UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
L—LI—1987

REMARK ON NORMAL AND POWER BASES (ABSTRACT)*

JURAJ KOSTRA

Theorem. Let K be a normal field of algebraic numbers of the prime degree p over the field of rational numbers Q. Let $\varepsilon = \varepsilon_1, \varepsilon_2, \dots, \varepsilon_p$ be an integral normal basis of the field K over Q, where ε_i are units of the field K. Then for each prime l, for which $K_l = Q_l(\varepsilon)$ is a nontrivial extension of the field of l-adic numbers Q_l, there holds that the power basis $l, \varepsilon, \dots, \varepsilon^{p-1}$ is an integral basis of the field K_l over Q_l.

By proving of this theorem, we show that if the assumptions of the theorem are satisfied then the conditions (a), (b) of the following proposition are satisfied.

Proposition. ([1], Hasse) For an integral element from K/Q the relation $m_l(\varepsilon) = 1$ holds if and only if for each prime ideal $\mathscr{L}$ lying over l in the field K the following two conditions are satisfied:

$$\text{(a)} \qquad \varepsilon \equiv \begin{cases} v_{\mathscr{L}} \bmod \mathscr{L} & \text{for } e_{\mathscr{L}} = 1 \\ v_{\mathscr{L}} + \pi_{\mathscr{L}} \bmod \mathscr{L}^2 & \text{for } e_{\mathscr{L}} > 1\,, \end{cases}$$

where $v_{\mathscr{L}}$ is a representative in the inertia field $T_{\mathscr{L}}$ of primitive element $w_{\mathscr{L}}$ from the residue class extension $R_{\mathscr{L}}/R_l$ for $K_{\mathscr{L}}/Q_l$ and $\pi_{\mathscr{L}}$ is a prime element belonging to $\mathscr{L}$ in K.

(b) these elements $w_{\mathscr{L}}$ in fields $R_{\mathscr{L}}$ are pairwise nonconjugate over R_l.

Where $T_{\mathscr{L}}/Q_l$, $R_{\mathscr{L}}$ respectively R_l is the field of residue classes of the $K_{\mathscr{L}}$ respectively Q_l and $m_l(\varepsilon)$ is inessential divisor of the discriminant $d(\varepsilon)$ with respect to l.

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

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

* Math. Slovaca, 4 (1987), 357—362.

be a subroup of G generated by the automorphism $g\colon \xi \mapsto \varepsilon^{149}$. Since

$$149^4 \equiv 1 \pmod{653},$$

where 4 is the least natural number for which this congruence holds, we get that the order of the group G_0 is 4. Let K be the subfield of L invariant with respect to G_0. The field K is an extension of Q of the degree $[K:Q] = 163$, where 163 is prime. Let $H = G(K/Q)$. Let h be a generating automorphism of the group H. Put

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

It can be shown that $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{163}$, where $\varepsilon_i = \varepsilon^{h^{i-1}}$, $1 \leq i \leq 163$, is an integral normal basis of the field K over Q formed from units of the field K and that the power basis $1, \varepsilon, \ldots, \varepsilon^{162}$ is not an integral basis of the field K over Q.

REFERENCE

1. Hasse, H.: Number Theory, Akademie—Verlag—Berlin 1979.

Author's address:
Juraj Kostra
Matematický ústav SAV
Obrancov mieru 49
886 25 Bratislava

Received: 9. 12. 1985

SÚHRN

POZNÁMKA O NORMÁLNYCH A MOCNINNÝCH BÁZACH

Juraj Kostra, Bratislava

Ak K je normálne pole algebraických čísel prvočíselného stupňa p nad poľom racionálnych čísel Q a $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_p$ je celá normálna báza poľa K nad Q, pričom ε_i sú jednotky poľa K, potom mocninná báza $1, \varepsilon_i, \ldots, \varepsilon_i^{p-1}$ je celá báza poľa $Q_1(\varepsilon_i)$ nad poľom l-adických čísel, pre všetky l, pre ktoré je toto rozšírenie netriviálne.

РЕЗЮМЕ

ЗАМЕТКА О НОРМАЛЬНЫХ И СТЕПЕННЫХ БАЗИСАХ

Юрай Костра, Братислава

Если K нормальное поле алгебраических чисел, имеющее степень p, где p-простое число и $\varepsilon = \varepsilon_1, \varepsilon_1, \ldots, \varepsilon_p$ — целей нормальный базис поля K над полем рациональных чисел Ъ 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.