Illinois Journal of Mathematics
Volume 46, Number 2, Summer 2002, Pages 571–585
S 0019-2082

ON THE DEGREE OF A LINEAR FORM IN CONJUGATES OF AN ALGEBRAIC NUMBER

ARTURAS DUBICKAS

Abstract. We investigate the connection between the degree of an algebraic number over a field of characteristic zero and the degree of a linear form in its conjugates. Special attention is given to the case of linear forms in two distinct conjugates. In the process, we show that certain relations with dominant term are impossible, generalizing a result obtained by Smyth for the field of rational numbers. We also prove analogous multiplicative results. As an application, we describe algebraic numbers of prime degree which can be expressed as sums of two distinct conjugates of an algebraic number of the same degree.

1. Introduction

Unless stated otherwise, K denotes an arbitrary field of characteristic 0 and $U(K)$ its multiplicative group of roots of unity. Assume that α is an algebraic number of degree d over the field K with conjugates $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d$, and let $G = G(\alpha)$ be the Galois group of $K(\alpha_1, \dots, \alpha_d)/K$.

The aim of this paper is to investigate which degrees over K the linear form $k_1\alpha_1 + \cdots + k_d\alpha_d$ can take, under some restrictions on the coefficients $k_1, \dots, k_d \in K$, and especially on d. We also consider multiplicative forms $\alpha_1^{q_1} \dots \alpha_d^{q_d}$, where $q_1, \dots, q_d \in \mathbb{Z}$.

Throughout this paper, $\mathbb{Z}$ and $\mathbb{Q}$ denote, respectively, the ring of integers and the field of rational numbers. We use the same notation $\mathbb{Q}$ to denote the subfield of K which is isomorphic to the field of rational numbers.

Note that the problem of representing zero or, equivalently (see the Remark in [8] or Section 4 below), an element of K, by the linear form $k_1\alpha_1 + \cdots + k_d\alpha_d$ is, in fact, a question of the above type for degree 1. In order to avoid confusion (in Theorem 1, for instance), zero is also assumed to be of degree 1 over K. Earlier, Kurbatov [13] (see also his earlier papers [11] and [12]), Smyth [16], Girstmair [7][8], Drmota and Skalba [3][4] (see also their paper with Baron [1]), and Dixon [2] investigated various aspects of this problem,

Received September 14, 2001; received in final form December 7, 2001.
2000 *Mathematics Subject Classification.* Primary 11R04. Secondary 11R09, 12E05.

and also the question whether 1 can be represented by the corresponding multiplicative form $\alpha_1^{q_1} \dots \alpha_d^{q_d}$. The author and Smyth [6] gave necessary and sufficient conditions on a number to be expressible as $\alpha - \alpha'$ (or as α/α') with conjugate algebraic numbers α and α'.

This paper is organized as follows. In Section 2 we state our results for additive forms. Their multiplicative analogues are stated in Section 3. In Section 4 we prove Theorems 4 and 4′. The remaining proofs are given in Section 5. In the final section we show that every algebraic number whose degree over K is not a power of 2 can be expressed as the sum of two distinct algebraic numbers conjugate over K. For the case $K = \mathbb{Q}$ we investigate how small the degree of α can be if the sum of its two distinct conjugates is of some fixed prime degree over $\mathbb{Q}$.

2. Additive forms

Apparently, Kurbatov [13] was the first author to show that for certain fields K, including $K = \mathbb{Q}$, the equation $k_1\alpha_1 + \dots + k_d\alpha_d = 0$ with d prime can only hold if $k_1 = \dots = k_d$. This result was also obtained as a corollary in [3], [7], [8] and [10], and it is contained in the following theorem which shows that the degree of a linear form is divisible by d unless all d of its coefficients are equal. Recall that throughout K is a field of characteristic 0, and *all* elements of K are of degree 1 over K.

THEOREM 1. *Let α be an algebraic number of prime degree d over K. If the polynomial $x^{d-1} + \dots + x + 1$ is irreducible over K, then for $k_1, \dots, k_d \in K$ not all equal the degree of the linear form $k_1\alpha_1 + \dots + k_d\alpha_d$ over K is divisible by d.*

Clearly, for $d = 2$ the polynomial $x + 1$ is irreducible over every field K, and for $d = 3$ the polynomial $x^2 + x + 1$ is irreducible over K if $x^2 + 3$ is irreducible. Note that if d is composite, say $d = s\ell$ with integers $s, \ell > 1$, then, defining α as a root of an irreducible polynomial of ℓth degree at x^s, we have the nontrivial relation $\alpha_1 + \dots + \alpha_s = 0$. Our next theorem describes the situation when the degree of a linear form in two distinct conjugates is small.

THEOREM 2. *Suppose that α is an algebraic number of degree d over K. Let D be the degree of $\alpha + k\alpha'$ over K, where $\alpha \neq \alpha'$ are conjugate over K and $k \in K$. If $D! < d$, then $k \in U(K)$.*

Note that the inequality $D! < d$ cannot be weakened. Indeed, let β be of degree D over K with the Galois group of $K(\beta_1, \dots, \beta_D)/K$ the full symmetric group on D symbols S_D, where $\beta_1, \dots, \beta_D$ is the full set of conjugates of $\beta = \beta_1$ over K. Setting

$$\alpha = \beta_1 + m\beta_2 + \dots + m^{D-2}\beta_{D-1} + m^{D-1}\beta_D,$$

where $m > 1$ is a positive integer, we see that $\alpha + k\sigma(\alpha) = (1 - m^D)\beta$ is of degree D over K with $k = -m \notin U(K)$, where σ is the $D-$cycle $(\beta_1, \beta_2, \ldots, \beta_D) \to (\beta_2, \beta_3, \ldots, \beta_1)$. If, in addition, m is such that none of the $D!(D! - 1)$ nonzero polynomials

$$(\beta_{\tau(D)} - \beta_{\tau'(D)})z^{D-1} + \cdots + (\beta_{\tau(2)} - \beta_{\tau'(2)})z + (\beta_{\tau(1)} - \beta_{\tau'(1)})$$

vanishes at m, where $\tau \neq \tau'$ both are in S_D, then $\alpha \neq \sigma(\alpha)$ and α is of degree $d = D!$ over K.

