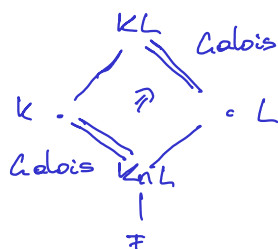


14.4 Composite and simple extensions.

Cool: Understand



Theorem. Let K/F be Galois, L/F arbitrary.

Then KL/L is Galois and $\text{Gal}(KL/L) \cong \text{Gal}(K/K \cap L)$.

Proof. Let K be the splitting field of $f(x) \in F[x]$. Then KL is the splitting field of $f(x)$ over L , hence KL is Galois over L .

Consider

$$\begin{array}{ccc} \text{Res}_K^{KL}: \text{Gal}(KL/L) & \rightarrow & \text{Gal}(K/K \cap L) \\ \sigma & \mapsto & \sigma|_K \end{array}$$

(well defined since K/F is Galois and every embedding σ of K fixing F also stabilize K).

1) $\sigma \in \text{Res}_K^{KL}$ iff $\sigma|_K = \text{id}_K$

Then σ fixes K and L , hence $\sigma = \text{id}_{KL}$. So Res_K^{KL} is injective.

2) For the image of Res_K^{KL} consider

$$E := \text{Fix}(\text{Res}_K^{KL}(\text{Gal}(KL/L))) \subseteq K$$

$$\text{Then } K \cap L \subseteq E \subseteq \text{Fix}(\text{Gal}(K/K \cap L)) = K \cap L$$

yields $E = K \cap L$.

$$\text{Then } \text{Res}_K^{KL}(\text{Gal}(KL/L)) = \text{Gal}(K/K \cap L).$$

Hence Res_K^{KL} is an iso.

□

Corollary. If K/F is Galois and L/F is finite, then

$$[KL:F] = \frac{[K:F][L:F]}{[K \cap L:F]}.$$

Theorem. Let K/F and L/F be Galois. Then

- (1) $K \cap L/F$ is Galois.
- (2) KL/F is Galois with

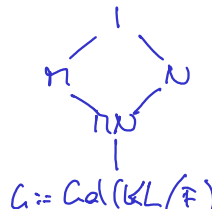
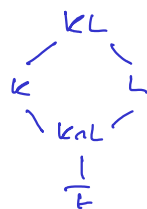
$$\text{Gal}(KL/F) \cong \{(\sigma, \tau) \in \text{Gal}(K/F) \times \text{Gal}(L/F) : \sigma|_{K \cap L} = \tau|_{K \cap L}\}$$

"subdirect product"

Proof. Let K, L be splitting fields of $(f(x), g(x)) \in F[x]$, respectively.

Then KL is the splitting field of $(\text{lcm}(f(x), g(x)))$, hence KL is Galois over F .

By FTAT



$$\pi, N \trianglelefteq G \Rightarrow \langle \pi, N \rangle = \pi N \trianglelefteq G$$

So $K \cap L / F$ is Galois and (1) is proved.

For the second part of (2) consider

$$\begin{aligned} \varphi: G &\rightarrow \pi \times N \\ G &\mapsto (G|_K, G|_L) \end{aligned}$$

$$\text{a) ker } \varphi = \{\text{id}_G\}$$

\rightarrow Finished on last page!

Corollary. Let E/F be Galois. Then

$$\text{Gal}(\overbrace{KL}^E / F) \cong M \times N$$

iff there exist Galois extensions $K/F, L/F$ with $KL = E, K \cap L = F$. In this case $M \cong \text{Gal}(K/F), N \cong \text{Gal}(L/F)$.

Proof. \Leftarrow immediate from previous Thm

\Rightarrow Let $K := \text{Fix}(\pi), L := \text{Fix}(N)$. By FTAT

$$KL = \text{Fix}(\underbrace{\pi \cap N}_1) = E$$

$$K \cap L = \text{Fix}(\underbrace{\pi \times N}_G) = F.$$

Example.

$$\begin{array}{c} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \\ \swarrow \quad \searrow \\ \mathbb{Q}(\sqrt{2}) \quad \mathbb{Q}(\sqrt{3}) \\ \swarrow \quad \searrow \\ \mathbb{Q} \end{array}$$

Corollary. Let E/F be finite, separable. Then there exists a minimal K/E such that K/F is Galois (and L/F is not Galois for any $E \leq L < K$).

