QUADRATIC IRRATIONALS

A. Belov-Kanel, P. Kozlov and A. Skopenkov

abridged translation from Russian by P. Dergach and A. Skopenkov

Introduction.

In this note we sketch an elementary proof of the following result concerning constructibility of regular polygons.

The Gauss Theorem. *A calculator (calculating with absolute precision) has operations*

$$1, \quad +, \quad -, \quad \times, \quad : \quad \textit{and} \quad \sqrt{}$$

(and infinite memory). If

$$n = 2^{\alpha} p_1 \dots p_l,$$

where $p_1, \dots, p_l$ are distinct primes of the form $2^{2^s}+1$, then the number $\cos\dfrac{2\pi}{n}$ is calculable at this calculator.

In order to make the above Gauss Theorem (and the main idea of the Galois theory) less accessible, they are usually explained in terms of 'fields extensions' and 'Galois groups'. The proof sketched below is elementary and does not use these terms (it does not even use the term 'group'!). However, the idea presented is one of the main ideas of the Galois theory ('*group and rule*', or '*unite and rule*'). The proof of the constructibility is implicitly contained in the Gauss papers and is explicitly known in (at least USSR math circles) folklore.

Steps of the proof are presented as problems marked with bold numbers. If the statement of a problem is an assertion, then the problem is to prove this assertion.

Constructions by compass and ruler.

A. Using segments of length a and b construct (from now on: by means of compass and ruler) segments of length $a+b$, $a-b$, ab/c, $\sqrt{ab}$.

A real number is called a *quadratic irrationality* or *calculable*, if we can calculate this number using our calculator. For example, the numbers

$$1+\sqrt{2}, \quad \sqrt[4]{2}=\sqrt{\sqrt{2}}, \quad \sqrt{2\sqrt{3}}, \quad \sqrt{2}+\sqrt{3}, \quad \sqrt{1+\sqrt{2}}, \quad \frac{1}{1+\sqrt{2}} \quad \text{and} \quad \cos 3^\circ$$

are calculable. This is not evident for the last two numbers.

B. Every calculable number is constructible.

This result is a corollary of A. It shows that if the number $\cos\frac{2\pi}{n}$ is *calculable* then the regular n-gon is *constructible*.

C*. *Main theorem of the theory of geometric constructions.* Every constructible number is calculable.

From this result it follows that if we cannot calculate the number $\cos\frac{2\pi}{n}$, then we cannot construct the regular n-gon.

D. If a complex number z is *complex-calculable* (the definition is analogous with only one distinction: the calculator gives *two* square roots of a complex number), then the real part and the imaginary part of z are calculable.

E. If the regular mn-gon is constructible, then the regular m-gon is constructible.

F. The regular triangle and the regular pentagon are constructible. Or, equivalently, $\cos\frac{2\pi}{3}$ and $\cos\frac{2\pi}{5}$ are calculable.

G. The regular 120-gon is constructible. Or, equivalently, the angle 3° is constructible. The following problems are hints.

H. If the regular n-gon is constructible, then the regular $2n$-gon is constructible.

I. If the regular n-gon and m-gon are constructible and $GCD(m,n)=1$, then the regular mn-gon is constructible.

Hint to problem C. Consider all possible cases of construction of new objects (points, lines, circles) and prove that the coordinates of all the constructed points and the coefficients of equations of all the constructed lines and circles are quadratic irrationals.

Hint to problem D. If $\sqrt{a+bi}=u+vi$, then u,v are expressed by quadratic radicals of a and b.

Hint to problem H. Bisect the angle or apply the half angle formula.

Hint to problem I. Since $GCD(m,n)=1$, it follows that there exist integers a,b such that $am+bn=1$.

The constructibility in the Gauss theorem.

It is not difficult to prove the constructibility in the Gauss theorem for $n\le 16$.

Proof of the constructibility in the Gauss theorem for $n=5$. It suffices to calculate the number $e=\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}$. We shall construct some functions of e. We know that $e+e^2+e^3+e^4=-1$. It is easy to see that $(e+e^4)(e^2+e^3)=e+e^2+e^3+e^4=-1$. Denote $A_0:=e+e^4$ and $A_1:=e^2+e^3$. Then A_0 and A_1 are roots of the equation $t^2+t-1=0$ by the Vieta theorem. Hence these numbers are calculable. Since $e\cdot e^4=1$, the numbers e and e^4 are roots of the equation $t^2-A_0t+1=0$ by the Vieta theorem. Therefore we can calculate e (and e^4).

