mathematics

MDPI

Article

On the Degree of Product of Two Algebraic Numbers

Lukas Maciulevičius

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

Abstract: A triplet (a, b, c) of positive integers is said to be product-feasible if there exist algebraic numbers α, β and γ of degrees (over $\mathbb{Q}$) a, b and c, respectively, such that $\alpha\beta\gamma = 1$. This work extends the investigation of product-feasible triplets started by Drungilas, Dubickas and Smyth. More precisely, for all but five positive integer triplets (a, b, c) with $a \leq b \leq c$ and $b \leq 7$, we decide whether it is product-feasible. Moreover, in the Appendix we give an infinite family or irreducible compositum-feasible triplets and propose a problem to find all such triplets.

Keywords: algebraic numbers; product-feasible; compositum-feasible; subgroups of symmetric groups

MSC: 11R04; 11R32

1. Introduction

Following [1], we say that a triplet $(a, b, c) \in \mathbb{N}^3$ is *sum-feasible* (resp., *product-feasible*) if there exist algebraic numbers α, β, γ of degrees a, b, c (over $\mathbb{Q}$), respectively, such that $\alpha + \beta + \gamma = 0$ (resp., $\alpha\beta\gamma = 1$). In [1], the problem of finding all sum-feasible triplets was proposed. In the same paper and in its continuations [2–4], an analogous problem for number fields was considered. Namely, we say that a triplet $(a, b, c) \in \mathbb{N}^3$ is *compositum-feasible* if there exist number fields K and L of degrees a and b (over $\mathbb{Q}$), respectively, such that the degree of their compositum KL is c. All sum-feasible triplets $(a, b, c) \in \mathbb{N}^3$, satisfying $a \leq b \leq c$, $b \leq 7$, and all possible compositum-feasible triplets (a, b, c), satisfying $a \leq b \leq c$, $b \leq 9$, were determined in [1,2,4]. Moreover, it was proved in [1,4] that the three feasibility problems are related in the following way: if $\mathcal{C}$, $\mathcal{S}$ and $\mathcal{P}$ denote sets of all possible compositum-feasible, sum-feasible and product-feasible triplets, respectively, then

$$\mathcal{C} \subsetneq \mathcal{S} \subsetneq \mathcal{P}. \tag{1}$$

Therefore all sum-feasible triplets that were found in the preceding papers are also product-feasible, but they do not exhaust *all* possible product-feasible triplets (a, b, c) for which $a \leq b \leq c$ and $b \leq 7$. There comes a natural motivation to investigate the case of the product more closely.

In this paper, we consider product-feasible triplets (a, b, c) under the same restrictions $a \leq b \leq c$, $b \leq 7$. More precisely, we prove the following:

Theorem 1. *All the triplets $(a, b, c) \in \mathbb{N}^3$ with $a \leq b \leq c$, $b \leq 7$ that are product-feasible are given in Table 1, with five possible exceptions that are circled.*

Citation: Maciulevičius, L. On the Degree of Product of Two Algebraic Numbers. *Mathematics* **2023**, *11*, 2131. https://doi.org/10.3390/math11092131

Academic Editor: Li Guo

Received: 13 March 2023
Revised: 25 April 2023
Accepted: 28 April 2023
Published: 2 May 2023

Table 1. Triplets (a, b, c), $a \leq b \leq c$, and $b \leq 7$, which are product-feasible with 5 possible exceptions.

$b \backslash a$	1	2	3	4	5	6	7
1	1						
2	2	2, 4					
3	3	3, 6	3, 6, 9				
4	4	4, 8	6, 12	4, 6, 8, 12, 16			
5	5	10	15	5, 10, 20	5, 10, 20, 25		
6	6	6, 12	6, 9, 12, 18	6, 8 12, 24	10, 15 30	6, 8, 9, 12, 15, 18, 24, 30, 36	
7	7	14	21	7, 14 28	35	7, 14, 21, 42	7, 14, 21, 28, 42, 49

Moreover, we obtain several results related to triplets that include prime components.

Theorem 2. *The triplet $(n-1, n, n)$, $n \geq 2$, is product-feasible if and only if n is a prime number.*

In [1] (Theorem 8), it was proved that the triplet $(2, t, t) \in \mathbb{N}^3$ is product-feasible if and only if $2|t$ or $3|t$. We obtain an analogous result for triplets $(p, t, t) \in \mathbb{N}^3$, where $p > 2$ is a prime number.

Theorem 3. *Suppose a prime number p and a positive integer t satisfy $t \geq p > 2$. Then, the triplet (p, t, t) is product-feasible if and only if $p|t$.*

The following theorem, taking $d = 1$, implies the sufficiency part of Theorem 2.

