Def: A **number field** K is a character 0 field,

s.t. $[K:\mathbb{Q}]<\infty$

Egs:
- $\mathbb{Q}(\sqrt{n})$, $n \neq k^2$.
- $\mathbb{Q}(e^{\frac{2\pi i}{n}}) \subset \mathbb{C}$
- $\mathbb{Q}(\sqrt[3]{2}) = K \subset \mathbb{C}$, $K^{Gal} = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$ ★

Recall:

If $[L:k]<\infty$ an extension of a field.

$\#\,Aut(L/k) \leq [L:k]$.

L-normal iff "$=$"

$Aut(L/k)$ - Galois group of L/k, write $Gal(L/k)$

If L, K perfect (char 0 or finite field),

then $\#\,Hom_K(L, \bar{K}) = [L:k]$ ($\bar{K}$: algebraic closure.)

Lemma: Let K be an number field, Let $\alpha \in K$ fixed,

TFAE:

① $\mathbb{Z}[\alpha]$ is a finitely generated abelian group

② α satisfies a monic poly equation over $\mathbb{Z}$.

③ The minimal polynomial equation of α over $\mathbb{Q}$ is integral 整係數的

We call such α an **algebraic integer**.

$\frac{1}{2}$ 不是 algebraic integer, 因為 $\mathbb{Z}[\frac{1}{2}]$ 包含任意 $\frac{1}{2^n}$, 不是 finitely generated.

所以它叫 algebraic "integer"

Pf:
- ② ⇒ ③: trivial ✓ ★ 我們需要 minimal 是 monic 的.
- ③ ⇒ ①: Let $f(x) = x^n + \cdots \in \mathbb{Z}[x]$, $f(\alpha) = 0$

Note $\alpha^n \in span(1, \alpha, \cdots, \alpha^{n-1})_{\mathbb{Z}}$,

$\Rightarrow \alpha^{n+1} \in span(\alpha, \cdots, \alpha^n)_{\mathbb{Z}} \subseteq span(1, \alpha, \cdots, \alpha^{n-1})_{\mathbb{Z}}$

• ① ⇒ ③: Assume $\mathbb{Z}[\alpha]$ finitely generated, $\Rightarrow \exists\, r_1, \cdots r_k \in \mathbb{Z}[\alpha]$, s.t.

$\text{span}(r_1, \cdots, r_k)_{\mathbb{Z}} = \mathbb{Z}[\alpha]$.

Let $D = \max$ deg used in $\{r_i\}$, $\Rightarrow \mathbb{Z}[\alpha] = \text{span}(1, \cdots, r^D) \ni \alpha^{D+1}$

这是那个"第一项"

$\Rightarrow \exists$ monic (?) $f(x) \in \mathbb{Z}[x]$, s.t. $f(\alpha) = 0$

f 是 ℤ 里的 min, g 是 ℚ 里的, 我们假设它们不一样.

Let $g \in \mathbb{Q}[x]$ be the monic poly of $\alpha / \mathbb{Q}$.

这里的本质是 f 在 ℤ 上 irre. ⇒ 在 ℚ 上 irre. ?

$\therefore \exists$ monic $h(x) \in \mathbb{Q}[x]$, s.t. $g(x) h(x) = f(x)$. Assume $g \notin \mathbb{Z}[x]$.

这里总有某个分母有因子 p, 我们乘上足够的 p.

$\Rightarrow \exists$ prime p, s.t. p appears in the denominator of a coef of g.

分母上没 p.

Let $a, b \in \mathbb{Z}_{\geq 0}$ (min.), s.t. $p^a g(x)$, $p^b h(x)$ are integral @ p.

$\Rightarrow p^{a+b} f(x) = p^a g\, p^b h$

$\Downarrow$ reduce mod p

$\mathbb{F}_p[x]$

$\overline{0} = (\overline{p^a g(x)})(\overline{p^b h(x)})$ ≠ ≠ → 要不然可以消一 ? ☆ ✓

← 就是说我们取的 a, b 是最小的那两个. 如果 $p^a g(x) \equiv 0 \pmod p$ $\Rightarrow p^{a-1} g(x) \in \mathbb{Z}[x]$.

contradiction, integral domain.

Def: $O_K \subset K$ the sets of all algebric integers.

→ number field. 一个 ℚ 的 finite extension.

和 "ℤ 里的 algebric number" 的区别在于我们需要 minimal poly 是 monic 的.

Lemma: O_K is a ring.

Pf: Let $\alpha, \beta \in O_K$, $\Rightarrow \mathbb{Z}[\alpha], \mathbb{Z}[\beta]$ finitely generated.

$\Rightarrow \exists\, D > 0$, s.t. $\mathbb{Z}[\alpha] = \text{span}(1, \cdots, \alpha^D)$, $\mathbb{Z}[\beta] = \text{span}(1, \cdots, \beta^D)$.

$\mathbb{Z}[\alpha, \beta] = \langle \alpha^i b^j \mid i, j \geq 0 \rangle = \langle \alpha^i b^j \mid 0 \leq i, j \leq D \rangle$

$\Rightarrow \mathbb{Z}[\alpha, \beta]$ finitely generated abelian groups.

$\alpha + \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta] \Rightarrow \mathbb{Z}[\alpha+\beta], \mathbb{Z}[\alpha\beta] \subset \mathbb{Z}[\alpha, \beta]$

$\Rightarrow \alpha + \beta, \alpha\beta \in O_K$.

$a + b\sqrt{5}$ 显然, 因为 $\sqrt{5} \subset \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$

E.g. Let $K = \mathbb{Q}(\sqrt{5})$ $\Rightarrow O_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$

↑

$\frac{a}{2} + \frac{b}{2}\sqrt{5}$ (a, b odd)

可以用 $\frac{1+\sqrt{5}}{2}$, $\frac{1-\sqrt{5}}{2}$ 构造出来.

Let $\alpha = a + b\sqrt{5}$

$\bar{\alpha} = a - b\sqrt{5}$

$(x-\alpha)(x-\bar{\alpha}) = x^2 - 2ax + a^2 - 5b^2$

Need: $2a \in \mathbb{Z}$, $a^2 - 5b^2 \in \mathbb{Z}$.

$\Rightarrow$ $a \in \mathbb{Z}$, $b \in \mathbb{Z}$.

or $a + \frac{1}{2} \in \mathbb{Z}$, $b + \frac{1}{2} \in \mathbb{Z}$.

Trace and Trace pairing.

Recall: If L/k finite, $\alpha \in L$,

$\Rightarrow tr_{L/k}(\alpha) \in k$, $\begin{cases} x\alpha : L \to L \\ \sigma_1, \dots, \sigma_n : L \hookrightarrow \bar{k} \end{cases}$, $tr(x\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$ if L, k perfect

$x\alpha$: $L \to L$ of k-vector space; operator. 这是个 operator

$tr(x\alpha)$ 这是 operator 的 trace.

$\sigma_1, \dots, \sigma_n$: embeddings. $n = [L:k]$

Lemma: These two def are the same.

Pf: ① Assume $k(\alpha) = L$. Let $p(x)$ be the character polynomial of "$x\alpha$"

By Caley-Hamilton theorem, $P("x\alpha") = 0 \Rightarrow 0 = P("x\alpha") \cdot 1 \overset{\star}{=} P(\alpha)$

$\Rightarrow p(x)$ is the minimal poly of α/k. 因为 $k(\alpha) = L$, 所以 L/k 的 degree $= n$ 是这个 minimal.

$p(x) = x^n + a_1 x^{n-1} + \dots + a_n$

$p("x\alpha")(1) = (x\alpha)^n \cdot 1 + a_1 (x\alpha)^{n-1} \cdot 1 + \dots + a_n \cdot 1$

$= \alpha^n + a_1 \alpha^{n-1} + \dots + a_n$

$= P(\alpha)$

In $\bar{k}$, $P(x) \overset{\star}{=} \prod_{i=1}^{n} (x - \sigma_i(\alpha))$ σ_i permutes all roots. 所以 $\{\sigma_i(\alpha)\}$ 就是了所有的 root.

$= x^n - \left(\sum_{i=1}^{n} \sigma_i(\alpha)\right) x^{n-1} + \dots$

$\sum_{i=1}^{n} \sigma_i(\alpha) = tr("x\alpha")$

② General Case: Let $M = k(\alpha)$, $k \subset M \subset L$.

$tr_{M/k}("x\alpha") = \sum_{i=1}^{m} \tau_i(\alpha)$, where $m = [M:k]$, $\{\tau_i\}$ embeddings. $M \hookrightarrow \bar{k}$

- $tr_{L/k}("x\alpha")$ $L \cong M^{[L:M]}$ as k-vector space by picking an M-basis for L.

$= [L:M]\, tr_{M/k}("x\alpha")$

also as "$x\alpha$" modules.

- $\mathrm{Hom}(L, \bar{k}) \longrightarrow \mathrm{Hom}(M, \bar{k})$ is surjective with fibers of size $[L:M]$

$$\Rightarrow \sum_{i=1}^{n} \sigma_i(\alpha) = [L:M] \sum_{i=1}^{n} \tau_i(\alpha)$$

Norms: Let L/k be finite extension of perfect field, $\alpha \in L$,

Then $Nm_{L/k}(\alpha) \in k$

$\hookrightarrow$ $\det$ ("$\times\alpha$")

$\prod_{i=1}^{n} \sigma_i(\alpha)$, $\{\sigma_1, \cdots, \sigma_n\} = \mathrm{Hom}(L, \bar{k})$

Propersition: (Transitions between tr, Nm)

$k \subset M \subset L$, finite field extension $\alpha \in L$.

then $tr_{L/k}(\alpha) = tr_{M/k}(tr_{L/M}(\alpha))$

$Nm_{L/k}(\alpha) = Nm_{M/k}(Nm_{L/M}(\alpha))$

Pf:

Trace paring: Given L/k finite get a symmetric paring on L as a k-vector space, $Q(\alpha,\beta) = tr_{L/k}(\alpha\beta)$

Propersition: Assume L, k char 0.

(1) Q is non-degenerate 并非值为0的元素吧?

(2) $tr_{L/k}(O_L) \subset O_k$.

(3) If $k = \mathbb{Q}$, $\alpha, \beta \in O_L$.

then $Q(\alpha,\beta) \in \mathbb{Z}$.

pf: (1) If $\alpha \neq 0$, $\mathbb{Q}(\alpha, \alpha^{-1}) = tr_{L/K}(1) = [L:K] \neq 0$

(2) If $\alpha \in O_L$, $tr_{L/K}(\alpha) = \sum_{\sigma \in Hom(L,\bar{K})} \sigma(\alpha) \in O_L$. (why σ fix K?)

这里相当于要证 $\alpha \in O_L \Rightarrow \sigma(\alpha) \in O_L$.

Now, $O_L \cap K = O_K$.

☆ $P(\alpha) = 0 \Rightarrow \sigma(P(\alpha)) = 0 \Rightarrow \sigma(\alpha^n) + \sigma(a_{n-1}\alpha^{n-1}) + \cdots + \sigma(a_0) = 0$

$\sigma(a_{n-1}) = a_{n-1}$? $\Rightarrow \sigma^n(\alpha) + a_{n-1}\sigma^{n-1}(\alpha) + \cdots = 0$

$\Rightarrow P(\sigma(\alpha)) = 0$.

(3) √ $O_{\mathbb{Q}} = \mathbb{Z}$. $\mathbb{Q}(\alpha,\beta) = tr_{L/\mathbb{Q}}(\alpha\beta) \in tr_{L/\mathbb{Q}}(\alpha\beta) \subseteq O_{\mathbb{Q}} = \mathbb{Z}$.

K – # field, $O_K \subset K$

Trace paring: $\mathbb{Q}: K \times K \longrightarrow \mathbb{Q}$

$\mathbb{Q}(\alpha, \beta) = tr_{K/\mathbb{Q}}(\alpha\beta) \to \in \mathbb{Q}$

因为 $tr_{L/K}(\alpha) = tr(x_\alpha)$ where $x_\alpha: L \to L$, L as vector space of K. so $\in K$

Lemma: $O_K \subset K$ is a lattice. i.e.

① O_K spans K over $\mathbb{Q}$

② $O_K \cong \mathbb{Z}^{[K:\mathbb{Q}]}$ as free abelian group

K是$\mathbb{Q}$的某个 finite extension, 说明K里全都是"algebric decimals". 我们要说明的是每个"algebric decimals"乘上一个足够大的整数后就变成"algebric integers"了.

"free group"是 generator 们组成的所有 word, 加上 abelian 后就可以 permute 顺序, 所以可以 $\cong \mathbb{Z}^n$..

Pf: ① Let $\alpha \in K$, $\exists a_0 \cdots a_n \in \mathbb{Z}$,

s.t. $\sum_{i=0}^{m} a_i \alpha^i = 0$, $m \geq 1$, $a_m \neq 0$

$\Rightarrow \sum_{i=0}^{m} \frac{a_i (N\alpha)^i}{N^i} = 0$.

$\Rightarrow \sum_{i=0}^{m} N^{m-i} a_i (N\alpha)^i = 0$, let $N = a_m$, divide a_m

$\Rightarrow \sum_{i=0}^{m} \frac{a_m^{m-i}}{a_m} a_i (a_m\alpha)^i = 0$ → a monic polynomial.

$\Rightarrow a_m \alpha \in O_K$. ☆ √

② Let $\alpha_1, \cdots, \alpha_n$ be a $\mathbb{Q}$ basis for K. 因为 $K/\mathbb{Q}$, K是个$\mathbb{Q}$-vector space, $\alpha_i \in K$.

By scaling, assume $\alpha_i \in O_K$.

定义!!! 所以定义在$\mathbb{Z}$.

Def $L = \langle \alpha_1, \cdots, \alpha_n \rangle_{\mathbb{Z}}$. $\subseteq O_K$ since O_K is a ring.

☆ why this L^*? $L^* = \{ b \in K : \forall l \in L, \mathbb{Q}(b, l) \in \mathbb{Z} \} \supseteq O_K$, since $\mathbb{Q}(O_K, O_K) \subseteq \mathbb{Z}$ ($\hookrightarrow O_K$)

then $L^* \supset O_K \supset L$. ← free-abelian group of rank n ($L^* \cong Hom(L, \mathbb{Z})$)

$L^* = L$ since $L \cong \mathbb{R}^n$?

free abelian group of rank n.

E.g.: $K = \mathbb{Q}(\sqrt{5})$

$L = \langle 1, \sqrt{5} \rangle_{\mathbb{Z}}$.

L^* : $b = r + s\sqrt{5}$ $(r, s \in \mathbb{Q})$

(the only embedding is conjugacy.)

$tr(b, 1) = 2r = tr(r+s\sqrt{5}) = (r+s\sqrt{5}) + (r - s\sqrt{5}) = 2r$.

$tr(b, \sqrt{5}) = 10 \cdot s = tr(\sqrt{5}r + 5s) = 10s$.

$\Rightarrow L^* = \langle \frac{1}{2}, \frac{\sqrt{5}}{10} \rangle_{\mathbb{Z}} \neq L^*$ ☆?

$\frac{1}{\sqrt{5}} \in O_K^*$, $O_K^* \neq O_K$. why?

Archimedean embeddings of O_K:

Let K a # field, $[K:\mathbb{Q}] = n$, $\# \mathrm{Hom}(K, \mathbb{C}) = n$. ☆

r_1 : # real embeddings $\sigma_1, \cdots \sigma_{r_1}$

$2r_2$: # complex embeddings $\tau_1 \cdots \tau_{r_2}, \bar{\tau}_1, \cdots, \bar{\tau}_{r_2}$.

Consider $\sigma : K \hookrightarrow \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ $(\cong K \otimes_{\mathbb{Q}} \mathbb{R})$

$\alpha \longmapsto (\sigma_1(\alpha), \cdots, \sigma_{r_1}(\alpha), \tau_1(\alpha), \cdots, \tau_{r_2}(\alpha))$

$\sigma(K)$ 里面是一堆形如 的向量. 想说明的是 span.

Prop: ① $\langle \sigma(K) \rangle_{\mathbb{R}} = \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ ($\mathbb{Z}$?)

② $\sigma(O_K)$ is a lattice inside $\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$

$\Rightarrow$ 1) $\sigma(O_K) < \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ is discrite

$\Updownarrow$ i.e., $\exists \varepsilon > 0$, s.t. $B(0, \varepsilon) \cap \sigma(O_K) = \{0\}$

2) $\langle \sigma(O_K) \rangle_{\mathbb{R}} = \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$

E.g. ① $K = \mathbb{Q}(\sqrt[3]{2})$, $r_1 = 1$, $r_2 = 1$, $r_1 + 2r_2 = 3$.

$\sigma_1 = \sqrt[3]{2} \to \sqrt[3]{2}$.

$\sigma_2 : \sqrt[3]{2} \to \sqrt[3]{2} e^{\frac{2\pi i}{3}}$

$\sigma : K \hookrightarrow \mathbb{R} \oplus \mathbb{C}$

$1 \longmapsto (1, 1)$

$\sqrt[3]{2} \longmapsto (\sqrt[3]{2}, \sqrt[3]{2} e^{\frac{2\pi i}{3}})$

$\sqrt[3]{4} \longmapsto (\sqrt[3]{4}, \sqrt[3]{4} e^{\frac{4\pi i}{3}})$

③ $\langle (1,1), (\sqrt{2}, \sqrt{2}) \rangle_{\mathbb{Z}} < \mathbb{R}^2$

<u>Lemma:</u> Let $L < \mathbb{R}^n$ be $L \cong \mathbb{Z}^n$, TFAE:

① L is discrete → "每一个方向上只有一个L的元素"

② $\langle L \rangle_{\mathbb{R}} = \mathbb{R}^n$ ↙ 这意味着"L占满了每个方向"

<u>Pf:</u> ② → ① : Suppose $\langle L \rangle_{\mathbb{R}} = \mathbb{R}^n$,

let $l_1, \cdots, l_n$ be a $\mathbb{Z}$-basis for L.

$\Rightarrow \exists$ invertible matrix $A \in GL_n(\mathbb{R})$, s.t.

$A = (a_{ij})$, $\sum_j a_{ij} l_j = e_i$ (standard basis)

Let $v = (v_1, \cdots, v_n) \in \mathbb{Z}^n$

Then $\sum_{i=1}^n v_i l_i = \sum_{i=1}^n w_i e_i$, where

where $w = A^{-1} \cdot v$

$\Rightarrow v = Aw \Rightarrow \|w\| \geq \frac{\|v\|}{n\|A\|}$ (where $\|v\| = \max(|v_i|)$)

① → ② : "$\neg$② ⇒ $\neg$①"

Suppose $\langle l_1, \cdots, l_n \rangle_{\mathbb{R}} \neq \mathbb{R}^n$

$\Rightarrow \exists \sum_{i=1}^n a_i l_i = 0$, $\vec{a} = (a_i) \neq 0$

By Dirichlet's Box principle: $\forall \varepsilon > 0$, $\exists N > 0$, $|N \cdot a_i - [N a_i]| < \varepsilon$.

$\Rightarrow \sum_{i=1}^n N a_i l_i = \underbrace{\sum_{i=1}^n [N a_i] l_i}_{\in L} + \underbrace{\sum_{i=1}^n \{N a_i\} l_i}_{\in B_\varepsilon}$

Week 2:

K - # field, $[K : \mathbb{Q}] = n = r_1 + 2r_2$,

$\sigma : K \to \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ 这里说的是虽然 O_K 作为一个field很稠密，但 O_K 很稀疏.

Thm: $\sigma(O_K) < \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ is a lattice. → 这个东西 literally 就是"布满所有

Pf①: $\sigma(O_K)$ is discrete. 方向的晶格"，所以说稀疏且相当于 $\mathbb{Z}^n$. all finite extension is algebraic.

Note $\text{norm}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{r_1}\sigma_i(\alpha)\cdot\prod_{j=1}^{r_2}|\tau_j(\alpha)|^2 \in \mathbb{Q}$ → 所以这个是 minimal poly 的常数项的平方之类的，$\in \mathbb{Q}$. （K.）

$\alpha \in O_K \Rightarrow \text{norm}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ → 同理，in $\mathbb{Z}$. $\alpha \in O_K \setminus \{0\}$

$\Rightarrow \text{norm}_{K/\mathbb{Q}}(\alpha) \geq 1$

$\Rightarrow |\sigma_i(\alpha)| \geq 1$ for some σ_i

Cor: $B \subset \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2} = \{(\alpha_i),\ |\alpha_i|<1\}$

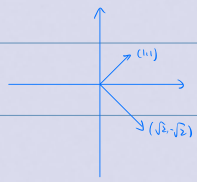
$B \cap O_K = \{0\}$.

e.g. $K = \mathbb{Q}(\sqrt{2})$ $\sigma_1 = \text{id}$, $\sigma_2 = \sqrt{2} \to -\sqrt{2}$.

$O_K = \langle 1, \sqrt{2}\rangle$.

$1 \mapsto \begin{pmatrix}1\\1\end{pmatrix}$

$\sqrt{2} \to \begin{pmatrix}\sqrt{2}\\-\sqrt{2}\end{pmatrix}$



Pf②: 这里就是在证 $\langle \sigma(O_K)\rangle_{\mathbb{R}} = \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$

$\langle \alpha_1, \cdots, \alpha_n\rangle_{\mathbb{Z}} = O_K$.

want: $\text{span}\big((\sigma_1(\alpha_j), \cdots, \tau_{r_2}(\alpha_j))_{j\in\{1,2,\cdots,n\}}\big) = \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$.

$\Leftrightarrow$ row span $A = \begin{pmatrix} \sigma_1(\alpha_1) \cdots \sigma_{r_1}(\alpha_1), \text{Real}(\tau_1(\alpha_1)), \text{Im}(\tau_1(\alpha_1)), \cdots, \text{Im}(\tau_{r_2}(\alpha_1)) \\ \vdots \end{pmatrix} = \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$.

$\Leftrightarrow \det(A) \neq 0$ ↓ 想证 ↓ 相邻两列加减，只差常数倍.

$\Leftrightarrow \det\begin{pmatrix} \sigma_1(\alpha_1) \cdots \sigma_{r_1}(\alpha_1), \tau_1(\alpha_1), \overline{\tau_1(\alpha_1)}, \cdots, \tau_{r_2}(\alpha_1), \overline{\tau_{r_2}(\alpha_1)} \\ \vdots \end{pmatrix}$

- Pick $\alpha \in K$, s.t. $\mathbb{Q}(\alpha) = K$ α是"那个数"！所以有

By scaling, wlog, $\alpha \in O_K$. 前面说的"algebric decimals"

$\langle 1, \alpha, \cdots, \alpha^{n-1}\rangle_{\mathbb{Z}} \subset O_K$ with finte index.

set $\alpha_i = \alpha^{i-1}$ 这里是在找出 $\mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$ 的那些 basis".

$\Rightarrow \det(\quad) = \prod_{\sigma\neq\sigma'\in \text{Hom}(K,\mathbb{C})}(\sigma(\alpha)-\sigma'(\alpha))$ Vandermond

因为 $\sigma_i(\alpha^k) = (\sigma_i(\alpha))^k$ 所以是这个形式

$\det\begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ & & \vdots & & \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} = \prod_{i\neq j}(x_i - x_j)$

高斯消元可推

好像贝转置后的行列式，但 det 不变.

$\neq 0$ 因为 $\forall \sigma, \sigma'$, $\sigma(\alpha) \neq \sigma'(\alpha)$

Pf ③: Let $R: \langle \sigma(K) \rangle_{\mathbb{R}}$.

$\Rightarrow R \subseteq \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ $\mathbb{R}$-subalgebra.

Fact: the only $\mathbb{R}$-subalgebras are given by setting

(i) complex-coordinate equal

(ii) complex-coordinate real

(iii) complex-coordinate conjugate.

Discriminant:

Def: Let $\langle \alpha_1, \cdots, \alpha_n \rangle_{\mathbb{Z}} = O_K$

上面的矩阵.

