<u>Thm 2.6.3</u> Given points $Q_1, \dots, Q_d$ representing the cosets in $E(K)/mE(K)$, there's an algorithm to determine $E(K)_{tors}$ and the rank r of E, and points $P_1, \dots, P_r$ representing a $\mathbb{Z}$-basis of $E(K)/E(K)_{tors} \cong \mathbb{Z}^r$.

<u>Pf</u> By pf of "weak M-W $\Rightarrow$ M-W", you can find generators $R_1, \dots, R_b$ of $E(K)$.

The rank r of E over K is the size of a max. lin. indep. subset of $R_1 \otimes 1, \dots, R_b \otimes 1$ in $E(K) \otimes \mathbb{R}$.

Consider the map

$$f : \mathbb{Z}^b \twoheadrightarrow E(K) \otimes \mathbb{R} \cong \mathbb{R}^r$$

$$(a_1, \dots, a_b) \mapsto (a_1 R_1 + \dots + a_b R_b) \otimes 1.$$

We can find a matrix representing this map. $\Rightarrow$ We can find elements $v_1, \dots, v_c \in \ker(f)$ spanning $\ker(f) \otimes_{\mathbb{Z}} \mathbb{R}$.

Then, find elements $w_1, \dots, w_c$ spanning the free $\mathbb{Z}$-module $\ker(f)$.

We obtain points $P_1, \dots, P_c \in E(K)$ (P_i = the lin. comb. of $R_1, \dots, R_b$ corr. to $w_i \in \mathbb{Z}^b$) generating $E(K)_{tors}$. $\square$

Rmk We only have an algorithm that ~~conjecturally~~ determines $Q_1, \dots, Q_d$.
(It never produces wrong results, but we don't know if it always terminates!)

Rmk The above algorithms are far from optimal!

2.7. Hermite's finiteness theorem

Thm 2.7.1 For any $n \geq 1$, $T \geq 1$, there are only finitely many number fields K of degree n and discriminant satisfying
$|D_K| \leq T$.

Pf Let L be the Galois closure of $K|\mathbb{Q}$.
The embeddings $K \hookrightarrow \mathbb{C}$ correspond to elements of $Gal(L|\mathbb{Q})/Gal(L|K)$
(compose with a fixed embedding $L \hookrightarrow \mathbb{C}$).

$$\begin{array}{c} L \\ | \\ K \\ | \\ K' \\ | \\ \mathbb{Q} \end{array}$$

For any $\mathbb{Q} \subseteq K' \subseteq K$

$$\begin{tikzcd}
\{\text{emb. } K \hookrightarrow \mathbb{C}\} \arrow[r, leftrightarrow] \arrow[d, "\text{restriction}"] & Gal(L|\mathbb{Q})/Gal(L|K) \arrow[d, "\text{quotient}", "{[K:K']\text{-to-1 map}}"'] \\
\{\text{emb. } K' \hookrightarrow \mathbb{C}\} \arrow[r, leftrightarrow] & Gal(L|\mathbb{Q})/Gal(L|K')
\end{tikzcd}$$

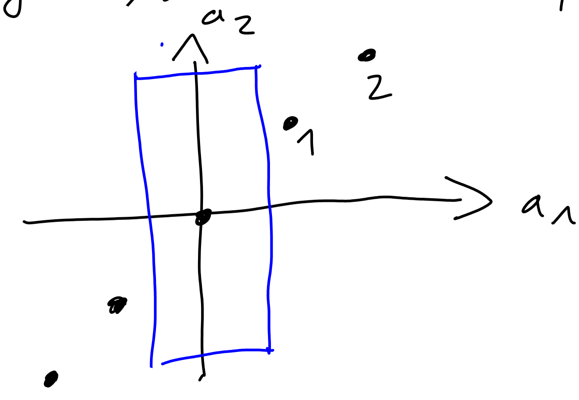
$\Rightarrow$ If $K' \subsetneq K$, then every embedding $K' \hookrightarrow \mathbb{C}$ has multiple extensions to K. (I)

For simplicity, consider only totally real number fields K, with n real embeddings $\sigma_1, \dots, \sigma_n$.

