Kronecker's proof of Galois insolvability theorem

presented by D. Gerasimov, E. Kogan,
E. Morozov, Y. Pan, A. Skopenkov*

Contents

1 Introduction and main results 2
1.1 Overview and motivation 2
1.2 Insolvability in real radicals 3
1.3 Insolvability in complex radicals 4
1.4 Recommendations for participants 5
2 Proofs as sequences of problems 6
2.1 Representations using only one square root . . . 6
2.2 Representations using only one cubic root 7
2.3 Representations using only one root of prime order 8
2.4 Multiple root extractions 9
2.5 Towards the proof of Kronecker's theorem 10
2.6 Solutions of some problems before the semifinal . 11
2.7 Solutions of other problems 15

*We are grateful to V. Volkov for useful discussions.
D. Gerasimov: Phystex-Lyceum (Dolgoprudnyi).
E. Kogan, E. Morozov: Higher School of Economics (Moscow).
Y. Pan: Henan Institute of Science and Technology (China).
A. Skopenkov: Moscow Institute of Physics and Technology, Independent University of Moscow. `https://users.mccme.ru/skopenko/`.

And the leap is not — is not what I think you sometimes see it as — as breaking, as acting. It's something much more like a quiet transition after a lot of patience and — tension of thought, yes — but with that [enlightenment] as its discipline, its orientation, its truth. Not confusion and chaos and immolation and pulling the house down, not something experienced as a great significant moment.

I. Murdoch, The Message to the Planet

1 Introduction and main results

1.1 Overview and motivation

This subsection is formally not used later.

We present a short exposition of Kronecker's proof of the well-known Galois theorem 1.3.2 on insolvability of algebraic equations in radicals. This proof is interesting because it is presumably the shortest.

We do not use the terms 'Galois group' and even 'group'. However, our presentation is hopefully a nicely paved shortcut to the edge of Galois theory. In the proof of the main result we introduce the idea of conjugation. This is an important particular case of 'field isomorphism' sufficient for the main result. So this project provides a bridge (by showing that there is no gap) between elementary mathematics and Galois theory.

The project is accessible to students familiar with polynomials and complex numbers (permutations are not involved).

We claim no novelty (except possibly expository novelty). The idea of proof presented here is known [Do65, §25], [Pr07, Ti03] and is presumably due to Kronecker. (A mistake in these expositions [Sk21m, Remark 8.4.18b] is corrected in expositions [Sk08, PC19], [Sk21m, §8].) Unfortunately, this proof is not well-known.

The proof presented is also interesting because it does not involve permutations. Thus as the 'reason' for the insolvability we see not that the group A_5 of even permutations is not solvable, but that there is a degree 5 polynomial with rational coefficients irreducible over $\mathbb{Q}$, having more than one real root and having at least one non-real root. So this proof is different from other proofs of Galois and Abel theorems

presented in [Al04, Ay82, Be10, Be06, Br, Ed84, FT, Ha78, Le11, PC19, Pe04, Ro95, St94, Sk15] (see comments and corrections of some mistakes in [Sk15]).

1.2 Insolvability in real radicals

A real number is called **expressible in 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 in 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

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

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

1.2.1. (a) Any real root of a quadratic equation with rational coefficients is expressible in real radicals.

(b) The equation $x^3 + x + 1 = 0$ has exactly one real root which is expressible in real radicals.

(c) The equation $x^4 + 4x - 1 = 0$ has two real roots; both of them are expressible in real radicals.

Theorem 1.2.2. (a) The number $\cos(2\pi/9)$ is not expressible in real radicals.

(b) There exists a cubic polynomial with rational coefficients (for example, $x^3 - 3x + 1$) none of whose roots is expressible in real radicals.

You can prove part (b) of this theorem after solving the problems before the semifinal. You can use without proof part (b) for other problems (only) of §1.2.

1.2.3. (a) For any $n \geqslant 3$ there exists a polynomial of degree n with rational coefficients, one of whose roots is not expressible in real radicals.

(b)* The analogue of (a) with the words 'one of the roots is not expressible' replaced by 'none of the roots is expressible' is correct. (At

the same time, the roots of *some* equations of high degrees, for example, $x^5 = 2$, may well be expressible in real radicals.)

