View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Diposit Digital de Documents de la UAB

Publ. Mat. **56** (2012), 413–448
DOI: 10.5565/PUBLMAT_56212_07

A DEGREE PROBLEM FOR TWO ALGEBRAIC NUMBERS AND THEIR SUM

Paulius Drungilas, Artūras Dubickas, and Chris Smyth

Abstract: For all but one positive integer triplet (a,b,c) with $a \leqslant b \leqslant c$ and $b \leqslant 6$, we decide whether there are algebraic numbers α, β and γ of degrees a, b and c, respectively, such that $\alpha+\beta+\gamma=0$. The undecided case $(6,6,8)$ will be included in another paper. These results imply, for example, that the sum of two algebraic numbers of degree 6 can be of degree 15 but cannot be of degree 10. We also show that if a positive integer triplet (a,b,c) satisfies a certain triangle-like inequality with respect to every prime number then there exist algebraic numbers α, β, γ of degrees a, b, c such that $\alpha+\beta+\gamma=0$. We also solve a similar problem for all (a,b,c) with $a \leqslant b \leqslant c$ and $b \leqslant 6$ by finding for which a, b, c there exist number fields of degrees a and b such that their compositum has degree c. Further, we have some results on the multiplicative version of the first problem, asking for which triplets (a,b,c) there are algebraic numbers α, β and γ of degrees a, b and c, respectively, such that $\alpha\beta\gamma=1$.

2010 Mathematics Subject Classification: 11R04, 11R32.

Key words: algebraic number, sum-feasible, *abc* degree problem.

1. Introduction and results

The purpose of this paper is to propose the following problem:

Find all possible triplets $(a,b,c) \in \mathbb{N}^3$ *for which there exist three algebraic numbers* α, β, γ, *with degrees* a, b, c *(over* $\mathbb{Q}$*), respectively, such that*

$$\alpha+\beta+\gamma=0.$$

This is our *abc degree problem* for algebraic numbers. When such α, β, γ exist, we say that the triplet (a,b,c) is *sum-feasible*. It seems that this *abc* degree problem for sums of algebraic numbers is unrelated to the famous *abc conjecture* for integers proposed by Oesterlé and Masser in 1985.

Even for small values of a, b and c it is sometimes very difficult to decide whether the triplet (a,b,c) is sum-feasible. See, for instance,

the proof of Theorem 38, where we establish that $(6, 6, 10)$ is not sum-feasible. With the methods used here we were, however, unable to settle our *abc* degree problem in the case $(6, 6, 8)$. This case has now been shown elsewhere to not be sum-feasible – see [**6**].

We propose a similar problem for the compositum of fields by saying that a triplet $(a, b, c) \in \mathbb{N}^3$ is *compositum-feasible* if there are number fields K and L of degrees a and b, respectively, over the field of rationals $\mathbb{Q}$ such that the degree of their compositum KL is c. For example, the triplet $(2, 2, 4)$ is compositum-feasible ($K = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt{3})$, $KL = \mathbb{Q}(\sqrt{2}, \sqrt{3})$), whereas the triplet $(2, 2, 5)$ is not compositum-feasible, since $[KL : \mathbb{Q}]$ cannot exceed $[K : \mathbb{Q}] \cdot [L : \mathbb{Q}]$.

Similarly, we say that a triplet $(a, b, c) \in \mathbb{N}^3$ is *product-feasible* if there are algebraic numbers α, β and γ of degrees (over $\mathbb{Q}$) a, b and c, respectively, such that $\alpha\beta\gamma = 1$.

Note that if a triplet (a, b, c), $a \leqslant b \leqslant c$, is sum-feasible, compositum-feasible or product-feasible then $c \leqslant ab$. If (a, b, c), $a \leqslant b \leqslant c$, is compositum-feasible then $a \mid c$ and $b \mid c$. These are obvious necessary conditions. In Section 2 we give another simple necessary condition for a triplet to be sum-feasible, compositum-feasible or product-feasible (see Lemma 14).

These three problems are related.

Proposition 1. *If the triplet $(a, b, c) \in \mathbb{N}^3$ is compositum-feasible then it is also sum-feasible and product-feasible.*

Proof: Suppose that K and L are number fields. Then, by the primitive element theorem, $K = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\beta)$ for some $\alpha \in K$ and $\beta \in L$. Furthermore, the compositum $KL = \mathbb{Q}(\alpha, \beta)$ can be expressed as $KL = \mathbb{Q}(\alpha + t\beta)$ and also as $KL = \mathbb{Q}(\alpha(t+\beta))$ for all but finitely many rational numbers t. See the proof of Theorem 4.6 in [**16**] for the case $\alpha + t\beta$. The proof for $\alpha(t+\beta)$ is the same. Indeed, consider the field $K_t = \mathbb{Q}(\alpha(t+\beta))$. Since $\mathbb{Q} \subseteq K_t \subseteq \mathbb{Q}(\alpha, \beta)$, there are two distinct rational numbers t and t' for which $K_t = K_{t'}$. Assume without loss of generality that $\alpha(t'+\beta) \neq 0$. Then, as the quotient of $\alpha(t+\beta)$ and $\alpha(t'+\beta)$ belongs to K_t, we obtain $(t - t')/(t' + \beta) = (t + \beta)/(t' + \beta) - 1 \in K_t$. Thus $\beta \in K_t$. This implies $\alpha \in K_t$, so that $K_t = \mathbb{Q}(\alpha, \beta)$.

Since $[K : \mathbb{Q}] = a$, $[L : \mathbb{Q}] = b$, $[KL : \mathbb{Q}] = c$, choosing an appropriate $t \in \mathbb{Q}$, in the additive case we see that the degrees of α, $t\beta$ and $-\alpha - t\beta$ are a, b, c, respectively. In the multiplicative case, the degrees of α, $t+\beta$ and $\alpha^{-1}(t + \beta)^{-1}$ are a, b, c. □

The converse of Proposition 1 is false in general. Clearly, if the triplet (a, b, c) is sum-feasible (resp. product-feasible) then for any permutation $\{a', b', c'\}$ of $\{a, b, c\}$ the triplet (a', b', c') is also sum-feasible (resp. product-feasible). However, the compositum problem is not symmetric with respect to a, b, c. The triplet $(n, n, 1)$, $n > 1$, is not compositum-feasible, since the degree of the compositum of two number fields of degree n is divisible by n. Meanwhile $(n, n, 1)$ is sum-feasible and product-feasible: for $\alpha = \sqrt[n]{2}$, $\beta = -\alpha$, $\gamma = 0$ we have $\alpha+\beta+\gamma = 0$, whereas $\alpha' = \sqrt[n]{2}$, $\beta' = \alpha'^{-1}$, $\gamma' = 1$ gives $\alpha'\beta'\gamma' = 1$. The less trivial example $(4, 4, 6)$ (which is sum-feasible and product-feasible but not compositum-feasible) follows from Proposition 29 (ii) (Section 3). The reason for not being compositum-feasible is that 4 does not divide 6. We do not know of any example $(a, b, c) \in \mathbb{N}^3$ satisfying $a \mid c$, $b \mid c$ which is sum-feasible (or product-feasible) but is not compositum-feasible.

We have found little in the literature directly related to our problem apart from the 'generic' case (a, b, ab) which has long been known to be compositum-feasible (and hence sum-feasible and product-feasible) – see Proposition 19 below. In particular, one result, due to Isaacs [**11**] who generalized an earlier result of Kaplansky [**15**, p. 71], implies that if α has degree a (over $\mathbb{Q}$), β has degree b and $\gcd(a, b) = 1$ then $\alpha + \beta$ has degree ab. Let us state this result in the following symmetric form.

Proposition 2 ([**11**])**.** *If the triplet $(a, b, c) \in \mathbb{N}^3$ is sum-feasible and two particular numbers from the list a, b, c are coprime then the third number is the product of these two.*

See also [**2**], [**7**] and [**8**], where some conditions for the degree of $\alpha+\beta$ to be 'maximal possible' $\deg(\alpha) \cdot \deg(\beta)$ are given without assumption that $\deg(\alpha)$ and $\deg(\beta)$ are coprime. (Throughout, we denote by $\deg(\alpha)$ the degree of an algebraic number α over $\mathbb{Q}$.) In particular, it is remarked in [**2**, p. 261] that the proof of Isaac's result quoted above shows that if (a, b, ab) is compositum-feasible then it is sum-feasible (i.e., a special case of Proposition 1).

We conjecture that

Conjecture 3. *If the triplet $(a, b, c) \in \mathbb{N}^3$ is sum-feasible then it is also product-feasible.*

The converse of Conjecture 3 is false. The triplet $(2, 3, 3)$ is not sum-feasible, by Proposition 2. Hence $(2, 3, 3)$ is not compositum-feasible either. However, $(2, 3, 3)$ is product-feasible. For example, the numbers

$$\alpha = (-1 - i\sqrt{3})/4, \quad \beta = \sqrt[3]{2}, \quad \gamma = (-1 + i\sqrt{3})/\sqrt[3]{2}$$

have product 1 and degrees 2, 3, 3, respectively.

Conjecture 4. *If the triplets* $(a,b,c),(a',b',c') \in \mathbb{N}^3$ *are sum-feasible (resp. product-feasible, compositum-feasible) then the triplet* (aa',bb',cc') *is also sum-feasible (resp. product-feasible, compositum-feasible).*

Some partial cases of Conjecture 4 are given in Lemma 26, Corollary 27, Proposition 28 and Proposition 32.

The main result of this paper is the following.

Theorem 5. *All the triplets* (a,b,c) *of positive integers with* $a \leqslant b \leqslant c$, $b \leqslant 6$ *that are sum-feasible are given in Table 1, with one possible exception* $(6,6,8)$. *Every such triplet is also compositum-feasible, except for* $(4,4,6)$, $(4,6,6)$, $(6,6,8)$, $(6,6,9)$ *and* $(6,6,15)$.

Table 1. Triplets (a,b,c), $a \leqslant b \leqslant c$, $b \leqslant 6$, that are sum-feasible. (Because of [**6**, Theorem 1], the case $(6,6,8)$ does not appear.)

b\a	**1**	**2**	**3**	**4**	**5**	**6**
1	1					
2	2	2, 4				
3	3	6	3, 6, 9			
4	4	4, 8	12	4, 6, 8, 12, 16		
5	5	10	15	20	5, 10, 20, 25	
6	6	6, 12	6, 12, 18	6, 12, 24	30	6, 9, 12, 15, 18, 24, 30, 36

By our observation above (Proposition 1), if the triplet (a,b,c) is not sum-feasible then it is not compositum-feasible. For example, there are exactly five triplets (a,b,c), $a \leqslant b \leqslant c$, with $a = b = 4$ that are sum-feasible, namely $(4,4,4)$, $(4,4,6)$, $(4,4,8)$, $(4,4,12)$ and $(4,4,16)$. However, since 6 is not a multiple of 4, the triplet $(4,4,6)$ is not compositum-feasible. Taking $K = \mathbb{Q}(\sqrt{2},\sqrt{3})$ and L, say, $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2},\sqrt{5})$,

$\mathbb{Q}(\sqrt{5},\sqrt{7})$ we see that the triplets $(4,4,4)$, $(4,4,8)$, $(4,4,16)$ are compositum-feasible. Further, taking any quartic algebraic number α such that the Galois group of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is the full symmetric group S_4 and its conjugate $\alpha' \neq \alpha$, we see that $[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\alpha'):\mathbb{Q}] = 4$ and $[\mathbb{Q}(\alpha,\alpha'):\mathbb{Q}] = 12$. This shows that the triplet $(4,4,12)$ is also compositum-feasible.

Let p be a prime number. For a positive integer n we define the nonnegative integer $\operatorname{ord}_p(n)$ by

$$p^{\operatorname{ord}_p(n)} \mid n \quad \text{and} \quad p^{\operatorname{ord}_p(n)+1} \nmid n.$$

We say that a triplet (a,b,c) satisfies the *exponent triangle inequality with respect to a prime number* p if

$$\operatorname{ord}_p(a)+\operatorname{ord}_p(b) \geqslant \operatorname{ord}_p(c), \quad \operatorname{ord}_p(b)+\operatorname{ord}_p(c) \geqslant \operatorname{ord}_p(a) \quad \text{and}$$
$$\operatorname{ord}_p(a)+\operatorname{ord}_p(c) \geqslant \operatorname{ord}_p(b).$$

For example, the triplet $(6,6,10)$ satisfies the exponent triangle inequality with respect to every prime number p except for $p=5$.

Theorem 6. *If a triplet of positive integers (a,b,c) satisfies the exponent triangle inequality with respect to every prime number then the triplet (a,b,c) is sum-feasible and product-feasible.*

The exponent triangle inequality condition in Theorem 6 is not necessary. For instance, the triplet $(3,3,6)$ is sum-feasible and product-feasible (e.g., if α and α' are two distinct roots of the polynomial x^3-x-1 then the degrees of α and α'^{-1} are 3, the degree of α'/α is 6 and $\alpha\cdot\alpha'^{-1}\cdot(\alpha'/\alpha)=1$), while the exponent triangle inequality with respect to the prime number 2 is not satisfied. In fact, one can be 'very far' from the exponent triangle inequality. By Proposition 29 (i) combined with Proposition 1, the triplet $(a,b,c) = (2^m+1, 2^m+1, 2^m(2^m+1))$ is sum-feasible, whereas

$$\operatorname{ord}_2(c) - \operatorname{ord}_2(b) - \operatorname{ord}_2(a) = m$$

can be arbitrarily large.

