SOME TOPICS IN ALGEBRAIC EQUATIONS

EUGENE TYRTYSHNIKOV

Institute of Numerical Mathematics, Russian Academy of Sciences, Moscow
tee@inm.ras.ru

1. Foreword. Applications do not necessarily mean practical applications. In these notes, in particular, we can see some very useful applications of linear algebra to ancient problems of construction by compasses and ruler and then to the problem of solvability of algebraic equations by radicals.

In this lecture course we go straightforwardly to some famous results of algebra in the hope that a concise and rigorous exposition may help to make difficult topics more friendly and less difficult. The notes produce the whole picture of the course and contain all basic steps and fundamental theorems. However, the proofs are not in the notes and will be presented during the school.

Please be aware that next to none of the steps evolved in these notes is trivial. So the proofs are essential part of the course. I hope we can enjoy them together as the ideas and even details of the proofs are generally deep, ingenious and beautiful.

2. Background knowledge. Groups, cyclic groups, subgroups, normal subgroups, conjugate elements, quotient (factor) groups, symmetric groups, alternating groups, abelian groups, isomorphisms, homomorphisms. Fields, subfields, extension fields. Algebraic equations, fundamental theorem of algebra. Symmetric polynomials, elementary symmetric polynomials.

3. Extension fields as linear spaces. For any two fields with the property $K \subset L$ we say that L is an *extension field* over K. In such cases we simply write $L = L : K$.

An extension field $L : K$ can be viewed as a linear space over the field K. The extension is called *finite* if the dimension of this space, called also *degree of extension* and denoted by $\dim(L : K)$, is finite.

Theorem 3.1. *Assume that extensions $L : K$ and $M : L$ are finite. Then the extension $M : K$ is finite and* $\dim(M : K) = \dim(M : L) \dim(L : K)$.

4. Algebraic extensions. Any finite extension $L : K$ is *algebraic.* That means that *any element $\theta \in L$ is a root of a nonzero polynomial $f(x) \in K[x]$, where $f(x)$ depends on θ.*

To prove this, consider the elements

$$1 = \theta^0, \theta^1, \dots, \theta^n \in L.$$

If $n = \dim(L : K)$ then these elements are linearly dependent over K, i.e. there exist elements $a_0, \dots, a_n \in K$ such that

$$a_0 + a_1\theta + \dots a_n\theta^n = 0$$

and at least one of the coefficients a_i is nonzero. Then

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \in K[x] \quad \text{and} \quad f(\theta) = 0.$$

A nonzero polynomial of minimal degree with the property $f(\theta) = 0$ is called a *minimal polynomial* for the element $\theta \in L$. Any root of a nonzero polynomial over K is called an *algebraic element* over K.

Let us require that the senior coefficient of $f(x)$ is unity. Then it is easy to prove that the minimal polynomial for θ is unique. If it has only simple roots, then θ is called a *separable element* over K.

Irreducible polynomials with multiple roots exist: let $\mathbb{Z}_2$ be a field just with two elements (remainders modulo 2), then a polynomial $f(x) = x^2 - u$ is irreducible over $\mathbb{Z}_2(u)$ (rational functions of u with coefficients in $\mathbb{Z}_2$) but has a multiple root.

If K contains $\mathbb{Q}$ then it is easy to prove that any algebraic element over K is separable. The same holds true if K is a finite field. If all elements in $L = L : K$ are separable over K, then the extension $L : K$ is called *separable.*

5. Adjunction of an element. Let $L = L : K$ and $\theta \in L\backslash K$ be an algebraic element over K. Denote by $K(\theta)$ the intersection of all subfields F in L such that $F = F : K$ and $\theta \in F$. Note that $K(\theta)$ is an extension field over K. We say that $K(\theta)$ is obtained by *adjunction of θ to the field K.*

THEOREM 5.1. *Let n be the degree of minimal polynomial for $\theta \in L\backslash K$. Then*

$$K(\theta) = \{g(\theta) : \ g(x) \in K[x], \ \deg g(x) \leq n - 1\}.$$

COROLLARY 5.2. *The extension $K(\theta) : K$ is finite and*

$$\dim(K(\theta) : K) = n.$$

COROLLARY 5.3. *If θ is a root of an irreducible polynomial $f(x) \in K[x]$, then*

$$\dim(K(\theta) : K) = \deg f(x).$$

THEOREM 5.4. *If $L : K$ is finite and separable, then there exists a single element $\theta \in L$ such that $L = K(\theta)$.*

If $L = K(\theta)$, then θ is called a *primitive element* of the extension $L : K$.