By Minkowski's theorem, there is a number $C > 0$ depending on n and T, but not on K such that the convex centrally symmetric set

$$\{(a_1, \dots, a_n) \in \mathbb{R}^n \mid |a_1|, \dots, |a_{n-1}| < 1,\ |a_n| < C\}$$

contain a nonzero element of the integer lattice $\{(\sigma_1(a), \dots, \sigma_n(a)) \mid a \in \mathcal{O}_K\}$.



Since $1 \leq |N_m(a)| = \underbrace{|\sigma_1(a)|}_{<1} \cdots \underbrace{|\sigma_{n-1}(a)|}_{<1} \cdot |\sigma_n(a)|$,

we have $|\sigma_n(a)| > 1$.

Hence, $\sigma_n(a) \neq \sigma_i(a)$ for $i = 1, \dots, n-1$, so the restriction of σ_n to $\mathbb{Q}(a)$ is different from the restrictions of $\sigma_1, \dots, \sigma_{n-1}$ to $\mathbb{Q}(a)$.

$\underset{(I)}{\Longrightarrow}$ $K = \mathbb{Q}(a)$.

The coeff. of the min. pol.

$$f(X) = (X - \underbrace{\sigma_1(a)}_{|\cdot|<1}) \cdots (X - \underbrace{\sigma_{n-1}(a)}_{|\cdot|<1})(X - \underbrace{\sigma_n(a)}_{|\cdot|<C}) \in \mathbb{Z}[X]$$

are bounded.

$\Rightarrow$ There are only fin. many possible minimal pol. $f(X)$.

$\Rightarrow$ Only fin. many possible $a \in \overline{\mathbb{Q}}$.

$\Rightarrow$ Only fin. many possible K. $\square$

Lemma 2.7.2 Let k be a nonarchimedean local field of characteristic 0, and $n \geq 1$. Then, there are only finitely many extensions $L|k$ of degree n.

Pf Since the Galois closure of $L|k$ has degree $\leq n!$, it suffices to consider only Galois extensions.

Since the Galois group of a Gal. ext. of local fields is solvable (follows from the theory of higher ramification groups), by induction, it suffices to consider only cyclic extensions.

By class field theory, they correspond to open subgroups U of $k^\times$ with $k^\times/U \cong \mathbb{Z}/n\mathbb{Z}$.

Note that ~~then~~ $U \supseteq k^{\times n}$. But $k^\times \cong \mathcal{O}_k^\times \times \mathbb{Z}$,
$$u \cdot \pi_k^t \leftarrow (u, t)$$

so $k^{\times n} = \mathcal{O}_k^{\times n} \times n\mathbb{Z}$.

By Hensel's lemma, every $a \in \mathcal{O}_k^\times$ with $a \equiv 1 \bmod \mathfrak{p}_k^{2v_{\mathfrak{p}}(n)+1}$ has an

n-th root in $\mathcal{O}_k^\times$. (Lift the root 1 of $X^n - a$ modulo $\mathfrak{q}_k^{2v_{\mathfrak{q}}(n)+1}$.)

$\Rightarrow \mathcal{O}_k^\times / \mathcal{O}_k^{\times n} \hookrightarrow \left(\mathcal{O}_k / \mathfrak{q}_k^{2v_{\mathfrak{q}}(n)+1}\right)^\times$ is finite.

$\Rightarrow k^\times / k^{\times n} = \mathcal{O}_k^\times / \mathcal{O}_k^{\times n} \times \mathbb{Z}/n\mathbb{Z}$ is finite

$\Rightarrow$ There are only finitely many U.

$\square$

Serre: Formules de masse ...

