Lectures 3, September 17
REPRESENTABILITY BY RADICALS

We will discuss a procedure which allows to represent an element by radicals. Usually representability by radicals is considered for elements belonging to some field. The fact that we deal with fields is barely used in the construction of representation by radicals.

To emphasize this, we describe this construction where a field is replaced with an algebra V, which may even be non-commutative.

In fact, we do not even need to multiply different elements of the algebra. We will only use the operation of taking an integer power k of an element, and the fact that this operation is homogeneous of degree k under multiplications by elements of the base field:

$$(\lambda a)^k = \lambda^k a^k$$

for all $a \in V$, $\lambda \in K$).

Let V be an algebra over the field K containing all roots of unity. Let G be a group of order acting by automorphisms of the algebra V.

Definition 1. *The subalgebra V_0 consisting of all fixed elements x fixed under the G action, i.e. of such x that for any $g \in G$ the identity $g(x) = x$ holds, is called the invariant subalgebra of V.*

Proposition 1. *Let G be a finite commutative group of order n acting by automorphisms of the algebra V over a field K. Suppose that K contains all roots of unity of degree n.*

Then every element of the algebra V is representable as a sum of $k \leq n$ elements $x_i \in V$, $i = 1, \ldots, k$, such that x_i^n lies in the invariant subalgebra V_0.

Proof. Consider a finite dimensional vector subspace L in the algebra V spanned by the G-orbit of an element x.

The space L splits into a direct sum $L = L_1 \oplus \cdots \oplus L_k$ of eigenspaces for all operators from G.

Therefore, the vector x can be represented in the form

$$x = x_1 + \cdots + x_k,$$

where $x_1, \ldots, x_k$ are eigenvectors for all the operators from the group.

The corresponding eigenvalues are n-th roots of unity. Therefore, the elements $x_1^n, \ldots, x_k^n$ belong to the invariant subalgebra V_0. □ □

DEFINITION. We say that an element x of the algebra V is an *n-th root of an element a*, if $x^n = a$.

We can now restate Proposition 1 as follows:

Every element x of the algebra V is representable as a sum of n-th roots of some elements of the invariant subalgebra.

Definition 2. *A group G is* **solvable** *if it has a chain of nested subgroups*

$$G = G_0 \supset \cdots \supset G_m = e,$$

in which:

1) the group G_m consists of the identity element e only;

2) every group G_i is a normal subgroup in the group G_{i-1};

3) the quotient group G_{i-1}/G_i is commutative.

Theorem 1. *Let G be a finite solvable group of automorphisms of the algebra V of order n. Suppose that the field K contains all roots of unity of degree n.*

Then every element x of the algebra V can be obtained from the elements of the invariant subalgebra V_0 by root extractions and summations.

We first prove the following simple statement about an action of a group on a set.

Suppose that a group G acts on a set X, that H is a normal subgroup of G, and that X_0 is a subset of X consisting of all points fixed under the action of G.

Proposition 2. *The subset X_H of the set X consisting of the fixed points under the action of the normal subgroup H is invariant under the action of G.*

There is a natural action of the quotient group G/H on the set X_H with the fixed point set X_0.

Proof. Suppose that $g \in G$, $h \in H$. Then the element

$$g^{-1}hg$$

belongs to the normal subgroup H.

Let $x \in X_H$. Then

$$g^{-1}hg(x) = x, \quad \text{or} \quad h(g(x)) = g(x),$$

which means that the element $g(x) \in X$ is fixed under the action of the normal subgroup H.

Thus the set X_H is invariant under the action of the group G. Under the action of G on X_H, all elements of H correspond to the identity transformation.

Hence the action of G on X_H reduces to an action of the quotient group G/H. $\square$

Proof of Theorem 1. Since the group G is solvable, it has a chain of nested subgroups

$$G = G_0 \supset \cdots \supset G_m = e,$$

in which the group G_m consists of the identity element e only, and every group G_i is a normal subgroup in the group G_{i-1}, moreover, the quotient group G_{i-1}/G_i is commutative.

Let

$$V_0 \subset \cdots \subset V_m = V$$

denote the chain of invariant subalgebras of the algebra V with respect to the action of the groups

$$G_0, \ldots, G_m.$$

By Proposition 2, the commutative group G_{i-1}/G_i acts naturally on the invariant subalgebra V_i, leaving the subalgebra V_{i-1} pointwise fixed.

The order m_i of the quotient group G_{i-1}/G_i divides the order of the group G. Therefore, Proposition 1 is applicable to this action.

