UDC 512.5

A. Dubickas (Vilnius Univ. and Inst. Math. and Inform., Lithuania)

MULTIPLICATIVE RELATIONS WITH CONJUGATE ALGEBRAIC NUMBERS*

МУЛЬТИПЛІКАТИВНІ СПІВВІДНОШЕННЯ ЗІ СПРЯЖЕНИМИ АЛГЕБРАЇЧНИМИ ЧИСЛАМИ

We study which algebraic numbers can be represented by a product of conjugate over a fixed number field K algebraic numbers in fixed integer powers. The problem is nontrivial if the sum of these integer powers is equal to zero. The norm over K of such number must be a root of unity. We show that there are infinitely many algebraic numbers whose norm over K is a root of unity and which cannot be represented by such product. Conversely, every algebraic number can be expressed by every sufficiently long product in conjugate over K algebraic numbers. We also construct nonsymmetric algebraic numbers, i.e., such that none elements of the respective Galois group acting on the full set of their conjugates form a Latin square.

Досліджено, які алгебраїчні числа можуть бути зображені у вигляді добутку спряжених над фіксованим числовим полем K алгебраїчних чисел у фіксованих цілих степенях. Розглядувана задача є нетривіальною, якщо сума цих цілих степенів дорівнює нулю. Норма над K такого числа має бути коренем з одиниці. Показано, що існує нескінченно багато алгебраїчних чисел, норма над K яких є коренем з одиниці і які не можуть бути зображені згаданим добутком. Навпаки, кожне алгебраїчне число можна виразити будь-яким достатньо довгим добутком спряжених над K алгебраїчних чисел. Побудовано також несиметричні алгебраїчні числа, тобто такі, що жоден елемент відповідної групи Галуа, яка діє на повній множині їхніх спряжень, не формує Латинський квадрат.

1. Introduction. Let K be a number field, i.e., a finite extension of the field of rational numbers $\mathbb{Q}$. In this paper we investigate multiplicative relations with conjugate algebraic numbers. More precisely, given $\beta \in \overline{\mathbb{Q}}$ and $k_1, \dots, k_n \in \mathbb{Z}^*$, our main concern is to determine whether or not β can be expressed as $\alpha_1^{k_1} \dots \alpha_n^{k_n}$ with some algebraic numbers $\alpha_1, \dots, \alpha_n$ conjugate over K. (Throughout, as usual, $\overline{\mathbb{Q}}$ denotes the set of algebraic numbers, and $\mathbb{Z}^*$ denotes the set of non-zero integers.)

Let $\mathcal{M}(K; k_1, \dots, k_n)$ be the set of all β expressible as $\alpha_1^{k_1} \dots \alpha_n^{k_n}$. Here, we do not assume that $\alpha_1, \dots, \alpha_n$ are all distinct, nor we assume that the degree of $\alpha = \alpha_1$ over K is equal to n. Throughout, we reserve the letter d for the degree of β over K. Also, with $\beta_1 = \beta, \beta_2, \dots, \beta_d$ being the full set of conjugates of β over K, let $L = K(\beta_1, \dots, \beta_d)$ be the normal closure of $K(\beta)$ over K, and let $G = \mathrm{Gal}\,(L/K)$ be the Galois group of L/K.

As in [1], it is easily seen that $\mathcal{M}(K; k_1, \dots, k_n) = \overline{\mathbb{Q}}$, unless $k_1 + \dots + k_n = 0$. (Just take $\alpha_1 = \dots = \alpha_n = \beta^{1/(k_1+\dots+k_n)}$.) Also,

$$\mathcal{M}(K; 1, -1) \subset \mathcal{M}(K; k_1, \dots, k_n).$$

Indeed, the equality $k_1 + \dots + k_n = 0$ with non-zero $k_1, \dots, k_n$ implies that $n \geq 2$. The above inclusion now easily follows, by setting $\alpha_2 = \dots = \alpha_n$ and observing that $\mathcal{M}(K; kk_1, \dots, kk_n) = \mathcal{M}(K; k_1, \dots, k_n)$ for $k \in \mathbb{Z}^*$ (by Theorem 1 below).

The structure of $\mathcal{M}(K; k_1, \dots, k_n)$ is nontrivial if $n \geq 2$ and $k_1 + \dots + k_n = 0$ (see, for instance, Corollary 2 in Section 5). Note that if $\beta \in \mathcal{M}(K; k_1, \dots, k_n)$ with $k_1, \dots$

* This research was partially supported by the Lithuanian State Science and Studies Foundation.

$\dots, k_n \in \mathbb{Z}^*$ such that $k_1 + \dots + k_n = 0$, then its norm over K, namely, $\mathrm{Norm}(\beta) = \beta_1, \dots, \beta_d$ must be a root of unity. Indeed, setting F for the normal closure of $L(\alpha)$ over K and substituting $\beta = \alpha_1^{k_1} \dots \alpha_n^{k_n}$, we deduce that

$$\mathrm{Norm}_{F/K}(\beta) = \prod_{\sigma \in \mathcal{G}} \sigma(\beta) = \prod_{j=1}^{n} \mathrm{Norm}_{F/K}(\alpha_j)^{k_j} = \mathrm{Norm}_{F/K}(\alpha)^{k_1+\dots+k_n} = 1,$$

where $\mathcal{G} = \mathrm{Gal}(L/K)$. Since $\mathrm{Norm}_{F/K}(\beta)$ is a natural power of $\mathrm{Norm}(\beta)$, the latter number is a root of unity.

In the next section, we state the main results of this paper. Their comparison with earlier results (in particular, with additive results) will be discussed in Section 3. In Section 4, we prove Theorem 1 and Corollary 1. Section 5 contains the proofs of Theorems 2 and 3 which show that the condition on the norm of β is not sufficient for it to belong to $\mathcal{M}(K; k_1, \dots, k_n)$. In Section 6 we prove Theorem 4 which asserts that every β whose norm is a root of unity can be represented by every sufficiently long multiplicative form. We also present an example showing how, for a given β, one can find the respective α. The last section contains the construction of nonsymmetric numbers (see the definition at the end of Section 2).