We remark that the condition of Theorem 6 is not sufficient for a triplet to be compositum-feasible. For example, the triplet $(6,10,15)$ satisfies the exponent triangle inequality with respect to every prime number. However, it is not compositum-feasible, because the compositum of two extensions of $\mathbb{Q}$ of degrees 6 and 10 has degree divisible by $\operatorname{lcm}(6,10) = 30$.

More generally, an extra condition for a triplet $(a,b,c) \in \mathbb{N}^3$ to be compositum-feasible can be written as

$$\max\{\mathrm{ord}_p(a),\, \mathrm{ord}_p(b)\} \leqslant \mathrm{ord}_p(c)$$

for every prime number p. This necessary condition becomes sufficient for triplets (a,b,c) satisfying the exponent triangle inequality with respect to any prime number. This result can readily be written in the following form.

Theorem 7. *If a triplet of positive integers (a,b,c) satisfies*

$$\max\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\} \leqslant \mathrm{ord}_p(c) \leqslant \mathrm{ord}_p(a) + \mathrm{ord}_p(b) \tag{1}$$

for every prime number p then the triplet (a,b,c) is compositum-feasible.

Let (a,b,c) be any triplet of positive integers. It is easy to see that the triplet $\big(a(abc)^n, b(abc)^n, c(abc)^{n+1}\big)$ satisfies (1) for all primes p provided that n is large enough. Therefore Theorem 7 implies that the triplet $\big(a(abc)^n, b(abc)^n, c(abc)^{n+1}\big)$ is compositum-feasible (and hence sum-feasible and product-feasible) for each sufficiently large $n \in \mathbb{N}$.

Note that for p a prime number and $t \in \mathbb{N}$ the triplet (p,t,t) is sum-feasible if and only if $p \mid t$. The necessity follows from Proposition 2, the sufficiency from the example $\alpha = -2{\cdot}2^{1/p}$, $\beta = 2^{1/p}+3^{p/t}$, $\gamma = 2^{1/p}-3^{p/t}$, where t is a positive integer divisible by p. In particular, for $p = 2$, the triplet $(2,t,t)$ is sum-feasible if and only if $2 \mid t$. In case of the product we have the following result.

Theorem 8. *The triplet $(2,t,t) \in \mathbb{N}^3$ is product-feasible if and only if $2 \mid t$ or $3 \mid t$.*

The paper is organized as follows. In Section 2 we prove auxiliary results and some necessary conditions for a triplet to be sum-feasible or compositum-feasible. Section 3 contains some explicit constructions for Table 1 as well as the proofs of Theorems 6 and 7. In Section 4 we prove Theorem 8 and provide impossibility proofs which are used in the proof of Theorem 5 later on. The proof of Theorem 5 is divided into two parts. At the end of Section 3 we prove that each triplet given in Table 1 is sum-feasible. The proof that no other triplets are sum-feasible is given at the end of Section 4.

2. Lemmas

Lemma 9 (Part of [**23**, Lemma 1])**.** *Let α_1, α_2, α_3 be distinct conjugate algebraic numbers. Then $\alpha_2 \pm \alpha_3 \neq \pm 2\alpha_1$ for all four choices of signs $\pm$.*

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of a nonzero separable polynomial $f(x) \in \mathbb{Q}[x]$ of degree $n \geqslant 2$. An *additive relation* between $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a relation of the kind

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \in \mathbb{Q},$$

where all the $a_j \in \mathbb{Q}$. We call this additive relation *trivial* if $a_1 = a_2 = \cdots = a_n$.

Recall that the Galois group G of f is 2-*transitive* if for any two pairs of the roots of f, say, α, α', $\alpha \neq \alpha'$, and α_i, α_j, $\alpha_i \neq \alpha_j$, there is an automorphism $\sigma \in G$ such that $\sigma(\alpha) = \alpha_i$ and $\sigma(\alpha') = \alpha_j$.

Lemma 10 (Part of Theorem 3 in [**1**] – see also [**24**])**.** *Suppose that the Galois group of a separable polynomial $f(x) \in \mathbb{Q}[x]$ of degree n is 2-transitive. Then there are no nontrivial additive relations between the roots of f.*

For a polynomial of prime degree we have the following.

Lemma 11 (Special case of [**5**, Theorem 2])**.** *There are no nontrivial additive relations between the roots $\alpha_1, \alpha_2, \ldots, \alpha_p$ of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of prime degree p.*

Lemma 12 ([**16**, Theorem 1.12])**.** *If K and L are number fields and $K/\mathbb{Q}$ is Galois then*

$$[KL : \mathbb{Q}] = \frac{[K : \mathbb{Q}] \cdot [L : \mathbb{Q}]}{[K \cap L : \mathbb{Q}]}.$$

Lemma 13 ([**21**])**.** *Suppose that α is a root of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$. Let r be the number of linear factors of $f(x)$ over $\mathbb{Q}(\alpha)$. Then r divides the degree of $f(x)$.*

As usual, denote by $\operatorname{lcm}(a, b)$ and $\gcd(a, b)$ the least common multiple and the greatest common divisor of positive integers a and b, respectively.

Lemma 14. *Suppose that a triplet (a, b, c) is sum-feasible, product-feasible or compositum-feasible. Then $c \mid \operatorname{lcm}(a, b) \cdot t$ for some positive integer $t \leqslant \gcd(a, b)$.*

Proof: Assume that a triplet (a, b, c) is sum-feasible, product-feasible or compositum-feasible. Then there exist algebraic numbers α, β, γ or degrees a, b, c, respectively, such that $\alpha + \beta + \gamma = 0$ or $\alpha\beta\gamma = 1$ or $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$. In any case, it is clear that the degree D of the compositum $\mathbb{Q}(\alpha, \beta)$ is divisible by $\operatorname{lcm}(a, b)$, since $a \mid D$ and $b \mid D$, so that $D = \operatorname{lcm}(a, b) \cdot t$ say. Clearly,

$$\begin{aligned} D &= [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\beta)] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] \leqslant [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = ab. \end{aligned}$$

Hence $t \leqslant ab/\operatorname{lcm}(a,b) = \gcd(a,b)$. Finally, note that $c \mid D$, because $\mathbb{Q}(\gamma)$ is a subfield of $\mathbb{Q}(\alpha,\beta)$. □

3. Constructions

Let K be a number field of degree n over $\mathbb{Q}$, with $\mathcal{O}_K$ its ring of integers, d_K its discriminant, and $\sigma_1,\dots,\sigma_n$ be the n distinct $\mathbb{Q}$-invariant embeddings of K into $\mathbb{C}$. If α is an arbitrary element of K then its discriminant, which we shall denote by $d_K(\alpha)$, is defined by

$$d_K(\alpha) = \prod_{1\leqslant i<j\leqslant n} (\sigma_i(\alpha)-\sigma_j(\alpha))^2.$$

It is well-known that if $\alpha \in \mathcal{O}_K$ then $d_K(\alpha)$ is a rational integer which is divisible by d_K (see [**20**, Proposition 2.13]).

Lemma 15 ([**19**, Exercise 4.5.4 and solution])**.** *If α is a root of an irreducible polynomial $x^n + ax + b \in \mathbb{Z}[x]$, $n \geqslant 2$, then*

$$d_K(\alpha) = (-1)^{n(n-1)/2}\Big(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n\Big)$$

where $K = \mathbb{Q}(\alpha)$.

Lemma 16. *For any positive integers n and D there exists an extension $K/\mathbb{Q}$ of degree n whose discriminant d_K is coprime to D.*

Proof: If $D = 1$ then one can take any number field K of degree n. If $n = 1$ then one can take $K = \mathbb{Q}$, since $d_{\mathbb{Q}} = 1$. So we can assume that $D \geqslant 2$ and $n \geqslant 2$.

Suppose that the set of primes that divide D is $\{p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s\}$ where $p_i \mid n$ and $q_j \nmid n$ for $i = 1,\dots,r$ and $j = 1,\dots,s$. Choose a prime number q such that

$$q > \max\{p_1,\dots,p_r,q_1,\dots,q_s\}.$$

Eisenstein's Criterion implies the irreducibility of the polynomial

$$x^n + qq_1\cdots q_s x + q.$$

Let α be any root of this polynomial. Then, by Lemma 15, we obtain

$$d_{\mathbb{Q}(\alpha)}(\alpha) = (-1)^{n(n-1)/2}\cdot q^{n-1}\Big(n^n + (-1)^{n-1}(n-1)^{n-1}q(q_1\cdots q_s)^n\Big).$$

It is easy to see that the number $d_{\mathbb{Q}(\alpha)}(\alpha)$ is coprime to $p_1\cdots p_r q_1\cdots q_s$, and therefore coprime to D. Hence the discriminant of the number field $K = \mathbb{Q}(\alpha)$, which is a divisor of $d_K(\alpha)$, is coprime to D. □

Lemma 17 ([**10**, Theorem 87], [**19**, Exercise 6.5.14 and solution])**.** *If K and L are number fields, of degrees m and n, respectively, whose discriminants are coprime numbers, then their compositum is a field of degree mn.*

Lemma 18 (Part of [**10**, Theorem 88])**.** *If K and L are number fields of degrees m and n, respectively, with coprime discriminants d_K and d_L, respectively, then the discriminant of their compositum KL is $d_K^n d_L^m$.*

Proposition 19. *For any positive integers a and b the triplet (a, b, ab) is compositum-feasible and hence both sum-feasible and product-feasible.*

Proof: Let K be a number field of degree a. By Lemma 16, there exists an extension $L/\mathbb{Q}$ of degree b whose discriminant d_L is coprime to d_K. By Lemma 17, we have $[KL : \mathbb{Q}] = ab$, and hence (a, b, ab) is compositum-feasible. By Proposition 1, the triplet (a, b, ab) is both sum-feasible and product-feasible. □

Lemma 20. *Suppose that α and β are algebraic numbers and that β is of the same degree d over $\mathbb{Q}$ and over $\mathbb{Q}(\alpha)$. Then for any conjugate α' of α the degree of β over $\mathbb{Q}(\alpha')$ is also d.*

Proof: Assume that β has degree n, $1 \leqslant n < d$, over the field $\mathbb{Q}(\alpha')$, where α' is a conjugate of α. Then β is a root of a polynomial P of degree n with coefficients in $\mathbb{Q}(\alpha')$. Take an automorphism σ of the Galois group of $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ which maps α' to α. It maps P to a polynomial of degree n with coefficients in $\mathbb{Q}(\alpha)$ whose root is $\sigma(\beta)$. So the conjugate $\beta' = \sigma(\beta)$ of β over $\mathbb{Q}$ has degree at most n over $\mathbb{Q}(\alpha)$, a contradiction. □

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

Proof: Since β is of degree n over $\mathbb{Q}(\alpha)$, for any j, $1 \leqslant j \leqslant n$, there exists an automorphism of the Galois group of $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ which fixes α and maps β to β_j. Hence all the numbers $\alpha + \beta_j$ (resp. $\alpha\beta_j$), $1 \leqslant j \leqslant n$, are conjugate over $\mathbb{Q}$.

Note that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] = mn$, and therefore α is of degree m over $\mathbb{Q}(\beta)$. By Lemma 20, α is of degree m over $\mathbb{Q}(\beta_j)$ for any j, $1 \leqslant j \leqslant n$. Now fix j, $1 \leqslant j \leqslant n$. For any i, $1 \leqslant i \leqslant$

m, there exists an automorphism of the Galois group of $\mathbb{Q}(\alpha,\beta)/\mathbb{Q}$ which fixes β_j and maps α to α_i. Hence all mn numbers $\alpha_i+\beta_j$ (resp. $\alpha_i\beta_j$), where $1\leqslant i\leqslant m$ and $1\leqslant j\leqslant n$, are conjugate over $\mathbb{Q}$. □

Lemma 22. *Suppose that p is a prime number and u, v, w are nonnegative integers such that $\max(u,v)\leqslant w\leqslant u+v$. Then for any positive integer D there exist number fields K and L of degrees p^u and p^v, respectively, such that the degree of the compositum KL is p^w and the discriminant d_{KL} of KL is coprime to D.*

Proof: Set $C=u+v-w$, $A=w-v$ and $B=w-u$, so that $A\geqslant 0$, $B\geqslant 0$, $C\geqslant 0$. By Lemma 16, there exist number fields K_1, L_1 and M of degrees p^C, p^A and p^B, respectively, such that

$$\begin{aligned}&\gcd(d_{K_1},D)=1,\\&\gcd(d_{L_1},D\cdot d_{K_1})=1,\\&\gcd(d_M,D\cdot d_{K_1}\cdot d_{L_1})=1.\end{aligned}$$

Then, by Lemma 17, we have

$$\begin{aligned}[K_1L_1:\mathbb{Q}]&=p^C\cdot p^A=p^u,\\[K_1M:\mathbb{Q}]&=p^C\cdot p^B=p^v,\\[K_1L_1M:\mathbb{Q}]&=p^C\cdot p^A\cdot p^B=p^w.\end{aligned}$$

Put $K=K_1L_1$ and $L=K_1M$. Lemma 18 implies that the discriminant d_{KL} of the number field $KL=K_1L_1M$ is coprime to D. □

Note that in Proposition 1 the algebraic numbers α, β and the rational number t can be chosen so that α is not a conjugate of $-\alpha$, $t+\beta$ is not a conjugate of $-t-\beta$ and $\alpha^{-1}(t+\beta)^{-1}$ is not a conjugate of $-\alpha^{-1}(t+\beta)^{-1}$. Combining this argument with Lemma 22, by choosing an appropriate α, β and $t\in\mathbb{Q}$ in the multiplicative case, we obtain the following.

