Rmk Let $f(X) \in K[X]$ be irreducible with slope $-\frac{a}{b}$ $(\gcd(a,b)=1)$.
Let $\alpha \in \overline{K}$ be a root of $f(X)$. ($\Rightarrow v(\alpha) = \frac{a}{b}$) and
$L = K(\alpha) \cong K[X]/f(X)$. Then $b \mid e(L|K)$ because

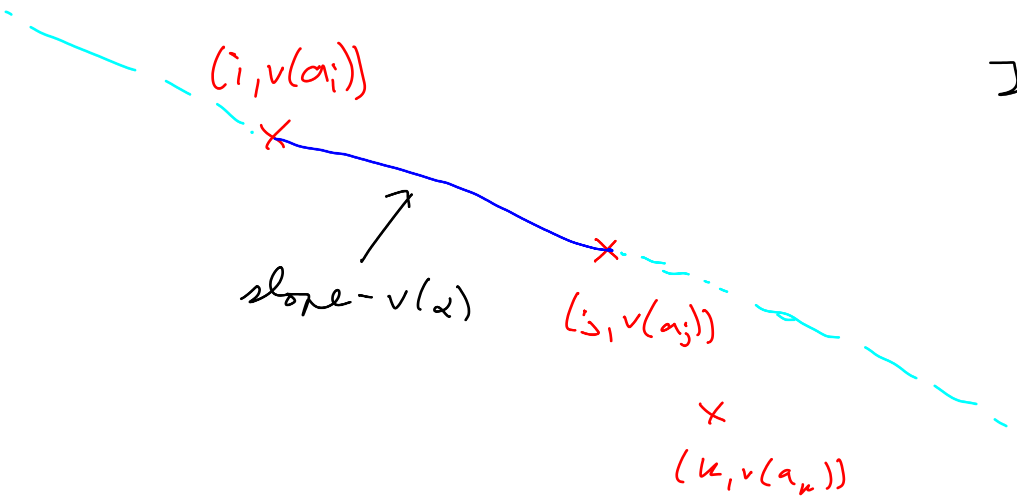
$$\frac{a}{b} \in v_K(L^\times) = \frac{1}{e}\cdot\mathbb{Z}.$$

Warning We might have $b \neq e$.
For example, look at $X^2 - 3 \in \mathbb{Q}_2[X]$. $\rightsquigarrow$ slope $0 = \frac{0}{1}$
But
$$v_2(1-\sqrt{3}) = \frac{1}{2} v_2(N_{\mathbb{Q}_2(\sqrt{3})|\mathbb{Q}_2}(1-\sqrt{3}))$$
$$= \frac{1}{2} v_2(1-3) = \frac{1}{2}, \text{ so } e = 2.$$

Another proof that $f(\alpha)=0 \Rightarrow v(\alpha) = -$slope of a line seg.

Write $f(X) = \sum_i a_i X^i$.
Then monomials have valuation $v(a_i\alpha^i) = v(a_i) + i\cdot v(\alpha)$.
If the min. val. t occured in just one monomial $a_i\alpha^i$, then $v(f(\alpha)) = t$, so $f(\alpha) \neq 0$. ↯
$\Rightarrow$ The min. val. occurs in at least two monomials $a_i\alpha^i$, $a_j\alpha^j$.

$$\Rightarrow v(a_j) - v(a_i) = -(j-i)\cdot v(\alpha).$$



If there were a third point $(k, v(a_k))$ below the line, then
$v(a_k\alpha^k) < v(a_i\alpha^i)$.
↯ $\square$

1.8. Classification of local fields

<u>Thm</u> The local fields are: nonarchimedean

- the fin. ext. K of $\mathbb{Q}_p$
- the fields $K = \mathbb{F}_q((T))$.

<u>Pf</u> Let $\kappa_K = \mathbb{F}_q$, $q = p^f$.

<u>Case 1: $\mathrm{char}(K) = 0$</u>

$\Rightarrow \mathbb{Q} \subseteq K$

$p = 0$ in $\mathbb{F}_q \Rightarrow v_K(p) \geq 1$.

$\Rightarrow v_K|_{\mathbb{Q}}$ is a multiple of the p-adic valuation on $\mathbb{Q}$

$\Rightarrow K$ is an ext. of $\mathbb{Q}_p$ with $f(K|\mathbb{Q}_p) = [\mathbb{F}_q : \mathbb{F}_p] = f < \infty$

$e(K|\mathbb{Q}_p) = v_K(p) < \infty$

of degree $n = e \cdot f < \infty$.