Then K is the Galois closure of E/F (unique up to isomorphism).

Application. Degree computations are easier in Galois closures.

Proof. Let π be the splitting field of the min polynomials of the basis elements of E over F .

Then π/F is Galois, $E \subseteq \pi$.

$$K := \bigcap \{ L \mid E \subseteq L \subseteq \pi, L/F \text{ is Galois} \} \text{ is min. Galois over } F \quad \square$$

The Primitive Element Theorem.

Question. When is a finite extension K/F simple, i.e., $K = F(\alpha)$ for some $\alpha \in K$?

Example. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

Recall. For K finite, $K^* = \langle \alpha \rangle$ and $K = F(\alpha)$.

Artin's Theorem. Let K/F be finite. Then $K = F(\alpha)$ for some $\alpha \in K$ iff $\{L : F \leq L \leq K\}$ is finite. (# of fields between F and K is finite).

Proof. Let $S := \{L : F \leq L \leq K\}$.

" \Rightarrow " Assume $K = F(\alpha)$. Then

$$D := \{g(x) \in K[x] : g(x) \mid m_{K,F}(x)\}.$$

Claim: $h : S \rightarrow D, L \mapsto m_{K,L}(x)$, is injective.

$$\text{For } m_{K,L}(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n$$

$$F(a_0, \dots, a_{n-1}) \subseteq L. \text{ Then}$$

$$[K : F(a_0, \dots, a_{n-1})] = \deg m_{K,L}(x) = [K : L]$$

$$\text{implies } F(a_0, \dots, a_{n-1}) = L.$$

Hence h is uniquely determined by $m_{K,L}(x)$ and h is injective. Thus $|S| \leq |D| < \infty$.

" \Leftarrow " Assume $|S| < \infty$. Induct on $[K : F]$.

Assume $[K : F] = 1$. Let $\alpha \in K \setminus F$.

$$F \subsetneq F(\alpha) \subseteq K$$

By induction $K = F(\alpha, \beta)$ for some $\beta \in K \setminus F(\alpha)$.

Consider

$$K_t := F(\alpha + t\beta) \text{ for } t \in F.$$

Since S is fin, F inf, we have $s \neq t \in F$ s.t. $K_t = K_s$.

$$\text{Then } \beta = \frac{\alpha + s\beta - (\alpha + t\beta)}{s-t} \in K_t.$$

$$\text{Hence } \alpha \in K_t \text{ and } K_t = K.$$

□

Primitive Element Theorem. Every finite separable extension K/F is simple.

Proof. Apply Artin's Thm to the Galois closure L of K/F . □

Corollary. Every finite Galois extension is simple

Example. $\bar{F} = \bar{F}_p(x, y) \quad |\bar{F}_p| = p \text{ prime}$

$$K = \bar{F}(x, \beta) \text{ with } x^p = x, \beta^p = y$$

$$[K : \bar{F}] = p^2.$$

K/\bar{F} is not simple.

$$\text{For any } g \in K \setminus \bar{F}, \quad x^p \in \bar{F}, \quad [\underbrace{\bar{F}(g) : \bar{F}}_{\neq K}] = p.$$

Proof of subdirect representability of $\text{Gal}(KL/F)$, continued:

$$b) \varphi(G) = \{ (g, \tau) \in \Pi \times N \mid g|_{KL} = \tau|_{KL} \} \quad (*)$$

For the converse, let (g, τ) in the r.h.s.

Extend g, τ to $g', \tau' \in G$.

Since $g'|_{KL} = \tau'|_{KL}$, we have $g' = \tau' \pmod{KN}$.

We have $\alpha \in \Pi, \beta \in N$ such that $g' \alpha \beta = \tau'$.

Let $G := g' \alpha = \tau' \beta^{-1}$. Then

$$G \equiv g' \pmod{\Pi}$$

$$G = \tau' \pmod{N}$$

$$G|_K = g'|_K = g$$

$$G|_L = \tau'|_L = \tau$$

Hence $(G) = (g, \tau)$ and " \supseteq " in $(*)$ is proved. □