Canad. Math. Bull. 2025, pp. 1–16
http://dx.doi.org/10.4153/S0008439525101148
© The Author(s), 2025. Published by Cambridge University Press on behalf of Canadian Mathematical Society. This is an Open Access article, distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives licence (https://creativecommons.org/licenses/by-nc-nd/4.0), which permits non-commercial re-use, distribution, and reproduction in any medium, provided that no alterations are made and the original article is properly cited. The written permission of Cambridge University Press must be obtained prior to any commercial use and/or adaptation of the article.

Linear relations of four conjugates of an algebraic number

Žygimantas Baronėnas, Paulius Drungilas, and Jonas Jankauskas

Abstract. We characterize all algebraic numbers α of degree $d \in \{4,5,6,7\}$ for which there exist four distinct algebraic conjugates α_1, α_2, α_3, and α_4 of α satisfying the relation $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$. In particular, we prove that an algebraic number α of degree 6 satisfies this relation with $\alpha_1 + \alpha_2 \notin \mathbb{Q}$ if and only if α is the sum of a quadratic and a cubic algebraic number. Moreover, we describe all possible Galois groups of the normal closure of $\mathbb{Q}(\alpha)$ for such algebraic numbers α. We also consider similar relations $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ and $\alpha_1 + \alpha_2 + \alpha_3 = \alpha_4$ for algebraic numbers of degree up to 7.

1 Introduction

Let $\alpha_1 := \alpha, \alpha_2, \dots, \alpha_d$ be the algebraic conjugates of an algebraic number α of degree d over $\mathbb{Q}$. In the present article, we will be interested in algebraic numbers α of small degree d (namely, $d \leqslant 7$) whose conjugates satisfy one of the equations

$$(1) \qquad \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0, \ \alpha_1 + \alpha_2 + \alpha_3 = \alpha_4 \ \text{ or } \ \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4.$$

The main motivation to study 1 stems from the article of Dubickas and Jankauskas [5] where they investigated the linear relations $\alpha_1 = \alpha_2 + \alpha_3$ and $\alpha_1 + \alpha_2 + \alpha_3 = 0$ in conjugates of an algebraic number α of degree $d \leqslant 8$ over $\mathbb{Q}$. They proved 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 gave explicit formulas for all possible minimal polynomials of such algebraic numbers. In particular, equation $\alpha_1 = \alpha_2 + \alpha_3$ is solvable in roots of an irreducible sextic polynomial if and only if it is an irreducible polynomial of the form

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

Similarly, for d in the range $4 \leqslant d \leqslant 8$ (the case $d = 3$ is trivial), equation $\alpha_1 + \alpha_2 + \alpha_3 = 0$ is solvable 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 $t \in \mathbb{Z}$.

Received by the editors July 16, 2025; revised August 18, 2025; accepted August 19, 2025.
Published online on Cambridge Core September 4, 2025.
AMS subject classification: **11R04**, **11R32**.
Keywords: Algebraic numbers, linear relations in algebraic conjugates.

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

Let $\alpha_1, \alpha_2, \alpha_3$ be three distinct algebraic conjugates of an algebraic number α of degree $d \leqslant 8$. Recently, Virbalas [16] extended the research of Dubickas and Jankauskas [5] by determining all possible linear relations of the form $a\alpha_1 + b\alpha_2 + c\alpha_3 = 0$ with non-zero rational numbers a, b, c. He also obtained a complete list of transitive groups that can occur as Galois groups for the minimal polynomial of such an algebraic number α. Moreover, Virbalas [15] proved that for any prime number $p \geqslant 5$ there does not exist an irreducible polynomial $p(x) \in \mathbb{Q}[x]$ of degree $2p$ with three distinct roots adding up to zero.

Recently, Dubickas and Virbalas [7] proved that every nontrivial linear relation between algebraic conjugates has a corresponding multiplicative relation. They also gave a complete characterization of all possible linear relations between four distinct algebraic conjugates of degree 4 (see also [10]). Moreover, Serrano Holgado [8] characterized irreducible quartic polynomials (not necessarily over $\mathbb{Q}$) having nontrivial multiplicative relations among their roots.

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 $|\alpha_j| < 1$. Dubickas, Hare, and Jankauskas in [4] showed that there are no Pisot numbers whose conjugates satisfy the equation $\alpha_1 = \alpha_2 + \alpha_3$. They also proved the impossibility of

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 \tag{2}$$

in conjugates of a Pisot number of degree $d > 4$, by showing that there is a unique Pisot number, namely, $\alpha = (1 + \sqrt{3 + 2\sqrt{5}})/2$ whose conjugates satisfy 2. This particular number α was first found in [6].

Throughout this article, the term *algebraic number* means algebraic number over the field of rational numbers $\mathbb{Q}$. Similarly, the term *irreducible polynomial* means irreducible over $\mathbb{Q}$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ be the algebraic conjugates of an algebraic number α of degree d. Then $tr(\alpha) := \alpha_1 + \alpha_2 + \cdots + \alpha_d$ is called *the trace* (or *the absolute trace*) of α. In the present article, we restrict ourselves to the degrees in the range $4 \leqslant d \leqslant 7$. The case $d = 8$ is more complicated and will be treated in the future. We will not assume that α is a Pisot number in the equations 1. For the first two equations in 1, we have the following result.

Theorem 1 *Let α be an algebraic number of degree d, where $d \in \{4, 5, 6, 7\}$.*

(i) *Some four distinct algebraic conjugates of α satisfy the relation*

$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$$

if and only if $d = 4$ and $tr(\alpha) = 0$ or $d = 6$ and the minimal polynomial of α is an irreducible polynomial of the form

$$x^6 + ax^4 + bx^2 + c \in \mathbb{Q}[x].$$

(ii) *No four distinct conjugates of α satisfy the relation*

$$\alpha_1 + \alpha_2 + \alpha_3 = \alpha_4.$$

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

The following theorem treats algebraic numbers α of degree $d \in \{4, 5, 6, 7\}$ with some four distinct algebraic conjugates satisfying the relation

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

Note that for any $r \in \mathbb{Q}$, replacing α with $\alpha - r$ does not affect the relation (3). By setting $r = tr(\alpha)/d$, we obtain an algebraic number $\alpha - tr(\alpha)/d$ whose trace equals zero. Therefore, without loss of generality, we assume that α has zero trace.

Theorem 2 *Let α be an algebraic number of degree $d \in \{4, 5, 6, 7\}$ and $tr(\alpha) = 0$. Denote by $p(x)$ the minimal polynomial of α. Suppose that some four distinct algebraic conjugates of α satisfy the relation (3). Then either $d = 4$ or $d = 6$. Moreover, the following statements are true:*

(i) *If $d = 4$, then $p(x)$ is an irreducible polynomial of the form*

$$p(x) = x^4 + ax^2 + b$$

for some rational numbers $a, b \in \mathbb{Q}$. Conversely, for any such irreducible polynomial $p(x)$, the four distinct roots of $p(x)$ satisfy the relation (3).

(ii) *Suppose that $d = 6$ and the sum $\alpha_1 + \alpha_2$ in (3) is a rational number. Then $p(x)$ is an irreducible polynomial of the form*

$$p(x) = x^6 + ax^4 + bx^2 + c$$

for some rational numbers $a, b, c \in \mathbb{Q}$. Conversely, for any such irreducible polynomial $p(x)$, some four distinct roots of $p(x)$ satisfy the relation (3).

