

Algebraic Number Theory

Ref. <<代数数论>> - 马克勤

Chap 1 代数数域. 代数整数环

1.1 代数数域

①、有限扩张称为代数数域. 简记**数域**

Thm (单扩张) 数域扩张 L/K (即 K, L 为数域) 为单扩张

Pf $\forall \alpha \in L \setminus K$ 有限 $\Rightarrow L/K$ 有限 只需对 $L = K(\alpha, \beta)$ 证明

α, β 在 K 上极小多项式 f, g . 在 $\mathbb{C}$ 中有分解 $f(x) = \prod_{i=1}^r (x - \alpha_i)$ $g(x) = \prod_{i=1}^m (x - \beta_i)$ $\alpha = \alpha_1, \beta = \beta_1$
 $\overline{f(x)} \Rightarrow$ 无重根

$A = \left\{ \frac{\alpha_i - \alpha_j}{\beta_k - \beta_l} \mid \begin{matrix} k \neq l \\ i \neq j \end{matrix} \right\}$ 有限. 取 $c \in \mathbb{Q}^* \setminus A$ $\gamma = \alpha + c\beta$

$h(x) = f(\gamma - cx)$ 以 β_1 为根. $\beta_2 \sim \beta_m$ 不为根

$\Rightarrow (h(x), g(x))_{\mathbb{C}} = x - \beta_1 \Rightarrow (h(x), g(x))_{K(\gamma)} = x - \beta_1$

即 $x - \beta_1 \in K(\gamma)[x] \Rightarrow \beta_1 \in K(\gamma)$ $\alpha = \gamma - c\beta_1 \in K(\gamma)$

$\Rightarrow K(\alpha, \beta) \subseteq K(\gamma) \subseteq K(\alpha, \beta) \quad \checkmark$

Thm: L/K 数域扩张. $[L:K] = n$ 则每个嵌入 $\sigma: K \rightarrow \mathbb{C}$

有 n 个延拓嵌入 $\tau_i: L \rightarrow \mathbb{C} \quad (1 \leq i \leq n)$

Pf. 近世代数已证.

对 $K=\mathbb{Q}$ $L=\mathbb{Q}(\gamma)$ f 为 γ 的极小多项式 $\rightarrow r_1$ 实根
 $\rightarrow r_2$ 虚根
 r_1, r_2 为 L 的共轭量 (与 γ 选取无关)

Def. L/K n -次数域扩张 $(1 \leq i \leq n)$ 则 $\sigma_i: L \rightarrow \mathbb{C}$ 为 n 个 K -嵌入
 对 $\alpha \in L$ 定义范 $N_{L/K}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$
 迹 $T_{L/K}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha)$

Prop (1) $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) N_{L/K}(\beta)$ $T_{L/K}(\alpha+\beta) = T_{L/K}(\alpha) + T_{L/K}(\beta)$
 (2) 对 $\alpha \in K$ 有 $N_{L/K}(\alpha) = \alpha^n$ $T_{L/K}(\alpha) = n\alpha$
 (3) 对 $\alpha \in L$ $f(x) = x^n - C_1 x^{n-1} + \dots + (-1)^n C_n$ 为 α 在 K 上极小多项式
 则 $N_{L/K}(\alpha) = C_n$ $T_{L/K}(\alpha) = \frac{n}{1} C_1$ 均为 K 的元素

Pf. (1)(2) 平凡. 对 (3), 设 $f(x)$ 的根为 $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$

每个 K -嵌入 $\tau_i: K(\alpha) \rightarrow \mathbb{C}$ 可延拓为 n 个嵌入 $\sigma_{ij}: L \rightarrow \mathbb{C}$

$$\text{故 } N_{L/K}(\alpha) = \prod_{i=1}^n \prod_{j=1}^n \sigma_{ij}(\alpha) = \prod_{i=1}^n \prod_{j=1}^n \alpha_i = C_n$$

$$T_{L/K}(\alpha) = \sum_{i=1}^n \sum_{j=1}^n \alpha_i = \frac{n}{1} C_1 \quad \checkmark$$

Thm (传递公式) $\alpha \in L$ L/M M/K 数域扩张. 则

$$N_{L/K}(\alpha) = N_{M/K}(N_{L/M}(\alpha)) \quad T_{L/K}(\alpha) = T_{M/K}(T_{L/M}(\alpha))$$

对数域的 n 次扩张 L/K $G \sim G_n: L \rightarrow \mathbb{C}$ 为 K -嵌入

对任意 $\alpha_1, \dots, \alpha_n \in L$ 定义 $d_{L/K}(\alpha_1, \dots, \alpha_n) = |(\sigma_i(\alpha_j))|^2$ 判别式

Lemma (1) $d_{L/K}(\alpha_1, \dots, \alpha_n) = |(\tau_{L/K}(\alpha_i, \alpha_j))|^2 \in K$

(2) $d_{L/K}(\alpha_1, \dots, \alpha_n) \neq 0 \Leftrightarrow \alpha_1, \dots, \alpha_n$ K -线性无关

(3) $L = K(\alpha)$ $f(x)$ 为 α 在 K 上最.小.多项式. 根为 $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$

R) $d_{L/K}(\alpha) \triangleq d_{L/K}(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(f'(\alpha))$

Pf (2) $\Rightarrow$ 若 $k_1, \dots, k_n \in K$ $k_1 \alpha_1 + \dots + k_n \alpha_n = 0 \Rightarrow k_1 \sigma_1(\alpha_1) + \dots + k_n \sigma_1(\alpha_n) = 0$

则 $\{\sigma_i(\alpha_j)\}$ 相关. 矛盾

$\Leftarrow$ 若 $d_{L/K} = 0$ 由 (1) $(\tau_{L/K}(\alpha_i, \alpha_j))$ 的行 $R_1 \sim R_n$ 相关

设 $k_1 R_1 + \dots + k_n R_n = 0$ 且 $k_1 \alpha_1 + \dots + k_n \alpha_n \neq 0$

而 $\tau_{L/K}(\alpha_i, \alpha_j)$ 为 $k_1 R_1 + \dots + k_n R_n = 0$ 中的第 j 个元素. 故为 0

又 $\alpha_1, \dots, \alpha_n$ 构成 L 的 K -基. 则 $\alpha^{-1} \in L$ 可被 α 生成 $\Rightarrow \tau_{L/K}(1) = 0$. 矛盾!

(3) LHS = $|(\alpha_i^j)|^2 \stackrel{\text{Vandermonde}}{=} \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2$
 $= (-1)^{\frac{n(n-1)}{2}} \prod_{r=1}^n \prod_{s \neq r} (\alpha_r - \alpha_s) \stackrel{f'(\alpha_r)}{=} \text{RHS}$

例. 分圆域 $L = \mathbb{Q}(\omega)$ $\omega = e^{\frac{2\pi i}{p^n}}$ p 奇素数

$S = p^n - p^{n-1}$ ω 的最.小.多项式为 $f(x) = \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1}$

可证 $f'(\omega) = \frac{p^n}{\omega(\omega^{p^{n-1}} - 1)}$
 有 $d_L(\omega) = (-1)^{\frac{S(S-1)}{2}} \frac{N(p^n)}{N(\omega) N(\omega^{p^{n-1}} - 1)}$

$N(p^n) = p^{nS}$
 $N(\omega) = 1$

令 $\zeta = \omega^{p^{n-1}}$ 在 $\mathbb{Q}$ 上最.小.多项式为 $g(x) = x^{p-1} + \dots + x + 1$
 $\Rightarrow \zeta - 1, \dots$ 为 $g(x+1) = x^{p-1} + \dots + x + p$

$M = \mathbb{Q}(\zeta) \Rightarrow N_{L/\mathbb{Q}}(\zeta - 1) = N_{M/\mathbb{Q}}(N_{L/M}(\zeta - 1)) = N_{M/\mathbb{Q}}((\zeta - 1)^{p^{n-1}})$
 $\Rightarrow d_L(\omega) = (-1)^{\frac{S(S-1)}{2}} p^{p^{n-1}(p-1)} = p^{p^{n-1}} (-1)^{p-1} = p^{p^{n-1}}$

数域 K 中的单位根全体 W_K (单位根群)