Theorem 4. *For any prime number p and each divisor d of $p-1$, the triplet $(p-1, p, pd)$ is product-feasible.*

It was conjectured in [1] that the set $\mathcal{C}$ of compositum-feasible triplets is a multiplicative semigroup, i.e., if $(a, b, c), (a', b', c') \in \mathcal{C}$, then $(aa', bb', cc') \in \mathcal{C}$. This conjecture was proved in [3] (Theorem 1.3) assuming the answer to the inverse Galois problem is positive, i.e., that every finite group occurs as a Galois group of some normal field extension of $\mathbb{Q}$. Therefore, it is natural to consider irreducible elements of $\mathcal{C}$. In Appendix A, we give an infinite family of irreducible elements of $\mathcal{C}$ (see Proposition A1). Finally, at the end of Appendix A, we propose a problem of finding all irreducible compositum-feasible triplets.

The paper is organized as follows. The proof of Theorem 1 is given in Section 3 and is based on Theorems 2–4. In Section 2, we state some auxiliary results. Appendix A is devoted to irreducible elements of $\mathcal{C}$.

2. Auxiliary Results

Lemma 1 (Lemma 14, [1])**.** *Suppose that a triplet (a, b, c) is product-feasible. Then, $c \mid \operatorname{lcm}(a, b) \cdot t$ for some positive $t \leq \gcd(a, b)$.*

Lemma 2 (Proposition 19, [1])**.** *For any positive integers a and b, the triplet (a, b, ab) is compositum-feasible and hence both sum-feasible and product-feasible.*

Lemma 3 (Lemma 7, [4])**.** *Suppose that positive integers $a \leq b \leq c$ satisfy $ab < 2c$. Then, if the triplet $(a, b, c) \in \mathbb{N}^3$ is not compositum-feasible, then it is neither sum-feasible nor product-feasible.*

Lemma 4 (Theorem 8, [1])**.** *The triplet* $(2, t, t) \in \mathbb{N}^3$ *is product-feasible if and only if* $2|t$ *or* $3|t$*.*

Let p be a prime number and $n \in \mathbb{N}$. Denote by $\mathrm{ord}_p(n)$ the exponent to which p appears in the prime factorization of n (if $p \nmid n$ set $\mathrm{ord}_p(n) = 0$). We say that a triplet (a, b, c) satisfies the *exponent triangle inequality with respect to a prime p* if

$$\mathrm{ord}_p(a) + \mathrm{ord}_p(b) \geq \mathrm{ord}_p(c),\ \mathrm{ord}_p(a) + \mathrm{ord}_p(c) \geq \mathrm{ord}_p(b) \text{ and}$$
$$\mathrm{ord}_p(b) + \mathrm{ord}_p(c) \geq \mathrm{ord}_p(a).$$

Lemma 5 (Proposition 28, [1])**.** *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 product-feasible triplet* $(a', b', c') \in \mathbb{N}^3$*, the triplet* (aa', bb', cc') *is also product-feasible.*

Lemma 6 (Proposition 21, [1])**.** *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* $\alpha_i\beta_j$*,* $1 \leq i \leq m$*, and* $1 \leq j \leq n$ *are conjugate over* $\mathbb{Q}$ *(although not necessarily distinct).*

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

$$\prod_{i=1}^{n} \alpha_i^{k_i} \in \mathbb{Q},$$

where all the $k_j \in \mathbb{Q}$. We call this multiplicative relation *trivial* if $k_1 = k_2 = \cdots = k_n$.

Lemma 7 (Theorem 1, [5])**.** *Let* $p > 2$ *be a prime number and* $f(x) \in \mathbb{Q}[x]$ *an irreducible monic polynomial* $\neq x^p + a_0$ *of degree* p *over* $\mathbb{Q}$*. Then, there are no nontrivial multiplicative relations between the roots* $\alpha_1,\ \alpha_2, \ldots, \alpha_p$ *of* $f(x)$*.*

Lemma 8 (Problem 6523, [6])**.** *Suppose* $f(x)$ *is an irreducible polynomial of degree* d *over the field of rational numbers, and suppose* $f(x)$ *has two roots* α*,* β *with* $\frac{\alpha}{\beta}$ *a primitive nth root of unity. Then,* $\varphi(n) \leq d$*.*

Let G be a group acting transitively on a set S. If the cardinality of S equals $n \in \mathbb{N}$, we say G is a group of *degree n*. A nonempty subset $\Delta \subseteq S$ is called a *block* for G if for each $x \in G$ either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \emptyset$, here $\Delta^x = \{\delta^x : \delta \in \Delta\}$. Every group acting transitively on S has S and the singletons $\{\alpha\}$, $\alpha \in S$, as blocks. These are called the *trivial* blocks. Any other block is called *nontrivial*. For example, the cyclic group $G = \langle(1, 2, 3, 4, 5, 6)\rangle$ acting on $S = \{1, 2, 3, 4, 5, 6\}$ has nontrivial blocks $\{1, 4\}$, $\{2, 5\}$, $\{3, 6\}$, $\{1, 3, 5\}$, $\{2, 4, 6\}$ and in fact these are the only nontrivial blocks for G (see Exercise 1.5.2, [7]). We say that a group G acting transitively on a set S is *primitive* if G has no nontrivial blocks on S. For instance, the symmetric group S_n and the alternating group A_n acting on $S = \{1, 2, \ldots, n\}$ are primitive for any $n \in \mathbb{N}$. One more example—the cyclic group $G = \langle(1, 2, 3, 4, 5)\rangle$ acting on $S = \{1, 2, 3, 4, 5\}$ is primitive (see Lemma 9).

