MATH 5020

$G_{\mathbb{Q}}$

# GALOIS REPRESENTATIONS

LECTURE 3

SPRING 2022

INSTRUCTOR: ÁLVARO LOZANO-ROBLEDO
MONT 233
ALOZANO.CLAS.UCONN.EDU/MATH5020S22
ALVARO.LOZANO-ROBLEDO@UCONN.EDU

# Review of finite! Galois Theory (Part 2)

**Def** Let $K/F$ be a finite field extension. Then, $K$ is said to be Galois over $F$ and $K/F$ is a Galois extension if
$$\# \mathrm{Aut}(K/F) = [K:F].$$
In this case, $\mathrm{Gal}(K/F) := \mathrm{Aut}(K/F)$.

**Cor** If $K$ is the splitting field over $F$ of a sep. polynomial $f(x)$ then $K/F$ is Galois.

**ex**

$\mathbb{Q}(\zeta_8)/\mathbb{Q}$ $\qquad \zeta_8 = e^{2\pi i/8} = e^{\pi i/4} = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}$

$$= \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} = \frac{\sqrt{2}}{2}(1+i)$$

$$\mathbb{Q}(i) = \mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$$

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong \underbrace{\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})}_{\langle\tau\rangle} \times \underbrace{\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})}_{\langle\sigma\rangle} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\begin{tikzcd}
 & \{id\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\tau\rangle \arrow[dr, dash] & \langle\sigma\rangle \arrow[d, dash] & \langle\tau\sigma\rangle \arrow[dl, dash] \\
 & \langle\tau\rangle \times \langle\sigma\rangle &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(i,\sqrt{2}) \arrow[dl, dash, "\langle\tau\rangle"'] \arrow[d, dash, "\langle\sigma\rangle"] \arrow[dr, dash, "\langle\tau\sigma\rangle"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(i) \arrow[d, dash] & \mathbb{Q}(\sqrt{-2}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

# Thm (Fundamental Theorem of Galois Theory)

Let $k/F$ be a finite Galois ext'n, w/ $G = \mathrm{Gal}(k/F)$. Then:

$$\begin{tikzcd} k \arrow[d, dash, "H", "\#H"'] \\ E \arrow[d, dash, "\#G/H"'] \\ F \arrow[uu, bend right, dash, "G"'] \end{tikzcd}$$

$$\left\{ \begin{array}{c} \text{subfields} \\ F \subseteq E \subseteq k \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgps} \\ H \leq G \end{array} \right\}$$

$$E \longmapsto \mathrm{Gal}(k/E)$$

$$k^H \longleftarrow\!\shortmid\; H$$

Moreover:

(1) If $F \subseteq E_1 \subseteq E_2 \subseteq K$ then $\{Id\} \subseteq H_2 \subseteq H_1 \subseteq G$. (where $E_i = k^{H_i}$)

(2) $[k:E] = |H|$, $[E:F] = |G/H|$

(3) $k/E$ is Galois, $\mathrm{Gal}(k/E) = H$.

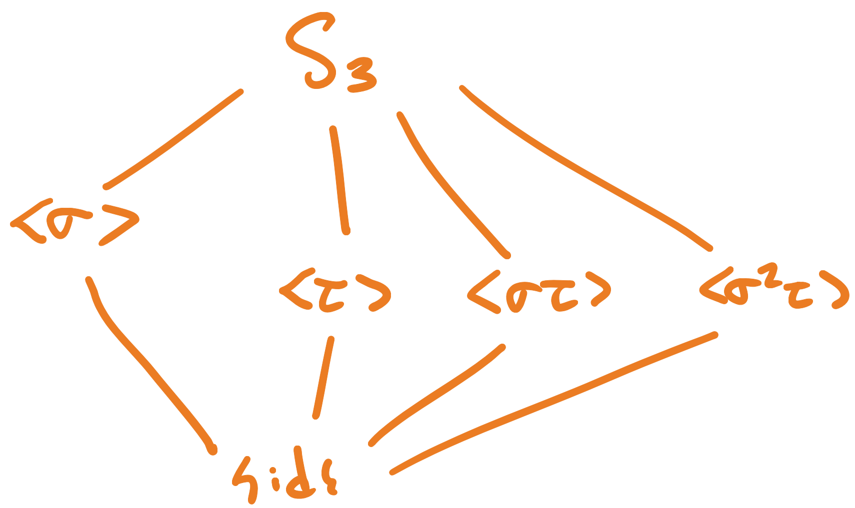
(4) $E/F$ is Galois iff $H \trianglelefteq G$ (if so, $\mathrm{Gal}(E/F) \cong G/H$)

