J. Ramanujan Math. Soc. **30,** No.2 (2015) 219–235

Simple linear relations between conjugate algebraic numbers of low degree

Artūras Dubickas and Jonas Jankauskas

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania
e-mail: arturas.dubickas@mif.vu.lt

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania
e-mail: jonas.jankauskas@gmail.com

Communicated by: Sujatha Ramdorai

Received: October 2, 2014

Abstract. We consider the linear equations $\alpha_1 = \alpha_2 + \alpha_3$ and $\alpha_1 + \alpha_2 + \alpha_3 = 0$ in conjugates of an algebraic number α of degree $d \leq 8$ over $\mathbb{Q}$. We prove that solutions to those equations exist only in the case $d = 6$ (except for the trivial solution of the second equation in cubic numbers with trace zero) and give explicit formulas for all possible minimal polynomials of such algebraic numbers. For instance, the first equation is solvable in roots of an irreducible sextic polynomial if and only if it is an irreducible polynomial of the form $x^6+2ax^4+a^2x^2+b \in \mathbb{Q}[x]$. The proofs involve methods from linear algebra, Galois theory and some combinatorial arguments.

2000 *Mathematics Subject Classification.* 11R06, 11R09, 11R32, 12F10.

1. Introduction

Let $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_d$ be a full set of the algebraic conjugates of an algebraic number α of degree d over $\mathbb{Q}$. In the present paper we will be interested in algebraic numbers α of small degree d (namely, $d \leq 8$) whose conjugates satisfy one of the equations

$$\alpha_1 = \alpha_2 + \alpha_3 \quad \text{or} \quad \alpha_1 + \alpha_2 + \alpha_3 = 0. \tag{1}$$

One may think of equations (1) as the examples of simplest non-trivial linear additive relations that may occur among roots of irreducible integer polynomials.

The research on this subject started with a question of Browkin who asked if there is an irreducible non-cyclotomic polynomial whose distinct roots $\alpha_1, \alpha_2, \alpha_3$ satisfy

$$\alpha_1 = \alpha_2\alpha_3. \tag{2}$$

Note that the first equation of (1) is simply the additive version of (2). It was Schinzel who gave the first example of the algebraic number α satisfying (2), thus answering Browkin's question in the affirmative. Schinzel's example $p(x) = x^6 - 2x^4 - 6x^3 - 2x^2 + 1$ is mentioned in the papers [1,7]. Subsequently, Drmota and Skałba investigated the solvability of the multiplicative equations $\alpha_1^a\alpha_2^b\alpha_3^c = 1$, where $a, b, c \in \mathbb{Z}$, in Abelian number fields in [7], as well as some more general polynomial relations in [1,6]. From this viewpoint, our Theorems 1.1 and 1.2 below can be viewed as the additive generalization of Schinzel's example and also as the additive extension of the results from the paper [7] on the multiplicative equation (2) into non-Abelian cases of low degree.

An additional motivation to study the equations (1) stems from our recent joint work with Hare [3] on *Pisot numbers*. Recall that a real algebraic integer $\alpha > 1$ is called a Pisot number if all of its conjugates α_j, other than α itself, satisfy $|\alpha_j| < 1$. In [3], we showed that there are no Pisot numbers whose conjugates satisfy the first equation in (1), and also proved that there is a unique Pisot number whose conjugates satisfy another simple linear equation

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4. \tag{3}$$

This unique Pisot number is $\alpha = (1 + \sqrt{3 + 2\sqrt{5}})/2$, it was first found in [5]. The impossibility of (3) in conjugates of a Pisot number of degree $d > 4$ has some interesting geometric implications concerning the set of conjugates of a Pisot number that lie on the lines parallel to the real or imaginary axis of the complex plane $\mathbb{C}$ and answers some questions raised in [5].

The basic method that was used in [3] was first to prove the restrictions on the degree d of a Pisot number α: the upper bounds $d \le 8$ and $d \le 18$ were derived for the degree of the solutions of the equations (1) and (3), respectively. We also proved that such Pisot numbers must be confined to certain short sub-intervals of $[1, 2]$ and $[1, 3]$. In this way all possible solutions were found and verified with computers in [3]. In particular, in showing that the equation $\alpha_1 = \alpha_2 + \alpha_3$ has no solutions in conjugates of a Pisot number the main difficulty was to deal with the case $d = 8$.

Now, we will show that the equations (1) can be solved by using some combinatorial and group theoretical arguments. The main advantage of such

approach is that one no longer needs to assume that α is a Pisot number, as we did in [3].

Theorem 1.1. *Let d be an integer in the range $3 \le d \le 8$ and let α be an algebraic number of degree d over $\mathbb{Q}$. Then some three of its conjugates α_1, α_2, α_3 satisfy the relation*

$$\alpha_1 = \alpha_2 + \alpha_3$$

if and only if $d = 6$ and the minimal polynomial of α over $\mathbb{Q}$ is an irreducible polynomial of the form

$$p(x) = x^6 + 2ax^4 + a^2x^2 + b \in \mathbb{Q}[x].$$

The second equation in (1) has a trivial cubic solution, since three conjugates of each cubic algebraic number with trace zero satisfy $\alpha_1+\alpha_2+\alpha_3 = 0$. Also, one can easily construct examples of algebraic numbers whose three conjugates add up to zero for each degree d that is a multiple of 3. For instance, one can take an algebraic number θ of degree m with conjugates $\theta_1, \dots, \theta_m$ over $\mathbb{Q}$ and two polynomials $u, v \in \mathbb{Q}[x]$ of degree at most $m-1$. Then

$$p(x) = \prod_{j=1}^{m} (x^3 + u(\theta_i)x + v(\theta_i)) \in \mathbb{Q}[x]$$

defines the minimal polynomial of an algebraic number α of degree $d = 3m$ (if $p(x)$ is irreducible over $\mathbb{Q}$) whose three conjugates sum to zero.

However, there exist algebraic numbers of degree d whose three conjugates satisfy $\alpha_1 + \alpha_2 + \alpha_3 = 0$ with d not necessarily divisible by 3; see [4]. One does not know yet what is the smallest possible degree d of such an algebraic number: according to [4] and our next Theorem 1.2, such a minimal value of d lies in the range $10 \le d \le 20$. More so, a complete description of solutions to the equations (1) seems to be a daunting task for any degree $d \ge 9$. Restricting to the degrees in the range $4 \le d \le 8$ we have the following:

Theorem 1.2. *Let d be an integer in the range $4 \le d \le 8$ and let α be an algebraic number of degree d over $\mathbb{Q}$. Then some three of its conjugates α_1, α_2, α_3 satisfy the relation*

$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

if and only if $d = 6$ and the minimal polynomial of α over $\mathbb{Q}$ is an irreducible polynomial of the form

$$p(x) = x^6 + 2ax^4 + 2bx^3 + (a^2 - c^2t)x^2 + 2(ab - cet)x + b^2 - e^2t$$

for some rational numbers $a, b, c, e \in \mathbb{Q}$ and some square-free integer $t \in \mathbb{Z}$.