We conclude that every element of the algebra V_i can be expressed with the help of summation and root extraction through the elements of the algebra V_{i-1}.

Repeating the same argument, we will be able to express every element of the algebra V through the elements of the algebra V_0 by a chain of summations and root extractions. □ □

PERMUTATION GROUPS AND EQUATIONS OF DEGREE $2-4$

Theorem 1 explains why equations of low degrees are solvable by radicals.

Suppose that the algebra V is the polynomial ring in the variables x_1, $\ldots$, x_n over the field K. The symmetric group $S(n)$ consisting of all permutations of n elements acts on this ring, permuting the variables $x_1, \ldots, x_n$ in polynomials from this ring. The invariant subalgebra of this action consists of all symmetric polynomials.

Definition 3. *The following symmetric polynomials in n variables are called the elementary symmetric functions $\sigma_1, \ldots, \sigma_n$, where $\sigma_1 = x_1 + \cdots + x_n$, $\sigma_2 = \sum_{i<j} x_i x_j$, $\ldots$, $\sigma_n = x_1 \ldots x_n$.*

The following classical statement plays a key role for creating formulas solving equations of small degree:

Every symmetric polynomial can be represented explicitly as a polynomial of the elementary symmetric functions.

If you forget how to prove this classical Theorem you can prove it yourself by solving the follwing problem.

Problem 1. *1. Let $[P]$ be the lexicographically highest order term of a polynomial P. Then $[P][Q] = [PQ]$.*

2. Let $\sigma_1, \ldots, \sigma_n$ be elementary symmetric functions in $x_1, \ldots, x_n$. Then, for any symmetric polynomial P in $x_1, \ldots, x_n$, there exist the numbers $m_1, \ldots, m_n$ such that

$$[P] = [\sigma_1^{m_1} \ldots \sigma_n^{m_n}].$$

3. Show that 1) and 2) implies a constructive proof of the above theorem.

Theorem 2 (Vieta's Theorem)**.** *Consider the general algebraic equation*

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

of degree n. The coefficients of this equation are equal up to a sign to the elementary symmetric functions of its roots $x_1, \ldots, x_n$. Namely,

$$\sigma_1 = -a_1, \ldots, \sigma_n = (-1)^n a_n.$$

Problem 2. *Check that the Vieta's Theorem follows from the following identity:*

$$x^n + a_1 x^{n-1} + \cdots + a_n = (x - x_1) \cdot \cdots \cdot (x - x_n).$$

For $n = 2, 3, 4$, the group $S(n)$ is solvable.

Suppose that the field K contains all roots of unity of degree $2, 3, 4$ respectively. Applying Theorem 1, we obtain that every polynomial of $x_1, \ldots, x_n$ can be expressed through the elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$ using root extraction, summation and multiplication by rational numbers. Therefore, Theorem 1 **for $n = 2, 3, 4$ proves the representability of the roots of a degree n algebraic equation through the coefficients of this equation using root extractions, summation and multiplication by rational numbers**. Now we will present these formulas explicitly using technique of Lagrange interpolation polynomials.

Equations of the second degree. The polynomial ring $K[x_1, x_2]$ carries a linear action of the permutation group $S(2) = \mathbb{Z}_2$ of two elements. This group consists of the identity map and some operator of order 2. The element x_1 has two Lagrange resolvents with respect to the action of this operator:

$$R_1 = \frac{1}{2}(x_1 + x_2) = \frac{1}{2}\sigma_1,$$

$$R_{-1} = \frac{1}{2}(x_1 - x_2).$$

The square of the Lagrange resolvent R_{-1} is a symmetric polynomial.

$$R_{-1}^2 = \frac{1}{4}((x_1 + x_2)^2 - 4x_1x_2) = \frac{1}{4}(\sigma_1^2 - 4\sigma_2).$$

We obtain a representation of the polynomial x_1 through the elementary symmetric polynomials $x_1 = R_1 + R_{-1} = \frac{\sigma_1 \pm \sqrt{\sigma_1^2 - 4\sigma_2}}{2}$.

Equations of the third degree. Suppose that the field K contains all three cubic roots of unity. On the polynomial ring $K[x_1, x_2, x_3] = V$, there is an action of the permutation group $S(3)$ of three elements.

The alternating group $A(3)$, which is a cyclic group of order 3, is a normal subgroup of the group $S(3)$.

The group $A(3)$ is generated by the operator B defining the permutation x_2, x_3, x_1 of the variables x_1, x_2, x_3.