6. Irreducibility of polynomials overs $\mathbb{Q}$. The following important observation is due to Gauss.

THEOREM 6.1. *Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}$ if and only if it is irreducible over $\mathbb{Z}$.*

THEOREM 6.2. *Let p be prime. Then $f(x) = 1 + x + \ldots + x^{p-1} \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Z}$.*

COROLLARY 6.3. *If p is prime then $f(x) = 1 + x + \ldots + x^{p-1} \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$.*

7. Constructions by compasses and ruler. Assume that a segment of length 1 is drawn on a plane, and we are asked to construct a segment of length θ using only compasses and ruler. When analysing this problem, sooner or later one naturally reveals that such a construction is possible if and only if there exists a chain of extension fields

$$\mathbb{Q} = \mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \ldots \subset \mathbb{Q}_s$$

such that $\theta \in \mathbb{Q}_s$ and

$$\dim(\mathbb{Q}_k : \mathbb{Q}_{k-1}) = 2, \quad 1 \le k \le s.$$

THEOREM 7.1. *A regular polyhedron with n edges can be constructed by compasses and ruler if and only if $n = 2^m p_1 \ldots p_k$, where $p_1, \ldots, p_k$ are prime numbers of the form $p_i = 2^{l_i} + 1, \quad 1 \le i \le k$.*

The main ingredient of proof is the case of a prime $n \ge 3$. Let us prove right away that it is necessary for the construction that $n = 2^l + 1$.

Assume that the above chain of extension fields exists with the property

$$\theta = \cos\frac{2\pi}{n} \in \mathbb{Q}_s.$$

Consider the nth root of unity

$$\zeta = \exp\{\mathbf{i}\,2\pi/n\}, \quad \mathbf{i} = \sqrt{-1}.$$

Then $2\theta = \zeta + \zeta^{-1}$. Hence, ζ is a root of the quadratic polynomial

$$f(x) = x^2 - 2\theta x + 1 \in \mathbb{Q}_s[x],$$

which is irreducible over $\mathbb{Q}_s$. Therefore, we can extend the chain so that

$$\mathbb{Q}_{s+1} = \mathbb{Q}_s(\zeta) : \mathbb{Q}_s, \quad \dim(\mathbb{Q}_{s+1} : \mathbb{Q}_s) = 2.$$

By Theorem 3.1,

$$\dim(\mathbb{Q}_{s+1} : \mathbb{Q}) = 2^{s+1}.$$

At the same time,

$$\mathbb{Q}(\zeta) \subset \mathbb{Q}_{s+1},$$

and from Theorems 6.2 and 5.1 it follows that

$$\dim(\mathbb{Q}(\zeta) : \mathbb{Q}) = n - 1$$

so long as n is prime. Consequently, $n-1$ is a divisor of 2^{s+1}. Thus, n must be of the form $n = 2^l + 1$.

The condition on a prime n, that it is of the form $n = 2^l + 1$, is also sufficient for the construction of a regular n-hedron by compasses and ruler. However, we are not ready to prove this at this moment, we will be able to do this only after some nontrivial preparations.

8. Normal extensions. A finite extension $L : K$ is called *normal* if any irreducible polynomial over K with a root belonging to L has all its roots from L.

THEOREM 8.1. *An extension $L : K$ is normal if and only if L can be obtained from K by the adjunction of all roots of a single polynomial over K.*

If $\theta_1, \ldots, \theta_n$ are all roots of a polynomial $f(x) \in K[x]$, then

$$L = K(\theta_1, \ldots, \theta_n) = K(\theta_1)(\theta_2) \ldots (\theta_n)$$

is called a *splitting extension* for the polynomial $f(x)$ over K. Theorem 8.1 states that normal extensions are same as splitting extensions.

By definition, any normal extension $L : K$ is finite, and determined, by Theorem 8.1, by some polynomial over K. However, finding the degree of $L : K$ might be not easy. For example, let $K = \mathbb{Q}$ and L be obtained by the adjunction to K of all roots of the polynomial

$$f(x) = x^5 - 25x + 5 \in K[x].$$

What is the value of $\dim(L : K)$? In order to be able to calculate this dimension we need a deeper insight into the theory of extension fields proposed by Galois.

