Lecture 11, October 15

A CRITERIUM OF SOLVABILITY OF EQUATIONS BY RADICALS

An algebraic equation over a field K is said to be *solvable by radicals* if there exists a chain of extensions

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

in which every field K_{j+1} is obtained from the field K_j, $j = 0, \ldots, n-1$, by adjoining some radical, and the field K_n contains all roots of this algebraic equation.

Is a given algebraic equation solvable by radicals?

Galois theory was created to answer this question.

First we consider the multiplicative group of all n-th roots of unity that lie in a given field K.

Then we consider the Galois group of the equation $x^n = a$.

After that finally we give a criterion of solvability of an algebraic equation by radicals (in terms of the Galois group of this equation).

ROOTS OF UNITY

Let K be a field. Let

$$K_E^*$$

denote the multiplicative group of all roots of unity lying in the field i.e. $a \in K_E^*$ if and only if $a \in K$, and, for some positive integer n, we have

$$a^n = 1.$$

Proposition 1. *If there is a subgroup of the group K_E^* consisting of l elements, then the equation $x^l = 1$ has exactly l solutions in the field K, and the subgroup under consideration is formed by all these solutions.*

Proof. Every element in a group of order l satisfies the equation

$$x^l = 1.$$

The field contains no more than l roots of this equation, and the subgroup has exactly l elements by our assumption. □ □

From Proposition it follows, in particular, that the group K_E^* has at most one subgroup of any given finite order.

Problem 1. *A finite Abelian group that has at most one cyclic subgroup of any given finite order is cyclic. In particular, every finite subgroup in the group* K_E^* *is cyclic.*

HINT: Every finite cyclic group is isomorphic to the group

$$G = (\mathbb{Z}/p_1^{k_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_n^{k_n}\mathbb{Z}).$$

Show that if such group satisfies the assumptions of the Problem then it is cyclic by the Chinese Remainder Theorem.

Remark 1. *Therefore the groups of roots of unity with the given number* m *of elements are isomorphic to each other. In the field of complex numbers any multiplicative group of order* m *consisting of roots of unity and is obviously cyclic.*

A cyclic group with m elements identifies with the group of residues modulo m.

Proposition 2. *The full automorphism group of the group*

$$\mathbb{Z}/m\mathbb{Z}$$

is isomorphic to the multiplicative group of all invertible elements in the ring of residues modulo m.

In particular, this automorphism group is commutative.

Proof. An automorphism F of the group

$$\mathbb{Z}/m\mathbb{Z}$$

is uniquely determined by the element $F(1)$, which must obviously be invertible in the multiplicative group of the ring of residues. This automorphism coincides with the multiplication by $F(1)$. $\square$ $\square$

Proposition 3. *Suppose that a Galois extension P of a field K is obtained from the field K by adjoining some roots of unity. Then the Galois group of the field P over the field K is commutative.*

Proof. All roots of unity that lie in the field P form a cyclic group with respect to multiplication.

A transformation from the Galois group defines an automorphism of this group and is uniquely determined by this automorphism, i.e. the Galois group embeds into the full automorphism group of a cyclic group.

Thus the needed statement follows from the previous Proposition. $\square$

$\square$

GALOIS GROUP OF THE EQUATION $x^n = a$

Proposition 4. *Suppose that a field K contains all roots of unity of degree n and n is not divisible by the characteristic is of the field.*

Then the Galois group of the equation

$$x^n - a = 0$$

over the field K is a subgroup of the cyclic group with n elements (provided that $a \in K$).

Proof. The group of all roots of unity of degree n is cyclic.

Let ξ be any generator of this group. Fix any root x_0 of the equation

$$x^n - a = 0.$$

Then we can label all roots of the equation $x^n - a = 0$ with residues i modulo n by setting

$$x_i = \xi^i x_0.$$

Suppose that a transformation g in the Galois group takes the root x_0 to the root x_i. Then

$$g(x_k) = g(\xi^k x_0) = \xi^k q(x_0) = \xi^{k+i} x_0 - x_{k+i}$$

(recall that, by our assumption, $\xi \in K$, hence $g(\xi) = \xi$),

i.e. every transformation in the Galois group defines a cyclic permutation of the roots.