Let $M = (\sigma(\alpha_i))_{\substack{i \in \{1,\cdots,n\} \\ \sigma \in \mathrm{Hom}(K,\mathbb{C})}}$ 找 O_K 的 basis 放进 embedding 形成 M 算 det.

$D_K = (\det M)^2$ (complex) 不加 ^{2} 会在 sign 上出问题（排列如果交换顺序会有问题）

Claim: $D_K \in \mathbb{Z} \setminus \{0\}$

$\mathrm{sign}(D_K) = (-1)^{r_2}$.

e.g.: $K = \mathbb{Q}(\sqrt{d})$

$d = 2$: $\det \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix}^2 = 8$

$d = -2$. $\det \begin{pmatrix} 1 & 1 \\ \sqrt{-2} & -\sqrt{-2} \end{pmatrix}^2 = -8$

$d = \mathbb{Q}(\sqrt[3]{2})$

$$\det \begin{pmatrix} 1 & 1 & 1 \\ \sqrt[3]{2} & w\sqrt[3]{2} & w^2\sqrt[3]{2} \\ \sqrt[3]{4} & w\sqrt[3]{4} & w\sqrt[3]{4} \end{pmatrix}^2 = 4 \det \begin{pmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{pmatrix}^2$$

$$= 4 \big(\underbrace{(w-1)}_{-3w} \underbrace{(w-w^2)}_{-3} \underbrace{(w^2-1)}_{-3w^2} \big)^2 = -108.$$

Pf ①: Galois theory: ↗ Galois group 是包含 K 的最小的 galois group，就是把 K 里元素的 min. poly 的所有根都加进去.
($\mathbb{Q}(\sqrt[3]{2})$ 为例)

Let $L = K^{Gal}$, $G = \mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Aut}(L/\mathbb{Q})$

note that ① G acts on $\mathrm{Hom}(K, \mathbb{C})$ $g \circ \sigma_i(\alpha) = \sigma_i(g\alpha)$

抄错了吧… $\mathcal{O}_L$?

② $D_K \in L$.

Let $g \in Gal(L/\mathbb{Q})$. $(g(\det(M)))^2 = (\det(gM))^2 = (\det(\sigma^g(\alpha_i)))^2 = \det(M)^2$ 这意味着 $\det M$ 在 G 的作用下保持不变, 所以 $\det M \in \mathbb{Q}$ (因为 $G/\mathbb{Q}$)

($= g(\det(M))^2$ ← automorphism; g permutes σs.)

$\Rightarrow \det(M)^2 \in \mathbb{Q}$ (fixed by Galois groups)

Also, $D_K \in \mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z} \Rightarrow \det(M)^2 \in \mathbb{Z}$.

Pf②: trace paring

$$\det(M)^2 = \det(M \cdot M^t) = \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \vdots & & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}$$

ij th entry: $\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = tr_{K/\mathbb{Q}}(\alpha_i\alpha_j)$ ($\in \mathcal{O}_\mathbb{Q} = \mathbb{Z}$.)

$= \det(tr_{K/\mathbb{Q}}(\alpha_i\alpha_j))$ ($\in \mathbb{Z}$.)

同理之前那个证明 $tr_{L/K}(\mathcal{O}_L) \in \mathcal{O}_K$.

$\alpha \in \mathcal{O}_L \Rightarrow \sigma(\alpha) \in \mathcal{O}_L \Rightarrow \sum \sigma(\alpha) \in \mathcal{O}_L$. ($= tr(\alpha)$)

因为 $P(\alpha)=0 \Rightarrow \sigma(P(\alpha))=0$
$\Rightarrow P(\sigma(\alpha))=0$.

然后 $tr(\alpha) = tr(\text{"}x_\alpha\text{"})$ ← 在 K 中的.

$\Rightarrow tr(\alpha) \in K \cap \mathcal{O}_L = \mathcal{O}_K$.

Pf (sign): (? 后正确)

$$\left(\sigma_1 \cdots \sigma_{r_1}\ \tau_1, \bar{\tau}_1, \cdots, \tau_{r_2}, \bar{\tau}_{r_2}\right) = \frac{1}{(2i)^{r_2}} \det\left(\sigma_1 \cdots \sigma_{r_1}, Re\,\tau_1, Im\,\tau_1, \cdots, Re\,\tau_{r_2}, Im\,\tau_{r_2}\right)$$

sign comes from here.

Falinre of UFD: $\mathbb{Z}[\sqrt{-6}]$ $6 = 2\cdot 3 = \sqrt{-6}(-\sqrt{-6})$

UFD of Ideals: $I_2 = (2, \sqrt{-6})$, $I_3 = (3, \sqrt{-6})$

$I_2^2 = (2)$, $I_3^2 = (3)$, $I_2 I_3 = (\sqrt{-6})$

$IJ = \left\{ \sum^{\text{finite}} i_k j_k \mid i_k j_k \in I, J \right\}$. 但这种东西好像拿 generator 们乘起来就行?

Noetherants:

Def: A R-module M is noetherian if every increasing chain of submodules stabilizes: Noe 本身没说是 R-module 上的.

i.e, $M_1 \subset \cdots \subset M_k \subset M_{k+1} \subset \cdots \Rightarrow M_t = M_{t+1}$ for $t > T$.

e.g. $\mathbb{Z}$ ✓, $\mathbb{C}[x]$ ✓, fields ✓ ($\mathbb{Z}$, $\mathbb{Z}^{\mathbb{N}}$) ✗

判断可表示及Noe 实际看是否所有submodule有限生成.

Lemma: M is Noe $\Leftrightarrow$ every submodule of M is finite. gene..

pf: "$\Rightarrow$" Let $N \subset M$, N not f.g. 如果不f.g.我们总是不停地加generator进去即可.

$N_0 = \{0\}$, $N_{i+1} = \langle N_i, \alpha \rangle_R$, contradiction.

"$\Leftarrow$" Let $M_1 \subset \cdots \subset M_k \subset \cdots$,

Let $N = \cup M_i$ submodule, $N = \langle n_1, \cdots, n_k \rangle_R$.

$\Rightarrow \exists T > 0$, $\{n_1, \cdots, n_k\} \subseteq M_T$.

Def: A ring R is Noe. if R is a Noe. R-module.

Lemma: Let R be a ring,

$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$ exact sequence of R-modules

M Noe $\Leftrightarrow$ L, N Noe.

pf: "$\Rightarrow$" $L \subset M$ noetherian.

$\{\text{submodules of } N\} \xrightarrow{A \to g^{-1}(A)} \{\text{submod of } M\}$

N Noe ☆

"$\Leftarrow$" $M_1 \subset M_2 \subset \cdots \subset M_k \subset \cdots$

for $k > T$, $M_k \cap L = M_{k+1} \cap L$, $g(M_k) = g(M_{k+1})$

$\Rightarrow M_k = M_{k+1}$ ☆

Cor: if R Noe, then R-module M Noe. iff M finite. gene.

Thm: R is Noe. $\Rightarrow R[x]$ Noe.

(Cor: finitely generated algebras of Noe rings are Noe)

pf: Let $I \subset R[x]$ be an ideal (submodule), show f.g.

Define $J = \{a \in R,\ ax^n + \cdots \in I\}$

(R 是 Noe.)

Then J is an ideal. $\Rightarrow$ J finitely generated. $J=(j_1,\cdots,j_s)$

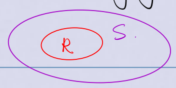
Let $N\in\mathbb{N}$, s.t. all j_i occur as leading-coef of an $i\in I$, $\deg(i)=N$.

Let $(i_1,\cdots,i_s)$ be the polynomials

$\therefore I=(i_1,\cdots,i_s)+(I\cap R[x]_{\deg<N})$ → R-submodule of R^N

$\Rightarrow$ finitely generated.

Def: Let $R\subset S$ be domains, we say R is **integrally closed** in S if every $s\in S$ satisfying a monic polynomial over R is itself in R.



任何R里 monic poly 的根都在R里 (只要在S里就) ← 这个很重要的.

但主要是不该任意 monic poly 在S里有根.

Def: A **dedeking domain** is a ring R, s.t.

① R is noetherian 没有 infinite chain (所有 submodule 都有限生成)

② R is a domain 没有 zero divisor.

③ R is integrally closed in $\mathrm{Frac}(R)$ 如果 monic $P(\frac{\alpha}{\beta})=0$ $\Rightarrow$ $\frac{\alpha}{\beta}\in R$.

④ Every non-zero prime ideal is maximum.

一般有的是 maximal $\Leftrightarrow$ prime. 这里加上了反向的箭头

Lemma: If K a # field, then O_K is a dedeking domain.

Pf: ① O_K is a finitely generated $\mathbb{Z}$-algebraic. ☆

② $O_K\subset K$ (field.) field 里是没有 zero divisor 的, 所以子集里也没有.

③ $\mathrm{Frac}(O_K)=K$.

Let $\alpha\in K$, suppose $P(x)\in O_K[x]$ (monic, deg n), $P(\alpha)=0$

$\alpha^N\in\langle 1,\alpha,\cdots,\alpha^{N-1}\rangle_{O_K}$.

$\Rightarrow$ $O_K(\alpha)$ is a finitely generated O_K module.

$\Rightarrow$ a finitely generated $\mathbb{Z}$ module.

$\Rightarrow$ $\alpha\in O_K$.

⊕ Let $P \subseteq O_K$ a non-zero prime ideal.

Let $\alpha \in P \setminus \{0\}$ (index finite?)

$O_K/P \hookleftarrow O_K/(\alpha)$ (finite since $\det(\text{"}x\alpha\text{"}) \neq 0$)

$\Rightarrow O_K/P$ a finite integral domain, $\Rightarrow$ field.

Lemma: PID $\Rightarrow$ Dedekind domain

Pf: Suppose R PID,

(1) Principle ideals are finitely generated, therefore noetherian.

(2) WTS: Prime ideal $\Rightarrow$ Maximal

Let $P \subset R$ be a $\neq \emptyset$ prime ideal,

Assume $Q \subset R$ is maximal, $P \subsetneq Q$

So $P = (p)$, $Q = (q)$. $q \in P$.

$P \subsetneq Q \Rightarrow p = qr \Rightarrow r \in P$ (prime) $\Rightarrow r = pu$

$\Rightarrow p = p \cdot q \cdot u \Rightarrow 1 = qu \Rightarrow Q = R$. ✗.

(3) Let $K = \mathrm{Frac}(R)$ $\alpha \in K$, integral over R,

$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$, $a_i \in R$.

$\alpha = \frac{r_1}{r_2} \Rightarrow r_1^n + a_1 r_1^{n-1} r_2 + a_2 r_1^{n-2} r_2^2 + \cdots + a_n r_2^n = 0$

$\Rightarrow r_1^n \in (r_2) \Rightarrow (r_1, r_2)^n \in (r_2)$

$(r_1, r_2) = (r_3)$ for some $r_3 \in R$.

$\Rightarrow r_1 \to \frac{r_1}{r_3}$, $r_2 \to \frac{r_2}{r_3}$. So WLOG, $(r_1, r_2) = R < (r_2)$

$\Rightarrow r_2 \in R^\times$, $\Rightarrow \alpha \in R$

Def: A fractional ideal is a finitely generated R-submodule of K. e.g. $\frac{1}{2}(\mathbb{Z}) < \mathbb{Q}$

↳ dedekind domain

↳ Frac(R)

K 里分数们，它们形为 R-submodule. 也就是说对分数加法和整数乘法封闭.

U 对 ideal

Lemma: Every fractional ideal is of the form $r^{-1}I$, $r \in R \setminus \{0\}$, $I \subset R$ ideal.

要满足个 "ideal". 像"分数乘法" ⇒ "分数和整数乘法"

所以我的理解是这里的 r^{-1} 是"最大的那个分母".

Addendum: If $R = \mathcal{O}_K$, can take $r \in \mathbb{Z}$.

看吧，巨大分母.

Let $I_R = \{$non-zero fractional ideals$\}$

Thm: I_R is a group under multiplication with identity $= R$.

"ideal" 间的乘法.

封: $(r_1^{-1}I_1)(r_2^{-1}I_2) = (r_1r_2)^{-1}I_1I_2 \in I_R$.

结: trivial

幺: $(r^{-1}I)R = r^{-1}I$.

$\subseteq$ fractional ideal 的定义 ("对整数乘法 close")

$\supseteq$ 取 $1 \in R$.

Eg: • $I_{\mathbb{Z}} \cong \mathbb{Q}_+^\times$ $(q) \mapsto q$. $q \in \mathbb{Z}$.

• Assume R PID (dedekind), then $I_R \cong K^\times / R^\times$

可以反到个逆.

Pf: (1) Only need to prove invertible.

$\forall$ non-zero $I \subset R$, $\exists P_1, \cdots, P_n$, non-zero prime ideals, s.t.

$I \supset P_1P_2\cdots P_n$.

Pf: Suppose not, let I be maximal such.

Now, I is not prime, so $\exists a, b \in R$, $a, b \notin I$,

s.t. $ab \in I$. $\Rightarrow I \supset (I, a)\cdot(I, b)$, contradiction.

$<I$ $<I$

反证 $P_1 = I$.

• prime ideals are invertible.

pf: Take an non-zero $\beta \in P$, prime

$P_1 \cdots P_m < (\beta) \leq P$, pick m minimal.

因为 P prime, 所以 $m = 1$.

WLOG, $P_1 = P$.

Pick $\gamma_2 \in P_2$, $\gamma_m \in P_m$, s.t. $\gamma_2\gamma_3\cdots\gamma_m \notin \beta$ $\quad \gamma = \gamma$

$\Rightarrow \gamma \in (\beta)$, $\gamma P < (\beta) \Rightarrow \frac{\gamma}{\beta} P < R$

elements of K.

Consider $I = (1, \frac{\gamma}{\beta})$, $P < IP < R$ 没有个等号. $\frac{\gamma}{\beta} \notin R$.

if $IP = R$, done.

Suppose $IP = P \Rightarrow \frac{\gamma}{\beta} \cdot P = P$

Say $P = (a_1, \cdots, a_k)_R$, $\frac{\gamma}{\beta} a_i = \sum_j m_{ij} a_j$

因为这是个 P 里的元素.

integrally closed.

$\det(\frac{\gamma}{\beta} I - M) = 0 \Rightarrow \frac{\gamma}{\beta} \in R$

• Every Ideal has inverse:

Pf: Assume not, and assume I maximal.

$\Rightarrow \exists$ prime ideals $P \supset I \Rightarrow R \supset IP^{-1}$

① if $IP^{-1} \neq I$, ✓ (maximal)

② if $IP^{-1} = I$,

Contradiction.

Clarification:

R - dedekind domain

$K = \mathrm{Frac}(R)$

$I < K$ fractional ideal

Lemma: if $t \in K$, $tI \in I$ ($\forall I$), then $t \in R$.

Pf: $\varphi : R^n \twoheadrightarrow I$ as R-modules.

$t : I \to I$, $t \in \mathrm{Hom}_R(I, I)$

$\downarrow t$ $\quad \uparrow \varphi \circ$ $\quad \mathrm{Hom}_R(R^n, I)$

$\alpha \in \mathrm{Hom}_R(R^n, R^n)$ $\quad \uparrow$ Lift

"Lift": $R^n \twoheadrightarrow I$

$\uparrow \quad \nearrow \uparrow t$

$R^n \to I$

poly

$(\det(xI - \alpha))(\omega) = 0$

$\Rightarrow (\det(xI - \alpha))(t) = 0.$

Cor: I, J — fractional ideals,

Say $I \mid J$ if $JI^{-1} < R$. TFAE

("actual ideal")

$I \neq 1$, $I \neq I$

$JI^{-1} = \pm(qI^{-1}) = \exists R < R$.

① $I \mid J$ 越细的 fractional ideal 含整除退得的 fractional ideal

② $I \supset J$. 与数的整除是反过来的，含有越多素的 frac. ideal 含整除含有越少素的 frac. ideal.

Pf: ① $\Rightarrow$ ②:

$JI^{-1} < R \Rightarrow I \cdot (JI^{-1}) < I \cdot R \Rightarrow J < I.$

② ⇒ ①

$I \supset J \Rightarrow II^{-1} = R \supset JI^{-1}$

fractional ideal 可以在乘法意义下构成以 R 为 identity 的 group.

Thm: Every $\neq 0$ ideal $I \subset R$ can be uniquely expressed as a product of prime ideals up to permutation.

Pf: **Existance:** Let I be a maximal ideal that not a product of primes, then $I \neq R$, $\exists$ prime ideal $P \supset I$.

maximal 和 prime 意味着 minimal?

$\Rightarrow R \supset IP^{-1} \supsetneq I$

$\Rightarrow IP^{-1} = \Pi$ prime (maximality)

$\Rightarrow I = P \cdot \Pi$ prime.

Uniqueness: Assume not, $P_1 \cdots P_m = Q_1 \cdots Q_n$, m minimal,

Since $Q_1 \cdots Q_n \subset P_1$, $\exists Q_i \subset P_1$, $\Rightarrow Q_i = P_1$ (wlog, prime, max.)

$\Rightarrow P_2 \cdots P_m = Q_2 \cdots Q_n$, contradiction.

Cor: Every non-zero fraction ideal is uniquely a product of finitely many integer powers of primes.

Pf: **Existance:** Let $I \subset k$ $\neq 0$ frac ideal

Let $I = rJ$, $J \subset R$.

$J = \Pi$ primes, $(r) = \Pi$ primes. (inverse)

Uniqueness: 未完待续 power 变成 actual ideal.

Cor: (Chinese Remainder Theorem)

Suppose $I = \prod_{i=1}^{m} p_i^{e_i}$, p_i distinct, $e_i > 0$

$\psi: R/I \to \prod_{i=1}^{m} R/p_i^{e_i}$ is an isomorphism. (isomorphism)

Pf: Injectivity: Let $\psi: R \to \prod_{i=1}^{m} R/p_i^{e_i}$, $k = \ker(\psi)$

So $K = \bigcap_{i=1}^{m} P_i^{e_i}$

Write $K = \prod_{i=1}^{m} P_i^{d_i} \cdot \prod_{j=1}^{n} Q_j^{f_j}$, $f_j > 0$.

$K \subset P_i^{e_i} \Leftrightarrow P_i^{e_i} \mid K \Rightarrow e_i \le d_i$

So $K = \prod_{i=1}^{n} P_i^{e_i} = I$.

K the largest ideal satisfying

Surjectivity: Let $e_i = (0,0,\dots,\underset{i\text{th}}{1},\dots,0)$ // ith diagonal entry

Need: find $\alpha \in R$, s.t.

$$\begin{cases} \alpha \equiv 1 \pmod{P_i^{e_i}} & \text{wlog, } i=1. \\ \alpha \in P_j^{e_j} & j \neq i \end{cases}$$

Consider $H = \prod_{j>1} P_j^{e_j}$

$P_1 \nmid H \Rightarrow H \notin P_1$.

$\Rightarrow \exists \beta \in H \setminus P_1$, $\beta \in P_j^{e_j}$.

$\Rightarrow (\beta, P_1) = R$.

$\Rightarrow (\beta, P_1)^e = R$.

$\Rightarrow \exists \alpha \in R$, $\beta \mid \alpha$, $\alpha \in P_j^{e_j}$, $\alpha \equiv 1 \pmod{P_1^{e_1}}$

Cor: Every (fractional) ideal in R is generated by most 2 elements.

Pf: Let $I \subset R$, $I \neq \{0\}$.

take $\alpha \in I \setminus \{0\}$

Consider $I = \prod P_i^{e_i}$ ($e_i \ge 0$), $(\alpha) = \prod P_i^{d_i}$

$\Rightarrow d_i \ge e_i$

Pick $r_i \in P_i^{e_i} \setminus P_i^{e_i+1}$ $\quad \beta \in P_i^{e_i} \Rightarrow P_i^{e_i} \mid (\beta)$

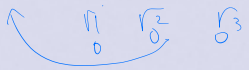
By CRT, take $\beta \in R$, s.t. $\beta \equiv r_i \bmod P_i^{e_i+1}$. $\forall i$

$(\beta) = \prod_{i=1}^{m} P_i^{e_i} \prod_{j=1}^{n} Q_j^{f_j}$ $\quad P_i^{e_i+1} \nmid (\beta)$

$(\alpha, \beta) \subset P_i^{e_i} \setminus P_i^{e_i+1}$ $\quad \beta \not\equiv$

$P/2 \cong P/P_3^{e_3} \cdots$

$(\alpha, \beta) \nsubseteq \mathcal{O}_j$ (as)



$\Rightarrow (\alpha, \beta) = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i} = I$.

GCD, LCM

$I, J, \neq 0$ fractional ideals.

Def: $GCD(I,J)$ = smallest fractional ideal containing I, J.

$LCM(I,J)$ = Largest fractional ideal contained in I, J.

$LCM(I,J) = I \cap J$.

$GCD(I,J) = I + J$.

If $I = \prod \mathfrak{p}_i^{e_i}$, $J = \prod \mathfrak{p}_i^{f_i}$ $e_i, f_i \in \mathbb{Z}$. (≤ 0 maybe)

Then $GCD(I,J) = \prod \mathfrak{p}_i^{\min(e_i, f_i)}$

$LCM(I,J) = \prod \mathfrak{p}_i^{\max(e_i, f_i)}$

$\Rightarrow I \cdot J = LCM(I,J)\, GCD(I,J)$

$= (I \cap J)(I + J)$

Class Group:

Def: $J_R :=$ (non-zero fractional ideals)

$\alpha \mapsto (\alpha)$ (kernels)

Class group of R.

$0 \to R^\times \to K^\times \to J_R \to Cl(R) \to 0$.

exact sequence

Thm: If K is a # field, $\underbrace{Cl(\mathcal{O}_K)}_{Cl(K)}$ is finite.

Lemma: If $\mathfrak{p} \subset R$ prime ideal, $\beta \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$.

(Dedekind domain)

$\therefore \psi : R/\mathfrak{p} \xrightarrow{\times \beta} \mathfrak{p}^n/\mathfrak{p}^{n+1}$ is an (R-module) isomorphism.

Pf: inj: Consider $\psi : R \xrightarrow{\times \beta} \mathfrak{p}^n/\mathfrak{p}^{n+1}$

$\ker(\psi) \supset \mathfrak{p}$, $\ker(\psi) \neq R \Rightarrow \ker(\psi) = \mathfrak{p}$ ($\mathfrak{p}$ prime)

surj: Let $\overline{\gamma} \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$, $\gamma \in \mathfrak{p}^n$.

Want: $(\gamma + \mathfrak{p}^{n+1}) \cap (\beta) \neq \emptyset$

$\Leftrightarrow \gamma \in P^{n+1} + (\beta) = \gcd(P^{n+1}, \beta) = P^n$

$\exists\, r \in P^{n+1},\ s \in (\beta),\ \gamma + r = s \Leftrightarrow \gamma = s - r.$

Def: If $I \subset O_k$ non-zero

$\mathrm{Norm}(I) := [O_k : I]$

If $\alpha \in R \setminus \{0\}$, then $\mathrm{norm}(\alpha) = |\det(\text{"}x\alpha\text{"})| = |\mathrm{Norm}_{K/\mathbb{Q}}(\alpha)|$

Lemma: If $I, J \subset R \neq 0$, $\mathrm{Norm}(IJ) = \mathrm{Norm}(I)\mathrm{Norm}(J)$

Pf: $I = \prod P_i^{e_i}$, by CRT,

$\mathrm{Norm}(I) = \prod_i \mathrm{Norm}(P_i^{e_i})$

$= \prod_i \mathrm{Norm}(P_i)^{e_i}$

Lemma: $I \mid (\mathrm{Norm}(I))$

Pf: Need $\mathrm{Norm}(I) \in I$

$\| $

$[O_k : I]$

Cor ①: Let $\langle \beta_1, \cdots, \beta_n \rangle_{\mathbb{Z}} = O_k$. Let $I \subset O_k$ non-zero ideal,

Then $\exists\, m_i \in \mathbb{Z}$, $|m_i| \leq \lceil \sqrt[n]{\mathrm{Norm}(I)} \rceil$, $\sum \beta_i m_i \in I$.

