Lecture 12, October 20

A CRITERION OF SOLVABILITY BY k-RADICALS

We say that an algebraic equation over a field K is *solvable by k-radicals* if there exists a chain of extensions

$$K = K_0 \subset K_1 \cdots \subset K_n,$$

in which, for every j, $0 \leq j < n$, either
the field K_{j+1} is obtained from the field K_j by adjoining a radical,
or the field K_{j+1} is obtained from the field K_j by adjoining a root of some equation over the field K_j of degree at most k,
and the field K_n contains all roots of the initial equation.

Is a given algebraic equation solvable by k-radicals?

we answer this question below. First we discuss the properties of k-solvable groups. and than we prove a criterion of solvability by k-radicals.

Let us start with the following simple statement.

Proposition 1. *The Galois group of an equation of degree $m \leq k$ is isomorphic to a subgroup of the group $S(k)$.*

Proof. Every element of the Galois group permutes the roots of the equation, and is uniquely determined by the permutation of roots thus obtained. Hence the Galois group of a degree m equation is isomorphic to a subgroup of the group $S(m)$. For $m \leq k$, the group $S(m)$ is a subgroup of the group $S(k)$. □ □

PROPERTIES OF of k-SOLVABLE GROUPS

Properties of k-solvable groups are similar to some properties of solvable groups. s

We start with Lemma which characterizes subgroups of the group $S(k)$.

Lemma 1. *A group is isomorphic to a subgroup of the group $S(k)$ if and only if it has a collection of m subgroups, $m \leq k$, such that*

1. *the intersection of these subgroups contains no nontrivial normal subgroups of the entire group;*

2. *the sum of indices of these subgroups does not exceed k.*

Proof. Suppose that G is a subgroup of the group $S(k)$.

Consider a representation of the group G as a subgroup of permutations of a set M with k elements.

Suppose that, under the action of the group G, the set M splits into m orbits. Choose a single point x_i in every orbit.

The collection of stabilizers of points x_i satisfies the conditions of the lemma.

Indeed, the index of the stabilizer H_i of x_i equals the cardinality of the orbit of x_i, hence the sum of these indices is k.

Let H be the intersection of all stabilizers H_i. Suppose that H contains a non-trivial normal subgroup F. Every element x of M has the form $x = gx_i$ for some $g \in G$ and i. It follows that x is a fixed point for all elements of gFg^{-1}, since x_i is a fixed point for all elements of F.

We conclude that F acts trivially on M, a contradiction.

Conversely, let a group G have a collection of subgroups $G_1, \ldots, G_n$ satisfying the conditions of the lemma.

Let P denote the union of the sets P_i, where $P_i = G/G_i$ consists of all right cosets with respect to the subgroup G_i, $1 \leq i \leq n$. The group G acts naturally on the set P. The representation of the group G in the group $S(P)$ of all permutations of P is faithful, since the kernel of this representation lies in the intersection of the groups G_i.

The group $S(P)$ embeds into the group $S(k)$ since the number of elements in the set P is the sum of the indices of the subgroups G_i. $\square$

$\square$

Corollary 2. *Any quotient group group of any subgroup of the symmetric group $S(k)$ is isomorphic to a subgroup of $S(k)$.*

Proof. Suppose that a group G is isomorphic to a subgroup of the group $S(k)$, and G_i are subgroups in G satisfying the conditions of the lemma. Let π be an arbitrary homomorphism of the group G (onto some other group). Then the collection of the subgroups $\pi(G_i)$ in the group $\pi(G)$ also satisfies the conditions of the lemma. □ □

We say that a normal subgroup H of a group G is of *depth at most* k if the group G has a subgroup G_0 of index at most k such that H is the intersection of all subgroups conjugate to G_0. We say that a group is of depth at most k if its identity subgroup is of depth at most k.

A normal tower of a group G is a nested chain of subgroups

$$G = G_0 \supset \cdots \supset G_n = \{e\},$$

in which every next group is a normal subgroup of the preceding group.

Corollary 3. *If a group G is a subgroup of the group $S(k)$, then the group G has a nested chain of subgroups*

$$G = \Gamma_0 \supset \cdots \supset \Gamma_m = \{e\},$$

in which the group Γ_m is trivial, and for every $i = 0, 1, \ldots, m-1$, the group Γ_{i+1} is a normal subgroup of the group Γ_i of depth at most k.

Proof. Let G_i be a collection of subgroups of the group G satisfying the conditions of the lemma.

Let F_i denote the normal subgroup of the group G obtained as the intersection of all subgroups conjugate to the subgroup G_i.

The chain of subgroups
$\Gamma_1 = F_1, \Gamma_2 = F_1 \cap F_2, \dots, \Gamma_m = F_1 \cap F_2 \cap \dots \cap F_m$
satisfies the conditions of the corollary. $\square$ $\square$

Lemma 4. *A group G is k-solvable if and only if it admits a normal tower of subgroups*

$$G = G_0 \supset \dots \supset G_n = \{e\},$$

in which, for every i, $0 < i \le n$,

either the normal subgroup G_i has depth at most k in the group G_{i-1},

or the quotient G_{i-1}/G_i is commutative.

