New York Journal of Mathematics

New York J. Math. **29** (2023) 171–192.

Compositum of two number fields of prime degree

Paulius Virbalas

ABSTRACT. In this paper by exploiting the properties of transitive permutation groups of prime degree we provide an answer to the following problem: given two number fields K and L both of prime degree p over $\mathbb{Q}$, what values the degree of their compositum KL can take? We show that if K and L are linearly disjoint over $\mathbb{Q}$, then necessarily KL has degree p^2 or, for example, if K and L are number fields of prime degree p such that $p = (q^n-1)/(q-1)$ with q prime or a power of a prime, $n \geq 3$, and some intermediate group between the projective special linear group $\mathrm{PSL}(n,q)$ and the projective semilinear group $\mathrm{P\Gamma L}(n,q)$ is realizable over $\mathbb{Q}$, then the degree of KL is pq^{n-1}. In addition, for any divisor s of $p-1$, there exist number fields K and L of prime degree p such that their compositum KL has degree ps. As a numerical application, we determine the complete list of values the degree of compositum KL can take if K and L are two number fields of degree 13. We also give an answer to the related problem, namely, given two algebraic numbers α and β both of prime degree p, what values the degree of $\alpha+\beta$ and $\alpha\beta$ can take?

CONTENTS

1. Introduction

A triplet of positive integers $(a,b,c) \in \mathbb{N}^3$ is said to be *compositum-feasible* if there exist number fields K and L of degrees a and b over the field of rationals $\mathbb{Q}$ such that the degree of their compositum KL is c. Equivalently, $(a,b,c) \in \mathbb{N}^3$ is compositum-feasible if and only if there exist algebraic numbers α and

Received February 14, 2022.
2020 *Mathematics Subject Classification.* 11R04, 11R32, 12F05, 20B35.
Key words and phrases. Algebraic numbers, compositum of two number fields, transitive permutation groups of prime degree, Galois groups.

ISSN 1076-9803/2023

β of degrees a and b over $\mathbb{Q}$ such that $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = c$. This definition was introduced in [9] by Drungilas, Dubickas and Smyth. Among other things, they found some sufficient but not necessary conditions for a triplet (a,b,c) to be compositum-feasible and described all compositum-feasible triplets (a,b,c) satisfying $a \le b \le 6$.

For two positive integers a and b, let $\mathrm{lcm}(a,b)$ denote their least common multiple, and let $\gcd(a,b)$ denote their greatest common divisor. Clearly, if the triplet (a,b,c) is compositum-feasible, then

$$c \le ab \quad \text{and} \quad \mathrm{lcm}(a,b) \mid c. \tag{1}$$

From (1) it immediately follows that if $\gcd(a,b) = 1$ and the triplet (a,b,c) is compositum-feasible, then $c = ab$. Note however, that condition (1) is not sufficient for a triplet (a,b,c) to be compositum-feasible. For example, the triplet $(5,5,15)$ satisfies (1), but it was shown in [9, Theorem 36] that this triplet is not compositum-feasible . In the follow-up paper by Drungilas, Dubickas and Luca [8] it was noted that "even a natural question of describing which values $[KL : \mathbb{Q}]$ can take if K and L are two extensions of prime degree p over $\mathbb{Q}$ is open". The purpose of this paper is to answer this question. Some partial results can be found in [8, Theorem 1.2], where it was established that the degree of compositum KL over $\mathbb{Q}$ can never be equal to $p(p-l)$, provided that l is a positive integer satisfying $2 \le l < (1+\sqrt{4p-3})/2$. It is also clear from (1), that $[KL : \mathbb{Q}]$ must be divisible by p and be smaller than or equal to p^2. Therefore the problem can be restated as follows:

Problem. *Find all compositum-feasible triplets of the form (p,p,ps) such that p is prime and $s \in \{1,2,\ldots,p\}$.*

If $s = p$, then it is known that (p,p,ps) is compositum-feasible for any p [9, Proposition 19]. On the the other hand, if $s < p$ and (p,p,ps) is compositum-feasible, then by applying a modified version of [8, Theorem 1.4] we demonstrate that there exists a transitive permutation group G of prime degree p, which has two subgroups H_1 and H_2 such that

$$[G : H_1] = [G : H_2] = p \quad \text{and} \quad [G : H_1 \cap H_2] = ps. \tag{2}$$

All transitive permutation groups of prime degree p are classified, therefore G must be one of the groups listed in [6, Corollary 3.5]. In this particular case, it is also relatively well-known what type of subgroups have index p in G. In this paper, by applying certain properties of such subgroups, we determine all possible values of p and s in (2).

In the context of groups, the notation $A \le B$ is used to indicate that A is a subgroup of B. As usually, $\mathrm{PSL}(n,q)$ and $\mathrm{P\Gamma L}(n,q)$ denote the projective special linear group and the projective semilinear group, respectively, of dimension n over the finite field of q elements [5, Chapter 1.7]. The main result of this paper is the following:

Theorem 1.1. *The triplet (p,p,ps) with p prime is compositum-feasible if and only if one of the following conditions is satisfied:*

(a) $s = p$,
(b) $s \mid (p-1)$,
(c) $(p, s) = (11, 6)$,
(d) $(p, s) = ((q^n - 1)/(q-1), q^{n-1})$, *where q is prime or a power of a prime, $n \geq 3$, and there exists a transitive permutation group G of prime degree p satisfying* $\mathrm{PSL}(n, q) \leq G \leq \mathrm{P\Gamma L}(n, q)$, *which is realizable over* $\mathbb{Q}$.

Parts (c) and (d) of Theorem 1.1 to a great extent follow from the result first published by Feit [16, Corollary 4.5], namely that a group G has two non-equivalent doubly transitive permutation representations of prime degree p only if $G = \mathrm{PSL}(2, 11)$ and $p = 11$ or $\mathrm{PSL}(n, q) \leq G \leq \mathrm{P\Gamma L}(n, q)$ and $p = (q^n - 1)/(q-1)$ for some $n \geq 3$. The smallest example corresponding to case (d) of Theorem 1.1 can be found in [8, Theorem 1.3], where the properties of the projective special linear group $\mathrm{PSL}(2, 7)$ were applied to prove that $(7, 7, 7 \cdot 4)$ is compositum-feasible. Observe that $7 = (2^3 - 1)/(2-1)$, thus acoording to the notation used in Theorem 1.1, we have that $q^{n-1} = 2^2 = 4$ and $\mathrm{PSL}(3, 2) \leq G \leq \mathrm{P\Gamma L}(3, 2)$. Since $\mathrm{PSL}(3, 2) \cong \mathrm{PSL}(2, 7)$ is realizable over $\mathbb{Q}$ [13], the triplet $(7, 7, 7 \cdot 4)$ is compositum-feasible.

Consider the equation

$$p = \frac{q^n - 1}{q - 1}, \tag{3}$$

where p is a prime, q is a prime or a power of a prime and $n \geq 3$. For (3) to hold some necessary conditions can be found in the work by Estes, Guralnick, Schacher and Straus [14, Lemma 1]. Primes p satisfying (3) are examples of repunit primes to base q (primes, which contain only the digit 1 in base q). From the lists of repunit primes in the works by Dubner [11], Williams and Seah [29] one can deduce that the only triplets (p, q, n) satisfying (3) with $p < 1000$ are

$$(7, 2, 3), (13, 3, 3), (31, 2, 5), (31, 5, 3), (73, 8, 3), (127, 2, 7), (307, 17, 3),$$
$$(757, 27, 3).$$

Thus, for primes $p < 1000$ there are eight examples for which part (d) of Theorem 1.1 applies. However, this still leaves the question open whether the corresponding projective groups are realizable over $\mathbb{Q}$, since at the present time only the triplets $(7, 2, 3)$ and $(13, 3, 3)$ have been confirmed to be compositum-feasible. Finally, note that for $p = 31$ we have two cases to consider. In fact, if the conjecture of Ratat and Goormaghtigh [23, Conjecture A] is true, then $p = 31$ is the only prime for which (3) has two solutions.

To this day all compositum-feasible triplets (a, b, c) satisfying $a \leq b \leq 9$ have been found [9, Theorem 5], [8, Corollary 1.5], [10, Theorem 1]. As an application of Theorem 1.1, we find all compositum-feasible triplets $(a, 13, c)$ satisfying $a \leq 13$.

Corollary 1.2. *The triplet $(a, 13, c)$, where $a \leq 13$ is compositum-feasible if and only if $c = 13a$ or $a = 13$ and $c = 13s$ with $s \in \{1, 2, 3, 4, 6, 9, 12\}$.*

Observe that the triplet $(13, 13, 13 \cdot 9)$ is the second smallest example of a compositum-feasible triplet corresponding to part (d) of Theorem 1.1.