Lem. W_K 有限

$\in \mathbb{Z}[x]$

Pf. ω 为 n 次单位根 极小多项式 $f(x) = x^n + c_1 x^{n-1} + \dots + c_m \mid x^n - 1$

则 f 的根 $\omega = \omega_1, \omega_2, \dots, \omega_m$ 均有 $\omega_i^n = 1 \Rightarrow |\omega_i| = 1 \xrightarrow{\text{Vieta}} |c_i| \leq C_m$

又 $m = [O(\omega) : \mathbb{Q}] \leq [K : \mathbb{Q}]$ 故 f 只有有限多个 $\checkmark$

Cor W_K 为有限循环群. 阶记为 w_K

(域中有有限乘法群均循环)

例: (1) K 为实数域. 则 $W_K = \{\pm 1\}$, $w_K = 2$

(2) $K = \mathbb{Q}(\sqrt{d})$ $d=1$ $W_K = \{\pm 1, \pm i\}$ $w_K = 4$

$d=3$ $W_K = \{\pm 1, \pm \omega, \pm \omega^2\}$ $w_K = 6$

$d>3$ $W_K = \{\pm 1\}$ $w_K = 2$

1.2 代数整数环

Def. α 称为代数整数 (简称整数). 若存在整系数首一多项式将 α 化零
为 α 在 $\mathbb{Z}$ 中元素为有理整数 记 K 中的整数集合为 O_K

Lem α 为代数数. $f(x)$ 为 α 在 $\mathbb{Q}$ 上极小多项式. 则 α 为整数 $(\Rightarrow f(x) \in \mathbb{Z}[x])$

Cor. O_K 中整数为有理整数.

Thm. $K = \mathbb{Q}(\sqrt{d})$ d 无平方因子整数 则 $O_K = \begin{pmatrix} \mathbb{Z} & \mathbb{Z}\omega \\ \mathbb{Z}\omega & \mathbb{Z} \end{pmatrix}$ 其中 $\omega = \begin{cases} \frac{\sqrt{d}}{2} & d \equiv 1 \pmod{4} \\ \sqrt{d} & d \equiv 2,3 \pmod{4} \end{cases}$

pf. 由 Lem. $\alpha + \beta\sqrt{d} \in O_K \Leftrightarrow \exists \alpha, \beta \in \mathbb{Z} \text{ s.t. } d\alpha^2 - \beta^2 \in \mathbb{Z}$

则若 $\alpha + \beta\sqrt{d} \in O_K$ 有 $(2\alpha)^2 - (2\beta)^2 d \in 4\mathbb{Z} \Rightarrow (2\beta)^2 d \in \mathbb{Z} \Rightarrow 2\beta \in \mathbb{Z}$

(i) $d \equiv 2,3 \pmod{4}$ 若 $2\alpha, 2\beta$ 均奇 则 $(2\alpha)^2 \equiv 1 \not\equiv d \equiv (2\beta)^2 d \pmod{4}$ 矛盾

又 $(2\alpha)^2 \equiv (2\beta)^2 d \pmod{4} \Rightarrow 2\alpha, 2\beta$ 均偶 $\alpha, \beta \in \mathbb{Z} \checkmark$

(ii) $d \equiv 1 \pmod{4}$ 同上 $2\alpha, 2\beta$ 同奇偶 $\alpha, \beta \in \mathbb{Z}$

$$\alpha + \beta\sqrt{d} = (\alpha - \beta) + 2\beta\omega \in \mathbb{Z}\omega$$

反之对 $a, b \in \mathbb{Z}$ $a + b\omega = a + \frac{b}{2} + \frac{b}{2}\sqrt{d}$ 代入二次式 $x^2 - (2a+b)x + (a+\frac{b}{2})^2 - \frac{b^2 d}{4}$

$$\underbrace{\quad}_{\in \mathbb{Z}} \quad \underbrace{\quad}_{a^2 + ab + b^2 \frac{1-d}{4} \in \mathbb{Z}} \in \mathbb{Z} \checkmark$$

上列中 O_K 为 K 的子环. 事实上这是一般的

Thm. $\alpha \in \mathbb{C}$ TFAE:

(1) α 为整数 (2) $\mathbb{Z}[\alpha]$ 的加法群有限生成

(3) α 为 $\mathbb{C}$ 的子环 R 中的元素 且 R 的加法...

(4) $\exists$ 有限生成非零加法子群 $A \subset \mathbb{C}$ s.t. $\alpha A \subseteq A$

pf. 仅 (4) $\Rightarrow$ (1) 证明. 设 $\alpha_1, \dots, \alpha_n$ 生成 A

$$\alpha A \subseteq A \Rightarrow \begin{pmatrix} \alpha \alpha_1 \\ \vdots \\ \alpha \alpha_n \end{pmatrix} = \underbrace{M}_{\in \mathbb{Z}^{n \times n}} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \Rightarrow (\alpha I_n - M) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$$

$$\Rightarrow |\alpha I_n - M| = 0 \Rightarrow \alpha \text{ 为整数}$$

Cor. $\forall$ 数域 K , O_K 为 K 的子环. 称为 K 的 (代数) 整数环

Thm O_K 为秩 $n = [K:\mathbb{Q}]$ 的自由 Abelian 群

pf. $\alpha_1, \dots, \alpha_n$ 为 K 的 $\mathbb{Q}$ -基. 则 $\exists 0 \neq M \in \mathbb{Z}$ s.t. $M\alpha_i \in O_K$ (why?)

且 $M\alpha_i$ 仍为 $\mathbb{Q}$ -基 故 $\alpha_i \in O_K$

$\forall \gamma \in O_K$. $\gamma = x_1\alpha_1 + \dots + x_n\alpha_n$ $x_i \in \mathbb{Q}$ 设 $\sigma_1, \dots, \sigma_n: K \hookrightarrow \mathbb{C}$

$$\sigma_i(\gamma) = x_1\sigma_i(\alpha_1) + \dots + x_n\sigma_i(\alpha_n) \in O_K$$

由 Cramer 法则 $x_j = \frac{\gamma_j}{\delta}$ $\delta = (\sigma_i(\alpha_j))$ $\delta^2 = d = d_K(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$

故 $\gamma_j \delta = x_j d \in \mathbb{Q} \cap O_K = \mathbb{Z} \stackrel{\neq 0}{\Rightarrow} \gamma \in \mathbb{Z} \frac{\alpha_1}{d} \oplus \dots \oplus \mathbb{Z} \frac{\alpha_n}{d} \quad \checkmark$

则设 $O_K = \mathbb{Z}w_1 \oplus \dots \oplus \mathbb{Z}w_n$ $w_1, \dots, w_n$ 为 K 的一组 **整基**

整基不唯一. 设 $\beta_1, \dots, \beta_n, \gamma_1, \dots, \gamma_n$ 为两组整基 则 $\exists M, N \in \mathbb{Z}^{n \times n}$

$$M \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \quad \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = N \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \Rightarrow M = N^{-1} \quad |M| = |N| = \pm 1$$

$\Rightarrow d_K(\beta_1, \dots, \beta_n) = d_K(\gamma_1, \dots, \gamma_n)$ 不变量! **域 K 的判别式 $d(K) \in \mathbb{Z}^*$**

Lemma (1) $\alpha_1, \dots, \alpha_n \in O_K$. 若 $d_K(\alpha_1, \dots, \alpha_n) = d(K)$ 或 $d_K(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^*$ 无平方因子
则 $\alpha_1, \dots, \alpha_n$ 为整基

(2) K, L 为数域 $[K:\mathbb{Q}] = m$ $[L:\mathbb{Q}] = n$ $[KL:\mathbb{Q}] = mn$

且 $(d(K), d(L)) = 1$ 则 (a) $O_{KL} = O_K O_L$

(b) $\{\alpha_1, \dots, \alpha_m\} \cup \{\beta_1, \dots, \beta_n\}$ 为 K, L 的整基.

