LECTURE 20

12.04.2024

Splitting field

- Let K be a field. A polynomial $f(x)$ in $K[x]$ is said to split over a field $S \supseteq K$ if $f(x)$ can be factored as a product of linear factors in $S[x]$.
- A field S containing K is said to be a splitting field for $f(x)$ over K if $f(x)$ splits over S, but over no intermediate field of S/K.

Example

1. Consider the fields $\mathbb{C}$ and $\mathbb{R}$, and the polynomial x^2+1 on $\mathbb{R}$. $\mathbb{C}$ is a splitting field over $\mathbb{R}$.
   - x^2+1 splits over $\mathbb{C}$ into $(x+i)(x-i)$.
   - Also, $[\mathbb{C}:\mathbb{R}] = 2$. If there is any such intermediate field,

then $[\mathbb{C}:\mathbb{R}] = [\mathbb{C}:L][L:\mathbb{R}]$. So, $L = \mathbb{C}$ or, $\mathbb{R}$.

(2) Consider the fields $\mathbb{C}$ and $\mathbb{Q}$, and the polynomial x^2+1 over $\mathbb{Q}$. $\mathbb{C}$ is not a splitting field of x^2+1 over $\mathbb{Q}$, as $\mathbb{Q}(i)$ is an intermediate field over which x^2+1 splits.

H.W. Let K be field and $f(x) \in K[x]$. Let F/K be a field extension s.t. $f(x)$ splits over F, that is,

$$f(x) = c(x-c_1)(x-c_2) \cdots (x-c_n)$$

in F. Then, $K(c_1, c_2, \cdots, c_n)$ is a splitting field for $f(x)$ over K.

Let us now discuss about the existence and uniqueness of splitting fields.

Proposition (Existence): Let K be a field and $f(x)$ be a non-constant polynomial over K. Then there exists a splitting field of $f(x)$ over K.

Proof idea: By induction on the degree of the polynomial $f(x)$.

Base Step: $\deg f(x) = 1$. Then the splitting field is K itself.

Assume **I.H.**

I.S.: Take $\deg f(x) = n+1$. $f(x)$ has a root c_1 in some field extension K_1/K.

Then, $f(x) = (x - c_1) f_1(x)$. Apply I.H. and complete the proof.

Proposition (Uniqueness): Let K be a field and $f(x)$ be a non-constant polynomial over K. Show that any two splitting fields S and S' of $f(x)$ are isomorphic.

Proof idea: We also prove this by applying induction on the degree of the polynomial $f(x)$.

Base Step: $\deg f(x) = 1$. Then $S = S' = K$.

Assume I.H.

I.S.: $\deg f(x) = n+1$. Without loss of generality, let us assume $f(x)$ to be irreducible. Let c_1 be a root of $f(x)$ in S and c_1' be the same in S'. Then, $K[c_1] = K(c_1)$ and $K[c_1'] = K(c_1')$.

Define an isomorphism $\alpha : K(c_1) \to K(c_1')$: $c_1 \mapsto c_1'$ and extend it to an isomorphism from S to S' using induction hypothesis. This would complete the proof.

Example

Consider $\mathbb{Q}[x]$ and consider the polynomial $x^4 - 3$.

- First we would show that $x^4 - 3$ is irreducible over $\mathbb{Q}$. We would use

Eisenstein Criteria :

[Let $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ be a polynomial with integer coefficients. Let there be a prime number p s.t. : (i) $p \nmid a_n$, (ii) $p \mid a_i$, $i = 0, 1, \ldots, n-1$ and, (iii) $p^2 \nmid a_0$.

Then the polynomial is irreducible over $\mathbb{Q}$.]

Thus, we have that $x^4 - 3$ is irreducible over $\mathbb{Q}$ $(p = 3)$.

Then we have a field $F = \mathbb{Q}[x] / (x^4 - 3)$

which has a root of $x^4 - 3$, namely, $x + (x^4 - 3) = \lambda_1$, say.

Then, we can write the following:

$$\mathbb{Q}[x] / (x^4 - 3) = \mathbb{Q}(\lambda_1) = \{ a + b\lambda_1 + c\lambda_1^2 + d\lambda_1^3 : a, b, c, d \in \mathbb{Q} \}.$$

Indeed, $\{1, \lambda_1, \lambda_1^2, \lambda_1^3\}$ forms a basis of $\mathbb{Q}(\lambda_1)$ over $\mathbb{Q}$ (as, $x^4 - 3$ forms the minimal polynomial of λ_1 over $\mathbb{Q}$).

So, $x^4 - 3 = (x - \lambda_1)\, g(x)$.

Repeating the same argument, we would finally have $\mathbb{Q}(\lambda_1)(\lambda_2)(\lambda_3)(\lambda_4)$
$= \mathbb{Q}(\lambda_1, \lambda_2, \lambda_3, \lambda_4)$, with

$$x^4 - 3 = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)(x-\lambda_4).$$

Without loss of generality we can say, $\lambda_2 = -\lambda_1$ and $\lambda_4 = -\lambda_3$.

Now, if we consider the polynomial $x^4 - 3$ in $\mathbb{Q}(\lambda_1)$, we can write,

$$x^4 - 3 = (x^2 - \lambda_1^2)(x^2 + \lambda_1^2)$$
$$= (x-\lambda_1)(x+\lambda_1)(x^2+\lambda_1^2)$$

We have: $(x^2+\lambda_1^2)$ is irreducible over $\mathbb{Q}(\lambda_1)$ (Check!). And considering λ_3 to be a root of $x^2+\lambda_1^2$ over $\mathbb{Q}(\lambda_1)$, we have $[\mathbb{Q}(\lambda_1,\lambda_3) : \mathbb{Q}(\lambda_1)] = 2$.

Also, $[\mathbb{Q}(\lambda_1) : \mathbb{Q}] = 4$

So, $[\mathbb{Q}(\lambda_1,\lambda_3) : \mathbb{Q}] = [\mathbb{Q}(\lambda_1,\lambda_3) : \mathbb{Q}(\lambda_1)][\mathbb{Q}(\lambda_1) : \mathbb{Q}]$
$= 4 \cdot 2 = 8.$