9. Galois extensions. Any automorphism σ of $L : K$ such that $\sigma(a) = a$ for any $a \in K$ is called an *automorphism of L over K*. The set of all such automorphisms is a group under the composition of automorphisms. This group is denoted by $\mathrm{Aut}(L : K)$.

THEOREM 9.1. *If an extension $L : K$ is finite then*

$$|\mathrm{Aut}(L : K)| \leq \dim(L : K).$$

An instructive example is given by $K = \mathbb{Q}$ and $L = \mathbb{Q}(2^{1/3})$. In this case

$$|\mathrm{Aut}(L : K)| = 1 \quad \text{while} \quad \dim(L : K) = 3.$$

A finite extension $L : K$ is called a *Galois extension* if

$$|\mathrm{Aut}(L : K)| = \dim(L : K).$$

In the case of Galois extension the number of automorphisms of L over K is maximal possible. In such cases the group $\mathrm{Aut}(L : K)$ is referred to as *Galois group* of the extension $L : K$.

10. Galois theory. Consider a Galois extension $M : K$ and its Galois group $G = \mathrm{Aut}(M : K)$. Then, by definition, $|G| = \dim(M : K)$. Given any subgroup $H \subset G$, denote by M^H a set of all elements in M that do not move under all actions of the group H:

$$M^H = \{a \in M : \ h(a) = a \ \forall \ h \in H\}.$$

Evidently, M^H is an intermediate field (called the *fixed field* for H) in between of K and M:

$$K \subseteq M^H \subseteq M.$$

Theorem 10.1. *A finite extension $M : K$ is a Galois extension if and only if $K = M^G$, where $G = \mathrm{Aut}(M : K)$.*

Theorem 10.2. *An extension $M : K$ is a Galois extension if and only if it is normal and separable, and moreover, if and only if M is the splitting field for a polynomial over K with only simple roots.*

Theorem 10.3. *Suppose that $M : K$ is a Galois extension, $G = \mathrm{Aut}(M : K)$. Let L be an intermediate field in between of K and M, and let H be a subgroup in G. Then $H = \mathrm{Aut}(M : L)$ if and only if $L = M^H$. Moreover, the extension $L : K$ is normal if and only if H is a normal subgroup in G. If $L : K$ is normal, then $\mathrm{Aut}(L : K)$ is isomorphic to the quotient group G/H.*

11. Sufficiency for the construction of regular n-hedrons. Let n be a prime number of the form $n = 2^l + 1$ and $\zeta = \exp\{\mathbf{i}2\pi/n\}$. Then for $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta)$ the extension $L : K$ is normal (prove this) and we may consider its Galois group $G = \mathrm{Aut}(L : K)$. The form of n implies that $|G| = 2^l$.

Theorem 11.1. *For any group G of order $|G| = 2^s$, a chain of subgroups*

$$G = G_0 \supset G_1 \supset \ldots \supset G_s = \{e\}$$

exists such that G_i is normal in G_{i-1} and $|G_i/G_{i-1}| = 2$ for every $1 \le i \le s$.

Corollary 11.2. *Let $K = \mathbb{Q}$, an extension $L : K$ be normal, $\dim(L : K) = 2^s$. Then there exists a chain of extension fields*

$$K = L_0 \subset L_1 \subset \ldots \subset L_s = L$$

such that any extension $L_i : L_{i-1}$ is normal and $\dim(L_i : L_{i-1}) = 2$.

It remains to note that any Galois extension $L : K$ of degree 2 is obtained by the adjunction of a root of quadratic polynomial over K. It can be proved as follows.

In such a case the group $G = \mathrm{Aut}(L : K)$ is cyclic, let $\sigma \in G$ be a non-trivial automorphism. Pick up $\theta \in L$ so that

$$\alpha = \theta - \sigma(\theta)$$

is different from 0. It is easy to see that $\sigma(\alpha) = -\alpha$, and hence

$$\sigma(\alpha^2) = \alpha^2.$$

By the Galois theory, $\alpha^2 = a \in K$. Thus, α is a root of the equation $x^2 - a = 0$ with $a \in K$. Consequently, α can be constructed by compasses and ruler.

12. Radical extensions. Let $K = K : \mathbb{Q}$. Then an extension $L : K$ is called *simple radical* in the two cases:

- if $L = K(\varepsilon)$, where ε is a primitive nth root of unity ($\varepsilon^n = 1$ and ε generates all roots of degree n of unity);
- if $\varepsilon \in K$, where ε is a primitive nth root of unity, and $L = K(\alpha)$, where $\alpha^n = a \in K$.