(iii) *Suppose that $d = 6$ and the sum $\alpha_1 + \alpha_2$ in (3) is not a rational number (i.e., $\alpha_1 + \alpha_2 \in \mathbb{C}\backslash\mathbb{Q}$). Then $p(x)$ is an irreducible polynomial of the form*

$$p(x) = x^6 + (2b - 3a)x^4 + 2cx^3 + (3a^2 + b^2)x^2 + 2c(3a + b)x \\ - a^3 - 2a^2b - ab^2 + c^2$$

for some rational numbers $a, b, c \in \mathbb{Q}$. Conversely, for any such irreducible polynomial $p(x)$, some four distinct roots of $p(x)$ satisfy the relation (3).

The following theorem gives an alternative description of sextic algebraic numbers α that satisfy the relation (3) with $\alpha_1 + \alpha_2 \notin \mathbb{Q}$. We will derive this result from Proposition 11 (see Section 2).

Theorem 3 *Let α be an algebraic number of degree 6. Some four distinct algebraic conjugates of α satisfy the relation $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 =: \beta \notin \mathbb{Q}$ if and only if α equals the sum of a quadratic and a cubic algebraic number.*

Let α be an algebraic number of degree d and let G be the Galois group of the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Note that this normal closure is also the splitting field of the minimal polynomial of α over $\mathbb{Q}$, and therefore G is the Galois group of this polynomial. The group G is determined (in a unique way) by its action on $\mathcal{S} = \{\alpha_1, \alpha_2, \dots, \alpha_d\}$: it corresponds to some transitive subgroup of the full symmetric

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

Table 1: One-parameter families of even sextic polynomials $p(x)$ with corresponding Galois groups G.

Polynomial $p(x)$	Galois group G of $p(x)$
$x^6 + (t^2+5)x^4 + ((t-1)^2+5)x^2 + 1$	C_6
$x^6 + 3t^2$	S_3
$x^6 + 2t^2$	D_6
$x^6 - 3t^4x^2 - t^6$	A_4
$x^6 - 3t^2x^2 + t^3$	$A_4 \times C_2$
$x^6 + t^2x^4 - t^6$	S_4^+
$x^6 + (31t^2)^2x^2 + (31t^2)^3$	S_4^-
$x^6 + (2t^2)^2x^2 + (2t^2)^3$	$S_4 \times C_2$

group S_d. Next, we will consider possible groups G, related to the algebraic numbers α in Theorems 1 and 2.

If $d = 4$ and the linear relation in Theorem 1 is satisfied, then G is isomorphic to one of five transitive subgroups of the symmetric group S_4, namely, V_4 (Klein 4-group), C_4 (a cyclic group of order 4), D_4 (a dihedral group of order 8), A_4 (the alternating group), or S_4 itself. There are no more transitive subgroups of S_4 (see, e.g., [2, Chapter 3] or [12]).

If $d = 6$ and some four distinct conjugates of α satisfy the relation in (i) of Theorem 1, then we need to look at the transitive subgroups of S_6. Awtrey and Jakes in [1] investigated the Galois groups of even sextic polynomials $x^6 + ax^4 + bx^2 + c$ with coefficients from a field of characteristic $\neq 2$. In this particular case, there are eight possibilities for the Galois group G:

$$C_6,\ S_3,\ D_6,\ A_4,\ A_4 \times C_2,\ S_4^+,\ S_4^-,\ S_4 \times C_2, \tag{4}$$

where S_4^+ and S_4^- are certain transitive subgroups of S_6 of order 24. Note that, in total, there are 16 transitive subgroups of S_6 (see, e.g., [2, Chapter 3]). Awtrey and Jakes in [1] also provided one-parameter families of even sextic polynomials (for values of $t \in \mathbb{Q}$ that result in irreducible polynomials) with specified Galois group over $\mathbb{Q}$ (see Table 1).

If $d = 4$ and the linear relation in (3) is satisfied, then G is one of three transitive subgroups of the symmetric group S_4: V_4, C_4, or D_4. This result is due to Kappe and Warren (see [9, Theorem 3]). Again, Awtrey and Jakes in [1] provided one-parameter families of even quartic polynomials (except for values of $t \in \mathbb{Q}$ that result in reducible polynomials) with specified Galois group over $\mathbb{Q}$ (see Table 2).

If $d = 6$ and some four distinct conjugates of α satisfy $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 \in \mathbb{Q}$, then the Galois group is, again, one of the already mentioned eight transitive subgroups in 4.

The most interesting case is the following.

Theorem 4 *Let α be an algebraic number of degree 6 and $tr(\alpha) = 0$. Suppose that some four distinct algebraic conjugates of α satisfy the relation*

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 =: \beta \notin \mathbb{Q}.$$

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

Table 2: One-parameter families of even quartic polynomials $p(x)$ with corresponding Galois groups G.

Polynomial $p(x)$	Galois group G of $p(x)$
$x^4 + (2t+1)^2$	V_4
$x^4 + 4tx^2 + 2t^2$	C_4
$x^4 + t^2 + 1, \ t \neq 0$	D_4

Table 3: Minimal polynomials $p(x)$ from part (iii) of Theorem 2 with the corresponding Galois groups G.

Polynomial $p(x)$	(a, b, c)	Galois group G of $p(x)$
$x^6 - 6x^4 + 4x^3 + 12x^2 + 24x - 4$	$(2, 0, 2)$	D_6
$x^6 - 3x^4 + 2x^3 + 12x^2 - 12x + 17$	$(-1, -3, 1)$	C_6
$x^6 - 3x^4 + 8x^3 + 12x^2 - 48x + 32$	$(-1, -3, 4)$	S_3

Table 4: Polynomials $p(x)$ that are not of the form given in (iii) of Theorem 2 with the corresponding Galois groups G.

Polynomial $p(x)$	Galois group G of $p(x)$
$x^6 + 2x^3 + 2$	D_6
$x^6 + x^3 + 1$	C_6
$x^6 + 54x^3 + 1029$	S_3

Then, the Galois group of the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is isomorphic to one of three groups: the dihedral group D_6 of order 12, the symmetric group S_3, or the cyclic group C_6.

Theorem 4 follows from Proposition 11, which gives more details on the possible Galois group of the normal closure of $\mathbb{Q}(\alpha)$. Moreover, all three groups in Theorem 4 arise as Galois groups in this setting, i.e., for any group $G \in \{D_6, S_3, C_6\}$, there exists an algebraic number α of degree 6 satisfying $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 \notin \mathbb{Q}$ such that the Galois group of the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is isomorphic to G. Corresponding examples are provided in Table 3.

The converse of Theorem 4 is false, i.e., for any group $G \in \{D_6, S_3, C_6\}$, there exists an algebraic number α of degree 6 such that the Galois group of the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is isomorphic to G and no four distinct algebraic conjugates of α satisfy the relation $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$. Indeed, it suffices to take an irreducible polynomial of degree 6, having the specified Galois group, which is not of the form given in (iii) of Theorem 2. Such examples are provided in Table 4.

The article is organized as follows. Some auxiliary results are stated in Section 2. The proofs of the main results are given in Section 3. We first prove Propositions 10 and 11. Theorem 4 directly follows from Proposition 11. Then, we use Proposition 11 to prove Theorem 3, which then is used to prove Theorem 2.

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

2 Auxiliary results

The following result is due to Kurbatov [11]. We will use it to eliminate impossible relations among algebraic conjugates.

Lemma 5 *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* $k_1 = k_2 = \cdots = k_d$.

Smyth's result from [13] is useful for similar purposes.