1. If 2^m+1 is a prime then m is a power of 2.

Idea of proof of the constructibility in the Gauss theorem. It suffices to prove the Gauss Theorem for $n=2^m+1$ a prime (then m is necessarily a power of 2). It suffices to calculate

$$e=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}.$$

First it would be good to split the sum

$$e+e^2+\cdots+e^{n-1}=-1$$

into two summands A_0 and A_1 whose *product* is calculable (or, in other words, to *group* the roots of the equation

$$1+e+e^2+\cdots+e^{n-1}=0$$

in a clever way). Then A_0 and A_1 would be calculable by the Vieta Theorem.

Next it would be good to split the sum A_0 into two summands A_{00} and A_{01} whose product is calculable, and analogously split $A_1=A_{10}+A_{11}$. And so on, until we calculate $A_{0\ldots0}=e$.

It is however quite non-trivial to find the necessary splittings.

Primitive Root Theorem. For each prime $p=2^m+1$ there exists an integer g such that the residues modulo p of $g^1,g^2,g^3\ldots,g^{2^m}$ are distinct.

Construction of necessary splittings is given in problems 3a, 4a and 5a below.

2. *Proof of the Primitive Root Theorem.* Suppose that p is a prime and a is not divisible by p.

(a) Suppose that k is the smallest positive integer such that $a^k \equiv 1\ (p)$. Then $p-1$ is divisible by k. (Use the Fermat Little Theorem.)

(b) For every integers n and a the congruence $x^n \equiv a\ (p)$ has at most n solutions.

(c) If $p-1$ is divisible by d then the congruence $x^d \equiv 1\ (p)$ has exactly d solutions.

(d) Prove the Primitive Root Theorem for $p = 2^m + 1$. (Only this case is necessary for the Gauss theorem.)

(e)* Prove the Primitive Root Theorem for $p = 2^m \cdot 3^n + 1$.

(f)* Prove the Primitive Root Theorem for *arbitrary* prime p.

(g)* Is it true that 3 is a primitive root modulo p for every prime of the form $p = 2^m + 1$?

From now on let g be a primitive root modulo a prime $p = 2^m + 1$.

3. (a) Set

$$A_0 := e^{g^2} + e^{g^4} + e^{g^6} + \cdots + e^{g^{2^m}} \quad \text{and} \quad A_1 := e^{g^1} + e^{g^3} + e^{g^5} + \cdots + e^{g^{2^m-1}}.$$

Prove that $A_0 A_1 = -\frac{p-1}{4}$.

The following problems are hints.

(b) $g^k + g^l \equiv 0\ (p)$ iff $k - l \equiv \frac{p-1}{2}\ (p-1)$.

(c) We have

$$A_0 A_1 = \sum_{s=1}^{2^m} e^s \alpha(s),$$

where $\alpha(s)$ is the number of solutions (k, l) (in residues modulo $p-1$) of the congruence

$$g^{2k} + g^{2l+1} \equiv s\ (p).$$

(d) $\alpha(s) = \alpha(gs)$.

(e) $\alpha(s)$ does not depend on s.

4. (a) Set

$$A_{00} := e^{g^4} + e^{g^8} + e^{g^12} + \cdots + e^{g^{2^m}} \quad \text{and}$$

$$A_{01} := e^{g^2} + e^{g^6} + e^{g^{10}} + \cdots + e^{g^{2^m-2}}.$$

Prove that $A_{00} A_{01} = sA_0 + tA_1$ for certain integers s and t (in fact, $s + t = \frac{p-1}{8}$).

(b) (hint) The congruence

$$g^{4k} + g^{4l+2} \equiv s\ (p)$$

has the same number of solutions (k, l) (in residues modulo $p-1$) as the congruence

$$g^{4k} + g^{4l+2} \equiv sg^2\ (p).$$

We have $g^a + g^b \equiv 0\ (p)$ if and only if $a - b \equiv 2^{m-1}\ \ (p-1)$.

5. (a) Set

$$A_{10} := e^{g^1} + e^{g^5} + e^{g^9} + \cdots + e^{g^{2^m-3}} \quad \text{and}$$

$$A_{11} := e^{g^3} + e^{g^7} + e^{g^{11}} + \cdots + e^{g^{2^m-1}}.$$

Prove that $A_{10} A_{11} = uA_0 + vA_1$ for certain integers u and v (in fact, $u + v = \frac{p-1}{8}$).

(b) $\cos\frac{2\pi}{17}$ is calculable.

(c) Complete the proof of possibility in the Gauss theorem.

6. Find an explicit expression involving square roots for

(a) $\cos\dfrac{2\pi}{17}$. (b)* $\cos\dfrac{2\pi}{257}$. (c)* $\cos\dfrac{2\pi}{65537}$.

Using the above method and computer, this problem is easily solvable (in spite of the story from *J. Littlewood, Mathematical Miscellany*).

