Recollection (not including ζ-fcts)

$K/\mathbb{Q}$ finite ext. "number fields",

$n := [K:\mathbb{Q}]$

Ex: 1) $K = \mathbb{Q}(\sqrt{d})$ quadratic,

$d \in \mathbb{Z}$ squarefree

2) $K = \mathbb{Q}(\zeta_N)$, $\zeta_N = e^{2\pi i/N}$

cyclotomic

3) K cubic, e.g. $\mathbb{Q}(\sqrt[3]{2})$

1) are related 2):

K quadratic $\Rightarrow$ $K \subseteq \mathbb{Q}(\zeta_N)$,

$N = |\Delta_K|$ (Prop. 7.5.1.)

Not true for 3): $K \cdot \mathbb{Q}(\zeta_3)$ has Galois group S_3

while $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \overset{\varphi}{\simeq} (\mathbb{Z}/N)^\times$ is abelian

⚠ can.:

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \arrow[d, "\wr"] \\
\mathrm{Aut}(\mu_N) \\
(\mathbb{Z}/N)^\times \arrow[u, "\wr"']
\end{tikzcd}$$

$\mu_N = \{x \in \mathbb{C} \mid x^N = 1\}$

$\mu_N \subseteq \mathbb{Q}(\zeta_N)$

ind. by $\mathbb{Z} \to \mathrm{End}(\mu_N)$

Each $\#$-field K comes equipped with a canonical subring $\mathcal{O}_K \subseteq K$ "the ring of integers"

$$\mathcal{O}_K = \{x \in K \mid \exists m \geq 1, a_1, \dots, a_m \in \mathbb{Z}$$
$$x^m + a_1 x^{m-1} + \dots + a_m = 0\}$$

$$= \{x \in K \mid \text{min. poly of } x \text{ over } \mathbb{Q} \text{ has coeff. in } \mathbb{Z}\}$$

Thm: $\mathcal{O}_K$ is finite free $/\mathbb{Z}$ of rk n

Recall proof:

1) $tr: K \times K \to \mathbb{Q}, (x,y) \mapsto Tr_{K/\mathbb{Q}}(x \cdot y)$

non-degenerate
(holds for gen. fin. <u>sep.</u> field extensions)

2) $M \subseteq \mathcal{O}_K$, $\mathbb{Q} \otimes_{\mathbb{Z}} M = K$
finite free of rk n

$$\Rightarrow \quad M \subseteq \mathcal{O}_K \subseteq \mathcal{O}_K^{\vee} \subseteq M^{\vee}$$

dual w.r.t. tr

In part, $\mathcal{O}_K \subseteq \dfrac{1}{[M^{\vee} : M]} \cdot M$

($\rightsquigarrow$ helpful for calc. $\mathcal{O}_K$)

If $M = \langle \alpha_1, \dots, \alpha_n \rangle_{\mathbb{Z}}$

$$\det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)) \quad (|\ \ | = [M^{\vee} : M])$$

If $(\beta_1, \dots, \beta_n) = (\alpha_1, \dots, \alpha_n) \cdot C$, $C \in GL_n(\mathbb{Z})$

$$\Rightarrow \det(\mathrm{Tr}_{K/\mathbb{Q}}(\beta_i \beta_j)) = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)) \cdot \underbrace{\det C^2}_{=1}$$

$\Delta_K := \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j))$ for

$\alpha_1, \dots, \alpha_n$ integral basis, i.e.

$\langle \alpha_1, \dots, \alpha_n \rangle = \mathcal{O}_K$

Most imp. prop. of Δ_K

A prime $p \in \mathbb{Z}$ ramifies in $\mathcal{O}_K$, i.e.