An extension $L : K$ is called *radical* if there is a chain of extension fields

$$K = L_0 \subset L_1 \subset \ldots \subset L_s = L$$

such that any extension $L_i : L_{i-1}$ is simple radical.

If all roots of an algebraic equation with the coefficients from K belong to a radical extension $L : K$, then we say that this equation is *solved by radicals.*

Theorem 12.1. *Any radical extension $L : K$ can be extended to $M : L$ so that the extension $M : K$ is both radical and normal.*

13. Galois groups for simple radical extensions. A simple radical extension $L : K$ is normal (prove this). Let $G = \mathrm{Aut}(L : K)$ be the Galois group of $L : K$.

Consider the case $L = K(\alpha)$, where $\alpha^n \in K$ and it is assumed that a primitive nth root of unity, denoted by ε, belongs to K. Then, for any automorphisms $g_1, g_2 \in G$ we have

$$g_1(\alpha) = \varepsilon^i \alpha, \quad g_2(\alpha) = \varepsilon^j \alpha.$$

Consequently,

$$g_1 g_2(\alpha) = g_1(\varepsilon^j \alpha) = \varepsilon^{i+j} \alpha.$$

Therefore, we obtain an isomorphism between G and an additive subgroup of

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$$

(remainders modulo n). Thus, the group G is cyclic (and hence, abelian).

In the case $L = K(\varepsilon)$, where ε is a primitive nth root of unity, we have

$$g_1(\varepsilon) = \varepsilon^i, \quad g_2(\varepsilon) = \varepsilon^j, \quad g_1 g_2(\varepsilon) = \varepsilon^{ij}.$$

Now, we obtain an isomorphism between G and a multiplicative subgroup of $\mathbb{Z}_n$. Thus, the Galois group in this case is also abelian (and cyclic, if n is prime).

14. Solvable groups. A group G is called *solvable* if a chain of subgroups

$$G = G_0 \supset G_1 \supset \ldots \supset G_s = \{e\}$$

exists such that G_i is normal in G_{i-1} and G_i/G_{i-1} is abelian for all $1 \le i \le s$.

Theorem 14.1. *If a Galois extension $L : K$ is radical, then its Galois group is solvable.*

Theorem 14.2. *Let $f(x) \in K[x]$ have only simple roots and $L : K$ be the splitting field for $f(x)$. If an algebraic equation $f(x) = 0$ is solvable by radicals, then the Galois group of $L : K$ is solvable. And vice versa.*

15. Unsolvability of symmetric groups. If $n \leq 4$, then S_n is solvable. That can be proved by construction of a chain of subgroups from the definition of solvable group. However, S_5 and larger groups are not solvable.

THEOREM 15.1. *Symmetric groups S_n are not solvable for $n \geq 5$.*

To prove this, consider a normal subgroup $H \subset S_n$. If S_n/H is abelian, then $abH = baH$ for any $a, b \in S_n$, and it follows that

$$a^{-1}b^{-1}ab \in H \quad \text{for any} \quad a, b \in S_n.$$

In particular, $(kji)(mli)(ijk)(ilm) = (ikm)$, so H contains all cycles of length 3. Moreover, $(ljm)(ijk)(ijl) = (ik)(lm)$. Thus, H contains all products of two transpositions (dependent or independent), and by this reason it must coincide with A_n.

A similar technique applies to prove that if H is a normal subgroup in A_n with abelian quotient group A_n/H, then $H = A_n$.

16. Unsolvability by radicals. It is possible to find a quintic polynomial over $\mathbb{Q}$, for which the Galois group of the splitting extension field $L : \mathbb{Q}$ is equal (isomorphic) to S_5. Since we already know that S_5 is not solvable, from Theorem 14.2 it follows that this equation cannot be solved by radicals.

An example of quintic polynomial with this property is

$$f(x) = x^5 - 80x + 2.$$

First of all, $f(x)$ is irreducible over $\mathbb{Q}$ (prove this). Then, $f(-2) > 0$ and $f(2) < 0$. Therefore, $f(x)$ has at least 3 real roots. And it cannot have more than 3 real roots, because the equation $f'(x) = 0$ has only 2 real solutions: $x = \pm 2$.

