Toward algorithms of solving algebraic equations

presented by A. Enne, A. Chilikov,
A. Glebov, A. Skopenkov, B. Vukorepa *

1 Introduction and statements of results

1.1 What is this collection of problems about

There are famous Ruffini, Abel and Galois Theorems 2.7, 1.3, 1.4[1] on insolvability of algebraic equations in radicals. They are classical results of algebra, which are interesting for the computer science (theory of symbolic computations). All these theorems are formulated below.

The main content of this text is exposition of deep algebraic ideas (more precisely, of Galois theory) via simple and beautiful proofs of these theorems (see [ZSS, § 27]). It is the more remarkable that for these proofs one only needs the abilities to prove irrationality, to divide polynomials with a remainder, to take the root of a complex number, to multiply permutations, and to solve systems of linear equations. Even those who will not arrive to a complete proof of main results could solve research problems (see [E2, Es, AB, Ko17, Saf] and the references therein).

*We are grateful to Ya. Abramov, G. Chelnokov, D. Eliseev, A. Kanunnikov, N. Khoroshavkina, O. Orel, A. Petukhov and the jury of SCTT for useful discussions and for translation of some parts of the text.

A. Enne: Petrozavodsk State University.
A. Chilikov: Bauman Moscow State Technical University, Moscow Institute of Physics and Technology.
A. Glebov: Novosibirsk State University.
A. Skopenkov: Moscow Institute of Physics and Technology, Independent University of Moscow. http://www.mccme.ru/~skopenko.
B. Vukorepa: University of Zagreb.

[1]From §1 in what follows we use only §1.5, so you can read that subsection and start solving problems.

Before proving the insolvability of algebraic equations we consider a general way for their solution: Lagrange resolvent method . In fact, the main idea of Abel and Galois is the following: if an equation is solvable in radicals at all, then it is solvable by Lagrange method. Lagrange method is used to construct algorithms, e.g. to recognize whether the equation is solvable by radicals.

For practical purposes approximative methods of solving equations are more useful than 'radical formulae'. Besides, the equation can be solved using transcendental functions (see Vieta method [ZSS, § 4.2] and [PSo]; for further development of these ideas see e.g. [Sk10]). However, the problem of 'solvability in radicals' is interesting as a test problem of the modern theories of symbolic computations and computational complexity.

On the novelty. Proofs which are provided in solutions are not assumed to be new (but the reader could find new proofs). However, this text contains many pedagogical inventions (see [ZSS, §5.2.1, 5.2.2]). The proofs are different from proofs which are presented and quoted in [ZSS, §5]. Unfortunately, the proofs presented here are not well-known. Standard textbooks of algebra first expose Galois theory and then use its results to prove these theorems. However, it is much more economic and clearer not only to solve directly quadratic and cubic equations but also to prove corresponding theorems directly[2] . Of course, for such direct proofs, one should re-discover and use key ideas of Galois theory.

[2]See e.g. [Dor, § 25], [Pr07-2, appendix 8], [FT, Lecture 5], [ZSS, §5], [Dor, St94, Kol, Ler, T, Sk11, Sk15] and this text. Exposition in [Al] is closer to this 'direct' style. Large part of [Al] contains theory not required to prove the weak version of Abel theorem announced as the main result, see [Sk15, end of remark 7]. However, the author of [Al] succeeded in avoiding unmotivated exposition of the most complicated part of the theory. The proof from [Al] is exposed a shorter and easier way in [FT, Lecture 5], [Sk11].
Note that proofs in many of these sources are incomplete. See [ZSS, footnote 12 in p. 113 and end of §5.5.4], [Sk15, Discussion]. In spite of these drawbacks the above elementary expositions were more useful to us than formal expositions (in standard textbooks intended for the theory) which start with several hundreds pages of definitions and results whose role in the proof of the insolvability theorem is not clear at the moment of their statements.

1.2 Insolvability in real radicals

A real number is called **expressible by real radicals** if it can be obtained using number 1 and operations of addition, subtraction, multiplication, division by a non-zero number, and taking the n-th root of a positive number, where n is a positive integer. In other words, a real number a is expressible by real radicals if some set containing this number can be obtained starting from the set $\{1\}$ and using the following operations. To a given set $M \subset \mathbb{R}$ containing numbers $x, y \in M$ one can add

$$\text{numbers} \quad x+y, x-y, xy, \quad \text{number } x/y \text{ when } y \neq 0,$$

$$\text{and number } \sqrt[n]{x} \text{ for } x > 0 \text{ and integer } n > 0.$$

A number a is expressible by real radicals if and only if there exist

- positive integers $s, k_1, \ldots, k_s$,
- real numbers $f_1, \ldots, f_s$ and polynomials $p_0, p_1, \ldots, p_s$ with rational coefficients of $0, 1, \ldots, s$ variables respectively such that

$$\begin{cases} f_1^{k_1} = p_0 \\ f_2^{k_2} = p_1(f_1) \\ \ldots \\ f_s^{k_s} = p_{s-1}(f_1, \ldots, f_{s-1}) \\ a = p_s(f_1, \ldots, f_s) \end{cases}.$$

Remark 1.1. (a) Any real root of a quadratic equation with rational coefficients is expressible by real radicals.

(b) The equation $x^3 + x + 1 = 0$ has exactly one real root which is expressible by real radicals [ZSS, §4.2], see also Problem 2.8 (c).

(c) The equation $x^4 + 4x - 1 = 0$ has two real roots; both of them are expressible by real radicals [ZSS, §4.2], see also Problem 2.10 (d).

(d) Any real constructible number [ZSS, §5.1.2] is expressible by real radicals.

(e) There exists a cubic polynomial with rational coefficients such that none of its roots is expressible by real radicals (for example, $x^3 - 3x + 1$). (This statement is proven in Remark (f).)

(f) The number $\cos(2\pi/9)$ is not expressible by real radicals.

Let us apply the triple-angle formula for cosine. Then the numbers $\cos(2\pi/9)$, $\cos(8\pi/9)$, $\cos(14\pi/9)$ are the roots of the polynomial $8y^3 - 6y + 1 = 0$. By Theorem 1.2 none of these numbers is expressible by real radicals.

(g) The trisection of an angle is impossible in real radicals. That is, there exists a number α (for example, $\alpha = 2\pi/3$) such that the number $\cos\alpha$ is expressible by real radicals and the number $\cos(\alpha/3)$ is not expressible by real radicals. (This statement follows from Remark (f).)

Theorem 1.2 (solvability in real radicals)**.** For a cubic polynomial with rational coefficients the following conditions are equivalent:

(i) the polynomial has either at least one rational root or exactly one real root;

(ii) the polynomial has a root which is expressible by real radicals;

(iii) all the real roots of the polynomial are expressible by real radicals.

The uniqueness of the real root of the 'shortened' equation $x^3 + px + q = 0$ is equivalent to the following condition: '$p = q = 0$ or $(p/3)^3 + (q/2)^2 > 0$' [ZSS, Problem 8.1.5.d].

Obviously, $(ii) \Leftrightarrow (iii)$. This follows from Remark 1.1.a. The solvability in Theorem 1.2 (that is $(i) \Rightarrow (ii)$) can be proved by *del Ferro method* [ZSS, §4.2]; see another proof in §2.3. The insolvability in Theorem 1.2 (that is $(ii) \Rightarrow (i)$) has more complicated proof. It is easier to prove the similar result on *insolvability in polynomials*, see § 2.5.

1.3 Insolvability in complex radicals

Now consider formulae which involve complex numbers. It turns out that a cubic equation (for example, $x^3 - 3x + 1$) that is not solvable in real radicals can be solved in complex radicals.

A complex number is called **expressible by radicals** if it can be obtained using number 1 and operations of addition, subtraction, multiplication, division by a non-zero number and taking the n-th root, where n is a positive integer.

In other words, a complex number a is expressible by radicals if some set containing this number can be obtained starting from the set $\{1\}$ and using the following operations. To a given set $M \subset \mathbb{C}$

containing numbers $x, y \in M$ one can add

$$\text{numbers} \quad x+y, x-y, xy, \quad \text{number } x/y \text{ when } y \neq 0,$$

and any number $r \in \mathbb{C}$ such that $r^n = x$ for some integer $n > 0$.

For example, any (complex) root of a quadratic equation with rational coefficients is expressible by radicals. Similar assertions hold for equations of 3-rd and 4-th degree. These assertions can be proved by *del Ferro and Ferrari methods* [ZSS, §4.2]; see another proof in §2.3. However, analogous assertions for equations of higher degrees do not hold.

Theorem 1.3 (Galois)**.** There exists an equation of 5-th degree with rational coefficients (for example, $x^5 - 4x + 2 = 0$) neither of whose roots are expressible by radicals.

The famous problem of solvability in radicals was solved by weaker Ruffini-Abel theorems proved a little earlier. The Ruffini Theorem 2.7 has more complicated statement. But it leads us to the proof of Galois theorem. The precise statement of Abel theorem is even more complicated. It is not presented here, see [Sk15, Remark 7]. An easier way to solve the solvability problem is to prove the following Galois Theorem 1.4. This theorem is weaker than Galois Theorem 1.3 and has an easier proof. For $X \subset \mathbb{C}$, a complex number a is called *X-expressible by radicals* if a can be expressed using the set $X \cup \{1\}$ and the operations from the definition of the expressibility by radicals.

Theorem 1.4 (Galois)**.** There are $a_0, a_1, a_2, a_3, a_4 \in \mathbb{C}$ such that no root of the equation $x^5 + a_4x^4 + \ldots + a_1x + a_0 = 0$ is $\{a_0, a_1, \ldots, a_4\}$-expressible by radicals.

Theorem 1.5. There is an algorithm to recognize whether all the roots of the equation $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ are expressible by radicals (if $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$ are known).

