Last time:

$E/F$ $\qquad Gal(E/F) : Aut_F(E)$ - automorphisms that are identity on $F$: Galois group.

Thm $\quad |Gal(E/F)| \leq [E:F]$.

Notion of splitting field.

Under an automorphism $\sigma : E \to E$ that fixes elements of $F$, roots go to roots.

Irreducible $f(x) \in F[x]$ is called separable if it does not have multiple roots in any extension $E/F$.

$f(x) \in F[x]$ is called separable if each irreducible factor of $f$ is separable

$f(x) = f_1(x) \ldots f_r(x)$ ← repeat factors ok, each separable

Inseparable (not separable) polynomials are possible only if char $F = p$, $F$ is infinite, and not all el's of $F$ have $p$-th roots in $F$. $\quad x^p - t$, $\sqrt[p]{t} \notin F$.

$$
\begin{tikzcd}
E \arrow[r, "\sigma"] \arrow[d, dash] & E \arrow[d, dash] \\
F(\alpha) \arrow[r] \arrow[dr, dash] & F(\sigma(\alpha)) \arrow[d, dash] \\
 & F
\end{tikzcd}
$$

$irr(\alpha, F) = irr(\sigma(\alpha), F)$

<u>Thm</u> (Rotman, Thm 51, p.56) Let $\sigma: F \to F'$ be an isomorphism of fields. $f(x) \in F[x]$ and $f^*(x) = \sigma(f(x)) \in F'[x]$ the corresponding polynomial $/F'$.

Let $E/F$ be a splitting field of $f$ in $F$,
$E'/F'$ be a splitting field of $f^*$ in $F'$.

$$\begin{tikzcd} E \arrow[d, dash] & E' \arrow[d, dash] \\ F \arrow[r, "\sigma"'] & F' \end{tikzcd}$$

1) there exists an isomorphism $\tilde{\sigma}: E \to E'$ extending $\sigma$.
2) if $f(x)$ is separable, then $\sigma$ has exactly $[E:F]$ extensions

<u>Proof</u> 1) Induction on $[E:F]$

Note that for intermediate field $F \subset B \subset E$, $E$ is a splitting field of $f$ over $B$.

<u>Induction base</u>: $[E:F]=1$ Nothing to prove $E=F$, $E'=F'$, one $\sigma$.

Otherwise choose irreducible factor $p(x)$ of $f(x)$, $\deg p(x) \geq 2$

$f(x), p(x) \in F[x] \to f^*(x), p^*(x) \in F'[x]$

$\alpha \in E$ root of $p(x)$ in $E$ replace coefficients using isomorphism $\sigma$.
$\exists\, \alpha' \in E'$ root of $p^*(x)$

$$\begin{tikzcd} E \arrow[d, dash] & E' \arrow[d, dash] \\ F[\alpha] \arrow[d, dash] \arrow[r, "\hat{\sigma}"] & F'[\alpha'] \arrow[d, dash, "m"] \\ F \arrow[r, "\sigma"'] & F' \end{tikzcd}$$

intermediate field $F[\alpha]$

$m = \deg p = \deg p^*$

fix $\alpha$: $m$ choices for $\alpha'$ if $p(x)$ $(= p^*(x))$ is separable (always so in char 0).

$\Rightarrow$ $m$ choices for $\hat{\sigma}$, one for each root $\alpha'$ of $p^*(x)$ in $E'$

<u>$\#$roots $= \deg p(x)$ iff $p$ is separable.</u>

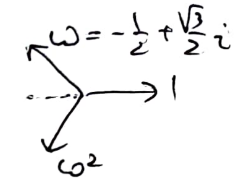
Now apply induction hypothesis to $E/F[\alpha]$ and $E'/F'[\alpha']$

Examples:

1) $x^3-2 \in \mathbb{Q}[x]$ $\quad B = \mathbb{Q}[\alpha]/(\alpha^3-2)$ $\quad [B:\mathbb{Q}]=3$ basis $1, \alpha, \alpha^2$

$\mathrm{Aut}_{\mathbb{Q}}(B) = 1$ only trivial automorphism. Other roots of $x^3-2$ are not in $B$.

