Algebraic numbers as vectors

The Jury of the project: I. Vorobyov, S. Dorichenko, A. Kanel–Belov, A. Kanunnikov, B. Frenkin, A. Zhilina

Introduction

In geometry, we are used to add *vectors* anf multiply them by *scalars* (numbers). This geometrical language often occurs to be useful in quite non-geometrical situations. In this project the role of vectors is played by *algebraic numbers*, that is, the roots of polynomials with rational coefficients. Rational numbers then are in the role of scalars.

We call complex numbers $x_1, \ldots, x_n$ *linearly independent* over the field of rational numbers $\mathbb{Q}$ if the equation $a_1x_1 + \ldots + a_nx_n = 0$ with $a_1, \ldots, a_n \in \mathbb{Q}$ holds only for $a_1 = \ldots = a_n = 0$ (cf. non-complanar vectors at Fig. 1). Consideration of algebraic numbers as vectors occurs to be very natural and productive in general because it enables us to apply geometrical ideas in algebraic problems.

$$a_1\overrightarrow{v_1} + a_2\overrightarrow{v_2} + a_3\overrightarrow{v_3} = 0 \Rightarrow a_1 = a_2 = a_3 = 0$$

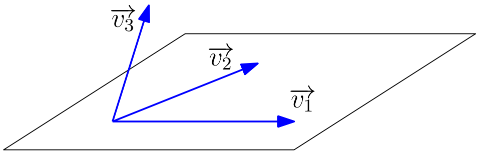


Fig. 1

The project is arranged as follows. To warm up, we start with some olympiad problems on radicals. Some of them are solvable by usual school methods, and the others require further background, namely some information about algebraic numbers and fields, presented in the second section. You will learn to apply some suitable language and tools for a wide scope of problems. This is the preliminary part of the project.

The further section will be presented at the conference for the participants having chosen this project. In the third section we formulate the main theorem and suggest to prove it according to the outline based on the preceding information. Finally we present a research problem which develops and generalizes the main theorem. For participation in the project it is not required to solve any definite number of problems from the preliminary part.

The necessary background amounts to basic facts about complex numbers and polynomials. The most relevant operations are rootsquaring of complex numbers and division of polynomials with remainder. The problems on square radicals will be available for you even if you have little knowledge of complex numbers.

The foundations of the theory of algebraic numbers were laid by Karl Gauss's treatise "Disquisitiones arithmeticae" (1801) which has played the great role in number theory. Together with Lagrange's works, it prepared the discoveries of Évarist Galois who established the criterion for solvability of equations in radicals (1830) and laid the foundations of branches of modern algebra, such as group theory and field theory. Galois theory and theory of algebraic number fields were developed and systematized in the second half of XIX and the beginning of XX century due to Kummer, Kronecker, Hilbert e.a.

1. Warmup problems

If some of these problems create difficulties for you then you may return to them after Section 2.

1.1. Prove irrationality of the following numbers: **a)** $\sqrt[3]{1001}$; **b)** $\sqrt{2}+\sqrt{3}+\sqrt{6}$; **c)** $\sqrt{2}+\sqrt[3]{3}$; **d)*** $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}+\sqrt{11}$; **e)*** $\sqrt[5]{3}-\sqrt[5]{2}$; **f)**** $\sqrt{\dfrac{3}{5}} + \dfrac{\sqrt[17]{2020!}}{2020} + \sqrt[5^5]{7^{7^{7^7}}}$.

If you have no idea how to deal with the last markedly weird number then the first hint is as follows: it is worth while to prove a stronger assertion regarding linear independence. For instance, in part **b)** it would be as follows:

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0 \text{ where } a, b, c, d \in \mathbb{Q} \implies a = b = c = d = 0.$$

1.2. Find the polynomial of minimum degree with rational coefficients and the following root: **a)** $\sqrt[3]{4}$; **b)** $\sqrt{2}+\sqrt{3}$; **c)** $\sqrt[3]{2}+\sqrt[3]{4}$; **d)*** $\sqrt[8]{8}+\sqrt[9]{9}$; **e)*** $\sqrt{6}+\sqrt{10}+\sqrt{15}$;
f) $\sqrt[3]{1+\sqrt{2}}+\sqrt[3]{1-\sqrt{2}}$; **g)** $\sqrt[3]{7+5\sqrt{2}}+\sqrt[3]{7-5\sqrt{2}}$ (similarity in appearance is misleading!);
h) $\cos\frac{2\pi}{5}$; **i)** $\cos\frac{2\pi}{9}$; **j)*** $\cos\frac{2\pi}{97}$; **k)**** $\cos\frac{2\pi}{n}$ for any $n\in\mathbb{N}$.