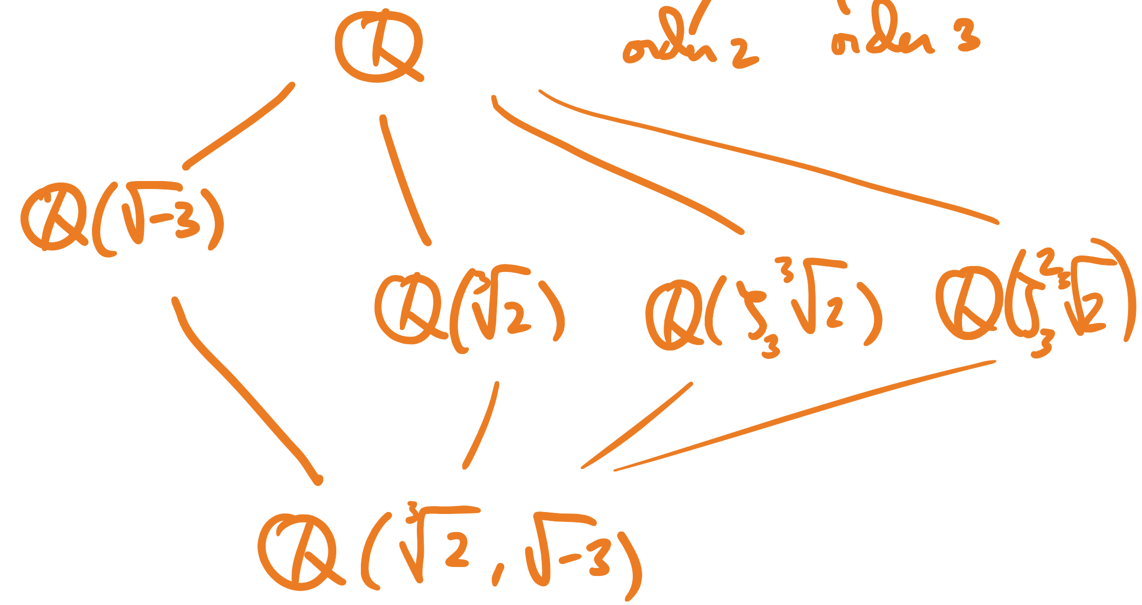
(5) $E_i = k^{H_i}$ then $E_1 \cap E_2 = K^{\langle H_1, H_2 \rangle}$

$E_1 E_2 = K^{H_1 \cap H_2}$

(lattices of subfields and subgps are dual)

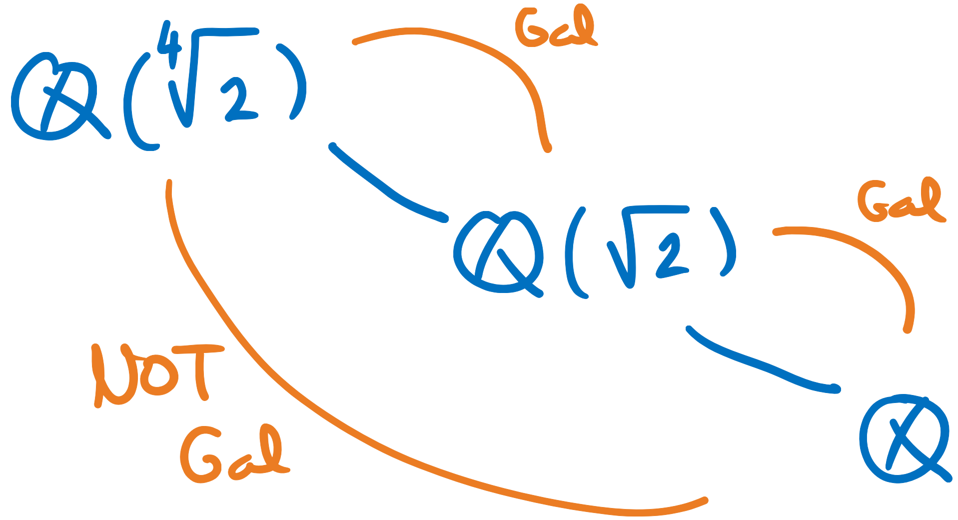
**ex** $\mathrm{Splt}(x^3-2) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) =: k$, $\mathrm{Gal}(k/\mathbb{Q}) \cong S_3 \cong \langle \underset{\text{order } 2}{\tau}, \underset{\text{order } 3}{\sigma} \rangle$




**WARNING**: A Galois ext'n of a Galois ext'n is <u>not</u> nec. Galois.

**ex**




What is $\mathrm{Gal}(\mathrm{Splt}(\sqrt[4]{2})/\mathbb{Q})$

$$\| $$

$\mathrm{Splt}(x^4-2)$

## §. Finite Fields

Let $p$ be a prime, let $q = p^n$, for some $n \geq 1$, and let $\mathbb{F}$ be a finite field of char $p$.