Remark. There is another proof of constructibility, like the previous one, but without use of complex numbers. For example, consider the regular 17-gon. Set $a_k = \cos(2\pi k/17)$. Then $a_k = a_{17-k}$, $2a_ka_l = a_{k+l} + a_{k-l}$ and $a_1 + a_2 + a_3 + \cdots + a_8 = -1/2$. First calculate $a_1 + a_2 + a_4 + a_8$ and $a_3 + a_5 + a_6 + a_7$. Then calculate $a_1 + a_4$, $a_2 + a_8$, $a_3 + a_5$ and $a_6 + a_7$. Finally calculate a_1.

Hints and solutions to some problems concerning constructability.

Hint to problem 1. If n is odd, then $2^{kn} + 1$ is divisible by $2^k + 1$.

Hint to problem 2b. Let us prove the following more general statement: a polynomial of degree n cannot have more than n roots in $\mathbb{Z}_p$. Here by a polynomial we mean the collection of coefficients but not the function.

Assume that a polynomial $P(x)$ of degree n has in $\mathbb{Z}_p$ different roots $x_1, \ldots, x_n, x_{n+1}$. Represent $P(x)$ as

$$P(x) = b_n(x - x_1)\ldots(x - x_n) + b_{n-1}(x - x_1)\ldots(x - x_{n-1}) + \cdots + b_1(x - x_1) + b_0$$

('*the Newton interpolation*'). Put in the congruence $P(x) \equiv 0\ (p)$ residues $x = x_1, \ldots, x_n, x_{n+1}$ in this order. We obtain $b_0 \equiv b_1 \equiv \cdots \equiv b_{n-1} \equiv b_n \equiv 0\ (p)$.

The same solution can be presented in the following way. Let P be a polynomial. Then polynomial $P - P(a)$ is divisible by $x - a$, i.e. $P - P(a) = (x - a)Q$ for some polynomial Q such that $\deg Q < \deg P$. Since $P(a) = 0$, it follows that $P = (x - a)Q$ for some polynomial Q of degree less than $\deg P$. Now the required statement can be proved by induction on the degree of the polynomial P.

Hint to problem 2c. Obviously, polynomial $x^{p-1} - 1$ in $\mathbb{Z}_p$ has exactly $p - 1$ roots and is divisible by $x^d - 1$. Prove that if a polynomial of degree a have a roots and is divisible by a polynomial of degree b, then the polynomial of degree b has exactly b roots.

Hint to problem 2d. If there are no primitive roots, then by problem 2a the congruence $x^{2^{m-1}} \equiv 1\ (p)$ has $p - 1 = 2^m > 2^{m-1}$ solutions.

Hint to problem 2ef. Similary to 2d.

Remark to problem 2f. It is easy to deduce from the existence of a primitive root that for $p - 1 = p_1^{a_1} \ldots p_k^{a_k}$ the number of primitive roots is $(p-1)(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_k}) = \varphi(p-1)$.

Hint to problem 3c. Open the parenthesis and group the equal elements of the sum.

Hint to problem 3d. If (k, l) is a solution of the congruence $g^{2k} + g^{2l+1} \equiv s\ (p)$, then $(l, k+1)$ is a solution of the congruence $g^{2k} + g^{2l+1} \equiv gs\ (p)$.

If (k, l) is a solution of the congruence $g^{2k} + g^{2l+1} \equiv gs\ (p)$, then $(l-1, k)$ is a solution of the congruence $g^{2k} + g^{2l+1} \equiv s\ (p)$.

Proof of the impossibility in the Gauss theorem.

Before the proofs of the the Gauss theorem some of their ideas are demonstrated one by one on the easiest examples (problems 1, 2c and 3). However, these examples give the solution of

classical antique problems of the doubling of a cube and the trisection of an angle, which were awaiting for their solutions nearly 2000 years. The first proof of the impossibility in the Gauss theorem is sketched in problems 2ab, 4-7. Seemingly different (but in essence the same) proofs are sketched in problems 8-11 (we use 4, but not use 6), 12 and 13-16. The second proof is the most close to ideas of Gauss.

1. There are no rational numbers a, b, c, d such that $\sqrt[3]{2} =$

(a) $a + \sqrt{b}$; (b) $a - \sqrt{b}$; (c) $\dfrac{1}{a + \sqrt{b}}$; (d) $a + \sqrt{b} + \sqrt{c}$; (e) $a + \sqrt{b} + \sqrt{c} + \sqrt{bc}$;

(f) $a + \sqrt{b + \sqrt{c}}$; (g) $a + \sqrt{b} + \sqrt{c} + \sqrt{d}$.

2. (a) Delete the button ':' from (the complex analogue of) the calculator defined in the Gauss theorem, but allow to use all rational numbers. Then the set of numbers realizable using the new calculator will remain the same.