则 $\{\alpha_i, \beta_j\}$ 为 KL 的整基

(c) $d(KL) = d(K)^n d(L)^m$

(i.e. 若)

例). (1) $K = \mathbb{Q}(\zeta_{p^n})$ $i\zeta_{p^n} = \zeta_{p^n}$ $S = \varphi(p^n) = (K:\mathbb{Q})$

ω 为整数 $\Rightarrow \mathbb{Z}[\omega] \subseteq \mathcal{O}_K$ 希望 $\mathcal{O}_K \subseteq \mathbb{Z}[\omega]$

$\forall \alpha \in \mathcal{O}_K \quad \alpha = t_0 + t_1\omega + \dots + t_{s-1}\omega^{s-1}$

设 $\text{Gal}(K/\mathbb{Q}) = \{\tau_1 \dots \tau_s\}$ 同前 $t_j = \frac{\gamma_j}{s}$

$s = |(\mathbb{Z}[\omega^k])|$
 γ_j : 将第 j 列替换

又 $\tau_i(\omega^k)$ $\tau_i(\alpha)$ 为整数 故 γ_i s 为整数

$s^2 = d = (-1)^{\frac{s(s-1)}{2}} p^{p^{n-1}(np-n-1)}$

同前 $s\gamma_j = d \underset{m_j}{t_j} \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$

$\alpha = \frac{m_0}{d} + \frac{m_1}{d}\omega + \dots + \frac{m_{s-1}}{d}\omega^{s-1}$

替换 $\frac{m_0}{d} + \frac{m_1}{d}(1-\omega) + \dots + \frac{m_{s-1}}{d}(1-\omega)^{s-1}$ $m_j \in \mathbb{Z}$

$\exists i \in d/m_j \Rightarrow \alpha \in \mathbb{Z}[\omega]$
 (反之)

则 $1, \omega, \omega^2, \dots, \omega^{s-1}$ 为整基 $d(K) = (-1)^{\frac{s(s-1)}{2}} p^{p^{n-1}(np-n-1)}$

对一般 $m = p_1^{d_1} \dots p_r^{d_r} \not\equiv 2 \pmod{4}$

$r=2$ 时 $K_1 = \mathbb{Q}(\zeta_{p_1^{d_1}})$ $K_2 = \mathbb{Q}(\zeta_{p_2^{d_2}})$ 有 $(d(K_1), d(K_2)) = 1$

由引理(2)有 $\mathcal{O}_K = \mathcal{O}_{K_1} \mathcal{O}_{K_2} = \mathbb{Z}[\zeta_m]$

$d(K) = d(K_1)^{\varphi(p_2^{d_2})} d(K_2)^{\varphi(p_1^{d_1})} = (-1)^{\frac{\varphi(m)}{2}} \frac{m^{\varphi(m)}}{\prod_{p|m} p^{\frac{\varphi(m)}{p-1}}}$

1/3 为奇数对 $r \geq 2$ 也成立

(2) $K = \mathbb{Q}(\sqrt{D})$ 整基 $(1, \frac{D+\sqrt{D}}{2})$

$D = \begin{cases} d, & d \equiv 1 \pmod{4} \\ 4d, & d \equiv 2, 3 \pmod{4} \end{cases}$

$d(K) = \left| \begin{vmatrix} \frac{D+\sqrt{D}}{2} \\ \frac{D-\sqrt{D}}{2} \end{vmatrix} \right|^2 = D$

(3) $x^5 - x + 1 \in \mathbb{Q}[x]$ $K = \mathbb{Q}(\theta)$

$d_K(\theta) = N_{K/\mathbb{Q}}(f'(\theta)) \stackrel{\text{例}}{=} 19 \cdot 151$

$\Rightarrow 1, \theta, \dots, \theta^4$ 为整基

$\mathcal{O}_K = \mathbb{Z}[\theta]$ $d(K) = 19 \cdot 151$

Chap 2 O_K 的素分解

2.1 分解的存在唯一性

Def 整环 R 称为 **Dedekind 整环**. 若

- (1) R 为 Noether 整环
- (2) R 的非零素理想均极大
- (3) R 整闭

Lemma (1) PID $\rightarrow$ Dedekind

(2) Noether 整环 R 中 每个理想 I . $\exists$ 素理想 $P_1 \sim P_n$ s.t. $I \supseteq R \cdots P_n$

(3) A 为 Dedekind 整环 R 的理想 $A \neq R$. K 为 R 的商域

(R) $\exists \gamma \in K - R$ s.t. $\gamma A \subseteq R$

Prop (1) I 为 Dedekind 整环 R 的理想 $\exists R$ 中另一个理想 J s.t. IJ 为主理想

(2) A, B, C 为 Dedekind 整环 R 的理想 则 $AB = AC \Rightarrow B = C$

(3) A, B 则 $A \supseteq B \Leftrightarrow \exists$ 理想 C . $B = AC$

pf. (1) 取 $0 \neq \alpha \in I$. $J \triangleq \{\beta \in R \mid \beta I \subseteq (\alpha)\}$ 易见 $J \cap R$ $IJ \subseteq (\alpha)$

$A = \frac{1}{\alpha} IJ \cap R$ 若 $A \neq R$ 则由 Lemma (3) $\exists \gamma \in K - R$ s.t. $\gamma A \subseteq R$

$J \neq \emptyset \Rightarrow \gamma J \subseteq R$. 任取 $\beta \in J$ 有 $\gamma \beta I \subseteq \gamma J I \subseteq \alpha R = (\alpha) \Rightarrow \gamma \beta \in J$

设 $J = (\alpha_1 \cdots \alpha_n)$. (R) $\gamma \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \Rightarrow \gamma J \subseteq J$

$|\gamma I - M| = 0 \xrightarrow{R \text{ 整闭}} \gamma \in R$ 矛盾 $\Rightarrow A = R$ $IJ = (\alpha)$

(2) 取 $J \cap R$ $AJ = (\alpha) \Rightarrow \alpha B = ABJ = ACJ = \alpha C \xrightarrow{R \text{ 整闭}} B = C$

(3) 显然:

$\Rightarrow$ 取 $J \cap R$ s.t. $AJ = (\alpha)$ $A \supseteq B \Rightarrow C = \frac{1}{\alpha} JB \cap R$

且 $B = AC \checkmark$

Thm. Dedekind 整环 R 的非零理想可不计次序地唯一表示为有限个素理想之积

Pf 存在性: $S = \{R \text{ 中能表为有限个素理想之积的理想}\}$

$R \notin S$ 若 $S \neq \emptyset$ 则有极大元 $M \neq R$. M 包含于某个极大(主)理想 P 中
(0个素理想)
 $\Rightarrow \exists I \subset R, S + M = PI \Rightarrow I \not\subset M$ 则 $I \in S \Rightarrow M = PI \cdot P_1 \cdots P_n$ 矛盾!
唯一性: 改下标, 反复用消去律

Lem. R Dedekind 整环. 则 R PID $\Leftrightarrow$ UFD

Pf. $\Leftarrow$ 若不为 PID, R 中有非主理想. 则 R 中有非主素理想 P

$S = \{I \subset R \mid IP \text{ 为主理想}\} \xrightarrow{\text{Prop. 11}} S \neq \emptyset \Rightarrow$ 极大元 $M, PM = (d)$

若 $\alpha = \beta\gamma \Rightarrow P \mid (\alpha) = (\beta)(\gamma) \Rightarrow P \mid (\beta)$ 或 $P \mid (\gamma)$

假设 $P \nmid (\beta) \Rightarrow J \in S$ 又 $J \mid PM \Rightarrow JM$ 极大矛盾!

又 $P \nmid (\alpha) R \neq P \Rightarrow M \nmid (\alpha)$ 取 $\delta \in P - (\alpha) \quad \epsilon \in M - (\alpha)$

$(\alpha) = MP \supseteq (\delta)(\epsilon) = (\delta\epsilon) \quad \alpha \mid \delta\epsilon$ 但 $\alpha \nmid \delta, \alpha \nmid \epsilon$

与 R 为 UFD 矛盾! 故 R 为 PID

Thm. 数域 K . 则 O_K 为 Dedekind 整环

Pf. (1) Noether: O_K 为有限生成自由 Abelian 群 $\Rightarrow$ 理想 I 的加法群有限生成
 $\Rightarrow I$ 作为理想 f.g.

