SOLVING EQUATIONS USING ONE RADICAL

presented by D. Akhtyamov[1], I. Bogdanov[2], A. Glebov[3], A. Skopenkov[4], E. Streltsova[5], and A. Zykin[6]

This project is devoted to several classical results and methods in pure mathematics which are also interesting from the point of view of computer science (related to symbolic computations). The main problems of the project are 3.3.d, 4.2, 5.5.c, 6.7, and 6.17.bc. The principal difference of this set of problems from standard textbooks in this topic is that we do not use the notion of the Galois group (and even the notion of group). Despite of the lack of these *words*, the *ideas* of the proofs presented below are starting points for the Galois theory [S09] and the *constructive Galois theory* [E].

We suggest to all the students working on the project to *consult* with the jury on any questions on the project, or on ideas of the solutions. Their results may be used as sources of talks on the students' conferences, e.g., [M].

The students who work on the project well enough will get several *extra problems*.

A student (or a group of students) working on this project get a "star" for every solution which has been written down and marked with either '+' or '+.'. The jury may also award extra stars for beautiful solutions, solutions of hard problems, or (some) solutions typeset in TEX. The jury has infinitely many stars. One may submit a solution in oral form, but he loses a star with each attempt.

We will tell the solutions of 1.1.ab, 1.2.ab, 1.4.ab, 1.5.a, 2.1.a″f, 2.3.abcd, 3.1.a, 3.2.a, 4.1.a, 5.1.a, 5.2.a, and 5.4.ab at the initial presentation; thus you may submit the solutions of these problems only before this presentation (but you may make this in oral form without loss of stars).

If a problem looks just like a statement, a proof of this statement is required in this problem. If you are stuck on a certain problem, we suggest to try looking at the next ones. They may turn out to be helpful.

We denote the set of rational numbers by $\mathbb{Q}$. A 'polynomial with rational coefficients' is referred to merely as *polynomial*. A polynomial is *irreducible* over a set F, if it cannot be decomposed as a product of polynomials of lower degrees with coefficients in F.

Problems before the Semifinal

1 Solving equations of degree 3 and 4

1.1. (a) Solving an equation $ax^3 + bx^2 + cx + d = 0$ can be reduced by substitution of variable to solving an equation of the form $x^3 + px + q = 0$.

(b) Solving an equation $ax^4 + bx^3 + cx^2 + dx + e = 0$ can be reduced by a substitution of variable to solving an equation of the form $x^4 + px^2 + qx + r = 0$.

In the next two problems, we allow to use without proof the *Intermediate value theorem* for polynomials: *If a polynomial P satisfies $P(a) > 0$ and $P(b) < 0$ for some $a < b$, then there exists a real number $c \in [a, b]$ such that $P(c) = 0$.*

1.2. Find the number of real roots of the equation

(a) $x^3 + 2x + 7 = 0$; (b) $x^3 - 4x - 1 = 0$.

[1]Saint-Petersburg State University

[2]Moscow Institute of Physics and Technology

[3]Novosibirsk State University

[4]Supported by the D. Zimin's "Dynasty" fund; Moscow Institute of Physics and Technology, Independent Moscow University; www.mccme.ru/~skopenko

[5]Moscow State University

[6]National Research University "Higher School of Economics"

1.3. (a) Which relations on p and q are equivalent to the condition that the equation $x^3+px+q=0$ has exactly two roots?

(b) Under these relations, express the roots in terms of p and q.

(c) Find the number of real roots of $x^3+px+q=0$ in terms of the values of p and q.

Hereafter, 'to solve an equation' always means 'to find *all* its *real* roots'. However, we recommend also to find all the complex roots as well.

1.4. (a) Prove that $\sqrt[3]{2+\sqrt{5}}-\sqrt[3]{\sqrt{5}-2}=1$.

(b) Find at least one root of the equation $x^3-3\sqrt[3]{2}x+3=0$.

Hint: del Ferro's method. Since $(b+c)^3=b^3+c^3+3bc(b+c)$, the number $x=b+c$ satisfies the equation $x^3-3bcx-(b^3+c^3)=0$.

(c) Solve the equation $x^3-3\sqrt[3]{2}x+3=0$.

(d)* Solve the equation $x^3-3x-1=0$.

1.5. (a) Factor the expression $a^3+b^3+c^3-3abc$.

(b) Decompose $a^3+b^3+c^3-3abc$ into a product of linear factors with complex coefficients.

1.6. (a) Formulate and prove a theorem describing all real roots of the equation $x^3+px+q=0$ in a case when del Ferro's method (see problem 1.4) allows to obtain all of them. Under which relations on p and q this method it applicable, if we allow taking square roots only of positive numbers?

(b) The same question for finding all complex roots.

1.7. Solve the equation (a) $(x^2+2)^2=18(x-1)^2$;

(b) $x^4+4x-1=0$; (c) $x^4+2x^2-8x-4=0$; (d) $x^4-12x^2-24x-14=0$.

Hint to 1.7.b: Ferrari's method. Find numbers α, b, c such that

$$x^4+4x-1=(x^2+\alpha)^2-(bx+c)^2.$$

For this purpose, one may search for a value of α such that the trinomial $(x^2+\alpha)^2-(x^4+4x-1)$ is a square of a linear function. To that end, find the discriminant of this trinomial. (This discriminant is a cubic polynomial in α; it is called the *cubic resolution* of the polynomial $x^4+4x-1=0$.)

2 Representability with use of only one radical

2.1. Determine whether the following number can be represented in the form $a+\sqrt{b}$ with $a,b\in\mathbb{Q}$:

(a) $\sqrt{3+2\sqrt{2}}$; (a′) $\sqrt{2+\sqrt{2}}$; (a″) $\dfrac{1}{7+5\sqrt{2}}$; (b) $\sqrt[3]{\sqrt{5}+2}-\sqrt[3]{\sqrt{5}-2}$;

(c) $\sqrt[3]{7+5\sqrt{2}}$; (d) $\cos(2\pi/5)$; (e) $\sqrt[3]{2}$; (f) $\sqrt{2}+\sqrt[3]{2}$; (g) $\cos(2\pi/9)$; (h)* $\cos(2\pi/7)$.

2.2. The number $\cos(2\pi/9)$ is a root of the polynomial $8x^3-6x+1$.

2.3. Assume that $r\in\mathbb{R}\setminus\mathbb{Q}$ is chosen so that $r^2\in\mathbb{Q}$.

(a) *Irreducibility Lemma.* The polynomial x^2-r^2 is irreducible over $\mathbb{Q}$.

(b) *Linear Independence Lemma.* If $a+br=0$ with $a,b\in\mathbb{Q}$, then $a=b=0$.

(c) If r is a root of some polynomial, then this polynomial is divisible by x^2-r^2.

(d) **Conjugation Theorem.** *If r is a root of a polynomial, then $-r$ is also its root.*

(e) *Corollary.* If a polynomial has a root $a+br$ with $a,b\in\mathbb{Q}$, then $a-br$ is also a root of this polynomial.

(f) *Corollary.* If a cubic polynomial has a root of the form $a+br$ with $a,b\in\mathbb{Q}$, then this polynomial has a rational root.

2.4. Proposition. *If a polynomial of degree at least 3 is irreducible over $\mathbb{Q}$, then none of its roots has the form $a\pm\sqrt{b}$ with $a,b\in\mathbb{Q}$.*

2.5. Determine whether the following number can be represented in the form $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ with $a, b, c \in \mathbb{Q}$:

(a) $\sqrt{3}$; (a′) $\dfrac{1}{1+5\sqrt[3]{2}+\sqrt[3]{4}}$; (b) $\cos(2\pi/9)$; (c) $\sqrt[5]{3}$; (d) $\sqrt[3]{3}$;

(e) the least positive root of $x^3-4x+2=0$;

(f)* the unique real root of $x^3-6x-6=0$;

(g)* the unique real root of $x^3-9x-12=0$.

Hereafter, we use the notation

$$\varepsilon_q = \cos\frac{2\pi}{q} + i\sin\frac{2\pi}{q}.$$

2.6. Assume that $r \in \mathbb{R}\setminus\mathbb{Q}$ is chosen so that $r^3 \in \mathbb{Q}$.

(a) *Irreducibility Lemma.* The polynomial x^3-r^3 is irreducible over $\mathbb{Q}$.

(b) *Linear Independence Lemma.* If $a+br+cr^2=0$ with $a, b, c \in \mathbb{Q}$, then $a=b=c=0$.

(c) If r is a root of a polynomial, then this polynomial is divisible by x^3-r^3.

(d) **Conjugation Theorem.** *If r is a root of a polynomial, then the numbers $\varepsilon_3 r$ and $\varepsilon_3^2 r$ are also its roots.*

(e) *Corollary.* If a polynomial has a root $x_1=a+br+cr^2$ with $a, b, c \in \mathbb{Q}$, then the numbers

$$x_2 = a+b\varepsilon_3 r + c\varepsilon_3^2 r^2 \quad \text{and} \quad x_3 = a+b\varepsilon_3^2 r + c\varepsilon_3 r^2$$

are also its roots.

(a′) *Strong Irreducibility Lemma.* The polynomial x^3-r^3 is irreducible over

$$\mathbb{Q}[\varepsilon_3] = \{x+y\varepsilon_3 \colon\ x, y \in \mathbb{Q}\}.$$

(b′) *Strong Linear Independence Lemma.* If $k, \ell, m \in \mathbb{Q}[\varepsilon_3]$ satisfy $k+\ell r+mr^2=0$, then $k=\ell=m=0$.

2.7. Assume that $r \in \mathbb{R}\setminus\mathbb{Q}$ and $a, b, c, r^3 \in \mathbb{Q}$.

(a) *Rationality Lemma.* The number $a+br+cr^2$ is a root of some cubic polynomial.

(b) **Proposition.** *Assume that an irrational number $a+br+cr^2$ is a root of a polynomial which is irreducible over $\mathbb{Q}$; then this polynomial is cubic and it has exactly one real root.*

3 Equations of degree 3 solvable using one radical

Initially, Cheburashka gets a number 1. To the numbers he already has got before, he can apply addition, subtraction, multiplication, and division (by a non-zero number) for free. Moreover, for one yuan Cheburashka can extract an arbitrary degree root of a positive number which he already has got during the calculations. All other operations are out of his reach. But he performs the allowed operations with absolute precision, and he has an unbounded memory.

3.1. (a) Help Cheburashka in obtaining $\sqrt[3]{2}+\sqrt[3]{4}$ for 1 yuan.

(b) Help Cheburashka in obtaining $\sqrt[3]{2+\sqrt{3}}+\sqrt[3]{2-\sqrt{3}}$ for 2 yuans.

(c) Help Cheburashka in obtaining $\dfrac{1}{1+5\sqrt[3]{2}+\sqrt[3]{4}}$ for 1 yuan, if the operation of division is prohibited, but he may use all rational numbers for free.

3.2. (a) A number can be obtained for 1 yuan paid for extracting a square root, if and only if the number has the form $a\pm\sqrt{b}$ with $a, b \in \mathbb{Q}$.

(b) A number can be obtained for 1 yuan paid for extracting a cubic root, if and only if the number has the form $a+br+cr^2$ with $r \in \mathbb{R}$ and $a, b, c, r^3 \in \mathbb{Q}$.

