Juraj Kostra

On integral normal bases over intermediary fields

Czechoslovak Mathematical Journal, Vol. 39 (1989), No. 4, 622–626

Persistent URL: http://dml.cz/dmlcz/102337

Czechoslovak Mathematical Journal, 39 (114) 1989, Praha

ON INTEGRAL NORMAL BASES OVER INTERMEDIARY FIELDS

JURAJ KOSTRA, Bratislava

(Received April 8, 1987)

Let L be a Galois extension of degree n over an algebraic number field K. Let $g_1, g_2, \ldots, g_n$ denote the elements of the Galois group $G(L/K)$. It is known that L may possess a normal basis for the integers Z_L over Z_K consisting of the conjugates

$$\alpha^{g_1}, \alpha^{g_2}, \ldots, \alpha^{g_n}$$

for an integer α. Such a basis is called an *integral normal basis* of L over K.

Let M, L, K be algebraic number fields such that $M \supset L \supset K$ and all the extensions are Galois. In the present paper we shall show that if there are integral normal bases for M/L and M/K, then the existence of an element α generating the integral normal basis for both M/K and M/L is equivalent to the existence of an integral normal basis for L/K generated by a unit of Z_K. It will be shown that there are exactly two cubic fields over the rational number field Q for which there exists an integral normal basis generated by a unit.

Proposition 1. *Let M, L, K be algebraic number fields such that $M \supset L \supset K$ and all the extensions are Galois. If an element α generate an integral normal basis for M/K, then $\mathrm{Tr}_{M/L}(\alpha)$ generates an integral normal basis for L/K.*

Proof. $x \in Z_L$. Then

$$x^h = x \tag{1}$$

for $h \in G(M/L)$ and

$$x = \sum_{g \in G(M/K)} a_g \alpha^g ,$$

where $a_g \in Z_K$. α generates an integral normal basis for M/K. Consequently, by virtue of (1),

$$\alpha^{g.h} = \alpha^{g'} \quad \text{for} \quad h \in G(M/L)$$

implies

$$a_g = a_{g'} .$$

Therefore

$$x = \sum_{f \in G(L/K)} a_f (\mathrm{Tr}_{M/L}(\alpha))^f$$

where $a_f \in Z_K$, hence $\mathrm{Tr}_{M/L}(\alpha)$ generates an integral normal basis for L/K.

Proposition 2. *Let M, L, K be algebraic number fields such that $M \supset L \supset K$ and let α and β generate an integral normal basis for M/L and L/K, respectively. Then $\alpha\beta$ generates an integral normal basis for M/K.*

Proof. Let $x \in Z_M$. Then

$$x = \sum_{g \in G(M/L)} y_g \alpha^g ,$$

where $y_g \in Z_L$. Further

$$y_g = \sum_{h \in G(L/K)} a_{gh} \beta^h ,$$

where $a_{gh} \in Z_K$ and so

$$x = \sum_{g,h} a_{gh} \alpha^g \beta^h ,$$

where for

$$f \in G(M/K)$$

we evidently have

$$(\alpha^g \beta^h)^f = \alpha^{g'} \beta^{h'} .$$

Hence $\alpha\beta$ generates an integral normal basis for M/K.

Proposition 3. *If α generates an integral normal basis for L/K, then $\mathrm{Tr}_{L/K}(\alpha)$ is a unit of Z_K.*

Proof. We have

$$1 = \sum_{g \in G(L/K)} \frac{1}{\mathrm{Tr}_{L/K}(\alpha)} \alpha^g$$

and so

$$\frac{1}{\mathrm{Tr}_{L/K}(\alpha)} \in Z_K .$$

Theorem 1. *Let M, L, K be algebraic number fields such that $M \supset L \supset K$ and all the extensions are Galois. Let integral normal bases exist for M/K and M/L. Then there exists an element α which generates an integral normal basis for both M/K and M/L if and only if there exists an integral normal basis for L/K generated by a unit of Z_L.*

Proof. Let α generate integral normal bases for M/L and M/K. By Proposition 1 and Proposition 3 the element $\mathrm{Tr}_{M/L}(\alpha)$ is a unit of Z_L and generates an integral normal basis for L/K.