$(p) = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$, $\mathfrak{p}_i \subseteq \mathcal{O}_K$ max'l

$e_i \geq 2$ $\qquad\qquad$ $\mathfrak{p}_i \neq \mathfrak{p}_j$, $i \neq j$

if and only if $p \mid \Delta_K$ #

$|\Delta_K| = [\mathcal{O}_K^\vee : \mathcal{O}_K]$ $\qquad$ $n > 1$

$$\text{Fact: } \sqrt{|\Delta_K|} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!} \overset{!}{>} 1$$

Ex: 1) $K = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ squarefree

$$\Rightarrow \mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right], & d \equiv 1 \ (4) \\ \mathbb{Z}[\sqrt{d}], & d \equiv 3 \ (4) \end{cases}$$

$$\Delta_K = \begin{cases} d \\ 4d \end{cases}$$

2) $K = \mathbb{Q}(\zeta_N) \Rightarrow \mathcal{O}_K = \mathbb{Z}[\zeta_N]$,

$$\{p \mid \Delta_K\} = \{p \mid N\}, \quad N \geq 3$$

3) $K = \mathbb{Q}(\sqrt[3]{7}) \Rightarrow \mathcal{O}_K = \mathbb{Z}[\sqrt[3]{7}]$

Useful: 1) Eisenstein crit. Prop. 1.3.8.

($\rightsquigarrow$ useful for finding $\mathcal{O}_K$)

2) Prop. 1.3.2:

$$|\mathrm{Disc}(1, \alpha, \ldots, \alpha^{n-1})| = |N_{K/\mathbb{Q}}(f'(\alpha))|$$

f min. Poly of α, & $K = \mathbb{Q}(\alpha)$

Other invariants

$r_1 := \# \mathrm{Hom}_{\mathbb{Q}\text{-alg}}(K, \mathbb{R})$

$r_2 := \#$ pairs of cpl.-conj. emb.

$\sigma : K \hookrightarrow \mathbb{C}, \ \sigma(K) \not\subseteq \mathbb{R}$

$$= \frac{n - r_1}{2}$$

In short: $\mathbb{R} \underset{\mathbb{Q}}{\otimes} K \underset{\text{as } \mathbb{R}\text{-alg.}}{\simeq} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

$U_K = \mathcal{O}_K^\times = \{ x \in \mathcal{O}_K \mid N_{K/\mathbb{Q}}(x) \in \{\pm 1\} \}$

$\cup\!\!\mid$

$W_K = \{ x \in K \mid x^N = 1 \text{ for some } N \geq 1 \}$

Dirichlet's unit thm

1) W_K finite cyclic

2) U_K/W_K is a finite free abelian group of rk r_1+r_2-1

Idea of proof:

$$K \overset{\lambda}{\hookrightarrow} \mathbb{R}^{r_1}\times\mathbb{C}^{r_2},\ x\mapsto(\sigma_1(x),\dots,\sigma_{r_1}(x), \sigma_{r_1+1}(x),\dots,\sigma_s(x))$$

$\cup$

$$\begin{tikzcd}
U_K \arrow[r, hook] \arrow[dr, "\ell"'] & (\mathbb{R}^\times)^{r_1}\times(\mathbb{C}^\times)^{r_2} \arrow[d, "\mathrm{Log}"] \\
& \mathbb{R}^{r_1+r_2}
\end{tikzcd}$$

$$(\mathbb{R}^\times)^{r_1}\times(\mathbb{C}^\times)^{r_2} \ni (x_1,\dots,x_{r_1}, z_1,\dots,z_{r_2}) \mapsto (\log|x_i|, 2\log|z_j|)$$

$\operatorname{Ker}\ell = W_K \leftarrow |N_{K/\mathbb{Q}}(x)|=1$

& $\ell(U_K) \subseteq H := \{(y_1,\dots,y_{r_1+r_2})\in\mathbb{R}^{r_1+r_2} \mid \sum y_i = 0\}$

full lattice

$$R_K = \frac{1}{\sqrt{r_1+r_2}} \cdot \mathrm{vol}\left(H / \ell(U_K)\right)$$

$$= \left| \det(n, \ell(u_1), \dots, \ell(u_{r_1+r_2-1})) \right|$$

$u_1, \dots, u_{r_1+r_2-1}$ gen of U_K / W_K

$\in \mathbb{R}^{r_1+r_2}$

s.t. $\sum n_i = 1$

R_K "regulator" (not easy to calculate)

Finally, the class grp of $\mathcal{O}_K$

$Cl_K := I / P$, $I := \{ 0 \neq I \subseteq K \text{ fract. ideal} \}$

$\cup\!|$

$P := \{ (a) \mid a \in K^* \}$

$\frac{1}{d} I \subseteq \mathcal{O}_K$ for some $d \in \mathcal{O}_K$

$\mathcal{I}$ abelian group under multiplication

(This holds for <u>all</u> Dedekind

domains)

noeth, int. cld, domain

s.t. non-zero primes

are maximal (e.g. $\mathcal{O}_K$)