$x^3-2$ 3 roots in $\mathbb{C}$. $\sqrt[3]{2} \in \mathbb{R}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$ $\quad \omega = e^{2\pi i/3}$




$\Rightarrow$ 3 homomorphisms

$$\begin{tikzcd} B \arrow[rr, "\sigma"] & & \mathbb{C} \\ & \mathbb{Q} \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \qquad \alpha \mapsto \sqrt[3]{2},\ \omega\sqrt[3]{2},\ \omega^2\sqrt[3]{2}$$

($\sigma$ not autom.)

$E = \mathbb{Q}[\sqrt[3]{2}, \omega\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2}, \omega]$ splitting field

$$x^3-2 = (x-\sqrt[3]{2})\underbrace{(x^2+\sqrt[3]{2}\,x+\sqrt[3]{4})}_{=(x-\omega\sqrt[3]{2})(x-\omega^2\sqrt[3]{2})}$$

irreducible $/\mathbb{Q}(\sqrt[3]{2}]$

factors in $E$

$$\begin{tikzcd} E = \mathbb{Q}[\sqrt[3]{2}, \omega] \subset \mathbb{C} \arrow[d, dash, "2"'] \\ \mathbb{Q}[\sqrt[3]{2}] \simeq B \arrow[d, dash, "3"'] \\ \mathbb{Q} \end{tikzcd}$$

add $\omega$, $\omega^2+\omega+1$ $\quad \mathrm{irr}(\omega, \mathbb{Q}[\sqrt[3]{2}]) = \mathrm{irr}(\omega, \mathbb{Q})$

$E$ - splitting field, $x^3-2$ separable (char 0)

$$\Rightarrow |\mathrm{Gal}(E/\mathbb{Q})| = [E:\mathbb{Q}] = [E:\mathbb{Q}[\sqrt[3]{2}]][\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}] = 2\cdot 3 = 6$$

$\mathrm{Gal}(E/\mathbb{Q})$ has order 6. Permutes roots of $x^3-2$ $\Rightarrow$ $\mathrm{Gal}(E/\mathbb{Q}) \simeq S_3$.

Note that some symmetries take real numbers to complex numbers that are not real. Here we are discussing symmetries defined on the subfield $E$ of $\mathbb{C}$, not on the entire $\mathbb{C}$.

2) Let $E/F$, $[E:F]=2$. Take $\alpha \in E \setminus F$. Then $\{1, \alpha\}$ is a basis of $E$ as $F$-vect. space $\Rightarrow \alpha^2 + b\alpha + c = 0$ some $b, c \in F$.
$\Rightarrow \alpha$ is a root of $f(x) = x^2 + bx + c \in F[x]$

If char $F \neq 2$, can use familiar method to understand $F$.

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

let $\mathcal{D} = b^2 - 4c \in F$ Discriminant of $f$.

need 2 to be invertible in $F$

$$= \frac{1}{4}\left((2x+b)^2 - \mathcal{D}\right) = \frac{1}{4}\left(y^2 - \mathcal{D}\right)$$

let $y = 2x + b$ linear change of variables
$x = \frac{1}{2}(y - b)$.

<u>Exercise</u>: $\underset{\underset{E}{\cong}}{F[x]/(x^2 + bx + c)} \cong F[y]/(y^2 - \mathcal{D})$ char $F \neq 2$

In char $\neq 2$, a quadratic extension reduces to $F[y]/(y^2 - \mathcal{D})$
$\mathcal{D}$ not a square in $F$.

$$E \cong F[y]/(y^2 - \mathcal{D}) \cong F[\beta]/(\beta^2 - \mathcal{D})$$

$x^2 - \mathcal{D} = (x - \beta)(x + \beta)$

$\{\beta, -\beta\}$ roots of $x^2 - \mathcal{D}$ in $E$.

