mathematics

Article

Degree of the Product of Two Algebraic Numbers One of Which Is of Prime Degree

Paulius Virbalas

Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania; paulius.virbalas@mif.stud.vu.lt

Abstract: Let α and β be two algebraic numbers such that $\deg(\alpha) = m$ and $\deg(\beta) = p$, where p is a prime number not dividing m. This research is focused on the following two objectives: to discover new conditions under which $\deg(\alpha\beta) = mp$; to determine the complete list of values $\deg(\alpha\beta)$ can take. With respect to the first question, we find that if the minimal polynomial of β over $\mathbb{Q}$ is neither $x^p + c$ nor $x^2 + cx + c^2$, then necessarily $\deg(\alpha\beta) = mp$ and $\alpha\beta$ is a primitive element of $\mathbb{Q}(\alpha, \beta)$. This supplements some earlier results by Weintraub. With respect to the second question, we determine that if $p > 2$ and $p - 1$ divides m, then for every divisor k of $p - 1$, there exist α and β such that $\deg(\alpha\beta) = mp/k$.

Keywords: degree of an algebraic number; Galois theory; transitive permutation groups

MSC: 11R04; 11R32

1. Introduction

Suppose α and β are two algebraic numbers such that $\deg(\alpha) = a$ and $\deg(\beta) = b$, where $\deg(\gamma)$ denotes the degree of an algebraic number γ over the field $\mathbb{Q}$. In [1], Dubickas established some necessary and sufficient conditions under which

$$\deg(\alpha + \beta) = ab \quad \text{and} \quad \deg(\alpha\beta) = ab. \tag{1}$$

Unfortunately, most of the conditions found in [1] are rather difficult to check. This motivates a search for alternative criteria allowing us to conclude when the equalities in (1) hold.

The additive case of (1) seems to have been first considered by Nagell [2] and then followed by Kaplansky ([3], Part I, Theorem 63), Isaacs [4], Browkin, and Diviš and Schinzel [5]. A detailed discussion of this question together with some applications can also be found in the work by Cagliero and Szechtman [6]. In contrast, the multiplicative case of (1) to our knowledge has been investigated only by Dubickas [1] and Weintraub [7].

One of the most important results on this topic is due to Isaacs [4], who showed that if a and b are coprime, then $\deg(\alpha + \beta) = ab$. The primary objective of this research is to investigate whether the same condition is sufficient for the multiplicative case of (1) to hold. As the next example shows, the answer is negative. Indeed, we can set $\alpha = \zeta$ and $\beta = \sqrt[p]{2}$, where $p > 2$ is a prime number and ζ is a primitive p^{th} root of unity; i.e., $\zeta = e^{2\pi i/p}$. Then, $\deg(\alpha) = p - 1$ and $\deg(\beta) = p$, but

$$\deg(\alpha\beta) = \deg(\sqrt[p]{2}\zeta) = p \neq (p - 1)p. \tag{2}$$

We have found that the example in (2) can be generalized as follows:

Theorem 1. *Let p be a prime number. Then there exist algebraic numbers α, β such that* $\deg(\alpha) = p - 1$, $\deg(\beta) = p$, *and* $\deg(\alpha\beta) = (p - 1)p/k$ *for any divisor k of $p - 1$.*

check for updates

Citation: Virbalas, P. Degree of the Product of Two Algebraic Numbers One of Which Is of Prime Degree. *Mathematics* **2023**, *11*, 1485. https://doi.org/10.3390/math11061485

Academic Editor: Jiyou Li

Received: 2 February 2023
Revised: 15 March 2023
Accepted: 16 March 2023
Published: 18 March 2023

For an illustration, suppose that $p = 7$ and $k = 3$. Following the construction process described in the proof of Theorem 1, we should set $\alpha = 1 + \zeta + \zeta^3$ and $\beta = \sqrt[7]{2}$, where $\zeta = e^{2\pi i/7}$. Then, by calculations with SAGE one can check that:

$$\deg(\alpha) = 7 - 1 = 6, \quad \deg(\beta) = 7 \quad \text{and} \quad \deg(\alpha\beta) = 6 \cdot 7/3 = 14.$$

Motivated by the investigations that led to Theorem 1, in this paper we restrict our attention to the situation in which $\deg(\alpha) = m$ is an arbitrary positive integer and $\deg(\beta) = p$ is a prime number such that $p \nmid m$. In this setting, we focus on the following two objectives: to discover new conditions under which $\deg(\alpha\beta) = \deg(\alpha) \cdot \deg(\beta)$; to determine the complete list of values $\deg(\alpha\beta)$ can take.

Our research methods are similar to the ones applied by Dubickas and Jankauskas [8] in their work on relations between algebraic conjugates. By using Galois theory together with a well-known result of Drmota and Skałba [9] on the multiplicative relations between algebraic conjugates of prime degree, we deduce the following sufficient condition under which $\deg(\alpha\beta) = \deg(\alpha) \cdot \deg(\beta)$:

Theorem 2. *Let p be a prime number and let m be a positive integer such that $p \nmid m$. Suppose that α, β are algebraic numbers such that $\deg(\alpha) = m$, $\deg(\beta) = p$, and the minimal polynomial of β over $\mathbb{Q}$ is $f(x)$.*

(a) If $p > 2$ and $f(x) \neq x^p + c$, where $c \in \mathbb{Q}$, then $\deg(\alpha\beta) = mp$.

(b) If $p = 2$ and $f(x) \neq x^2 + cx + c^2$, where $c \in \mathbb{Q}$, then $\deg(\alpha\beta) = mp$.

These findings supplement some observations on primitive elements of field extensions made by Weintraub [7]. If α and β are algebraic numbers satisfying the assumptions of Theorem 2, then it immediately follows that $\alpha\beta$ is a primitive element of $\mathbb{Q}(\alpha, \beta)$; i.e., $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha\beta)$. For example, take

$$\alpha = \sqrt{\sqrt{2} + 2} \quad \text{and} \quad \beta = 1 + \sqrt[3]{2} + \sqrt[3]{4}.$$

Calculations with SAGE show that the minimal polynomial of α is $x^4 - 4x^2 + 2$, and that the minimal polynomial of β is $x^3 - 3x^2 - 3x - 1$. We see that $\deg(\alpha) = 4$, $\deg(\beta) = 3$, and the minimal polynomial of β is not of the form $x^3 + c$. Therefore, Theorem 2 implies that the minimal polynomial of $\alpha\beta$ has a degree equal to $4 \cdot 3 = 12$, and that the generating element of the composite field extension $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ can be chosen to be $\alpha\beta$.

It should be noted that Theorem 2 provides a sufficient but not necessary condition, as even if the minimal polynomial of β is equal to $x^p + c$ (or $x^2 + cx + c^2$ if $p = 2$), one can always choose α of degree m so that $p \nmid m$ and $\deg(\alpha\beta) = mp$.

As far as our second research objective is concerned, by applying Theorem 2 together with the theory of transitive permutation groups, we provide the complete list of values that $\deg(\alpha\beta)$ can take in the case $\deg(\alpha) = m$, $\deg(\beta) = p$, and p is a prime such that $p \nmid m$:

Theorem 3. *Let p be a prime number and let m be a positive integer such that $p \nmid m$. Suppose that α, β are algebraic numbers such that $\deg(\alpha) = m$ and $\deg(\beta) = p$.*

(a) If $p > 2$ and $p - 1 \nmid m$, then $\deg(\alpha\beta) = mp$.

(b) If $p > 2$ and $p - 1 \mid m$, then $\deg(\alpha\beta) = mp/k$, where k is a divisor of $p - 1$. In fact, for any divisor k of $p - 1$, such α and β exist.

(c) If $p = 2$ and $3 \nmid m$, then $\deg(\alpha\beta) = 2m$.

(d) If $p = 2$ and $3 \mid m$, then $\deg(\alpha\beta) = vm$, where $v = 1, 2$. In fact, for both values of v, such α and β exist.

Theorem 3 has a strong connection with investigations on product-feasible triplets, which, together with similar notions of sum-feasible and compositum-feasible triplets, were introduced by Drungilas, Dubickas, and Smyth [10]. A triplet $(a, b, c) \in \mathbb{N}^3$ is called product-feasible if there exist three algebraic numbers α, β, γ with degrees a, b, c over $\mathbb{Q}$, respectively, such that $\alpha\beta\gamma = 1$. To this day, all sum-feasible and compositum-feasible triplets (a, b, c) satisfying $a \leq b \leq 9$ have been found [11–13]. Conversely, due to additional obstacles arising in the multiplicative setting of the problem, the search for all product-feasible (a, b, c) triplets satisfying $a \leq b \leq 9$ has not been completed yet. We show how Theorem 3 can be directly applied for further research on product-feasible triplets. First, we reformulate it as follows:

Corollary 1. *Let p be a prime number and let a be a positive integer such that $p \nmid a$. Then, the triplet (a, p, c) is product-feasible if and only if at least one of the following conditions holds:*

(a) $c = ap$.
(b) $p - 1 \mid a$ *and* $c = ap/k$ *for some divisor* k *of* $p - 1$.
(c) $p = 2$ *and* $c = 2a$ *or* $c = a$.