Thm: A Dedekind, $0 \neq I \subseteq A$

ideal

$\Rightarrow \exists$ unique fact. $I = \mathfrak{P}_1 \cdot \ldots \cdot \mathfrak{P}_r$

$\mathfrak{P}_i \subseteq A$ max'l

up to

permutation

For $\mathcal{O}_K \subseteq K$ a number field

Cl_K is finite

Sketch of proof:

$\iota : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} =: \mathbb{R}^n$

For $0 \neq J \subseteq K$ fract. ideal:

$\Rightarrow \iota(J) \subseteq \mathbb{R}^n$ lattice

$\mathrm{vol}(\mathbb{R}^n / \iota(J)) = 2^{-r_2} \sqrt{|\Delta_K|}$

$N(J)$ ~ If $J \subseteq \mathcal{O}_K$

$\Rightarrow N(J) = [\mathcal{O}_K : J]$

& ex. non-zero $\alpha \in J$, s.t.

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \sqrt{|\Delta_K|} \cdot N(J)$$

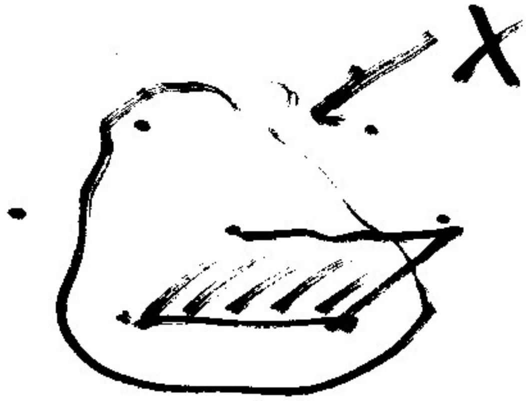
$\Uparrow$

Minkowski's lm: $\Lambda \subseteq \mathbb{R}^n$ lattice,

$X \subseteq \mathbb{R}^n$ centrally sym.

$\mu(X) > 2^n \cdot \mathrm{vol}(\mathbb{R}^n / \Lambda)$

$\Rightarrow \Lambda \cap X \neq \{0\}$



Minkowski bdd:

Each class $C \in Cl_K$ contains $\mathfrak{a} \subseteq \mathcal{O}_K$ with

$$N(\mathfrak{a}) \le \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \sqrt{|\Delta_K|}$$

($\rightsquigarrow$ useful for calculating Cl_K,
e.g. $Cl_{\mathbb{Q}(\sqrt[3]{2})} = 1$)

$h_K := \# Cl_K$ class number of K

$h_K = 1 \iff \mathcal{O}_K$ PID

Another important topic:

Decompositions of primes

L/K ext. of number fields,

$\mathfrak{p} \subseteq \mathcal{O}_K$

$$\underset{\substack{\uparrow\\ \text{unique fact. in } \mathcal{O}_L}}{\Rightarrow} \quad \mathfrak{p} \cdot \mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_g^{e_g}$$

$\mathfrak{q}_i \subseteq \mathcal{O}_L$ prime,

$\mathfrak{q}_i \neq \mathfrak{q}_j,\ i \neq j$

$$n = \sum_{i=1}^{g} e_i f_i$$

$e_i =: e(\mathfrak{q}_i | \mathfrak{p})$ ramification degree

$$f_i = [k(\mathfrak{q}_i) : k(\mathfrak{p})] = f(\mathfrak{q}_i | \mathfrak{p})$$

$$k(\mathfrak{q}_i) := \mathcal{O}_L/\mathfrak{q}_i \underset{\mathfrak{p}}{\supseteq} \mathcal{O}_K/\mathfrak{p} =: k(\mathfrak{p})$$

$$\mathfrak{q}_i \cap \mathcal{O}_K = \mathfrak{p}$$

Three phenomena:

1) splitting $(g \geq 2)$

2) ramification ($e_i \geq 2$ for some i, occurs exactly for primes $\mathfrak{p}$ dividing the relative discriminant $\Delta_{L/K}$)

3) residue field extensions ($f_i \geq 2$)

How to find factorizations?