Lemma 9 (Theorem 8.3, [8])**.** *A transitive group of prime degree is primitive.*

Lemma 10 (Proposition 1, [4])**.** *Suppose that* $n > 4$ *is a positive integer and* $p > 2$ *is a prime number that is not a divisor of* $n - 1$*. Moreover, assume that* p *does not divide the order of any transitive subgroup of the symmetric group* S_n*, except possibly for* A_n *and* S_n*. Then, for any positive integer* $k > n$ *divisible by* p*, the triplet* (n, n, k) *is not product-feasible.*

Lemma 11 (Theorem 3.3, [7])**.** *Let G be a subgroup of the symmetric group S_n acting on the set $\{1, 2, \ldots, n\}$. Suppose that G is primitive and contains a cycle of length p, where p is a prime number. Then, either G contains the alternating group A_n as a subgroup, or $n \le p + 2$.*

Lemma 12 ([8] (Theorem 3.7) Special case of [8] (Theorem 3.7) taking any Sylow subgroup U of G and any $\alpha \in \operatorname{fix} U$.)**.** *In a transitive group G, the normalizer of every Sylow subgroup Q of G is transitive on the points left fixed by Q.*

Lemma 13 (N/C theorem, see, e.g., Example 2.2.2, [7])**.** *Let H be a subgroup of a group G. Then, $C_G(H) \lhd N_G(H)$ and the qoutient $N_G(H)/C_G(H)$ is isomorphic to some subgroup of $\operatorname{Aut} H$, here*

$$N_G(H) = \{g \in G : gH = Hg\} \text{ and } C_G(H) = \{g \in G : gh = hg \ \forall h \in H\}$$

are the normalizer and the centralizer of H in G, respectively.

3. Proofs

Proof of Theorem 2. *Necessity.* Suppose that the triplet $(n-1, n, n)$ is product-feasible. Then, there exist algebraic numbers α and β, such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n - 1$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = n$. Since $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are subfileds of $\mathbb{Q}(\alpha, \beta)$, we find that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is divisible both by $n-1$ and n. Then, $\gcd(n-1, n) = 1$ implies that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is divisible by $(n-1)n$. On the other hand, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \le [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}] = (n-1)n$. Hence, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = (n-1)n$ and we have the following diagram (see Figure 1):

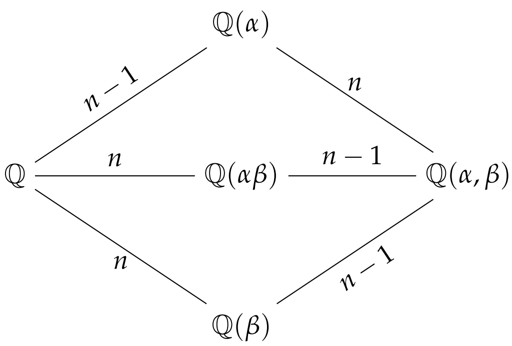

Figure 1. Diagram for $(n-1, n, n)$.

Let $\beta_1 := \beta, \beta_2, \ldots, \beta_n$ be the distinct conjugates of β over $\mathbb{Q}$. All the numbers

$$\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_n$$

are pairwise distinct and, by Lemma 6, they all are conjugate over $\mathbb{Q}$. Hence, these are all the algebraic conjugates of $\alpha\beta$. Consequently the product

$$(\alpha\beta_1) \cdots (\alpha\beta_n) = \alpha^n \beta_1 \beta_2 \cdots \beta_n$$

is a nonzero rational number. On the other hand, $\beta_1\beta_2 \cdots \beta_n \in \mathbb{Q} \setminus \{0\}$ too. So, α^n is a non-zero rational number, say r. Therefore, α is a root of the polynomial $x^n - r$. The minimal polynomial of α is of degree $n-1$ and divides the polynomial $x^n - r$. Hence, $x^n - r$ has a root that is a rational number, say r_0. Then, $r = r_0^n$. Assume that n is not a prime number. Then, there exist integers $a > 1$ and $b > 1$ such that $n = ab$. Note that

$$x^n - r = x^{ab} - r_0^{ab} = (x^a - r_0^a)(x^{a(b-1)} + \cdots + r_0^{a(b-1)}).$$

So, the minimal polynomial of α divides either $x^a - r_0^a$ or the polynomial $x^{a(b-1)} + \cdots + r_0^{a(b-1)}$. However, this is impossible since the degree of either of these polynomials is strictly less than $n-1$. Therefore, n is a prime number.