(c) **Calculator Theorem.** *A number can be obtained for 1 yuan, if and only if the number has the form $A(r)$, where A is a polynomial and r is a real number such that $r^n \in \mathbb{Q}$ for some positive integer n.*

3.3. (a) Present some nonzero rational numbers p and q such that Cheburashka can obtain one of the roots of $x^3 + px + q = 0$ for 1 yuan.

(a′) Present some nonzero rational numbers p and q such that the polynomial $x^3 + px + q$ has no rational roots, but Cheburashka still can obtain one of its roots for 1 yuan.

(b3) Can Cheburashka obtain at least one root of $x^3 + 3x + 6 = 0$ for 3 yuans?

(b2) . . . for 2 yuans?

(b1)* . . . for 1 yuan?

(c) If an equation of degree 3 with rational coefficients has exactly one real root, then Cheburashka can obtain this root for 2 yuans.

(d)* **Main problem.** Given rational p and q, determine whether Cheburashka can obtain at least one root of the equation $x^3 + px + q = 0$ for 1 yuan.

3.4. * (a) Does there exist a cubic equation with rational coefficients such that Cheburashka cannot get any of its roots for 2 yuans?

(b) The same question about 10000 yuans.

Let us reformulate the previous problems using mathematically precise language. Consider a calculator with the following buttons:

$$1, \quad +, \quad -, \quad \times, \quad : \quad \text{and} \quad \sqrt[n]{} \quad \text{for every } n.$$

The calculator has absolute precision and unlimited memory. It returns an error if division by 0 is carried out.

Assume first that the calculator is *real*, i.e. that it works only with real numbers; so extracting an even degree root of a negative number results in an error.

Here are mathematically rigorous (and slightly modified) statements of the problems 3.3.cd and 3.4.

Proposition on Solvability in real radicals. *If a cubic polynomial with rational coefficients has precisely one real root, this root can be obtained using the real calculator.*

Moreover, this can be done by extracting roots only twice, once of the second and once of the third degree.

Theorem on Insolvability in real radicals. *There exists a cubic polynomial with rational coefficients (e.g. x^3-3x+1) such that none of its roots can be obtained using the real calculator.*

Moreover, if a cubic polynomial with rational coefficients has three distinct real roots, then none of these roots can be obtained with the real calculator.

Notice here that if there are exactly two roots, then they are both rational (cf. problem 1.3.ab).

Question. *How can one decide whether the cubic polynomial with rational coefficients has a root which can be obtained on the calculator using the radical sign only once? Is there an algorithm deciding whether a polynomial belongs to the described class?*

4 Equations of degree 4 solvable using one radical

We say that a polynomial is *k-solvable* if one of its roots can be obtained by using the real calculator with extracting at most k roots.

4.1. (a) Assume that a biquadratic polynomial (of degree 4) has a real root. Is this polynomial necessarily 2-solvable?

(b)* Given rational p and s, determine whether the polynomial $x^4 + px^2 + s$ is 1-solvable.

(c)* Is every quartic polynomial having a real root 4-solvable?

4.2. Main problem. $(4, 1)$ Given a polynomial $x^4 + px^2 + qx + s = 0$ with rational coefficients, determine whether it is 1-solvable.

Is there an algorithm for deciding 1-solvability?

$(4,2)$ *(The jury does not know a solution)* The same question for 2-solvability.

(n) *(The jury does not know a solution for any $n \geq 4$)* Given a polynomial of degree n with rational coefficients, determine whether it is ∞-solvable?

Is there an algorithm for deciding ∞-solvability?

(n,k) *(The jury does not know a solution)* Given a polynomial of degree n with rational coefficients, determine whether it is k-solvable?

Is there an algorithm for deciding k-solvability?

4.3. (a) Present rational numbers p, q, and s such that $qs \neq 0$ and that the polynomial $x^4 + px^2 + qx + s$ is irreducible over $\mathbb{Q}$ and 1-solvable.

(b) Determine whether the polynomial $x^4 - 6x^2 + 72x - 99$ is 1-solvable.

4.4. Assume that $p < 0$ and that the cubic resolution of the polynomial $x^4 + px^2 + qx + s$ has a root $\alpha \in \mathbb{Q}$ such that $-p > 2\alpha > p$. Prove that this polynomial is 2-solvable (on the real calculator).

4.5. If a degree 4 polynomial irreducible over $\mathbb{Q}$ has a root that can be obtained using real calculator by extracting only one root, and this extraction provides a root of degree 4, then the cubic resolution of the polynomial has a rational root.

4.6. Formulate and prove the analogues of the Conjugation Theorems 2.3.d and 2.6.d for degree 4 polynomials.

5 Formal expressibility in real radicals

The priority goal of the first problem in this section is to formalize the notion of 'to determine'. We give such a formalization after the problem statement. So you have a chance to approach the basic definition starting from simple examples. The solutions themselves should not be difficult for you.

5.1. (a) Given $x + y$ and xy, is it always possible to determine $x - y$? To determine x?

The primary formalization of the notion 'to determine' in the problem above can be given in the following way: *does there exist a mapping $f : \mathbb{R}^2 \to \mathbb{R}$ such that $f(x + y, xy) = x - y$ for all $x, y \in \mathbb{R}$?*[7]

(b) Given $x+y+z$, $xy+yz+zx$ and xyz, is it always possible to determine $(x-y)(y-z)(z-x)$?

(The formalization is similar to that in (a).)

The basic definition in this text is yet another formalization of the notion 'to determine'.

Definition. A polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$ is **expressible in real radicals via the collection of polynomials** $a_1, \ldots, a_t \in \mathbb{R}[x_1, \ldots, x_n]$, if one can append f to this collection by a sequence of operations of the following types:

• if several polynomials $b_1, \ldots, b_k$ are already in the collection and $F \in \mathbb{R}[t_1, \ldots, t_k]$ is an arbitrary polynomial, then it is allowed to append the polynomial $F(b_1, b_2, \ldots, b_k)$ to the collection;

• if some polynomial in the collection has the form p^k for some $p \in \mathbb{R}[x_1, \ldots, x_n]$ and integer $k > 1$, then one may append p to the collection.

[7] Another formalization of the notion 'to determine' which is not further used is as follows: *does there exist a mapping f from $\mathbb{R}^2$ to the set $2^{\mathbb{R}}_{fin}$ of all finite subsets of $\mathbb{R}$ such that $f(x + y, xy) \ni x - y$ for all $x, y \in \mathbb{R}$?* Let us show that this question (together with its generalizations to several variables) is trivial.

Mappings $f : \mathbb{R}^2 \to 2^{\mathbb{R}}_{fin}$ (i.e. real finite-valued functions of $\mathbb{R}^2$) may be defined by formulae. For example, the formula $f(x) = \pm x$ is a reduction of the formula $f(x) = \{x, -x\}$ which defines the (at most)-2-valued mapping f. (*Exercise:* Establish how-many-valued mapping is defined by the formula $f(x) = \frac{\pm x}{\pm x}$.) Denote by $f(p, q)$ the (finite) set of (real) solutions of the equation $t^2 + pt + q = 0$. Then the formula $x - y = f(x+y, xy) - f(x+y, xy)$ defines the desired mapping (Why?).

For example, if a collection contains x^2+2y and $x-y^3$, then one may apply the first operation in order to append the polynomial $-5(x^2+2y)^2+3(x^2+2y)(x-y^3)^6$; moreover, if a collection already contains $x^2-2xy+y^2$, then applying the second operation one may append $x-y$ and $y-x$.

5.2. Determine if the following polynomial is expressible in real radicals via $x+y$ and xy:
(a) $x-y$; (b) x.

The answer to 5.2.b shows that *the root of a quadratic equation is expressible in real radicals via its coefficients.* The formalization of this statement will be given later in problem 6.17.

5.3. (a,b,c) Represent

$$x^2+y^2+z^2, \quad x^2y+y^2z+z^2x+x^2z+z^2y+y^2x, \quad x^3+y^3+z^3$$

as polynomials in

$$\sigma_1=x+y+z, \quad \sigma_2=xy+yz+zx \quad \text{and} \quad \sigma_3=xyz.$$

(d) Is $(x^8y+y^8z+z^8x)(x^8z+z^8y+y^8x)$ representable as a polynomial in $\sigma_1,\sigma_2,\sigma_3$?

5.4. (a) The multi-degree of the product of polynomials (in several variables) is the sum of their multi-degrees.

(b) We say that a polynomial f in two variables x,y is *symmetric* if the polynomials $f(x,y)$ and $f(y,x)$ are equal. Prove that every symmetric polynomial in two variables x,y is a polynomial in $x+y$ and xy.

(c) We say that a polynomial f in three variables x,y,z is *symmetric* if the polynomials $f(x,y,z)$, $f(y,z,x)$ and $f(y,x,z)$ are equal. Prove that every symmetric polynomial in three variables x,y,z is a polynomial in σ_1, σ_2 and σ_3.

(d) Formulate and prove the main theorem about symmetric polynomials in n variables.

5.5. Determine whether the following polynomial is expressible in real radicals via $\sigma_1,\sigma_2,\sigma_3$:
(a) $(x-y)(y-z)(z-x)$; (b) $x^2y+y^2z+z^2x$. (c)* x?

Hints and Solutions for the initial presentation

1.1. Use the substitution (a) $y = x + \frac{b}{3a}$ and (b) $y = x + \frac{b}{4a}$.

1.2. (a) *Answer*: 1. Since the degree is odd, the polynomial has a real root. Since the polynomial is monotonous, this root is unique.

(b) *Answer:* 3. Let $f(x) = x^3 - 4x - 1$. We have $f(-2) < 0$, $f(-1) > 0$, $f(0) < 0$, $f(3) > 0$. By the Intermediate value theorem, the equation has three real roots.

1.3. (c) *Hint:* Determine the intervals of monotonicity of $f(x) = x^3 + px + q$. Find the points of local extrema and the values of f at these points. For this purpose, explore the sign of $\dfrac{f(x_1) - f(x_2)}{x_1 - x_2}$ (or, if you are educated enough, take a derivative of f).

1.4. (b) *Answer*: $x = -1 - \sqrt[3]{2}$.

Hint: $x^3 - 3\sqrt[3]{2}x + 3 = x^3 - 3bcx + (b^3 + c^3)$, where $b = 1$, $c = \sqrt[3]{2}$.

1.5. (a) The given polynomial vanishes at $a = -b - c$, which means that it is divisible by $a + b + c = a - (-b - c)$. Now one may divide $a^3 - 3abc + (b^3 + c^3)$ by $a + b + c$ in a usual way.

2.1. (a″) *Answer:* Yes. $\dfrac{1}{7 + 5\sqrt{2}} = \dfrac{7 - 5\sqrt{2}}{7^2 - 2 \cdot 5^2} = -7 + 5\sqrt{2}$.

(f) *Answer:* No.

