

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

$$(1.1) \quad m_1\alpha_1 + \dots + m_d\alpha_d \in K$$

with coefficients  $m_1, \dots, m_d \in K$  is called a *linear* (or *additive*) relation between the conjugates of  $\alpha$ . From the properties of symmetric polynomials, it follows that if  $m_1 = \dots = m_d$ , a relation in (1.1) always holds; such relations are called *trivial*. In contrast, the reasons behind *non-trivial* linear relations are far less understood. As we might expect, non-trivial relations imply special conditions on the minimal polynomial of  $\alpha$ . 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 Skalba (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 Skalba [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 a 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 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 combinatorial 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*

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

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

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

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

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

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

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  $1, \zeta, \dots, \zeta^{p-1}$  is*

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

*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*

$$(2.1) \quad \alpha_i + \alpha_j + \alpha_k = 0,$$

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 (2.1) implies that  $\alpha_i = 0$ , a contradiction. Thus,  $\alpha_i \neq \alpha_k$ . From (2.1) it follows that  $\alpha_k/\alpha_i = -2$ . However, this is impossible because the quotient of two distinct conjugate algebraic numbers is rational only if it is a root of unity. Whence the claim.  $\square$

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  $\Omega$  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  $\Psi = \{\mathcal{B}_1, \dots, \mathcal{B}_p\}$ . Consider the induced action of  $G$  on  $\Psi$  with kernel  $N$ . Then, one of the following holds.*

1. *For any  $x \in \Omega$  the point stabilizer  $\text{St}(x)$  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

$$(2.2) \quad \alpha_i + \alpha_j + \alpha_k = 0.$$

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 (2.2) 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 (2.2) and let  $n$  be the number of times  $\alpha_1$  occurs among those  $N$  equalities. Then

$$(2.3) \quad 3N = 10n.$$

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,  $\text{Tr}(\alpha_1) = 0$  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

$$(2.4) \quad \alpha_1 + \alpha_{n_2} + \alpha_{n_3} = \alpha_1 + \alpha_{n_4} + \alpha_{n_5} = \alpha_1 + \alpha_{n_6} + \alpha_{n_7}$$

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  $\alpha_i$ . Let  $\text{St}(\alpha_1)$  denote the stabilizer of  $\alpha_1$  in  $A_5$ . Then  $\text{St}(\alpha_1)$  consists of six permutations

$$(2.5) \quad \begin{aligned} \text{St}(\alpha_1) = \{ & \text{id}, (2, 4, 5)(3, 6, 9)(7, 8, 10), (2, 5, 4)(3, 9, 6)(7, 10, 8), \\ & (2, 7)(4, 10)(5, 8)(6, 9), (2, 8)(3, 6)(4, 7)(5, 10), \\ & (2, 10)(3, 9)(4, 8)(5, 7) \} \end{aligned}$$

which act in three orbits

$$(2.6) \quad \mathcal{O}_1 = \{1\}, \quad \mathcal{O}_2 = \{2, 4, 5, 7, 8, 10\}, \quad \mathcal{O}_3 = \{3, 6, 9\}.$$

Note that any  $\tau \in \text{St}(\alpha_1)$  must act as a permutation on the three equalities in (2.4), since those are the only equalities with  $\alpha_1$ . In view of (2.5) and (2.6), 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 (2.4) and using  $\text{Tr}(\alpha_1) = 0$  we get

$$(2.7) \quad 2\alpha_1 = \alpha_3 + \alpha_6 + \alpha_9.$$

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

$$(2.8) \quad 2\alpha_3 = \alpha_1 + \alpha_5 + \alpha_8, \quad 2\alpha_6 = \alpha_2 + \alpha_1 + \alpha_{10} \quad \text{and} \quad 2\alpha_9 = \alpha_4 + \alpha_7 + \alpha_1.$$

By adding all equalities in (2.7) and (2.8) we obtain

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

Therefore,  $\alpha_3 + \alpha_6 + \alpha_9 = 0$ . But from (2.7) it follows then that  $\alpha_1 = 0$ , a contradiction. This completes the proof.  $\square$

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  $\alpha_1, \dots, \alpha_{2p}$  be all roots of  $f(x)$ . Consider the equation

$$(2.9) \quad m_1\alpha_1 + m_2\alpha_2 + \dots + m_{2p}\alpha_{2p} = 0$$

for some  $m_1, \dots, m_{2p} \in \mathbb{Q}$ . By applying all  $2p$  permutations of  $C_{2p}$  on (2.9) we get the following system of  $2p$  linear equations

$$(2.10) \quad \begin{pmatrix} m_1 & m_2 & \cdots & m_{2p} \\ m_{2p} & m_1 & \cdots & m_{2p-1} \\ \vdots & \vdots & \vdots & \vdots \\ m_2 & m_3 & \cdots & m_1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{2p} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