To illustrate how Corollary 1 works, we find all product-feasible triplets $(a, 7, c)$ satisfying $a < 7$.

Corollary 2. *The triplet $(a, 7, c)$, where $a < 7$, is product-feasible if and only if $c = 7a$ or $a = 6$ and $c = 6 \cdot 7/k$ with $k \in \{2, 3, 6\}$.*

In the next section, we provide some auxiliary results that will be used later. Then, in Section 3, we prove Theorem 1 and show how to construct non-trivial examples satisfying Theorem 1 for any prime p. In Section 4 we investigate the multiplicative relations between the polynomial roots in order to complete the proof of Theorem 2. Finally, via the fundamental theorem of Galois theory and the results from earlier sections, the proofs of Theorem 3 and Corollary 1 and Corollary 2 are derived in Section 5.

2. Auxiliary Results

We start with some basic results from abstract algebra.

Lemma 1 ([14], Chapter 4.1, Exercise 9)**.** *Assume that G acts transitively on a finite set Ω and let H be a normal subgroup of G. Then, all orbits of H on Ω have the same cardinality.*

Lemma 2 ([15], Theorem 1.6A)**.** *Let G be a group acting transitively on a set Ω and let H be a normal subgroup of G. If the index $[G : H]$ is finite, then the number of orbits of H divides $[G : H]$.*

Lemma 3. *Let G be a group acting transitively and faithfully on a set Ω of size m and let N denote a point stabilizer in G. If N is normal in G, then $|G| = m$.*

Proof. Consider the group action of G on Ω. Since G acts transitively, we know that all point stabilizers are conjugate to N in G. However, N is normal in G, hence $gNg^{-1} = N$ for all $g \in G$. Thus, N stabilizes all points of Ω. Since G acts faithfully, we conclude that N consists only of the identity element; i.e., $|N| = 1$. Finally, by the orbit-stabilizer theorem, we have that $|G| = 1 \cdot m = m$. □

Lemma 4. *Let $f(x)$ be the minimal polynomial of α over $\mathbb{Q}$ and suppose L is a normal extension of $\mathbb{Q}(\alpha)$ such that $f(x)$ splits in L. Let G denote the Galois group of $L/\mathbb{Q}$. Assume that the number of distinct automorphisms in G fixing α is equal to k. Then, $\deg(\alpha) = |G|/k$.*

Proof. Let $\deg(\alpha) = d$ and let $\Omega = \{\alpha_1 = \alpha, \ldots, \alpha_d\}$ be the set of all conjugates of α. Consider the group action of G on Ω. Then, the set of all automorphisms in G that fix α form the stabilizer subgroup G_α. Thus, $|G_\alpha| = k$. Since G is transitive, it is well-known that $[G : G_\alpha] = d$. Therefore, $d = |G|/k$. □

The following lemma will be frequently used in the proof of Theorem 1.

Lemma 5. *Let p be a prime number and let ζ be a primitive p^{th} root of unity; i.e., $\zeta = e^{2\pi i/p}$. Let $\{b_1, \dots, b_n\}$ and $\{c_1, \dots, c_n\}$ be two subsets of $\{0, 1, \dots, p-1\}$. If*

$$\zeta^{b_1} + \ldots + \zeta^{b_n} = \zeta^{c_1} + \ldots + \zeta^{c_n},$$

then $\{b_1, \dots, b_n\} = \{c_1, \dots, c_n\}$.

Proof. The claim follows easily from the fact that if p is a prime number and $\zeta = e^{2\pi i/p}$, then the only linear relation over $\mathbb{Q}$ between the numbers $1, \zeta, \dots, \zeta^{p-1}$ is

$$1 + \zeta + \cdots + \zeta^{p-1} = 0,$$

or a non-zero constant multiplied by the above relation (see the proof of Lemma 4 in [16]). □

The next two lemmas were derived by Drungilas, Dubickas, and Smyth in [10].

Lemma 6 ([10], Proposition 21)**.** *Suppose that α and β are algebraic numbers of degrees m and n over $\mathbb{Q}$, respectively. Let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$ be the distinct conjugates of α and let $\beta_1 = \beta, \beta_2, \dots, \beta_p$ be the distinct conjugates of β. If β is of degree n over $\mathbb{Q}(\alpha)$, then all the numbers $\alpha_i\beta_j$, $1 \le i \le m$, $1 \le j \le n$ are conjugate over $\mathbb{Q}$ (although not necessarily distinct).*

Lemma 7. *Suppose that $\deg(\alpha) = a$, $\deg(\beta) = b$, and $\deg(\alpha\beta) = c$. Then, for any positive integer v, there exist algebraic numbers α' and β' such that $\deg(\alpha') = av$, $\deg(\beta') = b$, and $\deg(\alpha'\beta') = cv$.*

Proof. Recall that a triplet $(a, b, c) \in \mathbb{N}^3$ is called product-feasible if there exist three algebraic numbers α, β, γ of degrees a, b, c over $\mathbb{Q}$, respectively, such that $\alpha\beta\gamma = 1$. By assumption, α and β are algebraic numbers such that $\deg(\alpha) = a$, $\deg(\beta) = b$, and $\deg(\alpha\beta) = c$. Set $\gamma := 1/\alpha\beta$. Note that $\deg(\gamma) = c$ and $\alpha\beta\gamma = 1$, hence the triplet (a, b, c) is product-feasible. It is also trivial to check that the triplet $(v, 1, v)$ is product-feasible for any positive integer v. Moreover, the triplet $(v, 1, v)$ satisfies the exponent triangle inequality with respect to any prime number p (see ([10], Theorem 6)). Therefore, from Theorem 28 in [10], it follows that the triplet $(a \cdot v, b \cdot 1, c \cdot v)$ is also product-feasible. Thus, there exist algebraic numbers α', β', γ' of degrees av, b, cv, respectively, such that $\alpha'\beta'\gamma' = 1$. Since $\deg(\alpha'\beta') = \deg(\gamma')$, the conclusion follows. □

Now we turn our attention to the multiplicative relations between algebraic conjugates. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of a non-zero separable polynomial $f(x) \in \mathbb{Q}[x]$ of degree $n \ge 2$. A multiplicative relation between $\alpha_1, \dots, \alpha_n$ is a relation of the kind

$$\alpha_1^{k_1}\alpha_2^{k_2} \cdots \alpha_n^{k_n} \in \mathbb{Q},$$

where all the $k_i \in \mathbb{Z}$. If $k_1 = k_2 = \ldots = k_n$, the multiplicative relation is called trivial.

Lemma 8 ([9], Theorem 1)**.** *Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial over $\mathbb{Q}$ of prime degree $p > 2$. If there exists a non-trivial multiplicative relation between the roots $\alpha_1, \dots, \alpha_p$ of $f(x)$, then $f(x) = x^p + c$.*

The fact that the analogous statement to Lemma 8 is no longer true for algebraic conjugates of non-prime degrees prevents us from extending the methods used in this paper to algebraic numbers, whose degrees are non-prime.

The proof of the following lemma mimics the proof of Theorem 2′ in [17], which deals with a slightly different relation.

Lemma 9. *Suppose that α is an algebraic number of degree $d \ge 2$ over $\mathbb{Q}$ and let $\alpha' \ne \alpha$ be a conjugate of α. Assume also that $\alpha^r\alpha'^q = 1$, where $r, q \in \mathbb{Z}$. Then, α is a root of unity or $r = \pm q$.*

Proof. Let K denote the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and let σ be an automorphism of K defined by

$$\sigma : K \to K,\ \alpha \mapsto \alpha'. \tag{3}$$

Assume that the order of σ is equal to m, so that

$$\sigma^0(\alpha) = \sigma^m(\alpha) = \alpha. \tag{4}$$

By definition of σ in (3), the equality $\alpha^r \alpha'^q = 1$ can be rewritten as

$$\alpha^r \sigma(\alpha)^q = 1. \tag{5}$$

By applying σ repeatedly on (5) and taking into account that $\sigma(1) = 1$, we derive that

$$(\sigma^{j-1}(\alpha))^r \cdot (\sigma^j(\alpha))^q = 1 \tag{6}$$

for any $j = 1, \ldots, m$. Thus, by raising both sides of (6) to the power of $r^{m-j}(-q)^{j-1}$, we obtain m equalities of the following form

$$(\sigma^{j-1}(\alpha))^{r^{m-j+1}(-q)^{j-1}} \cdot (\sigma^j(\alpha))^{-r^{m-j}(-q)^j} = 1, \tag{7}$$

where $j = 1, \ldots, m$. By multiplying all m equalities in (7) and taking into account (4), we obtain

$$\alpha^{r^m - (-q)^m} = 1. \tag{8}$$

Put $r^m - (-q)^m = t$. If $t \neq 0$, then from (8) it follows that α is a t^{th} root of unity.

