ACTA ARITHMETICA
107.1 (2003)

Additive relations with conjugate algebraic numbers

by

Artūras Dubickas (Vilnius)

1. Introduction. Let K be a field of characteristic zero, unless stated otherwise. As usual, $\overline{K}$ denotes the algebraic closure of K and $K^* = K \setminus \{0\}$. There are two types of problems about additive relations in conjugates. A typical problem of the first type is to decide whether, for given $k_1, \ldots, k_n \in K$, the linear form $k_1\alpha_1 + \ldots + k_n\alpha_n$ vanishes with some non-zero $\alpha_1, \ldots \ldots, \alpha_n \in \overline{K}$ conjugate over K. This problem was studied earlier by C. J. Smyth [10], J. D. Dixon [2], K. Girstmair [6], [7], M. Drmota and M. Skałba [3] (see also [1] and [4]).

A problem of the second type can be stated as follows. Given a positive integer n and $k_1, \ldots, k_n \in K^*$, which $\beta \in \overline{K}$ can be written as

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

with $\alpha_1, \ldots, \alpha_n \in \overline{K}$ conjugate over K? We write $\mathcal{A}(K; k_1, \ldots, k_n)$ for the set of such numbers β. Here, there is no restriction on $\alpha = \alpha_1$ whose degree over K is not necessarily equal to n. (For instance, α may be zero.) We also do not assume that the conjugates of α over K, $\alpha_1, \ldots, \alpha_n$, are all distinct. Our purpose is to study the set $\mathcal{A}(K; k_1, \ldots, k_n)$. The structure of this set is non-trivial if $n \geq 2$ and $k_1 + \ldots + k_n = 0$. It is worth pointing out that under these conditions the set $\mathcal{A}(K; k_1, \ldots, k_n)$ is neither a linear space over K nor even an additive semigroup (see Corollary 2).

Given $\beta \in \overline{K}$, let throughout L be the Galois closure of $K(\beta)$ over K, and let G be the Galois group of L/K. In [5] the author and C. J. Smyth described the set $\mathcal{A}(K; 1, -1)$: an algebraic number β can be written as a difference $\alpha_1 - \alpha_2$ of algebraic numbers α_1, α_2 conjugate over K if and only if there is a $\sigma \in G$ such that $\sum_{j=0}^{v-1} \sigma^j(\beta) = 0$. (Here, v is the order of the cyclic group $\langle\sigma\rangle$ generated by σ.) Although the result is only stated for K being a number field, the proof remains the same for an arbitrary field of characteristic zero. We begin by observing that $\mathcal{A}(K; 1, -1)$ is contained in every other set $\mathcal{A}(K; k_1, \ldots, k_n)$.

2000 *Mathematics Subject Classification*: 11R04, 11R32, 11R80.

Proposition. *If n is a positive integer and $k_1, \dots, k_n \in K^*$, then $\mathcal{A}(K; 1, -1) \subset \mathcal{A}(K; k_1, \dots, k_n)$.*

Proof. Note that $\mathcal{A}(K; kk_1, \dots, kk_n) = \mathcal{A}(K; k_1, \dots, k_n)$ for every $k \in K^*$. Also, if $\sum_{j=1}^n k_j \neq 0$, then $\mathcal{A}(K; k_1, \dots, k_n) = \overline{K}$. Indeed, this follows immediately by setting $\alpha_1 = \dots = \alpha_n = \beta/(\sum_{j=1}^n k_j)$. For $\sum_{j=1}^n k_j = 0$, by taking $\alpha_2 = \dots = \alpha_n$, the Proposition follows easily.

2. Main results. For $\beta \in \overline{K}$, let $\mathcal{L}(\beta)$ be the linear space $\sum_{j=1}^d K\beta_j$ with $\beta_1, \dots, \beta_d$ being all d distinct conjugates of β over K. In other words, $\mathcal{L}(\beta)$ is the usual $K[G]$-module $K[G]\beta = \sum_{\sigma \in G} K\sigma(\beta)$. Here, $K[G]$ is the group ring whose elements are $\sum_{\sigma \in G} e_\sigma \sigma$, $e_\sigma \in K$ (see Section 1 of [7]). Our first theorem reduces the search for possible α.