Arguing indirectly, we assume $\sqrt{2} + \sqrt[3]{2} = a + \sqrt{b}$ for some $a, b \in \mathbb{Q}$. This number is a root of the polynomial $P(x) = ((x - \sqrt{2})^3 - 2)((x + \sqrt{2})^3 - 2)$ having rational coefficients. Applying Conjugation Theorem 2.3.d to $r = \sqrt{b}$ and polynomial $P(a + t)$ (or applying Corollary 2.3.e to $r = \sqrt{b}$ and polynomial $P(t)$), we obtain $P(a - \sqrt{b}) = 0$. By the rational roots theorem, the polynomial P has no rational roots. Therefore, $b \neq 0$, so the roots $a \pm \sqrt{b}$ are distinct. However, the polynomial P has only two real roots, namely $\sqrt{2} + \sqrt[3]{2}$ and $-\sqrt{2} + \sqrt[3]{2}$. Thus $a + \sqrt{b} = \sqrt{2} + \sqrt[3]{2}$ and $a - \sqrt{b} = -\sqrt{2} + \sqrt[3]{2}$, whence $\sqrt[3]{2} = a \in \mathbb{Q}$. This is a contradiction.

2.3. (a) If the polynomial $x^2 - r^2$ is reducible over $\mathbb{Q}$, then it has a linear factor with rational coefficients. Thus it has a rational root, which is impossible since $\pm r \notin \mathbb{Q}$.

(b) If $b \neq 0$, then $r = -a/b \in \mathbb{Q}$ which is impossible. Hence $b = 0$, and thus $a = 0$ as well.

(c) Divide our polynomial by $x^2 - r^2$ with residue; this residue is linear, and it vanishes at $x = r$. By (b), the residue is 0, as required.

(d) Follows from (c), since the polynomial $x^2 - r^2$ has roots $\pm r$.

3.1. (a) For 1 yuan we get $\sqrt[3]{2}$, which allows us to obtain $\sqrt[3]{2} + \sqrt[3]{4} = \sqrt[3]{2} + (\sqrt[3]{2})^2$.

3.2. (a) Clearly, each number of required form can be obtained for 1 yuan. It remains to prove that all such numbers are of this form. Surely, it would suffice to prove that the set of all numbers of the form $a \pm \sqrt{b}$ is closed under arithmetical operations; but this is obviously false. So we act in a bit different way.

Let $r = \sqrt{s}$ be a square root which has been obtained for 1 yuan (so $s \in \mathbb{Q}$). If $r \in \mathbb{Q}$, then the result is trivial since all obtained numbers are rational. Otherwise, we show that all the obtained numbers have the form $a + br$ with $a, b \in Q$. It suffices to prove that the result of an arithmetical operation applied to two numbers of this form also has the same form. This is trivial for all operations except division, for which the claim holds due to $\dfrac{1}{a + br} = \dfrac{a - br}{a^2 - b^2 s}$.

4.1. (a) *Answer:* yes. Since the squares of a real root of a biquadratic polynomial is a roots of a quadratic equation, this square may be obtained for one extraction. Thus the root itself can be obtained in two extractions.

5.1. (a) Consider the pairs $(x, y) = (1, 2)$ and $(x, y) = (2, 1)$.

5.2. (a) $(x - y)^2 = (x + y)^2 - 4xy$.

5.4. (b) We use the lexicographical induction on the multi-degree of the polynomial. Given a symmetric polynomial f of multi-degree (α, β) with $\alpha \geq \beta$ (i.e. with the lexicographically leading monomial of the form $kx^\alpha y^\beta$), one may reduce it to the polynomial $f - k(xy)^\beta (x+y)^{\alpha-\beta}$.

6 Additional Problems at the Semifinal

1. Solving equations of degree 3 and 4

6.1. * (a) Formulate and prove the theorem describing all real roots of the equation $x^4 + px^2 + qx + s = 0$. In the formulation and proof, you may use a root α of the cubic resolution of this equation.

Hint. Use Ferrari's method (see problem 1.7.ab). Do not forget to treat all possible cases!

(b) The same for all complex roots of this equation.

2. Representability with use of only one radical

6.2. Determine whether the following number can be represented in the form $a_0 + a_1\sqrt[7]{2} + a_2\sqrt[7]{2^2} + \cdots + a_6\sqrt[7]{2^6}$ with $a_0, a_1, a_2, \ldots, a_6 \in \mathbb{Q}$:

(a) $\sqrt{3}$; (b) $\cos(2\pi/21)$; (b′) any of the roots of the equation $x^7 - 4x + 2$;

(c) $\sqrt[11]{3}$; (d) $\sqrt[7]{3}$.

Hint: Apply lemmas formulated below.

6.3. Let q be a prime number, and let $r \in \mathbb{R} \setminus \mathbb{Q}$ be a number such that $r^q \in \mathbb{Q}$.

(a) *Irreducibility Lemma.* The polynomial $x^q - r^q$ is irreducible over $\mathbb{Q}$.

(b) *Linear Independence Lemma.* If r is a root of a polynomial A whose degree is less than q, then $A = 0$.

(c) **Conjugation Theorem.** *If r is a root of a polynomial, then all the numbers of the form $r\varepsilon_q^k$, $k = 1, 2, 3, \ldots, q-1$, are also roots of this polynomial.*

(d) *Rationality Lemma.* If A is a polynomial, then the number $A(r)$ is a root of some nonzero polynomial of degree at most q.

In the sequel, we use the notation

$$\mathbb{Q}[\varepsilon_q] = \{a_0 + a_1\varepsilon_q + a_2\varepsilon_q^2 + \cdots + a_{q-2}\varepsilon_q^{q-2} \mid a_0, \ldots, a_{q-2} \in \mathbb{Q}\}.$$

6.4. Let q be a prime number, and let $r \in \mathbb{C} \setminus \mathbb{Q}[\varepsilon_q]$ be a number such that $r^q \in \mathbb{Q}[\varepsilon_q]$.

(a) Prove that the polynomial $x^q - r^q$ is irreducible over $\mathbb{Q}[\varepsilon_q]$.

(b,c) Prove the analogues of the parts (b,c) of the previous problem for the polynomials with coefficients in $\mathbb{Q}[\varepsilon_q]$.

6.5. * Let q be a prime number, and let $r \in \mathbb{R} \setminus \mathbb{Q}$ be a number such that $r^q \in \mathbb{Q}$.

(a) *Strong Irreducibility Lemma.* The polynomial $x^q - r^q$ is irreducible over $\mathbb{Q}[\varepsilon_q]$.

(b) *Strong Linear Independence Lemma.* If A is a polynomial of degree less than q with coefficients in $\mathbb{Q}[\varepsilon_q]$ and $A(r) = 0$, then $A = 0$.

6.6. (a) **Proposition.** *Assume that a polynomial (of degree greater than 1) is irreducible over $\mathbb{Q}$ and has a root of the form $A(r)$, where A is a polynomial and r is a real number such that $r^q \in \mathbb{Q}$ for some prime q. Then this polynomial has degree q; moreover, if $q \neq 2$, it has no other real root.*

(b) Does the statement still hold if we replace the primality condition for q by the condition $r^2, \ldots, r^{q-1} \notin \mathbb{Q}$?

3. Equations of degree 3 solvable using one radical

Set

$$D_{pq} = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2.$$

We regard every implication in the next problem as a separate problem for which you may submit solution.

6.7. Theorem. *For a cubic equation $x^3+px+q=0$ with rational coefficients, the following conditions are equivalent:*

(1-solvability) at least one of its roots can be obtained on the real calculator with extracting at most one root;

($a+br+cr^2$) this equation has a root of the form $a+br+cr^2$, where $r\in\mathbb{R}$ and $a,b,c,r^3\in\mathbb{Q}$;

($\sqrt{D_{pq}}\in\mathbb{Q}$) either it has a rational root, or $D_{pq}\geq 0$ and $\sqrt{D_{pq}}\in\mathbb{Q}$.

6.8. If y_0, y_1, y_2 are the three complex roots (with multiplicity) of the polynomial x^3+px+q, then

$$-108D_{pq}=(y_0-y_1)^2(y_1-y_2)^2(y_0-y_2)^2.$$

Assume that $\mu\in\mathbb{C}$. We introduce the following notation:

$$\mathbb{Q}[\mu]=\{P(\mu)\mid P \text{ is a polynomial with rational coefficients}\}.$$

Notice that this notation agrees with the particular case introduced above.

6.9. Assume that μ is a root of some nonzero polynomial. Prove that $1/t\in\mathbb{Q}[\mu]$ for every nonzero $t\in\mathbb{Q}[\mu]$.

6.10. (a) Assume that $r\in\mathbb{R}\setminus\mathbb{Q}$ and $r^n\in\mathbb{Q}$ for some integer $n>1$. Take any $\alpha\in\mathbb{Q}[r]$. Then there exists a positive integer k such that $\alpha\in\mathbb{Q}[r^k]$ and $r^k\in\mathbb{Q}[\alpha]$ (in other words, $\mathbb{Q}[r^k]=\mathbb{Q}[\alpha]$).

(b) **Proposition.** *Assume that a polynomial of degree n is irreducible over $\mathbb{Q}$; moreover, assume that this polynomial is 1-solvable. Then this polynomial has a root of the form $A(r)$, where A is a polynomial, and a number $r\in\mathbb{R}$ satisfies $r^n\in\mathbb{Q}$.*

The *complex calculator* has the same buttons as the real one, but it operates with complex numbers, giving all the complex values of the root when the button '$\sqrt[n]{}$' is pressed. We say that *a number can be obtained using the complex calculator*, if the calculator can be used to get a set of numbers containing the given one.

We say that a polynomial is *k-solvable in the complex sense* if one of its roots can be obtained on the complex calculator using only k root extractions. The main problem 4.2 (as well as other problems in this section) remains interesting if we replace the real k-solvability by the complex one. The complex versions of these problems may turn out to be easier than the real ones.

6.11. (a) Every cubic polynomial is 2-solvable in the complex sense.

(b) Given rational p and q, decide whether the polynomial x^3+px+q is 2-solvable in the complex sense.

(c) Every polynomial of degree 4 is 4-solvable in the complex sense.

4. Equations of degree 4 solvable using one radical

6.12. Conjugation Theorem. *Let $a,b,c,d,r^4\in\mathbb{Q}$ and $r^2\notin\mathbb{Q}$. Assume that the number $x_0=a+br+cr^2+dr^3$ is a root of some polynomial. Then the numbers*

$$x_1=a+bri-cr^2-dr^3i,\quad x_2=a-br+cr^2-dr^3,\quad x_3=a-bri-cr^2+dr^3i$$

are also its roots.

6.13. Let a polynomial of degree 4 (with zero coefficient of x^3) have complex roots y_0, y_1, y_2, and y_3 (regarding multiplicity). Then

(a) the number $\dfrac{y_0y_1+y_2y_3}{2}$ is a root of the cubic resolution[8] of our polynomial;

[8]Recall that the cubic resolution $R_f(\alpha)$ of a polynomial $f(x)=x^4+px^2+qx+s$ is a polynomial in α defined as the discriminant of the quadratic polynomial $(x^2+\alpha)^2-f(x)$ with respect to x, i.e.,

$$R_f(\alpha)=q^2-4(2\alpha-p)(\alpha^2-s)=-8\alpha^3+4p\alpha^2+8s\alpha+(q^2-4ps).$$

(b) the numbers $\frac{y_0y_1+y_2y_3}{2}$, $\frac{y_0y_2+y_1y_3}{2}$, $\frac{y_0y_3+y_1y_2}{2}$ are all the complex roots of the cubic resolution (regarding multiplicity).

