NAP 2019, MODULE-III, LECTURE # 3 & 4: JUNE 7, 2019

SHIV PRAKASH PATEL & SHREEDEVI MASUTI

*On 5th June 2019, Wednesday there was a holiday so the lecture did not take place. To make up this loss we had two lecture on Friday. This is summary of both of these lectures on Friday.

Today's Aim: Our aim today is to discuss several basic examples that give us a better idea of theorems which we have discussed in earlier lectures.

We recall the statements of the following theorem which was discussed in the previous lectures.

Theorem 1. *Let $\Sigma : K$ be a splitting field extension for a polynomial $f(X) \in K[X]$, and $i : K \to L$ be a monomorphism from K into a field L. Then*

$$\boxed{\exists \text{ a monomorphism } j : \Sigma \to L \text{ with } j|_K = i} \Leftrightarrow \boxed{i(f(X)) \text{ splits over } L.}$$

It has the following immediate corollaries.

Corollary 2. *Let $iK \to K'$ be an isomorphism of fields and $f(X) \in K[X]$. Let $\Sigma : K$ be a splitting field extension for $f(X)$ and $\Sigma' : K'$ a splitting field for $i(f(X))$. Then there exists an isomorphism $j : \Sigma \to \Sigma'$ such that $j|_K = i$.*

Corollary 3. *Let $f(X) \in K[X]$ be an irreducible polynomial and $\Sigma : K$ a splitting field extension for $f(X)$. Let α, β be roots of f in Σ. Then there exists an automorphism $\sigma : \Sigma \to \Sigma$ such that $\sigma(\alpha) = \beta$. and $\sigma|_K$ is the identity map on K.*

Example 4. For $f(X) = X^p - 2 \in \mathbb{Q}[X]$ where p is a prime number. We found that the field $L := \mathbb{Q}(2^{\frac{1}{p}}, \omega)$ (which is contained in $\mathbb{C}$) is a splitting fields for $f(X)$ where $2^{\frac{1}{p}}$ is the real root of $f(X)$ and $\omega \neq 1$ is any p-th root of unity (which is a complex number). We also pointed out that if p is not a prime number then any $\omega \neq 1$ will not work. We computed the degree $[L : Q]$ which is $p(p-1)$ by considering the intermediate extensions, $\mathbb{Q} \subset \mathbb{Q}(2^{\frac{1}{p}}) \subset L$ and $\mathbb{Q} \subset \mathbb{Q}(\omega) \subset L$ which have degree p and $p-1$ respectively. Note that $[L : \mathbb{Q}] = p(p-1) \leq p!$.

Example 5. For $f(X) = X^6 - 1 \in \mathbb{Q}[X]$ we showed that the field $\mathbb{Q}(\omega)$ (which is contained in $\mathbb{C}$), where $\omega \neq 1$ is a cube root of unity, is a splitting field for $X^6 - 1$. Moreover, $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$ which is $\leq 6!$.

Example 6. For $f(X) = X^6 + 1 \in \mathbb{Q}[X]$ we proved that the field $\mathbb{Q}(\omega, \iota)$ (which is contained in $\mathbb{C}$), where $\omega \neq 1$ is a cube root of unity and ι is a square root of -1, is a splitting field of $X^6 + 1$. Moreover the degree $[\mathbb{Q}(\omega, \iota) : \mathbb{Q}] = 4$ which is $\leq 6!$.

Example 7. Consider $f(X) = X^2 + aX + b \in L[X]$ for an arbitrary field K in which 2 is invertible. Then write $f(X) = (X + \frac{a}{2})^2 - \frac{a^2-4b}{4}$. Write $\mu := \frac{a^2-4b}{4}$.
Case 1: If there is a $\nu \in K$ such that $\mu = \nu^2$ then $f(X) = (X + \frac{a}{2} + \nu)(X + \frac{a}{2} - \nu)$, that is $f(X)$ splits over K and therefore K itself is a splitting field for $f(X)$.
Case 2: If there is a no $\nu \in K$ such that $\mu = \nu^2$ then $f(X)$ is irreducible. Then there is a degree 2

extension $L : K$ which is a splitting field extension for $f(X)$. If we write ν for a square root of μ then L cab be taken to be $K(\nu)$. One can also take L to be $K[X]/(f(X))$.