Sufficiency. Assume n is a prime number. Let ζ_n be the primitive nth root of unity. Then, the degree of $\alpha = \frac{1}{\zeta_n}$ equals $n-1$. The numbers $\beta = \sqrt[n]{2}\zeta_n$ and $\gamma = \frac{1}{\sqrt[n]{2}}$ are of degree n and $\alpha\beta\gamma = 1$. Hence, the triplet $(n-1, n, n)$ is product-feasible. $\square$

Proof of Theorem 3. *Necessity.* Assume that the triplet (p, t, t) is product-feasible. Suppose for the contrary, that $p \nmid t$. We have that there exist algebraic numbers α and β such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha\beta) : \mathbb{Q}] = t$. Since $\gcd(p, t) = 1$, we obtain similarly as in the proof of Theorem 2 the following diagram (see Figure 2):

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha) \arrow[dr, dash, "t"] & \\
\mathbb{Q} \arrow[ur, dash, "p"] \arrow[r, dash, "t"] \arrow[dr, dash, "t"'] & \mathbb{Q}(\alpha\beta) \arrow[r, dash, "p"] & \mathbb{Q}(\alpha,\beta) \\
 & \mathbb{Q}(\beta) \arrow[ur, dash, "p"'] &
\end{tikzcd}$$

Figure 2. Diagram for (p, t, t).

Using Lemma 6 analogously as in the proof of Theorem 2, we find that $\alpha^t \in \mathbb{Q}$. Hence, α is a root of a binomial equation $x^t - a = 0$, $a \in \mathbb{Q} \setminus \{0\}$. On the other hand, $\deg \alpha = p > 2$ is a prime number. Therefore, Lemma 7 implies that the minimal polynomial of α over $\mathbb{Q}$ is of the form $x^p - b$, $b \in \mathbb{Q} \setminus \{0\}$. We find that $x^t - a$ is divisible by $x^p - b$. Let $t = pq + r$, where q and r are non-negative integers and $r < p$. Since $t \geq p$ and $p \nmid t$, we find that $r > 0$ and $q > 0$. Note that

$$x^t - a = x^{pq+r} - a = (x^p - b + b)^q x^r - a \equiv b^q x^r - a \pmod{x^p - b}.$$

The remainder polynomial $b^q x^r - a$ is of degree $r > 0$, which is strictly less than p. Hence, $x^p - b$ does not divide the polynomial $x^t - a$. A contradiction. Therefore, t is divisible by p.

Sufficiency. Let $t \geq p > 2$ and $t = pk$ for some positive integer k. The triplet $(1, k, k)$ is obviously product-feasible, whereas the triplet (p, p, p) satisfies the exponent triangle inequality. By Lemma 5, the triplet $(p, t, t) = (p \cdot 1, p \cdot k, p \cdot k)$ is product-feasible. $\square$

Proof of Theorem 4. If $p = 2$, the assertion is obvious. If $d = p - 1$, our triplet is product-feasible by Lemma 2. Suppose that $d < p - 1$. Consider a field extension $\mathbb{Q}(\zeta_{2p}) : \mathbb{Q}$, here $\zeta_{2p} = e^{\frac{2\pi i}{2p}}$. As a cyclotomic extension, it is normal for degree $\varphi(2p) = p - 1$ and its Galois group G is isomorphic to the multiplicative group of the ring of residues modulo $2p$ (see, e.g., [9]), which means G is cyclic (Recall a well-known fact that the multiplicative group of the ring of residues modulo $n > 1$ is cyclic if and only if $n = 2, 4, p^\alpha$ or $2p^\alpha$ where $p > 2$ is prime and $\alpha \in \mathbb{N}$ (see, e.g., [10]).). Therefore, for every divisor d of $|G| = p - 1$, the group G has a unique subgroup of order $(p-1)/d$, say H. Let K be an intermediate field that corresponds to the subgroup H in the Galois correspondence, i.e., K consists of all elements of the field $\mathbb{Q}(\zeta_{2p})$, which are left invariant by every automorphism in H. Then, the degree of K over $\mathbb{Q}$ equals $|G|/|H| = d$. By the primitive element theorem $K = \mathbb{Q}(\theta)$ for some $\theta \in \mathbb{Q}(\zeta_{2p})$. Let g be a primitive root modulo $2p$. Then, the automorphism $\sigma \in G$ defined by

$$\sigma : \zeta_{2p} \mapsto \zeta_{2p}^g$$

generates G. We claim that $\deg(\theta\zeta_{2p}) = p-1$. It suffices to show that all the numbers

$$\sigma^k(\theta\zeta_{2p}),\ k = 1,2,\dots,p-1,$$

are distinct. Indeed, assume that $\sigma^k(\theta\zeta_{2p}) = \sigma^l(\theta\zeta_{2p})$ for some $1 \le k < l \le p-1$. So that $\sigma^k(\theta)\zeta_{2p}^{g^k} = \sigma^l(\theta)\zeta_{2p}^{g^l}$ and

$$\frac{\sigma^k(\theta)}{\sigma^l(\theta)} = e^{\frac{(g^l-g^k)\pi i}{p}}.$$

Note that $g^l - g^k = 2m$, where $p \nmid m$. Therefore, $\sigma^k(\theta)/\sigma^l(\theta)$ is a primitive pth root of unity, which contradicts Lemma 8 since $d < p-1$. Hence, $\deg(\theta\zeta_{2p}) = p-1$.