6.14. Assume that $p, q, s \in \mathbb{Q}$ and $p < 0 < q$.

(a) If $q^2 = 2p(4s - p^2)$ and $\sqrt{2q} \in \mathbb{Q}$, then the polynomial $x^4 + px^2 + qx + s$ has a root which can be obtained using the real calculator extracting only one root which is the root of degree four.

(b) Is the converse true?

5. Formal expressibility in real radicals

The negative answer to 5.5.c (and to problem 6.17.b below) show that *a root of a cubic equation is not expressible in real radicals via its coefficients.* Try to realize why this result does not contradict the Cardano Formula which expresses the root of a cubic equation via its coefficients (the clue to the answer is in the expression for discriminant in terms of roots, see problem 6.8).

Definition. The polynomial f in variables $x_1, x_2, \ldots, x_n$ is *cyclically symmetric* if the polynomials $f(x_1, x_2, \ldots, x_n)$ and $f(x_2, x_3 \ldots, x_{n-1}, x_n, x_1)$ are equal.

6.15. Express $x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ in radicals via cyclically symmetric polynomials in $x_1, x_2, \ldots, x_{10}$.

The negative answer to 5.5.c can be derived from the following problem.

6.16. Let $f, g \in \mathbb{R}[x, y, z]$.

(a) If the polynomial f^q is cyclically symmetric for some positive integer q, then f itself is cyclically symmetric.

(b) If $fg = 0$, then $f = 0$ or $g = 0$.

(c) If $fg \neq 0$, then $f^2 + fg + g^2 \neq 0$.

6.17. We say that *the generic polynomial equation of degree n is solvable in real radicals* if there exist

• non-negative integers $s, k_1, \ldots, k_s$ and

• polynomials $p_0, p_1, \ldots, p_s$ with real coefficients and in $n, n+1, \ldots, n+s$ variables, respectively,

such that if $a_0, \ldots, a_{n-1}, x \in \mathbb{R}$ and

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0,$$

then there are $f_1, \ldots, f_s \in \mathbb{R}$ for which

$$f_1^{k_1} = p_0(a_0, \ldots, a_{n-1}), \quad f_2^{k_2} = p_1(a_0, \ldots, a_{n-1}, f_1), \quad \ldots$$

$$\ldots \quad f_s^{k_s} = p_{s-1}(a_0, \ldots, a_{n-1}, f_1, \ldots, f_{s-1}), \quad x = p_s(a_0, \ldots, a_{n-1}, f_1, \ldots, f_s).$$

Note that we have defined a property of *the number n* rather than of a specific equation with given coefficients like in the *Galois Theorem* [S].

(a) The generic polynomial equation of degree 2 is solvable in real radicals.

(b)* The generic polynomial equation of degree 3 is not solvable in real radicals.

(c)* The similar result for each $n \geq 3$.

The results of problems 5.5.c and 6.17.b (and the comparison of them with the Cardano Formula) show that the definition of expressibility in real radicals given above is not a perfect formalization of the concept of solvability in radicals. On one hand, it is more reasonable to consider complex numbers instead of reals — this idea is realized in Section 7. On the other hand, we can work with numbers rather than with polynomials — this leads to the Galois Theorem [S]. However, investigating this imperfect formalization, one may see the main idea of the proof of Ruffini's theorem, see [S'].

Hints and Solutions distributed at the Semifinal

1. Solving equations of degree 3 and 4

1.3. (c) *Answer:* If $p = q = 0$, then there is one root. Otherwise, if $D_{pq} > 0$, then there is one root, if $D_{pq} = 0$, there are two roots, and if $D_{pq} < 0$, there are three roots.

1.4. (c) *Answer*: $x = -1 - \sqrt[3]{2}$.

Hint: By the result of 1.5.a, the equation $x^3 - 3\sqrt[3]{2}x + 3 = 0$ is equivalent to the equation

$$(x + b + c)(x^2 + b^2 + c^2 - bc - bx - cx) = 0, \quad \text{where} \quad b = 1 \quad \text{and} \quad c = \sqrt[3]{2}.$$

(d) *Answer:* $2\cos\frac{\pi}{9}$, $2\cos\frac{7\pi}{9}$, and $2\cos\frac{13\pi}{9}$.

Substituting $x = 2y$ we transform the equation $x^3 - 3x - 1 = 0$ to $4y^3 - 3y = \frac{1}{2}$. Using the identity $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ we get that all the numbers $\cos\frac{\pi}{9}$, $\cos\frac{7\pi}{9}$, and $\cos\frac{13\pi}{9}$ are roots of $4y^3 - 3y = \frac{1}{2}$.

1.5. (a,b) *Answer:*

$$a^3+b^3+c^3-3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca) = (a+b+c)(a+b\varepsilon_3+c\varepsilon_3^2)(a+b\varepsilon_3^2+c\varepsilon_3).$$

1.6. (a) *Answer:* Del Ferro's method is applicable, if $D_{pq} \geq 0$.

Theorem. *Let $p, q \in \mathbb{R}$.*

If $D_{pq} \geq 0$, then the equation $x^3 + px + q = 0$ has a unique real root

$$\sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}} - \sqrt[3]{\frac{q}{2} + \sqrt{D_{pq}}}.$$

If $D_{pq} = 0$, then all real roots of the equation are $-2\sqrt[3]{q/2}$ and $-\sqrt[3]{q/2}$ (they are distinct, provided that $q \neq 0$).

(b) **Theorem.** *Let $p, q \in \mathbb{C}$ and $pq \neq 0$. Let*

- *$\sqrt{D_{pq}}$ be any of the two values of a square root of D_{pq};*
- *u be any of the three values of a cubic root of $-\frac{q}{2} - \sqrt{D_{pq}}$;*
- *$v = -\frac{p}{3u}$. (Since $p \neq 0$, we have $(q/2)^2 \neq D_{pq}$, whence $u^3 = -\frac{q}{2} - \sqrt{D_{pq}} \neq 0$.)*

Then the three roots of the equation $x^3 + px + q = 0$ are $u + v$, $u\varepsilon_3 + v\varepsilon_3^2$, and $u\varepsilon_3^2 + v\varepsilon_3$. (They are not necessarily distinct, even if $q \neq 0$.)

1.7. *Answers*:

(a) $\dfrac{-3\sqrt{2} \pm \sqrt{10 + 12\sqrt{2}}}{2}$; (b) $\dfrac{-\sqrt{2} \pm \sqrt{4\sqrt{2} - 2}}{2}$; (c) $\dfrac{\sqrt{2} \pm \sqrt{8\sqrt{2} - 6}}{2}$;

(d) $\sqrt{2} \pm (\sqrt[4]{2} + \sqrt[4]{8})$.

2. Representability with use of only one radical

2.1. Answers: (a,a″,b,c,d) — yes; (a′,e,f,g,h) — no.

(a,c) $\sqrt{3 + 2\sqrt{2}} = \sqrt[3]{7 + 5\sqrt{2}} = 1 + \sqrt{2}$.

(a″) Notice that $(1+5\sqrt[3]{2}+\sqrt[3]{4})(3+\sqrt[3]{2}-8\sqrt[3]{4}) = -75$. (This equality can be found easily by the method of undetermined coefficients. Another way of obtaining it is the Euclid algorithm used to find the linear representation of the g.c.d. of x^3-2 and x^2+5x+1, see solution of 3.2.b; that problem claims in fact that such coefficients can be found always.) Therefore,

$$\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}} = -\frac{1}{25} - \frac{1}{75} \cdot \sqrt[3]{2} + \frac{8}{75} \cdot (\sqrt[3]{2})^2.$$

(b) $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2} = 1$.

(d) $\cos(2\pi/5) = (\sqrt{5} - 1)/4$.

(e) Assume that it is possible. Then we get $2 = (\sqrt[3]{2})^3 = (a^3 + 3ab) + (3a^2 + b)\sqrt{b}$. Since $3a^2 + b \neq 0$, we have $\sqrt{b} \in \mathbb{Q}$. Thus $\sqrt[3]{2} \in \mathbb{Q}$, which is a contradiction.

Another proofs may be obtained similarly to those of (f,g) or of Proposition 2.4.

(g) Assume that it is possible. By 2.2, our number $\cos(2\pi/9)$ is a root of $4x^3 - 3x = -\frac{1}{2}$. Now by Corollary 2.3.f this equation has a rational root, which is wrong.

Another proof is similar to that of Proposition 2.4.

2.2. By the triple angle formula for cosine we have $-1/2 = \cos(2\pi/3) = 4\cos^3(2\pi/9) - 3\cos(2\pi/9)$.

2.3. (e) Let P be a given polynomial, and set $G(t) = P(a + bt)$. Then $G(r) = 0$. By (d), we get $G(-r) = 0$.

(f) Follows from (e) combined with the Vieta theorem.

2.4. Arguing indirectly, suppose that the given polynomial $P(x)$ has a root $x_0 = a \pm \sqrt{b}$. By corollary 2.3.e and analogously to it, the number $x_1 = a \mp \sqrt{b}$ is also a root of P. If $b = 0$, then the statement is obvious; so we assume that $b \neq 0$. This implies $x_0 \neq x_1$. Therefore, P is divisible by $(x - a)^2 - b$. Since the degree of P is greater than 2, it is reducible. This is a contradiction.

2.5. *Answer:* (a,b,c,d,e,g) no; (f) yes.

Set $r = \sqrt[3]{2}$.

(a) *First solution.* Assume that it is possible. Then

$$3 = (a^2 + 4bc) + (2ab + 2c^2)\sqrt[3]{2} + (2ac + b^2)\sqrt[3]{4}.$$

Since the polynomial $x^3 - 2$ has no rational roots, it is irreducible over $\mathbb{Q}$. Thus, $2ab + 2c^2 = 2ac + b^2 = 0$ (cf. 2.6.b). So we have $b^3 = -2abc = 2c^3$. It follows that either $b = c = 0$ or $\sqrt[3]{2} = b/c$. Both cases are impossible.

Second solution. Assume that it is possible. Set $P(x) = x^2 - 3$. Then P has three roots x_1, x_2, and x_3 defined in Corollary 2.6.e. Since none of them is rational, the equality $b = c = 0$ does not hold. So, by Strong Linear Independence Lemma 2.6.b′, all three roots are distinct. This is a contradiction.

(b) Assume that it is possible. The number $\cos(2\pi/9)$ is a root of the equation $4x^3 - 3x = -\frac{1}{2}$. Its other two real roots are $\cos(8\pi/9)$ and $\cos(4\pi/9)$.

On the other hand, the polynomial $8x^3 - 6x - 1$ has three roots x_1, x_2, x_3 defined in Corollary 2.6.e. Since none of them is rational, the equality $b = c = 0$ is impossible. By Strong Linear Independence Lemma 2.6.b′, all three roots are distinct.

Since $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$, we have $\overline{x_2} = x_3$. Thus, x_2 and x_3 can not be both real and distinct. This is a contradiction.

(c) Assume the contrary. According to Rationality Lemma 2.7.a, there exists a cubic polynomial whose root is $a + br + cr^2$. But the polynomial $x^5 - 3$ is irreducible over $\mathbb{Q}$. This is a contradiction.

2.6. (a) Suppose that $x^3 - r^3$ is reducible. Then it has a rational root. This is a contradiction.

