Galois Extensions

Defn For L/F finite and $H \leq \mathrm{Gal}(L/F)$,

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

is the fixed field of H.

Moral Exc L^H is a field.

Thm L/F finite. TFAE:

(a) L is the splitting field of a separable polynomial in $F[x]$
(b) $F = L^{\mathrm{Gal}(L/F)}$
(c) L/F normal & separable.

Pf (a) $\Rightarrow$ (b): Let $K = L^{\mathrm{Gal}(L/F)}$. Clearly $L/K/F$, and the goal is to show $K = F$. Note L is also the splitting field of f over K, so $[L:F] = |\mathrm{Gal}(L/F)|$ & $[L:K] = |\mathrm{Gal}(L/K)|$. Also note $\mathrm{Gal}(L/K) \leq \mathrm{Gal}(L/F)$ since $\sigma|_K = \mathrm{id} \Rightarrow \sigma|_F = \mathrm{id}$. But $\mathrm{Gal}(L/F) \leq \mathrm{Gal}(L/K)$ as well b/c K is the fixed field of $\mathrm{Gal}(L/F)$. Thus $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/F)$ and $[L:F] = [L:K]$. Since $[L:F] = [L:K][K:F]$, we have $[K:F] = 1 \Rightarrow K = F$. ✓

(b) $\Rightarrow$ (c): Suppose $F = L^{\mathrm{Gal}(L/F)}$ and let $\alpha \in L$. Let $\{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r\} = \mathrm{Gal}(L/F) \cdot \{\alpha\}$. Consider $h(x) = \prod_{i=1}^{r} (x - \alpha_i) \in L[x]$.

Claim $h \in F[x]$ & h is irred/F.

Note that each $\sigma \in \mathrm{Gal}(L/F)$ permutes $\{\alpha_1, \dots, \alpha_r\}$, so it also permutes the factors $x - \alpha_i$ of h. Thus the coeffs of h are fixed by $\mathrm{Gal}(L/F) \Rightarrow h \in L^{\mathrm{Gal}(L/F)}[x] = F[x]$.

Next let $g \in F[x]$ be the irred factor of h vanishing at α. Then $\sigma(\alpha)$ is a root of g $\forall \sigma \in \mathrm{Gal}(L/F) \Rightarrow$ all α_i are roots of g, whence $h \mid g \Rightarrow h$ irred. ✓

Thus $h = m_{\alpha, F}$. Hence

- Normality: If $f \in F[x]$ irred w/ root $\alpha \in L$, then $f = ah$ for some $a \in F^\times$. Thus f splits completely over L, proving normality.

· Separability: If $\alpha \in L$, then its minimal poly is h. Then α sep since h is. ✓

(c)⇒(a): Suppose L/F normal & sep. Then $L = F(\alpha_1, \dots, \alpha_n)$ where each $p_i = m_{\alpha_i, F}$ is sep. Let $q_1, \dots, q_r$ be the distinct elts of $\{p_1, \dots, p_n\}$, and set $f = q_1 \cdots q_r$. Then f is sep and L is the splitting field of f over F (check!). □

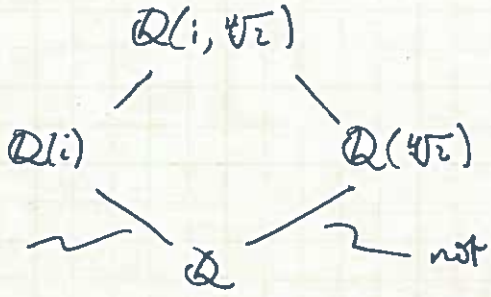
Defn An extn L/F is a Galois extn if it is finite and satisfies any of the equiv conditions of the Thm.

Note $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ Galois, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not.

Prop Suppose L/F is Galois and $L/K/F$ is a subextension. Then L/K is Galois.

Pf Use condition (a). □

e.g. $\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}$ is the splitting field of x^4-2 and hence is Galois.



Galois: splits x^2+1

not Galois: $m_{\sqrt[4]{2}, \mathbb{Q}} = x^4-2$ does not split completely.

Thm Let L/F be finite. Then $|\mathrm{Gal}(L/F)| \mid [L:F]$.

Note Already proved $|\mathrm{Gal}(L/F)| \le [L:F]$ w/ equality iff L/F Galois.

Pf Let $K = L^{\mathrm{Gal}(L/F)}$. Then $L/K/F$ & $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/F)$. Thus $K = L^{\mathrm{Gal}(L/K)}$ so L/K is Galois. Hence

$$[L:F] = [L:K][K:F] = |\mathrm{Gal}(L/K)|\,[K:F] = |\mathrm{Gal}(L/F)|\,[K:F]. \quad \square$$

Finite separable extns

Prop L/F finite. L sep $/F$ iff $L = F(\alpha_1, \dots, \alpha_n)$ w/ each α_i sep $/F$.

Pf ($\Rightarrow$) ✓

($\Leftarrow$) Suppose $L = F(\alpha_1, \dots, \alpha_n)$ with each α_i sep /F. Let $p_i = m_{\alpha_i, F}$, and let $q_1, \dots, q_r$ be the distinct elts of $\{p_1, \dots, p_n\}$. Then $f = q_1 \cdots q_r$ is sep. Let M be the splitting field of f over L. Then $M = L(\beta_1, \dots, \beta_m)$ for β_i roots of f. Claim: $M = F(\beta_1, \dots \beta_m)$. Clearly $\supseteq$. But the α_i are among the β_j, so $L = F(\alpha_1, \dots, \alpha_n) \subseteq F(\beta_1, \dots, \beta_m) \Rightarrow M \subseteq F(\beta_1, \dots, \beta_m)$, so equal. Thus M/F Galois and hence sep. Since $L \subseteq M$, every elt of L is sep./F. □

Galois closure

Prop If L/F finite sep, then M/L as above is Galois over F and is the smallest such extn of L.

Pf Reading (Prop 7.1.7). □

Defn Call M as above the Galois closure of L/F.