Math 491, Thursday, April 23 Chapter 23

Sage 22 <u>Back</u>

Final Mon AM, May 11 (details later)

Fri Chapter 23

Sun 11:59 PM Written Project

Theorem $\wedge$ E/F $\boxed{E_{\underline{G(E/F)}}} = F$

E splitting field of a seperable polynomial $f(x) \in F[x]$

automorphisms of E, fixing F element-wise

elements of E that are fixed by <u>every</u> automorphism in G

no special hypotheses $\Rightarrow$ $E_{G(E/F)} \supseteq F$

$\uparrow$ EZ proof

Theorem $f(x) \in F[x]$, E splitting field of F, $f(x)$ separable,

then $\underbrace{|G(E/F)|}$ $=$ $\underbrace{[E:F]}$

orders of (small) finite groups

degrees of extensions, dimensions of (infinite) vector spaces

Proof BUSTED

Corollary F finite field, (finite) extension of E, $[E:F]=k$

$\Rightarrow$ $G(E/F)$ is cyclic of order k.

Proof $|E| = p^m$, $|F| = p^n$ ($\Rightarrow$ $n|m$) $k = m/n$

$\sigma: E \to E$ $\sigma(x) = x^{p^n}$ (Frobenius map)

① σ fixes F $\sigma(f) = f^{p^n} = f$

element-wise

f root of $x^{p^n} - x = 0 \Rightarrow f^{p^n} = f$

② $\sigma(e_1+e_2) = (e_1+e_2)^{p^n} \underset{\underset{\text{char}(E)=p}{\uparrow}}{=} e_1^{p^n} + e_2^{p^n} = \sigma(e_1)+\sigma(e_2)$

③ σ has order k

$$\sigma^k(e) = \underbrace{\sigma(\sigma(\cdots\sigma(e)))}_{k \text{ times}} = e$$

④ $|G(E/F)| = k$

$\Rightarrow G(E/F) = \langle \sigma \rangle$

Theorem E finite separable extension of F, then there is a primitive element $a \in E$ so that $E = F(a)$. ← simple extension

Ex

$$\begin{tikzcd} \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[d, dash, "\deg 2"'] \\ \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "\deg 2"'] \\ \mathbb{Q} \end{tikzcd}$$

degree 4

then $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\underset{\underset{\sqrt{2}+\sqrt{3}\,?}{\uparrow}}{\ })$

Proof Constructive / Sage