Theorem 1. *Given $k_1, \dots, k_n \in K$, assume that β can be represented by the linear form $k_1\alpha_1 + \dots + k_n\alpha_n$ with $\alpha_1, \dots, \alpha_n \in \overline{K}$ conjugate to α over K. Then α can be chosen in $\mathcal{L}(\beta)$.*

Set $T_H = \sum_{\sigma \in H} \sigma$ for a subset H of a Galois group $\mathcal{G}$ of some finite Galois extension of K. If G is a subgroup of $\mathcal{G}$, then $T_{\mathcal{G}}(\beta) = (|\mathcal{G}|/d)(\beta_1 + \dots + \beta_d)$, so $T_{\mathcal{G}}(\beta) = 0$ if and only if the trace of β (over K) is equal to 0.

It is easily seen that the trace of every $\beta \in \mathcal{A}(K; k_1, \dots, k_n)$, where $k_1 + \dots + k_n = 0$, is 0. Indeed, setting F for the Galois closure of $L(\alpha)$ over K, $\mathcal{G} = \mathrm{Gal}(F/K)$ and using $\beta = k_1\alpha_1 + \dots + k_n\alpha_n$, we deduce that

$$T_{\mathcal{G}}(\beta) = \sum_{j=1}^n k_j T_{\mathcal{G}}(\alpha_j) = T_{\mathcal{G}}(\alpha) \sum_{j=1}^n k_j = 0,$$

so the trace of β over K is 0.

Generally speaking, the property of β to lie in $\mathcal{A}(K; k_1, \dots, k_n)$ depends on $k_1, \dots, k_n$, on G, and on linear relations with conjugates of β. Since the trace of β is zero, every linear relation can be expressed as $\nu_1\beta_1 + \dots + \nu_d\beta_d = 0$, where $\nu_1, \dots, \nu_d \in K$, and, without loss of generality, $\nu_1 + \dots + \nu_d = -1$. More precisely, $\beta \in \mathcal{A}(K; k_1, \dots, k_n)$ if and only if there exist $\sigma_2, \dots, \sigma_n \in G$ and a linear relation normalized as above such that the linear system

$$M(x_1, x_2, \dots, x_d)^{\mathrm{t}} = (\nu_1 + 1, \nu_2, \dots, \nu_d)^{\mathrm{t}} \tag{1}$$

has a solution. Here, t stands for the transpose, $M = \|m_{ij}\|_{i,j=1,\dots,d}$ is the $d \times d$ matrix with $m_{ij} = \sum k_r$, the sum being taken over every r, $1 \le r \le n$, such that $\sigma_r(\beta_i) = \beta_j$, where σ_1 is the identity. If there are no such r, then $m_{ij} = 0$. (Using Theorem 1 and writing $\alpha = x_1\beta_1 + \dots + x_d\beta_d$, where $x_1, \dots, x_d$ is the solution of (1), we have $\sum_{j=1}^n k_j\sigma_j^{-1}(\alpha) = (1+\nu_1)\beta + \nu_2\beta_2 + \dots + \nu_d\beta_d = \beta$.)

As in [5], it turns out that the condition on the trace of β to be zero, although necessary, is not sufficient for β to belong to $\mathcal{A}(K; k_1, \dots, k_n)$.

The next statement is a useful criterion which allows one to construct such numbers.

THEOREM 2. *Suppose that $\beta \in \mathcal{A}(K; k_1, \dots, k_n)$ with $k_1, \dots, k_n \in K^*$ satisfying $k_1 + \dots + k_n = 0$. Then there is a subgroup H of G which is generated by at most $n-1$ elements such that $T_H(\beta) = 0$.*

Of course, if $H = G$, then $T_H(\beta) = 0$. However, for $H \neq G$, $T_H(\beta) \neq 0$ provided that the linear relation $n_1\beta_1 + \dots + n_d\beta_d = 0$ with non-negative integers n_i such that $n_1 + \dots + n_d \leq |G|$ is satisfied only if $n_1 = \dots = n_d$. In particular, this is the case if $\lambda(\beta) = 0$ for $\lambda \in K[G]$ implies that $\lambda = kT_G$ with $k \in K$.

Assume that $E \subset \overline{K}$ is a finite Galois extension of K with Galois group $\mathcal{G}$. By the normal basis theorem, there is a $w \in E$ such that $E = K[\mathcal{G}]w$. Set $\beta = w - T_{\mathcal{G}}(w)/|\mathcal{G}|$. Then $\mathcal{G} = G$, $T_{\mathcal{G}}(\beta) = 0$, and $T_H(\beta) \neq 0$ for every subset H of G, $H \neq G$.

