Extending Automorphisms to Polynomials

F, F' fields, $\sigma : F \to F'$ isomorphism

Define $\sigma_x : F[x] \to F'[x]$,

$$f(x) = a_0 + a_1 x + \dots + a_n x^n \mapsto \sigma_x(f)(x) = \sigma(a_0) + \sigma(a_1) x + \dots + \sigma(a_n) x^n.$$

<u>Lemma</u>: If $\alpha \in F$, $\sigma(f(\alpha)) = \sigma_x(f)(\sigma(\alpha))$

As a consequence, we have an important observation about field extensions and roots:

<u>Prop</u>: Let E be an ext. field of F and suppose σ is an automorphism of E fixing F. Then σ permutes the roots of $f(x) \in F[x]$

<u>Proof</u>: Since $f(x) \in F[x]$, $\sigma_x(f)(x) = f(x)$ and therefore if $\alpha \in E$ is a root of $f(x)$

$$0 = f(\alpha) \Rightarrow 0 = \sigma(f(\alpha)) = \sigma_x(f)(\sigma(\alpha)) = f(\sigma(\alpha))$$

Thus $\sigma(\alpha)$ is a root of $f(x)$. $\square$

<u>Ex</u>: If $f(x) \in \mathbb{Q}[x]$ and $f(a + b\sqrt{2}) = 0$ then $f(a - b\sqrt{2}) = 0$.

<u>Ex</u>: If $f(x) \in \mathbb{R}[x]$ and $f(a + ib) = 0$ then $f(a - ib) = 0$.

Properties of Field Extensions

- finite
- algebraic
- simple
- algebraically closed

THREE NEW ONES

- separable
- splitting field
- normal (aka Galois)

normal = separable + splitting field

Def: A field extension E/F is separable if for every $\alpha \in E$, the polynomial $\operatorname{irr}(\alpha, F)$ has no repeated roots in the algebraic closure $\bar{E}$ of E.

Most fields are separable!

— non-separable fields are weird.

Ex: $\mathbb{Q}(\sqrt[3]{2})$ is a separable ext. of $\mathbb{Q}$ so $x^3 - 2$ has three distinct roots

Ex: $\mathbb{Q}(\sqrt{2})$ is separable and $\sqrt{2}$ is a root of $x^4 - 4x^2 + 4$ but $x^4 - 4x^2 + 4$ has repeated roots, so it must be reducible!

$$x^4 - 4x^2 + 4 = (x^2 - 2)^2.$$

Def: Let $P \subseteq F[x]$. A field ext. K of F is a splitting field for P if

- each $f(x) \in P$ splits into linear factors in $K[x]$

  equiv. all roots of $f(x)$ are in K

- if $F \subseteq E \subsetneq K$ is an intermediate field, some $f(x) \in P$ does <u>NOT</u> split into linear factors in $E[x]$

  equiv. F is smallest field where poly's in P all split into linear factors

Ex: $\mathbb{Q}(\sqrt{2})$ is a splitting field of $P = \{x^2-2\}$
$\mathbb{C}$ is <u>NOT</u> because it is too big!

Ex: $\mathbb{Q}(\sqrt[3]{2})$ is <u>NOT</u> the splitting field of x^3-2

$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\, e^{2\pi i/3}, \sqrt[3]{2} e^{4\pi i/3}) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ is!

<u>Theorem</u>: Splitting fields exist and are given by adjoining all the roots!