However, if $t = 0$, then from $r^m = (-q)^m$ it follows that $r = \pm q$. Whence, the proof is complete. □

The final lemma with minor adjustments is a special case of a theorem proved by Dubickas ([17], Theorem 4′), who generalized an earlier result of Smyth ([18], Lemma 1).

Lemma 10. *Suppose that $\alpha_1, \ldots, \alpha_n$, where $n \geq 3$ are distinct algebraic numbers conjugate over $\mathbb{Q}$. If $q_1, \ldots, q_n \in \mathbb{Z}$ are non-zero numbers such that $|q_1| = |q_2| + \ldots + |q_n|$ and $\alpha_1^{q_1} = \alpha_2^{-q_2} \cdots \alpha_n^{-q_n}$, then $\alpha_2^w \alpha_1^q = 1$ and $\alpha_3^l \alpha_1^s = 1$ with integers $w > 0, l > 0, q$, and s.*

Proof. If α is torsion-free over $\mathbb{Q}$ (α is called torsion-free if none of the ratios α_i/α_j with $1 \leq i \neq j \leq n$ has a root of unity), then the result follows directly by following the proof of Theorem 4′ in [17]. Note, however, that the assumption of α being torsion-free in the proof of [17] was needed only to ensure that there is no restriction of generality by considering the case in which

$$\alpha_1^{q_1} \alpha_2^{q_2} \cdots \alpha_n^{q_n} = 1. \tag{9}$$

Since in our lemma it is assumed that $\alpha_1^{q_1} = \alpha_2^{-q_2} \cdots \alpha_n^{-q_n}$, the equality in (9) holds. Therefore, it is not necessary to require that α be torsion-free. □

3. Proof of Theorem 1

Proof. If $p = 2$, the claim is trivial. Therefore, for the rest of the proof we assume that $p > 2$. First, we treat the case in which $k > 1$; i.e., k denotes a non-unit divisor of $p - 1$. It is well-known that for any such k one can choose $r \in \{2, \ldots, p-1\}$ so that k is the order of r modulo prime p; i.e., k is the least positive integer for which $r^k \equiv 1 \bmod p$. Set

$$a_i := r^0 + r^1 + \ldots + r^{i-1} \mod p, \tag{10}$$

where $i \in \{1, \ldots, k\}$. Since $r \not\equiv 1 \bmod p$, observe that

$$a_i \equiv r^0 + r^1 + \ldots + r^{i-1} \equiv \frac{r^i - 1}{r - 1} \mod p. \tag{11}$$

By the choice of k and r, it immediately follows from (11) that $a_k \equiv 0 \bmod p$. Moreover, since $2 \leq k \leq p-1$ and $r^k - 1 \equiv 0 \bmod p$, we derive that

$$\begin{aligned} a_1 + \ldots + a_{k-1} &\equiv \frac{(r-1) + (r^2-1) + \ldots + (r^{k-1}-1)}{r-1} \\ &\equiv \frac{r + r^2 + \ldots + r^{k-1} + 1}{r-1} - \frac{k \cdot 1}{r-1} \\ &\equiv \frac{r^k - 1}{(r-1)^2} - \frac{k}{r-1} \equiv -\frac{k}{r-1} \not\equiv 0 \mod p. \end{aligned} \tag{12}$$

Finally, note that $a_1, a_2, \ldots, a_{k-1}$ are all distinct mod p. Indeed, for any $1 \leq i < j \leq k-1$, we see that

$$a_j - a_i \equiv \frac{r^j - 1}{r-1} - \frac{r^i - 1}{r-1} \equiv \frac{r^i(r^{j-i} - 1)}{r-1} \not\equiv 0 \mod p, \tag{13}$$

because k is the least positive integer such that $r^k - 1 \equiv 0 \bmod p$ and $0 < j - i < k$.

Let ζ be a primitive p^{th} root of unity. Set

$$\alpha := 1 + \zeta^{a_1} + \zeta^{a_2} + \ldots + \zeta^{a_{k-1}}, \tag{14}$$

where $a_1, \ldots, a_{k-1}$ are defined in (10). Next, we will prove that α as defined in (14) has degree $p-1$.

Proposition 1. *The degree of α over $\mathbb{Q}$ is $p-1$.*

Proof. Suppose, conversely, that $\deg(\alpha) \neq p-1$. It is clear that all the conjugates of α lie in $\mathbb{Q}(\zeta)$. Moreover, the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1$. Thus, $\deg(\alpha) < p-1$, which implies that there exists a non-identity automorphism σ of $\mathbb{Q}(\zeta)$ such that $\sigma(\alpha) = \alpha$. Clearly, $\sigma(\zeta) = \zeta^s$ for some $s \in \{2, \ldots, p-1\}$. Hence,

$$\alpha = 1 + \zeta^{a_1} + \ldots + \zeta^{a_{k-1}} = \sigma(\alpha) = 1 + \zeta^{sa_1} + \ldots + \zeta^{sa_{k-1}}. \tag{15}$$

Since $a_1, \ldots, a_{k-1}$ are all distinct mod p, as are the numbers $sa_1, \ldots, sa_{k-1}$. Thus, Lemma 5 implies that

$$\{a_1, \ldots, a_{k-1}\} = \{sa_1, \ldots, sa_{k-1}\} \mod p.$$

Consequently,

$$(sa_1 + \ldots + sa_{k-1}) - (a_1 + \ldots + a_{k-1}) = (s-1)(a_1 + \ldots + a_{k-1}) \equiv 0 \mod p.$$

Since $s \not\equiv 1 \mod p$, we must have $a_1 + \ldots + a_{k-1} \equiv 0 \mod p$. However, this is a contradiction to (12). Therefore, $\deg(\alpha) = p-1$. □

Let $\beta = \sqrt[p]{2}$ and α be defined as before.

Proposition 2. *The degree of $\alpha\beta$ over $\mathbb{Q}$ is $(p-1)p/k$.*

Proof. It is well-known that the minimal polynomial of β over $\mathbb{Q}$ is $f(x) = x^p - 2$. Further, the splitting field of $f(x)$ is $\mathbb{Q}(\beta, \zeta)$ and $[\mathbb{Q}(\beta, \zeta) : \mathbb{Q}] = p(p-1)$. Since

$$\alpha\beta = (1 + \zeta^{a_1} + \ldots + \zeta^{a_{k-1}})\beta \in \mathbb{Q}(\beta, \zeta), \tag{16}$$

the minimal polynomial of $\alpha\beta$ also splits in $\mathbb{Q}(\beta, \zeta)$. Next, we are going to show that there are exactly k automorphisms of $\mathbb{Q}(\beta, \zeta)$ that fix $\alpha\beta$. Consider the automorphism $\phi \in \mathrm{Gal}(\mathbb{Q}(\zeta, \beta)/\mathbb{Q})$ defined by $\phi(\zeta) = \zeta^r$ and $\phi(\beta) = \beta\zeta$ (recall that $r \in \{2, \ldots, p-1\}$

was chosen so that k be in the order of $r \bmod p$). Then, it is not difficult to show that ϕ is also of order k; i.e., k is the least positive integer such that $\phi^k(\zeta) = \zeta$ and $\phi^k(\beta) = \beta$. Further, from the definition of a_i in (11), we derive that

$$a_i r + 1 \equiv \frac{r(r^i - 1)}{r - 1} + 1 \equiv \frac{r^{i+1} - r}{r - 1} + 1 \equiv \frac{r^{i+1} - 1}{r - 1} \equiv a_{i+1} \mod p. \tag{17}$$

Recall that $a_1 = 1$ and $a_k = 0$, which implies that $\zeta^{a_1} = \zeta^1$ and $\zeta^{a_k} = \zeta^0 = 1$. Hence, as a result of the relation in (17), we have

$$\begin{aligned}\phi(\alpha\beta) &= \phi((1 + \zeta^{a_1} + \ldots + \zeta^{a_{k-1}} + \zeta^{a_{k-1}})\beta) = (1 + \zeta^{a_1 r} + \ldots + \zeta^{a_{k-2} r} + \zeta^{a_{k-1} r})\beta\zeta \\ &= (\zeta^1 + \zeta^{a_1 r + 1} + \ldots + \zeta^{a_{k-2} r + 1} + \zeta^{a_{k-1} r + 1})\beta \\ &= (\zeta^{a_1} + \zeta^{a_2} + \ldots + \zeta^{a_{k-1}} + \zeta^{a_k})\beta = (\zeta^{a_1} + \ldots + \zeta^{a_{k-1}} + 1)\beta = \alpha\beta.\end{aligned}$$

Therefore, all k distinct automorphisms $\phi, \phi^2, \ldots, \phi^k$ fix $\alpha\beta$. We will show that there are no more automorphisms of $\mathbb{Q}(\zeta, \beta)$ that fix $\alpha\beta$.

