https://doi.org/10.15388/vu.thesis.679
https://orcid.org/0009-0008-3516-8301

VILNIUS UNIVERSITY

Lukas Maciulevičius

Some Degree Problems in Number Fields

DOCTORAL DISSERTATION

Natural Sciences,
Mathematics (N 001)

VILNIUS 2024

The dissertation was prepared between 2020 and 2024 at Vilnius University.

Academic supervisor – Prof. Dr. Paulius Drungilas (Vilnius University, Natural Sciences, Mathematics, N 001).
Academic consultant – Prof. Habil. Dr. Artūras Dubickas (Vilnius University, Natural Sciences, Mathematics, N 001).

This doctoral dissertation will be defended in a public meeting of the Dissertation Defence Panel:

Chairman – Prof. Habil. Dr. Antanas Laurinčikas (Vilnius University, Natural Sciences, Mathematics, N 001).
Members:
Assoc. Prof. Dr. Jonas Jankauskas (Vilnius University, Natural Sciences, Mathematics, N 001),
Prof. Dr. Chris Smyth (University of Edinburgh, Natural Sciences, Mathematics, N 001),
Prof. Dr. Darius Šiaučiūnas (Vilnius University, Natural Sciences, Mathematics, N 001),
Prof. Dr. Jonas Šiaulys (Vilnius University, Natural Sciences, Mathematics, N 001).

The dissertation shall be defended at a public meeting of the Dissertation Defence Panel at 15:30 on 24th October 2024 in Room 103 of the Faculty of Mathematics and Informatics, Vilnius University.
Address: Naugarduko st. 24, Vilnius, Lithuania.
Tel. +370 5219 3050; e-mail: mif@mif.vu.lt.
The text of this dissertation can be accessed at the Library of Vilnius University, as well as on the website of Vilnius University:
www.vu.lt/lt/naujienos/ivykiu-kalendorius

https://doi.org/10.15388/vu.thesis.679
https://orcid.org/0009-0008-3516-8301

VILNIAUS UNIVERSITETAS

Lukas Maciulevičius

Tam tikri laipsnių uždaviniai skaičių kūnuose

DAKTARO DISERTACIJA

Gamtos mokslai,
matematika (N 001)

VILNIUS 2024

Disertacija rengta 2020–2024 metais Vilniaus universitete.

Mokslinis vadovas – prof. dr. Paulius Drungilas (Vilniaus universitetas, gamtos mokslai, matematika, N 001).
Mokslinis konsultantas – prof. habil. dr. Artūras Dubickas (Vilniaus universitetas, gamtos mokslai, matematika, N 001).

Gynimo taryba:
Pirmininkas – prof. habil. dr. Antanas Laurinčikas (Vilniaus universitetas, gamtos mokslai, matematika, N 001).
Nariai:
doc. dr. Jonas Jankauskas (Vilniaus universitetas, gamtos mokslai, matematika, N 001),
prof. dr. Chris Smyth (Edinburgo universitetas, gamtos mokslai, matematika, N 001),
prof. dr. Darius Šiaučiūnas (Vilniaus universitetas, gamtos mokslai, matematika, N 001),
prof. dr. Jonas Šiaulys (Vilniaus universitetas, gamtos mokslai, matematika, N 001).

Disertacija ginama viešame Gynimo tarybos posėdyje 2024 m. spalio mėn. 24 d. 15:30 Vilniaus universiteto Matematikos ir informatikos fakulteto 103 auditorijoje.
Adresas: Naugarduko g. 24, Vilnius, Lietuva.
Tel. +370 5219 3050; el. paštas mif@mif.vu.lt.

Disertaciją galima peržiūrėti Vilniaus universiteto bibliotekoje ir Vilniaus universiteto interneto svetainėje adresu:
https://www.vu.lt/naujienos/ivykiu-kalendorius

Contents

Acknowledgements **9**

1 Introduction **11**
1.1 Research topic 11
1.2 Aims and problems 12
1.3 Methods 12
1.4 Actuality and novelty 12
1.5 History of the problem and the main results 13
1.6 Approbation 19
1.7 Main publications 20

2 Literature review **21**
2.1 Prerequisites from abstract algebra 21
2.2 Relations between the polynomial roots 25

3 Compositum-feasible triplets **29**
3.1 Statement of the results 29
3.2 Proof of Theorem 3.4 31
3.3 Proof of Theorem 3.3 34
3.4 Proof of Theorem 3.1 38
3.5 Supplementary result 40
3.6 Irreducible compositum-feasible triplets 43

4 Product-feasible triplets **46**
4.1 Statement of the results 46
4.2 Auxiliary lemmas 48
4.3 Proofs of Theorems 4.2 and 4.3 51
4.4 Proof of Theorem 4.4 54
4.5 Proof of Theorem 4.5 57
4.6 Proof of Theorem 4.1 61

4.7 The triplet $(4,6,8)$ 62

5 Conclusions **68**

Bibliography **73**

Santrauka (Summary in Lithuanian) **74**

Tyrimo objektas 74

Tikslai ir uždaviniai 75

Metodai 75

Aktualumas ir naujumas 76

Tyrimų istorija ir rezultatai 76

Aprobacija 82

Publikacijos 83

Išvados 83

Trumpos žinios apie autorių **84**

Acknowledgements

I would like to express special thanks to the following people:

- Prof. Paulius Drungilas, my academic supervisor, for the guidance and extensive support, and particularly for his insight into which mathematical problems could be the most appropriate to me.
- Prof. Artūras Dubickas, my academic consultant, for the fruitful collaboration on the paper [11].
- Prof. Ramūnas Garunkštis, for providing important encouragements during my bachelor's studies.
- Paulius Virbalas, my dear colleague, for valuable discussions on mathematics and beyond.

It is my great luck to be in touch with all of you.

Notation

$\mathbb{N}$	set of positive integers
$\mathbb{Z}$	ring of integers
$\mathbb{Q}$	field of rational numbers
$\mathbb{R}$	field of real numbers
$\mathbb{C}$	field of complex numbers
$\mathbb{Q}_{>0}$	set of positive rational numbers
$\deg \alpha$	degree of an algebraic number α (over $\mathbb{Q}$)
L/K	field extension ($L \supseteq K$)
$[L:K]$	degree of a field extension L/K
$\mathrm{Gal}(L/K)$	Galois group of a field extension L/K
$\mathrm{char}\, K$	characteristic of a field K
$K[x_1, x_2, \ldots, x_n]$	polynomial ring in n variables over a field K
$\varphi(n)$	Euler's totient function
ζ_n	primitive nth root of unity $e^{\frac{2\pi i}{n}}$
$S(X)$	symmetric group on a set X
S_n	symmetric group of degree n
A_n	alternating group of degree n
$\langle \sigma \rangle$	subgroup generated by an element σ
$H \lhd G$	H is a normal subgroup of G
$\cong$	indicates that two structures are isomorphic
$\mathrm{im}\, \varphi$	image of a homomorphism φ
$\ker \varphi$	kernel of a homomorphism φ

Chapter 1

Introduction

1.1 Research topic

The research presented in this thesis is centered around *algebraic numbers* and the main framework is constituted by *number fields*. Recall that a complex number α is called *algebraic* if there exists a nonzero polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with rational coefficients a_i, having α as a root. If there is no such a polynomial of degree less than n, then we say that α is an *algebraic number of degree* n. Meanwhile, by a *number field of degree* n we refer to an extension field K of the field of rational numbers $\mathbb{Q}$ such that K, regarded as a vector space over $\mathbb{Q}$, has finite dimension n.

It is well known that the set of algebraic numbers itself forms a field, i.e., for any algebraic numbers α and β, the sum $\alpha + \beta$ and the product $\alpha \cdot \beta$, as well as the additive and multiplicative inverses $-\alpha$ and α^{-1} (provided $\alpha \neq 0$ for the second case), are also algebraic. Therefore, given two algebraic numbers α and β of certain degrees, one can ask, for instance, what are the possible degrees of $\alpha + \beta$ (or $\alpha \cdot \beta$). In 2012 Drungilas, Dubickas and Smyth [8] introduced a problem to this end:

Find all possible positive integer triplets $(a, b, c) \in \mathbb{N}^3$ *for which there exist two algebraic numbers* α *and* β*, with degrees* a *and* b*, respectively, such that the degree of* $\alpha + \beta$ *equals* c*.*

When such α and β exist, it is said that the triplet (a, b, c) is *sum-feasible*. In fact, Dubickas asked this question in 2007; independently, it is one of

the questions at MathOverflow[1] posed in 2010.

In [8], there are also proposed similar problems for the product of algebraic numbers and the compositum of numbers fields by saying that a triplet $(a, b, c) \in \mathbb{N}^3$ is

- *product-feasible* if there exist algebraic numbers α and β of degrees a and b, respectively, such that the degree of $\alpha \cdot \beta$ is c,
- *compositum-feasible* if there exist number fields K and L of degrees a and b, respectively, such that the degree of their compositum KL is c.

This doctoral thesis extends the investigation of product-feasible and compositum-feasible triplets started in the study by Drungilas et al. [8].

1.2 Aims and problems

In the thesis we aim to

- extend the previous classification of compositum-feasible triplets;
- introduce the notion of an irreducible compositum-feasible triplet and obtain nontrivial examples of such triplets;
- initiate the classification of product-feasible triplets.

1.3 Methods

Most of the methods used in the thesis falls within the scope of abstract algebra. We mainly elaborate the techniques of finite group theory, field theory and Galois theory. Besides various classical theorems, some specific results on the relations between polynomial roots are also used. All these auxiliary results as well as some prerequisites from abstract algebra are overviewd in Chapter 2.

1.4 Actuality and novelty

Most of the results presented in this thesis ar new. A minor exception is Theorem 4.2. The first (quite cumbersome) proof of this theorem

[1] `http://mathoverflow.net/questions/30151/`

appeared in [38]. We proved it independently and published in [26] almost at the same time. Nevertheless, our proof is considerably simpler.

Although algebraic numbers and number fields are very classical objects, their study is still a significant trend in modern mathematics. Apart from general algebraic number theory, these objects are also widely used in computational number theory, Diophantine equations, Diophantine approximations, etc. We hope that our results will be of interest to other researches. Also, study of arithmetical properties of algebraic numbers and number fields is one of directions of Lithuanian school of number theory[2], and our work continues this tradition.

1.5 History of the problem and the main results

Some prehistory As it is noted by Stillwell in [34], one of the first appearances when algebraic numbers took place in its own rigths was in the works of Euler [14]. Namely, Euler performed some far-reaching (though incomplete) manipulations with algebraic numbers to prove that the only positive integer solution of the equation $y^3 = x^2 + 2$ is $(x, y) = (5, 3)$ (see also [34] for a sketch of the Euler's argument).

The more systematic investigation of algebraic numbers was started by Gauss [15]. He studied a particular instance of algebraic numbers, the so-called *Gaussian integers*

$$a + bi, \text{ where } a, b \in \mathbb{Z},$$

as a tool for developing the theory of biquadratic residues. Correspondingly, in studying the cubic residues, Jacobi [19] and Eisenstein [13] developed the arithmetic of the algebraic numbers

$$a + be^{\frac{2\pi i}{3}}, \text{ where } a, b \in \mathbb{Z},$$

which are nowadays known as the *Eisenteins integers*.

This path was followed by Kummer [22, 21]. Speaking in modern terms, Kummer studied the algebraic integers[3] of the pth cyclotomic field for a prime number p (the Gaussian and the Eisenteins integers are

[2] See surveys on the number theory in Lithuania [24, 25].

[3] Recall that an algebraic number is called *algebraic integer* if all the coefficients of its minimal polynomial are in $\mathbb{Z}$.

special cases of these when $p=2$ and $p=3$, respectively). He noticed that these numbers in general do not possess the unique factorization into 'primes' (i.e., the analogue of the fundamental theorem of arithmetic). In order to overcome this defect, Kummer introduced the notion of an *ideal number*. Using this concept, he was able to prove the famous Fermat's last theorem for certain prime exponents, called *regular primes* (for the definitions of an ideal number and a regular prime, see [28, 16]).

Dedekind [4] refined the concept of an ideal number by introducing the more clever notion of an *ideal* which today is basic in ring theory. Also, Dedekind was the first who defined the notion of a number field. He recognized the significant analogy between the arithmetic of number fields and the arithmetic of *algebraic function fields* (that is, algebraic extensions of the field of rational functions $\mathbb{C}(x)$ in one variable x over $\mathbb{C}$). The ideas of Dedekind was further developed by Hilbert, Noether, Artin et al. creating the foundations of modern algebra and algebraic number theory.

The three problems Although our three feasibilty problems seem quite natural, only a few directly related results we can find in the literature until 2012. For instance, [17, 2, 9, 10] provide some sufficient conditions under which the degree of $\alpha+\beta$ is 'maximal possible', i.e., $\deg(\alpha+\beta)=\deg\alpha\cdot\deg\beta$. In particular,

Proposition 1.1 ([17])**.** *Let α and β be algebraic numbers. Suppose $\deg\alpha=a$, $\deg\beta=b$ and $\gcd(a,b)=1$. Then $\deg(\alpha+\beta)=ab$.*

That is to say, if the triplet (a,b,c) is sum-feasible and $\gcd(a,b)=1$, then $c=ab$. Anyway, the systematic treatment of the question on the degree of two algebraic numbers was started in the study of Drungilas et al. [8], and then it was continued in [7, 6].

The three feasibilty problems are related in the following way:

Proposition 1.2 ([8, Proposition 1])**.** *Each compositum-feasible triplet is also sum-feasible.*

Proposition 1.3 ([6, Theorem 1.1])**.** *Each sum-feasible triplet is also product-feasible.*

In other words, if $\mathcal{C}$, $\mathcal{S}$ and $\mathcal{P}$ denote sets of all possible compositum-feasible, sum-feasible and product-feasible triplets, respectively, then the

following inclusions hold:

$$\mathcal{C} \subseteq \mathcal{S} \subseteq \mathcal{P}. \tag{1.1}$$

Consequently, if a triplet is not product-feasible, then it is neither compositum-feasible nor sum-feasible. Moreover, both inclusions in (1.1) are proper. Indeed, as for the first inclusion note that the triplet $(n,n,1)$ is sum-feasible for any positive integer n (e.g., take $\alpha = \sqrt[n]{2}$ and $\beta = -\alpha$). However, it is clear that the triplet $(n,n,1)$ is not compositum-feasible for any integer $n > 1$. As for the second inclusion, note that the triplet $(2,3,3)$ is product-feasible (e.g., take $\alpha = e^{\frac{2\pi i}{3}}$ and $\beta = \sqrt[3]{2}$; then $\alpha\beta$ is conjugate to β and also has degree 3). However, $(2,3,3)$ is not sum-feasible since the sum of any quadratic number and any cubic number must be of degree 6 due to Proposition 1.1.

Clearly, if the triplet (a,b,c) is sum-feasible (resp. product-feasible), then so are all the six possible permutations of (a,b,c). In the case of compositum-feasible triplets, only the degrees a and b (but not c) can be permuted. However, if the triplet (a,b,c) is compositum-feasible, then obviously $a \leqslant c$ and $b \leqslant c$. Thus, when finding sum-feasible, product-feasible or compositum-feasible triplets we may without loss of generality restrict ourselves to the triplets (a,b,c) satisfying $a \leqslant b \leqslant c$.

Note that for any algebraic numbers α and β,

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

This, together with the primitive element theorem, implies that if a triplet (a,b,c) is sum-feasible, product-feasible or compositum-feasible, then we must have

$$c \leqslant ab. \tag{1.2}$$

Moreover, if (a,b,c) is compositum-feasible, then, by the tower law for field extensions,

$$a|c \text{ and } b|c. \tag{1.3}$$

The following proposition gives one more necessary condition for a triplet to be of some feasibility type:

Proposition 1.4 ([8, Lemma 14]). *Suppose that a triplet (a,b,c) is sum-feasible, product-feasible or compositum-feasible. Then $c \mid \operatorname{lcm}(a,b)\cdot t$ for some positive integer $t \leqslant \gcd(a,b)$.*

However, these are not sufficient conditions, and sometimes it may be difficult to decide whether a triplet is of some feasibility type. In [8], all compositum-feasible and also all sum-feasible triplets (a,b,c) satisfying $a \leqslant b \leqslant c$, with $b \leqslant 6$, have been described except for one special case $(6,6,8)$. In [7], the missing case $(6,6,8)$ from that classification has been treated by showing that the triplet $(6,6,8)$ is not sum-feasible, and therefore not compositum-feasible. Thus, the classification has been extended to $b \leqslant 7$.

Chapter 3 of the thesis is devoted to the compositum problem. We extend the previous classification of compositum-feasible triplets to the case $b \leqslant 9$ by proving the following

Theorem 3.1. *Let a and c be positive integers.*

1. *The triplet $(a,8,c)$, $a \leqslant 8$, is compositum-feasible if and only if $c \leqslant 8a$, $a \mid c$ and $8 \mid c$, with a single exceptional triplet $(8,8,40)$, which is not compositum-feasible.*

2. *The triplet $(a,9,c)$, $a \leqslant 9$, is compositum-feasible if and only if $c \leqslant 9a$, $a \mid c$ and $9 \mid c$, with only two exceptional triplets $(9,9,45)$ and $(9,9,63)$, which are not compositum-feasible.*

Apart from the partial classification, [8, 7] also provide more general results on certain special forms of triplets.

Proposition 1.5 ([8, Proposition 19]). *For any positive integers a and b the triplet (a,b,ab) is compositum-feasible.*

Proposition 1.6 ([8, Proposition 29]). *Let $n \geqslant 2$ be an integer.*

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

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

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

In Chapter 3, we obtain some new results related to triplets of the form (n,n,k):

Theorem 3.3. *Let $n \geqslant 4$ be an integer. The triplet $(n, n, n(n-2))$ is compositum-feasible for even n and is not product-feasible for odd n.*

Theorem 3.4. *Let $n \geqslant 8$ be an integer. Then, for any prime number p satisfying $\frac{n}{2} < p < n-2$, the triplet (n, n, np) is not product-feasible.*

Also, in [8], some interesting results related to so called *exponential triangle inequality* were obtained. 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 (for $p \nmid n$ we set $\mathrm{ord}_p(n) = 0$). We say that a triplet $(a, b, c) \in \mathbb{N}^3$ satisfies the *exponent triangle inequality with respect to a prime number p* if

$$\begin{gathered} \mathrm{ord}_p(a) \leqslant \mathrm{ord}_p(b) + \mathrm{ord}_p(c), \quad \mathrm{ord}_p(b) \leqslant \mathrm{ord}_p(a) + \mathrm{ord}_p(c), \quad \text{and} \\ \mathrm{ord}_p(c) \leqslant \mathrm{ord}_p(a) + \mathrm{ord}_p(b). \end{gathered} \tag{1.4}$$

Proposition 1.7 ([8, Theorem 6])**.** *If a triplet $(a, b, c) \in \mathbb{N}^3$ satisfies the exponent triangle inequality with respect to every prime number, then (a, b, c) is sum-feasible and product-feasible.*

Note that the analogous statement for compositum-feasible triplets does not hold. For instance, the triplet $(a, b, c) = (6, 10, 15)$ satisfies (1.4) with respect to every prime p. However, it is not compositum-feasible, because the necessary conditions (1.3) are not satisfied. Nevertheless, Proposition 1.7 can be fixed for the compositum case by replacing (1.4) with a slightly stronger condition:

Proposition 1.8 ([8, Theorem 7])**.** *If a triplet $(a, b, c) \in \mathbb{N}^3$ satisfies*

$$\max\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\} \leqslant \mathrm{ord}_p(c) \leqslant \mathrm{ord}_p(a) + \mathrm{ord}_p(b) \tag{1.5}$$

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

Proposition 1.8 follows from a more general result:

Proposition 1.9 ([8, Corollary 27])**.** *Suppose p is a prime and u, v, w are nonnegative integers such that $\max\{u, v\} \leqslant q \leqslant u + v$. Then, for any compositum-feasible triplet (a, b, c), the triplet (ap^u, bp^v, cp^w) is also compositum-feasible.*

In order to prove Proposition 1.8, take any triplet (a, b, c) satisfying (1.5), and then, starting with the compositum-feasible triplet $(1, 1, 1)$,

apply Proposition 1.9 repeatedly for each prime p that divides at least one of the numbers a, b and c. In particular, it follows

Corollary 1.10. *Suppose p is a prime and u, v, w are nonnegative integers such that $\max\{u,v\} \leqslant q \leqslant u+v$. Then the triplet (p^u, p^v, p^w) is compositum-feasible.*

By the way, Proposition 1.9 is a partial case of the following conjecture which was proposed in [8]:

Conjecture 1.11 ([8, Conjecture 6])**.** *If the triplets (a,b,c) and (a',b',c') are compositum-feasible (resp. sum-feasible, product-feasible), then the triplet (aa',bb',cc') is also compositum-feasible (resp. sum-feasible, product-feasible).*

In general, it is not known whether this conjecture is true or false even for compositum-feasible triplets. (Note that if the conjecture were true for sum-feasible either product-feasible triplets, then it would also hold for compositum-feasible triplets due to Propositions 1.2 and 1.3.) One more specific example for the conjecture is the following

Proposition 1.12 (Special case of [6, Proposition 3.2.])**.** *Suppose that the compositum-feasible triplets (a,b,c) and (a',b',c') are attained with number fields K, L, and K', L', respectively, i.e.,*

$$[K:\mathbb{Q}] = a,\ [L:\mathbb{Q}] = b,\ [KL:\mathbb{Q}] = c,$$
$$[K':\mathbb{Q}] = a',\ [L':\mathbb{Q}] = b',\ [K'L':\mathbb{Q}] = c'.$$

Let M be the Galois closure of $K'L'$. If the Galois group $\mathrm{Gal}(M/\mathbb{Q})$ is solvable, then the triplet (aa',bb',cc') is compositum-feasible.