$\mathrm{Gal}(E/F) \cong C_2 \quad \beta \longleftrightarrow -\beta$

identity, and permutation $\beta \mapsto -\beta$
$a + b\sqrt{\mathcal{D}} \xrightarrow{\sigma} a - b\sqrt{\mathcal{D}}$
The only nontrivial Galois symmetry

$x^2 + bx + c \quad \sqrt{\mathcal{D}} \notin F \Rightarrow$ irreducible separable polynomial

$|C_2| = 2 = [E:F]$

Case $F = \mathbb{Q}$. $\mathcal{D} = \frac{n}{m} \quad \sqrt{\frac{n}{m}} = \frac{1}{m}\sqrt{\underset{\smile}{nm}}$ integer $\quad \sqrt{k^2 n} = k\sqrt{n}$

$\Rightarrow$ Can reduce to $n = \pm p_1 \dots p_r$ product of distinct primes

Exercise Degree 2 extensions $E/\mathbb{Q}$ are classified by

$n = \pm p_1 \dots p_r$ a finite set of prime numbers

$E \simeq \mathbb{Q}[x]/(x^2-n)$ splitting field of $x^2-n$ $x^2-2, x^2-3, x^2-5, x^2-6, \dots$

$E \simeq \mathbb{Q}[x]/(x^2+n)$ — " — $x^2+n$

Note each such $E$ is isomorphic to a subfield of $\mathbb{C}$.

There are 2 field homomorphisms

$E = \mathbb{Q}[\alpha]/(\alpha^2-n)$ $E \to \mathbb{C}$ $\mathbb{Q} \to \mathbb{C}$ only 1 homomorphism

$\alpha \mapsto \sqrt{n} \in \mathbb{R}_+$

$\alpha \mapsto -\sqrt{n} \in \mathbb{R}_-$

$\mathrm{Gal}(E/\mathbb{Q}) \simeq C_2$ id, $\alpha \mapsto -\alpha$

---

Finite field $E/\mathbb{F}_p$ $[E:\mathbb{F}_p]=n$ splitting field of $x^q - x = x^{p^n}-x$

$\sigma = \sigma_p : a \mapsto a^p$ Frobenius automorphism $\sigma_p = \mathrm{id}$ on $\mathbb{F}_p$, not id on larger field

Order of $\sigma$? $\sigma^n(a) = a^{p^n} = a \quad \forall a \in E$

$\sigma(a) = a^p$

$\sigma^2(a) = (a^p)^p = a^{p^2}$

$\sigma^3(a) = (a^{p^2})^p = a^{p^3}$

$\sigma^n(a) = a^{p^n} = a$

$\sigma^n = 1$. Smaller $\sigma^m(a) = a^{p^m}$ if $m<n$

$x^{p^m} = x$ has at most $p^m$ solutions in $E$.

$\Rightarrow |\sigma| = n$. $\{1, \sigma, \sigma^2, \dots \sigma^{n-1}\}$ all el's of $\mathrm{Gal}(E/\mathbb{F}_p)$

Thm $\mathrm{Gal}(E/\mathbb{F}_p)$ for $|E| = p^n$ is a cyclic group of order $n$ generated by the Frobenius automorphism.

$\alpha^4 = \alpha(\alpha+1) = \alpha^2+\alpha$

$\mathrm{Gal}(\mathbb{F}_4/\mathbb{F}_2) = \langle 1, \sigma \rangle \simeq C_2$

$\sigma(\alpha) = \alpha+1$

$\mathrm{Gal}(\mathbb{F}_8/\mathbb{F}_2) \simeq C_3$

$\alpha^3+\alpha+1$ $x^3+x+1 = (x+\alpha)(x+\alpha^2)(x+\alpha^4)$

$\alpha \xrightarrow{\sigma} \alpha^2 \xrightarrow{\sigma} \alpha^4$, $\alpha^4 \xrightarrow{\sigma} \alpha$ roots of the same irrep

$\beta = \alpha+1 \xrightarrow{\sigma} (\alpha+1)^2 \xrightarrow{\sigma} (\alpha+1)^4$

$\alpha+1 \to \alpha^2+1 \to \alpha^2+\alpha+1$