Let $\alpha \neq \alpha'$ be conjugate over K. If $\alpha + l\alpha' = l'$, where $l, l' \in \mathbb{Q} \subset K$, then, by Theorem 2, $l \in U(K) \cap \mathbb{Q} \subset \{1, -1\}$. The case $l = -1$, i.e., $\alpha - \alpha' = l' \neq 0$ is impossible (see [6]). It follows that $l = 1$, in which case the degree of α over K must be even. (A simple proof of this last statement will be given in Section 5.)

COROLLARY 1. *Let α and α' be distinct algebraic numbers conjugate over K. If α, α' and 1 are linearly dependent over $\mathbb{Q}$, then $\alpha + \alpha' \in \mathbb{Q}$, and the degree of α over K is even.*

Let (a, b) denote the greatest common divisor of two integers a and b. The next result gives a useful lower bound for the degree of the sum, the product, the difference, and the quotient of two algebraic numbers. (The definition of a torsion–free algebraic number over K will be given in the next section.)

PROPOSITION 1. *Assume that the sum of three algebraic numbers of degree d_1, d_2, and d_3 over K is equal to 0 (or that the numbers are torsion–free over K and their product is equal to 1). Then either at most one number in the set $\{(d_1, d_2), (d_1, d_3), (d_2, d_3)\}$ is equal to 1, or at least one number in the set $\{d_1, d_2, d_3\}$ is equal to 1, and the other two are equal.*

On applying the proposition to $\alpha + k\alpha'$, where $k \in K$ is nonzero and α, α' are conjugate over K (so that $d_1 = d_2 = d$), we easily get the following. If the degree of $\alpha + k\alpha'$ over K, say $D = d_3$, is prime, then we have the first possibility, so D divides d. Also, if D is a (positive integer) power of 2, then d is even. In the case $k = 1$ the last statement can be strengthened as follows.

THEOREM 3. *If the degree of $\alpha + \alpha'$ over K, where $\alpha \neq \alpha'$ are conjugate over K, is a power of 2, then the degree of α over K is divisible by 4.*

Let $\alpha_1, \ldots, \alpha_n$, where $n \leqslant d$, be some distinct conjugates of α over K. For the proof of Theorem 3 we shall need the following result which shows that a linear relation with dominant term is impossible. This result generalizes Lemma 1(a) of Smyth's paper [15] and Corollary 2 in his paper [16], which give partial results for the case $K = \mathbb{Q}$. Since in our context K is an arbitrary field of characteristic 0, the argument of [15], which is based on mapping α_1 to

the conjugate of largest modulus, can no longer be used. The main difficulty in our proof is to find an alternative to this argument.

THEOREM 4. *Suppose that $\alpha_1, \alpha_2, \dots, \alpha_n$, where $n \geqslant 3$, are distinct algebraic numbers conjugate over K. If $q_1, q_2, \dots, q_n \in \mathbb{Q}$ are nonzero numbers such that $|q_1| \geqslant |q_2| + \cdots + |q_n|$, then*

$$q_1\alpha_1 + q_2\alpha_2 + \cdots + q_n\alpha_n \notin K.$$

REMARK. As we shall see in the proof, Theorem 4 holds under weaker assumptions, namely with $\mathbb{Q}$ replaced by any subfield R of real numbers such that K contains a subfield isomorphic to R.

How far can Theorem 4 be generalized? Assume that K is a subfield of the field of complex numbers. With this additional condition on K it is clear that

$$k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n \notin K$$

for all $k_1, \dots, k_n \in K$ such that $|k_1| > |k_2| + \cdots + |k_n|$. (As in the proof of Theorem 4, it is sufficient to show that $k_1\alpha_1 + \cdots + k_n\alpha_n \neq 0$, which follows by mapping α_1 to the conjugate with the largest absolute value.) If $|k_1| = |k_2| + \cdots + |k_n|$, this is in general false, but it is true for real $k_1, \dots, k_n$ (see the above remark).

COROLLARY 2. *Given a subfield of the complex numbers K, suppose that $\alpha_1, \dots, \alpha_n$, where $n \geqslant 3$, are distinct algebraic numbers conjugate over K. If $k_1, k_2, \dots, k_n \in K$ are nonzero real numbers such that $|k_1| \geqslant |k_2| + \cdots + |k_n|$, then*

$$k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n \notin K.$$

We cannot omit the condition that $k_1, \dots, k_n$ are real, as the following example shows. Take $K = \mathbb{Q}(\sqrt{-3})$, and let $\alpha_1, \alpha_2, \alpha_3$ be $2^{1/3}, 2^{1/3}\varepsilon, 2^{1/3}\varepsilon^2$, respectively, where $2^{1/3}$ is real and ε is a complex number satisfying $\varepsilon^3 = 1$. Set $k_1 = 2, k_2 = -\varepsilon^2, k_3 = -\varepsilon$. Then

$$k_1\alpha_1 + k_2\alpha_2 + k_3\alpha_3 = 2^{1/3}(2 - \varepsilon^3 - \varepsilon^3) = 0.$$

This example also shows that Corollary 1 is false if $\mathbb{Q}$ is replaced by $\mathbb{Q}(\sqrt{-3})$, because $\alpha_2 - \varepsilon\alpha_1 = 0$, whereas α is of odd degree 3 over K if, say, K itself is $\mathbb{Q}(\sqrt{-3})$.

3. Multiplicative forms in torsion–free algebraic numbers

In order to avoid the situation when some powers of two distinct conjugates of α are equal we need an additional condition on α. In [8], where the problem of linear relations in conjugates was reformulated in terms of pairs of groups, a similar problem was to avoid torsion elements. We say, for brevity, that an algebraic number α over K is *torsion–free* if none of the ratios α_i/α_j with

$1 \leqslant i \neq j \leqslant d$ is a root of unity. We have the following multiplicative analogues of the above statements for torsion–free algebraic numbers.

THEOREM 1′. *Let α be a torsion–free algebraic number of prime degree d over K. Then for $q_1, \dots, q_d \in \mathbb{Z}$ not all equal the degree of $\alpha_1^{q_1} \dots \alpha_d^{q_d}$ over K is divisible by d.*

THEOREM 2′. *Suppose that α is a torsion–free algebraic number of degree d over K. Let D be the degree of $\alpha^r \alpha'^q$ over K, where $\alpha \neq \alpha'$ are conjugate over K and $r, q \in \mathbb{Z}$. If $D! < d$, then $r = \pm q$.*

COROLLARY 1′. *Let α and α' be distinct torsion–free algebraic numbers conjugate over K. If $\alpha^r \alpha'^q \in \mathbb{Q}$ with nonzero $r, q \in \mathbb{Z}$, then $(\alpha\alpha')^r \in \mathbb{Q}$, and the degree of α over K is even.*

THEOREM 3′. *If the degree of $\alpha\alpha'$ over K, where α is torsion–free and $\alpha \neq \alpha'$ are conjugate over K, is a power of 2, then the degree of α over K is divisible by 4.*

For the proof of Theorem 3′ we shall need the following generalization of Lemma 1(b) in [15] and Corollary 2 in [16]. (In the proof of Theorem 4′ we use Theorem 2′.)

