

Lecture 50

Wednesday, April 29, 2015 10:01 AM

Fields & Galois Theory

F a field

$f \in F[x]$ In order to study $F[x]$ roots of polynomials

we might look for a (potentially) larger field $K \supseteq F$ in which f factors into linear terms.

e.g. • $f(x) = x^2 - 1 \in \mathbb{Q}[x] \Rightarrow f(x) = (x+1)(x-1)$.

• $g(x) = x^2 + 1 \in \mathbb{Q}[x]$ but does not factor over \mathbb{Q}

but $g(x) = (x+i)(x-i)$ in $\mathbb{C}[x]$

or over $\mathbb{Q}(i) = \text{Frac}(\mathbb{Z}[i])$.

Main idea of field extensions Given $f \in F[x]$,

\exists a smallest field $K \supseteq F$ such that f has all its roots in K .

Notation/Terminology: $K =$ splitting field of f

$F \subseteq K$ is written K/F and say K is an (algebraic) extension of F .

② Not all ext'ns are algebraic.

E.g. $\mathbb{C}(x)$ = field of ration fns in x over \mathbb{C}

$\mathbb{C}(x)/\mathbb{C}$ is a transcendental extension.

If $p(x) \in F[x]$ is irreducible, then

$K = F[x]/(p(x))$ is a field ($(p(x)) \subseteq F[x]$ is

a max' ideal) and $\bar{x} = x + (p(x))$

is a root of $p(y) \in K[y]$.

$x^2 + 1 \in \mathbb{Q}[x]$ is irreducible

$$\mathbb{Q}[x]/(x^2+1) \cong \mathbb{Q}(i) = \text{Frac}(\mathbb{Z}[i])$$

$$a + b\bar{x} \longleftrightarrow a + bi$$

$$\text{Aut}(K/F) = \left\{ \sigma : K \xrightarrow{\text{field iso}} K \mid \sigma a = a \ \forall a \in F \right\}$$

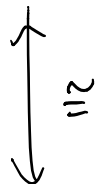
Fact $|\text{Aut}(K/F)| \leq [K:F] = \dim_F K$

$\leq \deg(f)$
for K a splitting field of f .

Def'n K/F is Galois if $|\text{Aut}(K/F)| = [K:F]$.

Thm If K/F is a Galois extension, then

$$\left\{ E \text{ fields } (F \subseteq E \subseteq K) \right\} \quad K^H = \left\{ a \in K \mid \sigma a = a \forall \sigma \in H \right\}$$



$$\left\{ H \leq \text{Aut}(K/F) \right\} \quad \parallel \quad \text{Gal}(K/F)$$



$$\left\{ \sigma \mid \sigma e = e \forall e \in E \right\}$$