3. Reminder on Galois theory

Let $K \subset L$ be a field extension

$x \in L$ and consider $\varphi_x : K[X] \to L$, $f \mapsto f(x)$

Def 1) x is called transcendental / K if φ_x is injective. Otherwise x is called algebraic / K.

2) if x alg / $K \Rightarrow \ker(\varphi_x) = (f_0)$ $f_0 \neq 0$, f_0 is called minimal polynom. of x / K.

3) $K \subset L$ is called algebraic / K if $\forall x \in L$ is alg. / K

4) $K \subset L$ is called finite extension if $\dim_K L < \infty$. Notation: $[L:K] = \dim_K L$

Recall: a) a finite ext. is algebraic

b) if $K \subset L \subset F$ tower of field ext., then $[F:K] = [F:L] \cdot [L:K]$

5) A field F is alg. closed if $\forall f \in F[x]$ $\exists x \in F : f(x) = 0 \iff \forall f \in F[x]$ splits, i.e. $f = a \cdot \prod_{i=1}^{\deg f} (X - x_i)$, $a, x_i \in F$

6) An alg. ext. $K \subset L$ is separable if $\forall x \in L$ the min. poly of x has no multiple roots (in any ext. of K)

Remarks 1) $K \subset L$ alg. ext. $x \in L$

$\varphi_x : K[x] \to L$, $\ker \varphi_x = (f_0)$

$\frac{K[x]}{(f_0)} \cong \mathrm{Im}(\varphi_x)$ = the subfield gen. by x

2) $\forall$ field K $\exists$ an alg. closed field $\bar{K}$, and $K \subset \bar{K}$ is alg. $\bar{K}$ is called the alg. closure of K, it is unique up to an isomorphism.

3) Assume $\mathrm{char}\, K = 0$. Then $\forall$ alg. ext. of K is separable; also $\forall$ alg. ext of a finite field $\mathbb{F}_q$, $q = p^n$ is separable.

Example (inseparable ext) $K = \mathbb{F}_p(t)$

Let $f = X^p - t$. Then

$L = K/(f)$ is inseparable / K

In $\overline{K}$ f has a root denoted by $\sqrt[p]{t}$. Then $f = (X - \sqrt[p]{t})^p$

Prop. 3.1 Let $K \subset L$ be a finite ext. and $u: K \hookrightarrow F$ an embedding into an alg. closed field F. Then:

1) $\exists$ an embedding $\sigma: L \hookrightarrow F$ over K (i.e. $\sigma|_K = u$)

2) If $K \subset L$ is separable, then $\exists$ exactly $[L:K]$ different embeddings $\sigma_i: L \to F$ over K.

Idea of proof 1) Induction on $[L:K]=n$

For $n=1$ nothing to prove

Assume $n>1$; take $x \in L \setminus K$

f = min. poly of x /K

$$K \subset \frac{K[X]}{(f)} \subset L$$

By induction may assume $L \cong \frac{K[X]}{(f)}$

F alg. closed $\Rightarrow$ f a root $\alpha \in F$

$$\varphi_\alpha : K[X] \longrightarrow F$$
$$X \longmapsto \alpha$$

$\ker \varphi_\alpha = (g)$, but $f \in \ker(\varphi_\alpha)$

$\Rightarrow f = g \cdot h$, but f is irred,

so $h \in K \Rightarrow \varphi_\alpha$ induces

$$\sigma : \frac{K[x]}{(f)} \simeq L \hookrightarrow F$$

2) As before, enough to consider $L \simeq \frac{K[x]}{(f)}$, then f has exactly $\deg(f) = [L:K]$ different root in F by separability. $\square$

Def 1) $K \subset L$ extension.

$$\mathrm{Aut}(L/K) = \{ g : L \xrightarrow{\sim} L \text{ field automorph, s.t. } g|_K = id \}$$

Note, that if $u : K \hookrightarrow F$, F alg. closed, and $\sigma : L \hookrightarrow F$ over K, then $g \in \mathrm{Aut}(L/K)$ $\sigma \circ g : L \hookrightarrow F$ / K