(b) Number A is constructible if and only if there are positive $r \in \mathbb{Z}$ and $a_1, \dots a_r \in \mathbb{R}$ such that

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_r \subset Q_{r+1} \supset A, \quad \text{where} \quad a_k \in Q_k, \quad \sqrt{a}_k \notin Q_k,$$

$$Q_{k+1} = Q_k[\sqrt{a}_k] := \{\alpha + \beta\sqrt{a}_k \mid \alpha, \beta \in Q_k\} \quad \text{for each} \quad k = 1, ..., r-1.$$

Such a sequence is called *a sequence of quadratic extensions* (this term is considered as one word, we do not use the term 'quadratic extension' alone).

(c) $\sqrt[3]{2}$ is not constructible. (Hence the doubling of a cube by ruler and compass is impossible.)

3. (a) Number $\cos(2\pi/9)$ is a root of the cubic equation $8x^3 - 6x + 1 = 0$.

(b) There are no rational numbers a and b such that $\cos(2\pi/9) = a + \sqrt{b}$.

(c) Number $\cos(2\pi/9)$ is not constructible (hence the trisection of angle $\pi/3$ by ruler and compass is impossible and the regular 9-angled polygon is not constructible).

(d) The roots of a cubic equation with rational coefficients are constructible if and only if one of these roots is rational.

4. *Conjugation lemma.* Using the notation of 2b define the conjugation map $\bar{\cdot} : Q_k[\sqrt{a}] \to Q_k[\sqrt{a}]$ by the following formula: $\overline{x + y\sqrt{a}} = x - y\sqrt{a}$. Then

(a) This map is well-defined.

(b) $\overline{z + w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z}\,\overline{w}$ and $\overline{z} = z \Leftrightarrow z = x + 0\sqrt{a} \in Q_{k-1}$.

(c) If $z \in Q_k[\sqrt{a}]$ is a root of a polynomial P with rational coefficients, then $P(\overline{z}) = 0$.

(Compare with the lemma on complex roots of polynomials with real coefficients.)

5. (a) Prove that polynomial $\Phi(x) := x^{12} + x^{11} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$.

Hint: if you have difficulties use the Gauss lemma and the Eisenstein criterion (see below).

(b) If number $e = \cos(2\pi/13) + i\sin(2\pi/13)$ is constructible, then there exists a sequence $\mathbb{Q} = Q_1 \subset Q_2 \subset \ldots \subset Q_k \subset Q_{k+1}$ of quadratic extensions such that $\Phi(x)$ is reducible over Q_{k+1} and is irreducible over Q_k.

(c) If Φ is divisible by polynomial P with coefficients in Q_{k+1}, then Φ is divisible by conjugate (relatively to Q_k) polynomial $\overline{P}$.

(d) The decomposition of polynomial $\Phi(x)$ over Q_{k+1} into irreducible factors is divided into pairs of conjugate (relatively to Q_k) factors.

(e) For each of these factors there exists a sequence analogous to (b) but possibly has another n.

(f) Number $\cos(2\pi/13)$ is not constructible.

(g) Number $\cos(2\pi/p)$ is not constructible for p a prime, $p \neq 2^m + 1$.

6. (a) *The Gauss lemma.* If a polynomial with integer coefficients is irreducible over $\mathbb{Z}$, then it is irreducible over $\mathbb{Q}$ [Pr].

(b) *The Eisenstein criterion.* Let p be a prime. If the leading coefficient of a polynomial with integer coefficients is not divisible by p, other coefficients are divisible by p and the constant term is not divisible by p^2, then this polynomial is irreducible over $\mathbb{Z}$ [Pr].

7. (a) Polynomial $\Phi(x) = 1 + x^{17} + x^{34} + x^{51} + \cdots + x^{272}$ is irreducible over $\mathbb{Q}$.

Hint: use the Gauss lemma and the Eisenstein criterion.

(b) Number $\cos(2\pi/289)$ is not constructible.

(c) Prove the impossibility in the Gauss theorem.

8. Number $\cos(2\pi/7)$ is not constructible (hence the regular heptagon is not constructible).

9. Let $n = 4k + 3$ be a prime. Denote $f_s = e^s + e^{-s}$. The least length of a minimal sequence from problem 2b is called a *rank* of α.

(a) For each k number $f_1^k + f_2^k + \cdots + f_{(p-1)/2}^k$ is rational.

(b) After openning the parenthesis and grouping the equal elements in the equation $(x - f_1)(x - f_2)\ldots(x - f_{(p-1)/2})$ we obtain a polynomial with rational coefficients.

(c) Ranks of numbers $e, e^2, \ldots, e^{p-1}$ are equal.

(d) Ranks of numbers $f_1, \ldots, f_{(p-1)/2}$ are equal.

(e) Number $\cos(2\pi/n)$ is not constructible.