Thus, $f(x)$ has 3 different real roots and 2 complex-conjugate roots, θ and $\overline{\theta}$. Denote by L the splitting extension field $L : \mathbb{Q}$ for $f(x)$, and let g be an automorphism defined by the rule $g(z) = \overline{z}$. As is readily seen, $g \in G = \mathrm{Aut}(L : \mathbb{Q})$. We can consider the Galois group G as a subgroup of S_5 (since the roots of $f(x)$ are permuted by any action of G). In this regard, g is exactly a transposition, for it swaps θ and $\overline{\theta}$ and does not move other roots. Finally, the assertion that $G = S_5$ is based on the following facts.

A subgroup G of S_n is called *transitive* if for any integers $1 \leq i, j \leq n$ there exists $g \in G$ such that $g(i) = j$.

THEOREM 16.1. *The Galois group of splitting extension $L : K$ of an irreducible polynomial with simple roots over K is transitive.*

THEOREM 16.2. *Assume that n is prime and a transitive subgroup G in S_n contains a transposition. Then $G = S_n$.*

17. Calculation of the Galois group. Given a field K, consider a polynomial $f(x) \in K[x]$ of degree n with simple roots $\alpha_1, \ldots, \alpha_n$. Let us introduce independent variables $u_1, \ldots, u_n$ and set

$$\theta = u_1\alpha_1 + \ldots + u_n\alpha_n.$$

Then, construct the following polynomial of variables $x, u_1, \ldots, u_n$ (for brevity we write u instead of $u_1, \ldots, u_n$):

$$F(x,u) = F(x, u_1, \ldots, u_n) = \prod_{\sigma \in S_n} (x - \theta_\sigma),$$

$$\theta_\sigma = u_1 \alpha_{\sigma(1)} + \ldots + u_n \alpha_{\sigma(n)}.$$

Since $F(x,u)$ does not change under any substitution of $\alpha_1, \ldots, \alpha_n$, all its coefficients belong to K, i.e. $F(x,u) \in K[x,u]$. Factorize $F(x,u)$ over K into a product of irreducible polynomials

$$F(x,u) = F_1(x,u)\, F_2(x,u)\, \ldots\, F_m(x,u),$$

where each F_i is a product of some polynomials of the form $x - \theta_\sigma$. Note that each F_i is also irreducible as a polynomial of x over $K[u]$, and equivalently, as a polynomial of x over $K(u)$ (the latter is a generalization of Theorem 6.1 to polynomials over *factorial rings*: they are irreducible if and only if they are irreducible over the corresponding quotient field).

Suppose that $x - \theta$ devides $F_1(x,u)$. Denote by $G \subseteq S_n$ a subset of substitutions involved in the factorization of $F_1(x,u)$. Then

$$F_1(x,u) = \prod_{g \in G} (x - \theta_g).$$

Let σF_1 denote a polynomial

$$\sigma F_1(x,u) = \prod_{g \in G} (x - \theta_{g\sigma}).$$

Obviously, $\sigma F_1(x,u)$ can be obtained from $F_1(x,u)$ by a substitution of variables $u_1, \ldots, u_n$:

$$\sigma F_1(x,u) = F_1(x, u_{\sigma^{-1}}), \quad u_{\sigma^{-1}} = \left(u_{\sigma^{-1}(1)}, \, \ldots \, , u_{\sigma^{-1}(n)}\right).$$

Hence, $\sigma F_1(x,u)$ has its coefficients belonging to K and remains to be irreducible over K. Thus, $\sigma F_1(x,u) = F_i(x,u)$ for some i. If $\sigma \in G$ then $\sigma F_1(x,u) = F_1(x,u)$, otherwise F_1 and F_i would have a common divisor over K. Thus, if $\sigma, g \in G$ then $\sigma g \in G$, and based on this, we easily come to conclusion that G is a group. Moreover, $\sigma \in G$ if and only if $\sigma F_1(x,u) = F_1(x,u)$.

Suppose that $L = L : K$ is the splitting field for $f(x) \in K[x]$. Let us consider $\mathrm{Aut}(L : K)$ as a group of substitutions of the roots of $f(x)$. As is readily seen, if $\sigma \in \mathrm{Aut}(L : K)$ then $\sigma F_1(x,u) = F_1(x,u)$. Therefore, $\mathrm{Aut}(L : K) \subseteq G$.

Note that $L(u) = L(u_1, \ldots, u_n)$ is the splitting field for $f(x)$ over $K(u) = K(u_1, \ldots, u_n)$, and it can be proved that the corresponding Galois group is isomorphic to a subgroup of $\mathrm{Aut}(L : K)$. Since $F_1(x,u)$ is irreducible over $K(u)$, the number of automorphisms in this group cannot be less than the degree of $F_1(x,u)$ as a polynomial from $K(u)[x]$. Hence, $|G| \leq |\mathrm{Aut}(L : K)|$. Consequently, $G = \mathrm{Aut}(L : K)$.