(2) $P \mid O_K$ 素. $0 \neq \alpha \in P$ 令 $m = N_{K/Q}(\alpha) \in \mathbb{Z} - \{0\}$

$\frac{m}{\alpha} \in O_K \Rightarrow m = \alpha \cdot \frac{m}{\alpha} \in P \Rightarrow (m) \subseteq P$

取整基 $\{w_1, \dots, w_n\} \Rightarrow O_K / mO_K = \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n / \mathbb{Z}mw_1 \oplus \cdots \oplus \mathbb{Z}mw_n \cong (\mathbb{Z}/m\mathbb{Z})^n$

由 $O_K/P \cong O_K/mO_K / P/mO_K$

有 $|O_K/P| \leq m^n \Rightarrow O_K/P$ 有限整环 $\Rightarrow$ 域

(3) 整闭: $\alpha \in K$ $f(\alpha)=0$ $f(x)=x^m+\dots+c_m \in O_K[x]$

则 $R=\mathbb{Z}[c_1, \dots, c_m]$ 的加法群 f.g. $\exists PR=\mathbb{Z}\gamma_1+\dots+\mathbb{Z}\gamma_s$

由 $f(\alpha)=0 \Rightarrow \forall \alpha^r (r \geq 1)$ 可由 $1, \alpha, \dots, \alpha^{m-1}$ R -表示

$$\Rightarrow [c_1, \dots, c_m, \alpha] = R[\alpha] = R + R\alpha + \dots + R\alpha^{m-1}$$

$$= \mathbb{Z}\gamma_1 + \dots + \mathbb{Z}\gamma_s + \mathbb{Z}\alpha\gamma_1 + \dots + \mathbb{Z}\alpha\gamma_s + \dots \quad \text{也 f.g.}$$

则 $\alpha \in O_K$ 故 O_K 整闭 $\checkmark$

则 O_K 的非零理想可分解为素理想之积

Lem. A 为 O_K 的非零理想. 则 A 的加法群为秩为 $n=[K:\mathbb{Q}]$ 的自由 Abelian 群

Pf 只须证 A 的秩为 n . 取整基 $w_1, \dots, w_n$

$$\forall 0 \neq \alpha \in A \quad \exists t = N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z} \Rightarrow \frac{t}{\alpha} \in O_K \Rightarrow t = \alpha \cdot \frac{t}{\alpha} \in A$$

则 $tw_1, \dots, tw_n$ 为 A 中 $\mathbb{Z}$ -线性无关元. $\checkmark$

则对 $A \triangleleft O_K$ 取 $w_1, \dots, w_n$ 为 O_K 的整基 且 A 有 $\mathbb{Z}$ -基 $\alpha_1, \dots, \alpha_n$

$$\text{则 } \exists T \in \mathbb{Z}^{n \times n} \quad \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = T \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

$$\text{对另一组基 } (w'_1, \dots, w'_n), (\alpha'_1, \dots, \alpha'_n) \quad \text{则 } \begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = N \begin{pmatrix} w'_1 \\ \vdots \\ w'_n \end{pmatrix}$$

$$(\det M = \pm 1, \det N = \pm 1)$$

$$\text{则 } \begin{pmatrix} \alpha'_1 \\ \vdots \\ \alpha'_n \end{pmatrix} = M T N \begin{pmatrix} w'_1 \\ \vdots \\ w'_n \end{pmatrix}$$

故 $|\det T|$ 与基无关!

↓
理想 A 的范 $N_K(A) = N_{K/\mathbb{Q}}(A)$

Thm. A 为 O_K 中非零整理想. 则 $N_K(A) = |O_K/A|$

Pf. 取 $\mathbb{Z}$ -基 $w_1 \dots w_n$ s.t. $A = \mathbb{Z}\alpha_1 w_1 \oplus \dots \oplus \mathbb{Z}\alpha_n w_n$ $\alpha_i \in \mathbb{Z}$

$$\text{则 } N_K(A) = |\alpha_1 \dots \alpha_n| = \prod_{i=1}^n |\mathbb{Z}/\alpha_i \mathbb{Z}| = |\mathbb{Z}/\alpha_1 \mathbb{Z} \oplus \dots \oplus \mathbb{Z}/\alpha_n \mathbb{Z}| \\ = |O_K/A| \quad \checkmark$$

Thm. A, B 为 O_K 中的理想. $A = p_1^{e_1} \dots p_r^{e_r}$ (p_i 为素理想, $e_i \geq 1$)

$$\text{则 (1) } N_K(A) = N_K(p_1)^{e_1} \dots N_K(p_r)^{e_r}$$

$$(2) N_K(AB) = N_K(A)N_K(B)$$

$$(3) \{\alpha_1 \dots \alpha_n\} \text{ 为 } A \text{ 的 } \mathbb{Z}\text{-基. 则 } d_K(\alpha_1 \dots \alpha_n) = N_K(A)^2 d(K)$$

$$(4) A = (\alpha) \text{ 则 } N_K(A) = |N_{K/Q}(\alpha)|$$

Pf (1) 由 CRT. 只需证 $N_K(p^r) = N_K(p)^r$ (p 素理想)

$$\text{取 } \alpha \in p^k - p^{k+1} \text{ 定义 } \varphi: O_K \rightarrow (O_K + p^{k+1})/p^{k+1} \\ (\alpha) = p^k A' \quad (A', p) = 1 \quad x \mapsto \alpha x + p^{k+1} \quad \ker \varphi = p$$

$$(O_K + p^{k+1})/p^{k+1} = (p^k A' + p^{k+1})/p^{k+1} = p^k$$

$$\Rightarrow O_K/p \cong p^k/p^{k+1}$$

$$\Rightarrow N_K(p^r) = |O_K/p^r|$$

$$= |O_K/p| |p^2/p| \dots |p^{r-1}/p^r|$$

$$= |N_K(p)|^r$$

$$(3) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} \quad G_i \sim G_n: K \hookrightarrow \mathbb{C} \text{ 为 } \overline{\mathbb{Q}} \text{ 上 } \lambda$$

$$\Rightarrow \begin{pmatrix} G_i(\alpha_1) \\ \vdots \\ G_i(\alpha_n) \end{pmatrix} = M \begin{pmatrix} G_i(w_1) \\ \vdots \\ G_i(w_n) \end{pmatrix}$$

$$d_K(\alpha_1 \dots \alpha_n) = \det(G_i(\alpha_j))^2 = |M|^2 \det(G_i(w_j))^2 = N_K(A)^2 d(K)$$

$$(4) \text{ 由 (3) } d_K(\alpha w_1 \dots \alpha w_n) = N_K(A)^2 d(K)$$

$$\det^{\text{II}}(G_i(\alpha w_j))^2$$

$$\left(\prod_{i=1}^n G_i(\alpha) \right)^2 |G_i(w_j)|^2 = d(K) \cdot N_{K/Q}(\alpha)^2$$

2.2 分歧指数 剩余类域次数 分裂次数

Lem. L/K 数域扩张. $\mathfrak{p} \nmid \mathcal{O}_L$ 素理想. 则

(1) $\mathfrak{p} \cap \mathcal{O}_K$ 为 $\mathcal{O}_K$ 素理想 且 $\mathfrak{p} \cap \mathcal{O}_K = \mathfrak{p} \Leftrightarrow \mathfrak{p} | \mathfrak{p}$

(2) 若 $\mathfrak{p} \cap \mathcal{O}_K = \mathfrak{p}$ 则 $\mathcal{O}_K/\mathfrak{p}$ 和 $\mathcal{O}_L/\mathfrak{p}$ 为有限域. 前者可视为后者子域

则对 $\mathcal{O}_K$ 中素理想 $\mathfrak{p} \mathcal{O}_L \stackrel{\text{分解}}{=} \beta_1^{e_1} \cdots \beta_g^{e_g}$ 其中 $\beta_i \cap \mathcal{O}_K = \mathfrak{p}$

$e(\mathfrak{p}_i/\mathfrak{p}) = e_i$: β_i 的 **分歧指数** g : **分裂次数**

若某个 β_i 分歧. 则称 $\mathfrak{p}$ 分歧

$[\mathcal{O}_L/\beta_i : \mathcal{O}_K/\mathfrak{p}]$: β_i 的 **剩余类域次数**. $\circ f(\beta_i/\mathfrak{p}) = f_i$

Thm. $n = [L:K]$ 则 $\sum_{i=1}^g e_i f_i = n$

若 e_i 不全为 1 则称 $\mathfrak{p}$ **分歧**

$g=n$ 时 e_i, f_i 均为 1. 此时称 $\mathfrak{p}$ 在 L 中 **完全分裂**

$e=n$ 时 $g=1$ $\mathfrak{p} \mathcal{O}_L = \beta^n$ 称 $\mathfrak{p}$ 在 L 中 **完全分歧** ($f=1$)