Therefore, the Galois group embeds into the cyclic group with n elements. $\square$ $\square$

Lemma 1. *The Galois group G of the equation*

$$x^n - a = 0$$

over the field K has a commutative normal subgroup

$$G_1$$

such that the corresponding quotient

$$G/G_1$$

is commutative.

In particular, the group G is solvable.

Proof. Let P be an extension of the field K obtained by adjoining all roots of the equation

$$x^n = a$$

to this field.

The ratio of any two roots of the equation $x^n = a$ is a root of unity of degree n.

This implies that the field P contains all n-th roots of unity. Let

$$K_1 \supset K$$

denote the extension of the field K obtained by adjoining all roots of unity of degree n.

We have the inclusions

$$K \subset K_1 \subset P.$$

Let G_1 denote the Galois group of the equation $x^n = a$ over the field K_1.

By As we already proved the group G_1 is commutative.

The group G_1 is a normal subgroup of the group G, since the field K_1 is a Galois extension of the field K.

The quotient group G/G_1 is commutative since, by Lemma 8.4, the Galois group of the field K_1 over the field K is commutative. $\square$ $\square$

SOLVABILITY BY RADICALS

The following criterion of solvability of algebraic equations by radicals holds:

Theorem 2 (A criterion of solvability of equations by radicals)**.** *An polynomial equation over some field K is solvable by radicals if and only if its Galois group is solvable.*

We assume that the equation has no multiple root and the degree of the equation is not divisible by the characteristic of the field K.

Proof. Suppose that an equation can be solved by radicals.

Solvability of the equation by radicals over a field K means the existence of a chain of extensions

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

in which every field K_{j+1} is obtained from the field K_j, $j = 0, 1, \ldots, n-1$, by adjoining a radical, and the field K_n contains all roots of the initial equation.

Let G_j denote the Galois group of our equation over the field K_j.

Let us see what happens with the Galois group when we pass from the field K_j to the field K_{j+1}.

According to Theorem we proved above the group G_{j+1} is a normal subgroup of the group G_j, moreover, the quotient G_j/G_{j+1} is simultaneously a quotient of the Galois group of the field K_{j+1} over the field K_j.

Since the field K_{j+1} is obtained from the field K_j by adjoining a radical, we conclude by that the Galois group of the field K_{j+1} over the field K_j is solvable.

(In the case, where the field K contains all roots of unity, the Galois group of the field K_{j+1} over the field K_j is commutative).

Since all roots of the algebraic equation lie in the field K_n by our assumption, the Galois group G_n of the algebraic equation over the field K_n is trivial.

Thus, if the equation can be solved by radicals, then its Galois group admits a chain of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_n,$$

in which every group G_{j+1} is a normal subgroup of the group G_j with a solvable quotient G_j/G_{j+1}, and the group G_n is trivial.

(If the field K contains all roots of unity, then the quotients G_j/G_{j+1} are commutative.)

Thus, if the equation is solvable by radicals, then its Galois group is solvable.

Suppose now that the Galois group G of an algebraic equation over the field K is 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 algebraic equation over the bigger field $\tilde{K}$ is a subgroup of the Galois group G.

Hence the Galois group $\tilde{G}$ is solvable. Let $\tilde{P}$ denote the field obtained from the field $\tilde{K}$ by adjoining all roots of the algebraic equation.

The solvable group $\tilde{G}$ acts by automorphisms of the field $\tilde{P}$ with the invariant subfield $\tilde{K}$. By Theorem 1.2, every element of the field $\tilde{P}$ is expressible by radicals through the elements of the field $\tilde{K}$. By definition of the field $\tilde{K}$, every element of this field is expressible through the roots of unity and the elements of the field K. The theorem is proved. $\square$ $\square$