Algebraic numbers as vectors

A. Kanunnikov, I. Vorobyov

§1. Introduction

How can we prove irrationality of the numbers

$$\sqrt[3]{\frac{121}{111}},\ \sqrt{2}+\sqrt{3},\ \sqrt{2}+\sqrt[3]{3},\ \sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7},\ \sqrt[5]{3}-\sqrt[5]{2},\ \sqrt{\frac{3}{5}+\frac{\sqrt[17]{2021!}}{2021}+\sqrt[5^{5^5}]{\frac{7^{7^7}}{3^{3^3}}}}?$$

Irrationality of a single radical is a simple purely arithmetical question which amounts to prime decomposition.

Lemma 1. *Suppose $A, B, k \in \mathbb{N}$ and $\gcd(A,B) = 1$. Then $\sqrt[k]{A/B} \in \mathbb{Q}$ iff the degrees of all primes in decompositions of A and B are multiples k.*

Proof. Suppose $\sqrt[k]{A/B} = a/b$, where $a, b \in \mathbb{N}$, then $Ab^k = Ba^k$. Each prime divisor p of A does not divide B, and its degrees in decompositions of a^k and b^k are multiples of k, so the degree of p in the decomposition of A also is a multiple of k. The argument for the prime divisors of B is similar. The converse is obvious.

The number $\sqrt[3]{\frac{121}{111}} = \sqrt[3]{\frac{11^2}{3\cdot 37}}$ is irrational by lemma 1. Irrationality of the sum $\sqrt{2}+\sqrt{3}$ is reduced to the irrationality of $\sqrt{6}$ by squaring.

Suppose that $\sqrt{2}+\sqrt[3]{3} = a \in \mathbb{Q}$ and cube the equality $\sqrt[3]{3} = a - \sqrt{2}$: we have $3 = a^3 + 6a - (3a^2+2)\sqrt{2}$ and arriving to a contradiction: $\sqrt{2} = \frac{a^3+6a-3}{3a^2+2} \in \mathbb{Q}$.

However the remaining numbers are not handled so simply: the straightforward exponentiation would only increase the number of radicals.

Perhaps a reader thinks: „Is it possible that after reading this article I will understand the reason of irrationality even for the last, especially weird number? “ „Yes, — we would answer, — but if you know how to divide polynomials with a remainder and extract roots from complex numbers. If it is not the case for this moment then you can at any rate deal with arbitrarily long sums of square radicals.“

In fact we will prove more: between the roots from rational numbers no linear relations with rational coefficients exist, except the obvious proportionalities, for instance $\sqrt{8} = 2\sqrt{2}$. The precise formulation is as follows.

Theorem 1. *Suppose $N, k_1, \ldots, k_N \in \mathbb{N}$, $N > 1$, $0 < Q_1, \ldots, Q_N \in \mathbb{Q}$ and $\sqrt[k_i]{Q_i} / \sqrt[k_i]{Q_j} \notin \mathbb{Q}$ for $i \neq j$. Then the equality*

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

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

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 $a_1 \in \mathbb{Q}$.

To apply Theorem 1, we have to check irrationality of specific radicals $\sqrt[k_i k_j]{Q_i^{k_j}/Q_j^{k_i}}$ by lemma 1.

Problem 1. Deduce from Theorem 1 and Lemma 1 irrationality of three numbers before Lemma 1.

In terms of vectors, the formulation of Theorem 1 is as follows: the numbers $\sqrt[k_1]{Q_1}, \ldots, \sqrt[k_N]{Q_N}$ *are linearly independent over* $\mathbb{Q}$ (cf. non-complanar vectors at fig. 1). In these terms, the condition $\sqrt[k_i]{Q_i} / \sqrt[k_j]{Q_j} \notin \mathbb{Q}$ expresses linear independence of $\sqrt[k_i]{Q_i}$ and $\sqrt[k_j]{Q_j}$ over $\mathbb{Q}$ (linear independence of two vectors amounts to their non-collinearity).

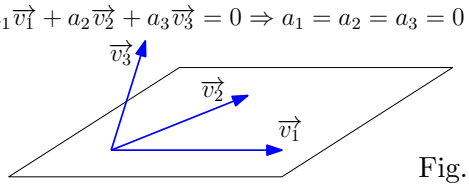


Fig. 1

In general, it is natural and productive to consider algebraic numbers (in particular radicals) as vectors: it enables us to apply geometric methods in algebraic problems.

Now we formulate a theorem which is more convenient for proving but occurs to be equivalent.

Theorem 2. *Suppose $k, n \in \mathbb{N}$, $p_1, \ldots, p_n$ are distinct primes, $r_1 = \sqrt[k]{p_1}, \ldots, r_n = \sqrt[k]{p_n}$. Then the system $\{r_1^{l_1} \ldots r_n^{l_n} \mid 0 \leqslant l_1, \ldots, l_n < k\}$ of k^n numbers is linearly independent over $\mathbb{Q}$.*

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

Problem 2. a) What is the relation between the tuples of numbers at the parallel sides of the square at fig. 2a and at parallel edges and faces of the cube at fig. 2b? b) Try to draw a hypercube (4-dimensional cube) and place radicals in its vertices on the same principle.

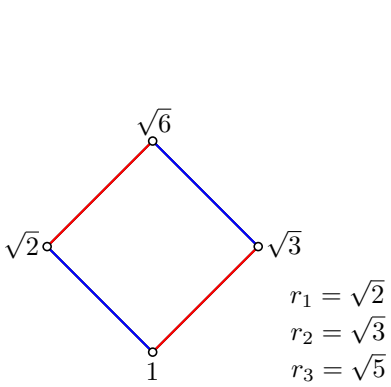
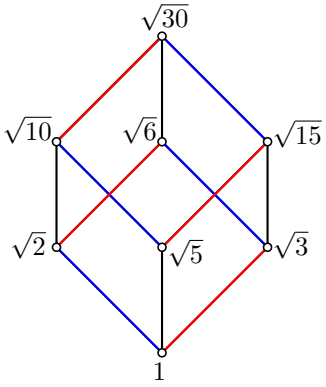


Fig. 2ab



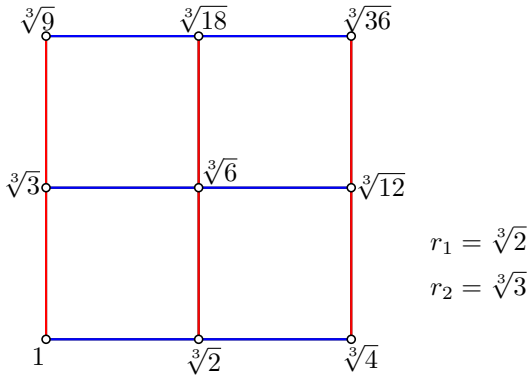


Fig. 2c

Problem 3. Deduce Theorems 1 and 2 from each other. *Hint.* $1 \Rightarrow 2$: the numbers for the system in Theorem 2 are pairwise non-proportional over $\mathbb{Q}$; $2 \Rightarrow 1$: generalize the argument from the following example.

Example 1. Let us reduce linear independence (by default, over $\mathbb{Q}$) of $1, \sqrt{1/2}, \sqrt[3]{4/3}$ to Theorem 2. Equalize the exponents of roots: $1, \sqrt[6]{1/2^3}, \sqrt[6]{2^4/3^2}$, multiply the second number by 2, and the third number by 3: $1, \sqrt[6]{2^3}, \sqrt[6]{2^4 \cdot 3^4}$ (this does not influence linear independence). We obtain a subsystem of the system $\{\sqrt[6]{2}^{l_1}\sqrt[6]{3}^{l_2} \mid 0 \leqslant l_1, l_2 \leqslant 5\}$, which is linearly independent by Theorem 2.

The case of square radicals has been repeatedly discussed in the literature for school students [2, 4, 6]. In §2 we will consider it for some examples arriving to some (although not all) ideas for the general situation. One more important idea appears in [5], where Theorem 2 is proved for $n = 1$. The general case is considered for instance in a research paper [7] which requires deep background (Galois theory). In §3 we prove Theorem 2 in a rather elementary way together with necessary information on algebraic numbers, which is interesting in its own. Finally we give a quite short proof of Theorem 1 available for a freshman. Everything necessary for understanding is gathered in §4.

§2. The case of square radicals

Theorem 2 for $k = 2$ can be proved by induction on n. The base $n = 1$: linear independence of 1 and $\sqrt{p_1}$ just denotes irrationality of $\sqrt{p_1}$ and is true by Lemma 1. Consider the cases $n = 2, 3$ for specific examples, this makes the ideas of the proof more clear. The complete argument for an arbitrary k by induction on n see below in §3.

Example 2. Let us prove that $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ (fig. 2a) are linearly independent. Suppose $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$, where $a, b, c, d \in \mathbb{Q}$. Separate $\sqrt{3}$: $a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3} = 0$. If $c + d\sqrt{2} = 0$ then $a + b\sqrt{2} = 0$, and then by irrationality $\sqrt{2}$, $c = d = 0$ and $a = b = 0$. And if $c + d\sqrt{2} \neq 0$ then

$$\sqrt{3} = -\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = -\frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = A + B\sqrt{2}, \text{ where } A = \frac{2bd - ac}{c^2 - 2d^2},\ B = \frac{ad - bc}{c^2 - 2d^2} \in \mathbb{Q}.$$

Square the equality $\sqrt{3} = A + B\sqrt{2}$:

$$3 = A^2 + 2B^2 + 2AB\sqrt{2} \implies AB = 0, \text{ otherwise } \sqrt{2} \in \mathbb{Q}.$$

For $A = 0$ we have $\sqrt{3/2} = B \in \mathbb{Q}$, and for $B = 0$ we have $\sqrt{3} = A \in \mathbb{Q}$, a contradiction with Lemma 1.