The system of homogeneous linear equations in (2.10) has non-zero solution only if the determinant of the corresponding coefficient 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

$$(2.11) \quad \det C_{2p} = \prod_{l=0}^{2p-1} (m_1 + \zeta^l m_2 + \zeta^{2l} m_3 + \dots + \zeta^{(2p-1)l} m_{2p}),$$

where  $\zeta := e^{2\pi i/(2p)}$  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  $u \in \{1, \dots, 2p\} \setminus \{i, j, k\}$  in (2.11), 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. This completes the proof.  $\square$

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

$$(2.12) \quad m_1\alpha_1 + m_2\alpha_2 + \cdots + m_{2p}\alpha_{2p} = 0$$

for some  $m_1, \dots, m_{2p} \in \mathbb{Q}$ . Analogously as in the previous lemma, from (2.12) 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  $\Theta_1, \Theta_2$  denote linear factors and  $\Phi_1, \dots, \Phi_{(p-1)/2}$  denote quadratic factors. Let

$$(2.13) \quad D_p = \langle r, s \mid r^p = s^2 = 1, sr s = r^{p-1} \rangle$$

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 reindexing if necessary, the two linear factors of  $\det(D_p)$  are

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

It is clear that after substituting  $m_i = m_j = m_k = 1$  and  $m_u = 0$  for all  $u \in \{1, \dots, 2p\} \setminus \{i, j, k\}$  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  $l \in \{1, \dots, (p-1)/2\}$  a quadratic factor  $\Phi_l$  vanishes. Set  $\Phi := \Phi_l$  and let  $\chi$  denote the character of the corresponding quadratic representation. The elements of  $D_p$  are denoted as  $g_1, \dots, g_{2p}$ . Then by the methods described in [4, Chapter 5] we deduce that  $\Phi$  has the following form

$$(2.14) \quad \begin{aligned} 2\Phi &= \chi(g_i)^2 + \chi(g_j)^2 + \chi(g_k)^2 - \chi(g_i^2) - \chi(g_j^2) - \chi(g_k^2) \\ &+ 2\chi(g_i)\chi(g_j) + 2\chi(g_k)\chi(g_i) + 2\chi(g_j)\chi(g_k) \\ &- 2\chi(g_i g_j) - 2\chi(g_k g_i) - 2\chi(g_j g_k). \end{aligned}$$

Let

$$(2.15) \quad D_p \rightarrow GL_2(\mathbb{C}), \quad g_t \mapsto \begin{pmatrix} a_t & b_t \\ c_t & d_t \end{pmatrix},$$

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

$$g_i^2 = \begin{pmatrix} a_i^2 + b_i c_i & a_i b_i + b_i d_i \\ c_i a_i + d_i c_i & c_i b_i + d_i^2 \end{pmatrix} \Rightarrow \chi(g_i^2) = \text{Tr}(g_i^2) = a_i^2 + 2b_i c_i + d_i^2.$$

Thus

$$\chi(g_i)^2 - \chi(g_i^2) = (a_i + d_i)^2 - (a_i^2 + 2b_i c_i + d_i^2) = 2a_i d_i - 2b_i c_i.$$

Similarly

$$g_i g_j = \begin{pmatrix} a_i a_j + b_i c_j & a_i b_j + b_i d_j \\ c_i a_j + d_i c_j & c_i b_j + d_i d_j \end{pmatrix} \Rightarrow \text{Tr}(g_i g_j) = a_i a_j + b_i c_j + b_j c_i + d_i d_j.$$

Thus

$$\begin{aligned} \chi(g_i)\chi(g_j) - \chi(g_i g_j) &= (a_i + d_i)(a_j + d_j) - (a_i a_j + b_i c_j + b_j c_i + d_i d_j) \\ &= a_i d_j + a_j d_i - b_i c_j - b_j c_i. \end{aligned}$$

By applying the same calculations for other factors of  $\Phi$  and substituting them in (2.14) 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

$$(2.16) \quad (a_i + a_j + a_k)(d_i + d_j + d_k) = (b_i + b_j + b_k)(c_i + c_j + c_k).$$

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 (2.13),  $\zeta = e^{2\pi i/p}$  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 (2.15) it is not difficult to derive that for any  $t \in \{i, j, k\}$  we have either

$$(2.17) \quad \begin{aligned} a_t = \zeta^{n_t}, \quad d_t = \zeta^{-n_t}, \quad b_t = 0, \quad c_t = 0 \\ \text{or} \end{aligned}$$

$$a_t = 0, \quad d_t = 0, \quad b_t = \zeta^{n_t}, \quad c_t = \zeta^{-n_t}$$

for some integer  $n_t \in \{0, \dots, p-1\}$ . If all  $a_i, a_j, a_k$  are non-zero (or all  $b_i, b_j, b_k$  are non-zero), then (2.17) implies that the equality in (2.16) 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 (2.17) implies that the equality in (2.16) 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.  $\square$