Present the polynomial found even if you aren't sure in minimality of its degree. In all parts except **c)**, **d)**, **j)**, **k** write down the polynomial in standard form. Surprisingly, in parts **j)**, **k)** it is worth while to pass to the complex plane.

1.3. Which numbers of the form $\dfrac{a+bi}{a-bi}$ with $a,b\in\mathbb{Z}$ are roots of unity?

Below are some problems on square irrationalities. They contain an important idea... (let us avoid spoilers).

1.4. Are there any rational numbers a,b,c,d such that $(a+b\sqrt{2})^2+(c+d\sqrt{2})^2=7+5\sqrt{2}$?

1.5. Determine first 1000 decimal places of $(6+\sqrt{37})^{1001}$.

1.6. Prove that the product of all 2^{100} expressions of the form

$$\pm\sqrt{1}\pm\sqrt{2}\pm\ldots\pm\sqrt{99}\pm\sqrt{100}$$

(for all combinations of signs) is **a)** an integer; **b)** a squared integer.

2. A bit of theory: fields and algebraic numbers

Linear independence of 1 and $\sqrt{2}$ (over $\mathbb{Q}$) is nothing but irrationality of $\sqrt{2}$ which has been known already by ancient Greeks. Let us increase the number of radicals.

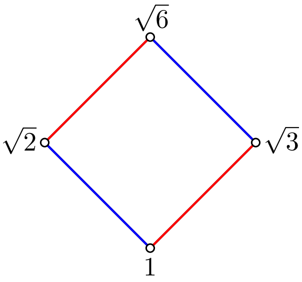


Fig. 2a

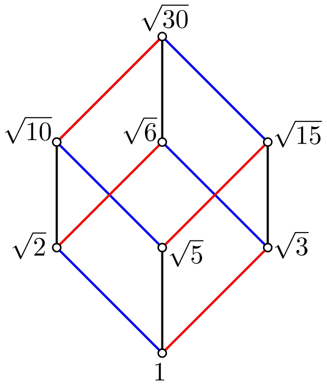


Fig. 2b

2.1. Fill in the gaps in the following argument.

Let us prove that $1,\sqrt{2},\sqrt{3},\sqrt{6}$ are linearly independent over $\mathbb{Q}$. Suppose

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=0 \text{ with } a,b,c,d\in\mathbb{Q}.$$

Separate the radical $\sqrt{3}$:

$$a+b\sqrt{2}+(c+d\sqrt{2})\sqrt{3}=0.$$

If $c+d\sqrt{2}=0$ then ____

On the other hand, if $c+d\sqrt{2}\neq 0$ then

$$\sqrt{3}=-\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=A+B\sqrt{2} \text{ with } A=\underline{\qquad\qquad}\in\mathbb{Q},\ B=\underline{\qquad\qquad}\in\mathbb{Q}.$$

There are various ways to complete the proof.

The above example demonstrates certain ideas. Linear independence of the numbers from Fig. 2a has been reduced to the fact that $\sqrt{3}$ is «alien» for the set

$$\mathbb{Q}+\mathbb{Q}\sqrt{2}=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$$

(more formally, $\sqrt{3}$ doesn't belong to it) just as $\sqrt{2}$ is alien for $\mathbb{Q}$. And it was of importance that in the set $\mathbb{Q}+\mathbb{Q}\sqrt{2}$ we are able not only to add, subtract, multiply but moreover divide (not by 0) as in $\mathbb{Q}$ by *removing the irrationality from the denominator.*

A *number field* is a set of numbers which contains 0 and 1 and is closed under four arithmetic operations. We will omit the word „number" [1]. Thus K is a field if $0, 1 \in K$ and for any $a, b \in K$ we have $a \pm b, ab \in K$ and $a/b \in K$ for $b \neq 0$. Clearly $\mathbb{Q}$ is a field and moreover a „minimal" one: any (number) field contains it. If $K \subseteq L$ are two fields then K is called a *subfield* of L.