We have reduced linear independence of the numbers at Fig. 2a to the fact that $\sqrt{3}$ is „foreign“ for the set $\mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ (formally, $\sqrt{3}$ does not lie in it), just as $\sqrt{2}$ is „foreign“ for $\mathbb{Q}$. Moreover it occurs important that in the set $\mathbb{Q} + \mathbb{Q}\sqrt{2}$ we can not only add, subtract, multiply but also divide (not by 0) as in $\mathbb{Q}$. Before the next step, let us introduce some notions.

A bit of theory. A set of numbers containing 0 and 1 and closed under four arithmetical operations is called *a umber field*. In the sequel the word „number“ will be omitted. Thus K is a field iff $0, 1 \in K$ and for any $a, b \in K$ we have $a \pm b, ab \in K$ and $a/b \in K$ for $b \neq 0$. It is easily seen that $\mathbb{Q}$ is a field, and moreover „the

least one": any number field includes it[1]. In a field K is included in a field L then we say that K is a *subfield* in L. In the section, all fields lie in the field $\mathbb{R}$ of rationals.

Numbers $x_1, \ldots, x_n$ are called *linearly independent over a field* K if the equality $a_1x_1 + \ldots + a_nx_n = 0$ where $a_1, \ldots, a_n \in K$ holds only for $a_1 = \ldots = a_n = 0$. For example, the numbers 1 and $\sqrt{2}$ are linearly independent over $\mathbb{Q}$ but linearly dependent over $\mathbb{R}$ (the equality $a_1 \cdot 1 + a_2\sqrt{2} = 0$ holds for $a_1 = \sqrt{2}$ and $a_2 = -1$).

Problem 4. Check the property of linear dependence/independence over an arbitrary field K:

a) if a system contains zero or two numbers whose ratio lies in K then it is linear dependent over K;

b) a subsystem of a linearly independent system is linearly independent;

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

d) the coefficients $a_1, \ldots, a_n \in K$ 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.

The least (by inclusion) field including a field K and numbers $\alpha_1, \ldots, \alpha_n$, is denoted $K(\alpha_1, \ldots, \alpha_n)$ and is called the field generated by these numbers over K. Let us describe the field generated over K by a single square radical $\sqrt{d} \notin K$ where $d \in K$. Obviously the field $K(\sqrt{d})$ consists of ratios of numbers having the form $a + b\sqrt{d}$, where $a, b \in K$. We can remove irrationality in the denominator multiplying it by the *conjugate* $a - b\sqrt{d}$: $\dfrac{1}{a + b\sqrt{d}} = \dfrac{a - b\sqrt{d}}{a^2 - db^2}$ (as in Example 2). Hence

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

Example 3. Suppose p, q are distinct primes. Similarly to Example 2, $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$ and the numbers $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$ are linearly independent over $\mathbb{Q}$. Hence

$$\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p})(\sqrt{q}) = \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \mid a, b, c, d \in \mathbb{Q}\},$$

and such representation is unique.

Example 4. Let us prove that the numbers at Fig. 2b are linearly independent over $\mathbb{Q}$. Suppose

$$a_1 + a_2\sqrt{2} + \ldots + a_8\sqrt{30} = 0, \text{ where } a_1, a_2, \ldots, a_8 \in \mathbb{Q}.$$

Step 1. Put $\sqrt{5}$ out of brackets to obtain an equality of the form $A + B\sqrt{5} = 0$, where $A, B \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$:

$$\underbrace{a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_5\sqrt{6}}_{A} + \underbrace{(a_4 + a_6\sqrt{2} + a_7\sqrt{3} + a_8\sqrt{6})}_{B}\sqrt{5} = 0. \tag{1}$$

It suffices to prove that $A = B = 0$. Then according to Example 2, we have $a_1 = a_2 = a_3 = a_5 = 0$ and $a_4 = a_6 = a_7 = a_8 = 0$.

Step 2. We have to prove that 1 and $\sqrt{5}$ are linearly independent over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. This is equivalent to condition $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (Problem 4c).

Step 3. Suppose $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and in view of the description of this field in Example 3 we have

$$\sqrt{5} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \text{ where } a, b, c, d \in \mathbb{Q}. \tag{2}$$

A big number of radicals does not stimulate to square. But we can perform this more cleverly grouping the summands in one of two ways:

$$\underbrace{a + b\sqrt{2}}_{C} + (\underbrace{c + d\sqrt{2}}_{D})\sqrt{3} = \sqrt{5} = \underbrace{a + c\sqrt{3}}_{C'} + (\underbrace{b + d\sqrt{3}}_{D'})\sqrt{2}, \tag{3}$$

not ,,troubling" C, D, C', D'. Square the first equality:

$$C^2 + 3D^2 + 2CD\sqrt{3} = 5.$$

Since 1 and $\sqrt{3}$ are linearly independent over $\mathbb{Q}(\sqrt{2})$, we have $CD = 0$. Similarly $C'D' = 0$. We have 4 cases: $C = C' = 0$, $C = D' = 0$, $C' = D = 0$ or $D = D' = 0$. If $C = C' = 0$ then $a = b = c = 0$, hence $\sqrt{5} = d\sqrt{6}$, and this contradicts Lemma 1. In the other cases we obtain a similar contradiction because the right side of (2) reduces to a single nonzero summand.

[1]There exist other fields as well: the fields of residues $\mathbb{Z}_p$, the field of rational functions etc. Any field includes either $\mathbb{Q}$ or $\mathbb{Z}_p$ for some p.

PROBLEM 5. Prove Theorem 2 for $k = 2$: perform an induction step from $n-1$ to n similarly to Example 4.

Before consideration of radicals of higher exponents, let us discuss how to perform the last step without squaring, with the general case in mind. Perhaps you would agree that a straightforward exponentiating by 5 would hardly lead to a contradiction for equality as harmless as $\sqrt[5]{3} = a + b\sqrt[5]{2}$ $(a, b \in \mathbb{Q})$... So let us try to deal with the equality (3)using conjugates.

Numbers of the form $a \pm b\sqrt{d}$ over a field K where $a, b, d \in K$, $\sqrt{d} \notin K$ are called conjugate. In (3) the conjugate to $C + D\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is $C - D\sqrt{3}$, and the conjugate for $C' + D'\sqrt{2}$ over $\mathbb{Q}(\sqrt{3})$ is $C' - D'\sqrt{2}$. At the same time, the conjugate to $\sqrt{5}$ over both fields is $-\sqrt{5}$. Since the numbers are equal, their conjugates are equal as well:

$$C - D\sqrt{3} = -\sqrt{5} = C' - D'\sqrt{2}. \tag{4}$$

This and (3) imply that $C = C' = 0$, which is impossible as was shown above.

Unfortunately this argument only seems strict by contains a ,,hole". However it can be closed. The logical error is rather subtle, and a reader may be proud if he would manage to find and improve it.

PROBLEM 6. Why the transition from (3) to (4) is not justified and how to improve this?

Using of conjugates often is effective. Below are some olympiad problems on this subject.

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

PROBLEM 8. Find 1000 first digits after the point in the decimal record of $(6 + \sqrt{35})^{1000}$.

PROBLEM 9. prove that the product of 2^{100} numbers $\pm\sqrt{1} \pm \sqrt{2} \pm \ldots \pm \sqrt{99} \pm \sqrt{100}$ is a perfect square.

§3. The general case

Let us start the proof of Theorem 2 for an arbitrary k according to the plan from Example 4. Each step will enlarge our difficulties.

Step 1: splitting of the last radical. The linear relation over $\mathbb{Q}$ (that is, with coefficients from $\mathbb{Q}$) for the nine numbers at fig.c 2c can be represented as

$$f_0(\sqrt[3]{2}) + f_1(\sqrt[3]{2})\sqrt[3]{3} + f_2(\sqrt[3]{2})\sqrt[3]{9} = 0,$$

where f_0, f_1, f_2 are polynomials of degrees less than 3 over $\mathbb{Q}$ (grouping the summands as in (1)). So the linear independence of these numbers would follow from two facts:

$$\text{the numbers } 1, \sqrt[3]{3}, \sqrt[3]{9} \text{ are linearly independent over the field } \mathbb{Q}(\sqrt[3]{2}); \tag{5}$$

$$\text{the numbers } 1, \sqrt[3]{2}, \sqrt[3]{4} \text{ are linearly independent over the field } \mathbb{Q}. \tag{6}$$

In fact, (5) implies $f_0(\sqrt[3]{2}) = f_1(\sqrt[3]{2}) = f_2(\sqrt[3]{2}) = 0$, and then (6) implies that the coefficients of f_0, f_1, f_2 are zero. Let us generalize this argument to show that it suffices to prove **Theorem 2′**: *in the notation of Theorem 2 the numbers* $1, r_n, \ldots, r_n^{k-1}$ *are linearly independent over the field* $\mathbb{Q}(r_1, \ldots, r_{n-1})$.