Knowing which values $[KL : \mathbb{Q}]$ can take if K and L are two extensions of degrees a and b over $\mathbb{Q}$ is related to the following question posed in *MathOverflow*[4]: given two algebraic numbers α and β of degrees a and b over $\mathbb{Q}$, respectively, what are the possible values for the degree of $\alpha+\beta$ and $\alpha\beta$? The research on this matter began in [9], where the following definitions were introduced. A triplet $(a, b, c) \in \mathbb{N}^3$ is called *sum-feasible* (resp. *product-feasible*) if there exist three algebraic numbers α, β, γ with degrees a, b, c over $\mathbb{Q}$ respectively, such that $\alpha+\beta+\gamma = 0$ (resp. $\alpha\beta\gamma = 1$). As opposed to compositum-feasible triplets, if the triplet (a, b, c) is sum-feasible (resp. product-feasible), then clearly, for any permutation $\{a', b', c'\}$ of $\{a, b, c\}$, the triplet (a', b', c') is also sum-feasible (resp. product-feasible). Thus, the triplet (a, b, c) can be sum-feasible (resp. product-feasible) even if $c < \max\{a, b\}$, while if (a, b, c) is compositum-feasible, then necessarily $c \geq \max\{a, b\}$, since c is divisible by $\operatorname{lcm}(a, b)$.

Let $\mathbb{PF}$ denote the set of all product-feasible triplets, $\mathbb{SF}$ - the set of all sum-feasible triplets and $\mathbb{CF}$ - the set of all compositum-feasible triplets. Then

$$\mathbb{CF} \subset \mathbb{SF} \subset \mathbb{PF}. \tag{4}$$

Indeed, if the triplet is compositum-feasible triplet, then it is also sum-feasible and product-feasible [9, Proposition 1]. Thus, for example, Corollary 1.2 implies that there exist three algebraic numbers α, β, γ satisfying $\alpha + \beta + \gamma = 0$ (resp. $\alpha\beta\gamma = 1$) such that the degree of both α and β is 13 while the degree of γ is $13 \cdot 9$. In [7, Theorem 1.1] it was proved that if the triplet is sum-feasible then it is also product-feasible. On the other hand, consider the following algebraic numbers

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

The degrees of α, β, γ are equal to $2, 3, 3$, respectively, and clearly, $\alpha\beta\gamma = 1$. Hence, the triplet $(2, 3, 3)$ is product-feasible. However by [9, Theorem 5], the triplet $(2, 3, 3)$ is not sum-feasible. Another example is the triplet $(4, 6, 6)$, which by [9, Theorem 29.ii] is sum-feasible. However, it is not compositum-feasible, as 4 does not divide 6.

From (4) it follows that every compositum-feasible triplet arising from Theorem 1.1 is also sum-feasible and product-feasible. It turns out that with few exceptions, there are no other sum-feasible or product-feasible triplets of the type (p, p, l), where p is prime and l is some positive integer.

Theorem 1.3. *If the triplet (p, p, l) with p prime is sum-feasible, then it is also compositum-feasible or $l = 1$.*

Assume, that α and β are two algebraic numbers, both of degree p over $\mathbb{Q}$ and $\alpha + \beta \notin \mathbb{Q}$. Then Theorem 1.3 tells us that the degree of $\alpha + \beta$ can only take values equal to ps, where s is determined in Theorem 1.1. In the case of product-feasible triplets we prove the following:

Theorem 1.4. *If the triplet (p, p, l) with p prime is product-feasible, then it is also compositum-feasible or $l \in \{1, p-1\}$.*

In Section 2, some known auxiliary results are provided related to our topic as well as several new lemmas are formulated such as Lemma 2.4, Lemma 2.7 and Lemma 2.8. In Section 3, we determine the properties of non-solvable transitive permutation groups of prime degree, which will be essential in the proofs of Theorem 1.1 and Theorem 1.3. In Section 4, we complete the proof of Theorem 1.1 for compositum-feasible triplets and give a numerical example in Corollary 1.2. In Section 5, Theorem 1.3 is proved for sum-feasible triplets. Finally in Section 6, Theorem 1.4 is proved for product-feasible triplets.

2. Auxiliary results

Lemma 2.1. *Let* $\gcd(a, b) = 1$. *Then* $(a, b, c) \in \mathbb{N}^3$ *is compositum-feasible if and only if* $c = ab$.

Proof. If the triplet $(a, b, c) \in \mathbb{N}^3$ is compositum-feasible, then there exist algebraic numbers α and β of degrees a and b, respectively, such that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = a, \quad [\mathbb{Q}(\beta) : \mathbb{Q}] = b \quad \text{and} \quad [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = c.$$

On the one hand,

$$c = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = ab. \tag{5}$$

On the other hand, from $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$ and $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha, \beta)$ together with $\gcd(a, b) = 1$, we get

$$\operatorname{lcm}(a, b) = ab \mid c. \tag{6}$$

Combining (5) and (6) we have that, $c = ab$. In the other direction, (a, b, ab) is compositum-feasible by [9, Proposition 19]. □

Lemma 2.2 ([9, Proposition 2])**.** *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.*

Lemma 2.3 ([9, Proposition 1])**.** *If the triplet $(a, b, c) \in \mathbb{N}^3$ is compositum-feasible, then it is also sum-feasible and product-feasible.*

Let K and L be two field extensions of $\mathbb{Q}$ contained in some common field. K is said to be linearly disjoint from L over $\mathbb{Q}$ if every finite set of elements of K that is linearly independent over $\mathbb{Q}$ is still so over L. Let M^{Gal} denote the Galois closure of the number field M. The next lemma, which is due to P. Drungilas, indicates that two number fields of prime degree p are either linearly disjoint over $\mathbb{Q}$ or their Galois closures coincide.

Lemma 2.4. *Suppose that K and L are number fields both of prime degree p. If $[KL : \mathbb{Q}] < p^2$, then $K^{\mathrm{Gal}} = L^{\mathrm{Gal}}$.*

Proof. Suppose on the contrary, that $[KL : \mathbb{Q}] < p^2$ and $K^{\mathrm{Gal}} \neq L^{\mathrm{Gal}}$. It follows then that either $K \nsubseteq L^{\mathrm{Gal}}$ or $L \nsubseteq K^{\mathrm{Gal}}$. Assume without loss of generality, that $K \nsubseteq L^{\mathrm{Gal}}$. The number field $K \cap L^{\mathrm{Gal}}$ is a proper subfield of K whose degree over $\mathbb{Q}$ is a prime number. Therefore $K \cap L^{\mathrm{Gal}} = \mathbb{Q}$, implying that K and L^{Gal} are linearly disjoint over $\mathbb{Q}$ [28, Lemma 3.4.17]. Since the subextensions of linearly disjoint extensions are also linearly disjoint [22, Chapter 8, Proposition 3.1], it follows that the number field K and a subfield L of L^{Gal} are linearly disjoint over $\mathbb{Q}$, which happens if and only if $[KL : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [L : \mathbb{Q}] = p^2$ [28, Lemma 3.4.16], a contradiction. Therefore, if $[KL : \mathbb{Q}] < p^2$, then $K^{\mathrm{Gal}} = L^{\mathrm{Gal}}$. It is also evident that if $K^{\mathrm{Gal}} \neq L^{\mathrm{Gal}}$, then $[KL : \mathbb{Q}] = p^2$; i.e., K and L are linearly disjoint. □

Lemma 2.5. *Suppose that K and L are number fields both of prime degree p and $[KL : \mathbb{Q}] < p^2$. Then $(KL)^{\mathrm{Gal}} = L^{\mathrm{Gal}} = K^{\mathrm{Gal}}$.*

Proof. Since $[KL : \mathbb{Q}] < p^2$, Lemma 2.4 implies that $L^{\mathrm{Gal}} = K^{\mathrm{Gal}}$. It is clear that $L^{\mathrm{Gal}} = K^{\mathrm{Gal}} \subseteq (KL)^{\mathrm{Gal}} \subseteq K^{\mathrm{Gal}} L^{\mathrm{Gal}}$. By [12, Chapter 14, Corollary 20],

$$[K^{\mathrm{Gal}} L^{\mathrm{Gal}} : \mathbb{Q}] = \frac{[K^{\mathrm{Gal}} : \mathbb{Q}][L^{\mathrm{Gal}} : \mathbb{Q}]}{[K^{\mathrm{Gal}} \cap L^{\mathrm{Gal}} : \mathbb{Q}]} = \frac{[L^{\mathrm{Gal}} : \mathbb{Q}][L^{\mathrm{Gal}} : \mathbb{Q}]}{[L^{\mathrm{Gal}} : \mathbb{Q}]} = [L^{\mathrm{Gal}} : \mathbb{Q}].$$

Therefore, $L^{\mathrm{Gal}} = K^{\mathrm{Gal}} L^{\mathrm{Gal}}$ and hence, $L^{\mathrm{Gal}} = K^{\mathrm{Gal}} = (KL)^{\mathrm{Gal}}$. □

Lemma 2.6 ([8, Theorem 1.4]). *A triplet $(a, b, c) \in \mathbb{N}^3$ is compositum-feasible if and only if there exists an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree c such that the Galois group G of its splitting field has two subgroups H_1 and H_2 such that $[G : H_1] = a$, $[G : H_2] = b$ and $[G : H_1 \cap H_2] = c$.*

Lemma 2.6 shows that compositum-feasible triplets of the form (p, p, ps) with p prime can be determined by checking all possible transitive permutation subgroups of the full symmetric group S_{ps}, which occur as Galois groups for some irreducible polynomial of degree ps in $\mathbb{Q}[x]$. Note that this method is difficult to apply in practice, as it requires knowing the complete list of Galois groups of degree ps. However if $s < p$, the next lemma shows that it is sufficient to know Galois groups only of prime degree p.