Lemma 6 *If* $\alpha_1, \alpha_2, \alpha_3$ *are three conjugates of an algebraic number satisfying* $\alpha_1 \neq \alpha_2$ *then* $2\alpha_1 \neq \alpha_2 + \alpha_3$.

The following result is a generalization of Lemma 6 proved by Dubickas [3].

Lemma 7 *If* $\beta_1, \beta_2, \ldots, \beta_n$, *where* $n \geqslant 3$, *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* $|k_1| \geqslant |k_2| + \cdots + |k_n|$ *then*

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

Dubickas and Jankauskas, in their paper [5], proved the following result.

Lemma 8 *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* $tr(\alpha) := \alpha_1 + \alpha_2 + \cdots + \alpha_d = 0$.

The following result is a partial case of Theorem 1.3 in [17].

Lemma 9 *Suppose that* α *and* β *are algebraic numbers over* $\mathbb{Q}$ *of degree* m *and* n, *respectively. If* m *and* n *are coprime integers, then* $\alpha + \beta$ *is a primitive element of the compositum* $\mathbb{Q}(\alpha, \beta)$, *i.e.,* $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$.

To prove Proposition 11 and Theorem 2, we will need the following result.

Proposition 10 *Let* α *be an algebraic number of degree* $d = 6$ *and* $tr(\alpha) = 0$. *Suppose that some four distinct conjugates of* α *satisfy the relation*

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4.$$

Then either $\alpha_1 + \alpha_2 = 0$ *or* $\alpha_1 + \alpha_2$ *is an algebraic number of degree* 3 *and* $tr(\alpha_1 + \alpha_2) = 0$.

Denote $\pi := (1\ 2\ 5\ 4\ 3\ 6)$, $\sigma = \pi^4 = (1\ 3\ 5)(2\ 6\ 4)$, and $\tau = (1\ 2)(3\ 4)(5\ 6)$, permutations of the symmetric group S_6. Theorem 4 is a corollary of the following proposition, which will also be used in the proof of Theorem 3.

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

Proposition 11 *Let α be an algebraic number of degree 6 and $tr(\alpha) = 0$. Suppose that some four distinct algebraic conjugates of α satisfy the relation*

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 =: \beta \notin \mathbb{Q}.$$

Then, β is a cubic algebraic number and it is possible to label the algebraic conjugates $\alpha_1, \alpha_2, \ldots, \alpha_6$ of α in such a way that these satisfy the relations

$$\begin{cases} \beta_1 = \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4, \\ \beta_2 = \alpha_2 + \alpha_5 = \alpha_3 + \alpha_6, \\ \beta_3 = \alpha_1 + \alpha_6 = \alpha_4 + \alpha_5, \end{cases} \tag{5}$$

where $\beta_1 = \beta, \beta_2, \beta_3$ are the algebraic conjugates of β. Let G be the Galois group of the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Consider G as a subgroup of S_6, acting on the indices of the conjugates $\alpha_1, \alpha_2, \ldots, \alpha_6$ of α. Then, given the relations (6), there are exactly three possible cases:

(1) $G = \langle \tau, \pi \mid \tau^2 = \pi^6 = id,\ \tau\pi\tau = \pi^5 \rangle \cong D_6$;
(2) $G = \langle \pi \mid \pi^6 = id \rangle \cong C_6$;
(3) $G = \{id, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} \cong S_3$.

3 Proofs

Proof of Theorem 1 (i) Suppose that some four distinct algebraic conjugates of an algebraic number α of degree $d \in \{4, 5, 6, 7\}$ satisfy the relation $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$. The case $d = 4$ is trivial in view of $tr(\alpha) = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$. By Lemma 5, d cannot be 5 or 7. Let $d = 6$. Lemma 8 implies that $tr(\alpha) = 0$. Then, $\alpha_5 + \alpha_6 = tr(\alpha) - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) = 0$. Hence, $\alpha_6 = -\alpha_5$. Let $p(x)$ be the minimal polynomial of α over $\mathbb{Q}$. We have that $p(\alpha_6) = p(-\alpha_5) = 0$. Hence, α_5 is a root of $p(-x)$. Thus, $p(x)$ divides the polynomial $p(-x)$. Since both polynomials $p(x)$ and $p(-x)$ are of the same degree and their constant terms coincide, we have that $p(-x) = p(x)$. So $p(x)$ is of the form

$$x^6 + ax^4 + bx^2 + c \in \mathbb{Q}[x].$$

The converse is clear, since the roots $\alpha_1, \alpha_2, \ldots, \alpha_6$ of such polynomial satisfy

$$\alpha_1 = -\alpha_2, \quad \alpha_3 = -\alpha_4, \quad \alpha_5 = -\alpha_6.$$

Thus, $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$.

(ii) Suppose that some four distinct algebraic conjugates of an algebraic number α of degree $d \in \{4, 5, 6, 7\}$ satisfy the relation $\alpha_1 + \alpha_2 + \alpha_3 = \alpha_4$. If $d = 4$, then, by Lemma 8, $tr(\alpha) = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ and we obtain $\alpha_4 + \alpha_4 = (\alpha_1 + \alpha_2 + \alpha_3) + \alpha_4 = 0$. A contradiction. By Lemma 5, d cannot be 5 or 7. Hence, $d = 6$. By Lemma 8, $tr(\alpha) = \alpha_1 + \cdots + \alpha_6 = 0$. Since $\alpha_1 + \alpha_2 + \alpha_3 = \alpha_4$, we have that

$$0 = \alpha_1 + \cdots + \alpha_6 = 2\alpha_4 + \alpha_5 + \alpha_6,$$

which is impossible in view of Lemma 7. ∎

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

Proof of Proposition 10 Let α be an algebraic number of degree $d = 6$ such that $tr(\alpha) = 0$ and some four distinct conjugates of α satisfy the relation

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 =: \beta.$$

Let

$$\mathcal{S} := \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$$

be the full set of algebraic conjugates of α. Then, in view of $tr(\alpha) = 0$, we have

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = \beta, \quad \alpha_5 + \alpha_6 = -2\beta.$$

Let G be the Galois group of the normal closure of $\mathbb{Q}(\alpha_1)$ over $\mathbb{Q}$. The 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_6. First, consider the trivial case:

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = a, \quad \alpha_5 + \alpha_6 = -2a,$$

where $a \in \mathbb{Q}$. Select an automorphism $\phi \in G$ that maps α_1 to α_5. Setting $\phi(\alpha_2) = \alpha_k$, we obtain $\alpha_5 + \alpha_k = a$. We claim that $k = 6$. Indeed, if $1 \leqslant k \leqslant 2$, then $\alpha_1 + \alpha_2 = a$ together with $\alpha_5 + \alpha_k = a$ imply $\alpha_5 = \alpha_1$ or $\alpha_5 = \alpha_2$, which is impossible. Similarly, if $3 \leqslant k \leqslant 4$, then $\alpha_3 + \alpha_4 = a$ together with $\alpha_5 + \alpha_k = a$ imply $\alpha_5 = \alpha_3$ or $\alpha_5 = \alpha_4$, and we get another contradiction. Clearly, $k \neq 5$, so the only option is $\alpha_5 + \alpha_6 = a$. But we already know that $\alpha_5 + \alpha_6 = -2a$. Thus, $a = -2a$, meaning that $a = 0$.

Now assume that

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = \beta, \quad \alpha_5 + \alpha_6 = -2\beta,$$

where $\beta \notin \mathbb{Q}$. We will prove that $\beta_1 := \beta$ is a cubic algebraic number.

