NAP 2019, MODULE-III, LECTURE 7: JUNE 12, 2019

SHIV PRAKASH PATEL & SHREEDEVI MASUTI

In the last lecture we have seen that if $L : K$ is normal and M is an intermediate field, then $M : K$ need not be normal. The following theorem gives a necessary and sufficient conditions for $M : K$ to be normal. We remark that the theorem is true even if $L : K$ is not finite. In the lecture we proved the theorem for finite extensions.

Theorem 1. *Suppose that $L : K$ is a finite normal extension and that M is an intermediate field. Then following are equivalent:*

(a) $M : K$ is normal;
(b) if σ is an automorphism of L which fixes K, then $\sigma(M) \subseteq M$;
(c) if σ is an automorphism of L which fixes K, then $\sigma(M) = M$.

We then started Chapter 10 on Separability. We defined separable extensions and proved few properties of these extensions.

Definition 2. (1) Let $f \in K[X]$ be an irreducible polynomial of degree n. Let $L : K$ be a splitting field extension for f. Then

$$f = \lambda(X - \alpha_1) \cdots (X - \alpha_n)$$

for some $\lambda \in K$ and $\alpha_1, \ldots, \alpha_n \in L$. We say that f is *separable* (over K) if $\alpha_1, \ldots, \alpha_n$ are distinct.
(2) Let $f \in K[X]$ be an arbitrary polynomial. Since $K[X]$ is a UFD, there exist irreducible polynomials $f_1, \ldots, f_k$ and positive integers $n_1, \ldots, n_k$ such that

$$f = u f_1^{n_1} \cdots f_k^{n_k}$$

where u is a unit in $K[X]$. We say that f is *separable* if each f_i is separable. (Note that since $K[X]$ is a UFD, $f_i's$ are unique upto unit and permutation. Hence definition is well-defined).
(3) Let $L : K$ be an extension. An element $\alpha \in L$ is *separable* (over K) if α is algebraic over K and its minimal polynomial over K is separable. An extension $L : K$ is separable if each $\alpha \in L$ is separable.

We discussed some examples and non-examples of separable extensions.

Example 3. (1) Consider the polynomial $f = X^2 - 2$ over $\mathbb{Q}$. Since f has no roots in $\mathbb{Q}$, f is irreducible over $\mathbb{Q}$. Moreover, $f = (X - \sqrt{2})(X + \sqrt{2})$ in $\mathbb{Q}(\sqrt{2})[X]$ and hence its roots are distinct. Thus f is separable over $\mathbb{Q}$.

(2) Consider $f = (X - 1)^2 \in \mathbb{Q}[X]$. Since the irreducible factor $X - 1$ of f is separable, f is separable over $\mathbb{Q}$.

(3) Consider an extension $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$. Then $\sqrt{2}$ is separable over $\mathbb{Q}$ since its minimal polynomial is $X^2 - 2$ and it has distinct roots in $\mathbb{Q}(\sqrt{2})$. Is $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ separable ? For this we need to verify that each $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is separable over $\mathbb{Q}$. If $b = 0$, then α is clearly separable over $\mathbb{Q}$. Assume that $b \neq 0$. In this case the minimal polynomial for α over $\mathbb{Q}$ is $X^2 - 2aX + (a^2 - 2b^2) = (X - \alpha)(X + \beta)$ where $\beta = a - b\sqrt{2}$. Since α and β are distinct, $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ separable over $\mathbb{Q}$.

(4) Consider an extension $\mathbb{Z}_p(t^{1/p}) : \mathbb{Z}_p(t)$ where t is an indeterminate over $\mathbb{Z}_p$. Then $t^{1/p}$ satisfies the polynomial $X^p - t$ over $\mathbb{Z}_p(t)$. In fact, $X^p - t$ is the minimal polynomial for $t^{1/p}$ over

$\mathbb{Z}_p(t)$. But $X^p - t = (X^p - t^{1/p})^p$ in $\mathbb{Z}_p(t^{1/p})[X]$ which has repeated roots. Therefore $t^{1/p}$ is not separable over $Z_p(t)$.

Unlike in the normal case, in the separable case if $L : K$ is separable and M is intermediate field, then both $L : M$ and $M : K$ are separable. We proved this theorem.

Theorem 4. *Suppose that $L : K$ is separable and that M is an intermediate field. Then $L : M$ and $M : K$ are separable.*

Let $L : K$ be a finite extension. We know that the number of automorphisms of L which fixes K is finite. How many such automorphisms of L are possible ? Our goal is to answer this when $L : K$ is normal and separable. As a first step in this direction we proved the following result for simple algebraic extensions.

Theorem 5. *Suppose that $K(\alpha) : K$ is a simple algebraic extension of degree d and $j : K \longrightarrow L$ is a monomorphism. If α is separable over K and $j(m_\alpha)$ splits over L (here m_α is the minimal polynomial for α over K) then there are exactly d monomorphisms from $K(\alpha)$ to L extending j; otherwise there are fewer than d such monomorphisms.*