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

$$(3.1) \quad \alpha_i + \alpha_j + \alpha_k = 0.$$

Due to Lemma 2.4, we can assume that all roots in (3.1) are distinct. Let  $\Omega = \{\alpha_1, \alpha_2, \dots, \alpha_{2p}\}$  be the full set of roots of  $f(x)$ . Since by assumption  $p \geq 5$ , the relation in (3.1) can hold only if  $\text{Tr}(\alpha_1) = 0$  by Lemma 2.2. 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  $\Omega$ . 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  $\mathcal{B}_1, \dots, \mathcal{B}_p$ . Let  $\Psi = \{\mathcal{B}_1, \dots, \mathcal{B}_p\}$ . After reindexing if necessary we can assume that

$$(3.2) \quad \alpha_1 + \alpha_2 + \alpha_3 = 0.$$

By applying Lemma 2.5 to (3.2), it follows that no two of the conjugates  $\alpha_1, \alpha_2, \alpha_3$  can belong to the same block. Thus, without loss of generality, we can suppose that

$$(3.3) \quad \mathcal{B}_1 = \{\alpha_1, \alpha_4\}, \quad \mathcal{B}_2 = \{\alpha_2, \alpha_5\}, \quad \mathcal{B}_3 = \{\alpha_3, \alpha_6\}.$$

Consider the group action of  $G$  on  $\Psi$ . 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  $\alpha_1$  in  $G$ , namely  $\text{St}(\alpha_1)$ , acts transitively on the set  $\Omega \setminus \mathcal{B}_1$  of size  $2p - 2$ . In particular, for any  $i \in \{1, \dots, 2p\} \setminus \{1, 4\}$  there exists  $\sigma_i \in \text{St}(\alpha_1)$  such that  $\sigma_i(\alpha_2) = \alpha_i$ . Consider  $2p - 2$  equalities of the form

$$(3.4) \quad \sigma_i(\alpha_1 + \alpha_2 + \alpha_3) = 0,$$

for  $i \in \{1, \dots, 2p\} \setminus \{1, 4\}$ . Observe that all three conjugates  $\sigma_i(\alpha_1), \sigma_i(\alpha_2), \sigma_i(\alpha_3)$  belong to three separate blocks of  $\Psi$ . Moreover, no two distinct equalities of the form in (3.4) can share exactly two elements. These observations imply that by adding all  $2p - 2$  equalities in (3.4) we get

$$(3.5) \quad \begin{aligned} 0 &= \sum_{i \in \{1, \dots, 2p\} \setminus \{1, 4\}} \sigma_i(\alpha_1 + \alpha_2 + \alpha_3) \\ &= (2p - 2) \cdot \alpha_1 + 2(\alpha_2 + \alpha_3 + \dots + \alpha_{2p}) - 2\alpha_4 \\ &= (2p - 4) \cdot \alpha_1 + 2 \cdot \text{Tr}(\alpha_1) - 2\alpha_4. \end{aligned}$$

Since  $\text{Tr}(\alpha_1) = 0$ , the relation in (3.5) simplifies to

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

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

CASE II. There exists  $\tau \in N \subset G$  such that for any  $i \neq j$ , an element  $\tau$  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  $\tau$  to the relation in (3.2) we get

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

Since  $\tau \in N$ , in view of (3.3) 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

$$(3.6) \quad \alpha_2 + \alpha_3 = \alpha_5 + \alpha_6.$$

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 (3.6) we get

$$(3.7) \quad \alpha_5 + \alpha_3 = \alpha_2 + \alpha_6.$$

From (3.6) and (3.7) it follows that

$$\alpha_5 = \alpha_2,$$

a contradiction. This completes the proof.  $\square$

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  $p$ , denoted  $\mathcal{B}_1, \mathcal{B}_2$ . After reindexing if necessary, we can assume that

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

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 loss of generality that  $i = 1, j = 2$  and  $k = p + 1$ . Thus

$$(3.8) \quad \alpha_1 + \alpha_2 + \alpha_{p+1} = 0,$$

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 (3.8) it follows that

$$(3.9) \quad \sigma(\alpha_1) + \sigma(\alpha_2) + \alpha_t = 0$$

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

$$(3.10) \quad \tau\sigma(\alpha_1) + \tau\sigma(\alpha_2) + \tau(\alpha_t) = \sigma(\alpha_1) + \sigma(\alpha_2) + \tau(\alpha_t) = 0.$$

