Recall: If $E \supset F$ is a field extension, then its Galois group is

$$G(E/F) := \{\sigma \in \mathrm{Aut}(E) \mid \sigma(\alpha) = \alpha, \forall \alpha \in F\}.$$

If E is the s.f. of $f(x) \in F[x]$ and $\alpha \in E$ is a root of $f(x)$, then $\sigma(\alpha)$ is also a root of $f(x)$.

i.e., $G(E/F)$ acts on the set X of roots of $f(x)$.

Def. Let $E \supset F$ be an algebraic field extension. We call $\alpha, \beta \in E$ are conjugate over F if α, β have the same minimal polynomial over F.

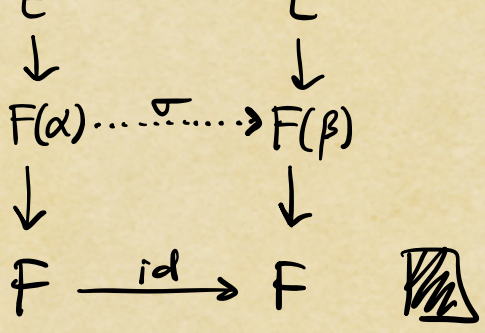
Ex $a+bi \in \mathbb{C}$. If $b=0$, min. poly. over $\mathbb{R}$ is $x-a$. If $b \neq 0$, min. poly. over $\mathbb{R}$ is

$$(x-(a+bi))(x-(a-bi)) = x^2 - 2ax + (a^2+b^2).$$

i.e., $a+bi$ & $a-bi$ have the same min. poly. over $\mathbb{R}$.

Prop. Let $E \supset F$ be an algebraic field extension and let $\alpha, \beta \in E$ be conjugate over F. Then there is an isomorphism $\sigma : F(\alpha) \longrightarrow F(\beta)$ which restricts to the identity on F.

(Proof.) Apply yesterday's lemma to



Thm. Suppose $E \supset F$ is the s.f. of a polynomial $f(x) \in F[x]$ which has no repeated roots. Then

$$|G(E/F)| = [E:F].$$

(Proof.) Induction on $[E:F]$.

Base case: $[E:F] = 1 \Rightarrow E = F \Rightarrow G(E/F) = \{id\}$ ✓

Inductive hypothesis: Theorem holds for s.f.s of degree less than $[E:F] > 1$.

Write $f(x) = p(x)q(x)$, where $p(x)$ is irreducible and $\deg p(x) > 1$.

(If every irred. factor of $f(x)$ is linear, then $f(x)$ splits $\Rightarrow E = F$.)

For any root α of $p(x)$ and any injective homom.

$$\phi: F(\alpha) \to E,$$

same proof as yesterday

$\beta := \phi(\alpha)$ is a root of $p(x)$, and we have a field isomorphism $\phi: F(\alpha) \to F(\beta)$.

from prev. prop.

Consider all such isomorphisms $\phi_i : F(\alpha) \to F(\beta_i)$, with ϕ_i fixing F, where $\beta_1, \beta_2, \ldots, \beta_d$ are the roots of $p(x)$. Note: $p(x)$ has no repeated roots.

For each ϕ_i, $1 \leq i \leq d$, consider

$$\begin{array}{ccc} E & \xrightarrow{\phi_i \circ \psi} & E \\ \downarrow & & \downarrow \\ F(\alpha) & \xrightarrow{\phi_i} & F(\beta_i) \\ \downarrow & & \downarrow \\ F & \xrightarrow{id} & F \end{array}$$

Here ψ is some automorphism of E that fixes $F(\alpha)$.
That is, $\psi \in Gal(E/F(\alpha))$.

Note:

$$[E:F(\alpha)] = \frac{[E:F]}{[F(\alpha):F]} = \frac{[E:F]}{d} < [E:F].$$

By I.H., $|G(E/F(\alpha))| = [E:F(\alpha)]$.