Let us write all possible distinct expressions of β_1 in terms of $\alpha_i + \alpha_j$ (sum of two distinct α conjugates). Assume that there are exactly l distinct expressions (two expressions $\alpha_i + \alpha_j$ and $\alpha_u + \alpha_v$ are distinct if $\{i, j\} \neq \{u, v\}$):

$$\beta_1 = \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = \alpha_u + \alpha_v = \dots.$$

Notice that $l \geqslant 2$, since the equality $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$ provides at least two distinct expressions of β_1. We will show that $l = 2$. Indeed, assume that $l \geqslant 3$. Then, we have at least three distinct expressions of β_1 as a sum of two distinct conjugates of α:

$$\beta_1 = \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = \alpha_u + \alpha_v. \tag{6}$$

Then, $\{u, v\} = \{5, 6\}$. Indeed, if $u \in \{1, 2, 3, 4\}$, then (6) implies that α_v coincides with one of the conjugates α_1, α_2, α_3, α_4, which is impossible, since all three expressions in (6) are distinct. Similarly, $v \in \{1, 2, 3, 4\}$ also leads to a contradiction. Hence, $\{u, v\} = \{5, 6\}$. So (6) becomes

$$\beta_1 = \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = \alpha_5 + \alpha_6.$$

Adding all these expressions of β_1, we obtain

$$3\beta_1 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 + \alpha_6 = 0,$$

which is impossible in view of $\beta_1 \notin \mathbb{Q}$.

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

Now, we have that $l = 2$ and

$$\beta_1 = \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4. \tag{7}$$

Next, we will obtain an upper bound for $\deg(\beta_1)$. Note that by acting on (7) with an appropriate automorphism from G, we can obtain expressions of the form (7) for every algebraic conjugate of β_1:

$$\begin{aligned} \beta_1 &= \alpha_1 \quad + \alpha_2 \quad = \alpha_3 \quad + \alpha_4, \\ \beta_2 &= \alpha_{i_{21}} + \alpha_{i_{22}} = \alpha_{i_{23}} + \alpha_{i_{24}}, \\ &= \cdots \quad \cdots \\ \beta_t &= \alpha_{i_{t1}} + \alpha_{i_{t2}} = \alpha_{i_{t3}} + \alpha_{i_{t4}}. \end{aligned} \tag{8}$$

Here, t is the degree of β_1 and $\beta_1, \beta_2, \ldots, \beta_t$ are the algebraic conjugates of β_1. We have precisely $2 \cdot t$ distinct expressions of the form $\alpha_i + \alpha_j$ in (8), since there are exactly t algebraic conjugates of β_1 and every such conjugate has exactly two expressions. On the other hand, since $\deg(\alpha) = 6$, we have at most $\binom{6}{2} = 15$ possible pairs of indices for distinct expressions $\alpha_i + \alpha_j$. Hence, $2t \leqslant 15$ and $t = \deg(\beta_1) \leqslant 7$.

Next, we will show that, in fact, $\deg(\beta_1)$ is divisible by 3. Indeed, in (8), there are $2t$ distinct expressions of conjugates of β_1 as sums $\alpha_i + \alpha_j$. Each such sum contains two conjugates of α. Hence, there are exactly $2 \cdot 2t$ appearances of conjugates of α in (8). On the other hand, since G is transitive on the set of algebraic conjugates of α, each α_i must appear the same number of times in (8). Suppose that every α_i appears exactly k times in (8). So we have exactly $k \cdot \deg(\alpha) = 6k$ appearances of conjugates of α in (8). Hence, $4t = 6k$, and therefore t is divisible by 3. Recall that $t = \deg(\beta_1) \leqslant 7$. So $\deg(\beta_1) = 3$ or 6.

Finally, we will show that $\deg(\beta_1) \neq 6$. Indeed, assume that $\deg(\beta_1) = 6$. Since each conjugate of β_1 has exactly two distinct expressions of the form $\alpha_i + \alpha_j$, we obtain $6 \cdot 2 = 12$ distinct expressions. Recall that there are at most $\binom{6}{2} = 15$ possible pairs of indices for distinct expressions $\alpha_i + \alpha_j$ and also

$$-2\beta_1 = -(\alpha_1 + \alpha_2) - (\alpha_3 + \alpha_4) = \alpha_5 + \alpha_6.$$

By applying all automorphisms from G to $-2\beta_1 = \alpha_5 + \alpha_6$, we get at least $\deg(\beta_1) = 6$ expressions of the form $\alpha_i + \alpha_j$ for algebraic conjugates of $-2\beta_1$. These expressions must be distinct from each other and from the 12 expressions that we already have. Note that there is no pair of indices (i, j) such that $\beta_i = -2\beta_j$. Indeed, let $q(x)$ be the minimal polynomial of the $\beta_1, \beta_2, \ldots, \beta_t$ and assume that $\beta_i = -2\beta_j$. In such a case, $q(x)$ and $(-2)^t q(-\frac{x}{2})$ would be the same polynomial. This implies that either $t = 0$ or $q(x) = x^t$, which are both impossible. But in that case, there would be

$$12 + 6 = 18$$

distinct expressions $\alpha_i + \alpha_j$. A contradiction, since there are at most 15 distinct such expressions. Hence, $\deg(\beta_1) \neq 6$, and the only possibility is $\deg(\beta_1) = 3$. ■

Proof of Proposition 11 Let α be an algebraic number of degree $d = 6$ and $tr(\alpha) = 0$. Assume that some four distinct algebraic conjugates of α satisfy the relation

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 =: \beta \notin \mathbb{Q}. \tag{9}$$

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

Then, by Proposition 10, β is a cubic algebraic number and $tr(\beta) = 0$. Let $\beta_1 = \beta, \beta_2, \beta_3$ be the algebraic conjugates of β. Let G be the Galois group of the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Consider G as a subgroup of S_6, acting on the indices of the conjugates $\alpha_1, \alpha_2, \ldots, \alpha_6$ of α. Take two automorphisms of G such that one maps β_1 to β_2 and another maps β_1 to β_3. Acting with these automorphisms on (9), we obtain

$$\begin{cases} \beta_1 = \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4, \\ \beta_2 = \alpha_{i_{21}} + \alpha_{i_{22}} = \alpha_{i_{23}} + \alpha_{i_{24}}, \\ \beta_3 = \alpha_{i_{31}} + \alpha_{i_{32}} = \alpha_{i_{33}} + \alpha_{i_{34}}, \end{cases} \tag{10}$$

where each $\alpha_{i_{kl}}$ is an algebraic conjugate of α. In view of $tr(\alpha) = 0$, we also obtain corresponding relations

$$\begin{cases} -2\beta_1 = \alpha_5 + \alpha_6, \\ -2\beta_2 = \alpha_{i_{25}} + \alpha_{i_{26}}, \\ -2\beta_3 = \alpha_{i_{35}} + \alpha_{i_{36}}. \end{cases} \tag{11}$$

Note that for every $k = 2, 3$ the numbers $i_{k1}, i_{k2}, i_{k3}, i_{k4}, i_{k5}, i_{k6}$ are distinct. We will specify the indices in (10) and (11) by relabeling the conjugates $\alpha_1, \alpha_2, \ldots, \alpha_6$, if necessary. First, we will prove that each $-2\beta_k$ has a unique expression in terms of $\alpha_i + \alpha_j$ (recall that two expressions $\alpha_i + \alpha_j$ and $\alpha_u + \alpha_v$ are distinct if $\{i, j\} \neq \{u, v\}$). Indeed, say, $-2\beta_1$ has two distinct expressions:

$$-2\beta_1 = \alpha_5 + \alpha_6 = \alpha_u + \alpha_v. \tag{12}$$

If $u = 5$ (or $u = 6$), then by (12), $v = 6$ (or $v = 5$, respectively). In this scenario, the expressions $\alpha_u + \alpha_v$ and $\alpha_5 + \alpha_6$ become identical. This implies that $u \notin \{5, 6\}$. A similar argument shows that $v \notin \{5, 6\}$. Consequently, $u, v \in \{1, 2, 3, 4\}$. Without loss of generality, let $u = 1$. We then examine the following cases for (u, v):