Theorem 1.5 is proved using Galois Solvability Criterion 2.13.b and an estimation of the number of operations.

1.4 Plan

This project consists of three formally independent parts. In the first two parts the definition of 'expressibility by radicals' from §2.2 is used.

(1) In §2.3 we discuss Lagrange's resolvent method used to solve equations. Formally this method is not used to prove insolvability. However, familiarity with this method is useful because

• proofs of insolvability were invented during the analysis of this method,

• this familiarity helps to check intermediate conjectures (which occur in attempts to prove insolvability), and

• this method is required to prove Theorem 1.5.

(2) The proof of the Ruffini theorem 2.7 is based on the idea of symmetry and is sketched in §3.1. This proof is prepared by §2.5. Subsection 2.4 prepares to §2.5 and to the proof of Galois Theorem 1.4.

(3) The proof of Theorem 1.2 on solvability in real radicals is based on the idea of conjugation (or of algebraic symmetry). This proof is prepared by §2.1, §3.2 and §3.3.

Theorems 1.3 and 1.5 are not proved here. See the proof of Theorem 1.3 in [ZSS, §5], [Sk19, §9]. Galois Theorem 1.4 is proved in additional problems, cf. [Sk15], [Sk19, §5]. The proof is based on reduction to Ruffini Theorem 2.7 using the idea of conjugation (§2.1, §3.2 and §3.3).

1.5 Recommendations for participants

For every solution which has been written down and marked with either '+' or '+.' a student (or a group of students) get a 'bean'. The jury may also award extra bean for beautiful solutions, solutions of hard problems, or solutions typeset in TEX. The jury has infinitely many beans. One may submit a solution in oral form, but one loses a bean with each 5 attempts (successful or not).

If a problem is marked by bold and named 'theorem' ('lemma', 'corollary', etc.), then this statement is important. Usually we provide (as a problem) the *formulation* of beautiful or important statement *before* its *proof*. In this case to prove this statement one possibly needs to solve next problems. If you are stuck on a certain problem, try looking at the next ones. They may turn out to be helpful. We suggest to all the students working on the project to *consult* the jury on any questions on the project. Students who successfully work on the project will get interesting *extra problems*.

Please notify us if you already know solutions of several problems. If you confirm your knowledge by presenting some of them, you will be allowed not to receive plus-marks for their solutions, but to use them in solutions of other problems.

2 Problems before the semifinal

In this text equality signs involving polynomial f (or f_j) mean equality of polynomials (i.e. componentwise equality). In §§2.1, 3.2 and 3.3 'polynomial with rational coefficients' is called a 'polynomial'. Denote

$$\varepsilon_q := \cos(2\pi/q) + i\sin(2\pi/q).$$

2.1 Representability using only one square root

2.1. Can the following number be represented as $a+\sqrt{b}$ with $a, b \in \mathbb{Q}$:

(a) $\sqrt{3+2\sqrt{2}}$; (b) $\frac{1}{7+5\sqrt{2}}$; (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)* $\sqrt{2+\sqrt{2}}$; (i)* $\cos(2\pi/7)$; (j) $\sqrt{2}+\sqrt{3}+\sqrt{5}$?

Lemma 2.2. Assume that $r \in \mathbb{R}-\mathbb{Q}$ and $r^2 \in \mathbb{Q}$.

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

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

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

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

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

(f) If $a, b \in \mathbb{Q}$ and a cubic polynomial has a root $a+br$, then this polynomial has a rational root.

Theorem 2.3. If a polynomial of degree at least 3 is irreducible over $\mathbb{Q}$, then none of its roots equals to $a \pm \sqrt{b}$ for some $a, b \in \mathbb{Q}$.

Lemma 2.4 (Extension)**.** Suppose we can obtain a number using number 1, several operations of addition, subtraction, multiplication,

division by a non-zero number and exactly one operation of taking the square root of a positive number. Then the number can be represented as $a \pm \sqrt{b}$, where $a, b \in \mathbb{Q}$ and $b > 0$.

2.5.* Find all n such that the number $\cos(2\pi/n)$ can be represented as $a + \sqrt{b}$, where $a, b \in \mathbb{Q}$.

Hints to §2.1

2.2. (a) If the polynomial $x^2 - r^2$ is reducible over $\mathbb{Q}$, then it has a rational root. This is a contradiction.

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

(c) Divide our polynomial with a remainder[3] by $x^2 - r^2$:

$$P(x) = (x^2 - r^2)Q(x) + mx + n.$$

Substitute $x = r$. By the Linear independence lemma (see (b)) the reminder is equal to zero.

(d) By (c) if $R^2 = r^2$, then R is a root of the polynomial.

(e) Let P be given polynomial, and set $G(t) := P(a + bt)$. Then $G(r) = 0$. Hence by (d) we obtain $G(-r) = 0$.

(f) If $b = 0$ the assertion is proved. Otherwise by (e) the polynomial has the roots $a \pm br$. These roots are distinct. Hence the third root is rational by the Vieta theorem.

2.4. It would suffice to prove that the set of all numbers of the form $a \pm \sqrt{b}$ is closed under operations of addition, subtraction, multiplication and division. This is obviously false: $(1 + \sqrt{2}) + (1 + \sqrt{3})$ cannot be represented as $a \pm \sqrt{b}$, where $a, b \in \mathbb{Q}$ (prove this!).

2.2 Definition of the expressibility by radicals for polynomials

The solution of quadratic equation can be expressed by the following formulae:

$$(x - y)^2 = (x + y)^2 - 4xy \quad \text{and} \quad x = \frac{x + y + (x - y)}{2}.$$

[3]The division with a reminder is equivalent to 'replacing' x^2 by r^2.

These formulae show that *the root x of a quadratic equation is expressible by radicals* using the coefficients $x+y, xy$ of the equation. The rigorous definition of expressibility by radicals is given below.

Denote the elementary symmetric polynomials by

$$\sigma_1(x_1,\dots,x_n) := x_1+\dots+x_n, \quad \dots, \quad \sigma_n(x_1,\dots,x_n) = x_1\cdot\dots\cdot x_n.$$

If the number n and the arguments $x_1,\dots,x_n$ are clear from the context, we omit them from the notation.

A polynomial $p\in\mathbb{C}[x_1,\dots,x_n]$ is called **expressible by (complex) radicals**, if one can add p to the collection $\{\sigma_1,\dots,\sigma_n\}\cup\mathbb{C}$ of polynomials by a sequence of the following operations:

• if the polynomials f and g are already contained in the collection one can add their sum $f+g$ and their product fg;

• if the polynomial g is already contained in the collection and $g=f^k$ for some $f\in\mathbb{C}[x_1,\dots,x_n]$ and integer $k>1$ one can add f to the collection.

Remark 2.6. (a) E.g. if a collection contains x^2+2y and $x-y^3$, then one may apply the first operations and add the polynomial

$$-5(x^2+2y)^2+3(x^2+2y)(x-y^3)^6$$

to the collection; moreover, if a collection already contains $x^2-2xy+y^2$, then one may apply the second operation and add $x-y$ (or $y-x$).

(b) If we use only first operations we can add a polynomial with complex coefficients of polynomials which are already available.

(c) By Vieta theorem $\sigma_1,\dots,\sigma_n$ are the coefficients of the polynomial

$$t^n-\sigma_1t^{n-1}+\dots+(-1)^{n-1}\sigma_{n-1}t+(-1)^n\sigma_n\in\mathbb{C}[x_1,\dots,x_n][t]$$

with roots $x_1,\dots,x_n$. Therefore, the expressibility by radicals of the polynomial x_1 is equivalent to the expressibility (in the above sense) of its root x_1 in terms of the coefficients of this polynomial.

(d) The polynomial x_1 is expressible by radicals if and only if there exist:

• positive integers $s,k_1,\dots,k_s$,

• polynomials $f_1, \dots, f_s$ and $p_0, p_1, \dots, p_s$ with complex coefficients of n and of $n, n+1, \dots, n+s$ variables respectively, such that

$$\begin{cases} f_1^{k_1} = p_0(\sigma_1, \dots, \sigma_n) \\ f_2^{k_2} = p_1(\sigma_1, \dots, \sigma_n, f_1) \\ \dots \\ f_s^{k_s} = p_{s-1}(\sigma_1, \dots, \sigma_n, f_1, \dots, f_{s-1}) \\ x_1 = p_s(\sigma_1, \dots, \sigma_n, f_1, \dots, f_s) \end{cases} .$$

Here we omit the variables $(x_1, \dots, x_n)$ of the polynomials $\sigma_1, \dots, \sigma_n, f_1, \dots, f_s$.

(e) Given $x + y$ and xy, is it always possible to find x?

A simple formalization of this question is the following: *does there exist a map* $f : \mathbb{R}^2 \to \mathbb{R}$ *such that* $f(x + y, xy) = x$ *for any* $x, y \in \mathbb{R}$*?* The answer is no. Indeed, consider the pairs $x = 1, y = 2$ and $x = 2, y = 1$. Therefore, the expressibility by radicals does not allow 'to find x' in the sense described above.

Analogously, given $\sigma_1 = x + y + z$, $\sigma_2 = xy + yz + zx$ and $\sigma_3 = xyz$ is it not always possible to find $(x - y)(y - z)(z - x)$. Indeed, consider the triples $x = 0, y = 1, z = -1$ and $x = 0, y = -1, z = 1$.

Theorem 2.7 (Ruffini)**.** For every positive integer $n \geqslant 5$ the polynomial x_1 is not expressible by radicals.

The proof shows that even the polynomial $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$ is not expressible by radicals for $n = 5$.

2.3 Solution of equations of low degrees

2.8. Which of the following polynomials are expressible by radicals for $n = 3$?

(a) $(x - y)(y - z)(z - x)$; (b) $x^9y + y^9z + z^9x$; (c) x.