若 $\mathfrak{p} \mathcal{O}_L = \mathfrak{p}$ ($g=1, f=n$) 称 $\mathfrak{p}$ 在 L 中 **惯性**

Thm. $L/M, M/K$ 为数域扩张. $\mathfrak{p}, \beta, \mathfrak{P}$ 为 $\mathcal{O}_K, \mathcal{O}_M, \mathcal{O}_L$ 素理想

且 $\mathfrak{P} | \beta | \mathfrak{p}$ 则 $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\beta) \cdot e(\beta/\mathfrak{p})$

$f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\beta) f(\beta/\mathfrak{p})$

Thm $L = K(\alpha)$ $\alpha \in O_L$ $n = [L:K]$ $f(x) = x^n + c_1 x^{n-1} + \dots + c_n \in O_K[x]$ 为

α 在 K 上极小多项式. 则

(a) $O_K(\alpha)$ 为 O_K 的子环. 且 $O_K/O_K(\alpha)$ 为有限群

(b) 设 p 为素数. P 为 O_K 的主理想. $P|P$ 则 O_K/P 为特征 p 有限域

(c) 若 $P \nmid P$ $f(x)$ 在 $(O_K/P)[x]$ 中分解为

$$f(x) = p_1(x)^{e_1} \dots p_g(x)^{e_g} \pmod{P}$$

其中 $p_1(x) \dots p_g(x)$ 为 $O_K[x]$ 中两两互素. 且在 $(O_K/P)[x]$ 中两两不互

$$\text{则 } PO_L = \beta_1^{e_1} \dots \beta_g^{e_g} \quad \beta_i = (P, p_i(\alpha)) \quad e_i = e(\beta_i/P)$$

$$f(\beta_i/P) = \deg p_i(x)$$

(3), $f(x) = x^3 + x + 1$ 有一个根 ω $K = \mathbb{Q}(\omega)$ 三次域

$$d_K(1, \omega, \omega^2) = N_{K/\mathbb{Q}}(f'(\omega)) = -31 \text{ 无平方因子} \Rightarrow \{1, \omega, \omega^2\} \text{ 基}$$

$$O_K = \mathbb{Z}[\omega]$$

$$f(x) = x^3 + ax + b$$

$$\Rightarrow d(f) = (-1)^{\frac{n(n-1)}{2}} [(-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}]$$

对 $p=2$ $f(x) = x^3 + x + 1$ 有 $\mathbb{F}_2[x]$ 中不可约 $\Rightarrow$ 惯性

$$N_K(P) = 3 \quad f_1 = 1$$

$p=3$ $f(x) = (x-1)(x^2+x+1)$ 在 $\mathbb{F}_3[x]$ 中 $\Rightarrow 3O_K = P_1 P_2$

$$P_1 = (3, \omega-1)$$

$$P_2 = (3, \omega^2 + \omega + 1)$$

$$N_K(P_1) = 3 \quad f_1 = 1$$

$$P_1 = (3, \omega-1)$$

$$P_2 = (3, \omega-14)$$

$$N_K(P_1) = N_K(P_2) = 31$$

$p=31$ $f(x) = (x-3)(x-14)^2 \pmod{31} \Rightarrow 31O_K = P_1 P_2^2$

$\Rightarrow 31$ 分歧. 3 不分歧

13). 定义 $P \nmid d$ Legendre 符号 $\left(\frac{d}{p}\right) = \begin{cases} 1 & d \text{ 为模 } p = \text{二次剩余} \\ -1 & d \text{ 不为} \dots \end{cases}$

Thm: $K = \mathbb{Q}(\sqrt{d})$ (a) 若 $P \nmid d(K)$ 则 $PO_K = P^2$ $N(P) = P$ $P \nmid d(K)$ 且
 (b) 若 $P \geq 3$, $P \nmid d(K)$ 则 $\left(\frac{d}{P}\right) = 1 \Rightarrow PO_K = P \cdot P_1$, $N_{K/\mathbb{Q}}(P_1) = N_{\mathbb{Q}/\mathbb{Q}}(P_1) \cdot P$ 且 P_1 在 K 中
 $\left(\frac{d}{P}\right) = -1 \Rightarrow PO_K = P$ 惯性
 (c) $P = 2$, $P \nmid d(K)$ 则 $d \equiv 1 \pmod{4}$ $\begin{cases} d \equiv 1 \pmod{8} & 2 \text{ 在 } K \text{ 中完全分裂} \\ d \equiv 5 \pmod{8} & 2 \text{ 在 } K \text{ 中惯性} \end{cases}$

Pf. (i) $d \equiv 2, 3 \pmod{4}$ 则 $O_K = \mathbb{Z}[\omega]$ $\omega = \frac{1+\sqrt{d}}{2}$ 极小多项式 $x^2 - d$ $d(K) = 4d$
 $P \geq 3$, $P \nmid d$, $\left(\frac{d}{P}\right) = 1$ 则 $x^2 - d \equiv (x-a)(x+a) \pmod{P} \xrightarrow{P \nmid d} a \neq -a \pmod{P}$
 此时 $PO_K = P \cdot P_1$ $P_1 = (P, \sqrt{d}-a)$ $P_2 = (P, \sqrt{d}+a)$
 若 $\left(\frac{d}{P}\right) = -1$ 则 $x^2 - d \not\equiv (x-a)(x+a) \pmod{P}$...
 $P \nmid d$ 则 $x^2 - d \equiv x^2 \pmod{P} \Rightarrow PO_K = P^2$ $P = (P, \sqrt{d})$
 $P = 2$ 若 $d \equiv 2 \pmod{4} \Rightarrow x^2 - d \equiv x^2 \pmod{2} \Rightarrow 2O_K = P^2$ $P = (2, \sqrt{d})$
 $d \equiv 3 \pmod{4} \Rightarrow x^2 - d \equiv (x+1)^2 \pmod{2} \Rightarrow 2O_K = P^2$ $P = (2, \sqrt{d}+1)$
 (ii) $d \equiv 1 \pmod{4}$ $\omega = \frac{1+\sqrt{d}}{2}$ 极小多项式 $x^2 - x - \frac{1}{4}(d-1)$ $d(K) = d$
 $P \geq 3$ $|O_K / \mathbb{Z}[\omega]| = |\mathbb{Z}[\omega] / \mathbb{Z}[\bar{\omega}]| = 2 \Rightarrow P \nmid |O_K / \mathbb{Z}[\omega]|$
 用 $\mathbb{Z}[\bar{\omega}]$ 则同 (i) 中讨论
 $P = 2$ $d \equiv 1 \pmod{8}$ 时 $x^2 - x - \frac{1}{4}(d-1) \equiv x(x-1) \pmod{2} \Rightarrow 2O_K = P_1 P_2$
 $P_1 = (2, \omega)$ $P_2 = (2, \omega-1)$
 $d \equiv 5 \pmod{8}$ 时 $x^2 - x - \frac{1}{4}(d-1) \equiv x^2 + x + 1 \pmod{2}$ 不可约 $\checkmark$

在二次域中素数 P 分歧 $\Leftrightarrow P \mid d(K)$ 事实上这对一般数域也都对
 下面用代数的语言讨论该问题

设环 B 为域 F 上的代数 $\{\xi_1, \dots, \xi_n\}$ 为一组 F -基

$$\text{则 } \forall \xi \in B, \quad \xi(\xi_1, \dots, \xi_n) = (\xi_1, \dots, \xi_n) A(\xi)$$

$\text{Tr} A(\xi)$ ξ 关于 B/F 的迹 记为 $T_{B/F}(\xi)$

$$n \text{ 个元素 } \xi_1, \dots, \xi_n \text{ 的判别式为 } d_{B/F}(\xi_1, \dots, \xi_n) = \det(T_{B/F}(\xi_i, \xi_j))$$

例 $\mathcal{O}$ 为 K 的整型 $\mathcal{O}/P$ 则 $P \in \mathcal{O}^e \cap \mathbb{Z} \quad e = e(P/P) \Rightarrow P\mathbb{Z} \subseteq \mathcal{O}^e \cap \mathbb{Z} \subseteq \mathbb{Z}$
 $\Rightarrow \mathcal{O}^e \cap \mathbb{Z} = P\mathbb{Z}$

$$\text{定义 } \varphi: \mathbb{Z} \rightarrow \mathcal{O}_K/P\mathcal{O}_K \quad \ker \varphi = \mathcal{O}^e \cap \mathbb{Z} = P\mathbb{Z}$$