<u>Case 2: $\mathrm{char}(K) \neq 0$</u>

$\mathrm{char}(K) = 0$ in $K \Rightarrow \mathrm{char}(K) = 0$ in $\kappa_K = \mathbb{F}_q$

$\Rightarrow \mathrm{char}(K) = p$.

$\Rightarrow \mathbb{F}_p \subseteq K$.

$\mathbb{F}_q$ is the splitting field of the separable polynomial $X^q - X = \prod_{t \in \mathbb{F}_q} (X - t)$ over $\mathbb{F}_p$.

By Hensel's lemma, it splits completely in K,

$\Rightarrow \mathbb{F}_q \subseteq K$.

$\Rightarrow$ We can write any el. x of K in base π_K with digits in $\mathbb{F}_q$:

$x = \sum_{i=-r}^{\infty} a_i \pi_K^i \quad (a_i \in \mathbb{F}_q)$. $\Rightarrow K \cong \mathbb{F}_q((T))$

$\pi_K \leftrightarrow T$ $\square$

2. Infinite Galois theory

Reference: Chapter 4.2 in Bosch: Algebra from the viewpoint of Galois theory

Def A Galois ext. $L|K$ is an algebraic field ext. which is normal and separable.

If an irred. pol. $f(x) \in K[X]$ has a root in L,

then it split completely in L — then all its roots in $\overline{K}$ are distinct (equivalently, $f'(x) \neq 0$).

Ex The separable closure K^{sep} of K is the maximal Galois extension of K.

2.1. Computing infinite Galois groups

Question What is $Gal(\overline{\mathbb{F}}_q | \mathbb{F}_q)$?

Thm Let $M|K$ be a Gal. ext. and let $\mathcal{L}$ be any set of finite galois ext. $L \subseteq M$ of K such that $M = \bigcup_{L \in \mathcal{L}} L$.

Then, $Gal(M|K) \cong \varprojlim_{L \in \mathcal{L}} Gal(L|K)$, the set

$$\sigma \longmapsto (\sigma|_L)_L.$$

of tuples $(\sigma_L)_L \in \prod_{L \in \mathcal{L}} Gal(L|K)$ such that

$$\sigma_{L_2}\big|_{L_1} = \sigma_{L_1} \quad \text{for all } L_1 \subseteq L_2 \quad (\text{in } \mathcal{L}).$$

Pf The preimage of $(\sigma_L)_L \in \varprojlim \mathrm{Gal}(L|K)$ is

$$\sigma : M \to M$$
$$x \mapsto \sigma_L(x) \text{ for any } x \in L \in \mathcal{L}.$$

Well-def: Assume $x \in L_1, L_2 \in \mathcal{L}$.

Look at the composition $L_1 \cdot L_2$.

We have $L_1 \cdot L_2 = K(y)$ for some $y \in M$.

Let $y \in L_3 \in \mathcal{L}$. $\Rightarrow L_1, L_2 \subseteq L_1 \cdot L_2 \subseteq L_3$.

$$\Rightarrow \sigma_{L_1}(x) \underset{L_1 \subseteq L_3}{=} \sigma_{L_3}(x) \underset{L_2 \subseteq L_3}{=} \sigma_{L_2}(x)$$

Field hom.: Let $x, y \in M$. Let $K(x,y) \subseteq L \in \mathcal{L}$.

$$\Rightarrow \sigma(x \pm y) = \sigma_L(x \pm y) = \sigma_L(x) \pm \sigma_L(y) = \sigma(x) \pm \sigma(y)$$

Fixes K: Let $x \in K$. Take any $L \in \mathcal{L}$.

$$\Rightarrow \sigma(x) = \sigma_L(x) = x. \qquad \square$$

Ex The fin. ext. of $\mathbb{F}_q$ are $\mathbb{F}_{q^n}$ with $n \geq 1$.

$$\Rightarrow \mathrm{Gal}(\overline{\mathbb{F}}_q \mid \mathbb{F}_q) \cong \varprojlim_{n \geq 1} \mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q)$$

We have $\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$

$$\varphi_q \longmapsto 1 \bmod n$$

where φ_q is the Frobenius automorphism $x \mapsto x^q$.