Corollary 23. *Suppose that p is a prime number and u, v, w are nonnegative integers such that $\max(u,v)\leqslant w\leqslant u+v$. Then for any positive integer D there exist algebraic numbers α, β, γ of degrees p^u, p^v, p^w such that $\alpha+\beta+\gamma=0$ (resp. $\alpha\beta\gamma=1$) and the discriminant $d_{\mathbb{Q}(\alpha,\beta)}$ of the number field $\mathbb{Q}(\alpha,\beta)$ is coprime to D.*

Furthermore, in the multiplicative case, $\alpha\beta\gamma=1$, the numbers α, β and γ can be chosen so that $-\alpha$ is not a conjugate of α, $-\beta$ is not a conjugate of β and $-\gamma$ is not a conjugate of γ.

Note that one can also give an explicit construction illustrating Lemma 22 and Corollary 23 assuming that p does not divide D. Take u distinct prime numbers $p_1, \ldots, p_u$ and v distinct prime numbers $q_1, \ldots, q_v$ so that the first $C = u+v-w$ (where w in the range $\max(u, v) \leqslant w \leqslant u+v$) numbers in those sets are the same

$$p_1 = q_1, \ldots, p_C = q_C,$$

i.e.,

$$\{p_1, p_2, \ldots, p_u\} \cap \{q_1, q_2, \ldots, q_v\} = \{p_1, p_2, \ldots, p_C\}.$$

Assume that the prime numbers p_i $(1 \leqslant i \leqslant u)$ and q_i $(1 \leqslant i \leqslant v)$ are all greater than p and D and that p does not divide D. Set

$$K = \mathbb{Q}(p_1^{1/p}, \ldots, p_u^{1/p}), \quad L = \mathbb{Q}(q_1^{1/p}, \ldots, q_v^{1/p}).$$

Then

$$KL = \mathbb{Q}(p_1^{1/p}, \ldots, p_u^{1/p}, q_{C+1}^{1/p}, \ldots, q_v^{1/p}).$$

Clearly, K is of degree p^u, L is of degree p^v and KL is of degree $p^u p^{v-C} = p^w$ with discriminant coprime to D.

To illustrate Corollary 23 we can take

$$\alpha = p_1^{1/p} + \cdots + p_u^{1/p}, \quad \beta = q_1^{1/p} + \cdots + q_v^{1/p},$$

and

$$\gamma = -2p_1^{1/p} - \cdots - 2p_C^{1/p} - p_{C+1}^{1/p} - \cdots - p_u^{1/p} - q_{C+1}^{1/p} - \cdots - q_v^{1/p}$$

for the sum and

$$\alpha = (p_1^{1/p}+1)\cdots(p_u^{1/p}+1), \quad \beta = (q_1^{1/p}+1)\cdots(q_v^{1/p}+1), \quad \gamma = (\alpha\beta)^{-1}$$

for the product. In both cases, $\deg(\alpha) = p^u$, $\deg(\beta) = p^v$, $\deg(\gamma) = p^u p^{v-C} = p^w$.

Lemma 24. *Suppose that α, β, γ, δ, μ and ν are algebraic numbers of degrees a, b, c, a', b' and c', respectively, such that $\alpha+\beta+\gamma = 0$ (resp. $\alpha\beta\gamma = 1$) and $\delta+\mu+\nu = 0$ (resp. $\delta\mu\nu = 1$ and, in addition, δ is not a conjugate of $-\delta$, μ is not a conjugate of $-\mu$, ν is not a conjugate of $-\nu$). If*

$$\gcd(d_{\mathbb{Q}(\alpha)}, d_{\mathbb{Q}(\delta)}) = \gcd(d_{\mathbb{Q}(\beta)}, d_{\mathbb{Q}(\mu)}) = \gcd(d_{\mathbb{Q}(\gamma)}, d_{\mathbb{Q}(\nu)}) = 1$$

then the triplet (aa', bb', cc') is sum-feasible (resp. product-feasible).

Proof: Let us first deal with the additive case when

$$\alpha+\beta+\gamma = \delta+\mu+\nu = 0.$$

Since $\gcd(d_{\mathbb{Q}(\alpha)}, d_{\mathbb{Q}(\delta)}) = 1$, by Lemma 17, we obtain $[\mathbb{Q}(\alpha,\delta):\mathbb{Q}] = aa'$. We claim that

$$\mathbb{Q}(\alpha,\delta) = \mathbb{Q}(\alpha+\delta). \tag{2}$$

Indeed, let $\alpha_1, \alpha_2, \dots, \alpha_a$ and $\delta_1, \delta_2, \dots, \delta_{a'}$ be all the distinct conjugates of α and δ, respectively. Without loss of generality we may assume that $a, a' \geqslant 2$, since otherwise (2) automatically holds.

By Proposition 21, all the numbers $\alpha_i + \delta_j$, $1 \leqslant i \leqslant a$, $1 \leqslant j \leqslant a'$, are conjugate. Suppose that $\mathbb{Q}(\alpha,\delta) \neq \mathbb{Q}(\alpha+\delta)$. Then $\alpha_i + \delta_j = \alpha_k + \delta_l$ with certain $i \neq k$ and $j \neq l$. So $\alpha_i - \alpha_k = \delta_l - \delta_j$. The difference of two distinct conjugates of an algebraic number of degree at least two is irrational, e.g., by trace consideration or by Hilbert's theorem 90. (See [**9**] for the description of all algebraic numbers expressible as the difference of two conjugate numbers.) Therefore,

$$L := \mathbb{Q}(\alpha)^{\mathrm{Gal}} \cap \mathbb{Q}(\delta)^{\mathrm{Gal}} \neq \mathbb{Q}, \tag{3}$$

where K^{Gal} denotes the Galois closure of the number field K.

Since $L = \mathbb{Q}(\alpha)^{\mathrm{Gal}} \cap \mathbb{Q}(\delta)^{\mathrm{Gal}} \neq \mathbb{Q}$, by Minkowski's theorem, we must have $|d_L| > 1$. However, the discriminants of the fields $\mathbb{Q}(\alpha)^{\mathrm{Gal}}$ and $\mathbb{Q}(\delta)^{\mathrm{Gal}}$ are both divisible by d_L, which is impossible in view of $\gcd(d_{\mathbb{Q}(\alpha)}, d_{\mathbb{Q}(\delta)}) = 1$. (For any prime number p we have $p \mid d_K$ if and only if $p \mid d_{K^{\mathrm{Gal}}}$; see [**20**, p. 159].) This proves (2).

Analogously, we obtain $[\mathbb{Q}(\beta,\mu):\mathbb{Q}] = bb'$ and $\mathbb{Q}(\beta,\mu) = \mathbb{Q}(\beta+\mu)$. Also, $[\mathbb{Q}(\gamma,\nu):\mathbb{Q}] = cc'$ and $\mathbb{Q}(\gamma,\nu) = \mathbb{Q}(\gamma+\nu)$. Hence

$$\deg(\alpha+\delta) = [\mathbb{Q}(\alpha,\delta):\mathbb{Q}] = aa', \tag{4}$$

$$\deg(\beta+\mu) = [\mathbb{Q}(\beta,\mu):\mathbb{Q}] = bb', \tag{5}$$

$$\deg(\gamma+\nu) = [\mathbb{Q}(\gamma,\nu):\mathbb{Q}] = cc' \tag{6}$$

and $(\alpha+\delta)+(\beta+\mu)+(\gamma+\nu) = 0$. This completes the proof of additive version of the lemma.

To prove the multiplicative version, where $\alpha\beta\gamma = \delta\mu\nu = 1$, we first claim that

$$\mathbb{Q}(\alpha,\delta) = \mathbb{Q}(\alpha\delta). \tag{7}$$

As above, let $\alpha_1, \alpha_2, \dots, \alpha_a$ and $\delta_1, \delta_2, \dots, \delta_{a'}$ be all the distinct conjugates of α and δ, respectively. We may also assume that $a, a' \geqslant 2$, since otherwise (7) certainly holds.

Suppose that $\mathbb{Q}(\alpha,\delta) \neq \mathbb{Q}(\alpha\delta)$. Then $\alpha_i\delta_j = \alpha_k\delta_l$ with some $i \neq k$ and $j \neq l$. So $\alpha_i/\alpha_k = \delta_l/\delta_j$. We shall prove that in this case (3) also holds. Indeed, observe that the quotient of two distinct conjugate algebraic numbers is rational if and only if it is a root of unity. The

only such number distinct from 1 is -1. So $\delta_l/\delta_j \in \mathbb{Q}$ if and only if $\delta_l = -\delta_j$ which is impossible, by our extra assumption that δ is not a conjugate of $-\delta$. Now, exactly the same argument as above leads to a contradiction and completes the proof of (7).

Next, by the same argument, we must have $[\mathbb{Q}(\beta,\mu) : \mathbb{Q}] = bb'$ and $\mathbb{Q}(\beta,\mu) = \mathbb{Q}(\beta\mu)$ and also $[\mathbb{Q}(\gamma,\nu) : \mathbb{Q}] = cc'$ and $\mathbb{Q}(\gamma,\nu) = \mathbb{Q}(\gamma\nu)$. Hence, instead of (4)–(6), we obtain

$$\begin{aligned}\deg(\alpha\delta) &= [\mathbb{Q}(\alpha,\delta) : \mathbb{Q}] = aa',\\ \deg(\beta\mu) &= [\mathbb{Q}(\beta,\mu) : \mathbb{Q}] = bb',\\ \deg(\gamma\nu) &= [\mathbb{Q}(\gamma,\nu) : \mathbb{Q}] = cc'\end{aligned}$$

and $(\alpha\delta)\cdot(\beta\mu)\cdot(\gamma\nu) = 1$. □

Remark 25. In fact, if α, β, γ, δ, μ and ν are algebraic numbers of degrees a, b, c, a', b' and c', respectively, such that $\alpha+\beta+\gamma = 0$ and $\delta+\mu+\nu = 0$ and if

$$[\mathbb{Q}(\alpha,\delta)] = aa', \quad [\mathbb{Q}(\beta,\mu)] = bb' \quad \text{and} \quad [\mathbb{Q}(\gamma,\nu)] = cc'$$

then there is a rational number t such that

$$\deg(\alpha+t\delta) = aa', \quad \deg(\beta+t\mu) = bb' \quad \text{and} \quad \deg(\gamma+t\nu) = cc'.$$

Since $(\alpha+t\delta)+(\beta+t\mu)+(\gamma+t\nu) = 0$, the triplet (aa', bb', cc') is sum-feasible.

Lemma 26. *Suppose that K_1, L_1, K_2, L_2 are number fields of degrees a_1, b_1, a_2, b_2, respectively. Let $c_1 = [K_1L_1 : \mathbb{Q}]$ and $c_2 = [K_2L_2 : \mathbb{Q}]$, and suppose that the discriminant $d_{K_1L_1}$ of the compositum K_1L_1 is coprime to the discriminant $d_{K_2L_2}$ of K_2L_2. Then the triplet (a_1a_2, b_1b_2, c_1c_2) is compositum-feasible.*

Proof: It is well-known that if K is a subfield of a number field L then d_K divides d_L (see, e.g., [**20**, Proposition 2.16]). So the discriminant of any subfield of K_1L_1 is coprime to the discriminant of any subfield of K_2L_2. Hence, by Lemma 17, we have

$$\begin{aligned}[K_1K_2 : \mathbb{Q}] &= a_1a_2,\\ [L_1L_2 : \mathbb{Q}] &= b_1b_2,\\ [K_1L_1K_2L_2 : \mathbb{Q}] &= c_1c_2.\end{aligned}$$

Here $K_1L_1K_2L_2$ is the compositum of K_1L_1 and K_2L_2 which coincides with the compositum of K_1K_2 and L_1L_2. Therefore the triplet (a_1a_2, b_1b_2, c_1c_2) is compositum-feasible. □

Corollary 27. *Suppose that p is a prime number and u, v, w are nonnegative integers such that $\max(u,v) \leqslant w \leqslant u+v$, and that the triplet $(a,b,c) \in \mathbb{N}^3$ is compositum-feasible. Then the triplet (ap^u, bp^v, cp^w) is also compositum-feasible.*

Proof: Since the triplet (a,b,c) is compositum-feasible, there exist number fields K_1 and L_1 of degrees a and b, respectively, such that the degree of the compositum K_1L_1 is c. By Lemma 22 with $D = d_{K_1L_1}$, there exist number fields K_2 and L_2 of degrees p^u and p^v, respectively, such that the degree of the compositum K_2L_2 is p^w and the discriminant $d_{K_2L_2}$ of K_2L_2 is coprime to the discriminant $d_{K_1L_1}$ of K_1L_1. Then Lemma 26 implies that the triplet (ap^u, bp^v, cp^w) is compositum-feasible. □

Proof of Theorem 6: Let $p_1 < p_2 < \cdots < p_s$ be the primes dividing the product abc. Only p_1 can be even. Assume that the exponents of p_i in a, b, c are $u_i \geqslant 0$, $v_i \geqslant 0$, $w_i \geqslant 0$, respectively, so that

$$a = \prod_{i=1}^{s} p_i^{u_i}, \quad b = \prod_{i=1}^{s} p_i^{v_i}, \quad c = \prod_{i=1}^{s} p_i^{w_i}.$$