**Def** The Frobenius map is $\phi : \mathbb{F} \longrightarrow \mathbb{F}$
$$k \longmapsto k^p$$

**Prop** $\phi$ is 1) a field hom.
2) injective
3) surjective

In particular, any $f \in \mathbb{F}$ is a $p$th power.

**Thm** Let $n \geq 1$ and $f(x) = x^{p^n} - x \;/ \mathbb{F}_p$.

- $f(x)$ is separable
- $\mathrm{Split}(f(x)) =: \mathbb{F}_{p^n}$ is a field of size $p^n$ of char $p$.
- $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$.
- If $\mathbb{F}/\mathbb{F}_p$ is a finite extension of degree $n$ then $\mathbb{F} \cong \mathbb{F}_{p^n}$.
- $\mathbb{F}_{p^n}/\mathbb{F}$ is Galois w/ $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$,
- $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi \rangle$ where $\phi$ is the Frob. auto. of $\mathbb{F}_{p^n}$.
- If $\gcd(m,n) = 1$, then $\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_p$.

ex

$$\begin{tikzcd}
 & \mathbb{F}_{p^{nm}} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{F}_{p^n} \arrow[dr, dash] & & \mathbb{F}_{p^m} \arrow[dl, dash] \\
 & \mathbb{F}_p &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \{id\} \arrow[dl, dash] \arrow[dr, dash] & \\
n\mathbb{Z}/nm\mathbb{Z} \arrow[dr, dash] & & m\mathbb{Z}/nm\mathbb{Z} \arrow[dl, dash] \\
 & \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} &
\end{tikzcd}$$

- If $m \mid n$ then $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, there is a map

$$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \longrightarrow \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p)$$

corresponding to $\qquad \sigma \longmapsto \sigma|_{\mathbb{F}_{p^m}} \qquad$ (restriction)

corresponding to

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

$$a \bmod n \longmapsto a \bmod m$$

ex

$$\begin{tikzcd}
\mathbb{F}_{p^4} \arrow[d, dash, "2\mathbb{Z}/4\mathbb{Z}"] \arrow[dd, bend left, dash, "\mathbb{Z}/4\mathbb{Z}"] \\
\mathbb{F}_{p^2} \arrow[d, dash, "\cong \mathbb{Z}/2\mathbb{Z}"] \\
\mathbb{F}_p
\end{tikzcd}$$

$$\frac{\mathbb{Z}/\cancel{4\mathbb{Z}}}{2\mathbb{Z}/\cancel{4\mathbb{Z}}} \cong \mathbb{Z}/2\mathbb{Z}$$

**Cor.**

- $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$

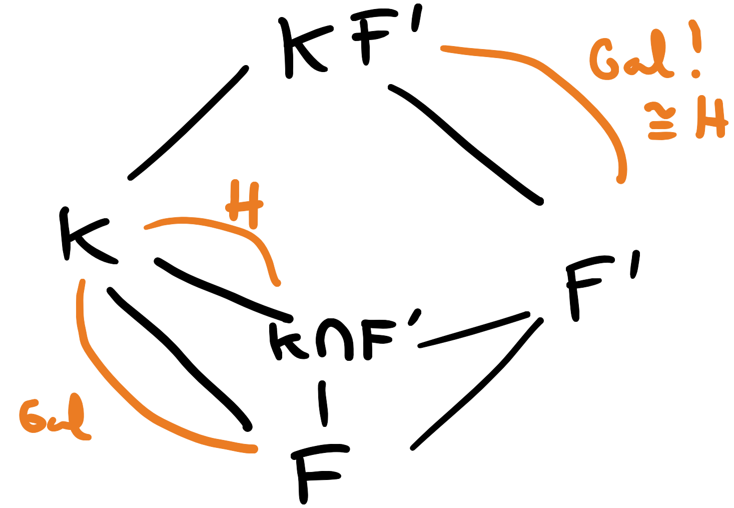
- For every $n \geq 1$, there is a <u>unique</u> extension $\mathbb{F}_p \subseteq F \subseteq \overline{\mathbb{F}_p}$ of degree $n$ over $\mathbb{F}_p$, namely $\mathbb{F}_{p^n}$.