Lemma 2.7. *Let p be a prime number and $s \in \{1, 2, ..., p-1\}$. A triplet (p, p, ps) is compositum-feasible if and only if there exists an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree p such that the Galois group G of its splitting field has two subgroups H_1 and H_2 such that $[G : H_1] = p$, $[G : H_2] = p$ and $[G : H_1 \cap H_2] = ps$.*

Proof. *Necessity.* Suppose that a triplet (p, p, ps) is compositum-feasible. Then there exist number fields K and L, both of degree p over $\mathbb{Q}$, such that their compositum KL has degree ps over $\mathbb{Q}$. By the primitive element theorem, there exists an algebraic number α such that $K = \mathbb{Q}(\alpha)$. Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Clearly, $\deg(f(x)) = p$. Note that K^{Gal} is the splitting field of $f(x)$. Let G denote the Galois group of $f(x)$; i.e.,

$$G = \{\tau \in \mathrm{Aut}(K^{\mathrm{Gal}}) \mid \tau(t) = t \text{ for all } t \in \mathbb{Q}\}.$$

Since $[KL : \mathbb{Q}] = ps < p^2$, Lemma 2.5 implies that $K^{\mathrm{Gal}} = (KL)^{\mathrm{Gal}}$. Hence, $(KL)^{\mathrm{Gal}}$ has the Galois group isomorphic to G. Finally, by the fundamental theorem of Galois theory ([12, Chapter 14, Theorem 14]), the group G has two subgroups H_1 and H_2 corresponding to fields K and L such that $[G : H_1] = p$, $[G : H_2] = p$ and $[G : H_1 \cap H_2] = ps$, where $H_1 \cap H_2$ corresponds to compositum KL.

Sufficiency. The sufficiency part does not require Lemma 2.5, therefore we omit its proof as it is identical to that of Lemma 2.6 provided in [8, Theorem 1.4]. □

Lemma 2.7 implies that in order to find all compositum-feasible triplets (p, p, ps) with p prime and $s \in \{1, 2, ..., p-1\}$ it is enough to study only Galois groups G of prime degree p instead of degree ps. Recall that if (p, p, ps) is compositum-feasible, then $s \leq p$. Also, as it was noted in the Introduction, the case $s = p$ is a trivial one. Therefore, for the rest of the paper we can assume that $s \in \{1, 2, ..., p-1\}$. Next, we state some results on transitive permutations groups G of prime degree separating the cases when G is solvable and non-solvable (for a definition of solvability see, for example, [28, Definition 4.3.1]). The following lemma is due P. Drungilas.

Lemma 2.8. *Let p be a prime number and $s \in \{1, 2, ..., p-1\}$.*

(a) If G is a solvable transitive permutation group of prime degree p and H_1, H_2 are two subgroups of G such that $[G : H_1] = [G : H_2] = p$, then $[G : H_1 \cap H_2] = ps$ and $s \mid (p-1)$.

(b) If $s \mid (p-1)$, then there exists a solvable Galois group G of prime degree p, which has two subgroups H_1 and H_2 such that $[G : H_1] = [G : H_2] = p$ and $[G : H_1 \cap H_2] = ps$.

Proof. (a) Since G is transitive of prime degree p, we have that $|G|$ is divisible by p. On the other hand, solvability of G implies that $|G|$ divides $p(p-1)$ [28, Corollary A.1.8]. Thus, if H_1 and H_2 are two subgroups of G such that $[G : H_1] = [G : H_2] = p$, then clearly $[G : H_1 \cap H_2] = ps$ and $s \mid (p-1)$.
(b) Let $s \mid (p-1)$ and consider a finite field $\mathbb{F}_p$ of p elements. It is well-known that the multiplicative group $\mathbb{F}_p^\times$ is cyclic of order $p-1$. Let C be a cyclic subgroup of $\mathbb{F}_p^\times$ whose order is s. Consider the group G of invertible affine transformations

$$f_{a,b} : \mathbb{F}_p^\times \to \mathbb{F}_p^\times, \quad a \in C, \quad b \in \mathbb{F}_p, \quad f_{a,b}(x) = ax + b.$$

It is well-known (see, e.g., Example 3.4.1 of [6]) that G is the Frobenius group of degree p whose order is ps. Since $ps \mid p(p-1)$, the group G is solvable [28, Corollary A.1.8]. Also, every Frobenius group is realizable over $\mathbb{Q}$ (see, e.g., Theorem 1 of [26]); i.e., G is a Galois group over $\mathbb{Q}$. Let $c \in C$ be a generator of C. Let H_1 and H_2 be the subgroups of G generated by $f_{c,0}$ and $f_{c,1}$, respectively. One can easily check that both subgroups H_1 and H_2 are cyclic of order s and that $[G : H_1] = [G : H_2] = p$ and $[G : H_1 \cap H_2] = ps$. □

From Lemma 2.7 applied to the result of Lemma 2.8 it follows that the triplet (p, p, ps) with p prime and $s \mid p-1$ is compositum-feasible, and there is no other form of compositum-feasible triplets induced by solvable Galois groups of prime degree p. The situation with non-solvable Galois groups of prime degree is more subtle and will be dealt with in more depth in Section 3. Let S_p, A_p and M_p denote the symmetric, the alternating and Mathieu groups of degree p, respectively.

Lemma 2.9 ([16, Corollary 4.2]; see also [17, Corollary 2.39])**.** *If G is a non-solvable transitive permutation group of prime degree p, then:*

(a) $G = A_p$ *or* $G = S_p$,
(b) $G = M_{11}$ *with* $p = 11$ *or* $G = M_{23}$ *with* $p = 23$,
(c) $G = \mathrm{PSL}(2, 11)$ *with* $p = 11$,
(d) $\mathrm{PSL}(n, q) \leq G \leq \mathrm{P\Gamma L}(n, q)$ *with* $p = (q^n - 1)/(q - 1)$, *where q is a prime or a power of a prime;*

If $G \cong M_{23}$ or $\mathrm{PSL}(n, q) \leq G \leq \mathrm{P\Gamma L}(n, q)$ it is not known whether G is realizable over $\mathbb{Q}$, while all other groups in the list of Lemma 2.9 indeed occur as Galois groups of prime degree p.

Lemma 2.10 ([6, Corollary 3.5.B])**.** *A transitive permutation group of prime degree p is doubly transitive or solvable.*

Lemma 2.10 implies that all non-solvable groups of prime degree are doubly transitive. If a group G acts on a set X, then for any $x \in X$, the stabilizer of x in G is denoted by G_x.

Lemma 2.11. *Let G be a non-solvable transitive permutation group acting on a set X such that $|X| = p$ and p is prime. Then $[G : G_{x_i} \cap G_{x_j}] = p(p-1)$ for all $x_i, x_j \in X$ whenever $x_i \neq x_j$.*

Proof. G is non-solvable, hence, by Lemma 2.10, it is doubly transitive. Consequently, G_{x_i} is transitive on $X \setminus \{x_i\}$ for any $x_i \in X$. From the orbit-stabilizer theorem [6, Theorem 1.4A] it follows easily that for $x_i \neq x_j$ we have

$$|G| = [G : G_{x_i}][G_{x_i} : G_{x_i,x_j}]|G_{x_i,x_j}| = p(p-1) \cdot |G_{x_i,x_j}|, \tag{7}$$

where $G_{x_i,x_j} = \{g \in G \mid g \cdot x_i = x_i \text{ and } g \cdot x_j = x_j\}$. Observe also that $G_{x_i,x_j} = G_{x_i} \cap G_{x_j}$, therefore by rearranging (7) we get

$$[G : G_{x_i} \cap G_{x_j}] = [G : G_{x_i,x_j}] = |G|/|G_{x_i,x_j}| = p(p-1).$$

□

Lemma 2.11 implies that the index of a two-point stabilizer in a doubly transitive permutation group of prime degree p is equal to $p(p-1)$. The following lemma will be useful in Section 3.

Lemma 2.12 ([5, Theorem 1.50]). *Let V be an n-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements. For any $1 \leq k \leq n$, the number of k-dimensional subspaces belonging to V is equal to*

$$\frac{\prod_{i=0}^{k-1}(q^n - q^i)}{\prod_{i=0}^{k-1}(q^k - q^i)}.$$

Finally, we state a theorem of Capelli, which will be applied in the proof of Theorem 1.4.

Lemma 2.13 ([27, p. 92]). *Let K be a field and let $m \geq 2$ be an integer. The polynomial $x^m - a$, where $a \in K$, is irreducible over K except when, for some $b \in K$, either $a = -4b^4$ and $4 \mid m$ or $a = b^p$ with some prime $p \mid m$.*

3. Non-solvable transitive permutation groups of prime degree

A linear representation of a group G on a vector space V over a field $\mathbb{F}$ is a group homomorphism $\phi : G \to \mathrm{GL}(V)$. The general linear group $\mathrm{GL}(V)$ is composed of all bijective linear transformations $V \to V$. If V is of finite dimension n with basis $(e_1, \dots e_n)$, it is common to identify $\mathrm{GL}(V)$ with $GL(n, \mathbb{F})$, the group of all invertible $n \times n$ matrices over $\mathbb{F}$. The dimension of V is called the degree of the representation. Let V be a finite-dimensional vector space over $\mathbb{F}$ and let $\mathrm{Tr}(\phi(g))$ denote the trace of a matrix $\phi(g)$ with $g \in G$. The character of ϕ is the function $\chi_\phi : G \to \mathbb{F}$ given by $\chi_\phi(g) = \mathrm{Tr}(\phi(g))$. The space of all complex characters has an inner product structure defined as

$$\langle \chi_\phi, \chi_\psi \rangle_G := \frac{1}{|G|} \sum_{g \in G} \chi_\phi(g) \overline{\chi_\psi(g)},$$

where the characters χ_ϕ and χ_ψ correspond to representations ϕ and ψ of G, respectively, and $\overline{\chi_\psi(g)}$ denotes the complex conjugate of $\chi_\psi(g)$ [12, p. 870].