We start with p_1 and, by Corollary 23 with $D = D_1 = 1$, construct the numbers α_1, β_1, γ_1 of degrees $p_1^{u_1}$, $p_1^{v_1}$, $p_1^{w_1}$, respectively, such that $\alpha_1 + \beta_1 + \gamma_1 = 0$ (resp. $\alpha_1\beta_1\gamma_1 = 1$). Set $D_2 = d_{\mathbb{Q}(\alpha_1,\beta_1)}$. By Corollary 23 with $D = D_2$ and Lemma 24, there exist algebraic numbers α_2, β_2, γ_2 of degrees $p_2^{u_2}$, $p_2^{v_2}$, $p_2^{w_2}$, respectively, such that $\alpha_2 + \beta_2 + \gamma_2 = 0$ (resp. $\alpha_2\beta_2\gamma_2 = 1$). Moreover, since p_2 is odd, α_2, β_2, γ_2 are of odd degree (so the multiplicative version of Lemma 24 is applicable) and the degrees of $\alpha_1+\alpha_2$, $\beta_1+\beta_2$, $\gamma_1+\gamma_2$ (resp. $\alpha_1\alpha_2$, $\beta_1\beta_2$, $\gamma_1\gamma_2$) are $p_1^{u_1}p_2^{u_2}$, $p_1^{v_1}p_2^{v_2}$, $p_1^{w_1}p_2^{w_2}$, respectively. Next, selecting $D_i = d_{\mathbb{Q}(\alpha_1,\beta_1,\ldots,\alpha_{i-1},\beta_{i-1})}$ for $i = 3,\ldots,s$ and continuing step-by-step in this fashion (by Corollary 23 with $D = D_i$ at ith step and Lemma 24) we will end up with the numbers

$$\alpha = \alpha_1 + \cdots + \alpha_s, \quad \beta = \beta_1 + \cdots + \beta_s, \quad \gamma = \gamma_1 + \cdots + \gamma_s$$

(resp. $\alpha = \alpha_1 \cdots \alpha_s$, $\beta = \beta_1 \cdots \beta_s$, $\gamma = \gamma_1 \cdots \gamma_s$) of degrees $\prod_{i=1}^{s} p_i^{u_i} = a$, $\prod_{i=1}^{s} p_i^{v_i} = b$, $\prod_{i=1}^{s} p_i^{w_i} = c$, respectively, satisfying $\alpha + \beta + \gamma = 0$ (resp. $\alpha\beta\gamma = 1$.) □

Proof of Theorem 7: Assume that the inequality

$$\max\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\} \leqslant \mathrm{ord}_p(c)$$

holds for every prime number p. Now, as above, repeated application of Corollary 27 (for primes dividing c) implies that the triplet (a,b,c) is compositum-feasible. □

As a consequence of Corollary 23 and Lemma 24, we also state the following proposition (which is a partial case of Conjecture 4).

Proposition 28. *Suppose that the triplet* $(a, b, c) \in \mathbb{N}^3$ *satisfies the exponent triangle inequality with respect to any prime number. Then for any sum-feasible (resp. product-feasible) triplet* $(a', b', c') \in \mathbb{N}^3$ *the triplet* (aa', bb', cc') *is also sum-feasible (resp. product-feasible).*

Proof: Suppose that the triplet (a', b', c') is product-feasible. We can start with the triplet α', β', γ' of degrees a', b', c' such that $\alpha'\beta'\gamma' = 1$ and with $D = d_{\mathbb{Q}(\alpha',\beta')}$. Then, as above, we apply Corollary 23 and Lemma 24 for each prime dividing abc. The proof in the additive case is the same except that in this case we do not need to use the second part of Corollary 23. □

Proposition 29. *Suppose that* $n \geqslant 2$ *is a positive integer.*

(i) *The triplets* (n, n, n) *and* $(n, n, n(n-1))$ *are compositum-feasible.*

(ii) *The triplet* $(n, n, n(n-1)/2)$ *is sum-feasible and product-feasible, but if* n *is even then it is not compositum-feasible.*

(iii) *The triplet* $(n, n, 2n)$ *is compositum-feasible.*

Proof: (i) Take K to be an arbitrary number field of degree n over $\mathbb{Q}$. Then the compositum $KK = K$ also has degree n. Therefore the triplet (n, n, n) is compositum-feasible for every $n \in \mathbb{N}$.

Let α and α' be two distinct conjugate algebraic numbers of degree n such that the Galois group of their minimal polynomial is the symmetric group S_n. We claim that the degree of α' over $\mathbb{Q}(\alpha)$ equals $n-1$. Indeed, we have $[\mathbb{Q}(\alpha, \alpha') : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\alpha, \alpha') : \mathbb{Q}(\alpha)] \leqslant n(n-1)$. On the other hand, if the degree of α' over the field $\mathbb{Q}(\alpha)$ were less than $n-1$ then the degree of the splitting field of the minimal polynomial of α is less than $n!$, a contradiction. So $[\mathbb{Q}(\alpha, \alpha') : \mathbb{Q}] = n(n-1)$, and therefore $(n, n, n(n-1))$ is compositum-feasible. Of course, combining this with Proposition 1, we also have that the triplets (n, n, n), $n \in \mathbb{N}$, and $(n, n, n(n-1))$, $n \geqslant 2$, are both sum-feasible and product-feasible.

(ii) Let α be an algebraic number of degree n such that the Galois group of its minimal polynomial is S_n. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be distinct conjugates of α over $\mathbb{Q}$. Consider the following set

$$A = \{\alpha_i + \alpha_j \mid i, j = 1, 2, \ldots, n,\ i < j\}.$$

Each element of A is a conjugate of $\alpha_1+\alpha_2$, because S_n is 2-transitive. If two numbers of A, say $\alpha_i+\alpha_j$ and $\alpha_k+\alpha_l$ with either $i\neq k$ or $j\neq l$, were equal, then we would have a nontrivial additive relation between the conjugates of α, which is impossible in view of Lemma 10. So the set A contains exactly $n(n-1)/2$ distinct numbers, and therefore the triplet $(n,n,n(n-1)/2)$ is sum-feasible.

For the product we cannot use Lemma 10 directly. Nevertheless, by the same argument, considering the set

$$A_1=\{\alpha_i\alpha_j \mid i,j=1,2,\dots,n,\ i<j\}$$

we will deduce that the triplet $(n,n,n(n-1)/2)$ is product-feasible. Indeed, assume that $\alpha_i\alpha_j=\alpha_k\alpha_l$, where $\{i,j\}\neq\{k,l\}$. We have an immediate contradiction, unless the list α_i, α_j, α_k, α_l contains four distinct numbers. In this latter case, we must have $n\geqslant 4$. Since the Galois group of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ contains the transposition (i,l), from $\alpha_i\alpha_j=\alpha_k\alpha_l$ we obtain $\alpha_l\alpha_j=\alpha_k\alpha_i$. Thus $\alpha_i^2=\alpha_l^2$. Since $\alpha_i\neq\alpha_l$, this implies $\alpha_i=-\alpha_l$, which is impossible by Lemma 10.

Note that if a triplet (a,b,c) is compositum-feasible then $a\mid c$ and $b\mid c$. However, n does not divide $n(n-1)/2$ for even $n\geqslant 2$. Hence for n even the triplet $(n,n,n(n-1)/2)$ is not compositum-feasible.

(iii) If n is even then the triplet $(n,n,2n)$ is compositum-feasible, by Theorem 7.

Now suppose that $n>1$ is odd. Let $p>2$ be a prime number dividing n. Proposition 5.5.2 of [**13**] implies that the dihedral group D_p can be realized as a Galois group of a number field over $\mathbb{Q}$, i.e., there exists a number field L of degree $2p$ over $\mathbb{Q}$ whose Galois group is isomorphic to the dihedral group D_p (also see [**14**], [**18**]). Let H be a subgroup of D_p of order 2 and let $K\subset L$ be the fixed field of H. By the primitive element theorem, $K=\mathbb{Q}(\theta)$ for some algebraic number θ of degree p. The extension $K/\mathbb{Q}$ is not Galois, because H is not a normal subgroup of D_p. So there is a conjugate θ' of θ such that $L=\mathbb{Q}(\theta,\theta')$. Therefore, the triplet $(p,p,2p)$ is compositum-feasible.

Let $p_1,p_2,\dots,p_k$ be the set of primes (not necessarily distinct) dividing n/p, so that $n/p=p_1p_2\cdots p_k$. Since the triplet $(p,p,2p)$ is compositum-feasible, by Corollary 27, the triplet $(pp_1,pp_1,2pp_1)$ is also compositum-feasible. Now, the repeated application of Corollary 27 (for prime numbers $p_2,p_3,\dots,p_k$) implies that the triplet $(pp_1\cdots p_k,\ pp_1\cdots p_k,\ 2pp_1\cdots p_k)=(n,n,2n)$ is compositum-feasible. □

Proposition 29 can be generalized as follows. Let $\theta_1, \theta_2, \ldots, \theta_n$ be distinct conjugate algebraic numbers of degree $n \geqslant 2$ (over $\mathbb{Q}$) such that the Galois group of their minimal polynomial is the full symmetric group S_n. We shall say that the triplet $(a, b, c) \in \mathbb{N}^3$ is *symmetrically generated* if there exist algebraic numbers α, β and γ of degrees a, b and c, respectively, such that $\alpha + \beta + \gamma = 0$ and both α and β (and hence γ too) are linear forms in conjugates of θ (of degree n with Galois group S_n), i.e., there exist $x_i, y_i \in \mathbb{Z}$, $i = 1, 2, \ldots, n$, such that

$$\alpha = x_1\theta_1 + x_2\theta_2 + \cdots + x_n\theta_n,$$
$$\beta = y_1\theta_1 + y_2\theta_2 + \cdots + y_n\theta_n.$$

Suppose that α is a linear form in conjugates of θ, i.e., there exists a function $f\colon \{1, 2, \ldots, n\} \to \mathbb{Z}$ such that

$$\alpha = f(1) \cdot \theta_1 + f(2) \cdot \theta_2 + \cdots + f(n) \cdot \theta_n.$$

Let

$$A_f = \{f(1), f(2), \ldots, f(n)\} \setminus \{0\}, \quad m_f = |A_f|,$$

and for $j \in A_f$ let k_j be the number of indices i in $\{1, 2, \ldots, n\}$ for which $f(i) = j$. If $A_f = \emptyset$ then $\alpha = 0$, and therefore $\deg(\alpha) = 1$. Suppose that $A_f \neq \emptyset$. Then in view of Lemma 10 it is easy to see that the degree of α (over $\mathbb{Q}$) is

$$\deg(\alpha) = \frac{n \cdot (n-1) \cdots (n - m_f + 1)}{\prod_{j \in A_f} k_j!}. \tag{8}$$

Similarly, writing

$$\beta = g(1) \cdot \theta_1 + g(2) \cdot \theta_2 + \cdots + g(n) \cdot \theta_n$$

and

$$\gamma = h(1) \cdot \theta_1 + h(2) \cdot \theta_2 + \cdots + h(n) \cdot \theta_n,$$

where $h(x) = -f(x) - g(x)$, we find that

$$\deg(\beta) = \frac{n \cdot (n-1) \cdots (n - m_g + 1)}{\prod_{j \in A_g} k_j!} \tag{9}$$

and

$$\deg(\gamma) = \frac{n \cdot (n-1) \cdots (n - m_h + 1)}{\prod_{j \in A_h} k_j!}. \tag{10}$$

The triplet $(\deg(\alpha), \deg(\beta), \deg(\gamma))$ given in (8)–(10) is symmetrically generated for any functions $f, g\colon \{1, 2, \ldots, n\} \to \mathbb{Z}$.

Consider an example with $\alpha=\theta_1$ and $\beta=\theta_2$. Then α and β are both of degree n while the degree of $\gamma=-(\alpha+\beta)=-\theta_1-\theta_2$ is $n(n-1)/2$. Analogously, $\alpha=\theta_1$ and $\beta=2\theta_2$ are both of degree n while the degree of $\gamma=-(\alpha+\beta)=-\theta_1-2\theta_2$ is $n(n-1)$. So both triplets $(n,n,n(n-1)/2)$ and $(n,n,n(n-1))$ are symmetrically generated (see Proposition 29).

In order to get some new symmetrically generated triplets let us fix $i,j\in\mathbb{N}$ satisfying $i+j\leqslant n$ and take

$$\alpha=x_1\theta_1+\cdots+x_i\theta_i,\quad \beta=x_{i+1}\theta_{i+1}+\cdots+x_{i+j}\theta_{i+j},\quad \gamma=-(\alpha+\beta).$$

Selecting $x_1=x_2=\cdots=x_{i+j}=1$ we find that the triplet

$$\left(\binom{n}{i},\binom{n}{j},\binom{n}{i+j}\right)$$

is symmetrically generated. Selecting $x_k=k$ for $k=1,\dots,i+j$ we deduce that the triplet

$$\left(i!\binom{n}{i},j!\binom{n}{j},(i+j)!\binom{n}{i+j}\right)$$

is symmetrically generated.

Lemma 30 ([**3**])**.** *Suppose that α is a root of an irreducible trinomial $f(x)=x^n+ax+b\in\mathbb{Z}[x]$. Let $\Delta(f)$ be the discriminant of f, i.e.,*

$$\Delta(f)=(-1)^{n(n-1)/2}\Big(n^nb^{n-1}+(-1)^{n-1}(n-1)^{n-1}a^n\Big).$$

If $\gcd(n,a)=\gcd(a(n-1),b)=1$ and $|\Delta(f)|$ is not the square of an integer then the Galois group of f is the full symmetric group S_n.