Pf: Consider $\{\sum e_i \beta_i\}$, $0 \leq e_i \leq \lceil \sqrt[n]{\mathrm{Norm}(I)} \rceil$

So 2 elements in ↖ are the same mod I 手抽屉 (?)

NTS: The finiteness of $Cl(k)$

Pf: • Step 1: Fix basis $\langle \beta_1, \cdots, \beta_n \rangle_{\mathbb{Z}} = O_k$.

Given $\alpha \in O_k$, $\alpha = \sum_1^n m_i \beta_i$

$H(\alpha) := \mathrm{Max}(|m_i|)$

— $H(\alpha+\beta) \leq H(\alpha) + H(\beta)$

— $H(\alpha\beta) \le H(\alpha)\cdot H(\beta)\cdot C_k$ ← 与 basis 有关

re express $\beta_i\beta_j$ in $\langle\beta_1,\cdots,\beta_n\rangle$

↓ int the same

— $Norm(\alpha) \le H(\alpha)^n \cdot C_k$

• Step2: Let $I\subset R$, By Cor①, $\exists\, \alpha\in I$, s.t. $H(\alpha)\le\lceil\sqrt[n]{Norm(I)}\rceil$

$\Rightarrow Norm(\alpha)\le Norm(I)\cdot C_K$.

$\Rightarrow Norm((\alpha)I^{-1})\le C_k$.

↓ coset of class group

Note $[(\alpha)I^{-1}]=[I]^{-1}$

$[I]\in Cl(K)$

• Step3: Claim: every element in $Cl(K)$ has an integral representative $I\subset O_K$ s.t. $Norm(I)\le C_k$

Pf: let $[J]\in Cl(K)$, J- frac ideal.

for large enough $N\in\mathbb{N}$, $NJ^{-1}\subset O_K$.

By (2), $\exists I\subset O_K$, $Nm(I)\le C_k$,

$[I]\sim I[NJ^{-1}J]=[J]$.

• Step4: the set of ideals $I\subset O_K$ with $Norm(I)\le C_k$ is finite.

Pf: Unique factorization of ideals.

Minkowsk bound:

k: # field, $[K:\mathbb{Q}]=n=r_1+2r_2$.

Thm: $\forall g\in Cl(k)$, $\exists$ ideal $I\subset O_K$,

s.t. $[I]=g$, $Norm(I)\le \sqrt{|D_k|}\cdot \frac{n!}{n^n}\cdot\left(\frac{4}{\pi}\right)^{r_2}$

"main term"; $\frac{n!}{n^n}\approx\frac{1}{e^n}$; D_k: discriminant; $\frac{4}{\pi}<3$

Example: ① $|Cl(\mathbb{Q})|=1$ $\mathbb{Z}$ PID. 其实等价于 ideal 数?

② $|Cl(\mathbb{Q}(i))|=1$ since $\mathbb{Z}[i]$ PID.

③ $|Cl(\mathbb{Q}(\sqrt{-3}))|=1$, $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ PID.

④ $K=\mathbb{Q}(\sqrt{-5})$

$\alpha = a+b\sqrt{-5} \Rightarrow (x-\alpha)(x-\bar{\alpha}) = x^2-2ax+a^2+5b^2$ (min poly)

$O_K = \langle 1, \sqrt{-5}\rangle_{\mathbb{Z}}$, $D_K = \begin{vmatrix} 1 & \sqrt{-5} \\ 1 & -\sqrt{-5} \end{vmatrix}^2 = -20$

$M_K = \sqrt{20}\cdot\frac{2}{2^2}\cdot\frac{4}{\pi} = \frac{\sqrt{5}}{2}\cdot\frac{4}{\pi} < 5$

Since $I \mid (\text{Norm}(I))$, factor (2), (3)

Assume $P_2 \mid (2) \Rightarrow \text{Norm}(P_2) \mid \underbrace{\text{Norm}(2)}_{4}$

$O_K \cong \mathbb{Z}[X]/(X^2+5) \Rightarrow O_K/(2) \cong \mathbb{Z}[X]/(X^2+5,2) \cong \mathbb{F}_2[X]/(X^2+1) \cong \mathbb{F}_2[X]/(X+1)^2$ (这里就有 prime: $(X+1)$)

R comm. ring, $\text{Nil}(R) = \{x\in R \mid x^n = 0, \exists n\in\mathbb{N}\}$,

$\text{Prime}(R) \cong \text{Prime}(R/\text{Nil}(R))$

$\psi: O_K \to O_K/(2) \cong \mathbb{F}_2[X]/(X^2+1) \Rightarrow P_2 = \psi^{-1}((1+X)) = (1+\sqrt{-5}, 2)$

So $(2) = P_2^2$, $P_2^2 = (4, 2+2\sqrt{-5}, -4+2\sqrt{-5})$

$O_K/(3) \cong \mathbb{F}_3[X]/(X^2-1) \cong \mathbb{F}_3 \oplus \mathbb{F}_3$

$(X+1), (X-1)$

So $(3) = P_3 P_3' = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$

Is P_2 principle? if Yes, $P_2 = (a+b\sqrt{-5})$

$2 = \text{Norm}(P_2) = |\text{Nm}_{K/\mathbb{Q}}(a+b\sqrt{-5})| = a^2+5b^2$.

$\Rightarrow \langle [P_2] \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Is P_3 principle? No! same.

Claim: $[P_2] = [P_3]$, enough to check P_2P_3 principle.

$P_2P_3 = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) = (6, 1+\sqrt{-5}, (1+\sqrt{-5})^2) = (1+\sqrt{-5})$

⑤ $K = \mathbb{Q}(\sqrt{-23})$ $O_K = \langle 1, \frac{1+\sqrt{-23}}{2}\rangle_{\mathbb{Z}}$

$D_K = -23$, $M_K = \sqrt{23}\cdot\frac{4}{\pi}\cdot\frac{1}{2} < 4$

$t = \frac{1+\sqrt{-23}}{2} \Rightarrow (2t-1)^2 = -23 \Rightarrow t^2-t+6 = 0$.

(2), $O_K/(2) = \mathbb{F}_2[t]/t^2-t \Rightarrow (2) = (2, t-1)(2, t)$

$(3) = (3, t-1)(3, t)$

Claim: (exercise): $[(2, t-1)^2] = [(2, t)]$

$[(3, t)] = [(2, t-1)]$

(6) $K = \mathbb{Q}(\sqrt{15})$ $\quad Cl(K) \cong \mathbb{Z}/2\mathbb{Z}$

$(3, \sqrt{15})^2 = (3)$

if $(\alpha) = (3, \sqrt{15}) \Rightarrow (\alpha^2) = (3, \sqrt{15})^2 = (3)$

$\Rightarrow \alpha^2 = 3 \cdot u \quad u \in O_K^\times = \pm 1 < 4 + \sqrt{15} >$.

(co-) Volumes of Ideals:

- $L \subset \mathbb{R}^n$ is a lattice, Assume $\langle v_1, \cdots, v_n \rangle_{\mathbb{Z}} = L$.
- Let $w = dx_1 \wedge \cdots \wedge dx_n$ on $\mathbb{R}^n$. $(V = \mathbb{R}^n)$

Consider the co-volume of L: $\text{covol}(L) = \text{Vol}(\mathbb{R}^n/L) = \left| \int_{\mathbb{R}^n/L} w \right|$

$= \left| \int_P w \right|$, $P = \left\{ \sum_{i=1}^n a_i v_i \,,\ 0 \le a_i < 1 \right\}$

Lemma: Let A be the change of basis matrix from $(\vec{v})$ to $(\vec{e})$

then $\text{covol}(L) = |\det(A)|$

Pf: $\det : V^n \to \mathbb{R}$ is multi-linear, alternating.

↖ unique up to scale.

define $\overset{\text{sign}}{\text{scovol}}(v_1, \cdots, v_n) = \int_{[0,1]^n} f^* w$, $f : \begin{matrix} \mathbb{R}^n \to \mathbb{R}^n \\ e_i \mapsto v_i \end{matrix}$ multi-linear, alternating.

$\text{scovol}(e_1, \cdots, e_n) = 1 = \det(e_1, \cdots, e_n)$ done.

Property: if $L \subset L' \subset \mathbb{R}^n$

then $\dfrac{\text{covol}(L)}{\text{covol}(L')} = [L : L']$

Let K be a # field, $r_1+2r_2=n$, $\sigma_1,\cdots,\sigma_{r_1},\tau_1,\cdots\tau_{r_2}$ $K\hookrightarrow\mathbb{C}$

$\sigma: K \hookrightarrow \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}$.

$\varphi: \mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}\cong\mathbb{R}^n$

$(x_1,\cdots,x_{r_1},z_1,\cdots,z_{r_2}) \longmapsto (x_1,\cdots,x_{r_1},Re(z_1),Im(z_1),\cdots,Re(z_{r_2}),Im(z_{r_2}))$

$(x+yi)\to dxdy$.

Let w be the canonical volume form on $\mathbb{R}^n$.

For $I<K$ a $\neq 0$ fractional ideal, define

$$covol(I)=\left|\int_{\mathbb{R}^{r_1}\oplus\mathbb{C}^{r_2}/\sigma(I)} w\right|$$

Lemma: $covol(O_K)=2^{-r_2}\sqrt{|D_K|}$

Pf: Let $\langle\alpha_1,\cdots,\alpha_n\rangle_{\mathbb{Z}}=O_K$.

$$D_K=\left|\begin{matrix}\sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \tau_1(\alpha_1) & \overline{\tau_1}(\alpha_1) & \cdots & \tau_{r_2}(\alpha_1) & \overline{\tau_{r_2}}(\alpha_1)\\ & & & & & & & \end{matrix}\right|^2$$

$$covol(O_K)=\left|\sigma_1(\omega_1)\cdots\sigma_{r_1}(\omega_1),Re(\tau_1(\omega_1)),Im(\tau_1(\omega_1)),\cdots,Re(\tau_{r_2}(\omega_1)),Im(\tau_{r_2}(\omega_1))\right|$$

fractional ideal

Lemma: $covol(I)=Norm(I)\cdot covol(O_K)$

Pf: 1) $I<O_K$, $norm(I)=[O_K:I]$ ✓

2) In general, $\exists m\in\mathbb{N}$ s.t. $mI<O_K$.

$$covol(I)=[I:mI]^{-1}\cdot covol(mI)$$

$$=[I:mI]^{-1}\cdot Norm(mI)\cdot covol(O_K)$$

$=Norm(I)$ ← check.

Lemma: (minkowski)

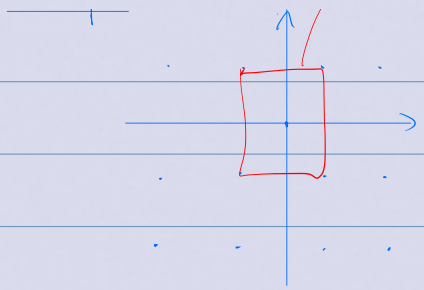
Let $S<\mathbb{R}^n$ be a convex symmetric body ($S=-S$)

Let L be a lattice. s.t. $2^n covol(L)<vol(S)$

因为 $\{0\}<L\cap S$.

Then $L\cap S\neq\{0\}$

example:



Pf: $\pi: S \longrightarrow \mathbb{R}^n/L$ is locally volume perserving.

π injective $\Rightarrow$ $\mathrm{Vol}(S) = \mathrm{Vol}(\pi(S))$

$\leq \mathrm{Vol}(\mathbb{R}^n/L) = \mathrm{covol}(L)$

等价

$\mathrm{Vol}\left(\frac{S}{2}\right) = \frac{\mathrm{Vol}(S)}{2^n} > \mathrm{covol}(L)$

$\Rightarrow \exists\, x, y \in \frac{S}{2},\ x \neq y,\ \pi(x) \neq \pi(y),\ s.t.\ x - y \in L - \{0\}$

$\Rightarrow x - y = \frac{2x + (-2y)}{2} \in S$ (symmetric, $\leq S$)

Cor1: Let $I \subset k$ fractional ideal

$\exists\, a \in I \setminus \{0\}$, with $|N_{k/\mathbb{Q}}(a)| \leq \mathrm{Norm}(I) \cdot \sqrt{|D_k|} \cdot \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}$

Cor2: $\forall\, g \in Cl(k),\ \exists\, [I] = g,\ |\mathrm{Norm}(I)| \leq \sqrt{|D_k|} \cdot \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}$

Cor3: $\sqrt{|D_k|} \geqslant \frac{n^n}{n!} \cdot \left(\frac{\pi}{4}\right)^{r_2} > 1$

Pf of Cor 1:

Let $S \subset \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ be defined by (Lebesgue measurable)

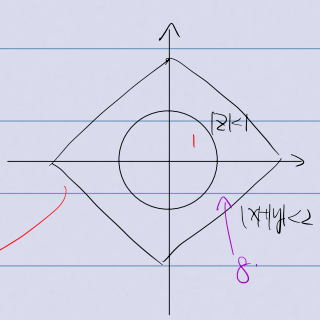
$S = \left\{ (x_i, z_j) \in \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2},\ s.t.\ \sum_{i=1}^{r_1} |x_i| + \sum_{j=1}^{r_2} |z_j|^2 \leq M \right\}$

Note: $\prod |x_i| \prod |z_j|^2 \leq \left(\frac{\sum |x_i| + 2\sum |z_j|}{n} \right)^n$ (均值不等式!!!!)

$\Rightarrow S \supset T = \left\{ (x_i, z_j) : \sum |x_i| + 2\sum |z_j| \leq n \cdot M^{\frac{1}{n}} \right\}$.

Want: $\mathrm{Vol}(T) > 2^n \mathrm{covol}(I) = 2^n \cdot \mathrm{Norm}(I) \sqrt{|D_k|} \cdot 2^{-r_2}$.

Define $T' = \left\{ (x_i, z_j) : \sum |x_i| + \sum |\mathrm{Re}(z_j)| + |\mathrm{Im}(z_j)| \leq n \cdot M^{\frac{1}{n}} \right\}$.



$\Rightarrow \mathrm{Vol}(T) = \left(\frac{\pi}{8}\right)^{r_2} \cdot \mathrm{Vol}(T') = \left(\frac{\pi}{8}\right)^{r_2} \frac{2^n \cdot M \cdot n^n}{n!}$ 算完就行了.

want: $\left(\frac{\pi}{8}\right)^{r_2} \frac{2^n \cdot M \cdot n^n}{n!} \geq 2^n \, Nm(I) \cdot \sqrt{|D_k|} \cdot 2^{-r_2}$

pick $M > \sqrt{|D_k|}\, Nm(I) \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}$

By. Minkowski lemma,

$I \cap T \neq \{0\} \Rightarrow I \cap S \neq \{0\}$.

$\Rightarrow \exists \alpha \in I,\ Nm(\alpha) \leq \sqrt{|D_k|}\, Nm(I) \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}$

UNIT GROUPS:

$\sigma : K \hookrightarrow \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$

$\sigma(O_k^\times) \subset Nm^{-1} < \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ (Nm-one subspace.)

Consider $\sigma^\times : K^\times \hookrightarrow \mathbb{R}^{r_1} \oplus \mathbb{R}^{r_2}$

$\sigma^\times := \log \circ \sigma$

$\sigma^\times(\alpha) = \left(\ln|\sigma_1(\alpha)|, \cdots, \ln|\sigma_{r_1}(\alpha)|, \ln|\tau_1(\alpha)|, \cdots, \ln|\tau_{r_2}(\alpha)| \right)$

$W < \mathbb{R}^{r_1} \oplus \mathbb{R}^{r_2} = \left\{ \vec{x} : \sum_{i=1}^{r_1} x_i + 2 \sum_{j=r_1+1}^{r_1+r_2} x_j = 0 \right\}$

$\sigma^\times(O_k^\times) < W$.

Lemma: $\sigma^\times(O_k^\times) < W$ is discrete.

Pf: (1) $\left(\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}\right)^\times \to \mathbb{R}^{r_1} \oplus \mathbb{R}^{r_2}$ is a proper topological map.

$\Rightarrow$ image of discrete set is discrete.

$\sigma(O_k) < \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ is discrete.

$\Rightarrow \sigma(O_k \setminus \{0\}) < \left(\mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}\right)^\times$ discrete.

(2) For $\varepsilon > 0$, if $\sigma^\times(\alpha) < B_\varepsilon$

$\Rightarrow \forall \psi \in \mathrm{Hom}(K, \mathbb{C}),\ e^{-\varepsilon} < |\psi(\alpha)| < e^{\varepsilon}$

compact (bounded) $\Rightarrow$ finitely many α_i.

Lemma: $O_k \cap \ker \sigma^\times = \{\text{roots of unity in } K\} = O_k^\times[\mathrm{tor}]$

Pf: Let $\alpha \in O_k^\times$, $\ker \sigma^\times$

$\Rightarrow \forall m \in \mathbb{Z}_{>0}$, α^m is also $\in O_k \cap \ker \sigma^\times$

$\Rightarrow \{\alpha^m, m \in \mathbb{Z}_{>0}\} \subset$ compact set (bounded

$\Rightarrow$ finite.

$\Rightarrow \exists\, m_1 \neq m_2$ s.t. $\alpha^{m_1} = \alpha^{m_2} \Rightarrow \alpha^{m_1 - m_2} = 1$ 单位根.

↓ the part

Cor: $\operatorname{rank} O_k^\times = \operatorname{rank} \sigma^\times(O_k^\times) \leq \dim W = r_1 + r_2 - 1$

Example (Pell's equation:)

$K = \mathbb{Q}(\sqrt{15})$, $O_K = \mathbb{Z}[\sqrt{15}]$

$O_k^\times = O_k^{(nm=1)} = \{a + b\sqrt{15} : a^2 - 15b^2 = 1\}$.

$4 + \sqrt{15} \in O_k^\times$

Claim: $O_k^\times = \{\pm 1\} \oplus (4+\sqrt{15})^{\mathbb{Z}}$

Pf: Let $\sigma_1, \sigma_2 : K \hookrightarrow \mathbb{C}$, s.t. $\sigma_1(\sqrt{15}) = \sqrt{15}$

$N \subset O_k^\times : \{\alpha : \sigma_1(\alpha) > 0\}$

WTS: $N \cong (4+\sqrt{15})^{\mathbb{Z}}$.

If Not, $\exists\, m > 2$, s.t. $4+\sqrt{15} = B^m$, $B \in N$.

we know

$0 < \sigma_1(B) = (4+\sqrt{15})^{\frac{1}{m}} < \sqrt{8} = 2\sqrt{2}$

$0 < \sigma_2(B) = (4-\sqrt{15})^{\frac{1}{m}} < 1$

Let $B = a + b\sqrt{15}$

$2b\sqrt{15} = \dfrac{\sigma_1(B) - \sigma_2(B)}{2}$

$\Rightarrow |2b\sqrt{15}| \leq \dfrac{|\sigma_1(B)| + |\sigma_2(B)|}{2} < 2$

$\Rightarrow |b\sqrt{15}| < 1 \Rightarrow b = 0$, contradiction.

If $(\alpha) = (3, \sqrt{15})$, not principle. $\Rightarrow (\alpha)^2 = (3) \Rightarrow \alpha^2 = 3 \cdot u$ has not. $|u| = 1$

WTS: $\{\pm 3, \pm 3(4+\sqrt{15})\}$ not square.

$\sigma^\times : K^\times \hookrightarrow \mathbb{R}^{r_1+r_2}$

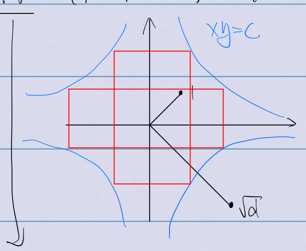
$\sigma^\times(\alpha) = (\ln|\sigma_1(\alpha)| \cdots \ln|\tau_{r_2}(\alpha)|)$

$W \subset \mathbb{R}^{r_1+r_2}$, $\{(y_1, \dots, y_{r_1+r_2}),\ \sum^{r_1} y_i + \sum^{r_2} 2y_i = 0\}$

$\sigma^\times(\mathcal{O}_K^\times) \subset W$

Thm: $\sigma^\times(\mathcal{O}_K^\times) \subset W$ lattice.

Pf: (Motivation): $K = \mathbb{Q}(\sqrt{d})$, $d>0$, $r_1=1$, $r_2=0$.



□ ▭ 足够长，里面可以找到元素 ☆ 啊?

这tm到底啥啊

denote $\tau_j = \sigma_{i+j}$.

Lemma: $\exists C>0$, s.t. $\forall\, 2 \le k \le r_1+r_2$, $\forall\, M>0$ $\exists$ unit $\alpha \in \mathcal{O}_K^\times$, s.t.

$\sigma_1^\times(\alpha) > M$, $\sigma_k^\times(\alpha) < -M$.

$|\sigma_j^\times(\alpha)| \le C$ (some constant) $j \ne 1, k$.

"Lemma $\Rightarrow$ Thm":

Equivalently, let $A \in M_{r_1+r_2,\, r_1+r_2-1}(\mathbb{R})$, s.t. $\begin{cases} \sum_{j=1}^{r_1+r_2} A_{ij} = 0 \ \text{(row)} \\ A_{i,1} > M \\ A_{i,i+1} < -M \\ \forall j \ne 1, i+1,\ |A_{ij}| < C. \end{cases}$

Then $\operatorname{rank} A = r_1+r_2-1$ if $M \gg 0$

$\begin{pmatrix} 100 & -100 & 0 \\ 170 & -5 & -165 \end{pmatrix}$

$\begin{pmatrix} 1 & -1 & & \\ & & -1 & \\ & & & -1 \ \ddots \end{pmatrix}$

Pf: If not, $\exists\, b_1, \dots, b_{r_1+r_2-1}$,

s.t. $\sum \vec{A_i}\, b_i = 0$

WLOG, $|b_1| = \max(|b_i|)$, $0 = \sum_{j=1}^{r_1+r_2} A_{i,2} \cdot b_i \le b_1 \cdot M + (r_1+r_2-1)\cdot|b_1|\cdot C < 0$

Pf of the Lemma: Let $B_M \subset \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ be defined by:

$\{ |\sigma_1(\alpha)| \le e^M$

$$\begin{cases} |\sigma_k(\alpha)| \le e^{-M} \quad (\text{or } e^{-M/2} \text{ if } k > r_1) \\ |\sigma_i(\alpha)| \le C_0 \quad \forall \text{ other } i\text{'s}. \end{cases}$$

where C_0 is that s.t. $\mathrm{Vol}(B_m) > 2^n \cdot \mathrm{Covol}(O_K)$

By Minkowski, B_m has a point α, $|N_{m_K/\mathbb{Q}}(\alpha)| \le C_1$.

Now let T be # ideals in O_K, Norm $\le C_1$

for $1 \le j \le T+1$, let α_j be the number we get from B_{M_j}

Claim: If $M \gg 0$, the α_j are distinct.

pf: Note $\frac{e^{M_j}}{C_0^n} \le |\sigma_1(\alpha_j)| \le e^{M_j}$

$\Rightarrow \exists j_1 \ne j_2 : (\alpha_{j_1}) = (\alpha_{j_2})$, $\beta_i = \frac{\alpha_{j_1}}{\alpha_{j_2}} \in O_K^\times$

if $\langle \alpha_1, \cdots, \alpha_{r_1+r_2-1} \rangle_{\mathbb{Z}} = O_K^\times / \text{torsion}$

write $A = \underbrace{(\log|\sigma_i(\alpha_j)|)}_{r_1+r_2}\}_{r_1+r_2-1} \subset W$

$|\det(A - \text{column})|$ regulator of K.

