LECTURE 19

09.04.2024

Proposition: If F/K is a finite field extension, then every element of F is algebraic over K.

Proof: Let $[F:K] = n$. Take any $c \in F$. To show that c is algebraic over K.

Case I: $c = 0$. Our required polynomial is x.

Case II. $c = 1$. A required polynomial is $x - 1$.

Case III. $c \neq 0, 1$. Let us consider the set $\{1, c, c^2, \ldots, c^n\}$.

(a) Not all of them are distinct.

Then there exist j, l, say, such that $c^j = c^l$, $0 \leq j < l \leq n$. So, $c^{l-j} = 1$, and our required polynomial can be given by $x^{l-j} - 1$.

(b) All of them are distinct.

Then $\{1, c, c^2, \cdots c^n\}$ forms a linearly dependent set. (Why?). Then, there exist $k_0, k_1, k_2 \cdots, k_n \in K$, not all zero, such that $k_0 + k_1 c + k_2 c^2 + \cdots + k_n c^n = 0$, which gives us our required polynomial.

This completes the proof.

Problem: Show that $x^2 - 7$ is irreducible in $\mathbb{Q}(\sqrt{3})[x]$

Solution: Suppose not. Then,

$$x^2 - 7 = \left(x - (a + b\sqrt{3})\right)\left(x - (c + d\sqrt{3})\right),$$ where, $a, b, c, d \in \mathbb{Q}$

Then, $$x^2 - 7 = x^2 - \left((a+c) + (b+d)\sqrt{3}\right)x + \left(ac + 3bd + (ad+bc)\sqrt{3}\right)$$

So: $(a+c) + (b+d)\sqrt{3} = 0$

and, $ac + 3b + (ad+bc)\sqrt{3} = -7$

Now, $\{1, \sqrt{3}\}$ forms a basis over $\mathbb{Q}$ for the field extension $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$.

We have: $a + c = 0$, or, $a = -c$

and $b + d = 0$, or $b = -d$.

So, $(-a^2 - 3b^2) + (-2ab)\sqrt{3} = -7$.

Similarly, we have:

$-a^2 - 3b^2 = -7$ and $-2ab = 0$

But then, $a = 0$ or, $b = 0$.

Case I. $a = 0$. Then $3b^2 = 7$. But $b \in \mathbb{Q}$.

Then, $b = \frac{p}{q}$, where p, q are integers, $q \neq 0$

and p and q are relatively prime to each other.

Then, $3p^2 = 7q^2$, a contradiction.

So this case is not possible.

Case II. $b = 0$. Then $a^2 = 7$, a contradiction. So, this case is also not possible.

Hence, x^2-7 is irreducible in $\mathbb{Q}(\sqrt{3})[x]$.
This completes the solution.

Intermediate Field

Let F/K be a field extension. A subfield L of F is called an intermediate field of F/K if $K \subseteq L \subseteq F$. We note that L is also a subspace of F over K.

H.W. Let F/K be a field extension and L be an intermediate field. Show that $[F:K] = [F:L][L:K]$.

Example

$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$: Consider the intermediate field $\mathbb{Q}(\sqrt{2})$ where $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$.

Then, we have the field extensions

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}(\sqrt{2})$. Now, x^2-2 is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$, x^2-3 is the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. Thus, $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ and $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$, and finally, following the given homework above,

$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 2\cdot 2 = 4$, with basis

$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

Proposition Let F/K be a field extension. Let L be the set of all elements in F that are algebraic over K. Then, L is a intermediate field of F/K.

Proof: Of course, $L \subseteq F$. Let us now show that $K \subseteq L$. Take $k \in K$. Then $x - k$ is the required polynomial showing that k is algebraic over K. So, $k \in L$, and hence $K \subseteq L$. So, $K \subseteq L \subseteq F$.

It remains to be shown that L is a field. Take $a, b \in L$ with $b \neq 0$. It is enough to show that $a - b \in L$ and $ab^{-1} \in L$.

Let m be the degree of the minimal polynomial of a over K and n be the same for b over K. Consider the field extensions $K(a)/K$ and $K(a,b)/K(a)$.

Now, $[K(a) : K] = m$

and $[K(a,b) : K(a)] \leq n$ (Why?).

Thus, $[K(a,b) : K]$ is finite.

So, every element of $K(a,b)$ is algebraic over K. Since $K(a,b)$ forms a field, and $a, b \in K(a,b)$; $a-b$, $ab^{-1} \in K(a,b)$. So, $a-b$ and ab^{-1} are algebraic over K, and hence, $a-b$, $ab^{-1} \in L$. Thus L forms a field. This completes the proof.

We will now consider the existence of such field extensions which are generated by roots of polynomials. First, we will study the following result which gives a positive answer regarding existence of roots of any polynomial over a field.

Theorem: Let K be a field and let $f(x)$ be a non-constant polynomial in $K[x]$. Then, there exists a field extension F/K such that F contains a root of $f(x)$.

Proof: Without loss of generality we can assume that $f(x)$ is irreducible in

$K[x]$. (Why?). Then $K[x]/(f(x))$ forms a field. Take $F = K[x]/(f(x))$. We need to show the following:

(i) K can be embedded in F, that is, there is an injective homomorphism from K into F.

(ii) F contains a root of $f(x)$.

<u>Proof of (i)</u>:

Consider the natural homomorphism,

$\alpha : K[x] \to K[x]/(f(x)) : g(x) \mapsto g(x) + (f(x))$

Now, $K \subseteq K[x]$. And, $K \cap (f(x)) = \{0\}$.

Consider $a, b \in K$ s.t. $\alpha(a) = \alpha(b)$.

So, $a + (f(x)) = b + (f(x))$, implies,

$a - b \in (f(x))$ implies $a - b = 0$, as $a-b \in K$.

So, $a = b$, and hence $\alpha|_K$ is injective.

Then, $K \cong \operatorname{Im}(\alpha|_K) \subseteq F$. So, we can say that F/K is a field extension.

Proof of (ii).

To show that $f(x)$ has a root in $F = K[x]/(f(x))$

Now, $\alpha(f(x)) = 0_F$.
Also, $\alpha(f(x)) = f(x) + (f(x))$.

$$= f(x + (f(x)))$$

$$= f(\alpha(x))$$

So, $f(\alpha(x)) = 0_F$

Hence, $\alpha(x)$ is a root of $f(x)$ in F.
This completes the proof.