THEOREM 4′. *Let $\alpha_1, \alpha_2, \dots, \alpha_n$, where $n \geqslant 3$, be distinct torsion–free algebraic numbers conjugate over K. If $q_1, q_2, \dots, q_n \in \mathbb{Z}$ are all nonzero and $|q_1| \geqslant |q_2| + \dots + |q_n|$, then*

$$\alpha_1^{q_1} \alpha_2^{q_2} \dots \alpha_n^{q_n} \notin K.$$

Without any condition on α none of the above theorems remains true since examples in which α is a root of unity can be easily constructed. For instance, $\alpha = \beta_1 \beta_2^m \dots \beta_D^{m^{D-1}}$ with $\alpha\sigma(\alpha)^{-m} = \beta^{1-m^D}$ is an example showing that the inequality $D! < d$ in Theorem 2′ cannot be weakened.

Equivalently, α is torsion–free if and only if, for every nonzero integer m, the degree of α^m over K is equal to the degree of α over K. The next result shows that an algebraic number α over $\mathbb{Q}$ is torsion–free if this condition holds for $2 \leqslant m \leqslant (e^\gamma + o(1))d^2 \log\log d$, where the term $o(1)$ tends to 0 as $d \to \infty$ and γ is Euler's constant.

PROPOSITION 2. *Let α be an algebraic number of degree $d \geqslant 3$ over $\mathbb{Q}$. There is a positive constant c such that if the degree of α^m over $\mathbb{Q}$ equals d for every integer m in the range $2 \leqslant m < cd^2 \log\log d$, then α is torsion–free. Moreover, the above holds with $c = 1.7811$ for all sufficiently large d.*

The proof of Proposition 2 is based on the trivial inequality $\deg(\alpha/\alpha') \leqslant d(d-1)$, where α and α' are conjugate algebraic numbers of degree d over $\mathbb{Q}$.

It would be of interest to see whether this inequality can be replaced by the inequality $\deg(\alpha/\alpha') \leqslant d$ provided that α/α' is a root of unity. If so, then the bound $cd^2 \log\log d$ in the proposition could be replaced by $cd \log\log d$.

4. Forms with dominant term

Proof of Theorem 4. Let $q_1, \dots, q_n \in R \subset K$, where R is a subfield of the real numbers. Assume that

$$q_1\alpha_1 + q_2\alpha_2 + \cdots + q_n\alpha_n = k \in K.$$

Note that there is no loss of generality in assuming that $k = 0$. Indeed, if $q_1 + q_2 + \cdots + q_n = 0$, then applying all automorphisms of the Galois group to this equation and summing the resulting equations we obtain $0 = (q_1 + \cdots + q_n)\mathrm{Trace}(\alpha) = k|G|$ with $G = G(\alpha)$, which implies $k = 0$. (Throughout this paper, the notation $|\quad|$ is used for the number of elements of a *set* and for the modulus of a complex *number*. Also, $\mathrm{Trace}(\alpha) = \alpha_1 + \cdots + \alpha_d$ denotes the trace of α over K.) If, on the other hand, $q = q_1 + q_2 + \cdots + q_n \neq 0$, then on replacing α_1 by $\alpha_1 - k/q$ the right–hand side becomes 0.

On applying all $|G|$ automorphisms $\sigma \in G$ to the equation

$$q_1\alpha_1 + q_2\alpha_2 + \cdots + q_n\alpha_n = 0$$

we obtain a linear homogeneous system in d unknowns $\alpha_1, \dots, \alpha_n, \dots, \alpha_d$. The coefficients in each equation are the numbers $q_1, \dots, q_n$, and $d - n$ zeros. Let $A = (a_{ij})$ be the matrix associated to this system, consisting of $|G|$ rows and d columns. Suppose that I is a subset of $\{1, \dots, |G|\}$ and J is a subset of $\{1, \dots, d\}$. We denote by $A(I, J)$ the submatrix of A obtained as the intersection of rows with indices in I and columns with indices in J. Also, for brevity, we let $J^* = \{1, \dots, d\} \setminus J$. We claim that either A has rank equal to d (in which case $\alpha_1 = \cdots = \alpha_d = 0$ is the only solution and we are finished), or there exist I and J such that $|I| \geqslant |J| \geqslant 3$, the rank of $A(I, J)$ is at least $|J| - 1$, and the elements of $A(I, J^*)$ are all equal to zero.

There is nothing to prove if the rank of A equals d. Assume that this rank is smaller than d. Then there is a linear relation between the columns $\mathbf{c}_1, \dots, \mathbf{c}_d$ of A,

$$u_1\mathbf{c}_1 + \cdots + u_d\mathbf{c}_d = 0,$$

with real numbers $u_1, \dots, u_d$. Without loss of generality we may assume that u_1 is positive and $u_1 \geqslant |u_i|$ for every $i \leqslant d$. We start by setting $J = \{1\}$ and letting I be the set of all indices i such that $a_{i1} = q_1$. At this stage, we have $|I| \geqslant |J| \geqslant 1$. From the equations

$$u_1q_1 + u_2a_{i2} + \cdots + u_da_{id} = 0,$$

where $i \in I$ and $\{a_{i2}, \dots, a_{id}\} = \{q_2, \dots, q_n, 0, \dots, 0\}$, we deduce that, firstly,

$$\varepsilon_1 q_1 = \varepsilon_2 q_2 + \cdots + \varepsilon_n q_n,$$

where ε_s is the sign of q_s, and, secondly, $u_\ell = -\varepsilon_s u_1/\varepsilon_1$ for every $\ell > 1$ such that $a_{i\ell} = q_s$ for at least one $i \in I$ and at least one $s > 1$. This associates a plus sign or a minus sign to each column which belongs to I. Also, it is easily seen that the rank of A equals d if $|q_1| > |q_2| + \cdots + |q_n|$.

