Glasnik Matematički

SERIJA III

www.math.hr/glasnik

Paulius Virbalas

Linear relations between three algebraic conjugates of degree twice a prime

Manuscript accepted
April 9, 2025.

LINEAR RELATIONS BETWEEN THREE ALGEBRAIC CONJUGATES OF DEGREE TWICE A PRIME

Paulius Virbalas
Vilnius University, Lithuania

Abstract. In this paper, we show that there is no irreducible polynomial $f(x)$ of degree $2p$ ($p \geq 5$ is a prime number) over $\mathbb{Q}$ whose three distinct roots sum up to zero. This extends some earlier results on the linear relations between three algebraic numbers. In particular, let d be the smallest positive integer, not a multiple of 3, for which there exists an irreducible polynomial $f(x)$ of degree d whose three distinct roots add up to zero. In 2015, Dubickas and Jankauskas found that $10 \leq d \leq 20$. As a corollary, we show that it is either $d = 16$ or $d = 20$.

1. Introduction

Let $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_d$ be distinct algebraic conjugates of an algebraic number α of degree d over the field K. A relation of the form

$$m_1\alpha_1 + \ldots + m_d\alpha_d \in K \tag{1.1}$$

with coefficients $m_1, \ldots, m_d \in K$ is called a *linear* (or *additive*) relation between the conjugates of α. From the properties of symmetric polynomials, it follows that if $m_1 = \ldots = m_d$, a relation in (1.1) always holds (such relations are called *trivial*). In contrast, the reasons behind *non-trivial* linear relations are much less understood. As we might expect, non-trivial relations imply special conditions on the minimal polynomial of α. For example, in [11, Theorem 1.1] Dubickas and Jankauskas found that an irreducible polynomial $f(x)$ of degree $d \leq 8$ over $\mathbb{Q}$ has three distinct roots satisfying the relation $\alpha_i = \alpha_j + \alpha_k$ if and only if

$$f(x) = x^6 + 2ax^4 + a^2x^2 + b.$$

2020 *Mathematics Subject Classification.* 11R32, 11F05, 12F10, 20B35.
Key words and phrases. Linear relations between polynomial roots, non-trivial additive relations between algebraic conjugates, transitive permutation groups.

The relation $\alpha_i = \alpha_j + \alpha_k$ is an additive version of the multiplicative relation $\alpha_i = \alpha_j\alpha_k$ which has been investigated earlier by Schinzel and then by Drmota and Skałba (see [7], [8]). Unless some special conditions are met (see, e.g., [9, Theorem 4]) or the degree of $f(x)$ is low, it is not known how to efficiently decide whether a given linear relation can occur between the roots of some polynomial $f(x)$. The most general result in this direction can be found in a recent paper by Ellenberg and Hardt [14], in which they prove Smyth's conjecture (see also [21]).

A different approach was initiated by Girstmair, who approached the topic with an emphasis on Galois groups rather than the form of polynomials (see [16], [17]). Among other things, he showed that there are only six primitive groups of transitivity degree $d \leq 15$ that admit non-trivial linear relations. For example, from [16, Proposition 6] we know that a direct product $S_3 \times S_3$ occurs as Galois group for some irreducible polynomial of degree 9 whose roots satisfy

$$4\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 - 2(\alpha_6 + \alpha_7 + \alpha_8 + \alpha_9) = 0.$$

A substantial amount of research has been focused on linear relations of the simplest form, namely, $\alpha_i + \alpha_j + \alpha_k = 0$ or $\alpha_i = \alpha_j + \alpha_k$. The conditions for such relations to exist have been studied in the works by Baron, Drmota and Skałba [1], [8]; by Dixon [6]; by Dubickas and Jankauskas [11], [12]; by Girstmair [17], [18], [19], [20]; and by Lalande [26], [27]. Most of the findings apply to algebraic conjugates of low degree or to specific classes of Galois groups. The main contribution of this paper is the following result.

THEOREM 1.1. *Let $p \geq 5$ be a prime number and let $f(x)$ be an irreducible polynomial of degree $2p$ over the field K such that $\mathbb{Q} \subseteq K \subset \mathbb{C}$. Then*

$$\alpha_i + \alpha_j + \alpha_k \neq 0$$

for any three roots $\alpha_i, \alpha_j, \alpha_k$ of $f(x)$.

The simplest possible linear relation between two roots of irreducible polynomial $f(x)$ is $\alpha_i + \alpha_j = 0$. Such relation implies that the degree d of $f(x)$ is divisible by 2 (because $f(x) = g(x^2)$ for some polynomial $g(x)$). It is natural to ask, does the relation $\alpha_i + \alpha_j + \alpha_k = 0$ imply that d is divisible by 3? In [11], it was shown how to construct irreducible polynomial $f(x)$ for any degree that is a multiple of 3 such that some three distinct roots of $f(x)$ sum up to zero. However, there exist polynomials of degree d whose three distinct roots add up to zero with d not necessarily divisible by 3. It is not known what is the smallest possible degree d of such polynomial: according to [11, Theorem 1.2] such a minimal value of d lies in the range $10 \leq d \leq 20$. As an implication of Theorem 1.1 together with some other auxiliary results, we have the following corollary.

COROLLARY 1.2. *Let d be the smallest positive integer, not multiple of 3, for which there exists an irreducible polynomial $f(x)$ of degree d over $\mathbb{Q}$ whose three roots add up to zero. Then either $d = 16$ or $d = 20$.*

With respect to Corollary 1.2, in [10], there is an example of a polynomial with $d = 20$. In particular, it was shown that the irreducible polynomial

$$f(x) = x^{20} + 4 \cdot 5^9 \cdot x^{10} + 16 \cdot 5^{15}$$

has three distinct roots, which sum up to zero. In contrast, the case of $d = 16$ still remains undecided. Our proof of the case $d = 2p$, where $p \geq 5$ is a prime number, relied on the specific properties of transitive permutation groups of degree $2p$. Thus, the case of $d = 16$ requires a different approach.