In order to verify whether a given polynomial

$$p(x) = x^6 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Q}[x]$$

is of the form given in Theorem 1.2 or not we set $a := a_4/2$, $b := a_3/2$. Then, using $4c^2t = a_4^2 - 4a_2$, $4e^2t = a_3^2 - 4a_0$ and $4cet = a_3a_4 - 2a_1$, we can rewrite the condition of the theorem as follows:

$$(a_4^2 - 4a_2)(a_3^2 - 4a_0) = (a_3a_4 - 2a_1)^2. \tag{4}$$

For instance, the polynomial $g(x) = x^6 + 4x^4 + 2x^3 + 2x^2 - 1 \in \mathbb{Q}[x]$ satisfies (4). Thus, by Theorem 1.2, the sum of its three roots is zero. The reason behind this is the fact that $p(x)$ is the product of the polynomials $x^3 + (2+\sqrt{2})x + 1 + \sqrt{2}$ and $x^3 + (2-\sqrt{2})x + 1 - \sqrt{2}$. In the proof of the theorem we will show that a sextic irreducible polynomial whose three roots sum to zero is always the product of two polynomials $x^3 + ux + v$ and $x^3 + u'x + v'$, where u, u' and v, v' are two pairs of conjugate algebraic numbers lying in a quadratic field K.

In the next section we give some auxiliary results. Then, in Section 3, we prove Theorem 1.1 for degrees $3 \le d \le 7$. In Section 4 we show that the first equation of (1) has no solutions in conjugates of an algebraic number of degree 8, and thus complete the proof of Theorem 1.1. Finally, in Section 5 we will prove Theorem 1.2.

2. Auxiliary results

The next result was first proved by Kurbatov [9] (see also [2] for various generalizations and more references on this problem).

Lemma 2.1. *The equality*

$$k_1\alpha_1 + k_2\alpha_2 + \cdots + k_d\alpha_d = 0$$

with conjugates $\alpha_1, \alpha_2, \ldots, \alpha_d$ of an algebraic number α of prime degree d over $\mathbb{Q}$ and $k_1, k_2, \ldots, k_d \in \mathbb{Z}$ can only hold if $k_1 = k_2 = \cdots = k_d$.

In [10] Smyth proved that

Lemma 2.2. *If $\alpha_1, \alpha_2, \alpha_3$ are three conjugates of an algebraic number satisfying $\alpha_1 \ne \alpha_2$ then $2\alpha_1 \ne \alpha_2 + \alpha_3$.*

A more general version of Lemma 2.2 is Theorem 4 of [2]:

Lemma 2.3. *If $\beta_1, \beta_2, \ldots, \beta_n$, where $n \ge 3$, are distinct algebraic numbers conjugate over a field of characteristic zero K and $k_1, k_2, \ldots, k_n$ are non-zero rational numbers satisfying $|k_1| \ge |k_2| + \cdots + |k_n|$ then*

$$k_1\beta_1 + k_2\beta_2 + \cdots + k_n\beta_n \notin K.$$

We shall also need the following simple observation:

Lemma 2.4. *The equality*

$$k_1\alpha_1 + k_2\alpha_2 + \cdots + k_d\alpha_d = 0$$

with conjugates $\alpha_1, \alpha_2, \ldots, \alpha_d$ *of an algebraic number* α *of degree* d *over* $\mathbb{Q}$ *and* $k_1, k_2, \ldots, k_d \in \mathbb{Z}$ *satisfying* $\sum_{i=1}^{d} k_i \neq 0$ *can only hold if* $tr(\alpha) := \alpha_1 + \cdots + \alpha_d = 0$.

Proof. Let G be the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$. Applying all automorphisms of G to $k_1\alpha_1 + \cdots + k_d\alpha_d = 0$ and adding the obtained $|G| = dm$, equalities, where $m \in \mathbb{N}$, we find that

$$k_1 m\mathrm{tr}(\alpha) + \cdots + k_d m\mathrm{tr}(\alpha) = m\mathrm{tr}(\alpha)\sum_{i=1}^{d} k_i = 0,$$

whence the result. □

Let $G = \mathrm{Gal}(L/K)$ denote the Galois group of the Galois closure L of an algebraic number field K. Drmota and Skałba [7] investigated in detail the existence of solutions of the multiplicative equation $\alpha_1 = \alpha_2\alpha_3$ in conjugate algebraic numbers of degree d in the field L. (See also papers [1,6] for related results on multiplicative and additive independence). Among other things, they proved that if L/K is an Abelian extension then the equation $\alpha_1 = \alpha_2\alpha_3$ has no solutions when $6 \nmid d$. Once again, this is no longer true without assuming that the extension L/K is Abelian; the multiplicative version of the construction given in [4] gives an example of an algebraic number α of degree $d = 20$ whose three conjugates satisfy $\alpha_1 = \alpha_2\alpha_3$. We will make use of the results [7] (adapted to our additive setting), as well as group determinants later in proof of Theorem 1.1 in Section 4.

Consider the linear relation $\sum_{\sigma\in G} x_\sigma\alpha_\sigma = 0$, where $\alpha_\sigma = \sigma(\alpha)$ and the indeterminate coefficients $x_\sigma \in \mathbb{Q}$ that are indexed by the elements $\sigma \in G$. By applying all automorphisms $\tau \in G$ to this linear relation, we obtain a system of linear equations

$$\sum_{\sigma\in G} x_\sigma\alpha_{\tau\sigma} = \sum_{\sigma\in G} x_{\tau^{-1}\sigma}\alpha_\sigma = 0, \quad \tau \in G.$$

If a vector $(\alpha_\sigma)_{\sigma\in G} \in L^{|G|}$ is a non-trivial solution to this system of equations, then the determinant of the coefficient matrix

$$A_G = (x_{\tau^{-1}\sigma})$$

must vanish if one substitutes the appropriate values $x_\sigma = k_\sigma \in \mathbb{Q}$. The determinant $\det A_G$ is called *the group determinant of* G. By the theorem of

Frobenius, if the group G is Abelian and $\hat{G}$ denotes the group of characters of G, then $\det A_G$ factors over $\mathbb{C}$ into the product of degree 1 terms:

$$\det A_G = \prod_{\chi \in \hat{G}} \left(\sum_{\sigma \in G} \chi(\sigma) x_\sigma \right).$$

Lemma 2.5 (Drmota, Skałba [7]). *Let H be an Abelian subgroup of the Galois group $G = Gal(L/K)$. Assume that H acts transitively on the set $\{\alpha_i, \alpha_j, \alpha_k\}$ of conjugate algebraic numbers in L (that is, α_i, α_j, α_k are conjugate over the subfield L^H fixed by H). If $\alpha_i = \alpha_j + \alpha_k$, then the order of H is divisible by* 6.