COROLLARY 1. *Let $k_1, \dots, k_n \in K^*$ be such that $k_1 + \dots + k_n = 0$. Assume that K has a Galois extension of degree D over K whose Galois group is not generated by $n-1$ of its elements. Then there is an algebraic number of degree D over K with zero trace which is outside the set $\mathcal{A}(K; k_1, \dots, k_n)$.*

In particular, if $E \subset \overline{K}$ is an abelian extension of K with Galois group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$, where $\mathbb{Z}$ denotes the set of integers, then $\overline{K} \setminus \mathcal{A}(K; k_1, \dots, k_n)$ contains an algebraic number of degree $D = 2^n$ over K with zero trace, because every subgroup of $(\mathbb{Z}/2\mathbb{Z})^n$ generated by $n-1$ elements is of order at most $2^{n-1} < 2^n$. Of course, not every field K has such an extension E. (For instance, for the field of real numbers $\mathbb{R}$, we have $[E : \mathbb{R}] \leq [\overline{\mathbb{R}} : \mathbb{R}] = 2$.)

If K is a number field, i.e. a finite extension of the field of rational numbers $\mathbb{Q}$, then such an extension exists for every n. Let $p_1, p_2, \dots, p_n$ be prime numbers such that $\sqrt{p_1} \notin K$, $\sqrt{p_2} \notin K(\sqrt{p_1}), \dots, \sqrt{p_n} \notin K(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})$. Setting $E = K(\sqrt{p_1}, \dots, \sqrt{p_n})$ and

$$w = (1 + \sqrt{p_1}) \dots (1 + \sqrt{p_n}), \tag{2}$$

we have $E = K[\mathrm{Gal}(E/K)]w$, where $\mathrm{Gal}(E/K)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$ (see Lemma 1 below). Clearly, $\beta = w - 1$ is the sum of $2^n - 1$ square roots. Note that every number $\sqrt{v}$, where $v \in \mathbb{Z}$ is not a perfect square, belongs to $\mathcal{A}(K; 1, -1)$. By the Proposition, it also belongs to every set $\mathcal{A}(K; k_1, \dots, k_n)$ with $k_1, \dots, k_n \in K^*$ satisfying $k_1 + \dots + k_n = 0$. The number $\beta = w - 1$, where w is defined by (2), is the sum of square roots, but $\beta \notin \mathcal{A}(K; k_1, \dots, k_n)$, by Corollary 1.

COROLLARY 2. *If $k_1, \dots, k_n \in K^*$, where K is a number field, and $k_1 + \dots + k_n = 0$, then $\mathcal{A}(K; k_1, \dots, k_n)$ is not an additive semigroup.*

If $\beta \notin \mathcal{A}(K; k_1, \ldots, k_n)$, then $k\beta \notin \mathcal{A}(K; k_1, \ldots, k_n)$ for every $k \in K^*$, so that $\overline{K} \backslash \mathcal{A}(K; k_1, \ldots, k_n)$ contains an infinite set of numbers with zero trace. On the other hand, *every* β of trace 0 is represented by *every* sufficiently long linear form in conjugates of α.

Before we give a precise version of this statement, note that every field of characteristic 0 contains a subfield isomorphic to $\mathbb{Q}$. In Theorem 3, $\mathbb{R}$ stands for a possible image of the usual $\mathbb{R}$ under this isomorphism. We say that $\beta \in \overline{K}$ of degree d over K is *symmetric* over K if there exist $\sigma_2, \ldots, \sigma_d \in G$ such that the matrix $\|\sigma_i(\beta_j)\|_{i,j=1,\ldots,d}$ is a Latin square, that is, each of its rows and each of its columns is a permutation of $\beta_1, \ldots, \beta_d$. Here, σ_1 is the identity. (Non-symmetric numbers exist! The smallest possible degree for them to occur is 6. We will give the proof of this in a subsequent paper on multiplicative relations.) Since every $\mathcal{A}(K; k_1, \ldots, k_n)$ contains all numbers of prime degree over K with zero trace, the next theorem is enounced for $d \geq 4$ only.

