May 14

Recall that a field extension $K \subset L$

- separable if for every $\alpha \in L$ algebraic/K, the min poly of α has distinct roots in its splitting field
- normal if $\forall f \in K[x]$ irred with one root in L, then f splits/L
- finite if $|L:K|$ is finite

$\mathbb{F}_p(x) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{F}_p[x], g \neq 0 \right\}$

→ • Galois if separable, normal & finite

- Any char 0 field extension is separable
- any ext. of finite fields is separable

Ex: $\mathbb{F}_p(\alpha^p) \subset \mathbb{F}_p(\alpha)$ not separable. The min poly of α is

$K = K(\alpha^p)$, $K(\alpha)$

$f(x) = x^p - \alpha^p \in K[x]$

$= (x-\alpha)^p$ in $K(\alpha)[x]$

roots not distinct →

Finite & separable field extensions are simple!

Prop: If $K \subset L$ is finite & separable field ext, then $\exists \alpha \in L$ such that $L = K(\alpha)$

ILB in Hungerford

Sketch Know $L = K(\alpha_1, \dots, \alpha_n)$

Suffices to show that $\forall \alpha, \beta \in L$

$K(\alpha, \beta) = K(\gamma)$ for some γ

Idea: Take $\gamma = \alpha + c \cdot \beta$ for a "random" $c \in K$

Ex: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

But $\exists$ finite number of c's that will not work.

$\rightsquigarrow$ If K is infinite, a random c is will.

$\rightsquigarrow$ If K is finite, we can check directly.

$\mathbb{F}_p \subset \mathbb{F}_{p^n} = L$

Know $L^\times \cong \mathbb{Z}/p^n - 1$ cyclic

Choose $\alpha \in L^\times$ generator

$\rightsquigarrow \{0, 1, \alpha, \alpha^2, \dots \alpha^{p^n - 1}\} = \mathbb{F}_{p^n}$

$\Rightarrow \mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$

Ques: Find an example of $\alpha, \beta \in \mathbb{C}$ algebraic s.t. $\mathbb{Q}(\alpha, \beta) \neq \mathbb{Q}(\alpha + \beta)$.

Galois field extensions

Recall $K \subset L$ is Galois if finite + separable + normal.

Defn For $K \subset L$ field ext

$$\mathrm{Gal}(L/K) = \{ \text{field auts } \sigma: L \to L \text{ over } K \}$$

$\sigma(x) = x \quad \forall x \in K$

Important fact

$K \subset L$ Galois $\iff$

$$\#\mathrm{Gal}(L/K) = |L:K|$$

In fact, it's always true

$$\#\mathrm{Gal}(L/K) \leq |L:K|$$

Exs:

1. $\mathbb{R} \subset \mathbb{C}$ Galois

$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$ $\sigma: \mathbb{C} \to \mathbb{C}$ complex conj

2. $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ not Galois

$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$

Fund Thm of Galois Theory

Let $K \subset L$ be a Galois field ext.

There is a bijection

$$\left\{ \begin{array}{c} \text{intermediate field ext} \\ K \subset E \subset L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{subgroups} \\ H \subset \mathrm{Gal}(L/K) \end{array} \right\}$$

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

$$L^H \longleftarrow\!\shortmid H$$

with additional properties (to be spelled out later)

Here, given $H \subset \mathrm{Gal}(L/K)$,

the fixed field

$$L^H = \{ a \in L \mid \forall \sigma \in H \ \ \sigma(a) = a \}$$

Note: L^H is an intermediate field ext

$$K \subset L^H \subset L$$

Fund Thm of Galois Theory

Let $K \subset L$ be a Galois field ext.

There is a bijection

$$\left\{\begin{array}{l}\text{intermediate field ext} \\ K \subset E \subset L\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{subgroups} \\ H \subset \mathrm{Gal}(L/K)\end{array}\right\}$$

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

$$L^H \longleftarrow\!\shortmid\ H$$

with additional properties (to be spelled out later)

Here, given $H \subset \mathrm{Gal}(L/K)$,

the fixed field

$$L^H = \{\alpha \in L \mid \forall \sigma \in H,\ \sigma(\alpha) = \alpha\}$$

Note: L^H is an intermediate field ext

$$K \subset L^H \subset L$$

Going from left to right, observe if $K \subset E \subset L$

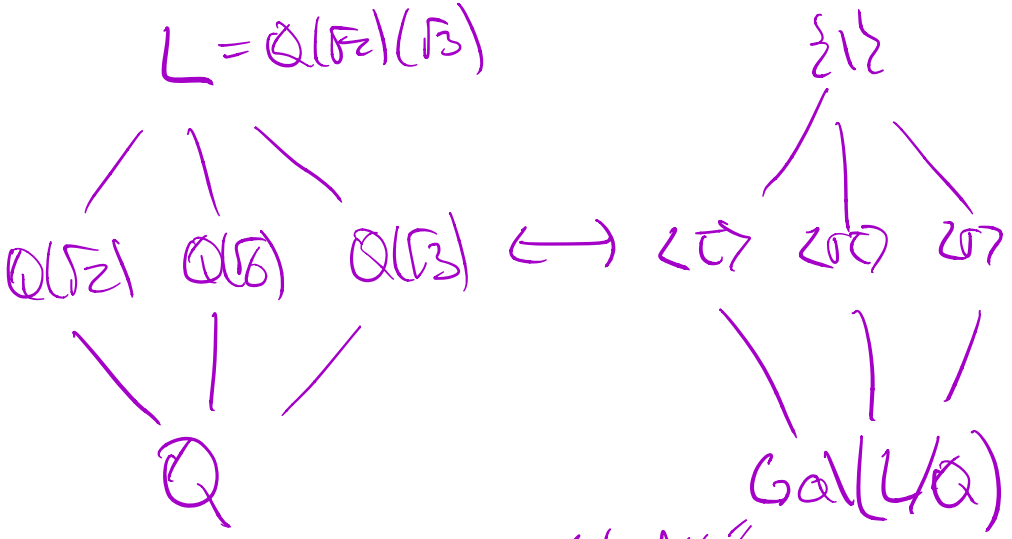
$$\mathrm{Gal}(L/E) \subset \mathrm{Gal}(L/K)$$

Why? if $\sigma : L \to L$ auto / E then it's also an auto / K

Example: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) = L$

$$\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

where $\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$ | $\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$



Fund Thm of Galois Theory

Let $K \subset L$ be a Galois field ext.

There is a bijection

$$\left\{\begin{array}{l}\text{intermediate field ext} \\ K \subset E \subset L\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{subgroups} \\ H \subset \mathrm{Gal}(L/K)\end{array}\right\}$$

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

$$L^H \longleftarrow H$$

with additional properties (to be spelled out later)

Consequence

Implicit in the statement is that these operations are inverses.

① For any $K \subset E \subset L$

$$E \longmapsto \mathrm{Gal}(L/E) \longmapsto L^{\mathrm{Gal}(L/E)}$$

Cor: $E = L^{\mathrm{Gal}(L/E)}$

② Given $H \subset \mathrm{Gal}(L/K)$

$$H \longmapsto L^H \longmapsto \mathrm{Gal}(L/L^H)$$

Cor $H = \mathrm{Gal}(L/L^H)$