Lecture 50

Wednesday, April 29, 2015 10:01 AM

Fields & Galois Theory

F a field

$f \in F[x]$ In order to study ~~F~~ / ~~$F[x]$~~

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 $\mathbb{Q}(i) = \mathrm{Frac}(\mathbb{Z}[i])$.

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.

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

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

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

$K = F[x]/(p(x))$ is a field $\big((p(x)) \subseteq F[x]$ is a max'l ideal$\big)$ and $\bar{x} = x + (p(x))$ is a root of $p(y) \in K[y]$.

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

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

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

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

<u>Fact</u> $|\mathrm{Aut}(K/F)| \le [K:F] := \dim_F K$

$\le \deg(f)$

for K a splitting field of f.

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

Thm If K/F is a Galois extension, then

$$\begin{tikzcd}
\{E \text{ fields} \mid F \subseteq E \subseteq K\} \arrow[d, leftrightarrow, "\cong"] & K^H = \{a \in K \mid \sigma a = a \ \forall \sigma \in H\} & E \arrow[d, mapsto] \\
\{H \le \mathrm{Aut}(K/F)\} & H \arrow[u, mapsto] & \{\sigma \mid \sigma e = e \ \forall e \in E\}
\end{tikzcd}$$

$$\mathrm{Aut}(K/F) = \mathrm{Gal}(K/F)$$