field of l-adic numbers. If ε is a unit of the field K and if $Q_l(\varepsilon)/Q_l$ is a non-trivial extension, then

$$\{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}\}$$

is an integral basis of the field $Q_l(\varepsilon)$ over Q_l. By an example we show that an analogous statement does not hold for the field extension K/Q.

We shall need the following proposition.

Proposition 1. [3, p. 243] Let K/Q and $G = G(K/Q)$ be as in the introduction. *Let l be a prime and $\mathcal{L}$ any prime ideal lying over (l) in the field K. Then the corresponding extension $K_{\mathcal{L}}/Q_l$ of the l-adic field is normal and there is a canonical embedding of its Galois group $G(K_{\mathcal{L}}/Q_l)$ into G. The index of $G(K_{\mathcal{L}}/Q_l)$ in G equals the number of prime ideals lying above (l) in K.* (This makes sense provided we identify $G(K_{\mathcal{L}}/Q_l)$ with its image in G).

Lemma 1. *Let K/Q, $G = G(K/Q)$ and $\{\varepsilon, \varepsilon^g, \ldots, \varepsilon^{g^{p-1}}\}$ be as in the introduction. Let l be a prime such that $Q_l(\varepsilon)$ is a non-trivial extension of the field of l-adic numbers Q_l, then $\{\varepsilon, \varepsilon^g, \ldots, \varepsilon^{g^{p-1}}\}$ is an integral normal basis of $Q_l(\varepsilon)$ over Q_l. Moreover, there is a unique prime ideal $\mathcal{L}$ lying over (l) in K.*

Proof. According to Proposition 1, for all prime l the extension $K_{\mathcal{L}}/Q_l$, where $\mathcal{L}$ is a prime ideal of K lying over (l), is normal and there is a canonical embedding of $G(K_{\mathcal{L}}/Q_l)$ into G such that the index of $G(K_{\mathcal{L}}/Q_l)$ in G is equal to the number of prime ideals lying over (l) in K. Using the fact that the extension $Q_l(\varepsilon)/Q_l$ is non-trivial and that $[K:Q] = p$, where p is a prime, we have that $K_{\mathcal{L}} = Q_l(\varepsilon)$ and $[K_{\mathcal{L}}:Q_l] = p$. From the above it follows that there is a unique prime ideal $\mathcal{L}$ lying over (l) in K. Clearly $\{1, \varepsilon, \ldots, \varepsilon^{p-1}\}$ is a basis of the field $Q_l(\varepsilon)$ over Q_l. The elements of this basis can be obtained as linear combinations with integral rational coefficiens of the elements $\varepsilon, \varepsilon^g, \ldots, \varepsilon^{g^{p-1}}$. Hence $\{\varepsilon, \varepsilon^g, \ldots,$

..., $\varepsilon^{g^{p-1}}\}$ is a normal basis of the field $Q_l(\varepsilon)$ over Q_l. The field $K_{\mathscr{L}} = Q_l(\varepsilon)$ is the completion of K with respect to the valuation belonging to the unique prime ideal $\mathscr{L}$ lying over (l) in K. Each element x of the ring of integers $Z_{K_{\mathscr{L}}}$ of the field $K_{\mathscr{L}}$ is the limit of a sequence $\{x_n\}$ of integers of the field K. Hence

$$x = \lim_{n\to\infty} x_n = \lim_{n\to\infty} (a_{1,n}\varepsilon + \dots + a_{p,n}\varepsilon^{g^{p-1}})$$

where $a_{i,n}$, $1 \leqslant i \leqslant p$ are integral rational numbers. According to [4, p. 555] the sequence $\{x_n\}$ is fundamental in K if and only if for all i, $1 \leqslant i \leqslant p$, the sequences $\{a_{i,n}\}$ are fundamental in Q_l and therefore

$$x = a_1\varepsilon + a_2\varepsilon^g + \dots + a_p\varepsilon^{g^{p-1}}$$

where $a_i \in Z_l$, where Z_l is the ring of integral l-adic numbers. From this we get that $\{\varepsilon, \varepsilon^g, \dots, \varepsilon^{g^{p-1}}\}$ is an integral normal basis of the field $Q_l(\varepsilon)$ over Q_l.