In Section 2, we state some auxiliary results and analyze a few exceptional groups via group determinant. Then, in Section 3, Theorem 1.1 together with Corollary 1.2 are proved. Our methods rely on linear algebra, Galois theory, and some combinatorical arguments.

2. AUXILIARY RESULTS

LEMMA 2.1 (cf. [25]; see also [23, Proposition 2]). *Let K be a field such that $\mathbb{Q} \subseteq K \subset \mathbb{C}$. The equality*

$$m_1\alpha_1 + m_2\alpha_2 + \ldots + m_p\alpha_p = 0$$

with distinct conjugates $\alpha_1, \alpha_2, \ldots, \alpha_p$ of an algebraic number α of prime degree p over K and $m_1, m_2, \ldots, m_p \in \mathbb{Q}$ can hold only if $m_1 = m_2 = \ldots = m_p$.

LEMMA 2.2 (cf. [11, Lemma 2.4]). *Let K be a field such that $\mathbb{Q} \subseteq K \subset \mathbb{C}$. The equality*

$$m_1\alpha_1 + m_2\alpha_2 + \ldots + m_d\alpha_d = 0$$

with distinct conjugates $\alpha_1, \alpha_2, \ldots, \alpha_d$ of an algebraic number α of degree d over K and $m_1, m_2, \ldots, m_d \in \mathbb{Q}$ satisfying $\sum_{i=1}^{d} m_i \neq 0$ can hold only if

$$\mathrm{Tr}(\alpha) := \sum_{i=1}^{d} \alpha_i = 0.$$

LEMMA 2.3 (see [13, Lemma 4]). *Let p be a prime number and let $\zeta := e^{2\pi i/p}$ be a primitive p-th root of unity. The only linear relation over $\mathbb{Q}$ between the numbers $1, \zeta, \ldots, \zeta^{p-1}$ is*

$$c \cdot (1 + \zeta + \ldots + \zeta^{p-1}) = 0,$$

where $c \in \mathbb{Q} \setminus \{0\}$.

LEMMA 2.4. *Let $f(x)$ be an irreducible polynomial over the field K such that $\mathbb{Q} \subseteq K \subset \mathbb{C}$. If for some three roots $\alpha_i, \alpha_j, \alpha_k$ of $f(x)$ the following relation holds*

$$\alpha_i + \alpha_j + \alpha_k = 0, \tag{2.2}$$

then all $\alpha_i, \alpha_j, \alpha_k$ are distinct.

PROOF. Assume on the contrary, that $\alpha_i = \alpha_j$. If $\alpha_k = \alpha_i$, then (2.2) implies that $\alpha_i = 0$, a contradiction. Thus, $\alpha_i \neq \alpha_k$. From (2.2) it follows that $\alpha_k/\alpha_i = -2$. However, this is impossible because the quotient of two distinct conjugate algebraic numbers is rational if and only if it is a root of unity. Whence the claim. □

The key ingredient in the proof of Theorem 1.1 is a result of Potočnik and Šajna [28], a modified version of which is presented below.

LEMMA 2.5 (part of [28, Theorem 1]). *Let G be a permutation group acting transitively on a set Ω of size $2p$, where $p \geq 5$ is a prime number. Suppose that G has no blocks of imprimitivity of size p but admits a system of imprimitivity with blocks of size 2, say $\Psi = \{\mathcal{B}_1, \ldots, \mathcal{B}_p\}$. Consider the induced action of G on Ψ with kernel N. Then, one of the following holds.*

1. *For any $x \in \Omega$ the point stabilizer $\mathrm{St}(x)$ in G acts transitively on the set $\Omega \setminus \mathcal{B}_i$ of size $2p-2$, where $\mathcal{B}_i \in \Psi$ is a block containing x.*
2. *For any two blocks $\mathcal{B}_i, \mathcal{B}_j \in \Psi$ there exists a permutation $\tau \in N \subseteq G$ fixing $\mathcal{B}_i$ pointwise and $\mathcal{B}_j$ setwise but not pointwise.*

Lemma 2.5 allows us to prove Theorem 1.1 for almost all transitive permutation groups of degree $2p$. The exceptional groups are treated below. We begin with the only simply primitive (primitive but not doubly transitive) groups of degree $2p$, namely, the alternating group A_5 and the symmetric group S_5. Both groups act on the 10 pairs of a 5-element set. Thus, they are considered as transitive subgroups of S_{10}.

LEMMA 2.6. *Let $f(x)$ be an irreducible polynomial of degree 10 over the field K such that $\mathbb{Q} \subseteq K \subset \mathbb{C}$. If the Galois group G of $f(x)$ is isomorphic to A_5 or S_5, then*

$$\alpha_i + \alpha_j + \alpha_k \neq 0$$

for any three roots of $f(x)$.