Proposition 31. *For any positive integers $n>1$ and D there exists a number field K of degree n (over $\mathbb{Q}$) whose normal closure L has Galois group isomorphic to the full symmetric group S_n and whose discriminant d_L of $L/\mathbb{Q}$ is coprime to D.*

Proof: Suppose that the set of primes that divide D is

$$\{p_1,p_2,\dots,p_r,q_1,q_2,\dots,q_s\},$$

where $p_i\mid n$ and $q_j\nmid n$ for $i=1,\dots,r$ and $j=1,\dots,s$. Set $a=q_1q_2\cdots q_s$ if $s\geqslant 1$ and $a=1$ otherwise. Consider the polynomial

$$f(x)=x^n+ax+q\in\mathbb{Z}[x],$$

where q is a sufficiently large prime number.

Note that this condition guarantees the irreducibility of $f(x)$ over $\mathbb{Q}$. Indeed, assume that $f(x)$ is reducible over $\mathbb{Q}$, so $f(x) = u(x)v(x)$ with $u(x), v(x) \in \mathbb{Z}[x]$, $\deg(u), \deg(v) \geqslant 1$. Since q is a prime number we have either $u(0) = \pm 1$ or $v(0) = \pm 1$. So $f(x)$ has a root x_0 such that $|x_0| \leqslant 1$. But then

$$q = | - ax_0 - x_0^n| \leqslant |a| \cdot |x_0| + |x_0|^n \leqslant a + 1 \leqslant q_1 q_2 \cdots q_s + 1,$$

which is false for q sufficiently large.

By Lemma 15 and the choice of a and q, the discriminant

$$\Delta(f) = (-1)^{n(n-1)/2}\Big(n^n q^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n\Big)$$

of $f(x)$ is coprime to D. Suppose that α is a root of $f(x)$ and $K = \mathbb{Q}(\alpha)$. It is well known that the discriminant d_K of K divides $\Delta(f)$ (see Proposition 2.13 in [**20**]). Therefore, d_K is also coprime to D.

It remains to show that there exists a prime q for which the Galois group of the normal closure of K is isomorphic to the full symmetric group S_n.

Clearly, if $n = 2$ then the extension $K/\mathbb{Q}$ is normal and its Galois group is S_2. Suppose that $n = 3$. Then

$$|\Delta(f)| = 27q^2 + 4a^3 \equiv 3 \pmod 4,$$

because q is odd. Hence $|\Delta(f)|$ is not the square of an integer. Now, Lemma 30 implies that the Galois group of the polynomial $f(x)$ (and hence the Galois group of the normal closure of K) is S_3.

Assume that $n \geqslant 4$. We claim that for each sufficiently large prime number q the Galois group of the normal closure of K is isomorphic to the full symmetric group S_n. Let us check the the conditions of Lemma 30. Clearly the condition

$$\gcd(n, a) = \gcd(a(n-1), q) = 1$$

of Lemma 30 is satisfied for q sufficiently large. So it remains only to prove that for each sufficiently large q the number

$$|\Delta(f)| = n^n q^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n$$

is not the square of an integer.

Consider the curve

$$y^2 = Ax^{n-1} + B, \tag{11}$$

where $A = n^n$ and $B = (-1)^{n-1}(n-1)^{n-1}a^n$. The polynomial $Ax^{n-1} + B \in \mathbb{Z}[x]$ is separable, and therefore the genus of the curve (11) is at least 1. By a well-known theorem of Siegel (see [**22**]), the curve (11) has a finite number of integer points. If the curve (11) does have integer

solutions, let (x_1, y_1) be the one with largest $|x_1|$. Set $x_1 = 1$ if the curve (11) has no integer solutions. Then for any positive integer $q > x_1$ the number $|\Delta(f)|$ is not the square of an integer. Now, selecting a sufficiently large prime number q we see that the conditions of Lemma 30 are satisfied. So there exists a number field $K = \mathbb{Q}(\alpha)$ of degree n whose normal closure L has Galois group isomorphic to S_n and the discriminant d_K of $K/\mathbb{Q}$ is coprime to D.

Finally, as we already observed above, by [**20**, p. 159], if p is a prime number then $p \mid d_K$ if and only if $p \mid d_L$. Hence d_L is coprime to D. □

In addition to Proposition 28 we obtain one more special case of Conjecture 4 (see Section 1).

Proposition 32. *Suppose that the triplet $(a, b, c) \in \mathbb{N}^3$ is sum-feasible. Then for any symmetrically generated triplet $(a', b', c') \in \mathbb{N}^3$ the triplet (aa', bb', cc') is also sum-feasible.*

Proof: Fix any algebraic numbers α, β, γ of degrees a, b, c such that $\alpha+\beta+\gamma = 0$. Suppose that D is the discriminant of the field $\mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\alpha, \beta)$. Since the triplet (a', b', c') is symmetrically generated, there is an $n \in \mathbb{N}$ and algebraic numbers α', β', γ' of degrees a', b', c' such that $\alpha' + \beta' + \gamma' = 0$ and α' and β' are linear forms in conjugates of an algebraic number θ of degree $n \geqslant 2$ whose Galois group is S_n.

By Proposition 31, there is a number field K of degree n (over $\mathbb{Q}$) whose normal closure L has the Galois group isomorphic to the full symmetric group S_n and the discriminant d_L of L is coprime to D. We can take $K = \mathbb{Q}(\theta)$ and then select α', β', γ' of degrees a', b', c' as linear forms in conjugates of θ. Applying Lemmas 17 and 24, we find that the degrees of $\alpha + \alpha'$, $\beta + \beta'$ and $\gamma + \gamma'$ are aa', bb' and cc', respectively, whereas their sum is zero. □

Proof of Theorem 5 (constructions): We first prove that the triplets displayed in Table 1 are compositum-feasible except for

$$(4, 4, 6), \quad (4, 6, 6), \quad (6, 6, 8), \quad (6, 6, 9), \quad (6, 6, 15).$$

There are 40 such triplets. Then we show that the triplets $(4, 4, 6)$, $(4, 6, 6)$, $(6, 6, 9)$ and $(6, 6, 15)$ are sum-feasible. (The triplet $(6, 6, 8)$ is left undecided here, but it is shown to be not sum feasible in [**6**].) The proof that no other triplets are sum-feasible is given at the end of the next section.

Theorem 7 shows that the following 33 triplets, given in Table 2, are compositum-feasible.

Table 2. Compositum-feasible triplets from Theorem 7.

b \a	**1**	**2**	**3**	**4**	**5**	**6**
1	1					
2	2	2, 4				
3	3	6	3, 9			
4	4	4, 8	12	4, 8, 16		
5	5	10	15	20	5, 25	
6	6	6, 12	6, 18	12, 24	30	6, 12, 18, 36

The triplets $(3, 3, 6)$, $(4, 4, 12)$, $(5, 5, 20)$ and $(6, 6, 30)$ are compositum-feasible, by Proposition 29. Since the triplet $(3, 3, 6)$ is compositum-feasible, Corollary 27 implies that the triplets $(3, 6, 12)$ and $(6, 6, 24)$ are both compositum-feasible. The triplet $(5, 5, 10)$ is compositum-feasible, by Proposition 29 (iii). This gives $33+4+2+1 = 40$ compositum-feasible triplets.

So all the triplets of Table 1 are compositum-feasible except for

$$(4, 4, 6), \quad (4, 6, 6), \quad (6, 6, 8), \quad (6, 6, 9), \quad (6, 6, 15).$$

(If $a \nmid c$ or $b \nmid c$ then the triplet (a, b, c) is not compositum-feasible.) This completes the proof of the compositum part of Theorem 5.

For the sum-feasible part of Theorem 5, note that, by Proposition 1, if the triplet is compositum-feasible then it is sum-feasible as well. So all the triplets of Table 1, except possibly

$$(4, 4, 6), \quad (4, 6, 6), \quad (6, 6, 8), \quad (6, 6, 9), \quad (6, 6, 15),$$

are sum-feasible. It remains to show that the triplets

$$(4, 4, 6), \quad (4, 6, 6), \quad (6, 6, 9), \quad (6, 6, 15)$$

are sum-feasible, the triplet $(6, 6, 8)$ being left undecided. Indeed, the triplets $(4, 4, 6)$ and $(6, 6, 15)$ are sum-feasible, by Proposition 29 (ii), while the triplets $(4, 6, 6)$ and $(6, 6, 9)$ are sum-feasible, by Theorem 6. □

The proof that the remaining triplets (those not in Table 1) are not sum-feasible is given at the end of the next section.

4. Impossibility proofs

We first prove Theorem 8. Then we show that the four special cases from the set

$$\mathcal{S} = \{(3,6,9), (4,6,8), (5,5,15), (6,6,10)\} \tag{12}$$

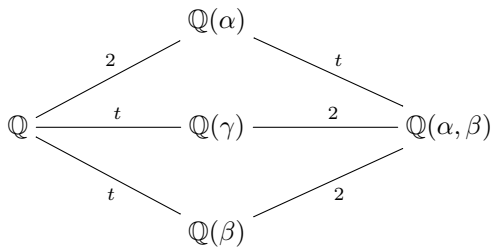
are not sum-feasible. At the end of the section we will complete the proof of Theorem 5 by showing that each triplet (a,b,c), $a \leqslant b \leqslant c$, $b \leqslant 6$ that is not in Table 1 is not sum-feasible.

Proof of Theorem 8: Let $t = 2n$, where $n \in \mathbb{N}$, and put $\alpha = \sqrt{-1}$ and $\beta = \sqrt[t]{2}$. Then $\alpha\beta$ is conjugate to β, and so of degree t. Hence the triplet $(2, 2n, 2n)$ is product-feasible. Similarly, for $t = 3n$, $\alpha = e^{2\pi i/3}$ and $\beta = \sqrt[t]{2}$, $\alpha\beta$ is again conjugate to β, and so of degree t. Hence the triplet $(2, 3n, 3n)$ is product-feasible.

Suppose next that t is a positive integer that is not divisible by 2 or by 3. Assume that the triplet $(2,t,t)$ is product-feasible. Clearly $t > 1$. Then there exist three algebraic numbers α, β and γ of degrees 2, t and t, respectively, such that $\alpha\beta = \gamma$. The degree $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}]$ is divisible by 2 and by t, because $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are the subfields of $\mathbb{Q}(\alpha,\beta)$. On the other hand,

$$[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \leqslant [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = 2t.$$

So $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = 2t$ and we have the following diagram.



Let $\beta_1 = \beta, \beta_2, \ldots, \beta_t$ be the distinct conjugates of β over $\mathbb{Q}$. From the diagram we see that β is of degree t over $\mathbb{Q}(\alpha)$. Hence for every $j \in \{1, 2, \ldots, t\}$ there exists an automorphism σ_j in the Galois group of the normal closure of $\mathbb{Q}(\alpha,\beta,\gamma) = \mathbb{Q}(\alpha,\beta)$ over $\mathbb{Q}$ which fixes α and

sends $\beta = \beta_1$ to β_j. On applying σ_j, $j = 1, \dots, t$, to $\alpha\beta = \gamma$ we obtain

$$\begin{aligned} \alpha\beta_1 &= \gamma_1, \\ \alpha\beta_2 &= \gamma_2, \\ &\vdots \\ \alpha\beta_t &= \gamma_t, \end{aligned} \tag{13}$$

where $\gamma_j = \sigma_j(\gamma)$, $1 \leqslant j \leqslant t$. Then all the conjugates γ_j, $1 \leqslant j \leqslant t$, are distinct. (If $\gamma_i = \gamma_j$ with $i \neq j$ then (13) implies $\beta_i = \beta_j$, which is not the case.) On multiplying together all the equalities in (13) we obtain $\alpha^t = r \in \mathbb{Q}$, because the numbers $\beta_1\beta_2 \cdots \beta_t$ and $\gamma_1\gamma_2 \cdots \gamma_t$ are absolute norms of β and γ, respectively. It follows that the quadratic algebraic number α is a root of a polynomial $p(x) = x^t - r$ for some $r \in \mathbb{Q}$. Let $\theta = r^{1/t}$ be the real root of $p(x)$ (recall that t is odd and > 1) and let $\varepsilon = e^{2\pi i/t}$ be the primitive tth root of unity. Then all the roots of $p(x)$ are

$$\theta, \theta\varepsilon, \theta\varepsilon^2, \dots, \theta\varepsilon^{t-1}.$$

Let $\alpha' \neq \alpha$ be the (only) conjugate of α over $\mathbb{Q}$. Then α' also is a root of $p(x)$. So $\alpha = \theta\varepsilon^k$ and $\alpha' = \theta\varepsilon^l$ with certain $k, l \in \{0, 1, \dots, t-1\}$, $k \neq l$. We claim that $l = t - k$. Indeed, note that $\alpha\alpha' = \theta^2\varepsilon^{k+l} \in \mathbb{Q}$. Since θ^2 is real, so is ε^{k+l}. Hence $\varepsilon^{k+l} = \pm 1$. This yields $k + l \in \{t/2, t, 3t/2\}$, since $0 < k + l < 2t$. Therefore, $k + l = t$, because t is odd. This implies

$$\alpha = \theta\varepsilon^k, \quad \alpha' = \theta\varepsilon^{t-k} = \theta\varepsilon^{-k}.$$

It follows that $\alpha + \alpha' = \theta(\varepsilon^k + \varepsilon^{-k}) \in \mathbb{Q}$ and $\alpha\alpha' = \theta^2 \in \mathbb{Q}$. Combining this with $\theta^t \in \mathbb{Q}$, where t is odd, we deduce that $\theta \in \mathbb{Q}$. Hence $\varepsilon^k + \varepsilon^{-k} = (\alpha + \alpha')/\theta \in \mathbb{Q}$. The number $\varepsilon^k + \varepsilon^{-k} = 2\cos(2\pi k/t)$ is an algebraic integer, so it must be a rational integer. Consequently,

$$\varepsilon^k + \varepsilon^{-k} = 2\cos(2\pi k/t) \in \{0, \pm 1, \pm 2\}.$$

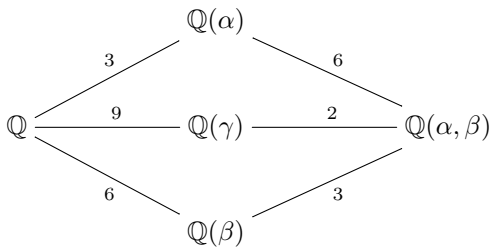
(See also [**12**] and [**25**].)