Proof. Let H act on the set of conjugates of α_i over the field L^H. Assume that $\sigma, \tau, \eta \in H$ are the elements of H such that $\alpha_\sigma = \alpha_i$, $\alpha_\tau = \alpha_j$, $\alpha_\eta = \alpha_k$. Since $\alpha_i = \alpha_j + \alpha_k$, the group determinant $\det A_H$ must vanish when one substitutes $x_\sigma = 1$, $x_\tau = x_\eta = -1$ and sets all other $x_h = 0$ (for $h \neq \sigma, \tau, \eta$). Hence, some factor in the Frobenius formula must vanish. Therefore, we have $\chi(\sigma) = \chi(\tau) + \chi(\eta)$, or $\chi(\tau\sigma^{-1}) + \chi(\eta\sigma^{-1}) = 1$. Since the values of the characters of G are the roots of unity, we must have $\{\chi(\tau\sigma^{-1}), \chi(\eta\sigma^{-1})\} = \{\zeta, \zeta^{-1}\}$, where $\zeta = e^{\pi i/3}$ is the primitive root of unity of order 6. Since the order of a group character divides $|G|$, the proof is complete. □

Lemma 2.6. *Let $G \cong Q_8$ be generated by permutations*

$$(1,2,3,4)(5,6,7,8) \quad \textit{and} \quad (1,5,3,7)(2,8,4,6)$$

of the set $\{\alpha_1, \ldots, \alpha_8\}$. Then the group determinant of G factors as

$$\det A_G = F_1 \cdot F_2 \cdot F_3 \cdot F_4 \cdot F_5^2,$$

where the polynomials $F_1, F_2, F_3, F_4, F_5 \in \mathbb{Z}[x_1, \ldots, x_8]$ are given by

$$\begin{aligned}
F_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8,\\
F_2 &= x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8,\\
F_3 &= -x_1 - x_2 - x_3 - x_4 + x_5 + x_6 + x_7 + x_8,\\
F_4 &= -x_1 + x_2 - x_3 + x_4 + x_5 - x_6 + x_7 - x_8,\\
F_5 &= (x_1 - x_3)^2 + (x_2 - x_4)^2 + (x_5 - x_7)^2 + (x_6 - x_8)^2.
\end{aligned}$$

The variables are indexed as $x_{\sigma(1)}$, $\sigma \in G$.

Proof. We evaluated this group determinant directly on SAGE [11]. □

Lemma 2.7. *Let $G \cong D_4$ be generated by permutations*

$$(1,2,3,4)(5,6,7,8) \quad \textit{and} \quad (1,6)(2,5)(3,8)(4,7)$$

of the set $\{\alpha_1, \ldots, \alpha_8\}$. *Then the group determinant of G factors as*

$$\det A_G = F_1 \cdot F_2 \cdot F_3 \cdot F_4 \cdot F_5^2,$$

where the polynomials $F_1, F_2, F_3, F_4, F_5 \in \mathbb{Z}[x_1, \ldots, x_8]$ *are given by*

$$\begin{aligned}
F_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8,\\
F_2 &= -x_1 - x_2 - x_3 - x_4 + x_5 + x_6 + x_7 + x_8,\\
F_3 &= -x_1 + x_2 - x_3 + x_4 + x_5 - x_6 + x_7 - x_8,\\
F_4 &= x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8,\\
F_5 &= -(x_1 - x_3)^2 - (x_2 - x_4)^2 + (x_5 - x_7)^2 + (x_6 - x_8)^2.
\end{aligned}$$

Proof. As above, this is checked by a direct evaluation with SAGE [11].

□

3. Proof of Theorem 1.1 for $3 \le d \le 7$

We first prove that $-\alpha$ is a conjugate of α. Assume it is not. Consider an automorphism σ of the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ that maps α_1 to α_2. Setting $\sigma(\alpha_2) = \alpha_k$ and $\sigma(\alpha_3) = \alpha_l$, we obtain $\alpha_1 = \alpha_2 + \alpha_3$ and $\alpha_2 = \alpha_k + \alpha_l$. We claim that $k, l > 3$. Indeed, otherwise, as α_k and α_l are distinct, $k \neq l$, assuming without loss of generality that $k < l$, we must have $1 \le k \le 3$. Clearly, $k \neq 2$. If $k = 1$ then, by adding both equalities, we obtain $\alpha_3 + \alpha_l = 0$, which is impossible (otherwise, $-\alpha$ is a conjugate of α). If $k = 3$ then, by subtracting $\alpha_2 = \alpha_3 + \alpha_l$ from $\alpha_1 = \alpha_2 + \alpha_3$, we find that $2\alpha_2 = \alpha_1 + \alpha_l$, which contradicts Lemma 2.2. Thus, without restriction of generality, we may assume that $k = 4$ and $l = 5$, namely,

$$\alpha_1 = \alpha_2 + \alpha_3 \quad \text{and} \quad \alpha_2 = \alpha_4 + \alpha_5. \tag{5}$$

In particular, this shows that $d \ge 5$, so d cannot be 3 and 4. By Lemma 2.1, d cannot be 5 and 7, so $d = 6$.

Now, assume that $d = 6$. By Lemma 2.4, the sum of all 6 conjugates of α is equal to 0. Thus, by adding both equalities in (5), we find that

$$\alpha_1 + \alpha_2 = \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = -\alpha_1 - \alpha_6.$$

This implies $2\alpha_1 + \alpha_2 + \alpha_6 = 0$, which contradicts Lemma 2.3 with $n = 3$ and $K = \mathbb{Q}$. This proves that $-\alpha$ is a conjugate of α. Consequently, $d = 4$ or $d = 6$. However, if $d = 4$ and $\alpha_1 = \alpha_2 + \alpha_3$, then $\alpha_2, \alpha_3 \neq -\alpha_1$, since otherwise $2\alpha_1 = \alpha_i$, where $i = 2$ or $i = 3$, contrary to Lemma 2.3. So $\alpha_4 = -\alpha_1$. This yields $\alpha_2 = -\alpha_3$, which leads to $\alpha_1 = 0$, a contradiction again.

It remains to investigate the case $d = 6$. Since $-\alpha$ is a conjugate of α, the minimal polynomial of α (of degree 6) over $\mathbb{Q}$ must be of the form $x^6 + 2ax^4 + cx^2 + b \in \mathbb{Q}[x]$. (Here, $2a \in \mathbb{Q}$ and not just a is taken for convenience in order to avoid fractions in the resulting polynomial.) Let $\beta_1, \beta_2, \beta_3$ be the roots of the polynomial $x^3 + 2ax^2 + cx + b$, so that $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\} = \{\pm\sqrt{\beta_1}, \pm\sqrt{\beta_2}, \pm\sqrt{\beta_3}\}$. Note that the relation $\sqrt{\beta_1} = -\sqrt{\beta_1} \pm \sqrt{\beta_2}$ leads to $4\beta_1 = \beta_2$, which is impossible, by Lemma 2.3.