For the both cases of sum-feasible and product-feasible triplets the following partial result takes place:

Proposition 1.13 ([8, Proposition 28])**.** *Suppose that the triplet $(a,b,c) \in \mathbb{N}^3$ satisfies the exponent triangle inequality with respect to any prime number. Then for any sum-feasible (resp. product-feasible) triplet (a',b',c') the triplet (aa',bb',cc') is also sum-feasible (resp. product-feasible).*

Again, for the compositum case the analogous statement is not true (for a counterexample, take a compositum-feasible triplet $(a,b,c) = (1,1,1)$ and $(a',b',c') = (6,10,15)$).

The last section of Chapter 3 contains some more remarks on Conjecture 1.11 for the compositum case. In particular, we introduce a new notion of an *irreducible compositum-feasible tripet*, i.e., a triplet that cannot be obtained in the form (aa', bb', cc') for some compositum-feasible triplets (a,b,c) and (a',b',c'). Moreover, we give a nontrivial example of an infinite family of such triplets:

Theorem 3.16. *For any integer $n \geqslant 2$ the compositum-feasible triplet $(n, n, n(n-1))$ is irreducible.*

We note that in [8, 7], there are no particular consideration of product-feasible triplets, only some simple cases being handled, e.g.,

Proposition 1.14 ([8, Theorem 8])**.** *The triplet $(2,t,t) \in \mathbb{N}^3$ is product-feasible if and only if $2|t$ or $3|t$.*

The special case (p,b,c), where p is a prime number and $p \nmid b$, has been studied by Virbalas [38]. In particular, he proved the following

Proposition 1.15 ([38, Theorem 3])**.** *Let α and β be algebraic numbers. Suppose $\deg\alpha = p$, $\deg\beta = b$, where $p > 2$ is a prime number, $p \nmid b$ and $p-1 \nmid b$. Then $\deg(\alpha\beta) = pb$.*

That is to say, if the triplet (p,b,c) is product-feasible, where $p > 2$ is prime, $p \nmid b$ and $p-1 \nmid b$, then $c = pb$.

Chapter 4 is devoted to the product question. We describe all product-feasible triplets (a,b,c), satisfying $a \leqslant b \leqslant c$, with $b \leqslant 7$:

Theorem 4.1. *All the triplets $(a,b,c) \in \mathbb{N}^3$ with $a \leqslant b \leqslant c$, $b \leqslant 7$ that are product-feasible are given in Table 4.1.*

By the way, in Chapter 4 we study triplets of some particular forms, among which the most interesting case is $(n,(n-1)k,nk)$, where $k \geqslant 1$ and $n \geqslant 2$. We prove the following

Theorem 4.5. *Let $k \geqslant 1$ be an integer. Then the triplet $(n,(n-1)k,nk)$, $n \geqslant 2$, is product-feasible if and only if n is a prime number.*

1.6 Approbation

The results of the thesis were presented at the 32th International Conference *Journées Arithmétiques* (JA 2023, July 3 - 7, 2023, Nancy, France),

at the International Scientific Conference Dedidacted to the 160th anniversary of Prof. Dr. Hermann Minkowski (June 20 - 22, 2024, Kaunas, Lithuania), at the 64th conference of Lithuanian Mathematical Society (LMS 2023, June 21 - 22, Vilnius, Lithuania), as well as at the Number Theory Seminar of Vilnius University.

Abstracts for conferences:

1. Maciulevičius L. Some degree problems in number fields. Abstracts of JA 2023, July 3 - 7, 2023, Nancy, France, pp. 44.

2. Maciulevičius L. Apie skaičių kūnų kompozito bei algebrinių skaičių sandaugos laipsnius. Lietuvos matematikų draugijos LXIV konferencijos santraukos. Vilniaus universiteto leidykla, 2023, pp. 11.

1.7 Main publications

The results of the thesis are published in the following papers:

1. Drungilas P., and Maciulevičius L. A degree problem for the compositum of two number fields. *Lith. Math. J. 59*, 1 (2019), 39 - 47.

2. Maciulevičius L. On the degree of product of two algebraic numbers. *Mathematics 11*, 2131 (2023).

3. Dubickas A., and Maciulevičius L. The product of a quartic and a sextic number cannot be octic. *Open Math. 22*, 1 (2024), Paper No. 20230184, 10.

Chapter 2

Literature review

2.1 Prerequisites from abstract algebra

In this section, we recall some prerequisite knowledge of algebra. Although our research is concerned only with the number fields, for the sake of completness we present the basics in a more general set up (over arbitrary fields).

Throughout, let L/K denotes a *field extension*, i.e., K is a subfield of L.

Algebraic elements An element $\alpha \in L$ is said to be *algebraic over* K if there exists a non-zero polynomial $f(x) \in K[x]$ such that $f(\alpha) = 0$. Let $p(x) \in K[x]$ be a monic polynomial of least degree such that $p(\alpha) = 0$. For any $\alpha \in L$ that is algebraic over K there exists exactly one such a polynomial $p(x)$. It is called the *minimal polynomial of* α *over* K and its degree is called the *degree of* α *over* K. Recall the simplest properties of minimal polynomials.

Proposition 2.1 ([40, Chapter II,§2])**.** *Let $p(x)$ be the minimal polynomial of $\alpha \in L$ over K. Then $p(x)$ is irreducible over K. If $f(x) \in K[x]$ is any other polynomial such that $f(\alpha) = 0$, then $p(x)$ divides $f(x)$ over K.*

If elements $\alpha, \beta \in L$ are algebraic over K and have the same minimal polynomial over K, then we say that α and β are *conjugate* over K.

A field Ω is called *algebraically closed* if every polynomial in $\Omega[x]$ of degree $\geqslant 1$ has a root in Ω. Recall that any field K can be embedded in some algebraically closed field Ω (see [40, Chapter II,§14]), e.g., if $K = \mathbb{Q}$, then Ω can be taken to be $\mathbb{C}$.

Finite field extensions Note that given any field extension L/K we can regard L as a vector space over K. The dimension of this vector space is called the *degree of the field extension* L/K and it is denoted by $[L:K]$. If $[L:K]$ is finite, then L/K is said to be a *finite extension*. Note that finiteness of L/K implies that any $\alpha \in L$ is algebraic over K.

The degree of an extension possesses the following multiplicative property which is called the *tower law*:

Proposition 2.2 ([36, Theorem 9.110]). *Let M be an intermediate field between K and L, i.e., $K \subseteq M \subseteq L$. If the extensions M/K and L/M both are finite, then L/K is also finite and*

$$[L:K] = [L:M] \cdot [M:K].$$

Now take any elements $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$. Evidently, the set

$$\left\{ \frac{f(\alpha_1, \alpha_2, \ldots, \alpha_n)}{g(\alpha_1, \alpha_2, \ldots, \alpha_n)} : \ f, g \in K[x_1, x_2, \ldots, x_n],\ g(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0 \right\}$$

is an intermediate field between K and L. It is denoted by $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ and is referred to as the *field generated by $\alpha_1, \alpha_2, \ldots, \alpha_n$ over K*. If, in particular, $n = 1$ and $\alpha_1 =: \alpha \in L$ is algebraic over K, then $K(\alpha)$ is called a *simple algebraic extension of K*. The structure of such extensions can be described as follows:

Proposition 2.3 ([40, Chapter II,§2]). *Let $\alpha \in L$ be algebraic element over K of degree n. Then the elements $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ form a basis of $K(\alpha)$, regarded as a vector space over K, i.e., $[K(\alpha):K] = n$ and*

$$K(\alpha) = \{c_{n-1}\alpha^{n-1} + \cdots + c_2\alpha^2 + c_1\alpha + c_0 : \ c_i \in K\}.$$

In fact, any finite extension of a field of zero characteristic is a simple algebraic extension. This is known as the *primitive elemenet theorem*:

Proposition 2.4 ([36, Theorem 11.122]). *Let* $\operatorname{char} K = 0$*, and let L/K be a finite extension. Then there exists $\alpha \in L$ such that $L = K(\alpha)$.*

Galois group of a field extension With any field extension L/K we can associate the group $\mathrm{Aut}(L/K)$ consisting of all the *K-automorphisms of L*, i.e., field automorphisms $\sigma : L \to L$ such that $\sigma(k) = k$ for any $k \in K$.

This is a group under the composition of functions. If L/K is a finite extension, then $|\mathrm{Aut}(L/K)| \leqslant [L:K]$ (see [36, Proposition 10.68]). A finite extension L/K is said to be a *Galois extension* if $|\mathrm{Aut}(L/K)| = [L:K]$. In that case, $\mathrm{Aut}(K/L)$ is called *the Galois group of the extension* L/K and is denoted by $\mathrm{Gal}(L/K)$.

At least when $\mathrm{char}\, K = 0$, any finite extension L/K can be improved to be Galois by making the extension possibly larger. Indeed, consider the extension L/K as contained in some algebraically closed field Ω. Write $L = K(\alpha)$ for some $\alpha \in L$ (this is possible by Proposition 2.4), and let $p \in K[x]$ be the minimal polynomial of α over K. Take M to be the *splitting field of* f *over* K, i.e., $M = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$, where $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_n \in \Omega$ are all the roots of f. Then the extension M/K is Galois (see [36, Theorem 10.76]) and $M \supseteq L$. We refer to the field M obtained in such a way as the *Galois closure of* L *over* K.

The proposition below gives a characterization of conjugate elements in terms of field automorphisms.

Proposition 2.5 ([35, Chapter VII, Section 50])**.** *Let L/K be a Galois extension, and let $\alpha, \beta \in L$. The elements α and β are conjugate over K if and only if there exists an automorphism $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\alpha) = \beta$.*

Group actions Let G be a group and let X be a nonempty set. Recall that a *group action* of G on X is a map $G \times X \to X$, the image of (g, x) being denoted by $g \circ x$, such that

1. $e \circ x = x$ for all $x \in X$, here e is the identity element of G,
2. $g \circ (h \circ x) = (gh) \circ x$ for all $x \in X$ and all $g, h \in G$.

Having a group action, to each element $g \in G$ we can associate a map $\alpha_g : X \to X$, defined by a rule $\alpha_g(x) = g \circ x$ for all $x \in X$. Then $\alpha_g \in S(X)$ and the map $\alpha : G \to S(X)$, $g \mapsto \alpha_g$, is a group homomorphism from G to $S(X)$. The kernel of α consists of those elements $g \in G$ which do not move any element of X, i.e.,

$$\ker \alpha = \{g \in G : \alpha_g = \mathrm{id}\} = \{g \in G : g \circ x = x \text{ for all } x \in X\}.$$

A group action is called *effective*, if $\ker \alpha = \{e\}$. By the First Isomorphism Theorem, $G/\ker \alpha \cong \mathrm{im}\, \alpha \subseteq S(X)$. Therefore, in the case of effec-

tive action, the group G is isomorphic to a subgroup of $S(X)$.

Transitive actions Assume $|X| \geqslant k$, here $k \in \mathbb{N}$. It is said that an action of G on X is *k-transitive* (or G acts *k-transitively* on X) if given any two sets $\{x_1, x_2, \ldots, x_k\}$ and $\{y_1, y_2, \ldots, y_k\}$ of distinct elements of X (not necessarily disjoint), there exists an element $g \in G$ such that $g \circ x_i = y_i$ for any $i \in \{1, 2, \ldots, k\}$. In the case when $k = 1$ we simply say that an action is *transitive*. For instance, setting $X := \{1, 2, \ldots, n\}$, the symmetric group S_n acts n-transitively on X, whereas the alternating group A_n acts $(n-2)$-transitively on X for $n > 2$. Note that any k-transitive action is also m-transitive for each $m \in \{1, 2, \ldots, k\}$. Moreover, when G and X both are finite, we have the following

Proposition 2.6 ([18, Chapter 8, 8A])**.** *Suppose a finite group G acts k-transitively on a set X of cardinality n. Then $|G|$ is divisible by $n(n-1)\cdots(n-k+1)$.*

Primitive actions Let a group G acts transitively on a finite set X of cardinality n. Suppose that X can be partitioned into m $(1 < m < n)$ pairwise disjoint subsets

$$\Delta_1, \Delta_2, \ldots, \Delta_m \tag{2.1}$$

of equal size n/m, so that any $g \in G$ maps each Δ_i to some Δ_j $(1 \leqslant i, j \leqslant m)$. In such a case we say that the action of G on X is *imprimitive* and the collection (2.1) is called a *system of blocks*. Otherwise, if no such a partitioning is possible, then the action is said to be *primitive*. For instance, the action of the Klein four-group

$$V_4 = \{\mathrm{id}, (1,2), (3,4), (1,2)(3,4)\}$$

on $X = \{1, 2, 3, 4\}$ is imprimitive with a system of blocks $\Delta_1 = \{1, 2\}$ and $\Delta_2 = \{3, 4\}$. On the other hand, for any $n \in \mathbb{N}$ the symmetric group S_n and the alternating group A_n both acts primitively on $X = \{1, 2, \ldots, n\}$.

Remark. Here and in the following, given a subgroup G of S_n, we implicitly understand that G acts on $X = \{1, 2, \ldots, n\}$ via

$$\sigma \circ i = \sigma(i),\ \sigma \in G,\ i \in X.$$

In particular, instead of saying *G acts transitively (resp. primitively) on $\{1,2,\dots,n\}$*, we will simply say *G is a transitive (resp. primitive) subgroup of S_n*.

From the definition of primitivity, it follows immediately that

Proposition 2.7 ([18, Corollary 8.12])**.** *A transitive group action on a set of prime cardinality is always primitive.*

The following classical result is due to Jordan:

Proposition 2.8 ([18, Theorem 8.23])**.** *Let G be a primitive subgroup of S_n, and assume that G contains a cycle of length p, where p is prime. Then either G contains A_n as a subgroup, or $n \leqslant p+2$.*

Galois group of a polynomial Consider K as a subfield of some algebraically closed field Ω. Let $f(x) \in K[x]$ be a separable[1] polynomial of degree $n \geqslant 1$. Set $M = K(\alpha_1, \alpha_2, \dots, \alpha_n)$, where $\alpha_1 := \alpha, \alpha_2, \dots, \alpha_n \in \Omega$ are all the roots of $f(x)$ (i.e., M is the Galois closure of $K(\alpha)$ over K). Since the extension M/K is Galois, we may consider the Galois group $\mathrm{Gal}(M/K)$. It is called the *Galois group of a polynomial $f(x)$ over K*.

Note that any automorphism $\sigma \in \mathrm{Gal}(M/K)$ preserves the set $X := \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ of the roots of $f(x)$, and, in fact, $\mathrm{Gal}(M/K)$ acts on X via $\sigma \circ \alpha_i := \sigma(\alpha_i)$, $i \in \{1,2,\dots,n\}$. Moreover, this action is effective, since an automorphism $\sigma \in \mathrm{Gal}(M/K)$ preserving each root $\alpha_i \in X$ must be the identity automorphism of $M = K(\alpha_1, \alpha_2, \dots, \alpha_n)$. Therefore, the Galois group of a separable polynomial $f(x) \in K[x]$ of degree n can be considered as a subgroup of S_n acting on $\{1,2,\dots,n\}$. Moreover, Proposition 2.5 implies that for irreducible polynomials this action is transitive:

Proposition 2.9 ([33, Proposition 22.3])**.** *Let $f(x) \in K[x]$ be irreducible over K. Then the Galois group of $f(x)$ over K acts transitively on the set of all the roots of $f(x)$.*

2.2 Relations between the polynomial roots

Throughout, let $f(x) \in K[x]$ be a separable polynomial of degree $n \geqslant 2$. Again, consider K as a subfield of a fixed algebraically closed field Ω,

[1] Recall that a polynomial $f(x) \in K[x]$ is said to be *separable*, if it does not have multiple roots in any extension of K (particularly, in Ω).

and let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \Omega$ be all the roots of $f(x)$. By a *polynomial relation over* K we mean a relation of the kind

$$P(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0,$$

where $P(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n]$.

Roughly speaking, the Galois group of $f(x)$ over K can be understood as a subgroup of S_n consisting exactly of those permutations σ which preserves any polynomial relation over K between the roots $\alpha_1, \ldots, \alpha_n$, i.e.,

$$\text{if } P(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0, \text{ then also } P(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)) = 0.$$

Such an approach leads to the general problem of describing the possible polynomial relations between the roots of $f(x)$ depending on the structure of the Galois group of $f(x)$. Various subproblems and related questions has been considered, for instance, by Smyth [32], Baron, Drmota and Skalba [5, 1]. We will use some former results related to so called *additive* and *multiplicative relations*.

- An *additive relation* between $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a relation of the kind

  $$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \in K$$

  where all the $a_j \in K$ (i.e., $P(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} a_i x_i + a_0$, $a_0 \in K$).

- A *multiplicative relation* between $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a relation of the kind

  $$\alpha_1^{k_1}\alpha_2^{k_2}\cdots\alpha_n^{k_n} \in K$$

  where all the $k_j \in \mathbb{Z}$ (i.e., $P(x_1, x_2, \ldots, x_n) = x_1^{k_1}x_2^{k_2}\ldots x_n^{k_n} + a_0$, $a_0 \in K$).

We call these relations *trivial* if $a_1 = a_2 = \cdots = a_n$ and, respectively, $k_1 = k_2 = \ldots = k_n$.

For instance, take a polynomial of the form $f(x) = x^n - r$, where $r \in K$ and $n \geqslant 2$, and suppose it is separable (this is the case at least when $\operatorname{char} K = 0$, see [37, Proposition 10.72.]). Then there is an obvious

nontrivial multiplicative relation between the roots of $f(x)$, namely,

$$\alpha_1^n \alpha_2^0 \cdots \alpha_n^0 = r \in K.$$

In particular, if $r = 1$ and $n > 2$, take any two roots $\neq 1$ of $f(x)$, say, α_1 and α_2. Then the product $\alpha_1\alpha_2$ is another root of $f(x)$, say, α_3. Thus, we obtain a nontrivial multiplicative relation $\alpha_1^1\alpha_2^1\alpha_3^{-1} = 1 \in K$.

Schinzel provided the following interesting example of a polynomial $\neq x^n - 1$ whose one root is a product of two other roots[2]. Let $K = \mathbb{Q}$. Take the polynomial

$$\begin{aligned} f(x) &= x^6 - 2x^4 - 6x^3 - 2x^2 + 1 \\ &= (\underbrace{x^3 + \sqrt{2}x^2 + \sqrt{2}x - 1}_{=:f_1(x)})(\underbrace{x^3 - \sqrt{2}x^2 - \sqrt{2}x - 1}_{=:f_2(x)}). \end{aligned}$$

By Eisentein's criterion, $f(x)$ is irreducible over $\mathbb{Q}$, and hence it is separable (see [36, Corollary 10.73]). Let α_1 and α_2 be two distinct roots of $f_1(x)$. Then, by Vieta's theorem, the third root of $f_1(x)$ is $(\alpha_1\alpha_2)^{-1}$. Note that the polynomial $f(x)$ is *self-reciprocal*, i.e., $f(x) = f(x^{-1})$. Hence, $\alpha_1\alpha_2 =: \alpha_3$ is also a root of $f(x)$ and $\alpha_3 \notin \{\alpha_1, \alpha_2, (\alpha_1\alpha_2)^{-1}\}$. Again, this yields a nontrivial multiplicative relation $\alpha_1^1\alpha_2^1\alpha_3^{-1} \in \mathbb{Q}$.

However, for the polynomials of prime degree > 2 we have the following

Proposition 2.10 ([5, Theorem 1])**.** *Let $p > 2$ be a prime number and $f(x) \in \mathbb{Q}[x]$ an irreducible polynomial $\neq x^p - r$ of degree p over $\mathbb{Q}$. Then there are no nontrivial multiplicative relations between the roots $\alpha_1, \alpha_2, \ldots, \alpha_p$ of $f(x)$.*

The following fact concerning multiplicative relations will be useful in the proof of Theorem 4.5:

Proposition 2.11 (Part of [32, Lemma 1])**.** *Let β_1, β_2, β_3 be distinct algebraic numbers conjugate over $\mathbb{Q}$. If $\beta_1^2 = \beta_2\beta_3$, then $\beta_1^m = \beta_2^m$ for some positive integer m.*

As concerned with nontrivial additive relations, it turns out that 2-transitivity of the Galois group of $f(x)$ eliminates the possibility for such relations:

[2]The example is mentioned in [1, 5].

Proposition 2.12 ([1, Part of Theorem 3])**.** *Suppose that the Galois group of a separable polynomial $f(x) \in \mathbb{Q}[x]$ is 2-transitive. Then there are no nontivial additive relations between the roots of f.*

In Section 4.2 we give a useful criteria to decide whether the Galois group of a polynomial is 2-transitive.

For the general analogues of Propositions 2.10, 2.11 and 2.12 over arbitrary fields see the corresponding references.

