14.4 Composite and simple extensions.

Goal: Understand

$$\begin{tikzcd} & KL \arrow[dl, dash] \arrow[dr, dash, "\text{Galois}"] & \\ K \arrow[dr, dash, "\text{Galois}"'] \arrow[rr, phantom, "\Rightarrow"] & & L \arrow[dl, dash] \\ & K\cap L \arrow[d, dash] & \\ & F & \end{tikzcd}$$

Theorem. *Let K/F be Galois, L/F arbitrary.*
Then KL/L is Galois and $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K\cap L)$.

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

$$\mathrm{Res}^{KL}_{K} : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/K\cap L)$$
$$\sigma \mapsto \sigma|_K$$

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

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

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

2) For the image of Res^{KL}_{K} consider

$E := \mathrm{Fix}\left(\mathrm{Res}^{KL}_{K}(\mathrm{Gal}(KL/L))\right) \subseteq K$

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

yields $E = K\cap L$.

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

Hence Res^{KL}_{K} is an iso. $\square$

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*

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

"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 $\mathrm{lcm}(f(x), g(x))$, hence Galois over F.

By FTGT

$$\begin{tikzcd}[column sep=small]
 & KL \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & L \arrow[dl, dash] \\
 & K\cap L \arrow[d, dash] & \\
 & F &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[dr, dash] & \\
M \arrow[dr, dash] & & N \arrow[dl, dash] \\
 & MN \arrow[d, dash] & \\
 & G := \mathrm{Gal}(KL/F) &
\end{tikzcd}$$

$M, N \trianglelefteq G$
$\Rightarrow \langle M, N \rangle = MN \trianglelefteq G$

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

For the second part of (2) consider

$$\varphi : G \to M \times N$$
$$\sigma \mapsto (\sigma|_K, \sigma|_L)$$

a) $\ker \varphi = \{ \mathrm{id}_{KL} \}$

$\Rightarrow$ Finished on last page!

Corollary. *Let E/F be Galois. Then*

$$\mathrm{Gal}(\cancel{KL}\, E/F) \cong M \times N$$

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

Proof. $\Leftarrow$ immediate from previous Thm

$\Rightarrow$ Let $K := \mathrm{Fix}(M)$, $L := \mathrm{Fix}(N)$. By FTGT

$$KL = \mathrm{Fix}(\underbrace{M \cap N}_{=1}) = E$$
$$K \cap L = \mathrm{Fix}(\underbrace{M \times N}_{G}) = F.$$

□

Example.

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

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 M be the splitting field of the min polynomials of the basis elements of E over F.

Then M/F is Galois, $E \subseteq M$.

$K := \bigcap \{ L \mid E \leq L \leq M,\ L/F \text{ is Galois} \}$ is min. Galois over F □

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

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

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

For $m_{\alpha,L}(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1} + x^n$

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

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

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

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

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

Assume $|K:F| > 1$. Let $\alpha \in K \setminus F$.

$F \lneq F(\alpha) \leq K$

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

Consider

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

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

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

Hence $\alpha \in K_t$ and $K_t = K$. $\square$

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

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

Corollary. *Every finite Galois extension is simple*

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

$K = F(\alpha, \beta)$ with $\alpha^p = x$, $\beta^p = y$

$[K:F] = p^2$.

K/F is not simple.

For any $\gamma \in K \setminus F$, $\gamma^p \in F$, $[\underbrace{F(\gamma)}_{\neq K} : F] = p$.

Proof of subdirect representation of $Gal(KL/F)$, continued:

b) $\varphi(G) \subseteq \{ (\varrho, \tau) \in M \times N \mid \varrho|_{K \cap L} = \tau|_{K \cap L} \}$ $(*)$

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

Extend ϱ, τ to $\varrho', \tau' \in G$.

Since $\varrho'|_{K \cap L} = \tau'|_{K \cap L}$, we have $\varrho' \equiv \tau' \mod MN$.

We have $\alpha \in M$, $\beta \in N$ such that $\varrho' \alpha \beta = \tau'$.

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

$\sigma \equiv \varrho' \mod M$ $\qquad$ $\sigma \equiv \tau' \mod N$

$\sigma|_K = \varrho'|_K = \varrho$ $\qquad$ $\sigma|_L = \tau'|_L = \tau$

Hence $\varphi(\sigma) = (\varrho, \tau)$ and "$\supseteq$" in $(*)$ is proved. $\square$