(b) Assume the contrary. Divide $x^3 - r^3$ by $a + bx + cx^2$ with residue. Due to (a), the residue is nonzero. Both polynomials $x^3 - r^3$ and $a + bx + cx^2$ have a root $x = r$. Hence the residue has the same root $x = r$. This implies that the residue is linear and has an irrational root, which is impossible.

(c) Divide our polynomial by $x^3 - r^3$ with residue. Substituting $x = r$ and applying Linear Independence Lemma (b), we get that the residue is zero.

(d) By (c), if $R^3 = r^3$, then R is a root of our polynomial.

(e) Let P be the given polynomial, and set $G(t) = P(a + bt + ct^2)$. Then $G(r) = 0$. By (d) we get $G(r\varepsilon_3) = 0 = G(r\varepsilon_3^2)$.

(a′) If our polynomial is reducible, it must have a root in $\mathbb{Q}[\varepsilon_3]$. Therefore, $r \in \mathbb{Q}[\varepsilon_3] \cap \mathbb{R} = \mathbb{Q}$, which is a contradiction.

This part can also be derived from (b′).

(b′) Consider the real and imaginary parts separately.

This part can also be derived from (a′).

2.7. (a) *First solution.* Due to the substitution $x = y + a$, it suffices to prove the claim for the vase when $a = 0$. Now notice that the number $t = br + cr^2$ satisfies $t^3 = b^3r^3 + c^3r^6 + 3bcr^3t$.

(In other words, by the equality from the solution of 1.5.a, the number $a + br + cr^2$ is a root of the polynomial $(x - a)^3 - 3bcr^3(x - a) - b^3r^3 - c^3r^6$.)

Second solution. Set $x_0 = a + br + cr^2$. Expand the numbers x_0^k with $k = 0, 1, 2, 3$ as polynomials in r:

$$x_0^k = a_k + b_k r + c_k r^2.$$

In order to solve the problem, it suffices to find numbers $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$, not all zeroes, such that $\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \lambda_3\alpha^3 = 0$. This condition will be satisfied if these numbers satisfy the system of equations

$$\lambda_0 a_0 + \cdots + \lambda_3 a_3 = 0, \quad \lambda_0 b_0 + \cdots + \lambda_3 b_3 = 0, \quad \lambda_0 c_0 + \cdots + \lambda_3 c_3 = 0.$$

It is known that a homogeneous (i.e. with zero right hand parts) system of linear equations with rational coefficients has a nontrivial rational solution, provided that the number of equations is less than the number of variables. This yields the required result.

The obtained polynomial has degree 3 and is irreducible; this follows from problem 2.6.eb′.

Remark. Yet another proof is shown in the first solution of (more general) Rationality Lemma 6.3.d.

3. Equations of degree 3 solvable using one radical

3.1. (b) Clearly, Cheburashka can obtain $\sqrt[3]{2+\sqrt{3}}$ for 2 yuans. It remains to notice that

$$\sqrt[3]{2-\sqrt{3}} = \frac{1}{\sqrt[3]{2+\sqrt{3}}} = \left(\sqrt[3]{2+\sqrt{3}}\right)^2 \cdot (2-\sqrt{3}).$$

(The last equality shows that one may avoid division by an irrational number in this case.)

(c) See the solution of 2.1.a″.

3.2. (b) Clearly, each described number can be obtained for 1 yuan. To prove the converse, as before, we show that all the obtained numbers have the form $a + br + cr^2$, where $r = \sqrt[3]{s}$ is a cubic root obtained for 1 yuan. The only nontrivial step is, however, a bit harder now: we need to prove that a number $\dfrac{1}{a + br + cr^2}$ has the required form (in case $r = \sqrt[3]{s} \notin \mathbb{Q}$).

By the Irreducibility Lemma, the polynomial $x^3 - r^3$ is irreducible over $\mathbb{Q}$, so it is coprime with $a + bx + cx^2$. Therefore, there exist polynomials g and h such that $h(x)(a + bx + cx^2) + g(x)(x^3 - r^3) = 1$. Then $h(r) = \dfrac{1}{a + br + cr^2}$, which yields the result.

3.3. (a) As an example one may take the equation $x^3 - 3x + 2 = 0$ with root 1.

(a′) An example is provided by the equation $x^3 - 6x - 6 = 0$ with a root $\sqrt[3]{2} + \sqrt[3]{4}$ (cf. problem 3.1.b). One may find this equation as in the proof of Rationality Lemma 2.7.a.

(b3, b2) *Answer:* Yes.

By del Ferro's method we get that one of the roots of our equation is

$$\sqrt[3]{-3+\sqrt{10}} + \sqrt[3]{-3-\sqrt{10}} = \sqrt[3]{-3+\sqrt{10}} - \frac{1}{\sqrt[3]{-3+\sqrt{10}}}.$$

(b1) A negative answer follows from the solution of (d), i.e., from Theorem 6.7.

(c) By 1.1.a we may assume that the equation has the form $x^3+px+q=0$. If $p=0$, the statement is trivial. Otherwise, since the equation has only one real root, we obtain hat $D_{pq}>0$ due to the solution of 1.3. Therefore, the number $u=\sqrt[3]{-\frac{q}{2}-\sqrt{D_{pq}}}$ appearing in the theorem in solution of 1.6.a can be obtained for 1 yuan. After that, the number $v=\sqrt[3]{-\frac{q}{2}+\sqrt{D_{pq}}}=-\frac{p}{3b}$ is obtained for free. By the same theorem, a root $u+v$ of the initial equation also can be obtained for 2 yuans.

(d) See Theorem 6.7.

4. Equations of degree 4 solvable using one radical

4.1. (b) *Hint:* One may express the root x_0 of the polynomial in terms of p and s, and then equalize this expression for x_0 to $br+cr^2+dr^3$, where $b,c,d,r^4\in\mathbb{Q}$, $r\in\mathbb{R}$.

(c) *Conjecture:* no.

Try to prove the following statement: Assume that a degree 4 polynomial has a cubic resolution with three real roots (in other words, this resolution has a negative *discriminant*); then this polynomial is not 10000-solvable. On the other hand, the formula presenting a root of a degree four polynomial whose the cubic resolution does not have three distinct real roots (or it has nonnegative discriminant) using four root extractions is the aim of problem 6.1.a.

4.3. (a) For example, the polynomial $x^4-12x^2-24x-14$ from problem 1.7.d has a root $\sqrt[4]{2}+\sqrt{2}+\sqrt[4]{8}$. (How can one *find* this polynomial, given its root?)

(b) *Answer:* yes, due to problem 6.14.a.

5. Formal expressibility in real radicals

5.1. (b) Consider the triples $(x,y,z)=(0,1,-1)$ and $(x,y,z)=(0,-1,1)$.

5.2. (b) $x=\dfrac{(x+y)+(x-y)}{2}$.

5.3. *Answer:* (a) $\sigma_1^2-2\sigma_2$; (b) $\sigma_1\sigma_2-3\sigma_3$; (c) $\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$.

(d) Apply 5.4.c.

5.4. (c) Again, we use the lexicographical induction on the multi-degree of the polynomial. Given a symmetric polynomial of multi-degree (k,ℓ,m) with $k\ge\ell\ge m$ and $k\ge 1$ (i.e., the lexicographically leading monomial of the polynomial has the form $ax^ky^\ell z^m$), one may reduce it to the polynomial $f-a\sigma_1^{k-\ell}\sigma_2^{\ell-m}\sigma_3^m$.

5.5. (a) Notice that the polynomial $(x-y)^2(y-z)^2(z-x)^2$ is symmetric. One may also reduce this problem to the next one.

(b) Set $M=x^2y+y^2z+z^2x$ and $N=y^2x+x^2z+z^2y$. Then $M+N$ and MN are symmetric polynomials. Therefore, they are polynomials in elementary symmetric functions $\sigma_1,\sigma_2,\sigma_3$. (We present the explicit expressions in the solution of 6.8.) Finally, M itself now can be expressed via $M+N$ and MN by the formula providing the roots of a quadratic equation.

Hints and Solutions distributed at the Final

1. Solving equations of degree 3 and 4

1.6. *Proof of the theorem formulated in (a).* Set $u = -\sqrt[3]{\frac{q}{2} + \sqrt{D_{pq}}}$ and $v = \sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}}$. We have $uv = -p/3$ and $u^3 + v^3 = -q$. By the formula from the solution of 1.5.a applied to $a = x$, $b = -u$, and $c = -v$, the number $u+v$ is a root of the polynomial $x^3+px+q = x^3-3uvx-u^3-v^3$. Since $2(x^2+u^2+v^2-xu-xv-uv) = (x-u)^2+(x-v)^2+(u-v)^2$, in the case $D_{pq} > 0$ we have no other roots, and if $D_{pq} = 0$, then there is an additional (multiple) root $u = v = -\sqrt[3]{q/2}$.

Proof of the theorem formulated in (b). We have $uv = -p/3$ and $u^3+v^3 = -q$. So it suffices to apply the formula from the solution of 1.5.b to $a = x$, $b = -u$, and $c = -v$.

6.1. If $q = 0$, then the equation is biquadratic, so it is easy to solve it. Henceforth we assume that $q \neq 0$.

(a) **Theorem.** *Suppose that $p, q, s \in \mathbb{R}$ and $q \neq 0$. Then there exists $\alpha > p/2$ such that $q^2 = 4(2\alpha - p)(\alpha^2 - s)$. For each such value of α define $A = \sqrt{2\alpha - p}$. Then all the real roots of the equation $x^4 + px^2 + qx + s = 0$ are:*

$$\begin{cases} \text{no roots,} & \text{if } 2\alpha + p > 2|q|/A; \\ x_\pm = \left(-A \pm \sqrt{-2\alpha - p + \frac{2q}{A}}\right)/2, & \text{if } -2q/A < 2\alpha + p \le 2q/A; \\ y_\pm = \left(A \pm \sqrt{-2\alpha - p - \frac{2q}{A}}\right)/2, & \text{if } 2q/A < 2\alpha + p \le -2q/A; \\ x_\pm,\ y_\pm, & \text{if } 2\alpha + p \le -2|q|/A \end{cases}.$$

Proof. Set $R(x) = 4(2x-p)(x^2-s) - q^2$. Note that $R(p/2) = -q^2 < 0$. On the other hand, for large enough values of x we have $R(x) > 0$. By the Intermediate value theorem, there exists $\alpha > p/2$ such that $R(\alpha) = 0$.

Since $p = 2\alpha - A^2$ and α is a root of the resolution, we get $s = \alpha^2 - \frac{q^2}{4(2\alpha-p)} = \alpha^2 - \frac{q^2}{4A^2}$. Therefore,

$$x^4 + px^2 + qx + s = \left(x^2 - Ax + \alpha + \frac{q}{2A}\right)\left(x^2 + Ax + \alpha - \frac{q}{2A}\right).$$

Solving two quadratic equations, we obtain the required formulas.

(b) **Theorem.** *Suppose $p, q, s \in \mathbb{C}$ and $q \neq 0$. Denote by α any of the roots of the equation $q^2 = 4(2\alpha - p)(\alpha^2 - s)$, and let A be any of two values of square root of $2\alpha - p$. Then all the roots of the equation $x^4 + px^2 + qx + s = 0$ are*

$$\left(A + \sqrt{-2\alpha - p - \frac{2q}{A}}\right)/2 \quad \text{and} \quad \left(-A + \sqrt{-2\alpha - p + \frac{2q}{A}}\right)/2,$$

where $\sqrt{y}$ is a multi-valued function providing both values of the root of y. Notice that, since $q^2 = 4A^2(\alpha^2 - s) \neq 0$, we have $A \neq 0$.