Suppose that Theorem 2′ has been proven. Let us prove Theorem 2 by induction on n. For $n = 1$ the theorems are identical: $\mathbb{Q}(r_1, \ldots, r_{n-1}) = \mathbb{Q}$. Let $n > 1$. Reformulate Theorem 2: *if* $F(x_1, \ldots, x_n)$ *is a polynomial over* $\mathbb{Q}$*such that the degree of each variable is less than* k*, and* $F(r_1, \ldots, r_n) = 0$ *then* $F = 0$ *(that is, all coefficients of* F *are zero).* Express F in the form

$$F(x_1, \ldots, x_n) = f_0(x_1, \ldots, x_{n-1}) + f_1(x_1, \ldots, x_{n-1})x_n + \ldots + f_{k-1}(x_1, \ldots, x_{n-1})x_n^{k-1}.$$

By condition $F(r_1, \ldots, r_n) = 0$. By Theorem 2′ we have $f_j(r_1, \ldots, r_{n-1}) = 0$ for all $j = 0, \ldots, k-1$. By induction $f_0 = \ldots = f_{n-1} = 0$, thus $F = 0$.

Step 2: ,,otherness" of the last radical. Let K is any field, r is a number such that $r^k \in K$. Let us determine when

$$\text{the numbers } 1, r, \ldots, r^{k-1} \text{ are linearly independent } K. \tag{7}$$

In other words, r must not be a root of a polynomial with degree less than k and coefficients from K. For $k = 2$ this means simply that $r \notin K$ (Problem 4c). For $k > 2$ the situation is much more complicated and interesting.

A bit of theory. The set of the polynomials over a field K is denoted $K[x]$. A polynomial over K of positive degree, which is not a product of polynomials of lower degrees is called *irreducible* over K. Polynomials over a field allow division with remainder (,,long division").

Suppose a number α is a root of a nonzero polynomial over a field K. Then it is called *an algebraic number over* K. Among these polynomials there is a single polynomial of minimal degree with the leading coefficient 1 (if there were two then their difference would be a polynomial of lesser degree with the root α). It is called *the minimal polynomial* of the number α over K and will be denoted $\mu_\alpha^K(x)$ or $\mu_\alpha(x)$ if the field K is clear. The degree of this polynomial is the least $m \in \mathbb{N}$ such that the numbers $1, \alpha, \dots, \alpha^m$ are linearly dependent over K. The basic properties of $\mu_\alpha^K(x) = \mu_\alpha(x)$ are as follows:

1) the polynomial $\mu_\alpha(x)$ is irreducible over K;

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

3) the polynomial $p(x)$ irreducible over K and having the root α and the leading coefficient 1 equals $\mu_\alpha(x)$.

Proof. 1) If μ_α decomposes into a ptoduct of polynomials over K of lesser degrees then α is a root of one of the factors which contradicts to minimality of degree of $\deg \mu_\alpha$.

2) Suppose $f \in K[x]$ and $f(\alpha) = 0$. Divide f by μ_α with a remainder: $f = \mu_\alpha q + s$, where $q, s \in K[x]$ and either $s = 0$ or $\deg s < \deg \mu_\alpha$. The second case is impossible because $s(\alpha) = f(\alpha) - \mu_\alpha(\alpha)q(\alpha) = 0$.

3) By part 2), $p(x)$ is a multiple of $\mu_\alpha(x)$, and since $p(x)$ is irreducible over K, we have $p(x)/\mu_\alpha(x) = c \in K$. Since the leading coefficients of $p(x)$ and $\mu_\alpha(x)$ are equal to 1, we have $c = 1$. □

Thus (7) $\Leftrightarrow \mu_r^K(x) = x^k - r^k \Leftrightarrow$ the binomial $x^k - r^k$ is irreducible over K.

For instance, statements (5) and (6) are respectively equivalent to irreducibility of the binomial $x^3 - 3$ over $\mathbb{Q}(\sqrt[3]{2})$ and of the binomial $x^3 - 2$ over $\mathbb{Q}$ which means that $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$ and $\sqrt[3]{2} \notin \mathbb{Q}$ (a cubic polynomial is irreducible over a field iff it has no roots in this field). In general, the condition of „otherness“ $r \notin K$ is necessary but not sufficient. Although in our case the actors K and r are in the field $\mathbb{R}$, we will leave it for the complex plane, the field $\mathbb{C}$ where the binomial $x^k - r^k$ decomposes into linear factors By the de Moivre formula [3]

$$x^k - r^k = (x - r)(x - r\varepsilon)\dots(x - r\varepsilon^{k-1}), \text{ where } \varepsilon = \varepsilon_k = \cos\tfrac{2\pi}{k} + i\sin\tfrac{2\pi}{k}. \tag{8}$$

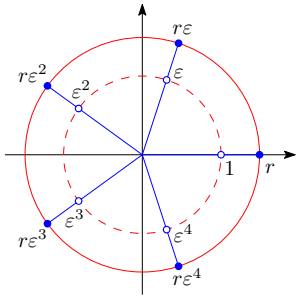


Fig. 3

Lemma 2. *Suppose K is a subfield in $\mathbb{R}$, $r \in \mathbb{R}$, $r^k \in K$ and $r, \dots, r^{k-1} \notin K$. Then the binomial $x^k - r^k$ is irreducible over K.*

Proof. Let $x^k - r^k$ have a factor in $K[x]$ with degree $l \in \{1, \dots, k-1\}$ such that its intercept is c. From the decomposition (8) we have $c = (-r)^l\varepsilon^s$ for some integer s. Since $c \in K \subseteq \mathbb{R}$, $r \in \mathbb{R}$ and $|\varepsilon^s| = 1$, we have $r^l = \pm|c| \in K$ which contradict the condition. □

Remark. For $r \notin \mathbb{R}$ the lemma fails: for instance, for $k = 3$ and $r = \varepsilon$ we have $\varepsilon, \varepsilon^2 \notin \mathbb{R}$ but the binomial $x^3 - 1$ is irreducible.

Example 5. For any prime p and positive integer $k > 1$ we have $\sqrt[k]{p}, \dots \sqrt[k]{p^{k-1}} \notin \mathbb{Q}$ (Lemma 1), hence the binomial $x^k - p$ is irreducible over $\mathbb{Q}$ (Lemma 2)[2], hence $\mu^{\mathbb{Q}}_{\sqrt[k]{p}}(x) = x^k - p$.

In general Theorem 2′ reduces to **Theorem 2″** by Lemma 2: *in the same notation*

$$r_n, \dots, r_n^{k-1} \notin \mathbb{Q}(r_1, \dots, r_{n-1}). \tag{9}$$

For $n = 1$ this follows from Lemma 1. To arrive to a contradiction for $n > 1$, let us express the numbers from $\mathbb{Q}(r_1, \dots, r_{n-1})$ in the form of polynomials in $r_1, \dots, r_{n-1}$. For instance, the condition $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$ takes the form $\sqrt[3]{3} \neq a + b\sqrt[3]{2} + c\sqrt[3]{4}$ with $a, b, c \in \mathbb{Q}$.

Step 3: removal of the irrationality from the denominator. The well-known multiplication by conjugates applies only for square radicals. The necessary operations for $k > 2$ will be first shown by an example.

[2]In [5] linear independence 1, $\sqrt[k]{p}, \dots \sqrt[k]{p^{k-1}}$ also is reduced to irreducibility of $x^k - p$ which follows from the Eisenstein criterion.

Example 6. Let us remove irrationality from the denominator of $\dfrac{1}{\sqrt[3]{4}+\sqrt[3]{2}+3}$. Denote $r=\sqrt[3]{2}$ and $f(x)=x^2+x+3$. We have to find a polynomial $u\in\mathbb{Q}[x]$ such that $\frac{1}{f(r)}=u(r)$. This means that $f(x)u(x)-1$ has the root r and so is a multiple of $\mu_r^{\mathbb{Q}}(x)=x^3-2$ (Example 5). Thus

$$u(x)f(x)+v(x)(x^3-2)=1$$

for some polynomial $v\in\mathbb{Q}[x]$. Polynomials u and v can be found using Euclid algorithm:

Euclid algorithm	Reversal of Euclid algorithm
$x^3-2=(x^2+x+3)(x-1)-2x+1$ $x^2+x+3=(2x-1)\left(\frac{1}{2}x+\frac{3}{4}\right)+\frac{15}{4}$	$\frac{15}{4}=f(x)-\big(f(x)(x-1)-(x^3-2)\big)\left(\frac{1}{2}x+\frac{3}{4}\right)=$ $=(x^3-2)\left(\frac{1}{2}x+\frac{3}{4}\right)+f(x)\left(-\frac{1}{2}x^2-\frac{1}{4}x+\frac{7}{4}\right)$

So $(2x^2+x-7)(x^2+x+3)-(2x+3)(x^3-2)=-15$, and for $x=r$ this implies

$$\frac{1}{\sqrt[3]{4}+\sqrt[3]{2}+3}=\frac{7-\sqrt[3]{2}-2\sqrt[3]{4}}{15}.$$

Now we will prove a general assertion following the above example.