10. Denote $e = \cos(2\pi/13) + i\sin(2\pi/13)$, $g = 2$ is a primitive root modulo 13,

$$A_0 = e^{g^0} + e^{g^3} + e^{g^6} + e^{g^9}, \quad A_1 = e^{g^1} + e^{g^4} + e^{g^7} + e^{g^{10}} \quad \text{and} \quad A_2 = e^{g^2} + e^{g^5} + e^{g^8} + e^{g^{11}}.$$

$$(a) \quad A_0^2 = 4 + A_1 + 2A_2, \quad A_1^2 = 4 + A_2 + 2A_0 \quad \text{and} \quad A_2^2 = 4 + A_0 + 2A_1.$$

(b) Numbers A_0, A_1, A_2 are roots of an irreducible cubic equation with rational coefficients.

(c) Numbers A_0, A_1, A_2 have the same rank.

(d) Number $\cos(2\pi/13)$ is not constructible.

11. Number $\cos(2\pi/p)$ is not constructible for

(a) $p = 3 \cdot 2^k + 1$ a prime.

(b) p a prime, $p \neq 2^m + 1$.

(c) $p = 289$.

(d) number p that is not a product of a power of 2 and distinct prime numbers of the form $2^m + 1$.

12. Consider polynomial with given constructible number as a root. Prove that the minimal degree of such a polynomial is a power of two. Then prove the impossibility in the Gauss theorem.

The idea of another proof of the impossibility in the Gauss theorem is expressed by the notions of *a field* and *the dimension of a field.*

13. Consider a subset of the set $\mathbb{C}$ of complex numbers. This subset is called *a (numerical) field* if it is closed under addition, subtraction, multiplication and division.

(a) The following sets are fields: $\mathbb{Q}$, the set of constructible numbers, the set of real numbers, $\mathbb{Q}[\sqrt{2}] := \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Q}\}$, each Q_k in a sequence of quadratic extensions and

$$\mathbb{Q}[e] := \{\alpha_0 + \alpha_1 e + \alpha_2 e^2 + \alpha_3 e^3 + \cdots + \alpha_{12} e^{12} \mid \alpha_i \in \mathbb{Q}\}, \quad \text{where} \quad e = \cos\frac{2\pi}{13} + i\sin\frac{2\pi}{13}.$$

(b) Any field contains field $\mathbb{Q}$.

(c) Any field that contains $\sqrt{2}$ should contain $\mathbb{Q}[\sqrt{2}]$.

(d) Any field that contains e should contain $\mathbb{Q}[e]$.

14. *The dimension* $\dim F$ of a field F is the least k for which there exist

$$b_2, b_3 \ldots, b_k \in F, \quad \text{such that} \quad F = \{\alpha_1 + \alpha_2 b_2 + \alpha_3 b_3 + \cdots + \alpha_k b_k \mid \alpha_i \in \mathbb{Q}\},$$

if such k exists.

(a) $\dim \mathbb{Q} = 1$.

(b) $\dim \mathbb{Q}[\sqrt{2}] = 2$.

(c) In a sequence of quadratic extensions $\dim Q_k = 2 \dim Q_{k-1}$ for $k \geq 1$.

(d) In a sequence of quadratic extensions $\dim Q_k = 2^{k-1}$.

(e) If $G \subset F$ are fields, then $\dim F$ is divisible by $\dim G$.

15. (a) $\dim \mathbb{Q}[\cos \frac{2\pi}{13} + i \sin \frac{2\pi}{13}] \leq 12$.

(b) If $\dim \mathbb{Q}[\cos \frac{2\pi}{13} + i \sin \frac{2\pi}{13}] < 12$, then $P(e) = 0$ for some polynomial P with rational coefficients, where the degree of P is less than 12.

(c) Use the previous assertions to prove that number $\cos(2\pi/13)$ is not constructible.

16. (a) $\dim \mathbb{Q}[\cos \frac{2\pi}{289} + i \sin \frac{2\pi}{289}] = 272$.

(b) Use the previous assertions to prove that number $\cos(2\pi/289)$ is not constructible.

(c) Prove the impossibility in the Gauss theorem.

17. (a) Any constructible number is algebraic, i.e. it is a root of an polynomial with rational coefficients. (This fact together with the transcendence of $\sqrt{\pi}$ implies the impossibility of squaring the circle by compass and ruler. The transcendence of $\sqrt{\pi}$ is an implication of the transcendence of π that is proved by Lindemann in 1883.)

(b) Let P be a polynomial with constructible roots. If P has rational coefficients and has an odd degree, then one of its roots is rational.

(c)* The roots of a polynomial of degree 4 with rational coefficients are constructible if and only if the *resolution cubic equation* [Ko, Pr] has a rational root.

Hints and solutions to some problems concerning impossibility.

Hint to problem 1c. Multiply by conjugate.

Hint to problem 2a. Induction on the number of operations of the calculator, which are necessary to construct given number; use multiplication by conjugate.