Assume, conversely, that there exists an automorphism $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta, \beta)/\mathbb{Q})$ such that $\tau(\alpha\beta) = \alpha\beta$ and $\tau \neq \phi^u$ for any $u \in \{1, \ldots, k\}$. Let

$$\tau(\zeta) = \zeta^x \quad \text{and} \quad \tau(\beta) = \beta\zeta^y, \tag{18}$$

where $x \in \{1, \ldots, p-1\}$ and $y \in \{0, \ldots, p-1\}$ (it is well-known that all automorphisms in $\mathrm{Gal}(\mathbb{Q}(\zeta, \beta)/\mathbb{Q})$ are of this form). From $\tau(\alpha\beta) = \alpha\beta$, it follows that

$$\begin{aligned}(\zeta^0 + \zeta^{a_1} + \ldots + \zeta^{a_{k-1}})\beta &= (1 + \zeta^{a_1} + \ldots + \zeta^{a_{k-1}})\beta \\ &= \alpha\beta \\ &= \tau(\alpha\beta) \\ &= (\zeta^y + \zeta^{y + x a_1} + \ldots + \zeta^{y + x a_{k-1}})\beta.\end{aligned} \tag{19}$$

Hence,

$$\zeta^0 + \zeta^{a_1} + \ldots + \zeta^{a_{k-1}} = \zeta^y + \zeta^{y + x a_1} + \ldots + \zeta^{y + x a_{k-1}}. \tag{20}$$

By applying Lemma 5 to the equality in (20), we obtain

$$\{0, a_1, \ldots, a_{k-1}\} = \{y, y + x a_1, \ldots, y + x a_{k-1}\} \mod p. \tag{21}$$

Therefore,

$$\begin{aligned}0 &\equiv (y + (y + x a_1) + \ldots + (y + x a_{k-1})) - (0 + a_1 + \ldots + a_{k-1}) \\ &\equiv ky + (x - 1)(a_1 + \ldots + a_{k-1}) \mod p.\end{aligned} \tag{22}$$

Recall from (12) that $(a_1 + \ldots + a_{k-1}) \not\equiv 0 \mod p$. If $y = 0$, then $x = 1$. In this case, τ is the identity automorphism; i.e., $\tau = \phi^k$, a contradiction. If $y \neq 0$, then from (21) it follows that

$$y = a_j \tag{23}$$

for some $j \in \{1, \ldots, k-1\}$. Substituting (11) and (12) into (22) we obtain

$$0 \equiv k \cdot \frac{r^j - 1}{r - 1} + (x - 1) \cdot \frac{-k}{r - 1} \equiv \frac{k(r^j - x)}{r - 1} \mod p. \tag{24}$$

The equality in (24) implies that

$$x \equiv r^j \mod p. \tag{25}$$

Consider the automorphism ϕ^j. Note that $\phi^j(\zeta) = \zeta^{r^j}$. We also know that $\phi^j(\beta) = \beta\zeta^w$ for some $w \in \{0, \ldots, p-1\}$. Since $\phi^j(\alpha\beta) = \alpha\beta$, by applying the same arguments as in (19), we deduce that

$$\{0, a_1, \ldots, a_{k-1}\} = \{w, w + r^j a_1, \ldots, w + r^j a_{k-1}\} \mod p. \tag{26}$$

Taking into account (11), (12) and (26), we derive that

$$\begin{aligned} 0 &\equiv (w + (w + r^j \cdot a_1) + \ldots + (w + r^j \cdot a_{k-1})) - (0 + a_1 + \ldots + a_{k-1}) \\ &\equiv kw + (r^j - 1)(a_1 + \ldots + a_{k-1}) \\ &\equiv kw + (r^j - 1) \cdot \frac{-k}{r-1} \\ &\equiv kw - ka_j \equiv k(w - a_j) \mod p. \end{aligned} \tag{27}$$

Therefore,

$$w \equiv a_j. \tag{28}$$

As a result of (18), (23), (25) and (28) we obtain

$$\phi^j(\zeta) = \zeta^{r^j} = \zeta^x = \tau(\zeta) \quad \text{and} \quad \phi^j(\beta) = \beta\zeta^w = \beta\zeta^{a_j} = \beta\zeta^y = \tau(\beta).$$

Consequently, $\tau = \phi^j$, a contradiction. Thus, we have proved that there are exactly k automorphisms of $\mathbb{Q}(\zeta, \beta)$ fixing $\alpha\beta$. Finally, by applying Lemma 4 we obtain that

$$\deg(\alpha\beta) = \frac{(p-1)p}{k}.$$

□

As a result of Proposition 1 and Proposition 2, we obtain that there exist α and β such that

$$\deg(\alpha) = m, \quad \deg(\beta) = p, \quad \deg(\alpha\beta) = \frac{(p-1)p}{k},$$

where $k > 1$ can be chosen as any non-unit divisor of $p - 1$.

Finally, we treat separately the case in which $k = 1$; i.e., $(p-1)p/k = (p-1)p$. Let α, γ be arbitrary algebraic numbers of degrees $p - 1$ and p, respectively. Then, it follows easily that the extension $\mathbb{Q}(\alpha, \gamma)$ over $\mathbb{Q}$ has degree $(p-1)p$. Therefore, for all but finitely many rational numbers r we have $\mathbb{Q}(\alpha, \gamma) = \mathbb{Q}(\alpha(r + \gamma))$ (see [10], Proposition 1). Set $\beta := r + \gamma$. Then, we have:

$$\deg(\alpha) = p - 1, \quad \deg(\beta) = p, \quad \deg(\alpha\beta) = (p-1)p,$$

which finalizes the proof of the remaining case $k = 1$. Therefore, the proof of Theorem 1 is complete. □

For an illustration of the construction process described in the proof of Theorem 1, take $p = 11$ and $k = 5$. First, we need to find $r \in \{2, \ldots, 10\}$, which has order 5. It is easy to check that $r = 3$ is one possible choice. Then, we calculate the exponents of ζ mod 11:

$$a_1 \equiv 1, \;\; a_2 = \frac{3^2 - 1}{3 - 1} \equiv 4, \;\; a_3 = \frac{3^3 - 1}{3 - 1} \equiv 2, \;\; a_4 = \frac{3^4 - 1}{3 - 1} \equiv 7.$$

Thus, $\alpha = 1 + \zeta^1 + \zeta^4 + \zeta^2 + \zeta^7$ and $\beta = \sqrt[11]{2}$. It is clear that $\deg(\beta) = 11$ and by calculations with SAGE one can verify that

$$\deg(\alpha) = 11 - 1 = 10 \quad \text{and} \quad \deg(\alpha\beta) = 10 \cdot 11/5 = 22.$$

We recall that examples of this kind cannot be constructed if $k = 1$. In this case, one can simply take $\alpha = \zeta$ and $\beta = \sqrt[p]{2}$, where ζ is a primitive p^{th} root of unity.

4. Proof of Theorem 2

Proof. It is clear that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = p$. Since $p \nmid m$, it easily follows that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = mp$. Let $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = d$. Note that $\mathbb{Q}(\alpha\beta) \subseteq \mathbb{Q}(\alpha, \beta)$. Hence, $d \mid mp$ and therefore,

$$d = \deg(\alpha\beta) = \frac{mp}{k} \tag{29}$$

for some positive integer k.

(**a**) We have that $p > 2$ is a prime number and $f(x) \neq x^p + c$, where $f(x)$ is the minimal polynomial of β over $\mathbb{Q}$. We will show that under these conditions

$$\deg(\alpha\beta) = \deg(\alpha) \cdot \deg(\beta) = mp, \tag{30}$$

which is equivalent to $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = mp$.

Assume, conversely, that $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] \neq mp$. Then, (30) holds for some positive integer $k > 1$. If $m = 1$, then $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = 1 \cdot p$ for any prime p, a contradiction. Thus, for the rest of the proof we assume that $m \geq 2$. The relations between the degrees of α, β and $\alpha\beta$ are illustrated below.