Theorem 1. *Let K/Q, $G = G(K/Q)$ and $\{\varepsilon, \varepsilon^g, \dots, \varepsilon^{g^{p-1}}\}$ be as in the introduction. Let ε be a unit of the field K. Then for each prime l for which $Q_l(\varepsilon)/Q_l$ is a non-trivial extension, the power basis $\{1, \varepsilon, \dots, \varepsilon^{p-1}\}$ is an integral basis of the field $Q_l(\varepsilon)$ over Q_l.*

To prove Theorem 1 we shall need Proposition 2 [2, p. 445]. First we recall some concepts.

Under an inessential divisor $m(\varepsilon)$ of the discriminant $d(\varepsilon)$ of the basis $\{1, \varepsilon, \dots, \varepsilon^{p-1}\}$ we shall understand the fraction $d(\varepsilon)/d(K)$, where $d(K)$ is the discriminant of the field K. By $m_l(\varepsilon)$ we shall denote l^t, where t is the maximal integer such that $l^t | m(\varepsilon)$.

In the theorem we suppose that the extension $Q_l(\varepsilon)/Q_l$ is non-trivial. By Lemma 1, there is a unique ideal $\mathscr{L}$ lying over (l) in K. Hence

$$e \cdot f = p$$

where e is the index of ramification of (l) in K and $f = [R_{\mathscr{L}} : R_l]$ where $R_{\mathscr{L}}$, resp. R_l, are the fields of residue classes of the local field $Q_l(\varepsilon)$, resp. Q_l. Because p is prime, there are two cases:

$$(A) \qquad (l) = \mathscr{L}^p$$
$$(B) \qquad (l) = \mathscr{L}.$$

By Z_l we denote a ring of integral l-adic numbers and by $\Pi_{\mathscr{L}}$ a prime element belonging to $\mathscr{L}$ in K.

The following proposition is a modification of Hasse's theorem [2, p. 445] for our situation.

Proposition 2. In the case (A) for an integral element β from K the relation $m_l(\beta) = 1$ holds if and only if

$$\beta \equiv x + \Pi_{\mathscr{L}} \quad mod\ \mathscr{L}^2$$

where $x \in Z_l$, $x \not\equiv 0\ mod\ \mathscr{L}$.

In the case (B) for an integral element β from K the relation $m_l(\beta) = 1$ holds if and only if β is a representant of a primitive element from the residue class extension $R_{\mathscr{L}}/R_l$.

Proof of Theorem 1. To prove Theorem 1 means to show $m_l(\varepsilon) = 1$ for all prime l such that $Q_l(\varepsilon)/Q_l$ is a non-trivial extension.

(A) Let $(l) = \mathscr{L}^p$. The proof is given by contradiction. Suppose, that $m_l(\varepsilon) \neq 1$. By Proposition 2 it does not hold that

$$E \equiv x + \Pi_{\mathscr{L}} \quad mod\ \mathscr{L}^2$$

where $x \in Z_l$, $x \not\equiv 0\ mod\ \mathscr{L}$. Since ε is a unit, $\varepsilon \not\equiv 0\ mod\ \mathscr{L}$ and $R_{\mathscr{L}} = R_l$, we can suppose that for $x \in Z_l$

$$\varepsilon \equiv x \quad mod\ \mathscr{L}$$

implies

$$\varepsilon \equiv x \quad mod\ \mathscr{L}^2.$$

By Lemma 1 we have

$$\Pi_{\mathscr{L}} = a_1\varepsilon + a_2\varepsilon^g + \ldots + a_p\varepsilon^{g^{p-1}},$$

where for $1 \leqslant i \leqslant p$, $a_i \in Z_l$. Hence

$$\Pi_{\mathscr{L}} \equiv \sum_{i=1}^{p} a_i x \quad mod\ \mathscr{L}^2$$

From $\Pi_{\mathscr{L}} \equiv 0\ mod\ \mathscr{L}$ we get

$$\sum_{i=1}^{p} a_i x \quad mod\ \mathscr{L}.$$

Both a_i and x belong to Z_l and $(l) = \mathscr{L}^p$, hence the last congruence holds also $mod\ \mathscr{L}^2$. From this we get $\Pi_{\mathscr{L}} \equiv 0\ mod\ \mathscr{L}^2$, which contradicts the fact that $\Pi_{\mathscr{L}}$ is a prime element belonging to $\mathscr{L}$. Therefore in the case (A) we have $m_l(\varepsilon) = 1$.