Change of fields:

$L \supset K$ # fields,

If $I \subset K$ is a fractional ideal of O_K. 这都是对于O_K的.

$$\begin{array}{ccc} L & & I_L \\ | & & \uparrow \\ K & \Leftrightarrow & I \end{array}$$

$I_L = (\alpha : \alpha \in I) \subset L$. $= (I)_L$ 用 I (在 O_L 里) generate 出来的东西.

$= \{\sum_{i=1}^{r} a_i b_i, a_i \in I, b_i \in O_L.\}$.

$I_L = \mathrm{conorm}_{L/K}(I)$

$$I \longrightarrow I_L$$

$\{\text{frac. ideals of } K\} \longrightarrow \{\text{frac. ideals of } L\}$.

考虑 $(\ )_L$ a map.

- $(0)_L = 0_L$. (zero ideal in L.) (L的 frac. ideal)
- $(IJ)_L = I_L J_L$.

- $(I+J)_L = I_L + J_L$

  $\subseteq$ is obvious.

- $(I \cap J)_L = I_L \cap J_L$

  ↓

  Pf: $(I \cap J) \cdot (I+J) = IJ$.

  $\Rightarrow (I \cap J)_L \cdot (I+J)_L = (IJ)_L$

  $\| = \checkmark \cdot \| \vee \quad \| \vee$ (cancelation)

  $(I_L \cap J_L) \cdot (I_L \cdot J_L) = I_L J_L$

  ↓ fractional ideals in O_K, forms a group.

Cor: $I \to I_L$ is a group homomorphism preserving gcd and lcm.

Prop: $I_L = J_L \Rightarrow I = J$ (injective)

In fact, $I_L \cap K = I$.

↓ 意思是，在 O_K 中，被 α generate 的 frac. ideal

Lemma: If $\alpha \in K$, $(\alpha O_K)_L = \alpha O_L$. → O_L 中……

Lemma: Every non-zero fractional ideal $I \subset K$ becomes principle in some L/K.

Pf: $\exists\, h \in \mathbb{N}$, s.t. $I^h = \alpha O_K$, $\alpha \in K$.

↓ identity in $Cl(O_K)$. ← finite.

class group finite 的意义是可以把不 principle 的 I power 成为 principle.

Let $L = K(\beta)$, where $\beta^h = \alpha$

"let" ??? 不通 根本假不通

$\Rightarrow (I_L)^h = (I^h)_L = (\alpha O_K)_L = \alpha O_L = (\beta O_L)^h$.

$\Rightarrow I_L = (\beta O_L)$ (Because unique fractional ideal)

Lemma: $Norm(I_L) = Norm(I)^{[L:K]}$

Pf: Case 1: $I = \alpha O_K$ for some $\alpha \in K$

$\Rightarrow Norm(I) = |Norm_{K/\mathbb{Q}}(\alpha)|$

$\Rightarrow Norm(I_L) = |Norm_{L/\mathbb{Q}}(\alpha)| = |Norm_{K/\mathbb{Q}}(\alpha)|^{[L:K]}$

Case 2: In general, $I^h = \alpha O_K$

$Norm(I_L) = Norm(I^h)^{[L:K]}$ norm is multiplicative.

Pf: Let $J = I_L \cap K$. $J \supseteq I$ obvious.

$J I_L$.

$\Rightarrow J_L \supseteq J_L \supseteq I_L \Rightarrow J_L = I_L$

$\Rightarrow \text{Norm}(J) = \text{Norm}(J_L)^{\frac{1}{[L:K]}} = \text{Norm}(I)$

$\Rightarrow \text{Norm}(IJ^{-1}) = 1$ (IJ^{-1}: actual ideal) $\Rightarrow IJ^{-1} = O_K \Rightarrow I = J$.

- If $M \supset L \supset K$, $I \subset K$ fractional ideal,

  $(I_L)_M = I_M$

- If $L \supset K$, then $I \to I_L$ descents to a map $Cl(K) \to Cl(L)$ (not necessarily injective)

  $\varinjlim_L Cl(K) = 0$.

$L \supset K$ is a normal extension

$G = Gal(L/K)$ acts on L, O_L, fractional ideals, $Cl(L)$

$\mathbb{I}_L = \{$non-zero fractional ideals in $L\}$.

$L^G = K$, $O_L^G = O_K$.

But $\mathbb{I}_L^G \neq \mathbb{I}_K$, $Cl(L)^G \neq Cl(K)$.

Examples: • $L = \mathbb{Q}(\sqrt{5})$, $K = \mathbb{Q}$, $I = (\sqrt{5})$

$G = Gal(L/\mathbb{Q}) = \{1, \sigma\}$. $\sigma(I) = \sigma(\sqrt{5}) = (-\sqrt{5}) = \sqrt{5} = I$.

• $L = \mathbb{Q}(\sqrt{-6})$, $K = \mathbb{Q}$ $Cl(L) \cong \mathbb{Z}/2\mathbb{Z}$, $Cl(L)^G \cong \mathbb{Z}/2\mathbb{Z}$

Norms of ideals:

L/K normal, $G = Gal(L/K)$

$I \in \mathbb{I}_L$.

$$\begin{cases} Nm_{L/K}(I) := \prod_{\sigma\in G} \sigma(I) \in \mathbb{I}_L^G \\ Norm_{L/K}(I) := \left(Nm_{L/K}(\alpha), \alpha\in I\right) \in \mathbb{I}_K. \end{cases}$$

ideal?

$$\begin{array}{ccc} L & \hookleftarrow & I \\ \uparrow & & \downarrow \\ K & \hookleftarrow & Nm(I) \end{array}$$

Remark: If $I = \alpha O_L$, then $Nm_{L/K}(I) = Nm_{L/K}(\alpha)\cdot O_L$, $Norm_{L/K}(I) = Nm_{L/K}(\alpha)\cdot O_K$.

Thm: $Nm_{L/K}(I) = (Norm_{L/K}(I))_L$.

Pf: • $Norm_{L/K}(I)_L \subset Nm_{L/K}(I)$.

• If $\alpha\in I$, $Norm_{L/K}(I) \supset (Nm_{L/K}(\alpha))_K$. $(= Nm_{L/K}(\alpha) O_K)$

$\Rightarrow Norm_{L/K}(I) \mid (Nm_{L/K}(\alpha))_K$

• WLOG, $I \subset O_L$.

CRT

Recall: $\forall$ ideal J, can find $\alpha\in O_K$, s.t. $I \mid (\alpha)$, $\gcd(\alpha I^{-1}, J) = (1)$

↓

(rel)proof: Let $p_1,\dots,p_n$ be the prime divisors of I, J.

Let $M >$ any exponent.

By CRT, pick α s.t. each p_i divides α as much as it divides I.

$Norm_{L/K}(I)_L = J\cdot Nm_{L/K}(I) = J\prod_{\sigma\in G}\sigma(I)$

Note: $J\in \mathbb{I}_L^G$ (Galois-invariant)

∀? only one α?

Let $\alpha\in O_K$, s.t. $I\mid(\alpha)$, $\gcd((\alpha), (Norm(J))) = (1)$

Also we know: $Norm_{L/K}(I)_L \mid (Nm_{L/K}(\alpha))_L = Nm_{L/K}(I)\, Nm_{L/K}(\alpha I^{-1})$

But $\gcd(J, \alpha I^{-1}) = (1) \Rightarrow \gcd(J, \sigma(\alpha I^{-1})) = 1$

$\Rightarrow \gcd(J, \underbrace{\prod \sigma(\alpha I^{-1})}_{= Nm_{L/K}(\alpha I^{-1})}) = 1$

$\Rightarrow J = O_L$.

In general, Suppose L/K arbitrary, let $M = L^{Gal} \Rightarrow M/L/K$.

$I\in\mathbb{I}_L$

$Norm_{L/K}(I) = \left(Nm_{L/K}(\alpha), \alpha\in I\right)_K \in \mathbb{I}_K$.

Thm: $\mathrm{Norm}_{L/K}(I)_M = \prod_{\sigma \in \mathrm{Gal}(M/K)/\mathrm{Gal}(M/L)} \sigma(I_M) = \left(\prod_{G \mid G/K} \sigma(I_M)\right)^{\frac{1}{[M:L]}}$

Pf: Same.

- $M > L > K$. $\mathrm{Norm}_{L/K}(\mathrm{Norm}_{M/L}(I)) = \mathrm{Norm}_{M/K}(I)$

BIG PICTURE

Given K, Let $\mathbb{P}_K := \{\text{prime ideals of } K\}$

$\mathbb{I}_K \cong \mathbb{Z}^{\oplus \mathbb{P}_K}$

$\cup$ unique factorization $\cong$ $N^{\oplus \mathbb{P}_K}$.

Ideals in $\mathcal{O}_K$

$\mathbb{P}_L$ — finite to 1 → $\mathbb{P}_K$

Given $L > K$, $\mathbb{I}_K \xrightarrow{\text{inclusion}} \mathbb{I}_L$, $\mathbb{I}_L \xrightarrow{I \to \mathrm{Norm}_{L/K}(I)} \mathbb{I}_K$ (×[L:K])

Say that $P < \mathcal{O}_L$ a prime ideal

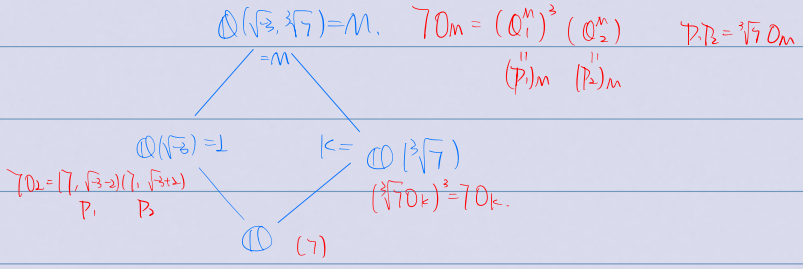
$\Rightarrow P \cap \mathcal{O}_K$ also a prime ideal.

$\Rightarrow P \mid (P \cap \mathcal{O}_K)_L$.

$\neq 0$

On the other hand, $P \cap \mathcal{O}_K$ is the only prime ideal of K that P divides.

Example:



Def: Given a $\neq 0$ prime ideal $P \subset O_K$, O_K/P the **residue field** at P. Namely, $\mathbb{F}_P$

Def: if L/K # field. primes $P \subset O_L$. $Q \subset O_K$,

P **lies over** Q (Q **lies under** P)

if $P \mid Q_L \Leftrightarrow Q = P \cap O_K$.

$$\begin{array}{ccc} L & \supset & P \to O_L/P \cong \mathbb{F}_P \\ | & & | \\ K & \supset & Q \to O_K/Q \cong \mathbb{F}_Q \end{array}$$

$\downarrow = P \cap O_K$.

- If P lies over Q, $\mathbb{F}_Q \hookrightarrow \mathbb{F}_P$

$$\begin{array}{ccc} \| & & \| \\ O_K/Q & \hookrightarrow & O_L/P \end{array}$$

Def: $f(P/Q) = [\mathbb{F}_P : \mathbb{F}_Q]$, $\mathrm{Norm}(P) = \mathrm{Norm}(Q)^{f(P/Q)}$ ← inertial degree

Def: $e(P/Q)$: $P^{e(P/Q)} \| Q_L$. ← exact degree

↖ ramification of P over Q / Q in L.

e.g. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$ $O_L = \mathbb{Z}[\sqrt[3]{2}]$

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2}) & \leftarrow & P \\ | & & | \\ \mathbb{Q} & \leftarrow & Q \end{array}$$

① $Q = (2)$, $Q_L = 2O_L = (\sqrt[3]{2})^3$

$P = (\sqrt[3]{2})$, $Q = P^3$, $e(P/Q) = 3$, $f(P/Q) = 1$

② $Q = (5)$ $O_L/Q \cong \mathbb{Z}[X]/(X^3-2, 5) \cong \mathbb{F}_5[X]/X^3-2$ $\quad X^3-2 = (X-3)(X^2+3X+4)$

$\Rightarrow \cong \mathbb{F}_5[X]/(X-3) \oplus \mathbb{F}_5[X]/(X^2+3X+4)$

$\Rightarrow P_2 = (5, \sqrt[3]{2}-3)$, $P_1 = (5, \sqrt[3]{4}+3\sqrt[3]{2}+4)$

$\mathrm{Norm}(P_1) = 5^2$, $\mathrm{Norm}(P_2) = 5$, $\mathrm{Norm}(Q_L) = \mathrm{Norm}(Q)^3 = 5^3$

$\Rightarrow Q = P_1 P_2$.

$\Rightarrow e(P_1/Q) = e(P_2/Q) = 1$

$f(P_1/Q) = 2$, $f(P_2/Q) = 1$.

In general, $\mathcal{O}_L = \prod_{i=1}^{g} P_i^{e(P_i/\mathcal{O})}$ $\{P_1, \cdots, P_g\}$ primes dividing $\mathcal{O}_L$.

- $\mathrm{Norm}(\mathcal{O})^{[L:k]} = \mathrm{Norm}(\mathcal{O}_L) = \prod_{i=1}^{g} \mathrm{Norm}(P_i)^{e(P_i/\mathcal{O})} = \prod_{i=1}^{g} \mathrm{Norm}(\mathcal{O})^{f(P_i/\mathcal{O})e(P_i/\mathcal{O})}$

Thm: $[L:k] = \sum_{i=1}^{g} e(P_i/\mathcal{O}) f(P_i/\mathcal{O})$

- If $[L:k]=2$ (a) $g=1$, $e=1$, $f=2$ ← $\mathcal{O}$ stays inert
  (b) $g=2$, $e=1$, $f=1$ ← $\mathcal{O}$ splits
  (c) $g=1$, $e=2$, $f=1$ ← $\mathcal{O}$ ramifies.

(if $k=\mathbb{Q}$, $L=\mathbb{Q}[i]$, 2 ramifies
p splits $\Leftrightarrow p \equiv 1 \pmod 4$
p inert $\Leftrightarrow p \equiv 3 \pmod 4$)

- Assume L/k Galois, $G = \mathrm{Gal}(L/k)$
- $\mathcal{O} < \mathcal{O}_k$ prime, $S_{\mathcal{O}} = \{$primes in $\mathcal{O}_L$ over $\mathcal{O}\}$

Thm: (1) $\mathrm{Gal}(L/k)$ acts on $S_{\mathcal{O}}$
(2) $\mathrm{Gal}(L/k)$ acts transitively on $S_{\mathcal{O}}$
(3) $\forall P_1, P_2 \in S_{\mathcal{O}}$, $\underbrace{e(P_1/\mathcal{O}) = e(P_2/\mathcal{O})}_{e(\mathcal{O})}$, $\underbrace{f(P_1/\mathcal{O}) = f(P_2/\mathcal{O})}_{f(\mathcal{O})}$

Pf: (1) $g \in G$, $P \mid \mathcal{O}_L \Rightarrow P \supset \mathcal{O}_L$.
$\Rightarrow gP \supset g\mathcal{O}_L = \mathcal{O}_L$. ☆
$\Rightarrow gP \mid \mathcal{O}_L$.

(2) Let $P_1, P_2 \in S_{\mathcal{O}}$.
$\mathrm{Norm}_{L/k}(P_1) \in \mathbb{I}_k$ (ideal of k.)
$\downarrow = \prod_{g \in G} gP_1$
$\Rightarrow \mathrm{Norm}_{L/k}(P_1)\mathcal{O}_L + \mathcal{O}_L \neq \mathcal{O}_L$.
$\Rightarrow \mathrm{Norm}_{L/k}(P_1)\mathcal{O}_L + \mathcal{O} \neq \mathcal{O}_k \Rightarrow \mathcal{O} \mid \mathrm{Norm}_{L/k}(P_1)$

$\Rightarrow Q_2 \mid (\text{Norm}_{L/K}(P_1))_L$

$\Rightarrow P_2 \mid (\text{Norm}_{L/K}(P_1))_L$

$\Rightarrow \exists g_1$ s.t. $P_2 = gP_1$

(3) $g: O_L \xrightarrow{\sim} O_L$, $g: P_1 \simeq P_2$

$\Rightarrow g: \mathbb{F}_{P_1} \xrightarrow{\sim} \mathbb{F}_{P_2} \Rightarrow f(P_1/Q) = f(P_2/Q)$

$Q_L = \prod_{P \mid Q} P^{e(P/Q)} = \prod_{P \mid Q} (gP)^{e(P/Q)} \Rightarrow e(P_1/Q) = e(P_2/Q)$

$\Rightarrow [L:K] = g(Q)\, e(Q) f(Q)$

$\|$

$|S_Q|$

Def: Given P over Q,

Decomposition group of P to be

$D_P := \text{stab}(P) < G$.

$[G : D_P] = g(Q)$

Note: If $\sigma \in D_P$, then σ acts on $O_L/P = \mathbb{F}_P$

fixes $\mathbb{F}_Q < \mathbb{F}_P$

$\Rightarrow$ get a homomorphism $\varphi_P : D_P \to \text{Gal}(\mathbb{F}_P/\mathbb{F}_Q)$

Def: Inertial group $I_P < D_P$ be $\ker \varphi_P$.

Thm: φ_P is surjective.

Cor: $[D_P : I_P] = f(Q)$ $\quad |I_P| = e(Q)$

Pf: Let $\alpha \in \mathbb{F}_P$, s.t. $\mathbb{F}_P = \mathbb{F}_Q(\alpha)$

Let $\tilde{\alpha} \in O_L$, s.t. $\tilde{\alpha} \to \alpha$

$\tilde{f}(x) \in L[x]$, $\tilde{f}(x) = \prod_{\sigma \in G} (x - \sigma\tilde{\alpha})$

$\tilde{f}(x) \in k[x]$, $\tilde{f}(x) \to \tilde{f}(x) \in \mathbb{F}_P(x)$

$\Downarrow$ $\qquad\qquad\qquad\qquad \| $

$f(x) \in \mathbb{F}_Q[x]$. $\qquad \prod_{\sigma \in G} (x - \varphi_P(\sigma)\alpha)$

L/k Galois with galois group G

$Q \subset O_k$, $Q_L = \prod_{i=1}^{g_Q} P_i^{e_Q}$, $f_Q = f(P_i/Q) = [\mathbb{F}_P : \mathbb{F}_Q]$.

$G \circlearrowright \{P_1, \cdots, P_{g_Q}\}$ transitive.

$D_{P/Q} \subset G$, $:\{g \in G,\ g \text{ fix } P_i\}$

Thm: $D_{P/Q} \longrightarrow Gal(\mathbb{F}_{P_i}/\mathbb{F}_Q)$ surjective.

Pf: WLOG, $i=1$, Take $\alpha \in \mathbb{F}_{P_1}$, s.t. $\mathbb{F}_{P_1} = \mathbb{F}_Q(\alpha)$

Let $\tilde{\alpha} \in O_L$. s.t. $\{\tilde{\alpha} \equiv \alpha \bmod P_1,\ \tilde{\alpha} \equiv 0 \bmod P_{i+1}\}$ (By CRT)

"$\tilde{\alpha} \to 0 \bmod P_{i+1}$" ← notation.

$\tilde{f}(x) = \prod_{\sigma \in G} (x - \sigma\tilde{\alpha}) \in O_k[x]$

Let $\tilde{f}(x) \to f(x) \in \mathbb{F}_Q[x]$, $f(\alpha) = 0$. $(\tilde{f}(\tilde{\alpha}) = 0)$

$\Rightarrow \forall$ conjugate $\beta \in \mathbb{F}_{P_1}$ of α, $\exists \sigma \in G$, $\sigma\tilde{\alpha} \to \beta \bmod P_1$

If $\sigma \notin D_{P/Q}$, $\tilde{\alpha} \in \sigma^{-1}P_1 \Rightarrow \sigma\tilde{\alpha} \in P_1$ contradiction.

Def: $I_{P/Q} := \ker(D_{P/Q} \to Gal(\mathbb{F}_P/\mathbb{F}_Q))$ ← Inertial group of P over Q.

Cor: $-[D_{P/Q} : I_{P/Q}] = f_Q$.

$- D_{P/Q}/I_{P/Q} \cong \mathbb{Z}/f_Q\mathbb{Z} \cong Gal(\mathbb{F}_P/\mathbb{F}_Q)$

Note: $I_{P/Q} = \{\sigma \in G,\ \sigma P = P,\ \forall \alpha \in O_L,\ \sigma\alpha - \alpha \in P\}$.

Consider $M \supset L \supset k$, M/k Galois.

$G = Gal(M/k)$, $H = Gal(M/L)$ $\quad H < G$.

$M \to R$
$L \to Q$
$k \to p$

Let $p \subset O_k$ prime ideal, $Q \subset O_L$, $R \subset O_M$ prime ideals s.t. R over Q over p.

G

Lemma: ① $D_{R/p} \cap H = D_{R/Q}$

② $I_{R/p} \cap H = I_{R/Q}$.

Pf: ① $D_{R/p} \cap H = \{\sigma \in H : \sigma R = R\} \overset{\text{def}}{=} D_{R/Q}$.

② $I_{R/p} \cap H = \{\sigma \in H : \forall \alpha \in O_M, \sigma\alpha - \alpha \in R\} \overset{\text{def}}{=} I_{R/Q}$

Cor: Suppose $p O_M = \prod_{i=1}^{g_{M/k}} R_i^{e_{M/k}}$, $R = R_1$.

Let $e_{M/k}$, $f_{M/k}$ ramification, inertial degrees.

Let $Q_1 \cdots Q_{g_{L/k}}$ be the orbit of H on $\{R_1, \cdots, R_{g_{M/k}}\}$.

Then $p_L = \prod_{i=1}^{g_{L/k}} Q_i^{e_{L/k}}$, $\quad Q_1 = Q$.

where primes in M over Q_i are O_j.

Moreover, let $R_i \subset O_j$ consider

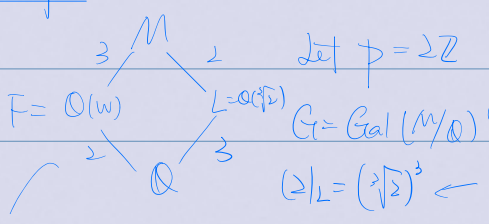
$$Stab_H(R_i) \cap I_{R_i/p} = I_{R_i/Q_i}$$

$$e_{Q_i/p_i} = \frac{|I_{R/p}|}{|Stab_H(R_i) \cap I_{R/p}|}$$

$$Stab_H(R_i) = D_{R_i/Q_i}$$

$$\Rightarrow f_{Q_i/p_i} = \frac{|Stab_H(R_i)|}{e_{Q_i/p_i}}$$

Example: $k = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, $M = \mathbb{Q}(\sqrt[3]{2}, w)$



Let $p = 2\mathbb{Z}$

$G = Gal(M/\mathbb{Q}) \cong S_3$.

$(2)_L = (\sqrt[3]{2})^3 \leftarrow \mathbb{Q}$

$2\mathcal{O}_F$ is prime. (x^2+x+1 stays irred in $\mathbb{F}_2$)

Case 1: $f_{M/K}=2$, $g_{M/K}=1$ $(2)_M=\mathfrak{P}^3$, $\mathbb{F}_{\mathfrak{P}}\cong\mathbb{F}_4$

Case 2: $f_{M/K}=1$, $g_{M/K}=2$. $(2)_M=(\mathfrak{P}_1^3)(\mathfrak{P}_2^3)$, $\mathbb{F}_{\mathfrak{P}_i}\cong\mathbb{F}_2$.

Case 3: $f_{M/K}=g_{M/K}=1$, $e_{M/K}=6$. $(2)_M=\mathfrak{P}^6$, $\mathbb{F}_{\mathfrak{P}}\cong\mathbb{F}_2$

We know $f_{\mathcal{O}_F/2\mathbb{Z}}=2 \Rightarrow 2\mid f_{M/K}$. $\Rightarrow$ case 1

for case 2: to rule out

$A_3\lhd S_3$ is the stabilizer of $\mathfrak{P}_1$ and $\mathfrak{P}_2$.

$F=M^{A_3}$, $(2)_F$ Factors into 2 distinct primes

Contradiction.