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha) \arrow[dr, dash, "p"] & \\
\mathbb{Q} \arrow[ur, dash, "m"] \arrow[r, dash, "mp/k"] \arrow[dr, dash, "p"'] & \mathbb{Q}(\alpha\beta) \arrow[r, dash, "k"] & \mathbb{Q}(\alpha, \beta) \\
 & \mathbb{Q}(\beta) \arrow[ur, dash, "m"'] &
\end{tikzcd}$$

Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ be all the distinct conjugates of α over $\mathbb{Q}$ and let $\beta_1 = \beta, \beta_2, \ldots, \beta_p$ be all the distinct conjugates of β over $\mathbb{Q}$. Consider the following list of mp numbers $\alpha_i\beta_j$ with $i \in \{1, \ldots, m\}$ and $j \in \{1, \ldots, p\}$:

$$\alpha_1\beta_1, \ldots, \alpha_1\beta_p, \alpha_2\beta_1, \ldots, \alpha_2\beta_p, \ldots, \alpha_m\beta_1, \ldots, \alpha_m\beta_p. \tag{31}$$

Lemma 6 implies that all numbers in (31) are conjugates (not necessarily distinct) of $\alpha\beta$. Since the degree of $\alpha\beta$ is mp/k, it can be easily deduced that each distinct conjugate of $\alpha\beta$ appears exactly k times among the numbers listed in (31). Let

$$\mathcal{A}_i = \{\alpha_i\beta_1, \ldots, \alpha_i\beta_p\}, \quad i \in \{1, \ldots, m\}. \tag{32}$$

Clearly, $|\mathcal{A}_i| = p$ for all $i \in \{1, \ldots, m\}$, because all p elements in the set $\mathcal{A}_i$ are distinct. Since $k \geq 2$, there exists an index $i^* \in \{2, \ldots, m\}$ such that $\mathcal{A}_1 \cap \mathcal{A}_{i^*} \neq \emptyset$. Without the restriction of generality, we may assume that $i^* = 2$ and that

$$\alpha_1\beta_1 = \alpha_2\beta_2. \tag{33}$$

Let L denote the Galois closure of $\mathbb{Q}(\alpha_1, \beta_1)$ over $\mathbb{Q}$ and let $G := \mathrm{Gal}(L/\mathbb{Q})$ denote the Galois group of $L/\mathbb{Q}$. Since β_1 is of degree p over $\mathbb{Q}(\alpha_1)$ and the extension $L/\mathbb{Q}(\alpha_1)$ is Galois, Cauchy's theorem implies that there exists an automorphism σ of order p in G, which fixes α_1 and acts as a p-cycle on the conjugates of β_1. Hence, $\sigma(\alpha_1) = \alpha_1$ and $\sigma^p(\beta_j) = \beta_j$ for any $j \in \{1, \ldots, p\}$. By applying σ^p to equality in (33) we obtain $\alpha_1\beta_1 = \sigma^p(\alpha_2) \cdot \beta_2$. Therefore, $\alpha_2\beta_2 = \sigma^p(\alpha_2)\beta_2$ and thus, $\sigma^p(\alpha_2) = \alpha_2$.

Let r be the least positive integer for which $\sigma^r(\alpha_2) = \alpha_2$. Then, $r = 1$ or $r = p$. We will treat both cases separately.

Case I. First, consider the case $r = 1$. By multiplying all equalities $\sigma^u(\alpha_1\beta_1) = \sigma^u(\alpha_2\beta_2)$, where $u = 1, \dots, p$, we obtain

$$\alpha_1^p \cdot \prod_{j=1}^{p} \beta_j = \alpha_2^p \cdot \prod_{j=1}^{p} \beta_j.$$

Since $\prod_{j=1}^{p} \beta_j \neq 0$, it follows that $\alpha_1^p = \alpha_2^p$. By raising both sides of the equality in (33) to the p^{th} power, we obtain $\alpha_1^p\beta_1^p = \alpha_2^p\beta_2^p$ and therefore, $\beta_1^p = \beta_2^p$. This constitutes a non-trivial multiplicative relation between the conjugates of β_1. Thus, Lemma 8 implies that the minimal polynomial of β_1 is $f(x) = x^p + c$, a contradiction.

Case II. Now we consider the case $r = p$. Let K denote the Galois closure of $\mathbb{Q}(\alpha_1)$ over $\mathbb{Q}$ and let $\overline{\sigma}$ denote the restriction of σ to K. From the properties of σ, it follows that $\overline{\sigma}$ acts as a product of p-cycles on the conjugates of α_1. It is also clear that $\overline{\sigma}(\alpha_1) = \alpha_1$ and $\overline{\sigma}(\alpha_2) \neq \alpha_2$. Without loss of generality, assume that $\overline{\sigma}$ represented as a permutation of the conjugates of α_1 contains the following p-cycle: $(\alpha_2, \dots, \alpha_{p+1})$. Clearly, this is possible only if the degree of α is at least $p + 1$; i.e., $m \geq p + 1$. By multiplying all equalities $\sigma^u(\alpha_1\beta_1) = \sigma^u(\alpha_2\beta_2)$, where $u = 1, \dots, p$, we obtain

$$\alpha_1^p \cdot \prod_{j=1}^{p} \beta_j = \alpha_2\alpha_3 \cdots \alpha_{p+1} \cdot \prod_{j=1}^{p} \beta_j.$$

Since $\prod_{j=1}^{p} \beta_j \neq 0$, it follows that

$$\alpha_1^p = \alpha_2\alpha_3 \cdots \alpha_{p+1}. \tag{34}$$

Since $p > 2$, by applying Lemma 10 to (34) we deduce that

$$\alpha_2^w\alpha_1^q = 1 \quad \text{and} \quad \alpha_3^l\alpha_1^s = 1 \tag{35}$$

for some integers $w > 0, l > 0, q$, and s. We will show that (35) implies a non-trivial multiplicative relation among the conjugates of β_1, which, by applying Lemma 8, forces the minimal polynomial of β_1 to be $f(x) = x^p + c$, a contradiction. Throughout, we will implicitly use the fact that $\sigma(\beta_j)$ is also a conjugate of β for any $j \in \{1, \dots, p\}$.

With respect to the equalities in (35), Lemma 9 implies that either α_1 is a root of unity or $q = \pm w$ and $s = \pm l$. If α_1 is a root of unity, then for some positive integer t we have $\alpha_1^t = \alpha_2^t$. Then, analogous to Case I, we deduce that $\beta_1^t = \beta_2^t$. Suppose now instead that α_1 is not a root of unity. Then, $q = \pm w$ and $s = \pm l$. If $q = -w$, then $\alpha_1^w = \alpha_2^w$, which implies that $\beta_1^w = \beta_2^w$. If $w = q$ and $s = -l$, then $\alpha_1^l = \alpha_3^l$. By applying σ to the equality in (33) we obtain $\alpha_1 \cdot \sigma(\beta_1) = \alpha_3 \cdot \sigma(\beta_2)$. Thus, $\alpha_1^l \cdot (\sigma(\beta_1))^l = \alpha_3^l \cdot (\sigma(\beta_2))^l$ and consequently

$$(\sigma(\beta_1))^l = (\sigma(\beta_2))^l. \tag{36}$$

Since $\sigma(\beta_1) \neq \sigma(\beta_2)$, the equality in (36) constitutes a non-trivial multiplicative relation between the conjugates of β_1. Finally, if $q = w$ and $s = l$, then from equalities $(\alpha_1^w\alpha_2^w)^l = 1$ and $(\alpha_1^l\alpha_3^l)^w = 1$, it follows that $\alpha_2^{lw} = \alpha_3^{lw}$. We also know that

$$\alpha_1\beta_1 = \alpha_2\beta_2 \quad \text{and} \quad \sigma(\alpha_1\beta_1) = \sigma(\alpha_2\beta_2). \tag{37}$$

We have $\sigma(\alpha_1) = \alpha_1$ and $\sigma(\alpha_2) = \alpha_3$; thus, by multiplying both equalities in (37) and raising to the suitable power we obtain

$$\alpha_1^{lw}\beta_1^{lw}\alpha_3^{lw} \cdot (\sigma(\beta_2))^{lw} = \alpha_2^{lw}\beta_2^{lw}\alpha_1^{lw} \cdot (\sigma(\beta_1))^{lw}.$$

Hence,

$$\beta_1^{lw} \cdot (\sigma(\beta_2))^{lw} = \beta_2^{lw} \cdot (\sigma(\beta_1))^{lw}. \tag{38}$$

Because $\sigma(\beta_1) \neq \beta_1$, the equality in (38) constitutes a non-trivial multiplicative relation between the conjugates of β_1.

Analysis of *Case I* and *Case II* demonstrates that the assumption of $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] \neq mp$ leads to a contradiction. Therefore, $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = mp$; i.e., $\deg(\alpha\beta) = mp$, as claimed.

