NAP 2018 Module-V: Applications of Galois theory Lecture 6: July 17, 2018 (Tuesday)

We will discuss how to construct n degree cyclic Galois extensions of a field F.

Example 1. (a) Some examples of quadratic extensions over $\mathbb{Q}$ you have seen.

$$\begin{array}{ccccc} \mathbb{Q}(\sqrt{2}) & \mathbb{Q}(\sqrt{3}) & \mathbb{Q}(i) & \cdots & \mathbb{Q}(\sqrt{d}) \\ | & | & | & & | \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} & \cdots & \mathbb{Q} \end{array}$$

All these extensions are Galois.

(b) Some examples of degree three extensions of $\mathbb{Q}$.

$$\begin{array}{cccc} \mathbb{Q}(2^{\frac{1}{3}}) & Q(3^{\frac{1}{3}}) & \mathbb{Q}(5^{\frac{1}{3}}) & \cdots \\ | & | & | & \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} & \cdots \end{array}$$

But all these extensions are **NOT** Galois extensions! These extensions are not normal. For example, in $\mathbb{Q}(2^{\frac{1}{3}})$ we have only one root of the polynomial $X^3 - 2 \in \mathbb{Q}[X]$.

(c) Examples of degree four extensions of $\mathbb{Q}$?

$$\begin{array}{cccc} \mathbb{Q}(2^{\frac{1}{4}}) & Q(3^{\frac{1}{4}}) & \mathbb{Q}(5^{\frac{1}{4}}) & \cdots \\ | & | & | & \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} & \cdots \end{array}$$

But all these extensions are **NOT** Galois extensions! These are not normal extensions.

Question 2. Are these all possible quadratic extension of $\mathbb{Q}$? (You have seen the answer before.)

For any quadratic extension $E/\mathbb{Q}$ there exists $d \in \mathbb{Z}$ which is not a square in $\mathbb{Z}$ and $E = \mathbb{Q}(\sqrt{d})$.

Question 3. How to construct degree three, degree four or degree n cyclic Galois extensions over $\mathbb{Q}$?

We have realised, for example, that only adding one root of $X^3 - 2$ is not enough. We must add all the root of this polynomial to get a normal extension, that is $2^{\frac{1}{3}}\omega$ and $2^{\frac{1}{3}}\omega^2$ where ω is a cube root of unity. The filed extension will be $\mathbb{Q}(2^{\frac{1}{3}}, \omega)$ over $\mathbb{Q}$. Now the degree of this extension is six (not three). Imagine if ω was an element in $\mathbb{Q}$, then this extension $\mathbb{Q}(2^{\frac{1}{3}})/\mathbb{Q}$ would have been normal and of degree three but unfortunately this is not the case.

Similarly, if we try to add one root of $X^n - 2 \in \mathbb{Q}[X]$ to construct a n-degree cyclic Galois extension over $\mathbb{Q}$ then it will not work since n-th root of unity are not in $\mathbb{Q}$ for $n \geq 3$.

Our approach: We want to construct n-degree cyclic Galois extension of a field F and we wanted to do this by adding a root of a polynomial of type $X^n - a$ for suitable $a \in F$. This approach works very well if n-th roots of unity are in F (which is not the case if $F = \mathbb{Q}$ and $n \geq 3$).

Remark 4. In order to make our approach work we assume that our base field F has all *distinct* n-th root of unity. This will also require that the characteristic p of the field F does not divide n.

Theorem 5. *Let F be a field which contains a primitive root of unity. Let $E = F(\alpha)$ where $\alpha^n \in F$ and no smaller power of $\alpha \in F$. Then E is a Galois extension of F with cyclic Galois group of order n. Conversely, if E is a cyclic extension of F of degree n, then $E = F(\alpha)$ for some α with $\alpha^n \in F$.*

It may be the case, $F(\alpha) = F(\beta)$. For example;

Example 6. (a) Quadratic extension: Fix $F = \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{8}) = \mathbb{Q}(\sqrt{18})$ and $\mathbb{Q}(\sqrt{11}) = \mathbb{Q}(\sqrt{44}) = \mathbb{Q}(\sqrt{99})$ etc.

(b) Degree three extension: Fix $F = \mathbb{Q}(\omega)$ where ω is a primitive third root of unity. Then $F(2^{\frac{1}{3}}) = F(4^{\frac{1}{3}}) = F(16^{\frac{1}{3}}) = F(54^{\frac{1}{3}})$ and $F(3^{\frac{1}{3}}) = F(9^{\frac{1}{3}}) = F(24^{\frac{1}{3}}) = F(81^{\frac{1}{3}})$ etc.

(c) Degree your extension: Fix $F = \mathbb{Q}(i)$ where i is a primitive fourth root of unity. Then $F(2^{\frac{1}{4}}) = F(8^{\frac{1}{4}}) = F(32^{\frac{1}{4}}) = F(162^{\frac{1}{4}})$ and $F(3^{\frac{1}{4}}) = F(48^{\frac{1}{4}}) = F(27^{\frac{1}{4}})$ etc.

Theorem 7. *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 $F^\times / F^{\times n}$.*