Example: $p=3\mathbb{Z}$.

$(3)_F=(\sqrt{-3})^2$

$(3)_L$: $x^3-2=(x-2)^3$

$(3)_L=(3,\sqrt[3]{2}-2)^3$

$\Rightarrow (3)_M=\mathfrak{P}^6$ 可为 2/e, 3/e.

Prop: $M\supset L\supset K$, $H=\mathrm{Gal}(M/L)\lhd G=\mathrm{Gal}(G/K)$

$G/H\cong\mathrm{Gal}(L/K)$

$\mathfrak{R}$ over $\mathcal{O}$ over $\mathfrak{P}$. prime ideals.

- $\sigma\in G$, $D_{\sigma\mathfrak{P}/\mathfrak{p}}=\sigma D_{\mathfrak{P}/\mathfrak{p}}\sigma^{-1}$

  $I_{\sigma\mathfrak{P}/\mathfrak{p}}=\sigma I_{\mathfrak{P}/\mathfrak{p}}\sigma^{-1}$ ✓

- $D_{\mathcal{O}/\mathfrak{p}}=\mathrm{im}(D_{\mathfrak{P}/\mathfrak{p}})$ $I_{\mathcal{O}/\mathfrak{p}}=\mathrm{im}(I_{\mathfrak{P}/\mathfrak{p}})$ ☆

Pf: if $\sigma_0(\sigma\mathfrak{R})=\sigma(\mathfrak{R})$, then $(\bar\sigma^{-1}\sigma_0\sigma)(\mathfrak{R})=\mathfrak{P}$

$\sigma_0\alpha-\alpha\in\sigma\mathfrak{R}\Leftrightarrow \bar\sigma^{-1}\sigma_0\alpha-\bar\sigma^{-1}\alpha\in\mathfrak{R}$

$\Leftrightarrow(\bar\sigma^{-1}\sigma_0\sigma)(\bar\sigma^{-1}\alpha)-\bar\sigma^{-1}\alpha\in\mathfrak{R}$

$\tau\in D_{\mathcal{O}/\mathfrak{p}}\Leftrightarrow\tau\mathcal{O}=\mathcal{O}$

If $\sigma \in D_{\mathfrak{P}/\mathfrak{p}} \Leftrightarrow \sigma\mathfrak{P} = \mathfrak{P} \Rightarrow \sigma\mathfrak{P} \cap \mathcal{O}_L = \mathfrak{P} \cap \mathcal{O}_L = \mathfrak{Q}$ ($\mathfrak{P} \supset \mathfrak{Q}$)

$\Rightarrow \psi_i : D_{\mathfrak{P}/\mathfrak{p}} \to D_{\mathfrak{Q}/\mathfrak{p}}$

Remains to show its surjective.

Let $\tau \in D_{\mathfrak{Q}/\mathfrak{p}}$, pick $\tilde{\tau} \in G$, $\tilde{\tau} \to \tau$. ($G \twoheadrightarrow G/H$, G surjective)

$\tau\mathfrak{P}, \mathfrak{P}$, i.e. over $\mathfrak{Q}$. $\exists \sigma_0 \in H$; $\sigma_0(\tilde{\tau}\mathfrak{P}) = \mathfrak{P}$ (transitivity of action.)

$\sigma_0\tilde{\tau} \in D_{\mathfrak{P}/\mathfrak{p}}$, $\sigma_0\tilde{\tau} \to \tau$.

Let $\sigma \in I_{\mathfrak{P}/\mathfrak{Q}}$, $\forall \alpha \in \mathcal{O}_L$. $\sigma\alpha - \alpha \in \mathfrak{P}$

$\Rightarrow \sigma\alpha - \alpha \in \mathfrak{P} \cap \mathcal{O}_L = \mathfrak{Q}$.

$\therefore \psi : I_{\mathfrak{P}/\mathfrak{p}} \to I_{\mathfrak{Q}/\mathfrak{p}}$.

$$\begin{array}{ccccc} 0 & & 0 & & \\ \downarrow & & \downarrow & & \\ I_{\mathfrak{P}/\mathfrak{p}} & \to & I_{\mathfrak{Q}/\mathfrak{p}} & & \text{surjective.} \\ \downarrow & & \downarrow & & \\ D_{\mathfrak{P}/\mathfrak{p}} & \to & D_{\mathfrak{Q}/\mathfrak{p}} & & \\ \downarrow & & \downarrow & & \\ Gal(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) & \to & Gal(\mathbb{F}_{\mathfrak{Q}}/\mathbb{F}_{\mathfrak{p}}) & & \\ \downarrow & & \downarrow & & \\ 0 & & 0 & & \end{array}$$

RAMIFICATION and DISCRIMINANT.

Goal: $\mathfrak{P} \mid \mathfrak{D}_{K/\mathbb{Q}} \Leftrightarrow \mathfrak{p}$ ramifies in K.

Def: The different $\mathfrak{d}_{K/\mathbb{Q}}$ is the ideal of $\mathcal{O}_K$, s.t.

$$\mathfrak{d}_{K/\mathbb{Q}}^{-1} = \{\alpha \in K : \forall \beta \in \mathcal{O}_K, \operatorname{tr}_{K/\mathbb{Q}}(\alpha\beta) \in \mathbb{Z}\}.$$

pf: if $\forall \gamma \in \mathcal{O}_K$, $\beta \in \mathfrak{d}_{K/\mathbb{Q}}^{-1}$, $\alpha \in \mathcal{O}_K$,

$\operatorname{tr}_{K/\mathbb{Q}}(\gamma\beta\alpha) = \operatorname{tr}_{K/\mathbb{Q}}(\beta(\alpha\gamma)) \in \mathbb{Z} \Rightarrow \forall \beta \in \mathfrak{d}_{K/\mathbb{Q}}^{-1}$

$\Rightarrow \mathfrak{d}^{-1}$ from. ideal.

$\mathfrak{d}_{K/\mathbb{Q}}^{-1} \supset \mathcal{O}_K \Rightarrow \mathfrak{d}_{K/\mathbb{Q}} \subset \mathcal{O}_K$

Eg: $\mathbb{Q}(\sqrt{5})$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ $\mathfrak{d}_{K/\mathbb{Q}}^{-1} = (\sqrt{5})^{-1}\mathcal{O}_K$. $\Rightarrow \mathfrak{d}_{K/\mathbb{Q}} = (\sqrt{5})\mathcal{O}_K$.

$\mathbb{Q}(\sqrt{3})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ $\mathfrak{d}_{K/\mathbb{Q}}^{-1} = \langle \frac{1}{2}, \frac{1}{\sqrt{3}} \rangle_{\mathbb{Z}} = \frac{1}{\sqrt{3}}\mathcal{O}_K \Rightarrow \mathfrak{d}_{K/\mathbb{Q}} = \sqrt{3}\mathcal{O}_K$.

Thm: $\mathrm{Norm}(\mathfrak{d}_{K/\mathbb{Q}}) = |D_{K/\mathbb{Q}}|$

Pf: Let $L = \mathcal{O}_K$, $Q : L \times L \to \mathbb{Z}$.

$Q(\alpha, \beta) = \mathrm{tr}_{K/\mathbb{Q}}(\alpha\beta)$, $D_{K/\mathbb{Q}} = \mathrm{Disc}(\mathcal{O})$

$L = \langle \omega_1, \cdots, \omega_n \rangle_{\mathbb{Z}} \longrightarrow = \det(\mathrm{tr}(\omega_i\omega_j))$

$\mathfrak{d}_{K/\mathbb{Q}}^{-1} \cong L^*$ ← dual claim $\Leftrightarrow [L^* : L] = \mathrm{Disc}(\mathcal{O})$

① check invariance under L.

② Reduce to diagonal Q

③ check 1-dim case

Thm: Let $\mathfrak{Q} \subset \mathcal{O}_K$ be a prime ideal lying over $p \in \mathbb{Z}$.

$\mathfrak{Q}^e \| p\mathcal{O}_K$.

$\therefore \mathfrak{Q}^{e-1} \mid \mathfrak{d}_{K/\mathbb{Q}}$ $\mathfrak{Q}^e \mid \mathfrak{d}_{K/\mathbb{Q}} \Leftrightarrow p \mid e$

($\mathfrak{Q}$ is wildly ramified)

Pf: $\mathfrak{Q}^{e-1} \mid \mathfrak{d}_{K/\mathbb{Q}} \Leftrightarrow \mathfrak{Q}^{e-1} \supset \mathfrak{d}_{K/\mathbb{Q}} \Leftrightarrow \mathfrak{Q}^{1-e} \subset \mathfrak{d}_{K/\mathbb{Q}}^{-1}$

Let $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{Q}_i^{e_i}$ $\mathfrak{Q} = \mathfrak{Q}_1$

$\mathrm{tr}(\mathfrak{Q}^{1-e}) \subset \mathbb{Z} \Leftrightarrow \mathrm{tr}((p)\mathfrak{Q}^{1-e}) \subseteq p\mathbb{Z}$

tr of every element of $\Leftrightarrow \mathrm{tr}(\mathfrak{Q}_1 \cdot \prod_{i=2}^{g} \mathfrak{Q}_i^{e_i}) \subset p\mathbb{Z}$

Let $\alpha \in \mathfrak{Q}_1 \prod_{i=2}^{g} \mathfrak{Q}_i^{e_i}$, $\tilde{\alpha} \in \mathcal{O}_{K/p} \cong \bigoplus_{i=1}^{g} \mathcal{O}_{K/\mathfrak{Q}_i^{e_i}}$

Note $x\tilde{\alpha}$ is nilpotent, $\mathrm{tr}(x\tilde{\alpha}) = 0$.

Other part:

$\mathfrak{Q}^e \mid \mathfrak{d}_{K/\mathbb{Q}} \Leftrightarrow \mathrm{tr}\left(\prod_{i=2}^{g} \mathfrak{Q}_i^{e_i}\right) \subset p\mathbb{Z}$.

$\alpha \in \prod_{i=2}^{g} \mathfrak{Q}_i^{e_i}$, $\tilde{\alpha} \in \mathcal{O}_{K/p} \cong \bigoplus_{i=1}^{g} \mathcal{O}_{K/\mathfrak{Q}_i^{e_i}}$

Class Number formula

Riemann-Zeta fn: ($K = \mathbb{Q}$)

$$\zeta_{\mathbb{Q}}(s) = \zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$$

$$= \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right)$$

$$= \prod_{p} (1 - p^{-s})^{-1}$$

- $\zeta(s)$ converges absolutely for $\mathrm{Re}(s) > 1$
  - $\left|\frac{1}{n^s}\right| = \frac{1}{n^{\mathrm{Re}(s)}}$ $\quad \sum_{n\geq 1} \frac{1}{n^\sigma} \sim \int_1^\infty \frac{1}{t^\sigma}\, dt$
  - $-\log|1 - p^{-s}| \sim -p^{-s}$
- Consider $\zeta_0(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots$

$$\to \zeta_0(s) = \zeta(s)\left(1 - 2^{-s}\right)\left(1 - \frac{1}{2^s} - \frac{1}{4^s} - \cdots\right) = \zeta(s)\left(1 - 2^{-s}\right)\left(1 - \frac{2^{-s}}{1 - 2^{-s}}\right) = \zeta(s)\left(1 - 2^{1-s}\right)$$

$$\zeta_0(s) = \left(1 - \frac{1}{2^s}\right) + \left(\frac{1}{3^s} - \frac{1}{4^s}\right) + \cdots$$

$$= \sum_{n\geq 1} \left(\frac{1}{(2n-1)^s} - \frac{1}{(2n)^s}\right)$$

Claim: This converges absolutely for $\mathrm{Re}(s) > 0$.

pf: $\frac{d}{dx} x^{-s} = (-s)x^{-s-1}$

$$\Rightarrow \left|\frac{1}{(2n-1)^s} - \frac{1}{(2n)^s}\right| = \left|\int_{2n-1}^{2n} s \cdot x^{-s-1}\, dx\right| \leq |s| \cdot |2n-1|^{-\mathrm{Re}(s)-1}$$

Cor: $\zeta(s)$ extends meromorphically with possible poles at $s = 1 + \frac{2\pi i}{\ln 2} \cdot \mathbb{Z}$.

Consider $\zeta_1(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} + \cdots$

$$= \zeta(s)\left(1 - 3^{-s}\right)\left(1 - \frac{2}{3^s} - \frac{2}{9^s} - \cdots\right)$$

$\Rightarrow \zeta_1(s)$ ✓

poles only at $s = 1 + \frac{2\pi i}{\ln 3} \cdot \mathbb{Z}$.

Intersection is just $s = 1$.

Thm: $\operatorname{Res}_{s=1} \zeta_{\mathbb{Q}}(s) = 1$

Pf: Consider $\zeta_{\mathbb{Q}}(s) - \int_1^\infty x^{-s}\,ds$. $\quad = \left.\frac{x^{1-s}}{1-s}\right|_1^\infty = -\frac{1}{1-s}$

$$= \sum_{n\geq 1} \frac{1}{n^s} - \int_n^{n+1} x^{-s}\,dx = \sum_{n\geq 1} \int_n^{n+1} (n^{-s} - x^{-s})\,dx$$

Converges absolutely as $\operatorname{Re}(s) > 0$.

Dedekind ζ fns:

Let k # field,

$$\zeta_k(s) = \sum_{\substack{I \leq \mathcal{O}_k \\ \text{ideals}}} \operatorname{Norm}(I)^{-s} = \sum_I N(I)^{-s}$$

$$= \prod_{\substack{P_{\neq 0} \text{ prime ideals}}} (1 - N(\mathfrak{p})^{-s})^{-1}$$

Lemma: For $\sigma \in \mathbb{R}_{>1}$, $d = [k:\mathbb{Q}]$

$$\zeta_k(\sigma) \leq \zeta_{\mathbb{Q}}(\sigma)^d.$$

Pf: $\forall$ prime number p,

$$p\mathcal{O}_k = \prod_{i=1}^g \mathfrak{p}_i^{e_i}, \quad N(\mathfrak{p}_i) = p^{f_i}$$

$$\Rightarrow \sum_{i=1}^g e_i f_i = d.$$

The "p-factor" of $\zeta_k(\sigma)$ is $\prod_{i=1}^g (1 + p^{-f_i\sigma} + p^{-2f_i\sigma} + \cdots)$

$$\leq (1 + p^{-\sigma} + p^{-2\sigma} + \cdots)^d$$

Multiply, give us the result.

Thm: (Class number formula)

$\zeta_k(s)$ extends meromorphically to $s > 1 - \frac{1}{d}$, with a unique simple pole at $s = 1$, $\operatorname{Res}_{s=1} \zeta_k(s) = \dfrac{2^{r_1}(2\pi)^{r_2} |Cl(k)| \operatorname{Reg}_k}{w_k \cdot |\operatorname{Disc}_k|^{\frac{1}{2}}}$ (regulator)

$w_k = |\mathcal{O}_k^\times[\text{tor}]| = \#$ roots of unity in k. $\quad A_k$.

Thm: Define $N_k(x) = \#\{I \leq \mathcal{O}_k,\ N(I) \leq x\}$

$(N_{\mathbb{Q}}(x) = \lfloor x \rfloor)$

thm $N_k(x) = A_k \cdot x + O(x^{1-\frac{1}{d}})$

$(f = O(g) \Rightarrow \exists c, \forall t, |f| < c|g|$

"Thm 2 $\Rightarrow$ Thm 1"

$$\zeta_k(s) = \sum_{I \subset \mathcal{O}_k} N(I)^{-s} = \sum_{n \geq 1} n^{-s}(N_k(n) - N_k(n-1))$$

$$= \sum_{n \geq 1} N_k(n) \cdot (n^{-s} - (n+1)^{-s})$$

$$= \sum_{n \geq 1} \left(A_k \cdot n + O(n^{1-\frac{1}{d}})\right) \cdot (n^{-s} - (n+1)^{-s})$$

$$\sum_{n \geq 1} O(n^{1-\frac{1}{d}}) \underbrace{(n^{-s} - (n+1)^{-s})}_{O(n^{-\mathrm{Re}(s)-1})}$$

$$= \sum_{n \geq 1} O\left(n^{\frac{1}{d} - \mathrm{Re}(s)}\right) \quad \text{converges abs if } \mathrm{Re}(s) > 1 - \frac{1}{d}$$

$$\sum_{n \geq 1} A_k \cdot n (n^{-s} - (n+1)^{-s}) = A_k \zeta_k(s)$$

e.g.: ① $k = \mathbb{Q}(i)$ $\qquad \mathcal{O}_k \setminus \{0\} \xrightarrow{4 \to 1} \{\text{non-zero ideals}\}$ ($\{\pm 1, \pm i\}$, pid)

$\alpha \longmapsto (\alpha)$

$\Rightarrow N_k(x) = \frac{1}{4} \#\{\alpha \in \mathcal{O}_k \setminus \{0\},\ N(\alpha) \leq x\}$ $\qquad W_k = 4$

$= (-\frac{1}{4}) + \frac{1}{4} \#\{(a,b) \in \mathbb{Z}^2 : a^2 + b^2 \leq x\}$ ("0")

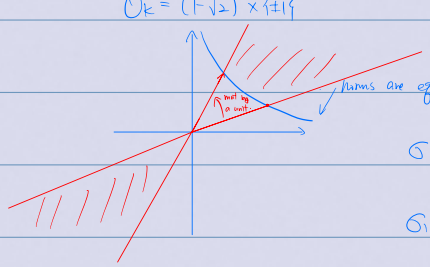
$= (-\frac{1}{4}) + \frac{1}{4} \pi x + O(x^{\frac{1}{2}})$ (area)

② $k = \mathbb{Q}(\sqrt{2})$ $\qquad \mathcal{O}_k \setminus \{0\} \xrightarrow{\infty \to 1} \{\text{non-zero ideals}\}$ (infinite many units, pid)

$\mathcal{O}_k^\times$

$\alpha \longmapsto (\alpha)$

$\mathcal{O}_k^\times = (1+\sqrt{2})^{\mathbb{Z}} \times \{\pm 1\}$

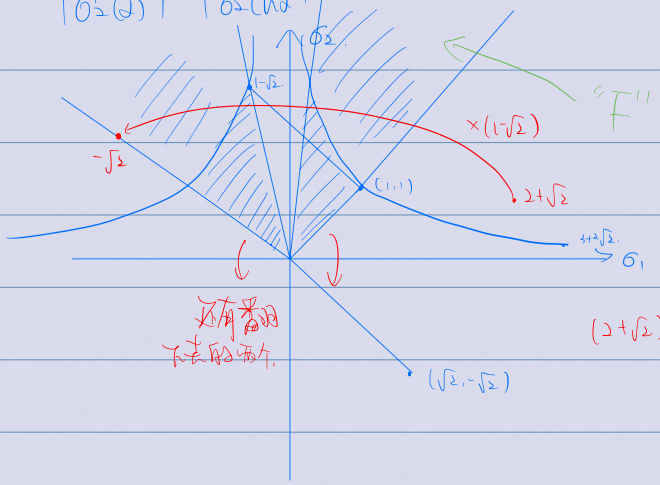


$\sigma_1, \sigma_2 : k \to \mathbb{R}$.

$\sigma_1(\sqrt{2}) = \sqrt{2}$

$\sigma_2(\sqrt{2}) = -\sqrt{2}$.

$$\left|\frac{\sigma_1(\omega)}{\sigma_2(\omega)}\right| = \left|\frac{\sigma_1(\lambda\omega)}{\sigma_2(\lambda\omega)}\right|$$



$(2+\sqrt{2})(1-\sqrt{2}) = -\sqrt{2}$.

$$F = \left\{\alpha \in O_k \setminus \{0\},\ s.t.\ \left|\frac{\sigma_1(\alpha)}{\sigma_2(\alpha)}\right| \le \left|\frac{\sigma_1(\omega)}{\sigma_2(\omega)}\right| \le \left|\frac{\sigma_1(1)}{\sigma_2(1)}\right| = 1\right\}$$

$O_k \cap \vec{\sigma}^{-1}(F) \xrightarrow{\lambda \to 1} \{\text{non-zero ideals}\}$ (因为 ± 1)

$\alpha \longmapsto (\alpha)$

$\Rightarrow N_k(x) = \#\{\alpha \in O_k \cap \vec{\sigma}^{-1}(F) : N(\alpha) \le x\}/2$.

Def: $F_{\le x} := F \cap \{(a,b) \in \mathbb{R}^2 : ab \le x\}$

$N_k(x) = \frac{\mathrm{Vol}(F_{\le x})}{2} + O(x^{\frac{1}{2}})$

$F_{\le x} = F_{\le 1} \cdot \sqrt{x}$

$\Rightarrow \mathrm{Vol}(F_{\le x}) = \mathrm{Vol}(F_{\le 1}) \cdot x$

$dxdy \xrightarrow{M=xy,\ N=\frac{x}{y}} x=\sqrt{MN},\ y=\sqrt{\frac{M}{N}}$

$x=e^s,\ y=e^t$. $dxdy = dtdse^{s+t} = 2dudve^v =$

$u=s+t,\ v=s-t$

$\int 2dudve^u$

$0 \le V \le \ln\left|\frac{\sigma_2(u)}{\sigma_1(u)}\right|$

$-\infty \le u \le 0$

$= 2 \cdot \ln\left|\frac{\sigma_2(u)}{\sigma_1(u)}\right|$ 2 × regulator.

Def: $S \subseteq \mathbb{R}^n$ is a manifold with boundary if S can be written as a disjoint finite union of images $\sigma: [0,1]^d \to \mathbb{R}^n$, where σ is C^1 and injective.

Lemma: For S as above, $t>0$,

$$\#(tS \cap \mathbb{Z}^n) = t^n \cdot \mathrm{Vol}(S) + O(t^{n-1})$$

Pf: Consider boxes of form $\vec{v} + [0,1]^n$, $\vec{v} \in \mathbb{Z}^n$,

$$\mathrm{Vol}(tS) = t^n \mathrm{Vol}(S) = \sum_{\vec{v}} \mathrm{Vol}(tS \cap (\vec{v} + [0,1]^n))$$

$$= \#(tS \cap \mathbb{Z}^n) + O(B_1(\partial S) \cap \mathbb{Z}^n)$$

$n-1$ dim $\Rightarrow$ $\#B_1(\partial S) \cap \mathbb{Z}^n \le \mathrm{Vol}(\pi_{\mathbb{R}^{n-1}}(\partial S)) \le O(t^{n-1})$.

Let K: #-field. $K_{\mathbb{R}} := \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$

$$K_{\mathbb{R}}^\times := (\mathbb{R}^\times)^{r_1} \oplus (\mathbb{C}^\times)^{r_2}.$$

$\mathbb{R}^\times \cong \mathbb{R} \times \mathbb{Z}/2$. $\quad r \to (\log \underbrace{|r|}_{t}, \operatorname{sing}|r|)$

$\Rightarrow dr = r\,dt = e^t dt$

$C^\times \cong \mathbb{R} \times S^1 \cong \mathbb{R}/2\pi\mathbb{Z}$ $\quad z \to (\log \underbrace{|z|}_{r}, \arg(z)^{\theta})$

$dA = e^r dr\, d\theta$

$K_{\mathbb{R}}^\times \cong \mathbb{R}^{r_1+r_2} \oplus (\mathbb{Z}/2)^{r_1} \oplus (S^1)^{r_2}$.

$T: \mathbb{R}^{r_1+r_2} \to \mathbb{R}$ $\quad T(x_1, \cdots, x_{r_1}, y_1, \cdots, y_{r_2}) = \sum x_i + 2\sum y_j$

$\Rightarrow \mathbb{R}^{r_1+r_2} \cong \mathbb{R} \oplus \ker(T)$ ($\mathbb{R}^{r_1+r_2-1}$)

$O_k^\times / O_{k,\mathrm{tor}}^\times \xrightarrow{\Psi} \ker T$.