Lemma 3 (on removal of an irrationality from the denominator)**.** *If a number α is algebraic over a field K and $\deg\mu_\alpha(x)=k$ then every number from the field $K(\alpha)$ is uniquely expressed as*

$$c_0+c_1\alpha+\ldots+c_{k-1}\alpha^{k-1},\ \textit{where } c_0,c_1,\ldots,c_{k-1}\in K. \tag{10}$$

Proof. The numbers of this form lie in $K(\alpha)$, so we have to check that they form a field. Obviously this set is closed under addition, subtraction and multiplication. Suppose $f\in K[x]$ and $f(\alpha)\neq 0$. Then $f(x)$ is not a multiple of $\mu_\alpha(x)$, hence these polynomials are mutually prime. Euclid algorithm provides polynomials $u,v\in K[x]$ such that $u(x)f(x)+v(x)\mu_\alpha(x)=1$. For $x=\alpha$ we get $1/f(\alpha)=u(\alpha)$ which is transformed to (10) when we replace u with its remainder of division by μ_α. The coefficients c_i are uniquely determined, otherwise α would be a root of a polynomial of degree less than k. □

Problem 10. Get rid of irrationality in the denominators: a) $\dfrac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}}$; b) $\dfrac{1}{\sqrt[4]{27}+2\sqrt[4]{3}-1}$.

Let us return to the proof of the Theorem 2″. By the inductive assumption, the binomial $x^k-r_1^k$ is irreducible over $\mathbb{Q}$, the binomial $x^k-r_2^k$ over $\mathbb{Q}(r_1)$, …, the binomial $x^k-r_{n-1}^k$ over $\mathbb{Q}(r_1,\ldots,r_{n-2})$. Consecutively removing irrationalities from the denominators, we uniquely represent each number from $\mathbb{Q}(r_1,\ldots,r_{n-1})$ as a sum of numbers of the form

$$ar_1^{l_1}\ldots r_{n-1}^{l_{n-1}},\ \text{where } a\in\mathbb{Q},\ 0\leqslant l_1,\ldots,l_{n-1}<k. \tag{11}$$

Suppose (9) fails, that is, r_n^l for some $l\in\{1,\ldots,k-1\}$ equals a sum of numbers of the form (11). This sum contains more than one summand, otherwise $r_n^l/(r_1^{l_1}\ldots r_{n-1}^{l_{n-1}})=a\in\mathbb{Q}$, a contradiction to Lemma 1. Hence one of the radicals $r_1,\ldots,r_{n-1}$ appears in two summands with different degrees, let it be r_{n-1}. Thus

$$r_n^l=A_0+A_1r_{n-1}+\ldots+A_{k-1}r_{n-1}^{k-1}, \tag{12}$$

where at least two of $A_0,\ldots,A_{k-1}\in\mathbb{Q}(r_1,\ldots,r_{n-2})$ are nonzero. This is the most interesting, particularly difficult moment in comparison with the case $k=2$. Indeed, for $k=2$ the equality (12) is not terrible at all: $\sqrt{p_n}=A_0+A_1\sqrt{p_{n-1}}$, the squaring is of no difficulty. But for $k>2$ even the idea of exponentiating of (12) to kth degree is unpleasant... Minimal polynomials again will help us. But if the minimal polynomial for the left part is found easily, for the right part even its algebraicity is not obvious.

Example 7. Let us obtain a contradiction in the above equality $\sqrt[5]{3}=a+b\sqrt[5]{2}$, where $a,b\in\mathbb{Q}$, this is a particular case of (12). By Lemma 1, $a\neq 0$ and $b\neq 0$. By Example 5, $\mu_{\sqrt[5]{3}}(x)=x^5-3$ and $\mu_{\sqrt[5]{2}}(x)=x^5-2$, hence $\mu_{a+b\sqrt[5]{2}}(x)=(x-a)^5-2b^5$ (we have done the linear substitution $x\mapsto\frac{x-a}{b}$ and multiplied by b^5). A contradiction:

$$x^5-3=(x-a)^5-2b^5=x^5-5ax^4+\ldots\ \Longrightarrow\ a=0.$$

Problem 11. Solve in positive integers: $\sqrt[5]{m}+\sqrt[5]{n}=2021$.

Problem 12. Disprove the equality $\sqrt[6]{3}=a\sqrt[3]{2}+b\sqrt{2}$, where $a,b\in\mathbb{Q}$.

In general, the way to the minimal polynomial of the right side in (12) passes through *conjugate numbers*. But we have defined this notion only for quadratic irrationalities, and also at the end of §2 we have indicated some argument using conjugates.

A bit more of theory. Suppose a number $\alpha\in\mathbb{C}$ is algebraic over a field K, and

$$\mu_\alpha(x)=(x-\alpha_1)\dots(x-\alpha_k)$$

(by the fundamental theorem of algebra, any polynomial over $\mathbb{C}$ decomposes into linear factors[3]). The numbers $\alpha_1,\dots,\alpha_k$ are called *conjugates for* α over K. Denote their sum by $\sigma(\alpha)$. By Vieta theorem

$$\sigma(\alpha)=\alpha_1+\ldots+\alpha_k \iff \mu_\alpha(x)=x^k-\sigma(\alpha)x^{k-1}+\dots \tag{13}$$

Example (7) shows that just the coefficient $-\sigma(\alpha)$ plays the key role.

Remark. The numbers $\alpha_1,\dots,\alpha_k$ are different (this is not used in the proof): if $\mu_\alpha(x)=(x-\alpha_j)^2g(x)$ then the derivative $\mu'_\alpha(x)=2(x-\alpha_j)g(x)+(x-\alpha_j)^2g'(x)\in K[x]$ has the root α_j although $\deg\mu'_\alpha<\deg\mu_\alpha$.

Property 3) of the minimal polynomial implies that all numbers algebraic over K divide into classes of conjugates and each class consists of the roots of some polynomial irreducible over K.

Example 8. Decompose the binomial x^4-2 into irreducible factors and divide its roots into classes of conjugates over each of the fields $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt[4]{2})\subset\mathbb{Q}(\sqrt[4]{2},i)$:

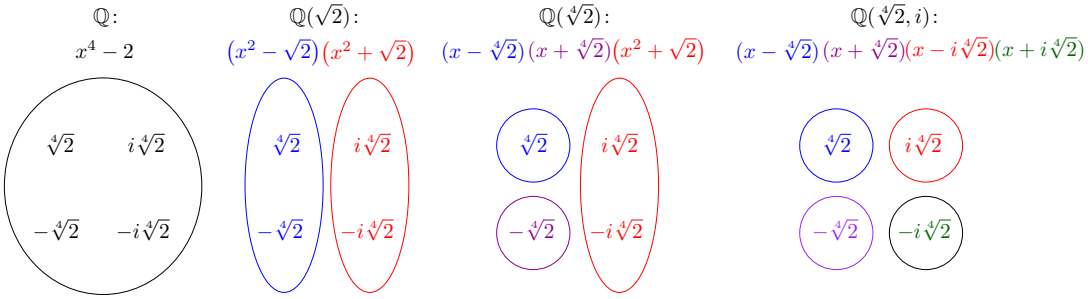


Fig. 4

Example 9. For square irrationalities $a\pm b\sqrt{d}$ ($a,b,d\in K$, $b\neq0$, $\sqrt{d}\notin K$) this definition agrees with the usual notion of conjugacy:

$$\mu^K_{a\pm b\sqrt{d}}(x)=x^2-2ax+a^2-db^2,\quad \sigma(a\pm b\sqrt{d})=2a.$$

(By the way, in the case $K=\mathbb{R}$, $d=-1$ we obtain complex conjugates $a\pm bi$.) This saves the above justification of the transition from (3) to (4).

Example 10. Suppose $a,b\in\mathbb{Q}$, $b\neq0$. The numbers $a\pm b\sqrt[k]{2}$ are not of course conjugates when $k>2$ (as in the case of square irrationalities). The conjugates for $a+b\sqrt[k]{2}$ are the roots of the polynomial $\mu_{a+b\sqrt[k]{2}}(x)=(x-a)^k-2b^k$ (similarly to the example 7), that is, they are equal to $a+b\sqrt[k]{2}\varepsilon^j$, $j=0,\dots,k-1$ (see an example at fig. 5).

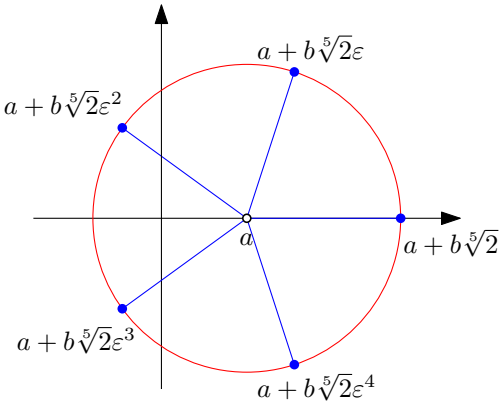


Fig. 5

[3]We will not use this: in the proof, all polynomials get explicit decompositions.

Step 4: transition to conjugates. Example 10 suggests the form of the conjugates for for a number of the form (10).

