LETTER TO THE EDITOR

1961

SovietRxiv

Abstract

Full Text

LETTER TO THE EDITOR

In the paper ([1]) B. Ethelbaum made an attempt to generalize the concept of G. F. Voronoi' s normal basis of a cubic field to an arbitrary algebraic field of degree n. His result, asserting the existence in every algebraic field of a normal basis $1, \omega_2, \dots, \omega_n$, for which the conditions

$$\omega_2\omega_i + f_i = \frac{D_{i+1}}{D_i}\omega_{i+1} \quad (i = 3, 4, \dots, n-1); \qquad \omega_2\omega_n + f_n = 0, \tag{1}$$

hold, where f_i and f_n are certain rational integers, is incorrect. Let us specify the notation used in paper ([1]). Denote the field into which $K(\rho)$ is transformed by $\overline{K}(\overline{\omega}_2)$ (in the paper, $K(\omega_2)$). Let the basis of this field be

$$1,\ \overline{\omega}_2,\ \overline{\omega}_3 = \frac{B_{3,1} + B_{3,2}\overline{\omega}_2 + \overline{\omega}_2^2}{D_3},$$

$$\dots,\ \overline{\omega}_i = \frac{B_{i,1} + B_{i,2}\overline{\omega}_2 + \dots + \overline{\omega}_2^{i-1}}{D_i}, \dots,\ \overline{\omega}_n = \frac{B_{n,1} + B_{n,2}\overline{\omega}_2 + \dots + \overline{\omega}_2^{n-1}}{D_n}$$

and let

$$x^n + \overline{f}_1 x^{n-1} + \dots + \overline{f}_n = 0$$

be the equation satisfied by $\overline{\omega}_2$. Form the products $\overline{\omega}_2\overline{\omega}_n,\ \overline{\omega}_2\overline{\omega}_i$:

$$\overline{\omega}_2\overline{\omega}_n = C_{n,1} + C_{n,2}\overline{\omega}_2 + C_{n,3}\overline{\omega}_3 + \dots + C_{n,n-1}\overline{\omega}_{n-1} + C_{n,n}\overline{\omega}_n, \tag{5'}$$

$$\overline{\omega}_2\overline{\omega}_i = C_{i,1} + C_{i,2}\overline{\omega}_2 + C_{i,3}\overline{\omega}_3 + \dots + C_{i,i}\overline{\omega}_i + \frac{D_{i+1}}{D_i}\overline{\omega}_{i+1}. \tag{6'}$$

These are the same equalities as (5), (6) in paper ([1]), but written in different notation ($C_{i,k} = c_{i,k},\ \overline{\omega}_i = \omega_i;\ i = 3, 4, \dots, n-1$). After passing to the new basis by the formulas $\omega_2 = \overline{\omega}_2 - C_{n,n}$, $\omega_i = \overline{\omega}_i - C_{i,2}$, $\omega_n = \overline{\omega}_n - C_{n,2}$, we obtain

$$\omega_2\omega_n = C_{n,1} + C_{n,3}\omega_3 + \dots + C_{n,n-1}\omega_{n-1}, \tag{7}$$

$$\omega_2\omega_i = C_{i,1} + C_{i,3}\omega_3 + \cdots + C_{i,i}\omega_i + \frac{D_{i+1}}{D_i}\omega_{i+1}. \tag{8}$$

Let

$$x^n + f_1x^{n-1} + \cdots + f_n = 0$$

be the equation satisfied by ω_2. The author then gives an erroneous proof that the basis $1, \omega_2, \dots, \omega_n$ will be normal, i.e. that $C_{n,3} = \cdots = C_{n,n-1} = 0$, $C_{i,3} = \cdots = C_{i,i} = 0$.

The proof of the latter is based on the assertion that it is possible to eliminate the unknowns $c_{i,3}, \dots, c_{i,i}$ or $c_{n,3}, \dots, c_{n,n-1}$ from the systems (10) or (11) ([1]) and to obtain an equation relating the coefficients b_{ij}, which enter into the basic numbers ω_i $(i = 3, 4, \dots, n)$, so that

$$\omega_i = \frac{b_{i,1} + b_{i,2}\omega_2 + \cdots + b_{i,i-1}\omega_2^{i-2} + \omega_2^{i-1}}{D_i}.$$

This would be possible if the number of independent equations in each of the systems (10), (11) were greater than the number of unknowns to be eliminated, as the author assumes. In fact, however, in each of the systems (10), (11) the number of independent equations is equal to the number of unknowns. This can be shown by carrying out the computations in accordance with the author' s arguments, at least for fields of the 4th and 5th degrees, as follows.

If, in the systems (10) and (11), one expresses $b_{i,j}$ in terms of $B_{i,j}, \bar{t}_1, \bar{t}_2, \dots, \bar{t}_n$, then systems are obtained in which it is not difficult to establish a linear dependence among the equations. Consequently, the equation relating $b_{i,j}$ will in fact be an identity.

The construction of a fundamental basis of type (1) in algebraic fields of degree n was also studied by D. G. Grebenyuk ([2]), whose article B. Epelbaum cites. It follows from the arguments given above that the fundamental basis of D. G. Grebenyuk also will not exist in every algebraic field.

That not every field has a normal basis is easy to show, for example, by the following example. Consider the field $K(\rho)$ generated by some root ρ of the equation $x^4 - 7x^2 + 4x + 1 = 0$. The discriminant of the equation is $1957 \cdot 2^4$. It is not hard to show that the numbers $(\rho^2 + \rho + 1)/2$ and $(\rho^3 + 1)/2$ are algebraic integers, and since 1957 is a prime number, the numbers $1, \rho, (\rho^2 + \rho + 1)/2, (\rho^3 + 1)/2$ may be taken as a basis of the field. The discriminant of the field is 1957. Let us try to pass from this basis to a basis of type (1). Obviously, one may assume that $\omega_2 = \rho - \tau$, $\omega_3 = (\rho^2 + \rho + 1)/2 + a_1\rho + a_2$, $\omega_4 = (\rho^3 + 1)/2 + b_1(\rho^2 + \rho + 1)/2 + b_2\rho + b_3$, where $\tau, a_1, a_2, b_1, b_2, b_3$ are rational integers chosen in accordance with the conditions (1). Substituting in the equalities (1) the values of $\omega_2, \omega_3, \omega_4$ and equating, in the first equality, the coefficients of ρ^2 on the left and on the right, and in the second—the coefficients of ρ^3, we obtain $1 + 2a_1 - \tau = b_1$, $b_1 - \tau = 0$, whence $1 + 2a_1 = 2\tau$; the latter equality cannot hold for any rational integers a_1, τ. Thus the field has no normal basis.

K. K. Billevich
T. K. Shulikina

CITED LITERATURE

[1] B. Epelbaum, DAN, **44**, No. 5 (1949). [2] D. G. Grebenyuk, Bull. Central Asian State Univ., No. 13 (1926).

T-09196 Signed for printing 18/X-1961. Print run 5440 copies. Order 2232
Paper size $70 \times 108^1/_{16}$. Printed sheets $22.61 + 6$ inserts. Paper sheets $8^1/_4$.
Publisher' s sheets 24.6
2nd Printing House of the Publishing House of the Academy of Sciences of the USSR, Moscow, Shubinsky Lane, 10

Note: Figure translations are in progress. See original paper for figures.