Hint to problem 2b. It is a simple corollary of problem 2a.

Solution of problem 2c. Suppose that $\sqrt[3]{2}$ is constructible. Then there exists a sequence of quadratic extensions

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_{r-1} \subset Q_r \quad \text{such that} \quad \sqrt[3]{2} \in Q_r \setminus Q_{r-1}.$$

Since $\sqrt[3]{2} \notin \mathbb{Q}$, it follows that $r \geq 2$. Then

$$\sqrt[3]{2} = \alpha + \beta\sqrt{a}, \quad \text{where} \quad \alpha, \beta, a \in Q_{r-1}, \quad \sqrt{a} \notin Q_{r-1} \quad \text{and} \quad \beta \neq 0.$$

Then

$$2 = (\sqrt[3]{2})^3 = (\alpha^3 + 3\alpha\beta^2 a) + (3\alpha^2\beta + \beta^3 a)\sqrt{a} = u + v\sqrt{a}.$$

Since $2 \in \mathbb{Q} \subset Q_{r-1}$, it follows that $2 - u \in Q_{r-1}$. From

$$v\sqrt{a} = 2 - u \quad \text{and} \quad v \in Q_{r-1} \quad \text{we obtain} \quad 0 = v = 3\alpha^2\beta + \beta^3 a.$$

Since $3\alpha^2 + \beta^2 a > 0$, it follows that $\beta = 0$. A contradiction.

Hint to problem 3a. Express $\cos 3\alpha$ by $\cos\alpha$.

Hint to problem 3b. If $\cos(2\pi/9) = a+\sqrt{b}$, then $a-\sqrt{b}$ is also a root of equation $8x^3-6x+1 = 0$. Hence by the by the Vieta theorem the third root is equal to $-(a+\sqrt{b}) - (a-\sqrt{b}) = -2a \in \mathbb{Q}$.

Solution of problem 3c. It is a corollary of 3a and 3d.

Proof of the theorem 3d for cubic equations all whose three roots are real (this case is sufficient to the impossibility of construction of regular 9-angled polygon). The part 'if' is obvious. Let us prove the 'only if' part. Suppose the contrary, i.e. that at least one of the roots is constructible. For each constructible root z consider the minimal sequence of quadratic extensions

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_{r-1} \subset Q_r, \quad \text{for which} \quad z_1 \in Q_r \setminus Q_{r-1}.$$

Consider the root $z = z_1$ with the least length l of minimal sequence.

Since the equation has no rational roots, it follows that $l \geq 2$. Hence,

$$z_1 = \alpha + \beta\sqrt{a}, \quad \text{where} \quad \alpha, \beta, a \in Q_{l-1}, \quad \sqrt{a} \notin Q_{r-1} \qquad \text{and} \quad \beta \neq 0.$$

Hence number $\overline{z}_1 = \alpha - \beta\sqrt{a}$ is also a root of the considered equation (by the Conjugation lemma). Since $\beta \neq 0$, it follows that $\alpha - \beta\sqrt{a} \neq \alpha + \beta\sqrt{a}$, i. e. $\overline{z}_1 \neq z_1$. Denote $z_2 := \overline{z}_1$. By the Vieta formula for our equation we have:

$$z_1 + z_2 + z_3 = (\alpha + \beta\sqrt{a}) + (\alpha - \beta\sqrt{a}) + z_3 = 2\alpha + z_3 \in \mathbb{Q}, \quad \text{hence} \quad z_3 \in Q_{l-1}.$$

Therefore for the root z_3 there exists a sequence of quadratic extensions whose length is less than that for the root z_1. A contradiction. □

Hint to problem 5a. Apply the Eisenstein criterion to $((x+1)^{13}-1)/x$ and the Gauss lemma.

Solution of problem 5b. Consider a sequence of quadratic extensions $\mathbb{Q} = Q_1 \subset Q_2 \subset \ldots \subset Q_{r-1} \subset Q_r \supset e$. Notice that polynomial Φ is reducible over Q_r (because Φ has e as a root). Hence there exists l for which polynomial Φ is reducible over Q_{l+1}. Let k be the minimal such l. From problem 5a it follows that $k \geq 1$. Now it is easy to see that the sequence $\mathbb{Q} = Q_1 \subset Q_2 \subset \ldots \subset Q_k \subset Q_{k+1}$ is the required.

Hint to problem 5c. Conjugate relatively to Q_k the equation $\Phi(x) = P(x)R(x)$.

Hint to problem 5d. It is sufficient to prove that if the polynomial P with coefficients in Q_{k+1} divides Φ, then P and $\overline{P}$ are relatively prime. For this prove that $GCD(P, \overline{P})$ has the coefficients in Q_k and use the irreducibility of polynomial Φ in Q_k.