故 $\mathbb{Z}/P\mathbb{Z}$ 可视为 $\mathcal{O}_K/P\mathcal{O}_K$ 的子域 $\Rightarrow \mathcal{O}_K/P\mathcal{O}_K$ 为 $\mathbb{Z}_P$ -代数

再对一般 $P \quad P\mathcal{O}_K = P_1^{e_1} \cdots P_g^{e_g} \Rightarrow \mathcal{O}_K/P\mathcal{O}_K \cong \mathcal{O}_K/P_1^{e_1} \oplus \cdots \oplus \mathcal{O}_K/P_g^{e_g}$
 $\Rightarrow \mathcal{O}_K/P\mathcal{O}_K$ 为 $\mathbb{Z}_P$ -代数

Lem. (a) $w_1, \dots, w_n$ 整基 则 $\{\bar{w}_1, \dots, \bar{w}_n\}$ 为 $B = \mathcal{O}_K/P\mathcal{O}_K$ 的 $\mathbb{Z}_P$ -基

$$(b) \lambda \in \mathcal{O}_K \text{ 则 } T_{B/\mathbb{Z}_P}(\bar{\lambda}) = \overline{T_{K/\mathbb{Q}}(\lambda)} \quad d_{B/\mathbb{Z}_P}(\bar{w}_1, \dots, \bar{w}_n) = \overline{d(K)}$$

若 $\mathbb{Z}_P$ -代数 $B_i = \mathcal{O}_K/P_i^{e_i}$ $|\mathcal{O}_K/P_i^{e_i}| = N(P_i^{e_i}) = P^{e_i f_i}$
 $\Rightarrow \dim_{\mathbb{Z}_P} B_i = e_i f_i$

Prop. $\eta_1, \dots, \eta_{e_i f_i}$ 为 B_i 的 $\mathbb{Z}_P$ -基 则 $d_{B_i/\mathbb{Z}_P}(\eta_1, \dots, \eta_{e_i f_i}) = 0 \Leftrightarrow e_i \geq 2$

P 的主下标: 若 $e \geq 2$ 则取 $\pi \in P - P^2$ 有 $\pi \neq 0 \quad \pi^e = 0$ (关于 P^e 的类)

$$\text{取基 } \{\xi_1, \dots, \xi_{ef}\} \text{ s.t. } \xi_1 = \pi$$

$$0 = (\pi \xi_j)^e (\xi_1, \dots, \xi_{ef}) = (\xi_1, \dots, \xi_{ef}) A(\pi \xi_j)^e$$

$$\Rightarrow A(\pi \xi_j) \text{ 非零} \Rightarrow T_{B/\mathbb{Z}_P}(\xi_i, \xi_j) = 0 \xrightarrow{\text{对 } i, j \text{ 求和}} d_{B/\mathbb{Z}_P}(\xi_1, \dots, \xi_{ef}) = 0$$

$$\Rightarrow d_{B/\mathbb{Z}_P}(\eta_1, \dots, \eta_{ef}) = 0$$

反之若 $e=1$ $B=O_K/p$ 为 $\mathbb{Z}_p$ 的分式域 $\Rightarrow$ 为 P^f 元域 且为单扩张

$B=\mathbb{Z}_p(\bar{\alpha})$ 极小多项式 $f(x)$ 不可约 f 次 根为 $\bar{\alpha}, \bar{\alpha}^p, \dots, \bar{\alpha}^{p^{f-1}}$

$$\text{令 } \bar{\mu}(\bar{\alpha}, \bar{\alpha}^p, \dots, \bar{\alpha}^{p^{f-1}}) = (\bar{\alpha}, \bar{\alpha}^p, \dots, \bar{\alpha}^{p^{f-1}}) A(\bar{\mu})$$

$f(A(\bar{\alpha})) = A(f(\bar{\alpha})) = 0 \Rightarrow f$ 为 $A(\bar{\alpha})$ 特征多项式 根 $\bar{\alpha}, \dots, \bar{\alpha}^{p^{f-1}}$

$$\Rightarrow T_{B/\mathbb{Z}_p}(\bar{\alpha}^i) = \sum_{j=0}^{f-1} (\bar{\alpha}^j)^{p^i}$$

可证 $d_{B/\mathbb{Z}_p}(\bar{\alpha}, \dots, \bar{\alpha}^{p^{f-1}}) \stackrel{\text{Vandermonde}}{\neq} 0$ 非 0!

Thm (Dedekind 判别式定理) P 在 K 中分歧 $\Leftrightarrow P | d(K)$

pf. 取 $\bar{w}_1, \dots, \bar{w}_n$ 为 $B=O_K/pO_K$ 的 $\mathbb{Z}_p$ -基. 则 $P | d(K) \Leftrightarrow d_{B/\mathbb{Z}_p}(\bar{w}_1, \dots, \bar{w}_n) = 0$

取 $\{\xi_{i,e}, f_i\}$ 为 $B_i = O_K/p_i$ 的 $\mathbb{Z}_p$ -基

$$\text{则 } d_{B/\mathbb{Z}_p}(\xi_{i,j}) = \prod_{i=1}^n d_{B_i/\mathbb{Z}_p}(\xi_{i,1}, \dots, \xi_{i,e_i}, f_i)$$

故 $P | d(K) \Leftrightarrow$ 至少有一个 $d_{B_i/\mathbb{Z}_p}(\xi_{i,1}, \dots, \xi_{i,e_i}, f_i) = 0 \stackrel{\text{prop}}{\Leftrightarrow}$ 分歧.

例. (1) 至多有有限个 P 分歧

(2) $K=\mathbb{Q}(\omega)$ $\omega^3+\omega+1=0$ $d(K)=-31 \Rightarrow$ 只有 $P=31$ 分歧

(3) $K=\mathbb{Q}(\zeta_5)$ $\zeta=\zeta_p$ 只有 P 分歧 事实上完全分歧

Thm $m \neq 0$ 无平方因子. 则 $m=ab^2$. a, b 互素且无平方因子.

$$\text{令 } \alpha = \sqrt[3]{m} \quad \beta = \sqrt[3]{a^2b} \quad \text{令 } K = \mathbb{Q}(\sqrt[3]{m}) = \mathbb{Q}(\alpha). \text{ 则}$$

(1) 若 $a^2 \not\equiv b^2 \pmod{9}$. 则 α, β 为 O_K 的整基

若 $a^2 \equiv b^2 \pmod{9}$ 则 $\{\alpha, \beta, \gamma = \frac{1+\alpha\beta+\beta^2}{3}\}$

$$(2) d(K) = \begin{cases} -27a^2b^2 & a^2 \not\equiv b^2 \pmod{9} \\ -3a^2b^2 & a^2 \equiv b^2 \pmod{9} \end{cases}$$

(3) $P | ab$ 则 P 完全分歧 $P=3$ 时 $\begin{cases} P \text{ 完全分歧} & a^2 \not\equiv b^2 \pmod{9} \\ 3O_K = P_1^2 P_2 & a^2 \equiv b^2 \pmod{9} \end{cases}$

2.3 Galois扩张的素理想分解

首先将理想的范 $N_K(A)$ 推广.

