Last time we stated this:

Thm. Let E be a finite extension of a finite field F of order p^r, s.t. $[E:F]=n$.
Then $G(E/F)$ is cyclic and generated by the Frobenius automorphism
$$\sigma_{p^r}(\alpha) = \alpha^{p^r}.$$
i.e. $G(E/F) \cong \mathbb{Z}_n$

Proof: Note: $\sigma_{p^r}(\alpha) = \alpha^{p^r}$ fixes elements of $E \iff \alpha$ is a root of $x^{p^r} - x$.
$\iff \alpha \in F$.

Thus, the Frobenius automorphism σ_{p^r} is an automorphism of E that fixes $F \Rightarrow \sigma_{p^r} \in G(E/F)$.

Next, observe $(\sigma_{p^r})^i$ is also an automorphism,

and $$(\sigma_{p^r})^i(\alpha) = \Big(\overbrace{\big(\alpha^{p^r}\big)^{p^r}\cdots}^{i}\Big) = \alpha^{p^{ri}}.$$

What is the order of σ_{p^r} in $G(E/F)$?

Sp. $(\sigma_{p^r})^i = \text{identity} \Rightarrow \alpha^{p^{ri}} = \alpha \quad \forall \alpha \in E.$

Notice: $x^{p^{ri}} - x$ has exactly p^{ri} roots, so $(\sigma_{p^r})^i$ can fix at most p^{ri} elements in K. But since $(\sigma_{p^r})^i = \text{identity}$, smallest $i = n$, because $|E| = p^{rn}$. Also, $\sigma_{p^{rn}}$ fixes all of E.

$\therefore$ order of σ_{p^r} is n. Since $|G(E/F)| = n$,
$$G(E/F) = \{e, \sigma_{p^r}, \sigma_{p^{2r}}, \dots, \sigma_{p^{(n-1)r}}\} \cong \mathbb{Z}_n.$$

Example: Calculate the Galois group of the splitting field of x^4+1 over $\mathbb{Q}$, and calculate the subgroups and corresponding subfields.

Complex:

The roots of x^4+1 are $\alpha = e^{i\pi/4}, \alpha^3, \alpha^5, \alpha^7$,

so splitting field is $\mathbb{Q}(\underset{\alpha}{e^{i\pi/4}}) = E \Rightarrow \deg [E:F] = 4$.

Every element of $G(E/\mathbb{Q})$ must map $\mathbb{Q} \xrightarrow{id} \mathbb{Q}$, $\alpha \mapsto \begin{cases} \alpha \\ \alpha^3 \\ \alpha^5 \\ \alpha^7 \end{cases}$:

$\alpha^4 = -1$

$\alpha^8 = 1$

automorphism are determined by their action on α.

Let $\phi_0 =$ identity, $\phi_3(\alpha) = \alpha^3$

ϕ_3 has order 2, is $(1,2)(3,4)$ as a permutation.

perm	root	ϕ_3(root)
1	α	α^3
2	α^3	$\alpha^9 = \alpha$
3	α^5	$\alpha^{15} = \alpha^7$
4	α^7	α^5

$\phi_5(\alpha) = \alpha^5$

ϕ_5 has order 2 $(1,3)(2,4)$

root	ϕ_5(root)
α	α^5
α^3	$\alpha^{15} = \alpha^7$
α^5	$\alpha^{25} = \alpha$
α^7	α^3

$\phi_3\phi_5 = (1,2)(3,4)(1,3)(2,4)$
$= (1,4)(2,3)$
$= \phi_7$

$\phi_7(\alpha) = \alpha^7$

$(1,4)(2,3)$ order 2.

root	ϕ_7(root)
α	α^7
α^3	$\alpha^{21} = \alpha^5$
α^5	$\alpha^{35} = \alpha^3$
α^7	α

$\therefore G(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, with $\phi_3 \leftrightarrow (1,0)$

$\phi_5 \leftrightarrow (0,1)$

$\phi_7 \leftrightarrow (1,1)$.

$e^{i\pi/4} = \frac{1+i}{\sqrt{2}} = \alpha$

$e^{3i\pi/4} = \frac{-1+i}{\sqrt{2}} = \alpha^3$

$e^{5\pi i/4} = \frac{-1-i}{\sqrt{2}} = \alpha^5$

$e^{7\pi i/4} = \frac{+1-i}{\sqrt{2}} = \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i = \alpha^7$

Subgroups: $\{e, \phi_3\}$, $\{e, \phi_5\}$, $\{e, \phi_7\}$

$\sqrt{2} = \alpha + \alpha^7 \qquad i\sqrt{2} = \alpha^3 + \alpha^5$

$i = \alpha^2$

$E = \mathbb{Q}(\sqrt{2}, i)$

$E = \{c_0 + c_1\sqrt{2} + c_2 i + c_3 i\sqrt{2} : c_j \in \mathbb{Q}\ \forall j\}$

Fixed fields: of $\{e, \phi_3\}$

$\phi_3(c_0 + c_1 \overset{\alpha+\alpha^7}{\sqrt{2}} + c_2 i + c_3 i\sqrt{2}) = (c_0 + c_1\sqrt{2} + c_2 i + c_3 i\sqrt{2})$