Example 11. Let us disprove the equality $\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, where $a, b, c \in \mathbb{Q}$. The conjugates for the left side are $\sqrt[3]{3}$, $\sqrt[3]{3}\varepsilon$, $\sqrt[3]{3}\varepsilon^2$, where $\varepsilon = \varepsilon_3$. On the other hand, consider the polynomial

$$F(x) = \big(x - (a + b\sqrt[3]{2} + c\sqrt[3]{4})\big)\big(x - (a + b\sqrt[3]{2}\varepsilon + c\sqrt[3]{4}\varepsilon^2)\big)\big(x - (a + b\sqrt[3]{2}\varepsilon^2 + c\sqrt[3]{4}\varepsilon)\big).$$

How can we prove $F(x) \in \mathbb{Q}[x]$ without troublesome removal of braclets? This is a purely algebraic issue: replace $\sqrt[3]{2}$ by y and $\sqrt[3]{4}$ by y^2. The resulting polynomial does not change under substitution of $y\varepsilon$ instead of y, hence y appears in it only with degrees divided by 3. Replacing y^3 by 2 we get a polynomial $F(x) \in \mathbb{Q}[x]$. Hence $F(x)$ is a multiple of $\mu_{\sqrt[3]{3}}(x) = x^3 - 3$, and thus $F(x) = x^3 - 3$. But the sum of the roots of F equals $3a$ (because $1 + \varepsilon + \varepsilon^2 = 0$). Hence $a = 0$ and $\sqrt[3]{3} = b\sqrt[3]{2} + c\sqrt[3]{4}$. Divide by $\sqrt[3]{2}$: $\sqrt[3]{3/2} = b + c\sqrt[3]{2}$. Similarly or as in Example 7 we obtain $b = 0$. Thus $\sqrt[3]{3} = c\sqrt[3]{4}$ which is impossible by Lemma 1.

Lemma 4. *Suppose K is a subfield in $\mathbb{R}$, $r \in \mathbb{R}$, $r \notin K$, $r^k \in K$ for some $k \in \mathbb{N}$. Then $\sigma(r) = 0$.*

Proof. There exists the least $m \in \mathbb{N}$ such that $r^m \in K$. By Lemma 2 the binomial $x^m - r^m$ is irreducible over K and hence equal to$\mu_r^K(x)$. Since $r \notin K$, we have $m > 1$ and $\sigma(r) = 0$. □

Lemma 5. *Let $\alpha_1 = \alpha, \ldots, \alpha_k$ be all the conjugates for a number α algebraic over a field K, and suppose $f \in K[x]$. Then $f(\alpha)$ is algebraic over K, and we have for some $d \in \mathbb{N}$*

$$\mu_{f(\alpha)}(x)^d = (x - f(\alpha_1)) \ldots (x - f(\alpha_k)). \tag{14}$$

Proof. For our goal, it suffices to consider the case $\mu_\alpha(x) = x^k - r^k$ where $r = \alpha$. The equality (14) takes the form

$$\mu_{f(r)}(x)^d = (x - f(r))(x - f(r\varepsilon)) \ldots (x - f(r\varepsilon^{k-1})). \tag{15}$$

1. Consider an auxiliary polynomial

$$G(x, y) = (x - f(y))(x - f(y\varepsilon)) \ldots (x - f(y\varepsilon^{k-1})).$$

It does not change under replacement of y by $y\varepsilon$ (the parentheses are moved cyclically), hence all degrees of y in it are multiples of k. Thus $G(x, r)$ is a polynomial with coefficients in K and the root $f(r)$. Hence $f(r)$ is algebraic over K, and $\mu_{f(r)}(x)$ divides $G(x, r)$.

2. The polynomial $\mu_{f(r)}(f(x)) \in K[x]$ has the root r and hence is a multiple of $\mu_r(x) = x^k - r^k$. Thus all roots $r, r\varepsilon, \ldots, r\varepsilon^{k-1}$ of this binomial are roots of the polynomial $\mu_{f(r)}(f(x))$, that is, the numbers $f(r), f(r\varepsilon), \ldots, f(r\varepsilon^{k-1})$ are conjugates.

3. Suppose $d \in \mathbb{N}$ is the least integer such that $\mu_{f(r)}(x)^d$ divides $G(x, r)$. Let us prove that $G(x, r) = \mu_{f(r)}(x)^d$. In fact, in the opposite case the polynomial $G(x, r)/\mu_{f(r)}(x)^d \in K[x]$ has a root $f(r\varepsilon^j)$ and hence is a multiple of $\mu_{f(r\varepsilon^j)}(x) = \mu_{f(r)}(x)$, a contradiction with minimality of d.

To prove the assertion in general case, let us consider the polynomial

$$G(x, y_1, \ldots, y_k) = (x - f(y_1)) \ldots (x - f(y_k)).$$

It does not change under substitutions of $y_1, \ldots, y_k$ and by the fundamental theorem on symmetric polynomials [1, p. 134] can be expressed in terms of x and elementary symmetric polynomials $\sigma_1, \ldots, \sigma_k$ defined by the equality

$$(x - y_1) \ldots (x - y_k) = x^k - \sigma_1 x^{k-1} + \sigma_2 x^{k-2} - \ldots + (-1)^k \sigma_k.$$

Since $(x - \alpha_1) \ldots (x - \alpha_k) = \mu_\alpha(x) \in K[x]$, we have $G(x, \alpha_1, \ldots, \alpha_k) \in K[x]$. The further argument is similar. □

In equality (15), equate the sums of roots (with multiplicities) in

$$d\sigma(f(r)) = f(r) + f(r\varepsilon) + \ldots + f(r\varepsilon^{k-1}).$$

Calculate the right part for $f(x) = c_0 + c_1 x + \ldots + c_{k-1} x^{k-1}$:

$$\begin{array}{lll} f(r) & = c_0 + c_1 r & + \ldots + c_{k-1} r^{k-1}, \\ f(r\varepsilon) & = c_0 + c_1 r\varepsilon & + \ldots + c_{k-1} r^{k-1} \varepsilon^{k-1}, \\ \ldots & & \\ f(r\varepsilon^{k-1}) & = c_0 + c_1 r\varepsilon^{k-1} & + \ldots + c_{k-1} r^{k-1} \varepsilon^{(k-1)^2}. \end{array}$$

Add the numbers in each column. Since $\varepsilon^k = 1$, then

$$1 + \varepsilon^j + \varepsilon^{2j} + \ldots + \varepsilon^{(k-1)j} = \frac{1 - \varepsilon^{kj}}{1 - \varepsilon^j} = 0,\ j = 1, \ldots, k-1.$$

Hence $f(r) + f(r\varepsilon) + \ldots + f(r\varepsilon^{k-1}) = kc_0$, so

$$\sigma(c_0 + c_1 r + \ldots + c_{k-1} r^{k-1}) = \tfrac{k}{d} \cdot c_0. \tag{16}$$

Finally we arrive to a contradiction in (12). Let A_j be the first nonzero coefficient in the sequence $A_0, \ldots, A_{k-1}$. Divide the equality (12) by r_{n-1}^j:

$$\frac{r_n^l}{r_{n-1}^j} = A_j + A_{j+1} r_{n-1} + \ldots + A_{k-1} r_{n-1}^{k-j-1}. \tag{17}$$

Suppose $K = \mathbb{Q}(r_1, \ldots, r_{n-2})$, $R = r_n^l / r_{n-1}^j$. Then $R \notin K$, otherwise $R = A_j$ and $A_{j+1} = \ldots = A_{k-1} = 0$ due to linear independence of $1, r_{n-1}, \ldots, r_{n-1}^{k-1}$ over K (remind that at least two of numbers $A_j, \ldots, A_{k-1}$ are nonzero). Furthermore $R^k = p_n^l / p_{n-1}^j \in \mathbb{Q}$, hence $\sigma(R) = 0$ by Lemma 4. But the value of σ corresponding to the right part of (17) is by (16) proportional to A_j (which plays the role of c_0) and hence is nonzero. This contradiction proves Theorem 2.

In fact we have proved more: each number from the field $\mathbb{Q}(r_1, \ldots, r_n)$ is a linear combination of k^n numbers

$$r_1^{l_1} \ldots r_n^{l_n} \quad (0 \leqslant l_1, \ldots, l_n < k)$$

with uniquely determined rational coefficients. In terms of vectors, these numbers form *a basis* of the field $\mathbb{Q}(r_1, \ldots, r_n)$ over $\mathbb{Q}$. This representation is obtained by removal of the irrationality in the denominator, and uniqueness of the coefficients is equivalent to linear independence of the system.

A short proof with use of trace

If you have a bit more information about algebraic numbers or know the foundations of linear algebra then you can give a short proof of Theorem 1 (without reduction to Theorem 2). The base for this argument is some value proportional to the sum of conjugates. Moreover it has the remarkable feature of linearity which minimizes the technical aspect.