Solution of problem 5e. Analogously to problem 5b.

Hint to problem 5f. Prove that the decomposition of polynomial $\Phi(x)$ constructed in problem 5d has exactly two factors (use the fact that if the coefficients of polynomial P are in Q_{k+1}, then the coefficients of polynomial $P\overline{P}$ are in Q_k). The same is true also for decompositions of new factors and so on. Using this prove that the degree of polynomial $\Phi(x)$ should be a power of two.

Hint to problem 5g. Analogously to problem 5f.

Hint to problem 6b. Suppose the contrary and apply indefinite coefficient method.

Hint to problem 7a. Apply the Eisenstein criterion to $\Phi(x+1)$ and the Gauss lemma.

Hint to problem 7b. Analogously to problem 5 prove that if number $\cos\dfrac{2\pi}{289}$ is constructible, then the degree of polynomial $\Phi(x)$ should be a power of two. A contradiction.

Solution of problem 8. Consider complex number $e = \cos(2\pi/7) + i\sin(2\pi/7)$. Since $e \neq 1$, it follows that number e is a root of an equation $e^6 + e^5 + e^4 + e^3 + e^2 + e + 1 = 0$. Let us divide both parts of the equation by e^3. Denote

$$f := e + e^{-1}, \quad \text{then} \quad e^2 + e^{-2} = f^2 - 2 \quad \text{and} \quad e^3 + e^{-3} = f(e^2 + e^{-2} - 1).$$

We have a cubic equation

$$f(f^2 - 3) + (f^2 - 2) + f + 1 = 0, \quad \text{i.e.} \quad f^3 + f^2 - 2f - 1 = 0.$$

The candidates for rational roots of this equation $f = \pm 1$ are easily rejected. Using theorem 3d on cubic equations one can observe that number $f = e + e^{-1}$ is not constructible. Hence e is not constructible (explain why).

Hint to problem 9a. Induction on k.

Hint to problem 9b. It is a corollary of problem 9a and the fact that every symmetric polynomial of variables $f_1, f_2, \ldots, f_{(p-1)/2}$ is rationaly expressed via polynomials of type $f_1^k + f_2^k + \cdots + f_{(p-1)/2}^k$.

Solution of problem 9c. Since for each $s, t \in \{1, 2, \ldots, p-1\}$ there exists k such that $e^s = (e^t)^k$, it follows that ranks of numbers $e, e^2, \ldots, e^{p-1}$ are the same.

Solution of problem 9d. Since $e^s + e^{-s}$ is rationaly expressed via $e + e^{-1}$, it follows that for each $s, t \in \{1, 2, \ldots, p-1\}$ number $e^s + e^{-s}$ is rationaly expressed via $e^t + e^{-t}$ (Analogously to problem 8). Hence ranks of numbers $f_1, \ldots, f_{(p-1)/2}$ are the same.

(Observe that $rk(e + e^{-1}) = rke - 1$.)

Solution of problem 9e. Let $r := rkf_s$. Hence for some sequence of quadratic extensions

$$f_s = \alpha_s + \beta_s\sqrt{a}, \quad \text{where} \quad \alpha_s, \beta_s, a \in Q_{r-1}, \quad \sqrt{a} \notin Q_{r-1} \quad \text{and} \quad \beta_s \neq 0.$$

Hence number $\overline{f}_s = \alpha_s - \beta_s\sqrt{a}$ is also a root of considered polynomial (by the Conjugation lemma). Since

$$\beta_s \neq 0, \quad \text{it follows that} \quad \alpha_s - \beta_s\sqrt{a} \neq \alpha_s + \beta_s\sqrt{a}, \quad \text{i. e.} \quad \overline{f}_s \neq f_s.$$

So roots $f_1, \ldots, f_{(p-1)/2}$ are split into pairs of conjugates. Hence number $(p-1)/2$ is even. A contradiction.

Solution of problem 10a. We prove the first formula (the others are proved analogously). Notice that $g^6 = -1$. Hence

$$A_0^2 = ((e^{g^0} + e^{-g^0}) + (e^{g^3} + e^{-g^3}))^2 \underset{(*)}{=}$$

$$= 2 + e^{g^1} + e^{-g^1} + 2 + e^{g^4} + e^{-g^4} + 2(e^{g^0} + e^{g^6})(e^{g^3} + e^{g^9}) = 4 + A_1 + 2A_2.$$

The last equation holds because

$$(e^{g^0}+e^{g^6})(e^{g^3}+e^{g^9}) = e^{g^0+g^3}+e^{g^3+g^6}+e^{g^6+g^9}+e^{g^9+g^0} = e^{g^0+g^3}A_0 \underset{(*)}{=} e^{g^8}A_0 = A_2.$$

(Equations marked with $(*)$ hold because $g = 2$.)