We say that a system of numbers[2] $x_1, \ldots, x_n \in \mathbb{C}$ is *linearly independent over* K if the equation $a_1x_1 + \ldots + a_nx_n = 0$ with $a_1, \ldots, a_n \in K$ is satisfied only by $a_1 = \ldots = a_n = 0$. For instance, numbers 1 and $\sqrt{2}$ are linearly independent over $\mathbb{Q}$ but linearly dependent over $\mathbb{R}$.

2.2. Elementary properties of linear dependence. Let K be a field. Prove the following:

a) a system containing 0 or two numbers proportional over K is linearly dependent over K;

b) a subsystem of a linearly independent system is linearly independent (over the same field);

c) the system $1, x$ is linearly independent over K iff $x \notin K$;

d) the factors $a_1, \ldots, a_n \in K$ in the expression $a_1x_1 + \ldots + a_nx_n$ are uniquely determined iff the system $x_1, \ldots, x_n$ is linearly independent over K.

To adjoin the numbers $\alpha_1, \ldots, \alpha_n$ *to the field* K means to consider the least field (by inclusion) that contains K and these numbers. Notation: $K(\alpha_1, \ldots, \alpha_n)$.

2.3. Adjoining a square radical. Let K be a subfield in $\mathbb{R}$, $0 < d \in K$ and $\sqrt{d} \notin K$ (for instance, $K = \mathbb{Q}$ and $d = 2$). Prove that

$$K(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in K\},$$

where $a, b \in K$ in $a + b\sqrt{d}$ are determined uniquely.

2.4. Prove that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

2.5. Remove the irrationality from the denominator: $\dfrac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}}$.

2.6. a) Prove that the numbers at the vertices of the cube at Fig. 2b are linearly independent over $\mathbb{Q}$.

b)* Add $\sqrt{7}$ to the above set of numbers, try to draw a hypercube and prove the assertion similar to part **a)**.

Perhaps it is time to formulate a general theorem on radicals of primes and to prove it by induction. In particular it would imply the solution of Problem **1.1d)**.

What is the sense of linear independence over K for powers $1, \alpha, \alpha^2, \ldots, \alpha^n$ of a certain number α? It is the existence of numbers $c_0, c_1, \ldots, c_n \in K$ such that at least one of them is nonzero and

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_n\alpha^n = 0.$$

In other words, α is a root of a nonzero polynimial with coefficients from K. Such α is called *algebraic over* K. Among these polynomials there is a unique one having the lowest degree and leading coefficient 1 (why?). It is called *the minimal polynomial* of α over K and is often denoted $\mu_\alpha^K(x)$. For instance, $\mu_i^{\mathbb{R}}(x) = x^2 + 1$, $\mu_i^{\mathbb{C}}(x) = x - i$. The degree $\deg \mu_\alpha^K(x)$ of this polynomial also is called *the degree* of α over K and is denoted $\deg_K(\alpha)$. The roots of $\mu_\alpha^K(x)$ are called *conjugate* with α over K.

For $K = \mathbb{Q}$ we simply say that such α are algebraic numbers.

2.7. Let a number $\alpha \in \mathbb{C}$ be algebraic over a field $K \subseteq \mathbb{C}$. Prove the following:

a) $\deg_K(\alpha)$ is the least $n \in \mathbb{N}$ such that $1, \alpha, \ldots, \alpha^n$ are linearly dependent over K;

b) the polynomial $\mu_\alpha^K(x)$ is irreducible over K (i.e., is not a product of polynomials from $K[x]$ of strictly lower degrees);

c) every polynomial from $K[x]$ with the root α is a multiple of $\mu_\alpha^K(x)$;

d) a polynomial with the root α and the leading coefficient 1, irreducible over K equals $\mu_\alpha^K(x)$.

The following criterion for irreducibility of a polynomial over $\mathbb{Q}$ may be used without proof.

[1] There exist other fields as well, for instance fields of residues, fields of rational functions e.a.

[2] A non-ordered tuple of numbers, perhaps with some repetitions.

Theorem 1 (Eisenstein's criterion)**.** *Let the coefficients of a polynomial* $a_nx^n + \ldots + a_1x + a_0 \in \mathbb{Z}[x]$ *satisfy the following conditions for some prime* p*:*

- $p \nmid a_n$,
- $p \mid a_{n-1}, \ldots, p \mid a_0$,
- $p^2 \nmid a_0$.