Chapter 3

Compositum-feasible triplets

3.1 Statement of the results

In this Chapter our principal aim is to extend the classification of compositum-feasible triplets given in the study by Drungilas et al. [8, 7]. Recall that in [8, 7] there are described all the compositum-feasible triplets (a,b,c) satisfying $a \leqslant b \leqslant c$, with $b \leqslant 7$. Now we can take two steps forward to the case $b \leqslant 9$.

Theorem 3.1. *Let a and c be positive integers.*

1. *The triplet $(a,8,c)$, $a \leqslant 8 \leqslant c$, is compositum-feasible if and only if $c \leqslant 8a$, $a|c$ and $8|c$, with a single exceptional triplet $(8,8,40)$, which is not compositum-feasible.*

2. *The triplet $(a,9,c)$, $a \leqslant 9 \leqslant c$, is compositum-feasible if and only if $c \leqslant 9a$, $a|c$ and $9|c$, with only two exceptional triplets $(9,9,45)$ and $(9,9,63)$, which are not compositum-feasible.*

Combining the results of [8, 7] with Theorem 3.1, we obtain the table that describes all possible compositum-feasible triplets (a,b,c) satisfying $a \leqslant b \leqslant c$, with $b \leqslant 9$ (Table 3.1).

Corollary 3.2. *Let a, b and c be positive integers satisfying $a \leqslant b \leqslant c$, $b \leqslant 9$. The triplet (a,b,c) is compositum-feasible if and only if $c \leqslant ab$, $a|c$ and $b|c$, with five exceptional triplets*

$$(5,5,15),\ (7,7,35),\ (8,8,40),\ (9,9,45),\ (9,9,63), \tag{3.1}$$

which are not compositum-feasible

Investigation of the exceptional triplets (3.1) led us to more general results.

$b\backslash a$	1	2	3	4	5	6	7	8	9
1	1								
2	2	2, 4							
3	3	6	3, 6, 9						
4	4	4, 8	12	4, 8, 12, 16					
5	5	10	15	20	5, 10, 20, 25				
6	6	6, 12	6, 12, 18	12, 24	30	6, 12, 18, 24, 30, 36			
7	7	14	21	28	35	42	7, 14, 21, 28, 42, 49		
8	8	8, 16	24	8, 16, 24, 32	40	24, 48	56	8, 16, 24, 32 48, 56, 64	
9	9	18	9, 18, 27	36	45	18, 36, 54	63	72	9, 18, 27, 36, 54, 72, 81

Table 3.1: Triplets (a,b,c), $a \leqslant b \leqslant c$, with $b \leqslant 9$, that are compositum-feasible

Theorem 3.3. *Let $n \geqslant 4$ be an integer. The triplet $(n, n, n(n-2))$ is compositum-feasible for even n and is not product-feasible for odd n.*

Hence, for n odd, $(n, n, n(n-2))$ is neither compositum-feasible nor sum-feasible. In particular, it follows that $(5, 5, 15)$, $(7, 7, 35)$ and $(9, 9, 63)$ are not compositum-feasible. Meanwhile, the cases $(8, 8, 40)$ and $(9, 9, 45)$ are specific manifestations of the following general result:

Theorem 3.4. *Let $n \geqslant 8$ be an integer. Then for any prime number p satisfying $\frac{n}{2} < p < n-2$ the triplet (n, n, np) is not product-feasible, and hence it is neither compositum-feasible nor sum-feasible.*

This chapter is organized as follows. In Sections 3.2, 3.3, 3.4 we prove the stated theorems. Then, in Section 3.5, we give a supplementary result which provides some ideas for the further classification of compositum-feasible triplets. Finally, Section 3.6 contains several remarks on Conjecture 1.11 for the compositum case.

3.2 Proof of Theorem 3.4

First of all, we prove two auxiliary propositions.

Proposition 3.5. *Let $n \geqslant 4$ be an integer. Suppose $p > 2$ is a prime number that satisfies the following conditions:*

(i) p does not divide $n-1$,

(ii) 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 integer k divisible by p, the triplet (n, n, k) is not product-feasible.

We will need the following

Lemma 3.6 ([23, Theorem 1.12])**.** *If K and L are number fields and $K/\mathbb{Q}$ is Galois, then*

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

Proof of Proposition 3.5. Let n, p and k satisfy the conditions of the proposition. Suppose to the contrary that the triplet (n,n,k) is product-feasible. Then there exist algebraic numbers α and β such that

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\beta):\mathbb{Q}] = n \text{ and } [\mathbb{Q}(\alpha\beta):\mathbb{Q}] = k.$$

Denote by K and L the Galois closures of $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ over $\mathbb{Q}$, respectively. Since $\mathbb{Q}(\alpha\beta)$ is a subfield of KL, we find that $[KL:\mathbb{Q}]$ is divisible by $[\mathbb{Q}(\alpha\beta):\mathbb{Q}] = k$. Moreover, by Lemma 3.6,

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

Hence at least one of the numbers $[K:\mathbb{Q}]$ or $[L:\mathbb{Q}]$ is divisible by p. Without loss of generality, we can assume that $[K:\mathbb{Q}]$ is divisible by p. On the other hand, $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to a transitive subgroup of S_n (see Section 2.1). Therefore, in view of the assumption (ii), $\mathrm{Gal}(K/\mathbb{Q})$ (up to isomorphism) is either A_n or S_n.

Denote by l the degree of α over $\mathbb{Q}(\beta)$. We claim that $2 \leqslant l \leqslant n-2$. Indeed, suppose $l \in \{1, n-1, n\}$. We have that

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\beta)]\cdot[\mathbb{Q}(\beta):\mathbb{Q}] = l\cdot n.$$

Therefore,

$$\begin{aligned} l\cdot n = [\mathbb{Q}(\alpha,\beta):\mathbb{Q}] &= [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha\beta)]\cdot[\mathbb{Q}(\alpha\beta):\mathbb{Q}] \\ &= [\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha\beta)]\cdot k. \end{aligned}$$

Since $p|k$, we obtain that p divides the product $l\cdot n$. By the assumption (ii), $p\nmid n$, since S_n contains a transitive subgroup of order n, e.g., the cyclic subgroup generated by $(1,2,\ldots,n)$. Hence, $p|l$, which contradicts both the assumptions (i) and (ii). This proves that $2 \leqslant l \leqslant n-2$.

Let $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_l$ be the algebraic conjugates of α over $\mathbb{Q}(\beta)$. Then, by Vieta's theorem, $\alpha_1+\alpha_2+\cdots+\alpha_l \in \mathbb{Q}(\beta)$. Thus, there exists a polynomial $f(x) \in \mathbb{Q}[x]$ such that

$$\alpha_1+\alpha_2+\cdots+\alpha_l = f(\beta). \tag{3.2}$$

Recall that $\mathrm{Gal}(K/\mathbb{Q})$ is either isomorphic to A_n or S_n. Both these

groups are l-transitive. Hence, for any collection of distinct indices $i_1, i_2, \ldots, i_l \in \{1, 2, \ldots, n\}$, there exists an automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that

$$\sigma(\alpha_1) = \alpha_{i_1},\ \sigma(\alpha_2) = \alpha_{i_2}, \ldots, \sigma(\alpha_l) = \alpha_{i_l}.$$

Applying σ to (3.2), we get

$$\alpha_{i_1} + \alpha_{i_2} + \ldots + \alpha_{i_l} = f(\sigma(\beta)). \tag{3.3}$$

In this way, we obtain $\binom{n}{l}$ relations of type (3.3) with distinct collections of indices $\{i_1, i_2, \ldots, i_l\}$. On the other hand, β has exactly n distinct algebraic conjugates over $\mathbb{Q}$. Since $2 \leqslant l \leqslant n-2$, we have $\binom{n}{l} > n$. This implies that at least two relations of type (3.3) have identical right-hand sides but different collections of indices $\{i_1, i_2, \ldots, i_l\}$. Equating two such relations, we find that there exists a nontrivial additive relation between the conjugates of α, which contradicts Proposition 2.12. This completes the proof of Proposition 3.5. □

Proposition 3.7. *Let G be a transitive subgroup of S_n such that $G \neq A_n$ and $G \neq S_n$. Then none of the prime numbers p satisfying $n/2 < p < n-2$ divides the order of G.*

Proof. Assume that the order of G is divisible by a prime p satisfying $n/2 < p < n-2$. Then, by Cauchy's theorem, there exists $\sigma \in G$ of order p. Evidently, $p > n/2$ yields σ is a cycle of length p. On the other hand, $p < n-2$ and G does not contain A_n as a subgroup. Hence, Proposition 2.8 implies that the action of G on $\{1, 2, \ldots, n\}$ is imprimitive. Let

$$\Sigma = \{\Delta_1, \Delta_2, \ldots, \Delta_m\},\ \Delta_i \subseteq \{1, 2, \ldots, n\},$$

be a system of blocks, here $2 \leqslant m < n$ (see Section 2.1). The subgroup $\langle\sigma\rangle$ acts on Σ in a natural way. We claim that this action is effective. Indeed, assume to the contrary that there exists $\tau \in \langle\sigma\rangle$, $\tau \neq \mathrm{id}$, such that $\tau(\Delta_i) = \Delta_i$ for all $i = 1, 2, \ldots, m$. Clearly, τ is also a cycle of length p. Let $\tau = (i_1, i_2, \ldots, i_p)$. Assume, without loss of generality, that $i_1 \in \Delta_1$. Note that $i_k \in \Delta_1,\ 1 \leqslant k \leqslant p-1$, implies $i_{k+1} = \tau(i_k) \in \tau(\Delta_1) = \Delta_1$.

Thus, $\{i_1, i_2, \ldots, i_p\} \subseteq \Delta_1$ and

$$p \leqslant |\Delta_1| = \frac{n}{m} \leqslant \frac{n}{2} < p,$$

a contradiction. Therefore, the action of $\langle\sigma\rangle$ on Σ is effective. Since $|\Sigma| = m$, it follows that $\langle\sigma\rangle$ is isomorphic to a subgroup of S_m. Thus, by Lagrange's theorem, $m!$ must be divisible by a prime p, a contradiction, since $p > n/2 \geqslant n/|\Delta_1| > m$. This completes the proof of Lemma 3.7. $\square$

Now we can prove Theorem 3.4. Take an integer $n \geqslant 8$ and let p be a prime number such that

$$\frac{n}{2} < p < n - 2. \tag{3.4}$$

Then p satisfies both conditions of Proposition 3.5. Indeed, for the condition (i) note that (3.4) implies $(n-1)/2 < p < n-1$ and there are no divisors of $n-1$ in the interval $((n-1)/2, n-1)$, whereas condition (ii) is satisfied by Proposition 3.7. Therefore, Proposition 3.5 with $k = np$ implies that (n, n, np) is not product-feasible. This completes the proof of Theorem 3.4.

3.3 Proof of Theorem 3.3

We shall need the following auxiliary

Proposition 3.8. *Suppose that the triplet $(a, b, c) \in \mathbb{N}^3$ satisfying $a \leqslant b \leqslant c$ is not compositum-feasible. If $ab < 2c$, then (a, b, c) is neither sum-feasible nor product-feasible.*

Proof. Assume to the contrary that the triplet $(a, b, c) \in \mathbb{N}^3$, with $a \leqslant b \leqslant c$ and $ab < 2c$, is sum-feasible (resp., product-feasible), but not compositum-feasible. Then there exist algebraic numbers α and β such that $\deg\alpha = a$, $\deg\beta = b$, and $\deg\gamma = c$, where $\gamma := \alpha + \beta$ (resp., $\gamma := \alpha\beta$). Denote $r := [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\gamma)]$. Then $r > 1$, since otherwise $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$, and this would imply that the triplet (a, b, c) is compositum-fesaible, contradicting our assumption. Hence,

$$2c \leqslant rc = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] \leqslant [\mathbb{Q}(\alpha) : \mathbb{Q}][\mathbb{Q}(\beta) : \mathbb{Q}] = ab < 2c,$$

again a contradiction. Therefore, the triplet $(a,b,c) \in \mathbb{N}^3$ is neither sum-feasible nor product-feasible. $\square$

We will also use the following

Lemma 3.9 ([30])**.** *Suppose that α is an algebraic number with the minimal polynomial $f(x) \in \mathbb{Q}[x]$. Let r be the number of linear factors of $f(x)$ over $\mathbb{Q}(\alpha)$. Then r divides the degree of $f(x)$.*

We may now proceed with the proof of Theorem 3.3. Suppose $n \geqslant 4$ is an even integer, i.e., $n = 2k$ for some $k \in \mathbb{N}$. By Proposition 1.6, the triplet $(k,k,k(k-1))$ is compositum-feasible. Hence, the triplet

$$(n,n,n(n-2)) = (2k,2k,4k(k-1))$$

is compositum-feasible by Proposition 1.9.

Let $n > 4$ be an odd integer. We will show that the triplet $(n,n,n(n-2))$ is not compositum-feasible. Then Lemma 3.8 will imply that this triplet is not product-feasible as well.

Suppose to the contrary that $(n,n,n(n-2))$ is compositum-feasible. Then, by the primitive element theorem, there exist algebraic numbers α and β such that

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\beta):\mathbb{Q}] = n \text{ and } [\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = n(n-2).$$

This yields

$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)] = \frac{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]}{[\mathbb{Q}(\alpha):\mathbb{Q}]} = n-2,$$

i.e., β is of degree $n-2$ over $\mathbb{Q}(\alpha)$. Therefore, the minimal polynomial $P(x) \in \mathbb{Q}[x]$ of β factorizes over $\mathbb{Q}(\alpha)$ as follows:

$$P(x) = (x^2 + a_1x + a_2)(x^{n-2} + b_1x^{n-3} + \cdots + b_{n-3}x + b_{n-2}), \qquad (3.5)$$

here both polynomials on the right-hand side have coefficients in $\mathbb{Q}(\alpha)$, and the polynomial $x^{n-2} + b_1x^{n-3} + \cdots + b_{n-3}x + b_{n-2}$ is irreducible over $\mathbb{Q}(\alpha)$.

We claim that the polynomial $x^2 + a_1x + a_2$ is also irreducible over

$\mathbb{Q}(\alpha)$. Indeed, it is clear that

$$x^2 + a_1 x + a_2 = (x - \beta_1)(x - \beta_2) \tag{3.6}$$

for some conjugates β_1 and β_2 of β over $\mathbb{Q}$. Assume to the contrary that $\beta_1 \in \mathbb{Q}(\alpha)$. Then $\mathbb{Q}(\beta_1) \subseteq \mathbb{Q}(\alpha)$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta_1) : \mathbb{Q}]$, we get $\mathbb{Q}(\beta_1) = \mathbb{Q}(\alpha)$. Hence, the minimal polynomial $P(x) \in \mathbb{Q}[x]$ of β_1 has exactly two linear factors over $\mathbb{Q}(\beta_1)$, which contradicts Lemma 3.9. Thus, β_1 and β_2 both are quadratic over $\mathbb{Q}(\alpha)$.

Let K be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Denote

$$\mathcal{A} := \{\alpha_1, \alpha_2, \ldots, \alpha_n\},\ \mathcal{B} := \{\beta_1, \beta_2, \ldots, \beta_n\}.$$

For $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and for any polynomial $p(x) \in K[x]$, set $p^\sigma(x)$ to be the polynomial obtained by applying σ to all the coefficients of $p(x)$. Note that $p(x) = p_1(x) \cdot p_2(x)$ if and only if $p^\sigma(x) = p_1^\sigma(x) \cdot p_2^\sigma(x)$, here $p_1(x), p_2(x) \in K[x]$. Consequently, if L is a subfield of K and $p(x) \in L[x]$ is irreducible over L, then $p^\sigma(x)$ is irreducible over $\sigma(L)$. Now, for any $\alpha_i \in \mathcal{A}$ take an automorphism $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$ that sends α to α_i. Applying σ_i to the both sides of (3.5), we find that $P^{\sigma_i}(x) = P(x)$ factorizes over $\mathbb{Q}(\alpha_i)$ into two irreducible factors, one of which has degree 2. Hence, for any $\alpha_i \in \mathcal{A}$ exactly two algebraic conjugates of β, say, β_k and β_l $(k \neq l)$, are quadratic over $\mathbb{Q}(\alpha_i)$. This naturally gives rise to a map

$$\varphi : \mathcal{A} \to \binom{\mathcal{B}}{2},\ \alpha_i \mapsto \{\beta_k, \beta_l\},$$

here $\binom{\mathcal{B}}{2}$ denotes the family of all subsets of $\mathcal{B}$ of size 2. In other words, $\varphi(\alpha_i)$ consists of those conjugates of β (over $\mathbb{Q}$) which are quadratic over $\mathbb{Q}(\alpha_i)$.

Claim 3.3.1. *For any $\beta_j \in \mathcal{B}$ there exists $\alpha_i \in \mathcal{A}$ such that $\beta_j \in \varphi(\alpha_i)$.*

Proof. Let L be the Galois closure of $\mathbb{Q}(\alpha, \beta)$ over $\mathbb{Q}$. Take an automorphism $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ that sends β_1 to β_j. Then $\tau(\alpha) = \alpha_i$ for some $\alpha_i \in A$. Applying τ to the both sides of (3.6), we find that β_j is quadratic over $\mathbb{Q}(\alpha_i)$. □

Claim 3.3.2. *If β_j is quadratic over $\mathbb{Q}(\alpha_i)$, then α_i is quadratic over $\mathbb{Q}(\beta_j)$.*

Proof. Assume that $[\mathbb{Q}(\alpha_i,\beta_j):\mathbb{Q}(\alpha_i)]=2$. Then,

$$\begin{aligned}[\mathbb{Q}(\alpha_i,\beta_j):\mathbb{Q}(\beta_j)] &= \frac{[\mathbb{Q}(\alpha_i,\beta_j):\mathbb{Q}]}{[\mathbb{Q}(\beta_j):\mathbb{Q}]} = \frac{[\mathbb{Q}(\alpha_i,\beta_j):\mathbb{Q}]}{[\mathbb{Q}(\alpha_i):\mathbb{Q}]} \\ &= [\mathbb{Q}(\alpha_i,\beta_j):\mathbb{Q}(\alpha_i)] = 2,\end{aligned}$$

i.e., α_i is quadratic over $\mathbb{Q}(\beta_j)$. □

Claim 3.3.3. *For any distinct $\alpha_i,\alpha_j\in\mathcal{A}$ either $\varphi(\alpha_i)\cap\varphi(\alpha_j)=\emptyset$ or $\varphi(\alpha_i)=\varphi(\alpha_j)$.*

Proof. Take two distinct conjugates $\alpha_i,\alpha_j\in\mathcal{A}$. If $\varphi(\alpha_i)\cap\varphi(\alpha_j)=\emptyset$, then there is nothing to prove. Suppose $\varphi(\alpha_i)=\{\beta_k,\beta_l\}$ and let $\beta_k\in\varphi(\alpha_j)$. We will show that β_l is quadratic over $\mathbb{Q}(\alpha_j)$. Then $\beta_l\in\varphi(\alpha_j)$ and the equality $\varphi(\alpha_i)=\varphi(\alpha_j)$ follows.

Claim 3.3.2 implies that α_i and α_j are quadratic conjugates over $\mathbb{Q}(\beta_k)$. Therefore, by Vieta's theorem, $\alpha_i+\alpha_j\in\mathbb{Q}(\beta_k)$. Hence, $\mathbb{Q}(\alpha_j,\beta_k)=\mathbb{Q}(\alpha_i,\beta_k)$ and

$$\mathbb{Q}(\alpha_j,\beta_k,\beta_l)=\mathbb{Q}(\alpha_i,\beta_k,\beta_l). \tag{3.7}$$

On the other hand, β_k and β_l are quadratic conjugates over $\mathbb{Q}(\alpha_i)$. Therefore, $\beta_k+\beta_l\in\mathbb{Q}(\alpha_i)$. Hence, $\beta_l\in\mathbb{Q}(\alpha_i,\beta_k)$. Combining this with (3.7) we find that

$$\mathbb{Q}(\alpha_j,\beta_k,\beta_l)=\mathbb{Q}(\alpha_i,\beta_k). \tag{3.8}$$

Recall that our aim is to show $[\mathbb{Q}(\alpha_j,\beta_l):\mathbb{Q}(\alpha_j)]=2$. Consider the extension $\mathbb{Q}(\alpha_j,\beta_k,\beta_l)/\mathbb{Q}(\alpha_j)$. In view of (3.8), we have that

$$\begin{aligned}[\mathbb{Q}(\alpha_j,\beta_k,\beta_l):\mathbb{Q}(\alpha_j)] &= [\mathbb{Q}(\alpha_i,\beta_k):\mathbb{Q}(\alpha_j)] = \frac{[\mathbb{Q}(\alpha_i,\beta_k):\mathbb{Q}]}{[\mathbb{Q}(\alpha_j):\mathbb{Q}]} \\ &= \frac{[\mathbb{Q}(\alpha_i,\beta_k):\mathbb{Q}]}{[\mathbb{Q}(\alpha_i):\mathbb{Q}]} = [\mathbb{Q}(\alpha_i,\beta_k):\mathbb{Q}(\alpha_i)] = 2,\end{aligned}$$

and thus there are no non-trival intermediate fields between $\mathbb{Q}(\alpha_j,\beta_k,\beta_l)$

and $\mathbb{Q}(\alpha_j)$. Since

$$\mathbb{Q}(\alpha_j) \subsetneq \mathbb{Q}(\alpha_j, \beta_l) \subseteq \mathbb{Q}(\alpha_j, \beta_k, \beta_l), \tag{3.9}$$

we obtain $\mathbb{Q}(\alpha_j, \beta_l) = \mathbb{Q}(\alpha_j, \beta_k, \beta_l)$. (As it is noted above, the minimal polynomial $P(x)$ of β factorizes over $\mathbb{Q}(\alpha_j)$ into two irreducible factors both having degree greater than 1, analogously as in (3.5). Hence, $\beta_l \notin \mathbb{Q}(\alpha_j)$ and the first inclusion in (3.9) is indeed proper.) Therefore, $[\mathbb{Q}(\alpha_j, \beta_l) : \mathbb{Q}(\alpha_j)] = 2$. □

Now we can finish the proof of Theorem 3.3. Claim 3.3.1 and Claim 3.3.3 imply that the distinct sets of a family

$$\varphi(\alpha_1), \varphi(\alpha_2), \ldots, \varphi(\alpha_n)$$

form a partition of $\mathcal{B} = \{\beta_1, \beta_2, \ldots, \beta_n\}$, i.e.,

$$\mathcal{B} = \varphi(\alpha_{i_1}) \sqcup \varphi(\alpha_{i_2}) \sqcup \cdots \sqcup \varphi(\alpha_{i_k}) \tag{3.10}$$

for some $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, n\}$, here $\sqcup$ denotes that the sets in the union are pairwise disjoint. Taking the cardinality of both sides in (3.10), we find that $n = 2k$, a contradiction since n is odd. This completes the proof of Theorem 3.3.