Theorem 17.1. *G is a group isomorphic to the Galois group of $f(x)$.*

If $f(x)$ has integer coefficients, then $F(x,u)$ is as well a polynomial with integer coefficients. Let G be the Galois group for $f(x)$ over $\mathbb{Q}$.

Choosing a prime number p, one can consider a decomposition of $F(x, u)$ into a product of polynomials irreducible modulo p. The irreducible polynomial with linear factor $x - \theta$ is a divisor of $F_1(x, u)$ modulo p. It follows that the Galois group of $f(x)$ modulo p, denote it by H, is a subgroup of G.

And H is easy to find: it is always cyclic and generated by a product of independent cycles with the lengths equal to the orders of irreducible modulo p polynomials whose product is $f(x)$ modulo p (prove this).

18. Problems.

1. Find all intermediate fields in between of $\mathbb{R}$ and $\mathbb{C}$.
2. Prove that the polynomial $f(x) = x^{2011} - 2$ is irreducible over $\mathbb{Q}$.
3. Let ε be any root of the polynomial $f(x) = 1 + x + \ldots + x^{2010}$. Prove that $\dim(\mathbb{Q}(\varepsilon) : \mathbb{Q}) = 2010$.
4. Let L be the splitting field for $f(x) = x^4 + 1$ over $\mathbb{Q}$. Calculate $\dim(L : \mathbb{Q})$ and find all intermediate fields in between of $\mathbb{Q}$ and L.
5. Find the minimal polynomial over $\mathbb{Q}$ for ε, where ε is a primitive root of degree 10 of unity.
6. Prove that the polynomial $f(x) = x^4 - 10x + 1$ is irreducible over $\mathbb{Q}$ but reducible modulo p for any prime p.
7. Prove that $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
8. Calculate $\dim(\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q})$, prove that the extension $\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}$ is normal and find its Galois group.
9. Let $p_1 < \ldots < p_n$ be prime numbers and $L = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Prove that $\dim(L : \mathbb{Q}) = 2^n$.
10. Elements a and b are algebraic over $\mathbb{Q}$. Prove that $a + b$ and ab are algebraic over $\mathbb{Q}$.
11. Prove that construction of a segment of length $2^{1/3}$ (doubling the cube problem) is not possible by compasses and ruler.
12. Prove that the angle of 60 degrees cannot be trisected by compasses and ruler.
13. Find an algorithm for construction of the regular 15-hedron by compasses and ruler.
14. Find an algorithm for construction of the regular 17-hedron by compasses and ruler.
15. Let ε be a primitive root of degree 9 of unity. Prove that $\dim(\mathbb{Q}(\varepsilon) : \mathbb{Q}) = 4$.
16. Prove that S_4 (symmetric group of degree 4) is solvable.
17. Prove that a group of all nonsingular upper triangular $n \times n$ matrices is solvable.
18. Prove that any subgroup of a solvable group is solvable.
19. Assume that H is a normal subgroup of a solvable group G. Prove that the quotient group G/H is solvable.
20. Elements a and b in a group G are called *conjugate* if $a = gbg^{-1}$ for some $g \in G$. Let G be a finite group. Prove that the number of elements that are conjugate to a fixed element a is a divisor of $|G|$.
21. Prove that a group of order pq, where p and q are different prime numbers, is solvable.
22. Prove that a group of order p^n, where p is a prime number, is solvable.
23. A set $Z = Z(G)$ of all elements of a group G that commutate with any element of G is called a *center* of G. Find $Z(G)$, where G is the multiplicative group of all nonsingular $n \times n$ matrices.