Case 1: If $(u, v) = (1, 1)$, then $\alpha_5 + \alpha_6 = 2\alpha_1$, which contradicts Lemma 6.
Case 2: If $(u, v) = (1, 2)$, then equations (10) and (12) yield $-2\beta_1 = \beta_1$ implying $\beta_1 = 0$. This contradicts the condition that $\beta_1 \notin \mathbb{Q}$.
Case 3: If $(u, v) = (1, 3)$, then we have $\beta_1 = \alpha_1 + \alpha_2$ and $-2\beta_1 = \alpha_1 + \alpha_3$. Substituting the first into the second gives $3\alpha_1 + 2\alpha_2 + \alpha_3 = 0$, which contradicts Lemma 7.
Case 4: Similarly, $(u, v) \neq (1, 4)$.

These cases imply that $u \notin \{1, 2, 3, 4\}$. Therefore, $-2\beta_1$ has a unique expression in terms of $\alpha_i + \alpha_j$. Since $\beta_1, \beta_2, \beta_3$ are algebraic conjugates of β_1, it follows that every $-2\beta_k$ (for $k = 1, 2, 3$) also has a unique expression in terms of $\alpha_i + \alpha_j$.

Now, we will prove that all the α's appear exactly once in (11). Indeed, note that each conjugate of α appears exactly three times counting both (10) and (11): the set $\{\alpha_1, \ldots, \alpha_6\}$, $\{\alpha_{i_{21}}, \ldots, \alpha_{i_{26}}\}$, and $\{\alpha_{i_{31}}, \ldots, \alpha_{i_{36}}\}$ make three copies of the set of conjugates of α, and since each appears exactly twice in (10) (as was proven in the proof of Proposition 10), there must be one full set of conjugates in (11).

We have that $\{\alpha_{i_{25}}, \alpha_{i_{26}}, \alpha_{i_{35}}, \alpha_{i_{36}}\} = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. Without loss of generality, we can assume that $\alpha_{i_{25}} = \alpha_1$. If $\alpha_{i_{26}} = \alpha_2$, then $-2\beta_2 = \beta_1$. Substituting this expression of β_1 into $tr(\beta) = \beta_1 + \beta_2 + \beta_3 = 0$ yields $\beta_2 = \beta_3$, which is impossible. Hence,

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

$\alpha_{i_{26}} \in \{\alpha_3, \alpha_4\}$. Note that α_3 and α_4 appear symmetrically in the first equation of (10). Without loss of generality, by relabeling α_3 and α_4, if necessary, we can assume that $\alpha_{i_{26}} = \alpha_4$. From this, we immediately derive that $\{\alpha_{i_{21}}, \alpha_{i_{22}}, \alpha_{i_{23}}, \alpha_{i_{24}}\} = \{\alpha_2, \alpha_3, \alpha_5, \alpha_6\}$. Note that $\beta_2 \neq \alpha_5 + \alpha_6$. Indeed, if $\beta_2 = \alpha_5 + \alpha_6$, then $\beta_2 = -2\beta_1$. Substituting this expression of β_2 into $tr(\beta) = \beta_1 + \beta_2 + \beta_3 = 0$ yields $\beta_1 = \beta_3$, which is impossible. Thus, α_5 and α_6 appear in distinct expressions of β_2 in (10), as well as α_2 and α_3. Without loss of generality, we can assume that $\alpha_{i_{21}} = \alpha_2$ and $\alpha_{i_{23}} = \alpha_3$. Since α_5 and α_6 appear symmetrically in the first equation of (11), by relabeling α_5 and α_6, if necessary, we can assume that $\alpha_{i_{22}} = \alpha_5$ and $\alpha_{i_{24}} = \alpha_6$. So far, we have obtained

$$\begin{cases} \beta_1 = \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4, \\ \beta_2 = \alpha_2 + \alpha_5 = \alpha_3 + \alpha_6, \\ \beta_3 = \alpha_{i_{31}} + \alpha_{i_{32}} = \alpha_{i_{33}} + \alpha_{i_{34}}, \end{cases} \qquad \begin{cases} -2\beta_1 = \alpha_5 + \alpha_6, \\ -2\beta_2 = \alpha_1 + \alpha_4, \\ -2\beta_3 = \alpha_{i_{35}} + \alpha_{i_{36}}. \end{cases}$$

Since $\{\alpha_{i_{35}}, \alpha_{i_{36}}\} = \{\alpha_2, \alpha_3\}$, without loss of generality, we assume that $\alpha_{i_{35}} = \alpha_2$ and $\alpha_{i_{36}} = \alpha_3$. Then, $\{\alpha_{i_{31}}, \alpha_{i_{32}}, \alpha_{i_{33}}, \alpha_{i_{34}}\} = \{\alpha_1, \alpha_4, \alpha_5, \alpha_6\}$. Note that $\beta_3 \neq \alpha_5 + \alpha_6$. Indeed, if $\beta_3 = \alpha_5 + \alpha_6$, then $\beta_3 = -2\beta_1$. Substituting this expression of β_3 into $tr(\beta) = \beta_1 + \beta_2 + \beta_3 = 0$ yields $\beta_1 = \beta_2$, which is impossible. Therefore, α_5 and α_6 appear in distinct expressions of β_3 in (10), as well as α_1 and α_4. Thus, without loss of generality, we can assume that $\alpha_{i_{31}} = \alpha_1$ and $\alpha_{i_{33}} = \alpha_4$. Now, we have two possible cases:

$$\beta_3 = \alpha_1 + \alpha_5 = \alpha_4 + \alpha_6 \quad \text{or} \quad \beta_3 = \alpha_1 + \alpha_6 = \alpha_4 + \alpha_5.$$

The first case is impossible. Indeed, by adding $\beta_1 = \alpha_1 + \alpha_2, \beta_2 = \alpha_2 + \alpha_5$ and $\beta_3 = \alpha_1 + \alpha_5$, we obtain

$$0 = \beta_1 + \beta_2 + \beta_3 = 2(\alpha_1 + \alpha_2 + \alpha_5) = 2(\beta_1 + \alpha_5),$$

and hence $\beta_1 = -\alpha_5$, which is impossible, since $6 = \deg(-\alpha_5) \neq \deg(\beta_1) = 3$. Finally, we can rewrite equations (10) and (11) as follows:

$$\begin{cases} \beta_1 = \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4, \\ \beta_2 = \alpha_2 + \alpha_5 = \alpha_3 + \alpha_6, \\ \beta_3 = \alpha_1 + \alpha_6 = \alpha_4 + \alpha_5, \end{cases} \tag{13}$$

$$\begin{cases} -2\beta_1 = \alpha_5 + \alpha_6, \\ -2\beta_2 = \alpha_1 + \alpha_4, \\ -2\beta_3 = \alpha_2 + \alpha_3. \end{cases} \tag{14}$$

Now, we will prove that the Galois group G is of order $|G| = 6$ or 12. Since G is transitive, the Orbit–Stabilizer Theorem implies

$$|G| = |\mathrm{Orb}(\alpha_1)| \cdot |\mathrm{Stab}(\alpha_1)| = 6 \cdot |\mathrm{Stab}(\alpha_1)|,$$

where $\mathrm{Stab}(\alpha_1) = \{\psi \in G : \psi(\alpha_1) = \alpha_1\}$. Hence, if we can show that $|\mathrm{Stab}(\alpha_1)| \leqslant 2$, then it follows that $|G| = 6$ or 12. Let $\psi \in \mathrm{Stab}(\alpha_1)$.

