COLLOQUIUM MATHEMATICUM

VOL. 143 2016 NO. 2

ON DEGREES OF THREE ALGEBRAIC NUMBERS WITH ZERO SUM OR UNIT PRODUCT

BY

PAULIUS DRUNGILAS and ARTŪRAS DUBICKAS (Vilnius)

Abstract. Let α, β and γ be algebraic numbers of respective degrees a, b and c over $\mathbb{Q}$ such that $\alpha+\beta+\gamma=0$. We prove that there exist algebraic numbers α_1, β_1 and γ_1 of the same respective degrees a, b and c over $\mathbb{Q}$ such that $\alpha_1\beta_1\gamma_1=1$. This proves a previously formulated conjecture. We also investigate the problem of describing the set of triplets $(a,b,c)\in\mathbb{N}^3$ for which there exist finite field extensions K/k and L/k (of a fixed field k) of degrees a and b, respectively, such that the degree of the compositum KL over k equals c. Towards another earlier formulated conjecture, under certain natural assumptions (related to the inverse Galois problem), we show that the set of such triplets forms a multiplicative semigroup.

1. Introduction. In [3], jointly with Chris Smyth, we proposed the following problem:

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

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

When such α, β, γ exist, we say that (a,b,c) is *sum-feasible*. For example, $(2,2,4)$ is sum-feasible (take $\alpha=\sqrt{2}$, $\beta=\sqrt{3}$, $\gamma=-(\sqrt{2}+\sqrt{3})$), whereas $(2,2,5)$ is not, since the degree of the sum of two algebraic numbers cannot exceed the product of their degrees.

This is a natural generalization of the trivial problem with two algebraic numbers summing to zero which only happens if their degrees are equal. With three numbers, even for small values of a, b and c it is sometimes difficult to determine whether (a,b,c) is sum-feasible. See, for instance, the proof of [2, Theorem 1.1], where, jointly with Florian Luca, we showed that $(6,6,8)$ is not sum-feasible (see also [3, Theorem 38]). In fact, [3, Theorem 5] combined with [2, Corollary 1.6] provides the description of all sum-feasible triplets (a,b,c) satisfying $a\le b\le c$ where $b\le 7$. In particular, by exploiting

2010 *Mathematics Subject Classification*: Primary 11R04; Secondary 11R32, 12F05, 20B35.
Key words and phrases: algebraic number, sum-feasible, product-feasible, compositum-feasible, inverse Galois problem, semigroup.
Received 15 May 2015; revised 3 August 2015.
Published online 3 December 2015.

the properties of the projective special linear group $\mathrm{PSL}(2,7)$ of order 168, we proved that $(7,7,28)$ is sum-feasible, although there is no particular reason for this to happen.

In a similar fashion, 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 respective degrees a, b and c over $\mathbb{Q}$ such that $\alpha\beta\gamma = 1$ ([1]). We conjectured (see [3, Conjecture 3]) that if $(a,b,c) \in \mathbb{N}^3$ is sum-feasible then it is also product-feasible. We can now prove this conjecture.

THEOREM 1.1. *If for $(a,b,c) \in \mathbb{N}^3$ there exist algebraic numbers α, β, γ of respective degrees a, b, c over $\mathbb{Q}$ satisfying*

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

then there also exist algebraic numbers $\alpha_1, \beta_1, \gamma_1$ of respective degrees a, b, c over $\mathbb{Q}$ such that

$$\alpha_1\beta_1\gamma_1 = 1.$$

Note that the converse of Theorem 1.1 is false, i.e., if $(a,b,c) \in \mathbb{N}^3$ is product-feasible then it is not necessarily sum-feasible. This can be easily seen from the following example. Let

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

Then α, β, γ have degrees $2, 3, 3$, respectively, and $\alpha\beta\gamma = 1$. Therefore, $(2,3,3)$ is product-feasible. However, it is not sum-feasible, by the main theorem of [4]. See [3, Theorem 8] for an infinite family of product-feasible triplets which are not sum-feasible.

Let k be a field. We say that a triplet $(a,b,c) \in \mathbb{N}^3$ is *compositum-feasible* over k if there exist finite field extensions K/k and L/k of degrees a and b such that the degree of their compositum KL (over k) is c. In case $k = \mathbb{Q}$ we simply say "compositum-feasible" instead of "compositum-feasible over $\mathbb{Q}$". In [3, Theorem 5] and [2, Corollary 1.5] we described all the compositum-feasible triplets (a,b,c) satisfying $a \le b \le c$ where $b \le 7$. Moreover, [2, Theorem 1.4] implies that given a triplet $(a,b,c) \in \mathbb{N}^3$ one can in principle find whether it is compositum-feasible or not by performing a finite calculation with all the subgroups of the full symmetric group S_c which appear as Galois groups of irreducible polynomials of degree c.