Let β generate an integral normal basis for M/L. Let γ be a unit of Z_L and let γ generate an integral normal basis for L/K. According to Proposition 2, the element $\beta\gamma$ generates an integral normal basis for M/K. Due to Proposition 3 the element $\mathrm{Tr}_{M/L}(\beta)$ is a unit of Z_L and so the element

$$\alpha = \frac{1}{\mathrm{Tr}_{L/K}(\beta)} \beta\gamma$$

generates an integral normal basis for M/L. Clearly

$$\frac{1}{\mathrm{Tr}_{L/K}(\beta)}\beta$$

generates an integral normal basis for M/L. Using Proposition 2 we obtain that the element α generates an integral normal basis for M/K.

In what follows, K_m will denote a cyclotomic field generated by an m-th primitive root of unity.

Example. Let $K_7 \supset K \supset Q$, $[K : Q] = 3$. Let ζ be a primitive 7-th root of unity. The element ζ generates an integral normal basis for K_7/Q. We shall show that ζ generates an integral normal basis for K_7/K, too. By Proposition 1 the element

$$\alpha = \mathrm{Tr}_{K_7/K}(\zeta) = \zeta + \zeta^6$$

generates an integral normal basis

$$\{\alpha^h \mid h \in G(K/Q)\} = \{\zeta + \zeta^6,\ \zeta^2 + \zeta^5,\ \zeta^3 + \zeta^4\}$$

for K/Q. To show that

$$\{\zeta^g \mid g \in G(K_7/K) = \{\zeta, \zeta^6\}$$

is an integral normal basis, it is sufficient to show that

$$\zeta^k = a\zeta + b\zeta^6\,,$$

where $a, b \in Z_K$ and $k = 1, 2, \ldots, 6$. But we have

$$\begin{aligned}
\zeta &= \zeta\,,\\
\zeta^2 &= -(\zeta^2 + \zeta^5)\,\zeta - [(\zeta + \zeta^6) + (\zeta^2 + \zeta^5)]\,\zeta^6\,,\\
\zeta^3 &= -(\zeta + \zeta^6)\,[2(\zeta^2 + \zeta^5) + (\zeta + \zeta^6)]\,\zeta - \zeta^6\,,\\
\zeta^4 &= -\zeta(\zeta + \zeta^6)\,[2(\zeta^2 + \zeta^5) + (\zeta + \zeta^6)]\,\zeta^6\,,\\
\zeta^5 &= -[(\zeta + \zeta^6) + (\zeta^2 + \zeta^5)]\,\zeta - (\zeta^2 + \zeta^5)\,\zeta^6\,,\\
\zeta^6 &= \zeta^6\,.
\end{aligned}$$

By the above example and due to Theorem 1 the element $\mathrm{Tr}_{K_7/K}(\zeta)$ is a unit of Z_K. This is only a special case of the following Proposition.

Proposition 4. *Let p and $l = 2kp + 1$ be primes. If $k = 1$ or $k = 2$, $K_1 \supset K \supset Q$, $[K : Q] = p$ and ζ is an l-th primitive root of unity, then* $\mathrm{Tr}_{K_1/K}(\zeta)$ *is a unit of* Z_K.

Proof. First we prove that $1 + \zeta^t$ is a unit for $t \not\equiv 0 \bmod l$. ζ is a root of

$$f_1(x) = x^{l-1} + x^{l-2} + \ldots + x + 1$$

and so

$$N_{K_1/Q}(1 + \zeta^t) = f_1(-1) = 1$$

for $t \not\equiv 0 \bmod l$.

Now we show that $\mathrm{Tr}_{K_1/K}(\zeta)$ can be expressed as a product of units of Z_1.

In the case $k = 1$ we have

$$\mathrm{Tr}_{K_1/K}(\zeta) = \zeta + \zeta^{-1} = \zeta(1 + \zeta^{-2}) .$$

In the case $k = 2$ we get

$$\mathrm{Tr}_{K_1/K}(\zeta) = \zeta + \zeta^t + \zeta^{-1} + \zeta^{-t} = \zeta(1 + \zeta^{t-1})(1 + \zeta^{-t-1}) .$$

We have shown that in the cases $k = 1, 2$, $\mathrm{Tr}_{K_1/K}(\zeta)$ is a unit of Z_K.

With respect to Theorem 1 it would be interesting to know for which algebraic number fields an integral normal basis generated by a unit exists. We shall show that there are only two cubic fields over Q for which a unit generates an integral normal basis. First we prove the following lemma.