For the purpose of our analysis, of particular importance is the permutation representation of a finite group G associated with a set X of size n. In general, the permutation representation of G on X is defined as a homomorphism $\phi : G \to \mathrm{Sym}(X)$ such that ϕ_g is the permutation of X, which sends $x \in X$ to $\phi_g(x)$. In this case we say that G acts on X and the image of x we denote as gx. A very useful observation is that every permutation representation can be analyzed as a linear representation. Indeed, if V denotes an n-dimensional vector space with basis $(e_x)_{x \in X}$ indexed by the elements of X, then the permutation representation of G on X corresponds to a homomorphism $\phi : G \to GL(V)$ such that ϕ_g is a bijective linear transformation from V to V, which sends e_x to e_{gx}. The elements of $\phi(G)$ in this case are the permutation matrices and the character of ϕ indicates the number of fixed points of X under the action of ϕ_g on X. Thus, the language of linear representations and that of permutation

groups can be used interchangeably when the permutation representation of a group G is considered (see [12, Chapter 18.3, Example 3]).

Let ϕ and ψ be two permutation representations of the same group G on sets X and Y, respectively. These representations are called equivalent if there is a bijection $f : X \to Y$ such that $f(\phi_g(x)) = \psi_g(f(x))$; i.e., $\phi(G)$ and $\psi(G)$ permutes elements in the same way on the sets X and Y after two sets are matched appropriately. Every transitive action of a group G is equivalent to an action of G on some coset space G/H, where H is a subgroup of G. Assume that H_1 and H_2 are two subgroups of index n in G. Then two permutation representations of G on G/H_1 and on G/H_2, respectively, are equivalent if and only if H_1 and H_2 are conjugate subgroups in G [6, p. 22].

If V is the one-dimensional vector space and I is the identity automorphism of V, then a homomorphism $\rho : G \to GL(V)$ given by $\rho(g) = I$ for all $g \in G$ is called the trivial representation of G with character χ_ρ denoted by 1_G. It is a well-known fact in the representation theory of groups, that the permutation representation of G on the coset space G/H can be obtained as a representation of G induced by the trivial representation of H [25, Chapter 3.3, Example 2]. The character of such induced representation is denoted by $\mathrm{Ind}_H^G 1_H$. Since $[G : H_1] = [G : H_2] = n$, the induced representations of G by the trivial representations of H_1 and H_2, respectively, have the same degree. If $n = p$, where p is a prime number, it turns out that any two such representations afford the same character [15, Theorem 6.2]. This fact will be implicitly used in the proof of Corollary 3.2, which shows that the analysis of non-solvable simple groups can be narrowed to two types of groups as far as our research question is concerned.

Lemma 3.1 ([16, Corollary 4.5])**.** *Let p be a prime and suppose that G has two non-equivalent doubly transitive permutation representations on p points which afford the same character. Then either $p = 11$ and $G = \mathrm{PSL}(2, 11)$ or $p = (q^n - 1)/(q - 1)$ for some $n \geq 3$ and $\mathrm{PSL}(n, q) \leq G \leq \mathrm{P\Gamma L}(n, q)$.*

Corollary 3.2. *Suppose that p is a prime number and let G be a non-solvable transitive permutation group on p points such that neither $G \cong \mathrm{PSL}(2, 11)$ nor $\mathrm{PSL}(n, q) \leq G \leq \mathrm{P\Gamma L}(n, q)$. Then G contains the unique conjugacy class of subgroups of index p, namely, point stabilizers.*

Proof. Let H denote a point stabilizer in G. Clearly, $[G : H] = p$. Since G is transitive, all point stabilizers in G form a single conjugacy class [6, Corollary 1.4A]. Thus, G has at least one conjugacy class of subgroups of index p. Assume that G contains $k > 1$ conjugacy classes of subgroups of index p. It follows then that G has k non-equivalent permutation representations of degree p, which afford the same character. The group G is non-solvable, therefore by Lemma 2.10, it is doubly transitive. Hence, Lemma 3.1 implies that $G \cong \mathrm{PSL}(2, 11)$ or $\mathrm{PSL}(n, q) \leq G \leq \mathrm{P\Gamma L}(n, q)$, a contradiction. Consequently, the set of all point stabilizers is the unique conjugacy class of subgroups of index p in G. $\square$

Corollary 3.3. *Suppose that p is a prime number and let G be a non-solvable transitive permutation group on p points such that neither $G \cong \mathrm{PSL}(2,11)$ nor $\mathrm{PSL}(n,q) \leq G \leq \mathrm{P\Gamma L}(n,q)$. If H_1 and H_2 are two subgroups of G such that $[G : H_1] = [G : H_2] = p$, then $[G : H_1 \cap H_2] = p(p-1)$.*

Proof. By Corollary 3.2, both H_1 and H_2 are point stabilizers. Thus it follows from Lemma 2.11 that $[G : H_1 \cap H_2] = p(p-1)$. □

In the following analysis we concentrate on subgroups of index p in G, when $G \cong \mathrm{PSL}(2,11)$ or $\mathrm{PSL}(n,q) \leq G \leq \mathrm{P\Gamma L}(n,q)$. First, we need the following lemma, which is a special case of a more general theorem of Tits [19].

Lemma 3.4. *Let G be a doubly transitive permutation group on a set X such that $|X| = n$ and let H be a subgroup of index n in G. If H is not transitive on X, then H has exactly two orbits on X.*

Proof. Let ϕ be the permutation representation of G and χ be the character of ϕ. Since G is doubly transitive, χ decomposes into two irreducible characters [25, Chapter 2.3, Exercise 2.6]:

$$\chi = 1_G + \theta \text{ such that } \langle 1_G, \theta\rangle_G = \langle \theta, 1_G\rangle_G = 0, \tag{8}$$

where 1_G is the trivial character and θ has degree $n-1$. Let ϕ_H denote the restriction of ϕ to H and let $\mathrm{Res}_H^G \chi$ denote the character of ϕ_H. If t is the number of orbits of H on X, then

$$\langle 1_H, \mathrm{Res}_H^G \chi\rangle_H = \langle \mathrm{Res}_H^G \chi, 1_H\rangle_H = \frac{1}{|H|}\sum_{h\in H} \mathrm{Res}_H^G \chi(h) = t, \tag{9}$$

(see [25, Chapter 2.3, Exercise 2.5 and Exercise 2.6]). Since H is not transitive on X, we have $t \geq 2$. Recall that $\mathrm{Ind}_H^G 1_H$ denotes the character of the representation of G induced by 1_H and it is equal to the character of the permutation representation of G on the coset space G/H [12, Chapter 19.3, Example 2]. By the Frobenius reciprocity theorem [25, Chapter 7.2, Theorem 13] and orthogonality relations for characters [25, Chapter 2.3, Theorem 3], we get

$$\langle \mathrm{Ind}_H^G 1_H, 1_G\rangle_G = \langle 1_H, 1_H\rangle_H = 1. \tag{10}$$

Hence,

$$\mathrm{Ind}_H^G 1_H = 1_G + \theta', \tag{11}$$

where θ' has degree $n-1$. By Frobenius reciprocity and (9), we have

$$2 \leq t = \langle 1_H, \mathrm{Res}_H^G \chi\rangle_H = \langle \mathrm{Ind}_H^G 1_H, \chi\rangle_G. \tag{12}$$

Using (8), (10), (11) and the fact that θ' and θ both have degree equal to $n-1$ with θ being irreducible, we get

$$\begin{aligned}\langle \mathrm{Ind}_H^G 1_H, \chi\rangle_G &= \langle \mathrm{Ind}_H^G 1_H, 1_G\rangle_G + \langle \mathrm{Ind}_H^G 1_H, \theta\rangle_G = 1 + \langle \mathrm{Ind}_H^G 1_H, \theta\rangle_G \\ &= 1 + \langle 1_G, \theta\rangle_G + \langle \theta', \theta\rangle_G = 1 + \langle \theta', \theta\rangle_G \leq 2.\end{aligned} \tag{13}$$

Consequently, from (12) and (13) it follows that $\theta' = \theta$ and $t = 2$. □

Lemma 3.5. *Let G be a transitive permutation group of prime degree p such that* $\mathrm{PSL}(n,q) \leq G \leq \mathrm{P\Gamma L}(n,q)$ *and* $p = (q^n-1)/(q-1)$. *Also let H_1 and H_2 be subgroups of G such that* $[G : H_1] = [G : H_2] = p$. *Then one of the following holds:*

(a) $[G : H_1 \cap H_2] = p(p-1)$,
(b) $[G : H_1 \cap H_2] = p(p-q^{n-1})$,
(c) $[G : H_1 \cap H_2] = pq^{n-1}$.