Finally, take

$$\alpha = \theta\zeta_{2p},\ \beta = \sqrt[p]{2},\ \gamma = \left(\sqrt[p]{2}e^{\frac{\pi i}{p}}\theta\right)^{-1}.$$

We have $\alpha\beta\gamma = 1$. It remains to show that $\deg\gamma = pd$. Let $\theta = \theta^{(1)}, \theta^{(2)}, \dots, \theta^{(d)}$ be all the conjugates of θ. Since the numbers $\deg(\sqrt[p]{2}e^{\frac{\pi i}{p}}) = p$ and $\deg\theta = d$ are coprime Lemma 6, it implies that all the numbers

$$\gamma_k^{(l)} := \left(\sqrt[p]{2}e^{\frac{\pi i}{p}}e^{\frac{2\pi ik}{p}}\theta^{(l)}\right)^{-1},\ k = 0,1,\dots,p-1,\ l = 1,2,\dots,d, \tag{2}$$

are conjugate to γ. It suffices to show that all these numbers are distinct. Indeed, assume that $\gamma_{k_1}^{(l_1)} = \gamma_{k_2}^{(l_2)}$, where $k_1, k_2 \in \{0,1,\dots,p-1\}$, $l_1, l_2 \in \{1,2,\dots,d\}$ and either $k_1 \ne k_2$ or $l_1 \ne l_2$. Note that if $k_1 = k_2$, then $l_1 = l_2$. Therefore, $k_1 \ne k_2$ and the equality $\gamma_{k_1}^{(l_1)} = \gamma_{k_2}^{(l_2)}$ implies

$$e^{\frac{2\pi i(k_1-k_2)}{p}} = \frac{\theta^{(l_2)}}{\theta^{(l_1)}}.$$

Since $e^{2\pi i(k_1-k_2)/p}$ is a primitive pth root of unity, by Lemma 8, we find that $p-1 = \varphi(p) \le \deg\theta = d$. This is a contradiction. Hence, all the numbers in (2) are distinct, and therefore $\deg\gamma = pd$. This completes the proof of the theorem. $\square$

Proposition 1. *The triplet $(6,6,10)$ is not product-feasible.*

Proof. The proof of [1] (Theorem 38) can be modified easily to the multiplicative case. Using same notations, we finally obtain $\beta_6^6 \in \mathbb{Q}$, hence the minimal polynomial of β is of the form $x^6 - r_2$, $r_2 \in \mathbb{Q}$. Interchanging α and β in the proof of [1] (Theorem 38), we find that the minimal polynomial of α is also of the form $x^6 - r_1$, $r_1 \in \mathbb{Q}$. Hence, $\alpha = \sqrt[6]{r_1}\varepsilon_6$ and $\beta = \sqrt[6]{r_2}\varepsilon_6'$, here ε_6 and ε_6' are some 6th roots of unity. This yields $\alpha\beta = \sqrt[6]{r_1r_2}\varepsilon_6\varepsilon_6'$ as a root of $x^6 - r_1r_2$, thus $\deg(\alpha\beta) \le 6$, a contradiction. $\square$

Proof of Theorem 1. Using Lemma 1, we determine all possible candidates to product-feasible triplets (a,b,c) with $a \le b \le c$, $b \le 7$. They are listed in Table 2.

Blue-colored triplets are sum-feasible, as is proved in [1,2]. Therefore, all these triplets are also product-feasible by (1).

Green-colored triplets are product-feasible too: $(2,3,3)$ is product-feasible by Lemma 4, the triplets $(3,6,9)$, $(3,4,6)$ and $(6,6,8)$ by Lemma 5, $(4,5,5)$ and $(6,7,7)$ by Theorem 2, whereas $(4,5,10)$, $(6,7,14)$, $(6,7,21)$ are product-feasible by Theorem 4 taking $(p,d) = (5,2)$, $(7,2)$ and $(7,3)$, respectively.

Red-colored triplets are not product-feasible: the triplets $(3,4,4)$, $(3,5,5)$, $(3,7,7)$, $(5,6,6)$ and $(5,7,7)$ are not product-feasible by Theorem 3, $(2,5,5)$, $(2,7,7)$ by Lemma 4, $(6,6,10)$ by Proposition 1, whereas $(5,5,15)$ and $(7,7,35)$ are not product-feasible by Lemma 3 and [2] (Corollary 1.5).

Table 2. Candidates to product-feasible triplets.