The three feasibility problems are related. For instance, if $(a,b,c) \in \mathbb{N}^3$ is compositum-feasible then it is also sum-feasible and product-feasible (see [3, Proposition 1]). The converse is false, since $(4,4,6)$ is sum-feasible, but not compositum-feasible (see, e.g., [3, Proposition 29]).

([1]) Note that the equalities $\alpha+\beta+\gamma = 0$ and $\alpha\beta\gamma = 1$ can be replaced by $\alpha+\beta+\gamma \in \mathbb{Q}$ and $\alpha\beta\gamma \in \mathbb{Q} \setminus \{0\}$, respectively.

Among other things, in [3] we conjectured that the set of compositum-feasible triplets forms a multiplicative semigroup:

CONJECTURE 1.2 (Part of [3, Conjecture 4]). *If* $(a,b,c),(a',b',c') \in \mathbb{N}^3$ *are compositum-feasible then so is* (aa',bb',cc').

Some partial cases of Conjecture 1.2 are given in [3, Lemma 26 and Corollary 27]. For example, if (a,b,c) is compositum-feasible and p is an arbitrary prime number then (ap,bp^2,cp^2) is also compositum-feasible.

In order to state our next result we first recall some basics related to the so-called *inverse Galois problem*. Let k be a field, and let G be a finite group. We say that G *occurs as a Galois group over* k if there exists a Galois extension K/k whose Galois group $\mathrm{Gal}(K/k)$ is isomorphic to G. Given a field k the inverse problem of Galois theory (or simply the inverse Galois problem) asks whether every finite group occurs as a Galois group over k (see, for instance, [5], [7], [10]). It is believed that in case $k=\mathbb{Q}$ (the classical inverse Galois problem) the answer is affirmative.

THEOREM 1.3. *If every finite group occurs over* $\mathbb{Q}$ *as a Galois group then Conjecture* 1.2 *is true.*

Recall that a field k is said to be *perfect* if every finite extension K/k is separable. For instance, fields of characteristic zero and finite fields are perfect. Theorem 1.3 is a corollary of the following result.

THEOREM 1.4. *Let* k *be a perfect field. Assume that every finite group occurs as a Galois group over* k. *Then for any* $(a,b,c),(a',b',c') \in \mathbb{N}^3$ *compositum-feasible over* k *the triplet* (aa',bb',cc') *is also compositum-feasible over* k.

Note that not every perfect field satisfies the assumption of Theorem 1.4. For example, only cyclic groups occur as Galois groups over finite fields.

There are fields for which the inverse Galois problem is solved. For instance, Riemann's existence theorem implies that every finite group occurs as a Galois group over the field $\mathbb{C}(t)$ of rational functions with indeterminate t and complex coefficients (see, e.g., [5]). Since the field $\mathbb{C}(t)$ is perfect (as it is of characteristic zero), Theorem 1.4 implies the following:

COROLLARY 1.5. *If* $(a,b,c),(a',b',c') \in \mathbb{N}^3$ *are compositum-feasible over* $\mathbb{C}(t)$ *then so is the product* (aa',bb',cc').

The proofs of Theorems 1.1 and 1.4 are based on quite different arguments, so they are given in two separate sections.

We remark that, by Propositions 3.1 and 3.2 below, the assumption in Theorem 1.4 that every finite group occurs as a Galois group over k can be replaced by the following weaker (but quite technical) condition. Assume that a triplet (a,b,c) over k is realizable by the fields K,L, so that

$a = [K : k]$, $b = [L : k]$, $c = [KL : k]$, with G being the Galois group of the normal closure of KL over k (and similarly that (a', b', c') is realizable by some fields K', L', so that $a' = [K' : k]$, $b' = [L' : k]$, $c' = [K'L' : k]$). We will show that then (aa', bb', cc') is compositum-feasible over k if the n-fold direct product G^n occurs as a Galois group over k, where n is the number of intermediate fields between k and $K'L'$ (including k and $K'L'$). At the end of Section 3 we will show that the number of intermediate fields m in a finite separable extension F/k of degree $d \geq 2$ (including k and F) is bounded by

$$m \leq 2 + \sum_{\ell} \binom{d-1}{\ell-1}, \tag{1.1}$$

where the sum is taken over all divisors ℓ of d satisfying $1 < \ell < d$. This bound is better than the one in [8, Exercise A-30] (i.e. $2^{d!}$) and the one in [12] (i.e. 2^{d-1}).