Proof. Let q be a prime or a power of prime and let $V = \mathbb{F}_q^n$ denote an n-dimensional vector space over the field $\mathbb{F}_q$. From Lemma 2.12 we see that V contains $(q^n-1)/(q-1)$ one-dimensional subspaces and $(q^n-1)/(q-1)$ hyperplanes (subspaces of codimension 1). It is also well-known that if $p = (q^n-1)/(q-1)$, where p is prime, q is prime or a power of a prime and $n \geq 3$, then G satisfying $\mathrm{PSL}(n,q) \leq G \leq \mathrm{P\Gamma L}(n,q)$, has two non-equivalent doubly transitive permutation representations of prime degree p corresponding to group action of G on the set of all one-dimensional subspaces of V or on the set of all hyperplanes of V, respectively (see [3, Main Theorem]; cf. [1, Theorem 1]). Thus, G has two conjugacy classes of subgroups of index p, namely, stabilizers of a one-dimensional subspace of V and stabilizers of a hyperplane of V. Note that if $n = 2$, one-dimensional subspaces of V coincide with hyperplanes of V, therefore in this case G has only one conjugacy class of subgroups of index p. Consequently, for any two such subgroups, say H_1 and H_2, we have that $[G : H_1 \cap H_2] = p(p-1)$ as a result of Lemma 2.11.

Suppose that $n \geq 3$. Let X be the set of all one-dimensional subspaces of V and let ϕ be the natural permutation representation of G on X. Also let $\langle v\rangle$ denote a one-dimensional subspace of V generated by a vector v, $G_{\langle v\rangle}$ - the stabilizer of $\langle v\rangle$ in G, $\langle v\rangle^G$ - the orbit of $\langle v\rangle$ under G, and G_W - the stabilizer of a hyperplane W. By Lemma 2.12, the hyperplane $W \subset V$ contains

$$(q^{n-1}-1)/(q-1) = (q^n-1)/(q-1) - q^{n-1} = p - q^{n-1}$$

one-dimensional subspaces of V. Hence, if we restrict ϕ to G_W, for any one-dimensional subspace $\langle w\rangle \subset W$ it holds that

$$|\langle w\rangle^{G_W}| \leq p - q^{n-1}. \tag{14}$$

From (14) it also follows that G_W is not transitive on X. Since $[G : G_W] = p$, Lemma 3.4 implies that G_W has exactly two orbits on X. Let $\langle u\rangle$ denote a one-dimensional subspace of V so that $\langle u\rangle \not\subset W$. Clearly, $\langle u\rangle \notin \langle w\rangle^{G_W}$. Thus,

$$|\langle w\rangle^{G_W}| + |\langle u\rangle^{G_W}| = p. \tag{15}$$

On the other hand, under the restriction of ϕ to G_W, the subspace $\langle u\rangle$ cannot be sent to any of the one-dimensional subspaces belonging to W. Hence

$$|\langle u\rangle^{G_W}| \leq p - (p - q^{n-1}) = q^{n-1}. \tag{16}$$

Combining (14) with (16) we get

$$\langle w\rangle^{G_W} + \langle u\rangle^{G_W} \leq (p - q^{n-1}) + q^{n-1} = p. \tag{17}$$

Therefore, from (15) together with (17) it follows that

$$|\langle w\rangle^{G_W}| = p - q^{n-1} \text{ and } |\langle u\rangle^{G_W}| = q^{n-1}; \tag{18}$$

i.e., G_W has two orbits on X, one of size $p-q^{n-1}$ and the other of size q^{n-1} (this fact is also mentioned in [20, Example I.(i)]). Finally, note that the intersection $G_W \cap G_{\langle v\rangle}$ is the stabilizer of $\langle v\rangle$ in G_W. Hence, from $[G : G_W] = p$ and the orbit-stabilizer theorem applied to (18) we get

$$[G : G_W \cap G_{\langle v\rangle}] = \begin{cases} p(p-q^{n-1}), & \text{if } \langle v\rangle \subset W \\ pq^{n-1}, & \text{if } \langle v\rangle \not\subset W. \end{cases} \tag{19}$$

Consequently, if H_1 and H_2 are two subgroups of index p in G belonging to distinct conjugacy classes, then (19) implies that

$$[G : H_1 \cap H_2] = p(p-q^{n-1}) \text{ or } [G : H_1 \cap H_2] = pq^{n-1}.$$

On the other hand, if H_1 and H_2 are subgroups of index p in G belonging to the same conjugacy class (i.e., both H_1 and H_2 correspond to stabilizers of different one-dimensional subspaces of V or both subgroups correspond to stabilizers of different hyperplanes of V), then Lemma 2.11 implies that

$$[G : H_1 \cap H_2] = p(p-1).$$

□

Next, we deal with the case $p = 11$ and $G \cong \mathrm{PSL}(2,11)$.

Lemma 3.6. *Let G be a non-solvable transitive permutation group of prime degree 11 such that $G \cong \mathrm{PSL}(2,11)$. Also let H_1 and H_2 be subgroups of G such that $[G : H_1] = [G : H_2] = 11$. Then one of the following holds:*

(a) $[G : H_1 \cap H_2] = 11 \cdot 10$,
(b) $[G : H_1 \cap H_2] = 11 \cdot 6$,
(c) $[G : H_1 \cap H_2] = 11 \cdot 5$.

Proof. The proof is based on the subgroup structure of $\mathrm{PSL}(2,11)$ provided in a paper by Buekenhout, Cara and Vanmeerbeek [2, Figure 1]. Inside $\mathrm{PSL}(2,11)$ there are two conjugacy classes of subgroups of index 11, both classes comprised of subgroups isomorphic to the alternating group A_5 and are denoted by A_5^A and A_5^B, respectively. In fact, A_5^A and A_5^B correspond to point stabilizers from two different representations of $\mathrm{PSL}(2,11)$ as a transitive permutation subgroup of S_{11}. Thus, if H_1 and H_2 are two subgroups of index 11 in $\mathrm{PSL}(2,11)$ belonging to the same conjugacy class, then by Lemma 2.11,

$$[\mathrm{PSL}(2,11) : H_1 \cap H_2] = 11 \cdot 10 \tag{20}$$

(alternatively, $H_1 \cap H_2 \cong S_3$, hence $[\mathrm{PSL}(2,11) : H_1 \cap H_2] = 660 : 6 = 11 \cdot 10$). On the other hand,

$$A_5^A \cap A_5^B = D_{10} \text{ or } A_5^A \cap A_5^B = A_4,$$

where D_{10} denotes the dihedral group of order 10 and A_4 the alternating group of order 12. Consequently, if H_1 and H_2 are subgroups of index 11 belonging to distinct conjugacy classes, then

$$[\mathrm{PSL}(2,11) : H_1 \cap H_2] = [\mathrm{PSL}(2,11) : D_{10}] = 11 \cdot 6$$

or

$$[\mathrm{PSL}(2,11) : H_1 \cap H_2] = [\mathrm{PSL}(2,11) : A_4] = 11 \cdot 5.$$

□

4. Proofs of Theorem 1.1 and Corollary 1.2

Proof of Theorem 1.1. Let p be a prime number. If the triplet (p, p, ps) is compositum-feasible, then $s \leq p$. If $s = p$, then the triplet (p, p, p^2) corresponding to part (a) of Theorem 1.1 is compositum-feasible by [9, Proposition 19], which states that the triplet (a, b, ab) is compositum-feasible. Hence, by taking $a = b = p$, we get the result. It remains to determine all compositum-feasible triplets (p, p, ps) such that $s \in \{1, 2, ..., p-1\}$. If $s \in \{1, 2, ..., p-1\}$, then Lemma 2.7 states that the triplet (p, p, ps) is compositum-feasible if and only if there exist Galois group G of prime degree p, which has two subgroups H_1 and H_2 such that

$$[G : H_1] = [G : H_2] = p \text{ and } [G : H_1 \cap H_2] = ps.$$

If G is solvable, then from Lemma 2.7 applied to the result of Lemma 2.8 it follows that $s \mid (p-1)$ and that for any divisor s of $(p-1)$, the triplet (p, p, ps) corresponding to part (b) of Theorem 1.1 is compositum-feasible.

The only candidates for non-solvable Galois group G of prime degree are non-solvable transitive permutation groups of prime degree as indicated in Lemma 2.9. Suppose that G is isomorphic to

$$A_p, \quad S_p, \quad M_{11} \quad \text{or} \quad M_{23}. \tag{21}$$

From Lemma 2.7 applied to Corollary 3.3 it follows that the groups in (21) can induce compositum-feasible triplets only of the form $(p, p, p(p-1))$. Since these triplets are covered by part (b) of Theorem 1.1, whether groups mentioned in (21) can actually occur as Galois groups over $\mathbb{Q}$ or not, has no effect on our problem of determining all compositum-feasible triplets (as it was mentioned, A_p, S_p and M_{11} are known to be realizable, while the case of M_{23} is still undecided).