(B) Let $(l) = \mathscr{L}$. By Proposition 2 it is sufficient to prove that ε is a representative of a primitive element of the extension $R_{\mathscr{L}}/R_l$. That means that $\bar{\varepsilon} \notin R_l$ where $\bar{\varepsilon}$ is the residue class belonging to ε. Clearly $\bar{\varepsilon} \in R_l$ if and only if $\bar{\varepsilon}^{g^i} \in R_l$ for all i. Let $\bar{\alpha}$ be a primitive element of extension $R_{\mathscr{L}}/R_l$. The element α is its representative in the ring $Z_{K_{\mathscr{L}}}$ of integral numbers of $K_{\mathscr{L}}$. Then due to Lemma 1 there holds

$$\alpha = a_1\varepsilon + a_2\varepsilon^g + \ldots + a_p\varepsilon^{g^{p-1}}$$

where $a_i \in Z_l$ (for $Q \leqslant i \leqslant p$), hence

$$\bar{\alpha} = \bar{a}_1\bar{\varepsilon} + \bar{a}_2\bar{\varepsilon}^g + \ldots + \bar{a}_p\bar{\varepsilon}^{g^{p-1}},$$

where $\bar{a}_i \in R_l$ for $1 \leqslant i \leqslant p$, hence $\bar{\varepsilon} \notin R_l$. We have $m_l(\varepsilon) = 1$. Theorem 1 is proved.

The following example shows that if the assumptions of Theorem 1 are satisfied, the power basis $\{1, \varepsilon, \ldots, \varepsilon^{p-1}\}$ need not be the integral basis of the field K over Q.

Example. Let $L = Q(\xi)$ where ξ is a primitive root of degree 653 of 1. Since 653 is a prime we get that $G = G(L/Q)$ is a cyclic group and $[L:Q] = 652$. Let G_0 be a subgroup of G generated by the automorphism

$$g : \xi \mapsto \xi^{149}.$$

Since

$$149^4 \equiv 1 \quad mod\, 653 \tag{1}$$

and 4 is the least natural number m for which

$$149^m \equiv 1 \quad mod\, 653$$

holds, we get that the order of the group G_0 is 4.

Now we define a field K and an integral normal basis of the field K over Q, which satisfied the assumptions of Theorem 1. Let K be the subfield of L invariant with respect to G_0. Let $H = G(K/Q)$. We have the following situation:

$$Q \subset K \subset L, \quad G = G(L/Q), \quad G_0 = G(L/K), \quad H = G(K/Q)$$

where $H \simeq G/G_0$, $[L:Q] = 652$, $[L:K] = 4$, $[K:Q] = [L:Q]/[L:K] = 163$. Note that 163 is a prime.

Let h be a generating automorphism of the group H. Put

$$\varepsilon = \xi + \xi^{149} + \xi^{652} + \xi^{504}.$$

We first show that $\varepsilon, \varepsilon^h, \ldots, \varepsilon^{h^{162}}$ is an integral normal basis of the field K over Q. For simplicity let us denote

$$\varepsilon_i = \varepsilon^{h^{i-1}}.$$

There holds

$$\varepsilon^g = (\xi + \xi^g + \xi^{g^2} + \xi^{g^3})^g = \xi^g + \xi^{g^2} + \xi^{g^3} + \xi = \varepsilon,$$

where g is the generating automorphism of the group G_0. Hence $\varepsilon \in K$.

The linear independence of $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{163}$ over Q follows from the linear independence of $\xi, \xi^2, \ldots, \xi^{652}$ over Q.