2. Main results. Below, $k_1, \dots, k_n$ are integers, K is an arbitrary number field, L is the normal closure of $K(\beta)$ over K, and $G = \mathrm{Gal}(L/K)$. Also, for $r \in \mathbb{Q}$, the number $\beta^r = \exp\{r \log \beta\}$ is defined by taking the principal branch of the logarithm.

Our first theorem shows that the set $\mathcal{M}(K; k_1, \dots, k_n)$ is invariant under multiplication by roots of unity. This implies that the search for possible a can be reduced to those numbers whose powers lie in the field L.

Theorem 1. *Suppose that* $\beta \in \mathcal{M}(K; k_1, \dots, k_n)$, $r \in \mathbb{Q}$, *and* ζ *is a root of unity. Then* $\zeta\beta, \beta^r \in \mathcal{M}(K; k_1, \dots, k_n)$.

***Corollary* 1.** *Given integers* $k_1, \dots, k_n$, *assume that* $\beta = \alpha_1^{k_1} \dots \alpha_n^{k_n}$, *where* $\alpha_1, \dots, \alpha_n$ *are all conjugate to* α *over* K. *Then* α *can be chosen so that one of its natural powers lies in* L.

In the next two theorems we show that not all algebraic numbers whose norm is a root of unity lie in the set $\mathcal{M}(K; k_1, \dots, k_n)$, where $k_1 + \dots + k_n = 0$. The proof of Theorem 3 is constructive and, at the same time, it is rather unusual for this kind of proofs. It uses, for instance, some elementary properties of the Pell equation.

Theorem 2. *Suppose that* $\beta \in \mathcal{M}(K; k_1, \dots, k_n)$ *with* $k_1, \dots, k_n \in \mathbb{Z}^*$ *such that* $k_1 + \dots + k_n = 0$. *Then there is a subgroup* H *of* G, *generated by* $n - 1$ (*not necessarily distinct*) *elements, such that* $\prod_{\sigma \in H} \sigma(\beta)$ *is a root of unity.*

Theorem 3. *Assume that* $k_1, \dots, k_n \in \mathbb{Z}^*$ *are such that* $k_1 + \dots + k_n = 0$. *Then there exists an algebraic number* $\beta \notin \mathcal{M}(K; k_1, \dots, k_n)$ *of degree* $d = 2^n$ *over* K *whose norm over* K *is equal to* 1.

Our final theorem shows that the condition on $\mathrm{Norm}(\beta)$ to be a root of unity is not only necessary, but also sufficient for β to lie in $\mathcal{M}(K; k_1, \dots, k_n)$, provided that n is sufficiently large.

Theorem 4. *Assume that* $k_1, \dots, k_n \in \mathbb{Z}^*$, *and* β *is an algebraic number of degree* d *over* K *whose norm over* K *is a root of unity. If* $n \geq 2d - 5$, *then* $\beta \in \mathcal{M}(K; k_1, \dots, k_n)$.

Similarly to Theorem 3 in [1], the inequality $n \geq 2d - 5$ can be replaced by $n \geq 2[d/2] - 1$ for *symmetric* β. Here, $[\ldots]$ stands for the integral part, and $\beta \in \overline{K}$ of degree d over K is called symmetric over K if there exist $\sigma_2, \ldots, \sigma_d \in G$ such that the matrix $\|\sigma_i(\beta_j)\|_{i,j=1,\ldots,d}$, where σ_1 stands for the identity, is a Latin square, namely, each of its rows and each of its columns is a permutation of $\beta_1, \ldots, \beta_d$. In Section 7 we will prove the result which was announced in [1]: the smallest possible degree for nonsymmetric numbers to occur is equal to 6.

3. Comparison with earlier results and comments. There are several types of problems concerning additive and multiplicative relations in conjugates of an algebraic number. Given a field K, an algebraic number β over K, and $k_1, \ldots, k_n \in K$, one can ask, for instance, whether β can be expressed as $k_1\alpha_1 + \ldots + k_n\alpha_n$ with distinct $\alpha_1, \ldots, \alpha_n$ conjugate over K. Similarly, for integer $k_1, \ldots, k_n$, one can ask whether β is expressible as $\alpha_1^{k_1} \ldots \alpha_n^{k_n}$. The cases $\beta = 0$ (and $\beta = 1$ in the multiplicative setting, respectively) were studied earlier by V. A. Kurbatov [2], C. J. Smyth [3, 4], K. Girstmair [5, 6], J. D. Dixon [7], M. Drmota and M. Skalba [8] (see also [9, 10]). Similar problems were also studied by E. M. Matveev [11], the author [12] and T. Zaimi [13 – 15].

Given a positive integer n and non-zero $k_1, \ldots, k_n \in K$, one can also ask which algebraic numbers β over K can be written as

$$\beta = k_1\alpha_1 + \ldots + k_n\alpha_n$$

with algebraic numbers $\alpha_1, \ldots, \alpha_n$ conjugate over K. For $n = 2$, the complete answer was given in [16]: an algebraic number β can be written as a difference $\alpha_1 - \alpha_2$ of algebraic numbers α_1, α_2 conjugate over a number field K if and only if there is $\sigma \in G$ such that $\sum_{i=0}^{v-1} \sigma^i(\beta) = 0$. (Here, v is the order of the cyclic group $\langle\sigma\rangle$ generated by σ.) The case $n \geq 3$ was the main subject of our paper [1]. Similarly, β can be written as a quotient α_1/α_2 of algebraic numbers α_1, α_2 conjugate over a number field k if and only if there is $\sigma \in G$ such that $\prod_{i=0}^{v-1} \sigma^i(\beta)$ is a root of unity. Note that in Hilbert's Theorem 90 (see, e.g., [17, 18] and also [19, 20] for generalizations), where both β and α are only allowed to lie in a fixed cyclic extension of K, the answer is different.