$O_{k,\mathrm{tor}}^\times$: 某个子群

$U_k := \mathrm{im}\,\Psi$

Take $P \subset \ker T$ - fundamental $\square$ for U_k.

$K_{\mathbb{R}}^\times \xrightarrow{\sim} \mathbb{R}^{r_1+r_2} \oplus (\mathbb{Z}/2)^{r_1} \oplus (S^1)^{r_2} \xrightarrow{\pi} \ker T$

$F \subset K_{\mathbb{R}}^\times := \pi^{-1}(P)$

$$N_k(X) = \sum_{\mathfrak{a} \in Cl(k)} N_{k,\mathfrak{a}}(X)$$

$N_{k,\mathfrak{a}}(X) = \#\{\alpha O_k^\times : \alpha \in \mathfrak{a},\ |\mathrm{Norm}(\alpha)| \le X\}$.

$$= \frac{1}{w_k} \#\{\alpha \in O_k : |\mathrm{Norm}(\alpha)| \le X,\ \sigma(\alpha) \in \mathcal{F}\}$$ (算法格点个数)

$$= \frac{1}{\sqrt{|\mathrm{Disc}(k)|}} \cdot \frac{1}{w_k} \cdot \mathrm{Vol}(\mathcal{F}_{\le X}) + O(X^{1-\frac{1}{d}})$$

$\mathrm{Vol}(\mathcal{F}_{\le X}) = X \cdot \mathrm{Vol}(\mathcal{F}_{\le 1})$

$$\mathrm{Vol}(\mathcal{F}_{\le 1}) = \int_{\mathcal{F}_{\le 1}} d\mu_{\mathrm{Haar}} = \int_{(S^1)^{r_2} \times (\mathbb{Z}/2)^{r_1}} \bigwedge_{i=1}^{r_2} d\theta_i \int_{[-\infty, X]^{r_1}} e^{T(\vec{r})} \wedge dr_i$$

$$= (2\pi)^{r_2} \cdot 2^{r_1} \cdot \int_{-\infty}^{0} e^X \cdot \mathrm{Vol}(\mathcal{P}) \qquad R_k$$

$\#(S \cap \mathbb{Z}^n) \sim \mathrm{Vol}(S)$

$L \subset \mathbb{R}^n \Rightarrow \#(S \cap L) \sim \frac{\mathrm{Vol}(S)}{\mathrm{Covol}(L)}$

$\mathcal{C} = [\mathcal{J}] \in Cl(k)$

$$N_{k,\mathcal{C}}(X) = \#\{\alpha O_k^\times : \alpha \in \mathcal{J}^{-1},\ |\mathrm{Norm}(\alpha)| \le \frac{X}{\mathrm{Norm}(\mathcal{J})}\}.$$

$$= \frac{1}{w_k} \#\{\alpha \in \mathcal{J}^{-1} : |\mathrm{Norm}(\alpha)| \le \frac{X}{N(\mathcal{J})},\ \sigma(\alpha) \in \mathcal{F}\}$$

$$= \frac{N(\mathcal{J})}{\sqrt{|\mathrm{Disc}(k)|}} \cdot \frac{1}{w_k} \cdot \mathrm{Vol}(\mathcal{F}_{\le \frac{X}{N(\mathcal{J})}}) + O(X^{1-\frac{1}{d}})$$

$= \frac{X}{N(\mathcal{J})} \mathrm{Vol}(\mathcal{F}_{\le 1})$

Applications:

$\chi : Cl(k) \longrightarrow \mathbb{C}^\times$

$$L(s, \chi) := \sum_{\mathcal{I} \subseteq O_k} \frac{\chi(\mathcal{I})}{N(\mathcal{I})^s} = \prod_{\mathcal{P} \subseteq O_k} \left(1 - \frac{\chi(\mathcal{P})}{N(\mathcal{P})^s}\right)^{-1}$$ (norm)

if $\chi \neq \mathbb{1}$

Thm: $L(s, \chi)$ analytically continuous to $\mathrm{Re}(s) > 1 - \frac{1}{d}$

Pf: Leading term is $\chi \cdot \frac{2^{r_1}(2\pi)^{r_2} R_k}{\sqrt{\mathrm{Disc}_k} \cdot w_k} \left(\sum_{\mathcal{C} \in Cl(k)} \chi(\mathcal{C})\right)$

Prop: if $\chi \neq \mathbb{1}$, $L(1, \chi) \neq 0$.

Why: e.g. $k = \mathbb{Q}(\sqrt{d})$

$$\zeta_k(s) = \prod_{\mathcal{P}} (1 - N(\mathcal{P})^{-s})^{-1}$$

For $p \in \mathbb{Z}$, if $\left(\frac{p}{d}\right) = 1$, $p O_k = P_1 P_2$ $(1-p^{-s})^{-2}$

if $\left(\frac{p}{d}\right) = -1$, $p O_k$ - Prime $(1-p^{-2s})^{-1}$.

$\zeta_K(s) = \prod_{(\frac{D}{d})=1} (1-p^{-2s})^{-1} \prod_{(\frac{D}{d})=1} (1-p^{-s})^{-2}$ $\quad 1-p^{2s} = (1-p^s)(1+p^s)$

$= \zeta_{\mathbb{Q}}(s) \prod_p (1-(\frac{D}{d})p^{-s})^{-1}$

Prime # theorems:

Cor: $\#\{\mathfrak{p} \subseteq \mathcal{O}_K,\ N(\mathfrak{p}) \le X\} \sim \frac{X}{\log X}$

"pf" $\frac{\zeta_K'(s)}{\zeta_K(s)} = \sum_{\mathfrak{p} \subseteq \mathcal{O}_K} \frac{(\log(N(\mathfrak{p}))}{p^{-s}}$ + small.

residue 1 at $s=1$. $\Rightarrow \sum_{N\mathfrak{p} \le X} \log(N(\mathfrak{p})) \sim X$

Cor: Let $K/\mathbb{Q}$ galois $\#\{p \in \mathbb{Z}\ p \le X,\ p \text{ splits in } K\}$

$\sim \frac{X}{\log X} \frac{1}{[K:\mathbb{Q}]}$

Chapter 3 of S-W

"Special fields"

(1) Cyclotonic fields

(2) Quadratic fields.

Field theory: (Recall)

ζ_n: primitive nth root of unity.

(1) minimal poly over $\mathbb{Q}$ with $\deg(\zeta_n) = \varphi(n)$ $\quad = [\mathbb{Q}(\zeta_n):\mathbb{Q}]$

(2) Conjugate of ζ_n: ζ_n^k, $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, $\begin{cases} \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n) \\ \zeta_n \to \zeta_n^k \end{cases}$ every embedding is complex.

when $n \neq 2$, $r_2 = \frac{1}{2}\varphi(n)$

(3) $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Now: $n = p^r$

Thm: $k = \mathbb{Q}(\zeta)$

① $\mathcal{O}_k = \mathbb{Z}[\zeta]$ if $n \geq 2$.

② $\mathrm{disc}(k) = \Delta_k = (-1)^{\frac{1}{2}\varphi(n)} p^{(p^{r-1}(pr-1))}$

Only prime that ramifies is (p) and $(p) = (1-\zeta)^{\varphi(p^r)}$, $\partial_{k/\mathbb{Q}} = (1-\zeta)^n$

Pf: (1) $\mathrm{disc}(\mathbb{Z}[\zeta]) = [\mathcal{O}_k : \mathbb{Z}[\zeta]]^2 \, \mathrm{disc}(k)$.

$\mathrm{disc}(1, \zeta, \zeta^2, \dots, \zeta^{\varphi(n)-1}) = \pm N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\Phi_n'(\zeta))$

α, f minimal poly, conjugates $\alpha_1, \dots, \alpha_n$

$f(t) = \sum \prod_{i \neq j} (t - \alpha_j) \Rightarrow f'(\alpha_k) = \prod_{k \neq i} (\alpha_k - \alpha_i)$

$G_k = G(\alpha)$, $G(f'(\alpha)) = f'(\alpha_k)$, $N_m(f'(\alpha)) = \pm \prod_{i \neq j} (\alpha_i - \alpha_j)^2$

$\Phi_{p^r}(t) = \frac{t^{p^r} - 1}{t^{p^{r-1}} - 1} \Rightarrow \Phi_{p^r}(t)(t^{p^{r-1}} - 1) = t^{p^r} - 1$

$\Rightarrow \Phi_{p^r}'(t)(t^{p^{r-1}} - 1) + \underbrace{m \cdot \Phi_{p^r}(t)}_{0} = p^r t^{p^{r-1}}$ (m: mth)

$\Rightarrow \Phi_{p^r}'(\zeta)(\zeta^{p^{r-1}} - 1) = p^r \zeta^{p^{r-1}}$

$\Rightarrow N_m(\Phi_{p^r}'(\zeta)) N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\zeta^{p^{r-1}} - 1) = \pm p^{r p^{r-1}(p-1)}$ (★?)

$N_m(p^r) = (p^r)^{p^{r-1}(p-1)}$

pth extension has deg $p^{r-1}(p-1)$

$\omega = \zeta^{p^{r-1}}$, $\omega^p = 1$, $\mathbb{Q}(\zeta)/\mathbb{Q}(\omega)/\mathbb{Q}$

$N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega - 1) = N_{\mathbb{Q}(\omega)/\mathbb{Q}}\left(N_{\mathbb{Q}(\zeta)/\mathbb{Q}(\omega)}(\omega - 1)\right)$

$= \left(N_{\mathbb{Q}(\zeta)/\mathbb{Q}(\omega)}(\omega - 1)\right)^{p^{r-1}}$

$= \pm p^{p^{r-1}}$ ($t^{p-1} + t^{p-2} + \dots + t + 1$)

$\Rightarrow N_m(\Phi_{p^r}'(\zeta)) = \pm p^{r p^{r-1}(p-1) - p^{r-1}}$

$\prod_{k \in \mathbb{Z}^\times / p\mathbb{Z}^\times} (1 - \zeta^k) = \Phi_{p^r}(1) = p$.

$\frac{1-\zeta^k}{1-\zeta} \in \mathcal{O}_k^\times$ (flip) $\frac{1-(\zeta^k)^p}{1-\zeta^k} \in \mathcal{O}_k^\times \Rightarrow (p) = (1-\zeta)^{\varphi(n)}$

$\frac{p}{(1-\zeta)^{\varphi(n)}} \in \mathcal{O}_k$.

Take $\alpha \in \mathcal{O}_k$, $p\alpha \in \mathbb{Z}[\zeta] = \mathbb{Z}[1-\zeta]$

$p\alpha = m_0 + m_1(1-\zeta) + \dots + m_{\varphi(n)-1}(1-\zeta)^{\varphi(n)-1}$, $m_j \in \mathbb{Z}$.

$\in p \mid m_j$, $\forall j$.

Now, $\frac{p}{(1-\zeta)} \in \mathcal{O}_k$, $\forall j < k$.

$\frac{p}{(1-\zeta)}\alpha = \frac{m_0}{(1-\zeta)} + m_1 + (\quad)$ ($\in \mathcal{O}_k$)

$\Rightarrow$ ($\in \mathcal{O}_k$) $\Rightarrow N_m\left(\frac{m_0}{1-\zeta}\right) \in \mathbb{Z}$.

$= \frac{N(m_0)}{N(1-\zeta)} = \frac{m_0^{\varphi(n)}}{p} \in \mathbb{Z} \Rightarrow p \mid m_0$

$\frac{p}{(1-\zeta)^2}\alpha = \frac{m_1}{1-\zeta} + (\quad) \in \mathcal{O}_k$.

Do the same thing.

$(p) = (1-\zeta)^{\varphi(n)}$, know that $e = \varphi(n)$, $fg = \varphi(n) \Rightarrow f = g = 1$.

Lemma: Let K_1, K_2 Galois / $\mathbb{Q}$,

① $K = K_1K_2$ and $K_1 \cap K_2$ Galois

② $[K : K_1] = [K_2 : K_1 \cap K_2]$.

③ $Gal(K/K_1 \cap K_2) \cong Gal(K_1/K_1 \cap K_2) \times Gal(K_2/K_1 \cap K_2)$

pf: ① $K_1 \cap K_2$ contains its conjugates.

for K:

$\sigma : K \hookrightarrow \mathbb{C}$, $\sigma(K_1) \le K_1$, $\sigma(K_2) \le K_2$

② Pick α, s.t. $K_1 = \mathbb{Q}(\alpha) \Rightarrow K = K_2(\alpha)$

α's min polynomial $f(t)$ over $K_1 \cap K_2$. $f(t) = K_1 \cap K_2$. $f(t) = g(t)h(t)$.

$\Rightarrow K_2[t]$

$[K : K_1] = \deg(f) = [K_2 : K_1 \cap K_2]$

Theorem: Let K_1, K_2 be Galois with coprime Disc, $K = K_1K_2$, then

① $K_1 \cap K_2 = \mathbb{Q}$

② $[K : \mathbb{Q}] = [K_1, \mathbb{Q}] \times [K_2, \mathbb{Q}]$

③ $\mathcal{O}_K = \mathcal{O}_{K_1}\mathcal{O}_{K_2}$ and $\partial_{K/\mathbb{Q}} = \partial_{K/\mathbb{Q}}\partial_{K/\mathbb{Q}}$ (different)

Note: $N_{L/K}$, $\partial_{M/\mathbb{Q}} = \partial_{M/L} \cdot \partial_{L/K}$.

Pf: ① In general, if I_1, I_2 are ideals w/ coprime norm, they are coprime. (Ideal contains its norm)

$\text{Norm}(I) = |\mathcal{O}_K / I|$

$\partial_{K_1/\mathbb{Q}}$, $\partial_{K_2/\mathbb{Q}}$ are coprime (in $\mathcal{O}_K$) $(\|I\mathcal{O}_L\| = \|I\|^n)$

$\partial_{K_1/\mathbb{Q}} = \partial_{K_1/K_1\cap K_2} \cdot \partial_{K_1\cap K_2/\mathbb{Q}}$

$\partial_{K_2/\mathbb{Q}} = \partial_{K/K_1\cap K_2} \cdot \partial_{K_1\cap K_2/\mathbb{Q}}$

↳ $K_1 \cap K_2 = \mathbb{Q}$

② $[K : K_1] = [K_2 : K_1 \cap K_2] = [K_2 : \mathbb{Q}]$

$[K : \mathbb{Q}] = [K : K_1][K_1 : \mathbb{Q}]$.

③ $\partial_{K/K_1} \cdot \partial_{K_1/\mathbb{Q}} = \partial_{K/\mathbb{Q}} = \partial_{K/K_2} \cdot \partial_{K_2/\mathbb{Q}}$ (coprime)

$\partial_{K/\mathbb{Q}} = I \, \partial_{K_1/\mathbb{Q}} \partial_{K/K_1}$

Δ_K (norm) $\quad \Delta_{K_1}^{[K_1:\mathbb{Q}]} \quad \Delta_{K_2}^{[K_1:\mathbb{Q}]}$

$\alpha_1, \cdots, \alpha_n$ integral bases for K_1

$\beta_1, \cdots \beta_m$ - - - - - - K_2

$\alpha_i \beta_j$ - - - - - - for K.

↳ $\mathbb{Q}$-basis.

$\forall \eta \in \mathcal{O}_K, \quad \eta = \sum_i \sum_j \frac{c_{ij}}{d} \alpha_i \beta_j, \quad c_{ij}, d \in \mathbb{Z}$.

$\gcd(d, \gcd(c_{ij})) = 1$.

Take $\sigma_1, \cdots, \sigma_n$ elements $\text{Gal}(K/K_2)$

restrict exactly to the elements of $\text{Gal}(K/\mathbb{Q})$

$\gamma_i = \sum_{j=1}^{m} \frac{c_{ij}}{d} \beta_j \in K_2, \quad \eta = \sum_{i=1}^{n} \gamma_i \alpha_i$

$\mathcal{O}_K \ni \sigma_j(\eta) = \sum_{i=1}^{n} \gamma_i \sigma_j(\alpha_i) \quad 1 \le j \le n$,

$A \begin{bmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{bmatrix} \in \mathcal{O}_K \qquad \text{adj}(A) A = \det(A) = \sqrt{\Delta_K}$.

$\Rightarrow \forall i, \ \sqrt{\Delta_K} \gamma_i = x_i \in \mathcal{O}_K$.

$\Delta_{k_1}\gamma_i = \sqrt{\alpha_{k_1}}\alpha_i$ is algebric

$\Delta_{k_1}\gamma_i = \sum_{j=1}^{m} \frac{\Delta_{k_1} c_{ij}}{d} \beta_j \in \mathcal{O}_{k_2}$.

$\Rightarrow d \mid \Delta_{k_1} c_{ij}$

$\Rightarrow d \mid \Delta_{k_1}$ coprime

$d \mid \Delta_{k_2}$

$\Rightarrow d = \pm 1$.

$m = m_1 m_2$, m_1, m_2 coprime,

$\zeta_{n_1} \to m_1$,

$\zeta_{n_2} \to m_2$.

$\zeta_n \to m$

$\exists\, x m_1 + y m_2 = 1$

Claim: $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})$

$\geq$ by taking $\zeta_{n_1}^{m_2} / \zeta_{n_2}^{m_1}$ 且 $\zeta_{n_1}^{m_1} = \zeta_{n_1}^{b}$, $\zeta_{n_2}^{m_2} = \zeta_{n_1}^{a}$.

$\zeta_n = \zeta_n^1 = \zeta_n^{m_1 x + m_2 y} = \zeta_{n_2}^{bx} \zeta_{n_1}^{ay} \Rightarrow =$

$\Downarrow$

① $K = \mathbb{Q}(\zeta_n)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$

② You know the disk and the norm.

③ primes that ramify are exactly those which divide n (except 2)

$p \mid m$, $m = p^r n$, $p \nmid n$.

$\mathbb{Q}(\zeta_n)$ e', f', g'

$p = (1-\zeta_n)^{\varphi(p^r)}$ $\mathbb{Q}(\zeta_n^{p^r})$ $\mathbb{Q}(\zeta_n^n)$ $(p) = \mathcal{O}_1 \cdots \mathcal{O}_g$

$e = 1$, f, g.

$\varphi(m) = e'f'g'$

$\varphi(p^r)\varphi(n)$

$\leq \varphi(p^r) fg$

$= \varphi(p^r)\varphi(m)$

$\Rightarrow f' = f \quad g' = g$

① $e' \geq \varphi(p^r)$

② $fg = \varphi(m)$

③ $f' \geq f,\ g' \geq g.$

p in $\mathbb{Q}(w)$

Let $\mathcal{Q}$ be a prime over p.

$\mathbb{Z}[w]/\mathcal{Q} / \mathbb{Z}/p\mathbb{Z}.$

deg = f = inertia degree.

Gal = generated by $\tau: x \to x^p$

$a \in \mathbb{Z}$, $\tau^a = 1 \Leftrightarrow \tau^a(w) \equiv w \pmod{\mathcal{Q}}$

w^{p^a}

$\Leftrightarrow w^{p^a - 1} \equiv 1 \pmod{\mathcal{Q}}$

$b = p^a \pmod n \quad 1 \leq b \leq n.$

$\Leftrightarrow w^{b-1} \equiv 1 \pmod{\mathcal{Q}}$

$(1-w)(1-w^2)\cdots(1-w^{n-1}) = n$

$\Leftrightarrow 1 - w^{b-1} \in \mathcal{Q}$

if $b-1 > 0$, then $n \in \mathcal{Q}$

$\mathcal{Q}$ lies over p, so $p \in \mathcal{Q}$

So $\tau^a = 1 \Leftrightarrow p^a \equiv 1 \pmod n$

$\mathrm{ord}(p) = \mathrm{ord}(\tau) = f$

$K = \mathbb{Q}(\sqrt{D})$, D sq free

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & D \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & D \equiv 1 \mod 4 \end{cases}$$

$$\Delta_K = \begin{cases} 4D & D \equiv 2,3 \pmod 4 \\ D & D \equiv 1 \mod 4 \end{cases}$$

$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$, $efg = 2$.

① $e = 2$ ↓ $p\mathcal{O}_K = \mathfrak{Q}^2$ ② $f = 2$ ↓ $p\mathcal{O}_K = \mathfrak{p}$ ③ $g = 2$ ↓ $p\mathcal{O}_K = \mathfrak{Q}_1\mathfrak{Q}_2$.

4/6 $L = \mathbb{Q}(\beta)$, f min poly, $\beta \in \mathcal{O}_L$, prime p

$\bar{f}(x) = \prod f_i(x) \Rightarrow p\mathcal{O}_L = \prod(\mathfrak{p}, \tilde{f}_i(\beta))$.

$x^2 - D$

① $p \neq 2$, $p \nmid D$, $\bar{x}^2 - D \pmod p$

if N a not	N not
$(\bar{x} - N)(\bar{x} + N)$	
$p\mathcal{O}_L = (p, \sqrt{D}+N)(p, \sqrt{D}-N)$	$p\mathcal{O}_L$.

② $p \mid D$. $p\mathcal{O}_L = (p, \sqrt{D})^2$

$(p, p\sqrt{D}, D) \subset \mathfrak{p}\mathcal{O}_K$.

(squarefree)

(3) $p=2$ D odd, $D \equiv 1, 3 \pmod 4$

i) $D \equiv 3 \pmod 4$, $\mathbb{Z}[D]/(X^2-D)$

$= \mathbb{F}_2[D]/(X^2-1)$

$= \mathbb{F}_2[D]/(X-1)^2$.

$\Rightarrow \mathfrak{p}\mathcal{O}_K = (2, \sqrt{D}-1)^2$

ii) $D \equiv 1 \pmod 8$ $X^2 - X + \frac{1-D}{4}$ (even) $\Rightarrow X^2 - X$.

$\mathfrak{p}\mathcal{O}_K = (2, \frac{1+\sqrt{D}}{2})(2, \frac{-1+\sqrt{D}}{2})$

iii) $D \equiv 5 \pmod 8$ $\frac{1-D}{4}$ odd

$X^2 - X + 1$ irred. $\mathfrak{p}\mathcal{O}_K$ is prime.

$aX^2 + bXY + cY^2$

$\mathrm{Norm}_K(X + \sqrt{D}Y) = X^2 - DY^2$

$0 \neq \mathfrak{I} \subseteq \mathcal{O}_K$. $m \in \mathbb{Z}$, $m\mathcal{O}_K \subseteq \mathfrak{I} \subseteq \mathcal{O}_K$.

$\mathfrak{I} = \langle \alpha_1, \alpha_2 \rangle_{\mathbb{Z}}$.

$\mathrm{Nm}_K(X_1\alpha_1 + X_2\alpha_2) = X_1^2(\mathrm{Nm}_K(\alpha_1)) + X_1X_2(\alpha\sigma(\alpha_2) + \alpha_2\sigma(\alpha_1)) + X_2^2\mathrm{Nm}_K(\alpha_2)$

$aX^2 + bXY + cY^2$, $b^2 - 4ac$

disc of this form is $\mathrm{disc}(\mathfrak{I}) = \mathrm{Norm}(\mathfrak{I})^2 \Delta_K$.

$M = GL_2(\mathbb{Z})$, $f(x,y) = aX^2 + bXY + cY^2$

$(M \cdot f)(x,y) = f((x,y)M)$

$a \geq |b|$ $a \leq c$.

$d = \mathrm{disc}(f)$ $\quad d = b^2 - 4ac$

$3a^2 \le 4a^2 - b^2 \le 4ac - b^2 = -d$

$\Rightarrow a \le \sqrt{\frac{-d}{3}}$

$b \le a$

Lemma: $p \in \mathbb{Z}$, $K = \mathbb{Q}(\sqrt{D})$, $h_K = 1$

if $p \le \frac{\pi}{4}\sqrt{|D|}$ then $p\mathcal{O}_K$ is prime

Pf: Thm: is a prime over p, $\mathcal{O}$,

$N(\mathcal{O}) = p$,

$\mathcal{O} = \left(\frac{m + n\sqrt{D}}{2}\right)$

Kronecker – Weber thm:

$\mathbb{Q}^{cyc} = \bigcup_{n \in \mathbb{N}^+} \mathbb{Q}(\mu_n) \subset \overline{\mathbb{Q}}$

$\mathrm{Gal}(\mathbb{Q}^{cyc}/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$

$= \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = (\hat{\mathbb{Z}})^\times$ Abelian

$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$

$\forall$ field k, consider the maximal $L \subset \bar{k}$,

s.t. L/k abelian. k^{ab}.