If ψ stabilizes α_2, then, in view of $-2\beta_2 = \alpha_1 + \alpha_4$ and $-2\beta_3 = \alpha_2 + \alpha_3$, ψ stabilizes β_2, α_3, and α_4. Since $\beta_2 = \alpha_2 + \alpha_5$, it follows that ψ stabilizes α_5. Hence, ψ stabilizes every conjugate of α. Therefore, $\psi = id$.

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

Suppose that $\psi(\alpha_2) \neq \alpha_2$. Since $\psi(\alpha_1) = \alpha_1$ and every conjugate of α appears exactly once in (14), it follows that ψ stabilizes β_2 and α_4. Moreover, from (13), we obtain that ψ maps $\beta_1 = \alpha_1 + \alpha_2$ to $\beta_3 = \alpha_1 + \alpha_6$ and vice versa. Hence, $\psi(\alpha_2) = \alpha_6$ and $\psi(\alpha_6) = \alpha_2$. Furthermore, ψ maps $-2\beta_1 = \alpha_5 + \alpha_6$ to $-2\beta_3 = \alpha_2 + \alpha_3$ and vice versa. So $\psi(\alpha_3) = \alpha_5$ and $\psi(\alpha_5) = \alpha_3$. Hence, $\psi = (2\,6)(3\,5) \in S_6$.

We have proved that if every $\psi \in \mathrm{Stab}(\alpha_1)$ stabilizes α_2, then the stabilizer subgroup $\mathrm{Stab}(\alpha_1)$ is trivial and G has order 6. If there exists $\psi \in \mathrm{Stab}(\alpha_1)$ which does not stabilize α_2, then $\mathrm{Stab}(\alpha_1) = \{id, (2\,6)(3\,5)\}$ and accordingly G has order $6 \cdot 2 = 12$. Hence, if G has order 12, then necessarily $(2\,6)(3\,5) \in G$.

Next, we will prove that the group G contains the permutation $\sigma := (1\,3\,5)(2\,6\,4) \in S_6$. Indeed, since β_1 is a cubic algebraic number, the Galois group G contains an element, denote it by φ, that permutes the conjugates of β_1. Without loss of generality, we can assume that

$$\varphi(\beta_1) = \beta_2, \quad \varphi(\beta_2) = \beta_3, \quad \varphi(\beta_3) = \beta_1$$

(by exchanging φ with φ^2, if necessary).

Relations in (14) imply that φ maps $\{\alpha_1, \alpha_4\}$ to $\{\alpha_2, \alpha_3\}$. Consider two possible cases: $\varphi(\alpha_1) = \alpha_2$ and $\varphi(\alpha_1) = \alpha_3$.

If $\varphi(\alpha_1) = \alpha_2$, then $\varphi(\alpha_4) = \alpha_3$. The expressions of β_1 and β_2 in (13) imply that φ maps $\{\alpha_1, \alpha_2\}$ to $\{\alpha_2, \alpha_5\}$. Since $\varphi(\alpha_1) = \alpha_2$, we obtain $\varphi(\alpha_2) = \alpha_5$. Similarly, we see that φ maps $\{\alpha_3, \alpha_4\}$ to $\{\alpha_3, \alpha_6\}$. Since $\varphi(\alpha_4) = \alpha_3$, we derive $\varphi(\alpha_3) = \alpha_6$. The expressions of β_2 and β_3 in (13) imply that φ maps $\{\alpha_2, \alpha_5\}$ to $\{\alpha_4, \alpha_5\}$. Since $\varphi(\alpha_2) = \alpha_5$, we obtain $\varphi(\alpha_5) = \alpha_4$. We are left with only one option for $\varphi(\alpha_6)$, i.e., $\varphi(\alpha_6) = \alpha_1$. Hence, $\varphi = (1\,2\,5\,4\,3\,6)$. Note that $\varphi^4 = (1\,3\,5)(2\,6\,4) = \sigma$. So that in this case ($\varphi(\alpha_1) = \alpha_2$) the permutation σ is contained in G.

If $\varphi(\alpha_1) = \alpha_3$, then $\varphi(\alpha_4) = \alpha_2$. The expressions of β_1 and β_2 in (13) imply that φ maps $\{\alpha_1, \alpha_2\}$ to $\{\alpha_3, \alpha_6\}$. Since $\varphi(\alpha_1) = \alpha_3$, we have $\varphi(\alpha_2) = \alpha_6$. Similarly, we see that φ maps $\{\alpha_3, \alpha_4\}$ to $\{\alpha_2, \alpha_5\}$. Since $\varphi(\alpha_4) = \alpha_2$, we get $\varphi(\alpha_3) = \alpha_5$. The expressions of β_2 and β_3 in (13) imply that φ maps $\{\alpha_2, \alpha_5\}$ to $\{\alpha_1, \alpha_6\}$. Since $\varphi(\alpha_2) = \alpha_6$, we obtain $\varphi(\alpha_5) = \alpha_1$. We are left with only one option for $\varphi(\alpha_6)$, i.e., $\varphi(\alpha_6) = \alpha_4$. Hence, $\varphi = (1\,3\,5)(2\,6\,4) = \sigma$.

We have proved that the group G contains the permutation $\sigma = (1\;3\;5)(2\;6\;4)$. Now, we are in a position to find all possible groups G.

A simple computation with SageMath [14] shows that there is a unique transitive subgroup of S_6 which has order 12 and contains permutations $(2\,6)(3\,5)$ and $\sigma = (1\,3\,5)(2\,6\,4)$. This subgroup is generated by the permutations $\tau = (1\,2)(3\,4)(5\,6)$ and $\pi = (1\,2\,5\,4\,3\,6)$ and is isomorphic to the dihedral group D_6 of order 12.

Similarly, there are exactly four transitive subgroups of S_6 which have order 6 and contain the permutation $\sigma = (1\,3\,5)(2\,6\,4)$. These are

- $G_1 = \langle \sigma, \tau \rangle$ isomorphic to S_3, where $\tau = (1\,2)(3\,4)(5\,6)$;
- $G_2 = \langle \pi \rangle$ isomorphic to the cyclic group C_6, where $\pi = (1\,2\,5\,4\,3\,6)$;
- $G_3 = \langle (1\,6\,5\,2\,3\,4) \rangle$ isomorphic to the cyclic group C_6;
- $G_4 = \langle (1\,4\,5\,6\,3\,2) \rangle$ isomorphic to the cyclic group C_6.

Note that the groups G_3 and G_4 do not preserve the relations in (14). Indeed, the generator of G_3 maps $\alpha_1 + \alpha_4$ to $\alpha_6 + \alpha_1$ while the generator of G_4 maps $\alpha_1 + \alpha_4$ to $\alpha_4 + \alpha_5$. Hence, $G \neq G_3$ and $G \neq G_4$.

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

We have proved that there are three options for the group G:

(1) $G = \langle \tau, \pi \rangle \cong D_6$;
(2) $G = \langle \sigma, \tau \rangle \cong S_3$;
(3) $G = \langle \pi \rangle \cong C_6$.