A function $f\colon L \to \mathbb{C}$ where L is a subfield in $\mathbb{C}$ is called *linear* (more precisely, $\mathbb{Q}$-linear) if $f(ax + by) = af(x) + bf(y)$ for all $x, y \in L$ and $a, b \in \mathbb{Q}$. Suppose $L = \mathbb{Q}(\sqrt[k_1]{Q_1}, \ldots, \sqrt[k_N]{Q_N})$. In §4 we will show that there exists a linear function $\mathrm{tr}\colon L \to \mathbb{C}$ called the trace, such that

$$\text{for every } \alpha \in L \text{ there exists } d \in \mathbb{N} \text{ such that } \mathrm{tr}(\alpha) = d\sigma(\alpha) \tag{18}$$

($\sigma(\alpha)$ is defined in (13)). Suppose that $a_1 \sqrt[k_1]{Q_1} + \ldots + a_N \sqrt[k_N]{Q_N} = 0$ where not all $a_1, \ldots, a_N \in \mathbb{Q}$ are zeroes. Assume that $a_N \neq 0$. Surprisingly we will separate not a radical but a coefficient. Divide both parts by $\sqrt[k_N]{Q_N}$ and denote $R_i = \sqrt[k_i]{Q_i} / \sqrt[k_N]{Q_N}$, $i = 1, \ldots, N-1$:

$$-a_N = a_1 R_1 + \ldots + a_{N-1} R_{N-1}. \tag{19}$$

Since $R_i^{k_i k_N} \in \mathbb{Q}$ and by condition $R_i \notin \mathbb{Q}$, we have $\sigma(R_i) = 0$ by Lemma 4, hence $\mathrm{tr}(R_i) = 0$ by (18). By linearity, the trace of the right part of (19) equals 0. On the other hand, $\sigma(-a_N) = -a_N \neq 0$, and by (18) we have $\mathrm{tr}(-a_N) \neq 0$. This contradiction completes the proof of Theorem 1.

§4. Appendix: regarding trace

We shall construct the function named trace $\mathrm{tr}\colon L \to L$ for any extension $L \supseteq \mathbb{Q}$ generated by a finite set of algebraic numbers, in particular for$L = \mathbb{Q}(\sqrt[k_1]{Q_1}, \ldots, \sqrt[k_N]{Q_N})$. We will perform this in two ways. The first way is closer to the argument in §3 and enriches it by translation to the language of Galois theory. After that we will give the basic definition of the trace, which explains its name, by the way. This way requires basic information from linear algebra:

– the basis and dimension of an extension, the tower theorem [4, §5];

– matrix operations, the inverse matrix [1, p. 41–44, 73];

– the matrix of a linear operator in a basis, its transformation under change of the basis [1, p. 234–236].

I approach (in spirit of Galois theory)

We need the following well-known fact [4, theorem 2]: *the set $\mathbb{A}$ of algebraic (over $\mathbb{Q}$) numbers is a field.* Thus $L \subseteq \mathbb{A}$ because L is generated by algebraic numbers over $\mathbb{Q}$.

Let us call the map $\varphi\colon L \to \mathbb{C}$ an *inclusion* if $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in L$ and $\varphi(c) = c$ for all $c \in \mathbb{Q}$. In particular, φ is linear: $\varphi(ca) = \varphi(c)\varphi(a) = c\varphi(a)$ for $c \in \mathbb{Q}$ and $a \in L$. In the sequel we show that there exists only a finite number of inclusions $\varphi_1, \ldots, \varphi_n$ of L. Put

$$\operatorname{tr}(\alpha) = \sum_{j=1}^{n} \varphi_j(\alpha). \tag{20}$$

Problem 13. Without further reading: a) prove that all inclusions $\mathbb{Q}(i) \to \mathbb{C}$ are of the form $a + bi \mapsto a \pm bi$ $(a, b \in \mathbb{Q})$; b) describe all inclusions $\mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right) \to \mathbb{C}$. Find $\operatorname{tr}(1+i)$ for each case.

The inclusions discover a new approach to conjugates described above in terms of roots of irreducible polynomials. Suppose $\alpha \in L$ and

$$\mu_\alpha(x) = x^m - c_{m-1}x^{m-1} - \ldots - c_1 x - c_0. \tag{21}$$

Apply any inclusion $\varphi\colon L \to \mathbb{C}$ to both parts of the equality $\mu_\alpha(\alpha) = 0$:

$$\varphi(\mu_\alpha(\alpha)) = \varphi(\alpha)^m - c_{m-1}\varphi(\alpha)^{m-1} - \ldots - c_1\varphi(\alpha) - c_0 = \mu_\alpha(\varphi(\alpha)) = \varphi(0) = 0.$$

We see that $\varphi(\alpha)$ is conjugate to α. Conversely suppose that α_j is some conjugate for $\alpha \in L$. Does there exist an inclusion $L \to \mathbb{C}$ such that α maps to α_j? This inclusion must be determined in $\mathbb{Q}(\alpha)$ by the rule $f(\alpha) \mapsto f(\alpha_j)$, where $f \in \mathbb{Q}[x]$ (by Theorem 3 each number from $\mathbb{Q}(\alpha)$ has this form). On the other hand, this rule is correct (does not depend on the choice of f) and determines an inclusion $\mathbb{Q}(\alpha) \to \mathbb{C}$ since for all $f, g \in \mathbb{Q}[x]$ we have

$$f(\alpha) = g(\alpha) \Leftrightarrow f(x) - g(x) \vdots \mu_\alpha(x) \Leftrightarrow f(\alpha_j) = g(\alpha_j),$$
$$f(\alpha) + g(\alpha) = (f+g)(\alpha),\ f(\alpha)g(\alpha) = (fg)(\alpha).$$

By the way it is not evident that this inclusion extends from $\mathbb{Q}(\alpha)$ to L but at any rate we are already able to describe the inclusions of *simple* extensions of $\mathbb{Q}$ (that is, extensions generated by a single number).

Theorem 3. *Let $\theta_1 = \theta, \ldots, \theta_n$ be the conjugates of $\theta \in \mathbb{A}$. Then the inclusions $\mathbb{Q}(\theta) \to \mathbb{C}$ are*

$$\varphi_j\colon f(\theta) \mapsto f(\theta_j)\ (f \in \mathbb{Q}[x]),\ j = 1, \ldots, n.$$

Luckily an extension generated by a finite set of algebraic numbers is generated by a single number as well (this number is called a *primitive element of the extension*).

Example 12. Let us show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Inclusion $\supseteq$ is evident. Conversely

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) \ni \frac{1}{\sqrt{2}+\sqrt{3}} = \sqrt{3} - \sqrt{2} \implies \mathbb{Q}(\sqrt{2}+\sqrt{3}) \ni \frac{\sqrt{3}+\sqrt{2}}{2} \pm \frac{\sqrt{3}-\sqrt{2}}{2} = \sqrt{3}, \sqrt{2}.$$

Theorem 4 (on the primitive element)**.** *There exists $\theta \in L$ such that $L = \mathbb{Q}(\theta)$.*

Proof. It suffices to find $\theta = \alpha + c\beta \in L$ for given $\alpha, \beta \in L$, such that $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \beta)$ (we proceed by induction in the number of generators). Let $\alpha = \alpha_1, \ldots, \alpha_m$ and $\beta = \beta_1, \ldots, \beta_n$ be the conjugates of α and β. The common roots of $\mu_\beta(x)$ and $\mu_\alpha(\theta - cx)$ are β_j such that $\theta - c\beta_j = \alpha_i$ for some i. Choose c so that $\alpha + c\beta \neq \alpha_i + c\beta_j$ for $(i, j) \neq (1, 1)$. Then β is the only root of the above polynomials, and since $\mu_\beta(x)$ has no multiple roots (see the remark after (13)) we have

$$\big(\mu_\beta(x), \mu_\alpha(\theta - cx)\big) = x - \beta \in \mathbb{Q}(\theta)[x].$$

Thus, $\beta \in \mathbb{Q}(\theta)$, and so $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$. □

In practice it occurs simpler to use several generators but of simpler nature.

Problem 14. Describe all inclusions of the fields $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$.

Let us prove that the function (20) has the required features. The linearity of the trace follows from the linearity of inclusions. Let us prove (18). Suppose $\alpha \in L$. By Theorem 4 $\alpha = f(\theta)$, where $f \in \mathbb{Q}[x]$. Furthermore $\varphi_j(\alpha) = \varphi_j(f(\theta)) = f(\varphi_j(\theta))$ which equals $f(\theta_j)$ by Theorem 3. Thus

$$\prod_{j=1}^{n}(x - \varphi_j(\alpha)) = \prod_{j=1}^{n}(x - f(\theta_j)) \overset{\text{Th.5}}{=} \mu_{f(\theta)}(x)^d = \mu_\alpha(x)^d,\ d \in \mathbb{N}. \tag{22}$$

Equate the sums of roots (with multiplicities) of polynomials in the left and right sides to get (18).

II approach (linear algebra only)

The trace $\operatorname{tr} A$ of a square matrix $A = (a_{ij})$ is the sum of its diagonal elements, $\operatorname{tr} A = \sum_i a_{ii}$. A straightforward checking shows that $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ for matrices A and B of the same size. This implies that the trace of the matrix of an operator is independent of the choice of a basis: $\operatorname{tr}(C^{-1}AC) = \operatorname{tr}(C^{-1}CA) = \operatorname{tr}(A)$. It is called the trace of the operator.