3.4 Proof of Theorem 3.1

Using necessary conditions (1.2) and (1.3), we determine all possible candidates to compositum-feasible triplets (a, b, c) with $a \leqslant b \leqslant c$ and $b \in \{8, 9\}$. They are all listed in Table 3.2.

$b \backslash a$	1	2	3	4	5	6	7	8	9
8	8	8, 16	24	8, 16, 24, 32	40	24, 48	56	8, 16, 24, 32, (40), 48, 56, 64	
9	9	18	9, 18, 27	36	45	18, 36, 54	63	72	9, 18, 27, 36, (45), 54, (63), 72, 81

Table 3.2: Candidates to compositum-feasible triplets

The triplets with c being circled are not compositum-feasible. Indeed, $(8,8,40)$ and $(9,9,45)$ are not compositum-feasible by Theorem 3.4 applied to $(n,p)=(8,5)$ and $(n,p)=(9,5)$, respectively, whereas $(9,9,63)$ - by Theorem 3.3.

All the remaining triplets are compositum-feasible. Indeed, the blue-marked triplets are compositum-feasible by Proposition 1.5, whereas the green-marked triplets - by Corollary 1.10. The triplets $(8,8,56)$ and $(9,9,72)$ are of the form $(n,n,n(n-1))$, hence, they are also compositum-feasible by Proposition 1.6. For the red-marked triplets note that $(3,4,12)$ and $(2,3,6)$ are compositum-feasible by Proposition 1.5, whereas $(4,4,12)$ and $(3,3,6)$ are compositum-feasible by Proposition 1.6. Applying Proposition 1.9 to these four triplets and suitable powers of $p=2$, we obtain that all the red-marked triplets are also compositum-feasible. (Alternatively, the triplet $(8,8,48)$ is compositum-feasible by Theorem 3.3.) Finally, we will prove that the triplet $(9,9,36)$ is compositum-feasible. Recall a well-known fact about the Galois group of a cubic polynomial:

Proposition 3.10 ([36, Example 10.80])**.** *Let $f(x)=x^3+px+q$ be an irreducible polynomial over $\mathbb{Q}$, and let G be its Galois group over $\mathbb{Q}$. Then*

$$G \cong \begin{cases} A_3 \text{ if } D(f) \text{ is a perfect square in } \mathbb{Q}, \\ S_3 \text{ otherwise,} \end{cases}$$

here $D(f)=-4p^3-27q^2$ is the discriminant of f.

Now, take the polynomial $f(x)=x^3+3x+1$. It is irreducible over $\mathbb{Q}$ as a cubic polynomial without rational roots. Let α and β be two distinct roots of $f(x)$, and let $K:=\mathbb{Q}(\alpha)$, $L:=\mathbb{Q}(\beta)$. Evidently, $KL=\mathbb{Q}(\alpha,\beta)$ is the splitting field of $f(x)$ over $\mathbb{Q}$, and hence $KL/\mathbb{Q}$ is a Galois extension. Since $D(f)=-135$ is not a perfect square in $\mathbb{Q}$, Proposition 3.10 implies that $\mathrm{Gal}(KL/\mathbb{Q})=S_3$, and hence $[KL:\mathbb{Q}]=|S_3|=6$. Thus, $(3,3,6)$ is a compositum-feasible triplet which is attained with fields K and L. Moreover, the group S_3 is solvable. Therefore, the triplet $(9,9,36)=(3\cdot 3,3\cdot 3,6\cdot 6)$ is compositum-feasible by Proposition 1.12. This completes the proof of Theorem 3.1.

3.5 Supplementary result

As wee see in Corollary 3.2, among all the candidates (a,b,c), with $a \leqslant b \leqslant c \leqslant ab$, $a|c$, $b|c$ and $b \leqslant 9$, the only triplets that are not compositum-feasible are of the form (n,n,nk), where $k = n-2$ or k is a prime strictly between $n/2$ and $n-2$. In particular, for $n \in \{1,2,\ldots,9\}$, all the triplets (n,n,nk), with $1 \leqslant k \leqslant n/2$, are compositum-feasible. It is natural to ask, is it true for any $n \in \mathbb{N}$. Theorem 3.11 below shows that the answer is 'no':

Theorem 3.11. *Suppose p, q and w are prime numbers such that $2 < w < q < p$, $p = 2q + w$ and $w \nmid (q-1)$. Then the triplet (p,p,pq) is not product-feasible, and hence it is neither compositum-feasible nor sum-feasible.*

For instance, none of the triplets

$$(13,13,13\cdot 5),\ (19,19,19\cdot 7),\ (29,29,29\cdot 11),\ (31,31,31\cdot 13)$$

is product-feasible. We need some preparation for the proof of this theorem.

Let G be a group. Consider the action of G on G itself by conjugation, i.e., $g \circ x = g \cdot x \cdot g^{-1}$ for any $g, x \in G$. Take any subgroup H of G. In order to restrict this action on H, collect all those $g \in G$ such that $g \cdot h \cdot g^{-1} \in H$ for any $h \in H$. All such g's form a subgroup of G which is called the *normalizer of H in G* and is denoted by $N_G(H)$. Equivalently,

$$N_G(H) = \{g \in G :\ g \cdot H \cdot g^{-1} = H\}.$$

Now, we may consider the conjugation action of $N_G(H)$ on H. Let $\alpha : N_G(H) \to S(H)$, $g \mapsto \alpha_g$, be the corresponding action homomorphism. Its kernel is denoted by $C_G(H)$, i.e.,

$$C_G(H) = \{g \in G :\ g \cdot h \cdot g^{-1} = h\ \forall h \in H\},$$

and it is called the *centralizer of H in G*. Evidently, for any $g \in N_G(H)$ the map $\alpha_g(h) = g \cdot h \cdot g^{-1}$, $h \in H$, is an automorphism of H, so that the image of α is a subgroup of $\mathrm{Aut}(H)$. Thus, the First Isomorphism Theorem yields the following corollary which is known as *N/C Theorem*:

Lemma 3.12 ([18, Corollary X.19])**.** *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* $\operatorname{Aut} H$*.*

In general, having an action of G on a set X, we denote

$$\operatorname{fix} G := \{\alpha \in X : g \circ \alpha = \alpha \; \forall g \in G\}.$$

Lemma 3.13 ([18, Problem 8A.6][1])**.** *Suppose that G acts transitively on X. Let Q be a Sylow subgroup of G. Then $N_G(Q)$ acts transitively on* $\operatorname{fix} Q$*.*

Proof of the Theorem 3.11. 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 Proposition 3.5 will imply that the triplet (p,p,pq) is not product-feasible. (Note that $p = 2q + w$ and $2 < w < q < p$ yields $q \nmid (p-1)$.)

Suppose to the contrary that the order of G is divisible by q. Let Q be a Sylow q-subgroup of G. The order of Q equals q or q^2, since Q is a subgroup of S_p, as well, and $\operatorname{ord}_q |S_p| = \operatorname{ord}_q(p!) = q^2$. 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 is of the same cyclic structure, we find that the subgroup Q also contains a cycle of length q. However, Proposition 2.7 implies that G is primitive, therefore we get a contradiction by Proposition 2.8. 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 get a contradiction by Proposition 2.8. Since $p = 2q + w < 3q$, it follows that σ must be a product of two disjoint cycles of length q, say, π and ρ. Therefore, $|\operatorname{fix} Q| = p - 2q = w$.

Lemma 3.13 and Proposition 2.6 imply that the order of the normalizer $N_G(Q)$ is divisible by $|\operatorname{fix} Q| = w$ which is prime. Hence, by Cauchy's theorem, there exists an element $\tau \in N_G(Q)$ of order w. We claim that $\tau \in C_G(Q)$. 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, Lemma 3.12 implies

[1] Special case of [18, Problem 8A.6] taking any Sylow subgroup P of G and any $\alpha \in \operatorname{fix} P$.

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, a contradiction.

As we have proved, $Q = \langle \pi \cdot \rho \rangle$, where $\pi, \rho \in S_p$ are two disjoint q-cycles. Set $\pi =: (i_1, i_2, \ldots, i_q)$ 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 have $\tau \cdot (\pi \cdot \rho) \cdot \tau^{-1} = \pi \cdot \rho$, i.e.,

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

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

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

or

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

In both cases, we get that

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

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

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

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 $q \nmid w$. 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 $\{1, 2, \ldots, p\}$ which are not fixed under η. Since the order of η equals w, it follows that η is a cycle of length w, which leads to a contradiction by Proposition

2.8. This completes the proof of Theorem 3.11. □

3.6 Irreducible compositum-feasible triplets

Recall Conjecture 1.11 for the compositum case:

Conjecture 3.14 (Partial case of Conjecture 1.11)**.** *If* $(a,b,c),(a',b',c') \in \mathbb{N}^3$ *are compositum-feasible triplets, then so is* (aa',bb',cc').

Through this section, as before, we denote the set of all possible compositum-feasible triplets by $\mathcal{C}$. Moreover, for $(a,b,c),(a',b',c') \in \mathcal{C}$ define a multiplication of triplets by

$$(a,b,c)\cdot(a',b',c') := (aa',bb',cc'). \tag{3.11}$$

So, in other words, Conjecture 3.14 asks whether the set $\mathcal{C}$ forms a semigroup with respect to the multiplication (3.11). As we already said, it is not known in general whether the conjecture is true or false. However, Drungilas and Dubickas [6] provided some hope for the affirmative answer. Namely, they proved Conjecture 3.14 assuming the affirmative answer to the *inverse Galois problem*. Recall that the inverse Galois problem asks whether every finite group occurs as a Galois group of some Galois extension K over $\mathbb{Q}$ (see [20, 27, 39]). It is believed that the answer is positive.

Proposition 3.15 ([6, Theorem 1.3])**.** *If every finite group occurs as a Galois group of some Galois extension* $K/\mathbb{Q}$*, then Conjecture 3.14 is true.*

If $\mathcal{C}$ indeed forms a semigroup (even if not), then it is natural to ask which elements of $\mathcal{C}$ are *irreducible*. More precisely, 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, the triplet $(A,B,C) \in \mathcal{C}$ is said to be *reducible*. For instance, every triplet $(p,p,pd) \in \mathcal{C}$, where p is a prime number and $1 \leqslant d < p$, is irreducible, whereas for any positive integer n the triplet $(n,n,n^2) = (n,1,n)\cdot(1,n,n)$ is reducible.[2] The following theorem gives one more family of irreducible triplets in $\mathcal{C}$.

[2]It is known (see [7, Lemmas 2.7, 2.8, Theorem 1.1]) that for any prime p

Theorem 3.16. *For any integer $n \geqslant 2$, the compositum-feasible triplet $(n,n,n(n-1))$ is irreducible.*[3]

Proof. Suppose to the contrary that

$$(n,n,n(n-1)) = (a_1,b_1,c_1)\cdot(a_2,b_2,c_2), \tag{3.12}$$

where (a_1,b_1,c_1) and (a_2,b_2,c_2) are compositum-feasible triplets both different from $(1,1,1)$. For $i=1,2$, we can factor $c_i = d_i^{(n)} d_i^{(n-1)}$, where

$$d_1^{(n)} d_2^{(n)} = n \text{ and } d_1^{(n-1)} d_2^{(n-1)} = n-1.$$

Since the triplet (a_1,b_1,c_1) is compositum-feasible, we find that a_1 divides $c_1 = d_1^{(n)} d_1^{(n-1)}$. Then $\gcd(a_1, d_1^{(n-1)}) = 1$ implies $a_1 | d_1^{(n)}$. Analogously, $a_2 | d_2^{(n)}$. If $a_1 < d_1^{(n)}$, then

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

i.e., $d_2^{(n)} < a_2$ and $a_2 \nmid d_2^{(n)}$, a contradiction. Therefore, $a_2 = d_1^{(n)}$ and $a_2 = d_2^{(n)}$. Analogously, $b_1 = d_1^{(n)}$ ir $b_2 = d_2^{(n)}$. Thus, omitting superscripts (n) and instead of $(n-1)$ using $'$, we can rewrite (3.12) as

$$(n,n,n(n-1)) = (d_1,d_1,d_1d_1')\cdot(d_2,d_2,d_2d_2').$$

Recall that for any compositum-feasible triplet (a,b,c) the inequality $c \leqslant ab$ holds. Hence, for $i=1,2$, we must have $d_i d_i' \leqslant d_i^2$, i.e., $d_i' \leqslant d_i$. Moreover, $\gcd(d_i', d_i) = 1$ and the numbers d_i', d_i cannot be both equal to 1, thus $d_i' \neq d_i$ for $i=1,2$. On the other hand, since $d_1 < n$, we deduce

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

i.e., $d_2' > d_2$, a contradiction. Hence, the triplet $(n,n,n(n-1))$ is irreducible. □

Evidently, any $(a,b,c) \in \mathcal{C}$ can be factored into a product of irre-

and for $d \in \{1,2,p-1\}$ the triplet (p,p,pd) is compositum-feasible, whereas, for $p - \frac{1+\sqrt{4p-3}}{2} < d \leqslant p-2$, it is not product-feasible, hence not compositum-feasible. Meanwhile, the triplet (n,n,n^2) is compositum-feasible for any $n \in \mathbb{N}$ by Proposition 1.5.

[3] In fact, the triplet $(n,n,n(n-1))$, $n \geqslant 2$, is compositum-feasible by Proposition 1.6.

ducible compositum-feasible triplets. However, it should be noted that this factorization is not necessarily unique. For instance, the triplet $(15,15,30)$, which is compositum-feasible by Proposition 1.6, can be factored into irreducible triplets in two different ways:

$$(15,15,30) = (3,3,3)\cdot(5,5,10) = (5,5,5)\cdot(3,3,6).$$

One can check by a routine calculation that among the compositum-feasible triplets (a,b,c), satisfying $a \leqslant b \leqslant c$ and $b \leqslant 9$, the only irreducible triplets are exactly of the forms $(1,p,p)$, (p,p,pd) and $(n,n,n(n-1))$, where p is prime, $1 \leqslant d < p$ and $n \geqslant 2$. We finish the present chapter by proposing the following

Problem. *Determine all irreducible compositum-feasible triplets.*

Chapter 4

Product-feasible triplets

4.1 Statement of the results

In the preceding chapter, combining the results of [8, 7] with Theorem 3.1, we obtained a complete description of all compositum-feasible triplets (a,b,c) satisfying $a \leqslant b \leqslant c$, with $b \leqslant 9$. According to Propositions 1.2 and 1.3, all these triplets that are given in Table 3.1 are also sum-feasible and product-feasible. But, in fact, they do not exhaust *all* possible sum-feasible triplets neither all product-feasible triplets (a,b,c) under the corresponding restrictions. Again, we can observe this by the results of [8, 7], where all sum-feasible triplets (a,b,c), with $a \leqslant b \leqslant c$, $b \leqslant 7$, were classified. There comes a natural motivation to investigate the product problem more closely.

The present chapter provides a full description of all the product-feasible triplets (a,b,c) satisfying $a \leqslant b \leqslant c$, with $b \leqslant 7$:

Theorem 4.1. *All the triplets $(a,b,c) \in \mathbb{N}^3$ with $a \leqslant b \leqslant c$, $b \leqslant 7$ that are product-feasible are given in Table 4.1.*

Table 4.1 contains nine triplets (with c being bold), which are not sum-feasible by [8, 7], namely,

$$\begin{gathered}(2,3,3),(3,4,6),(3,6,9),(6,6,8),\\ (4,5,5),(4,5,10),(6,7,7),(6,7,14),(6,7,21).\end{gathered} \tag{4.1}$$

Note that the triplet $(2,3,3)$ is product-feasible by Proposition 1.14.

$b\backslash a$	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, 12, 24	30	6, **8**, 9, 12, 15, 18, 24, 30, 36	
7	7	14	21	28	35	**7**, **14**, **21**, 42	7, 14, 21, 28, 42, 49

Table 4.1: Triplets (a,b,c), $a \leqslant b \leqslant c$, with $b \leqslant 7$, that are product-feasible

Consequently, the triplets

$$(3,4,6) = (3,2,3)\cdot(1,2,2),$$
$$(3,6,9) = (3,2,3)\cdot(1,3,3),$$
$$(6,6,8) = (3,3,2)\cdot(2,2,4)$$

are also product-feasible by Proposition 1.13. The remaining triplets of (4.1) are special cases of the following more general result.

Theorem 4.2. *For any prime number p and for each divisor d of $p-1$ the triplet $(p-1,p,pd)$ is product-feasible.*

Moreover, we prove a certain extension of Proposition 1.14:

Theorem 4.3. *Suppose a prime number p and a positive integer t satisfy $t \geqslant p > 2$. Then the triplet (p,t,t) is product-feasible if and only if $p|t$.*

In [8], there is proved separately that the triplet $(6,6,10)$ is not sum-feasible (see [8, Theorem 38]). Generalizing the ideas of this proof, we show that

Theorem 4.4. *For any prime number $p > 3$, the triplet $(p+1,p+1,2p)$ is not product-feasible.*

Finally, we have the following result:

Theorem 4.5. *Let $k \geqslant 1$ be an integer. Then the triplet $(n,(n-1)k,nk)$, $n \geqslant 2$, is product-feasible if and only if n is a prime number.*

In particular, choosing $(n,k)=(4,2)$, we find that the triplet $(4,6,8)$ is not product-feasible. Actually, this is the triplet that took a considerable amount of effort for us to decide whether it is product-feasible or not.

This chapter is organized as follows. In the next section we give several auxiliary lemmas that are repeatedly used in the proofs of the stated theorems. Then, in Section 4.3, we prove Theorems 4.2 and 4.3. The proof of Theorems 4.4 and 4.5 are given in separate Sections 4.4 and 4.5, respectively. In Section 4.6 we complete the classification of product-feasible triplets (a,b,c), with $a \leqslant b \leqslant c$, $b \leqslant 7$, by proving Theorem 4.1. Finally, Section 4.7 contains an alternative proof that the triplet $(4,6,8)$ is not product-feasible.

4.2 Auxiliary lemmas

While searching for product-feasible (or sum-feasible) triplets with bounded values of b, we can find all possible candidates using Proposition 1.4. For instance, all the triplets (a,b,c) with $a \leqslant b \leqslant c$, $b \leqslant 7$, satisfying the condition of Proposition 1.4, are listed in Table 4.2. Having all the candidates (a,b,c), we need to decide for which of them it is possible to find algebraic numbers α and β, such that

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

and for which candidates it is not. In this Chapter all our impossibility proofs start with the following observation:

Lemma 4.6. *Let α and β be algebraic numbers, such that*

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

If $ab<2\cdot\operatorname{lcm}(a,b,c)$, then $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=\operatorname{lcm}(a,b,c)$.

Proof. Since $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ and $\mathbb{Q}(\alpha\beta)$ are subfields of $\mathbb{Q}(\alpha,\beta)$, we find that $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$ is divisible by both a and b, as well as by c. Thus, $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]$ is divisible by $\operatorname{lcm}(a,b,c)$, i.e., $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]=k\cdot\operatorname{lcm}(a,b,c)$ for some $k\in\mathbb{N}$. On the other hand,

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

Therefore, $ab < 2 \cdot \mathrm{lcm}(a,b,c)$ yields

$$k \cdot \mathrm{lcm}(a,b,c) < 2 \cdot \mathrm{lcm}(a,b,c).$$

Hence, $k = 1$ and $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = \mathrm{lcm}(a,b,c)$. □

A simple lemma below also takes part is some of the proofs.

Lemma 4.7 ([8, Proposition 21])**.** *Suppose that α and β are algebraic numbers of degrees m and n (over $\mathbb{Q}$), respectively. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$ be the distinct conjugates of α over $\mathbb{Q}$, and let $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ be the distinct conjugates of β over $\mathbb{Q}$. If β is of degree n over $\mathbb{Q}(\alpha)$, then all the numbers $\alpha_i\beta_j$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, are conjugate over $\mathbb{Q}$ (although not necessarily distinct).*

Evidently, Proposition 2.5 implies that the numbers $\alpha_i\beta_j$, where $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$, cover all possible conjugates of $\alpha\beta$. Lemma 4.7 describes the situation when they are all conjugate over $\mathbb{Q}$.