Consequently, from (3.9) and (3.10) 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 viewed 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  $i \in \{2, \dots, p\}$  there exists  $\phi_i \in H$  such that  $\phi_i(\alpha_1) = \alpha_1$  and  $\phi_i(\alpha_2) = \alpha_i$ . By applying  $\phi_i$  on (3.8) we obtain the following  $p - 1$  equalities

$$(3.11) \quad \begin{aligned} \alpha_1 + \alpha_2 + \phi_2(\alpha_{p+1}) &= 0, \\ \alpha_1 + \alpha_3 + \phi_3(\alpha_{p+1}) &= 0, \\ &\vdots \\ \alpha_1 + \alpha_p + \phi_p(\alpha_{p+1}) &= 0. \end{aligned}$$

It is clear that  $\sigma_i(\alpha_{p+1}) \neq \sigma_j(\alpha_{p+1})$ , whenever  $i \neq j$ . Thus, summing all equalities in (3.11) we get

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

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

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

The last equality holds 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 also on  $\mathcal{B}_2$ . Let  $\text{St}(\alpha_{p+1})$  denote the point stabilizer of  $\alpha_{p+1}$  in  $G$ . Note that  $\text{St}(\alpha_{p+1})$  coincides with the stabilizer of  $\alpha_{p+1}$  in  $H$ . From the properties of Frobenius groups of prime degree [5, Chapter 3.4] follows that any non-identity  $\mu \in \text{St}(\alpha_{p+1})$  acts as a

product of  $s$ -cycles on  $\mathcal{B}_2$  and has exactly one fixed point, namely  $\alpha_{p+1}$ . By symmetric argument applied to the block  $\mathcal{B}_1$ , we deduce that any non-identity  $\mu \in \text{St}(\alpha_{p+1})$  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

$$(3.12) \quad \alpha_1 + \alpha_2 + \alpha_{p+1} = 0 \quad \text{and} \quad \mu(\alpha_1) + \mu(\alpha_2) + \alpha_{p+1} = 0.$$

Observe that the relations in (3.12) 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

$$(3.13) \quad \mu(\alpha_1) + \mu(\alpha_2) - \alpha_1 - \alpha_2 = 0.$$

Since  $\mu(\alpha_1), \mu(\alpha_2), \alpha_1, \alpha_2 \in \mathcal{B}_1$ , an equality in (3.13) 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 obtain the equality

$$(3.14) \quad \alpha_a + \alpha_b + \alpha_{p+1} = 0,$$

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 conclude that  $\mu$  interchanges  $\alpha_a$  with  $\alpha_b$ . Clearly, both  $\alpha_a$  and  $\alpha_b$  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 obtain a contradiction with 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.  $\square$

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 with the initial assumption in (3.1). This completes the proof.  $\square$

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 it follows that  $d$  cannot be equal to a prime number; this eliminates possibilities 11, 13, 17 and 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  $d = 20$ .  $\square$

#### ACKNOWLEDGEMENTS.

The author is grateful to A. Dubickas for suggesting the problem and for 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. Skalba, *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** (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. Skalba, *On multiplicative and linear independence of polynomial roots*, In Contributions to general algebra, 7 (Vienna, 1990), Hölder-Pichler-Tempsky, Vienna, 1991, 127–135.
- [8] M. Drmota and M. Skalba, *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.
- [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*, Izv. Vysš. Ucebn. Zaved. Matematika **21** (1977), 61–66.
- [26] F. Lalande, *La relation linéaire  $a = b + c + \dots + t$  entre les racines d'un polynôme*, J. Théor. 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](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

*Received:* 8.7.2023.

*Revised:* 2.12.2024.

## LINEARNI ODNOSI IZMEĐU TRI ALGEBARSKA KONJUGATA STUPNJA DVOSTRUKOG PROSTOG BROJA

P. VIRBALAS

SAŽETAK. U ovom radu pokazujemo da ne postoji ireducibilan polinom  $f(x)$  stupnja  $2p$  ( $p \geq 5$  je prost broj) nad  $\mathbb{Q}$  čija je suma tri različita korijena jednaka nuli. Ovo proširuje neke ranije rezultate o linearnim odnosima između tri algebarska broja. Konkretno, neka je  $d$  najmanji prirodan broj, koji nije višekratnik broja 3, za koji postoji ireducibilan polinom  $f(x)$  stupnja  $d$  čija je suma tri različita korijena jednaka nuli. Godine 2015. Dubickas i Jankauskas su utvrdili da je  $10 \leq d \leq 20$ . Kao korolar, pokazujemo da je  $d$  ili 16 ili 20.