2. Proof of Theorem 1.1. In the proof we shall use the following lemma.

LEMMA 2.1. *Let d and X be positive integers, and let $z_1, \dots, z_d$ be distinct complex numbers. Then there is a positive integer k for which the equality*

$$(k + z_1)^{x_1} \cdots (k + z_d)^{x_d} = 1 \tag{2.1}$$

does not hold for $x_1, \dots, x_d \in \mathbb{Z}$ satisfying $|x_1|, \dots, |x_d| \leq X$ unless $x_1 = \cdots = x_d = 0$.

Proof. Assume that there are no such k. Note that there are $(2X+1)^d$ vectors $(x_1, \dots, x_d) \in \mathbb{Z}^d$ satisfying

$$\max_{1 \leq i \leq d} |x_i| \leq X. \tag{2.2}$$

Hence, for some non-zero vector $(x_1, \dots, x_d) \in \mathbb{Z}^d$ satisfying (2.2), equality (2.1) holds for infinitely many positive integers k. Let $S \subset \mathbb{N}$ be the set of all such k. Let I and J be the sets of indices i in $\{1, \dots, d\}$ for which x_i are positive and negative respectively, so that $I \cap J = \emptyset$ and $I \cup J \subseteq \{1, \dots, d\}$. Without restriction of generality we may assume that $x_1 > 0$, so that $1 \in I$.

Consider the polynomial

$$P(z) := \prod_{i \in I} (z + z_i)^{x_i} - \prod_{j \in J} (z + z_j)^{-x_j},$$

where the second product is 1 if the set J is empty. By the definition of S, P and (2.1), we see that $P(k) = 0$ for each $k \in S$. However, P is a polynomial, so $P(z) \equiv 0$. In particular, from $1 \in I$ and $P(-z_1) = 0$ we deduce that $\prod_{j \in J} (-z_1 + z_j)^{-x_j} = 0$, which is impossible in view of $z_j \neq z_1$ for $j > 1$. ∎

Proof of Theorem 1.1. Let α, β, γ and a, b, c be as in the hypothesis. Also, let K be the Galois closure of $\mathbb{Q}(\alpha, \beta, \gamma)$ over $\mathbb{Q}$, and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Set $d = [K\colon \mathbb{Q}] = |G|$. By the normal basis theorem, there is $w \in K$ such that $w_j = \sigma_j(w)$, $j = 1, \dots, d$, where σ_j runs through all d automorphisms $\sigma_1, \dots, \sigma_d$ of G, is a basis of K. In particular, there are rational numbers $a_1, \dots, a_d$ for which

$$\alpha = a_1 w_1 + \cdots + a_d w_d.$$

Similarly, there exist $b_1, \dots, b_d \in \mathbb{Q}$ and $c_1, \dots, c_d \in \mathbb{Q}$ such that

$$\beta = b_1 w_1 + \cdots + b_d w_d, \quad \gamma = c_1 w_1 + \cdots + c_d w_d.$$

Clearly, $a = \deg \alpha$ is the number of distinct numbers in the list $\sigma(\alpha)$, where σ runs through the d automorphisms of G. For each $\sigma \in G$, we can write

$$\sigma(\alpha) = a_{\sigma(1)} w_1 + \cdots + a_{\sigma(d)} w_d,$$

where σ acts a permutation of $\{1, \dots, d\}$. As $w_1, \dots, w_d$ is a basis of K, we see that a is equal to the number of distinct vectors in the set

$$A := \{(a_{\sigma(1)}, \dots, a_{\sigma(d)}) \,:\, \sigma \in G\},$$

each repeated $d/|A| = d/a$ times. Similarly, the degrees b and c are equal to the numbers of distinct vectors in

$$B := \{(b_{\sigma(1)}, \dots, b_{\sigma(d)}) \,:\, \sigma \in G\}, \quad C := \{(c_{\sigma(1)}, \dots, c_{\sigma(d)}) \,:\, \sigma \in G\},$$

respectively. Also, $\alpha + \beta + \gamma = 0$ implies

$$a_i + b_i + c_i = 0 \tag{2.3}$$

for each $i = 1, \dots, d$.