$b \backslash a$	1	2	3	4	5	6	7
1	1						
2	2	2, 4					
3	3	3, 6	3, 6, 9				
4	4	4, 8	4, 6, 12	4, 6, 8, 12, 16			
5	5	5, 10	5, 15	5, 10, 20	5, 10, 15 20, 25		
6	6	6, 12	6, 9, 12, 18	6, 8, 12, 24	6, 10, 15, 30	6, 8, 9, 10 12, 15, 18, 24, 30, 36	
7	7	7, 14	7, 21	7, 14, 28	7, 35	7, 14, 21, 42	7, 14, 21, 28, 35, 42, 49

The circled triplets have not been examined yet. □

Let p and n be a prime number and a positive integer, respectively. Suppose that the triplet (p, p, n) is product-feasible. If $p \nmid n$, then, by Lemma 1, we find that $n < p$. Hence, if $n > p$, then $p \mid n$. Finally, we give another result related to product-feasible triplets containing prime components.

Proposition 2. *Suppose p, q and w are prime numbers such that $2 < w < q < p$, $p = 2q + w$ and $w \not|(q-1)$. Then, both triplets (p, p, pq) and $(p, p, 2pq)$ are not product-feasible.*

For instance, none of the triplets $(19, 19, 19 \cdot 7k)$, $(29, 29, 29 \cdot 11k)$ and $(31, 31, 31 \cdot 13k)$, $k = 1, 2$, are product-feasible. Moreover, suppose that p, q and w satisfy the conditions of Proposition 2. Then, for any positive integer $t \geq 3$, the triplet (p, p, pqt) is not product-feasible, by Lemma 1.

Proof of the Proposition. Let G be a transitive subgroup of the symmetric group S_p such that $G \neq A_p$ and $G \neq S_p$. We will show that q cannot divide the order of G. Then, Lemma 10 will imply that the triplets (p, p, pq) and $(p, p, 2pq)$ both are not product-feasible. (Note that from $p = 2q + w$, $2 < w < q < p$, it follows that $q \not|(p-1)$.).

Suppose for the contrary that the order of G is divisible by a prime q. Denote by Q a Sylow q-subgroup of G. The order of Q equals q or q^2 since Q is a subgroup of S_p and $\operatorname{ord}_q |S_p| = \operatorname{ord}(p!) = q^2$. We claim that $|Q| = q$. Indeed, assume that $|Q| = q^2$. Then, Q is a Sylow q-subgroup of S_p, too. Take any cycle $\tau \in S_p$ of length q. Then, a cyclic subgroup $\langle \tau \rangle$ is contained in some Sylow q-subgroup of S_p. Since any two Sylow q-subgroups are conjugated and conjugate elements in S_p are of the same cyclic structure, we find that the subgroup Q of G also contains a cycle of length q. However, Lemma 9 implies G is primitive, therefore we obtain a contradiction by Lemma 11. Hence, $|Q| = q$, which means Q is a cyclic subgroup generated by an element $\sigma \in G$ of order q. If σ were a cycle of length q, we would obtain a contradiction by Lemma 11. Since $p = 2q + w < 3q$, it follows that σ must be a product of two disjoint cycles of length q, say, π and $\rho \in G$. Therefore, $|\operatorname{fix} Q| = p - 2q = w$, here $\operatorname{fix} Q := \{n \in \{1, 2, \ldots, p\} : n^\tau = n \ \forall \tau \in Q\}$.

Note that Lemma 12 implies the order of the normalizer $N_G(Q)$ is divisible by $|\operatorname{fix} Q| = w$, which is prime. Hence, there exists an element $\tau \in N_G(Q)$ of order w. We claim that in fact $\tau \in C_G(Q) \subseteq N_G(Q)$. Indeed, if $\tau \notin C_G(Q)$, then the order of $\tau C_G(Q)$ in the qoutient group $N_G(Q)/C_G(Q)$ equals w. Therefore, by Lemma 13, we find that ω divides the order of $\operatorname{Aut} Q$. However, $|\operatorname{Aut} Q| = \varphi(q) = q - 1$ and $\omega \nmid (q-1)$ by our assumption (here φ denotes the Euler's totient function—a contradiction).

We have proved $Q = \langle \pi \cdot \rho \rangle$, where $\pi, \rho \in S_p$ are two disjoint q-cycles. Let us denote $\pi = (i_1, i_2, \ldots, i_q)$ and $\rho = (j_1, j_2, \ldots, j_q)$. Since

$$\tau \in C_G(Q) = \{\sigma \in G : \ \sigma \cdot \eta \cdot \sigma^{-1} = \eta \ \forall \eta \in Q\},$$

we obtain $\tau \cdot (\pi \cdot \rho) \cdot \tau^{-1} = \pi \cdot \rho$, i.e.,

$$(i_1^\tau, i_2^\tau, \ldots, i_q^\tau)(j_1^\tau, j_2^\tau, \ldots, j_q^\tau) = (i_1, i_2, \ldots, i_q)(j_1, j_2, \ldots, j_q).$$

