Last Time:

$F \subseteq E$ field extension

$$\mathrm{Aut}(E) = \{\varphi : E \to E \mid \varphi \text{ iso.}\}$$

$$G(E/F) = \{\varphi \in \mathrm{Aut}(E) \mid \varphi(a) = a \ \forall a \in F\}$$

Picture: $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

$\mathrm{Aut}(\mathbb{Q}[\sqrt{2},\sqrt{3}]) = \{\varphi_0, \varphi_1, \varphi_2, \varphi_3\}$ where

$$\varphi_0 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$
$$\varphi_1 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$
$$\varphi_2 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$$
$$\varphi_3 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

Lattice of Subfields

$$\begin{tikzcd}
 & E = \mathbb{Q}[\sqrt{2},\sqrt{3}] = E_{G_0} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
E_{G_2} = \mathbb{Q}[\sqrt{2}] \arrow[dr, dash] & E_{G_1} = \mathbb{Q}[\sqrt{3}] \arrow[d, dash] & E_{G_3} = \mathbb{Q}[\sqrt{6}] \arrow[dl, dash] \\
 & F = \mathbb{Q} = E_G &
\end{tikzcd}$$

Lattice of Subgroups

$$\begin{tikzcd}
 & G = \{\varphi_0, \varphi_1, \varphi_2, \varphi_3\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
G_1 = \{\varphi_0, \varphi_1\} \arrow[dr, dash] & G_2 = \{\varphi_0, \varphi_2\} \arrow[d, dash] & G_3 = \{\varphi_0, \varphi_3\} \arrow[dl, dash] \\
 & G_0 = \{\varphi_0\} &
\end{tikzcd}$$

Relationship between subfields and subgroups!

Def: $F \subseteq E$ field extension, $S \subseteq G(E/F)$.
The <u>invariant subfield</u> E_S is
$$E_S = \{a \in E \mid \varphi(a) = a \ \forall \varphi \in S\}$$

Motivation: algebra studies algebraic equations, like polynomial equations

Goal: study / find solutions of polynomial equations

$$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = 0$$

algebraically.

A super successful particular case: quadratic formula!

$$ax^2 + bx + c = 0 \quad , \quad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a} = 0$$

$$a\left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a} - c$$

$$\sqrt{\left(x + \frac{b}{2a}\right)^2} = \sqrt{\frac{b^2 - 4ac}{4a^2}} \Rightarrow x + \frac{b}{2a} = \frac{\pm\sqrt{b^2 - 4ac}}{2a}$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad \checkmark$$

Ex: $ax^3 + bx^2 + cx + d$ $\leftarrow$ approach to solving this equation algebraically

Splitting Fields:

S'pose we want to find a root of a polynomial $p(x)$ with coefficients in $\mathbb{Q}$.

Idea: instead of searching $\mathbb{C}$, find roots in some smaller field extension of $\mathbb{Q}$.

Def: An <u>algebraic closure</u> of a field F is a field $\overline{F}$ satisfying the property that every $p(x) \in F[x]$ has a root in $\overline{F}$, and it is minimal among field extensions with this property.

Ex: $\overline{\mathbb{Q}} = \{ z \in \mathbb{C} \mid z \text{ is algebraic over } \mathbb{Q} \}$

Note: $\mathbb{C}$ is uncountable, $\overline{\mathbb{Q}}$ is countable
$\overline{\mathbb{Q}}$ is still a huge field extension of $\mathbb{Q}$.

If I am interested in just a finite set $P = \{ f_1(x), \ldots, f_r(x) \} \subseteq \mathbb{Q}[x]$ we can use a much smaller field extension of $\mathbb{Q}$ called the splitting field!

Def: Let F be a field, $P = \{ f_1(x), \ldots, f_r(x) \} \subseteq F[x]$.
A <u>splitting field</u> for P is a field extension $F \subseteq E$ where each $f_j(x)$ factors as a product of linear factors in $E[x]$, and where E is minimal among field extensions with this property.

Ex: $x^2+1 \in \mathbb{Q}[x]$, $\underline{E = \mathbb{Q}[i]}$

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

$\underbrace{(x+i)}_{\in E[x]}\underbrace{(x-i)}_{\in E[x]}$ in $E[x]$

$E = \mathbb{Q}[i]$

$E[x] = \mathbb{Q}[i][x]$
$= \mathbb{Q}[i, x]$

E is minimal $\therefore$ E is a splitting field for x^2+1.

Ex: $K = \mathbb{Q}[y] / \langle y^2+1 \rangle$ $\longleftarrow$ this IS a field!

$y^2+1=0$
$-y^2 = 1$

$x^2+xy-xy-y^2 = x^2-y^2$
$= x^2+1$

$x^2+1 = (x+y)(x-y) \in K[x]$

Another splitting field for x^2+1

$\underline{Ex}$: $\zeta_6 = \cos(\frac{\pi}{3}) + i\sin(\frac{\pi}{3})$

$\zeta_6 = \frac{1}{2} + \frac{i\sqrt{3}}{2}$

$x^3 - 1 \in \mathbb{Q}[x]$

x^3-1 factors as a product of linear factors in $E[x]$ for $E = \mathbb{Q}[\zeta_6]$.

$$(x^3-1) = \underbrace{(x-\zeta_6^2)}_{\in E[x]}\underbrace{(x-\zeta_6^4)}_{\in E[x]}\underbrace{(x-1)}_{\in E[x]}$$

Q: is E the splitting field of $\{x^3-1\}$?

A: $\underline{\text{Yes}}$!

$E = \mathbb{Q}[e^{\pi i/12}] \leftarrow$ x^3-1 splits here

$\cup\!\!\!\!\!\!\not\;$

$\boxed{\mathbb{Q}[\zeta_6]}$

$\mathbb{Q}[\zeta_6] = \mathbb{Q}[\zeta_3]$

$x^6 - 1$

$= (x^3-1)(x^3+1)$

$\underline{Ex}$: $x^4 - 5x^2 + 6 = (x^2-2)(x^2-3)$

has splitting field $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

$(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$

$\underline{\text{Theorem}}$: Let F be a field and $P = \{f_1(x), \dots, f_r(x)\} \subseteq F[x]$
Then there exists a field extension $E \supseteq F$ which is a splitting field for P.

<u>Proof</u>: Consider the algebraic closure $\overline{F}$ of F.

Take $\Lambda = \{\alpha \in \overline{F} \mid \alpha \text{ is a root of } f_j(x) \text{ for some } j\} \subseteq \overline{F}$

$\Lambda = \{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m\}$

Set $E = F[\Lambda] = F[\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m]$.

Because we have all the roots, any $f_j(x)$ will factor as $f_j(x) = (x - \alpha_{k_1})(x - \alpha_{k_2}) \cdots (x - \alpha_{k_r})$

so f_j splits $/ E$.

IF $E' \subseteq E$ where all the f_j's split $/ E'$, then E' contains all the roots of the f_j's

$\Rightarrow E' \supseteq F[\alpha_1, \ldots, \alpha_m] = E \quad \Rightarrow E' = E$. $\square$