From [4, Theorems 8 and 9] it follows that the extensions generated by a finite number of algebraic elements are just the finite extensions, that is, the extensions of finite dimension. (By the way, this is one more way to understand why $\mathbb{A}$ is a field.) The degree of a finite extension $L \supseteq K$ is denoted $[L : K]$. So let $L \supseteq \mathbb{Q}$ be any finite extension, $L \subset \mathbb{C}$. Suppose $\alpha \in L \subset \mathbb{C}$. The trace of a linear operator $L \to L$, $x \mapsto \alpha x$, is called the trace of the number α and is denoted $\operatorname{tr}^L_{\mathbb{Q}}(\alpha)$, or $\operatorname{tr}(\alpha)$ if the extension $L \supseteq \mathbb{Q}$ is fixed.

Example 13. The matrix of multiplication by $\sqrt[3]{2}$ in the basis $1, \sqrt[3]{2}, \sqrt[3]{4}$ of the extension $\mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$ is of the form $A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ because $1 \mapsto \sqrt[3]{2} \mapsto \sqrt[3]{4} \mapsto 2$. Hence $\operatorname{tr}(\sqrt[3]{2}) = \operatorname{tr} A = 0$.

Clearly $\operatorname{tr}(\alpha)$ depends of α linearly. We will specify the sense of the factor d in (18) and prove the formula

$$\boxed{\operatorname{tr}(\alpha) = [L : \mathbb{Q}(\alpha)]\sigma(\alpha),\ \alpha \in L.} \tag{23}$$

For this, let us choose a suitable basis in $L/\mathbb{Q}$. We retain the notation (21). Then $1, \alpha, \dots, \alpha^{m-1}$ form a basis in $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}$. Take any basis $e_1, \dots, e_d$ in the extension $L \supseteq \mathbb{Q}(\alpha)$. By [4, Tower theorem 9]

$$\underbrace{e_1, e_1\alpha, \dots, e_1\alpha^{m-1}}_{\text{1st block}}, \dots, \underbrace{e_d, e_d\alpha, \dots, e_d\alpha^{m-1}}_{d\text{th block}}$$

form a basis in $L \supseteq \mathbb{Q}$. Under multiplication by α the vectors of ith block transform according to the rule

$$e_i \mapsto e_i\alpha \mapsto e_i\alpha^2 \mapsto \dots \mapsto e_i\alpha^{m-1} \mapsto e_i\alpha^m = e_i(c_0 + c_1\alpha + \dots + c_{m-1}\alpha^{m-1}).$$

Hence in this basis the matrix of multiplication by α is block diagonal with d identical blocks

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & c_0 \\ 1 & 0 & 0 & \dots & 0 & c_1 \\ 0 & 1 & 0 & \dots & 0 & c_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & c_{m-2} \\ 0 & 0 & 0 & \dots & 1 & c_{m-1} \end{pmatrix}$$

and its trace equals dc_{m-1}. Since $d = [L : \mathbb{Q}(\alpha)]$ and $c_{m-1} = \sigma(\alpha)$, the formula (23) is proven. Observe that it also follows from (22):

$$d = \frac{n}{\deg \mu_\alpha(x)} = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = [L : \mathbb{Q}(\alpha)].$$

Thus two above definitions of the trace are equivalent.

In conclusion observe that $\mu_\alpha(x)$ is the minimal polynomial for the operator of multiplication by α, and $\mu_\alpha(x)^d$ is its characteristic polynomial.

References

[1] *E. B. Vinberg.* A course of algebra (in Russian). M.: MCCME. 2019.

[2] *L. Kamnev.* Irrationality of the sum of radicals (in Russian). Kvant, 1972, #2.

[3] *A. Kanunnikov.* Algebra and geometry of complex numbers (in Russian). Kvant, 2017, #5, 6.

[4] *A. L. Kanunnikov.* Algebraic numbers as vectors (in Russian). // Matematicheskoye prosveshcheniye. Ser. 3. Iss. 26. M.: MCCME. 2020. P. 91–122.

[5] *V. Oleynikov.* Irrationality and irreducibility (in Russian). // Kvant, 1986, #10.

[6] *V. A. Ufnarovsky.* Mathematical aquarium (in Russian). M.: MCCME. 2010.

[7] *I. Richards.* An Application of Galois Theory to Elementary Arithmetic. Advances in Mathematics 13, p. 268–273. 1974.

Solutions of the problems

1. All three sums of radicals are irrational because all radicals and their ratios in each sum are irrational by Lemma 1. For the radical $\sqrt[17]{2021!}$ in the last sum it suffices to observe that the prime $p = 2011$ appears in the decomposition of 2021! with exponent 1.

2. a) One tuple is obtained from another using multiplication by some radical, for instance,

$$(\sqrt{5}, \sqrt{10}, \sqrt{15}, \sqrt{30}) = \sqrt{5}(1, \sqrt{2}, \sqrt{3}, \sqrt{6}).$$

b) To draw a hypercube, first draw a 3-dimensional cube placing a square inside another square and connecting the corresponding vertices (fig. 1a). (This is top view of a cube made of jelly and deformed falling on the table.) Now we draw similarly a cube inside another cube and connect the corresponding vertices to obtain a hypercube. The radicals on the inner cube are already indicated at fig. 2b. Multiply these by $\sqrt{7}$ to obtain the radicals for the corresponding vertices of the outer cube.

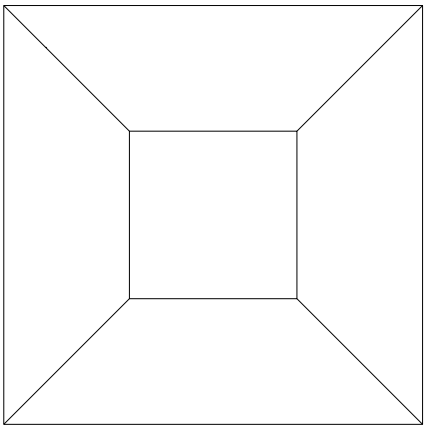


Fig. 1a

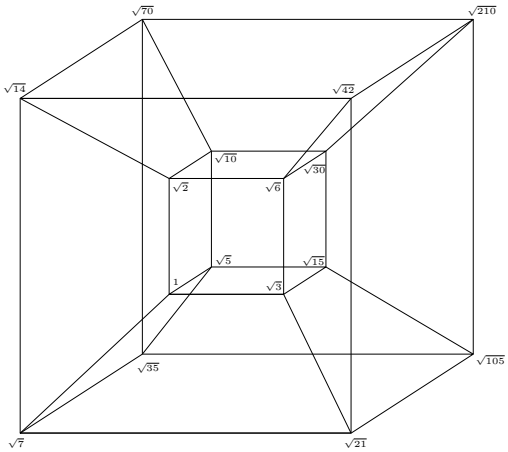


Fig. 1b

3. $1 \Rightarrow 2$. Apply Theorem 1 to $\{Q_1, \ldots, Q_N\} = \{r_1^{l_1} \ldots r_n^{l_n} \mid 0 \leqslant l_1, \ldots, l_n < k\}$ and $k_1 = \ldots = k_N = k$. The condition $\sqrt[k]{Q_i/Q_j} \notin \mathbb{Q}$ for $i \neq j$ holds by Lemma 1.

$2 \Rightarrow 1$. Let $p_1, \ldots, p_n$ be prime divisors of the numerators and denominators in the irredundant representation of $Q_1, \ldots, Q_N$ and $k = k_1 \ldots k_N$. Then $\sqrt[k_i]{Q_i} = \sqrt[k]{Q_i^{k/k_i}}$ is proportional with a rational coefficient to a number of the form $\sqrt[k]{p_1^{l_1} \ldots p_n^{l_n}}$, where $0 \leqslant l_1, \ldots, l_n < k$.

4. a) For zero we can take any nonzero coefficient, and for proportional numbers kx and lx $(0 \neq k, l \in K)$ we can take the coefficients l and $-k$ respectively. Take the zero coefficients for the other elements of the system to get a zero linear combination with not only zero coefficients.

b) Suppose the system $x_1, \ldots, x_m, x_{m+1}, \ldots, x_n$ is linearly independent over K and $a_1x_1 + \ldots + a_mx_m = 0$. Then $a_1x_1 + \ldots + a_mx_m + 0x_{m+1} + \ldots + 0x_n = 0$ implies $a_1 = \ldots = a_m = 0$.

c) If $x \in K$ then put $a = x$ and $b = -1$ in $a \cdot 1 + b \cdot x = 0$ to obtain that 1 and x are linearly dependent over K. Conversely, if $x \notin K$ then $a \cdot 1 + b \cdot x = 0$ with $a, b \in K$ implies $b = 0$ (otherwise $x = -a/b \in K$) and hence $a = 0$.

d) If $a_1x_1+\ldots+a_nx_n = b_1x_1+\ldots+b_nx_n$ with $a_1, b_1, \ldots, a_n, b_n \in K$ then $(a_1-b_1)x_1+\ldots+(a_n-b_n)x_n = 0$. Linear independence of $x_1, \ldots, x_n$ is equivalent to the equalities $a_1 - b_1 = \ldots = a_n - b_n = 0$.