Thm 3.2.3. (Kummer)

If $\alpha \in \mathcal{O}_L$, s.t. $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \underbrace{\mathcal{O}_K/\mathfrak{p}}_{k(\mathfrak{p})}[\bar{\alpha}]$

f min. poly of α,

$$* \quad \bar{f}(x) = \prod_{i=1}^{g} g_i(x)^{e_i} \in k(\mathfrak{p})[x]$$

monic irred., $g_i \neq g_j$ $i \neq j$

$\Rightarrow \quad \mathfrak{q}_i = (\mathfrak{p}, h_i(\alpha))$, $f_i = \deg(g_i)$

$\bar{h}_i = g_i \qquad e(\mathfrak{q}_i|\mathfrak{p}) = e_i$

The situations simplifies if

L/K Galois, $G := \mathrm{Gal}(L/K)$

⚠ G acts trans. on the primes above p, i.e. $\{\mathfrak{q}_1, \dots, \mathfrak{q}_g\}$

$$(\Rightarrow) \overset{e=}{e_1} = \dots = e_g,\ f_1 = \dots = f_g =: f$$

$$n = g \cdot e \cdot f \,/$$

Pick $\mathfrak{q} \mid p \cdot \mathcal{O}_L$ decomposition grp

$$1 \to I(\mathfrak{q}|p) \to \underset{\substack{\text{ij} \\ \mathrm{Stab}_G(\mathfrak{q}) \\ \shortparallel \\ \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}}}{D(\mathfrak{q}|p)} \to \underset{\substack{\shortparallel \\ \langle \mathrm{Frob}_q \rangle \cong \mathbb{Z}/f}}{\mathrm{Gal}\left(k(\mathfrak{q})/k(p)\right)} \to 1$$

$$\overset{=}{\#} e(\mathfrak{q}|p) \qquad \# = e \cdot f \qquad \overset{=}{\#} f(\mathfrak{q}|p)$$

If $\mathfrak{p}$ unram.

$\Rightarrow$ get $\sigma(\mathfrak{q}|\mathfrak{p}) \in G$ Frobenius

uniquely det. by $\sigma(x) \equiv x^{q} \ (\mathfrak{q})$

$\forall x \in \mathcal{O}_L$

$\sigma(\mathfrak{q}|\mathfrak{p})$ determines spl. beh. of $\mathfrak{p}$

Ex: $K = \mathbb{Q}(\zeta_N)$, $p \nmid N$

$$\Rightarrow \quad \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N)^{*}$$

$$\sigma(\mathfrak{q}|(p)) \mapsto p$$

$\rightsquigarrow$ can determine splitting beh. of primes in quadratic number fields

Prop. 7.5.1: $K = \mathbb{Q}(\sqrt{\Delta_K})$ quadr.,

$$K \subseteq \mathbb{Q}(\zeta_{\Delta_K})$$

$$\chi_K : \quad Gal(\mathbb{Q}(\zeta_{\Delta_K})/\mathbb{Q}) \twoheadrightarrow Gal(K/\mathbb{Q})$$

$$\begin{array}{ccc} \wr\wr & & \wr\wr \\ (\mathbb{Z}/\Delta_K)^\times & \longrightarrow & \{\pm 1\} \end{array}$$

given as follows

a) $\chi_K(-1) = \dfrac{\Delta_K}{|\Delta_K|} = (-1)^{r_2} = \begin{cases} 1, & K \text{ real} \\ -1, & K \text{ imag.} \end{cases}$

b) $\chi_K(2) = (-1)^{\frac{\Delta_K^2 - 1}{8}}$

if $2 \in (\mathbb{Z}/\Delta_K)^\times \Leftrightarrow \Delta_K \equiv 1\ (4)$

c) $\chi_K(p) = \underbrace{\left(\dfrac{\Delta_K}{p}\right)}_{\text{Legendre symbol}}$, p odd, $p \nmid \Delta_K$

$(a,p) = 1$

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & , a \text{ is a square mod } p \\ -1 & , a \text{ is not a square mod } p \end{cases}$$

$\Rightarrow$ Can eff. comp. splitting of primes in K, when combined with

Thm (Gauss reciprocity law)
p, q dist. odd primes

$$\Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right),$$ where

$$p^* = (-1)^{\frac{p-1}{2}} \cdot p = \begin{cases} p, & p \equiv 1\ (4) \\ -p, & p \equiv 3\ (4) \end{cases}$$

Used $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$