Thus, $\alpha_1 - \alpha_2 - \alpha_3 = 0$ is equivalent to $\theta_1\sqrt{\beta_1} + \theta_2\sqrt{\beta_2} + \theta_3\sqrt{\beta_3} = 0$ with some $\theta_1, \theta_2, \theta_3 \in \{-1, 1\}$. Dividing both sides by θ_1 we find that $\sqrt{\beta_1} + \theta_4\sqrt{\beta_2} + \theta_5\sqrt{\beta_3} = 0$ with some $\theta_4, \theta_5 \in \{-1, 1\}$. It is easy to see that this is equivalent to

$$(\sqrt{\beta_1} - \sqrt{\beta_2} - \sqrt{\beta_3})(\sqrt{\beta_1} - \sqrt{\beta_2} + \sqrt{\beta_3})$$
$$(\sqrt{\beta_1} + \sqrt{\beta_2} - \sqrt{\beta_3})(\sqrt{\beta_1} + \sqrt{\beta_2} + \sqrt{\beta_3}) = 0.$$

The product of the first and the fourth terms is $\beta_1 - \beta_2 - \beta_3 - 2\sqrt{\beta_2\beta_3}$, whereas the product of the second and the third is $\beta_1 - \beta_2 - \beta_3 + 2\sqrt{\beta_2\beta_3}$. Therefore, the product of the four terms on the left hand side is equal to

$$(\beta_1 - \beta_2 - \beta_3)^2 - 4\beta_2\beta_3 = (\beta_1 + \beta_2 + \beta_3)^2 - 4(\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1).$$

As $\beta_1 + \beta_2 + \beta_3 = -2a$ and $\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1 = c$, we conclude that the relation $\alpha_1 = \alpha_2 + \alpha_3$ between some three roots of the polynomial $x^6 + 2ax^4 + cx^2 + b$ holds if and only if $(-2a)^2 - 4c = 4a^2 - 4c = 0$. Thus, $c = a^2$ and $x^6 + 2ax^4 + cx^2 + b = x^6 + 2ax^4 + a^2x^2 + b \in \mathbb{Q}[x]$, as claimed. The converse is clear, since for the polynomial of the form

$$x^3 + 2ax^2 + a^2x + b = (x - \beta_1)(x - \beta_2)(x - \beta_3)$$

we have $(\beta_1 + \beta_2 + \beta_3)^2 = 4(\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1)$. In view of the above factorization, this implies the equality $\alpha_1 = \alpha_2 + \alpha_3$ for some three roots $\alpha_1 = \sqrt{\beta_1}, \alpha_2 = \theta_4\sqrt{\beta_2}, \alpha_3 = \theta_5\sqrt{\beta_3}$ (where $\theta_4, \theta_5 \in \{-1, 1\}$) of the polynomial $(x^2 - \beta_1)(x^2 - \beta_2)(x^2 - \beta_3)$. This completes the proof of Theorem 1.1 in case $d = 6$.

4. Proof of Theorem 1.1 for $d = 8$

For the rest of this section, let L be the Galois closure of the field $K = \mathbb{Q}(\alpha)$ and let $G = \mathrm{Gal}(L/\mathbb{Q})$. Let $\mathcal{S} := \{\alpha_1, \alpha_2, \ldots, \alpha_8\}$ be the full set of conjugates of α over $\mathbb{Q}$. The Galois group G is determined (in a unique way) by its action on $\mathcal{S}$: it corresponds to some transitive subgroup of the full symmetric group S_8.

We assume, contrary to Theorem 1.1, that the equation $\alpha_1 = \alpha_2 + \alpha_3$ has a solution in conjugate algebraic numbers of degree 8. Then, by the transitivity

of G, each conjugate of α in $\mathcal{S}$ has a representation by a sum of some two conjugates in $\mathcal{S}$. The numbers α_i, α_j and α_k in the representation $\alpha_i = \alpha_j + \alpha_k$ must be pairwise distinct. Our goal is to show that these representations induce serious combinatorial restrictions on the group G.

Lemma 4.1. *Each representation $\alpha_i = \alpha_j + \alpha_k$ is unique.*

Proof. Assume that α_1 has two distinct representations, for instance, $\alpha_1 = \alpha_2 + \alpha_3$ and $\alpha_1 = \alpha_4 + \alpha_5$. (Clearly, the four conjugates α_2, α_3, α_4, α_5 must be pairwise distinct.) By adding these representations and using Lemma 2.4, one obtains

$$2\alpha_1 = \alpha_2+\alpha_3+\alpha_4+\alpha_5 = \mathrm{tr}(\alpha)-(\alpha_1+\alpha_6+\alpha_7+\alpha_8) = -\alpha_1-\alpha_6-\alpha_7-\alpha_8.$$

Hence

$$3\alpha_1 + \alpha_6 + \alpha_7 + \alpha_8 = 0.$$

This contradicts Lemma 2.3. □

The lemma yields the following corollary:

Corollary 4.2. *Suppose that an automorphism $\sigma \in G$ sends $\alpha_i \mapsto \alpha_j$. If $\alpha_i = \alpha_k + \alpha_l$, $\alpha_j = \alpha_m + \alpha_n$, then σ sends $\{\alpha_k, \alpha_l\} \mapsto \{\alpha_m, \alpha_n\}$.*

Proof. One has $\alpha_j = \sigma(\alpha_i) = \sigma(\alpha_k) + \sigma(\alpha_l)$. If $\{\sigma(\alpha_k), \sigma(\alpha_l)\} \neq \{\alpha_m, \alpha_n\}$, then α_j has two distinct representations as sum of elements in $\mathcal{S}$ which contradicts Lemma 4.1. □

We next prove several restrictions on cycle types of elements in group G represented as permutations of the set $\mathcal{S}$.

Lemma 4.3. *G contains no transpositions or cycles of length* 3.

Proof. Assume that G contains a transposition, say, $\sigma = (1, 2)$. Notice that σ stabilizes any α_j with $j > 2$. Consider representations $\alpha_1 = \alpha_k + \alpha_l$ and $\alpha_2 = \alpha_m + \alpha_n$, where $k < l$ and $m < n$. By Corollary 4.2, σ sends $\{\alpha_k, \alpha_l\} \mapsto \{\alpha_m, \alpha_n\}$. If $k > 2$, then $\{\alpha_k, \alpha_l\} = \{\alpha_m, \alpha_n\}$, a contradiction. Similarly, for $k = 1$ we obtain $\alpha_1 = \alpha_1 + \alpha_l$, Thus, $\alpha_l = 0$, a contradiction. The only remaining case is $k = 2$. Then $\sigma(\alpha_2) = \alpha_1$ and $\sigma(\alpha_l) = \alpha_l$. Adding the equalities $\alpha_1 = \alpha_2 + \alpha_l$ and $\alpha_2 = \alpha_1 + \alpha_l$ we arrive at $2\alpha_l = 0$, which is impossible. It follows that G contains no transpositions.