Theorem 3. *Let β be an algebraic number of degree $d \geq 4$ over K and of trace* 0 *over K. If $k_1, \ldots, k_n \in K^* \cap \mathbb{R}$, where $n \geq 2d - 5$, then $\beta \in \mathcal{A}(K; k_1, \ldots, k_n)$. Moreover, if β is symmetric over K, then the above is true for $n \geq 2[d/2] - 1$.*

Throughout, $[\ldots]$ denotes the integral part. Note that $2[d/2] - 1$ equals $d-1$ and $d-2$ for even and odd d, respectively. In particular, let $\mathcal{A}_d$ be the set of algebraic numbers (over $\mathbb{Q}$) of degree at most d. If $n \geq 2d - 5$, and $k_1, \ldots, k_n \in \mathbb{Q}^*$, then $\mathcal{A}_d \subset \mathcal{A}(\mathbb{Q}; k_1, \ldots, k_n)$.

For $d = 4$, we deduce that every β of degree ≤ 4 over $\mathbb{Q}$ can be represented by every linear form $k_1\alpha_1 + k_2\alpha_2 + k_3\alpha_3$ of length 3 with fixed $k_1, k_2, k_3 \in \mathbb{Q}^*$ and some algebraic numbers $\alpha_1, \alpha_2, \alpha_3$ conjugate over $\mathbb{Q}$. Thus, for $d = 4$ the inequality $n \geq 3$ of Theorem 3 is sharp. It cannot be replaced by $n \geq 2$, which is shown by the example of $\beta = \sqrt{2} + \sqrt{3} + \sqrt{6} \notin \mathcal{A}(\mathbb{Q}; 1, -1)$ (see [5]).

The final section of this paper contains some results on the dimension of $\mathcal{L}(\beta)$—so it deals with a question that may appear to be somewhat apart from the foregoing results.

3. Auxiliary results

Lemma 1. *Given a number field K, let $p_1, \ldots, p_n$ be prime numbers such that $[K(\sqrt{p_1}, \ldots, \sqrt{p_n}) : K] = 2^n$. Then*

$$E = K(\sqrt{p_1}, \ldots, \sqrt{p_n}) = K[\mathrm{Gal}(E/K)]w,$$

where $\mathrm{Gal}(E/K)$ *is isomorphic to* $(\mathbb{Z}/2\mathbb{Z})^n$ *and where w is given by* (2).

Proof. Clearly, w is of degree 2^n over K. It suffices to show that the conjugates of w, $(1 \pm \sqrt{p_1}) \ldots (1 \pm \sqrt{p_n})$, are linearly independent over K.

Assume, for contradiction, that they are linearly dependent over K. Then the numbers $(1 \pm \sqrt{p_1}) \ldots (1 \pm \sqrt{p_{n-1}})$ are linearly dependent over $K(\sqrt{p_n})$ and so on. At the end of the argument we find that the numbers $1+\sqrt{p_1}$ and $1-\sqrt{p_1}$ are linearly dependent over $K(\sqrt{p_2}, \ldots, \sqrt{p_n})$. This however is not the case, because $(1+\sqrt{p_1})/(1-\sqrt{p_1}) \notin K(\sqrt{p_2}, \ldots, \sqrt{p_n})$.

LEMMA 2. *Let $d \geq 4$. Suppose that M is a $d \times d$ matrix with real negative entries on the main diagonal and non-negative entries outside the main diagonal such that the sums of its elements in every row and in every column are all equal to zero. If either the first row contains at least $d-2$ positive entries, or M is a Latin square and, say, the first row contains at least $[d/2]$ positive entries, then the rank of the matrix is $d-1$.*

Proof. Let $M = \|m_{ij}\|_{i,j=1,\ldots,d}$. Suppose we have a linear relation

$$u_1\mathbf{r}_1 + \ldots + u_d\mathbf{r}_d = 0 \tag{3}$$

between its rows with real $u_1, \ldots, u_d$, where $u_i \neq 0$ for at least one i. Assume $u_j = u$ has the largest modulus among u_i, $i = 1, \ldots, d$. Set $\mathcal{J} = \{j\}$. Given j, there are some $i \neq j$ such that $m_{ij} > 0$, because $m_{jj} < 0$. Now, by considering the jth entry of the vector on the left-hand side of (3), we see that every such u_i is equal to u. We increase $\mathcal{J}$ by adding all such indices i. We continue in this fashion with every j in the new $\mathcal{J}$ as before increasing $\mathcal{J}$ step by step. Assume that at the end of the argument we obtain a set of indices which, by abuse of notation, we denote by $\mathcal{J}$ again. Then $u_j = u$ for every $j \in \mathcal{J}$, but $u_j \neq u$ for $j \notin \mathcal{J}$. The task is now to show that $\mathcal{J} = \{1, \ldots, d\}$.