Note that, by replacing the initial w by $w + k$, where $k \in \mathbb{Z}$, we get $\alpha + (a_1 + \cdots + a_d)k$ instead of α, and similarly $\beta + (b_1 + \cdots + b_d)k$ (instead of β) and $\gamma + (c_1 + \cdots + c_d)k$ (instead of γ). Hence, the degrees of the new α, β, γ are a, b, c again. Furthermore, the sum of these new α, β, γ is zero, by (2.3). Note that by multiplying each α, β, γ by the common denominator of the numbers $a_1, \dots, a_d, b_1, \dots, b_d, c_1, \dots, c_d \in \mathbb{Q}$, we do not change the degrees a, b, c and the property $\alpha + \beta + \gamma = 0$ still holds. Thus, we can assume that these $3d$ numbers are all in $\mathbb{Z}$. Define

$$L := \max\{|a_1|, \dots, |a_d|, |b_1|, \dots, |b_d|, |c_1|, \dots, |c_d|\}. \tag{2.4}$$

Consider the following three numbers in K:

$$\alpha_1 := (w_1 + k)^{a_1} \cdots (w_d + k)^{a_d},$$

where $k > \max_{1 \le i \le d} |w_i|$ is a positive integer to be chosen later,

$$\beta_1 := (w_1 + k)^{b_1} \cdots (w_d + k)^{b_d}$$

and

$$\gamma_1 := (w_1 + k)^{c_1} \cdots (w_d + k)^{c_d}.$$

In view of (2.3) and $w_i + k \neq 0$ for $1 \leq i \leq d$, we obtain

$$\alpha_1\beta_1\gamma_1 = 1. \tag{2.5}$$

It remains to show that for some positive integer k we have $\deg \alpha_1 = a$, $\deg \beta_1 = b$ and $\deg \gamma_1 = c$. This time, all the conjugates of α_1 are

$$(w_1 + k)^{a_{\sigma(1)}} \cdots (w_d + k)^{a_{\sigma(d)}},$$

where σ runs through d permutations of $\{1, \dots, d\}$. Evidently, two such numbers, say, $(w_1+k)^{a_{\sigma(1)}} \cdots (w_d+k)^{a_{\sigma(d)}}$ and $(w_1+k)^{a_{\tau(1)}} \cdots (w_d+k)^{a_{\tau(d)}}$, where σ, τ are permutations of $\{1, \dots, d\}$, are equal when the vectors $(a_{\sigma(1)}, \dots, a_{\sigma(d)})$ and $(a_{\tau(1)}, \dots, a_{\tau(d)})$ are equal. Hence, $\deg \alpha_1 = |A| = a$ if

$$(w_1 + k)^{a_{\sigma(1)}} \cdots (w_d + k)^{a_{\sigma(d)}} \neq (w_1 + k)^{a_{\tau(1)}} \cdots (w_d + k)^{a_{\tau(d)}}$$

whenever the vectors $(a_{\sigma(1)}, \dots, a_{\sigma(d)})$ and $(a_{\tau(1)}, \dots, a_{\tau(d)})$ are distinct. By Lemma 2.1, with $X = 2L$ and L defined in (2.4), we see that such $k \in \mathbb{N}$ can be chosen. Thus, $\deg \alpha_1 = a$. By the same argument, we have $\deg \beta_1 = |B| = b$ and $\deg \gamma_1 = |C| = c$. This shows the existence of a triplet of algebraic numbers $\alpha_1, \beta_1, \gamma_1$ of degrees a, b, c, respectively, satisfying (2.5), and so completes the proof of the theorem. ∎

3. Proof of Theorem 1.4. Let K and L be two field extensions of a field k which are contained in some common field. Then K is said to be *linearly disjoint* from L over k if every finite set of elements of K that is linearly independent over k is still so over L (see, e.g., [6, p. 360]). It is well-known (see, e.g., [9, Lemma 20.4]) that if K/k and L/k are finite extensions then the linear disjointness of K from L over k (and vice versa) is equivalent to

$$[KL\colon k] = [K\colon k] \cdot [L\colon k]. \tag{3.1}$$

If L/k is a Galois extension then $[KL\colon k] \cdot [K \cap L\colon k] = [K\colon k] \cdot [L\colon k]$, so the fields K and L are linearly disjoint if and only if (see [11, Corollary 3.4.5])

$$K \cap L = k. \tag{3.2}$$

The following result is essentially a part of [1, Theorem 4.2]. For the sake of completeness we give its proof.