To solve Problem 2.8 and the following problems, one can use the fundamental theorem on symmetric polynomials,see for example [Sk19, 4.6.3c]. Hints for part (c) are Problems 2.9.a and 2.11.c.

2.9. A polynomial $f \in \mathbb{C}[u_1, u_2, \dots, u_n]$ is called **cyclic symmetric** if $f(u_1, u_2, \dots, u_n) = f(u_2, u_3, \dots, u_{n-1}, u_n, u_1)$.

(a) Find at least one pair $\alpha, \beta \in \mathbb{C}$ such that the polynomial $(u + v\alpha + w\beta)^3$ is cyclic symmetric, but the polynomial $u + v\alpha + w\beta$ is not.

(b) Express $x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ by operations from the definition of expressibility by radicals starting with some *cyclic symmetric* polynomials in $x_1, x_2, \dots, x_{10}$.

2.10. Which of the following polynomials are expressible by radicals for $n = 4$?

(a) $(x-y)(x-z)(x-t)(y-z)(y-t)(z-t)$;

(b) $xy + zt$; (c) $x + y - z - t$; (d) x.

2.11. Solve the following systems of equations (x, y, z, t are unknowns, a, b, c, d are known):

$$\text{(a)} \quad \begin{cases} x+y+z+t=a, \\ x+y-z-t=b, \\ x-y+z-t=c, \\ x-y-z+t=d; \end{cases} \qquad \text{(b)} \quad \begin{cases} x+y+z+t=a, \\ x+iy-z-it=b, \\ x-y+z-t=c, \\ x-iy-z+it=d; \end{cases}$$

$$\text{(c)} \quad \begin{cases} x+y+z=a, \\ x+\varepsilon_3 y+\varepsilon_3^2 z=b, \\ x+\varepsilon_3^2 y+\varepsilon_3 z=c. \end{cases}$$

Expressions from Problem 2.11 are called *Lagrange resolvents*. They are 'better' than roots because they are 'more symmetric' in the following sense.

Solution of cubic equation using Lagrange resolvents (solution of Problem 2.8 (c)). To find the roots x, y, z of a cubic equation, it suffices to find the expressions a, b, c from Problem 2.11 (c). Notice that the del Ferro method from [Sk19, 4.2.2] leads us to the same expressions. By Vieta theorem, $a = a(x, y, z)$ is the coefficient of the equation. Under the substitution $x \leftrightarrow y$, polynomial $b = b(x, y, z)$ goes to $\varepsilon_3 c$, and $c = c(x, y, z)$ goes to $\varepsilon_3^2 b$ (check this!). Therefore, the polynomials bc and $b^3 + c^3$ do not change under this substitution. Analogously, they do not change under substitution $z \leftrightarrow y$. Therefore the polynomials bc and $b^3 + c^3$ are *symmetric*, i.e., they do not change under any permutation of variables. From the theorem on representability of a symmetric polynomial as a polynomial in elementary symmetric polynomials (see e.g. [Sk19, 4.6.3c]) and Vieta theorem it follows that the bc and $b^3 + c^3$ polynomials in x, y, z can be represented as polynomials in the coefficients of the equation. Hence we can obtain b^3 and c^3 by

solving certain quadratic equation. Now, by solving certain quadratic equation we can obtain b^3 and c^3.

By Ruffini Theorem 2.7, Lagrange resolvent method demonstrated by solving equations of degrees 3 and 4 (Problems 2.8 (c) and 2.10 (d)) does not work for degree 5. Guess why!

Denote by Σ_q the set of permutations of the set $\{1, 2, \ldots, q\}$. For a permutation $\alpha \in \Sigma_q$ denote

$$\vec{u}_\alpha := (u_{\alpha(1)}, \ldots, u_{\alpha(q)}).$$

Define the *Lagrange resolvent* by

$$t(u_1, \ldots, u_q) := \varepsilon_q u_1 + \varepsilon_q^2 u_2 + \ldots + \varepsilon_q^q u_q.$$

Define *Galois resolvent* by

$$Q(u_1, \ldots, u_q, y) := \prod_{\alpha \in \Sigma_q} (y - t(\vec{u}_\alpha)) \in \mathbb{Q}[\varepsilon_q][u_1, \ldots, u_q, y].$$

2.12. (a) We have $Q(\varepsilon_q u_1, \ldots, \varepsilon_q u_q, y) = Q(u_1, \ldots, u_q, y)$.

(b) For some $R_Q \in \mathbb{Q}[\varepsilon_q][u_1, \ldots, u_q, z]$ we have $Q(u_1, \ldots, u_q, y) = R_Q(u_1, \ldots, u_q, y^q)$.

(c) If $x_1, \ldots, x_q \in \mathbb{C}$ are the roots of a polynomial $f \in \mathbb{Q}[x]$ of degree q, then $Q(x_1, \ldots, x_q, y) \in \mathbb{Q}[\varepsilon_q][y]$ and even $Q(x_1, \ldots, x_q, y) \in \mathbb{Q}[y]$.

The polynomial $R_Q(x_1, \ldots, x_q, z) \in \mathbb{Q}[z]$ is called *the resolvent polynomial* for f.

(d)* All the roots of the resolvent polynomial for $f(x) = x^5 + 15x + 11$ (and therefore, all the roots of f) are expressible by radicals.

Theorem 2.13.* (a) For $a, b \in \mathbb{R}$ all the roots of the equation $x^5 + ax + b = 0$ are expressible by radicals if and only if $a = \dfrac{15 \pm 20c}{c^2 + 1}$ and $b = \dfrac{44 \mp 8c}{c^2 + 1}$ for some $c \in \mathbb{Q}$, $c \geqslant 0$.

(b) (**Galois Solvability Criterion**) For each $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$ all the roots of the equation $A(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ are expressible by radicals if and only if a set of degree 1 polynomials over $\mathbb{Q}$ can be obtained from $\{A\}$ using the following operations:

• (factorization) if one of our polynomials equals to $P_1 P_2$ for some non-constant $P_1, P_2 \in \mathbb{Q}[x]$, then replace $P_1 P_2$ by P_1 and P_2;

• (extracting a root) if one of our polynomials equals to $P(x^q)$ for some $P \in \mathbb{Q}[x]$, then replace $P(x^q)$ by $P(x)$;

• (taking Galois resolvent) replace one of our polynomials P by the polynomial $Q(y_1, \dots, y_q, y)$, where $y_1, \dots, y_q$ are all the roots of P. (Analogously to Problem 2.12.c $Q(y_1, \dots, y_q, y) \in \mathbb{Q}[y]$.)

Part (a) is derived from (b) [PSo]. Part 'if' in (b) is easier. This part can be proved using Lagrange resolvent method which is considered in this subsection. Part 'only if' in (b) is more complicated. This can be proved similarly to Galois Theorems 1.3, 1.4.

2.4 There is only one way to solve quadratic equation

Systems of equations studied here and in the following subsection arise when solving equations by radicals ('using one radical'), see Remark 2.6.d.

2.14. (a,b) Solve the system of equations in polynomials $f(x, y)$, $p(u, v)$ and $q(u, v, w)$ with real coefficients:

(a) $\begin{cases} f^2(x, y) = p(x + y, xy) \\ x = q\,(x + y, xy, f(x, y)) \end{cases}$.

(b) $\begin{cases} f^k(x, y) = p(x + y, xy) \\ x = q\,(x + y, xy, f(x, y)) \end{cases}$, where $k > 0$ is an integer.

(c,d*) Solve the analogues of (a,b) where the polynomial f is replaced by a function $f : \mathbb{R}^2 \to \mathbb{R}$ (which is not assumed to be continuous).

The system of equations from 2.14.a is satisfied, for example, by the polynomials

$$f(x, y) = x - y, \quad p(u, v) = u^2 - 4v \quad \text{and} \quad q(u, v, w) = \frac{u + w}{2}.$$

2.15. Assume that $f, g \in \mathbb{R}[x, y]$.

(a) **Lemma.** If $fg = 0$, then $f = 0$ or $g = 0$.

Warnings. There exist functions $F, G : \mathbb{R} \to \mathbb{R}$ such that $FG = 0$, $F \neq 0$ and $G \neq 0$. There exist two different polynomials in two variables which are equal at an infinite set of points. Do not use without proof the fact that if the values of polynomials in two variables are equal in any point, then the polynomials are equal.

(b) If $f^2 = g^2$, then $f = g$ or $f = -g$.
(c) If $f^2 + fg + g^2 = 0$, then $f = 0$ or $g = 0$.
(d) If $f^3 = g^3$, then $f = g$.
(e) If $f^5 = g^5$, then $f = g$.
(f) $f^5 - g^5 = (f - g)(f - \varepsilon_5 g)(f - \varepsilon_5^2 g)(f - \varepsilon_5^3 g)(f - \varepsilon_5^4 g)$.

To prove the assertions 2.14.bd, the following notions and lemma are useful.

A polynomial f in two variables x, y is called *symmetric*, if $f(x, y) = f(y, x)$. A polynomial f is called *antisymmetric*, if $f(x, y) = -f(y, x)$.

2.16. (a) **Lemma.** If $f \in \mathbb{R}[x, y]$ is a polynomial with real coefficients in two variables such that f^2 is symmetric, then f is either symmetric or antisymmetric.

(b) **Lemma.** If $f \in \mathbb{R}[x, y]$ is such that f^{2k+1} is symmetric, then f is symmetric.

(c) If $f \in \mathbb{R}[x, y]$ is antisymmetric, then there exists a symmetric polynomial $a \in \mathbb{R}[x, y]$ such that $f = (x - y)a$.

To prove the assertions above and to solve other problems, Lemma 2.15.a would be useful.