Note that $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ if and only if $n \mid m$ (so $\mathbb{F}_{q^m} = \mathbb{F}_{(q^n)^{m/n}}$) and that in this case

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{F}_{q^m} \mid \mathbb{F}_q) \arrow[d, "\text{restriction}"'] & \cong & \mathbb{Z}/m\mathbb{Z} \arrow[d, "\text{reduction mod } n"] \\
\mathrm{Gal}(\mathbb{F}_{q^n} \mid \mathbb{F}_q) & \cong & \mathbb{Z}/n\mathbb{Z}
\end{tikzcd}
\qquad
\begin{tikzcd}
\varphi_q \arrow[r, mapsto] \arrow[d, mapsto] & 1 \bmod m \arrow[d, mapsto] \\
\varphi_q \arrow[r, mapsto] & 1 \bmod n
\end{tikzcd}$$

$$\mathrm{Gal}(\overline{\mathbb{F}}_q \mid \mathbb{F}_q) = \varprojlim_{n \geq 1} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$

$$\Big\uparrow$$

set of $(a_n)_n \in \prod_n \mathbb{Z}/n\mathbb{Z}$

s.t. $a_n = a_m \bmod n \ \forall n \mid m$

Ex $\mathbb{Q}(\zeta_\infty) = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n)$ is a field (in fact a Gal. ext.)

because $\mathbb{Q}(\zeta_n)\cdot\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{nm})$.

$\Rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) &\cong (\mathbb{Z}/n\mathbb{Z})^\times \\ \phi_k &\longmapsto k \bmod n\end{aligned}$$

where ϕ_k is the automorphism $\zeta_n \mapsto \zeta_n^k$.

Note that $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m)$ if and only if $n \mid \mathrm{lcm}(m,2)$.
(note that $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ for n odd).
In particular, $\mathbb{Q}(\zeta_{2n}) \subseteq \mathbb{Q}(\zeta_{2m})$ if and only if $n \mid m$.

In this case,

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}(\zeta_{2m})|\mathbb{Q}) \arrow[r, phantom, "\cong"] \arrow[d, "\text{restriction}"'] & (\mathbb{Z}/2m\mathbb{Z})^\times \arrow[d, "\text{reduction mod } 2n"] \\
\mathrm{Gal}(\mathbb{Q}(\zeta_{2n})|\mathbb{Q}) \arrow[r, phantom, "\cong"] & (\mathbb{Z}/2n\mathbb{Z})^\times
\end{tikzcd}$$

$$\begin{tikzcd}
\phi_k \arrow[r] \arrow[d, mapsto] & k \bmod 2m \arrow[d, mapsto] \\
\phi_k \arrow[r] & k \bmod 2n
\end{tikzcd}$$

$$\begin{aligned}\Rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}) &= \varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_{2n})|\mathbb{Q}) \\ &= \varprojlim (\mathbb{Z}/2n\mathbb{Z})^\times \\ &= \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times \\ &= \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times.\end{aligned}$$

2.2. Fundamental theorem

Fund. thm. finite of Galois theory

Let $M|K$ be a finite Gal. ext. with $G = Gal(M|K)$.
Then, there is a bijection

$$\{\text{field } K \subseteq L \subseteq M\} \longleftrightarrow \{\text{subgroup } H \subseteq G\}$$

$$L \longmapsto Gal(M|L) = \{\sigma \in G \mid \sigma(x) = x \ \forall x \in L\}$$

$$M^H = \{x \in M \mid \sigma(x) = x \ \forall \sigma \in H\} \longleftarrow\!\shortmid \ H$$

$$\begin{tikzcd}
M \arrow[dd, dash, "G"'] \arrow[dr, dash, "H"] & \\
& L \arrow[dl, dash] \\
K &
\end{tikzcd}$$

$M|L$ is always Galois.
$L|K$ is Galois if and only if H is a normal subgroup of G. Then, H is the kernel of $G \longrightarrow Gal(L|K)$,
$$\sigma \longmapsto \sigma|_L$$
so $Gal(L|K) \cong G/H$.

What goes wrong for infinite Galois extensions?

We might have $Gal(M|M^H) \supsetneq H$.

Not every $H \leq G$ is of the form $Gal(M|L)$ for some L.

<u>Ex</u> $G = Gal(\overline{\mathbb{F}_q}|\mathbb{F}_q) \cong \hat{\mathbb{Z}}$

$$\begin{array}{ccc} \cup\!\!\mid & & \cup\!\!\mid \\ H = & \langle \varphi_q \rangle & \cong \mathbb{Z} \\ & \varphi_q & \longrightarrow 1 \end{array}$$

$$\overline{\mathbb{F}_q}^H = \{x \in \overline{\mathbb{F}_q} \mid \varphi_q(x) = x\}$$
$$= \{x \in \overline{\mathbb{F}_q} \mid x^q = x\}$$
$$= \mathbb{F}_q$$

$$\Rightarrow Gal(\overline{\mathbb{F}_q}|\overline{\mathbb{F}_q}^H) = Gal(\overline{\mathbb{F}_q}|\mathbb{F}_q) = G \supsetneq H.$$