Let $k_1, \ldots, k_n \in \mathbb{Z}^*$. Assume that $\beta = \alpha_1^{k_1} \ldots \alpha_n^{k_n}$ with $\alpha_1, \ldots, \alpha_n$ conjugate to α over a number field K. In [1] we asked whether it is true that α can be chosen so that its natural power is equal to $a\beta_1^{a_1} \ldots \beta_d^{a_d}$ with integer $a, a_1, \ldots, a_d$? This, as we claimed, would be sufficient in order to give the additive theorems of [1] in the multiplicative form. In the present paper, we use a much weaker version of this statement (Corollary 1), but still attain the same goals as in [1].

There is nothing like Theorem 1 needed in the additive case, because, for $r \in \mathbb{Q}$, the numbers $r\alpha$ and $r\alpha'$ are conjugate over K if so are α and α'. This is, in general, false in the multiplicative case: α^r and α'^r need not be conjugate for α and α' being conjugate. Theorem 2 is a direct analogue of the respective additive theorem in [1] both in terms of the result and in terms of the proof. The proof of Theorem 3 is much more subtle compared to its additive analogue (see the construction before Corollary 1 in [1]), because now we cannot use the normal basis theorem. The present construction uses, for instance, the fact that the Pell equation $X^2 - mY^2 = 1$, where m is square-free, has infinitely many solutions in positive integers X, Y. It also involves an extra part of combinatorics. Finally, Theorem 4 looks essentially the same as does

its additive analogue (Theorem 3 in [1]), although, because of what was said earlier, the practical computation becomes more difficult (see the example in Section 6). In particular, for $d = 4$, it follows that every β of degree ≤ 4 over $\mathbb{Q}$ can be represented by every form $\alpha_1^{k_1}\alpha_2^{k_2}\alpha_3^{k_3}$ of length 3 with fixed $k_1, k_2, k_3 \in \mathbb{Z}^*$ and some algebraic numbers $\alpha_1, \alpha_2, \alpha_3$ conjugate over $\mathbb{Q}$. Thus, for $d = 4$, the inequality $n \ge$ ≥ 3 of Theorem 4 is sharp. It cannot be replaced by $n \ge 2$, which is shown by the example of $\beta = 1 + \sqrt{2} + \sqrt{6} \notin \mathcal{M}(\mathbb{Q}; 1, -1)$ (see [16] or apply Theorem 2 with $n =$ $= 2$ combined with the fact that, for this β, G is the Klein 4-group).

4. Restrictions on algebraic numbers. ***Proof of Theorem*** **1.** Write $\beta =$ $= \alpha_1^{k_1} \dots \alpha_n^{k_n}$ with $\alpha_1, \dots, \alpha_n$ conjugate over a number field K. Assume that m is a positive integer and $\zeta_1, \dots, \zeta_n$ are arbitrary mth roots of unity. We will show first that there is a positive integer a such that $\zeta_1 a^{1/m}\alpha_1, \dots, \zeta_n a^{1/m}\alpha_n$ are conjugate over K. Here, $a^{1/m}$ denotes the positive mth root of a.

Indeed, let F be the normal closure of $K(\alpha, \mu_m)$ over K, where μ_m is the primitive mth root of unity. Take a positive integer a such that the polynomial $z^m -$ $- a$ is irreducible over F. (This is possible, e.g., by Theorem 16 on p. 221 in Lang's book [18].) Then, firstly, $\alpha_1, \dots, \alpha_n$ are all conjugate over $K(a^{1/m})$, for otherwise the minimal polynomial of α over K is reducible over $K(a^{1/m})$. We thus get

$$D > [K(a^{1/m}, \alpha) : K(a^{1/m})] = \frac{[K(a^{1/m}, \alpha) : K(\alpha)][K(\alpha) : K]}{[K(a^{1/m}) : K]} = [K(\alpha) : K] = D,$$

where D is the degree of α over K, a contradiction. Secondly, $F(a^{1/m})/F$ and F/K are both Galois extensions, hence there are automorphisms $\tau_1, \dots, \tau_n$ in the Galois group of $F(a^{1/m})/K$ fixing F and taking $a^{1/m}$ to $\zeta_1 a^{1/m}, \dots, \zeta_n a^{1/m}$, respectively. Finally, $F(a^{1/m})/K(a^{1/m})$ is a Galois extension whose Galois group isomorphic to that of F/K (see, for instance, Theorem 4 of Ch. VIII in. [18]). Thus there are automorphisms $\sigma_1, \dots, \sigma_n$ in the Galois group of $F(a^{1/m})/K$ fixing $K(a^{1/m})$ and taking α to $\alpha_1, \dots, \alpha_n$, respectively. Note that $\tau_j\sigma_j(a^{1/m}\alpha) =$ $= \tau_j(a^{1/m}\alpha_j) = \zeta_j a^{1/m}\alpha_j$, where $j = 1, \dots, n$. It follows that $\zeta_1 a^{1/m}\alpha_1, \dots, \zeta_n a^{1/m}\alpha_n$ are all conjugate over K, as claimed.

Write $\zeta = \exp\{2\pi\sqrt{-1}u/m\}$ with $u < m$ coprime. Let k' be the greatest common divisor of $k_1, \dots, k_n$. We can certainly assume that $k' = 1$, for otherwise the initial set of conjugates $\alpha_1, \dots, \alpha_n$ can be replaced by the set $\alpha_1^{k'}, \dots, \alpha_n^{k'}$. Clearly, there exist nonnegative integers $r_1, \dots, r_n < m$ such that $r_1 k_1 + \dots + r_n k_n$ is equal to u modulo m. Take $a \in \mathbb{Z}^*$ so that $\delta_1 = \mu_m^{r_1} a^{1/m}\alpha_1, \dots, \delta_n = \mu_m^{r_n} a^{1/m}\alpha_n$ are conjugate over K. Using $k_1 + \dots + k_n = 0$ (which can be assumed without loss of generality, for otherwise $\mathcal{M}(K; k_1, \dots, k_n) = \overline{\mathbb{Q}}$, and there is nothing to prove), we obtain that

$$\delta_1^{k_1} \dots \delta_n^{k_n} = \mu_m^{r_1 k_1 + \dots + r_n k_n}\alpha_1^{k_1} \dots \alpha_n^{k_n} = \mu_m^u\beta = \zeta\beta.$$

Consequently, $\zeta\beta \in \mathcal{M}(K; k_1, \dots, k_n)$.

