NAP 2018 Module-V: Applications of Galois theory Lecture 7 & 8: July 18 & 19, 2018

1. Kummer Theory

Recall that we have a description of cyclic Galois extension E/F when the field F contains a primitive n-th root of unity.

Theorem 1. *Let F be a field containing a primitive n-th root of unity. Two cyclic extensions $F(a^{\frac{1}{n}})$ and $F(b^{\frac{1}{n}})$ of F of degree n are equal if and only if $a = b^r c^n$ for some $r \in \mathbb{Z}$ relatively prime to n and some $c \in F$ if and only if a and b generate the same subgroup of $F^\times / F^{\times n}$. (This was discussed in last lecture!).*

Definition 2. A field extension E/F which is a Galois extension is said to be an *abelian* extension if the Galois group $\mathrm{Gal}(E/F)$ is an abelian group.

Now we will discuss finite extensions E/F which are abelian extensions.

Question 3. How are (finite) abelian groups built?

Theorem 4 (Structure theorem of finite abelian groups)**.** *Every finite abelian group is isomorphic to a direct product of (finite) cyclic groups. In other words, if G is a finite abelian group then there exists $n_1, \cdots, n_k \in \mathbb{Z}$ such that*

$$G \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}).$$

Note that we have a description of cyclic Galois extensions E/F if the field F contains a primitive n-th roots of unity. Since finite abelian groups are *"made of"* finite cyclic groups, it is possible to use the description of cyclic Galois extension to describe abelian Galois extensions. This discription / discusiion is what is referred as Kummer theory which aims to describe abelian extensions of a fixed *exponent* (see below).

Definition 5. A group G is said to have exponentn $n \in \mathbb{Z}$ if $x^n = id \in G$ for all $x \in G$ and n is the smallest positive integer for which this is true.

Some discussion: Let E/F be a finite Galois extension with the Galois group G. Write $E^{\times n} := \{x^n : x \in E^\times\} \subset E^\times$. We have the following "short exact sequence"

$$1 \to \mu_n \to E^\times \to E^{\times n} \to 1$$

Following some generalities form Group cohomology one obtains a "long exact sequene"

$$1 \to \mu_n \to F^\times \to E^{\times n} \cap F^\times \to H^1(G, \mu_n) \to H^1(G, E^\times) \to \cdots$$

Hilbert's theorem 90: $\Rightarrow H^1(G, E^\times) = 1$.
We also have $H^1(G, \mu_n) = \mathrm{Hom}(G, \mu_n)$.
We obtain

$$(E^{\times n} \cap F^\times)/F^{\times n} \xrightarrow{\sim} \mathrm{Hom}(G, \mu_n).$$

The map is described as follows: let $a = \alpha^n \in F^\times \cap E^{\times n}$ where $a \in F^\times$ and $\alpha \in E^\times$. Then a is mapped to a homomorphism such that $\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$.
Recall that for finite abelian groups of exponent n we have $\mathrm{Hom}(G, \mu_n) = \mathrm{Hom}(G, \mathbb{C}^\times)$ and then

$$|\mathrm{Hom}(G, \mu_n)| = \text{ no. of elements in } G.$$

Now we describe finite abelian Galois extensions as follows.

Theorem 6. *Let F be a field containing a primitive n-th root of unity. There is a bijection between the finite abelian extensions E/F of exponent n (contained in some fixed algebraic closure Ω of F) and the subgroups B of $F^{\times}$ containing $F^{\times n}$ as a finite index subgroup (i.e. $(B : F^{\times n}) < \infty$) given by*

$$E \mapsto F^{\times} \cap E^{\times n}.$$

The extension corresponding to B is $F[B^{\frac{1}{n}}]$ the smallest subfield of Ω containing F and an n-th root of each element of B. Moreover, if the extension E/F corresponds to the subset B then

$$[E : F] = (B : F^{\times n}).$$

Note that a finite abelian group of exponent 2 is isomorphic to direct product of finitely many copies of $\mathbb{Z}/2\mathbb{Z}$, i.e. $(\mathbb{Z}/2\mathbb{Z})^k$ for some $k \in \mathbb{Z}$. Here are a few examples for $n = 2$.

Example 7. (1) For $F = \mathbb{R}$ and $n = 2$. The one-to-one correspondence is with the subgroups of $\mathbb{R}^{\times}/\mathbb{R}^{\times 2} \cong \{\pm 1\}$.
(2) For $F = \mathbb{Q}$ and $n = 2$. The one-to-one correspondence is with finite subgroups of $\mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$.

Remark 8. Let E/F be a finite abelian extesion of exponent n. Let $B(E)$ be the subgroup of $F^{\times}$ corresponding to the extension E/F as in Theorem 6. Then there is a *perfect pairing*

$$\frac{B(E)}{F^{\times n}} \times Gal(E/F) \to \mu_n$$

which is given by

$$(a, \sigma) \mapsto \frac{\sigma(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}.$$

2. Galois' Solvability Theorem

Definition 9. Let F be a field and $f(X) \in F[X]$. We say that $f(X) = 0$ is *solvable in radicals* if the solution can be written using algebraic operations of addition, substraction, multiplication, division and the extraction of m-th roots. More precisely, there exists a tower of fields

$$F = F_0 \subset F_1 \subset \cdots \subset F_m$$

such that

(a) $F_i = F_{i-1}[\alpha]$ where $\alpha^{m_i} \in F_{i-1}$ and
(b) F_m contains a splitting field of $f(X)$.

Definition 10 (Galois 1832)**.** A group G is called solvable if there exists a sequence of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{1\}$$

such that each G_i is normal in G_{i-1} and G_{i-1}/G_i is a cyclic group.

Theorem 11. *Let F be a field of characteristic zero. Then $f(X) \in F[X]$ is solvable in radicals if and only if the Galois group of $f(X)$ is solvable.*

Warning: If a polynomial $f(X) \in F[X]$ is not solvable by radicals, it DOES NOT mean that it has no roots in any field extension. It only says that its root can not be expressed in terms of radicals.

Remark 12. The theorem of Galois as stated above is only for characteristic zero. For example, take $F = \mathbb{F}_2$ and $f(X) = X^2 + X + 1 \in \mathbb{F}_2[X]$. Then the roots of $f(X)$ can not be written in terms of radical but the Galois group is $\mathbb{Z}/2\mathbb{Z}$ which is abelian and hence solvable.

Example 13. Take $F = \mathbb{Q}$ and $n \in \mathbb{Z}$. Then there exists a polynomial $f \in \mathbb{Q}[X]$ for which the Galois group G_f is S_n (the symmetric group on n-symbols). Moreover, from group theory one knows that the group S_n, for $n \geq 5$, is not solvable. We conclude that there exists polynomials over $\mathbb{Q}$ which are not solvable, i.e the roots cannot be expressed in terms of radicals. Note that the degree of such a polynomial will have to be ≥ 5.

For $n = 5$, one can take the polynomials $X^5 - X + 1, X^5 - 10X + 5 \in \mathbb{Q}[X]$ etc. which have the Galois group S_5 and hence their roots can not be written in terms of radicals.