

Galois Theory

Robert F. Coleman

Lecture 9

Primitive Element Theorem

Suppose, C/K is algebraically closed. Recall,

Theorem. *If L is a separable extension of K of degree n there exist exactly n distinct K -homomorphisms from L into C .*

Theorem. *Let L be a finite separable element of K . Then there exists $\alpha \in L$ such that $l = K(\alpha)$.*

We'll prove this when K is infinite.

Lemma. *If V is a vector space over K , V is not the union of finitely many proper subspaces.*

Proof. Suppose

$$V = H_1 \cup \cdots \cup H_r.$$

Proof of theorem.

Non-Example.

Splitting Fields

Suppose $P(x)$ is a polynomial over K , L is an extension of K and $\alpha_1, \dots, \alpha_n \in L$ such that $L = K(\alpha_1, \dots, \alpha_n)$ and

$$P(x) = \prod_i (x - \alpha_i).$$

Then L is called a **splitting field** of P over K .

Examples. (i) $f(x) = x^3 + 3x - 2$. Viete says look at $g(E) = E^6 + 2E^3 - 1$ and if α is a root of g , $1/\alpha - \alpha$ is a root of f . The 6 roots of g are (usually) $j^i \alpha$ and $-j^i/\alpha$, $0 \leq i \leq 2$

$$(\alpha^3 + 1)^2 = 2$$

(ii) $K = \mathbf{F}_p(t)$, $P(x) = x^p - t$.

You will prove all splitting fields of P over K are isomorphic.

Lemma. Suppose $P(x) = x^3 + pX + q$ is irreducible, $P'(x) \neq 0$, a is a root of P and $D(P) = -4p^3 - 27q^2$. then the splitting field of $P(x)$ is $K(a, \sqrt{D(P)})$.

Proof. Let b and c be the “other” roots of P . Then,

$$((a - b)(a - c)(c - b))^2 = D(P).$$

$$(a - b)(a - c) = 2a^2 - q/a$$

Read §7.1-7.2.

Homework for Monday

Do exercise 7.1. Prove all splitting fields of $P(x) \in K[x]$ over K are isomorphic.

(Hint: Use results from lecture 8.)