(**b**) We have that $p = 2$ and $f(x) \neq x^2 + cx + c^2$, where $f(x)$ is the minimal polynomial of β over $\mathbb{Q}$. We will show that under these conditions $\deg(\alpha\beta) = 2m$, which is equivalent to $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = 2m$. Assume, conversely, that $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] \neq 2m$. From (29) it follows then that

$$d = [\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = 2m/k, \tag{39}$$

for some positive integer $k > 1$. Analogous to part (a) of the proof, we deduce that $m \geq 2$ and that all $2m$ numbers

$$\alpha_1\beta_1, \ldots, \alpha_m\beta_1, \alpha_1\beta_2, \ldots, \alpha_m\beta_2$$

are conjugates of $\alpha\beta$. Moreover, all m numbers

$$\alpha_1\beta_j, \ldots, \alpha_m\beta_j \tag{40}$$

are distinct for $j = 1, 2$. Hence, $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = d \geq m$, which, together with (39), forces $d = m$. Therefore, all numbers in (40) for a fixed j correspond to the full set of conjugates of $\alpha\beta$. By comparing the products of all such numbers with $j = 1$ and $j = 2$ we derive that

$$\prod_{i=1}^{m} \alpha_i \cdot \beta_1^m = \prod_{i=1}^{m} \alpha_i \cdot \beta_2^m.$$

From $\prod_{i=1}^{m} \alpha_i \neq 0$ it follows that $\beta_1^m = \beta_2^m$. Hence, $\beta_2 = \beta_1\omega$, where ω is an m^{th} root of unity. It is well-known that ω is also a primitive n^{th} root of unity for some $n \mid m$ and that $\deg(\omega) = \phi(n)$, where $\phi(n)$ denotes Euler's totient function. Since $2 \nmid m$; i.e., m is odd, n must also be odd. Further, β_1 is quadratic over $\mathbb{Q}$, hence the splitting field of $f(x)$ is $\mathbb{Q}(\beta_1)$. Consequently, $\beta_2/\beta_1 = \omega \in \mathbb{Q}(\beta)$ and therefore, $\mathbb{Q}(\omega) \subseteq \mathbb{Q}(\beta)$. Since $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$, we deduce that

$$\deg(\omega) = \phi(n) = 1 \quad \text{or} \quad \deg(\omega) = \phi(n) = 2. \tag{41}$$

From (41), it easily follows that $n \in \{1, 2, 3, 4, 6\}$. However, n is odd, whence $n = 1$ or $n = 3$. If $n = 1$, then $\omega = 1$ and $\beta_1 = \beta_2$, a contradiction. If $n = 3$, then ω is a 3^{rd} root of unity. Thus, $\omega^3 = 1, 1 + \omega + \omega^2 = 0$, and $3 \mid m$. From Vieta's formulas we obtain $\beta_1^2\omega \in \mathbb{Q}$ and $\beta_1(1 + \omega) \in \mathbb{Q}$. Thus, $\beta_1(1 + \omega) = -\beta_1\omega^2 \in \mathbb{Q}$ and $(\beta_1^2\omega)(\beta_1\omega^2) = \beta_1^3 \in \mathbb{Q}$. Set $q := \beta_1^3$. Then, β_1 is a root of $h(x) = x^3 - q$. It is clear that $h(x) = x^3 - q$ is reducible if and only if $q = c^3$ for some $c \in \mathbb{Q}$. Hence, $h(x) = x^3 - c^3$ and the minimal polynomial of β_1 is $f(x) = x^2 + cx + c^2$, a contradiction. □

5. Proofs of Theorem 3 and Corollary 1

Proof of Theorem 3. We continue to use the same notation as in the proof of Theorem 2.

(**a**) We have that $p > 2$ is a prime number and $p - 1 \nmid m$. We will show that under these conditions

$$\deg(\alpha\beta) = \deg(\alpha) \cdot \deg(\beta) = mp,$$

which is equivalent to $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = mp$.

Assume, conversely, that $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] \neq mp$. Thus, $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = mp/k$ for some positive integer $k > 1$. Let $f(x)$ be the minimal polynomial of β over $\mathbb{Q}$. If $f(x) \neq x^p + c$, then Theorem 2 implies that $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = mp$, a contradiction. Thus, for the rest of the proof we assume that $f(x) = x^p + c$. Consider the sets $\mathcal{A}_i$, which were defined in (32). By the same arguments as in the proof of Theorem 2, we deduce that there exists an index

$i^* \in \{2, \dots, m\}$ such that $\mathcal{A}_1 \cap \mathcal{A}_{i^*} \neq \emptyset$. Without loss of generality, we may suppose that $\alpha_1\beta_1 = \alpha_2\beta_2$. Since the minimal polynomial of β_1 is $f(x) = x^p + c$, we have

$$\frac{\alpha_2}{\alpha_1} = \frac{\beta_1}{\beta_2} = \zeta, \tag{42}$$

where ζ denotes a primitive p^{th} root of unity. Hence, $\alpha_2 = \alpha_1\zeta$ and therefore,

$$\alpha_1(\beta_j\zeta) = \alpha_2\beta_j$$

for any $j \in \{1, \dots, p\}$. Observe that the sets $\{\beta_1, \dots, \beta_p\}$ and $\{\beta_1\zeta, \dots, \beta_p\zeta\}$ coincide, as they both represent all p roots of $f(x)$. Therefore, $|\mathcal{A}_1 \cap \mathcal{A}_2| = p$ and thus $\mathcal{A}_1 = \mathcal{A}_2$. It is also clear that $\alpha_1^p = \alpha_2^p$. Since $i^* = 2$ was chosen arbitrarily, we conclude that if $\mathcal{A}_1 \cap \mathcal{A}_i \neq \emptyset$, then $\mathcal{A}_1 = \mathcal{A}_i$ and $\alpha_1^p = \alpha_i^p$. Recall that $\alpha_1\beta_1$ appears exactly k times among the numbers listed in (31) and that for each $i \in \{1, \dots, m\}$, all p conjugates of $\alpha_1\beta_1$ belonging to $\mathcal{A}_i$ are distinct. Thus,

$$k \leq m. \tag{43}$$

From the last arguments it also follows that there are exactly k indices in the set $\{1, \dots, m\}$, say, $1, 2, \dots, k$ such that

$$\mathcal{A}_1 = \mathcal{A}_2 = \ldots = \mathcal{A}_k \quad \text{and} \quad \alpha_1^p = \alpha_2^p = \ldots = \alpha_k^p. \tag{44}$$

From (44) it is clear that for each $i \in \{2, \dots, k\}$ we have

$$\alpha_i = \alpha_1\zeta^{w_i}, \tag{45}$$

where $w_i \in \{\in 1, \dots, p-1\}$. Since all conjugates of α_1 are distinct, from (44) it also follows that

$$k \leq p. \tag{46}$$

Moreover, if $k < m$, then for any $i \in \{1, \dots, m\} \setminus \{1, \dots, k\}$ we obtain

$$\mathcal{A}_1 \cap \mathcal{A}_i = \emptyset \quad \text{and} \quad \alpha_1^p \neq \alpha_i^p, \tag{47}$$

as otherwise we would obtain a contradiction to the relations derived in (44). Recall that K denotes the Galois closure of $\mathbb{Q}(\alpha_1)$ over $\mathbb{Q}$. Let $G' := \mathrm{Gal}(K/\mathbb{Q})$ and let $\Omega = \{\alpha_1, \dots, \alpha_m\}$. Thus, G' acts transitively on Ω. Put

$$\mathcal{B} = \{\alpha_1, \dots, \alpha_k\}. \tag{48}$$

As a consequence of the relations in (44) and (47), it follows that for any automorphism $\lambda \in G'$ we have

$$\lambda(\mathcal{B}) = \mathcal{B} \quad \text{or} \quad \lambda(\mathcal{B}) \cap \mathcal{B} = \emptyset. \tag{49}$$

Therefore, the set $\Gamma = \{\lambda(\mathcal{B}) : \lambda \in G'\}$ constitutes a system of blocks for G' and also forms a partition of Ω. Since $|\mathcal{B}| = k$ and $|\Omega| = m$, we deduce that $k \mid m$. Since it was assumed that $p \nmid m$, we obtain that $p \nmid k$. In view of (46), the last statement implies that

$$k < p. \tag{50}$$

Next, we prove the lemma, which will allow us to finalize the proof of part (a) and will also be essential in the proof of part (b).