Now assume that G contains a 3-cycle, for instance, $\sigma = (1, 2, 3)$. Then

$$\alpha_1 = \alpha_i + \alpha_j, \qquad \alpha_2 = \alpha_k + \alpha_l, \qquad \alpha_3 = \alpha_m + \alpha_n, \tag{6}$$

where $i < j, k < l$ and $m < n$. By Corollary 4.2, σ sends

$$\{\alpha_i, \alpha_j\} \mapsto \{\alpha_k, \alpha_l\} \mapsto \{\alpha_m, \alpha_n\} \mapsto \{\alpha_i, \alpha_j\}.$$

As above we immediately get a contradiction if $i > 3$ or $i = 1$. So $i = 2$ or $i = 3$. If $i = 3$, then $j > 3$, and, by (6), we have $\alpha_1 = \alpha_3 + \alpha_j$, $\alpha_2 = \alpha_1 + \alpha_j$, $\alpha_3 = \alpha_2 + \alpha_j$. By adding these three equalities, we find that $3\alpha_j = 0$, a contradiction. By the exactly same argument, we exclude the case $i = 2$, $j > 3$. Finally, if $(i, j) = (2, 3)$, then

$$\alpha_1 = \alpha_2 + \alpha_3, \qquad \alpha_2 = \alpha_3 + \alpha_1, \qquad \alpha_3 = \alpha_1 + \alpha_2.$$

Consequently, $\alpha_1 = \alpha_2 = \alpha_3 = 0$, a contradiction. This completes the proof of the lemma. □

Lemma 4.4. *Suppose that an element $\alpha_i \in \mathcal{S}$ is a fixed point of an automorphism $\sigma \in G$, $\sigma \neq id$. If $\alpha_i = \alpha_j + \alpha_k$, then σ transposes α_j and α_k.*

Proof. By re-numbering the conjugates in the set $\mathcal{S}$ if necessary, we may assume that α_1 is the fixed point of σ and that $\alpha_1 = \alpha_2 + \alpha_3$.

Observe that none of the numbers from the set $\{\alpha_1, \alpha_2, \alpha_3\}$ can be equal to another number from the same set with $\pm$ sign: otherwise, from the equality $\alpha_1 = \alpha_2 + \alpha_3$ one arrives at the impossible relation $\alpha_i = 0$ or $\alpha_i = 2\alpha_j$. By Corollary 4.2, σ maps the set $\{\alpha_2, \alpha_3\}$ into itself. Contrary to the statement of the lemma, assume that α_2 and α_3 are fixed points of σ. Write

$$\alpha_2 = \alpha_i + \alpha_j, \qquad \alpha_3 = \alpha_k + \alpha_l. \tag{7}$$

We claim that none of the numbers

$$\alpha_i, \alpha_j, \alpha_k, \alpha_l \tag{8}$$

is equal to α_1, α_2, or α_3.

Indeed, if some of them is equal to α_1, say, $\alpha_i = \alpha_1$, then, adding the equations $\alpha_1 = \alpha_2 + \alpha_3$ and $\alpha_2 = \alpha_1 + \alpha_j$, one obtains $\alpha_3 = -\alpha_j$. Therefore, each element $\alpha_i \in \mathcal{S}$ has a conjugate of the from $-\alpha_i$ in the set $\mathcal{S}$. Thus, $-\alpha_1, -\alpha_2, -\alpha_3$ are conjugate to $\alpha_1, \alpha_2, \alpha_3$. Since σ fixes $\alpha_1, \alpha_2, \alpha_3$, the conjugates $-\alpha_1, -\alpha_2, -\alpha_3$ are also fixed points of σ. Hence, σ has at least six fixed points in the set $\mathcal{S}$ of eight elements. Since $\sigma \neq id$, σ must be a transposition, in contradiction to Lemma 4.3. Therefore, α_1 cannot appear in (8).

Clearly, $\alpha_i \neq \alpha_2$ and $\alpha_j \neq \alpha_2$ (see (7)). If one of the numbers α_i, α_j is equal to α_3, say, $\alpha_i = \alpha_3$, then, by adding the equalities $\alpha_1 = \alpha_2 + \alpha_3$ and $\alpha_2 = \alpha_3 + \alpha_j$ one obtains $2\alpha_3 = \alpha_1 - \alpha_j$ which contradicts Lemma 2.3. Similarly, none of α_k, α_j can be α_2 or α_3.

Therefore, the claim is true, and we can re-label the two roots α_i, α_j that appear in the expression of α_2 in (7) by α_4 and α_5, respectively, so that $\alpha_2 = \alpha_4 + \alpha_5$.

Next, notice that σ must contain the transposition $(4, 5)$. Indeed, since α_2 is a fixed point of σ, by Corollary 4.2, the set $\{\alpha_4, \alpha_5\}$ must be mapped into itself. If σ fixes at least one of element from the pair α_4, then it must fix another. In such a case, the conjugates $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ are five distinct fixed points of σ, therefore, σ is either a three cycle or a transposition of the remaining elements of $\mathcal{S}$. By Lemma 4.3, this is impossible.

Consider two remaining elements α_k, α_l in the expression of α_3 in (7). Clearly, $\{\alpha_k, \alpha_l\} \neq \{\alpha_4, \alpha_5\}$. Furthermore, none of α_k, α_l can be equal to α_4 or α_5. Otherwise, applying σ to, say, $\alpha_3 = \alpha_4 + \alpha_l$, where $l \neq 5$, we find that $\alpha_3 = \alpha_5 + \sigma(\alpha_l)$, contrary to Lemma 4.1. Thus, we can re-label the conjugates in such a way that elements α_k and α_l become α_6 and α_7. Then σ must contain the transposition $(6, 7)$, for otherwise, σ would have at least five fixed points $\alpha_1, \alpha_2, \alpha_3, \alpha_6, \alpha_7$ in $\mathcal{S}$ and the transposition $(4, 5)$, so it must be equal to the transposition, in contradiction to Lemma 4.3.