2) a finite ext $K \subset L$ is normal, if given alg. closed F and $\sigma : L \hookrightarrow F$ any other $\sigma' : L \hookrightarrow F$ over K is of the form $\sigma' = \sigma \circ g$ for some

$g \in Aut(L/K)$

Corollary (from Prop. 3.1) If $K \subset L$ a finite extension, then $|Aut(L/K)| \leq [L:K]$

Recall: if $G \subset Aut(L/K)$, let

$$L^G = \{x \in L \mid \forall g \in G \quad gx = x\}$$

Then L^G is a subfield

Def-prop. 3.2 A finite ext $K \subset L$ is called Galois ext. if it satisfies one of the equiv. conditions:

1) $K \subset L$ is normal and separable
2) $|Aut(L/K)| = [L:K]$
3) $L^{Aut(L/K)} = K$
4) $\forall f \in K[x]$ that has a root in L splits in L

In this case $Aut(L/K)$ is called Galois group of L/K, denoted

$$Gal(L/K)$$

Fund. thm. of Galois theory

Let $K \subset L$ be a Galois ext.

Consider the following sets an maps

$$\{\text{subgroups } G \subset Gal(L/K)\} \underset{Aut(L/H) \leftarrow H}{\overset{G \mapsto L^G}{\rightleftarrows}} \{\text{subfields } K \subset H \subset L\}$$

These maps are mutually inverse bijections, s.t. normal subgroups $G \subset Gal(L/K)$ correspond to Galois subextensions $K \subset H$ with $Gal(H/K) \cong \frac{Gal(L/K)}{G}$

Rmk 1) $\exists$ a version for infinite Galois extensions. For this version we need to introduce topology on $Gal(L/K)$ (pro-finite topology)

2) $\forall$ finite separable extension $K \subset L$ is contained in a finite Galois extension $K \subset L \subset F$. E.g. embed $\sigma_i: L \subset \overline{K}/K$ take F = subfield of $\overline{K}$ generated by $\sigma_i(L)$ for all possible embeddings/K

Primitive element thm If $K \subset L$ a finite separable extension, the $\exists\, x \in L$ s.t. $L = K(x) \cong \frac{K[X]}{(f)}$, f = min. poly of x.

Examples 1) $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] = \frac{\mathbb{Q}[X]}{(X^2-2)}$

$[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$

$\exists$ 2 embeddings $\sigma_{1,2} : \frac{\mathbb{Q}[X]}{(X^2-2)} \hookrightarrow \mathbb{C}$

$\sigma_1(X) = \sqrt{2} \in \mathbb{C}$

$\sigma_2(X) = -\sqrt{2} \in \mathbb{C}$

$\Rightarrow \mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ is a Galois ext.

2) $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] = \frac{\mathbb{Q}[X]}{(X^3-2)} = L_0$

$[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$

$X^3 - 2$ has 3 roots in $\mathbb{C}$:

$x_1 = \sqrt[3]{2} \in \mathbb{R}$,

$x_2 = \sqrt[3]{2} \cdot e^{2\pi i/3}$ $\quad x_3 = \overline{x_2}$

$\Rightarrow \exists$ 3 embeddings $\sigma_i : L_0 \hookrightarrow \mathbb{C} / \mathbb{Q}$

$\sigma_i(X) = x_i$

But $\mathrm{Im}(\sigma_1) \subset \mathbb{R}$, $\mathrm{Im}(\sigma_2) \not\subset \mathbb{R}$

$\Rightarrow \sigma_1$ and σ_2 are not conj. by an autom. of $L_0/\mathbb{Q}$.

$\Rightarrow \mathbb{Q} \subset L_0$ is not normal

In $L_0[x]$: $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$

to produce a Galois ext. we need to take quadratic ext $L_0 \subset L$

$[L : K] = 6$ $K \subset L$ Galois ext.