For every $r \in \mathbb{Q}$, there are roots of unity $\zeta_1, \dots, \zeta_n$ such that $\zeta_1\alpha_1^r, \dots, \zeta_n\alpha_n^r$ are all conjugate to α^r over K. (Recall that $\alpha^r = \exp\{r\log\alpha\}$ is defined by taking the principal branch of the logarithm.) Thus $\beta = \alpha_1^{k_1} \dots \alpha_n^{k_n}$ implies that

$$(\zeta_1\alpha_1^r)^{k_1} \dots (\zeta_n\alpha_n^r)^{k_n} = \zeta\beta^r$$

with some root of unity ζ. Hence $\zeta\beta^r$ lies in $\mathcal{M}(K; k_1, \dots, k_n)$, and, by the above, so does $\zeta^{-1}\zeta\beta^r = \beta^r$.

***Proof of Corollary* 1.** Let F be the normal closure of $L(\alpha)$ over K, and let $\mathcal{G} = = \mathrm{Gal}(F/K)$. We have that $K \subset L \subset F$. By the main theorem of Galois theory, $G = = \mathcal{G}/H$, where

$$H = \{\sigma \in \mathcal{G} \mid \sigma(x) = x \text{ for all } x \in L\}.$$

Assuming that $H = \{\sigma_1, \dots, \sigma_m\}$, we set

$$\varphi(x) = \sigma_1(x) \dots \sigma_m(x)$$

for every $x \in F$. Clearly, $\varphi(\beta) = \beta^m$, since $\beta \in L$. On applying φ to the equality $\beta = \alpha_1^{k_1} \dots \alpha_n^{k_n}$, we deduce that

$$\beta^m = \varphi(\alpha_1)^{k_1} \dots \varphi(\alpha_n)^{k_n}.$$

Also, as H is a group, $\sigma_j(\varphi(\alpha)) = \varphi(\alpha)$ for every $j = 1, \dots, n$. Hence

$$\varphi(\alpha) \in L = \{x \in F \mid \sigma(x) = x \text{ for all } \sigma \in H\}.$$

The numbers $\zeta_1\varphi(\alpha_1)^{1/m}, \dots, \zeta_n\varphi(\alpha_n)^{1/m}$ are conjugate over K for some m th roots of unity $\zeta_1, \dots, \zeta_n$. Now, as in the proof of Theorem 1, it follows that there is a positive integer a such that $\beta = \delta_1^{k_1} \dots \delta_n^{k_n}$, where $\delta_1 = \zeta_1 a^{1/m}\varphi(\alpha_1)^{1/m}, \dots, \delta_n = = \zeta_n a^{1/m}\varphi(\alpha_n)^{1/m}$ are all conjugate over K. This completes the proof, since $\delta_1^m = = \delta^m = a\varphi(\alpha) \in L$.

5. On numbers which cannot be represented. ***Proof of Theorem* 2.** Suppose that β can be expressed as $\alpha_1^{k_1} \dots \alpha_n^{k_n}$. By Corollary 1, there is a positive integer m such that $\alpha^m \in L$. On replacing $\beta, \alpha_1, \dots, \alpha_n$ by their m th powers (without changing the notation for α), we see that the new α lies in L. It follows that $\beta^m = = \alpha^{k_1}\sigma_2(\alpha)^{k_2} \dots \sigma_n(\alpha)^{k_n}$ with $\sigma_2, \dots, \sigma_n \in G$. Setting $H = \langle\sigma_2, \dots, \sigma_n\rangle$, we deduce that

$$\prod_{\sigma\in H}\sigma(\beta^m) = \prod_{\sigma\in H}\sigma(\alpha^{k_1}\sigma_2(\alpha)^{k_2} \dots \sigma_n(\alpha)^{k_n}) = \prod_{\sigma\in H}\sigma(\alpha)^{k_1+\dots+k_n} = 1,$$

which implies Theorem 2.

Let K be a number field, and let $p_1, \dots, p_n$ be prime numbers such that $\sqrt{p_1} \notin \notin K$, $\sqrt{p_2} \notin K(\sqrt{p_1}), \dots, \sqrt{p_n} \notin K(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})$. Let $S_1, \dots, S_l$ be all $l = 2^n - 1$ nonempty subsets of the set $\{p_1, \dots, p_n\}$ (in an arbitrary order). Set $m_i = \prod_{p\in S_i} p$. Assume that x_i, y_i are solutions of the Pell equations

$$X^2 - m_i Y^2 = 1$$

(in positive integers), where $i = 1, \dots, l$, satisfying $x_i > (2x_{i+1})^{l^2}$ for $1 \le i \le l - 1$. Consider the number

$$\beta = \prod_{i=1}^{l}(x_i + y_i\sqrt{m_i}).$$

Lemma 1. *The number* β *is a unit of degree* 2^n *over* K *such that no product of fewer than* 2^n *of its conjugates is a root of unity.*

***Proof of Lemma* 1.** We see at once that β is a unit, because it is a product of units $x_i + y_i\sqrt{m_i}$. Since

$$\left[K\left(\sqrt{p_1}, \dots, \sqrt{p_{n-1}}\right) : K\right] = 2^n,$$

it follows immediately that the degree of β over K is at most 2^n. The Galois group of $K(\sqrt{p_1}, \dots, \sqrt{p_n})/K$ is generated by n elements of order 2, say $\sigma_1, \dots, \sigma_n$, where σ_j maps $\sqrt{p_j}$ to $-\sqrt{p_j}$ and every other $\sqrt{p_i}$, $i \neq j$, to itself. The conjugates of β are all of the form

$$\beta' = \prod_{i=1}^{l} (x_i + \varepsilon_i y_i \sqrt{m_i}),$$

where $\varepsilon_i \in \{1, -1\}$. We call $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_l)$ the *signature* of β'. The signature of every β' is uniquely prescribed by the n signs ε_i which correspond to S_i containing exactly one prime number. Consider the table with 2^n rows and $2^n - 1 = l$ columns, whose first row contains $2^n - 1$ of plus signs, and whose other $2^n - 1$ rows correspond to the signatures of different β'.