If $2\cos(2\pi k/t) = 0$ then $2\pi k/t = \pi/2 + \pi s$ for some $s \in \mathbb{Z}$. This yields $4k = t(2s+1)$ which is impossible, because t is odd. Next, $2\cos(2\pi k/t) = \pm 1$ implies that t is divisible by 3, which is not the case. Finally, if $2\cos(2\pi k/t) = \pm 2$ then $2\pi k/t = \pi s$ for some $s \in \mathbb{Z}$. So $\varepsilon^k = \varepsilon^{-k} = (-1)^s$, and therefore $\alpha = \theta\varepsilon^k = \theta\varepsilon^{-k} = \alpha'$, a contradiction. □

Now, step by step, we give all necessary impossibility proofs for Theorem 5.

Theorem 33. *The triplet* $(3, 6, 9)$ *is not sum-feasible.*

Proof: Suppose that $(3,6,9)$ is sum-feasible. Then there exist algebraic numbers α, β, γ of degrees 3, 6, 9, respectively, such that $\alpha+\beta+\gamma=0$. The degree of $\mathbb{Q}(\alpha,\beta)$ over $\mathbb{Q}$ is divisible by 9, because $\mathbb{Q}(\gamma)=\mathbb{Q}(\alpha+\beta)$ is a subfield of $\mathbb{Q}(\alpha,\beta)$. Similarly, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$ is divisible by 6, because $\mathbb{Q}(\beta)\subset\mathbb{Q}(\alpha,\beta)$. On the other hand, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]\leqslant[\mathbb{Q}(\alpha):\mathbb{Q}]\cdot[\mathbb{Q}(\beta):\mathbb{Q}]=18$. Hence $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=18$ and we have the following diagram.



Let α_1, α_2, α_3 be the distinct conjugates of α over $\mathbb{Q}$, and let β_1, β_2, β_3, β_4, β_5, β_6 be the distinct conjugates of β over $\mathbb{Q}$. By the diagram, β is of degree 6 over $\mathbb{Q}(\alpha)$. Proposition 21 implies that all 18 (not necessarily distinct) numbers $\alpha_i+\beta_j$, $1\leqslant i\leqslant 3$, $1\leqslant j\leqslant 6$, are conjugate over $\mathbb{Q}$. Put

$$\Gamma_i=\{\alpha_i+\beta_1,\alpha_i+\beta_2,\alpha_i+\beta_3,\alpha_i+\beta_4,\alpha_i+\beta_5,\alpha_i+\beta_6\},\quad i=1,2,3.$$

Clearly, $|\Gamma_i|=6$ for $i=1,2,3$, because all six elements of the set Γ_i are distinct.

We next claim that $|\Gamma_1\cap\Gamma_2|=3$. Indeed, if $|\Gamma_1\cap\Gamma_2|<3$ then

$$|\Gamma_1\cup\Gamma_2|=|\Gamma_1|+|\Gamma_2|-|\Gamma_1\cap\Gamma_2|=12-|\Gamma_1\cap\Gamma_2|>9$$

which is impossible, because $\gamma=-(\alpha+\beta)$ is of degree 9 over $\mathbb{Q}$.

On the other hand, if $|\Gamma_1\cap\Gamma_2|\geqslant 4$ then there exist distinct indices j_1, j_2, j_3, j_4 and distinct indices k_1, k_2, k_3, k_4 such that

$$\alpha_1+\beta_{j_1}=\alpha_2+\beta_{k_1}, \tag{14}$$

$$\alpha_1+\beta_{j_2}=\alpha_2+\beta_{k_2}, \tag{15}$$

$$\alpha_1+\beta_{j_3}=\alpha_2+\beta_{k_3},$$

$$\alpha_1+\beta_{j_4}=\alpha_2+\beta_{k_4},$$

and $\{j_1,j_2,j_3,j_4,k_1,k_2,k_3,k_4\}\subseteq\{1,2,3,4,5,6\}$. Evidently,

$$\{j_1,j_2,j_3,j_4\}\cap\{k_1,k_2,k_3,k_4\}\neq\emptyset.$$

Assume without loss of generality that $j_1 = k_2$ ($j_1 = k_1$ would imply $\alpha_1 = \alpha_2$, which is not the case). Subtracting (15) from (14) we get

$$2\beta_{j_1} = \beta_{k_1} + \beta_{j_2}. \tag{16}$$

If $k_1 = j_2$ then $j_1 = k_1$ and (14) implies $\alpha_1 = \alpha_2$, which is impossible. So $\beta_{j_1}, \beta_{k_1}, \beta_{j_2}$ are distinct conjugates. But then (16) contradicts Lemma 9. This proves the inequality

$$|\Gamma_1 \cap \Gamma_2| \leqslant 3 \tag{17}$$

and so completes the proof of $|\Gamma_1 \cap \Gamma_2| = 3$. Analogously, $|\Gamma_1 \cap \Gamma_3| = 3$ and $|\Gamma_2 \cap \Gamma_3| = 3$.

Since $|\Gamma_1 \cap \Gamma_2| = 3$, after re-indexing the numbers β_1, β_2, β_3, β_4, β_5, β_6, if necessary, we can write

$$\alpha_1 + \beta_1 = \alpha_2 + \beta_{j_1}, \tag{18}$$

$$\alpha_1 + \beta_2 = \alpha_2 + \beta_{j_2}, \tag{19}$$

$$\alpha_1 + \beta_3 = \alpha_2 + \beta_{j_3}. \tag{20}$$

The indices j_1, j_2, j_3 in these equations are distinct. We claim that the set $\{j_1, j_2, j_3\}$ coincides with $\{4, 5, 6\}$. Indeed, assume the contrary, i.e., $\{j_1, j_2, j_3\} \cap \{1, 2, 3\} \neq \emptyset$. Then without loss of generality we can assume that $j_1 = 2$. Then (18) implies $\alpha_1 - \alpha_2 = \beta_2 - \beta_1$, whereas (19) implies $\alpha_1 - \alpha_2 = \beta_{j_2} - \beta_2$. So $\beta_2 - \beta_1 = \beta_{j_2} - \beta_2$, and therefore $2\beta_2 = \beta_1 + \beta_{j_2}$, contradicting Lemma 9.

Now, since $\{j_1, j_2, j_3\} = \{4, 5, 6\}$, after re-indexing the numbers β_4, β_5, β_6, if necessary, we obtain

$$\begin{aligned} \alpha_1 + \beta_1 &= \alpha_2 + \beta_4, \\ \alpha_1 + \beta_2 &= \alpha_2 + \beta_5, \\ \alpha_1 + \beta_3 &= \alpha_2 + \beta_6. \end{aligned} \tag{21}$$

Similarly, since $|\Gamma_1 \cap \Gamma_3| = 3$, we must have

$$\begin{aligned} \alpha_1 + \beta_{i_1} &= \alpha_3 + \beta_{j_1}, \\ \alpha_1 + \beta_{i_2} &= \alpha_3 + \beta_{j_2}, \\ \alpha_1 + \beta_{i_3} &= \alpha_3 + \beta_{j_3}, \end{aligned} \tag{22}$$

with $\{i_1, i_2, i_3, j_1, j_2, j_3\} = \{1, 2, 3, 4, 5, 6\}$. We claim that $\{i_1, i_2, i_3\} = \{4, 5, 6\}$. Indeed, if, say $i_1 \in \{1, 2, 3\}$ then $\alpha_1 + \beta_{i_1} \in \Gamma_1 \cap \Gamma_2 \cap \Gamma_3$.

However, this is impossible, because

$$\begin{aligned}|\Gamma_1 \cap \Gamma_2 \cap \Gamma_3| &= |\Gamma_1 \cup \Gamma_2 \cup \Gamma_3| - |\Gamma_1| - |\Gamma_2| - |\Gamma_3| + |\Gamma_1 \cap \Gamma_2| \\ &\quad + |\Gamma_1 \cap \Gamma_3| + |\Gamma_2 \cap \Gamma_3| \\ &= 9 - 6 - 6 - 6 + 3 + 3 + 3 = 0.\end{aligned}$$

So $i_1 \in \{4,5,6\}$. Analogously, $i_2, i_3 \in \{4,5,6\}$, so that $\{i_1,i_2,i_3\} = \{4,5,6\}$. Consequently, $\{j_1,j_2,j_3\} = \{1,2,3\}$ and, after rearranging the equalities in (22), we obtain

$$\begin{aligned}\alpha_1 + \beta_4 &= \alpha_3 + \beta_{k_1}, \\ \alpha_1 + \beta_5 &= \alpha_3 + \beta_{k_2}, \\ \alpha_1 + \beta_6 &= \alpha_3 + \beta_{k_3},\end{aligned} \tag{23}$$

where $\{k_1,k_2,k_3\} = \{1,2,3\}$.

Finally, by adding all six equalities in (21) and (23), we obtain

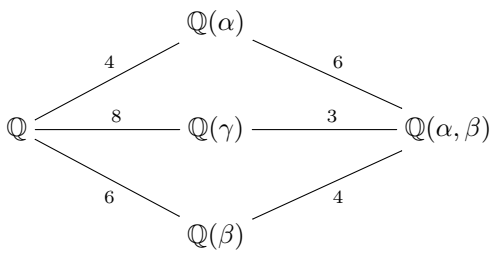
$$6\alpha_1 + \sum_{i=1}^{6} \beta_i = 3\alpha_2 + 3\alpha_3 + \sum_{i=1}^{6} \beta_i.$$

Thus $2\alpha_1 = \alpha_2 + \alpha_3$, which contradicts Lemma 9. □

Remark 34. Recall that the triplet $(3,2,3)$ is product-feasible (see Section 1 and Theorem 8). The triplet $(1,3,3)$ satisfies the exponent triangle inequality with respect to any prime number. Hence $(3,6,9) = (3,2,3)\cdot(1,3,3)$ is product-feasible, by Proposition 28. Since 6 does not divide 9, the triplet $(3,6,9)$ is not compositum-feasible.

Theorem 35. *The triplet* $(4,6,8)$ *is not sum-feasible.*

Proof: Suppose that $(4,6,8)$ is sum-feasible, so that there exist algebraic numbers α, β, γ of degrees 4, 6, 8, respectively, such that $\alpha+\beta+\gamma = 0$. The degree of $\mathbb{Q}(\alpha,\beta)$ over $\mathbb{Q}$ is divisible by 8, because $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha+\beta)$ is a subfield of $\mathbb{Q}(\alpha,\beta)$. Similarly, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$ is divisible by 6, because $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha,\beta)$. On the other hand, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] \leqslant [\mathbb{Q}(\alpha):\mathbb{Q}]\cdot[\mathbb{Q}(\beta):\mathbb{Q}] = 24$. Hence $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = 24$ and we have the following diagram.



Let α_1, α_2, α_3, α_4 be the distinct conjugates of α over $\mathbb{Q}$. Similarly, let β_1, β_2, β_3, β_4, β_5, β_6 be the distinct conjugates of β over $\mathbb{Q}$. By the diagram, β is of degree 6 over $\mathbb{Q}(\alpha)$. By Proposition 21, all 24 (not necessarily distinct) numbers $\alpha_i+\beta_j$, $1 \leqslant i \leqslant 4$, $1 \leqslant j \leqslant 6$, are conjugate over $\mathbb{Q}$. Set

$$\Gamma_i = \{\alpha_i+\beta_1, \alpha_i+\beta_2, \alpha_i+\beta_3, \alpha_i+\beta_4, \alpha_i+\beta_5, \alpha_i+\beta_6\}, \quad i = 1,2,3,4.$$

We have $|\Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \cup \Gamma_4| = 8$, because the number $\alpha+\beta = -\gamma$ is of degree 8 over $\mathbb{Q}$.

If $|\Gamma_1 \cap \Gamma_2| \leqslant 3$ then

$$8 = |\Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \cup \Gamma_4| \geqslant |\Gamma_1 \cup \Gamma_2| = |\Gamma_1| + |\Gamma_2| - |\Gamma_1 \cap \Gamma_2| \geqslant 6+6-3 = 9,$$

a contradiction. Hence $|\Gamma_1 \cap \Gamma_2| \geqslant 4$. However, then we get a contradiction in exactly the same way as in the proof of Theorem 33. (See the proof of inequality (17); the degree of β over $\mathbb{Q}$ is 6 as in Theorem 33, and we only use two distinct conjugates of α, i.e., α_1 and α_2.) □

Theorem 36. *The triplet* $(5,5,15)$ *is not compositum-feasible.*

Proof: It is known (see [**4**, p. 60]) that the Galois group of the splitting field of an irreducible polynomial of degree 5 is one of the following:

Table 3

Group	Generators	Order
S_5	(1 2 3 4 5), (1 2)	120
A_5	(1 2 3 4 5), (1 2 3)	60
$\mathrm{AGL}_1(5)$	(1 2 3 4 5), (2 3 5 4)	20
$\mathrm{ASL}_1(5)$	(1 2 3 4 5), (2 5)(3 4)	10
C_5	(1 2 3 4 5)	5

Assume the contrary, i.e., that the triplet $(5,5,15)$ is compositum-feasible. Then there exist algebraic numbers α and β such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = 15$.