PROOF. First, we show that A_5 does not admit the relation

$$\alpha_i + \alpha_j + \alpha_k = 0. \tag{2.3}$$

Since S_5 contains A_5 as a subgroup, the same arguments also remain valid in the case of S_5. The proof goes along similar lines as the proof of Theorem 1.1 in [11]. Suppose on the contrary, that the relation in (2.3) holds. By Lemma 2.4, we can assume that all roots are distinct. Let N be the number of distinct equalities obtained by applying all automorphisms of A_5 to (2.3) and let n be the number of times α_1 occurs among those N equalities. Then

$$3N = 10n. \tag{2.4}$$

Hence, n is divisible by 3. Note also 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 one element since $\{i,j,k\}\cap\{i',j',k'\}$ cannot consist of exactly two indices. Moreover, $\mathrm{Tr}(\alpha_1)=0$ due to Lemma 2.2. From these observations, it is not difficult to derive that $n=3$ (as $n\geq 6$ immediately would lead to a contradiction). We have

$$\alpha_1+\alpha_{n_2}+\alpha_{n_3}=\alpha_1+\alpha_{n_4}+\alpha_{n_5}=\alpha_1+\alpha_{n_6}+\alpha_{n_7} \tag{2.5}$$

for some distinct indices $n_2,\dots,n_7\in\{2,\dots,10\}$. Since A_5 has unique (up to conjugacy) representation as a transitive subgroup of S_{10}, we can assume according to the transitive group database [24], that A_5 is generated by two permutations

$$A_5=((1,9)(3,4)(5,10)(6,7),\ (1,3,5,7,9)(2,4,6,8,10)),$$

where an index i corresponds to a root α_i. Let $\mathrm{St}(\alpha_1)$ denote the stabilizer of α_1 in A_5. Then $\mathrm{St}(\alpha_1)$ consists of six permutations

$$\begin{aligned}\mathrm{St}(\alpha_1)=\{&\,\mathrm{id},\ (2,4,5)(3,6,9)(7,8,10),\ (2,5,4)(3,9,6)(7,10,8)\\ &(2,7)(4,10)(5,8)(6,9),\ (2,8)(3,6)(4,7)(5,10)\\ &(2,10)(3,9)(4,8)(5,7)\}\end{aligned} \tag{2.6}$$

which act in three orbits

$$\mathcal{O}_1=\{1\},\quad \mathcal{O}_2=\{2,4,5,7,8,10\},\quad \mathcal{O}_3=\{3,6,9\}. \tag{2.7}$$

Note that any $\tau\in\mathrm{St}(\alpha_1)$ must act as a permutation on the three equalities in (2.5), since those are the only equalities with α_1. In view of (2.6) and (2.7), it is not difficult to deduce that this is possible only if

$$\{n_2,n_3,n_4,n_5,n_6,n_7\}=\mathcal{O}_2=\{2,4,5,7,8,10\}.$$

By adding all three equalities in (2.5) and using $\mathrm{Tr}(\alpha_1)=0$ we get

$$2\alpha_1=\alpha_3+\alpha_6+\alpha_9. \tag{2.8}$$

Next we apply appropriately selected permutations of A_5, namely

$$(1,3)(2,7)(5,6)(8,9),\ (1,6)(2,3)(5,7)(9,10) \text{ and } (1,9)(3,4)(5,10)(6,7)$$

on (2.8). They map $\mathrm{St}(\alpha_1)$ to $\mathrm{St}(\alpha_3)$, $\mathrm{St}(\alpha_6)$ and $\mathrm{St}(\alpha_9)$, respectively. This leads to the following three equalities

$$2\alpha_3=\alpha_1+\alpha_5+\alpha_8,\quad 2\alpha_6=\alpha_2+\alpha_1+\alpha_{10}\quad\text{and}\quad 2\alpha_9=\alpha_4+\alpha_7+\alpha_1. \tag{2.9}$$

By adding all equalities in (2.8) and (2.9) we arrive at

$$2(\alpha_1+\alpha_3+\alpha_6+\alpha_9)=2\alpha_1+\mathrm{Tr}(\alpha_1).$$

Therefore, $\alpha_3+\alpha_6+\alpha_9=0$. But from (2.8) it follows then that $\alpha_1=0$, a contradiction. This completes the proof. ∎

Next we treat the only two groups of degree $2p$ which have order $2p$, namely, the cyclic group C_{2p} and the dihedral group D_p. We analyze these groups via group determinant, a method which was introduced by Smyth in [29] and later applied by others [11], [23].

LEMMA 2.7. *Let $p \geq 5$ be a prime number and let $f(x)$ be an irreducible polynomial of degree $2p$ over the field K such that $\mathbb{Q} \subseteq K \subset \mathbb{C}$. If the Galois group G of $f(x)$ is isomorphic to the cyclic group C_{2p} of order $2p$, then*

$$\alpha_i + \alpha_j + \alpha_k \neq 0$$

for any three roots of $f(x)$.

PROOF. Let $\alpha_1, \ldots, \alpha_{2p}$ be all roots of $f(x)$. Consider the equality

$$m_1\alpha_1 + m_2\alpha_2 + \ldots + m_{2p}\alpha_{2p} = 0 \tag{2.10}$$

for some $m_1, \ldots, m_{2p} \in \mathbb{Q}$. By applying all $2p$ permutations of C_{2p} on (2.10) we get the following system of $2p$ linear equations

$$\begin{pmatrix} m_1 & m_2 & \ldots & m_{2p} \\ m_{2p} & m_1 & \ldots & m_{2p-1} \\ \vdots & \vdots & \vdots & \vdots \\ m_2 & m_3 & \ldots & m_1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2p} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{2.11}$$

The system of homogeneous linear equations in (2.11) has non-zero solution only if the determinant of the corresponding efficient matrix vanishes. The determinant in question corresponds to the group determinant $\det C_{2p}$ which in the case of cyclic groups is called the circulant [9, Chapter 2] (see also [23, Proposition 2]. In particular

$$\det C_{2p} = \prod_{l=0}^{2p-1} (m_1 + \zeta^l m_2 + \zeta^{2l} m_3 \ldots + \zeta^{(2p-1)l} m_{2p}), \tag{2.12}$$

where $\zeta := e^{2\pi i/p}$ denotes a primitive $2p$-th root of unity.