- $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$.

Upcoming...

$$\left( \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \varprojlim \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}. \right)$$

## §. Composite and simple extensions




**Prop** $K/F$ is Galois, $F'/F$ any ext'n.
Then $KF'/F'$ is Galois with

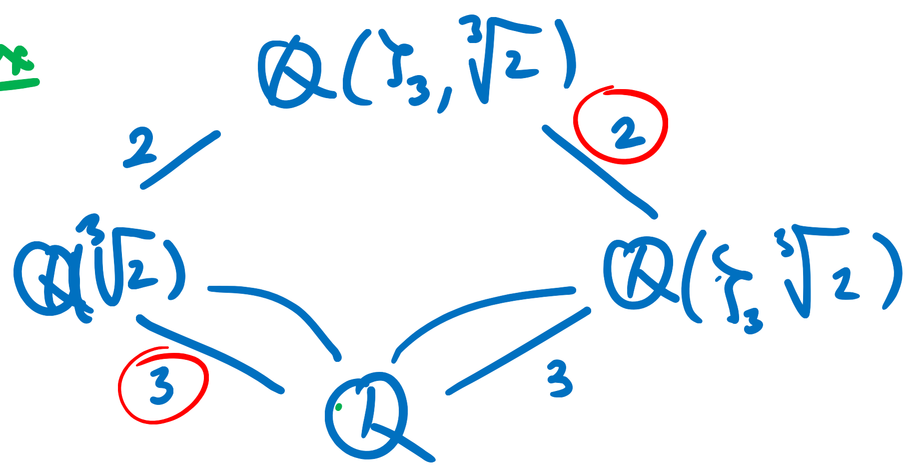
$$\mathrm{Gal}(KF'/F') \cong \mathrm{Gal}(K/K\cap F').$$

**Cor** $K/F$ is Galois, $F'/F$ any ext'n.
then

$$[KF':F'] = \frac{[K:F]\cdot[F':F]}{[K\cap F':F]}.$$

WARNING! This is not necessarily true if neither $K/F$ nor $F'/F$ is Gal!

ex




$3 \neq 2$

$$\mathbb{Q}(\sqrt[3]{2}) \cap \mathbb{Q}(\zeta_3\sqrt[3]{2}) = \mathbb{Q}$$

both of deg $3/\mathbb{Q}$ but composition is of degree 6.

**Prop** $K_1, K_2$ Galois over $F$. Then

(1) $K_1 \cap K_2$ is Galois over $F$

(2) $K_1 K_2$ is Galois over $F$

$$\begin{tikzcd}
 & K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \\
K_1 \arrow[dr, dash] \arrow[ddr, dash] & & K_2 \arrow[dl, dash] \arrow[ddl, dash] \\
 & K_1 \cap K_2 \arrow[d, dash] & \\
 & F &
\end{tikzcd}$$

and

$$\mathrm{Gal}(K_1K_2/F) \subseteq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$

$$\cong$$

$$\{(\sigma, \tau) : \sigma|_{K_1 \cap K_2} = \tau|_{K_1 \cap K_2}\}$$

$$\mathrm{Gal}(K_1K_2/F) \subseteq \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$$

$$\cong$$

$$\{(\sigma,\tau) : \sigma|_{K_1\cap K_2} = \tau|_{K_1 \cap K_2}\}$$

ex $K_1 = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$, $K_2 = \mathbb{Q}(\zeta_3, \sqrt[3]{5})$, $K_1K_2 = \mathbb{Q}(\zeta_3, \sqrt[3]{2}, \sqrt[3]{5})$

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_3,\sqrt[3]{2},\sqrt[3]{5}) \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\zeta_3,\sqrt[3]{2}) \arrow[dr, no head] & & \mathbb{Q}(\zeta_3,\sqrt[3]{5}) \arrow[dl, no head] \\
 & \mathbb{Q}(\sqrt{-3}) \arrow[d, no head] & \\
 & \mathbb{Q} &
\end{tikzcd}$$