(c) 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 in real radicals and the number $\cos(\alpha/3)$ is not expressible in real radicals.

1.3 Insolvability in complex radicals

A complex number is called **expressible in 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 in 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 $n > 0$.

1.3.1. (a) Any (complex) root of a quadratic equation with rational coefficients is expressible in radicals.

(b) The number $\cos(2\pi/9)$ is expressible in radicals.

(c,d) Same as (a) for equations of 3-rd and 4-th degree.

(e) If the real and the imaginary part of a complex number z are expressible in real radicals, then z is expressible in radicals.

(f) The converse to (e) is incorrect.

Analogous assertions to (a,c,d) for equations of higher degrees do not hold.

Theorem 1.3.2 (Galois)**.** There exists an equation of 5-th degree with rational coefficients (for example, $x^5 - 4x + 2 = 0$) none of whose roots is expressible in radicals.

The famous problem of solvability in radicals was solved by weaker Ruffini-Abel theorems proved a little earlier. Their rigorous statements are more complicated [Sk21m, Ruffini Theorem 8.2.2], [Sk15, Remark 7]. An easier way to solve the solvability problem is presented

in [Sk21m, Theorem 8.1.13 and its proof in §8.4.F]. Here we present an alternative short way: deduction of Galois Theorem 1.3.2 from the following result.

Theorem 1.3.3 (Kronecker)**.** If a polynomial with rational coefficients is irreducible over $\mathbb{Q}$ and has prime degree, has more than one real root and has at least one non-real root, then the polynomial has no roots expressible in radicals.

This theorem is interesting and nontrivial even for polynomials of degree 5. You can prove this theorem after solving the problems after the semifinal.

1.4 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 beans 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 mathematical fact is formulated as a problem, then the objective is to prove this fact. (Open-ended questions are called challenges or riddles; here one must come up with a clear wording, and a proof.) 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 advise 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 Proofs as sequences of problems

In this text 'polynomial with rational coefficients' is called a 'polynomial'. Denote

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

2.1 Representations using only one square root

2.1.1. 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) $\sqrt[3]{2}$;

(e) $\sqrt{2}+\sqrt[3]{2}$; (f) $\sqrt{2+\sqrt{2}}$; (g) $\sqrt{2}+\sqrt{3}+\sqrt{5}$; (h) $\cos(2\pi/9)$?

Observe that for (g) you would need ideas from §2.4.

Lemma 2.1.2 (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 $b > 0$.

Lemma 2.1.3. 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 2.1.4. 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 $a, b \in \mathbb{Q}$.

2.2 Representations using only one cubic root

2.2.1. 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 2.2.2. 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 2.2.3. Suppose an irreducible polynomial either has more than one real root or its degree is not equal to 1 or 3. Then this polynomial has no root $a + br + cr^2$ for any $r \in \mathbb{R} - \mathbb{Q}$, $a, b, c, r^3 \in \mathbb{Q}$.

Lemma 2.2.4 (Extension)**.** A number expressible in real radicals with only one extraction of a cubic root can be represented as $a+br+cr^2$, where $r \in \mathbb{R}$ and $a, b, c, r^3 \in \mathbb{Q}$.

2.3 Representations using only one root of prime order

2.3.1. 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 $x^7 - 4x + 2$?

Lemma 2.3.2. 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 whose 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

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

2.3.3. 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 2.3.4. * 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 2.3.5. Let q be a prime. Suppose an irreducible over $\mathbb{Q}$ polynomial P either has more than one real root or its degree is not equal to 1 or q. Then there are no polynomial $A \in \mathbb{Q}[x]$ and number $r \in \mathbb{R} - \mathbb{Q}$ such that $r^q \in \mathbb{Q}$ and $A(r)$ is a root of P.

Lemma 2.3.6 (Extension)**.** Any number expressible in 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 $r^q \in \mathbb{Q}$.

Thus if a polynomial of prime degree $q > 2$ is irreducible over $\mathbb{Q}$ and has more than one real roots, then none of these roots is expressible in radicals with only one root extraction.

2.4 Multiple root extractions

2.4.1. Are there rational numbers a, b, c, d for which $\sqrt[3]{2}$ is equal to

(a) $a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}$; (b) $\dfrac{a+\sqrt{b}}{c+\sqrt{b}}$; (c) $a + \sqrt{b} + \sqrt{c}$;

(d) $a + \sqrt{b + \sqrt{c}}$; (e) $a + \sqrt{b} + \sqrt{c} + \sqrt{d}$?