Assume on the contrary, that $\alpha_i + \alpha_j + \alpha_k = 0$. Due to Lemma 2.4 we can assume that roots $\alpha_i, \alpha_j, \alpha_k$ are distinct. After substituting $m_i = m_j = m_k = 1$ and $m_u = 0$ for all $u \in \{1, \ldots, 2p\} \setminus \{i, j, k\}$ in (2.12), we must get $\det C_{2p} = 0$. Clearly, this implies a non-trivial linear relation over $\mathbb{Q}$ between three $2p$-th roots of unity. Note that $2p$-th roots of unity can be generated by the primitive p-th root of unity and -1. Therefore, a non-trivial linear relation (over $\mathbb{Q}$) between three $2p$-th roots of unity implies a non-trivial linear relation (over $\mathbb{Q}$) between three p-th roots of unity. However, the latter is impossible according to Lemma 2.3. Whence the claim. ∎

LEMMA 2.8. *Let $p \geq 5$ be a prime number and let $f(x)$ be an irreducible polynomial of degree $2p$ over the field K such that $\mathbb{Q} \subseteq K \subset \mathbb{C}$. If the Galois*

group G of $f(x)$ is isomorphic to the dihedral group D_p of order $2p$, then

$$\alpha_i + \alpha_j + \alpha_k \neq 0$$

for any three roots of $f(x)$.

Proof. Consider the relation

$$m_1\alpha_1 + m_2\alpha_2 + \ldots + m_{2p}\alpha_{2p} = 0 \tag{2.13}$$

for some $m_1, \ldots, m_{2p} \in \mathbb{Q}$. Analogously as in the previous lemma, from (2.13) we construct a system of linear equations and investigate the group determinant $\det D_p$. From the character table of D_p we deduce the factorization of $\det D_p$ (see [4, Theorem 4]). In particular

$$\det(D_p) = \Theta_1 \cdot \Theta_2 \cdot \Phi_1^2 \cdot \Phi_2^2 \cdots \Phi_{(p-1)/2}^2,$$

where Θ_1, Θ_2 denote linear factors and $\Phi_1, \ldots, \Phi_{(p-1)/2}$ denote quadratic factors. Let

$$D_p = \langle r, s \mid r^p = s^2 = 1,\ srs = r^{p-1} \rangle \tag{2.14}$$

be the usual presentation of D_p. The two linear representations of D_p are given by

$$r \mapsto 1,\ s \mapsto 1 \quad \text{and} \quad r \mapsto 1,\ s \mapsto -1.$$

Thus, after re-indexation if necessary, the two linear factors of $\det(D_p)$ are

$$\Theta_1 = m_1 + \ldots + m_{2p} \quad \text{and} \quad \Theta_2 = m_1 + \ldots + m_p - m_{p+1} - \ldots - m_{2p}.$$

It is clear that after substituting $m_i = m_j = m_k = 1$ and $m_u = 0$ for all $u \in \{1, \ldots, 2p\} \setminus \{i, j, k\}$ we always have $\Theta_1 \neq 0$ and $\Theta_2 \neq 0$. It remains to show that all quadratic factors of $\det(D_p)$ are non-zero too.

Assume on the contrary that for some $l \in \{1, \ldots, (p-1)/2\}$ a quadratic factor Φ_l vanishes. Set $\Phi := \Phi_l$ and let χ denote the character of the corresponding quadratic representation. The elements of D_p are denoted as $g_1, \ldots, g_{2p}$. Then by the methods described in [4, Chapter 5] we deduce that Φ has the following form

$$\begin{aligned} 2\Phi = {} & \chi(g_i)^2 + \chi(g_j)^2 + \chi(g_k)^2 - \chi(g_i^2) - \chi(g_j^2) - \chi(g_k^2) \\ & + 2\chi(g_i)\chi(g_j) + 2\chi(g_k)\chi(g_i) + 2\chi(g_j)\chi(g_k) \\ & - 2\chi(g_ig_j) - 2\chi(g_kg_i) - 2\chi(g_jg_k). \end{aligned} \tag{2.15}$$

Let

$$D_p \ \to\ GL_2(\mathbb{C}), \quad g_t \mapsto \begin{pmatrix} a_t & b_t \\ c_t & d_t \end{pmatrix}, \tag{2.16}$$

where $t \in \{i, j, k\}$. By definition, $\chi(g_t) = \mathrm{Tr}(g_t)$. Thus, we can express Φ in terms of a_t, b_t, c_t, d_t. Observe that

$$g_i^2 = \begin{pmatrix} a_i^2 + b_ic_i & a_ib_i + b_id_i \\ c_ia_i + d_ic_i & c_ib_i + d_i^2 \end{pmatrix} \Rightarrow \chi(g_i^2) = \mathrm{Tr}(g_i^2) = a_i^2 + 2b_ic_i + d_i^2.$$

Thus

$$\chi(g_i)^2 - \chi(g_i^2) = (a_i + d_i)^2 - (a_i^2 + 2b_ic_i + d_i^2) = 2a_id_i - 2b_ic_i.$$

Similarly

$$g_ig_j = \begin{pmatrix} a_ia_j + b_ic_j & a_ib_j + b_id_j \\ c_ia_j + d_ic_j & c_ib_j + d_id_j \end{pmatrix} \Rightarrow \mathrm{Tr}(g_ig_j) = a_ia_j + b_ic_j + b_jc_i + d_id_j.$$

Thus

$$\begin{aligned} \chi(g_i)\chi(g_j) - \chi(g_ig_j) &= (a_i + d_i)(a_j + d_j) - (a_ia_j + b_ic_j + b_jc_i + d_id_j) \\ &= a_id_j + a_jd_i - b_ic_j - b_jc_i. \end{aligned}$$