By the definition of $\mathcal{J}$, the $|\mathcal{J}| \times d$ matrix formed by the rows whose indices belong to $\mathcal{J}$ has $d-|\mathcal{J}|$ zero columns. The row sums in the remaining $|\mathcal{J}| \times |\mathcal{J}|$ matrix M' are all zero. Thus so must be the column sums of M'. After interchanging some of the rows of M and, if necessary, some of the columns (which does not change the rank of M), we can write M in the form

$$\begin{pmatrix} M'' & 0 \\ 0 & M' \end{pmatrix}.$$

Here, M'' is a $(d-|\mathcal{J}|) \times (d-|\mathcal{J}|)$ matrix.

Assume that $|\mathcal{J}| < d$. Then $|\mathcal{J}|$ and $d-|\mathcal{J}|$ are both greater than or equal to 2. In the first case of the lemma, there is a row of M with at most $d-1-(d-2) = 1$ zero element, a contradiction. In the second case, M' and M'' are both Latin squares with at least $1+[d/2]$ non-zero elements. Hence, $|\mathcal{J}|$ and $d-|\mathcal{J}|$ are both greater than or equal to $1+[d/2]$. By adding them, we deduce that $d \geq 2+2[d/2]$, which is impossible.

4. Proofs

Proof of Theorem 1. Suppose $\beta \in \overline{K}$ can be expressed as $k_1\alpha_1 + \ldots + k_n\alpha_n$. Let F be the Galois closure of $L(\alpha)$ over K with Galois group $\mathcal{G}$. Then F is a semisimple $K[\mathcal{G}]$-module containing $\mathcal{L}(\beta)$ (see [8, Theorem 2.11, p. 23 and Proposition 2.2, p. 17]). Accordingly, $F = \mathcal{L}(\beta) \oplus U$ for some $K[\mathcal{G}]$-module U, where $\oplus$ stands for direct sum. Write $\alpha = \alpha' + \gamma$ with $\alpha' \in \mathcal{L}(\beta)$ and $\gamma \in U$. Let $\sigma_j \in \mathcal{G}$ be such that $\alpha_j = \sigma_j(\alpha)$. Then $\alpha_j = \sigma_j(\alpha') + \sigma_j(\gamma)$ and

$$\beta = k_1\alpha_1 + \ldots + k_n\alpha_n = \sum_{j=1}^{n} k_j\sigma_j(\alpha') + \sum_{j=1}^{n} k_j\sigma_j(\gamma).$$

Note that the left-hand side and the first sum on the right-hand side are both in $\mathcal{L}(\beta)$, whereas the second sum is in U. This implies that the latter sum is zero, hence $\beta = \sum_{j=1}^{n} k_j\sigma_j(\alpha')$ with $\alpha' \in \mathcal{L}(\beta)$, as claimed.

Proof of Theorem 2. Since $\beta = k_1\alpha_1 + \ldots + k_n\alpha_n$, it follows that $\beta \in \mathcal{L}(\alpha)$. By Theorem 1, α can be chosen in $\mathcal{L}(\beta)$, hence the Galois closure of $K(\alpha)$ over K is L. Write $\beta = k_1\alpha + \sum_{j=2}^{n} k_j\sigma_j(\alpha)$, where $\alpha_j = \sigma_j(\alpha)$, $j = 2, \ldots, n$, with $\sigma_j \in G$. Put $H = \langle\sigma_2, \ldots, \sigma_n\rangle$. Then $T_H(\alpha_j) = T_H(\alpha)$ for every $j = 2, \ldots, n$. It follows that $T_H(\beta) = (k_1 + \ldots + k_n)T_H(\alpha) = 0$.