We first show that every row except for the first contains $2^{n-1} - 1$ of plus signs and 2^{n-1} of minus signs. This is, of course, the case for $n = 1$. Assume that this is true with $n - 1$ instead of n. By adding the square root of the p_nth prime with plus sign, we increase the number of plus signs by $1 + (2^{n-2} - 1) = 2^{n-2}$. The total number of plus signs will be $2^{n-2} - 1 + 2^{n-2} = 2^{n-1} - 1$. Similarly, after adding the square root of the p_nth prime with minus sign, the total number of plus signs will be $2^{n-2} - 1 + 2^{n-2} = 2^{n-1} - 1$, unless all square roots $\sqrt{p_1}, \dots, \sqrt{p_{n-1}}$ were with plus signs. The latter situation however could be also achieved by adding the square root of the p_{n-1} th prime with minus sign which leads to the former situation. Alternatively, if just one p_n is with minus sign, then one can find the total number of minus signs by the formulae

$$1 + n - 1 + \binom{n-1}{2} + \dots + \binom{n-1}{n-1} = 2^{n-1}.$$

Furthermore, every column of the table contains 2^{n-1} of plus signs and 2^{n-1} of minus signs. Indeed, if the sign of the column is determined by the sign of the product of v signs, then it is minus in

$$\left(\binom{v}{1} + \binom{v}{3} + \dots + \binom{v}{2[(v-1)/2]+1}\right) 2^{n-v} = 2^{v-1+n-v} = 2^{n-1}$$

cases. The product of β and all different β' is thus equal to 1. Clearly, β and all β' are positive. Both remaining claims of the lemma will therefore follow if the product of $< 2^n$ (not necessarily distinct) conjugates β is newer equal to 1.

Suppose, contrary to our claim, that the product of some $s < 2^n$ conjugates of β is equal to 1. Let s_1 of these be β itself, and let $s - s_1$ be different from β. There is no loss of generality to assume that $s_1 \geq 1$, since we can map arbitrary β' to β. Now, consider the table with s rows and $2^n - 1$ columns which correspond to the

conjugates involved in the product, where every row is taken with corresponding multiplicity. The total number of plus signs in the new (smaller) table is equal to

$$s_1(2^n - 1) + (s - s_1)(2^{n-1} - 1) = s(2^{n-1} - 1) + s_1 2^{n-1}.$$

This number is greater than $s(2^n - 1)/2$, so that the number of plus signs is greater than the number of minus signs. By our construction, the product of conjugates is equal to

$$\prod_{i=1}^{l}(x_i + y_i\sqrt{m_i})^{e_i} = 1,$$

where e_i is the difference between the number of plus signs and the number of minus signs in the ith column. The last equality can be also written as

$$\prod_{j}(x_j + y_j\sqrt{m_j})^{e_j} = \prod_{k}(x_k + y_k\sqrt{m_k})^{-e_k},$$

where j are all indices with positive e_j, and k are all indices with negative e_k. (Here, at least one side is greater than 1, because $e_1 + \ldots + e_l > 0$.)

Assume that q is the smallest number among all j and all k. The side which contains the index q is at least $x_q + y_q\sqrt{m_q} > x_q$. We immediately have a contradiction if $q = l$. Otherwise, since $|e_i| \le s \le l$ and $x_i + y_i\sqrt{m_i} < 2x_i$, the other side is at most $(2x_{q+1})^{l(l-q)} < (2x_{q+1})^{l^2} < x_q$, a contradiction again. The proof of Lemma 1 is now completed.

***Proof of Theorem* 3.** Consider β as defined before Lemma 1. Every element of G, except for identity, is of order 2. Furthermore, G is abelian. Therefore, every subgroup of G generated by $n - 1$ of its elements has the order at most 2^{n-1}. By Theorem 2, it follows that if $\beta \in \mathcal{M}(K; k_1, \ldots, k_n)$, then the product of at most 2^{n-1} of its conjugates is a root of unity. This is however not the case, by Lemma 1, a contradiction. This completes the proof of Theorem 3, because, by Lemma 1 again, the degree of β over K is 2^n. (Norm $(\beta) = 1$, because every column in the table of signatures contains equal number of plus and minus signs.)

***Corollary* 2.** *Let* $k_1, \ldots, k_n \in \mathbb{Z}^*$ *be such that* $k_1 + \ldots + k_n = 0$. *Then* $\mathcal{M}(K; k_1, \ldots, k_n)$ *is not a multiplicative semigroup.*

By the results of [16], every algebraic number of prime degree whose norm is a root of unity belongs to $\mathcal{M}(K; 1, -1)$. Thus, as every quadratic unit $x_i + y_i\sqrt{m_i}$, where x_i, y_i are positive integers and m_i is an integer which is not a perfect square, is a quotient of two conjugates over a number field K, this number belongs to every $\mathcal{M}(K; k_1, \ldots, k_n)$. For the proof of Corollary 2, note that the algebraic number β considered in Theorem 3 (see Lemma 1) is the product of quadratic units $x_i + y_i\sqrt{m_i}$, but $\beta \notin \mathcal{M}(K; k_1, \ldots, k_n)$, by Theorem 3.