By the uniqueness of the cycle decomposition, there are two possible cases: either

$$(i_1^\tau, i_2^\tau, \ldots, i_q^\tau) = (i_1, i_2, \ldots, i_q) \text{ and } (j_1^\tau, j_2^\tau, \ldots, j_q^\tau) = (j_1, j_2, \ldots, j_q)$$

or

$$(i_1^\tau, i_2^\tau, \ldots, i_q^\tau) = (j_1, j_2, \ldots, j_q) \text{ and } (j_1^\tau, j_2^\tau, \ldots, j_q^\tau) = (i_1, i_2, \ldots, i_q).$$

In both cases, we find that

$$(i_1^{\tau^2}, i_2^{\tau^2}, \ldots, i_q^{\tau^2}) = (i_1, i_2, \ldots, i_q) \text{ and } (j_1^{\tau^2}, j_2^{\tau^2}, \ldots, j_q^{\tau^2}) = (j_1, j_2, \ldots, j_q).$$

Denote $\eta = \tau^2$. We will show that η fixes every element of the set

$$\{i_1, i_2, \ldots, i_q, j_1, j_2, \ldots, j_q\}.$$

Firstly, note that $\eta(i_1) = i_1$. Indeed, suppose for the contrary that $\eta(i_1) = i_{1+k}$ for some $k \in \{1, \ldots, q-1\}$. Then,

$$\eta^l(i_1) = i_{1+lk \ (\mathrm{mod}\ q)} = i_1 \Leftrightarrow 1 + lk \equiv 1 \pmod q \Leftrightarrow l \equiv 0 \pmod q,$$

which implies that η has a cycle of length q in its cycle decomposition, but this is impossible since the order of η equals w and $\gcd(w, q) = 1$. Hence, $\eta(i_1) = i_1$, and therefore $\eta(i_k) = i_k$ for every $k = 1, \ldots, q$. Analogously, $\eta(j_k) = j_k$ for every $k = 1, \ldots, q$.

Hence, there are at most $p - 2q = w$ elements in the set $\{1, 2, \ldots, p\}$ that are not fixed under η. Since the order of η equals ω, it follows that η is a cycle of length w, which leads to a contradiction by Lemma 11. This completes the proof of the proposition. □

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: The author thanks P. Drungilas for useful advice.

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

Appendix A

Drungilas, Dubickas and Smyth [1] proposed the following hypothesis:

Hypothesis A1 (Part of Conjecture 4, [1])**.** *If $(a, b, c), (a', b', c') \in \mathbb{N}^3$ are compositum-feasible, then so is (aa', bb', cc').*

It was proved in [3] that this hypothesis is true if the answer to the *inverse Galois problem* is positive. Recall that the inverse Galois problem asks whether every finite group occurs as a Galois group of some Galois extension K over $\mathbb{Q}$.

Theorem A1 (Theorem 1.3, [3])**.** *If every finite group occurs as a Galois group of some Galois extension $K/\mathbb{Q}$, then the Hypothesis A1 is true.*

For $(a,b,c),(a',b',c') \in \mathbb{N}^3$, let us denote

$$(a,b,c)\cdot(a',b',c') := (aa',bb',cc'). \tag{A1}$$

In other words, Theorem A1 implies that, assuming an affirmative answer to the inverse Galois problem, the set $\mathcal{C}$ of compositum-feasible triplets forms a semigroup with respect to the multiplication defined by (A1). It is natural to ask which elements of $\mathcal{C}$ are *irreducble*. We say that a triplet $(A,B,C) \in \mathcal{C}$ is *irreducible* if it cannot be written as $(A,B,C) = (a,b,c)\cdot(a',b',c')$, where $(a,b,c),(a',b',c') \in \mathcal{C} \setminus \{(1,1,1)\}$. Otherwise, we say that the triplet $(A,B,C) \in \mathcal{C}$ is *reducible*. For instance, every triplet $(p,p,pd) \in \mathcal{C}$, where p is a prime number and $1 \le d < p$, is irreducible, whereas for any positive integer n the triplet $(n,n,n^2) = (n,1,n)\cdot(1,n,n)$ is reducible (It is known (see Lemmas 2.7 and 2.8, Theorem 1.1, [2]) that for any prime p and for $d = 1,2,p-1$ the triplet (p,p,pd) is compositum-feasible, whereas for $p - \frac{1+\sqrt{4p-3}}{2} < d \le p-2$ it is not product-feasible, hence not compositum-feasible, too. Meanwhile, the triplet (n,n,n^2) is compositum-feasible for any $n \in \mathbb{N}$ by Lemma 2). The following proposition gives one more family of irreducible triplets in $\mathcal{C}$.