Next, consider the non-solvable transitive permutation group G of degree 11 isomorphic to

$$\mathrm{PSL}(2,11). \tag{22}$$

First, note that $\mathrm{PSL}(2,11)$ is realizable over $\mathbb{Q}$ as it is the Galois group of the following irreducible polynomial

$$x^{11} - 2x^{10} + 3x^9 + 2x^8 - 5x^7 + 16x^6 - 10x^5 + 10x^4 + 2x^3 - 3x^2 + 4x - 1$$

(see a database of number fields of degree 11 in [21]). Thus, from Lemma 2.7 applied to the result of Lemma 3.6 it follows that the full list of compositum-feasible triplets induced by PSL(2, 11) is the following:

$$(11, 11, 11 \cdot 10), \quad (11, 11, 11 \cdot 6), \quad (11, 11, 11 \cdot 5).$$

Observe that $5 \mid (11-1)$, thus $(11, 11, 11 \cdot 5)$ as well as $(11, 11, 11 \cdot 10)$ correspond to part (b), while $(11, 11, 11 \cdot 6)$ corresponds to part (c) of Theorem 1.1.

Finally, suppose that G is such that

$$\mathrm{PSL}(n, q) \leq G \leq \mathrm{P\Gamma L}(n, q) \text{ and } p = (q^n - 1)/(q - 1). \tag{23}$$

From Lemma 2.7 applied to the result of Lemma 3.5 it follows that groups in (23) can induce compositum-feasible triplets only of the following form:

$$(p, p, p(p-1)), \quad (p, p, p(p - q^{n-1})), \quad (p, p, pq^{n-1}).$$

Observe that

$$p - q^{n-1} = (q^n - 1)/(q - 1) - q^{n-1} = (q^{n-1} - 1)/(q - 1)$$

and

$$p - 1 = (q^n - 1)/(q - 1) - 1 = q((q^{n-1} - 1)/(q - 1)).$$

Hence, the triplet $(p, p, p(p - q^{n-1}))$ and obviously the triplet $(p, p, p(p-1))$ can be written as (p, p, ps) subject to $s \mid (p-1)$. Note that such triplets are covered by part (b) of Theorem 1.1, as they arise from solvable Galois groups. On the other hand, since q^{n-1} does not divide $p - 1 = q((q^{n-1} - 1)/(q - 1))$ for $n \geq 3$, the triplet (p, p, pq^{n-1}) can be induced only from the groups G indicated in (23) with the condition that $n \geq 3$. Unless $p = (q^n - 1)/(q - 1)$ is small, it is not known whether G occurs as a Galois group for some polynomial over $\mathbb{Q}$. In conclusion, (p, p, pq^{n-1}) is compositum-feasible if and only if G is realizable over $\mathbb{Q}$. This completes the proof of part (d) of Theorem 1.1.

Since the groups mentioned in (21), (22) and (23) exhaust all groups indicated in Lemma 2.9, there is no other form of compositum-feasible triplets, which could be induced by non-solvable Galois groups of prime degree p. Therefore, Theorem 1.1 is proved. □

Proof of Corollary 1.2. If $a < 13$, Lemma 2.1 implies that the triplet $(a, 13, c)$ is compositum-feasible if and only if $c = 13a$. If $a = 13$, then $(a, 13, c)$ is of the form $(13, 13, 13s)$ and Theorem 1.1 can be applied. Firstly, part (a) of Theorem 1.1 implies that $(13, 13, 13 \cdot 13)$ is compositum-feasible. Secondly, the triplets

$$(13, 13, 13 \cdot 1), (13, 13, 13 \cdot 2), (13, 13, 13 \cdot 3), (13, 13, 13 \cdot 4), (13, 13, 13 \cdot 6),$$
$$(13, 13, 13 \cdot 12)$$

are compositum-feasible by part (b) of Theorem 1.1. Since $1, 2, 3, 4, 6, 12$ are the only divisors of $13 - 1 = 12$, there are no more compositum-feasible triplets corresponding to part (b) of Theorem 1.1. Finally, it is easy to check that if q is a prime or a power of a prime, the equation $13 = (q^n - 1)/(q - 1)$ has a unique solution, namely $q = 3$ and $n = 3$. Thus, $q^{n-1} = 9$. By part (d) of Theorem 1.1,

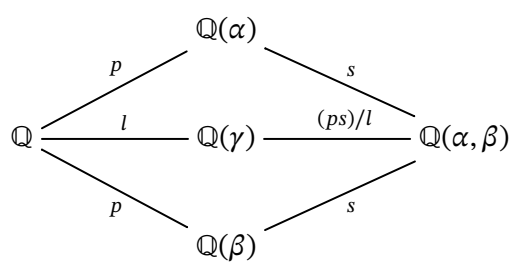
the triplet $(13, 13, 13 \cdot 9)$ is compositum-feasible if and only if there exists a realizable non-solvable group G so that $\mathrm{PSL}(3,3) \leq G \leq \mathrm{P\Gamma L}(3,3)$. Since the polynomial

$$x^{13} - x^{12} - 3x^{11} - 7x^{10} + 37x^9 - 9x^8 - 168x^7 + 24x^6 + 396x^5 + 20x^4 - 128x^3 + 192x^2 - 176x - 16$$

has Galois group isomorphic to $\mathrm{PSL}(3,3)$ (see a database of number fields of degree 13 in [21]), we conclude that $(13, 13, 13{\cdot}9)$ is compositum-feasible. There are no more triplets $(13, 13, 13s)$ satisfying one of the conditions of Theorem 1.1, therefore Corollary 1.2 is proved. □

5. Proof of Theorem 1.3

Proof. With p being prime, all triplets of the form $(p, p, l) = (p, p, ps)$ satisfying one of the conditions of Theorem 1.1 are compositum-feasible, sum-feasible and product feasible as a consequence of Lemma 2.3. Suppose that the triplet (p, p, l) is sum-feasible (resp. product-feasible) but is not compositum-feasible. Then there exists three algebraic numbers α, β, γ of degrees p, p, l, respectively, such that $\alpha + \beta + \gamma = 0$ (resp. $\alpha\beta\gamma = 1$). It is also clear that $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \beta)$, thus $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ is divisible by p. It follows then that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = ps$ for some positive integer s. Also, note that $\mathbb{Q}(\alpha + \beta)$ (resp. $\mathbb{Q}(\alpha\beta)$) $\subseteq \mathbb{Q}(\alpha, \beta)$ and $\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(-\gamma) = \mathbb{Q}(\gamma)$ (resp. $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\gamma^{-1}) = \mathbb{Q}(\gamma)$). Thus, $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\alpha, \beta)$ and therefore, $l \mid ps$. We have the following diagram.



The proof is divided into two cases, namely

$$\gcd(p, l) > 1 \text{ and } \gcd(p, l) = 1.$$

Lemma 5.1. *If* $\gcd(p, l) > 1$*, then there is no sum-feasible (resp. product-feasible) triplet* (p, p, l)*, which is not compositum-feasible.*

Proof. From $\gcd(p, l) > 1$ it follows that $l = pk$ for some positive integer k. Since $l \mid ps$, we get

$$k \mid s. \tag{24}$$

Note that (p, p, ps) is compositum-feasible triplet, therefore by Theorem 1.1:

(a) $s = p$,
(b) $s \mid (p - 1)$,
(c) $s = 6$ and $p = 11$,
(d) $s = q^{n-1}$ and $p = (q^n - 1)/(q - 1)$ with $n \geq 3$.

Assume firstly that $s = p$. Then (24) implies that $k = 1$ or $k = p$. Thus, $(p, p, l) = (p, p, p \cdot 1)$ or $(p, p, l) = (p, p, p \cdot p)$. In both cases (p, p, l) is compositum-feasible by Theorem 1.1, which contradicts our assumption that (p, p, l) is not compositum-feasible. If $s \mid (p-1)$, then from $k \mid s$ we get that $k \mid (p-1)$. Thus, the triplet $(p, p, l) = (p, p, pk)$ is compositum-feasible, a contradiction.

If $s = 6$ and $p = 11$, then from the proof of Theorem 1.1 it follows that the Galois closure of $\mathbb{Q}(\alpha, \beta)$ has Galois group isomorphic to $\mathrm{PSL}(2, 11)$. Note that if $k = 1$, $k = 2$ or $k = 6$, then $(p, p, l) = (p, p, pk)$ is compositum-feasible by Theorem 1.1, a contradiction. The only remaining value of k satisfying (24) is $k = 3$. In this case $l = 11 \cdot 3$ and $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 33$. Thus, from the fundamental theorem of Galois theory it follows that there exists subgroup J of index 33 in $\mathrm{PSL}(2, 11)$. However, from [2, Figure 1] we see that $\mathrm{PSL}(2, 11)$ does not have subgroup of index 33, a contradiction.

The only remaining case is $s = q^{n-1}$ with $p = (q^n - 1)/(q - 1)$ and $n \geq 3$. Since by assumption $(p, p, l) = (p, p, pk)$ is not compositum feasible and $k \mid s$, it follows that $k = q^r$ for some $0 < r < n - 1$. Thus, $l = pq^r$ and we have the following diagram.