6. Representation by sufficiently long forms. The next lemma is a part of Lemma 2 proved in [1].

Lemma 2. *Suppose that the* $d \times d$ *matrix, where* $d \ge 4$, *with negative real entries in the main diagonal and nonnegative real entries outside the main diagonal is such that the sums of its elements in every row and in every column are all equal to zero. If the first row contains at least* $d - 2$ *positive entries, then the rank of the matrix is equal to* $d - 1$.

***Proof of Theorem* 4.** For $d = 1$ the theorem follows from Theorem 1, whereas for every β of prime degree d (including $d = 2$ and $d = 3$) it follows from the fact that already $\mathcal{M}(K; 1, -1)$ contains β. It therefore suffices to prove the theorem for the case $d \geq 4$ and $\sum_{j=1}^{n} k_j = 0$, where $k_1, \ldots, k_n \in \mathbb{Z}^*$. As $n \geq 2d - 5$, at least $d - 2$ elements of the multiset $k_1, \ldots, k_n$ are either positive or negative. Without loss of generality we may assume that $k_2, \ldots, k_{d-1}$ are all positive. On replacing of the remaining ones k_1 and $k_d, \ldots, k_n$ by $k_1 + k_d + \ldots + k_n$ and $n - d + 1$ zeroes, respectively, and writing k_1 again for the sum $k_1 + k_d + \ldots + k_n$, we will show that there is an $m \in \mathbb{Z}^*$ such that

$$\beta^{md} = \alpha_1^{k_1} \ldots \alpha_d^{k_d},$$

where $k_d = 0$, has a solution in conjugates of α over K.

Since $(\beta_1 \ldots \beta_d)^m = 1$ for some positive integer m, we see that

$$\beta_1^{(d-1)m} \beta_2^{-m} \ldots \beta_d^{-m} = \beta_1^{md} = \beta^{md}.$$

Write $\alpha = \beta_1^{x_1} \ldots \beta_d^{x_d}$ with unknowns $x_1, \ldots, x_d \in \mathbb{Z}$. Choose the automorphisms $\sigma_2, \ldots, \sigma_d \in G$ such that $\sigma_i(\beta_1) = \beta_i$, $i = 2, \ldots, d$, and let σ_1 be the identity. Setting $\alpha_i = \sigma_i^{-1}(\alpha)$, where $i = 1, \ldots, d$, we deduce that

$$\sigma_1^{-1}(\alpha)^{k_1} \ldots \sigma_d^{-1}(\alpha)^{k_d} = \beta_1^{(d-1)m} \beta_2^{-m} \ldots \beta_d^{-m} = \beta^{md},$$

if

$$M(x_1, x_2, \ldots, x_d)^t = ((d-1)m, -m, \ldots, -m)^t$$

has a solution in $x_1, \ldots, x_d \in \mathbb{Z}$. Here, t stands for the transpose, and M is the $d \times d$ matrix $\| m_{ij} \|_{i,j=1,\ldots,d}$, where $m_{ij} = \sum k_r$ and the sum is taken over every r such that $\sigma_r(\beta_i) = \beta_j$.

By Lemma 2, the rank of M is equal to $d - 1$. Summing the rows of the $d \times (d + 1)$ matrix M^* which is obtained by adding the $(d + 1)$ st column

$$((d-1)m, -m, \ldots, -m)^t$$

to M, we see they are linearly dependent over $\mathbb{Q}$. It follows that $d - 1 = \operatorname{rank} M \leq \operatorname{rank} M^* \leq d - 1$, thus $\operatorname{rank} M = \operatorname{rank} M^* = d - 1$. By the Kronecker – Capelli theorem, we conclude that the linear system has a non-zero rational solution. Let x' be the least positive integer such that $x' x_i \in \mathbb{Z}^*$ for every $i = 1, \ldots, d$. On replacing every x_i by $x' x_i$ and m by $x' m$, we get the desired conclusion.

If in Lemma 2 the condition on the first row of the matrix to contain at least $d - 2$ positive entries is replaced by the condition to contain at least $[d/2]$ positive entries, and, in addition, the $d \times d$ matrix is a Latin square, then, by Lemma 2 of [1], its rank is also equal to $d - 1$. Hence, if β is symmetric over K and if $n \geq 2[d/2] - 1$, then at least $[d/2]$ elements among $k_1, \ldots, k_n$ are either positive or negative. Thus we can argue as above with the automorphisms $\sigma_2, \ldots, \sigma_d$ such that $\| \sigma_i(\beta_j) \|_{i,j=1,\ldots,d}$ is a Latin square. This shows that, for symmetric β, in Theorem 4 the inequality $n \geq 2d - 5$ can by replaced by the inequality $n \geq 2[d/2] - 1$.

Example. *Let* $K = \mathbb{Q}$, $\beta = 1 + \sqrt{2} + \sqrt{6}$, $d = 4$, $n = 3$, $k_1 = k_2 = 1$, $k_3 = -2$. *Then* α *can be chosen as* $((8 + 5\sqrt{2} + 4\sqrt{3} + 3\sqrt{6})/2)^{1/2}$.

By Theorem 4, we know that the equation

$$\beta = 1 + \sqrt{2} + \sqrt{6} = \alpha_1\alpha_2\alpha_3^{-2}$$

has a solution in conjugate over $\mathbb{Q}$ algebraic numbers $\alpha_1, \alpha_2, \alpha_3$. We will show how to find some solutions.