We now enlarge J (without changing the notation) by adding all these indices ℓ, and we enlarge I by adding all indices i such that $a_{ij} = q_1$ for at least one $j \in J$. The new sets I and J then satisfy $|I| \geqslant |J| \geqslant n$. Given $j \in J$, from the equations

$$u_1 a_{i1} + \cdots + u_j q_1 + \cdots + u_d a_{id} = 0,$$

where $i \in I$, we deduce that $u_\ell = -\varepsilon_s u_j/\varepsilon_1$ for every $\ell \notin J$ such that $a_{i\ell} = q_s$ for at least one $i \in I$ and for at least one $s > 1$. (We may get a contradiction if the sign associated to the same column by two different rows happens to be different, i.e., if for some ℓ, $u_\ell = u_1$ and, at the same time, $u_\ell = -u_1$. But in this case the rank of A equals d, which is impossible by our assumption.)

We again increase J (without changing notations) by adding all these new indices ℓ, and increase I as above, and so on. Since $|J| \leqslant d$, this process will terminate after finitely many steps. This happens as soon as we get a pair I, J such that in the matrix $A(I, J^*)$ no nonzero elements are left. Then all elements u_j with $j \in J$ are equal to $\pm u_1$, and every column of $A(I, J)$, except possibly the first, contains some q_s with $s > 1$. (Here, the value of s may be different for different columns.) Then the columns of the matrix $A(I, J')$, where $A(I, J')$ is obtained from $A(I, J)$ by removing an arbitrary column other than the first, are linearly independent. Indeed, suppose this were not the case, and assume the column which contains q_ℓ, where $\ell > 1$, is removed. Then, on dividing by u_1, we would have the relation

$$q_1 = \pm q_2 \pm \cdots \pm q_{\ell-1} \pm q_{\ell+1} \pm \cdots \pm q_n,$$

which is impossible. It follows that the rank of $A(I, J')$ is equal to $|J'| = |J| - 1$. Thus the rank of $A(I, J)$ is at least $|J| - 1$ as claimed.

From now on, it suffices to consider those conjugates of α_1 with indices in J, and we can ignore conjugates with indices in J^*. The homogeneous linear system in $|J|$ unknowns has a nonzero solution only if the rank of $A(I, J)$ is strictly smaller than $|J|$. By the above remark, in this case the rank must be equal to $|J| - 1$. Without loss of generality, we assume that the columns of $A(I, J')$, where now $A(I, J')$ is the matrix obtained from $A(I, J)$ by removing the *first* column, are linearly independent. On dividing by α_1, we obtain a nonhomogeneous linear system in $|J| - 1$ unknowns with coefficients in R. This system has a unique real solution. In particular, if, for example, $2, 3 \in J$, then $\alpha_2/\alpha_1 = r_1$ and $\alpha_3/\alpha_1 = r_2$ with $r_1, r_2 \in R \subset K$.

It follows easily that $\alpha_2 = -\alpha_1$. Indeed, assume that $\alpha_2 = \sigma(\alpha_1)$, where $\sigma \in G$ is of order m. Multiplying all equations $\sigma^j(\alpha_1) = r_1 \sigma^{j-1}(\alpha_1)$, $j = 1, \ldots, m$, and then dividing by $\alpha_1 \sigma(\alpha_1) \ldots \sigma^{m-1}(\alpha_1)$, we obtain $r_1^m = 1$. Since

$r_1 \in R$ and $r_1 \neq 1$, we must have $r_1 = -1$. Thus, $\alpha_2 = -\alpha_1$. Analogously, $\alpha_3 = -\alpha_1$, and so $\alpha_3 = \alpha_2$, which is a contradiction. □

Proof of Theorem 4′. Let

$$\alpha_1^{q_1}\alpha_2^{q_2}\dots\alpha_n^{q_n} = k \in K$$

with nonzero $q_1, q_2, \dots, q_n \in \mathbb{Z}$. There is no loss of generality in assuming that $k = 1$. Indeed, if $q_1 + q_2 + \dots + q_n = 0$, then we apply all automorphisms of the Galois group and multiply the resulting equations. This gives $1 = k^{|G|}$, and thus k is a root of unity. Replacing α_1 by its $|G|-$th power, which is torsion–free, results in replacing k by 1 on the right–hand side. If $s = q_1 + q_2 + \dots + q_n \neq 0$, then replacing α_1 by α_1^s/k reduces the problem to the case $k = 1$.

On applying all $|G|$ automorphisms $\sigma \in G$ to the equation

$$\alpha_1^{q_1}\alpha_2^{q_2}\dots\alpha_n^{q_n} = 1$$

we obtain a system of $|G|$ equations in d unknowns. This system has a solution with at least one $\alpha_j \neq 1$ if and only if the associated linear homogeneous system in unknowns $z_1, \dots, z_n, \dots, z_d$ has a nonzero solution. (Here, for convenience, one can take formal logarithms $z_i = \log \alpha_i$, and then take formal exponentials in order to change back to the multiplicative setting.) As above, the coefficients in each equation are $q_1, \dots, q_n$ and $d - n$ zeros. Analogously, the rank of the associated matrix A must be smaller than d. As above, this can only happen if

$$|q_1| = |q_2| + \dots + |q_n|$$

and, say, $z_2/z_1, z_3/z_1 \in \mathbb{Q}$.

We thus deduce that $\alpha_2^r\alpha_1^q = 1$ and $\alpha_3^\ell\alpha_1^s = 1$ with integers $r > 0, \ell > 0, q$ and s. By Theorem 2′ (whose proof will be given in the next section) it follows that $r = \pm q$ and $\ell = \pm s$. But $r \neq -q$ because α_1 is torsion–free. Similarly, $\ell \neq -s$. Therefore, $r = q$ and $\ell = s$. From $(\alpha_1\alpha_2)^r = (\alpha_1\alpha_3)^\ell = 1$ we deduce that $\alpha_2^r\alpha_3^{-\ell} = 1$. Thus, as above, we conclude that $r = -\ell$. From $(\alpha_1\alpha_2)^{-\ell} = (\alpha_1\alpha_3)^\ell = 1$ we see that $\alpha_2^\ell = \alpha_3^\ell$, which is a contradiction. □