PROPOSITION 3.1. *Suppose that K is a finite Galois extension of a field k with Galois group G. Assume that for every positive integer n the n-fold direct product G^n occurs as a Galois group over k. Then for any finite separable extension F/k there exists a Galois extension L over k with Galois group isomorphic to G which is linearly disjoint from F over k.*

Proof. By (3.2), the linear disjointness of F and a Galois extension L over k is equivalent to $L \cap F = k$. Therefore, it suffices to prove the existence of a normal extension L/k with Galois group G and $L \cap F = k$.

Since the extension F/k is finite and separable, the number of intermediate fields F' satisfying $k \subseteq F' \subseteq F$ (including k and F) is finite, say m. By hypothesis, there exists a finite Galois extension E/k with $\mathrm{Gal}(E/k) \cong G^m$. Define, for each $i = 1, \dots, m$,

$$N_i := \{(g_1, \dots, g_m) \in G^m : g_i = 1\}.$$

Obviously, N_i is a subgroup of G^m isomorphic to G^{m-1}. Denote by E_i the subfield of E corresponding to N_i. The extension E_i/k is normal, since N_i is a normal subgroup of G^m. Therefore, $\mathrm{Gal}(E_i/k) \cong G^m/N_i \cong G$. Hence, each extension E_i/k is normal and has Galois group isomorphic to G.

We claim that

$$E_i \cap E_j = k \quad \text{for } i \neq j. \tag{3.3}$$

Indeed, the intersection subgroup

$$N_i \cap N_j := \{(g_1, \dots, g_m) \in G^m : g_i = g_j = 1\}, \quad i \neq j,$$

is isomorphic to G^{m-2}, and therefore $G^m/N_i \cap N_j \cong G^2$. Moreover, as $N_i \cap N_j$ corresponds to the compositum E_iE_j, by the fundamental theorem of Galois theory, the index of $N_i \cap N_j$ in G^m equals the degree of E_iE_j (over k), i.e.,

$$[E_iE_j : k] = |G^m/N_i \cap N_j| = |G^2| = [E_i : k] \cdot [E_j : k].$$

Consequently, $[E_i \cap E_j : k] = 1$, which yields $E_i \cap E_j = k$. This proves (3.3).

Now, we claim that at least one of the fields E_i satisfies $E_i \cap F = k$. Indeed, if $E_i \cap F = E_j \cap F$ for some distinct i and j then $E_i \cap F$ is a subfield of $E_i \cap E_j$. This, in view of (3.3), implies $E_i \cap F = k$. Alternatively, if all the subfields $E_i \cap F$, $i = 1, \dots, m$, are distinct then one of them equals k, since there are exactly m distinct intermediate fields between k and F, including k and F. ∎

Note that in the proof of Proposition 3.1 we have used the separability of F only to ensure that the number of intermediate fields between k and F is finite.

PROPOSITION 3.2. *Suppose that $(a, b, c), (a', b', c') \in \mathbb{N}^3$ are compositum-feasible over a field k. Assume that there exist finite separable extensions K/k, L/k, K'/k, L'/k of degrees a, b, a', b', respectively, such that $[KL : k] = c$ and $[K'L' : k] = c'$. Let $G = \mathrm{Gal}(K'L'/k)$. Assume that for every positive integer n the n-fold direct product G^n occurs as a Galois group over k. Then the triplet (aa', bb', cc') is compositum-feasible over k.*

Proof. Let H_1 and H_2 be the subgroups of G fixing the subfields K' and L', respectively. Then $[G : H_1] = [K' : k] = a'$ and $[G : H_2] = [L' : k] = b'$. Moreover, the subgroup $H_1 \cap H_2$ corresponds to the compositum $K'L'$ (see, e.g., [6, Chapter 6, Corollary 1.3]). Therefore, by the fundamental the-

orem of Galois theory, the index of $H_1 \cap H_2$ in G equals the degree of $K'L'$ (over k). Consequently, $[G\colon H_1 \cap H_2] = [K'L'\colon k] = c'$.