Let us choose the following indices: $\beta_1 = 1 + \sqrt{2} + \sqrt{6}$, $\beta_2 = 1 - \sqrt{2} - \sqrt{6}$, $\beta_3 = 1 - \sqrt{2} + \sqrt{6}$ and $\beta_4 = 1 + \sqrt{2} - \sqrt{6}$. Now, following the proof of Theorem 4 with $m - 1$, we obtain the system of linear equations

$$\begin{aligned} x_1 + x_2 - 2x_3 &= 3, \\ x_1 + x_2 - 2x_4 &= -1, \\ -2x_1 + x_3 + x_4 &= -1, \\ -2x_2 + x_3 + x_4 &= -1. \end{aligned}$$

(Of course, there is no need to put the negative elements of M on the main diagonal. It suffices to assume that every row and every column of M contains precisely one negative element.) One of its solutions is $x_1 = x_2 = 0$, $x_3 = -3/2$, $x_4 = 1/2$. So we can choose $x' = 2$, which gives the integer solution $x_1 = x_2 = 0$, $x_3 = -3$, $x_4 = 1$ for $m = 2$. This choice shows that

$$\beta^8 = \delta_1\delta_2\delta_3^{-2},$$

where $\delta_1 = \beta_3^{-3}\beta_4$, $\delta_2 = \beta_3\beta_4^{-3}$, $\delta_3 = \beta_1^{-3}\beta_2$. On replacing δ by $-\delta$, we compute

$$\delta = \delta_1 = (1 + \sqrt{2} - \sqrt{6})^4(7 + 4\sqrt{3})^3 = 11591 - 8196\sqrt{2} + 6692\sqrt{3} - 4732\sqrt{6}.$$

The minimal polynomial of δ over $\mathbb{Q}$ is

$$Q(z) = z^4 - 46364z^3 + 10950z^2 - 284z + 1.$$

Since the polynomial

$$Q(5z^8) = 625z^{32} - 5795500z^{24} + 273750z^{16} - 1420z^8 + 1$$

is irreducible over $\mathbb{Q}$, the equation $\beta = \alpha_1\alpha_2\alpha_3^{-2}$ is solvable in conjugates of

$$\alpha = (\delta/5)^{1/8} = ((11591 - 8196\sqrt{2} + 6692\sqrt{3} - 4732\sqrt{6})/5)^{1/8}$$

of degree 32.

It is not the smallest possible degree for α. The polynomial $Q(z^8)$ is the product of three irreducible polynomials $z^8 + 16z^6 + 20z^4 + 8z^2 + 1$, $z^8 - 16z^6 + 20z^4 - 8z^2 + 1$, and $z^{16} + 216z^{12} + 146z^8 + 24z^4 + 1$. In this example, it happens that the roots of $Q(z^8)$ satisfying $1 + \sqrt{2} + \sqrt{6} = \alpha_1\alpha_2\alpha_3^{-2}$ are all roots of the second polynomial, namely, $z^8 - 16z^6 + 20z^4 - 8z^2 + 1$ (which is not always the case). The roots are $\alpha_1 = ((8 + 5\sqrt{2} + 4\sqrt{3} + 3\sqrt{6})/2)^{1/2}$, $\alpha_2 = ((8 - 5\sqrt{2} + 4\sqrt{3} - 3\sqrt{6})/2)^{1/2}$ and $\alpha_3 = ((8 + 5\sqrt{2} - 4\sqrt{3} - 3\sqrt{6})/2)^{1/2}$, giving the second solution with α of degree 8, as claimed.

7. Nonsymmetric numbers. Clearly, every β of prime degree d over K is symmetric, since the Galois group G contains a d-cycle. If, for $d = 4$, G does not

contain a 4-cycle, then it is the Klein 4-group, so the respective β is also symmetric. Hence the smallest d for nonsymmetric β must be greater than or equal to 6. We will show now that nonsymmetric numbers of degree 6 exist. For this, we first introduce an „auxiliary" number α.

Let α be of degree 4 over K with the Galois group of $K(\alpha_1, \alpha_2, \alpha_3, \alpha_4)/K$ isomorphic to the full symmetric group on four symbols. Assume that $\pm\alpha_1 \pm \alpha_2 \pm \pm \alpha_3 \pm \alpha_4 \neq 0$. (It is clear that such α exist.) Set $\beta = \beta_1 = \alpha_1 + \alpha_2$. Such β is of degree 6 over K with the remaining conjugates being $\beta_2 = \alpha_2 + \alpha_3$, $\beta_3 = \alpha_3 + \alpha_4$, $\beta_4 = \alpha_1 + \alpha_4$, $\beta_5 = \alpha_1 + \alpha_3$, $\beta_6 = \alpha_2 + \alpha_4$, and with Galois group G of order 24. We claim that β is nonsymmetric.

Assume that β is symmetric over K. Then some five elements of the full symmetric group acting on $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ can be chosen so that their action on the row $\beta_1, \ldots, \beta_6$ together with identity form a Latin square. Let S be the set of these five elements. Evidently, none of the elements in S is a transposition nor it is a product of two transpositions. The remaining fifteen elements are the identity τ_0, and the following fourteen elements: $\tau_1 = (123)$, $\tau_2 = (132)$, $\tau_3 = (124)$, $\tau_4 = (142)$, $\tau_5 = = (134)$, $\tau_6 = (143)$, $\tau_7 = (234)$, $\tau_8 = (243)$, $\tau_9 = (1234)$, $\tau_{10} = (1243)$, $\tau_{11} = (1324)$, $\tau_{12} = (1342)$, $\tau_{13} = (1423)$, $\tau_{14} = (1432)$, five of which do form the set S. Their action on $\beta_1, \ldots, \beta_6$ can be described as follows:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	2	5	6	4	2	6	5	4	2	6	3	5	3	4
2	5	1	3	5	6	1	3	6	3	4	6	4	5	1
3	4	6	5	2	4	5	6	2	4	5	1	6	1	2
4	6	3	1	6	5	3	1	5	1	2	5	2	6	3
5	1	2	2	3	3	4	4	1	6	1	2	3	4	6
6	3	4	4	1	1	2	2	3	5	3	4	1	2	5

Here, the symbol i in the first row means τ_i, whereas in other five rows i stands for β_i.