5. Other proofs

Proof of Theorem 1. Since d is a prime, in the Galois group $G = G(\alpha)$ there is a $d-$cycle. Without loss of generality we can assume that this $d-$cycle is $\sigma : (\alpha_1, \alpha_2, \dots, \alpha_d) \to (\alpha_2, \alpha_3, \dots, \alpha_1)$. Setting $k_1\alpha_1 + k_2\alpha_2 + \dots + k_d\alpha_d = \beta$, we obtain

$$(k_1 - k_d + 1)\alpha_1 + (k_2 - k_1 + 1)\alpha_2 + \dots + (k_d - k_{d-1} + 1)\alpha_d = \beta - \sigma(\beta) + \mathrm{Trace}(\alpha).$$

Without changing the notation we write $(k_1, k_2, \dots, k_d)$ for $(k_1 - k_d + 1, k_2 - k_1 + 1, \dots, k_d - k_{d-1} + 1)$. Note that the elements k_i are not all equal and their

sum is equal to d. Thus $k_1 + \cdots + k_d \neq 0$. On applying the d automorphisms, $1, \sigma, \sigma^2, ..., \sigma^{d-1}$, we obtain the linear system

$$M(\alpha_1, \alpha_2, \ldots, \alpha_d)^T = (\gamma, \sigma(\gamma), \ldots, \sigma^{d-1}(\gamma))^T,$$

where T denotes the transpose, $\gamma = \beta - \sigma(\beta) + \mathrm{Trace}(\alpha)$, and M is the $d \times d$ matrix whose rows are $(k_1, k_2, \ldots, k_d)$, $(k_d, k_1, \ldots, k_{d-1})$, $\ldots$, $(k_2, k_3, \ldots, k_1)$. The determinant of this matrix is called a *circulant*. It is a standard exercise to show that the circulant is given by

$$\det M = \prod_{s=0}^{d-1} \left(k_1 + k_2\omega^s + k_3\omega^{2s} + \cdots + k_d\omega^{(d-1)s} \right),$$

where $\omega = \exp(2\pi\sqrt{-1}/d)$ is the primitive dth root of unity. (See, e.g., Problem 479 in [14], where this formula is easily obtained by multiplying $\det M$ with the Vandermonde determinant $||\omega^{ij}||_{0 \leqslant i,j \leqslant d-1}$.) By the assumption on the field K, none of the factors $k_1 + k_2\omega^s + \cdots + k_d\omega^{(d-1)s}$ with $s > 0$ is equal to zero, for otherwise the nonzero polynomial $(k_1 - k_d) + \cdots + (k_{d-1} - k_d)x^{d-2}$ vanishes at ω^s. It follows that $\det M \neq 0$.

Let L be the Galois closure of $K(\beta)$ over K. The order of the Galois group $\mathrm{Gal}(L/K)$ is divisible by d, because this group contains G as a subgroup. On the other hand, by the main theorem of Galois theory, this order is also equal to $|H|[K(\beta) : K]$, where

$$H = \{\tau \in \mathrm{Gal}(L/K) \mid \tau(x) = x \text{ for every } x \in K(\beta)\}.$$

It suffices to show that d does not divide $|H|$. Assume, to the contrary, that d divides $|H|$. Since d is prime, H, which acts as a permutation group of $\alpha_1, \ldots, \alpha_d$, contains a $d-$cycle. Therefore $\sigma \in H$, and $\sigma(\beta) = \beta$. It follows that $\gamma = \mathrm{Trace}(\alpha) \in K$, so that $\alpha_1, \ldots, \alpha_d$ all belong to K. This is impossible because $d \geqslant 2$. □

Proof of Theorem 1′. Starting from $\alpha_1^{q_1} \ldots \alpha_d^{q_d} = \beta$ and arguing as in the proof of Theorem 1 (defining the new $(q_1, \ldots, q_d)$ as $(q_1 - q_d + 1, \ldots, q_d - q_{d-1} + 1)$ and letting $\gamma = \beta\alpha_1 \ldots \alpha_d/\sigma(\beta)$), we obtain that a nonzero integer power of α belongs to K, which is impossible because α is torsion–free. (The polynomial $q_1 + q_2x + \cdots + q_dx^{d-1}$ is equal to zero at $\omega^s \neq 1$ only if $q_1, \ldots, q_d$ are all equal. The fact that the polynomial beongs to $\mathbb{Q}(x)$ allows us to remove the extra condition that is present in the additive case.) □

Proof of Theorem 2. Let σ be an automorphism of the normal extension of $K(\alpha)$ over K which maps α to α'. Assume that the order of σ is equal to m, so that $\sigma^0(\alpha) = \sigma^m(\alpha) = \alpha$. Set $\alpha + k\alpha' = \beta$. On adding the m equations $\sigma^{j-1}(\alpha) + k\sigma^j(\alpha) = \sigma^{j-1}(\beta)$, $j = 1, 2, \ldots, m$, with weights $(-k)^{j-1}$, we obtain

$$\alpha(1 - (-k)^m) = \sum_{j=1}^{m} (-k)^{j-1}\sigma^{j-1}(\beta).$$

The right–hand side here is of degree at most $D! < d$, whereas the left–hand side is of degree d over K, unless it is equal to 0. It follows that $(-k)^m = 1$. Consequently, $-k$ is a root of unity, and hence so is k. Since $k \in K$, we deduce that $k \in U(K)$. □

Proof of Theorem 2′. Let again $\alpha' = \sigma(\alpha)$, where $\sigma \in G$ is of order m. Starting from $\alpha^r(\sigma(\alpha))^q = \beta$, we apply σ^{j-1} with $j = 1, \dots, m$ and then multiply all equations

$$\left(\sigma^{j-1}(\alpha)\right)^{r^{m-j+1}(-q)^{j-1}} \left(\sigma^j(\alpha)\right)^{-r^{m-j}(-q)^j} = \left(\sigma^{j-1}(\beta)\right)^{r^{m-j}(-q)^{j-1}},$$

where $j = 1, \dots, m$. The left–hand side of the product is equal to $\alpha^{r^m-(-q)^m}$ and of degree at most $D! < d$. Since α is torsion–free, this is only possible if $r^m = (-q)^m$. Thus, $r = \pm q$ is the only possibility. □

Proof of Corollary 1. Assume that the degree of α over K is odd, say, $2m + 1$. Consider all distinct sets $\{\sigma(\alpha), \sigma(\alpha')\}$, where σ runs over every element of G. There are at least $m + 1$ such sets, since m sets cover at most $2m$ conjugates, but the Galois group G is transitive. Hence there are at least two sets having one joint element. This is impossible, because the sums of the two elements in each such set are all equal. □