2.17. For which of the statements 2.15 and 2.16 their analogues for polynomials with complex coefficients hold?

Now we give a generalized form of assertion 2.14 for an arbitrary number of steps in the definition of the expressibility by radicals.

2.18. A *rational fraction* is a 'formal ratio of polynomials', i.e. a pair $f/g := (f, g)$ of polynomials with $g \neq 0$. We define $f/g \sim f'/g'$ if and only if $fg' = f'g$. The polynomial f is identified with the pair $(f, 1)$. Denote by $\mathbb{R}(u_1, \ldots, u_n)$ the set of all rational fractions with real coefficients in variables $u_1, \ldots, u_n$.

(a) Define the sum and the product of rational fractions. Are they well-defined? Check this!

(b) Consider the system of Remark 2.6.(d) for $n = 2$, where f_j and p_j are rational functions (not necessarily polynomials). Assume that the system is *minimal*. This means that there is no system with a smaller s, and that f_j^k is not a rational fraction of $x+y, xy, f_1, \ldots, f_{j-1}$ for any $j = 1, \ldots, s$ and $k < k_j$. Then $s = 1$, $k_1 = 2$, and there exists

a rational fraction $a \in \mathbb{R}(u, v)$ such that

$$f_1(x, y) = (x - y)a(x + y, xy).$$

(c)* State and prove the analogue of (a), where rational fractions $f_1, \dots, f_s$ are replaced by functions $\mathbb{R}^2 \to \mathbb{R}$ (while $p_0, \dots, p_s$ are still rational fractions) and equalities for rational fractions are replaced by equalities for functions defined for all $(x, y) \in \mathbb{R}^2$.

2.5 Insolvability 'in real polynomials'

In this subsection we often omit the arguments (x, y, z) of polynomials in formulae.

2.19. There are no polynomials $f(x, y, z)$, $p(u, v, w)$ and $q(u, v, w, \tau)$ with real coefficients such that

$$\begin{cases} f(x, y, z)^k = p\big(\sigma_1(x, y, z), \sigma_2(x, y, z), \sigma_3(x, y, z)\big) \\ x = q\big(\sigma_1(x, y, z), \sigma_2(x, y, z), \sigma_3(x, y, z), f(x, y, z)\big) \end{cases}.$$

(a) for $k = 1$; (b) for $k = 3$; (c) for $k = 2$;
(d) for any integer $k > 0$.

For the proof the following definition and statement are useful. A polynomial $f \in \mathbb{R}[x, y, z]$ is called **cyclic symmetric** if $f(x, y, z) = f(y, z, x)$.

2.20. If $f \in \mathbb{R}[x, y, z]$ and the polynomial
(a) f^3; (b) f^2
is cyclic symmetric, then f is cyclic symmetric.

Remark 2.21 (cf. solution of Problem 2.8.c)**.** There are no polynomials

$$f_1(x, y, z), \quad f_2(x, y, z), \quad p_0(u, v, w), \quad p_1(u, v, w, \tau_1), \quad p_2(u, v, w, \tau_1, \tau_2)$$

with real coefficients such that

$$\begin{cases} f_1^2 = p_0(\sigma_1, \sigma_2, \sigma_3) \\ f_2^3 = p_1(\sigma_1, \sigma_2, \sigma_3, f_1) \\ x = p_2(\sigma_1, \sigma_2, \sigma_3, f_1, f_2) \end{cases}.$$

A generalization of Remark 2.21 to an arbitrary number of steps can be formalized by the definition of *expressibility by real radicals*which is obtained from its complex analogue (§2.3) by replacing complex coefficients by real coefficients.

The formulae at the beginning of §2.2 show that x is expressible by real radicals for $n = 2$. The solution of Problem 2.8.ab shows that both polynomials

$$(x - y)(y - z)(z - x) \quad \text{and} \quad x^9y + y^9z + z^9x$$

are expressible by real radicals for $n = 3$.

Theorem 2.22. The polynomial x is not expressible by real radicals for $n = 3$.

Theorem 2.22 is yet another formalization of the fact that *a root of a cubic equation is not expressible by real radicals via its coefficients,* see Remark 1.1.e. Theorem 2.22 is implied by the following lemma.

Lemma 2.23 (keeping cyclic symmetry)**.** If $q > 0$ is an integer, $f \in \mathbb{R}[x, y, z]$ and the polynomial f^q is cyclic symmetric, then f is cyclic symmetric.

2.24. For which of the statements from this subsection their analogues for polynomials with complex coefficients hold?

Toward algorithms of solving algebraic equations

presented by A. Enne, A. Skopenkov,
A. Glebov, A. Chilikov, B. Vukorepa

3 Problems after the semifinal

3.1 Insolvability 'in polynomials'

The definition of expressibility by radicals for a polynomial is given in §2.2. Formally, the Ruffini Theorem 2.7 follows from Lemma 3.4. The most difficult and interesting task is to invent the statement of this lemma. In order to do that we prove the following simple facts. Explain why the polynomial x is not a polynomial of $x+y$ and xy.

3.1. The polynomial x_1 is not expressible by radicals in such a way that the second operation in the definition of expressibility is applied only for

(a) $k=2$ (*hint:* see Problem 2.24); (b) $k=3$.

3.2. Which of the following assertions are true for every $f \in \mathbb{C}[x_1,\dots,x_5]$?

(a) If f^3 is cyclic symmetric, then f is cyclic symmetric.

(b) If f^5 is cyclic symmetric, then f is cyclic symmetric.

(c) If f^3 is symmetric, then f is symmetric.

(d) If f^2 is symmetric, then f is symmetric.

A cycle of length 3 is a permutation of an n-element set which moves some 3 elements cyclically and does not change positions of any other elements. A polynomial $f \in \mathbb{C}[x_1,\dots,x_n]$ is **even symmetric** if for any cycle α of length 3 the polynomials $f(x_1,x_2,\dots,x_n)$ and $f(x_{\alpha(1)},x_{\alpha(2)},\dots,x_{\alpha(n)})$ are equal.

3.3. (a) Find a cyclic symmetric polynomial that is not even symmetric.

(b) If a permutation does not change the polynomial from your solution of Problem 3.2.d, then it can be represented as a composition of cycles of length 3.

Lemma 3.4 (keeping even symmetry)**.** If $q>0$ is an integer, $f \in \mathbb{C}[x_1,\dots,x_5]$, and the polynomial f^q is even symmetric, then f is even symmetric.

3.5. Suppose $f \in \mathbb{C}[x_1, \dots, x_n]$ is a polynomial.

(a) If the polynomial f^7 is even symmetric, then f is even symmetric.

(b) If $n \geqslant 5$ and the polynomial f^3 is even symmetric, then f is even symmetric.

(c) If $n \geqslant 5$, then any cycle of length 3 on an n-element set can be written as a product of permutations of the form $(ab)(cd)$, where a, b, c, d are pairwise distinct (i.e. as a product of compositions of transpositions with disjoint supports).

3.6. The definition of *rational* expressibility by real (complex) radicals is analogous to the definition of expressibility by radicals. Polynomials are replaced by rational fractions (with appropriate coefficients; see the definition in Problem 2.18). Is the polynomial x_1 rationally expressible by

(a) real radicals for $n = 3$?

(b) (complex) radicals for $n = 5$?

3.2 Representability using only one cubic root

Here we develop the ideas from § 2.1.

3.7. Can the following number be represented as $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ with $a, b, c \in \mathbb{Q}$:

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

(f) the maximal real root of $x^3 - 4x + 2 = 0$;

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

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

Lemma 3.8. Assume that $r \in \mathbb{R} - \mathbb{Q}$ and $r^3 \in \mathbb{Q}$.

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

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

(b′) **Linear independence over $\mathbb{Q}[\varepsilon_3]$.** If

$$k, \ell, m \in \mathbb{Q}[\varepsilon_3] := \{u + v\varepsilon_3 \colon u, v \in \mathbb{Q}\}$$

and $k + \ell r + mr^2 = 0$, then $k = \ell = m = 0$.

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

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

(e) **Conjugation.** If $a, b, c \in \mathbb{Q}$ and a polynomial has root $x_0 := a + br + cr^2$, then the numbers

$$x_1 := a + b\varepsilon_3 r + c\varepsilon_3^2 r^2 \quad \text{and} \quad x_2 := a + b\varepsilon_3^2 r + c\varepsilon_3 r^2$$

are also its roots.

(f) **Rationality.** If $a, b, c \in \mathbb{Q}$, then the number $a + br + cr^2$ is a root of some cubic polynomial.

Theorem 3.9. If a polynomial is irreducible over $\mathbb{Q}$ and has a root $a+br+cr^2$ for some $r \in \mathbb{R}-\mathbb{Q}$ and $a, b, c, r^3 \in \mathbb{Q}$, then this polynomial is cubic and it has exactly one real root.

Lemma 3.10 (Extension)**.** A number expressible by real radicals with only one extraction of a cubic root can be represented as $a+br+cr^2$, where $r \in \mathbb{R}$ and $a, b, c, r^3 \in \mathbb{Q}$.

3.3 Representability using only one root of prime order

3.11. Can the following number 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) $\cos\frac{2\pi}{21}$; (c) $\sqrt[11]{3}$; (d) $\sqrt[7]{3}$;

(e) some root of the polynomial $x^7 - 4x + 2$?

Answers: no. The arguments are similar to those in the solutions of problems 3.7. Use lemmas stated below.

Lemma 3.12. Let q be a prime number, $r \in \mathbb{R} - \mathbb{Q}$ and $r^q \in \mathbb{Q}$.