$\alpha^6 =$

$c_0 + c_1\underbrace{(\overset{\phi_3(\alpha)}{\alpha^3} + \overset{\phi_3(\alpha^7)}{\alpha^5})}_{-\sqrt{2}} + c_2(-i) + c_3(-i)\underbrace{(\alpha^3 + \alpha^5)}_{-\sqrt{2}}$

$\Rightarrow \phi_3(\omega) = c_0 - c_1\sqrt{2} - c_2 i + c_3 i\sqrt{2}$

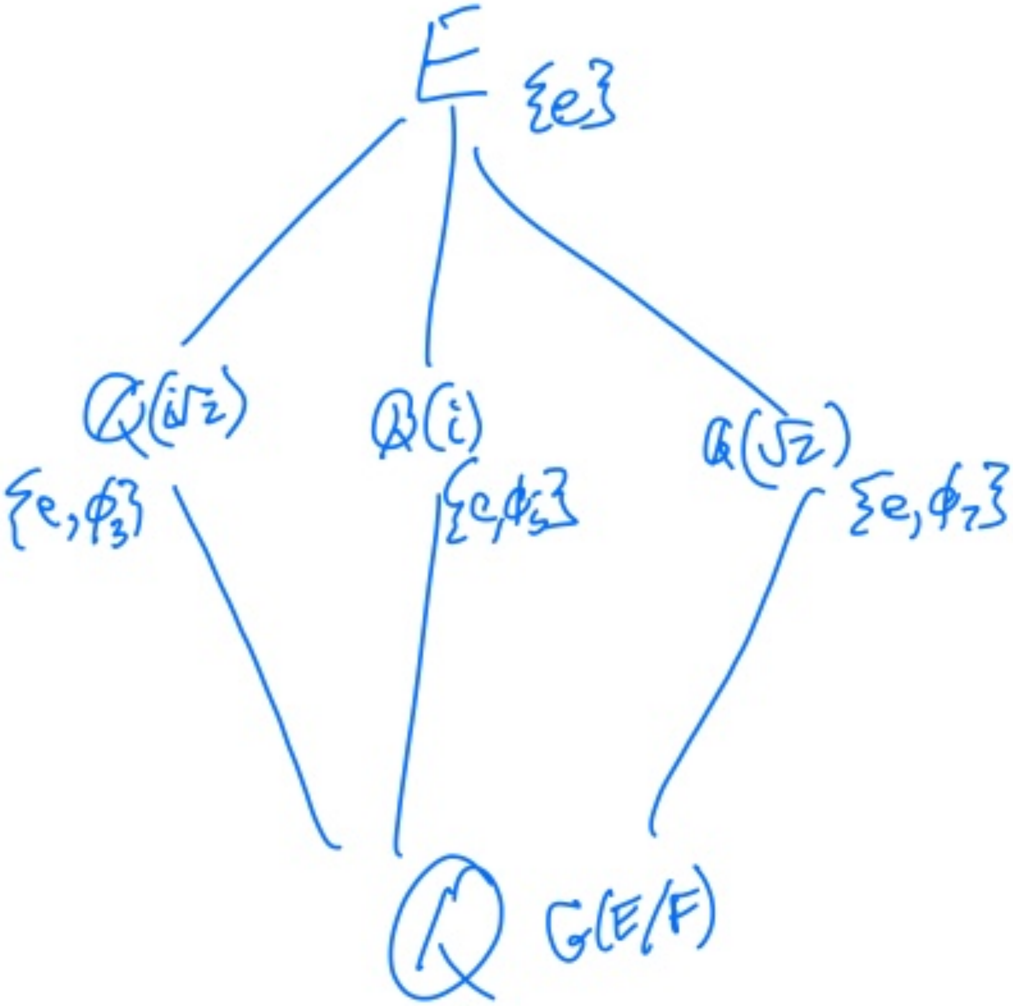
$E_{\{e,\phi_3\}} = \{c_0 + c_3 i\sqrt{2} : c_0, c_3 \in \mathbb{Q}\} = \mathbb{Q}(i\sqrt{2})$

$\phi_5(c_0 + c_1 \overset{\alpha+\alpha^7}{\sqrt{2}} + c_2 \overset{\alpha^2}{i} + c_3 i\sqrt{2})$

$(c_0 + c_1(\alpha^5 + \alpha^3) + c_2 i + c_3 i(\alpha^5 + \alpha^3))$

$= (c_0 - c_1\sqrt{2} + c_2 i - c_3 i\sqrt{2}) = (c_0 + c_1\sqrt{2} + c_2 i + c_3 i\sqrt{2})$

$\Rightarrow E_{\{e,\phi_5\}} = \mathbb{Q}(i).$


E
$\{e\}$
$\mathbb{Q}(i\sqrt{2})$
$\{e, \phi_3\}$
$\mathbb{Q}(i)$
$\{e, \phi_5\}$
$\mathbb{Q}(\sqrt{2})$
$\{e, \phi_7\}$
$\mathbb{Q}$
$G(E/F)$