Then this polynomial is irreducible over $\mathbb{Q}$*.*

2.8. a) Complete the solution of Problem **1.1e)**. *Hint.* Suppose $\sqrt[5]{3} - \sqrt[5]{2} = a \in \mathbb{Q}$, then $\sqrt[5]{3} = \sqrt[5]{2} + a$. Determine the minimal polynomials for the numbers in the left and right sides.

b) Solve in positive integers: $\sqrt[5]{m} + \sqrt[5]{n} = 2020$.

Let us now generalize Problem 2.3.

Theorem 2 (on disposal of the irrationality from the denominator)**.** *Let a number* α *be algebraic over a field* K *and have the degree* n*. Then any number from* $K(\alpha)$ *is uniquely expressed in the form*

$$c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}, \text{ where } c_0, c_1, \ldots, c_{n-1} \in K.$$

2.9. a) Remove the irrationality from the denominator of $\dfrac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 3}$.
Hint. The usual multiplication by the conjugate doesn't work in this case. Find polynomials $u(x), v(x) \in \mathbb{Q}[x]$ such that $u(x)(x^2 + x + 3) + v(x)(x^3 - 2) = 1$. For this, use either Euclidean algorithm in converse succession or the method of undetermined coefficients.

b) Prove Theorem 2.

By the fundamental theorem of algebra, every polynomial over $\mathbb{C}$ of degree $n > 0$ has n roots counted with multiplicities. By the following theorem, the polynomial $\mu_\alpha^K(x)$ has no multiple roots and thus *every algebraic number of degree* n *has just* n *conjugates (including itself).*

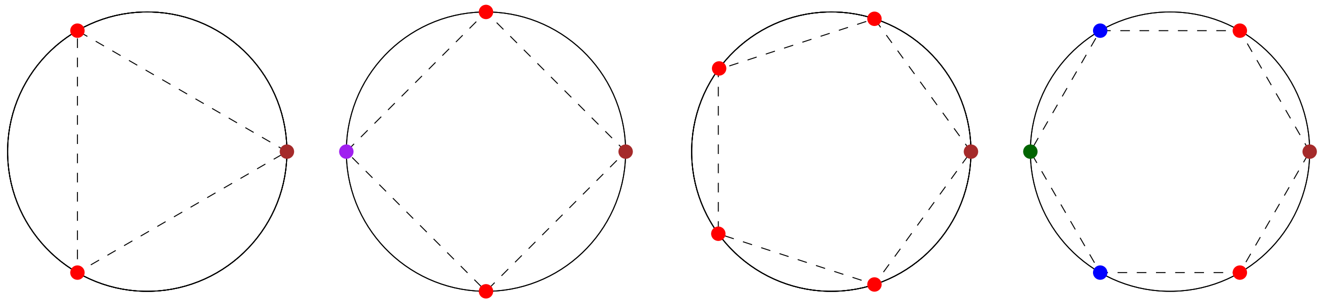
Theorem 3. *A polynomial irreducible over some subfield of* $\mathbb{C}$ *has no multiple complex roots.*

2.10. Decompose the binomial $x^4 - 2$ into irreducible ones and divide its roots into classes of conjugates over each of the fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$.

Now we have to emphasize on the roots of unity. As is well-known, the complex roots of $x^n = 1$ are of the form

$$1, \varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{n-1}, \text{ where } \varepsilon_n = \cos\tfrac{2\pi}{n} + i\sin\tfrac{2\pi}{n}$$

(a partial case of de Moivre's formula). Divide these into the classes of conjugates over $\mathbb{Q}$. For this, decompose the binomial $x^n - 1$ into irreducible factors over $\mathbb{Q}$: then the roots of each factor form a class of conjugate algebraic numbers. Let us consider examples for little n. At Fig. 3, each irreducible factor and its roots are marked with a specific color.



$x^3 - 1 = (x-1)(x^2+x+1)$ $x^4 - 1 = (x-1)(x+1)(x^2+1)$ $x^5 - 1 = (x-1)\times$ $\times(x^4+x^3+x^2+x+1)$ $x^6 - 1 = (x-1)(x+1)\times$ $\times(x^2+x+1)(x^2-x+1)$

Fig. 3

Only irreducibility of $x^4 + x^3 + x^2 + x + 1$ requires explanation. Below is a more general fact.

2.11. Prove that for any prime p the polynomial

$$\Phi_p(x) = x^{p-1} + \ldots + x + 1$$

is irreducible over $\mathbb{Q}$. *Hint.* Apply Eisenstein's criterion (Theorem 1). Think a little how to do this since all coefficients of $\Phi_p(x)$ are 1.

