(Skipping §5.4: Thm of Primitive Elements, which tells us that for infinite F, $L = F(\alpha_1, \dots, \alpha_n)$ w/ each α_i sep $/F$, $\exists \alpha \in L$ s.t. $L = F(\alpha)$. We may prove this later via Galois thy.)

The Galois Group

For $K, L/F$, a *field hom over F* is a hom $\varphi: K \to L$ s.t. $\varphi|_F = id_F$. Write $K \xrightarrow{\varphi} L$ with F.

Defn The *Galois group* of L/F is

$$\mathrm{Gal}(L/F) = \{ L \xrightarrow{\sigma} L \mid \sigma \text{ is an isomorphism} \}$$

$$= \text{automorphisms of } L/F.$$

Prop $\mathrm{Gal}(L/F)$ is a group under composition.

Pf
- $\sigma, \tau \in \mathrm{Gal}(L/F) \Rightarrow \sigma\tau = \sigma \circ \tau \in \mathrm{Gal}(L/F)$
- $id_L \in \mathrm{Gal}(L/F)$
- $\sigma \in \mathrm{Gal}(L/F) \Rightarrow \sigma^{-1} \in \mathrm{Gal}(L/F)$ □

e.g. $\bar{\ } \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ so $C_2 \cong \langle \bar{\ } \rangle \leq \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ (In fact, $=$)

Lemma L/F finite, $\sigma \in \mathrm{Gal}(L/F)$, $h \in F[x_1, \dots, x_n]$, $\beta_1, \dots, \beta_n \in L$ then $\sigma(h(\beta_1, \dots, \beta_n)) = h(\sigma(\beta_1), \dots, \sigma(\beta_n))$.

Pf σ preserves $+, \cdot$, fixes F. □

Prop L/F finite, $\sigma \in \mathrm{Gal}(L/F)$. Then

(a) If $h \in F[x]$ nonconst, $\alpha \in L$ root of h, then $\sigma(\alpha)$ is also a root of h lying in L.

(b) If $L = F(\alpha_1, \dots, \alpha_n)$, then σ is uniquely determined by its values on $\alpha_1, \dots, \alpha_n$.

Pf (a) $0 = \sigma(0) = \sigma(h(\alpha)) = h(\sigma(\alpha))$.

(b) Since L/F finite, $L = F[\alpha_1, \dots, \alpha_n]$, so $\beta \in L$ has $\beta = h(\alpha_1, \dots, \alpha_n)$ for some $h \in F[x_1, \dots, x_n]$. Then $\sigma(\beta) = \sigma(h(\alpha_1, \dots, \alpha_n)) = h(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$. □

Cor If L/F is finite, then $\mathrm{Gal}(L/F)$ is finite.

Pf Since L/F is finite, $L = F(\alpha_1, \dots, \alpha_n)$ with α_i alg/F.

If $p_i = m_{\alpha_i, F}$, then for $\sigma \in \mathrm{Gal}(L/F)$ must have $\sigma(\alpha_i)$ a root of p_i, and there are at most $\deg(p_i)$ of these. Since σ is determined by the values $\sigma(\alpha_i)$, conclude that $|\mathrm{Gal}(L/F)| \le \prod_{i=1}^{n} \deg(p_i) < \infty$. □

e.g. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$: $x^3 - 2$ only has one real root, $\sqrt[3]{2}$, and $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, so $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 1$.

e.g. $F = k(t)$, $\mathrm{char}(k) = p > 0$, L the splitting field of $f = x^p - t$. If $\alpha \in L$ a root of f, then $L = F(\alpha)$ and $f = (x - \alpha)^p$. Thus α is the only root of $f \Rightarrow \mathrm{Gal}(L/F) = 1$.

e.g. Roots of $x^2 + 1$ are $\pm i$, so $\langle \overline{(\ )} \rangle = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2$.

e.g. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong C_2$, gen'd by $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.

e.g. $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. For $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, know $\sigma(\sqrt{2}) = \pm\sqrt{2}$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$, so $|\mathrm{Gal}(L/\mathbb{Q})| \le 4$. If $= 4$, then $\mathrm{Gal}(L/\mathbb{Q}) \cong C_2 \times C_2$.

Prop If $L_1 \xrightarrow{\varphi}_{\cong} L_2$ (with $L_1, L_2 \supseteq F$), then $\mathrm{Gal}(L_1/F) \xrightarrow{\cong} \mathrm{Gal}(L_2/F)$, $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$. □

Defn Let $f \in F[x]$. The Galois group of f over F is $\mathrm{Gal}(L/F)$ for L a splitting field of F.

(Well-defined up to isomorphism by Prop.)

e.g. $\mathrm{Gal}(x^2 + 1/\mathbb{R}) \cong \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2$.