By applying the same calculations for other factors of Φ and substituting them in (2.15) we derive that

$$2\Phi = 2(a_i + a_j + a_k)(d_i + d_j + d_k) - 2(b_i + b_j + b_k)(c_i + c_j + c_k).$$

Hence, $\Phi = 0$ implies that

$$(a_1 + a_2 + a_3)(d_1 + d_2 + d_3) = (b_1 + b_2 + b_3)(c_1 + c_2 + c_3). \tag{2.17}$$

The quadratic irreducible representations of D_p are given by

$$r \mapsto \begin{pmatrix} \zeta^n & 0 \\ 0 & \zeta^{-n} \end{pmatrix} \quad \text{and} \quad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where r, s were defined in (2.14), $\zeta = e^{2\pi i/2}$ is a primitive p-th root of unity, and $1 \leq n \leq (p-1)/2$ (see [30, Example 3.0.3]. From this together with (2.16) it is not difficult to derive that for any $t \in \{i, j, k\}$ we have either

$$\begin{gathered} a_t = \zeta^{n_t}, \quad d_t = \zeta^{-n_t}, \quad b_t = 0, \quad c_t = 0 \\ \text{or} \\ a_t = 0, \quad d_t = 0, \quad b_t = \zeta^{n_t}, \quad c_t = \zeta^{-n_t} \end{gathered} \tag{2.18}$$

for some integer $n_t \in \{0, \ldots, p-1\}$. If all a_i, a_j, a_k are non-zero (or all b_i, b_j, b_k are non-zero), then (2.18) implies that the equality in (2.17) becomes

$$(\zeta^{n_i} + \zeta^{n_j} + \zeta^{n_k})(\zeta^{-n_i} + \zeta^{-n_j} + \zeta^{-n_k}) = 0$$

which immediately leads to a contradiction with respect to Lemma 2.3. Thus, at least one of a_i, a_j, a_k is non-zero. Then (2.18) implies that the equality in (2.17) up to a permutation of i, j, k becomes

$$(\zeta^{n_i} + \zeta^{n_j}) \cdot (\zeta^{-n_i} + \zeta^{-n_j}) = (\zeta^{n_k}) \cdot (\zeta^{-n_k})$$

which simplifies to

$$2 + \zeta^{n_i - n_j} + \zeta^{n_j - n_i} = 1,$$

again a contradiction to Lemma 2.3. This completes the proof. ∎

3. Proofs of Theorem 1.1 and Corollary 1.2

Proof of Theorem 1.1. Suppose on the contrary, that there exists an irreducible polynomial $f(x)$ of degree $2p$ over K whose three roots satisfy

$$\alpha_i + \alpha_j + \alpha_k = 0. \tag{3.19}$$

Due to Lemma 2.4, we can assume that all roots in (3.19) are distinct. Let $\Omega = \{\alpha_1, \alpha_2, \ldots, \alpha_{2p}\}$ be the full set of roots of $f(x)$. Since by assumption $p \geq 5$, the relation in (3.19) is possible only if $\mathrm{Tr}(\alpha_1) = 0$ due to Lemma2.2. Denote by L the splitting field of $f(x)$ over K and let G be the Galois group of L/K. For the rest of the proof we treat G as a transitive permutation group on Ω. The next two lemmas will show that G cannot be imprimitive. First we prove the following.

Lemma 3.1. *If G is imprimitive, then it must admit blocks of size p.*

Proof. Suppose on the contrary, that G is imprimitive but has no blocks of size p. It follows that G has a system of imprimitivity with blocks of size 2, say $\mathcal{B}_1, \ldots, \mathcal{B}_p$. Let $\Psi = \{\mathcal{B}_1, \ldots, \mathcal{B}_p\}$. After re-indexation if necessary we can assume that

$$\alpha_1 + \alpha_2 + \alpha_3 = 0. \tag{3.20}$$

By applying Lemma 2.5 on (3.20), it is not difficult to derive that no two of the conjugates $\alpha_1, \alpha_2, \alpha_3$ can belong to the same block. Thus, without restriction of generality, we can suppose that

$$\mathcal{B}_1 = \{\alpha_1, \alpha_4\}, \quad \mathcal{B}_2 = \{\alpha_2, \alpha_5\}, \quad \mathcal{B}_3 = \{\alpha_3, \alpha_6\}. \tag{3.21}$$

Consider the group action of G on Ψ. Let N denote the kernel of this action. We divide the analysis into two cases according to Lemma 2.5.

Case I. The stabilizer of α_1 in G, namely $\mathrm{St}(\alpha_1)$, acts transitively on the set $\Omega \setminus \mathcal{B}_1$ of size $2p-2$. In particular, for any $i \in \{1, \ldots, 2p\} \setminus \{1, 4\}$ there exists $\sigma_i \in \mathrm{St}(\alpha_1)$ such that $\sigma_i(\alpha_2) = \alpha_i$. Consider $2p-2$ equalities of the form

$$\sigma_i(\alpha_1 + \alpha_2 + \alpha_3) = 0 \tag{3.22}$$

for $i \in \{1, \ldots, 2p\} \setminus \{1, 4\}$. Observe that all three conjugates $\sigma_i(\alpha_1), \sigma_i(\alpha_2), \sigma_i(\alpha_3)$ belong to three separate blocks of Ψ. Moreover, no two distinct equalities of the form in (3.22) can share exactly two elements. These observations imply that by adding all $2p-2$ equalities in (3.22) we get

$$\begin{aligned} 0 = & \sum_{i \in \{1, \ldots, 2p\} \setminus \{1,4\}} \sigma_i(\alpha_1 + \alpha_2 + \alpha_3) \\ = & (2p-2) \cdot \alpha_1 + 2(\alpha_2 + \alpha_3 + \ldots + \alpha_{2p}) - 2\alpha_4 \\ = & (2p-4) \cdot \alpha_1 + 2 \cdot \mathrm{Tr}(\alpha_1) - 2\alpha_4. \end{aligned} \tag{3.23}$$

Since $\mathrm{Tr}(\alpha_1) = 0$, the relation in (3.23) simplifies to

$$(2p-4)\cdot\alpha_1 = 2\alpha_4.$$

The last equality is possible only if $2p-4 = -2$. This forces $p = 1$, a contradiction.