Def. 数域扩张 L/K . $\mathfrak{p}$ 为 K 中素理想. $\mathfrak{P}|\mathfrak{p}$. $f = f(\beta|\mathfrak{p})$

定义 $N_{L/K}(\mathfrak{p}) = \mathfrak{p}^f$

更一般对 $\alpha = \beta_1^{e_1} \cdots \beta_r^{e_r}$ 定义 $N_{L/K}(\alpha) = \prod_{i=1}^r N_{L/K}(\beta_i)^{e_i}$

假设 L/K Galois $G = \text{Gal}(L/K)$

$\forall \alpha \in \mathcal{O}_L$. $\sigma \in G$ 有 $\sigma(\alpha) \in \mathcal{O}_L \Rightarrow \sigma(\mathcal{O}_L) = \mathcal{O}_L$

若 $\mathfrak{p}$ 为 $\mathcal{O}_K$ 素理想 则 $\sigma(\mathfrak{p}) = \{\sigma(\alpha) | \alpha \in \mathfrak{p}\}$ 也为素理想. 称为 K -共轭理想

Thm L/K Galois 扩张. $n = [L:K]$. $\mathfrak{p}$ 为 $\mathcal{O}_K$ 素理想

$\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ $f_i = f(\beta_i|\mathfrak{p})$ 则

- (a) G 在 $\{\beta_1, \dots, \beta_g\}$ 上可逆作用
- (b) $\forall i$ $\{\beta_1, \dots, \beta_g\}$ 为 β_i 的全部 K -共轭理想
- (c) $e_1 = \dots = e_g \stackrel{\Delta}{=} e$, $f_1 = \dots = f_g \stackrel{\Delta}{=} f$ 则 $n = efg$
- (d) 任意 $\mathfrak{u}$ 为 L 中理想 有 $N_{L/K}(\mathfrak{u})\mathcal{O}_L = \prod_{\sigma \in G} \sigma(\mathfrak{u})$

(记略)

且有 $D_{\mathfrak{p}} = \{\sigma \in G | \sigma(\mathfrak{p}) = \mathfrak{p}\}$ 为 G 的 ef 阶子群: $\mathfrak{p}$ 的分解群

$\bar{L} = \mathcal{O}_L/\mathfrak{p}$ $\bar{K} = \mathcal{O}_K/\mathfrak{p}$

$\sigma \in D_{\mathfrak{p}} \rightsquigarrow \bar{\sigma}: \bar{L} \rightarrow \bar{L} \rightsquigarrow \pi: D_{\mathfrak{p}} \rightarrow \text{Gal}(\bar{L}/\bar{K})$
 $\alpha \mapsto \overline{\sigma(\alpha)} \quad \sigma \mapsto \bar{\sigma}$

Lemma. π 为满射. $\text{Ker } \pi = I_\beta = \{\sigma \in D_\beta \mid \sigma(\alpha) \equiv \alpha \pmod{\beta}, \forall \alpha \in \mathcal{O}_L\}$
 $|I_\beta| = e$. 且 D_β/I_β 为分裂域

pf. $\forall \bar{\sigma} \in \text{Gal}(\bar{L}/\bar{K})$ $\bar{L}/\bar{K}$ 有限域扩张 $\Rightarrow \bar{L} = \bar{K}(\bar{\alpha})$ $\bar{\alpha} \in \bar{\mathcal{O}}_L$

由 Galois 对应. 存在域 $K_0 = \{\alpha \in L \mid \sigma(\alpha) = \alpha, \forall \sigma \in I_\beta\}$

L/K_0 为 Galois 扩张. $\text{Gal}(L/K_0) = I_\beta$.

令 $\mathcal{O}_D = \mathcal{O}_{K_D}$ $\beta \cap \mathcal{O}_D = \beta_D$ β_D 对 L/K_0 自然. 由 Thm

$$\beta \cap \mathcal{O}_L = \beta^{e'} \quad e' = e(\beta/\beta_D) \quad f' = f(\beta/\beta_D)$$

$$\text{则 } e' \cdot e(\beta_D/p) = e \quad f' \cdot f(\beta_D/p) = f \quad e' f' = [L:K_0] = ef \Rightarrow e = e' \quad f = f' \\ e(\beta_D/p) = f(\beta_D/p) = 1$$

$$\text{故 } \mathcal{O}_D/p = \mathcal{O}_{K_D}/p$$

$$\alpha \text{ 在 } K_D \text{ 上极小多项式 } f(x) \in \mathcal{O}_D[x]. \xrightarrow{\text{mod } \beta_D} \bar{f}(x) \in \bar{K}[x] \\ (\text{根为 } \sigma(\alpha), \sigma \in I_\beta) \quad (\text{根为 } \bar{\sigma}(\bar{\alpha}) \dots) \Rightarrow \bar{\sigma}(\bar{\alpha}) \neq \bar{\sigma}(\alpha)$$

$$\text{Ker } \pi = \{\sigma \in D_\beta \mid \bar{\sigma} = 1\} = \{\sigma \in D_\beta \mid \sigma(\alpha) = \alpha, \forall \alpha \in \bar{L}\} = I_\beta \\ \Rightarrow D_\beta/I_\beta \cong \text{Gal}(\bar{L}/\bar{K}) \text{ 分裂域.}$$

I_β : 惯性群 为 D_β 的 e 阶子群

K_D : 分解域

$$K_I = \{\alpha \in L \mid \sigma(\alpha) = \alpha, \forall \sigma \in I_\beta\}: \text{惯性域}$$



Thm. L/K 为 Galois 扩张 $n = [L:K]$ P 为 K 中单因子多项式

$$PO_L = (\beta_1 \cdots \beta_g)^e \quad f = f(\beta_i/P) \quad \beta = \beta_1$$

Pr) (1) $L/K_I, L/K_D, K_I/K_D$ 均为 Galois 对 L/K Galois 群 $I_P, D_P, D_P/I_P$

(2) $\beta_I = \beta \cap O_I, \beta_D = \beta \cap O_D$ 则

$$(a) P = \beta_D \cap O_K, e(\beta_D/P) = f(\beta_D/P) = 1$$

当 $D_P \triangleleft \text{Gal}(L/K)$ 时 P 在 K_D 中完全分裂

$$(b) \beta_D O_I = \beta_I \quad f(\beta_I/\beta_D) = f \quad \text{即 } \beta_D \text{ 在 } K_I \text{ 中惯性}$$

$$(c) \beta_I O_L = P^e \quad f(\beta/\beta_I) = 1 \quad \text{即 } \beta_I \text{ 在 } L \text{ 中完全分裂}$$

现设 P 不分裂 in L 即 $PO_L = \beta_1 \cdots \beta_g, \beta = \beta_1 \Rightarrow I_P = \{1\}$

D_P 为 f 个互异的 P 群. $D_P \cong \text{Gal}(L/E)$ $|E| = |O_L/P| = N_K(P)$

则 $\text{Gal}(L/E)$ 由 $\{\gamma \mapsto \gamma^{N_K(P)}\}$ 生成

$$\sigma \mapsto \left(\frac{\beta_1}{\beta} \right) \in D_P$$

$$\text{由 } \left(\frac{\beta_1}{\beta} \right) \alpha \equiv \alpha^{N_K(P)} \pmod{\beta} \quad (\forall \alpha \in O_L) \text{ 刻画}$$

Prop. (1) $E_1/K, E_2/K$ Galois. $L = E_1 E_2$ 则 L/K Galois. 且

$\text{Gal}(L/K)$ 同构于 $\text{Gal}(E_1/K) \times \text{Gal}(E_2/K)$ 的一个子群

(2) K 中单因子多项式 P 在 L 中不分裂 $\Leftrightarrow P$ 在 E_1, E_2 中不分裂

(3) $\quad \quad \quad$ 完全分裂 $\Leftrightarrow \quad \quad \quad$ 完全分裂

(Galois 群 Abel)

Lem. L/K Abel 扩张 则 K_0 是使 P 完全分裂的最大中间域

$\downarrow$
 D_P 均相同 K_I 是使 P 不分裂的最大中间域

I_P

例. $K = \mathbb{Q}(\sqrt{5}, \sqrt{3})$ $G = \text{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$ $\sigma: \sqrt{5} \mapsto \sqrt{5}$
 $\sqrt{3} \mapsto \sqrt{3}$
 $\tau: \sqrt{5} \mapsto -\sqrt{5}$
 $\sqrt{3} \mapsto -\sqrt{3}$
 为Abel群. 3个中间域 $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{15})$
 $\parallel$ $\parallel$ $\parallel$
 K_1 K_2 K_3

2在 K_1 中分歧 K_2 中不分歧 $5 \equiv 5 \pmod{8}$

$\Rightarrow$ 2的惯性域为 K_2 又2在 K_2 中惯性 $\Rightarrow$ 2的分解域为 $\mathbb{Q}$

类似3的 惯性域为 K_3 分解域为 $\mathbb{Q}$

也可讨论p=5.

