Lecture 10

Author
Tom Jeong

February 12, 2025

Contents

1 Galois Extension

Theorem 1.1. $[L : K] < \infty$ Let $G = Aut(L, K)$ then $|G| \leq [L : K]$ and the following are equivalent:

1. $|G| = [L : K]$
2. There exists a polynomial $f(x) \in K[x]$ such that L is a splitting field of $f(x)$ and $f(x)$ has distinct roots in L
3. $K = \{x : \sigma(x) = x \forall \sigma \in G\}$

If any 1,2,3 hold then L/K is called a *Galois Extension* $G = Aut(L, K)$ is called the *Galois Group* of L/K

$f(x) = q_1^\alpha(x) \cdots q_m^\alpha(x)$ where q_i are irreducible and distinct in $K[x]$ and $\alpha \geq 1$
$\bar{f}(x) = q_1(x) \cdots q_m(x)$ where q_i are distinct in $L[x]$
It may happen that q_i even if it's irreducible, q_1 has multiple roots in L
A polynomial if $f \in K[x]$ is caled <u>separable</u> if f has distinct roots in its splitting field.
example:
$x^2 + 1$ doesn't have any roots in $\mathbb{Q}$.. where does the roots leave? the smallest field that contains the roots of $x^2 + 1$ is $\mathbb{Q}(i)$; inside this field we will have the roots of $x^2 + 1$

A field K is called <u>perfect</u> if all irreducible polynomials in $K[x]$ are separable.
$\mathbb{Q}-$perfect field

Lemma 1.2.
L is not the union of finitely many proper subfields M, $K \subseteq M \subsetneq L$

Proof.
$K-$infinite $L-$finite dimensional $K-$vector space $dim(L) = [L : K], dim(M) < dim(L)$
a finite dimensional vector space is not a union of finitely many proper subspaces.
$K-$ finite field and $L-$finite field.
$|L| = p^k$
any subfield M of L has $char(p) \rightarrow |M| = p^k$.. $k < n$
For every k there is at most 1 subfield of L of this size. Since any subfield of L of size p^k is the splitting field of $x^{p^k} - x$ over $\mathbb{Z}_p$

$1 + p + p^2 + \cdots + p^{k-1} < p^n$ since $1 + p + \cdots + p^{n-1} = \dfrac{p^n - 1}{p - 1} < p^n$

$\square$

Corollary 1.3.
There exists $z \in L$ such that the $stab(z) = \{\sigma \in G : \sigma(z) = z\} = \{e_G\}$
$\Rightarrow |\{\sigma(z) : \sigma \in G\}| = |G|$

$|G| = n$ and we have that $G = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$
Orbit of z $\sigma_1(z), \sigma_2(z), \cdots, \sigma_n(z)$
We know that these are distinct elements of L

$K \subsetneqq K(z) \subset L$
z has minimal polyonomial f_z

$$[L : K] \geq [K(z) : K] = deg(f_z) \geq n = |G|$$

Proof.
For $\sigma \in G$, $M_\sigma = \{x \in L : \sigma(x) = x\}$
M_σ is a field, $K \subseteq M$
$a, b \in M_\sigma$, $\sigma(a + b) = \sigma(a) + \sigma(b) = a + b$
$\sigma(ab) = \sigma(a)\sigma(b) = ab$
$\sigma(-a) = -\sigma(a)$
For every $\sigma \in G$ we are prohibiting a subfield M_σ since L is not the union of finitely many propert subfields
such z exists. There exists $z \in L \backslash \bigcup_{\sigma \in G | \sigma \neq e} M_\sigma$

□

Proof.

1. (1) $\Rightarrow$ (2)
   by the corollary we estabilished

   $$[L : K] \geq [K(z) : K] = deg(f_z) \geq n = |G|$$

   $deg(f_z) = n \to \sigma_1, \ldots \sigma_n$ are all of the roots of $f_z \to f_z$ has distinct roots in L
   $K(z) = L \to L$ is the splitting field of f_z since f_z splits over L
   and $K(z) = L \to f_z$ does not split over any subfield.

□