Lemma 11. *Let $p > 2$ be a prime number and let m be a positive integer such that $p \nmid m$. Suppose that α, β are algebraic numbers such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = p$. Finally, let ζ be a primitive p^{th} root of unity. If $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] \neq mp$, then $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\alpha)$.*

Proof. Let s be the degree of ζ over $\mathbb{Q}(\alpha_1)$. If $s = 1$, then there is nothing to prove. Suppose that $s > 1$. Then there exists an automorphism τ of K that fixes the subfield $\mathbb{Q}(\alpha_1)$ and sends ζ to ζ^u for some $u \in \{2, \ldots, p-1\}$. Since $\tau(\alpha_1) = \alpha_1$, from (48) and (49) it follows that $\tau(\mathcal{B}) = \mathcal{B}$. In view of (44) and (45), we must have that

$$\begin{aligned} \mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_k\} &= \{\alpha_1, \alpha_1\zeta^{w_2}, \ldots, \alpha_1\zeta^{w_k}\} \\ = \tau(\mathcal{B}) &= \{\alpha_1, \alpha_1\zeta^{uw_2}, \ldots, \alpha_1\zeta^{uw_k}\}, \end{aligned} \tag{51}$$

where $1 \le w_i \ne w_j \le p-1$ and $2 \le i \ne j \le k$. Therefore,

$$\{w_2, \ldots, w_k\} = \{uw_2, \ldots, uw_k\} \mod p. \tag{52}$$

The sum of all elements in both sets of (52) is the same mod p, hence

$$(u-1)(w_2 + \ldots + w_k) \equiv 0 \mod p. \tag{53}$$

Since $u \ne 1$ it follows that

$$(w_2 + \ldots + w_k) \equiv 0 \mod p. \tag{54}$$

If $k < m$, then there exists a conjugate of α, say α_{k+1}, which does not belong to block $\mathcal{B}$. Thus, we can choose an automorphism ϕ of K, which sends α_1 to α_{k+1}. Clearly, $\phi(\zeta) = \zeta^l$ for some positive integer l. Then

$$\phi(\mathcal{B}) = \{\alpha_{k+1}, \alpha_{k+1}\zeta^{lw_2}, \ldots, \alpha_{k+1}\zeta^{lw_k}\}. \tag{55}$$

As a result of (54) we have that

$$lw_2 + \ldots + lw_k = l(w_2 + \ldots + w_k) \equiv 0 \mod p. \tag{56}$$

Observe that $\phi(\alpha_2) = \phi(\alpha_1\zeta^{w_2}) = \alpha_{k+1}\zeta^{lw_2}$ is also a conjugate of α_1. Hence, there exists an automorphism ψ of K, which sends α_1 to $\alpha_{k+1}\zeta^{lw_2}$. Clearly, $\psi(\zeta) = \zeta^r$ for some positive integer r. Then

$$\begin{aligned} \psi(\mathcal{B}) &= \{\alpha_{k+1}\zeta^{lw_2}, \alpha_{k+1}\zeta^{lw_2}\zeta^{rw_2}, \ldots, \alpha_{k+1}\zeta^{lw_2}\zeta^{rw_k}\} \\ &= \{\alpha_{k+1}\zeta^{lw_2}, \alpha_{k+1}\zeta^{lw_2+rw_2}, \ldots, \alpha_{k+1}\zeta^{lw_2+rw_k}\}. \end{aligned} \tag{57}$$

Since $\phi(\mathcal{B}) = \psi(\mathcal{B})$, we must have

$$\begin{aligned} 0 \equiv l(w_2 + \ldots + w_k) &\equiv lw_2 + (lw_2 + rw_2) + \ldots + (lw_2 + rw_k) \\ &\equiv klw_2 + r(w_2 + \ldots + w_k) \\ &\equiv klw_2 \mod p, \end{aligned} \tag{58}$$

a contradiction, since neither of k, l, w_2 can be congruent to 0 mod p. Therefore, if $k < m$, then the degree of ζ over $\mathbb{Q}(\alpha)$ must be equal to 1; i.e., $Q(\zeta) \subseteq \mathbb{Q}(\alpha)$.

However, if $k \ge m$, then we must have $m = k$ due to (43). In this case

$$\alpha_1 \cdots \alpha_k = \alpha_1 \cdot \alpha_1\zeta^{w_2} \cdots \alpha_1\zeta^{w_k} \in \mathbb{Q}. \tag{59}$$

From (54) being applied to (59) we obtain that

$$\alpha_1^k \in \mathbb{Q}. \tag{60}$$

Thus, $x^k - \alpha_1^k$ is the minimal polynomial of α_1 over $\mathbb{Q}$. However, it follows then that

$$\alpha_1^k = \alpha_2^k = (\alpha_1\zeta^{w_2})^k = \alpha_1^k\zeta^{kw_2}, \tag{61}$$

which implies that $kw_2 \equiv 0 \bmod p$, a contradiction. Therefore, we conclude that the degree of ζ over $\mathbb{Q}(\alpha)$ must be equal to 1; i.e., $Q(\zeta) \subseteq \mathbb{Q}(\alpha)$. $\square$

To finish the proof of part (a) it is enough to observe that if $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] \neq mp$, then Lemma 11 implies that $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\alpha)$. Thus, from the tower law it follows that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ divides $[\mathbb{Q}(\alpha) : \mathbb{Q}] = m$, a contradiction. Therefore, $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = mp$, which implies that $\deg(\alpha\beta) = \deg(\alpha) \cdot \deg(\beta) = mp$. The proof is complete.

(**b**) First, we prove the conditional part of the statement; namely, that $\deg(\alpha\beta) = mp/k$, where k is a divisor of $p - 1$. If $k = 1$, there is nothing to prove. Thus, for the rest of the proof we assume that $k > 1$; i.e., $\deg(\alpha\beta) = mp/k \neq mp$, which is equivalent to $[\mathbb{Q}(\alpha\beta) : \mathbb{Q}] \neq mp$. Lemma 11 implies that $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(\alpha)$ and thus, $p - 1 \mid m$. Let

$$m = (p-1)t, \tag{62}$$

where t is some positive integer. From the tower law it follows that

$$[\mathbb{Q}(\alpha,\zeta) : \mathbb{Q}(\zeta)] = \frac{[\mathbb{Q}(\alpha,\zeta) : \mathbb{Q}]}{[\mathbb{Q}(\zeta) : \mathbb{Q}]} = \frac{t(p-1)}{(p-1)} = t; \tag{63}$$

i.e., α is of degree t over $\mathbb{Q}(\zeta)$.

Consider the group action of G' on Ω. For any subgroup H' of G', let $\alpha^{H'}$ denote the orbit of α under H'; i.e., $\alpha^{H'} = \{\mu(\alpha) \; : \; \mu \in H'\}$. Consider the subgroup $H := \mathrm{Gal}(K : \mathbb{Q}(\zeta))$ of G' corresponding to the fixed subfield $\mathbb{Q}(\zeta)$ of K. From (63) we deduce that $|\alpha^H| = t$. Moreover, as $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a normal extension, H is a normal subgroup of G'. Hence, Lemma 1 implies that all orbits of H have equal cardinality; namely,

$$|\alpha_i^H| = t \;\text{ for all }\; i \in \{1, \dots, m\}. \tag{64}$$

It follows that in total H has $m/t = p - 1$ orbits. Next, we will show that if

$$(\alpha_i)^p = (\alpha_j)^p \tag{65}$$

for some two distinct conjugates of α_1, then α_i and α_j lie in two different orbits under H.

Assume, conversely, that α_i and α_j lie in the same orbit under H. Then, there exists an automorphism $\mu \in H$ such that $\mu(\alpha_j) = \alpha_i$ and $\mu(\zeta) = \zeta$. It is also clear that $\alpha_i = \alpha_j\zeta^w$ for some $w \in \{1, \dots, p-1\}$. Thus

$$\begin{aligned} \mu(\alpha_i) &= \mu(\alpha_j\zeta^w) = \alpha_i\zeta^w \\ \mu^2(\alpha_i) &= \mu(\alpha_i\zeta^w) = \mu(\alpha_j\zeta^{2w}) = \alpha_i\zeta^{2w} \\ &\vdots \\ \mu^{p-1}(\alpha_i) &= \mu(\alpha_i\zeta^{(p-2)w}) = \mu(\alpha_j\zeta^{(p-1)w}) = \alpha_i\zeta^{(p-1)w} \\ \mu^p(\alpha_i) &= \mu(\alpha_i\zeta^{(p-1)w}) = \mu(\alpha_j\zeta^{pw}) = \alpha_i. \end{aligned} \tag{66}$$

From the equalities in (66), we see that $\mu(\alpha_i), \dots, \mu^{p-1}(\alpha_i), \alpha_i$ correspond to p distinct conjugates of α_1 satisfying

$$(\mu(\alpha_i))^p = \ldots = (\mu^{p-1}(\alpha_i))^p = \alpha_i^p. \tag{67}$$

By choosing any automorphism in G', which maps α_i to α_1, and applying it to the equalities in (67), we obtain p distinct conjugates, whose p^{th} powers are equal to α_1^p. In view of (44) and (47), the total number of such conjugates is equal to k, hence $p \leq k$. However, this is a contradiction to (50), where we have proved that $k < p$. Therefore, if $(\alpha_i)^p = (\alpha_j)^p, i \neq j$, then α_i and α_j lie in two different orbits under H.