2.12. Decompose $x^{12}-1$ into binomials irreducible over $\mathbb{Q}$. Draw the picture similar to Fig. 3.

Let ε be a root of unity. Its *order* is the least $n \in \mathbb{N}$ such that $\varepsilon^n = 1$. The roots of order n are called the *primitive* roots of degree n. It is easy to show that all these roots are of the form ε_n^k where k is mutually prime with n. The number of integers among $1, \dots, n$ that are mutually prime with n is denoted $\varphi(n)$, and the function φ is called *Euler function.*

Theorem 4. *Roots of unity having degree n are conjugate over $\mathbb{Q}$ iff they have the same order. In particular, $\deg_{\mathbb{Q}}(\varepsilon_n) = \varphi(n)$ for all $n \in \mathbb{N}$.*

This theorem is equivalent to irreducibility over $\mathbb{Q}$ for the so called *cyclotomic polynomials*

$$\Phi_n(x) = \prod_{1 \leqslant k \leqslant n, (k,n)=1} (x - \varepsilon_n^k).$$

Problem 2.11 is a simple particular case of it. In general case it is even obvious immediately that the coefficients of $\Phi_n(x)$ are rational. Theorem 4 in general form may be proved at the Conference but you may use it just now. Theorem 4 enables to solve Problem 1.3 very quickly.

Now fill in the blancs in the solution of Problem **1.2c)**. Determine the polynomial $\mu_{\sqrt[3]{4}+\sqrt[3]{2}}(x)$ (by default, over $\mathbb{Q}$). The key idea is as follows: $\sqrt[3]{2}$ is a root of $\mu_{\sqrt[3]{4}+\sqrt[3]{2}}(x^2+x)$ which consequently is a multiple of $\mu_{\sqrt[3]{2}}(x) = x^3 - 2$, and so has also the roots $\sqrt[3]{2}\varepsilon$ и $\sqrt[3]{2}\varepsilon^2$, where $\varepsilon = \varepsilon_3$. Hence the numbers $\sqrt[3]{4}+\sqrt[3]{2}$, $\sqrt[3]{4}\varepsilon^2 + \sqrt[3]{2}\varepsilon$, $\sqrt[3]{4}\varepsilon + \sqrt[3]{2}\varepsilon^2$ are conjugate. Furthermore all of them are distinct (why?). It remains to show that the polynomial

$$\bigl(x - \sqrt[3]{4} - \sqrt[3]{2}\bigr)\bigl(x - \sqrt[3]{4}\varepsilon^2 - \sqrt[3]{2}\varepsilon\bigr)\bigl(x - \sqrt[3]{4}\varepsilon - \sqrt[3]{2}\varepsilon^2\bigr)$$

has rational coefficients; then it equals $\mu_{\sqrt[3]{4}+\sqrt[3]{2}}(x)$. Show this.

The following theorem, one of the main theorems in this project, is a generalization of the above argument.

Theorem 5. *If $\alpha = \alpha_1, \dots, \alpha_n$ are all conjugates of α over a field K then for every polynomial $f(x) \in K[x]$ the number $f(\alpha)$ is algebraic over K and its conjugates are $f(\alpha_1), \dots, f(\alpha_n)$. This list may consider repetitions but then each element occurs the same number of times.*

2.13. Prove Theorem 5: **a)** for the case when α is a root of an irreducible binomial; **b)** for the general case. (Investigation of linear independence of radicals requires only the more simple part **a)**. For part **b)** you may use the main theorem on symmetrical polynomials.)

Below is the outline of the proof.

1) To prove that $f(\alpha)$ is algebraic and all its conjugates are among $f(\alpha_1), \dots, f(\alpha_n)$, consider the polynomial

$$F(x) = (x - f(\alpha_1)) \dots (x - f(\alpha_n))$$

and prove that $F(x) \in K[x]$.

2) To prove that $f(\alpha_1), \dots, f(\alpha_n)$ all are conjugate over K, consider the polynomial $\mu_{f(\alpha)} f(x)$.

3) To prove that all roots of $F(x)$ are of the same multiplicity, consider the polynomial $F(x)/\mu_{f(\alpha)}(x)$.