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha) \arrow[dr, dash, "q^{n-1}"] & \\
\mathbb{Q} \arrow[ur, dash, "p"] \arrow[r, dash, "pq^r"] \arrow[dr, dash, "p"'] & \mathbb{Q}(\gamma) \arrow[r, dash, "q^{n-1-r}"] & \mathbb{Q}(\alpha, \beta) \\
 & \mathbb{Q}(\beta) \arrow[ur, dash, "q^{n-1}"'] &
\end{tikzcd}$$

From the proof of Theorem 1.1 it follows that the Galois closure of $\mathbb{Q}(\alpha, \beta)$ has Galois group isomorphic to G such that $\mathrm{PSL}(n, q) \leq G \leq \mathrm{P\Gamma L}(n, q)$. Let $V = \mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$, X - the set of all one-dimensional subspaces of V and let ϕ denote the natural permutation representation of G on X. Using the same notation as in the proof of Lemma 3.5, we can assume that subfields $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ and $\mathbb{Q}(\alpha, \beta)$ correspond to subgroups $G_W, G_{\langle v \rangle}$ and $G_W \cap G_{\langle v \rangle}$, respectively. By the fundamental theorem of Galois theory, there exists subgroup J corresponding to subfield $\mathbb{Q}(\gamma)$ such that

$$G_W \cap G_{\langle v \rangle} \leq J \leq G \text{ and } [G : J] = pq^r. \tag{25}$$

Since $[G : G_W \cap G_{\langle v \rangle}] = pq^{n-1}$, we get

$$[J : G_W \cap G_{\langle v \rangle}] = \frac{pq^{n-1}}{pq^r} = q^{n-1-r}. \tag{26}$$

Note also that the compositum of $\mathbb{Q}(\gamma)$ and $\mathbb{Q}(\beta)$ is equal to $\mathbb{Q}(\alpha, \beta)$, which is the compositum of $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$. Thus, by the fundamental theorem of Galois theory

$$J \cap G_{\langle v \rangle} = G_W \cap G_{\langle v \rangle}. \tag{27}$$

Observe that

$$G_W \cap G_{\langle v\rangle} = G_{W,\langle v\rangle} \text{ and } J \cap G_{\langle v\rangle} = J_{\langle v\rangle}, \tag{28}$$

where $G_{W,\langle v\rangle}$ denotes the stabilizer of $\langle v\rangle$ under the restriction of ϕ to G_W and $J_{\langle v\rangle}$ denotes the stabilizer of $\langle v\rangle$ under the restriction of ϕ to J. From (26), (27), (28) and the orbit-stabilizer theorem we have that

$$[J : J_{\langle v\rangle}] = q^{n-1-r} \text{ and } |\langle v\rangle^J| = q^{n-1-r}.$$

Take some one-dimensional subspace $\langle u\rangle \neq \langle v\rangle$ such that $\langle u\rangle \in \langle v\rangle^J$. Consider the two-point stabilizer $J_{\langle v\rangle,\langle u\rangle}$. If the orbit of $\langle u\rangle$ under the restriction of ϕ to $J_{\langle v\rangle}$ has length m, then

$$m = |\langle u\rangle^{J_{\langle v\rangle}}| \leq |\langle u\rangle^J| = |\langle v\rangle^J| = q^{n-1-r} \leq q^{n-2}. \tag{29}$$

From the orbit-stabilizer theorem it follows that

$$[G : J_{\langle v\rangle,\langle u\rangle}] = [G : J_{\langle v\rangle}][J_{\langle v\rangle} : J_{\langle v\rangle,\langle u\rangle}] = pq^{n-1} \cdot m.$$

On the other hand, $J_{\langle v\rangle,\langle u\rangle}$ is a subgroup of $G_{\langle v\rangle,\langle u\rangle}$. Since G is doubly transitive, Lemma 2.11 implies that $[G : G_{\langle v\rangle,\langle u\rangle}] = p(p-1)$. Hence,

$$\frac{|G_{\langle v\rangle,\langle u\rangle}|}{|J_{\langle v\rangle,\langle u\rangle}|} = \frac{pq^{n-1}m}{p(p-1)} \in \mathbb{Z}.$$

Taking into account that $p - 1 = q(q^{n-1} - 1)/(q - 1)$ we see that

$$\frac{pq^{n-1}m}{p(p-1)} = \frac{pq^{n-1}m(q-1)}{pq(q^{n-1}-1)} = \frac{q^{n-2}m(q-1)}{q^{n-1}-1} \in \mathbb{Z}.$$

Clearly, q^{n-2} is coprime to $q^{n-1} - 1$. Hence, $m(q-1)$ is divisible by $q^{n-1} - 1$. However, from (29) we get that

$$m(q-1) \leq q^{n-2}(q-1) < q^{n-1} - 1,$$

a contradiction. Therefore, there is no such subgroup J in G, which satisfies (25). Consequently, there is no sum-feasible (resp. product-feasible) triplet $(p, p, l) = (p, p, pk)$ with $k \mid q^{n-1}$, which is not-compositum-feasible.

We have checked all the possible candidates for the value of $l = pk$, therefore Lemma 5.1 is proved. □

Lemma 5.2. *Suppose* $\gcd(p, l) = 1$. *Then* (p, p, l) *is sum-feasible if and only if* $(p, p, l) = (p, p, 1)$.

Proof. If $\gcd(p, l) = 1$, then by Lemma 2.2, $pl = p$. Therefore, $l = 1$. Clearly, the triplet $(p, p, 1)$ is sum-feasible, but is not compositum-feasible. □

By combining Lemma 5.1 with Lemma 5.2, Theorem 1.3 is proved. □

6. Proof of Theorem 1.4

Proof. From Lemma 5.1 it follows that it is enough to consider only the case $\gcd(p, l) = 1$. By Lemma 5.2, $(p, p, 1)$ is sum-feasible. Thus, it is also product-feasible [7, Theorem 1.1]. Assume that $l \neq 1$. Obviously, (p, p, l) is product-feasible if and only if (l, p, p) is product feasible.

Lemma 6.1. *Let* $\gcd(p, l) = 1$ *and* $l \neq 1$. *Then* (l, p, p) *is product-feasible if and only if* $l = p - 1$.

Proof. Identically as in the proof of Theorem 1.3, if the triplet (l, p, p) is product-feasible, then there exist algebraic numbers α, β, γ such that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = l, [\mathbb{Q}(\beta) : \mathbb{Q}] = p \text{ and } [\mathbb{Q}(\gamma) : \mathbb{Q}] = p.$$

Since $\gcd(p, l) = 1$, we get that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = pl$. Thus, we have the following diagram.

$$\begin{tikzcd}
 & \mathbb{Q}(\alpha) \arrow[dr, dash, "p"] & \\
\mathbb{Q} \arrow[ur, dash, "l"] \arrow[rr, dash, "p"] \arrow[dr, dash, "p"'] & \mathbb{Q}(\gamma) \arrow[r, dash, "l"] & \mathbb{Q}(\alpha, \beta) \\
 & \mathbb{Q}(\beta) \arrow[ur, dash, "l"'] &
\end{tikzcd}$$

Let $\beta_1 := \beta, \beta_2, ..., \beta_p$ be all conjugates of β. Clearly, the numbers

$$\alpha\beta_1, \alpha\beta_2, .., \alpha\beta_p \tag{30}$$

are all different. By [9, Proposition 21], all numbers in (30) are conjugates of $\alpha\beta$. By multiplying all of them we get

$$\alpha^p \beta_1 \beta_2 ... \beta_p \in \mathbb{Q}.$$

Since $\beta_1\beta_2 ... \beta_p \in \mathbb{Q}$, it follows that $\alpha^p \in \mathbb{Q}$. Let $\alpha^p = q$ for some $q \in \mathbb{Q}$. Then α is a root of

$$f(x) = x^p - q.$$

Assume $g(x)$ is the minimal polynomial of α. It follows that

$$g(x) \mid f(x).$$

Since $\deg(g(x)) = l$ and $\gcd(l, p) = 1$, the polynomial $f(x)$ is reducible over $\mathbb{Q}$. Hence, from Lemma 2.13 it follows that $q = q_1^p$ for some $q_1 \in \mathbb{Q}$. Then

$$\begin{aligned} f(x) = x^p - q &= x^p - q_1^p \\ &= (x - q_1) \cdot q_1^{p-1} \cdot \left(\left(\frac{x}{q_1}\right)^{p-1} + \left(\frac{x}{q_1}\right)^{p-2} + ... + 1 \right). \end{aligned} \tag{31}$$

Since the polynomial

$$x^{p-1} + x^{p-2} + ... + 1$$

is irreducible over $\mathbb{Q}$ [28, Example 4.1.8], the polynomial

$$\left(\frac{x}{q_1}\right)^{p-1} + \left(\frac{x}{q_1}\right)^{p-2} + \ldots + 1$$

is irreducible too. Recall that $\deg(g(x)) = l \neq 1$ by assumption. Thus, in light of (31), we conclude that the minimal polynomial of α, namely $g(x)$, has degree $p-1$; i.e., $l = p-1$. On the other hand, by [24, Theorem 4], the triplet $(p-1, p, p)$ is product-feasible. For example, one can take $\alpha = 1/\epsilon, \beta = 1/\sqrt[p]{2}$ and $\gamma = \sqrt[p]{2} \cdot \epsilon$, where $\epsilon = \mathrm{e}^{2\pi i/p}$ is a primitive p^{th} root of unity. □

Clearly, the triplet $(p, p, p-1)$ is product-feasible. On the other hand, $(p, p, p-1)$ is neither compositum-feasible as $p-1 < p$ nor it is sum-feasible as a result of Lemma 5.2. By combining Lemma 5.1 with Lemma 6.1, Theorem 1.4 is proved. □

We remark that Lemma 6.1 implies that the triplet $(4, 7, 7)$ is not product-feasible. This was left undecided in [24].

