4.6 Radical extensions

Def: $E, F \subset L$ subfields

The <u>composition EF of E and F in L</u> is the smallest subfield of L that contains both E and F.

For lemmas 1–3, we fix the situation

$$\begin{tikzcd}[column sep=small] & L \arrow[d, dash] & \\ & EF \arrow[dl, dash] \arrow[dr, dash] & \\ E \arrow[dr, dash] & & F \arrow[dl, dash] \\ & K & \end{tikzcd}$$

Note: if $E = K(a_i)$ and $F = K(b_j)$, then $EF = K(a_i, b_j)$.

Lemma 1: If E/K is normal / separable / finite, then EF/F is normal / separable / finite.

$$\begin{tikzcd}[column sep=small] & EF \arrow[dl, dash] \arrow[dr, dash, "\substack{\text{normal/}\\ \text{sep./}\\ \text{finite}}"] & \\ E \arrow[dr, dash, "\substack{\text{normal/}\\ \text{sep./}\\ \text{finite}}"'] \arrow[rr, phantom, "\Rightarrow"] & & F \arrow[dl, dash] \\ & K & \end{tikzcd}$$

proof: • E/K normal

Consider $\sigma: \begin{tikzcd}[column sep=small] EF \arrow[rr] \arrow[dr, dash] & & \overline{EF} \arrow[dl, dash] \\ & F & \end{tikzcd}$, i.e. $\sigma|_F = id_F$.

Thus $\sigma|_K = id_K$ and $\sigma(E) = E$ since E/K normal.

Thus $\sigma(EF) = \sigma(E)\,\sigma(F) = EF$, which shows that EF/F is normal.

• E/K separable

Then every $a \in E$ is separable over K, and thus separable over F. Since $EF = F(a \mid a \in E)$, EF/F is separable.

- E/K finite

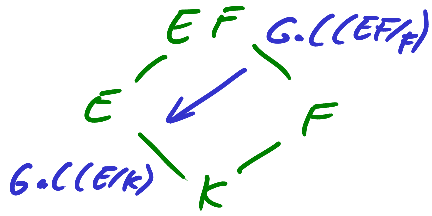
  Then $E = K(a_1, \ldots, a_n)$ where $a_1, \ldots, a_n$ alg. $/K$

  $\Rightarrow EF = F(a_1, \ldots, a_n)$ and $a_1, \ldots, a_n$ alg. $/F$

  $\Rightarrow EF/F$ finite. $\square$

<u>Lemma 2:</u> E/K finite Galois, F/K finite

Then EF/F is Galois and



$$\varphi : \mathrm{Gal}(EF/F) \longrightarrow \mathrm{Gal}(E/K)$$
$$\sigma \longmapsto \sigma|_E$$

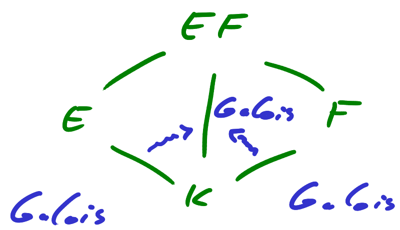
is an injective group homomorphism.

<u>proof:</u>
- By Lemma 1, EF/F is finite Galois.
- Since E/K is normal, $\sigma|_K = \mathrm{id}_K$ and $\sigma(E) = E$ for all $\sigma \in \mathrm{Gal}(EF/F)$. Thus $\sigma|_E : E \to E$ is well-defined as an element of $\mathrm{Gal}(E/K)$. Clearly, φ is a group hom.
- Consider $\sigma \in \ker \varphi$, i.e. $\sigma|_E = \mathrm{id}_E$.

  Since also $\sigma|_F = \mathrm{id}_F$, we have $\sigma = \mathrm{id}_{EF}$.

  Thus φ is injective. $\square$

<u>Lemma 3:</u> If both E/K and F/K are finite Galois, then EF/K is finite Galois.