Lemma. *Let K be a cubic field over Q and let an integral normal basis for K/Q exist. Let m be the minimal natural number such that $K \subset K_m$. Then for p prime $p \mid m$ implies that $p \equiv 1 \bmod 3$.*

Proof. The field K has an integral normal basis over Q and so by [3], $K \subset K_m$ with a square-free m. From $[K : Q] = 3$ it follows that there is a prime q, $q \mid m$ such that $q \equiv 1 \bmod 3$. Let p be a prime such that $p \mid m$ and $p \not\equiv 1 \bmod 3$. Then

$$K_m = K_{m_1} \,.\, K_{m_2}$$

where for l prime $l \mid m_1$ implies $l \not\equiv 1 \bmod 3$ while $l \mid m_2$ implies $l \equiv 1 \bmod 3$. Clearly

$$\varphi(m_1) = [K_{m_1} : Q] \not\equiv 0 \bmod 3 .$$

Since m is minimal such that $K \subset K_m$, we have

$$K \cap K_{m_1} = Q$$

and

$$K \cap K_{m_2} = Q .$$

Further,

$$[K \,.\, K_{m_2} : Q] = 3\, \varphi(m_2) .$$

Obviously

$$(K \,.\, K_{m_2})\, K_{m_1} = K_m$$

and hence

$$[(K \,.\, K_{m_2} \cap K_{m_1}) : Q] = 3 ,$$

which contradicts $\varphi(m_1) \not\equiv 0 \bmod 3$.

Theorem 2. *There are only two cubic fields over Q for which a unit generates an integral normal basis. They are determined by the polynomials $f_1(x) = x^3 + x^2 - 2x - 1$, $f_2(x) = x^3 + x^2 - 4x + 1$, respectively.*

Proof. Let K be a cubic field over Q with an integral normal basis and let m be the minimal natural number such that $K \subset K_m$. By Lemma if p is prime and $p \mid m$, then $p \equiv 1 \bmod 3$. Due to [2], an element α,

$$\alpha = \mathrm{Tr}_{K_m/K}(\zeta) ,$$

where ζ is the m-th primitive root of unity, generates an integral normal basis for K/Q and the minimal polynomial of α is

$$f_\alpha(x) = x^3 + x^2 - \left(\frac{m-1}{3}\right)x - \left(\frac{mc + 3m - 1}{27}\right),$$

where $4m = c^2 + 27d^2$ and $c \equiv 1 \bmod 3$.

It follows from the above that α may be a unit only for $m < 27$. Moreover, for p prime $p \mid m$ implies $p \equiv 1 \bmod 3$. Therefore α may be a unit only for $m = 7, 13, 19$ and by the table in [1] α is a unit for $m = 7, 13$ (this follows also from Proposition 4) and α is not a unit for $m = 19$.

By [4], in a cubic field with an integral normal basis over Q, the integral normal basis is unique. Hence there are only two cubic fields over Q for which a unit generates an integral normal basis. They are determined by the polynomials $f_1(x) = x^3 + x^2 - 2x - 1$ and $f_2(x) = x^3 + x^2 - 4x + 1$, respectively.

Corollary. *Let $L \supset K \supset Q$ and $[K : Q] = 3$. Let an element α generate integral normal bases for L/K and L/Q. Then either $7 \mid D(L)$ or $13 \mid D(L)$.*

Proof. According to Theorem 1, K/Q has an integral normal basis generated by a unit. By Theorem 2, the field K is determined by the polynomial $f_1(x)$ or by the polynomial $f_2(x)$ and either $D(K) = 7^2$ or $D(K) = 13^2$. Therefore $7 \mid D(L)$ or $13 \mid D(L)$.

Remark. There are only two quadratic fields over Q for which a unit generates an integral normal basis. This case is trivial and they are determined by the polynomials $x^2 + x + 1$ and $x^2 + x - 1$, respectively.

References

[1] *Dummit, D. S.* and *Kisilevsky, H.:* Indices in cyclic cubic fields. Number Theory and Algebra. Edited by Hans Zassenhaus. Academic press, New York–San Francisko–London, 1977.

[2] *Hasse, H.:* Arithmetische Bestimmungen von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern. Abd. Deutsch. Akad. Wiss. Berlin Kl. Math. Phys. Tech. 1948 (1950), nr. 2.

[3] *Leopoldt, H. W.:* Zur Arithmetik in abelschen Zahlkörpern. J. Reine Angew. Math. *209*, 1962.

[4] *Newman, M.* and *Taussky, O.:* On a Generalization of the Normal Basis in Abelian Algebraic Number Fields. Communications on Pure and Applied Mathematics. *9* (1956).

Author's address: 814 73 Bratislava, Obrancov mieru 49, Czechoslovakia (MÚ SAV).