Altogether, there are $[F(\alpha):F]$ choices for the bottom square and $[E:F(\alpha)]$ choices for the top square of our diagram.

$\therefore$ $[E:F(\alpha)] \cdot [F(\alpha):F] = [E:F]$

elements of $G(E/F)$.

Ex $H := \{id, \sigma, \tau, \sigma\tau\} \subseteq G(E/F)$.

$E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, $F = \mathbb{Q}$.

$\sigma: \sqrt{3} \mapsto -\sqrt{3}$, $\sqrt{5} \mapsto \sqrt{5}$

$\tau: \sqrt{3} \mapsto \sqrt{3}$, $\sqrt{5} \mapsto -\sqrt{5}$

B/c E is the s.f. of $(x^2-3)(x^2-5)$ over F,

$|G(E/F)| = [E:F] = 4$.

$\therefore$ $H = G(E/F)$.

Fact. Over a field of characteristic 0, every irreducible polynomial has no repeated roots.

"is separable"

A **separable extension** is a s.f. of a separable polynomial.

Thm (Primitive Element Theorem).
Let $E \supset F$ be a finite, separable field extension.
Then there exists an element $\alpha \in E$ s.t. $E = F(\alpha)$.

Upshot: Splitting fields of irreducible polynomials over $\mathbb{Q}$ are simple, separable extensions.

Fixed fields

Given a subgroup $G \leq \mathrm{Aut}(E)$, we can define

$$E_G := \{\alpha \in E \mid \sigma(\alpha) = \alpha, \ \forall \sigma \in G\}.$$

Check: E_G is a subfield of E.
We call E_G the **fixed field** of G.

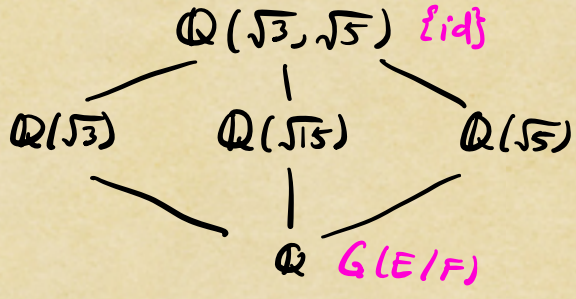
Ex. $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$, $F = \mathbb{Q}$

σ negates $\sqrt{3}$
τ negates $\sqrt{5}$

$G(E/F) = \{id, \sigma, \tau, \sigma\tau\}$.
$\{id, \sigma\}$, $\{id, \tau\}$, $\{id, \sigma\tau\}$ are subgroups.

$$E_{\{id,\sigma\}} = \mathbb{Q}(\sqrt{5}), \quad E_{\{id,\tau\}} = \mathbb{Q}(\sqrt{3})$$

$$E_{\{id,\sigma\tau\}} = \mathbb{Q}(\sqrt{15}) \leftarrow c_0 + c_1\sqrt{3} + c_2\sqrt{5} + c_3\sqrt{15}$$



Prop. Let $E \supset F$ be the s.f. of a separable polynomial over F. Then $E_{G(E/F)} = F$.

(Proof.) By def'n, $\sigma \in G(E/F) \Rightarrow \sigma(\alpha) = \alpha, \forall \alpha \in F$.

$\therefore F \subseteq E_{G(E/F)} \subseteq E$.

B/c E is a s.f. over F, it's also a s.f. over $E_{G(E/F)}$. Also, $G(E/F) = G(E/E_{G(E/F)})$, b/c any element of $G(E/F)$ fixes $E_{G(E/F)}$ by def'n.

Since E is the s.f. of a separable polynomial,

$$[E : E_{G(E/F)}] = |G(E/E_{G(E/F)}|$$

$$= |G(E/F)| = [E:F].$$

$$\therefore [E_{G(E/F)} : F] = \frac{[E:F]}{[E:E_{G(E/F)}]} = 1.$$

∎