Consider how to solve Problem **1.2i)** using Theorems 4 and 5. This problem is the crucual one in the proof for the part «only if» in Gauss — Wantzel theorem: *a regular n-gon can be constructed with compass and ruler iff $\varphi(n)$ is a power of 2, that is, if n is a product of a power of 2 and of some Fermat primes.* Fermat integers are integers of the form $2^{2^k}+1$. First five of them are primes: $3, 5, 17, 257, 65537$. Gauss has given the construction of the regular 17-gon. It would be of interest to construct the regular 257- and 65537-gons (a task for programmers).

2.14. Determine all $n \in \mathbb{N}$ such that $\cos\frac{2\pi}{n}$: **a)** is rational; **b)** can be expressed as $a + \sqrt{b}$, where $a, b \in \mathbb{Q}$, that is, $\deg_{\mathbb{Q}}\left(\cos\frac{2\pi}{n}\right) \leqslant 2$.

3. Construction of regular polygons

Let us think how theorems 4 and 5 can be used to solve problem **1.2i)**. This problem is crucial in the proof of the «only if» part of Gauss — Wantzel theorem: *a regular n-gon can be constructed by compass and ruler iff $\varphi(n)$ is a power of 2, that is, iff n is a product of a power of 2 and some Fermat primes.* The Fermat primes are the primes of the form $2^{2^k}+1$. First 5 integers of this form are primes: $3, 5, 17, 257, 65537$.

3.1. Using compass and ruler, construct a regular **a)** pentagon; **b)** 17-gon.

3.2. Develop an algorithm for construction of a regular p-gon for **a)** $p = 17$; **бb** $p = 257$; **c)** $p = 65537$.

Gauss constructed the regular 17-gon and proved constructibility of the regular p-gon for all Fermat primes p. This case (part a) is not estimated separately but forms an important step, so we recommend to analyze it.

The regular 257-gon was constructed by F.J. Richelot in the XIX century.

3.3. Using compass, ruler and trisector (the instrument for dividing an angle into three equal angles), construct the roots of the following polynomials: **a)** $8x^3 - 6x + 1$; **b)** $512x^9 - 1152x^7 + 864x^5 - 240x^3 + 18x + 1$. (The problem is related to 9- and 27-gons.)

3.4. Find all primes p such that there exists a unique $a \in \{1, \dots, p-1\}$ with $p \mid a^3 - 3a + 1$.

3.5. Using compass, ruler and trisector, construct a regular **a)** 7-gon; **b)** 13-gon.

"A too persistent research student drove his supervisor to say "Go away and work out the construction for a regular polygon of 65537 sides". The student returned 20 years later with a construction" (J. Littlewood "A mathematician's miscellany", p. 42-43). The library of Goettingen university possesses the manuscript on more than 200 pages which was written by I. G. Hermes in 1894 after more than 10 years of research and contains the construction of the regular 65537-gon. Now computers enable us to do this much quicker.

4. Linear independence of radicals

Theorem 6. *Suppose $N, k_1, \dots, k_N \in \mathbb{N}$, $N > 1$, $Q_1, \dots, Q_N \in \mathbb{Q}_+$, and futhermore $\sqrt[k_i]{Q_i}/\sqrt[k_j]{Q_j} \notin \mathbb{Q}$ for all $i \neq j$. Then the equality*

$$a_1 \sqrt[k_1]{Q_1} + \ldots + a_N \sqrt[k_N]{Q_N} = 0 \text{ for } a_1, \dots, a_N \in \mathbb{Q}$$

holds only if $a_1 = \ldots = a_N = 0$.

In particular, for $Q_1 = 1$ we have that *the sum $\sqrt[k_2]{Q_2} + \ldots + \sqrt[k_N]{Q_N}$ is irrational* since the equality $a_1 \sqrt[k_1]{1} + \sqrt[k_2]{Q_2} + \ldots + \sqrt[k_N]{Q_N} = 0$ fails for all $a_1 \in \mathbb{Q}$.

Irrationality of a single radical is a simple, purely arithmetical question which amounts to uniqueness of prime factorization.

Lemma 1. *For all $k \in \mathbb{N}$ and $Q \in \mathbb{Q}_+$ we have $\sqrt[k]{Q} \in \mathbb{Q}$ iff the degrees of all prime factors of the numerator and the denominator in the irreducible representation of Q are multiples of k.*

4.1. Prove Lemma 1.

4.2. Using Theorem 6 and Lemma 1, deduce irrationality of the numbers from Problem 1.1.

Without loss of generality, in Theorem 6 we may assume that all Q_i are positive integers and the degrees k_i are equal, obtaining the following equivalent formulation.