Denote by K and L the Galois closures of $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ over $\mathbb{Q}$, respectively. If neither the Galois group of K nor the Galois group of L is in $\{A_5, S_5\}$ then both numbers $[K : \mathbb{Q}]$ and $[L : \mathbb{Q}]$ are in $\{5, 10, 20\}$. Then, by Lemma 12, the degree of the compositum

$$[KL : \mathbb{Q}] = \frac{[K : \mathbb{Q}] \cdot [L : \mathbb{Q}]}{[K \cap L : \mathbb{Q}]}$$

is not divisible by 3. This is impossible, because the compositum KL has a subfield $\mathbb{Q}(\alpha,\beta)$ of degree 15 over $\mathbb{Q}$. So either $K/\mathbb{Q}$ or $L/\mathbb{Q}$ has Galois group in $\{A_5, S_5\}$.

Assume without loss of generality that the Galois group of $K/\mathbb{Q}$ is A_5 or S_5. Now $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=15$ implies that α is cubic over $\mathbb{Q}(\beta)$ and β is cubic over $\mathbb{Q}(\alpha)$. Let $P(x)\in\mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. We have two possibilities:

(a) Two conjugates of α lie in $\mathbb{Q}(\beta)$, i.e.,

$$P(x)=(x-\alpha')(x-\alpha'')(x^3+ax^2+bx+c),$$

where $\alpha',\alpha''\in\mathbb{Q}(\beta)$ and $x^3+ax^2+bx+c\in\mathbb{Q}(\beta)[x]$ is irreducible over $\mathbb{Q}(\beta)$.

(b) No conjugate of α belongs to $\mathbb{Q}(\beta)$, i.e.,

$$P(x)=(x^2+ax+b)(x^3+cx^2+dx+e),$$

where both polynomials $x^2+ax+b\in\mathbb{Q}(\beta)[x]$ and $x^3+cx^2+dx+e\in\mathbb{Q}(\beta)[x]$ are irreducible over $\mathbb{Q}(\beta)$.

Assume that (a) holds. Then $\alpha'=f(\beta)$ for a certain polynomial $f(x)\in\mathbb{Q}[x]$. So $\mathbb{Q}(\beta)$ has a subfield $\mathbb{Q}(\alpha')=\mathbb{Q}(f(\beta))$ which is of degree 5 over $\mathbb{Q}$. Thus $\mathbb{Q}(\alpha')=\mathbb{Q}(\beta)$. Then $P(x)$ has exactly two linear factors over $\mathbb{Q}(\alpha')$, contradicting Lemma 13.

Suppose now that (b) holds. Denote the Galois group of $K/\mathbb{Q}$ by G. Recall that $G=A_5$ or S_5. Assume that G acts on the set $\{\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5\}$ of distinct conjugates of α as follows: if τ is a permutation of G then $\tau(\alpha_j)=\alpha_{\tau(j)}$, $j=1,2,3,4,5$.

Suppose that α' and α'', $\alpha'\neq\alpha''$, are the conjugates of α that are quadratic over $\mathbb{Q}(\beta)$. Then $\alpha'+\alpha''\in\mathbb{Q}(\beta)$ and there exists a polynomial $f(x)\in\mathbb{Q}[x]$ such that $\alpha'+\alpha''=f(\beta)$. Since A_5 and S_5 are both 2-transitive groups, there exists $\tau\in G$ such that $\tau(\alpha')=\alpha_1$ and $\tau(\alpha'')=\alpha_2$. Then

$$\alpha_1+\alpha_2=f(\beta_1), \tag{24}$$

where $\beta_1=\tau(\beta)$ is a conjugate of β over $\mathbb{Q}$. On applying the automorphisms id, (23)(45), (24)(35), (25)(34), (123), (124) $\in A_5\subseteq G$ to (24)

we obtain

$$\begin{aligned}
\alpha_1 + \alpha_2 &= f(\beta_1),\\
\alpha_1 + \alpha_3 &= f(\beta_2),\\
\alpha_1 + \alpha_4 &= f(\beta_3),\\
\alpha_1 + \alpha_5 &= f(\beta_4),\\
\alpha_2 + \alpha_3 &= f(\beta_5),\\
\alpha_2 + \alpha_4 &= f(\beta_6),
\end{aligned} \tag{25}$$

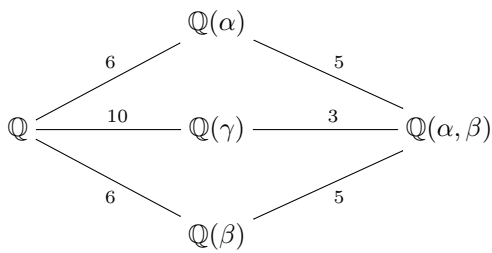
where β_1, β_2, β_3, β_4, β_5, β_6 are some conjugates of β. Since β is of degree 5 over $\mathbb{Q}$ then $\beta_i = \beta_j$ for some $i \neq j$. Then ith and jth lines of (25) imply that there is a nontrivial additive relation connecting at most 4 conjugates of α, contradicting Lemma 11. □

Corollary 37. *The triplet* $(5, 5, 15)$ *is neither sum-feasible nor product-feasible.*

Proof: Suppose that $(5, 5, 15)$ is either sum-feasible or product-feasible, with algebraic numbers α, β, γ of degrees 5, 5, 15, respectively, such that $\alpha + \beta + \gamma = 0$ or $\alpha\beta\gamma = 1$. In both cases, the degree of $\mathbb{Q}(\alpha, \beta)$ over $\mathbb{Q}$ is divisible by 15, because $\mathbb{Q}(\gamma)$ is a subfield of $\mathbb{Q}(\alpha, \beta)$. On the other hand, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leqslant [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = 25$. So $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 15$, contradicting Theorem 36. □

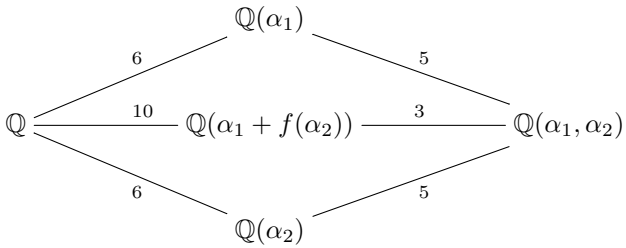
Theorem 38. *The triplet* $(6, 6, 10)$ *is not sum-feasible.*

Proof: Suppose that $(6, 6, 10)$ is sum-feasible, with algebraic numbers α, β, γ of degrees 6, 6, 10, respectively, such that $\alpha + \beta + \gamma = 0$. The degree of $\mathbb{Q}(\alpha, \beta)$ over $\mathbb{Q}$ is divisible by 10, because $\mathbb{Q}(\gamma) = \mathbb{Q}(\alpha + \beta)$ is a subfield of $\mathbb{Q}(\alpha, \beta)$. Similarly, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is divisible by 6, because $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$. Hence $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is divisible by 30. On the other hand, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leqslant [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = 36$. Consequently, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 30$ and we have the following diagram.

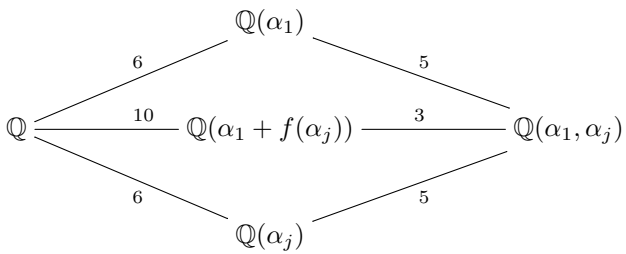


We see that β is of degree 5 over $\mathbb{Q}(\alpha)$. Hence β has exactly one conjugate, say, β_1, which lies in $\mathbb{Q}(\alpha)$. So $\beta_1 = f(\alpha)$ for certain polynomial $f(x) \in \mathbb{Q}[x]$ of degree at most 4. Let β_1, β_2, β_3, β_4, β_5, β_6 be all the distinct conjugates of β over $\mathbb{Q}$. For every $j = 1, 2, \dots, 6$ there exists an automorphism σ_j of the Galois group of $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ which sends β_1 to β_j. On applying σ_j to $\beta_1 = f(\alpha)$ we obtain $\beta_j = f(\alpha_j)$, $j = 1, 2, \dots, 6$. Here $\alpha_1 = \alpha$, α_2, α_3, α_4, α_5, α_6 are the (distinct) conjugates of α. Assume without loss of generality that $\beta = \beta_2 = f(\alpha_2)$. Then $-\gamma = \alpha_1 + f(\alpha_2)$.

The number field $\mathbb{Q}(\alpha_2)$ has a subfield $\mathbb{Q}(f(\alpha_2)) = \mathbb{Q}(\beta_2)$ of degree 6 over $\mathbb{Q}$. Therefore, $\mathbb{Q}(\beta) = \mathbb{Q}(f(\alpha_2)) = \mathbb{Q}(\alpha_2)$ and we obtain the following diagram.



Similarly, $\mathbb{Q}(\beta_j) = \mathbb{Q}(f(\alpha_j)) = \mathbb{Q}(\alpha_j)$ for $j = 1, 2, \dots, 6$. We claim that each α_i is of degree 5 over every $\mathbb{Q}(\alpha_j)$, $j \in \{1, 2, \dots, 6\} \setminus \{i\}$. Indeed, fix $j \in \{2, 3, 4, 5, 6\}$. Since α_2 is of degree 5 over $\mathbb{Q}(\alpha_1)$ (see the last diagram), the number α_j is conjugate to α_2 over the field $\mathbb{Q}(\alpha_1)$. Hence there exists an automorphism σ of the Galois group of $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$ which fixes α_1 and sends α_2 to α_j. Thus $\sigma(-\gamma) = \sigma(\alpha_1 + f(\alpha_2)) = \alpha_1 + f(\alpha_j)$ is a conjugate of $-\gamma$. It follows that $\alpha_1 + f(\alpha_j)$ is of degree 10 over $\mathbb{Q}$, and therefore we have the following diagram. (Recall that, as above, $\mathbb{Q}(\beta_j) = \mathbb{Q}(f(\alpha_j)) = \mathbb{Q}(\alpha_j)$.)



Now, we see that α_1 is of degree 5 over $\mathbb{Q}(\alpha_j)$ and all the numbers in $\{\alpha_1, \alpha_2, \dots, \alpha_6\} \setminus \{\alpha_j\}$ are conjugate to α_1 over $\mathbb{Q}(\alpha_j)$. Therefore,

each α_i, $i \in \{1, 2, \ldots, 6\} \setminus \{j\}$, is of degree 5 over $\mathbb{Q}(\alpha_j)$. Consequently, all the numbers $\alpha_i + f(\alpha_j)$, where $i \neq j$, are conjugate over $\mathbb{Q}$.

Consider the following table of numbers which are conjugate to $\alpha_1 + f(\alpha_2) = -\gamma$.

$$
\begin{array}{lllll}
\alpha_1 + f(\alpha_2) & & & & \\
\alpha_1 + f(\alpha_3) & \alpha_2 + f(\alpha_3) & & & \\
\alpha_1 + f(\alpha_4) & \alpha_2 + f(\alpha_4) & \alpha_3 + f(\alpha_4) & & \\
\alpha_1 + f(\alpha_5) & \alpha_2 + f(\alpha_5) & \alpha_3 + f(\alpha_5) & \alpha_4 + f(\alpha_5) & \\
\alpha_1 + f(\alpha_6) & \alpha_2 + f(\alpha_6) & \alpha_3 + f(\alpha_6) & \alpha_4 + f(\alpha_6) & \alpha_5 + f(\alpha_6).
\end{array} \tag{26}
$$

The table contains 15 numbers, while the degree of $-\gamma$ over $\mathbb{Q}$ is 10. Hence

$$\alpha_a + f(\alpha_b) = \alpha_c + f(\alpha_t) \tag{27}$$

with certain $a < b$, $c < t$ and either $a \neq c$ or $b \neq t$ (because $\deg f \leqslant 4$). We claim that $a \neq c$ and $b \neq t$. Indeed, if $b = t$ then $\alpha_a = \alpha_c$, and therefore $a = c$, which is impossible. Similarly, if $a = c$ then $f(\alpha_b) = f(\alpha_t)$ which implies $\beta_b = \beta_t$, and hence $b = t$, a contradiction. So $a \neq c$ and $b \neq t$. Assume without loss of generality that $a < c$. Then $a < c < t$, and therefore $t \notin \{a, b, c\}$.