Proof of Corollary 1′. By Theorem 2′, $r = \pm q$. Clearly, if $(\alpha/\alpha')^r = k \in \mathbb{Q}$, then by applying all automorphisms of G and taking the product, we obtain that $k^{|G|} = 1$. It follows that $k \in U(K) \cap \mathbb{Q} \in \{-1, 1\}$. In both cases, $\alpha^{2r} = (\alpha')^{2r}$, which is impossible because α is torsion–free. Consequently, $(\alpha\alpha')^r \in \mathbb{Q}$. As in the proof of Corollary 1, the degree of α^r over K is even, and since α is torsion–free, it is equal to the degree of α over K. □

Proof of Proposition 1. Assume that $\alpha + \beta + \gamma = 0$, where α, β and γ are algebraic numbers of degrees d_1, d_2 and d_3 over K, respectively, with $d_1 \geqslant d_2 \geqslant d_3$. Let L be the normal closure of $K(\alpha, \beta, \gamma)$ over K. Assume that there are N different vectors $\langle \alpha_i, \beta_j, \gamma_\ell \rangle$ such that $\alpha_i + \beta_j + \gamma_\ell = 0$ and $1 \leqslant i \leqslant d_1$, $1 \leqslant j \leqslant d_2$, $1 \leqslant \ell \leqslant d_3$. On applying the automorphisms of the Galois group of L/K which map α to its conjugates, we see that N is divisible by d_1. Similarly, N is divisible by d_2 and d_3. Write $N = m_1 d_1 = m_2 d_2 = m_3 d_3$. Note that $N \leqslant d_2 d_3$, because two vectors must differ in at least two positions. Thus $m_1 \leqslant d_2 d_3/d_1 \leqslant d_3$, $m_2 \leqslant d_3$ and $m_3 \leqslant d_2$.

Assume that $(d_1, d_3) = (d_2, d_3) = 1$. Then $m_3 = d_1 = d_2$, $m_1 = m_2 = d_3$. It follows that, given an arbitrary ℓ (say, $\ell = 1$), among the $N = d_2 d_3$ vectors there are d_2 vectors of the form $\langle \alpha_i, \beta_j, \gamma_1 \rangle$, where $1 \leqslant i, j \leqslant d_2$. Furthermore, the d_2 vectors $\langle \alpha_i, \beta_j \rangle$, without the component γ_1, differ in both positions. Thus, summing the corresponding equations we get $\mathrm{Trace}(\alpha) + \mathrm{Trace}(\beta) + d_2\gamma_1 = 0$. Hence $\gamma = \gamma_1 \in K$, so that $d_3 = 1$. Similarly, $(d_1, d_2) = (d_2, d_3) = 1$ implies that $m_2 = d_1 = d_3$, and thus $d_1 = d_2 = d_3$. Finally, from $(d_1, d_2) = (d_1, d_3) = 1$ we get $m_1 = d_2 = d_3$ and again $d_1 = d_2 = d_3$.

Replacing the sum by the product makes, of course, no difference in the above proof, except that the equation $\mathrm{Trace}(\alpha) + \mathrm{Trace}(\beta) + d_2\gamma_1 = 0$ is replaced by $\mathrm{Norm}(\alpha)\mathrm{Norm}(\beta)\gamma_1^{d_2} = 1$, where $\mathrm{Norm}(\alpha)$ is the product of all conjugates of α over K. Thus $\gamma_1^{d_2} \in K$. Because γ is torsion–free, this can only happen if $\gamma \in K$, so that $d_3 = 1$. □

Proof of Theorem 3. Let $\beta = \alpha + \alpha'$ be of degree D. Consider a graph Γ with d vertices, labeled by α and its conjugates. The edge of Γ connecting two vertices α_i and α_j is given the label $\ell \in \{1, \dots, D\}$ if $\beta_\ell = \alpha_i + \alpha_j$. Let f be the total number of edges labeled by ℓ, where ℓ is fixed. By mapping β to its conjugates, we see that the number f is independent of ℓ. Note that every vertex α has at most one edge with a given label incident to α, since $\alpha + \alpha' = \alpha + \alpha''$ implies that $\alpha' = \alpha''$. Consequently, given a vertex, there are at most D edges incident to it and labeled by one of the D numbers $\{1, \dots, D\}$. Suppose there are s such edges. (Again, by mapping α to its conjugates, we see that the number s is the same for every vertex.) By counting the number of labeled edges, we obtain the formula

$$2fD = sd,$$

where $s \leqslant D$.

For $D > 1$ we have $s < D$. Indeed, otherwise, on adding the $s = D$ equations corresponding to the vertex α, we obtain $\mathrm{Trace}(\beta) = D\alpha + S$, where S is the sum of D distinct conjugates of α, none of which is α itself. This is a contradiction to Theorem 4. If $D = 2^i$ with a positive integer i, then $2fD$ is divisible by 2^{i+1}, whereas $s < 2^i$. Since $d = 2fD/s$ we conclude that d is divisible by 4. □

Proof of Theorem 3′. This result follows as above by labeling the edges by $\beta_\ell = \alpha_i\alpha_j$ and using Theorem 4′ instead of Theorem 4 to show that $s < D$. □

Proof of Proposition 2. Assume that α is not torsion–free. Let m be the smallest positive integer such that $\deg \alpha^m < d$. There is a conjugate of α, $\alpha' \neq \alpha$, such that α/α' is the mth root of unity. It follows that $\phi(m) = \deg(\alpha/\alpha') \leqslant d(d-1)$, where ϕ is Euler's function. The result now follows from the relation

$$\liminf_{m\to\infty} \frac{\phi(m)\log\log m}{m} = e^{-\gamma},$$

where $\gamma = 0.577215\dots$ is Euler's constant (see Theorem 328 in [9]). □

6. Conjugate algebraic numbers whose sum is a given number

In this section we are interested in algebraic numbers over K that can be represented as sums of two distinct conjugates over K. Clearly, an algebraic number β can be expressed in this form if there exist fields E and F such that $[F : E] = 2$ and $K(\beta) \subset E \subset F \subset \overline{K}$, where $\overline{K}$ is the algebraic closure

of K. If $Q(x) = x^2 + ex + e'$ with $e, e' \in E$ is irreducible over E, then β is the sum of two zeros of the irreducible (over E) polynomial $Q(x - e/2 - \beta/2)$ with coefficients in E. These two zeros are conjugate over E and hence also over K. (See also Section 3 in [5], where we show that $\beta \neq 0$ is the product of two distinct conjugates over a number field.) On the other hand, if K is the field of real numbers and β is a complex number (so that β is of degree 2 over K), then β cannot be expressed as either a sum or a product of two distinct conjugates.