Remark: Note that for a degree two polynomial over a field, in which 2 is invertible, the splitting field is a simple extension which is obtained by *adding* a square root of some element of the field. However a two degree extension is not always obtained by *adding* a square root of some element of the field if 2 is not invertible in K, as in the next example.

Example 8. Consider $\mathbb{Z}_2 = \{0, 1\}$ which is a field of order 2. We wish to consider a degree two extension of this field. Then we need an irreducible polynomial of degree 2. Note that there are only 4 polynomials of degree two. These are as follows: $X^2 = X \cdot X, X^2 + X = X(X+1), X^2 + 1 = (X+1)^2$ and $X^2 + X + 1$. Only $X^2 + X + 1$ is irreducible as it does not have a root in $\mathbb{Z}_2$. Then there is $L : \mathbb{Z}_2$ a splitting field extension for $X^2 + X + 1$. Let α be a root of $X^2 + X + 1$ then $L = \mathbb{Z}_1(\alpha)$. Since $L : \mathbb{Z}_2$ is a degree two extension, the number of elements in L is 4. We can write $L = \{0, 1, \alpha, 1+\alpha\}$. One can write down the multiplication table in this case, e.g. $\alpha(1+\alpha) = 1, \alpha^2 = 1 + \alpha, (1+\alpha)^2 = \alpha$ etc.
Note that this extension $\mathbb{Z}_2(\alpha) : \mathbb{Z}_2$ is NOT obtained by *adding* a square root of any element of $\mathbb{Z}_2$.

Example 9. Extension of a monomorphism: Consider the polynomial $X^6 + 1 \in \mathbb{Q}[X]$ for which we know that $L = \mathbb{Q}(\omega, \iota)$ is a splitting field. Consider an intermediate extension $\mathbb{Q}(\iota) : \mathbb{Q}$, which is a splitting field for $X^2 + 1 \in \mathbb{Q}[X]$.

Consider the identity isomorphism $id_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}$. Since the polynomial $X^2 + 1$ has two distinct roots in $\mathbb{Q}(\iota)$, i.e. ι and $-\iota$, the isomorphism $id_{\mathbb{Q}}$ can be extended to $\mathbb{Q}(\iota)$ in exactly two ways, say $i_1, i_2 : \mathbb{Q}(\iota) \to \mathbb{Q}(\iota)$ where $i_1(\iota) = \iota$ and $i_2(\iota) = -\iota$.

Write $i : \mathbb{Q}(\iota) \to \mathbb{Q}(\iota)$ for any of the i_1, i_2 for the moment. Then $\mathbb{Q}(\omega, \iota) : \mathbb{Q}(\iota)$ is a splitting filed extension for $X^2 + X + 1 \in \mathbb{Q}(\iota)[X]$. Note that the polynomial $X^2 + X + 1$ is irreducible and has two distinct roots namely, ω, ω^2. Then the isomorphism i can be extended to $\mathbb{Q}(\omega, \iota)$ in exactly two ways, say $j_1, j_2 : \mathbb{Q}(\omega, \iota) \to \mathbb{Q}(\omega, \iota)$ where $j_1|_{\mathbb{Q}(\iota)} = i = j_2|_{\mathbb{Q}(\iota)}$ with $j_1(\omega) = \omega$ and $j_2(\omega) = \omega^2$.

Thus, there are exactly two automorphism of the field $\mathbb{Q}(\iota)$ and exactly four automorphisms of the field $\mathbb{Q}(\omega, \iota)$ which extend the identity automorphism of $\mathbb{Q}$. See the diagram below.

$$
\begin{tikzcd}
\mathbb{Q}(\omega, \iota) \arrow[r, "\text{four possible } j"] & \mathbb{Q}(\omega, \iota) \\
\mathbb{Q}(\iota) \arrow[u] \arrow[r, "\text{two possible } i"] & \mathbb{Q}(\iota) \arrow[u] \\
\mathbb{Q} \arrow[u] \arrow[r, "id_{\mathbb{Q}}"] & \mathbb{Q} \arrow[u]
\end{tikzcd}
$$