$K_1 \cap K_2 = \mathbb{Q}(\sqrt{-3})$

$$\mathrm{Gal}(K_1K_2/\mathbb{Q}) \subseteq S_3 \times S_3$$

$$\langle \tau_1, \sigma_1 \rangle \times \langle \tau_2, \sigma_2 \rangle$$

$$=$$

$$\{(g,h) \in S_3 \times S_3 : g(\sqrt{-3}) = h(\sqrt{-3})\}$$

$$\cong$$

$$\langle \tau, \sigma_1, \sigma_2 \;:\; \tau^2 = 1,\ \sigma_1^3 = \sigma_2^3 = 1,\ \tau\sigma_i\tau = \sigma_i^2,\ \sigma_1\sigma_2 = \sigma_2\sigma_1 \rangle$$

$$\cong$$

$$(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$$ where

$$\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$$
$$\tau \longmapsto \varphi(\tau)(\sigma) = \sigma^2$$

$$\langle \tau, \sigma_1, \sigma_2 \cdot \tau^2 = 1,\ \sigma_1^3 = \sigma_2^3 = 1,\ \tau\sigma_i\tau = \sigma_i^2$$
$$\sigma_1\sigma_2 = \sigma_2\sigma_1 \rangle$$

$$\cong$$

$$\boxed{(\underset{\langle\sigma_1,\sigma_2\rangle}{\underset{\shortparallel}{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}}}) \rtimes_\varphi \underset{\langle\tau\rangle}{\underset{\shortparallel}{\mathbb{Z}/2\mathbb{Z}}}}$$

where $\varphi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$

$$\tau \longmapsto \varphi(\tau)(\sigma) = \sigma^2$$

<u>Note</u>: $(\sigma_1, 1) \cdot (1, \tau) = (\sigma_1, \tau)$

$$(1, \tau) \cdot (\sigma_1, 1) = (\varphi(\tau)(\sigma_1), \tau) = (\sigma_1^2, \tau)$$

then $(1, \tau) \cdot (\sigma_1, 1) \cdot (1, \tau) = (1, \tau) \cdot (\sigma_1, \tau)$

$$= (\sigma_1^2, 1)$$

" $\tau\sigma_1\tau = \sigma_1^2$ "

**Cor** $K_1, K_2/F$ Galois, $K_1 \cap K_2 = F$

then $\mathrm{Gal}(K_1K_2/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.

**Conversely!** If $\mathrm{Gal}(K/F) \cong G_1 \times G_2$, then there are Gal. extn's $K_1, K_2/F$ st. $K = K_1K_2$ and

$$\mathrm{Gal}(K/F) \cong \underbrace{\mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)}_{\text{are quotients of } \mathrm{Gal}(K/F)}.$$

NOT subgroups.

**ex**

$K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$, then $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ exercise

Since $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow K \neq \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{d})$ for any $d \in \mathbb{Z}$.

(Recall: $\mathbb{Q}(2^\infty) = \mathbb{Q}(\{\sqrt{d} : d \in \mathbb{Z}\})$, $\mathbb{Q}(\sqrt{2+\sqrt{2}}) \not\subseteq \mathbb{Q}(2^\infty)$ )

**ex** $K = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ w/ $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

and $K = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$ $\big(K \subseteq \mathbb{Q}(2^\infty)\big)$

exercise.

**Prop** Let $E/F$ be any separable finite extension. Then there exists $K$

$$F \subseteq E \subseteq K$$ w/ $K/F$ is Galois and minimal,

in the sense that if $L/F$ is Galois and $E \subseteq L$, then

$$F \subseteq E \subseteq K \subseteq L.$$

**Def** $K$ as above is called the Galois closure of $E$ over $F$.

**ex** $$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \underbrace{\mathbb{Q}(\zeta_3, \sqrt[3]{2})}_{\text{Gal closure}} \subseteq \overline{\mathbb{Q}}$$

**Def** An extension $K/F$ is called simple if $\exists \alpha \in K$ s.t.
$K = F(\alpha)$ (as fields).

ex $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is simple, it's $\mathbb{Q}(\sqrt{2}+\sqrt{3})$
$\mathbb{Q}(\zeta_n)$ is simple.

**Prop** Let $K/F$ be finite. Then
$K = F(\theta)$ is simple iff there exists only finitely many subfields of $K$ containing $F$.

**Note:** $K/F$ finite is important
$\mathbb{Q}(\pi)/\mathbb{Q}$ is simple but $\mathbb{Q}(\pi) \supsetneq \mathbb{Q}(\pi^2) \supsetneq \mathbb{Q}(\pi^3) \supsetneq \dots \supseteq \mathbb{Q}$

exercise

**Thm** If $K/F$ is finite, <u>separable</u>, then $K/F$ is simple.

In particular all finite extn's in char 0 are simple.

**ex**

$\mathbb{F}_p(x, y) / \mathbb{F}_p(x^p, y^p)$ is finite, but NOT simple (not separable).

<u>exercise</u>.