Case II. There exists $\sigma \in N \subset G$ such that for any $i \neq j$, an element τ fixes $\mathcal{B}_i$ pointwise and $\mathcal{B}_j$ setwise but not pointwise. Therefore, we can choose $\tau \in N$ that fixes $\mathcal{B}_1$ pointwise and $\mathcal{B}_2$ setwise but not pointwise. By applying τ on the relation in (3.20) we get

$$0 = \tau(\alpha_1+\alpha_2+\alpha_3) = \alpha_1+\alpha_5+\tau(\alpha_3).$$

Since $\tau \in N$, in view of (3.21) we must have $\tau(\alpha_3) = \alpha_3$ or $\tau(\alpha_3) = \alpha_6$. The former leads to $\alpha_2 = \alpha_5$, a contradiction. Thus, $\tau(\alpha_3) = \alpha_6$. This implies that

$$\alpha_2+\alpha_3 = \alpha_5+\alpha_6. \tag{3.24}$$

Next choose $\hat{\tau} \in N$ which fixes $\mathcal{B}_3$ pointwise and $\mathcal{B}_2$ setwise but not pointwise. By applying $\hat{\tau}$ on (3.24) we get

$$\alpha_5+\alpha_3 = \alpha_2+\alpha_6. \tag{3.25}$$

From (3.24) and (3.25) follows that

$$\alpha_5 = \alpha_2,$$

a contradiction. This completes the proof. □

We have shown that if G is imprimitive, then it must contain a system of imprimitivity with blocks of size p. The next lemma is sufficient to conclude that G cannot be imprimitive.

LEMMA 3.2. *If G is imprimitive, then G does not admit blocks of size p.*

PROOF. Suppose on the contrary, that G has a system of imprimitivity consisting of two blocks of size p, say $\mathcal{B}_1, \mathcal{B}_2$. After re-indexation if necessary, we can assume that

$$\mathcal{B}_1 = \{\alpha_1, \ldots, \alpha_p\} \text{ and } \mathcal{B}_2 = \{\alpha_{p+1}, \ldots, \alpha_{2p}\}.$$

From $\alpha_i+\alpha_j+\alpha_k = 0$ and Lemma 2.1 follows that all of $\alpha_i, \alpha_j, \alpha_k$ cannot belong to the same block. Suppose without restriction of generality that $i = 1, j = 2$ and $k = p+1$. Thus

$$\alpha_1+\alpha_2+\alpha_{p+1} = 0, \tag{3.26}$$

where $\alpha_1, \alpha_2 \in \mathcal{B}_1$ and $\alpha_{p+1} \in \mathcal{B}_2$. Let $H \subset G$ denote the setwise stabilizer of $\mathcal{B}_1$ in G. Consider the transitive group action of H on $\mathcal{B}_1$. We will show that the kernel M of this action is trivial. If it is not, then there exists $\tau \in M \subset H$

such that $\mathcal{B}_1$ is fixed pointwise and $\tau(\alpha_t) \neq \alpha_t$ for some $\alpha_t \in \mathcal{B}_2$. Take any $\sigma \in G$ such that $\sigma(\alpha_{p+1}) = \alpha_t$. From (3.26) it follows that

$$\sigma(\alpha_1) + \sigma(\alpha_2) + \alpha_t = 0 \tag{3.27}$$

with $\sigma(\alpha_1), \sigma(\alpha_2) \in \mathcal{B}_1$. Thus

$$\tau\sigma(\alpha_1) + \tau\sigma(\alpha_2) + \tau(\alpha_t) = \sigma(\alpha_1) + \sigma(\alpha_2) + \tau(\alpha_t) = 0. \tag{3.28}$$

Consequently, from (3.27) and (3.28) we get

$$0 = (\sigma(\alpha_1) + \sigma(\alpha_2) + \alpha_t) - (\sigma(\alpha_1) + \sigma(\alpha_2) + \tau(\alpha_t)) \;\Rightarrow\; \alpha_t = \tau(\alpha_t),$$

a contradiction. Thus, we have shown that H acts faithfully on $\mathcal{B}_1$. This implies that $H \subset G$ can be treated as a transitive permutation group of prime degree p with respect to $\mathcal{B}_1$. We divide the rest of the analysis into two cases depending on whether H is non-solvable or solvable.