2.4.2. (a) The number $\sqrt[3]{2}$ is not expressible in radicals with only two extractions of square roots.

(b) The number $\cos(2\pi/9)$ is not expressible in radicals with only two root extractions.

If $F \subset \mathbb{C}$, $r \in \mathbb{C}$ and $r^q \in F$ for some positive integer q, then let

$$F[r] := \{a_0 + a_1 r + a_2 r^2 + \cdots + a_{q-1} r^{q-1} \mid a_0, \ldots, a_{q-1} \in F\}.$$

In this text a **field** is a subset of $\mathbb{C}$ which is closed under summation, subtraction, multiplication and division by a non-zero number. The conventional name is 'number field' (the technical term 'field' in mathematics refers to a more general object). This notion is useful for us because the Polynomial Remainder Theorem holds for polynomials with coefficients in a field.

Lemma 2.4.3 (Simple Radical Extension)**.** If a number $a \in \mathbb{C}$ is expressible in radicals, then some field containing a can be obtained from $\mathbb{Q}$ using only the following operations: replace a field F by $F[r]$ for $r \in \mathbb{C}$ and a prime q such that $r^q \in F$.

2.4.4. (a–d) Prove the analogues of Assertions 2.3.2.(a–d) with $\mathbb{Q}$ replaced by a field, and with polynomials over $\mathbb{Q}$ replaced by polynomials over the field.

Lemma 2.4.5. Let q be a prime, $F \subset \mathbb{R}$ a field, $r \in \mathbb{R} - F$ and $r^q \in F$. If a polynomial with coefficients in F has degree 3, has three real roots none of which lies in F, then none of the roots lies in $F[r]$.

2.5 Towards the proof of Kronecker's theorem

In this subsection $q > 2$ *is a prime,* $r \in \mathbb{C}$ *a number,* $\varepsilon = \varepsilon_q$ *and* $F \subset \mathbb{C}$ *a field containing* r^q, ε *but not* r.

Lemma 2.5.1. (a) **Irreducibility.** The polynomial $t^q - r^q \in F[t]$ is irreducible over F.

(b) **Linear independence.** If $P(r) = 0$ for some polynomial $P \in F[t]$ of degree less than q, then $P = 0$.

(c) **Conjugation.** If $P(r) = 0$ for some polynomial $P \in F[t]$, then $P(r\varepsilon^k) = 0$ for every $k = 1, \dots, q-1$.

(d) **Parametric conjugation.** If $P \in F[x,t]$ and $P(x,r) = 0$ as a polynomial in x, then $P(x, r\varepsilon^k) = 0$ as a polynomial in x for every $k = 0, 1, \dots, q-1$.

(e) **Rationality.** For any $H \in F[x,t]$ we have

$$H(x,r)H(x,\varepsilon r)\dots H(x,\varepsilon^{q-1}r) \in F[x].$$

(f) **Reality.** If $F = \overline{F}$ and either $r \in \mathbb{R}$ or $|r|^2 \in F$, then either among the values $A(r\varepsilon^k)$, $k = 0, 1, \dots, q-1$, of a polynomial $A \in F[t]$ at most one is real, or all these values are real.

2.5.2. (a) Suppose that $H \in F[x,t]$ is a polynomial such that $H(x,r)$ is irreducible over $F[r]$. Then for any $k = 0, 1, \dots, q-1$ the polynomial $H(x, r\varepsilon^k)$ is irreducible over $F[r]$ as well.

(b) Let $G \in F[x]$ be an irreducible over F polynomial. Suppose that $H \in F[x,t]$ is a polynomial such that $0 < \deg H < \deg G$ and $H(x,r)$ is an irreducible over $F[r]$ factor of G. Then G is divisible in F by the product

$$H(x,r)H(x,\varepsilon r)\dots H(x,\varepsilon^{q-1}r).$$

(c) If in addition to the assumptions of (b) $\deg G$ is a prime, then there is a polynomial $A \in F[t]$ such that the roots of G are $A(r\varepsilon^k)$ for $k = 0, 1, \dots, q-1$.