Proof of Theorem 3. It suffices to prove the assertion for the case $\sum_{j=1}^{n} k_j = 0$. We start with the first statement. As $n \geq 2d-5$, at least $d-2$ elements of the set $\{k_1, \ldots, k_n\}$ are either positive or negative; we may assume that $k_2, \ldots, k_{d-1}$ are all positive. On replacing the remaining ones, namely k_1 and $k_d, \ldots, k_n$, by their sum $k_1 + k_d + \ldots + k_n$ we shall write k_1 for it again. The task is now to show that

$$\beta = k_1\alpha_1 + \ldots + k_{d-1}\alpha_{d-1} + k_d\alpha_d,$$

where $k_d = 0$, has a solution in conjugates of $\alpha \in \mathcal{L}(\beta)$ over K.

For this, assume that σ_1 is the identity and $\sigma_2, \ldots, \sigma_d \in G$ are some automorphisms which map β to $\beta_2, \ldots, \beta_d$, respectively. Setting in (1) $\nu_1 = \ldots = \nu_d = -1/d$, we need to show that the linear system

$$M(x_1, x_2, \ldots, x_d)^{\mathrm{t}} = (1 - 1/d, -1/d, \ldots, -1/d)^{\mathrm{t}}$$

has a solution. Recall that the elements of M are given by the formulae $m_{ij} = \sum k_r$, the sum being taken over all r, $1 \leq r \leq n$, such that $\sigma_r(\beta_i) = \beta_j$. Then M is the matrix as in the first case of Lemma 2, hence its rank is $d-1$. The sum of the rows of the $d \times (d+1)$ matrix M^* obtained from M by adding to it the column $(1 - 1/d, -1/d, \ldots, -1/d)^{\mathrm{t}}$ is zero. We deduce 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 solution.

If β is symmetric and $n \geq 2[d/2]-1$, then at least $[d/2]$ elements of the set $\{k_1, \ldots, k_n\}$ are either positive or negative. Assuming that $k_2, \ldots, k_{[d/2]+1}$ are positive and arguing as above with the automorphisms $\sigma_2, \ldots, \sigma_d \in G$ such that the matrix $\|\sigma_i(\beta_j)\|_{i,j=1,\ldots,d}$ (with σ_1 being the identity) is a Latin square, we will obtain M as in the second case of Lemma 2 (because the numbers $\sigma_1(\beta), \ldots, \sigma_d(\beta)$ are all distinct). The proof can now be concluded as above.

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

By Theorem 3, the equation

$$\beta = \sqrt{2} + \sqrt{3} + \sqrt{6} = \alpha_1 + \alpha_2 - 2\alpha_3$$

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

Since G is the 4-group, we choose three remaining automorphisms $\sigma_2 = (12)(34)$, $\sigma_3 = (13)(24)$ and $\sigma_4 = (14)(23)$, where say $\beta_1 = \sqrt{2} + \sqrt{3} + \sqrt{6}$, $\beta_2 = -\sqrt{2} + \sqrt{3} - \sqrt{6}$, $\beta_3 = \sqrt{2} - \sqrt{3} - \sqrt{6}$ and $\beta_4 = -\sqrt{2} - \sqrt{3} + \sqrt{6}$. Now, setting $\nu_1 = \ldots = \nu_4 = -1/4$ in (1), we obtain the system of linear equations

$$\begin{aligned} x_1 + x_2 - 2x_3 &= 3/4, \\ x_1 + x_2 - 2x_4 &= -1/4, \\ -2x_1 + x_3 + x_4 &= -1/4, \\ -2x_2 + x_3 + x_4 &= -1/4. \end{aligned}$$

One of its solutions is $x_1 = x_2 = 0$, $x_3 = -3/8$, $x_4 = 1/8$. This immediately gives

$$\alpha = \alpha_1 = (-3\beta_3 + \beta_4)/8 = (-2\sqrt{2} + \sqrt{3} + 2\sqrt{6})/4.$$

Also,

$$\begin{aligned} \alpha_2 &= (2\sqrt{2} + \sqrt{3} - 2\sqrt{6})/4, \\ \alpha_3 &= (-2\sqrt{2} - \sqrt{3} - 2\sqrt{6})/4. \end{aligned}$$

One can easily check that $\sqrt{2} + \sqrt{3} + \sqrt{6} = \alpha_1 + \alpha_2 - 2\alpha_3$.