Case I. Suppose H is non-solvable. The classical result of Burnside [3] implies that H is doubly transitive on $\mathcal{B}_1$. Hence, for any $i \in \{2, \ldots, p\}$ there exists $\phi_i \in H$ such that $\phi_i(\alpha_1) = \alpha_1$ and $\phi_i(\alpha_2) = \alpha_i$. By applying ϕ_i on (3.26) we obtain the following $p-1$ equalities

$$\begin{aligned} &\alpha_1 + \alpha_2 + \phi_2(\alpha_{p+1}) = 0, \\ &\alpha_1 + \alpha_3 + \phi_3(\alpha_{p+1}) = 0, \\ &\qquad\qquad \vdots \\ &\alpha_1 + \alpha_p + \phi_p(\alpha_{p+1}) = 0. \end{aligned} \tag{3.29}$$

It is clear that $\sigma_i(\alpha_{p+1}) \neq \sigma_j(\alpha_{p+1})$, whenever $i \neq j$. Thus, by adding all equalities in (3.29) we arrive at

$$\begin{aligned} 0 =& (p-1) \cdot \alpha_1 + (\alpha_2 + \ldots + \alpha_p) + (\alpha_{p+1} + \ldots + \alpha_{2p} - \alpha_l) \\ =& (p-2) \cdot \alpha_1 + \mathrm{Tr}(\alpha_1) - \alpha_l \end{aligned}$$

for some $\alpha_l \in \mathcal{B}_2$. Since $\mathrm{Tr}(\alpha_1) = 0$, we obtain

$$(p-2) \cdot \alpha_1 = \alpha_l.$$

The last equality is possible only if $p - 2 = -1$. This forces $p = 1$, a contradiction.

Case II. Suppose H is solvable. From the classification of transitive permutation groups of prime degree follows, that either H is a cyclic group of order p or H is a Frobenius group of order ps for some non-unit divisor s of $p-1$ (see [5, Corollary 3.5B]; see also [2, Theorem 2.1]). If H is isomorphic to the cyclic group of order p, then G has order $|H| \cdot 2 = 2p$. It is well-known that the only regular transitive groups of degree $2p$ are the cyclic group C_{2p} and the dihedral group D_p [15]. According to Lemma 2.7 and Lemma 2.8, neither of these groups admit the relation of the form $\alpha_i + \alpha_j + \alpha_k = 0$. Thus, it remains to consider the situation in which H is a Frobenius group. Since H is of index 2 in G, it follows that it is a normal subgroup in G. Consequently,

H acts transitively not only on $\mathcal{B}_1$, but on $\mathcal{B}_2$ also. Let $\mathrm{St}(\alpha_{p+1})$ denote the point stabilizer of α_{p+1} in G. Note that $\mathrm{St}(\alpha_{p+1})$ coincides with the stabilizer of α_{p+1} in H. From the properties of Frobenius groups of prime degree [5, Chapter 3.4] follows that any non-identity $\mu \in \mathrm{St}(\alpha_{p+1})$ acts as a product of s-cycles on $\mathcal{B}_2$ and has exactly one fixed point, namely α_{p+1}. By symmetric argument applied to the block $\mathcal{B}_1$, we deduce that any non-identity $\mu \in \mathrm{St}(\alpha_{p+1})$ acts as a product of s-cycles on $\Omega = \mathcal{B}_1 \cup \mathcal{B}_2$ and has exactly two fixed points. Consider the following two equalities

$$\alpha_1 + \alpha_2 + \alpha_{p+1} = 0 \quad \text{and} \quad \mu(\alpha_1) + \mu(\alpha_2) + \alpha_{p+1} = 0. \tag{3.30}$$

Observe that the relations in (3.30) can hold simultaneously only if the sets $\{\alpha_1, \alpha_2\}$ and $\{\mu(\alpha_1), \mu(\alpha_2)\}$ coincide or their intersection is empty. If the latter holds, then

$$\mu(\alpha_1) + \mu(\alpha_2) - \alpha_1 - \alpha_2 = 0. \tag{3.31}$$

Since $\mu(\alpha_1), \mu(\alpha_2), \alpha_1, \alpha_2 \in \mathcal{B}_1$, an equality in (3.31) constitutes a non-trivial linear relation between polynomial roots of prime degree over some field K such that $\mathbb{Q} \subseteq K \subset \mathbb{C}$, a contradiction to Lemma 2.1. Hence, $\{\alpha_1, \alpha_2\} = \{\mu(\alpha_1), \mu(\alpha_2)\}$. By the same reasoning as in Lemma 2.6, we deduce the existence of equality

$$\alpha_a + \alpha_b + \alpha_{p+1} = 0, \tag{3.32}$$

where $\{a, b\} \neq \{1, 2\}$. Once again, by considering the equalities

$$\alpha_a + \alpha_b + \alpha_{p+1} = 0 \quad \text{and} \quad \mu(\alpha_a) + \mu(\alpha_b) + \alpha_{p+1} = 0$$

we derive that μ interchanges α_a with α_b. Clearly, both α_a and α_b belong to the same block $\mathcal{B}_i$, where $i = 1$ or $i = 2$. If $i = 2$, then $\alpha_a, \alpha_b, \alpha_{p+1} \in \mathcal{B}_2$ and we immediately get a contradiction via Lemma 2.1. If $i = 1$, then

$$\alpha_a + \alpha_b - \alpha_1 - \alpha_2 = 0$$

with $\alpha_a, \alpha_b, \alpha_1, \alpha_2 \in \mathcal{B}_1$ which again contradicts Lemma 2.1. This completes the proof. □

From Lemma 3.1 together with Lemma 3.2 follows that if some three roots of $f(x)$ satisfy $\alpha_i + \alpha_j + \alpha_k = 0$, then the Galois group G of $f(x)$ is primitive. Thanks to the classification of all finite simple groups, we know that a primitive permutation group of degree $2p$ (p is a prime number) is either doubly transitive or has degree 10 and is isomorphic to A_5 or S_5 (both acting on the set of pairs of a 5-element set) [22, Section 4]. However, due to Lemma 2.6, neither A_5 nor S_5 admit the relation $\alpha_i + \alpha_j + \alpha_k = 0$. On the other hand, doubly transitive groups do not admit any non-trivial linear relations at all [7]. Therefore, we have reached a contradiction to the initial assumption in (3.19). This completes the proof. □

PROOF OF COROLLARY 1.2. In [11], it was established that $10 \leq d \leq 20$. Since by assumption, d is not a multiple of 3, it follows that

$$d \in \{10, 11, 13, 14, 16, 17, 19, 20\}.$$

From Lemma 2.1 follows that d cannot be equal to a prime number; this eliminates values equal to $11, 13, 17, 19$. Theorem 1.1 implies that d is not equal twice a prime; this eliminates values equal to 10 and 14. Consequently, $d = 16$ or $d = 20$. □

ACKNOWLEDGEMENTS.