Acknowledgements. The author is grateful to A. Dubickas for pointing out many helpful suggestions, and to P. Drungilas for the proofs of Lemma 2.4 and Lemma 2.8. The author also thanks the referee for valuable comments.

References

[1] Bannai, Eiichi. Doubly transitive permutation representations of the finite projective special linear groups PSL(n, q). *Osaka Math. J.* **8** (1971), 437–445. MR0313412, Zbl 0253.20007. 182

[2] Buekenhout, Francis; Cara, Philippe; Vanmeerbeek Koen. Geometries of the group PSL$(2, 11)$. *Geom. Dedicata* **83** (2000), no. 1-3, 169–206. MR1800018, Zbl 0969.51018, doi: 10.1023/A:1005204612043. 183, 187

[3] Curtis, Charles W.; Kantor, William M.; Seitz, Gary M. The 2-transitive permutation representations of the finite Chevalley groups. *Trans. Amer. Math. Soc.* **218** (1976), 1–59. MR0422440, Zbl 0374.20002, doi: 10.2307/1997427. 182

[4] Delanoy, Ewan. What is the set of possible values of the degree of the sum of two algebraic numbers with fixed degrees? MathOverflow, 2010. https://mathoverflow.net/questions/30151/. 174

[5] Ding, Cunsheng; Tang, Chunming. Designs from linear codes. Second edition. *World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ*, 2022. xvii+521 pp. ISBN: 978-981-125-132-0; 978-981-125-133-7; 978-981-125-134-4. MR4451270, Zbl 1477.94006, doi: 10.1142/12697. 172, 179

[6] Dixon, John D.; Mortimer, Brian. Permutation groups. Graduate Texts in Mathematics, 163. *Springer-Verlag, New York*, 1996. xii+346 pp. ISBN: 0-387-94599-7. MR1409812, Zbl 0951.20001, doi: 10.1007/978-1-4612-0731-3. 172, 177, 178, 180

[7] Drungilas, Paulius; Dubickas, Artūras. On degrees of three algebraic numbers with zero sum or unit product. *Colloq. Math.* **143** (2016), no. 2, 159–167. MR3466006, Zbl 1409.11084, doi: 10.4064/cm6634-12-2015. 174, 189

[8] Drungilas, Paulius; Dubickas, Artūras; Luca, Florian. On the degree of compositum of two number fields. *Math. Nachr.* **286** (2013), no. 2-3, 171–180. MR3021474, Zbl 1277.11097, doi: 10.1002/mana.201200124. 172, 173, 176, 177

[9] Drungilas, Paulius; Dubickas, Artūras; Smyth, Chris. A degree problem for two algebraic numbers and their sum. *Publ. Mat.* **56** (2012), no. 2, 413–448. MR2978330, Zbl 1297.11133, doi: 10.5565/publmat_56212_07. 172, 173, 174, 175, 184, 189

[10] Drungilas, Paulius; Maciulevičius, Lukas. A degree problem for the compositum of two number fields. *Lith. Math. J.* **59** (2019), no. 1, 39–47. MR3935161, Zbl 1429.11192, doi: 10.1007/s10986-019-09428-x. 173

[11] Dubner, Harvey. Generalized repunit primes. *Math. Comp.* **61** (1993), no. 204, 927–930. MR1185243, Zbl 0783.11006, doi: 10.1090/s0025-5718-1993-1185243-9. 173

[12] Dummit, David S.; Foote, Richard M. Abstract algebra. *Prentice Hall, Inc, Englewood Cliffs, N.J.*, 1991. xiv+658 pp. ISBN: 0-13-004771-6. MR1138725, Zbl 0751.00001. 176, 177, 179, 180, 181

[13] Erbach, D. W.; Fischer, Jerrold.; McKay, John. Polynomials with PSL(2, 7) as Galois group. *J. Number Theory* **11** (1979), no. 1, 69–75. MR0527761, Zbl 0405.12011, doi: 10.1016/0022-314x(79)90020-9. 173

[14] Estes, Dennis R.; Guralnick, Robert M.; Schacher Murray M.; Straus Ernst G. Equations in prime powers. *Pacific J. Math.* **118** (1985), no. 2, 359–367. MR0789176, Zbl 0581.20009, doi: 10.2140/pjm.1985.118.359. 173

[15] Feit, Walter. The representation theory of finite groups. North-Holland Mathematical Library, 25. *North-Holland Publishing Co., Amsterdam-New York*, 1982. xiv+502 pp. ISBN: 0-444-86155-6. MR0661045, Zbl 0493.20007. 180

[16] Feit, Walter. Some consequences of the classification of finite simple groups. *The Santa Cruz Conference on Finite Groups* (Univ. California, Santa Cruz, Calif., 1979), pp. 175–181. Proc. Symp. Pure Math., 37. *Amer. Math. Soc., Providence, R.I.*, 1980. MR0604576, Zbl 0454.20014, doi: 10.1090/pspum/037/604576. 173, 178, 180

[17] Fengler, Svenja Transitive permutation groups of prime degree. Master Thesis, RWTH Aachen University, 2018. http://www.math.rwth-aachen.de/ Gerhard.Hiss/Students/MasterarbeitFengler.pdf. 178

[18] Hungerford, Thomas W. Algebra. Graduate Texts in Mathematics, 73. *Springer-Verlag, New York-Berlin*, 1980. xxiii+502 pp. ISBN: 0-387-90518-9. MR0600654, Zbl 0442.00002, doi: 10.1007/978-1-4612-6101-8.

[19] Ito, Noboru. On a class of doubly, but not triply transitive permutation groups. *Arch. Math. (Basel)* **18** (1967), 564–570. MR0223441, Zbl 0166.28606, doi: 10.1007/bf01898859. 181

[20] Ito, Noboru. On permutation groups of prime degree p which contain (at least) two classes of conjugate subgroups of index p. *Rend. Sem. Mat. Univ. Padova* **38** (1967), 287–292. MR0219603, Zbl 0157.35401. 183

[21] Klüners, Jürgen; Malle, Gunter. A database for number fields. http://galoisdb.math.upb.de/. 185, 186

[22] Lang, Serge. Algebra. Revised third edition. Graduate Texts in Mathematics, 211. *Springer-Verlag, New York*, 2002. xvi+914 pp. ISBN: 0-387-95385-X. MR1878556, Zbl 0984.00001, doi: 10.1007/978-1-4613-0041-0. 176

[23] Le, Maohua. On the Diophantine equation $(x^3-1)/(x-1) = (y^n-1)/(y-1)$. *Trans. Amer. Math. Soc.* **351** (1999), no. 3, 1063–1074. MR1443198, Zbl 0927.11014, doi: 10.1090/S0002-9947-99-02013-9. 173

[24] Maciulevičius, Lukas. On the degree of product of two algebraic numbers. Master thesis, Vilnius University, 2020. https://epublications.vu.lt/object/elaba:69467457. 190

[25] Serre, Jean-Pierre. Linear representations of finite groups. Translated from the second French edition by Leonard L. Scott. Graduate Texts in Mathematics, 42. *Springer-Verlag, New York-Heidelberg*, 1977. x+170 pp. ISBN: 0-387-90190-6. MR0450380, Zbl 0355.20006, doi: 10.1007/978-1-4684-9458-7. 180, 181

[26] Sonn, Jack. $SL(2, 5)$ and Frobenius Galois groups over $\mathbb{Q}$. *Canadian J. Math.* **32** (1980), no. 2, 281–293. MR0571923, Zbl 0436.12006, doi: 10.4153/cjm-1980-021-4. 177

[27] SCHINZEL, ANDRZEJ. Polynomials with special regard to reducibility. Encyclopedia of Mathematics and its Applications, 77. *Cambridge University Press, Cambridge, UK*, 2000. x+558 pp. ISBN: 0-521-66225-7. MR1770638, Zbl 0956.12001, doi: 10.1017/cbo9780511542916. 179

[28] WEINTRAUB, STEVEN H. Galois theory. Second edition. Universitext. *Springer, New York*, 2009. xiv+211 pp. ISBN: 978-0-387-87574-3. MR2459247, Zbl 1195.12001, doi: 10.1007/978-0-387-87575-0. 176, 177, 190

[29] WILLIAMS, HUGH C.; SEAH, ERIC. Some primes of the form $(a^n-1)/(a-1)$. *Math. Comp.* **33** (1979), no. 148, 1337–1342. MR0537980, Zbl 0417.10004, doi: 10.1090/s0025-5718-1979-0537980-7. 173

(Paulius Virbalas) INSTITUTE OF MATHEMATICS, FACULTY OF MATHEMATICS AND INFORMATICS, VILNIUS UNIVERSITY, NAUGARDUKO 24, VILNIUS LT-03225, LITHUANIA
paulius.virbalas@mif.stud.vu.lt

This paper is available via http://nyjm.albany.edu/j/2023/29-6.html.