The proof is similar to the proof of the theorem in part (a).

Remark. One may also express all complex roots of the equation as

$$x = (\pm\sqrt{2\alpha_1 - p} \pm \sqrt{2\alpha_2 - p} \pm \sqrt{2\alpha_3 - p}),$$

where α_1, α_2, and α_3 are the three roots of the cubic resolution, the number of 'minuses' in the formula is even, and the values of the roots are chosen so that their product equals $-q$.

2. Representability with use of only one radical

2.1. (a′) Assume that this number is representable. The roots of the polynomial $P(x) = (x^2-2)^2-2$ are four numbers of the form $\pm\sqrt{2\pm\sqrt{2}}$, where the choices of signs can be made independently. One can easily check that this polynomial has no rational roots, and moreover, that the product of any two its roots is also irrational. This means that the polynomial $P(x)$ has no non-constant factors of degree at most 2, thus $P(x)$ is irreducible. This contradicts Proposition 2.4.

(h) (I. Braude-Zolotarev) The equality $1+\varepsilon_7+\varepsilon_7^2+\cdots+\varepsilon_7^6=0$ implies that $\cos(2\pi/7)+\cos(4\pi/7)+\cos(6\pi/7) = -1/2$. Applying the formulas $\cos 2\alpha = 2\cos^2\alpha - 1$ and $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ we find that $\cos(2\pi/7)$ is a root of the equation $8t^3+4t^2-4t-1=0$. Substituting $u=2t$ we get $u^3+u^2-2u-1=0$. Since the last equation has no rational roots, the same holds for $8t^3+4t^2-4t-1=0$. Now the negative answer to the question follows from 2.3.f.

2.5. As in the previous parts, we set $r=\sqrt[3]{2}$.

(d) Similarly to (a) and (b), the complex roots of the polynomial x^3-3 have the form x_1, x_2, x_3 (see Corollary 2.6.e). Thus, $(a+br+cr^2)\varepsilon_3^s = a+br\varepsilon_3+cr^2\varepsilon_3^2$ for some $s\in\{1,2\}$. By Strong Linear Independence Lemma 2.6.b′, we have $a=0$ and $bc=0$. This implies that either $\sqrt[3]{3}=br$ or $\sqrt[3]{3}=cr^2$, which is a contradiction.

(e) Similar to (b).

(f) This equation has a root $\sqrt[3]{2}+\sqrt[3]{4}$.

(g) The unique real root of this equation is $\sqrt[3]{3}+\sqrt[3]{9}$. Assume that this number us representable in the required form. Then all the numbers x_1, x_2, and x_3 introduced in Corollary 2.6.e are roots of the given equation. By the Strong Linear Independence Lemma 2.6.b′ these roots are distinct, so they are all roots of the equation.

On the other hand, by the theorem formulated in the solution of 1.6.b, all roots of the equation are

$$y_1=\sqrt[3]{3}+\sqrt[3]{9},\quad y_2=\sqrt[3]{3}\varepsilon_3+\sqrt[3]{9}\varepsilon_3^2,\quad y_3=\sqrt[3]{3}\varepsilon_3^2+\sqrt[3]{9}\varepsilon_3.$$

Since the equation has exactly one real root, we have $x_0=y_0$; then we get either $x_1=y_1$, $x_2=y_2$, or $x_2=y_1$, $x_1=y_2$.

Donote $P(x)=\sqrt[3]{3}x+\sqrt[3]{9}x^2$. Set also $S(x)=a+brx+cr^2x^2$ for the former case above, and $S(x)=a+brx^2+cr^2x$ for the latter case. Then the polynomial $P(x)-S(x)$ has three distinct roots 1, ε_3, and ε_3^2. But the degree of this polynomial is at most 2; thus $P=S$ and, in particular, either $\sqrt[3]{3}=br$ or $\sqrt[3]{3}=cr^2$. Both cases are impossible.

2.7. (b) By Rationality Lemma 2.7.a, there exists a cubic polynomial having $a+br+cr^2$ as a root. Since the given polynomial P is irreducible over $\mathbb{Q}$ and has the same root, we conclude that $\deg P\le 3$.

On the other hand, P has three roots x_1, x_2, x_3 defined in Corollary 2.6.e. Since P is irreducible, none of its roots is rational. So, the equality $b=c=0$ cannot hold. By Strong Linear Independence Lemma 2.6.b′, all the roots of P are distinct. Hence $\deg P=3$.

Since $\overline{\varepsilon_3^k}=\varepsilon_3^{-k}$, we have $\overline{x_2}=x_3$. This implies that x_2 and x_3 cannot be simultaneously real and distinct. So, $x_2, x_3\in\mathbb{C}\setminus\mathbb{R}$. It follows that P has a unique real root.

6.2. *Answers:* no (in all parts).

We use the following notation: $r=\sqrt[7]{2}$ and $A(x)=a_0+a_1x+a_2x^2+\cdots+a_6x^6$.

(a) Assume that it is possible. By the Conjugation Theorem 6.3.c, the polynomial x^2-3 has roots $A(r\varepsilon_7^k)$ for $k=0,1,2,\ldots,6$. Since this polynomial has no rational roots, Strong Linear Independence Lemma 6.5.b yields that these roots are distinct. This is a contradiction.

(b′) Assume that it is possible. The given polynomial P has no rational roots by Eisenstein's criterion. Therefore, Conjugation Theorem 6.3.c and Strong Linear Independence Lemma 6.5.b

imply that P has distinct roots $x_k := A(r\varepsilon_7^k)$ with $k = 0, 1, 2, \dots, 6$. Since $P(0) > 0$, $P(1) < 0$, and $P(2) > 0$, the polynomial P has a real root x_k distinct from x_0.

Notice now that $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$. Therefore, $x_k = \overline{x_k} = x_{7-k}$, which is a contradiction.

(b) Assume that it is possible. Let P be a polynomial such that $\cos 7x = p(\cos x)$ (prove that it exists!). The roots of the polynomial $2P(x) + 1$ are real numbers $y_k = \cos\dfrac{2(3k+1)\pi}{21}$ with $k = 0, \dots, 6$. One of them, namely $y_2 = -1/2$, is rational.

On the other hand, we claim that y_0 is irrational. (Otherwise we would have $\varepsilon_{21}^2 - 2y_0\varepsilon_{21} + 1 = 0$, whence $\varepsilon_{21} = a + i\sqrt{b}$ for some $a, b \in \mathbb{Q}$. Then the number $\varepsilon_7 = \varepsilon_{21}^3$ would also have this form. But the number ε_7 is a root of the irreducible[9] polynomial $1 + x + \dots + x^6$, which contradicts the analogue of Proposition 2.4 for the numbers of the form $a + i\sqrt{b}$.)

Thus, the number y_0 is an irrational root of the polynomial $\dfrac{2P(x)+1}{x - y_2}$ which has degree 6. However, Conjugation Theorem 6.3.c combined with Strong Linear Independence Lemma 6.5.b show that this polynomial has seven distinct roots, which is absurd.

(c) Assume that the number has the required form. Then the Rationality Lemma 6.3.d yields that there exists a nonzero polynomial of degree at most 7 having $\sqrt[11]{3}$ as a root. This contradicts the rational irreducibility of the polynomial $x^{11} - 3$.

(d) Assume that the number has the required form. Similarly to (a) and (b′) we obtain that the complex roots of the polynomial $x^7 - 3$ have the form $A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \dots, 6$. Therefore, $A(r)\varepsilon_7^s = A(r\varepsilon_7)$ for some $s \in \{1, 2, 3, 4, 5, 6\}$. Now, by Strong Linear Independence Lemma 6.5.b we obtain that $a_k = 0$ for all $k \neq s$. Therefore, $\sqrt[7]{3} = a_s r^s$, which is a contradiction.

6.3. (a) The roots of the polynomial $x^q - r^q$ are precisely $r, r\varepsilon_q, r\varepsilon_q^2, \dots, r\varepsilon_q^{q-1}$. Assume that $x^q - r^q$ is reducible over $\mathbb{Q}$. Then the absolute value of a constant term of one of its irreducible factors is rational and equals to the product of absolute values of k of these roots, $0 < k < q$. Therefore, $r^k \in \mathbb{Q}$. Since q is prime, we get $kx + qy = 1$ for some integers x, y. Thus $r^{kx} = r(r^q)^{-y}$, which implies $r \in \mathbb{Q}$. This is a contradiction.

(b) Arguing indirectly, take a polynomial $A(x)$ violating the lemma statement of the minimal possible degree. Let $R(x)$ be the remainder of $x^q - r^q$ divided by $A(x)$. Then we have $\deg R < \deg A$, $R(r) = 0$, and $R(x) \neq 0$ by (a). This contradicts the choice of A.

(c) The solution is similar to that of 2.3.cd, 2.6.cd, and 6.12, with the use of (b).

(d) *First solution.* The product

$$\Pi = (x - A(x_0))(x - A(x_1)) \dots (x - A(x_{q-1}))$$

is a symmetric polynomial in $x_0, x_1, \dots, x_{q-1}$. This means that Π can be expressed as a polynomial in x and the elementary symmetric polynomials in $x_0, x_1, \dots, x_{q-1}$. The values of these elementary symmetric polynomials at $x_k = r\varepsilon_q^k$ $(k = 0, 1, \dots, q-1)$ are the coefficients of the polynomial $x^q - r^q$, thus they are rational. So Π is the required polynomial.

Second solution. One may also argue exactly as in the second proof of Rationality Lemma 2.7.a, with 3 being replaced by q (e.g., the range '$k = 0, 1, 2, 3$' in the first line of the proof should be replaced by '$k = 0, 1, \dots, q$').

6.4. (a) Assume that our polynomial is reducible, and consider any its nontrivial unitary factor. As in proof of Lemma 6.3.a, the constant term of this factor has the form $\pm r^k \varepsilon_q^m$ and lies in $\mathbb{Q}[\varepsilon_q]$; therefore, $r^k \in \mathbb{Q}[\varepsilon_q]$. Now, again as in proof of Lemma 6.3.a, we obtain that $r \in \mathbb{Q}[\varepsilon_q]$. This is a contradiction.

(b,c) The proofs are similar to those of 6.3.bc; one may need to implement problem 6.9.

[9]The irreducibility of the polynomial $g(x) = 1 + x + \dots + x^6$ may be proved, e.g., by applying Eisenstein's criterion to the polynomial $g(x+1)$. On the other hand, in ur situation it suffices to prove that g has no divisors with rational coefficients of degree 1 and 2.

6.5. (a) Suppose that the polynomial is reducible. Similarly to the proof of Irreducibility Lemma 6.4.a (over $\mathbb{Q}[\varepsilon_q]$), we establish that $r \in \mathbb{Q}[\varepsilon_q]$. Thus $r^2, r^3, \dots, r^{q-1} \in \mathbb{Q}[\varepsilon_q]$.

We claim that in this case r is a root of some polynomial of degree at most $q-1$; this clearly contradicts 6.3.a.