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

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

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

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

Denote

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

3.13. Let q be a prime number, $r \in \mathbb{C} - \mathbb{Q}[\varepsilon_q]$ and $r^q \in \mathbb{Q}[\varepsilon_q]$.

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

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

Lemma 3.14.* Let q be a prime number, $r \in \mathbb{R} - \mathbb{Q}$ and $r^q \in \mathbb{Q}$.

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

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

Theorem 3.15. Assume that a polynomial is irreducible over $\mathbb{Q}$ and has an irrational root $A(r)$, where A is a polynomial and $r \in \mathbb{R}$ is such that $r^q \in \mathbb{Q}$ for some prime q. Then the polynomial has degree q and, if $q \neq 2$, has no other real roots.

The proof is analogous to the proofs of Theorems 2.3, 3.9 and to the solutions of 3.11 (abc). Apply the Conjugation Lemma 3.12.c, the Rationality Lemma 3.12.d, and the Linear Independence over $\mathbb{Q}[\varepsilon_q]$ Lemma 3.14.b.

Lemma 3.16 (Extension)**.** The number expressible by real radicals with only one root extraction is equal to $A(r)$ for some $r \in \mathbb{R}$, $q \in \mathbb{Z}$ and $A \in \mathbb{Q}[x]$, with $r^q \in \mathbb{Q}$.

The proof is similar to the proof of the Extension Lemma 3.10.

3.17. (a–d) Prove the assertions analogous to Problem 3.12 with $\mathbb{Q}$ replaced by any set $F \subset \mathbb{R}$ which is closed under operations of addition, subtraction, multiplication and division by a non-zero number (and with polynomials over $\mathbb{Q}$ replaced by polynomials over F).

Solutions for problems before the semifinal

2.1. *Answers:* (a), (b), (c), (d) "— yes, (e), (f), (g), (h), (i) "— no.

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

(b) We have $\dfrac{1}{7+5\sqrt{2}} = \dfrac{7-5\sqrt{2}}{7^2-2\cdot 5^2} = -7+5\sqrt{2}$.

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

(e) Assume that $\sqrt[3]{2}$ is representable in this form. Then

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

Since $3a^2+b \neq 0$, we have $\sqrt{b} \in \mathbb{Q}$. Thus $\sqrt[3]{2} \in \mathbb{Q}$, which is a contradiction.

Other proofs are similar to the proof of Theorem 2.3.

(f) *A sketch for the first solution.* It is easier to prove right away that

$$\sqrt[3]{2} \neq a+p\sqrt{b}+q\sqrt{c}+r\sqrt{bc}, \quad \text{for any} \quad a,b,c,p,q,r \in \mathbb{Q}.$$

It sufficies to show that $\sqrt[3]{2} \neq u+v\sqrt{c}$ for any $u,v,c \in \mathbb{Q}[\sqrt{b}] := \{x+y\sqrt{b}\colon x,y \in \mathbb{Q}\}$. The idea of our proof is that numbers from $\mathbb{Q}[\sqrt{b}]$ (with b fixed) are ¡¡as good as¿¿ rational numbers, that is the sum, the difference, the product and the quotient of the numbers from $\mathbb{Q}[\sqrt{b}]$ are also the numbers from $\mathbb{Q}[\sqrt{b}]$ (or, scientifically speaking, $\mathbb{Q}[\sqrt{b}]$ — is a *number field*). Therefore we can prove the assertion simillary to (e).

A sketch for the second solution. Assume that $\sqrt{2}+\sqrt[3]{2} = a+\sqrt{b}$ 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. From (e) it follows that $\sqrt{2}+\sqrt[3]{2} \notin \mathbb{Q}$. Hence, $\sqrt{b} \notin \mathbb{Q}$. By the Conjugation Lemma 2.2 (e) for $r = \sqrt{b}$ we have $P(a-\sqrt{b}) = 0$. Since $\sqrt{b} \notin \mathbb{Q}$, then roots $a \pm \sqrt{b}$ are different. 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 $a-\sqrt{b} = -\sqrt{2}+\sqrt[3]{2}$. Therefore $\sqrt[3]{2} = a \in \mathbb{Q}$. This is a contradiction.

(g) Assume that $\cos(2\pi/9)$ is representable in this form. By the formula for the cosine of a triple angle $\cos(2\pi/9)$ is a root of the equation $4x^3-3x = -\frac{1}{2}$. By Lemma 2.2 (f) this equation has a rational root, which is a contradiction.

Another proof is analogous to Theorem 2.3.

(h) 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 signs need not agree. All these numbers are irrational. From Theorem 2.3 it follows that it is sufficient to prove that the polynomial P cannot be written as a product of two quadratic trinomials with rational coefficients. This irreducibility follows from the fact that the product of any two roots of P is irrational.

(i) (Here we use the text by I. Braude-Zolotarev.) The equality

$$\cos(2\pi/7) + \cos(4\pi/7) + \cos(6\pi/7) + \ldots + \cos(14\pi/7) = 0$$

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 $u^3 + u^2 - 2u - 1 = 0$. This equation has no rational roots. Hence the same holds for $8t^3 + 4t^2 - 4t - 1 = 0$. Thus the polynomial $8t^3 + 4t^2 - 4t - 1 = 0$ is irreducible over $\mathbb{Q}$. Now the negative answer to the question follows from Lemma 2.2.f.

(j) is similar to (f).

2.3. Suppose on the contrary that the given polynomial $P(x)$ has a root $x_0 = a \pm \sqrt{b}$. By the Conjugation Lemma 2.2.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 assume that $b \neq 0$. Then $x_0 \neq x_1$. Therefore, P is divisible by $(x-a)^2 - b$. Since $\deg P > 2$ then P is reducible. This is a contradiction.

2.4. Let $\sqrt{c}$ be a number we get with only one extraction of the root, where $c \in \mathbb{Q}$. Prove that all the obtained numbers have the form $a + b\sqrt{c}$ with $a, b \in \mathbb{Q}$.

2.5. Answer: The number is representable if and only if $n \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Or, equivalently, $\varphi(n) \in \{1, 2, 4\}$.

2.8. (a) The polynomial $(x-y)^2(y-z)^2(z-x)^2$ is symmetric.

(One may also reduce (a) to (b).)

(b) Set

$$M = x^9y + y^9z + z^9x \quad \text{and} \quad N = y^9x + x^9z + z^9y.$$

Then $M+N$ and MN are symmetric polynomials. Therefore they are polynomials in elementary symmetric polynomials $\sigma_1, \sigma_2, \sigma_3$. Finally, M itself now can be expressed via $M+N$ and MN by the 'formula for the roots of a quadratic equation', see beginning of §2.3.

2.9. (a) One possible answer is $u + v\varepsilon_3 + w\varepsilon_3^2$.

(b) Set

$$M = x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1 \quad \text{and}$$

$$N = x_2x_4 + x_4x_6 + x_6x_8 + x_8x_{10} + x_{10}x_2.$$

Now one can argue as in 2.8.b.

2.10. (a) The square $(x-y)^2(x-z)^2(x-t)^2(y-z)^2(y-t)^2(z-t)^2$ is symmetric, cf. 2.8.a.

(b) Set

$$M = xy + zt, \quad N = xz + yt, \quad K = xt + yz.$$

By 2.8.c, M can be expressed by radicals using the polynomials

$$M + N + K, \quad MN + MK + NK, \quad MNK.$$

Analogously to the solutions of Problems 2.8 c above and 2.10 (d) below, these polynomials are symmetric. Thus $M = xy + zt$ is expressible by radicals.

(c) Set

$$M = (x+y-z-t)^2, \quad N = (x+z-y-t)^2, \quad K = (x+t-y-z)^2.$$

Then repeat the solution of part (b) to obtain $M = (x+y-z-t)^2$. Then it is easy to obtain $x+y-z-t$.

Alternative solution. We have

$$(x+y-z-t)^2 = (x^2+y^2+z^2+t^2)+2(xy+tz)-2(xt+yz)-2(xz+yt).$$

The first summand is symmetric and the other summands are expressible by radicals due to part (b). Thus $x+y-z-t$ is expressible by radicals.

Solution of the equation of fourth degree using Lagrange resolvent method (solution of the problem 2.10 (d)). To find the roots x, y, z, t of the fourth degree equation it is enough to find the expressions for a, b, c, d from Problem 2.11 (a). By Vieta theorem, a is the coefficient of the equation. Under substitution $x \leftrightarrow y$, polynomials c^2 and d^2 are interchanged, and b^2 goes to itself. After cyclic permutation $x \to y \to z \to t \to x$, polynomials b^2 and d^2 are interchanged, and c^2 goes to itself. Therefore polynomials b^2, c^2, d^2 are permuted for every permutation of variables x, y, z, t. Hence their Vieta polynomials, i.e.

$$b^2+c^2+d^2, \quad b^2c^2+b^2d^2+c^2d^2, \quad b^2c^2d^2,$$

are symmetric. Then these polynomials in x, y, z can be represented as polynomials in the coefficients of the equation. Now by solving the cubic equation we can get b^2, c^2, d^2. Then it is easy to obtain b, c, d.

2.11. Repeatedly use the identities $1+\varepsilon+\varepsilon^2=0$ and $1+i+i^2+i^3=0$.

2.12. Here we show the solution for $q=5$.

(a) We have

$$t(\varepsilon_5\vec{u}_\alpha) = t(u_{\alpha(5)}, u_{\alpha(1)}, u_{\alpha(2)}, u_{\alpha(3)}, u_{\alpha(4)}) = t(\vec{u}_{\alpha\circ(54321)}).$$

Hence

$$Q(\varepsilon_5 u_1, \dots, \varepsilon_5 u_5, y) = \prod_{\alpha\in\Sigma_5} (y - t(\varepsilon_5\vec{u}_\alpha)) =$$

$$= \prod_{\alpha\in\Sigma_5} (y - t(\vec{u}_{\alpha\circ(54321)}) = Q(u_1, \dots, u_5, y).$$

Here

• $(54321) \in \Sigma_5$ is the cycle that sends 5 to 4, 4 to 3, ..., 1 to 5.