Let L be the Galois closure of $K(\beta)$ over K. We say that β is a *2–normal number* if the degree of β over K is a (nonnegative integer) power of 2 and $K(\beta) = L$. According to this definition, the elements of K are 2–normal numbers, but all algebraic numbers whose degree over K is not a power of 2 are certainly not 2–normal. The following result shows that an algebraic number whose degree over K is not a power of 2 can be expressed as the sum of two distinct conjugates.

THEOREM 5. *Let β be an algebraic number over K which is not a 2–normal number. Then there exist algebraic numbers $\alpha \neq \alpha'$ conjugate over K such that $\beta = \alpha + \alpha'$.*

Proof. Since $\beta \notin K$, we have $|\mathrm{Gal}(L/K)| > 1$. Assume first that $|\mathrm{Gal}(L/K)|$ is not a power of 2. Let $\sigma \in \mathrm{Gal}(L/K)$ be of odd prime order p. There is a conjugate of β, say β', such that $\sigma(\beta') \neq \beta'$, for otherwise σ maps every element of L to itself, which is a contradiction. If β' can be expressed as the sum of two distinct conjugates over K, then so can β (just map β' to β). Hence there is no loss of generality in assuming that β itself satisfies $\sigma(\beta) \neq \beta$.

Setting

$$\alpha = \sum_{i=0}^{p-1} (-1)^i (\sigma^i(\beta)/2) = \big(\beta - \sigma(\beta) + \cdots - \sigma^{p-2}(\beta) + \sigma^{p-1}(\beta)\big)/2,$$

we see that $\beta = \alpha + \sigma(\alpha)$. Furthermore, we have $\alpha \neq \sigma(\alpha)$, for otherwise, on applying σ^{-1} to the equation

$$\sigma(\beta) + \sigma^3(\beta) + \cdots + \sigma^{p-2}(\beta) = \sigma^2(\beta) + \sigma^4(\beta) + \cdots + \sigma^{p-1}(\beta),$$

we would have that $\sigma^{p-1}(\beta) = \beta$. Combining this with $\sigma^p(\beta) = \beta$ we deduce that $\sigma(\beta) = \beta$. This contradiction proves the result in the case $|\mathrm{Gal}(L/K)| \neq 2^n$.

Assume now that $|\mathrm{Gal}(L/K)| = 2^n$ with a positive integer n. Clearly, $[K(\beta) : K] = 2^m$. Furthermore, as β is 2–normal, $m < n$. By the Galois correspondence, there exists a subgroup H of order 2^{n-m} of $\mathrm{Gal}(L/K)$ corresponding to the field $K(\beta)$. The group H contains a subgroup H' of order 2^{n-m-1}. The fixed field of H', say F, is thus a quadratic extension of $K(\beta)$, and we can complete the proof as above with the pair $E = K(\beta)$, F. □

From now on, we assume for simplicity that $K = \mathbb{Q}$. Clearly, *every* algebraic number β over $\mathbb{Q}$ is equal to the sum of two *distinct* algebraic numbers α and α' conjugate over $\mathbb{Q}$. It suffices to take $\alpha = \beta/2 + \sqrt{p}$, where p is the prime number such that $\sqrt{p} \notin \mathbb{Q}(\beta_1, \ldots, \beta_D)$. Then α and $\alpha' = \beta/2 - \sqrt{p}$ are distinct conjugates of degree $2D$ over $\mathbb{Q}$ such that $\beta = \alpha + \alpha'$. What is the smallest possible value for the degree d of α in such a representation?

Let $d(\beta, \mathbb{Q})$ be the smallest possible value of d. The inequality $D \leqslant d(d-1)$ combined with the above example shows that $\sqrt{D} < d(\beta, \mathbb{Q}) \leqslant 2D$ for every β of degree D.

It is easy to see that for numbers β of degrees $D = 1, 2, 3$ we have $d(\beta, \mathbb{Q}) = 2, 4, 3$, respectively. Indeed, $d(\beta, \mathbb{Q}) = 2$ for every rational β, by the inequality $1 < d(\beta, \mathbb{Q}) \leqslant 2$. For $D = 2$, by Theorem 3, d is divisible by 4. Therefore, $d(\beta, \mathbb{Q}) = 4$ for every quadratic β. For a cubic β, $d(\beta, \mathbb{Q})$ is at least 3, by the remark following Proposition 1. On the other hand, as in Theorem 5, setting

$$\alpha = -\beta_2 + \mathrm{Trace}(\beta)/2$$

and mapping β_2 to β_3, we see that

$$\alpha + \alpha' = \mathrm{Trace}(\beta) - \beta_2 - \beta_3 = \beta_1 = \beta.$$

Consequently, for every cubic β, $d(\beta, \mathbb{Q}) = 3$, as claimed.

For β of degree $D > 3$ the answer depends not only on D, but also on the Galois group $G(\beta)$ of $\mathbb{Q}(\beta_1, \ldots, \beta_D)/\mathbb{Q}$ and on linear relations in conjugates of β. For example, for a quartic β, $d(\beta, \mathbb{Q})$ is divisible by 4 (see Theorem 3). If there is an α of degree 4 such that $\beta = \alpha + \alpha'$, then the formula $2fD = sd$ obtained in the proof of Theorem 3 with $D = d = 4$ gives the inequality $s = 2f < 4$. Thus $f = 1$ and the graph Γ is the 4−cycle, and so the linear relation $\beta_1 - \beta_2 + \beta_3 - \beta_4 = 0$ is a necessary condition for $d(\beta, \mathbb{Q}) = 4$ to hold. Such numbers β and α do exist. For example,

$$\beta = \sqrt{3 + \sqrt{2}} + \sqrt{3 - \sqrt{2}}$$

is the sum of two distinct conjugates of $\alpha = \sqrt{3 + \sqrt{2}} + \sqrt{2}$.

