- HW due ~~Tonight~~! Wednesday night!
- Exam Mulligan! Saturday @ midnight
- Typo in homework (fixed!)

<u>Today</u>: Study polynomials via their splitting fields and Galois groups

<u>Recall</u>: a <u>splitting field</u> for a polynomial $p(x) \in F[x]$ is a minimal field extension $E \supseteq F$ satisfying

$$p(x) = (x-a_1)(x-a_2)\cdots(x-a_n) \; ; \; a_1, a_2, \dots, a_n \in E.$$

<u>Def</u>: If $p(x) \in F[x]$ and E is a splitting field of $p(x)$, then $G(E/F)$ is called the <u>Galois group of $p(x)$</u>.

<u>Remark</u>: the Galois group is the same (up to iso.) regardless of the choice of splitting field.

<u>Ex</u>: $p(x) = x^2 - 2 \in \mathbb{Q}[x]$
- $\mathbb{Q}[\sqrt{2}]$ is a splitting field
- $\mathbb{Q}[t]/\langle t^2-2\rangle$ is a splitting field

Galois fantastic idea: use the structure of the Galois group of $p(x)$ to study the roots of $p(x)$

When can we write the roots of $p(x)$ as some sort of crazy radicals?

eg. $\sqrt[4]{1 - \sqrt{13 - \frac{1}{\sqrt{2}}}}$

Polynomials w/ roots of this form are

called <u>solvable by radicals</u>.

<u>Theorem</u>: $p(x)$ is solvable by radicals
$\Leftrightarrow$ it's Galois group is <u>solvable</u>.

<u>Def</u>: A finite group G is <u>solvable</u> if it has a chain of normal subgroups

$$\{e\} = H_n \trianglelefteq H_{n-1} \trianglelefteq H_{n-2} \trianglelefteq \cdots \trianglelefteq H_1 \trianglelefteq H_0 = G$$

with H_k / H_{k+1} abelian for all $n > k \geq 0$.

<u>Ex</u>: $S_3 = \{e, (123), (132), (12), (13), (23)\}$

$A_3 = \{e, (123), (132)\}$ normal subgroup

$\left(\ker : \begin{array}{l} S_3 \to \{\pm 1\} \\ \sigma \mapsto \mathrm{sgn}(\sigma) \end{array} \right)$

S_3/A_3 = abelian group!

A_3 = abelian group!

$$\boxed{\{e\} \trianglelefteq A_3 \trianglelefteq S_3}$$

$A_3/\{e\} = A_3$ (abelian) $\qquad S_3/A_3$ = group of order 2 (abelian)

<u>Ex</u>: S_n for $n \geq 5$ is <u>simple</u>. (no nontrivial proper normal subgroups!)

NOT SOLVABLE!

$$\{e\} \trianglelefteq S_5 \qquad \frac{S_5}{\{e\}} = S_5 \text{ not abelian}$$

If we find a polynomial w/ Galois group S_3, we know the polynomial will be solvable by radicals!

Ex: $p(x) = x^3 + 13x^2 + 14x + 27$ has Galois group S_3, so we know it is solvable by radicals!

This kind of seems far-fetched! What's the connection between the Galois group and the roots?

Prop: Let $p(x) = c_n x^n + \dots + c_1 x + c_0 \in F[x]$ and let E be a splitting field for F. Then $\sigma \in G(E/F)$ will permute the roots $a_1, a_2, \dots, a_n \in E$ of $p(x)$.

Proof:

We know $p(a_j) = 0$ for all $1 \leq j \leq n$.

$$\sum_{k=0}^{n} c_k a_j^k = 0 \qquad p \in F[x] \Rightarrow c_0, \dots, c_n \in F$$

$$\sigma\left(\sum_{k=0}^{n} c_k a_j^k\right) = \sigma(0)$$

$$\sum_{k=0}^{n} \sigma(c_k a_j^k) = 0$$

$$\underline{\sigma \in G(E/F)}$$

$$= \{\sigma \in \mathrm{Aut}(E) \mid \sigma(a) = a \ \forall a \in F\}$$

$$\sum_{k=0}^{n} \sigma(c_k)\sigma(a_j^k) = 0$$

$$\sum_{k=0}^{n} \sigma(c_k)\sigma(a_j)^k = 0$$

$$\sum_{k=0}^{n} c_k\left(\sigma(a_j)\right)^k = 0 \qquad p(x) = \sum_{k=0}^{n} c_k x^k$$

$$p(a_j) = 0 \Rightarrow p(\sigma(a_j)) = 0 \qquad \sigma(a_j) = a_{m_j} \text{ for some } m_j.$$

$$\boxed{\sigma : \{a_1, \dots, a_n\} \to \{a_1, \dots, a_n\}} \text{ injective.}$$

Since $\boxed{\sigma : E \to E}$ is an isomorphism, it must be injective

Thus σ is bijective and permutes the roots!

$\square$

Def: Let E be a field extension of F. We define the degree of the extension to be

$[E:F]$ = dimension of E as an F-vector space

Ex: $F = \mathbb{Q}$, $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, then $E = \text{span}_{\mathbb{Q}}\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ and all four are lin. indep. so $[E:F] = 4$

Theorem: Let $p(x) \in F[x]$ be a polynomial with no repeated roots and splitting field E.

Suppose $\phi : F \to L$ is an isomorphism of fields
$\text{id} : F \to F$
and define

$$g(x) = \sum_{k=0}^{n} \phi(a_k) x^k \quad \text{for } p(x) = \sum_{k=0}^{n} a_k x^k$$

and let K be a splitting field of $g(x)$

Then the number of isomorphisms

$$\begin{tikzcd} E \arrow[r, "\cong"] & E \\ F \arrow[u, "\subseteq"] \arrow[r, "="] & F \arrow[u, "\subseteq"'] \end{tikzcd} \qquad \begin{tikzcd} E \arrow[r, "\cong"] & K \\ F \arrow[u] \arrow[r, "\cong", "\varphi"'] & L \arrow[u] \end{tikzcd}$$

making this diagram commute is exactly $[E:F]$.

<u>Corollary</u>: If E is the splitting field of a polynomial w/ no repeated roots

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

<u>Ex</u>: $F = \mathbb{Q}$, $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, $[E:F] = 4$

So we know $|G(E/F)| = 4$.
We actually saw that a while back!

<u>Counting roots and Separability</u>:

We know a polynomial will always have a splitting field E

$p(x) \in F[x]$, $p(x) = (x-a_1)^{r_1}(x-a_2)^{r_2} \cdots (x-a_m)^{r_m}$
for some distinct $a_1, a_2, \ldots, a_m \in E$
and integers r_1, r_2, r_m all greater than 0.

<u>Def</u>: The <u>multiplicity</u> of a root a_j is the value of the exponent r_j. A root is called <u>simple</u> if its multiplicity is 1.

<u>Ex</u>: $p(x) = x^2 + 2x + 1$
-1 is a root w/ multiplicity 2
$q(x) = x^3 - 1$
Then 1, $e^{2\pi i/3}$, $e^{4\pi i/3}$ are all <u>simple roots</u>

<u>Quest</u>: can irreducible polynomials have non-simple roots?

<u>Ans</u>: mostly no. (except over <u>very</u> weird fields)