• the last equality holds because when α ranges through Σ_5, so does $\alpha \circ (54321)$.

(b) There is a homogeneous polynomial $P_k \in \mathbb{Q}[\varepsilon_5][u_1, \dots, u_5]$ (of 'degree' $120-k$) such that the coefficient of y^k in Q is $P(u_1, \dots, u_5)$,

i.e.

$$Q(u_1, \dots, u_5, y) = \sum_{k=0}^{120} P_k(u_1, \dots, u_5) y^k.$$

By (a) and by homogeneity we have

$$P_k(u_1, \dots, u_5) = P_k(\varepsilon_5 u_1, \dots \varepsilon_5 u_5) = \varepsilon_5^{-k} P_k(u_1, \dots, u_5).$$

If k is not divisible by 5, we obtain $P_k(u_1, \dots, u_5) = 0$ as required.

(c) The polynomial $Q(u_1, \dots, u_5, y)$ is symmetric in $u_1, \dots, u_5$. So all the coefficients (P_k from (b)) of the corresponding polynomial from $\mathbb{Q}[\varepsilon_5, u_1, \dots, u_5][y]$ are symmetric in $u_1, \dots, u_5$. Now the statement follows from the fundamental theorem on symmetric polynomials, Vieta theorem and the fact that the coefficients of f are rational.

2.14. (a) We will prove that there exists $\alpha \in \mathbb{R}$ such that $f(x, y) = \alpha(x - y)$.

Since the polynomial $f^2 = p$ is symmetric, we can assume that the polynomial q is linear in third variable, i.e. $q(u, v, w) = a(u, v) + b(u, v)w$ for some $a, b \in \mathbb{R}[u, v]$ (otherwise we can change q while preserving f, p). Then we have $x = a(x + y, xy) + b(x + y, xy) f(x, y)$.

Now we get $pb^2 = f^2 b^2 = (x - a)^2 = (y - a)^2$. By Lemma 2.15.b we get $x - a = a - y$, since the case $x - a = y - a$ is impossible. Hence $a = (x + y)/2$. Then $(x - y)^2 = 4f^2 b^2 = 4pb^2$. If the polynomial $p = f^2$ is constant, the polynomial $b = \pm(x - y)/2\sqrt{p}$ is not symmetric. Therefore p is not constant. Thus b is constant. Hence $2x = 2q = x + y + 2bf$, from which $b \neq 0$ and $f = \alpha(x - y)$ for $\alpha = 1/2b$.

(b) We will prove that k is even and that there exists $\alpha \in \mathbb{R}$ such that $f(x, y) = \alpha(x - y)$. We can use induction on k with the application of part (a) and the generalization of Lemmas 2.15.be, 2.16. If k is odd, from Lemma 2.16.b we get that f is symmetric. That contradicts the equality $x = q(x + y, xy, f(x, y))$. If $k = 4$, then f^2 is either symmetric or antisymmetric. The first case reduces to part (a). The second one gives us $f^2(x, y) + f^2(y, x) = 0$. We solve the case of arbitrary even k analogously.

(c) Analogously to part (a) we get $x = a + bf$. Therefore, f is a rational fraction. Now the solution is analogous to part (a).

2.15. (a) Define the *leading term* of a polynomial so that the leading term of the product is equal to the product of the leading terms of the factors.

(b) This follows from part (a).

(c) We have $f^2 + fg + g^2 = \left(f + \frac{g}{2}\right)^2 + \frac{3}{4}g^2 = (f - \varepsilon_3 g)(f - \varepsilon_3^2 g)$.

(d) This follows from part (c).

(e) This follows from part (f).

(f) Prove and apply the Bezout theorem for polynomials in u with coefficients in $\mathbb{R}[v]$.

2.16. (a) Since f^2 is symmetric, we have $f(x,y)^2 = f(y,x)^2$. Now by the statement 2.15.b we have $f(x,y) = \pm f(y,x)$.

(b) Use the analogues of statements 2.15.ce.

(c) See the hint for 2.15.f.

2.17. *Answer:* 2.15.abf, 2.16.abc.

2.22. For $n = 3$, the set of polynomials expressible by real radicals is contained in the set of cyclic symmetric polynomials. This statement can be proved by induction on the number of operations from the definition of expressibility in radicals. The induction step follows from Lemma 2.23 on the preservation of cyclic symmetry.

Since the polynomial x is not cyclic symmetric, it is also not expressible in real radicals.

2.23. The proof can be found in [Sk19, p. 9.4.2].

2.24. *Answer:* 2.19.abcd, 2.20.b, 2.23 for all q which are not divisible by 3.

Toward algorithms of solving algebraic equations

presented by A. Enne, A. Skopenkov,
A. Glebov, A. Chilikov, B. Vukorepa

Solutions for problems after the semifinal

3.1. (b) Use the analog of Problem 3.2.c for $n = 3$.

3.2. *Answer:* (c) — true, (a), (b), (d) — not true.

(a) See 2.9.a.

(b) Consider the polynomial $x_1 + \varepsilon_5 x_2 + \varepsilon_5^2 x_3 + \varepsilon_5^3 x_4 + \varepsilon_5^4 x_5$.

(d) Consider the polynomial $\prod\limits_{i<j}(x_i - x_j)$.

(c) Since f^3 is symmetric, we have

$$f^3(x_1, x_2, x_3, x_4, x_5) = f^3(x_2, x_1, x_3, x_4, x_5).$$

Extracting the third root, we have

$$f(x_1, x_2, x_3, x_4, x_5) = \varepsilon_3^q f(x_2, x_1, x_3, x_4, x_5) = \varepsilon_3^{2q} f(x_1, x_2, x_3, x_4, x_5).$$

Thus, $\varepsilon_3^{2q} = 1$, and so $\varepsilon_3^q = 1$. Similarly, $f(\vec{x}) = f(\vec{x}_\alpha)$ for any permutation α exchanging two elements from the set $\{x_1, x_2, x_3, x_4, x_5\}$. Therefore, f is symmetric.

3.3. (a) $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$.

(b) First prove that if a permutation maps the polynomial of Problem 3.2.d to itself, then the permutation is even. This implies that the permutation can be represented as a composition of cycles of length 3, see [ZSS, p. 23.2.4].

3.4. The proof can be found in [Sk15].

3.5. (c) $(abc) = (ac)(de)(ab)(de)$.

3.6. *Answer:* (a), (b) — no.

Lemmas 2.23 on keeping cyclic symmetry and 3.4 on keeping even symmetry also hold for rational fractions, see [Sk15], [Sk19, p. 9.4.2]. After that, we can proceed analogously to the solution of Problem 2.22.

3.7. *Answers*: (a), (c), (d), (e), (f), (h) "— no, (b), (g) "— yes.

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

(a) Assume that $\sqrt{3}$ is representable in this form.

First solution. 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. 3.8.b). So we have $b^3 = -2abc = 2c^3$. Hence either $b = c = 0$ or $\sqrt[3]{2} = b/c$. Both cases are impossible.

Second solution. Denote $P(x) := x^2 - 3$. By the Conjugation Lemma 3.8 (e), P has three roots x_0, x_1, x_2 defined in the statement of the lemma. Since none of them is rational, the equality $b = c = 0$ does not hold. So by the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_3]$ 3.8 (b′) the three roots are distinct. This is a contradiction.

(b) We have $(1 + 5\sqrt[3]{2} + \sqrt[3]{4})(3 + \sqrt[3]{2} - 8\sqrt[3]{4}) = -75$. (This equality can be easily obtained by the undetermined coefficients method or applying Euclid algorithm to $x^3 - 2$ and $x^2 + 5x + 1$, see solution of 3.10.) Therefore,

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

(c) Assume that $\cos(2\pi/9)$ is representable in this form. This number is a root of the equation $4x^3 - 3x = -\frac{1}{2}$. Its other two real roots are $\cos(8\pi/9)$ and $\cos(4\pi/9)$.

Repeat the second solution of (a) for $P(x) := 8x^3 - 6x - 1$. We obtain that the roots x_0, x_1, x_2 are distinct. Since $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$, we have $\overline{x_2} = x_1$. Thus, x_1 and x_2 can not be both real and distinct. This is a contradiction.

(d) Assume that $\sqrt[5]{3}$ is representable in this form. By the Rationality Lemma 3.8 (f), $\sqrt[5]{3}$ is a root of a cubic polynomial. This contradicts to the irreducibility of the polynomial $x^5 - 3$ over $\mathbb{Q}$.

(e) Analogously to (a) and (c), by the Conjugation Lemma 3.8 (e) it follows that the polynomial $x^3 - 3$ has three roots x_0, x_1, x_2 defined in the statement of the lemma. Thus, $(a + br + cr^2)\varepsilon_3^s = a + br\varepsilon_3 + cr^2\varepsilon_3^2$ for some $s \in \{1, 2\}$. By the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_3]$

3.8 (b′) we have $a = 0$ and $bc = 0$. Hence either $\sqrt[3]{3} = br$ or $\sqrt[3]{3} = cr^2$. This is a contradiction.

(f) The proof is analogous to (c).

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

(h) The only real root of this equation is $\sqrt[3]{3} + \sqrt[3]{9}$. Assume that this number is representable in the required form. Repeat the second solution of (a) for $P(x) := x^3 - 9x - 12$. We obtain that x_0, x_1, x_2 are all roots of P.