The next theorem describes all numbers β of odd prime degree $D = 2\ell + 1$ such that $d(\beta, \mathbb{Q}) = D$. Let $\sigma \in G(\beta)$ be the D−cycle $(\beta_1, \beta_2, \ldots, \beta_D) \to (\beta_2, \beta_3, \ldots, \beta_1)$, where $\beta = \beta_1$, and

$$t(\beta) = \beta + \sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{\ell-1}(\beta).$$

THEOREM 6. *Let β be an algebraic number of an odd prime degree D over $\mathbb{Q}$. Then $d(\beta, \mathbb{Q})$ is equal to D if the degree of $t(\beta)$ over $\mathbb{Q}$ is D, and equal to $2D$ otherwise.*

Note that the degree of $t(\beta)$ over $\mathbb{Q}$ is at least D, because the numbers $\sigma^i(t(\beta))$, $0 \leqslant i \leqslant 2\ell$, are all distinct, by Theorem 1. The degree of $t(\beta)$ over $\mathbb{Q}$ is equal to D if, for example, $G(\beta)$ is isomorphic to either the cyclic group

$\mathcal{C}_D$ of order D, or the dihedral group $\mathcal{D}_{2\ell+1}$ of order $2D = 4\ell + 2$ generated by the automorphisms σ of order $D = 2\ell+1$ and $\tau : (\beta_1, \beta_2, \dots, \beta_{D-1}, \beta_D) \to (\beta_D, \beta_{D-1}, \dots, \beta_2, \beta_1)$ of order 2.

For $D = 3$, we have that $t(\beta) = \beta$ is always of degree 3 since the Galois group of β is either $\mathcal{C}_3$ or $\mathcal{D}_3$. For other prime numbers $D > 3$, the degree of $t(\beta)$ can be greater than D, and usually this is the case. The Galois group $G(\beta)$ of a "generic" β is isomorphic to S_D. The degree of $t(\beta)$ for such β is equal to $(2\ell+1)!/\ell!(\ell+1)!$, which is clearly greater than $D = 2\ell+1$ for $\ell > 1$.

Proof of Theorem 6. Let $\beta = \alpha+\alpha'$ be of degree D over $\mathbb{Q}$, where $D = 2\ell+1$ is an odd prime. By the remark following Proposition 1, the degree of α over $\mathbb{Q}$ is divisible by D. Also, as was shown above, $d(\beta, \mathbb{Q}) \leqslant 2D$. Thus $d(\beta, \mathbb{Q})$ is either D or $2D$. Our task is to find all algebraic numbers β of degree D over $\mathbb{Q}$ for which there is an α of degree D over $\mathbb{Q}$ such that $\beta = \alpha + \alpha'$.

Consider the graph Γ constructed in the proof of Theorem 3. In the formula $2fD = sd$ we now have $D = d$. Since α is of prime degree, on applying Theorem 1 we see that different edges cannot have the same label. Hence $f = 1$, and the number of vertices is equal to the number of edges. It follows that every vertex is incident to exactly two edges. Consequently, the graph Γ is either the $D-$cycle, or a union of $s-$cycles. The latter case is impossible, because D is a prime. We thus deduce that the linear system $\sigma^j(\beta) = \sigma^j(\alpha) + \sigma^j(\alpha')$, $0 \leqslant j \leqslant 2\ell$, has a solution. Setting $\sigma^j(\alpha) = \alpha_{j+1}$ for $0 \leqslant j \leqslant 2\ell$, and $\alpha' = \alpha_{\ell+1}$, we obtain the linear system $\beta_1 = \alpha_1 + \alpha_{\ell+1}, \beta_2 = \alpha_2 + \alpha_{\ell+2}, \dots, \beta_{2\ell+1} = \alpha_{2\ell+1} + \alpha_\ell$. The unique solution of this system is

$$\alpha_j = \mathrm{Trace}(\beta)/2 - \sigma^j(t(\beta)),$$

where $j = 1, \dots, 2\ell + 1$. Clearly, $\alpha = \alpha_1$ is of degree D over $\mathbb{Q}$ if and only if so is $\sigma(t(\beta))$. The proof is now complete, since $\sigma(t(\beta))$ and $t(\beta)$ are conjugate over $\mathbb{Q}$ and thus of the same degree. □

Acknowledgements. I thank to Professor C.J. Smyth from whom I learned a lot while writing our paper [6] and during numerous e-mail exchanges afterwards. I also thank to Professor K. Girstmair for pointing out some relevant references. Comments by the referee allowed me to improve and strengthen some of the theorems. This research was partially supported by a grant from Lithuanian State Science and Studies Foundation.

References

[1] G. Baron, M. Drmota and M. Skalba, *Polynomial relations between polynomial roots,* J. Algebra **177** (1995), 827–846.

[2] J.D. Dixon, *Polynomials with nontrivial relations between their roots,* Acta Arith. **82** (1997), 293–302.

[3] M. Drmota and M. Skalba, *On multiplicative and linear dependence of polynomial roots,* Contributions to general algebra, 7 (Vienna, 1990), Teubner, Vienna, 1991, pp. 127–135.

[4] ———, *Relations between polynomial roots,* Acta Arith. **71** (1995), 65–77.
[5] A. Dubickas, *The Remak height for units,* Acta Math. Hung., to appear.
[6] A. Dubickas and C.J. Smyth, *Variations on the theme of Hilbert's Theorem 90,* Glasgow Math. J., to appear.
[7] K. Girstmair, *Linear dependence of zeros of polynomials and construction of primitive elements,* Manuscripta Math. **39** (1982), 81–97.
[8] ———, *Linear relations between roots of polynomials,* Acta Arith. **89** (1999), 53–96.
[9] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers,* Oxford University Press, Oxford, 1979.
[10] C.U. Jensen and N. Yui, *Polynomials with D_p as Galois group,* J. Number Theory **15** (1982), 347–375.
[11] V.A. Kurbatov, *On equations of prime degree,* Mat. Sb. N.S. **43(85)** (1957), 349–366.
[12] ———, *Linear dependence of conjugate elements,* Mat. Sb., N.S. **52(94)** (1960), 701–708.
[13] ———, *Galois extensions of prime degree and their primitive elements,* Soviet Math. (Iz. VUZ) **21** (1977), 49–52.
[14] I.V. Proskuriakov, *A collection of problems in linear algebra,* 6th ed., Nauka, Moscow, 1978.
[15] C.J. Smyth, *Conjugate algebraic numbers on conics,* Acta Arith. **40** (1982), 333–346.
[16] ———, *Additive and multiplicative relations connecting conjugate algebraic numbers,* J. Number Theory **23** (1986), 243–254.

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius 2600, Lithuania
E-mail address: arturas.dubickas@maf.vu.lt