It follows that σ stabilizes points $\alpha_1, \alpha_2, \alpha_3$ and contains the transpositions $(4, 5)$ and $(6, 7)$. Then the remaining element α_8 must be the fixed point of σ. Therefore, $\sigma = (4, 5)(6, 7)$, and one has

$$\alpha_1 = \alpha_2 + \alpha_3, \qquad \alpha_2 = \alpha_4 + \alpha_5, \qquad \alpha_3 = \alpha_6 + \alpha_7. \tag{9}$$

Let us write $\alpha_8 = \alpha_m + \alpha_n$ for the remaining element α_8. By Corollary 4.2, σ sends the set $\{\alpha_m, \alpha_n\}$ into itself. There can be no transposition of (m, n) in σ: as we already know, the transposed pairs $\{\alpha_4, \alpha_5\}$ and $\{\alpha_6, \alpha_7\}$ sum to α_2 and α_3, respectively. Obviously, $\alpha_m, \alpha_n \neq \alpha_8$. This means that $\{\alpha_m, \alpha_n\}$ is a subset of the set of fixed points $\{\alpha_1, \alpha_2, \alpha_3\}$, so α_8 is equal to the sum of two fixed elements. Also, $\alpha_8 \neq \alpha_2 + \alpha_3 = \alpha_1$. Hence,

$$\alpha_8 = \alpha_1 + \alpha_2 \quad \text{or} \quad \alpha_8 = \alpha_1 + \alpha_3. \tag{10}$$

In a combination with the first equality in (9), the first relation in (10) yields $2\alpha_2 = \alpha_8 - \alpha_3$, while the second relation in (10) combined with the first equality of (9) yields $2\alpha_3 = \alpha_8 - \alpha_2$. Both cases are impossible in view of Lemma 2.3. We have arrived at a contradiction, by assuming that σ fixes α_2 and α_3. Therefore, σ must transpose them. □

Lemma 4.5. *Each element $\sigma \in G$, $\sigma \neq id$ that does not move every conjugate in $\mathcal{S}$ has precisely 2 fixed points in $\mathcal{S}$.*

Proof. Suppose that σ has at least one fixed point. We first show that σ contains at most two fixed points. Indeed, if $\alpha_1, \alpha_2, \alpha_3$ are three distinct conjugates that are fixed points of σ, then can write $\alpha_1 = \alpha_i + \alpha_j$, $\alpha_2 = \alpha_k + \alpha_l$, $\alpha_3 = \alpha_m + \alpha_n$. According to Lemma 4.4, σ contains the transpositions (i, j), (k, l), (m, n). These are, clearly, disjoint transpositions. Hence, σ moves 6 elements, so it has at most 2 fixed points, a contradiction.

We next show that σ cannot have just one fixed point. Suppose that α_1 is a single fixed point of σ, and $\alpha_1 = \alpha_2 + \alpha_3$. Then σ contains a transposition $(2, 3)$. Since even numbers do not add to 5, by decomposing σ into disjoint cycles, one finds that there must be at least one cycle of odd length $k = 3$ or $k = 5$. Then the element $\tau = \sigma^k$ is not equal to id (it still possesses a transposition $(1, 2)$) and has ≥ 4 fixed points, which contradicts to what we have just proved above. □

Corollary 4.6. *G contains no elements σ that have the following cycle length formulas: $2 + 2$ (products of two disjoint transpositions), 4 (single 4-cycles), $2 + 4$ (disjoint products of a transposition and 4-cycle), $2 + 2 + 4$ (two transpositions and a 4-cycle, all disjoint).*

Proof. For any permutation σ with these cycle lengths, either the element σ or $\sigma^2 \neq id$ has precisely four fixed points in $\mathcal{S}$, which contradicts Lemma 4.5. □

Lemma 4.7. *There are no elements of order 8 in G.*

Proof. If $\tau \in G$ is an element of order 8, than it is a cycle of length 8 on $\mathcal{S}$. Consider the cyclic subgroup H generated by τ. It is an Abelian subgroup of G of order $|H| = 8$ that acts transitively on all elements of $\mathcal{S}$. By Lemma 2.5, if $\alpha_i = \alpha_j + \alpha_k$, then the order of H must be divisible by 6, a contradiction.

□

Lemma 4.8. *Let H be the stabilizer subgroup $H = St(\alpha_i, \alpha_j)$, $i \neq j$, in G. Then either $St(\alpha_i, \alpha_j) = \{id\}$ or $St(\alpha_i, \alpha_j) = \{id, \sigma\}$, where σ is a product of three disjoint transpositions.*

Proof. If there are no elements $\sigma \neq id$ in G that stabilize both α_i and α_j, we are done. Assume that such an element exists. For convenience, relabel elements α_i and α_j by α_1 and α_2. By Lemma 4.4, there exist four distinct conjugates α_3, α_4, α_5, α_6 in $\mathcal{S}$, all different from α_1 and α_2, such that $\alpha_1 = \alpha_3 + \alpha_4$, $\alpha_2 = \alpha_5 + \alpha_6$. Also, Lemma 4.4 implies that σ contains transpositions $(3, 4)$ and $(5, 6)$. Now, consider two remaining conjugates α_7 and α_8 in $\mathcal{S}$. By Lemma 4.5, they cannot remain stable under σ (as α_1 and α_2 are the only fixed points). Thus, σ transposes them. From this, we conclude that $\sigma = (3, 4)(5, 6)(7, 8)$. The permutation σ is unique (up to the re-numeration of elements of $\mathcal{S}$), since the representations of numbers $\alpha_1 = \alpha_3 + \alpha_4$ and $\alpha_2 = \alpha_5 + \alpha_6$ are unique, by Lemma 4.1. Therefore, the order of $\mathrm{St}(\alpha_i, \alpha_j)$ is at most 2. □

Lemma 4.9. *For each $\alpha_i \in \mathcal{S}$, the order of the stabilizer subgroup $H = St(\alpha_i)$ is at most 2.*

Proof. If $H = \{id\}$, we are done. Assume that H contains an element $\sigma \neq id$. We claim that σ is the only non-identity element in H. Indeed, suppose that $\tau \neq id$ is also in H. Then, by Lemma 4.5 and Lemma 4.8, both σ and τ are elements of order 2 (products of 3 disjoint transpositions). From this, it follows that any element of H that is not equal to id is of order 2. But then H must be Abelian. Moreover, by Lemma 4.5, σ has two fixed points: α_i, and some other fixed point α_j. Since $\tau \in H$, α_i is the fixed point of τ. By the commutativity in H, $\sigma\tau = \tau\sigma$. Hence, $\sigma(\tau(\alpha_j)) = \tau(\sigma(\alpha_j)) = \tau(\alpha_j)$. Therefore, $\tau(\alpha_j)$ is a fixed point of σ, and hence $\tau(\alpha_j) = \alpha_i$ or $\tau(\alpha_j) = \alpha_j$. The first case is impossible, because α_i is a fixed point of τ. Thus, $\tau(\alpha_j) = \alpha_j$. This means that both elements $\tau, \sigma \in \mathrm{St}(\alpha_i, \alpha_j)$. By Lemma 4.8, this group is of order ≤ 2, so $\tau = \sigma$ and $|H| \leq 2$. □