On the other hand, all roots of the equation are

$$y_0 := \sqrt[3]{3} + \sqrt[3]{9}, \quad y_1 := \sqrt[3]{3}\varepsilon_3 + \sqrt[3]{9}\varepsilon_3^2, \quad y_2 := \sqrt[3]{3}\varepsilon_3^2 + \sqrt[3]{9}\varepsilon_3.$$

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

Denote $R(x) := \sqrt[3]{3}x + \sqrt[3]{9}x^2$ and let $S(x) := a + brx + cr^2x^2$ or $S(x) := a + brx^2 + cr^2x$ in the first and second case, respectively. Then the polynomial $R(x) - S(x)$ has three distinct roots 1, ε_3, and ε_3^2. But the degree of this polynomial is at most 2. Thus, $R = S$. Hence either $\sqrt[3]{3} = br$ or $\sqrt[3]{3} = cr^2$. A contradiction.

3.8. (a) Suppose that $x^3 - r^3$ is reducible over $\mathbb{Q}$. 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 a remainder. By (a), the remainder is nonzero. Both polynomials $x^3 - r^3$ and $a + bx + cx^2$ have a root $x = r$. Hence the remainder has the root $x = r$. Thus, the remainder has an irrational root. This is impossible because the remainder has degree 1.

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

(c) Divide our polynomial by $x^3 - r^3$ with a remainder. Taking $x = r$ and applying Linear Independence Lemma (b), we get that the remainder 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 $G(r) = 0$. Hence by (d) we have $G(r\varepsilon_3) = 0 = G(r\varepsilon_3^2)$.

(f) *First solution.* Taking $x = y + a$ we see that it suffices to prove the assertion for $a = 0$. The number $t = br + cr^2$ satisfies $t^3 = b^3r^3 + c^3r^6 + 3bcr^3t$.

In other words, since $u^3+v^3+w^3-3uvw$ is divisible by $u+v+w$, 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. Denote $x_0 := a+br+cr^2$. Expand the numbers x_0^k, $k=0,1,2,3$, as polynomials in r:

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

It suffices to find numbers $\lambda_0,\lambda_1,\lambda_2,\lambda_3 \in \mathbb{Q}$, not all zeros, such that $\lambda_0+\lambda_1 x_0+\lambda_2 x_0^2+\lambda_3 x_0^3=0$. So, these numbers must satisfy the system of equations

$$\begin{cases} \lambda_0 a_0 + \ldots + \lambda_3 a_3 = 0, \\ \lambda_0 b_0 + \ldots + \lambda_3 b_3 = 0, \\ \lambda_0 c_0 + \ldots + \lambda_3 c_3 = 0. \end{cases}$$

It is known that a homogeneous (i.e. with zero right-hand parts) system of linear equations with rational coefficients, where the number of equations is smaller than the number of variables, has a nontrivial rational solution. Hence, the required numbers exist.

The obtained polynomial has degree exactly 3 by lemmas 3.8 (e, b′).

Third solution. Denote $A(x) := a+bx+cx^2$. The product $(x-A(t_0))(x-A(t_1))(x-A(t_2))$ is a symmetric polynomial in t_0,t_1,t_2. Hence this product is a polynomial in x and the elementary symmetric polynomials in t_0,t_1,t_2. The values of these elementary symmetric polynomials at $t_k = r\varepsilon_3^k$ $(k=0,1,2)$ are the coefficients of the polynomial x^3-r^3, and hence are rational. So the considered product is the required polynomial.

3.9. By the Rationality Lemma 3.8 (f) 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 $\deg P \leqslant 3$. By the Conjugation Lemma 3.8 (e), P has three roots x_0,x_1,x_2 defined in the statement of the lemma. Since P is irreducible over $\mathbb{Q}$, none of its roots is rational. So the equality $b=c=0$ is impossible. By the

Linear Independence Lemma over $\mathbb{Q}[\varepsilon_3]$ 3.8 (b′), x_0, x_1, x_2 are distinct. Hence $\deg P = 3$.

Since $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$, we have $\overline{x_2} = x_1$. Hence x_2 and x_1 cannot be real and distinct. So $x_2, x_1 \in \mathbb{C} - \mathbb{R}$. Then P has a unique real root.

3.10. Assume that after extracting the third root we get number r. If $|r| \in \mathbb{Q}$, the statement is trivial. If $|r| \notin \mathbb{Q}$, then the polynomial $x^3 - r^3$ is irreducible over $\mathbb{Q}$.

It suffices to prove that $\frac{1}{a+br+cr^2} = h(r)$ for some polynomial h. By the Irreducibility Lemma, the polynomial $x^3 - r^3$ is irreducible over $\mathbb{Q}$. Hence 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 is the required polynomial.

3.11. Denote $r := \sqrt[7]{2}$ and $A(x) := a_0 + a_1x + a_2x^2 + \ldots + a_6x^6$.

(a) Assume that $\sqrt{3}$ is representable in this form. By the Conjugation Lemma 3.12 (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, the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) yields that these roots are distinct. This is a contradiction.

(b) Assume that $\cos\frac{2\pi}{21}$ is representable in this form.

First solution. Analogously to part (a), the given polynomial P has pairwise distinct roots $x_k := A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \ldots, 6$. Since $P(0) > 0$, $P(1) < 0$, and $P(2) > 0$, the polynomial P has a real root x_k different from x_0. We have $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$. Hence $x_k = \overline{x_k} = x_{7-k}$. A contradiction.

Second solution. Denote by P the 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 $k = 0, \ldots, 6$. One of them, namely $y_2 = -1/2$, is rational.

In the following paragraph we prove that y_0 is irrational.

(Otherwise, the equality $\varepsilon_{21}^2 - 2y_0\varepsilon_{21} + 1 = 0$ implies that $\varepsilon_{21} = a + i\sqrt{b}$ for some $a, b \in \mathbb{Q}$. Then the number $\varepsilon_7 = \varepsilon_{21}^3$ also has this form. But ε_7 is a root of the irreducible[4] polynomial $1 + x + \cdots + x^6$,

[4]The irreducibility of the polynomial $g(x) = 1 + x + \ldots + x^6$ can be proved, e.g.,

which contradicts to the analogue of Theorem 2.3 for numbers of the form $a + i\sqrt{b}$.)

Thus the number y_0 is an irrational root of the polynomial $\frac{2P(x)+1}{2x+1}$ which has degree 6. Then Conjugation Lemma 3.12.c and Linear Independence over $\mathbb{Q}[\varepsilon_q]$ Lemma 3.14.b show that this polynomial has seven distinct roots, which is impossible.

(c) Assume that $\sqrt[11]{3}$ is representable in this form. Then by the Rationality Lemma 3.12 (d), there exists a nonzero polynomial of degree at most 7 having $\sqrt[11]{3}$ as a root. This contradicts the irreducibility of the polynomial $x^{11} - 3$ over $\mathbb{Q}$.

(d) Assume that $\sqrt[7]{3}$ is representable in this form. Analogously to (a), all the complex roots of the polynomial $x^7 - 3$ are $A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \ldots, 6$. Therefore, $A(r)\varepsilon_7^s = A(r\varepsilon_7)$ for some $s \in \{1, 2, 3, 4, 5, 6\}$. Hence by the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) we have $a_k = 0$ for each $k \neq s$. Therefore, $\sqrt[7]{3} = a_s r^s$. This is a contradiction.

(e) Assume that one of the roots is representable in this form. The given polynomial P has no rational roots. Then Conjugation Lemma 3.12.c and Linear Independence over $\mathbb{Q}[\varepsilon_q]$ Lemma 3.14.b yield that P has pairwise distinct roots $x_k := A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \ldots, 6$. Since $P(0) > 0$, $P(1) < 0$, and $P(2) > 0$, the polynomial P has a real root x_k distinct from x_0. From the equality $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$ it follows that $x_k = \overline{x_k} = x_{7-k}$. This is a contradiction.

3.12. (a) All the roots of the polynomial $x^q - r^q$ are $r, r\varepsilon_q, r\varepsilon_q^2, \ldots, r\varepsilon_q^{q-1}$. Assume that $x^q - r^q$ is reducible over $\mathbb{Q}$. Then the absolute value of the constant term of one of its unitary 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 have $kx + qy = 1$ for some integers x, y. Thus, $r = (r^k)^x (r^q)^y \in \mathbb{Q}$. This is a contradiction.

(b) Assume the contrary. Take the smallest degree polynomial $A(x)$ for which the statement is false. Let $R(x)$ be the remainder of $x^q - r^q$ divided by $A(x)$. Then $\deg R < \deg A$, $R(r) = 0$, and $R(x) \neq 0$ by (a). This contradicts the choice of A.

---

by applying the Eisenstein criterion to the polynomial $g(x + 1)$. However, in this particular case it suffices to prove that g has no divisors of degree 1 and 2 with rational coefficients.

(c) The solution is analogous to that of 2.2 (c, d), 3.8 (d). Use (b).

(d) The proofs repeat the second and the third proofs of the Rationality Lemma 3.8 (f). It is only necessary to replace 3 by q and 2 by $q-1$ throughout the proofs (for example, in the second line of the second proof put $k = 0, 1, 2, \dots, q$).

3.13. (a) Assume that our polynomial is reducible. The constant term of any its unitary factor lies in $\mathbb{Q}[\varepsilon_q]$ and equals to $\pm r^k \varepsilon_q^m$ for some m. Then $r^k \in \mathbb{Q}[\varepsilon_q]$. Now as in the proof of Lemma 3.12.a we obtain that $r \in \mathbb{Q}[\varepsilon_q]$. This is a contradiction.

Parts (b,c) are deduced from (a) analogously to the corresponding parts of 3.12.bc.

3.14. (a) Suppose that the polynomial is reducible. Analogously to the proof of the Irreducibility over $\mathbb{Q}[\varepsilon_q]$ Lemma 3.13 (a) we have $r \in \mathbb{Q}[\varepsilon_q]$. Thus, $r^2, r^3, \dots, r^{q-1} \in \mathbb{Q}[\varepsilon_q]$.