Now we shall compute the discriminant of the basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{163}$.

$$d(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{163}) = det \begin{vmatrix} Tr_{K/Q}(\varepsilon_1^2) & Tr_{K/Q}(\varepsilon_1\varepsilon_2) \ldots & Tr_{K/Q}(\varepsilon_1\varepsilon_{163}) \\ Tr_{K/Q}(\varepsilon_2\varepsilon_1) \ldots & & Tr_{K/Q}(\varepsilon_2\varepsilon_{163}) \\ \vdots & & \\ Tr_{K/Q}(\varepsilon_{163}\varepsilon_1) \ldots & & Tr_{K/Q}(\varepsilon_{163}^2) \end{vmatrix}.$$

Using the relation $Tr_{K/Q}(x) = (1/[L:K])\, Tr_{L/Q}(x)$ it can be easily proved that

$$Tr_{K/Q}(\varepsilon_i^2) = 649 \qquad \text{for } 1 \leqslant i \leqslant 163$$

and

$$Tr_{K/Q}(\varepsilon_i \varepsilon_j) = -4 \qquad \text{for } i \neq j,\ 1 \leqslant i, j \leqslant 163.$$

Hence $d(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{163}) = det\ circ_{163}(649, -4, \ldots, -4) = 653^{162}$. According to [3, Corollary 3, p. 262] we get that $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{163}$ is an integral basis and hence an integral normal basis of the field K over Q.

We next show that ε_i are units. Let β be a primitive root of 1 of a prime degree p and let $f_p(x) = x^{P-1} + x^{P-2} + \ldots + 1$ be the corresponding caclotomic polynomial. Then $N_{Q(\beta)/Q}(1 + \beta) = f(-1) = 1$. Hence, we have that

$$\varepsilon = \xi + \xi^{149} + \xi^{652} + \xi^{504} = \xi(1 + \xi^{148})(1 + \xi^{503})$$

where all factors on the right hand are units of the field L and therefore $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{163}$ are units of the field K.

We showed that the assumptions of Theorem 1 are fulfilled. Finally we show that $1, \varepsilon, \ldots, \varepsilon^{162}$ is not an integral basis of the field K over Q.

From (1), according to [1, Lemma 1.4, p. 139], we get that the polynomial $f(x) = (x - \varepsilon_1)(x - \varepsilon_2) \ldots (x - \varepsilon_{163})$ is completely reducible *mod* 149 and hence it has a multiple root *mod* 149. That means that the discriminant

$$d(f(x)) = d(1, \varepsilon, \ldots, \varepsilon^{162}) \equiv 0 \quad mod\ 149.$$

This proves that $1, \varepsilon, \ldots, \varepsilon^{162}$ is not an integral basis of the field K over Q.

REFERENCES

[1] CASSELS, J. W. S., FRÖHLICH. A.: Algebraic Number Theory. Russian edition, Izdateľstvo "MIR", Moscow 1969.

[2] HASSE, H.: Number Theory, Akademie-Verlag-Berlin 1979.

[3] NARKIEWICZ, W.: Elementary and Analytic Theory of Algebraic Numbers, PWN, Warszawa 1974.

[4] VAN DER WAERDEN, B. L.: Algebra. Russian edition, Izdateľstvo "Nauka", Moscow 1976.

Received November 28, 1984

Matematický ústav SAV
Obrancov mieru 49
814 73 Bratislava

ЗАМЕТКА О НОРМАЛЬНЫХ И СТЕПЕННЫХ БАЗИСАХ

Juraj Kostra

Резюме

В статье доказано, что если K-нормальное поле алгебраических чисел, имеющее степень p, где p-простое число, $\varepsilon = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ — целый нормальный базис поля K над полем рациональных чисел Q и ε является единицей поля K, то степенный базис $1, \varepsilon, \ldots, \varepsilon^{p-1}$ является целым базисом поля $Q_l(\varepsilon)$ над полем l-адичных чисел Q_l, для всех l, для которых это расширение нетривиально.