Lecture 13, October 22

UNSOLVABILITY OF THE GENERAL EQUATION OF THE DEGREE $k+1>4$ EQUATION BY k-RADICALS

A *generic algebraic equation* of degree k with coefficients in the field K is an equation

$$x^k + a_1 x^{k-1} + \cdots + a_k = 0, \tag{9}$$

whose coefficients are generic elements of the field K.

Closely related to generic equations is the *general* equation (9), in which the coefficients a_i are formal variables.

Do there exist formulas containing radicals (k-radicals), the variables $a_1, \ldots, a_k$ and constants from the field K that give solutions of an equation $x^k + a_1^0 x^{k-1} + \cdots + a_0^0 = 0$ as one substitutes the particular elements $a_1^0, \ldots, a_k^0$ of the field K for the variables?

This question can be formalized in the following way. The general algebraic equation can be viewed as an equation over the field

$$K\{a_1, \ldots, a_k\}$$

of rational functions in k independent variables $a_1^0, \ldots, a_k^0$ with coefficients in the field K (in this interpretation, the coefficients of general equation are the elements $a_1^0, \ldots, a_k^0$ of the field $K\{a_1, \ldots, a_k\}$).

We can now ask the question of whether general equation og degree n is solvable over the field $K\{a_1, \ldots, a_k\}$ by radicals (or by k-radicals).

Let us compute the Galois group of equation (7) over the field $K\{a_1, \ldots, a_k\}$.

Consider yet another copy $K\{x_1, \ldots, x_k\}$ of the field of rational functions in k variables equipped with the group $S(k)$ of automorphisms acting by permutations of the variables $x_1, \ldots, x_k$.

The invariant subfield $K_S\{x_1, \ldots, x_k\}$ consists of symmetric rational functions. By the Fundamental Theorem of Symmetric Functions, this field is isomorphic to the field of rational functions of $\sigma_1 = x_1 + \cdots + x_k, \ldots, \sigma_n = x_1 \ldots x_k$.

Therefore, the map

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

extends to an isomorphism

$$F : K\{a_1, \ldots, a_k\} \to K_S\{x_1, \ldots, x_k\}.$$

Let us identify the fields

$$K\{a_1, \ldots, a_k\} \quad \text{and} \quad K_S\{x_1, \ldots, x_k\}$$

by the isomorphism F

From the comparison of Vieta formulas with the formulas defining the map F, it becomes clear that under this identification,

the variables become the roots of equation (7),

the field $K\{x_1, \ldots, x_k\}$ becomes the extension of the field $K\{a_1, \ldots, a_k\}$ by adjoining all roots of equation (7),

the automorphism group $S(k)$ becomes the Galois group of equation (7).

Thus we have proved the following statement:

Proposition 1. *The Galois group of equation (7) over the field $K\{a_1, \ldots, a_k\}$ is isomorphic to the permutation group $S(k)$.*

Theorem 1. *The general equation of degree* $k+1 > 4$ *is not solvable by taking radicals and by solving auxiliary algebraic equations of degree* k *or less.*

Proof. The group $S(k+1)$ has the following normal tower of subgroups:

$$\{e\} \subset A(k+1) \subset S(k+1),$$

where $A(k+1)$ is the alternating group.

For $k+1 > 4$, the group $A(k+1)$ is simple.

The group $A(k+1)$ is not a subgroup of the group $S(k)$ since the group $A(k+1)$ has more elements than the group $S(k)$.

Thus, for $k+1 > 4$, the group $S(k+1)$ is not k-solvable. □ □

As a corollary, we obtain the following theorem.

Theorem 2 (Abel)**.** *The general algebraic equation of degree 5 and higher is not solvable by radicals.*

Remark. Abel had proved this theorem by a different method even before Galois theory appeared. His approach has been later developed by Liouville. Liouville's method allows, for example, to prove that many elementary functions their integrals cannot be computed by elementary functions.

UNSOLVABILITY OF COMPLICATED EQUATIONS BY SOLVING SIMPLIER EQUATIONS

Is it possible to solve a given complicated algebraic equation using the solutions of other, simpler, algebraic equations as admissible operations?

We have considered two well-posed questions of this kind:

the question of solvability of equations by radicals (in which the simpler equations are those of the form $x^n - a = 0$) and

the question of solvability of equations by k-radicals (in which the simpler equations are those of the form $x^n - a = 0$ and all algebraic equations of degree k or less).

Now we discuss the general question of solvability of complicated equation by solving simpler equations.