In the following paragraph we prove that r is a root of some polynomial of degree at most $q-1$. This would contradict the irreducibility of $x^q - r^q$ over $\mathbb{Q}$.

Expand the numbers r^k as polynomials in ε_q for $k = 0, 1, \dots, q-1$:

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

It suffices to find numbers $\lambda_0, \lambda_1, \dots, \lambda_{q-1} \in \mathbb{Q}$, not all of them zeros, such that

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

Such numbers exist analogously to the corresponding assertion in the second proof of the Rationality Lemma 3.8 (f).

Part (b) follows from (a).

3.15. Assume the contrary. Denote by P the given polynomial. The assumption $q < \deg P$ contradicts to the Rationality Lemma 3.12.d. If $q \geqslant \deg P$, then by the Conjugation Lemma 3.12.c and the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_q]$ 3.14 (b), the polynomial P has pairwise distinct roots $x_k = A(r\varepsilon_q^k)$ for $k = 0, 1, 2, \dots, q-1$. For $q > \deg P$ we get a contradiction. When $q = \deg P$ the conditions $q \neq 2$ and $\overline{x_k} = x_{q-k} \neq x_k$ yield the uniqueness of the real root.

References

[Al] *Alekseev V. B.*, Abel's Theorem in Problems and Solutions. Springer Netherlands, 2004.

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

[Dor] *Dörrie H.*, 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.

[E2] *Edwards H. M.*, The construction of solvable polynomials Bull. Amer. Math. Soc. 2009. V. 46. P 397–411. Errata: Bull. Amer. Math. Soc. 46 (2009), 703-704.

[Es] *Esterov A.*, Galois theory for general systems of polynomial equations, `https://arxiv.org/abs/1801.08260`

[FT] *Fuchs D., Tabachnikov S.*, Mathematical Omnibus. AMS, 2007.

[Had] *Hadlock Ch. R.*, Field Theory and its Classical Problems. The Mathematical Association of America, 1978. (Carus Mathematical Monographs, N 19.)

[Ka] *Kannunikov A. L.*, The beginning of Galois theory: solvability of algebraic equations by radicals (in Russian). `http://www.mathnet.ru/conf1015`.

[Ko17] *Kogan E.*, Set complexity of construction of a regular polygon, `https://arxiv.org/abs/1711.05807`.

[Kol] *Kolosov V. A.*, Theorems and problems in algebra, number theory and combinatorics (in Russian). M.: Helios, 2001.

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

[Pr07-2] *Prasolov V. V.*, Problems in algebra, arithmetics and analysis, Moscow, MCCME, 2007.

[PSo] *Prasolov V. V.*, *Solovyev Y. P.*, Elliptic Functions and Elliptic Integrals. AMS, 1997.

[Saf] *Safin A.*, A program for construction of regular polygons by compass and ruler. `http://www.mccme.ru/mmks/dec08/Safin.pdf`.

[Sk10] *Skopenkov A.*, Basic embeddings and Hilbert's 13th problem (in Russian), Mat. Prosveschenie, 14 (2010) 143–174, `http://arxiv.org/abs/1001.4011`. Abridged English translation: `http://arxiv.org/abs/1003.1586`.

[Sk11] *Skopenkov A.*, A simple proof of the Abel-Ruffini theorem on insolvability of equations in radicals (in Russian), Mat. Prosveschenie, 15 (2011) 113-126. `http://arxiv.org/abs/1102.2100`.

[Sk15] *Skopenkov A.*, A short elementary proof of the Ruffini-Abel Theorem. `http://arxiv.org/abs/1508.03317`.

[Sk19] *Skopenkov A.*, Mathematics via problems: from olympiads and math circles to a profession. Algebra. AMS, Providence, to appear.

[St94] *Stillwell J.*, Galois theory for beginners, Amer. Math. Monthly, 101 (1994), 22-27.

[T] *Tikhomirov V. M.*, Abel and his great theorem, Kvant. 2003. N 1. P. 11–15.

[Vag] *Vaguten H.*, Conjugated numbers (in Russian), Kvant. 1980. N 2. P. 26–32.

[Vi] *Vinberg E. B.*, Algebra of polynomials (in Russian). M.: Prosveschenie, 1980.

[ZSS] Mathematics via problems: from olympiads and math circles to a profession (in Russian). Editors: A. Zaslavsky, A. Skopenkov and M. Skopenkov. MCCME, 2018. Abridged version: `http://www.mccme.ru/circles/oim/materials/sturm.pdf`.

[SZ19] Mathematics via problems: from olympiads and math circles to a profession. Geometry and Combinatorics. Editors: A. Zaslavsky, and M. Skopenkov. AMS, Providence, to appear.

[W] *Van der Waerden B. L.*, Algebra. Frederick Ungar Publishing, 1970.

4 Additional problems for successful teams

4.1. (a) Let $x, y, r \in \mathbb{R}$, $p, g \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[u, v, w]$ be such that $g(x, y) \notin \mathbb{Q}(x + y, xy)$ and

$$\begin{cases} r^2 = p(x + y, xy) \\ g(x, y) = p_1(x + y, xy, r) \end{cases}$$

(cf. Problem 2.14.c). Then $r \in \mathbb{Q}(x, y)$.

(b) Let $x, y, r \in \mathbb{R}$, $p \in \mathbb{Q}[\sqrt{2}][u, v]$, $g \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[\sqrt{2}][u, v, w]$ be such that $g(x, y) \notin \mathbb{Q}(x + y, xy, \sqrt{2})$ and the equations of (a) hold. Then there are $\rho \in \mathbb{Q}(x, y)$, $\pi \in \mathbb{Q}[\sqrt{2}][u, v]$ and $\pi_1 \in \mathbb{Q}[\sqrt{2}][u, v, w]$ such that the equations of (a) hold with r, p, p_1 replaced by ρ, π, π_1.

(c) **Rationalization Lemma.** Let $x, y, r \in \mathbb{R}$ and $F \subset \mathbb{R}$ a field containing $x + y, xy, r^2$ but not r. If $F(r) \cap \mathbb{Q}(x, y) \not\subset F$, then there is $\rho \in \mathbb{Q}(x, y)$ such that $\rho^2 \in F$ and $F(\rho) = F(r)$.

4.2. Denote $a_j = \sigma_j(x_1, x_2, x_3)$, $j = 1, 2, 3$.

(a) Let $x_1, x_2, x_3, r \in \mathbb{R}$, $p, g \in \mathbb{Q}[u_1, u_2, u_3]$ and $p_1 \in \mathbb{Q}[u_1, u_2, u_3, v]$ be such that $g(x_1, x_2, x_3) \notin \mathbb{Q}(a_1, a_2, a_3)$ and

$$\begin{cases} r^2 = p(a_1, a_2, a_3) \\ g(x_1, x_2, x_3) = p_1(a_1, a_2, a_3, r) \end{cases}.$$

Then $r \in \mathbb{Q}(x_1, x_2, x_3)$.

(b) **Rationalization Lemma.** Let $x_1, x_2, x_3, r \in \mathbb{R}$ and $F \subset \mathbb{R}$ a field containing a_1, a_2, a_3, r^2 but not r. If $F(r) \cap \mathbb{Q}(x_1, x_2, x_3) \not\subset F$, then there is $\rho \in \mathbb{Q}(x_1, x_2, x_3)$ such that $\rho^2 \in F$ and $F(\rho) = F(r)$.

(c) **Proposition.** If $x_1, x_2, x_3 \in \mathbb{R}$ and x_1 is $\{a_1, a_2, a_3\}$-expressible by quadratic real radicals, then x_1 is $\{a_1, a_2, a_3\}$-expressible by quadratic real radicals so that every radical is in $\mathbb{Q}(x_1, x_2, x_3)$.

4.3. (a) Let $x, y, r \in \mathbb{C}$, $p \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[u, v, w]$ be such that

$$\begin{cases} r^3 = p(x + y, xy) \\ x = p_1(x + y, xy, r) \end{cases}$$

(cf. Problem 2.14.d for $k = 3$). Then $r \in \mathbb{Q}[\varepsilon_3](x, y)$.

(b) Same as (a) with $x = p_1(x + y, xy, r)$ replaced by $g(x, y) = p_1(x + y, xy, r)$ for some $g \in \mathbb{Q}[u, v]$ such that $g(x, y) \notin \mathbb{Q}(x + y, xy)$.

(c) **Rationalization Lemma.** Let $x, y, r \in \mathbb{C}$ and $F \subset \mathbb{C}$ a field containing $x+y, xy, \varepsilon_3, r^3$ but not r. If $F(r) \cap \mathbb{Q}(x,y) \not\subset F$, then there is $\rho \in \mathbb{Q}(x,y)$ such that $\rho^3 \in F$ and $F(\rho) = F(r)$.

(d) **Rationalization Lemma.** Same as (c) with x, y replaced by $x_1, \ldots, x_n$ and $x+y, xy$ replaced by $\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)$.

(e) **Rationalization Lemma.** Same as (d) with r^3, ρ^3 replaced by r^q, ρ^q for a prime q and ε_3 replaced by ε_q.

(f) **Proposition.** If

$$x_1, \ldots, x_n \in \mathbb{C}, \quad M := \{\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)\}$$

and x_1 is M-expressible by radicals, then x_1 is M-expressible by radicals so that every radical is in $\bigcup_{q=3}^{\infty} \mathbb{Q}[\varepsilon_q](x_1, \ldots, x_n)$.

4.4. There are numbers $x, y \in \mathbb{R}$ such that if $p \in \mathbb{Q}[u, v]$ and $p(x, y) = 0$, then $p = 0$.

Such numbers are called *algebraically independent over* $\mathbb{Q}$.