Recall that the Galois group of an irreducible polynomial acts transitively on the set of its roots (see Proposition 2.9). Lemma 4.8 below is a useful tool to decide whether this action is 2-transitive. The lemma follows from a more general group theoretical fact [18, Lemma 8.2]. For completeness and convenience, we give a proof adapted concretely for Galois groups.

Lemma 4.8. *Suppose that α is an algebraic number of degree $n \geqslant 3$. Let $\mathcal{A} := \{\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_n\}$ be the set of all the distinct conjugates of α over $\mathbb{Q}$, and let M be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Then the following conditions are equivalent:*

(i) the Galois group $\mathrm{Gal}(M/\mathbb{Q})$ acts 2-transitively on $\mathcal{A}$;

(ii) for some pair $\alpha_i \neq \alpha_j$, the degree of α_i over $\mathbb{Q}(\alpha_j)$ is equal to $n-1$;

(iii) for any pair $\alpha_i \neq \alpha_j$, the degree of α_i over $\mathbb{Q}(\alpha_j)$ is equal to $n-1$.

Proof. (ii) ⇒ (iii). Assume that the degree of α_i over $\mathbb{Q}(\alpha_j)$ equals $n-1$ for some pair $\alpha_i \neq \alpha_j$. Take any pair $\alpha_{i'} \neq \alpha_{j'}$ and write $\alpha_{j'} = \tau(\alpha_j)$, where $\tau \in \mathrm{Gal}(M/\mathbb{Q})$. Note that $\alpha_t \neq \alpha_{j'}$ implies $\tau^{-1}(\alpha_t) \neq \tau^{-1}(\alpha_{j'}) = \alpha_j$. Therefore, by the assumption, for any $\alpha_t \neq \alpha_{j'}$ there exists $\omega \in$

$\mathrm{Gal}(M/\mathbb{Q}(\alpha_j))$ such that $\omega(\tau^{-1}(\alpha_{i'})) = \tau^{-1}(\alpha_t)$. Set $\sigma := \tau \circ \omega \circ \tau^{-1}$. Then $\sigma(\alpha_{i'}) = \alpha_t$ and

$$\sigma(\alpha_{j'}) = (\tau \circ \omega)(\alpha_j) = \tau(\alpha_j) = \alpha_{j'},$$

i.e., $\sigma \in \mathrm{Gal}(M/\mathbb{Q}(\alpha_{j'}))$. Hence, any $\alpha_t \neq \alpha_{j'}$ is conjugate to $\alpha_{i'}$ over $\mathbb{Q}(\alpha_{j'})$, so that the degree of $\alpha_{i'}$ over $\mathbb{Q}(\alpha_{j'})$ equals $n-1$.

(iii) $\Rightarrow$ (i). Assume that the degree of α_i over $\mathbb{Q}(\alpha_j)$ equals $n-1$ for any pair $\alpha_i \neq \alpha_j$. Take any two pairs of conjugates $\alpha_i \neq \alpha_j$ and $\alpha_{i'} \neq \alpha_{j'}$. Suppose that $\alpha_{i'} \neq \alpha_j$. By the assumption, $\alpha_{i'}$ is conjugate to α_i over $\mathbb{Q}(\alpha_j)$. Hence, there exists $\tau \in \mathrm{Gal}(M/\mathbb{Q}(\alpha_j))$ such that $\tau(\alpha_i) = \alpha_{i'}$. Analogously, $\alpha_{j'}$ is conjugate to α_j over $\mathbb{Q}(\alpha_{i'})$. Hence, there exists $\omega \in \mathrm{Gal}(M/\mathbb{Q}(\alpha_{i'}))$ such that $\omega(\alpha_j) = \alpha_{j'}$. Set $\sigma := \omega \circ \tau$. Then

$$\begin{aligned}\sigma(\alpha_i) &= \omega(\alpha_{i'}) = \alpha_{i'},\\ \sigma(\alpha_j) &= \omega(\alpha_j) = \alpha_{j'}.\end{aligned}$$

Now consider the case when $\alpha_{i'} = \alpha_j$. Take any $t \in \{1,2,\ldots,n\} \setminus \{i,j\}$ (there is such t, since $n \geqslant 3$). By the same argument, there exist automorphisms $\tau \in \mathrm{Gal}(M/\mathbb{Q}(\alpha_i))$, $\rho \in \mathrm{Gal}(M/\mathbb{Q}(\alpha_t))$, and $\omega \in \mathrm{Gal}(M/\mathbb{Q}(\alpha_{i'})$ such that

$$\tau(\alpha_j) = \alpha_t,\ \rho(\alpha_i) = \alpha_{i'} \text{ and, } \omega(\alpha_t) = \alpha_{j'}.$$

Set $\sigma := \omega \circ \rho \circ \tau$. Then

$$\begin{aligned}\sigma(\alpha_i) &= (\omega \circ \rho)(\alpha_i) = \omega(\alpha_{i'}) = \alpha_{i'},\\ \sigma(\alpha_j) &= (\omega \circ \rho)(\alpha_t) = \omega(\alpha_t) = \alpha_{j'}.\end{aligned}$$

In both cases we find $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ which maps α_i to $\alpha_{i'}$ and α_j to $\alpha_{j'}$. Thus, $\mathrm{Gal}(M/\mathbb{Q})$ acts 2-transitively.

(i) $\Rightarrow$ (ii). Assume that the action of $\mathrm{Gal}(M/\mathbb{Q})$ on $\mathcal{A}$ is 2-transitive. Take any pair $\alpha_i \neq \alpha_j$. Then, for each $t \in \{1,2,\ldots,n\} \setminus \{j\}$, there exists $\sigma \in \mathrm{Gal}(M/\mathbb{Q}(\alpha_j))$ such that $\sigma(\alpha_i) = \alpha_t$, so that α_t is conjugate to α_i over $\mathbb{Q}(\alpha_j)$. Hence, the degree of α_i over $\mathbb{Q}(\alpha_j)$ equals $n-1$. (In fact, we proved the stronger statement that (i) implies (iii).) This completes the proof of Lemma 4.8. $\square$

4.3 Proofs of Theorems 4.2 and 4.3

Proof of Theorem 4.3. Necessity. Assume that the triplet (p,t,t) is product-feasible. Then there exist algebraic numbers α and β such that

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

Lemma 4.6 implies $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = \operatorname{lcm}(p,t) = pt$. Hence, we have the diagram as in Figure 4.1. Let $\beta_1 := \beta, \beta_2, \ldots, \beta_t$ be the distinct conjugates

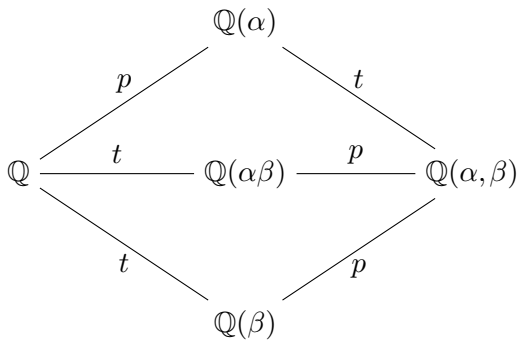

Figure 4.1: Diagram for the triplet (p,t,t)

of β over $\mathbb{Q}$. All the numbers

$$\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_t$$

are pairwise distinct and, by Lemma 4.7, they are all the conjugates of $\alpha\beta$ over $\mathbb{Q}$. Consequently, the product

$$(\alpha\beta_1)\cdots(\alpha\beta_t) = \alpha^t\beta_1\beta_2\cdots\beta_t$$

is a nonzero rational number. Moreover, $\beta_1\beta_2\cdots\beta_t \in \mathbb{Q}\setminus\{0\}$, so $\alpha^t =: a \in \mathbb{Q}\setminus\{0\}$. Therefore, α is a root of the polynomial $x^t - a$. On the other hand, $\alpha^t \in \mathbb{Q}$ is a nontrivial multiplicative relation between conjugates of α (with exponent t for α and zero exponents for other conjugates; see Section 2.2). Since $\deg\alpha = p > 2$ is a prime number, Proposition 2.10 implies that the minimal polynomial of α over $\mathbb{Q}$ is of the form $x^p - b$, $b \in \mathbb{Q}\setminus\{0\}$.

We have that $x^t - a$ is divisible by $x^p - b$. Hence, any root of $x^p - b$

is also a root of $x^t - a$, in particular, $x = b^{\frac{1}{p}}\zeta_p$. Thus,

$$b^{\frac{t}{p}}\zeta_p^t = a \in \mathbb{R} \Rightarrow \zeta_p^t \in \mathbb{R} \Rightarrow \sin\left(\frac{2\pi t}{p}\right) = 0 \Rightarrow \frac{2\pi t}{p} = \pi k,\ k \in \mathbb{Z} \Rightarrow 2t = pk.$$

Therefore, p divides $2t$. Clearly, $p \nmid 2$, since $p > 2$. Hence, we must have $p|t$. This completes the proof of the necessity.

Sufficiency. Let $t \geqslant p > 2$ and $t = pk$ for some positive integer k. The triplet $(1,k,k)$ obviously is product-feasible, whereas the triplet (p,p,p) satisfies the exponent triangle inequality with respect to any prime number (see Section 1.5). By Proposition 1.13, the triplet $(p,t,t) = (p\cdot 1, p\cdot k, p\cdot k)$ is product-feasible. This completes ther proof of Theorem 4.3. □

Now we turn to Theorem 4.2. Given any prime number $p > 2$ and any divisor d of $p-1$, we shall construct algebraic numbers α and β of degrees $p-1$ and p over $\mathbb{Q}$, respectively, whose product $\alpha\beta$ has degree pd. For the construction we will use so-called *Gaussian periods*. Let us briefly recall this classical notion.

Let n be a positive integer, and let $K_n := \mathbb{Q}(\zeta_n)$ be the *nth cyclotomic field*. Recall a well-known fact.

Theorem 4.9 ([29, Theorem 4.27])**.** *The extension $K_n/\mathbb{Q}$ is Galois of degree $\varphi(n)$, and its Galois group* $\mathrm{Gal}(K_n/\mathbb{Q})$ *is isomorphic to the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ of residues modulo n.*

In particular, if $n =: p$ is prime, then $\mathrm{Gal}(K_p/\mathbb{Q})$ is a cyclic group[1] of order $\varphi(p) = p-1$. Each generator σ of $\mathrm{Gal}(K_p/\mathbb{Q})$ is given by $\sigma : \zeta_p \mapsto \zeta_p^g$, where g is any primitive root modulo p.

Now take any divisor d of $p-1$ and set $m := (p-1)/d$. Consider the element

$$\theta_d = \zeta_p + \sigma^m(\zeta_p) + \sigma^{2m}(\zeta_p) + \cdots + \sigma^{(d-1)m}(\zeta_p), \tag{4.2}$$

where σ is any generator of $\mathrm{Gal}(K_p/\mathbb{Q})$. Note that θ_d does not depend on the choice of σ. We refer to θ_d as the *Gaussian d-period* corresponding to a prime number p. One can show easily that there are exactly d distinct

[1]Recall a well-known fact that the group $(\mathbb{Z}/n\mathbb{Z})^*$, $n > 1$, is cyclic if and only if $n = 2$, 4, p^k or $2p^k$, where $p > 2$ is prime and $k \in \mathbb{N}$ (see, e.g., [37]).

images of θ_d under all the automorphisms of $\mathrm{Gal}(K_p/\mathbb{Q})$. Therefore, $\deg\theta_d = d$.

We shall also use the following

Lemma 4.10 ([3, Problem 6523])**.** *Suppose α and β are algebraic conjugate numbers of degree d such that $\frac{\alpha}{\beta}$ is a primitive nth root of unity. Then $\varphi(n) = d$.*

Proof of Theorem 4.2. If $p = 2$, the assertion is obvious. If $d = p-1$, our triplet is product-feasible by Proposition 1.5. Suppose that $d < p-1$. Set

$$\alpha = \sqrt[p]{2},\ \beta = \theta_d\zeta_p,\ \gamma = \alpha\beta = \sqrt[p]{2}\zeta_p\theta_d,$$

here θ_d as in (4.2). Obviously, $\deg\alpha = p$. We claim that $\deg\beta = p-1$. Indeed, take any generator σ of $\mathrm{Gal}(K_p/\mathbb{Q})$. It suffices to show that all the numbers

$$\sigma^k(\theta_d\zeta_p),\ k = 1,2,\ldots,p-1,$$

are distinct. Assume to the contrary that $\sigma^k(\theta_d\zeta_p) = \sigma^l(\theta_d\zeta_p)$ for some k and l satisfying $1 \leqslant k < l \leqslant p-1$. Then $\sigma^k(\theta_d)\zeta_p^{g^k} = \sigma^l(\theta_d)\zeta_p^{g^l}$, and hence

$$\frac{\sigma^k(\theta_d)}{\sigma^l(\theta_d)} = e^{\frac{2(g^l-g^k)\pi i}{p}},$$

here g is a primitive root modulo p. Clearly, $g^l - g^k \not\equiv 0 \pmod p$. Therefore, $\sigma^k(\theta_d)/\sigma^l(\theta_d)$ is a primitive pth root of unity, which contradicts Lemma 4.10, since $d < p-1$. Hence, $\deg\beta = p-1$.

We now show that the degree of $\gamma = \sqrt[p]{2}\zeta_p\theta_d$ (over $\mathbb{Q}$) equals pd. Let $\theta_d = \theta_d^{(1)}, \theta_d^{(2)}, \ldots, \theta_d^{(d)}$ be all the conjugates of θ_d. Since the numbers $\deg(\sqrt[p]{2}\zeta_p) = p$ and $\deg\theta_d = d$ are coprime, Lemma 4.7 implies that all the numbers

$$\gamma_k^{(l)} := \sqrt[p]{2}\zeta_p^k\theta_d^{(l)},\ k = 0,1,\ldots,p-1,\ l = 1,2,\ldots,d, \tag{4.3}$$

are conjugate to γ over $\mathbb{Q}$. It suffices to show that all these numbers are distinct. Assume that $\gamma_{k_1}^{(l_1)} = \gamma_{k_2}^{(l_2)}$, where $k_1, k_2 \in \{0,1,\ldots,p-1\}$, $l_1, l_2 \in \{1,2,\ldots,d\}$, and either $k_1 \neq k_2$ or $l_1 \neq l_2$. Note that if $k_1 = k_2$,

then $l_1 = l_2$. Therefore, $k_1 \neq k_2$ and the equality $\gamma_{k_1}^{(l_1)} = \gamma_{k_2}^{(l_2)}$ implies

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

Since $e^{2\pi i(k_1-k_2)/p}$ is a primitive pth root of unity, Lemma 4.10 yields $p-1 = \varphi(p) \leqslant \deg\theta = d$, a contradiction. Hence, all the numbers in (4.3) are distinct, and therefore $\deg\gamma = pd$. This completes the proof of Theorem 4.2. □

4.4 Proof of Theorem 4.4

Suppose to the contrary that the triplet $(p+1, p+1, 2p)$ is product-feasible. Then there exist algebraic numbers α and β, such that

$$[\mathbb{Q}(\alpha):\mathbb{Q}] = [\mathbb{Q}(\beta):\mathbb{Q}] = p+1 \text{ and } [\mathbb{Q}(\alpha\beta):\mathbb{Q}] = 2p.$$

Note, that $\operatorname{lcm}(p+1, p+1, 2p) = p(p+1)$ and $(p+1)^2 < 2p(p+1)$. Therefore, Lemma 4.6 implies $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}] = p(p+1)$ and we have the following diagram:

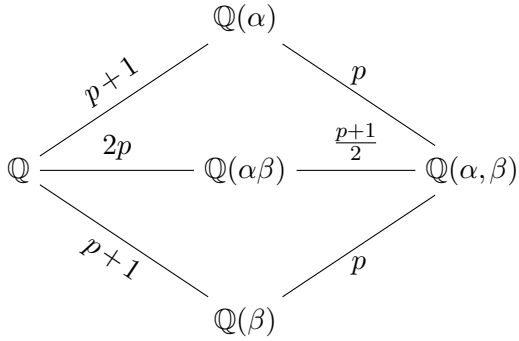

Figure 4.2: Degree diagram for α and β

Let M be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

Claim 4.4.1. *The Galois group* $\mathrm{Gal}(M/\mathbb{Q})$ *acts* 2*-transitively on the conjugates of* α *over* $\mathbb{Q}$.

Proof. Let $\beta_1, \beta_2 := \beta, \beta_3, \ldots, \beta_{p+1}$ be all the distinct conjugates of β over $\mathbb{Q}$. By Figure 4.2, β is of degree p over $\mathbb{Q}(\alpha)$. Consequently, β has exactly one conjugate, say, β_1 in $\mathbb{Q}(\alpha)$ (note that $\beta \notin \mathbb{Q}(\alpha)$, since otherwise

$\mathbb{Q}(\alpha,\beta)=\mathbb{Q}(\alpha)$ and $[\mathbb{Q}(\alpha,\beta):\mathbb{Q})]=p+1\neq p(p+1)$, a contradiction). Thus, for some $f(x)\in\mathbb{Q}[x]$

$$\beta_1=f(\alpha). \tag{4.4}$$

Analogously, for any conjugate β_j of β, there exists a conjugate of α, say, α_j, such that $\beta_j=f(\alpha_j)$. Indeed, let N be the Galois closure of $\mathbb{Q}(\alpha,\beta)$ over $\mathbb{Q}$. Then for each $j\in\{1,2,\ldots,p+1\}$ there exists $\sigma_j\in\mathrm{Gal}(N/\mathbb{Q})$ such that $\sigma_j(\beta_1)=\beta_j$. Applying it to (4.4) and setting $\sigma_j(\alpha)=:\alpha_j$, we get $\beta_j=f(\alpha_j)$. Here $\alpha_1:=\alpha,\alpha_2,\ldots,\alpha_{p+1}$ are the distinct cojugates of α over $\mathbb{Q}$ (note that if $\alpha_i=\alpha_j$ for some $i\neq j$, then (4.4) would imply $\beta_i=\beta_j$, a contradiction). In particular, $\beta=f(\alpha_2)$, and hence $\mathbb{Q}(\beta)=\mathbb{Q}(f(\alpha_2))\subseteq\mathbb{Q}(\alpha_2)$. Since $[\mathbb{Q}(\beta):\mathbb{Q}]=[\mathbb{Q}(\alpha_2):\mathbb{Q}]$, we get $\mathbb{Q}(\beta)=\mathbb{Q}(\alpha_2)$. Therefore, Figure 4.2 can be rewritten as follows (Figure 4.3):

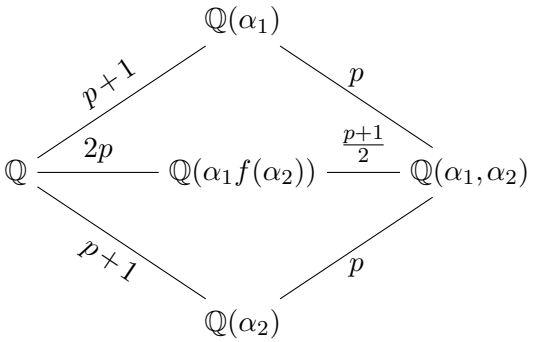

Figure 4.3: Degree diagram for α_1 and α_2

By Figure 4.3, α_2 is of degree p over $\mathbb{Q}(\alpha_1)$. Consequently, the Galois group $\mathrm{Gal}(M/\mathbb{Q})$ acts 2-transitively on $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ by Lemma 4.8. □

Set $A:=\{1,2,\ldots,p\}$. Claim 4.4.1 implies that for any indices $i,j\in A$, $i\neq j$, there exists an automorphism of $\mathrm{Gal}(M/\mathbb{Q})$ which maps $\alpha_1 f(\alpha_2)$ to $\alpha_i f(\alpha_j)$. Hence, all the numbers

$$\alpha_i f(\alpha_j),\ i,j\in A,\ i\neq j, \tag{4.5}$$

are conjugates of $\alpha_1 f(\alpha_2)$ over $\mathbb{Q}$. Evidently, the numbers $\alpha_i f(\alpha_j)$, $i,j\in A$, cover all possible conjugates of $\alpha_1 f(\alpha_2)$. Note that, for $i=j$,

we have $\alpha_i f(\alpha_i) \in \mathbb{Q}(\alpha_i)$, and hence

$$\deg(\alpha_i f(\alpha_i)) \leqslant \deg \alpha_i = p+1 < 2p = \deg(\alpha_1 f(\alpha_2)).$$

This means that none of the numbers $\alpha_i f(\alpha_i)$, $i \in A$, is conjugate to $\alpha_1 f(\alpha_2)$ over $\mathbb{Q}$. Therefore, (4.5) exhaust all the conjugates of $\alpha_1 f(\alpha_2)$. So, among $p(p+1)$ numbers in (4.5), there are exactly $2p$ distinct. Hence, there is a number, which occurs at least $p(p+1)/2p = (p+1)/2 =: k$ times. In other words, there exist distinct indices $i_1, i_2, \ldots, i_k$ and distinct indices $j_1, j_2, \ldots, j_k$ in A, with $i_l \neq j_l$, such that

$$\alpha_{i_1} f(\alpha_{j_1}) = \alpha_{i_2} f(\alpha_{j_2}) = \ldots = \alpha_{i_k} f(\alpha_{j_k}).$$

Since $k \geqslant 3$, we can assume that $i_1 \neq j_2$, so that

$$i_1 \notin \{j_1, i_2, j_2\}. \tag{4.6}$$

Consider the Galois group $\mathrm{Gal}(M/\mathbb{Q}) =: G$ as a subgroup of S_{p+1} acting on the set $A = \{1, 2, \ldots, p+1\}$, i.e., if $\sigma \in G$, then $\sigma(\alpha_k) = \alpha_{\sigma(k)}$, $k \in A$. The order of this group $|G|$ equals $[M : \mathbb{Q}]$. Since M has a subfield $\mathbb{Q}(\alpha_1, \alpha_2)$ of degree $p(p+1)$ over $\mathbb{Q}$, we find that $|G|$ is divisible by p. Therefore, by Cauchy's Theorem, there exists a permutation $\tau \in G$ of order p. Clearly, τ must be a cycle of length p. Thus, τ has exactly one fixed point, say, $k \in A$ i.e., $\tau(\alpha_k) = \alpha_k$.