First we set up the problem of B-solvability of equations and discuss a necessary condition of the solvability.

Than we discuss classes of groups related to the problem of B-solvability of equations.

A NECESSARY CONDITION OF OF SOLVABILITY

Let B be a collection of algebraic equations.

An algebraic equation defined over a field K is automatically defined over any bigger field K_1, $K \subset K_1$. We will assume that the collection B of algebraic equations contains, together with any equation defined over a field K, the same equation considered as an equation over any bigger field $K_1 \supset K$.

Definition. An algebraic equation over a field K is said to be *solvable by solving equations from the collection* B, or *B-solvable* for short, if there exists a chain of fields

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

such that all roots of the equation belong to the field K_n, and, for every $i = 0, \ldots, n-1$, the field K_{i+1} is obtained from the field K_i

by adjoining all roots of some algebraic equation from the collection B defined over the field K_i.

Denote by $G(B)$ the set of Galois groups of all equations belonging to class B.

Proposition 2. *The set $G(B)$ contains, together with any finite group, all subgroups of it.*

Proof. Suppose that some equation defined over the field K belongs to the collection B. Let P be the field obtained from K by adjoining all roots of this equation, G the Galois group of the field P over the field K, and $G_1 \subset G$ any subgroup. Let K_1 denote the intermediate field corresponding to the subgroup G_1. The Galois group of our equation over the field K_1 coincides with G_1. By our assumption, the collection

B contains, together with any equation defined over the field K, the same equation defined over the bigger field K_1. □ □

Theorem 3 (A necessary condition of B-solvability)**.** *If an algebraic equation over a field K is B-solvable, then its Galois group G admits a normal tower*

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

of subgroups, in which every quotient G_i/G_{i+1} is a quotient of some group from $G(B)$.

Proof. Indeed, the B-solvability of an equation over the field K means the existence of a chain of extensions

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

in which the field K_{i+1} is obtained from the field K_i by adjoining all roots of some equation from B, and the last field K_n contains all roots of the initial algebraic equation.

Let

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

be the chain of Galois groups of this equation over this chain of subfields.

We will show that the chain of subgroups thus obtained satisfies the property stated in the theorem.

Indeed, 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 of the

Galois group of the field K_{i+1} over the field K_i. Since the field K_{i+1} is obtained from the field K_i by adjoining all roots of some equation from B, the Galois group of the field K_{i+1} over the field K_i belongs to the set $G(B)$. □ □

CLASSES OF FINITE GROUPS

Let M be a set of finite groups.

DEFINITION. Define the *completion* $\mathcal{K}(M)$ of the set M as the minimal class of finite groups containing all groups from M and satisfying the following properties:

1. together with any group, the class $\mathcal{K}(M)$ contains all subgroups of it;

2. together with any group, the class $\mathcal{K}(M)$ contains all quotients of it;

3. if a group G has a normal subgroup H such that the groups H and G/H are in the class $\mathcal{K}(M)$, then the group G is in the class $\mathcal{K}(M)$.

The theorem proved above suggests the following problem:

for a given set M of finite groups, describe its completion $\mathcal{K}(M)$.

Recall the Jordan–Hölder theorem.

A normal tower

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

of a group G is said to be *unrefinable* (or *maximal*) if all quotient groups G_i/G_{i+1} of this tower are simple groups.

The Jordan–Hölder theorem asserts that *for every finite group G, the set of quotient groups associated to any unrefinable normal tower of the group G does not depend on the choice of an unrefinable tower* (and hence is an invariant of the group).

Proposition 3. *A group G belongs to the class $\mathcal{K}(M)$ if and only if every quotient group G_i/G_{i+1} with respect to an unrefinable normal tower of the group G is a subquotient of a group from M.*

A subquotient is a quotient of a subgroup.

Proof. Firstly, by definition of the class $\mathcal{K}(M)$, every group G satisfying the assumptions of the proposition belongs to the class $\mathcal{K}(M)$. Secondly, it is not hard to verify that groups G satisfying the assumptions of the proposition have properties 1–3 listed in the definition of the completion of M. □ □

Corollary 4. *The following statements hold.*

1. *The completion of the class of all finite Abelian groups is the class of all finite solvable groups.*

2. *The completion of the set consisting of all Abelian groups and the group $S(k)$ is the class of all finite k-solvable groups.*

Remark. Necessary conditions of solvability of algebraic equations by radicals and by k-radicals are particular cases of Theorem 10.2.