Theorem 7. *Suppose $k, n \in \mathbb{N}$, $p_1, \dots, p_n$ are distinct primes, $r_i = \sqrt[k]{p_i}$ for $i = 1, \dots, n$. Then the system $\{r_1^{l_1} \dots r_n^{l_n} \mid 0 \leqslant l_1, \dots, l_n < k\}$ of k^n numbers is linearly independent over $\mathbb{Q}$.*

It is convenient to represent this system as an n-dimensional grid, see examples at fig. 2 and 4.

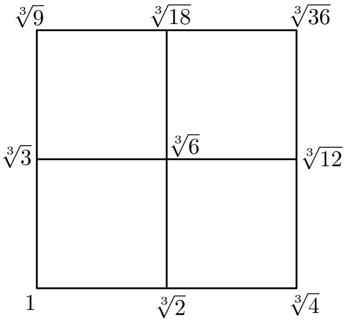


Fig. 4

4.3. Deduce Theorems 6 and 7 from each other.

4.4. Similarly to Problem 2.6, reduce Theorem 7 for $k = 2$ to the following statement and prove it:

$$\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}).$$

(We recommend to use conjugates, this helps to understand the case $k > 2$.)

4.5. Prove that Theorem 7 is equivalent to the following **Theorem 7′**: *in the notation from 7, the powers $1, r_n, \ldots, r_n^{k-1}$ are linearly independent over $\mathbb{Q}(r_1, \ldots, r_{n-1})$.*

4.6. Suppose K is a subfield of $\mathbb{R}$, $r \in \mathbb{R}$, $r^k \in K$ and $r, \ldots, r^{k-1} \notin K$. Prove that the binom $x^k - r^k$ is irreducible over K, and the powers $1, r, \ldots, r^{k-1}$ are linearly independent over K.

Thus Theorem 7′ amounts to the following **Theorem 7″**: *in the above notation*

$$r_n^l \notin \mathbb{Q}(r_1, \ldots, r_{n-1}) \text{ for all } l \in \{1, \ldots, k-1\}.$$

Suppose the contrary. By induction, every number from $\mathbb{Q}(r_1, \ldots, r_{n-1})$ is uniquely represented as a sum of products of the form $ar_1^{l_1} \ldots r_{n-1}^{l_{n-1}}$, where $a \in \mathbb{Q}$ and all $l_i \in \{0, \ldots, k-1\}$.

4.7. Obtain a contradiction if the above sum contains a single summand.

If the sum contains at least two summands then up to a permutation of radicals $r_1, \ldots, r_{n-1}$ we may assume

$$r_n^l = A_0 + A_1 r_{n-1} + \ldots + A_{k-1} r_{n-1}^{k-1}, \text{ where } A_0, \ldots, A_{k-1} \in \mathbb{Q}(r_1, \ldots, r_{n-2}), \tag{1}$$

and at least two of $A_0, \ldots, A_{k-1}$ are nonzero.

4.8. a) Prove that $A_0 = 0$.

b) Suppose A_j is the first nonzero coefficient in (1). Obtain a contradiction by proving that $A_j = 0$ (try to reduce this part to the preceding one). This completes the proof of Theorem 7.

4.9. Does Theorem 7 hold if each r_j $(j = 1, \ldots, n)$ is some complex value of $\sqrt[k]{p_j}$?

5. Dimension of field extensions

For deeper comprehension of algebraic numbers and dealing with more difficult problems we will consider the notion of vector space and its dimension as well as the technique of field extensions (everything for the case of number sets).

A set $V \subseteq \mathbb{C}$ containing a field K is called a *vector space over* K, and its elements are called *vectors* if V is closed under and multiplication by numbers from K and addition, that is, $a + b, ka \in V$ for any $a, b \in V$ and $k \in K$. For instance, every field is a vector space over any its subfield.

Suppose that a space $V \subseteq \mathbb{C}$ over a field K contains numbers $e_1, \ldots, e_n$ such that any $\alpha \in V$can be represented as

$$\alpha = k_1 e_1 + \ldots + k_n e_n \tag{2}$$

with uniquely determined coefficients $k_1, \ldots, k_n \in K$. Then the system $e_1, \ldots, e_n$ is called a *basis* of V over K, and the equality (2) is called the*decomposition* of α relative to this basis.