Claim 4.4.2. *The number α_k^{p+1} is rational.*

Proof. Consider the equality

$$\alpha_{i_1} f(\alpha_{j_1}) = \alpha_{i_2} f(\alpha_{j_2}). \tag{4.7}$$

Take $\sigma \in G$, which maps α_{i_1} to α_k. Applying it to (4.7) and setting $\sigma(j_1) =: a$, $\sigma(i_2) =: b$, $\sigma(j_2) =: c$, we obtain

$$\alpha_k f(\alpha_a) = \alpha_b f(\alpha_c). \tag{4.8}$$

Note that (4.6) implies $k \notin \{a, b, c\}$. Now, applying τ to (4.8) repeatedly, we obtain $(p-1)$ additional equalities

$$\alpha_k f(\alpha_{\tau^l(a)}) = \alpha_{\tau^l(b)} f(\alpha_{\tau^l(c)}),\ l = 1, 2, \ldots, p-1. \tag{4.9}$$

The orbits

$$\{a, \tau(a), \tau^2(a), \ldots, \tau^{p-1}(a)\},$$
$$\{b, \tau(b), \tau^2(b), \ldots, \tau^{p-1}(b)\},$$
$$\{c, \tau(c), \tau^2(c), \ldots, \tau^{p-1}(c)\}$$

coincide with the set $A \setminus \{k\}$, since none of a, b and c equals k. Thus, mutiplying (4.8), and all $(p-1)$ equalities of (4.9) we find that

$$\alpha_k^p \cdot \prod_{\substack{i=1 \\ i\neq k}}^{p+1} f(\alpha_i) = \prod_{\substack{i=1 \\ i\neq k}}^{p+1} \alpha_i \cdot \prod_{\substack{i=1 \\ i\neq k}}^{p+1} f(\alpha_i), \text{ i.e., } \alpha_k^p = \prod_{\substack{i=1 \\ i\neq k}}^{p+1} \alpha_i.$$

Consequently, $\alpha_k^{p+1} = \prod_{i=1}^{p+1} \alpha_i \in \mathbb{Q}$. □

We now can finish the proof of Theorem 4.4. Claim 4.4.2 implies that the minimal polynomial of α (over $\mathbb{Q}$) is of the form $x^{p+1} - r_1$, $r_1 \in \mathbb{Q}$. All the preceding part of the proof is symmetric with respect to α and β. Therefore, interchanging α and β, we find that the minimal polynomial of β is also of the form $x^{p+1} - r_2$, $r_2 \in \mathbb{Q}$. This yealds $\alpha\beta$ is a root of $x^{p+1} - r_1 r_2$. Hence, $\deg(\alpha\beta) \leqslant p+1 < 2p$, a contradiction.

4.5 Proof of Theorem 4.5

Sufficiency. Assume n is a prime number. Then the numbers

$$\alpha := \sqrt[n]{2},\ \beta := \zeta_n = e^{\frac{2\pi i}{n}},\ \text{and } \alpha\beta = \sqrt[n]{2}\zeta_n$$

are of degrees n, $\varphi(n) = n-1$, and n (over $\mathbb{Q}$), respectively. On the other hand, for any $k \geqslant 1$, the triplet $(1, k, k)$ satisfies the exponent triangle inequality with respect to any prime number. Consequently, the triplet $(n, (n-1)k, nk)$ is product-feasible by Proposition 1.13.

Necessity. Let $n \geqslant 2$ be a composite number. Then $n \geqslant 4$. Suppose to the contrary that the triplet $(a, b, c) = (n, (n-1)k, nk)$, $k \geqslant 1$, is product-feasible. Then there exist algebraic numbers α and β, satisfying

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

Note that

$$\operatorname{lcm}(a,b,c) = \operatorname{lcm}(b,c) = \frac{bc}{\gcd(b,c)} = \frac{(n-1)k \cdot nk}{k} = ab.$$

Hence, by Lemma 4.6, $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}] = ab$ and

$$[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha\beta)] = \frac{ab}{c} = n-1 = a-1.$$

Thus, we have the diagram as in Figure 4.4.

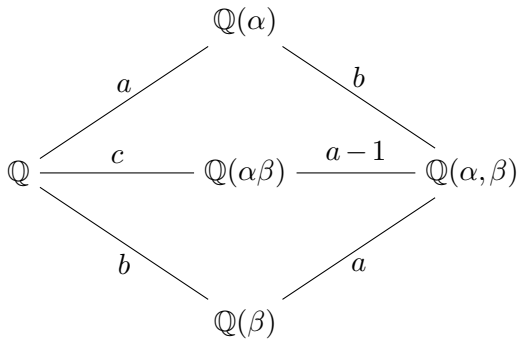

Figure 4.4: Degree diagram for α, β and $\alpha\beta$

Let $\alpha_1 := \alpha$, α_2, ..., α_a be the distinct conjugates of α over $\mathbb{Q}$, and let $\beta_1 := \beta$, β_2, ..., β_b be the distinct conjugates of β over $\mathbb{Q}$. Denote

$$A := \{1,2,\ldots,a\} \quad \text{and} \quad B := \{1,2,\ldots,b\}.$$

Moreover, for $s = 1,\ldots,a$, we set

$$\Gamma_s := \{\alpha_s\beta_1, \alpha_s\beta_2, \ldots, \alpha_s\beta_b\}.$$

Figure 4.4 and Lemma 4.7 imply that the set $\cup_{s=1}^{a}\Gamma_s$ exhausts all the conjugates of $\alpha\beta$ over $\mathbb{Q}$, and hence it must have exactly c distinct elements. Therefore, for any distinct $i,j \in A$, we have

$$c = |\cup_{s=1}^{a}\Gamma_s| \geqslant |\Gamma_i \cup \Gamma_j| = |\Gamma_i| + |\Gamma_j| - |\Gamma_i \cap \Gamma_j| = b + b - |\Gamma_i \cap \Gamma_j|,$$

which implies

$$|\Gamma_i \cap \Gamma_j| \geqslant 2b - c = 2(n-1)k - nk = nk - 2k > \frac{(n-1)k}{2} = \frac{b}{2}.$$

Thus, we obtain more than $b/2$ equalities of the form

$$\alpha_i\beta_u = \alpha_j\beta_v,$$

where u and v run through some subsets $U \subseteq B$ and $V \subseteq B$, respectively. Clearly, $|U| = |V| > b/2$ implies $U \cap V \neq \emptyset$. Take any $t \in U \cap V$. Then $\alpha_i\beta_t = \alpha_j\beta_u$ and $\alpha_i\beta_v = \alpha_j\beta_t$ for some $u \in U$ and $v \in V$. From $\alpha_i\beta_t/(\alpha_i\beta_v) = \alpha_j\beta_u/(\alpha_j\beta_t)$, we deduce $\beta_t^2 = \beta_u\beta_v$. If $u \neq v$, then, by Lemma 2.11, for some $m \in \mathbb{N}$ we get $\beta_t^m = \beta_u^m$. If $u = v$, then the same equality with $m = 2$ follows directly. Therefore, from $\alpha_i^m\beta_t^m = \alpha_j^m\beta_u^m$, we deduce

$$\alpha_i^m = \alpha_j^m, \tag{4.10}$$

here $m \in \mathbb{N}$ and $m > 1$ in view of $i \neq j$.

Set $\mathcal{A} := \{\alpha_1, \alpha_2, \ldots, \alpha_a\}$. Let M be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$.

Claim 4.5.1. *The Galois group* $\mathrm{Gal}(M/\mathbb{Q})$ *acts 2-transitively on* $\mathcal{A}$.

Proof. We will find a conjugate of α over $\mathbb{Q}$ which is of degree $a-1$ over $\mathbb{Q}(\alpha)$. Then the claim will follow in view of Lemma 4.8.

Since β is of degree b over $\mathbb{Q}(\alpha)$, all the numbers

$$\gamma_t := \alpha\beta_t,\ t = 1, 2, \ldots, b,$$

are conjugate to $\gamma_1 = \alpha\beta$ over $\mathbb{Q}$ by Lemma 4.7. Let the remaining conjugates of γ_1 over $\mathbb{Q}$ be

$$\gamma_{b+1}, \gamma_{b+2}, \ldots, \gamma_c.$$

In particular, $\gamma_c \neq \alpha\beta_t$ for $t \in B$. Hence, $\gamma_c = \alpha_i\beta_j$ for some $i \in A \setminus \{1\}$ and some $j \in B$.

Take the polynomials

$$g(x) := (x-\gamma_1)(x-\gamma_2)\cdots(x-\gamma_b) = \alpha^b P_\beta\Big(\frac{x}{\alpha}\Big),$$
$$h(x) := (x-\gamma_{b+1})(x-\gamma_{b+2})\cdots(x-\gamma_c) = \frac{P_\gamma(x)}{g(x)},$$

where $P_\beta(x)$ and $P_\gamma(x)$ are the minimal polynomials of β and γ over

$\mathbb{Q}$, respectively. Set $K := \mathbb{Q}(\alpha)$. Clearly, $g(x) \in K[x]$, and hence $h(x) \in K[x]$. This means that for t satisfying $b+1 \leqslant t \leqslant c$, we have

$$[K(\gamma_t) : K] \leqslant \deg h = c - b = nk - (n-1)k = k.$$

Evidently, $[K(\alpha_i) : K] \leqslant a - 1$. Also, $[K(\beta) : K] = [\mathbb{Q}(\beta) : \mathbb{Q}] = b$ implies that β and β_j are conjugate also over K, and hence $[K(\beta_j) : K] = b$. Therefore,

$$\begin{aligned} b = [K(\beta_j) : K] = [K(\gamma_c \cdot \alpha_i^{-1}) : K] \leqslant [K(\gamma_c) : K][K(\alpha_i^{-1}) : K] \leqslant \\ \leqslant k \cdot [K(\alpha_i) : K] \leqslant k(a-1) = (n-1)k = b. \end{aligned}$$

This implies $[K(\gamma_c) : K] = k$ and $[K(\alpha_i) : K] = a - 1$. Thus, α_i is of degree $a - 1$ over K. Therefore, $\mathrm{Gal}(M/\mathbb{Q})$ is 2-transitive on $\mathcal{A}$ by Lemma 4.8. □

Claim 4.5.2. *Under the previous notations, assume that there exists $m \in \mathbb{N}$ such that $\alpha_i^m \in \mathbb{Q}(\alpha_j)$ for some two distinct conjugates α_i, α_j of α over $\mathbb{Q}$. Then there exists a rational number r such that $\alpha_1^m = \alpha_2^m = \cdots = \alpha_n^m = r$.*

Proof. Write $\alpha_i^m = G(\alpha_j)$, where $G \in \mathbb{Q}[x]$. Take any $t \in A \setminus \{j\}$. By Claim 4.5.1, there is an automorphism of the Galois group $\mathrm{Gal}(M/\mathbb{Q})$ which maps α_i to α_t and α_j to α_j. Applying it to $\alpha_i^m = G(\alpha_j)$, we get $\alpha_t^m = G(\alpha_j)$. Therefore, α_t^m are equal for $t \in A \setminus \{j\}$. Choosing $t \notin A \setminus \{i, j\}$ we can apply the same argument to the equality $\alpha_i^m = \alpha_t^m$ by mapping α_i to α_j and α_t to α_t. This yields $\alpha_j^m = \alpha_t^m$, and hence $\alpha_1^m = \alpha_2^m = \cdots = \alpha_n^m$. Adding all these n equal elements, we obtain $\sum_{t=1}^n \alpha_t^m$, which is a rational number as a power sum of the roots of a polynomial over $\mathbb{Q}$. Thus, α_t^m, $t = 1, 2, \ldots, n$, are all equal to this rational number divided by n. □

Now we can finish the proof of Theorem 4.5. In view of Claim 4.5.2, equality (4.10) implies that the conjugates of α over $\mathbb{Q}$ all have the same moduli. Consider two cases depending on whether the composite number $a = n$ is even or odd. If n is even and α has no real conjugates, then the product w of all conjugates can be written in the form $w = (\alpha\overline{\alpha})^{n/2}$. If α has a real conjugate, say α', then $-\alpha'$ is also its conjugate (as the number of nonreal conjugates is even), so $w = -(\alpha_i\overline{\alpha_i})^{n/2}$ for any nonreal

α_i. Therefore, in both cases, there are two distinct indices $i, j \in A$ such that $\alpha_i^{n/2} \in \mathbb{Q}(\alpha_j)$. By Claim 4.5.2, we conclude that $\alpha_t^{n/2} = r \in \mathbb{Q}$ for every $t \in A$. So α is of degree at most $n/2$ over $\mathbb{Q}$, which is not the case, since α is of degree $n > n/2$ over $\mathbb{Q}$.

Likewise, if $a = n$ is odd, then α has a real conjugate α_i, and so the product w of all the conjugates of α can be written as α_i^n (in both cases $\alpha_i > 0$ and $\alpha_i < 0$). Hence, $\alpha_i^n = w \in \mathbb{Q} \setminus \{0\}$. Since α_i is of degree n over $\mathbb{Q}$, we find that the minimal polynomial of α_i as well as of α over $\mathbb{Q}$ is $x^n - w$. Consequently, the conjugates of α are

$$w^{1/n}\zeta_n^t, \quad t = 0, 1, \ldots, n-1,$$

here $\zeta_n = e^{\frac{2\pi i}{n}}$. By Claim 4.5.1 and Lemma 4.8, the number $w^{1/n}\zeta_n$ has degree $n-1$ over the field $\mathbb{Q}(w^{1/n})$, because $w^{1/n}\zeta_n \neq w^{1/n}$ are the conjugates of α. This implies that the degree of $\zeta_n = \frac{w^{1/n}\zeta_n}{w^{1/n}}$ over the field $\mathbb{Q}(w^{1/n})$ equals $n-1$. Consequently, the degree of ζ_n over its subfield $\mathbb{Q}$ must be at least $n-1$. However, the degree of ζ_n over $\mathbb{Q}$ equals $\varphi(n)$, and for each composite n we have $\varphi(n) < n-1$, a contradiction. This completes the proof of Theorem 4.5.

4.6 Proof of Theorem 4.1

Using Proposition 1.4 we determine all possible candidates to product-feasible triplets (a, b, c) with $a \leqslant b \leqslant c$ and $b \leqslant 7$. They are all listed in Table 4.2.

$b\backslash a$	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

Table 4.2: Candidates to product-feasible triplets

The triplets with c being circled are not product-feasible. Indeed, $(2,5,5)$ and $(2,7,7)$ are not product-feasible by Proposition 1.14, $(3,4,4)$, $(3,5,5)$, $(3,7,7)$, $(5,6,6)$ and $(5,7,7)$ - by Theorem 4.3, $(6,6,10)$ - by Theorem 4.4, $(5,5,15)$ and $(7,7,35)$ - by Theorem 3.3, whereas $(4,6,8)$ are not product-feasible by Theorem 4.5 with $(n,k)=(4,2)$. Finally, by Proposition 1.15, the product of a quartic number and a septic number must be of degree 28, whereas the product of a quintic number and a sextic number must be of degree 30. Hence, the triplets $(4,7,7)$, $(4,7,14)$, $(5,6,10)$ and $(5,6,15)$ are also not product-feasible.

The blue-marked triplets are product-feasible. Indeed, as we have noted at the beginning of the chapter, $(2,3,3)$, $(3,4,6)$, $(3,6,9)$ and $(6,6,8)$ are product-feasible by Propositions 1.14 and 1.13, whereas the triplets $(4,5,5)$, $(4,5,10)$, $(6,7,7)$, $(6,7,14)$ and $(6,7,21)$ are product-feasible by Theorem 4.2.

All the remaining triplets are sum-feasible by the results in [8, 7], and hence they are also product-feasible by Proposition 1.3. Hence, the proof of Theorem 4.1 is completed.

4.7 The triplet $(4,6,8)$

Recall that Theorem 4.5 with $(n,k)=(4,2)$ implies the following

Proposition 4.11. *The triplet* $(4,6,8)$ *is not product-feasible.*

In the present section we give another proof of Proposition 4.11. This alternative proof contains some new ideas that may be useful in treating similar problems for algebraic numbers of small degrees.

In the proof, assuming that there exist α and β of degree 4 and 6 over $\mathbb{Q}$, respectively, whose product $\alpha\beta$ is of degree 8, we will first show that the conjugates of α must all be of the same modulus. In 1969, Robinson [31] described algebraic integers α whose conjugates (including α itself) are all of the same modulus; see also [12] for the description of algebraic numbers with conjugates of two distinct moduli. Here, we need a more specific result for quartic algebraic numbers α whose all four conjugates have equal moduli.

Proposition 4.12. *Assume that* $p(x)$ *is a monic quartic polynomial in* $\mathbb{Q}[x]$ *which is irreducible over* $\mathbb{Q}$ *and whose all* 4 *roots have equal moduli. Then* $p(x)$ *must be of one of the following forms:*

(i) $x^4 - r$, *where* $r \in \mathbb{Q}_{>0}$;

(ii) $x^4 + sx^2 + r$, *where* $s, r \in \mathbb{Q}$ *and* $s^2 < 4r$;

(iii) $(x^2 + ux + r)(x^2 + u'x + r)$, *where* $r \in \mathbb{Q}$ *and* $u \neq u'$ *are conjugate real quadratic algebraic numbers satisfying* $\max(u^2, u'^2) < 4r$.

Proof of Proposition 4.12. Write

$$\begin{aligned} p(x) &= x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \\ &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4). \end{aligned} \tag{4.11}$$

Case 1. Assume first that $p(x)$ has a real root. By the assumptions of the proposition, not all four roots of $p(x)$ can be real. Thus, $p(x)$ must have a pair of complex conjugate roots, and another real root. So, after re-indexing the roots of $p(x)$, if necessary, we can write $\{\alpha_1, \alpha_2\} = \{\alpha, -\alpha\}$ and $\{\alpha_3, \alpha_4\} = \{\alpha e^{i\varphi}, \alpha e^{-i\varphi}\}$ for some $\alpha > 0$ and $\varphi \in (0, \pi)$. It follows that $a_0 = \alpha_1\alpha_2\alpha_3\alpha_4 = -\alpha^4$ is a negative rational number, say, $-r$, where $r \in \mathbb{Q}_{>0}$. Note that the polynomial $p(-x)$ also has α as a root. Therefore, $p(-x)$ is divisible by the minimal polynomial of α over $\mathbb{Q}$ which is $p(x)$. Since both polynomials $p(x)$ and $p(-x)$ are monic and of the same degree, we must have $p(-x) = p(x)$. Hence, $a_1 = a_3 = 0$ and so

$$p(x) = x^4 + a_2x^2 + a_0 = x^4 + a_2x^2 - r.$$

Now, by Vieta's theorem and $\alpha_1 + \alpha_2 = 0$, we deduce

$$\begin{aligned} a_2 &= \alpha_1\alpha_2 + (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) + \alpha_3\alpha_4 \\ &= \alpha_1\alpha_2 + \alpha_3\alpha_4 = \alpha \cdot (-\alpha) + \alpha e^{i\varphi} \cdot \alpha e^{-i\varphi} = -\alpha^2 + \alpha^2 = 0, \end{aligned}$$

which implies that $p(x)$ is as in (i).