For the proof, we argue similarly to the second solution of 2.7.a. Expand the numbers r^k with $k = 0, 1, \dots, q-1$ as polynomials in ε_q:

$$r^k = a_{k,0} + a_{k,1}\varepsilon_q + \dots + a_{k,q-2}\varepsilon_q^{q-2}.$$

Now it suffices to find numbers $\lambda_0, \lambda_1, \dots, \lambda_{q-1} \in \mathbb{Q}$, not all zeroes, such that all the equations

$$\lambda_0 a_{0,m} + \dots + \lambda_{q-1} a_{q-1,m} = 0 \qquad \text{for} \quad m = 0, 1, \dots, q-2$$

are satisfied. This is true by the theorem used in the aforementioned solution of 2.7.a.

(b) Follows from (a).

6.6. (a) *Hint:* Similar to the proofs of Propositions 2.4, 2.7.b and to the solutions of 6.2.ab′c. Apply Conjugation Theorem 6.3.c, Rationality Lemma 6.3.d, and Strong Linear Independence Lemma 6.5.b arriving at a contradiction.

Solution: Assume the contrary; let P be the given polynomial. The case $q < \deg P$ contradicts Rationality Lemma 6.3.d; so $q \geq \deg P$. Now, by Conjugation Theorem 6.3.c and Strong Linear Independence Lemma 6.5.b, the polynomial P has pairwise distinct roots $x_k = A(r\varepsilon_q^k)$ for $k = 0, 1, 2, \dots, q-1$. This is impossible unless $q = \deg P$; this proves the first assertion. Finally, if $q \neq 2$, then the relations $\overline{x_k} = x_{q-k} \neq x_k$ for $k = 1, 2, \dots, q-1$ yield the uniqueness of the real root.

(b) *Answer:* No. Set $r = \sqrt[6]{2}$; then the number $A(r)$, where $A(x) = x^3$, is a root of $x^2 - 2$.

3. Equations of degree 3 solvable using one radical

3.2. (c) Similarly to the previous parts, the only nontrivial claim is the following one:

Let $0 \neq d = a_0 + a_1 r + \dots + a_{n-1} r^{n-1}$, where $a_0, \dots, a_{n-1}, r^n$ are rational; then the number $1/d$ is representable in a required form.

The arguments from part (b) do not apply directly, since the polynomial $x^n - r^n$ may be reducible over $\mathbb{Q}$. In order to make them work, it suffices to replace this polynomial by its irreducible factor having r as a root.

We present also a different proof of the claim. We implement the following result similar to Rationality Lemma 2.7.a: *If $a_0, \dots, a_{n-1}, r^n \in \mathbb{Q}$, then the number $d = a_0 + a_1 r + \dots + a_{n-1} r^{n-1}$ is a (not necessarily unique) root of some polynomial whose degree does not exceed n.*

Suppose that d is a root of a polynomial $p_k d^k + \dots + p_0$; we may assume that $p_0 \neq 0$. Then

$$\frac{1}{d} = \frac{p_0}{p_0 d} = \frac{-p_1 d - \dots - p_k d^k}{p_0 d} = \frac{-p_1 - \dots - p_k d^{k-1}}{p_0}.$$

3.4. See [S, §§1.2 and 5.3].

6.7. $\underline{(\sqrt{D_{pq}} \in \mathbb{Q}) \Rightarrow \textit{(1-solvability).}}$ Set $r = \sqrt[3]{-\frac{q}{2} + \sqrt{D_{pq}}}$. By Cardano's formula (see the solution of problem 1.6), the unique real root of the equation $x^3 + px + q = 0$ equals

$$r - \frac{p}{3r} = r - \frac{p}{3r^3} \cdot r^2 = r - \frac{p}{3\left(-\frac{q}{2} + \sqrt{D_{pq}}\right)} \cdot r^2.$$

$\underline{(a + br + cr^2) \Rightarrow (\sqrt{D_{pq}} \in \mathbb{Q}).}$ If $r \in \mathbb{Q}$ or $b = c = 0$, then the equation has a rational root. In the remaining case, denote $\varepsilon = \varepsilon_3$. Each of the numbers x_1, x_2, and x_3 defined in

Corollary 2.6.e is a root of our equation. By Strong Linear Independence Lemma 2.6.b′, these three roots are distinct. Therefore, x_1, x_2, and x_3 are all the roots of our equation. Now, by 6.8 we have

$$\begin{aligned}-108D_{pq} &= (x_2-x_3)^2(x_1-x_3)^2(x_1-x_2)^2\\ &= \big(br(\varepsilon-\varepsilon^2)+cr^2(\varepsilon^2-\varepsilon)\big)^2\big(br(1-\varepsilon)+cr^2(1-\varepsilon^2)\big)^2\big(br(1-\varepsilon^2)+cr^2(1-\varepsilon)\big)^2\\ &= \varepsilon^2(1-\varepsilon)^6(br-cr^2)^2\big(br+cr^2(1+\varepsilon)\big)^2\big(br(1+\varepsilon)+cr^2\big)^2.\end{aligned}$$

Since $(1+\varepsilon)(1+\varepsilon^2)=(-\varepsilon)(-\varepsilon^2)=1$ and $(\varepsilon-1)^3=3\varepsilon-3\varepsilon^2=3\sqrt{3}\,i$, we obtain

$$\begin{aligned}-108D_{pq} &= -27\varepsilon^2(1+\varepsilon)^2(br-cr^2)^2\big(br(1+\varepsilon^2)+cr^2\big)^2\big(br(1+\varepsilon)+cr^2\big)^2\\ &= -27(\varepsilon+\varepsilon^2)^2(br-cr^2)^2\big(b^2r^2+br\cdot cr^2+c^2r^4\big)^2 = -27\big((br)^3-(cr^2)^3\big)^2.\end{aligned}$$

This yields the required result.

(1-solvability) $\Rightarrow (a+br+cr^2)$. If the given polynomial is reducible, then it has a rational root which has the required form. Otherwise the result follows directly from Proposition 6.10.b.

6.8. Set

$$M=y_0^2y_1+y_1^2y_2+y_2^2y_0 \quad\text{and}\quad N=y_0^2y_2+y_1^2y_0+y_2^2y_1.$$

Then $(y_0-y_1)(y_1-y_2)(y_0-y_2)=M-N$. Therefore,

$$(y_0-y_1)^2(y_1-y_2)^2(y_0-y_2)^2=(M+N)^2-4MN=(3q)^2-4(p^3+9q^2)=-4p^3-27q^2=-108D_{pq};$$

the second equality above follows from the relations $y_0+y_1+y_2=0$ (due to the Vieta theorem) combined with

$$\begin{aligned}M+N &= (y_0+y_1+y_2)(y_0y_1+y_1y_2+y_2y_0)-3y_0y_1y_2=0\cdot p+3q=3q,\\ MN &= (y_0y_1+y_1y_2+y_2y_0)^3+y_0y_1y_2(y_0+y_1+y_2)^3-6y_0y_1y_2\sum_{i\neq j}y_i^2y_j-9y_0^2y_1^2y_2^2=\\ &= p^3-q\cdot 0^3+6q(p\cdot 0+3q)-9q^2=p^3+9q^2.\end{aligned}$$

6.9. Similarly to the proof of Calculator theorem 3.2.c.

6.10. (a) The number r is a root of some nonzero polynomial with coefficients in $\mathbb{Q}[\alpha]$ (e.g., x^n-r^n. Choose such polynomial $f(x)$ of the minimal possible degree k.

Consider the g.c.d. of x^n-r^n and f; it also has r as a root, its coefficients lie in $\mathbb{Q}[\alpha]$, and its degree does not exceed k; this means that this g.c.d. is f itself. So all the complex roots of f have the form $r\varepsilon_n^m$. Then, by the Vieta theorem, the absolute value of the constant term of f equals r^k for some $k\le n-1$. Since this constant term is real, we obtain that $r^k\in\mathbb{Q}[\alpha]$.

Now it remains to prove that $\alpha\in\mathbb{Q}[r^k]$. Since $\alpha\in\mathbb{Q}[r]$, we have

$$\alpha=b_0(r^k)+rb_1(r^k)+\ldots+r^{k-1}b_{k-1}(r^k)$$

for some polynomials $b_0,\ldots,b_{k-1}\in\mathbb{Q}[x]$. If not all polynomials $b_1,\ldots,b_{k-1}$ are zeroes, then r is a root of a nonzero polynomial

$$(b_0(r^k)-\alpha)+xb_1(r^k)+\ldots+x^{k-1}b_{k-1}(r^k)$$

whose degree is k, and whose coefficients lie in $\mathbb{Q}[\alpha]$ (since $\alpha, r^k\in\mathbb{Q}[\alpha]$). This contradicts the choice of $f(x)$. Thus we arrive at $b_1=\cdots=b_{k-1}=0$, whence $\alpha=b_0(r^k)\in\mathbb{Q}[r^k]$.

(b) By Calculator Theorem 3.2.c, the given polynomial has a root $y_0\in\mathbb{Q}[R]$ for some $R\in\mathbb{R}$ and some positive integer D satisfying $R^D\in\mathbb{Q}$. By (a), we have $\mathbb{Q}[y_0]=\mathbb{Q}[R^k]$ for some k.

Denote $r = R^k$. Since $R^D \in \mathbb{Q}$, one may choose the minimal positive integer d such that $r^d \in \mathbb{Q}$; then $r, r^2, \dots, r^{d-1} \notin \mathbb{Q}$. Therefore, the polynomial $x^d - r^d$ is irreducible over $\mathbb{Q}$ (since the constant term of any its nontrivial unitary factor has an irrational absolute value r^t, $0 < t < d$; cf. 6.3.a).

Finally, the equality $\mathbb{Q}[y_0] = \mathbb{Q}[r]$, combined with the dimension argument similar to that in the solution of Strong Irreducibility Lemma 6.5.a, yield that any two irreducible (over $\mathbb{Q}$) polynomials, one with root y_0 and the other with root r, have equal degrees. This shows that $n = d$, as required.

6.11. (a) Follows from the Cardano formula (or, more exactly, from the theorem in the solution of problem 1.6.b) in a way similar to that in 3.3.c.

(b) **Conjecture.** *For a polynomial $p(x) = x^3 + px + q$ with $p, q \in \mathbb{Q}$, each of the conditions in Theorem 6.7 is equivalent to the complex 1-solvability of p.*

In this conjecture, one may prove almost all implications in a way similar to the proof of Theorem 6.7. The remaining implication is the following one.

Conjecture. *If a polynomial $x^3 + px + q$ with $p, q \in \mathbb{Q}$ is 1-solvable in the complex sense, then it has a root of the form $a + br + cr^2$, where $a, b, c, r^3 \in \mathbb{Q}$ and $r \in \mathbb{C}$.*

(c) Follows from the theorem in the solution of 6.1.b.

4. Equations of degree 4 solvable using one radical

4.2. $(4, 1)$ *Answer:* An irreducible over $\mathbb{Q}$ polynomial of the form $x^4 + px^2 + qx + s$ is 1-solvable if and only if

(4) one of its roots has the form $a + br + cr^2 + dr^3$, where $a, b, c, d, r^4 \in \mathbb{Q}$ but $r^2 \notin \mathbb{Q}$.