5. Suppose the theorem is proven for $n-1$ primes, and $\sqrt{p_n} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. By induction, each number in this field is uniquely expressed as a sum of 2^{n-1} summands of the form $a\sqrt{p_1}^{l_1} \ldots \sqrt{p_{n-1}}^{l_{n-1}}$, $a \in \mathbb{Q}$, $l_i = 0, 1$. The number $\sqrt{p_n}$ is equal to a sum of numbers of this form but not equal to any of them by Lemma 1. Thus the sum contains at least two summands, so some radical among $\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}$ appears in some summand and does not appear in another summand. Let this radical be $\sqrt{p_{n-1}}$. Then $\sqrt{p_n} = A + B\sqrt{p_{n-1}}$ where $A, B \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-2}}) = K$ with $AB \neq 0$. Square this equality: $p_n = A^2 + B^2p_{n-1} + 2AB\sqrt{p_{n-1}}$ to get $AB = 0$, a contradiction.

6.The core of the matter is the definition of a conjugate. In *each specific* field $K(\sqrt{d})$ conjugation is defined by the formula $f_d(a + b + \sqrt{d}) = a - b\sqrt{d}$ $(a, b \in K)$. This is correct: a, b are uniquely determined since $\sqrt{d} \notin K$. But we may not equate conjugate related to distinct fields: if $\alpha = a + b\sqrt{d} = a' + b'\sqrt{d'}$ then why $f_d(\alpha) = a - b\sqrt{d}$ must equal $f_{d'}(\alpha) = a - b\sqrt{d'}$?

The definition in question may be understood so that if α is represented as $a + b\sqrt{d}$ with $a, b, d \in K$, $\sqrt{d} \notin K$, then let the conjugate to α be equal to $a - b\sqrt{d}$. But then the implication

$$a + b\sqrt{d} = a' + b'\sqrt{d'} \implies a - b\sqrt{d} = a' - b'\sqrt{d'}$$

is nothing but verification of correctness of this definition!

The solution is to define conjugates in an invariant way not related to a specific expression in the form of a quadratic irrationality. Namely, let $\alpha \notin K$be a root of a polynomial of degree 2 over K. Then define the conjugate for α as the second root of this polynomial. Correctness of this definition reduces to obvious verification of uniqueness of this polynomial up to a number factor. Indeed, if $x^2 + px + q$ and $x^2 + p'x + q'$ are two polynomials with a root α over K then their difference $(p - p')x + q - q' \in K$ also has the root α whence $p = p'$ (otherwise $\alpha = \frac{q'-q}{p-p'} \in K$) and moreover $q = q'$. In fact the conjugates in general situation are defined just in this way.

7. The idea is to pass to conjugate numbers: $(a - b\sqrt{2})^2 + (c - d\sqrt{2})^2 = 7 - 5\sqrt{2} < 0$, a contradiction. The conceptual motivation of this transition is in verifying that the conjugation $f(a + b\sqrt{2}) = a - b\sqrt{2}$ $(a, b \in \mathbb{Q})$ is an inclusion (see definition at p. 9).

8. Sum up the given number and its conjugate: $(6 + \sqrt{35})^{1000} + (6 - \sqrt{35})^{1000}$. This sum is integer (by the formula for the Newton binomial). On the other hand, the conjugate is very small:

$$(6 - \sqrt{35})^{1000} = \frac{1}{(6 + \sqrt{35})^{1000}} < \frac{1}{10^{1000}}.$$

Hence the first 1000 digits of the original number are 9.

9. Consider 2^{99} polynomials $1 + \varepsilon_2x_2 + \ldots + \varepsilon_{100}x_{100}$, where $\varepsilon_i \in \{\pm 1\}$. Their product is a polynomial even in each variable, so it has the form $f(x_2^2, \ldots, x_{100}^2)$, where f is a polynomial with integer coefficients. In particular, for $x_2 = \sqrt{2}$, …, $x_{100} = \sqrt{100}$ we obtain an integer which we will denote by d. Now repeat the argument for the opposite by sign polynomials $-1 + \varepsilon_2x_2 + \ldots + \varepsilon_{100}x_{100}$ to obtain the same integer d (because the number of polynomials is even). Thus the product in question is equal to d^2.

10. a) $\frac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}} = \frac{1}{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}} = \frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{(1+\sqrt{2})^2-3(\sqrt{2}-1)^2} = \frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{8\sqrt{2}-6} = \frac{\left(1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}\right)(4\sqrt{2}+3)}{46}$.

b) Answer: $\frac{1}{7}\left(3\sqrt[4]{27} + 8\sqrt[4]{9} + 5\sqrt[4]{3} + 8\right)$.

11. $m = k^5$, $n = (2021 - k)^5$, $k = 1, \ldots, 2020$. The solution is similar to Example 7.

12. Divide both parts by $\sqrt[3]{2}$: $\mathrm{C}\sqrt[6]{3/4} = a + b\sqrt[6]{2}$. Now the contradiction is obtained similarly to Example 7.

13. We will prove a general statement.

Lemma 6. *Let K be a subfield in $\mathbb{C}$, $r \in \mathbb{C} \setminus K$, $r^2 \in K$. Then all the inclusion $K(r) \to \mathbb{C}$ over K (that is, identical on K) are of the form $a + br \mapsto a \pm br$.*

Proof. Clearly $K(r) = \{a + br \mid a, b \in K\}$ and each inclusion $\varphi\colon K(r) \to \mathbb{C}$ over K is determined by its value at r. Moreover $\varphi(r)^2 = \varphi(r^2) = r^2$, whence $\varphi(r) = \pm r$. For the plus sign we get an identical inclusion, and for the minus sign we get an analogue of the complex conjugation ($K = \mathbb{R}$, $r = i$): $\varphi(a + br) = a - br$. This is an inclusion over K: the properties $\varphi(x + y) = \varphi(x) + \varphi(y)$ and $\varphi(k) = k$ for $k \in K$ are obvious. Furthermore

$$\varphi((a+br)(c+dr)) = \varphi(ac+bdr^2+(ad+bc)r) = ac+bdr^2-(ad+bc)r = (a-br)(c-dr) = \varphi(a+br)\varphi(c-dr)$$

for all $a, b, c, d \in K$. □

a) Apply Lemma 6 for $K = \mathbb{Q}$ and $r = i$; $\operatorname{tr}(1+i) = (1+i) + (1-i) = 2$.

b) Denote $\varepsilon = \frac{1+i}{\sqrt{2}}$. Since $\varepsilon^2 = i$, we have $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\varepsilon, i) = \mathbb{Q}(\sqrt{2}, i)$. For any inclusion of the field $\mathbb{Q}(\sqrt{2}, i)$ we have$\sqrt{2} \mapsto \pm\sqrt{2}$ and $i \mapsto \pm i$. All combinations of signs are given by 4 inclusions: identical φ_{++}, inclusions from Lemma 6:

$$\varphi_{+-}\colon a + bi \mapsto a - bi, \qquad a, b \in \mathbb{Q}(\sqrt{2})$$
$$\varphi_{-+}\colon a' + b'\sqrt{2} \mapsto a' - b'\sqrt{2}, \quad a', b' \in \mathbb{Q}(i),$$

and their composition $\varphi_{--} = \varphi_{+-} \circ \varphi_{-+}$. Hence $\operatorname{tr}(1+i) = (\varphi_{++} + \varphi_{+-} + \varphi_{-+} + \varphi_{--})(1+i) = 4$.

Observe that the images of ε under all inclusions form the set of conjugates $\left\{\frac{1\pm i}{\pm\sqrt{2}}\right\} = \{\varepsilon, \varepsilon^3, \varepsilon^5, \varepsilon^7\}$ that are the roots of $\mu_\varepsilon(x) = x^4 + 1$. These are the primitive roots of degree 8 from 1 (fig. 2).

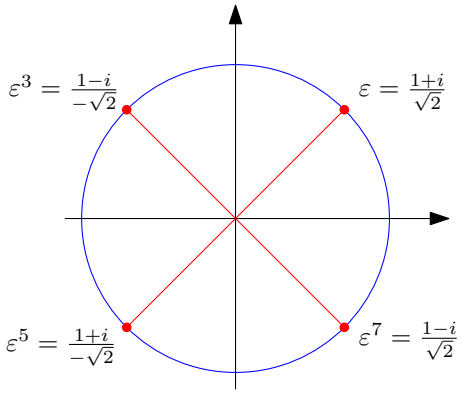


Fig. 2

14. Similarly to the solution of Problem 13b) we obtain 4 inclusions of the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ such that $\sqrt{2} \mapsto \pm\sqrt{2}$ and $\sqrt{3} \mapsto \pm\sqrt{3}$. Each of these extends to an inclusion of the field $K(\sqrt{5})$ in two ways: $\sqrt{5} \mapsto \pm\sqrt{5}$ (similarly by Lemma 6 take three inclusions that change the sign of a radical, and form all possible 2^3 combinations of them).

Now let us describe the inclusions of $L = \mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$. Put $r = \sqrt[12]{2}$. Then $\sqrt[4]{2} = r^3$, $\sqrt[6]{2} = r^2$ and $L = \mathbb{Q}(r^3, r^2) = \mathbb{Q}(r)$. By Example 5 we have $\mu_r(x) = x^6 - 2$, so by Theorem 3 all inclusions $\varphi_0, \ldots, \varphi_5$of the field $\mathbb{Q}(r)$ are defined by the conditions $\varphi_j\colon r \mapsto r\varepsilon^j$, where $\varepsilon = \frac{1+i\sqrt{3}}{2} \in \sqrt[6]{1}$.