Case 2. Next, consider the case when $p(x)$ has no real roots. Then, after re-indexing the roots of $p(x)$, if necessary, we can write $\{\alpha_1, \alpha_2\} = \{\varrho e^{i\varphi}, \varrho e^{-i\varphi}\}$ and $\{\alpha_3, \alpha_4\} = \{\varrho e^{i\xi}, \varrho e^{-i\xi}\}$ for some $\varrho > 0$ and $0 < \varphi < \xi < \pi$. This time, by (4.11), we obtain $a_0 = \alpha_1\alpha_2\alpha_3\alpha_4 = \varrho^4 \in \mathbb{Q}_{>0}$. Furthermore, by Vieta's theorem,

$$a_3 = -(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) = -2\varrho(\cos\varphi + \cos\xi) \tag{4.12}$$

and

$$a_1 = -a_0\left(\frac{1}{\alpha_1}+\frac{1}{\alpha_2}+\frac{1}{\alpha_3}+\frac{1}{\alpha_4}\right) = -a_0\frac{2(\cos\varphi+\cos\xi)}{\varrho}$$
$$= -\varrho^4\frac{2(\cos\varphi+\cos\xi)}{\varrho} = -2\varrho^3(\cos\varphi+\cos\xi) = \varrho^2 a_3.$$

Likewise, by Vieta's theorem, we deduce

$$a_2 = \alpha_1\alpha_2+\alpha_3\alpha_4+(\alpha_1+\alpha_2)(\alpha_3+\alpha_4) = 2\varrho^2+4\varrho^2\cos\varphi\cos\xi. \quad (4.13)$$

Subcase 2.1. If $a_3 = 0$, then $a_1 = \varrho^2 a_3 = 0$ and $\cos\varphi = -\cos\xi$ by (4.12). Thus, (4.13) yields

$$a_2 = 2\varrho^2(1-2\cos^2\xi) = -2\varrho^2\cos(2\xi) \in \mathbb{Q}.$$

Set $r := a_0 = \varrho^4$ and $s := a_2 = -2\sqrt{r}\cos(2\xi)$. Then $r \in \mathbb{Q}_{>0}$ and $s \in \mathbb{Q}$. Note that $\cos^2(2\xi) \neq 1$, since otherwise $p(x)$ has a real root. Therefore, we obtain the polynomial $p(x) = x^4+sx^2+r \in \mathbb{Q}[x]$ with $s^2 = 4r\cos^2(2\xi) < 4r$ as described in case (ii).

Subcase 2.2. Now, if $a_3 \neq 0$, then $a_1 = \varrho^2 a_3 \neq 0$ and $\varrho^2 = a_1/a_3 \in \mathbb{Q}_{>0}$. Set $r := \varrho^2$. Since $\alpha_1\alpha_2 = \alpha_3\alpha_4 = r$, setting

$$\begin{aligned} u &:= -(\alpha_1+\alpha_2) = -2\sqrt{r}\cos(\varphi), \\ u' &:= -(\alpha_3+\alpha_4) = -2\sqrt{r}\cos(\xi), \end{aligned} \quad (4.14)$$

by (4.11), we obtain

$$p(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4) = (x^2+ux+r)(x^2+u'x+r).$$

Here the numbers u and u' are both real by (4.14) and both irrational, because otherwise $p(x)$ were reducible over $\mathbb{Q}$. On the other hand, $u+u' = a_3 \in \mathbb{Q}$ and $uu' = a_2-2r \in \mathbb{Q}$. Consequently, u and u' are roots of the quadratic polynomial

$$x^2-(u+u')x+uu' \in \mathbb{Q}[x],$$

which is irreducible over $\mathbb{Q}$ due to $u, u' \notin \mathbb{Q}$, i.e., u and u' are real quadratic conjugates over $\mathbb{Q}$. Moreover, since the roots of x^2+ux+r and $x^2+u'x+r$ are all nonreal, we must have $u^2-4r<0$ and $u'^2-4r<0$.

Therefore, $p(x)$ is a polynomial of the form as described in (iii). This completes the proof of Proposition 4.12. □

Proof of Proposition 4.11. Suppose there exist algebraic numbers α and β satisfying

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=4,\ [\mathbb{Q}(\beta):\mathbb{Q}]=6,\ \text{and}\ [\mathbb{Q}(\alpha\beta):\mathbb{Q}]=8.$$

The beginning of the argument is the same as that in the proof of Theorem 4.5. Setting $(n,k)=(4,2)$ we obtain the diagram as in Figure 4.5. Moreover, for any $i,j\in\{1,2,3,4\}$ with $i\neq j$, we deduce the equality (4.10). In particular,

$$\alpha_1^{m_1}=\alpha_2^{m_1},\ \alpha_1^{m_2}=\alpha_3^{m_2},\ \text{and}\ \alpha_1^{m_3}=\alpha_4^{m_3}$$

for some $m_1,m_2,m_3\in\mathbb{N}$. This yields that the conjugates of α over $\mathbb{Q}$ all have the same moduli.

Again, as in the proof of Theorem 4.5, for $s=1,2,3,4$ we set

$$\Gamma_s:=\{\alpha_s\beta_1,\alpha_s\beta_2,\ldots,\alpha_s\beta_6\}.$$

By Lemma 4.7 with $(a,b)=(4,6)$, the full list of conjugates of $\alpha\beta$ is,

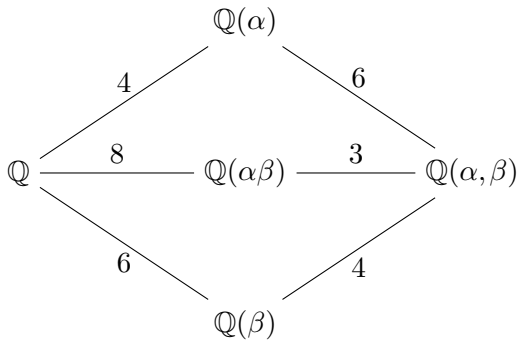

Figure 4.5: Diagram for the product-feasible triplet $(4,6,8)$

for instance,

$$\underbrace{\alpha\beta_1,\ \alpha\beta_2,\ldots,\alpha\beta_6}_{\Gamma_1},\ \alpha_i\beta_t,\ \alpha_j\beta_l \tag{4.15}$$

for some $i,j\in\{2,3,4\}$ and some $t,l\in\{1,2,3,4,5,6\}$. In (4.15) we can

choose any distinct products $\alpha_i\beta_t$ and $\alpha_j\beta_l$ which do not belong to Γ_1, i.e., for indices i and j, we must have

$$\Gamma_i \neq \Gamma_1 \text{ and } \Gamma_j \neq \Gamma_1. \tag{4.16}$$

Adding and multiplying all eight conjugates in (4.15) we obtain

$$\alpha r_1 + \alpha_i\beta_t + \alpha_j\beta_l =: r_2 \in \mathbb{Q} \quad \text{and} \quad \alpha^6 r_3(\alpha_i\beta_t)(\alpha_j\beta_l) =: r_4 \in \mathbb{Q}\setminus\{0\},$$

where $r_1 := \beta_1 + \beta_2 + \cdots + \beta_6 \in \mathbb{Q}$ and $r_3 := \beta_1\beta_2\cdots\beta_6 \in \mathbb{Q}\setminus\{0\}$. This yields

$$\alpha r_1 + \alpha_i\beta_t + \frac{r_4}{\alpha^6 r_3(\alpha_i\beta_t)} = r_2,$$

and hence

$$\alpha_i\beta_t + \frac{r_4}{\alpha^6 r_3(\alpha_i\beta_t)} = r_2 - \alpha r_1. \tag{4.17}$$

Squaring (4.17) and multiplying it by $\alpha_i^2\beta_t^2$, we find that

$$\alpha_i^4\beta_t^4 + \left(\frac{2r_4}{\alpha^6 r_3} - (r_2 - \alpha r_1)^2\right)\alpha_i^2\beta_t^2 + \frac{r_4^2}{\alpha^{12} r_3^2} = 0. \tag{4.18}$$

Thus, β_t is a root of degree 4 polynomial over the field $\mathbb{Q}(\alpha, \alpha_i^2)$.

Since all the conjugates of α have equal moduli, there are three possible cases for the minimal polynomial of α that are listed in Proposition 4.12. Consider each case separately.

In case (i), we have $\alpha_i = \alpha\varepsilon$ for some $\varepsilon \in \{-1, \pm i\}$. Then $\alpha_i^2 = \alpha^2$ or $\alpha_i^2 = -\alpha^2$, which implies $\mathbb{Q}(\alpha, \alpha_i^2) = \mathbb{Q}(\alpha)$. Therefore, the degree of β_t over $\mathbb{Q}(\alpha)$ is at most 4. On the other hand, by Figure 4.5, the degree of β over $\mathbb{Q}(\alpha)$ equals 6, thus β and β_t are also conjugate over $\mathbb{Q}(\alpha)$. So the degree of β_t over $\mathbb{Q}(\alpha)$ equals 6, a contradiction.

In case (ii), since both α^2 and α_i^2 are the roots of the polynomial $x^2 + sx + r$, we must have either $\alpha_i^2 = \alpha^2$ or $\alpha_i^2 = -s - \alpha^2$. In both cases $\mathbb{Q}(\alpha, \alpha_i^2) = \mathbb{Q}(\alpha)$, and we get the same contradiction.

It remains to consider case (iii). Then α is non-real. Assume without loss of generality that α_2 is the complex conjugate of $\alpha_1 = \alpha$. Note that in case (iii) both α_1 and $\alpha_2 = \overline{\alpha_1}$ are the roots of the same quadratic factor $x^2 + ux + r$ or $x^2 + u'x + r$, since $u, u', r \in \mathbb{R}$. Hence, $\alpha_2\alpha = r$.

If $\Gamma_1 \neq \Gamma_2$, then we can take in (4.15) $i = 2$, and so $\alpha_i = \alpha_2$. From $\alpha_i = \alpha_2 = r/\alpha$ we get $\mathbb{Q}(\alpha, \alpha_i^2) = \mathbb{Q}(\alpha)$, so that (4.18) leads to the same contradiction again.

In the alternative case, when $\Gamma_1 = \Gamma_2$, we obtain

$$\alpha\beta_\ell = \alpha_2\beta_{\tau(\ell)} \text{ for } \ell = 1, 2, \ldots, 6, \tag{4.19}$$

where $\{\tau(1), \tau(2), \ldots, \tau(6)\} = \{1, 2, \ldots, 6\}$. This time, in view of (4.16), we cannot take $i = 2$, so that $i \in \{3, 4\}$. Multiplying all equalities in (4.19) we obtain $\alpha^6 = \alpha_2^6$. Since $\alpha_2 = \overline{\alpha}$ and $\alpha_2\alpha = r$, this yields $r^6 = \alpha^6\alpha_2^6 = \alpha^{12}$. Consequently, α^6 is a rational number $r_5 \in \{-r^3, r^3\}$. Adding all equalities in (4.19) we derive that $r_1 = \beta_1 + \beta_2 + \ldots + \beta_6 = 0$, since $\alpha \neq \alpha_2$. Thus, by (4.17), we must have

$$\alpha_i\beta_t + \frac{r_4}{r_5 r_3 \alpha_i \beta_t} = r_2.$$

This means that $\delta := \alpha_i\beta_t$ is a rational number or a quadratic number. Evidently, δ cannot be rational, since α_i and β_t are of distinct degrees 4 and 6, respectively. On the other hand, if δ were quadratic, then the product of δ and the quartic number $1/\alpha_i$ would be the sextic number β_t. However, the triplet $(2, 4, 6)$ is not product-feasible by [26, Theorem 1]. This completes the proof of Theorem 4.11. □

Chapter 5

Conclusions

We briefly oveview the research presented in the thesis.

- The complete description of compositum-feasible triplets (a, b, c) satisfying $a \leqslant b \leqslant c$, with $b \leqslant 9$, is obtained.
- The notion of an irreducible compositum-feasible triplet is introduced and a problem of finding all such triplets is proposed.
- The complete description of product-feasible triplets (a, b, c) satisfying $a \leqslant b \leqslant c$, with $b \leqslant 7$, is obtained.

Bibliography

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

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

[3] Cantor, D. G., and Isaacs, I. M. Problems and Solutions: Solutions of Advanced Problems: 6523. *Amer. Math. Monthly 95*, 6 (1988), 561–562.

[4] Dedekind, R. Supplement X. In *Dirichlet's Vorlesungen über Zahlentheorie*. Vieweg, 1871.

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

[6] Drungilas, P., and Dubickas, A. On degrees of three algebraic numbers with zero sum or unit product. *Colloq. Math. 143*, 2 (2016), 159–167.

[7] Drungilas, P., Dubickas, A., and Luca, F. On the degree of compositum of two number fields. *Math. Nachr. 286*, 2-3 (2013), 171–180.

[8] Drungilas, P., Dubickas, A., and Smyth, C. A degree problem for two algebraic numbers and their sum. *Publ. Mat. 56*, 2 (2012), 413–448.

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

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

[11] Dubickas, A., and Maciulevičius, L. The product of a quartic and a sextic number cannot be octic. *Open Math. 22*, 1 (2024), Paper No. 20230184, 10.

[12] Dubickas, A., and Smyth, C. J. On the Remak height, the Mahler measure and conjugate sets of algebraic numbers lying on two circles. *Proc. Edinb. Math. Soc. (2) 44*, 1 (2001), 1–17.

[13] Eisenstein, G. Beweis des reciprocitätssatzes für die cubischen reste in der theorie der aus den dritten wurzeln der einheit zusammengesetzten zahlen. In *Mathematische Werke. Band II.* Chelsea Publishing Co., New York, 1975.

[14] Euler, L. *Elements of algebra.* Springer-Verlag, New York, 1984. Translated from the German by John Hewlett, Reprint of the 1840 edition, With an introduction by C. Truesdell.

[15] Gauss, C. F. Theoria residuorum biquadraticorum. In *Werke. Band II.* Georg Olms Verlag, Hildesheim, 1973. Reprint of the 1863 original.

[16] Hecke, E. *Lectures on the theory of algebraic numbers*, vol. 77 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

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

[18] Isaacs, I. M. *Finite group theory*, vol. 92 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 2008.

[19] Jacobi, C. G. J. Ueber die complexen primzahlen, welche in der theorie der reste der 5ten, 8ten und 12ten potenzen zu betrachten sind. *Journal für die reine und angewandte Mathematik 19* (1839), 314–318.

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

[21] Kummer, E. E. Über die zerlegung der aus wurzeln der einheit gebildeten complexen zahlen in ihre primfaktoren. In *Collected papers*. Springer-Verlag, Berlin-New York, 1975. Volume I: Contributions to number theory, Edited and with an introduction by André Weil.

[22] Kummer, E. E. Zur theorie der complexen zahlen. In *Collected papers*. Springer-Verlag, Berlin-New York, 1975. Volume I: Contributions to number theory, Edited and with an introduction by André Weil.

[23] Lang, S. *Algebra*, third ed., vol. 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[24] Laurinčikas, A. Number theory in Lithuania. In *XXXVI Conference of Lithuanian Mathematical Society, Proceedings* (1996), Vilniaus universiteto leidykla, pp. 87–171.

[25] Laurinčikas, A. Algebrinė skaičių teorija. In *Matematika Lietuvoje po 1945 metų*. Vilnius: Matematikos ir informatikos institutas, 2006, pp. 72–80.

[26] Maciulevičius, L. On the degree of product of two algebraic numbers. *Mathematics 11*, 2131 (2023).

[27] Malle, G., and Matzat, B. H. *Inverse Galois theory*, second ed. Springer Monographs in Mathematics. Springer, Berlin, 2018.

[28] Marcus, D. A. *Number fields*, second ed. Universitext. Springer, Cham, 2018. With a foreword by Barry Mazur.

[29] Narkiewicz, W. a. a. *Elementary and analytic theory of algebraic numbers*, third ed. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004.

[30] Perlis, A. R. Roots appear in quanta. *Amer. Math. Monthly 111*, 1 (2004), 61–63.

[31] Robinson, R. M. Conjugate algebraic integers on a circle. *Math. Z. 110* (1969), 41–51.

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

[33] Stewart, I. *Galois theory*, fourth ed. CRC Press, Boca Raton, FL, 2015.

[34] Stillwell, J. *Mathematics and its history*, third ed. Undergraduate Texts in Mathematics. Springer, New York, 2010.

[35] van der Waerden, B. L. *Modern Algebra. Vol. I*, german ed. Frederick Ungar Publishing Co., New York, 1949. With revisions and additions by the author.

[36] Vinberg, E. B. *A course in algebra*, vol. 56 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2003. Translated from the 2001 Russian original by Alexander Retakh.

[37] Vinogradov, I. M. *Elements of number theory*. Dover Publications, Inc., New York, 1954. Translated by S. Kravetz.

[38] Virbalas, P. Degree of the product of two algebraic numbers one of which is of prime degree. *Mathematics 11*, 1485 (2023).

[39] Völklein, H. *Groups as Galois groups*, vol. 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1996. An introduction.

[40] Zariski, O., and Samuel, P. *Commutative algebra. Vol. 1*, vol. No. 28 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg-Berlin, 1975. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition.

Santrauka (Summary in Lithuanian)

Tyrimo objektas

Šioje disertacijoje nagrinėjami uždaviniai, susiję su algebrinių skaičių bei skaičių kūnų laipsniais. Prisiminkime šias sąvokas.

Kompleksinis skaičius α vadinamas *algebriniu*, jeigu jis yra kokio nors nenulinio polinomo su racionaliaisiais koeficientais šaknis. Tarp visų nenulinių polinomų su racionaliaisiais koeficientais ir turinčių šaknį α, egzistuoja vienintelis mažiausio laipsnio normuotas polinomas (t.y. su vyriausiuoju koeficientu 1). Toks polinomas vadinamas algebrinio skaičiaus α *minimaliuoju polinomu*, o jo laipsnis vadinamas algebrinio skaičiaus α *laipsniu* (žymima $\deg\alpha$). Pavyzdžiui, $\sqrt{2}$, $\sqrt{3}$ ir $\sqrt{2}+\sqrt{3}$ yra, atitinkamai, 2-ojo, vėlgi 2-ojo ir 4-ojo laipsnio algebriniai skaičiai su minimaliaisiais polinomais, atitinkamai, x^2-2, x^2-3 ir x^4-10x^2+1.

Gerai žinoma, jog visų algebrinių skaičių aibė įprastų aritmetinių operacijų atžvilgiu sudaro kūną, t.y. dviejų algebrinių skaičių suma, skirtumas, sandauga bei dalmuo (aišku, jei dalijama iš nenulinio skaičiaus) taip pat yra algebriniai skaičiai. Kyla natūralus klausimas: jei sudėsim (arba sudauginsim) du algebrinius skaičius α ir β, kurių laipsniai iš anksto žinomi, koks gali būti sumos $\alpha+\beta$ (arba, atitinkamai, sandaugos $\alpha\cdot\beta$) laipsnis? Nagrinėjant šį klausimą įvedamos specialios sąvokos. Natūraliųjų skaičių trejetas (a,b,c) vadinamas S-trejetu (atitinkamai, P-trejetu), jei egzistuoja tokie algebriniai skaičiai α ir β, kurių laipsniai, atitinkamai, a ir b, o sumos $\alpha+\beta$ (atitinkamai, sandaugos $\alpha\cdot\beta$) laipsnis lygus c. Pavyzdžiui, $(2,2,4)$ yra ir S-trejetas (galime imti $\alpha=\sqrt{2}$ ir $\beta=\sqrt{3}$), ir P-trejetas (galime imti $\alpha=\sqrt{2}$ ir $\beta=1+\sqrt{3}$). 2012 metais Drungilas, Dubickas ir Smitas (Smyth) [8] pasiūlė uždavinį rasti visus įmanomus S-trejetus ir P-trejetus.

Šie autoriai taip pat suformulavo analogišką sąvoką bei uždavinį skaičių kūnams. Prisiminkim, jog

- kiekvienas kompleksinių skaičių kūno pokūnis K kartu yra tiesinė erdvė virš racionaliųjų skaičių kūno $\mathbb{Q}$. Šios tiesinės erdvės dimensija vadinama kūno K *laipsniu* (žymima $[K:\mathbb{Q}]$). Jei $[K:\mathbb{Q}]<\infty$, tai K vadinamas *skaičių kūnu*.

- jeigu K ir L yra tam tikro vieno kūno M pokūniai (pvz., $\mathbb{C}$ pokūniai), tuomet K ir L *kompozitu* (žymima KL) vadinamas pats mažiausias kūnas, kuriam priklauso ir K, ir L (t.y. KL lygu visų kūno M pokūnių, savyje turinčių ir K, ir L, sankirtai).

Atitinkamai, natūraliųjų skaičių trejetas (a,b,c) vadinamas *C-trejetu*, jei egzistuoja tokie skaičių kūnai K ir L, kurių laipsniai atitinkamai lygūs a ir b, o kompozito KL laipsnis lygus c.

2012 - 2013 metais Drungilas, Dubickas, Luka (Luca) ir Smitas [8, 7] nustatė visus C-trejetus (a,b,c), kuriuose $a\leqslant b\leqslant c$ ir $b\leqslant 7$, bei nustatė visus įmanomus S-trejetus su tais pačiais apribojimais. Disertacijoje toliau tęsiame C, S ir P-trejetų tyrinėjimus.

Tikslai ir uždaviniai

Disertacijos tikslai ir uždaviniai yra šie:

- pratęsti ankstesnę C-trejetų klasifikaciją;

- įvesti naują *neredukuojamo C-trejeto* sąvoką ir pateikti pavyzdžių;

- suklasifikuoti P-trejetus (a,b,c), $a\leqslant b\leqslant c$, su nedidelėmis skaičių a, b ir c reikšmėmis.

Metodai

Disertacijoje naudojami metodai priklauso abstrakčiosios algebros sričiai. Daugiausia taikome baigtinių grupių teorijos, kūnų teorijos bei Galua teorijos technikas. Šalia įvairių klasikinių teoremų, dar naudojame tam tikrus specifinius, mažiau žinomus rezultatus apie adityvius bei multiplikatyvius sąryšius tarp polinomo šaknų. Šiuos pagalbinius rezultatus, taip pat kai kuriuos bazinius abstrakčiosios algebros faktus apžvelgiame disertacijos 2 skyriuje.

Aktualumas ir naujumas

Iš esmės visi disertacijoje pristatyti rezultatai yra nauji. Išimtis tik dėl 4.2 teoremos. Pirmą kartą teorema įrodyta straipsnyje [38]. Mes ją įrodėme nepriklausomai ir publikavome straipsnyje [26] beveik tuo pat metu. Manome padarę pažangą, nes mūsų įrodymas žymiai paprastesnis.