Proof. 1. Suppose that the group G admits a normal tower

$$G = G_0 \supset \cdots \supset G_n = \{e\}$$

satisfying the conditions of the lemma.

If, for some i, the normal subgroup G_i has depth at most k in the group G_{i-1}, then the group G_{i-1}/G_i has a chain of subgroups

$$G_{i-1}/G_i = \Gamma_0 \cdots \supset \Gamma_m = \{e\},$$

in which the index of every next group in the preceding group does not exceed k.

For every such number i, we can insert the chain of subgroups

$$G_{i-1} = \Gamma_{0,i} \supset \cdots \supset \Gamma_{m_i,i}$$

between G_{i-1} and G_i, where $\Gamma_{j,i} = \pi^{-1}(\Gamma_j)$, and $\pi : G_{i-1} \to G_{i-1}/G_i$ is the canonical projection to the quotient group.

We thus obtain a chain of subgroups satisfying the definition of a k-solvable group.

2. Suppose that a group G is k-solvable, and

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

is a chain of subgroups satisfying the assumptions listed in the definition of a k-solvable group.

We will successively replace subgroups in the chain with smaller subgroups. Let i be the first number, for which the group G_i is not a normal subgroup in the group G_{i-1} but rather a subgroup of index $\leq k$.

In this case, the group G_{i-1} has a normal subgroup H lying in the group G_i and such that the group G_{i-1}/H is isomorphic to a subgroup of $S(k)$.

Indeed, we can take H to be the intersection of all subgroups in G_{i-1} conjugate to the group G_i. We can now modify the chain

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

in the following way:

all subgroups labeled by numbers less than i remain the same.

Every group G_j with $i \leq j$ is replaced with the group $G_j \cap H$. Repeat the same procedure for the chain of subgroups thus obtained, and so on.

Finally, we obtain a normal tower of subgroups satisfying the conditions of the lemma. □ □

Theorem 5. *The following statements hold.*

1. *Any subgroup and any quotient group of a k-solvable group are k-solvable.*

2. *If a group has a k-solvable normal subgroup such that the corresponding quotient group is k-solvable, then the group is also k-solvable.*

Proof. The only non-obvious statement of this theorem is that about a quotient group. It follows easily from Lemma 9.5. □ □

SOLVABILITY BY k-RADICALS

The following criterion of solvability by k-radicals holds:

Theorem 6 (A criterion of solvability of equations by k-radicals)**.** *A polynomial equation over a field K is solvable by k-radicals if and only if its Galois group over K is k-solvable.*

We assume that the equation over k has simple roots only and the characteristic of K does not divide any order or comutative factor- groups of subgroups in the Galois group.

Proof. 1. Suppose that the equation can be solved by k-radicals.

We need to prove that the Galois group of the equation is k-solvable. This is proved in exactly the same way as the statement that the Galois group of an equation solvable by radicals is solvable.

Let

$$K = K_0 \subset K_1 \subset \cdots \subset K_n$$

be a chain of fields that arises in the solution of the equation by k-radicals, and

$$G_0 \supset \cdots \supset G_n$$

the chain of Galois groups of the equation over these fields.

By the assumption, the field K_n contains all roots of the equation, therefore, the group G_n is trivial and, in particular, is k-solvable. Suppose that the group G_{i+1} is k-solvable.

We need to prove that the group G_i is also k-solvable.

If the field K_{i+1} is obtained from the field K_i by adjoining a radical, then the Galois group of the field K_{i+1} over the field K_i is solvable, hence

k-solvable. If the field K_{i+1} is obtained from the field K_i by adjoining all roots of an algebraic equation of degree at most k, then the Galois group of the field K_{i+1} over the field K_i is a subgroup of the group $S(k)$, hence is k-solvable.

As we know from the previous lectures, the group G_{i+1} is a normal subgroup of the group G_i;

moreover, the quotient group G_i/G_{i+1} is simultaneously a quotient group of the Galois group of the field K_{i+1} over the field K_i.

The group G_{i+1} is solvable by the induction hypothesis.

The Galois group of the field K_{i+1} over the field K_i is k-solvable, as we have just proved.

We conclude that the group G_i is k-solvable.

2. Suppose that the Galois group G of an algebraic equation over the field K is k-solvable.

Let $\tilde{K}$ denote the field obtained from the field K by adjoining all roots of unity.

The Galois group $\tilde{G}$ of the same equation over the bigger field $\tilde{K}$ is a subgroup of the group G. Therefore, the Galois group $\tilde{G}$ is k-solvable.

Let $\tilde{P}$ denote the field obtained from the field $\tilde{K}$ by adjoining all roots of the given algebraic equation.

The group $\tilde{G}$ acts by automorphisms on $\tilde{P}$ with the invariant subfield $\tilde{K}$. By the theorem we proved in the previous lectures.1, every element of the field $\tilde{P}$ can be expressed through the elements of the field $\tilde{K}$ by taking radicals, performing arithmetic operations and solving algebraic equations of degree at most k.

By definition of the field $\tilde{K}$, every element of this field is expressible through the elements of the field K and the roots of unity.

The theorem is proved. $\square$ $\square$