Hint to problem 10b. Prove that $A_0 + A_1 + A_2$, $A_0^2 + A_1^2 + A_2^2$, $A_0^3 + A_1^3 + A_2^3$ are rational.

Hint to problem 10c. Using problem 10a and $A_0 + A_1 + A_2 = -1$ prove that A_i is rationaly expressed via each A_j.

Hint to problem 10d. Solution is obtained from problems 10b и 10c analogously to problem 9e.

There is another solution that does not use 10c. Suppose that number A_0 has rank r. Conjugate A_0 relatively to Q_{r-1}. The obtained number will be one of the numbers A_i (explain why). Now one can observe that A_i's are split into pairs of conjugates. Hence the number of A_i's is even. A contradiction.

Hint to problem 11a. Analogously to problem 10.

Hint to problem 11b. Suppose that for $p = 2^k r + 1$ the number $\cos\dfrac{2\pi}{p}$ is constructible (where $r > 1$ is odd). Deduce that numbers

$$A_i = e^{g^i} + e^{g^{r+i}} + \cdots + e^{g^{(2^k-1)r+i}}, \quad 0 \le i \le r-1$$

have the same rank and are the roots of polynomial with rational coefficients and degree r.

Hint to problem 11c. Consider numbers

$$A_0 = e^{g^0} + e^{g^{17}} + \cdots + e^{g^{272}}, \quad A_1 = e^{g^1} + e^{g^{18}} + \cdots + e^{g^{273}}, \quad A_{16} = e^{g^{16}} + e^{g^{33}} + \cdots + e^{g^{288}}.$$

Hint to problem 12. Analogously to problem 5.

Hint to problem 14c. Prove that

$$Q_k = \{\alpha_1 + \alpha_2 b \mid \alpha_1, \alpha_2 \in Q_{k-1}\} \quad \text{for each} \quad b \in Q_k - Q_{k-1}.$$

Hint to problem 14d. It is a corollary of problems 14a and 14c.

Hint to problem 14e. The minimal k for which there exist

$$b_1, b_2, \ldots, b_k \in F \quad \text{such that} \quad F = \{\alpha_1 b_1 + \alpha_2 b_2 + \alpha_3 b_3 + \cdots + \alpha_k b_k \mid \alpha_i \in G\},$$

if such k exists, is called the dimension $\dim(F : G)$ of the field F over the field G. Prove that $\dim F = \dim G \dim(F : G)$.

Hint to problem 15b. Prove that there exist rational numbers $a_0, a_1, \ldots, a_{12}$, not all equal to 0 and such that

$$a_0 + a_1 e + \cdots + a_{11} e^{11} = 0. \qquad (*)$$

By definition of dimension there exist $b_1, \ldots, b_{11} \in \mathbb{Q}[\cos\dfrac{2\pi}{13} + i\sin\dfrac{2\pi}{13}]$ and $\alpha_{kl} \in \mathbb{Q}$ such that

$$e^{j-1} = \alpha_{j,1} b_1 + \alpha_{j,2} b_2 + \cdots + \alpha_{j,11} b_{11} \quad \text{for} \quad j = 1, 2, \ldots, 12.$$

Substitute these expressions for e^i to $(*)$. Then consider equations stating that coefficients of $b_1, \ldots, b_{11}$ are zeroes. Finally prove that the obtained system of equations has a nonzero rational solution.

Hint to problem 16a. Analogously to problems 15ab. Use the irreducibility of polynomial $\Phi(x) = 1 + x^{17} + x^{34} + x^{51} + \cdots + x^{272}$.

Hint to problem 17a. Let $a{=}a_1$ and $b{=}b_1$ be constructible numbers, P and Q polynomials with rational coefficients of minimal degree such that a and b are their roots, respectively. Let $a_2, \ldots, a_m$ be all other complex roots of P and $b_2, \ldots, b_n$ all other complex roots of Q. Notice that

$a + b$ is a root of polynomial $P(x - b_1) \ldots P(x - b_n)$,
$a - b$ is a root of polynomial $P(x + b_1) \ldots P(x + b_n)$,
ab is a root of polynomial $P(\frac{x}{b_1}) \ldots P(\frac{x}{b_n})$,
$\frac{a}{b}$ is a root of polynomial $P(xb_1) \ldots P(xb_n)$,
$\sqrt{a}$ is a root of polynomial $P(x^2)$.
Now it suffices to prove the lemma.

Lemma. Let $R(x, y)$ be a polynomial in two variables with rational coefficients, $b_1, b_2, \ldots, b_n$ are all complex roots of polynomial Q with rational coefficients. Then a polynomial $R(x, b_1)R(x, b_2) \ldots R(x, b_n)$ with one variable also has rational coefficients.

Solution of problem 17b. Analogously to problems 5bc.