Lemma 2.5.3 (Keeping Irreducibility)**.** Let $r \in \mathbb{C}$ be a number. Suppose that $F = \overline{F}$ and either $r \in \mathbb{R}$ or $|r|^2 \in F$. Take a polynomial $G \in F[t]$ of prime degree which has more than one real root and has at least one non-real root. If G is irreducible over F, then G is irreducible over $F[r]$.

Lemma 2.5.4 (Hard Radical Extension)**.** (a) If a number $a \in \mathbb{R}$ is expressible in radicals, then some field containing a can be obtained from $\mathbb{Q}$ using only the following operations: replace a field F by $F[r]$ for $r \in \mathbb{C}$ such that either $r \in \mathbb{R}$ or $|r|^2 \in F$, and $r^q \in F$ for a prime q.

(b) Same as (a) with $r^q \in F$ replaced by $r^q, \varepsilon \in F$.

In 2.5.4(b) you can use the following result without proof. For an elementary one-page proof see [Sk21m, §8.4.D].

Theorem 2.5.5 (Gauss Lowering Degree Theorem)**.** If q is a prime, then the number ε is expressible in radicals using only roots of degree $q-1$.

2.6 Solutions of some problems before the semifinal

1.2.2. (a) Apply the triple-angle formula for cosine. We see that the numbers $\cos(2\pi/9)$, $\cos(8\pi/9)$, $\cos(14\pi/9)$ are the roots of the equation $8y^3 - 6y + 1 = 0$. By (b) none of these numbers is expressible in real radicals.

1.2.3. (a,c) This follows from Theorems 1.2.2.b,a, respectively.

1.3.1. (c,d) Use *del Ferro and Ferrari methods* [Sk21m, §3].

2.1.2. 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!).

2.1.1. *Answers:* (a), (b), (c) — yes, (d), (e), (f), (g) — 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) 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.

(e) *Sketch of the first solution.* It is easier to prove the stronger assertion:

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

It suffices 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 $\mathbb{Q}[\sqrt{b}]$ (the common terminology: $\mathbb{Q}[\sqrt{b}]$ *is a number field*). Then we can prove the assertion similarly to (d).

Sketch of 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. We have $\sqrt{2} + \sqrt[3]{2} \notin \mathbb{Q}$ (prove this!). Hence $\sqrt{b} \notin \mathbb{Q}$. By the Conjugation Lemma 2.1.3 (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.

(f) 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 2.1.4 it follows that it is sufficient to prove that the polynomial P cannot be written as a product of two quadratic polynomials with rational coefficients. This irreducibility follows from the fact that the product of any two roots of P is irrational.

(g) See [Sk21m, Problem 8.3.1(g)].

(h) See [Sk21m, Problem 8.3.3($n = 9$)].

2.1.2. 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!).

2.1.3. (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[1] by $x^2 - r^2$:

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

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

Substitute $x = r$. By the Linear Independence Lemma (see (b)) the remainder is 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.

2.1.4. Suppose to the contrary that the given polynomial P has a root $x_0 = a \pm \sqrt{b}$, where $b \notin \mathbb{Q}$. By the Conjugation Lemma 2.1.3.e and analogously to it, the number $x_1 = a \mp \sqrt{b}$ is also a root of P. Since $\sqrt{b} \notin \mathbb{Q}$, we have $b \neq 0$. Then $x_0 \neq x_1$. Therefore P is divisible by $(x - a)^2 - b$. Since $\deg P > 2$, the polynomial P is reducible. This is a contradiction.

2.2.1. *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. 2.2.2.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 2.2.2 (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 $\mathbb{Q}[\varepsilon_3]$ 2.2.2 (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 2.2.4.) 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 $\cos(4\pi/9)$.

2.2.2. (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 2.2.2 (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.

2.2.4. 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.

2.3.1. *Answers: no.* The arguments are similar to those in the solutions of problems 2.2.1. Use lemmas stated below the problem.

2.3.5. The proof is analogous to the proofs of Theorems 2.1.4, 2.2.3 and to the solutions of 2.3.1 (abc).

2.3.6. The proof is similar to the proof of the Extension Lemma 2.2.4.

2.7 Solutions of other problems

2.1.2. Let $\sqrt{c}$ be the number we obtain 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 $a, b \in \mathbb{Q}$.