Since $\tau_{11}(\beta_1) = \tau_{13}(\beta_1)$, $\tau_{10}(\beta_2) = \tau_{12}(\beta_2)$, $\tau_9(\beta_5) = \tau_{14}(\beta_5)$, the set S contains at most one element from the pair $\{\tau_{11}, \tau_{13}\}$, at most one from $\{\tau_{10}, \tau_{12}\}$, and at most one from $\{\tau_{11}, \tau_{13}\}$. If $\tau_{11} \in S$, then $\tau_2 \notin S$, since $\tau_2(\beta_5) = \tau_{11}(\beta_5)$ (see the table). Similarly, $\tau_3, \tau_5, \tau_8 \notin S$, because $\tau_3(\beta_5) = \tau_{11}(\beta_5)$ and $\tau_5(\beta_2) = = \tau_8(\beta_2) = \tau_{11}(\beta_2)$. So, if $\tau_{11} \in S$, then the elements of $S_8 = \{\tau_1, \ldots, \tau_8\}$ belonging to S all must lie in the set $S_1 = \{\tau_1, \tau_4, \tau_6, \tau_7\}$. Similarly, if $\tau_{13} \in S$, or $\tau_{10} \in S$, or $\tau_{12} \in S$, or $\tau_9 \in S$, or $\tau_{14} \in S$, then the elements of S_8 belonging to S must lie, respectively, in $S_{-1} = \{\tau_2, \tau_3, \tau_5, \tau_8\}$, $S_2 = \{\tau_2, \tau_4, \tau_5, \tau_7\}$, $S_{-2} = \{\tau_1, \tau_3, \tau_6, \tau_8\}$, $S_3 = \{\tau_2, \tau_4, \tau_6, \tau_8\}$, $S_{-3} = \{\tau_1, \tau_3, \tau_5, \tau_7\}$. Note that $S_i \cap S_{-i} = \varnothing$ for $i = 1, 2, 3$ and, for any choice of signs, $|S_{\pm 1} \cap S_{\pm 2} \cap S_{\pm 3}| = 1$. We can therefore conclude by observing the following. If $|S \cap \{\tau_9, \ldots, \tau_{14}\}| = 3$, then $|S \cap S_8| = 1$, so $|S| = 3 + + 1 = 4$, a contradiction. If however $|S \cap \{\tau_9, \ldots, \tau_{14}\}| < 3$, then, once again, $|S| < < 3 + 2 = 5$, because $|S \cap S_8| \leq 2$. (Indeed, by symmetry, there is no loss of generality to assume that $\tau_1 \in S$. Then $\tau_4, \tau_5, \tau_8 \notin S$, and, moreover, at most one element from $\{\tau_2, \tau_3, \tau_6, \tau_7\}$ can belong to S.)

1. *Dubickas A.* Additive relations with conjugate algebraic numbers // Acta arithm. – 2003. – **107**. – P. 35 – 43.
2. *Kurbatov V. A.* Galois extensions of prime degree and their primitive elements // Sov. Math. (Izvest. VUZ). – 1977. – **21**. – P. 49 – 52.

3. *Smyth C. J.* Conjugate algebraic numbers on conics // Acta arithm. – 1982. – **40**. – P. 333 – 346.
4. *Smyth C. J.* Additive and multiplicative relations connecting conjugate algebraic numbers // J. Number Theory. – 1986. – **23**. – P. 243 – 254.
5. *Girstmair K.* Linear dependence of zeros of polynomials and construction of primitive elements // Manuscr. math. – 1982. – **39**. – P. 81 – 97.
6. *Girstmair K.* Linear relations between roots of polynomials // Acta arithm. – 1999. – **89**. – P. 53 – 96.
7. *Dixon J. D.* Polynomials with nontrivial relations between their roots // Ibid. – 1997. – **82**. – P. 293 – 302.
8. *Drmota M., Skalba M.* Relations between polynomial roots // Ibid. – 1995. – **71**. – P. 65 – 77.
9. *Baron G., Drmota M., Skalba M.* Polynomial relations between polynomial roots // J. Algebra. – 1995. – **177**. – P. 827 – 846.
10. *Dubickas A.* On the degree of a linear form in conjugates of an algebraic number // Ill. J. Math. – 2002. – **46**. – P. 571 – 585.
11. *Matveev E. M.* On linear and multiplicative relations // Rus. Acad. Sci. Sb. Math. (Mat. Sbornik). – 1994. – **78**. – P. 411 – 425.
12. *Dubickas A.* On numbers which are differences of two conjugates of an algebraic integer // Bull. Austral. Math. Soc. – 2002. – **65** – P. 439 – 447.
13. *Zaimi T.* On numbers which are differences of two conjugates over Q of an algebraic integer // Ibid. – 2003. – **68**. – P. 233 – 242.
14. *Zaimi T.* On the integer form of the Additive Hilbert's Theorem 90 // J. Linear Algebra and Appl. – 2004. – **390**. – P. 175 – 181.
15. *Zaimi T.* The cubics which are differences of two conjugates of an algebraic integer // J. Théor. Nombres Bordeaux. – 2005. – **17**. – P. 949 – 953.
16. *Dubickas A., Smyth C. J.* Variations on the theme of Hilbert's Theorem 90 // Glasgow Math. J. – 2002. – **44**. – P. 435 – 441.
17. *Hilbert D.* Die Theorie der algebraischen Zahlkörper // Jahresber. Deutsch. Math. Ver. – 1897. – **4**. – S. 175 – 546. (Engl. transl.: *Adamson I. T.* The theory of algebraic number fields. – Berlin: Springer, 1998.)
18. *Lang S.* Algebra. – Addison-Wesley, Reading, Mass., 1971.
19. *Hurlimann W.* A cyclotomic Hilbert 90 theorem // Arch. math. – 1984. – **43**. – P. 25 – 26.
20. *Lam T. Y., Leroy A.* Hilbert 90 theorems over division rings // Trans. Amer. Math. Soc. – 1994. – **345**. – P. 595 – 622.

Received 31.01.2005