This condition is equivalent to the following one, formulated by means of the coefficients:

(4i) there exists $\alpha \in \mathbb{Q}$ such that $2\alpha > p$ and $q^2 - 4(p - 2\alpha)(s - \alpha^2) = 0$, and moreover
(4ii) the number $\Gamma = 16(\alpha^2 - s)^2 - (\alpha^2 - s)(2\alpha + p)^2$ is a square of a rational number.

Clearly, the conditions *(4i)* and *(4ii)* are algorithmically decidable.

The statement *(4)* on the form of a root of a 1-solvable polynomial is proved in 6.10.b. The proof that *(4)* is equivalent to *(4i)* together with *(4ii)* is proved in [A, Theorem 2].

4.4. By the theorem from the solution of 6.1, the polynomial $x^4 + px^2 + qx + s$ has a root $x_+ = \left(A + \sqrt{-\frac{2q}{A} - 2\alpha - p}\right)/2$, where $A^2 = 2\alpha - p$ and $Aq \le 0$. By the problem condition, we have $2\alpha - p > 0$, so the number A can be obtained using one extraction of a square root. Moreover, we have $-\frac{2q}{A} - 2\alpha - p \ge -2\alpha - p > 0$. Therefore, the number x_+ can be obtained using two root extractions.

4.5. By the Calculator theorem 3.2.c, the given root x_0 of our polynomial $f(x) = x^4 + px^2 + qx + s$ has the form $x_0 = a + br + cr^2 + dr^3$, where $a, b, c, d, r^4 \in \mathbb{Q}$. We may assume that $r^2 \notin \mathbb{Q}$ (otherwise we may replace r by either $\sqrt{|r|}$ or $\sqrt[4]{|r|}$). Then, applying Conjugation theorem 6.12, we obtain that the numbers x_1, x_2, and x_3 (defined in the cited theorem) are also roots of our polynomial.

Since f is irreducible, the number x_0 is irrational, and moreover the numbers x_0 and x_2 cannot appear to be the two roots of a quadratic trinomial with rational coefficients. This excludes the case $b = d = 0$. Therefore, $b + dr^2 \ne 0$ due to 2.3.b. Hence the real numbers x_0 and x_2 are distinct. Similarly, the numbers x_1 and x_3 are non-real and distinct. Thus[10] $f(x) = (x - x_0)(x - x_1)(x - x_2)(x - x_3)$.

[10]Here is another proof of the fact that $f(x)$ coincides with $g(x) = (x - x_0)(x - x_1)(x - x_2)(x - x_3)$. We have $g(x) = [(x - a - cr^2)^2 - r^2(b + dr^2)][(x - a + cr^2)^2 + r^2(b - dr^2)] \in \mathbb{Q}[r^4][x] = \mathbb{Q}[x]$. (One may also prove that g has rational coefficients similarly to the second proof of Rationality Lemma 6.3.d.) Now, $f(x)$ is irreducible and has a common root x_0 with $g(x)$, and these two polynomials have the same degrees and leading terms; thus $f(x) = g(x)$.

By problem 6.13, the cubic resolution of $f(x)$ has a root $\alpha = \dfrac{x_0x_2 + x_1x_3}{2}$. Since $x_0 + x_1 + x_2 + x_3 = 0$, we have $a = 0$. Therefore,

$$2\alpha = x_0x_2 + x_1x_3 = \big((cr^2)^2 - (br + dr^3)^2\big) + \big((cr^2)^2 - (bri - dr^3i)^2\big)$$
$$= 2c^2r^4 - r^2(b + dr^2)^2 + r^2(b - dr^2)^2 = 2c^2r^4 - 4bdr^4 = r^4(2c^2 - 4bd) \in \mathbb{Q}.$$

4.6. An analogue of parts (d) looks as follows.

Theorem. *Assume that a polynomial has a root $r \in \mathbb{R}$ such that $r^4 \in \mathbb{Q}$ but $r^2 \notin \mathbb{Q}$. Then the numbers ir, $-r$ and $-ir$ are also roots of this polynomial.* (Notice here that $i = \varepsilon_4$.)

Irreducibility Lemma. Assume that $r \in \mathbb{R}$, $r^4 \in \mathbb{Q}$, but $r^2 \notin \mathbb{Q}$. Then the polynomial $x^4 - r^4$ is irreducible over $\mathbb{Q}$.

The proof of the lemma is similar to the proof of 6.3.a, since $r, r^2, r^3 \notin \mathbb{Q}$. The proof of the theorem follows the lines of proofs of other Conjugaion Theorems.

Problem 6.12 serves as an analogue of parts (e).

6.12. Let $P(x)$ be the given polynomial. Then, as in Corollary 2.6.e, it suffices to apply the theorem from the solution of 4.6 to the polynomial $P(a + bx + cx^2 + dx^3)$.

6.13. (a) Applying the Vieta theorem and taking into account that $\sum_i x_i = 0$, one may check that $q^2 = (y_0y_1 + y_2y_3 - p)((y_0y_1 + y_2y_3)^2 - 4s)$. See details in [A, Statement 2].

(b) Similarly to (a), the three given numbers are roots of the cubic resolution. Moreover, we have $y_0y_2 + y_1y_3 - y_0y_1 - y_2y_3 = (y_0 - y_3)(y_2 - y_1)$. Thus, if the roots y_1, y_2, y_3, and y_4 are distinct, the obtained roots of the cubic resolution are also distinct, and thus the resolution has no other roots. The case when our polynomial has a multiple root can also be treated easily.

Alternative solution to both (a) and (b). Applying the Vieta theorem and taking into account that $\sum_i x_i = 0$, we get

$$\big(2\alpha - (y_0y_1 + y_2y_3)\big)\big(2\alpha - (y_0y_2 + y_1y_3)\big)\big(2\alpha - (y_0y_3 + y_1y_2)\big)$$
$$= 8\alpha^3 - 4\alpha^2\sum_{i<j} y_iy_j + 2\alpha\sum_{j<k,\ i\notin\{j,k\}} y_i^2y_jy_k - \prod_{0<j<k,\ i\notin\{0,j,k\}} (y_iy_j + y_ky_\ell)$$
$$= 8\alpha^3 - 4p\alpha^2 + 2\alpha\cdot\left(\sum_i y_i\cdot\sum_{|\{i,j,k\}|=3} y_iy_jy_k - 4y_0y_1y_2y_3\right) - \left(y_0y_1y_2y_3\sum_i y_i^2 + \sum_{i<j<k} y_i^2y_j^2y_k^2\right)$$
$$= 8\alpha^3 - 4p\alpha^2 - 8s\alpha - (q^2 - 4ps) = -R_f(\alpha),$$

which yields the desired result.

6.14. (a) Since $q^2 = 2p(4s - p^2)$, the cubic resolution $q^2 - 4(2\alpha - p)(\alpha^2 - s)$ has a root $\alpha = -p/2$. Since $p < 0$, we have $2\alpha - p = -2p > 0$. Therefore, by 6.1, our polynomial has a root

$$-\sqrt{2\alpha - p} + \sqrt{\frac{2q}{\sqrt{2\alpha - p}} - 2\alpha - p} = -\sqrt{-2p} + \frac{\sqrt{2q}}{\sqrt[4]{-2p}}.$$

(b) *Answer:* no. For example, the polynomial $x^4 - 12x^2 - 24x - 14$ from the solution of 4.3.a has a root $\sqrt[4]{2} + \sqrt{2} + \sqrt[4]{8}$, but the number $2\cdot(-24) = -48$ is not a square of a rational number.

5. Formal expressibility in real radicals

5.4. (d) **Theorem.** *Every symmetric polynomial can be expressed as a polynomial in elementary symmetric polynomials.*

Proof. We prove the assertion by lexicographical induction on the multi-degree of a given polynomial $f(x_1, x_2, \dots, x_n)$. The base case $f = 0$ is evident.

To prove the induction step, let $u = ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ be the (lexicographically) leading monomial of the polynomial f.

Suppose that $k_i < k_{i+1}$ for some i. Along with u, the polynomial f must contain a monomial $ax_1^{k_1}\dots x_i^{k_{i+1}}x_{i+1}^{k_i}\dots x_n^{k_n}$, whose multi-degree is greater than that of u, which is impossible. So $k_1 \geq k_2 \geq \dots \geq k_n$.

According to (a), the leading monomial of the polynomial $g = a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\dots\sigma_{n-1}^{k_{n-1}-k_n}\sigma_n^{k_n}$ is u. Therefore, the multi-degree of the polynomial $f-g$ is less than the multi-degree of f. Application of the induction hypothesis to $f-g$ finishes the proof. □

6.15. Set $M = x_1x_3+x_3x_5+x_5x_7+x_7x_9+x_9x_1$ and $N = x_2x_4+x_4x_6+x_6x_8+x_8x_{10}+x_{10}x_2$. Now one may proceed as in 5.5.b.

6.16. (a) Denote $g(x,y,z) := f(y,z,x)$. Since f^q is cyclically symmetric, we have $f^q = g^q$. If q is odd, we obtain $f = g$, so f is cyclically symmetric. Otherwise, if q is even, then $f = \pm q$, which yields either $f = g$ (and thus the result holds) or $f = -g$. In the latter case we have

$$f(x,y,z) = -f(y,z,x) = f(z,x,y) = -f(x,y,z).$$

Thus $f = 0$, and f is cyclically symmetric again..

(b) Use the result of 5.4.a.

(c) $f^2+fg+g^2 = \left(\dfrac{f+g}{2}\right)^2 + \left(\dfrac{\sqrt{3}}{2}g\right)^2 = (f+\varepsilon_3 g)(f+\varepsilon_3^2 g)$.

6.17. (a) Take

$$s = 1, \quad k_1 = 2, \quad p_0(y_0,y_1) = y_1^2 - 4y_0, \quad p_1(y_0,y_1,z_1) = \frac{z_1-y_1}{2} \quad \text{and} \quad f_1 = 2x + a_1.$$

Check that $f_1^2 = p_0(a_0,a_1)$ and $x = p_1(a_0,a_1,f_1)$.

References

[A] D. Akhtyamov, Solvability of cubic and quartic equations using one radical, `http://arxiv.org/abs/1411.4990`

[CS] A.B. Skopenkov and G.R. Chelnokov, Almost symmetric polynomials, a collection of problems.

[E] H.M. Edwards, The construction of solvable polynomials, Bull. Amer. Math. Soc. 46 (2009), 397–411. Errata: Bull. Amer. Math. Soc. 46 (2009), 703–704.

[Le] L. Lerner, Galois Theory without abstract algebra, `http://arxiv.org/abs/1108.4593`.

[M] Moscow mathematical students' conference, `http://www.mccme.ru/mmks/index.htm`.

[S09] A. Skopenkov, Philosophical and methodical appendix, in: Mathematics as a sequence of problems, Ed. A. Zaslavsky, D. Permyakov, A. Skopenkov, M. Skopenkov, A. Shapovalov, MCCME, Moscow, 2009.

[S] A. Skopenkov, Some more proofs from the Book: solvability and insolvability of equations in radicals, `www.mccme.ru/circles/oim/kroneck.pdf`.

[S'] A. Skopenkov, A short elementary proof of the Ruffini-Abel Theorem, `www.mccme.ru/circles/oim/ruffini.pdf`.