The quotient group $S(3)/A(3)$ is a cyclic group of order 2.

Let V_1 denote the invariant subalgebra of the group $A(3)$ (consisting of all polynomials that remain unchanged under all even permutations of the variables), and V_2 the algebra of symmetric polynomials.

The element x_1 has three Lagrange resolvents with respect to the

generator B of the group $A(3)$:

$$R_1 = \frac{1}{3}(x_1 + x_2 + x_3),$$

$$R_{\xi_1} = \frac{1}{3}(x_1 + \xi_2 x_2 + \xi_2^2 x_3),$$

$$R_{\xi_2} = \frac{1}{3}(x_1 + \xi_1 x_2 + \xi_1^2 x_3),$$

where ξ_1, $\xi_2 = \frac{-1 \pm \sqrt{-3}}{2}$ are the cubic roots of unity different from one.

We have

$$x_1 = R_1 + R_{\xi_1} + R_{\xi_2},$$

and R_1^3, $R_{\xi_1}^3$, $R_{\xi_2}^3$ lie in the algebra V_1.

Moreover, the resolvent R_1 is a symmetric polynomial, and the polynomials $R^3_{\xi_1}$ and $R^3_{\xi_2}$ are interchanged by the action of the group $\mathbb{Z}_2 = S(3)/A(3)$ on the ring V_1.

Applying the construction used for solving quadratic equations to the polynomials $R^3_{\xi_1}$ and $R^3_{\xi_2}$, we obtain that these polynomials can be expressed through the symmetric polynomials

$$R^3_{\xi_1} + R^3_{\xi_2}, \;\; (R^3_{\xi_1} - R^3_{\xi_2})^2.$$

We finally obtain that the polynomial x_1 can be expressed through the symmetric polynomials

$$R_1 \in V_2, \; |R^3_{\xi_1} + R^3_{\xi_2} \in V_2 \;\; (R^3_{\xi_1} - R^3_{\xi_2})^2 \in V_2.$$

with the help of square and cubic root extractions and the arithmetic operations. To write down an explicit formula for the solution, it remains only to express these symmetric polynomials through the elementary symmetric polynomials.

Equations of the fourth degree. The reason for equations of the fourth degree being solvable is that the group $S(4)$ is solvable.

The group $S(4)$ is solvable because there exists a homomorphism $\pi : S(4) \to S(3)$, whose kernel is the commutative group $Kl = \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

The homomorphism π can be described in the following way. There exist exactly three ways to split a four-element set into pairs of elements.

Every permutation of the four elements gives rise to a permutation of these splittings.

This correspondence defines the homomorphism π. The kernel Kl of this homomorphism is a normal subgroup of the group $S(4)$ consisting of four permutations:

the identity permutation and

the three permutations, each of which is a product of two disjoint transpositions.

Suppose that the field K contains all three cubic roots of unity. The group $S(4)$ acts on the polynomial ring $K[x_1, x_2, x_3, x_4] = V$. Let V_1 denote the invariant subalgebra of the normal subgroup Kl of the group $S(4)$.

Thus the polynomial ring $V = K[x_1, x_2, x_3, x_4]$ carries an action of the commutative group Kl with the invariant subalgebra V_1.

On the ring V_1, there is an action of the solvable group $S(3) = S(4)/Kl$, and the invariant subalgebra with respect to this action is the ring V_2 of symmetric polynomials.

Let A and B be operators corresponding to the permutations x_2, x_1, x_4, x_3 and x_3, x_4, x_1, x_2 of the variables x_1, x_2, x_3, x_4.

The operators A and B generate the group Kl.

The following identities hold: $A^2 = B^2 = E$.

The roots of the polynomial $T(t) = t^2 - 1$ annihilating the operators

A and B are equal to $+1$, -1.

The group Kl is the sum of two copies of the group with two elements, the first copy being generated by A, and the second copy by B.

The element x_1 has four Lagrange resolvents with respect to the action of commuting operators A and B generating the group Kl:

$$R_{1,1} = \frac{1}{4}(x_1 + x_2 + x_3 + x_4),$$

$$R_{-1,1} = \frac{1}{4}(x_1 - x_2 + x_3 - x_4),$$

$$R_{1,-1} = \frac{1}{4}(x_1 + x_2 - x_3 - x_4),$$

$$R_{-1,-1} = \frac{1}{4}(x_1 - x_2 - x_3 + x_4).$$

The element x is equal to the sum of these resolvents:

$$x_1 = R_{1,1} + R_{-1,1} + R_{1,-1} + R_{-1,1},$$

the squares $R^2_{1,1}$, $R^2_{-1,1}$, $R^2_{1,-1}$, $R^2_{-1,1}$ of the Lagrange resolvents belong to the algebra V_1.