Corollary 4.10. *G is of order $|G| = 8$ or $|G| = 16$.*

Proof. Since G is a transitive permutation group of degree 8, the orbit stabilizer theorem implies that the index of $\mathrm{St}(\alpha_1) =: H$ is $[G : H] = 8$. By Lemma 4.9, the order $|H|$ equals 1 or 2. Therefore, we must have $|G| = [G : H] \cdot |H| = 8$ or 16. □

Lemma 4.11. *If G contains a subgroup $H \cong D_4$ or $H \cong Q_8$, then the action of H on $\mathcal{S}$ is not transitive.*

Proof. Suppose that the action of automorphisms of H on the elements of $\mathcal{S}$ is transitive. By the orbit stabilizer theorem, $\mathrm{St}_H(\alpha_1) = id$. Since the permutation action of H on $\mathcal{S}$ is isomorphic to the action on the left cosets of $\tau\,\mathrm{St}_h(\alpha_1)$, $\tau \in G$, all permutations of H can differ only by re-numeration of elements in $\mathcal{S}$. Therefore, one may assume that the permutation representations of G coincide with the one given in Lemma 2.7 or Lemma 2.6 (these representations, up to conjugation in S_8, correspond to the groups no. 8T4 and 8T5 in the GAP [8] database of transitive groups). If the relation $\alpha_i = \alpha_j + \alpha_k$ holds, then the respective group determinants given in Lemmas 2.7, 2.6 must vanish after the substitution $x_i = 1$, $x_j = x_k = -1$, $x_l = 0$ for $l \notin \{i, j, k\}$. By looking at the respective values of polynomials F_1, F_2, F_3, F_4 modulo 2, we see that they do not vanish. Notice that $F_5 \equiv F_1^2 \pmod 2$, so they also do not vanish. From this, it follows that $\alpha_i \neq \alpha_j + \alpha_k$. □

Now we can conclude the proof of Theorem 1.1 for $d = 8$. By Corollary 4.10, $|G| = 8$ or $|G| = 16$.

First, consider the case $|G| = 8$. Then G must be isomorphic to one of the 3 Abelian groups C_8, $C_4 \times C_2$, C_2^3 or one of the two non-commutative groups: the dihedral group D_4 or the quaternion group Q_8. The cases when G are Abelian are ruled out by Lemma 2.5. Therefore, $G \cong D_4$ or $G \cong Q_8$. By Lemma 4.11 (with $G = H$), this is impossible.

Now, consider the case $|G| = 16$. As we saw in the proof of Corollary 4.10, the stabilizer subgroups $H = \mathrm{St}(\alpha_j)$ must have order 2; the automorphisms $\sigma \neq id$ from H must have precisely 2 fixed points and 3 disjoint transpositions by Lemma 4.5 and Lemma 4.8. Then G must be isomorphic to one of the six groups from the GAP [8] list of transitive groups of degree 8: quaternion group Q_8, dihedral group D_8, the semi-direct product of Abelian groups $C_8 : C_2$, the quasi-dihedral (a.k.a semi-dihedral) group QD_{16}, the direct product $D_4 \times C_2$, the semi-direct product of Abelian groups $C_2^2 : C_4$ and the semi-direct product $Q_8 : C_2$ (GAP ID numbers for these groups are 8T6, 8T7, 8T8, 8T9, 8T10, 8T11, respectively). By looking into the cycle types of the permutation representations of these groups in GAP, one finds that the permutation groups groups $C_8 : C_2$, $D_4 \times C_2$, $C_2^2 : C_4$, $Q_8 : C_2$ contain permutations of the cycle type $2 + 2$ in the stabilizer subgroups $\mathrm{St}(\alpha_j)$, in contradiction to Lemma 4.6. In fact, GAP list contains only two groups whose stabilizer subgroups $\mathrm{St}(\alpha_j)$ has permutations of the right cycle types: the group D_8 and QD_{16}. However, both groups contain a cycle of length 8, which is impossible by Lemma 4.7. This completes the proof of Theorem 1.1.

5. Proof of Theorem 1.2

By Lemma 2.1, d cannot be 5 or 7. If $d = 4$, then $\alpha_1 + \alpha_2 + \alpha_3 = 0$ combined with Lemma 2.4 yields $\alpha_4 = 0$, which is impossible.

Assume next that $d = 8$. Let N be the number of distinct equalities $\alpha_i + \alpha_j + \alpha_k = 0$ obtained by applying all automorphisms of the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ to $\alpha_1 + \alpha_2 + \alpha_3 = 0$. Suppose also that each α_i occurs exactly ℓ times in these equalities. Then $3N = 8\ell$, so ℓ must be divisible by 3. In particular, $\ell \geq 3$. Note that the intersection of two distinct sets of indices $\{i, j, k\}$ and $\{i', j', k'\}$ satisfying $\alpha_i + \alpha_j + \alpha_k = 0$ and $\alpha_{i'} + \alpha_{j'} + \alpha_{k'} = 0$ is either empty or contains at most one element, since $\{i, j, k\} \cap \{i', j', k'\}$ cannot consist of exactly two indices. So, by considering the equalities of the form $\alpha_1 + \alpha_i + \alpha_j = 0$ (there are at least three such equalities), we find that after re-indexing the conjugates, the following three equalities

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \alpha_1 + \alpha_4 + \alpha_5 = 0, \quad \alpha_1 + \alpha_6 + \alpha_7 = 0$$

hold. Adding them and using the fact that, by Lemma 2.4, $\mathrm{tr}(\alpha) = 0$ we deduce $2\alpha_1 + \alpha_1 + \alpha_2 + \cdots + \alpha_7 = 2\alpha_1 - \alpha_8 = 0$. This contradicts Lemma 2.3.

It remains to consider the case $d = 6$. This time, the intersection of two distinct sets of indices $\{i, j, k\}$ and $\{i', j', k'\}$ satisfying $\alpha_i + \alpha_j + \alpha_k = 0$ and $\alpha_{i'} + \alpha_{j'} + \alpha_{k'} = 0$ cannot contain one element. Otherwise, if $i = i'$ is this element, and l the remaining index in the set $\{1, \ldots, 6\}$ after removing the indices i, j, k, j', k', then

$$0 = \alpha_i + \alpha_j + \alpha_k + \alpha_i + \alpha_{j'} + \alpha_{k'} = \alpha_i - \alpha_l$$

yields $\alpha_i = \alpha_l$, a contradiction. Thus, the intersection of the sets $\{i, j, k\}$ and $\{i', j', k'\}$ must be empty. Consequently, we have exactly two equalities of the form $\alpha_i + \alpha_j + \alpha_k = 0$, namely, $\alpha_1 + \alpha_2 + \alpha_3 = 0$ and $\alpha_4 + \alpha_5 + \alpha_6 = 0$.