(1) $L \subset \bar{k}$ finite, s.t. L_i/k abelian. $i = 1, 2$.

$L_1 L_2$ also finite abelian.

(2) $G_k = \mathrm{Gal}(\bar{k}/k)$, $k^{ab} = \bar{k}^H$ $H \lhd G_k$ closed.

G/H abelian. let $H = [G, G]$ – closed subgp.

Thm: $\mathbb{Q}^{ab} = \mathbb{Q}^{cyc}$ (every abelian ext^n of $\mathbb{Q}$ is contained in a cyclotomic field)

Remark: False for any $K \neq \mathbb{Q}$

i.e. $K^{cyc} < K^{ab}$ very difficult.

Kummer Theory:

Thm: (Hilbert 90) Let K = field with char 0.

Let L/K be an abelian extension, $Gal(L/K) \cong \mathbb{Z}/n\mathbb{Z}$.

Let $\langle \sigma \rangle = Gal(L/K)$, then

① Let $\beta \in L^\times$, s.t. $Nm_{L/K}(\beta) = 1$.

then $\exists \alpha \in L^\times$, $\beta = \frac{\sigma(\alpha)}{\alpha}$

② Let $\beta \in L^\times$, s.t. $Tr_{L/K}(\beta) = 1$ "0"?

then $\exists \alpha \in L^\times$, $\beta = \alpha - \sigma(\alpha)$

Pf: ①: Pick $t \in L$, s.t. $L = K(t)$,

Consider $S = \beta + \beta\sigma(\beta) + \beta\sigma(\beta)\sigma^2(\beta) + \cdots$

$$= \sum_{i=0}^{n-1} \prod_{j=0}^{i} \sigma^j(\beta)$$

$$\sigma(S) = \sigma(\beta) + \sigma(\beta)\sigma^2(\beta) + \cdots + \sigma(\beta)\sigma^2(\beta)\cdots\sigma^n(\beta)$$

$$= \sum_{i=0}^{n-1} \prod_{j=1}^{i+1} \sigma^j(\beta)$$

$$= \frac{S}{\beta}$$

If $S \neq 0$, $\frac{\sigma(S)}{S} = \beta^{-1} \Rightarrow \frac{\sigma(S^{-1})}{S^{-1}} = \beta$

For $r \in L$, $S_r = r\beta + \sigma(r)\beta\sigma(\beta) + \cdots$

$$= \sum_{i=0}^{n-1} \sigma^i(r) \prod_{j=0}^{i} \sigma^j(\beta)$$

$$\sigma(S_r) = \frac{S_r}{\beta}$$

Need: $\exists r \in L$, $S_r \neq 0$. 才能在 L 上的 linear map.

If $\forall r \in L$, $S_r = 0$, $\exists$ const $c_i \in L$, not all 0,

s.t. $\sum_{i=0}^{n-1} c_i \sigma^i = 0$.

Pick such a relation with fewest possible $c_i \neq 0$.

If $(c_0, \cdots, c_{n-1})$ gives a relation, pick $c \in L$,

$\Rightarrow (cc_0, \sigma(c)c_1, \cdots, \sigma^{n-1}(c)c_{n-1})$ also a such relation.

In particular: $c = t$, get another relation

which must be proptional to $(c_0, \cdots, c_{n-1})$ (等价类讲解3).

$(tc_0, \sigma(t)c_1, \cdots, \sigma^{n-1}(t)c_{n-1}) \sim (c_0, c_1, \cdots, c_{n-1})$

but $L = k(t)$, $\sigma^i(t)$ 可以不等一样, $\Rightarrow \Leftarrow$.

② $\beta \in L$, $\mathrm{Tr}_{L/k}\beta = 0$.

let $S = \beta + 2\sigma(\beta) + 3\sigma^2(\beta) + \cdots + n\sigma^{n-1}(\beta)$

$\sigma(S) = \sigma(\beta) + 2\sigma^2(\beta) + \cdots + (n-1)\sigma^{n-1}(\beta) + n\beta$

$\Rightarrow S - \sigma(S) = \sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{n-1}(\beta) - (n-1)\beta$

$= (\beta + \sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{n-1}(\beta)) - n\beta$

$= -n\beta$ ($\beta + \sigma(\beta) + \cdots + \sigma^{n-1}(\beta) = \mathrm{Tr}$)

Let $\alpha = \frac{-S}{n}$, $\alpha - \sigma(\alpha) = \beta$

Thm (Kummer)

L/k Gal with $\mathrm{char} = 0$, $\mathrm{Gal}(L/k) \cong \mathbb{Z}/n\mathbb{Z} = \langle \sigma \rangle$

Assume $\mathbb{Q}(\zeta_n) \subset k$.

then $\exists \alpha \in L^\times$, s.t. $L = k(\alpha)$, $\alpha^n = \beta \in k^\times$.

Note: If $\mathbb{Q}(\zeta_n) \subset k$, $L = k(\alpha)$, $\alpha^n = \beta \in k$,

$\Rightarrow L/k$ galois abelian

$\psi: Gal(L/k) \hookrightarrow \mu_n = \{x : x^n = 1\}$

$\tau \hookrightarrow \frac{\tau\alpha}{\alpha}$

well-defined since

$\tau_1(\tau_2(\alpha)) = \tau_1(\alpha \cdot \psi(\tau_2)) = \tau_1(\alpha)\cdot\tau_1(\psi(\tau_2)) = \alpha\,\psi(\tau_1)\cdot\psi(\tau_2)$

$\psi(\tau_1\tau_2) = \alpha\,\psi(\tau_1)\psi(\tau_2)$.

Pf: Let $\zeta_n \in k$: primitive nth root of unity.

$Nm\,\zeta_n = \prod \sigma^i(\zeta_n) = 1$

$\Rightarrow \exists \alpha \in L$, s.t. $\sigma(\alpha) = \zeta_n\alpha$.

$L = k(\alpha)$

$\sigma(\alpha^n) = (\sigma(\alpha))^n = (\zeta_n\alpha)^n = \alpha^n$

$\Rightarrow \alpha^n = \beta \in k$.

Cor: $\left\{ \begin{array}{l} L/k \\ Gal(L/k) \cong \mathbb{Z}/n\mathbb{Z} \end{array} \right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{ \begin{array}{l} G < k^\times/(k^\times)^n \\ G \cong \mathbb{Z}/n\mathbb{Z} \end{array} \right\}$.

Pf: Let $\tilde{\beta} \in k^\times/(k^\times)^n$, pick $\beta \in k^\times$ lifting to $\tilde{\beta}$

define $\psi(\tilde{\beta}) = k(\sqrt[n]{\beta})$

Well-defined otherwise if other lift $\beta' = \beta \cdot c^n$.

$k(\sqrt[n]{\beta}) = k(\sqrt[n]{\beta'})$

Suppose $Gal(L/k) \cong \mathbb{Z}/m\mathbb{Z}$, $m \mid n$, $m \neq n$.

Let $\langle\sigma\rangle = Gal(L/k)$, let $\alpha = \sqrt[n]{\beta}$, $\sigma\alpha = \zeta_n \cdot \alpha$.

$\Rightarrow \sigma(\alpha^m) = (\sigma\alpha)^m = \alpha^m$

$\Rightarrow \alpha^m \in k^\times \Rightarrow \beta = (\alpha^m)^{\frac{n}{m}} \in (k^\times)^{\frac{n}{m}}$

For Ψ:

Let $\alpha \in L^\times$, s.t. $\frac{\sigma(\alpha)}{\alpha} = \zeta_n$, $\langle\sigma\rangle = Gal(L/k)$

Given such α, α', $\alpha k^\times = \alpha' k^\times$

$\alpha^n \in k^\times$, $(\alpha')^n \in \alpha^n (k^\times)^n$

$\Rightarrow [\alpha^n] \in k^\times/(k^\times)^n$ well-defined.

$\psi(L) := \langle [\alpha^n] \rangle < k^\times/(k^\times)^n$

Cor: Let $\mathbb{Q}(\zeta_n) \subset k$,

let $k_n \subset \bar{k}$ be the maximal abe. extension of k,

order?

$\mathrm{ord}(\mathrm{Gal}(k_n/k)) \mid n$.

$\mathrm{Gal}(k_n/k) \cong \mathrm{Hom}(k^\times/(k^\times)^n, \mu_n)$

$\sigma \longrightarrow \left(\bar{\beta} \longrightarrow \frac{\sigma(\sqrt[n]{\beta})}{\sqrt[n]{\beta}}\right)$

Keith Conrad James Milne

Wild-Tame inertia

L/k galois of k-# field.

Let $\mathfrak{p} \in \mathcal{O}_k$ a prime ideal.

Showed: $\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{Q}_i^e$, $G = \mathrm{Gal}(L/k)$ act transitively on $\{\mathfrak{Q}_1, \dots, \mathfrak{Q}_g\}$.

Let $\mathfrak{Q} = \mathfrak{Q}_1$,

Let $D_{\mathfrak{Q}} = \mathrm{stab}(\mathfrak{Q})$ - decomposition group.

$|D_{\mathfrak{Q}}| = ef$

$1 \longrightarrow I_{\mathfrak{Q}} \longrightarrow D_{\mathfrak{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{F}_{\mathfrak{Q}}/\mathbb{F}_{\mathfrak{p}})$

($I_{\mathfrak{Q}}$: inertial group.)

$|I_{\mathfrak{Q}}| = e$, $I_{\mathfrak{Q}} = \ker D_{\mathfrak{Q}} \subset \mathbb{F}_{\mathfrak{Q}}$.

Def: $W_Q \lhd I_Q = \{g \in I_Q : \forall \bar{\alpha} \in \mathcal{O}_L/\mathfrak{Q}^2,\ g(\bar{\alpha}) = \bar{\alpha}\}$.

↑ wild inertial group

Lemma: Let $\pi \in \mathcal{O}_L$ be a uniformizer at/for $\mathfrak{Q}$,

$\mathfrak{Q} \| \pi$.

Let $\sigma \in I_Q$, $\sigma \in W_Q \Leftrightarrow \sigma\pi - \pi \in \mathfrak{Q}^2$ $\quad q = \#\mathbb{F}_Q$

Intuition: uniformizer $\longleftrightarrow$ local coord.

pf: $\Rightarrow$ clear.

$\Leftarrow$: Note that $\#(\mathcal{O}_L/\mathfrak{Q}^2)^\times = \#(\mathcal{O}_L/\mathfrak{Q})^\times \cdot \#(\mathfrak{Q}\mathcal{O}_L/\mathfrak{Q}^2)$

$= (q-1)q$

$\exists H < (\mathcal{O}_L/\mathfrak{Q}^2)^\times$ $\#H = q-1$, $H \xrightarrow{\sim} \mathbb{F}_Q^\times$

$\therefore (\mathcal{O}_L/\mathfrak{Q}^2)^\times \cong H \oplus (1+\pi\mathcal{O}_L)\mathfrak{Q}^2$ (mod $\mathfrak{Q}^2$)

$\sigma \in I_Q \Rightarrow \sigma$ acts trivially on $\mathbb{F}_Q^\times$

Therefore, σ ---------- H

$\sigma \in W_Q \Leftrightarrow \sigma$ fixes $(1+\pi\mathcal{O}_L)\mathfrak{Q}^2$

$\Leftrightarrow (\pi\mathcal{O}_L)/\mathfrak{Q}^2$

$\Leftrightarrow \pi\mathbb{F}_Q/\mathfrak{Q}^2$

$\Leftrightarrow$ fixing π, mod $\mathfrak{Q}^2$

L/K Galois, $G = \mathrm{Gal}(L/K)$ $P \subset \mathcal{O}_K$, $P = \prod_{i=1}^{g} \mathfrak{Q}_i^{e_i}$.

$W_Q \lhd I_Q \lhd D_Q$, $\mathfrak{Q} = \mathfrak{Q}_1$

$W_Q = \mathrm{Stab}(\mathcal{O}_L/\mathfrak{Q}^2) \lhd D_Q$.

$\Pi \in \mathcal{O}_L$ uniformizer at $\mathfrak{Q}$,

$\mathfrak{Q} \| \Pi\mathcal{O}_L$.

$W_Q = \{g \in I_Q,\ g\Pi = \Pi \bmod \mathfrak{Q}^2\}$

THM: $W_Q \lhd I_Q$ is the p-sylow subgroup.

Pf: Let $\tilde{\sigma} \in I_Q/W_Q$ $\sigma \in I_Q$ a lift of $\tilde{\sigma}$

Note that $\sigma\pi$ is also a uniformizer of Q

$Q/Q^2 \cong \mathbb{F}_Q$ as O_L – modules.

$\overline{\alpha\pi} \leftarrow \bar{\alpha}$

Get an well-defined $\frac{\sigma\pi}{\pi} \in \mathbb{F}_Q^\times$

Note: If π' another uniformizer, $\alpha\pi \equiv \pi \bmod Q^2$ $\alpha \notin Q$, $\alpha \in O_L$.

$$\frac{\sigma(\alpha\pi)}{\alpha\pi} = \frac{\sigma(\alpha)}{\alpha} \cdot \frac{\sigma(\pi)}{\pi}$$

$$\frac{\sigma(\tau(\pi))}{\pi} = \frac{\sigma(\tau(\pi))}{\tau(\pi)} \cdot \frac{\tau(\pi)}{\pi} = \frac{\sigma(\pi)}{\pi}\frac{\tau(\pi)}{\pi} \qquad \sigma, \tau \in I_Q.$$

If $\frac{\sigma(\pi)}{\pi} = 1 \in \mathbb{F}_Q^\times$, $\sigma\pi \equiv \pi \bmod Q^2$ $\tilde{\sigma} = 1 \in \frac{I_Q}{W_Q}$.

$I_Q/W_Q \hookrightarrow \mathbb{F}_Q^\times \leftarrow$ coprime to p.

- Let $\sigma \in W_Q \setminus \{1\}$

Claim: $\sigma\pi \neq \pi$

Pf: Assume $\sigma\pi = \pi$, then σ act trivally on O_L/Q^2

Claim: σ act trivally on O_L/Q^m, $\forall m$.

Pf: Assume true for $m-1$

$$\#\left(O_L/Q^m\right)^\times = (q-1)\cdot q^{m-1}$$

$\Rightarrow \exists H < (O_L/Q^m)$ $H = q-1$

$H \xrightarrow{\sim} \mathbb{F}_Q^\times$

Since $\sigma \in I_Q$, $\sigma H = H$.

For $\alpha \in \mathbb{F}_q^\times$, Let $[\alpha] \in H$ be its lift

Consider $\left\{ \sum_{i=0}^{m-1} c_i \pi^i \right\}$, $c_i \in H \cup \{0\}$.

$\cap$

O_L/Q^m

If $\sum c_i\pi^i = \sum c_j\pi^j \Rightarrow \sum (c_i - c_j)\pi^i = 0$

if i_0 smallest $c_i \neq c_j$, then $\sum (c_i - c_j)\pi^i \equiv (c_i - c_j)\cdot \pi^i \neq 0 \pmod{Q^{i+1}}$

$\Rightarrow O_L/Q^m$ is generated by H and π $\Rightarrow \sigma$ fixes O_L/Q^m.

If $\sigma \neq id$, $\exists \alpha \in \mathcal{O}_L$, $\sigma\alpha - \alpha \neq 0 \Rightarrow \exists k$ $\mathcal{Q}^k \| \sigma\alpha - \alpha$ $\Rightarrow \in$

- Let $\sigma \in W_0 \neq id$, $\sigma\pi \neq \pi$.

$\exists m$, s.t. $\mathcal{Q}^m \| \sigma\pi - \pi$, $m \geq 2$.

$\Rightarrow \exists \alpha \in \mathbb{F}_q^\times$, s.t. $\sigma\pi - \pi = \alpha\pi^m \mod \mathcal{Q}^{m+1}$

$\sigma\pi = \pi + \alpha\pi^m \mod \mathcal{Q}^{m+1}$

$\sigma^2\pi \equiv \sigma\pi + \sigma(\alpha)\alpha(\pi)^m \mod \mathcal{Q}^{m+1}$

$\equiv \pi + \alpha\pi^m + (\alpha+\alpha)(\pi+\pi^2)^m \mod \mathcal{Q}^{m+1}$

$\equiv \pi + 2\alpha\pi^m \mod \mathcal{Q}^{m+1}$

$\forall n \in \mathbb{Z}_{\geq 1}$, $\sigma^n\pi \equiv \pi + n\alpha\pi^m \mod \mathcal{Q}^{m+1}$

If $\sigma^n\pi = \pi \Rightarrow n\alpha\pi^m \in \mathcal{Q}^{m+1} \Rightarrow n \in \mathcal{Q} \Rightarrow p \mid n$

$\Rightarrow p \mid \mathrm{ord}(\sigma)$

■

$K = \mathbb{Q}$, $L = \mathbb{Q}[i]$ $p = 2\mathbb{Z}$.

$2\mathcal{O}_L = (1+i)^2$ $W_0 = I_0 = D_0 \cong \mathbb{Z}/2\mathbb{Z}$.

$\| \mathcal{Q}$.

$\pi = 1+i$, $\sigma(\pi) = 1-i = \pi - 2i = \pi - \pi^2$

$\pi^2 = i^2$

- $K = \mathbb{Q}(\sqrt{-3})$, $L = K(\zeta_9)$ $Gal(L/K) = \mathbb{Z}/3\mathbb{Z}$.

$p = (\sqrt{-3})$, $\mathcal{Q} = (1-\zeta_9)$, $W_0 = I_0 = D_0 = Gal(L/K) \cong \mathbb{Z}/3\mathbb{Z}$.

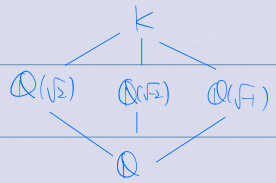
$\sigma(\zeta_9) = \zeta_9^4$, $\pi = 1-\zeta_9$. $\sigma(\pi) = 1-\zeta_9^4 = \pi + \zeta_9 - \zeta_9^4 = \pi + \zeta_9(1-\zeta_9^3)$

Eg: $K = \mathbb{Q}(\sqrt{-1})$.

$\left(\frac{1+i}{\sqrt{2}}\right)^2 = i$ $i^4 = 1$

$[K:\mathbb{Q}] = |(\mathbb{Z}/8\mathbb{Z})^\times| = 4$

$\| \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.



$K = \mathbb{Q}\left(\frac{\alpha}{\sqrt{2}}\right) = \mathbb{Q}(i, \sqrt{2})$

2 is the only ramified prime in K.

In $\mathbb{Q}(\sqrt{d})$, $d = -1, 2, -2$, $(e, f, g) = (2, 1, 1)$

In K, $2\mathcal{O}_K = \mathfrak{p}^4$, 2 totally ramified, $\mathfrak{p} = (1-\alpha)$

$\mathfrak{p}^2 = (1 - 2\alpha + \alpha^2) = (1 + i - 2\alpha) = (1+i)(1-(1-i)\alpha)$

$\pi = 1-\alpha$ is a uniformizer of $\mathfrak{p}$.

$v_{\mathfrak{p}}(\sigma\pi - \pi) \overset{?}{=} 1$, $\sigma \in Gal(K/\mathbb{Q})$

① $\sigma\alpha = \alpha^3$, $v_{\mathfrak{p}}((1-\alpha)^3 - (1-\alpha)) = v_{\mathfrak{p}}(\alpha^3 - 1) = 1 + v_{\mathfrak{p}}(\alpha - 1) + 2 = 2$. (?)

② $\sigma\alpha = \alpha^7$, $v_{\mathfrak{p}}(\alpha^7 - \alpha) = v_{\mathfrak{p}}(\alpha^7 - \alpha) = v_{\mathfrak{p}}(\alpha^2 - 1) = 2$.

α^{-1}

③ $\sigma\alpha = \alpha^5$, $v_{\mathfrak{p}}(\alpha^5 - \alpha) = v_{\mathfrak{p}}(\alpha^4 - 1) = \underbrace{v_{\mathfrak{p}}(\alpha - 1)}_{1} + \underbrace{v_{\mathfrak{p}}(\alpha + 1)}_{1} + \underbrace{v_{\mathfrak{p}}(\alpha^2 + 1)}_{2} = 4$. ($\alpha^2 + 1 = i$, $\alpha + 1 = 2 - (1-\alpha)$)

$4 \quad 2$

$\langle 1 \rangle < \langle -1, 5 \rangle < (\mathbb{Z}/8\mathbb{Z})^\times = Gal(K/\mathbb{Q})$, $4 \equiv 2 \pmod 2$

Pf of Kronecker–Webber:

Goal: $\mathbb{Q}^{ab} = \mathbb{Q}^{cycl}$.

$\Leftrightarrow$ $K/\mathbb{Q}$ abelian $\Rightarrow$ $K \subset \mathbb{Q}^{cycl}$

Reduction 0: Assume $Gal(K/\mathbb{Q})$ is a p-group for some p, and $\cong \mathbb{Z}/p^2$

$Gal(K/\mathbb{Q}) \cong \bigoplus_p G_p$ G_p p-group.

$K_p := K^{\bigoplus_{q \neq p} G_q}$, $K = K_2 K_3 \cdots$

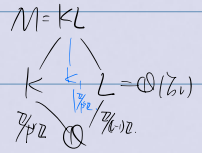
Reduction 2: Can assume further that p is the only prime that (potentially) totally ramified in K.

pf: Suppose not the case, $l \neq p$ is totally ramified in K. $L = \mathbb{Q}^{I_l}$, $\mathbb{F}_{\mathbb{Q}} \cong \mathbb{F}_l$.

$\mathbb{Z}/p^2 \cong I_{\mathbb{Q}} \hookrightarrow \mathbb{F}_{\mathbb{Q}}^\times \cong \mathbb{F}_l^\times \cong \mathbb{Z}/(l-1)$.

$\Rightarrow p^r \mid l-1$

Let $L = \mathbb{Q}(\zeta_l)$, $M = KL$



$\mathrm{Gal}(M/\mathbb{Q}) \lhd \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/(l-1)\mathbb{Z}$.

Since $p^r \mid l-1$, $\mathbb{Z}/(l-1)\mathbb{Z}$ is the largest cyclic subgroup of $\mathrm{Gal}(M/\mathbb{Q})$

Let $I < \mathrm{Gal}(M/\mathbb{Q})$ be the inertia group of a (all primes) prime above l.

I is cyclic since l tamely ramified.

$|I| \geq l-1 \quad \therefore I \cong \mathbb{Z}/(l-1)\mathbb{Z}$

Let $K_1 = M^I$, l is unramified in K_1.

$\therefore$ Nothing ramifies in $K_1 \cap L$.

$\therefore K_1 \cap L = \mathbb{Q}$ by Minkowsky's bound.

$|\mathrm{Disc}\, F| \geq \left(\frac{\pi}{4}\right)^{\frac{n}{2}} \cdot \frac{n^n}{n!} > 1$. prime divides Disc F ramifies

$[M : K_1] = l-1$

in K_1L/K_1, l is ramified to order $\geq l-1$

$\Rightarrow [K_1L : K_1] \geq l-1 \Rightarrow K_1L = M$

$\Rightarrow$ If K_1 is cyclotomic, so is K. 

Claim: $\mathrm{Gal}(K_1/\mathbb{Q}) \cong \mathbb{Z}/p^s\mathbb{Z}$ for some $s \leq r$.