24. Prove that if $G/Z(G)$ is cyclic ($Z(G)$ is a center of G), then G is abelian.
25. Given a group G, denote by H a set of all finite products of elements of the form $aba^{-1}b^{-1}$ with arbitrary $a, b \in G$. Prove that H is a normal subgroup in G (called a *commutator* of G) and the quotient group G/H is abelian.
26. Find the Galois groups over $\mathbb{Q}$ for the polynomials $f(x) = x^3 - 3x + 1$, $g(x) = x^3 + x + 1$, $h(x) = x^4 + x^2 + 1$.
27. $L : K$ is a Galois extension, its Galois group consists of automorphisms $g_1, \ldots, g_n$, and $\theta_1, \ldots, \theta_n \in L$ form a basis of L as a linear space over K. Prove that the matrix

$$A = \begin{bmatrix} g_1(\theta_1) & \ldots & g_1(\theta_n) \\ \ldots & \ldots & \ldots \\ g_n(\theta_1) & \ldots & g_n(\theta_n) \end{bmatrix}$$

is nonsingular.
28. Let $K = \mathbb{Q}(\mathbf{i})$ (adjunction of the imaginary unit), and assume that an extension $L : K$ is normal and $\dim(L : K) = 4$. Prove that $L = K(\theta)$, where θ is a root of the equation $x^4 = a$ for some $a \in K$.
29. Let L be the splitting field for the polynomial $f(x) = x^5 - 25x + 5$ over $\mathbb{Q}$. Prove that $\dim(L : \mathbb{Q}) = 120$.
30. Given a polynomial $f(x) \in \mathbb{Q}[x]$ with n simple roots $\alpha_1, \ldots, \alpha_n$, consider its Galois group. Prove that it is isomorphic to a group G of all substitutions of the roots of $f(x)$ that do not change any rational relation between the roots, that is, $\sigma \in G$ if and only if for any rational function $\Phi(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ with the property $\Phi(\alpha_1, \ldots, \alpha_n) = 0$ it follows that $\Phi(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$.
31. Let L be the splitting field for a polynomial $f(x) = \prod_{i=1}^{n} (x - \alpha_i) \in \mathbb{Q}[x]$. Prove that there exist integer numbers $u_1, \ldots, u_n$ such that the numbers

$$\theta_\sigma = u_1\alpha_{\sigma(1)} + \ldots + u_n\alpha_{\sigma(n)}$$

are different for different substitutions $\sigma \in S_n$. With $u_1, \ldots, u_n$ being any integers with this property, prove that L is obtained from $\mathbb{Q}$ by adjunction of $\theta = u_1\alpha_1 + \ldots + u_n\alpha_n$.
32. Assume that G is a subgroup in S_n and K is an infinite field. Prove that a polynomial $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ exists such that

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$$

holds for $\sigma \in S_n$ if and only if $\sigma \in G$.
33. A transitive subgroup G of the symmetric group S_n contains a transposition and a cycle with $n - 1$ terms. Prove that $G = S_n$.
34. Prove that any transitive subgroup of the symmetric group S_p for a prime number p contains a cycle with p terms.
35. Let p be prime and n be a positive integer. Prove that there exists a polynomial of order n with integer coefficients which is irreducible modulo p.
36. Let p be prime and $K = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ be the field of remainders modulo p (with p elements). Prove that any finite extension $L : K$ is normal and separable, and its Galois group is cyclic.
37. Find a polynomial of order 6 over $\mathbb{Z}$ such that its Galois group over $\mathbb{Q}$ coincides with the symmetric group of degree 6.