<u>proof</u>: · Since both E/K and F/K are normal,

every K-linear hom. $\sigma : EF \longrightarrow \overline{EF}$ satisfies

$\sigma(EF) = \sigma(E)\sigma(F) = EF \Rightarrow EF/K$ is normal.

· Since both E/K and F/K are finite separable,

EF/F is finite separable (Lemma 1),

and thus EF/K is finite separable $\square$

<u>Def</u>: L/K finite

(1) L/K is <u>solvable</u> if it is Galois with solvable Galois group.

(2) L/K is <u>simple radical</u> if it is separable and if $L = K(a)$ for some $a \in L$ that is a root of a polynomial $f \in K[T]$ of the form

$$f = T^n - b \qquad \text{where } \operatorname{char} K \nmid n,$$

or

$$f = T^p - T - b \qquad \text{where } \operatorname{char} K = p.$$

(3) L/K is <u>radical</u> if there exists a sequence

$$K = E_0 \subset E_1 \subset \cdots \subset E_e = L$$

of simple radical extensions E_i / E_{i-1} $(i = 1 \ldots e)$.
We call $E_0 \subset \ldots \subset E_e$ a <u>radical tower</u> for L/K.

(4) L/K is <u>contained in a radical extension</u> if there is a field extension E/L s.t. E/K is radical.

<u>Ex:</u> (1) Every cyclotomic, Kummer and Artin-Schreier extension is solvable (since abelian) and simple radical (by def.).

(2) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is simple radical since $\sqrt[3]{2}$ is a root of $f = T^3 - 2$, but not solvable since not normal.

<u>Lemma 4:</u> $K \subset E \subset L$ finite s.t. all of E/K, L/E, L/K are Galois. Then L/K is solvable if and only if both L/E and E/K are solvable.

$$\begin{tikzcd} L \arrow[d, dash, "\text{solv.}"] \\ E \arrow[d, dash, "\text{solv.}"] \\ K \arrow[uu, dash, bend left, "\text{solv.}"] \end{tikzcd}$$

<u>proof:</u> By the fund. thm. of Galois theory (Thm. 3.3.1), we have a short exact sequence

$$1 \to \mathrm{Gal}(L/E) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K) \to 1.$$

Thus the lemma follows from Exercise 1 of List 5. $\square$

Lemma 5: $K(a)/K$ simple radical, $\sigma : K(a) \to \bar{F}$ s.t. $\sigma(K) \subset F$ for some field F.

$$\begin{tikzcd} & F(\sigma(a)) \arrow[dr, dash, "\text{simp. rad.}"] & \\ K(a) \arrow[ur, "\sigma"] \arrow[dr, dash, "\text{simp. rad.}"'] & \rightsquigarrow & F \\ & K \arrow[ur, "\sigma|_K"'] & \end{tikzcd}$$

Then $F(\sigma(a))/F$ is simple radical.

proof: • $K(a)/K$ simple radical $\rightsquigarrow$ may assume that a is a root of a polynomial of the form $f = T^n - b$ ($\operatorname{char} K \nmid n$) or $f = T^p - T - b$ ($\operatorname{char} K = p$) with $b \in K$.

$\Rightarrow$ $\sigma(a)$ is a root of $\sigma(f) \in F[T]$.

Since $\operatorname{char} F = \operatorname{char} K$, this shows that $F(\sigma(a))/F$ is simple radical. $\square$

Lemma 6: $K \subset E \subset L$ finite.

$$\begin{tikzcd} L \arrow[d, dash, "\text{c rad.}"] \\ E \arrow[d, dash, "\text{c rad.}"] \\ K \end{tikzcd} \quad \text{c rad.}$$

Then L/K is contained in a radical extension if and only if both L/E and E/K are contained in radical extensions.

proof: "$\Rightarrow$": Assume that $L \subset F$ s.t. F/K is radical, i.e. there is a radical tower

$$K = F_0 \subset F_1 \subset \_\_ \subset F_e = F.$$

- Since $E \subset F$, E is contained in a radical extension.
- Define $F_i' = EF_i \subset F$. By lemma 5,

$$\begin{tikzcd} & F_{i+1}' = F_{i+1}E \arrow[dr, dash, "\text{simp. rad.}"] & \\ F_{i+1} \arrow[ur, dash] \arrow[rr, squiggly] & & F_i' = F_iE \\ & F_i \arrow[ul, dash, "\text{simp. rad.}"] \arrow[ur, dash] & \end{tikzcd}$$

F_{i+1}' / F_i' is simple radical. Thus

$$E = F_0' \subset \ldots \subset F_\ell' = F$$

is a radical tower $\Rightarrow L_E$ is contained in the radical extension F/E.