5.1. Prove that a basis of a space may be defined equivalently as a maximal (by inclusion) linearly independent system of elements. In other words, a system $e_1, \ldots, e_n$ is a basis of V over K iff it is linearly independent over K and the system $e_1, \ldots, e_n, \alpha$ is linearly dependent over K for any $\alpha \in V$.

A space having a finite basis is called finite-dimensional. An extension of the field having a finite basis is called a *finite extension.* The number of elements in a basis of a space V over K is called its *dimension* and is denoted $\dim_K L$. Correctness of this definition, that is, its independence of the choice of a basis is implied by the following lemma.

Lemma 2 (the basic lemma on linear dependence)**.** *If the numbers $f_1,\dots,f_m$ are linearly expressed over a field K through the numbers $e_1,\dots,e_n$ with $m>n$ then $f_1,\dots,f_m$ are linearly dependent over K.*

Let $U\subseteq W$ be finite-dimensional spaces over a field K. It is not difficult to check that any basis of U can be completed up to a basis of V. Thus $\dim_K U\leqslant\dim_K V$ and $\dim_K U=\dim_K V\Leftrightarrow U=V$.

If K is a subfield of a field L then we say that $L/K$is a field extension. Then clearly L is a vector space over K. The dimension of a finite extension L/K is also called its *degree* and is denoted $[L:K]$.

5.2. Let L/K be a finite extension. Prove that $[L:K]=2\Leftrightarrow L=K(\alpha)$ for some $\alpha\in L\setminus K$ such that $\alpha^2\in K$.

5.3. Prove that the numbers $1,\alpha,\dots,\alpha^{n-1}$ form a basis of the extension $K(\alpha)/K$ iff α is algebraic over K of degree n. Thus if α is algebraic over Kthen $\deg_K(\alpha)=[K(\alpha):K]$.

The following theorem is a useful tool in the theory of finite extensions (prove this theorem).

Theorem 8 (on dimension of a tower)**.** *If $K\subseteq P\subseteq L$ are finite extensions of fields then*

$$\boxed{\dim_K L=\dim_K P\cdot\dim_P L.}$$

Compare this with the property of logarithms $\log_a c=\log_a b\cdot\log_b c$.

Let us return to the warmup problem **1.1c)**.

5.4. Find all subfields of the fields: **a)** $\mathbb{Q}(\sqrt[11]{1024})$; **b)** $\mathbb{Q}(\sqrt[4]{3})$; **c)** $\mathbb{Q}(\varepsilon_5)$; **d)** $\mathbb{Q}(\varepsilon_8)$.

5.5*. Denote $\varepsilon=\varepsilon_{17}$. Theorem 2 and Problem 2.11 imply $\deg(\varepsilon)=16$.

a) Find all $\alpha\in\mathbb{Q}(\varepsilon)$ such that $\deg(\alpha)=2,4,8$. *Hint:* use Theorem 5 and consider the basis $\varepsilon,\varepsilon^3,\varepsilon^{3^2},\dots,\varepsilon^{3^{15}}$ in $\mathbb{Q}(\varepsilon)$ over $\mathbb{Q}$ (prove that this is a basis). This ordering is due to Gauss.

5.6. Find all conjugates over $\mathbb{Q}$ for the numbers **a)** $\sqrt{6}+\sqrt{10}+\sqrt{15}$; **b)** $\sqrt[3]{2}+\sqrt[3]{3}$.

b) Suppose $U_k=\{\alpha\in\mathbb{Q}(\varepsilon)\mid\deg(\alpha)\text{ divides }k\}$, $k=1,2,4,8,16$. In particular, $U_1=\mathbb{Q}$ and $U_{16}=\mathbb{Q}(\alpha)$. Prove that $U_1\subset U_2\subset U_4\subset U_8\subset U_{16}$ is a chain of quadratic (that is, of degree 2) extensions of fields. This enables us to construct a regular 17-gon using compass and ruler (discovery of Gauss).

A research problem. What regular n-gons can be constructed by compass, ruler and trisector? Particular cases: $n=7,13,19,37$.

A research problem. Develop an algorithm for determination of the degree of any algebraic number in the extension $\mathbb{Q}\left(\sqrt[k]{p_1},\dots,\sqrt[k]{p_n}\right)$, where $p_1,\dots,p_n$ are distinct primes. Particular cases: $k=2$; k is a prime.