38. Let $L = L : K$ and a polynomial $f(x) \in K[x]$ have only simple roots. Let K_f and L_f denote the splitting fields for $f(x)$ considered as a polynomial over K and over L, respectively. Prove that the group $\mathrm{Aut}(L_f : L)$ is isomorphic to a subgroup of $\mathrm{Aut}(K_f : K)$.
39. Assume that $L : K$ is a Galois extension and α is an algebraic element over K that does not belong to L. Prove that there exists $\beta \in L \cap K(\alpha)$ such that the group $\mathrm{Aut}(L(\alpha) : K(\alpha))$ is isomorphic to $\mathrm{Aut}(L : K(\beta))$ and $\beta = g(\alpha)$ for some polynomial $g(x) \in K[x]$. (Kronecker's theorem.)
40. Let ε be a primitive pth root of unity, p is prime. Assume that $\varepsilon \notin K = K : \mathbb{Q}$ and $\varepsilon \notin L$, where L is the splitting field for a polynomial $f(x)$ which is irreducible over K. Prove that $f(x)$ is irreducible over $K(\varepsilon)$.
41. Assume that $K = K : \mathbb{Q}$ contains a primitive pth root of unity, and p is prime. Let $\alpha^p \in K$, $\alpha \notin K$, and $\alpha \in L$, where L is the splitting field for an irreducible over K polynomial $f(x)$. Prove that if $f(x)$ is reducible over $K(\alpha)$, then it is a product of p polynomials which are irreducible over $K(\alpha)$ and are of the same degree.
42. Consider Galois extensions $L : K$ and $M : K$ with $K \subset L \subset M$, and let the Galois group G of $M : K$ be regarded as a subgroup of the symmetric group S_p for a prime p. Suppose that each substitution $g \in H = \mathrm{Aut}(M : L)$ is a function of the form $g(i) = ai + b$ modulo p, where $i = 1, \dots, p$ and a and b are integers depending on g but not on i. It is also assumed that H contains the cyclic substitution $\sigma(i) = i + 1$ modulo p. Prove that each substitution of G is of the same form.
43. Assume that the Galois group $G \subset S_p$ of a polynomial $f(x) \in \mathbb{Q}[x]$ with p simple roots consists of substitutions $g(i) = ai + b$ modulo p (a and b are integers depending on g) and p is prime. Prove that G is solvable and all roots of $f(x)$ are rationally expressed through any other two roots.
44. For any algebraic extension $L : K$, prove that $L = K(\theta)$ for some $\theta \in L$ if and only if the number of intermediate fields in between of K and L is finite.
45. Let H be a finite subgroup in the group of all automorphisms of a field M. Prove that $K = M^H = \{a \in M : h(a) = a \ \forall \ h \in H\}$ is a subfield of M and $M : K$ is a normal separable extension with the Galois group equal to H. (Artin's theorem.)
46. Prove that the equation $x^5 - x - 1 = 0$ is not solvable by radicals.
47. Let $a_1, \dots, a_s \in \mathbb{Q}$ and $K = \mathbb{Q}(\varepsilon)$, where ε is a primitive nth root of unity, and denote by L the splitting fields for $f(x) = (x^n - a_1) \dots (x^n - a_s)$ over K. Prove that the group $\mathrm{Aut}(L : K)$ is abelian.
48. Let G be a group of all automorphisms of a field M. For any $a \in M$, consider a set of all automorphisms for which a is a fixed point (this set is called a *stabilizer* of a):

$$\mathrm{Stab}(a) = \{g \in G : g(a) = a\}.$$

For any finite subroup $H \subseteq G$, prove that there exists $a \in L = M^H$ such that $\mathrm{Stab}(a) = H$.
49. A finite abelian group G consists of some automorpisms of a field M. Prove that any element $a \in M$ can be written as a finite sum of the form $a = \sum a_i$ with $a_i \in M$ and $a_i^n \in M^G$, where $n = |G|$.
50. Let G be a finite group of some automorphisms of an infinite field M. Prove that there exists $a \in M$ such that all elements of the orbit $g(a)$, $g \in G$, are different. Is this valid for a finite field M?

51. Let $f(x)$ be a minimal polynomial for α over a field K, and let

$$g(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)}.$$

Assume that $K(\alpha) : K$ is a Galois extension, and $\sigma_1, \ldots, \sigma_n$ are all different automorphisms of its Galois group. Consider a polynomial

$$D(x) = \det\left[\sigma_i \sigma_j g(x)\right]$$

and prove that $D^2(x) = 1$ modulo $f(x)$.

52. Let $L : K$ be a normal extension with $L \subset \mathbb{R}$, and assume that the extension degree $\dim(L : K)$ has a nontrivial odd divisor p. Suppose that $\alpha \in \mathbb{R}\backslash L$ and $\alpha^p = a \in K$. Prove that $\dim(L(\alpha) : K(\alpha))$ has still a nontrivial odd divisor.

53. Assume that $x_1, \ldots, x_n$ are independent variables and $\sigma_1, \ldots, \sigma_n$ are elementary symmetric functions of $x_1, \ldots, x_n$ over $K = K : \mathbb{Q}$. Let $\theta = a_1x_1 + \ldots + a_nx_n$, where $a_1, \ldots, a_n$ are pairwise different elements from K. Prove that $K(x_1, \ldots, x_n) = K(\sigma_1, \ldots, \sigma_n)(\theta)$.

54. Let $K = K : \mathbb{Q}$ and p be a prime number. Prove that for a polynomial $x^p - a$ with $a \in K$ to be reducible over K, it is necessary that $a = b^p$ for some $b \in K$.

55. Suppose that $M = M : K$ is the splitting field for a polynomial $f(x) \in K[x]$ and K contains $\mathbb{Q}$ and a primitive pth root of unity for a prime p. Let $\alpha \in M \cap K(\xi)$ with $\xi^p \in K$. Prove that $\alpha \in K(\theta)$, where $\theta^p \in K$ and $\theta \in M$.