2.2.1. (d) Assume that $\sqrt[5]{3}$ is representable in this form. By the Rationality Lemma 2.2.2 (f), $\sqrt[5]{3}$ is a root of a cubic polynomial. This

contradicts to the irreducibility of the polynomial $x^5 - 3$ over $\mathbb{Q}$.

Repeat the second solution of (a) for $P(x) := x^5 - 3$ has three roots x_1, x_2, x_3. all three roots are distinct. Therefore, $x^5 - 3$ is divisible by $(x - x_1)(x - x_2)(x - x_3)$.

First solution. Expand the numbers 1, $3^{1/5}$, $3^{2/5}$, and $3^{3/5}$ as polynomials in r. We get that these four numbers are linearly dependent This shows that there exists a nonzero polynomial of degree at most 3 having a root $3^{1/5}$. This contradicts the irreducibility of $x^5 - 3$ over $\mathbb{Q}$.

(e) Analogously to (a) and (c), by the Conjugation Lemma 2.2.2 (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 $\mathbb{Q}[\varepsilon_3]$ 2.2.2 (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, by the del Ferro theorem all roots of P 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 P has exactly one real root, $x_0 = y_0$. 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.

2.2.3. By the Rationality Lemma 2.2.2 (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 2.2.2 (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 $\mathbb{Q}[\varepsilon_3]$ 2.2.2 (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.

2.3.3. See [Sk21m, Problem 8.3.23].

2.3.4. See [Sk21m, Problem 8.3.24].

2.4.1. See [Sk21m, Problem 8.3.9].

2.4.2. (a) See [Sk21m, Theorem 8.1.2].
(b) See [Sk21m, Theorem 8.1.5].

2.4.3. See [Sk21m, Lemma 8.4.1b].

2.4.4. (a,b,c) See [Sk21m, Lemma 8.4.14].
(d) See [Sk21m, Lemma 8.4.17].

2.4.5. See [Sk21m, Lemma 8.4.11a].

For solutions of the remaining problems see [Sk21m, Lemma 8.4.14, §8.4.E,G]. In particular, proofs of Theorems 1.2.2.a and 1.3.3 are presented in [Sk21m, §8.4.E,G], respectively.

References

[Al04] *V. B. Alekseev*, Abel's Theorem in Problems and Solutions. Springer Netherlands, 2004.

[Ay82] *R. G. Ayoub*, On the Nonsolvability of the General Polynomial, Amer. Math. Monthly, 89:6 (1982), 397–401.

[Be06] *J. Bewersdorff,* Galois Theory for Beginners: A Historical Perspective, AMS, 2006.

[Be10] *J. Bergen*, A Concrete Approach to Abstract Algebra: From the Integers to the Insolvability of the Quintic, 2010.

[Br] *J. Brown,* Abel and the insolvability of the quintic, `http://www.math.caltech.edu/~jimlb/abel.pdf`.

[Do65] *H. Dörrie*, 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.

[Ed84] *H. M. Edwards* , Galois Theory. Springer Verlag, 1984.

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

[Ha78] *Ch. R. Hadlock*, Field Theory and its Classical Problems. The Mathematical Association of America, 1978.

[Le11] *L. Lerner*, Galois Theory without abstract algebra. `http://arxiv.org/abs/1108.4593`.

[PC19] *Y. Pan and Y. Chen.* On Kronecker's Solvability Theorem, `http://arxiv.org/abs/1912.07489`.

[Pe04] *P. Pesic*, Abel's Proof, The MIT Press, 2004, Cambridge, Massachusetts, London, England.

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

[Ro95] *M. I. Rosen*, Niels Hendrik Abel and Equations of the Fifth Degree, Amer. Math. Monthly, 102:6 (1995) 495-505.

[Sk08] *A. Skopenkov.* Some more proofs from the Book: solvability and insolvability of equations in radicals, `http://arxiv.org/abs/0804.4357`.

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

[Sk21m] *A. Skopenkov.* Mathematics Through Problems: from olympiades and math circles to a profession. Part I. Algebra. 2021, AMS, Providence. Preliminary version: `https://www.mccme.ru/circles/oim/algebra_eng.pdf`

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

[Ti03] *V. M. Tikhomirov*, Abel and his great theorem (in Russian), Kvant. 2003. N 1. P. 11–15.