Consider the Galois group G of the normal closure of $\mathbb{Q}(\alpha_1)$ over $\mathbb{Q}$ as acting as a subgroup of S_6 on the set of indices $\{1, 2, 3, 4, 5, 6\}$, i.e., if $\sigma \in G$ then $\sigma(\alpha_j) = \alpha_{\sigma(j)}$, $j = 1, 2, 3, 4, 5, 6$. The order of G is divisible by 5, because $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] = 30$. By Cauchy's Theorem (see, e.g., [**17**, Section 40, Theorem 2]), there exists an automorphism $\tau \in G$ of order 5 in G. Then τ (an element of S_6) is a cycle, say, $\tau = (i_1\, i_2\, i_3\, i_4\, i_5)$ with distinct numbers $i_1, i_2, i_3, i_4, i_5 \in \{1, 2, 3, 4, 5, 6\}$. Assume without loss of generality that $6 \notin \{i_1, i_2, i_3, i_4, i_5\}$. There exists an automorphism σ in G which maps α_t to α_6. On applying σ to (27) we obtain

$$\alpha_i + f(\alpha_j) = \alpha_k + f(\alpha_6) \tag{28}$$

with $i, j, k \in \{1, 2, 3, 4, 5\}$. Now, from (28) and $\tau(\alpha_6) = \alpha_6$ we deduce that

$$
\begin{aligned}
&\alpha_{\tau(i)} + f(\alpha_{\tau(j)}) = \alpha_{\tau(k)} + f(\alpha_6),\\
&\alpha_{\tau^2(i)} + f(\alpha_{\tau^2(j)}) = \alpha_{\tau^2(k)} + f(\alpha_6),\\
&\alpha_{\tau^3(i)} + f(\alpha_{\tau^3(j)}) = \alpha_{\tau^3(k)} + f(\alpha_6),\\
&\alpha_{\tau^4(i)} + f(\alpha_{\tau^4(j)}) = \alpha_{\tau^4(k)} + f(\alpha_6).
\end{aligned} \tag{29}
$$

The orbits

$$\begin{aligned}&\{i, \quad \tau(i), \quad \tau^2(i), \quad \tau^3(i), \quad \tau^4(i)\},\\ &\{j, \quad \tau(j), \quad \tau^2(j), \quad \tau^3(j), \quad \tau^4(j)\},\\ &\{k, \quad \tau(k), \quad \tau^2(k), \quad \tau^3(k), \quad \tau^4(k)\}\end{aligned}$$

coincide with the set $\{1,2,3,4,5\}$, because $\{i,j,k\} \subset \{i_1,i_2,i_3,i_4,i_5\}$. Thus adding (28) and all four equalities of (29) we find that

$$\sum_{i=1}^{5} \alpha_i + \sum_{i=1}^{5} f(\alpha_i) = \sum_{i=1}^{5} \alpha_i + 5f(\alpha_6),$$

and hence

$$\begin{aligned}6\beta_6 = 6f(\alpha_6) &= f(\alpha_1) + f(\alpha_2) + f(\alpha_3) + f(\alpha_4) + f(\alpha_5) + f(\alpha_6)\\ &= \beta_1 + \beta_2 + \beta_3 + \beta_4 + \beta_5 + \beta_6 \in \mathbb{Q},\end{aligned}$$

a contradiction. □

Proof of Theorem 5 (impossibility): Recall that if a triplet $(a,b,c) \in \mathbb{N}^3$ is sum-feasible then $c \leqslant ab$. Denote by $\mathcal{A}$ the set of triplets (a,b,c) of positive integers satisfying $a \leqslant b \leqslant c$, $b \leqslant 6$ and $c \leqslant ab$. The set $\mathcal{A}$ contains

$$\sum_{b=1}^{6}\sum_{a=1}^{b}(ab-b+1) = \sum_{b=1}^{6}(b^2(b+1)/2 - b(b-1)) = \frac{1}{2}\sum_{b=1}^{6} b(b^2-b+2)$$

$$= \frac{1}{2}\big(2+8+24+56+110+192\big) = 196 \text{ triplets.}$$

Let $\mathcal{T}$ be the set of triplets given in the Table 1. It contains 45 triplets (including $(6,6,8)$). At the end of the previous section we showed that each triplet in $\mathcal{T}$, except perhaps for $(6,6,8)$, is sum-feasible. So it remains to prove that none of the $196 - 45 = 151$ triplets in $\mathcal{A} \setminus \mathcal{T}$ is sum-feasible.

We first distinguish the set of 4 special triplets $\mathcal{S}$ defined in (12). The triplets of this set $(3,6,9)$, $(4,6,8)$, $(5,5,15)$ and $(6,6,10)$ are not sum-feasible by Theorem 33, Theorem 35, Corollary 37 and Theorem 38, respectively.

So we are left with the set $\mathcal{A} \setminus (\mathcal{T} \cup \mathcal{S})$ consisting of $151 - 4 = 147$ triplets. We next show that each triplet from the set $\mathcal{A} \setminus (\mathcal{T} \cup \mathcal{S})$ is not sum-feasible either by Proposition 2 or by Lemma 14. Those triplets in $\mathcal{A} \setminus (\mathcal{T} \cup \mathcal{S})$ that are not sum-feasible by Proposition 2 are given in Table 4. In each case, the triplet contains a pair of coprime numbers but the third number is not their product.

Table 4. Triplets that are not sum-feasible by Proposition 2.

$(2,2,3)$	$(2,3,3)$	$(2,3,4)$	$(2,3,5)$	$(2,4,5)$	$(2,4,7)$	$(2,5,5)$	$(2,5,6)$
$(2,5,7)$	$(2,5,8)$	$(2,5,9)$	$(2,6,7)$	$(2,6,9)$	$(2,6,11)$		
$(3,3,4)$	$(3,3,5)$	$(3,3,7)$	$(3,3,8)$	$(3,4,4)$	$(3,4,5)$	$(3,4,6)$	$(3,4,7)$
$(3,4,8)$	$(3,4,9)$	$(3,4,10)$	$(3,4,11)$	$(3,5,5)$	$(3,5,6)$	$(3,5,7)$	$(3,5,8)$
$(3,5,9)$	$(3,5,10)$	$(3,5,11)$	$(3,5,12)$	$(3,5,13)$	$(3,5,14)$	$(3,6,7)$	$(3,6,8)$
$(3,6,10)$	$(3,6,11)$	$(3,6,13)$	$(3,6,14)$	$(3,6,16)$	$(3,6,17)$		
$(4,4,5)$	$(4,4,7)$	$(4,4,9)$	$(4,4,11)$	$(4,4,13)$	$(4,4,15)$	$(4,5,5)$	$(4,5,6)$
$(4,5,7)$	$(4,5,8)$	$(4,5,9)$	$(4,5,10)$	$(4,5,11)$	$(4,5,12)$	$(4,5,13)$	$(4,5,14)$
$(4,5,15)$	$(4,5,16)$	$(4,5,17)$	$(4,5,18)$	$(4,5,19)$	$(4,6,7)$	$(4,6,9)$	$(4,6,11)$
$(4,6,13)$	$(4,6,15)$	$(4,6,17)$	$(4,6,19)$	$(4,6,21)$	$(4,6,23)$		
$(5,5,6)$	$(5,5,7)$	$(5,5,8)$	$(5,5,9)$	$(5,5,11)$	$(5,5,12)$	$(5,5,13)$	$(5,5,14)$
$(5,5,16)$	$(5,5,17)$	$(5,5,18)$	$(5,5,19)$	$(5,5,21)$	$(5,5,22)$	$(5,5,23)$	$(5,5,24)$
$(5,6,6)$	$(5,6,7)$	$(5,6,8)$	$(5,6,9)$	$(5,6,10)$	$(5,6,11)$	$(5,6,12)$	$(5,6,13)$
$(5,6,14)$	$(5,6,15)$	$(5,6,16)$	$(5,6,17)$	$(5,6,18)$	$(5,6,19)$	$(5,6,20)$	$(5,6,21)$
$(5,6,22)$	$(5,6,23)$	$(5,6,24)$	$(5,6,25)$	$(5,6,26)$	$(5,6,27)$	$(5,6,28)$	$(5,6,29)$
$(6,6,7)$	$(6,6,11)$	$(6,6,13)$	$(6,6,17)$	$(6,6,19)$	$(6,6,23)$	$(6,6,25)$	$(6,6,29)$
$(6,6,31)$	$(6,6,35)$						

There are exactly 124 triplets in Table 4. It remains to check the 'surviving' $147 - 124 = 23$ triplets that are in $\mathcal{A} \setminus (\mathcal{T} \cup \mathcal{S})$ but not in Table 4. These are listed in Table 5.

Table 5. The 23 triplets that are not sum-feasible by Lemma 14.

$(2,4,6)$	$(2,6,8)$	$(2,6,10)$					
$(3,6,15)$							
$(4,4,10)$	$(4,4,14)$	$(4,6,10)$	$(4,6,14)$	$(4,6,16)$	$(4,6,18)$	$(4,6,20)$	$(4,6,22)$
$(6,6,14)$	$(6,6,16)$	$(6,6,20)$	$(6,6,21)$	$(6,6,22)$	$(6,6,26)$	$(6,6,27)$	$(6,6,28)$
$(6,6,32)$	$(6,6,33)$	$(6,6,34)$					

One can easily check that each of those triplets is not sum-feasible, by Lemma 14. □

Remark 39. Recall that triplet $(3,3,2)$ is product-feasible (see Section 1). The triplet $(2,2,4)$ satisfies the exponent triangle inequality with respect to any prime number. Hence the triplet $(6,6,8) = (3,3,2) \cdot (2,2,4)$ is product-feasible, by Proposition 28.

Acknowledgements. We thank A. Schinzel for providing several useful references. The first-named author acknowledges a postdoctoral fellowship funded by European Union Structural Funds project "Postdoctoral Fellowship Implementation in Lithuania".

References

[1] G. Baron, M. Drmota, and M. Skałba, Polynomial relations between polynomial roots, *J. Algebra* **177(3)** (1995), 827–846. DOI: 10.1006/jabr.1995.1330.

[2] J. Browkin, B. Diviš, and A. Schinzel, Addition of sequences in general fields, *Monatsh. Math.* **82(4)** (1976), 261–268. DOI: 10.1007/BF01540597.

[3] S. D. Cohen, A. Movahhedi, and A. Salinier, Double transitivity of Galois groups of trinomials, *Acta Arith.* **82(1)** (1997), 1–15.

[4] J. D. Dixon and B. Mortimer, *"Permutation groups"*, Graduate Texts in Mathematics **163**, Springer-Verlag, New York, 1996.

[5] M. Drmota and M. Skałba, On multiplicative and linear independence of polynomial roots, in: *"Contributions to general algebra"*, 7 (Vienna, 1990), Hölder-Pichler-Tempsky, Vienna, 1991, pp. 127–135.

[6] P. Drungilas, A. Dubickas, and F. Luca, On the degree of the compositum of two number fields, submitted.

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

[8] A. Dubickas, Two exercises concerning the degree of the product of algebraic numbers, *Publ. Inst. Math. (Beograd) (N.S.)* **77(91)** (2005), 67–70. DOI: 10.2298/PIM0591067D.

[9] A. Dubickas and C. J. Smyth, Variations on the theme of Hilbert's Theorem 90, *Glasg. Math. J.* **44(3)** (2002), 435–441. DOI: 10.1017/S0017089502030082.

[10] D. Hilbert, *"The theory of algebraic number fields"*, Translated from the German and with a preface by Iain T. Adamson. With an introduction by Franz Lemmermeyer and Norbert Schappacher, Springer-Verlag, Berlin, 1998.

[11] I. M. Isaacs, Degrees of sums in a separable field extension, *Proc. Amer. Math. Soc.* **25** (1970), 638–641. DOI: 10.1090/S0002-9939-1970-0258803-3.

[12] J. Jahnel, When is the (co)sine of a rational angle equal to a rational number? Preprint (2010), arXiv:1006.2938v1 [math.HO].

[13] C. Jensen, A. Ledet, and N. Yui, *"Generic polynomials"*. Constructive aspects of the inverse Galois problem, Mathematical Sciences Research Institute Publications **45**, Cambridge University Press, Cambridge, 2002.

[14] C. U. Jensen and N. Yui, Polynomials with D_p as Galois group, *J. Number Theory* **15(3)** (1982), 347–375. DOI: 10.1016/0022-314X(82)90038-5.

[15] I. Kaplansky, *"Fields and rings"*, The University of Chicago Press, Chicago, Ill.-London, 1969.

[16] S. Lang, *"Algebra"*, Revised third edition, Graduate Texts in Mathematics **211**, Springer-Verlag, New York, 2002.

[17] W. Ledermann, *"Introduction to the theory of finite groups"*, 2d ed., Oliver and Boyd, Edinburgh and London; Interscience Publishers, Inc., New York, 1953.

[18] A. Ledet, Dihedral extensions in characteristic 0, *C. R. Math. Acad. Sci. Soc. R. Can.* **21(2)** (1999), 46–52.

[19] M. R. Murty and J. Esmonde, *"Problems in algebraic number theory"*, Second edition, Graduate Texts in Mathematics **190**, Springer-Verlag, New York, 2005.

[20] W. Narkiewicz, *"Elementary and analytic theory of algebraic numbers"*, Third edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.

[21] A. R. Perlis, Roots appear in quanta, *Amer. Math. Monthly* **111(1)** (2004), 61–63. DOI: 10.2307/4145020.

[22] C. L. Siegel, *"Über einige Anwendungen diophantischer Approximationen"*, Abh. Preuss. Akad. Wiss., 1929.

[23] C. J. Smyth, Conjugate algebraic numbers on conics, *Acta Arith.* **40(4)** (1981/82), 333–346.

[24] C. J. Smyth, Additive and multiplicative relations connecting conjugate algebraic numbers, *J. Number Theory* **23(2)** (1986), 243–254. DOI: 10.1016/0022-314X(86)90094-6.

[25] J. L. Varona, Rational values of the arccosine function, *Cent. Eur. J. Math.* **4(2)** (2006), 319–322 (electronic). DOI: 10.2478/s11533-006-0011-z.

Paulius Drungilas and Artūras Dubickas:
Department of Mathematics and Informatics
Vilnius University
Naugarduko 24
Vilnius LT-03225
Lithuania
E-mail address: pdrungilas@gmail.com
E-mail address: arturas.dubickas@mif.vu.lt

Chris Smyth:
School of Mathematics and
Maxwell Institute for Mathematical Science
University of Edinburgh
Edinburgh EH9 3JZ
Scotland, UK
E-mail address: c.smyth@ed.ac.uk

Primera versió rebuda el 14 de setembre de 2011,
darrera versió rebuda el 23 de setembre de 2011.