Proposition A1. *For any integer $n \ge 2$ the compositum-feasible triplet $(n,n,n(n-1))$ is irreducible (In fact, it is known that for any $n \ge 2$ the triplet $(n,n,n(n-1))$ is compositum-feasible (see Proposition 29, [1])).*

Proof. Suppose on the contrary that

$$(n,n,n(n-1)) = (a_1,b_1,c_1)\cdot(a_2,b_2,c_2), \tag{A2}$$

where (a_1,b_1,c_1) and (a_2,b_2,c_2) are compositum-feasible triplets that are both different from $(1,1,1)$.

For $i = 1,2$ we can factor $c_i = d_i^{(n)} d_i^{(n-1)}$, where $d_1^{(n)} d_2^{(n)} = n$ and $d_1^{(n-1)} d_2^{(n-1)} = n-1$. We assume that the triplet (a_1,b_1,c_1) is compositum-feasible, thus a_1 divides $c_1 = d_1^{(n)} d_1^{(n-1)}$. Since $\gcd(a_1, d_1^{(n-1)}) = 1$, it follows that $a_1 | d_1^{(n)}$. Analogously, $a_2 | d_2^{(n)}$. If $a_1 < d_1^{(n)}$, then

$$d_1^{(n)} d_2^{(n)} = n = a_1 a_2 < d_1^{(n)} a_2 \Rightarrow d_2^{(n)} < a_2,$$

thus $a_2 \nmid d_2^{(n)}$—a contradiction. Therefore, $a_2 = d_1^{(n)}$ and $a_2 = d_2^{(n)}$. Analogously, $b_1 = d_1^{(n)}$ is $b_2 = d_2^{(n)}$. Thus, omitting superscripts (n) and instead of $(n-1)$ using $'$ we can rewrite (A2) as

$$(n,n,n(n-1)) = (d_1,d_1,d_1 d_1')\cdot(d_2,d_2,d_2 d_2').$$

Note that $d_i' < d_i$, $i = 1,2$. Indeed, for any compositum-feasible triplet, (a,b,c) holds $c \le ab$, hence for $i = 1,2$ $d_i d_i' \le d_i^2$, i.e., $d_i' \le d_i$. Moreover, $\gcd(d_i', d_i) = 1$ and the numbers d_i', d_i cannot be both equal to 1, thus $d_i' \ne d_i$. Therefore,

$$d_2 d_2' = \frac{n}{d_1} \cdot \frac{n-1}{d_1'} \ge \frac{n}{d_1} \cdot \frac{n-1}{d_1 - 1} > \left(\frac{n}{d_1}\right)^2 = d_2^2 \Rightarrow d_2' > d_2,$$

since $d_1 < n$, a contradiction. Hence, the triplet $(n,n,n(n-1))$ is irreducible. □

One can check by a routine calculation that among the compositum-feasible triplets (a,b,c), $a \le b \le c$, $b \le 9$ (All such triplets are described in [1,2,4]), the only irreducible triplets are of the form $(1,p,p)$, (p,p,pd) and $(n,n,n(n-1))$, where p is prime, $1 \le d < p$ and $n \ge 2$. We finish our article by proposing the problem to find all irreducible compositum-feasible triplets.

References

1. Drungilas, P.; Dubickas, A.; Smyth, C. A degree problem for two algebraic numbers and their sum. *Publ. Mat.* **2012**, *56*, 413–448. [CrossRef]
2. Drungilas, P.; Dubickas, A.; Luca, F. On the degree of compositum of two number fields. *Math. Nachr.* **2013**, *286*, 171–180. [CrossRef]
3. Drungilas, P.; Dubickas, A. On degrees of three algebraic numbers with zero sum or unit product. *Colloq. Math.* **2016**, *143*, 159–167. [CrossRef]
4. Drungilas, P.; Maciulevičius, L. A degree problem for the compositum of two number fields. *Lith. Math. J.* **2019**, *59*, 39–47. [CrossRef]
5. Drmota, M.; Skał ba, M. On multiplicative and linear independence of polynomial roots. In *Contributions to General Algebra, 7 (Vienna, 1990)*; Hölder-Pichler-Tempsky: Vienna, Austria, 1991; pp. 127–135.
6. Cantor, D.G.; Isaacs, I.M. Problems and Solutions: Solutions of Advanced Problems: 6523. *Amer. Math. Monthly* **1988**, *95*, 561–562. [CrossRef]
7. Dixon, J.D.; Mortimer, B. Permutation Groups. In *Graduate Texts in Mathematics*; Springer: New York, NY, USA, 1996; Volume 163, pp. xii+346. [CrossRef]
8. Wielandt, H. *Finite Permutation Groups*; Translated from the German by R. Bercov; Academic Press: New York, NY, USA; London, UK, 1964; pp. x+114.
9. Narkiewicz, W.A.A. *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed.; Springer Monographs in Mathematics; Springer: Berlin, Germany, 2004; pp. xii+708. [CrossRef]
10. Vinogradov, I.M. *Elements of Number Theory*; Kravetz., S., Translater; Dover Publications, Inc.: New York, NY, USA, 1954; pp. viii+227.