5. Dimension of the linear space spanned by conjugates. Let β be an algebraic number of degree d over K. Although the next topic is beyond the main theme of this paper, we ask how small the dimension of the linear space $\mathcal{L}(\beta)$ over K can be, or, equivalently, how many linearly independent relations with conjugates of β can occur. If, for example, β is of trace zero over K, then $\dim_K \mathcal{L}(\beta) = d - 1$ reflects the fact that $T_G(\beta) = 0$ is the only linear relation between the conjugates of β, so that $\nu_1 = \ldots = \nu_d = -1/d$ is the only choice in (1).

We will first show that if β is an algebraic number of degree $d \geq 3$ over K which is a real extension of $\mathbb{Q}$, then $\dim_K \mathcal{L}(\beta) \geq 2$. Indeed, if $\dim_K \mathcal{L}(\beta) = 1$, then G is isomorphic to a multiplicative subgroup of K^*. Since G is finite, we deduce that $|G| \leq 2$ giving $d \leq 2$. (The above proof is entirely due to the referee. Our initial proof based on an argument of C. J. Smyth [9] and was somewhat longer.)

Theorem 4. *For every number field K, there is an infinite sequence of integers d such that for every such d there is an algebraic number β of degree d with* $\dim_K \mathcal{L}(\beta) = \log_2 d$.

Proof. As above, choose r prime numbers $p_1, \ldots, p_r$ such that $[K(\sqrt{p_1}, \ldots \ldots, \sqrt{p_r}) : K] = 2^r$. Set

$$\beta = \sqrt{p_1} + \ldots + \sqrt{p_r}.$$

Clearly, the degree of β over K equals $d = 2^r$ and its trace is zero. Also, $\dim_K \mathcal{L}(\beta) = r = \log_2 d$, which is the desired conclusion.

If $r = \dim_{\mathbb{Q}} \mathcal{L}(\beta)$, then the largest possible value for the degree d of β over $\mathbb{Q}$ turns out to be $2^r r!$ except for some r in the range $2 \leq r \leq 10$. (This was shown in a joint work of N. Berry, the author, N. Elkies, B. Poonen and C. J. Smyth (in preparation).)

In all previous cases [1]–[7], [10] not only additive, but also the respective multiplicative results were obtained. It would be of interest to find out whether a multiplicative analogue of Theorem 1 is true. (Its weaker form and other multiplicative results will appear elsewhere.) More precisely, let $k_0, k_1, \ldots, k_n$ be non-zero integers. Assume that the k_0th power of β can be represented as $\beta^{k_0} = \alpha_1^{k_1} \ldots \alpha_n^{k_n}$ with $\alpha_1, \ldots, \alpha_n$ conjugate to α over $\mathbb{Q}$. Is it true that α can be chosen so that some of its natural powers is equal to $v\beta_1^{v_1} \ldots \beta_d^{v_d}$ with $v, v_1, \ldots, v_d \in \mathbb{Z}$? (If so, it would be sufficient to prove this for the case $k_1 + \ldots + k_n = 0$, $n \geq 3$, for otherwise it is either trivial or, if $n = 2$, follows from the construction in [5, Section 5].)

Acknowledgements. I thank Chris Smyth for many stimulating conversations while working on our paper [5]. Some of the ideas we discussed did not appear in the final version of [5], but proved to be useful here. I also thank the referee whose remarks allowed me to simplify some of the arguments essentially.

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

References

[1] G. Baron, M. Drmota and M. Skałba, *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. Skałba, *Relations between polynomial roots*, ibid. 71 (1995), 65–77.

[4] A. Dubickas, *On the degree of a linear form in conjugates of an algebraic number*, Illinois J. Math., to appear.

[5] A. Dubickas and C. J. Smyth, *Variations on the theme of Hilbert's Theorem 90*, Glasgow Math. J., to appear.

[6] K. Girstmair, *Linear dependence of zeros of polynomials and construction of primitive elements*, Manuscripta Math. 39 (1982), 81–97.

[7] —, *Linear relations between roots of polynomials*, Acta Arith. 89 (1999), 53–96.

[8] B. Huppert, *Character Theory of Finite Groups*, de Gruyter, Berlin, 1998.

[9] C. J. Smyth, *Conjugate algebraic numbers on conics*, Acta Arith. 40 (1982), 333–346.

[10] —, *Additive and multiplicative relations connecting conjugate algebraic numbers*, J. Number Theory 23 (1986), 243–254.

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

Received on 12.6.2001
and in revised form on 29.4.2002 (4062)