Now, we consider two polynomials $p_1(x) := (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = x^3 + ux + v$ and $p_2(x) := (x - \alpha_4)(x - \alpha_5)(x - \alpha_6) = x^3 + u'x + v'$. Their product is the minimal polynomial of α over $\mathbb{Q}$:

$$p(x) = (x^3 + ux + v)(x^3 + u'x + v') \in \mathbb{Q}[x] \tag{11}$$

that expands to

$$p(x) = x^6 + (u + u')x^4 + (v + v')x^3 + uu'x^2 + (uv' + u'v)x + vv'. \tag{12}$$

Since $u + u' \in \mathbb{Q}$ and $uu' \in \mathbb{Q}$, the numbers u, u' are either both rational or they are quadratic conjugates. The same is true for the pair v, v'. Note that u and v cannot be both rational, since then $p_1(x) \in \mathbb{Q}[x]$ is the factor of $p(x)$, which is impossible in view of $\deg \alpha = 6$. So at least one pair consists quadratic conjugates lying in a quadratic field K. We claim that u, u' and v, v' actually lie in the same quadratic field K and that u is conjugate to u' and v is conjugate to v' over $\mathbb{Q}$.

Put $r := u + u' \in \mathbb{Q}$ and write the rational number $s := uv' + u'v$ (see (12)) in the form

$$s = uv' + (r - u)v = u(v' - v) + rv.$$

If $v \in \mathbb{Q}$, then v' must be equal to v, since $u \notin \mathbb{Q}$ and $v' \in \mathbb{Q}$ as $v \in \mathbb{Q}$. Also, $K = \mathbb{Q}(u)$ is quadratic over $\mathbb{Q}$ and contains u'. The above claim is true, since v, v' are rational numbers in $K = \mathbb{Q}(u)$ that are conjugate over $\mathbb{Q}$ in view of $v = v'$.

Assume next that $v \notin \mathbb{Q}$. Then v, v' are quadratic conjugates, $v \neq v'$, and $K = \mathbb{Q}(v) = \mathbb{Q}(v')$. One can express u in terms of r, s, v, v' as

$$u = (s - rv)/(v' - v).$$

Hence, $u \in K$, so it must be either rational or quadratic over $\mathbb{Q}$. If it is rational, then, by interchanging the roles of u's and v's in the argument given above, one easily shows that $u = u'$. Thus, the claim is true. If $u \in K$ is quadratic then its conjugate u' also belongs to K and the claim is also true.

Since the numbers u, u', v and v' all lie in the same quadratic field K, say $K = \mathbb{Q}(\sqrt{t})$, where t is a square-free integer, by writing $u = a + c\sqrt{t}$, $u' = a - c\sqrt{t}$ (and, similarly, v and v') we see that there exist some rational numbers a, b, c, e such that

$$\begin{aligned} u + u' &= 2a, \qquad v + v' = 2b \\ (u - u')^2 &= 4c^2t, \quad (v - v')^2 = 4e^2t. \end{aligned}$$

Here, c and e are not both zero, since otherwise $u = u' \in \mathbb{Q}$ and $v = v' \in \mathbb{Q}$, so $p_1(x) = p_2(x) \in \mathbb{Q}[x]$. From the above equalities one quickly deduces that

$$uu' = \frac{(u+u')^2 - (u-u')^2}{4} = a^2 - c^2 t,$$

$$vv' = \frac{(v+v')^2 - (v-v')^2}{4} = b^2 - e^2 t,$$

and, with an appropriate choice of the signs for the rational numbers c and e,

$$uv' + vu' = \frac{(u+u')(v+v') - (u-u')(v-v')}{2} = 2(ab - cet). \quad (13)$$

This proves the formula given in Theorem 1.2.

Conversely, if an irreducible polynomial $p(x) \in \mathbb{Q}[x]$ is of the form given by the formula of Theorem 1.2, namely,

$$x^6 + 2ax^4 + 2bx^3 + (a^2 - c^2 t)x^2 + 2(ab - cet)x + b^2 - e^2 t$$

with rational a, b, c, e and some square-free integer t, then $p(x)$ factors over the field $K = \mathbb{Q}(\sqrt{t})$ as $p(x) = p_1(x)p_2(x)$, where $p_1(x) = x^3 + ux + v \in K[x]$ and $p_2(x) = x^3 + u'x + v' \in K[x]$ are as in equations (11), (12) with coefficients u, u', v, v' of $p_1(x)$ and $p_2(x)$ defined as roots of the quadratic equations

$$x^2 - 2ax + a^2 - c^2 t = 0 \quad \text{and} \quad x^2 - 2bx + b^2 - e^2 t = 0,$$

respectively. This can be easily seen by working backwards through the formulas given in the previous part of the proof leading to the formula (13). Hence, the sum of three conjugates of α over $\mathbb{Q}$ that are roots of, say $p_1(x)$, must be zero and the proof of Theorem 1.2 is finished.

This research was supported in part by the Research Council of Lithuania Grant MIP-068/2013/LSS-110000-740.

References

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

[2] A. Dubickas, On the degree of a linear form in conjugates of an algebraic number, *Illinois J. Math.*, **46** (2002) 571–585.

[3] A. Dubickas, K. Hare and J. Jankauskas, No two non-real conjugates of a Pisot number have the same imaginary part, (submitted).

[4] A. Dubickas and C. J. Smyth, Problem 11123, American Mathematical Monthly, **111** (2004) 916.

[5] A. Dubickas and C. J. Smyth, On the lines passing through two conjugates of a Salem number, *Math. Proc. Camb. Phil. Soc.*, **144** (2008) 29–37.

[6] M. Drmota and M. Skałba, On multiplicative and linear independence of polynomial roots, in: Contributions to General Algebra 7 (eds. D. Dorninger, G. Eigenthaler, H. K. Kaiser and W. B. Muwller), Hoelder–Pichler–Tempsky, Wien; Teubner, Stuttgart (1991) 127–135.
[7] M. Drmota and M. Skałba, Relations between polynomial roots, *Acta Arith.*, **71** (1995) 65–77.
[8] The GAP Group, GAP – Groups, Algorithms, and Programming, (Version 4.7.5) (2014) http://www.gap-system.org.
[9] V. A. Kurbatov, Galois extensions of prime degree and their primitive elements, *Soviet Math. (Izv. VUZ)*, **21** (1977) 49–52.
[10] C. J. Smyth, Conjugate algebraic numbers on conics, *Acta Arith.*, **40** (1982) 333–346.
[11] W. A. Stein, *et al.*, Sage mathematics software, (Version 6.3), The Sage Development Team, (2014) http://www.sagemath.org.