The author is grateful to A. Dubickas for suggesting the problem and providing relevant references. The author also thanks the anonymous referee for a careful reading of the manuscript.

REFERENCES

[1] G. Baron, M. Drmota, and M. Skałba, *Polynomial relations between polynomial roots,* J. Algebra **177** (1995), 827–846.
[2] O. Ben-Shimol, *On Galois groups of prime degree polynomials with complex roots,* Algebra Discrete Math. (2009), 99–107.
[3] W. Burnside, Theory of Groups of Finite Order, 2nd ed., Cambridge Univ. Press, 1911.
[4] K. Conrad, *The origin of representation theory,* Enseign Math. (2) **44** (1998), 361–392.
[5] J. D. Dixon and B. Mortimer, Permutation groups, Springer-Verlag, New York, 1996.
[6] J. D. Dixon, *Polynomials with nontrivial relations between their roots,* Acta Arith. **82** (1997), 293–302.
[7] M. Drmota and M. Skałba, *On multiplicative and linear independence of polynomial roots,* Contributions to general algebra, 7 (Vienna, 1990), Hölder-Pichler-Temsky, Vienna, 1991, 127–135.
[8] M. Drmota and M. Skałba, *Relations between polynomial roots,* Acta Arith. **71** (1995), 65–77.
[9] A. Dubickas, *On the degree of a linear form in conjugates of an algebraic number,* Illinois J. Math. **46** (2002), 571–585.
[10] A. Dubickas and C. J. Smyth, *Polynomials with three distinct zeros summing to zero: Problem 11123*, Amer. Math. Monthly **113** (2006), 941-942.
[11] A. Dubickas and J. Jankauskas, *Simple linear relations between conjugate algebraic numbers of low degree,* J. Ramanujan Math. Soc. **30** (2015), 219–235.
[12] A. Dubickas, K. Hare, and J. Jankauskas, *No two non-real conjugates of a Pisot number have the same imaginary part,* Math. Comp. **86** (2017), 935–950.
[13] A. Dubickas, *On sums of two and three roots of unity,* J. Number Theory **192** (2018), 65–79.
[14] J. S. Ellenberg and W. Hardt *Smyth's conjecture and a non-deterministic Hasse principle,* `https://arxiv.org/abs/2503.15833`.
[15] J. A. Gallian, *The classification of groups of order 2p,* Math. Mag. **74** (2001), 60–61.
[16] K. Girstmair, *Linear dependence of zeros of polynomials and construction of primitive elements,* Manuscripta Math. **39** (1982), 81–97.
[17] K. Girstmair, *Linear relations between roots of polynomials,* Acta Arith. **89** (1999), 53–96.

[18] K. Girstmair, *The Galois relation $x_1 = x_2 + x_3$ and Fermat over finite fields,* Acta Arith. **124** (2006), 357–370.
[19] K. Girstmair, *The Galois relation $x_1 = x_2 + x_3$ for finite simple groups,* Acta Arith. **127** (2007), 301–303.
[20] K. Girstmair, *The Galois relations $x_1 = x_2 + x_3$ and $x_1 = x_2x_3$ for certain solvable groups,* Ann. Sci. Math. Quebec **32** (2008), 171–174.
[21] W. Hardt and J. Yin, *Linear relations among Galois conjugates over $\mathbb{F}_q(t)$,* Res. Number Theory **8** (2022), Paper No. 34, 14.
[22] A. Hujdurović, K. Kutnar, D. Marušič, and Š. Miklavič, *Intersection density of transitive groups of certain degrees,* Algebr. Comb. **5** (2022), 289–297.
[23] Y. Kitaoka, *Notes on the distribution of roots modulo a prime of a polynomial,* Unif. Distrib. Theory **12** (2017), 91–117.
[24] J. Klüners and G. Malle, *A database for number fields,* `http://galoisdb.math.upb.de/home`.
[25] V. A. Kurbatov, *Galois extensions of prime degree and their primitive elements,* Soviet Math. **21** (1977), 49–52.
[26] F. Lalande, *La relation linéaire $a = b + c + \ldots + t$ entre les racines d'un polynôme,* J. Theor. Nombres Bordeaux **19** (2007), 473–484.
[27] F. Lalande, *À propos de la relation galoisienne $x_1 = x_2 + x_3$,* J. Theor. Nombres Bordeaux **22** (2010), 661–673.
[28] P. Potočnik and M. Šajna, *A note on transitive permutation groups of degree twice a prime,* Ars Math. Contemp. **1** (2008) 165–168.
[29] C. J. Smyth, *Additive and multiplicative relations connecting conjugate algebraic numbers,* J. Number Theory **23** (1986), 243–254.
[30] P. Vaidyanathan, *Representation theory,* Lecture notes, IISER Bhopal, `https://home.iiserb.ac.in/~prahlad/documents/teaching/mth410_notes.pdf`.

P. Virbalas
Institute of Mathematics, Faculty of Mathematics and Informatics
Vilnius University
Naugarduko 24, Vilnius LT-03225
Lithuania
E-mail: `paulius.virbalas@mif.vu.lt`