Therefore, x_1 is expressible through the elements of the algebra V_1 with the help of the arithmetic operations and square root extractions.

In turn, the elements of the algebra V_1 can be expressed through symmetric polynomials, since this algebra carries an action of the group $S(3)$ with the invariant subalgebra V_2 (see solution of cubic equations above).

Let us show that this argument provides an explicit reduction of a fourth degree equation to a cubic equation. Indeed, the resolvent $R_{1,1} = \frac{1}{4}\sigma_1$ is a symmetric polynomial.

The squares of the resolvents $R_{-1,1}$, $R_{1,-1}$ and $R_{-1,1}$ are permuted under the action of the group $S(4)$ (see the description of the homo-

morphism $\pi : S(4) \to S(3)$ above).

Since the elements $R^2_{-1,1}$, $R^2_{1,-1}$ and $R^2_{-1,1}$ are only being permuted, the elementary symmetric polynomials of them are invariant under the action of the group $S(4)$ and hence belong to the ring V_2. Thus the polynomials

$$b_1 = R^2_{-1,1} + R^2_{1,-1} + R^2_{-1,1},$$

$$b_2 = R^2_{-1,1}R^2_{1,-1} + R^2_{1,-1}R^2_{-1,-1} + R^2_{-1,-1}R^2_{-1,1},$$

$$b_3 = R^2_{-1,1}R^2_{1,-1}R^2_{-1,-1}$$

are symmetric polynomials of x_1, x_2, x_3 and x_4.

Therefore, b_1, b_2 and b_3 are expressible explicitly through the coefficients of the equation

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0, \tag{4}$$

whose roots are x_1, x_2, x_3, x_4.

To solve equation (4), it suffices to solve the equation

$$r^3 - b_1r^2 + b_2r - b_3 = 0 \tag{5}$$

and set $x = \frac{1}{4}(-a_1 + \sqrt{r_1} + \sqrt{r_2} + \sqrt{r_3})$, where r_1, r_2 and r_3 are the roots of equation (5).

ANOTHER REDUCTION OF A FOUR DEGREE EQUATION TO A THIRD DEGREE EQUATION

Theorem 3. *The coordinates of the intersection points of two conics $P = 0$ and $Q = 0$, where P and Q are given second degree polynomials of x and y, can be found by solving one cubic and several quadratic equations*

Indeed, every conic of the pencil

$$P + \lambda Q = 0,$$

where λ is an arbitrary parameter, passes through the points we are looking for.

For some value λ_0 of the parameter λ the conic $P + \lambda Q = 0$ splits into a pair of lines.

This value satisfies the cubic equation

$$\det(\tilde{P} + \lambda\tilde{Q}) = 0,$$

where $\tilde{P}$ and $\tilde{Q}$ are 3×3-matrices of the quadratic forms corresponding to the equations of the conics in homogeneous coordinates.

The equation for each of the lines forming the degenerate conic $P + \lambda_0 Q = 0$ can be found by solving a quadratic equation.

Indeed, the center of a degenerate conic given in affine coordinates by an equation $f(x, y) = 0$, i.e. the intersection point of the two lines forming the degenerate conic, can be found by solving the system

$$\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = 0.$$

.

This is a linear system, thus a solution can be expressed as a rational function of the coefficients.

The intersection of a conic with any given line not passing through the center of the conic can be found by solving a quadratic equation. The two lines forming the degenerate conic are the lines connecting the center of the conic with the two intersection points. An equation of the line passing through two given points can be found with the help of arithmetic operations.

If the equations of the lines, into which the conic

$$P + \lambda_0 Q = 0$$

splits, are known, then to find the desired points, it remains only to solve the quadratic equations on the intersection points of the conic $P = 0$ and each of the two lines constituting the degenerate conic.

Theorem 4. *Therefore, the general equation of the fourth degree reduces to a cubic equation with the help of arithmetic operations and quadratic root extractions.*

Indeed, the roots of an equation

$$a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0$$

are projections to the x-axis of the intersection points of the conics

$$y = x^2 \quad \text{and} \quad a_0y^2 + a_1xy + a_2y + a_3x + a_4 = 0.$$