Pf: $\mathrm{Gal}(K_1/\mathbb{Q}) = \mathrm{Gal}(M/\mathbb{Q})/I$, $\mathbb{Z}/(p-1)\mathbb{Z} \cong I \lhd \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/(l-1)\mathbb{Z}$

Also, $I \cap \mathbb{Z}/p\mathbb{Z} \oplus \{1\} = \mathrm{id}$, because $K_1 \cap L = \mathbb{Q}$

which means $\langle I, \mathrm{Gal}(M/L) \rangle = \mathrm{Gal}(M/\mathbb{Q})$

$\mathbb{Z}/p\mathbb{Z} \oplus \mathrm{id}$

$\Rightarrow I \hookrightarrow \mathbb{Z}/(l-1)\mathbb{Z}$.

$\Rightarrow \mathrm{Gal}(M/\mathbb{Q})/I \hookrightarrow \mathbb{Z}/p\mathbb{Z}$.

Continue this process until the exponent r stabilizes.

i.e, $r = s$.

Claim: If $\mathfrak{q}$ is totally ramified in K_1, then $\mathfrak{q}$ totally ramified in K.

Pf: $r=s \Rightarrow Gal(M/\mathbb{Q}) \cong \mathbb{Z}/p^r\mathbb{Z} \oplus \mathbb{Z}/(p-1)\mathbb{Z}$.

$\mathfrak{q}$ ramifies in K_1, unramified in L, ramified on degree of $\mathfrak{q}$ in M is p^r, since $KL=M$, $\mathfrak{q}$ totally ramied in K.

$p=2$:

Lemma: If $K/\mathbb{Q}$ quadratic and 2 is the only prime ramified in K, then $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2})\}$. In particular, K real $\Rightarrow K = \mathbb{Q}(\sqrt{2})$

Pf: $K = \mathbb{Q}(\sqrt{d})$, d sqrfree, $p \mid d \Rightarrow p$ ramifies

For $m \in \mathbb{N}^+$, $K_m = \mathbb{Q}(\zeta_{2^{m+1}})$

$Gal(K_m/\mathbb{Q}) \cong (\mathbb{Z}/2^{m+1}\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/2^{m-1}\mathbb{Z}$

$(\mathbb{Z}/2^{m+1}\mathbb{Z})^\times = \{\pm 1, \pm 5\} = \langle -1, 5 \rangle \cong (1+4\mathbb{Z}/2^{m+1}\mathbb{Z})$

$\sigma(\zeta_{2^{m+1}}) = \zeta_{2^{m+1}}^{-1} = \overline{\zeta_{2^{m+1}}} \Rightarrow K_m^\sigma \subset \mathbb{R}$

For $m>1$, $K_m^\sigma > \mathbb{Q}(\sqrt{2})$ as its only quadratic subfield.

Let $K/\mathbb{Q}$, $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/2^n\mathbb{Z}$, $n \geq 2$, assume that 2 is the only prime that totally ramified in K.

Assume $K \subset \mathbb{R}$.

Consider $L = K K_{n+1}^\sigma \subset \mathbb{R}$.

Note $Gal(L/\mathbb{Q}) < Gal(K/\mathbb{Q}) \oplus Gal(K_{n+1}^\sigma) \cong \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z}$.

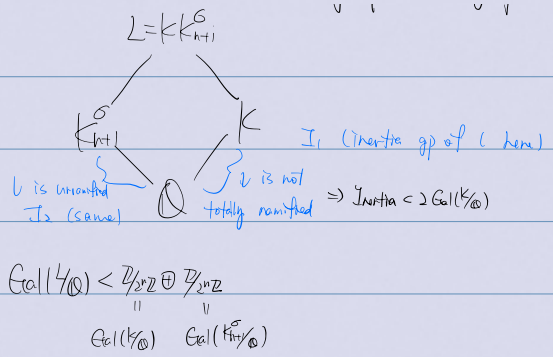
If $K \neq K_{n+1}^\sigma$, then $K \neq L$, $Gal(L/\mathbb{Q})$ is not cyclic.

$Gal(L/\mathbb{Q}) \cong \mathbb{Z}/2^s\mathbb{Z} \oplus \mathbb{Z}/2^s\mathbb{Z}$, $s \leq n$.

Note that L has 3 distinct real quadratic subfields, F_1, F_2, F_3.

Claim: 2 is the only prime that ramified in F_1, F_2, F_3.

Pf: Let $l \neq 2$, take I- inertia group of any prime above l.



$\mathrm{Gal}(L/\mathbb{Q}) < \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$\mathrm{Gal}(k/\mathbb{Q})$ $\quad$ $\mathrm{Gal}(k^{G}_{k+1}/\mathbb{Q})$

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

$P \subset \mathcal{O}_k$, $Q | P_2$, $\quad G > D_Q > I_Q > W_Q$

$Q || \pi$, $\varphi : I_Q/W_Q \hookrightarrow \mathbb{F}_Q^{\times}$ $\quad [\sigma] \to \frac{\sigma\pi}{\pi} \mod Q$.

Thm: Assume G abelian, then $\mathrm{im}\,\varphi \in \mathbb{F}_p^{\times}$

Pf: $\varphi(\sigma) = \varphi(\tau^{-1}\sigma\tau) = \frac{\tau^{-1}\sigma\tau(\pi)}{\pi} \mod Q$.

$= \bar{\tau}\left(\frac{(\sigma(\tau(\pi)))}{\tau(\pi)}\right) \mod Q$.

If $\tau \in D_Q$ $\quad = \bar{\tau}\left(\varphi(\sigma)\right)$ ($\frac{\sigma(\pi)}{\pi}$?)

Since $D_Q \longrightarrow \mathrm{Gal}(\mathbb{F}_Q/\mathbb{F}_p)$

$\therefore \varphi(\sigma) = \varphi(\sigma)^{\mathrm{Norm}(P)}$

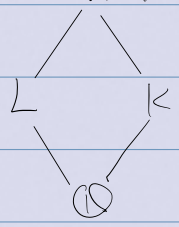
$\therefore \varphi(\sigma) \in \mathbb{F}_p$.

Reduction 2: contd: $K/\mathbb{Q}$ is abelian of order p^n, p is the only prime which ramifies in K.

Pf: Assume l ramifies in K, let I = inertia group of prime above l. $W \subset I$ is trivial.

$I \hookrightarrow \mathbb{F}_l^{\times}$ $\quad \therefore |I| \cong \mathbb{Z}/e\mathbb{Z}$, $e | l-1$

Let $L \subset \mathbb{Q}(\mu_l)$ be s.t. $[L:\mathbb{Q}]^{I} = e$.



I_M - inertia group of a prime above L.

$I_M \hookrightarrow \mathbb{Z}/e\mathbb{Z} \oplus \mathbb{Z}/e\mathbb{Z}$.

$\Rightarrow I_M \cong \mathbb{Z}/e\mathbb{Z}$.

$K' = M^{I_M}$, $K' \cap L = \mathbb{Q}$

$K'L/K'$ has degree $\geq e$, because l has to ramify

$\Rightarrow K'L = M = KL$. 我们在这里找到了 K', 满足 l 是个在 K 中 ramify 的 element.

Pf: Assume $K/\mathbb{Q}$ abelian, $[K:\mathbb{Q}] = 2^n$

2 is the only prime that ramifies.

Claim: K cyclotomic. WLOG, $K \supset \mathbb{Q}(i)$

Pf: Let $K_0 = K \cap \mathbb{R}$, $[K:K_0] = 2$, $K = K_0(i)$

Let $K_n/\mathbb{Q}$ be the cyclotomic field, which is real and

$Gal(K_n/\mathbb{Q}) \cong \mathbb{Z}/2^n\mathbb{Z}$.

Consider $M := KK_n$, $Gal(M/\mathbb{Q}) < \mathbb{Z}/2^n\mathbb{Z} \oplus \mathbb{Z}/2^n\mathbb{Z}$.

If $K_n \neq K$, then $Gal(M/\mathbb{Q})$ not cyclic.

$\Rightarrow M$ has at least 3 real quadratic subfield

$\Rightarrow \Leftarrow$

Key proposition:

Let $p > 2$ be prime, $\exists!\, K/\mathbb{Q}$, with galois group $\mathbb{Z}/p\mathbb{Z}$.

in which p is the only ramified prime

How does $\Rightarrow$ K-W thm?

By reduction #2, $K/\mathbb{Q}$ abelian of prime power p^n.

Wlog, $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$. Let $K_n \subset \mathbb{Q}(\zeta_{p^{n+1}})$ s.t. $[K_n:\mathbb{Q}] = p^n$.

$Gal(K_n/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$.

Let $M = KK_n$, $Gal(M/\mathbb{Q}) \hookrightarrow \mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^n\mathbb{Z}$.

If $K \neq K_n \Rightarrow Gal(M/\mathbb{Q})$ not cyclic

$\Rightarrow M$ contains $\geq p+1$ subfields which have Galois group $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Q}$ in which only p ramifies $\Rightarrow \in$.

Key Lemma: (Lemma 30 in H.P.F)

Let ζ be a primitive pth root of 1,

$L = \mathbb{Q}(\zeta)$, $\pi = 1-\zeta$, $(\pi)^{p-1} = p$

Let $\gamma \in \mathbb{Q}_L$ be a non-pth power, assume $\gamma \equiv 1 \bmod \pi^p$

Then $M = L(\sqrt[p]{\gamma})$ — π is unramified.

Pf: Suppose not, then $\pi \mathcal{O}_M = \mathcal{Q}^p$, $\mathbb{F}_{\mathcal{Q}} \cong \mathbb{F}_{(\pi)} \cong \mathbb{F}_p$

Let $\delta^p = \gamma$. Let $r = \frac{\delta - 1}{\pi}$

Claim: $r \in \mathcal{O}_M$.

conjugates of r over L are $\frac{\zeta^i\delta - 1}{\pi}$, $i \in \mathbb{Z}/p\mathbb{Z}$.

$$\Rightarrow f(x) = \prod_{i=1}^{p-1}\left(x - \frac{\zeta^i\delta - 1}{\pi}\right) = \frac{1}{\pi^p}\prod_{i=1}^{p-1}\left((\pi x - 1) - \zeta^i\delta\right)$$

$$= \frac{(\pi x - 1)^p - \gamma}{\pi^p}$$

$$\in \mathcal{O}_L[x]$$

$\therefore \exists m \in \mathbb{Z}$, $r - m \in \mathcal{O}$

$\therefore \forall \sigma \in Gal(M/L)$, $\sigma r - m \in \mathcal{Q}$

$\therefore \frac{\zeta\delta - 1}{\pi} - m \in \mathcal{Q}$, $\frac{\delta - 1}{\pi} \in \mathcal{Q}$

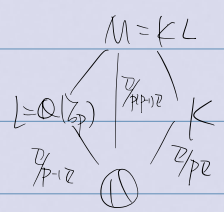
$\therefore \left(\frac{1-\zeta}{\pi}\right)\delta \in \mathcal{Q} \Rightarrow \delta \in \mathcal{Q}$, contradiction

Thm: p odd prime, $K/\mathbb{Q}$ — $\mathbb{Z}/p\mathbb{Z}$ extension

p — only prime ramifies in K.

$\Rightarrow K \subset \mathbb{Q}(\zeta_{p^2})$

Pf:



$Gal(M/\mathbb{Q}) = \langle \sigma \mid \sigma^{p(p-1)} = 1 \rangle$

$K = M^{\langle \sigma^p \rangle}$, $L = M^{\langle \sigma^{p-1} \rangle}$

p — only prime ramified in M.

By Kummer theory, $M = L(\alpha)$, where $\alpha^p = \beta \in L^\times$

We know: $\frac{\sigma\alpha}{\alpha}$ non-trivial root of unity

WLOG, $\frac{\sigma^{p-1}\alpha}{\alpha} = \zeta_p$ $\quad \langle \sigma^{p-1} \rangle = Gal(M/L)$

Note: $\sigma\zeta_p = \zeta_p^n$, $\overline{n} \in (\mathbb{Z}/p\mathbb{Z})^\times$, is a primitive root.

Claim: $M = L(\frac{\sigma\alpha}{\alpha})$ $\quad p = [M:L]$

Pf: If not, $\frac{\sigma\alpha}{\alpha} \in L$.

$$\frac{\sigma\alpha}{\alpha} = \sigma^{p-1}\left(\frac{\sigma\alpha}{\alpha}\right) = \frac{\sigma^p\alpha}{\sigma^{p-1}\alpha} = \frac{\sigma(\zeta_p\alpha)}{\zeta_p\alpha}$$

$$\frac{\sigma\alpha}{\alpha} = \frac{\sigma(\zeta_p\alpha)}{\zeta_p\alpha} \Rightarrow 1 = \frac{\sigma(\zeta_p)}{\zeta_p} \Rightarrow \Leftarrow$$

Rewrite $\alpha \to \frac{\sigma(\alpha)}{\alpha'}$, $\beta \to \frac{\sigma(\beta)}{\beta'}$

P_K, P_L, P_M are prime ideals above $p\mathbb{Z}$.

$$\beta O_L = \prod_{\text{prime} \in L} Q^{n_Q} \qquad n_Q \in \mathbb{Z}.$$

$$= P_L^r \cdot \prod_{Q \neq P} Q^{n_Q}$$

$$\sigma(\beta)O_L = P_L^r \cdot \prod_{Q \neq P} \sigma(Q)^{n_Q}$$

$$\frac{\sigma\beta\, O_L}{\beta} = \prod_{Q \neq P_L} Q^{m_Q} \qquad m_Q \in \mathbb{Z}.$$ 可除 β

So P_L does not occur in βO_L.

$\beta'' = \beta' N^p$ $\quad \alpha'' = \alpha' N$ $\quad N \in \mathbb{Z}$, s.t. $\beta'' \in O_L$.

$M = L(\alpha'')$, $\quad (\alpha'')^p = \beta''$

$\pi = 1 - \zeta_p \in O_L$. $\quad P_L = (\pi)$

- $\mathbb{F}_{\mathfrak{P}_2} \cong \mathbb{F}_p \Rightarrow \beta'' \bmod \mathfrak{P}_2 \equiv m \bmod \mathfrak{P}_2 \quad m \in \mathbb{N}$

Let $m_0 \equiv m^{-1} \bmod p$, $\beta'' \to m_0^p \beta''$, $\alpha'' \to m_0 \alpha''$

WLOG, $\beta'' \equiv 1 \bmod \mathfrak{P}_2$.

$\beta'' = 1 + c\pi \bmod \mathfrak{P}_2^2$, $c \in \mathbb{Z}/p\mathbb{Z}$.

$\zeta_p \equiv 1 - \pi \bmod \mathfrak{P}_2^2$

$\zeta_p^r \equiv 1 - r\pi \bmod \mathfrak{P}_2^2$.

$\beta'' = \zeta_p^{-c} \cdot \gamma$, where $\gamma \equiv 1 \bmod \mathfrak{P}_2^2$

Claim: $\gamma \in (L^\times)^p$

Pf: $(\alpha'')^p = \beta'' = \zeta_p^{-c} \cdot \gamma$

$\sigma^{p-1}\alpha'' = \alpha'' \cdot \zeta_p$

$\sigma\zeta_p = \zeta_p^n$, $n \in (\mathbb{Z}_p)^\times$

$\sigma^p(\alpha'') = \sigma(\sigma^{p-1}\alpha'') = \sigma(\alpha''\zeta_p) = \sigma(\alpha'') \cdot \zeta_p^n$

$\sigma^{p-1}(\sigma\alpha'') = \sigma(\alpha'') \cdot \zeta_p^n$

$\sigma^{p-1}(\alpha''^n) = (\alpha'')^n \cdot \zeta_p^n$

$\sigma^{p-1}\left(\frac{\sigma\alpha''}{\alpha''^n}\right) = \frac{\sigma(\alpha'')}{(\alpha'')^n}$

$\Rightarrow \frac{\sigma\alpha''}{(\alpha'')^n} \in M^{\langle\sigma^{p-1}\rangle} = L$.

$\Rightarrow \frac{\sigma\beta''}{(\beta'')^n} \in (L^\times)^p$ (non-zero)

$\frac{\sigma(\gamma\zeta_p^{-c})}{\gamma^n \zeta_p^{-nc}} \in (L^\times)^p$

$\therefore \frac{\sigma\gamma}{\gamma^n} \in (L^\times)^p$.

Claim: $\gamma \equiv 1 \bmod \mathfrak{P}_2^p$

Pf: Assume not, let $\mathfrak{P}^m \| \gamma - 1$

$\therefore 2 \le m \le p-1$, $\gamma = 1 + c\pi^m \bmod \mathfrak{P}_2^{m+1}$, $c \in (\mathbb{Z}/p\mathbb{Z})^\times$

$\gamma^n \equiv 1 + nc\pi^m \bmod \mathfrak{P}_2^{m+1}$ ($(\cdot)^n$)

$\Rightarrow$ note, $\sigma(\pi) = \sigma(1-\zeta_p) = 1 - \zeta_p^n = (1-\zeta_p)(1+\zeta_p+\zeta_p^2+\cdots+\zeta_p^{n-1})$

$\equiv \pi n \bmod \mathfrak{P}_2^2$

$\Rightarrow \sigma(\pi^m) = \pi^m u^m \mod \mathfrak{P}_L^{m+1}$

$\sigma(v) = 1 + c u^m \pi^m \mod \mathfrak{P}_L^{m+1}$

Note: $u^m \not\equiv u \mod p \quad (u \in \mathbb{Z}_p^\times)$

Cor: $\frac{\sigma(v)}{v^m} \equiv 1 + d\pi^m \mod \mathfrak{P}_L^{m+1}$, $d \in \mathbb{Z}_p^\times$

However, $\frac{\sigma(v)}{v^n} = \zeta^p$, $\zeta \in L$, $\mathfrak{P}_L$ not occur in (ζ)

$\zeta^p \equiv 1 \mod \mathfrak{P}_L \Rightarrow \zeta \equiv 1 \mod \mathfrak{P}_L$.

$\zeta = 1+t$, $\mathfrak{P}_L \nmid t$, $\zeta^p = 1 + pt + \cdots + t^p \equiv 1 \mod \mathfrak{P}_L^p$ ⇒⇐

$L(\sqrt[p]{v})/L$ is unramified above $\mathfrak{P}_L$.

$F := L(\sqrt[p]{v})$ $F < M(\zeta_{p^2})$, $F/\mathbb{Q}$ is abelian

$Gal(F/\mathbb{Q}) \supset I$: inertia above p

$|I| = p-1 \Rightarrow F^I/\mathbb{Q}$ is unramified everywhere $\Rightarrow F^I = \mathbb{Q}$, $F = L$.

$\Rightarrow \sqrt[p]{v} \in (L^\times)^p$

i.e. $M = \mathbb{Q}(\zeta_{p^2})$

■

Local Fields: p-adic

p prime,

$\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \cdots$

$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \{(a_1, a_2, a_3, \cdots, a_i, a_{i+1}), \ a_i \in \mathbb{Z}/p^i\mathbb{Z}, \ a_{i+1} \bmod p^i \equiv a_i\}$

Idea: p-adic integers $\mathbb{Z}_p$ – let you work mod all primes of a prime simultaneously.

$(a_i)_i + (b_i)_i = (a_i + b_i)_i$

$(a_i)_i \cdot (b_i)_i = (a_i b_i)_i$. → ring with exactly 1 maximal ideal

Properties: $\mathbb{Z}_p$ is a local ring with maximal ideal $p\mathbb{Z}_p$.

pf: $\forall n$, $a \in \mathbb{Z}/p^n\mathbb{Z} - p\mathbb{Z}/p^n\mathbb{Z} \Rightarrow a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$

If $p\mathbb{Z}_p = \mathbb{Z}_p$, then $p \in \mathbb{Z}_p^\times \Rightarrow p \in (\mathbb{Z}/p\mathbb{Z})^\times \Rightarrow \Leftarrow$

Cor: $\mathbb{Z}_p$ has characteristic 0.

If $n = 0$, then $n = a \cdot p^b$ (a: unit), $(a,p)=1$, $b \geq 1$, $p^b \neq 0$.

- $\mathbb{Z}_p$ an integral domain

Suppose $xy \neq 0$, $x = p^r v$, $y = p^s w$, $v, w \in \mathbb{Z}_p^\times$

$xy = p^{r+s} vw \neq 0$

- $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$, $\varphi^{-1}(p\mathbb{Z}_p) = p\mathbb{Z}$

$\Rightarrow \mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$

$\{\frac{a}{b} \mid p \nmid b\} \xrightarrow{\frac{a}{b} \to \frac{a}{b}}$

"Power series representation"

In $\mathbb{Z}/p^n\mathbb{Z}$, each x can be written (uniquely) as $x = x_0 + px_1 + \cdots + p^{n-1}x_{n-1}$

$x_i \in \{0, 1, \cdots, p-1\}$.

Define a metric $\| \ \|$ on $\mathbb{Z}_p$.

$\|0\| := 0$

$\|p^n v\| := \frac{1}{p^n}$, if v unit.

Properties: $\cdot \ \|\alpha\beta\| = \|\alpha\| \cdot \|\beta\|$

- Ultrametric triangul inequility.

$\|\alpha + \beta\| \leq \max(\|\alpha\|, \|\beta\|)$

Prop: $(\mathbb{Z}_p, \|\cdot\|)$ is a topological ring, $\mathbb{Z}_p \times \mathbb{Z}_p \xrightarrow{+, \cdot} \mathbb{Z}_p$ is cont,

$\mathbb{Z}_p$ is complete under $\|\cdot\|$

Pf: Let $r_1, r_2, \cdots \quad \|r_i - r_j\| \to \infty$

Then $\forall n \in \mathbb{N}$, $r_i \bmod p^n$ eventually becomes fixed to $s_n \in \mathbb{Z}/p^n\mathbb{Z}$

$S := (s_1, s_2, \cdots, s_n, \cdots)$

then $r_i \to s_i$

Cor: Every $x \in \mathbb{Z}_p$ has a unique rep as

$\sum_{i=1}^{\infty} x_i p^i$, $x_i \in \{0, 1, \cdots, p-1\}$

Cor: topologically, $\mathbb{Z}_p \cong (\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}}$

$\Rightarrow \mathbb{Z}_p$ is a compact topological group.

$\mathbb{Z}_p^\times = \mathbb{Z}_p - p\mathbb{Z}_p = \bigcup_{i=1}^{p-1} i + p\mathbb{Z}_p$. compact

Def: $\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p) = \mathbb{Z}_p[\frac{1}{p}]$

$\mathbb{Q}_p$ - field of p-adic numbers.

Each $x \in \mathbb{Q}_p \setminus \{0\}$, $x = p^n \cdot u$, $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$

$\|x\| = p^{-n}$.

Each $x \in \mathbb{Q}_p$ has a "Laurent series expansion"

$x = \sum_{i=n}^{\infty} x_i p^i$ $x \in \{0, 1, \cdots p-1\}$.

$\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ as a dense subfield.

Thm: $\mathbb{Q}_p$, p prime and $\mathbb{R}$, are all of the (up to isomorphism)

complete normed field containing $\mathbb{Q}$ as a dense subfield.

Define $|\cdot|_p$ on $\mathbb{Q}$ to be the restriction of $\|\cdot\|$ on $\mathbb{Q}_p$.

Define $|n|_\infty = n$

$\Rightarrow \forall \alpha \in \mathbb{Q}^\times$, $\prod_{v \in \{p, \infty\}} |\alpha|_v = 1$.

Let $\alpha = \frac{a}{b}$, $(a,b)=1$, then $\prod_{v \in \{p,\infty\}} |\alpha|_v$

$$= \prod_{p \nmid ab} \left|\frac{a}{b}\right|_p \cdot \prod_{p \mid a} \left|\frac{a}{b}\right|_p \cdot \prod_{p \mid b} \left|\frac{a}{b}\right|_p \cdot \left|\frac{a}{b}\right|$$

$\prod p^{-v_p(a)} = \frac{1}{|a|}$; $|b|$

$$= 1$$