This completes the proof of Proposition 11. ∎

Proof of Theorem 3 *Necessity.* Suppose that α is an algebraic number of degree 6 whose four distinct algebraic conjugates satisfy the relation $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 =: \beta \notin \mathbb{Q}$. Note that for any $r \in \mathbb{Q}$, the number $\alpha - r$ will also have this property. Moreover, α equals the sum of a quadratic and a cubic algebraic number if and only if $\alpha - r$ has the same property. Hence, by taking $r = tr(\alpha)/6$, we can assume that α has trace zero, $tr(\alpha) = 0$. Let G be the Galois group of the normal closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Consider G as a subgroup of S_6, acting on the indices of the conjugates $\alpha_1, \alpha_2, \dots, \alpha_6$ of α. Then, by Proposition 11, we have the following:

(i) β is a cubic algebraic number.
(ii) One can label the algebraic conjugates $\alpha_1, \alpha_2, \dots, \alpha_6$ of α in such a way that these satisfy the relations

$$\begin{cases} \beta_1 = \alpha_1 + \alpha_2 = \alpha_3 + \alpha_4, \\ \beta_2 = \alpha_2 + \alpha_5 = \alpha_3 + \alpha_6, \\ \beta_3 = \alpha_1 + \alpha_6 = \alpha_4 + \alpha_5, \end{cases} \tag{15}$$

where $\beta_1 = \beta, \beta_2, \beta_3$ are the algebraic conjugates of β.
(iii) Given the relations (15), there are exactly three options for the Galois group G:
  (1) $G = \langle \tau, \pi \mid \tau^2 = \pi^6 = id,\ \tau\pi\tau = \pi^5 \rangle \cong D_6$;
  (2) $G = \langle \pi \mid \pi^6 = id \rangle \cong C_6$;
  (3) $G = \{id, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} \cong S_3$.

Here, $\pi = (1\,2\,5\,4\,3\,6)$, $\sigma = (1\,3\,5)(2\,6\,4)$ and $\tau = (1\,2)(3\,4)(5\,6)$.

Consider the number $\alpha_1 - \alpha_4$. The expression of β_1 in (15) implies that $\alpha_2 - \alpha_3 = -(\alpha_1 - \alpha_4)$. Moreover,

$$\tau(\alpha_1 - \alpha_4) = \alpha_2 - \alpha_3 = -(\alpha_1 - \alpha_4),$$
$$\pi(\alpha_1 - \alpha_4) = \alpha_2 - \alpha_3 = -(\alpha_1 - \alpha_4),$$
$$\sigma(\alpha_1 - \alpha_4) = \alpha_3 - \alpha_2 = \alpha_1 - \alpha_4.$$

Hence, $\alpha_1 - \alpha_4$ is a quadratic algebraic number. Moreover, the relations $\beta_2 = \alpha_2 + \alpha_5 = \alpha_3 + \alpha_6$ together with $tr(\alpha) = 0$ imply $-2\beta_2 = \alpha_1 + \alpha_4$, which is equivalent to

$$\alpha_1 = \frac{\alpha_1 - \alpha_4}{2} - \beta_2.$$

Consequently, $\alpha = \alpha_1$ is the sum of the quadratic algebraic number $(\alpha_1 - \alpha_4)/2$ and the cubic algebraic number $-\beta_2$.

Sufficiency. Assume that α is the sum of a quadratic algebraic number γ and a cubic algebraic number δ. We will prove that α has degree 6 and some four distinct algebraic conjugates of α satisfy the relation $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 \notin \mathbb{Q}$. Indeed, let $\gamma_1 = \gamma$, γ_2 be the algebraic conjugates of γ and let $\delta_1 = \delta, \delta_2, \delta_3$ be the algebraic conjugates of δ. Since the

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

compositum $\mathbb{Q}(\gamma, \delta)$ contains γ and δ of degree 2 and 3, respectively, it follows that the degree of $\mathbb{Q}(\gamma, \delta)$ is divisible by $2 \cdot 3 = 6$. On the other hand, $[\mathbb{Q}(\gamma, \delta) : \mathbb{Q}] \leqslant [\mathbb{Q}(\gamma) : \mathbb{Q}] \cdot [\mathbb{Q}(\delta) : \mathbb{Q}] = 2 \cdot 3 = 6$. Hence, $[\mathbb{Q}(\gamma, \delta) : \mathbb{Q}] = 6$. By Lemma 9, we obtain that $\mathbb{Q}(\gamma, \delta) = \mathbb{Q}(\gamma + \delta)$. Therefore, $\alpha = \gamma + \delta$ has degree 6. Hence, the numbers $\gamma_i + \delta_j$, for $i = 1, 2$ and $j = 1, 2, 3$, are distinct algebraic conjugates of $\gamma + \delta$. The identity

$$(\gamma_1 + \delta_1) + (\gamma_2 + \delta_2) = (\gamma_1 + \delta_2) + (\gamma_2 + \delta_1)$$

implies that four distinct algebraic conjugates of $\alpha = \gamma + \delta$ satisfy

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4,$$

where $\alpha_1 = \gamma_1 + \delta_1$, $\alpha_2 = \gamma_2 + \delta_2$, $\alpha_3 = \gamma_1 + \delta_2$, and $\alpha_4 = \gamma_2 + \delta_1$. Finally, since $tr(\gamma) = \gamma_1 + \gamma_2$ and $tr(\delta) = \delta_1 + \delta_2 + \delta_3$ are rational numbers, we obtain that

$$\alpha_1 + \alpha_2 = \gamma_1 + \delta_1 + \gamma_2 + \delta_2 = tr(\gamma) + tr(\delta) - \delta_3$$

is a cubic algebraic number, and therefore $\alpha_1 + \alpha_2 \notin \mathbb{Q}$. ∎

Proof of Theorem 2 Let α be an algebraic number of degree $d \in \{4, 5, 6, 7\}$ such that $tr(\alpha) = 0$. Suppose that four distinct conjugates of $\alpha_1 := \alpha$ satisfy the relation

$$\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4. \tag{16}$$

By Lemma 5, $d \neq 5$ and $d \neq 7$. Hence, $d = 4$ or 6.

(i) Suppose that $d = 4$. Then, (16) together with $tr(\alpha) = 0$ imply $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = 0$. Hence, $\alpha_2 = -\alpha_1$, and therefore the minimal polynomial $p(x)$ of α is of the form $p(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$.

Conversely, let $p(x) = x^4 + ax^2 + b \in \mathbb{Q}[x]$ be an irreducible polynomial. Let $\beta, \gamma \in \mathbb{C}$ be two distinct roots of $p(x)$ such that $\gamma \neq -\beta$. Then $\alpha_1 = \beta$, $\alpha_2 = -\beta$, $\alpha_3 = \gamma$, and $\alpha_4 = -\gamma$ are all the roots of $p(x)$ and the relation (16) holds.

(ii) Suppose that $d = 6$ and the sum $\alpha_1 + \alpha_2$ in (16) is a rational number. Then, by Proposition 10, $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = 0$. This implies that $\alpha_2 = -\alpha_1$. Therefore, the minimal polynomial $p(x)$ of α is of the form $p(x) = x^6 + ax^4 + bx^2 + c \in \mathbb{Q}[x]$. Similarly, as in case (ii), we see that some four distinct roots of any such irreducible polynomial satisfy the relation (16).