Thm 2.7.3 Let K be a number field, let S be a finite set of primes of K, and let $n \geq 1$. Then, there are only finitely many extensions $L|K$ of degree n which are unramified at every prime $\mathfrak{q} \notin S$.

Ex $\mathbb{Q}$ has no unramified extensions (other than $\mathbb{Q}$).

Pf To apply Thm 2.7.1, we need an upper bound on $|D_L|$. By the relative discriminant formula,

$$|D_L| = \underbrace{\left|\mathrm{Nm}_{K|\mathbb{Q}}(\mathrm{disc}(L|K))\right|}_{= \prod_{\mathfrak{q} \in S} \mathrm{Nm}(\mathfrak{q})^{v_{\mathfrak{q}}(\mathrm{disc}(L|K))}} \cdot |D_K|^{[L:K]}$$

If $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ are the primes of L above $\mathfrak{q}$, then

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathfrak{q}} \cong \mathcal{O}_{\mathfrak{P}_1} \times \dots \times \mathcal{O}_{\mathfrak{P}_r}.$$

$$\begin{array}{cccc} L & \mathfrak{P}_1 \dots \mathfrak{P}_r & L_{\mathfrak{P}_1} \dots L_{\mathfrak{P}_r} & \mathcal{O}_{\mathfrak{P}_1} \dots \mathcal{O}_{\mathfrak{P}_r} \\ | & \backslash \quad / & \backslash \quad / & \backslash \quad / \\ K & \mathfrak{q} & K_{\mathfrak{q}} & \mathcal{O}_{\mathfrak{q}} \end{array}$$

$$\Rightarrow v_{\mathfrak{q}}(\mathrm{disc}(L|K)) = \underbrace{v_{\mathfrak{q}}(\mathrm{disc}(L_{\mathfrak{P}_1}|K_{\mathfrak{q}}))}_{\text{bounded}} + \dots + \underbrace{v_{\mathfrak{q}}(\mathrm{disc}(L_{\mathfrak{P}_r}|K_{\mathfrak{q}}))}_{\text{bounded}}$$

(only finitely many possible $L_{\mathfrak{P}_i}$)

$\square$

2.8. The Chevalley-Weil theorem

<u>Thm 2.8.1</u> Let $V \subseteq \mathbb{A}^a_K$, $W \subseteq \mathbb{A}^b_K$ be smooth varieties over a number field K and let $\varphi: V \longrightarrow W$ be a dominant finite unramified morphism.

Then, there is a finite set S of primes of K such that any $P \in V(\overline{K})$ with $Q := \varphi(P) \in W(\mathcal{O}_K)$ lies in $V(K')$ for a (finite) field ext. K' of K which is unramified at all primes $\mathfrak{q} \notin S$.

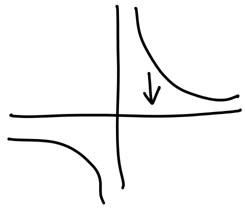
<u>Non-Ex</u> The morphism

$$\varphi : \mathbb{A}^1_{\mathbb{Q}} \longrightarrow \mathbb{A}^1_{\mathbb{Q}} \quad \text{is dominant and}$$
$$x \longmapsto x^2$$

finite, but ramified at 0.

The field ext. $\mathbb{Q}(\sqrt{y})|\mathbb{Q}$ for $y \in \mathbb{Z}$ can be ramified anywhere.

<u>Ex</u> The morphism



$$\varphi : \{(x,x') \in \mathbb{A}^2_K \mid xx'=1\} \longrightarrow \{(y,y') \in \mathbb{A}^2_K \mid yy'=1\}$$
$$(x,x') \longmapsto (x^2, x'^2)$$

is unramified.

The field ext. $K(\sqrt{y})|K$ for $(y,y') \in \mathcal{O}_K^2$ with $yy'=1$ (so $y \in \mathcal{O}_K^\times$)

is unramified at all primes not dividing 2.