"$\Leftarrow$": Assume E/K is contained in a radical extension with tower

$$K = F_0 \subset \ldots \subset F_\ell$$

and L/E is contained in a radical extension with tower

$$E = E_0 \subset \ldots \subset E_k.$$

Define $E_i' = E_i F_\ell$ for $i = 0 \ldots k$ (inside some fixed algebraic closure of E_k and F_ℓ).

By Lemma 5, E_i' / E_{i-1}' is simple radical for $i = 1 \ldots k$. Thus

$$K = F_0 \subset \ldots \subset F_\ell = E_0' \subset \ldots \subset E_k'$$

is a radical tower and $L \subset E_k \subset E_k'$. $\square$

<u>Thm 7:</u> L/K separable, finite.

Then L/K is contained in a radical extension if and only if L^{norm}/K is solvable.

proof: "$\Leftarrow$": Assume that L^{norm}/K is solvable, i.e.

$G = Gal(L^{norm}/K)$ is solvable.

Define

$$n = \prod_{\substack{q \mid \# G \text{ prime} \\ q \neq \operatorname{char} K}} q .$$

- In the following, we consider all fields as subfields of $\bar{K}$. Let $\zeta_n \in \bar{K}$ be a primitive n-th root of unity and $F = K(\zeta_n)$. By Thm. 4.3.2, F/K is abelian and thus F/K is solvable. Since ζ_n is a root of $T^n - 1$ and $\operatorname{char} K \nmid n$, F/K is simple radical.
- Let $E = L^{norm}$ and consider

$$\begin{tikzcd}
 & EF \arrow[dl, dash] \arrow[dr, dash, "\text{Galois (Lemma 1)}"] & \\
L^{norm} = E \arrow[dr, dash, "\text{Galois}"'] & & F = K(\zeta_n) \arrow[dl, dash, "\text{solvable \& radical}"] \\
 & K &
\end{tikzcd}$$

where $G' = Gal(EF/F)$ is a subgroup of $G = Gal(E/K)$ by Lemma 2.

By Lemma 3, EF/K is Galois.

- By Exercise 1 of List 5, G' is solvable, i.e. there exists a normal series

$$\{e\} = G_0 \triangleleft \ldots \triangleleft G_r = G'$$

with factors $G_i / G_{i-1} \simeq \mathbb{Z}/p_i\mathbb{Z}$ for prime numbers $p_1 \ldots p_r$. Define $E_i = (EF)^{G_i}$. Then

$$F = E_r \subset \ldots \subset E_0 = EF$$

is a tower of Galois extensions E_{i-1}/E_i with respective Galois groups

$$\mathrm{Gal}(E_{i-1}/E_i) = G_i/G_{i-1} \simeq \mathbb{Z}/p_i\mathbb{Z}$$

(by Thms. 3.3.1 & 3.3.3).

-> If $p_i \neq \mathrm{char}\, K$, then $p_i \mid n$ and $\# \mu_{p_i}(F) = p_i$. Thus E_{i-1}/E_i is Kummer and therefore simple radical.

-> If $p_i = \mathrm{char}\, K$, then E_{i-1}/E_i is Artin-Schreier and therefore simple radical.

- Thus $E_r \subset \ldots \subset E_0$ is a radical tower for EF/F. Since F/K is radical, EF/K is radical by Lemma 6. Thus L/K is contained in a radical extension. ∎

$\underline{`\Rightarrow'}$: Next Lecture.