(iii) Suppose that $d = 6$ and the sum $\alpha_1 + \alpha_2$ in (16) is not a rational number. Then, by Theorem 3, α is a sum of a quadratic algebraic number γ and a cubic algebraic number δ. Let $\gamma_1 = \gamma$, γ_2 be the algebraic conjugates of γ and let $\delta_1 = \delta$, δ_2, δ_3 be the algebraic conjugates of δ. Then, the numbers $\gamma_i + \delta_j$, for $i = 1, 2$ and $j = 1, 2, 3$, are the algebraic conjugates of $\alpha = \gamma + \delta$. We have that $tr(\alpha) = 0$. On the other hand, $tr(\alpha)$ equals the sum of all the numbers $\gamma_i + \delta_j$, for $i = 1, 2$ and $j = 1, 2, 3$. The later sum equals $3(\gamma_1 + \gamma_2) + 2(\delta_1 + \delta_2 + \delta_3)$. Hence, $0 = tr(\alpha) = 3tr(\gamma) + 2tr(\delta)$. Therefore, $tr(\gamma)/2 + tr(\delta)/3 = 0$ and we can represent α as

$$\alpha = \left(\gamma - \frac{tr(\gamma)}{2}\right) + \left(\delta - \frac{tr(\delta)}{3}\right).$$

Note that $\gamma - tr(\gamma)/2$ and $\delta - tr(\delta)/3$ are quadratic and cubic algebraic numbers, respectively, both having trace zero. Consequently, without loss of generality, we can assume that $tr(\gamma) = 0$ and $tr(\delta) = 0$ in the expression $\alpha = \gamma + \delta$. Then, the minimal

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

polynomial of γ is of the form $x^2 - a$ and the minimal polynomial of δ is of the form $R(x) = x^3 + bx + c$, where $a, b, c \in \mathbb{Q}$. Moreover, in view of $tr(\gamma) = 0$ and $\gamma_1\gamma_2 = -a$, we obtain that $\gamma_1 = \pm\sqrt{a}$ and $\gamma_2 = \mp\sqrt{a}$. Now, the minimal polynomial $p(x)$ of α can be expressed as

$$\begin{aligned} p(x) &= \prod_{\substack{i=1,2\\ j=1,2,3}} (x - \gamma_i - \delta_j) = \prod_{i=1,2} (x - \gamma_i - \delta_1)(x - \gamma_i - \delta_2)(x - \gamma_i - \delta_3) \\ &= R(x - \gamma_1)R(x - \gamma_2) = R(x - \sqrt{a})R(x + \sqrt{a}) \\ &= x^6 + (2b - 3a)x^4 + 2cx^3 + (3a^2 + b^2)x^2 + 2c(3a + b)x \\ &\quad - a^3 - 2a^2b - ab^2 + c^2. \end{aligned} \tag{17}$$

Conversely, given an irreducible polynomial $p(x)$ of the form (17), we can factor it as $p(x) = R(x - \sqrt{a})R(x + \sqrt{a})$, where $R(x) = x^3 + bx + c$. Note that $\sqrt{a} \notin \mathbb{Q}$, since $p(x)$ is irreducible. Consequently, $\sqrt{a}$ is a quadratic algebraic number. Moreover, $R(x)$ is irreducible. Indeed, if $R(x)$ factors as $R(x) = P(x)Q(x)$ with some polynomials $P(x), Q(x) \in \mathbb{Q}[x]$ both of degree $\geqslant 1$, then

$$p(x) = R(x - \sqrt{a})R(x + \sqrt{a}) = P(x - \sqrt{a})P(x + \sqrt{a})Q(x - \sqrt{a})Q(x + \sqrt{a})$$

with both polynomials $P(x - \sqrt{a})P(x + \sqrt{a})$ and $Q(x - \sqrt{a})Q(x + \sqrt{a})$ having rational coefficients. This contradicts the assumption that $p(x)$ is irreducible. Hence, $R(x)$ is irreducible. Finally, the factorization $p(x) = R(x - \sqrt{a})R(x + \sqrt{a})$ implies that every root of $p(x)$ is a sum of a quadratic algebraic number $\pm\sqrt{a}$ and a root of $R(x)$, which is a cubic algebraic number. Therefore, by Theorem 3, some four distinct roots of $p(x)$ satisfy the relation (16) with $\alpha_1 + \alpha_2 \notin \mathbb{Q}$. ■

Notes.

1. The polynomial in (17) is obtained by expanding the product $R(x - \sqrt{a})R(x + \sqrt{a})$. This can be done either by hand or using a computer algebra system, e.g., SageMath [14].
2. The polynomial in (17) is irreducible if and only if a is not the square of a rational number and the polynomial $R(x) = x^3 + bx + c$ has no roots in $\mathbb{Q}$.

Acknowledgments The authors would like to thank the anonymous referee for a careful and detailed reading of the manuscript and for several important suggestions.

References

[1] C. Awtrey and P. Jakes, *Galois groups of even sextic polynomials*. Can. Math. Bull. **63**(2020), no. 3, 670–676.

[2] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, 163, Springer New York, NY, 1996.

[3] A. Dubickas, *On the degree of a linear form in conjugates of an algebraic number*. Ill. J. Math. **46**(2002), no. 2, 571–585.

[4] A. Dubickas, K. G. Hare, and J. Jankauskas, *No two non-real conjugates of a Pisot number have the same imaginary part*. Math. Comput. **86**(2017), no. 304, 935–950.

[5] A. Dubickas and J. Jankauskas, *Simple linear relations between conjugate algebraic numbers of low degree*. J. Ramanujan Math. Soc. **30**(2015), no. 2, 219–235.

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.

[6] A. Dubickas and C. Smyth, *On the lines passing through two conjugates of a Salem number*. Math. Proc. Camb. Philos. Soc. **144**(2008), no. 1, 29–37.
[7] A. Dubickas and P. Virbalas, *Additive and multiplicative relations with algebraic conjugates*. Revista de la Uni ó n Matem á tica Argentina **16**(2025), 2025.
[8] Á. S. Holgado, *Nontriviality of the module of relations for degree 4 polynomials*. Acta Math. Hungar. **176**(2025), no. 1, 236–243.
[9] L.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*. Amer. Math. Month. **96**(1989), no. 2, 133–137.
[10] Y. Kitaoka, *Notes on the distribution of roots modulo a prime of a polynomial*. Uniform Distrib. Theory **12**(2017), no. 2, 91–117.
[11] V. A. Kurbatov, *Galois extensions of prime degree and their primitive elements*. Izv. Vys š. U č ebn. Zaved. Mat. **1**(1977), no. 176, 61–66.
[12] J. J. Rotman, *An introduction to the theory of groups*. 4th ed., Graduate Texts in Mathematics, 148, Springer New York, NY, 1995.
[13] C. J. Smyth, *Conjugate algebraic numbers on conics*. Acta Arith. **40**(1982), 333–346.
[14] The Sage Developers. *SageMath, the sage mathematics software system (version 10.6.0)*, (2025). https://www.sagemath.org.
[15] P. Virbalas, *Linear relations between three algebraic conjugates of degree twice a prime*. Glas. Mat. (2025), to appear.
[16] P. Virbalas, *Linear relations between three conjugate algebraic numbers of low degree*. J Korean Math Soc. **62**(2025), no. 2, 253–284.
[17] S. H. Weintraub, *Observations on primitive, normal, and subnormal elements of field extensions*. Monatsh. Math. **162**(2011), no. 2, 239–244.

Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania
e-mail: zygimantas.baronenas@mif.stud.vu.lt paulius.drungilas@mif.vu.lt jonas.jankauskas@mif.vu.lt

Downloaded from https://www.cambridge.org/core. 07 Oct 2025 at 06:43:09, subject to the Cambridge Core terms of use.