Recall that $\Gamma = \{\lambda(\mathcal{B}) : \lambda \in G'\}$ forms a system of blocks for G', where $\mathcal{B}$ was defined in (48). Consider the group action of G' on Γ. We claim that $|\mathcal{B}^H| = t$. Indeed, since $\alpha_1 \in \mathcal{B}$, we obtain that $|\mathcal{B}^H| \leq t$ due to (64). If $|\mathcal{B}^H| < t$, then we can find two automorphisms $\mu', \mu'' \in H$ such that

$$\mu'(\alpha_1) \neq \mu''(\alpha_1) \text{ and } \mu'(\mathcal{B}) = \mu''(\mathcal{B}). \tag{68}$$

Suppose that $\mu'(\alpha_1) = \alpha'$ and $\mu''(\alpha_1) = \alpha''$, where $\alpha' \neq \alpha''$. Let $\mu'^{-1}(\alpha'') = \alpha_i$, where μ'^{-1} is the inverse of μ'. Clearly, $i \neq 1$. By applying μ'^{-1} to the equalities in (68), we deduce that $\alpha_1, \alpha_i \in \mathcal{B}$. Thus, $i \in \{1, \ldots, k\}$ and in view of (44) this implies that $\alpha_1^p = \alpha_i^p$. Consequently, $\mu'(\alpha_1^p) = \mu'(\alpha_i^p)$ and hence, $(\alpha')^p = (\alpha'')^p$. Therefore, from the arguments following (65), we deduce that α' and α'' belong to different orbits under H. However, $\mu''\mu'^{-1}(\alpha') = \mu''(\alpha_1) = \alpha''$. Since $\mu''\mu'^{-1} \in H$, it follows that α' and α'' belong to the same orbit under H, a contradiction. Hence, $|\mathcal{B}^H| = t$ and since H is normal in G', we conclude that each orbit of H has cardinality equal to t. Recalling from (62) that $m = (p-1)t$, and using the fact that $|\Gamma| = m/k$, we deduce that the total number of orbits in H is equal to

$$\frac{m/k}{t} = \frac{(p-1)t/k}{t} = \frac{p-1}{k}.$$

Thus, $k \mid p-1$, as claimed.

To prove the existence part of the statement, recall from Theorem 1 that for any divisor k of $p-1$ there exist algebraic numbers α' and β' such that $\deg(\alpha') = p-1$, $\deg(\beta') = p$, and $\deg(\alpha'\beta') = (p-1)p/k$. Then, Lemma 7 implies that for any positive integer v there exist algebraic numbers α and β such that $\deg(\alpha) = v(p-1)$, $\deg(\beta) = p$, and $\deg(\alpha\beta) = v(p-1)p/k$. Set $v := m/(p-1)$ and the proof is complete.

(**c**) From the proof of part (b) of Theorem 2, we know that if $\deg(\alpha\beta) \neq 2m$, then $3 \mid m$. Hence, if $3 \nmid m$, then we must have $\deg(\alpha\beta) = 2m$.

(**d**) In the proof of part (b) of Theorem 2, we have already deduced that $\deg(\alpha\beta) = vm$, where $v \in \{1, 2\}$. It remains to show that both values of v are attainable. By Theorem 2, if the minimal polynomial of β over $\mathbb{Q}$ is not of the form $f(x) = x^2 + cx + c^2$, then $\deg(\alpha\beta) = 2m$. However, take $c = 1$ in the expression of $f(x)$. Then the roots of $f(x)$ are ω and ω^2, where ω is a primitive 3^{rd} root of unity. Set $\beta := \omega$ and $\alpha := \sqrt[m]{2}$. Consider the polynomial $h(x) = x^m - 2$. It is well-known that $h(x)$ is irreducible over $\mathbb{Q}$. Since $3 \mid m$, $\alpha\beta$ is also a root of $h(x)$. Therefore,

$$\deg(\alpha) = m, \deg(\beta) = 2 \text{ and } \deg(\alpha\beta) = m.$$

This completes the proof. □

Proof of Corollary 1. From the arguments in the proof of Lemma 7, it follows that the triplet (a, p, c) is product-feasible if and only if there exist algebraic numbers α and β such that $\deg(\alpha) = a$, $\deg(\beta) = p$, and $\deg(\alpha\beta) = c$. Hence, the proof follows directly from Theorem 3, by setting $a := m$ and $c := \deg(\alpha\beta)$ □

Proof of Corollary 2. Since $a < 7$, it is clear that $7 \nmid a$. If $a \in \{1, 2, 3, 4, 5\}$, then part (a) of Corollary 1 implies that the triplet $(a, 13, c)$ is product-feasible if and only if $c = 7a$. If $a = 6$, then part (b) of Corollary 1 implies that the triplet $(6, 13, c)$ is product-feasible if and only if $c = 6 \cdot 7/k$, where k is a divisor of $7 - 1 = 6$. Hence, $k \in \{1, 2, 3, 6\}$. Since $k = 1$ corresponds to $c = 6 \cdot 7$, we conclude that the triplet $(a, 7, c)$, where $a < 7$, is product-feasible if and only if $c = 7a$ or $a = 6$ and $c = 6 \cdot 7/k$ with $k \in \{2, 3, 6\}$.

Note that Corollary 1 cannot be applied in the search for product-feasible triplets $(a, 7, c)$ if $a = 7$, because in that case $7 \mid a$. However, all triplets of the form $(7, 7, c)$ can be determined using the results in [19]. □

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study.

Acknowledgments: The author thanks A. Dubickas for making many helpful suggestions. The author is also grateful to the reviewers for their constructive comments.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Dubickas, A. Two exercises concerning the degree of the product of algebraic numbers. *Publ. Inst. Math.* **2005**, *77*, 67–70. [CrossRef]
2. Nagell, T. Bemerkungen über zusammengesetzte Zahlkörper. *Avh. Norske Vid. Akad. Oslo* **1937**, *4*, 1–26.
3. Kaplansky, I. *Fields and Rings*; The University of Chicago Press: Chicago, IL, USA, 1969.
4. Isaacs, I.M. Degrees of sums in a separable field extension. *Proc. Am. Math. Soc.* **1970**, *25*, 638–641. [CrossRef]
5. Browkin, J.; Diviš, B.; Schinzel, A. Addition of sequences in general fields. *Monatsh. Math.* **1976**, *82*, 261–268. [CrossRef]
6. Cagliero, L.; Szechtman, F. On the theorem of the primitive element with applications to the representation theory of associative and Lie algebras. *Canad. Math. Bull.* **2014**, *10*, 735–748. [CrossRef]
7. Weintraub, S.H. Observations on primitive, normal, and subnormal elements of field extensions. *Monatsh. Math.* **2011**, *162*, 239–244. [CrossRef]
8. Dubickas, A.; Jankauskas, J. Simple linear relations between conjugate algebraic numbers of low degree. *J. Ramanujan Math. Soc.* **2015**, *30*, 219–235.
9. Drmota, M.; Skałba, M. On multiplicative and linear independence of polynomial roots. *Contrib. Gen. Algebra* **1991**, *7*, 127–135.
10. Drungilas, P.; Dubickas, A.; Smyth, C.J. A degree problem for two algebraic numbers and their sum. *Publ. Mat.* **2012**, *56*, 413–448. [CrossRef]
11. Drungilas, P.; Dubickas, A.; Luca, F. On the degree of compositum of two number fields. *Math. Nachr.* **2013**, *10*, 171–180. [CrossRef]
12. Drungilas, P.; Dubickas, A. On degrees of three algebraic numbers with zero sum or unit product. *Colloq. Math.* **2016**, *143*, 159–167. [CrossRef]
13. Drungilas, P.; Maciulevičius, L. A degree problem for the compositum of two number fields. *Lith. Math. J.* **2019**, *59*, 39–47. [CrossRef]
14. Dummit, D.S.; Foote, R.M. *Abstract Algebra*; Prentice Hall: Englewood Cliffs, NJ, USA, 1991.
15. Dixon, J.D.; Mortimer, B. *Permutation Groups*; Graduate Texts in Mathematics, 163; Springer: New York, NY, USA, 1996.
16. Dubickas, A. On sums of two and three roots of unity. *J. Number Theory* **2018**, *192*, 65–79. [CrossRef]
17. Dubickas, A. On the degree of a linear form in conjugates of an algebraic number. *Illinois J. Math.* **2002**, *46*, 571–585. [CrossRef]
18. Smyth, C.J. Conjugate algebraic numbers on conics. *Acta. Arith.* **1982**, *40*, 333–346. [CrossRef]
19. Virbalas, P. Compositum of two number fields of prime degree. *N. Y. J. Math.* **2023**, *29*, 171–192.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.