Nors algebriniai skaičiai ir skaičių kūnai yra klasikiniai objektai, tačiau jie toliau aktyviai tyrinėjami ir šiuolaikinėje matematikoje. Jau nekalbant apie algebrinę skaičių teoriją, algebriniai skaičiai bei skaičių kūnai dažnai sutinkami ir kitose srityse, pvz., spendžiant Diofanto lygtis, Diofanto aproksimacijų teorijoje, algoritminėje skaičių teorijoje ir t.t. Tikimės, kad mūsų rezultatai bus naudingi dirbantiems šiose srityse. Be to, algebrinių skaičių tyrinėjimai yra viena iš Lietuvos skaičių teorijos mokyklos krypčių[1], taigi ši disertacija pratęsia Lietuvos matematikų tradicijas.

Tyrimų istorija ir rezultatai

Literatūroje iki 2012 metų galime rasti tik keletą rezultatų, tiesiogiai susijusių su C, S ir P-trejetų klasifikacijos uždaviniais. Pavyzdžiui, straipsniuose [17, 2, 9, 10] nagrinėjama, kokioms sąlygos galiojant algebriniai skaičiai α ir β tenkins lygybę $\deg(\alpha+\beta)=\deg\alpha\cdot\deg\beta$. Viena paprasta sąlyga štai tokia:

1 teiginys ([17])**.** *Tarkime α ir β yra algebriniai skaičiai, kurių laipsniai, atitinkamai, a ir b. Jeigu* $\operatorname{dbd}(a,b)=1$*, tuomet* $\deg(\alpha+\beta)=ab$*.*

Kitaip tariant, jeigu (a,b,c) yra S-trejetas ir $\operatorname{dbd}(a,b)=1$, tuomet būtinai $c=ab$.

Sistemingai nagrinėti C, S ir P-trejetų klasifikacijos uždavinius pradėjo Drungilas, Dubickas ir Smitas [8] 2012 metais. Šie trys uždaviniai susiję štai tokiu būdu:

2 teiginys ([8, Proposition 1], [6, Theorem 1.1])**.** *Kiekvienas C-trejetas kartu yra ir S-trejetas, o kiekvienas S-trejetas - kartu ir P-trejetas.*

[1] Žr. apžvalgas [24, 25] apie skaičių teoriją Lietuvoje.

Kitaip tariant, jeigu visų įmanomų C, S ir P-trejetų aibes pažymėsim, atitinkamai, $\mathcal{C}$, $\mathcal{S}$ ir $\mathcal{P}$, tuomet

$$\mathcal{C} \subset \mathcal{S} \subset \mathcal{P}. \tag{5.1}$$

Iš čia išplaukia: jeigu (a,b,c) nėra P-trejetas, tuomet tai negali būti nei C-trejetas, nei S-trejetas. Be to, abu (5.1) įdėjimai griežti (t.y. $\subsetneq$). Iš tikro, pastebėkim, jog

- $(n,n,1)$ yra S-trejetas su bet kokiu $n \in \mathbb{N}$ (pvz., galime imti $\alpha = \sqrt[n]{2}$ ir $\beta = -\alpha$), tačiau tai nėra C-trejetas, jei $n > 1$. Taigi $\mathcal{C} \subsetneq \mathcal{S}$.
- $(2,2,3)$ yra P-trejetas (pvz., galime imti $\alpha = e^{\frac{2\pi i}{3}}$ ir $\beta = \sqrt[3]{2}$), tačiau tai nėra S-trejetas pagal 1 teiginį. Taigi $\mathcal{S} \subsetneq \mathcal{P}$.

Aišku, jeigu (a,b,c) yra S-trejetas (arba P-trejetas), tuomet, perstatę skaičius a, b ir c bet kokiu būdu, vėl gausim S-trejetą (atitinkamai, P-trejetą). Kita vertus, jeigu (a,b,c) yra C-trejetas, tuomet būtinai $a \leqslant c$ ir $b \leqslant c$, be to, perstatę skaičius a ir b, vėl gausim C-trejetą. Taigi, ieškant C, S arba P-trejetų, nemažindami bendrumo galime apsiriboti tik tokiais trejetais (a,b,c), kuriuose $a \leqslant b \leqslant c$.

Nesunku įsitikinti: jeigu (a,b,c) yra C, S arba P-trejetas, tuomet

$$c \leqslant ab. \tag{5.2}$$

Negana to, jeigu (a,b,c) yra C-trejetas, tai, pagal *bokštų taisyklę* [2] kūnų plėtiniams,

$$a|c \text{ ir } b|c. \tag{5.3}$$

Visgi, (5.2) ir (5.3) sąlygos bendru atveju nėra pakankamos, kad (a,b,c) būtų C, S arba P-trejetas (žr., pavyzdžiui, 3.1 teoremą). Nustatyti, ar duotas trejetas yra kurio nors iš šių tipų - tai gali būti sudėtingas uždavinys.

Straipsniuose [8, 7] nustatyti visi S-trejetai (a,b,c), tenkinantys sąlygas $a \leqslant b \leqslant c$ ir $b \leqslant 7$, bei nustatyti visi C-trejetai su tokiais pat apribojimais. Disertacijos 3 skyriuje pratęsiame C-trejetų klasifikaciją iki atvejo, kai $b \leqslant 9$, t.y., įrodome štai tokį tvirtinimą:

[2] Žr. 2.1 disertacijos poskyrį.

3.1 teorema. *Tarkime* $a, c \in \mathbb{N}$.

1. *Trejetas* $(a, 8, c)$, $a \leqslant 8 \leqslant c$, *yra C-trejetas tada ir tik tada, kai* $c \leqslant 8a$, $a|c$ *ir* $b|c$, *išskyrus vieną atvejį* $(8, 8, 40)$ *(tai nėra P-trejetas).*

2. *Trejetas* $(a, 9, c)$, $a \leqslant 9 \leqslant c$, *yra C-trejetas tada ir tik tada, kai* $c \leqslant 9a$, $a|c$ *ir* $b|c$, *išskyrus du atvejus* $(9, 9, 45)$ *ir* $(9, 9, 63)$ *(tai nėra P-trejetai).*

Šalia dalinės trejetų klasifikacijos, straipsniuose [8, 7] taip pat gauta rezultatų apie tam tikrų specialių pavidalų trejetus, pavyzdžiui,

3 teiginys ([8, Proposition 29])**.** *Tarkime* $n \in \mathbb{N}$ *ir* $n \geqslant 2$.

1. *Trejetai* (n, n, n) *ir* $(n, n, n(n-1))$ *yra C-trejetai.*

2. *Trejetas* $(n, n, n(n-1)/2)$ *yra S-trejetas. Jei skaičius* n *lyginis, tuomet tai nėra C-trejetas.*

3. *Trejetas* $(n, n, 2n)$ *yra C-trejetas.*

Disertacijos 3 skyriuje įrodome naujų rezultatų apie trejetus, kurių pavidalas (n, n, nk).

3.3 teorema. *Tarkime* $n \in \mathbb{N}$ *ir* $n \geqslant 4$. *Tuomet* $(n, n, n(n-2))$ *yra C-trejetas, jeigu* n *- lyginis, ir nėra P-trejetas, jeigu* n *- nelyginis.*

Iš čia būtent ir išplaukia, jog išskirtinis 3.1 teoremos trejetas $(9, 9, 63)$ nėra P-trejetas, todėl nei C, nei S-trejetas. Tuo tarpu $(8, 8, 40)$ bei $(9, 9, 45)$ yra štai tokio mūsų rezultato atskiri atvejai:

3.4 teorema. *Tarkime* $n \in \mathbb{N}$ *ir* $n \geqslant 8$, *o* p *- pirminis skaičius, tenkinantis sąlygą* $n/2 < p < n-2$. *Tuomet* (n, n, np) *nėra P-trejetas.*

Taigi, naudodamiesi 3.3 ir 3.4 teoremomis, tarp trejetų (n, n, nk), kur $n \geqslant 5$ ir $n/2 < k \leqslant n-2$, galime parinkti tokių, kurie nėra C-trejetai. Tuo tarpu kitas mūsų rezultatas rodo, jog tarp trejetų (n, n, nk), kur $n \geqslant 5$ ir $2 < k \leqslant n/2$, irgi tikrai ne visi yra C-trejetai.

3.11 teorema. *Tarkime* p, q *ir* w *yra pirminiai skaičiai, tenkinantys sąlygas* $2 < w < q < p$, $p = 2q + w$ *ir* $w \nmid q - 1$. *Tuomet* (p, p, pq) *nėra P-trejetas.*

Pavyzdžiui, $(13,13,13\cdot 5)$, $(19,19,19\cdot 7)$, $(29,29,29\cdot 11)$, $(31,31,31\cdot 13)$ nėra P-trejetai, todėl kartu nėra ir C-trejetai.

Straipsnyje [8] gauta keletas įdomių rezultatų, susijusių su taip vadinama *rodikline trikampio nelygybe*. Tarkime $n\in\mathbb{N}$ ir p yra bet koks pirminis skaičius. Simboliu $\mathrm{ord}_p(n)$ pažymėkim, su kokiu laipsnio rodikliu p įeina į skaičiaus n kanoninį išskaidymą (jei $p\nmid n$, tuomet susitarkim, jog $\mathrm{ord}_p(n)=0$). Sakysim, jog trejetas $(a,b,c)\in\mathbb{N}^3$ tenkina *rodiklinę trikampio nelygybę pirminio skaičiaus p atžvilgiu*, jeigu

$$\begin{gathered}\mathrm{ord}_p(a)\leqslant \mathrm{ord}_p(b)+\mathrm{ord}_p(c),\quad \mathrm{ord}_p(b)\leqslant \mathrm{ord}_p(a)+\mathrm{ord}_p(c)\quad \text{ir}\\ \mathrm{ord}_p(c)\leqslant \mathrm{ord}_p(a)+\mathrm{ord}_p(b).\end{gathered}\tag{5.4}$$

4 teiginys ([8, Theorem 6]). *Jeigu trejetas $(a,b,c)\in\mathbb{N}^3$ tenkina rodiklinę trikampio nelygybę kiekvieno pirminio skaičiaus atžvilgiu, tuomet (a,b,c) yra S-trejetas (todėl kartu ir P-trejetas).*

Pastebėkim, jog analogiškas teiginys C-trejetams negalioja. Pavyzdžiui, trejetas $(a,b,c)=(6,10,15)$ tenkina (5.4) sąlygas su kiekvienu pirminiu skaičiumi p, tačiau tai nėra C-trejetas, nes neišpildyta būtina sąlyga (5.3). Tačiau, (5.4) pakeitus kiek stipresne sąlyga, gaunamas įdomus tvirtinimas ir C-trejetams:

5 teiginys ([8, Theorem 7]). *Jei su kiekvienu pirminiu skaičiumi p trejetas $(a,b,c)\in\mathbb{N}^3$ tenkina sąlygą*

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

tuomet (a,b,c) yra C-trejetas.

Pastarasis teiginys išplaukia iš štai tokio bendresnio tvirtinimo:

6 teiginys ([8, Corollary 27]). *Tarkime p - pirminis skaičius, o u, v ir w - natūralieji skaičiai, tenkinantys sąlygą $\max\{u,v\}\leqslant q\leqslant u+v$. Jeigu (a,b,c) yra C-trejetas, tuomet (ap^u,bp^v,cp^w) taip pat bus C-trejetas.*

Savo ruožtu 6 teiginys yra štai tokios hipotezės, kuri iškelta straipsnyje [8], dalinis atvejis:

7 hipotezė ([8, Conjecture 6]). *Jeigu (a,b,c) ir (a',b',c') yra C-trejetai (atitinkamai, S-trejetai, P-trejetai), tuomet (aa',bb',cc') taip pat yra C-trejetas (atitinkamai, S-trejetas, P-trejetas).*

Kol kas netgi nėra žinoma, ar hipotezė C-trejetams bendru atveju yra teisinga. (Jeigu būtų teisinga hipotezė S-trejetams arba P-trejetams, tuomet, remiantis 2 teiginiu, būtų teisinga ir C-trejetams.) Drungilas ir Dubickas [6] parodė, kad hipotezė C-trejetams teisinga, jei atsakymas į taip vadinamą *atvirkštinį Galua teorijos uždavinį* yra teigiamas. Primename, jog šis uždavinys klausia, ar kiekvienai baigtinei grupei G egzistuoja toks Galua plėtinys $K/\mathbb{Q}$, kurio Galua grupė būtų kaip tik G. Atsakymas iki šiol nežinomas.

8 teiginys ([6, Theorem 1.3])**.** *Jei kiekviena baigtinė grupė yra kokio nors Galua plėtinio $K/\mathbb{Q}$ Galua grupė, tuomet 7 hipotezė C-trejetams teisinga.*

Kitaip tariant, jeigu atsakymas į atvirkštinį Galua teorijos uždavinį teigiamas, tai visų C-trejetų aibė $\mathcal{C}$ sudaro pusgrupę daugybos, apibrėžtos lygybe

$$(a,b,c)\cdot(a',b',c') := (aa',bb',cc'),$$

atžvilgiu. Aišku, C-trejetas $(1,1,1)$ būtų neutralus šios pusgrupės elementas. Bet kokiu atveju - sudaro pusgrupę ar nesudaro - natūralu klausti, kurių aibės $\mathcal{C}$ elementų neįmanoma išskaidyti į kitų dviejų jos elementų, nelygių $(1,1,1)$, sandaugą. Šiam klausimui nagrinėti įvedame naują sąvoką:

Apibrėžimas. C-trejetą (A,B,C) vadinsime *neredukuojamu*, jeigu jo neįmanoma užrašyti pavidalu

$$(A,B,C) = (a,b,c)\cdot(a',b',c'),$$

kur $(a,b,c),(a',b',c') \in \mathcal{C}\setminus\{(1,1,1)\}$.

Paprasčiausi neredukuojamų trejetų pavyzdžiai - tai C-trejetai, kurių pavidalas $(1,p,p)$ arba (p,p,pd), kur p - pirminis ir $1 \leqslant d < p$. Disertacijos 3 skyriaus pabaigoje pateikiame vieną sudėtingesnį pavyzdį:

3.16 teorema. *Tarkime $n\in\mathbb{N}$, $n\geqslant 2$. Tuomet C-trejetas $(n,n,n(n-1))$ yra neredukuojamas.*[3]

[3]Primename, jog, pagal 3 teiginį, tai iš tiesų yra C-trejetas su bet kokiu natūraliuoju $n\geqslant 2$.

Galiausiai 3 skyriuje suformuluojam uždavinį *nustatyti visus neredukuojamus C-trejetus.*

Darbuose [8, 7] beveik neskiriama atskiro dėmesio P-trejetams; išnagrinėti tik keli nesudėtingi atvejai, pavyzdžiui,

9 teiginys ([8, Theorem 8])**.** *Tarkime* $t \in \mathbb{N}$. *Trejetas* $(2,t,t)$ *yra P-trejetas tada ir tik tada, kai* $2|t$ *arba* $3|t$.

Kyla motyvacija panagrinėti P-trejetų klasifikacijos uždavinį nuodugniau. Tam skiriame 4 disertacijos skyrių. Jame nustatome visus P-trejetus (a,b,c), tenkinančius sąlygas $a \leqslant b \leqslant c$ ir $b \leqslant 7$:

4.1 teorema. *Visi P-trejetai* (a,b,c)*, tenkinantys sąlygas* $a \leqslant b \leqslant c$ *ir* $b \leqslant 7$*, pateikti 5.1 lentelėje.*

$b\backslash a$	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, 12, 24	30	6, **8**, 9, 12, 15, 18, 24, 30, 36	
7	7	14	21	28	35	**7**, **14**, **21**, 42	7, 14, 21, 28, 42, 49

5.1 lentelė Visi P-trejetai (a,b,c), tenkinantys sąlygas $a \leqslant b \leqslant c$ ir $b \leqslant 7$

Lentelėje yra devyni P-trejetai su paryškintomis skaičiaus c reikšmėmis:

$$\begin{gathered}(2,3,3),(3,4,6),(3,6,9),(6,6,8),\\(4,5,5),(4,5,10),(6,7,7),(6,7,14),(6,7,21).\end{gathered} \tag{5.5}$$

Remiantis rezultatais iš [8, 7], tai nėra S-trejetai. Atkreipkim dėmesį, jog $(2,3,3)$ yra P-trejetas pagal 9 teiginį, vadinasi

$$\begin{aligned}(3,4,6) &= (3,2,3)\cdot(1,2,2),\\(3,6,9) &= (3,2,3)\cdot(1,3,3),\\(6,6,8) &= (3,3,2)\cdot(2,2,4)\end{aligned}$$

yra P-trejetai pagal 1.13 teiginį. Tuo tarpu likusieji (5.5) trejetai yra štai tokio bendresnio tvirtinimo, kurį taip pat įrodome 4 skyriuje, atskiri atvejai:

4.2 teorema. *Tarkime p - pirminis skaičius ir $d|p-1$. Tuomet $(p-1,p,pd)$ yra P-trejetas.*

Taip pat įrodome tam tikrą 9 teiginio pratęsimą:

4.3 teorema. *Tarkime $t\in\mathbb{N}$, $p>2$ - pirminis skaičius ir $t\geqslant p$. Tuomet (p,t,t) yra P-trejetas tada ir tik tada, kai $p|t$.*

Straipsnyje [8] atskirai įrodoma, jog $(6,6,10)$ nėra S-trejetas (žr. [8, Theorem 38]). Apibendrindami šio įrodymo idėjas, gauname štai tokį rezultatą:

4.4 teorema. *Tarkime $p>3$ yra pirminis skaičius. Tuomet $(p+1,p+1,2p)$ nėra P-trejetas.*

Galiausiai disertacijos 4 skyriuje įrodome tokį tvirtinimą:

4.5 teorema. *Tarkime $k\in\mathbb{N}$. Trejetas $(n,(n-1)k,nk)$, kur $n\geqslant 2$, yra P-trejetas tada ir tik tada, kai skaičius n - pirminis.*

Atskiru atveju, imdami $(n,k)=(4,2)$, gauname, jog $(4,6,8)$ nėra P-trejetas. Paskutiniajame 4 skyriaus poskyryje pateikiame dar vieną įrodymą, jog tai iš tiesų nėra P-trejetas.

Aprobacija

Disertacijos rezultatai buvo pristatyti 32 tarptautinėje konferencijoje *Journées Arithmétiques* (JA 2023, liepos 3 - 7, 2023, Nansi, Prancūzija), tarptautinėje mokslinėje konferencijoje skirtoje prof. dr. Hermano Minkovskio (Hermann Minkowski) 160-ies metų jubiliejui (birželio 20 - 22, 2024, Kaunas), 64 Lietuvos matematikų draugijos konferencijoje (LMD 2023, birželio 21 - 22, 2023, Vilnius), taip pat Vilniaus universiteto skaičių teorijos seminaruose.

Konferencijų tezės:

1. Maciulevičius L. Some degree problems in number fields. Abstracts of JA 2023, July 3 - 7, 2023, Nancy, France, pp. 44.

2. Maciulevičius L. Apie skaičių kūnų kompozito bei algebrinių skaičių sandaugos laipsnius. Lietuvos matematikų draugijos LXIV konferencijos santraukos. Vilniaus universiteto leidykla, 2023, pp. 11.

Publikacijos

Disertacijos rezultatai paskelbti šiuose straipsniuose:

1. Drungilas P., and Maciulevičius L. A degree problem for the compositum of two number fields. *Lith. Math. J. 59*, 1 (2019), 39 - 47.

2. Maciulevičius L. On the degree of product of two algebraic numbers. *Mathematics 11*, 2131 (2023).

3. Dubickas A., and Maciulevičius L. The product of a quartic and a sextic number cannot be octic. *Open Math. 22*, 1 (2024), Paper No. 20230184, 10.

Išvados

Pagrindiniai disertacijos rezultatai yra šie:

- nustatyti visi C-trejetai (a,b,c), kuriuose $a \leqslant b \leqslant c$ ir $b \in \{8,9\}$;
- įvesta neredukuojamo C-trejeto sąvoka, pateikta netrivialių pavyzdžių ir iškeltas uždavinys rasti visus tokius trejetus;
- nustatyti visi P-trejetai (a,b,c), kuriuose $a \leqslant b \leqslant c$ ir $b \leqslant 7$.

Trumpos žinios apie autorių

Gimimo data ir vieta
1995 m. gruodžio 17 d., Prienai, Lietuva.

Išsilavinimas
2014 m. Prienų „Žiburio“ gimnazija (baigta su pagyrimu).
2018 m. Vilniaus universitetas, Matematika ir matematikos taikymai, bakalauro laipsnis (*Cum Laude*).
2020 m. Vilniaus universitetas, Matematika, magistro laipsnis (*Magna cum laude*).

Darbo patirtis
Vilniaus universitetas, Matematikos ir informatikos fakultetas:
2016 - 2017 m. ir 2018 - 2020 m. laborantas,
nuo 2020 m. jaunesnysis asistentas.

NOTES

NOTES

NOTES

Vilniaus universiteto leidykla
Saulėtekio al. 9, III rūmai, LT-10222 Vilnius
El. p. info@leidykla.vu.lt, www.leidykla.vu.lt
Tiražas 20 egz.