By Proposition 3.1, there exists a Galois extension N/k whose Galois group is isomorphic to G and which is linearly disjoint from KL over k. Let K_1 and L_1 be the subfields of N corresponding to H_1 and H_2, respectively. Then $[K_1\colon k] = [G\colon H_1] = a'$. Similarly, $[L_1\colon k] = [G\colon H_2] = b'$ and $[K_1L_1\colon k] = [G\colon H_1 \cap H_2] = c'$. This yields the linear disjointness of KL and K_1L_1. Hence K and K_1 are also linearly disjoint over k, since subextensions of linearly disjoint extensions are linearly disjoint (part of [6, Proposition 3.1]). Therefore, by (3.1), we obtain

$$[KK_1\colon k] = [K\colon k] \cdot [K_1\colon k] = aa'$$

and $[KLK_1L_1\colon k] = [KL\colon k] \cdot [K_1L_1\colon k] = cc'$. Similarly, $[LL_1\colon k] = bb'$, since L and L_1 are linearly disjoint over k. Thus, (aa', bb', cc') is compositum-feasible over k. ∎

Let $k = \mathbb{Q}$. In the case of a solvable group G the assertion of Proposition 3.2 involving the direct product G^n holds, since, by a well-known theorem of Shafarevich, every solvable group occurs as a Galois group over $\mathbb{Q}$ (see, e.g., [5, Theorem 0.2.4]).

Proof of Theorem 1.4. Assume that k and $(a, b, c), (a', b', c') \in \mathbb{N}^3$ satisfy the condition of the theorem. Then there exist field extensions K/k, L/k, K'/k, L'/k of degrees a, b, a', b', respectively, such that $[KL\colon k] = c$ and $[K'L'\colon k] = c'$. Since k is perfect, all these extensions are separable. Denote by G the Galois group of the Galois closure of $K'L'/k$. By assumption, G^n occurs as a Galois group over k for every positive integer n. Hence, by Proposition 3.2, (aa', bb', cc') is compositum-feasible over k. ∎

In conclusion, we shall prove the upper bound (1.1). It suffices to count those subfields M, $k \subset M \subset F$, different from k and $F = k(\alpha)$, and then add 2. Let M be such a field, $t := [M : k]$, and let $g(x)$ be the minimal polynomial of α over M. Note that

$$d = [F : k] = [F : M] \cdot [M : k] = [F : M]t,$$

so $\deg g = d/t = \ell$. Following the argument in [8, Proposition 5.3], the field M is generated by the coefficients of $g(x)$. Since $g(x)$ is a divisor of the minimum polynomial $f(x)$ of α over k, each M is uniquely determined by a collection of $\ell = d/t$ roots of $f(x)$, one of which is α and the other $\ell - 1$ roots are its conjugates over k. There are $\binom{d-1}{\ell-1}$ such collections, so there are at most $\binom{d-1}{\ell-1}$ possibilities for extensions M of degree $t = d/\ell$. Summing over all proper divisors ℓ of d (and adding 2) we obtain the bound (1.1).

References

[1] K. Conrad, *The Galois correspondence at work*, lecture notes, http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/galoiscorrthms.pdf.

[2] P. Drungilas, A. Dubickas and F. Luca, *On the degree of compositum of two number fields*, Math. Nachr. 286 (2013), 171–180.

[3] P. Drungilas, A. Dubickas and C. Smyth, *A degree problem for two algebraic numbers and their sum*, Publ. Mat. 56 (2012), 413–448.

[4] I. M. Isaacs, *Degrees of sums in a separable field extension*, Proc. Amer. Math. Soc. 25 (1970), 638–641.

[5] C. U. Jensen, A. Ledet and N. Yui, *Generic Polynomials. Constructive Aspects of the Inverse Galois Problem*, Cambridge Univ. Press, Cambridge, 2002.

[6] S. Lang, *Algebra*, 3rd revised ed., Grad. Texts in Math. 211, Springer, New York, 2002.

[7] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer, Berlin, 1999.

[8] J. S. Milne, *Fields and Galois theory*, course notes, http://www.jmilne.org/math/CourseNotes/FT.pdf.

[9] P. Morandi, *Field and Galois Theory*, Springer, New York, 1996.

[10] H. Völklein, *Groups as Galois Groups. An Introduction*, Cambridge Univ. Press, Cambridge, 1996.

[11] S. H. Weintraub, *Galois Theory*, 2nd. ed., Springer, New York, 2009.

[12] http://math.stackexchange.com/questions/522976/.

Paulius Drungilas
Department of Mathematics
and Informatics
Vilnius University
Naugarduko 24
Vilnius LT-03225, Lithuania
E-mail: pdrungilas@gmail.com

Artūras Dubickas
Department of Mathematics and Informatics
Vilnius University
Naugarduko 24
Vilnius LT-03225, Lithuania
and
Institute of Mathematics and Informatics
Vilnius University
Akademijos 4
Vilnius LT-08663, Lithuania
E-mail: arturas.dubickas@mif.vu.lt