例. 考虑分圆域 $K = \mathbb{Q}(\zeta_m)$ $m \not\equiv 2 \pmod{4}$

Thm. (a) p 在 K 中不分歧 $\Leftrightarrow p \nmid m$, 此时 $p\mathcal{O}_K = \mathfrak{p} \cdots \mathfrak{p}_g$ $g = \frac{\varphi(m)}{f}$
 $f = f(\mathfrak{p}/p)$ 为 p 模 m 的指数

(b) 若 $p \mid m$. 设 $m = p^r m'$ 则 $p\mathcal{O}_K = (\mathfrak{p} \cdots \mathfrak{p}_g)^e$
 其中 $e = \varphi(p^r)$ $g = \frac{\varphi(m')}{f}$ f 为 p 模 m' 的指数

则 $\mathfrak{p} \in \mathbb{Q}(\zeta_m)$ 中 惯性域为 $\mathbb{Q}(\zeta_{m'})$

分解域为 $\mathbb{Q}(\zeta_m)$ 中分解域. 且 $[K:\mathbb{Q}] = g$

Pf. (a) 因为 $d(K) = \frac{m}{\prod_{p \mid m} p} \frac{\varphi(m)}{p-1} \Rightarrow$ Dedekind 判别式定理

此时 $(\frac{K/\mathbb{Q}}{\mathfrak{p}}) \alpha \equiv \alpha^f \pmod{\mathfrak{p}} (\forall \alpha \in \mathcal{O}_K = \mathbb{Z}[\zeta_m])$

$\text{Gal}(K/\mathbb{Q})$

则 $f = \text{ord}(\frac{K/\mathbb{Q}}{\mathfrak{p}})$ 为 $\mathfrak{p}$ 的指数 $\epsilon^f \equiv 1 \pmod{m}$ 最小 f

$\Rightarrow (\frac{K/\mathbb{Q}}{\mathfrak{p}}) \zeta_m = \zeta_m^{\epsilon} \pmod{\mathfrak{p}}$ 再 $\exists i \in \mathbb{Z}$ $\epsilon \equiv p \pmod{m \nmid p}$

计算得: 2在 $\mathbb{Q}(\zeta_8)$ 中 惯性域为 $\mathbb{Q}(\zeta_4)$

分解域为 $\mathbb{Q}(\sqrt{-1})$

2.4 Kronecker-Weber 定理

定义 Gauss 和 $G_p(r) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^{ra} \in \mathbb{Q}(\zeta_p)$

Prop. 对 p 奇素数, 有 (1) $G_p(0) = 0$ (2) $G_p(r) = \left(\frac{r}{p}\right) G_p(1)$
(3) $G_p(1)^2 = \left(\frac{-1}{p}\right) p$

Thm (二次互反律) $p \neq q$ 奇素数. 则 (1) $p \nmid a$ 时 $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$
(2) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4} \\ -1, & p \equiv 3 \pmod{4} \end{cases}$
(3) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$
(4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{8}} = \begin{cases} 1, & p \equiv \pm 1 \pmod{8} \\ -1, & p \equiv \pm 3 \pmod{8} \end{cases}$

Thm $K = \mathbb{Q}(\sqrt{d})$ 则 $L = \mathbb{Q}(\zeta_{|d(K)|})$ 为包含 K 的极小分圆域

Pf. 设 $d = \pm p_1 \cdots p_s$, p_i 为不同奇素数. 记 $p_i^* = \left(\frac{-1}{p_i}\right) p_i \Rightarrow d = \pm p_1^* \cdots p_s^*$
又 $p_i \equiv 1 \pmod{4} \Rightarrow d = p_1^* \cdots p_s^*$ 时 $d(K) = d$
 $d = -\dots$ $d(K) = 4d$

$d(K) = d \Rightarrow G_{p_i}(1) \in \mathbb{Q}(\zeta_{p_i})$ 且 $G_{p_i}(1) = \pm \sqrt{p_i^*} \Rightarrow \sqrt{p_i^*} \in \mathbb{Q}(\zeta_{p_i})$

则 $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{p_1^* \cdots p_s^*}) \subseteq \mathbb{Q}(\sqrt{p_1^*} \cdots \sqrt{p_s^*}) \subseteq \mathbb{Q}(\zeta_{p_1} \cdots \zeta_{p_s}) = L$

$d(K) = 4d \Rightarrow \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{p_1^*}, \sqrt{p_s^*}) \subseteq \mathbb{Q}(\zeta_{4p_1} \cdots \zeta_{p_s}) = L$

再设 $d = \pm 2 p_1 \cdots p_s$ 此时 $|d(K)| = 8 p_1 \cdots p_s$

$\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\sqrt{\pm 2}, \sqrt{p_1^*}, \sqrt{p_s^*}) \subseteq \mathbb{Q}(\zeta_8, \zeta_{p_1}, \cdots, \zeta_{p_s}) = L$

综上 L 即为包含 K 的分圆域 证毕

设 $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_m)$ 若 $d = p_1^* \cdot p_2^*$ 则 p_1 在 $\mathbb{Q}(\sqrt{d})$ 中分歧 $\Rightarrow \mathbb{Q}(\zeta_m)$ 中分歧
 若 $d = -p_1^* \cdot p_2^*$ 则 p_1 和 2 分歧 $\Rightarrow 2|m$ $\Rightarrow p_1|m$
 $\Rightarrow |d(K)|/m$
 又 2 在 $\mathbb{Q}(\zeta_{2p_1 p_2}) = \mathbb{Q}(\zeta_{p_1 p_2})$ 中不分歧 $\Rightarrow 4|m \Rightarrow |d(K)|/m$
 $d = \pm 2p_1^* \cdot p_2^*$ 由 2 个 $\mathbb{Q}(\sqrt{\pm 2})$ 的最小分圆域为 $\mathbb{Q}(\zeta_8) \Rightarrow 8|m$ ✓

事实上这是如下重要定理的特殊情形

Thm (Kronecker-Weber) Abel 数域为分圆域的子域

Def. K 为 Abel 数域 若 $\mathbb{Q}(\zeta_m)$ ($m \neq 2 \bmod 4$) 为包含 K 的最小分圆域
 称 m 为 K 的 **导子** 记 $f(K)$

Def. 对 n -次 Galois 数域 K 若 $PO_K = (P \cdot P_g)^e$ $e f g = n$ 则称
 P 在 K 中的 **分解型式** 为 (e, f, g) $e=1$ 时也可略去

Thm (Abel 域中互反律) K Abel 域 p, p' 素且 $(p, f(K)) = (p', f(K)) = 1$

若 $p \equiv p' \bmod f(K)$ 则 p, p' 在 K 中分解型式相同

Pf. $K \subseteq L = \mathbb{Q}(\zeta_{f(K)})$ $G = \text{Gal}(L/\mathbb{Q}) \xrightarrow{\varphi} (\mathbb{Z}/f(K)\mathbb{Z})^\times$
 $\sigma_a \mapsto a \bmod f(K)$

若 N 为 K 的分圆子域 则 $\text{Gal}(K/\mathbb{Q}) \subseteq N \subseteq (\mathbb{Z}/f(K)\mathbb{Z})^\times / \varphi(N)$

$(p, f(K)) = 1 \Rightarrow p$ 在 L 中不分歧 从而在 K 中不分歧

$PO_K = P \cdot P_g$ $f = f(p, P)$ $f g = n$ $I_p = \{1\}$

此时 D_p 为 f 的循环群 由 $\tau_p = (\frac{k/a}{p})$ 生成

又 $\sigma_p = (\frac{L/a}{p})$ $\sigma_p|_K = \bar{\varphi} \Rightarrow f$ 为满足 $(\sigma_p|_K)^f = 1$ 的最小正数
 $\Rightarrow f$ 为满足 $\bar{p}^f \in \varphi(N) \dots$

设 $\varphi(N) = \{\bar{a}_1, \dots, \bar{a}_t\}$ $t = |N| = [L:K] \Rightarrow p^f \equiv a \pmod{f(K)}$ $a \in \{a_1, \dots, a_t\}$

故 f 只与 p 模 $f(K)$ 的同余类有关

例. $L = \mathbb{Q}(\omega)$ $\omega = \zeta_{17}$ $G = \text{Gal}(L/\mathbb{Q}) = \langle \sigma_3 \rangle$

K 为 L 的唯一的 4 次循环子域. 固定子群为 $N = \{\sigma_1, \sigma_{3^4}, \sigma_{3^8}, \sigma_{3^{12}}\}$
 $= \{\sigma_1, \sigma_{-4}, \sigma_{-1}, \sigma_4\}$

$\Rightarrow K = \mathbb{Q}(\zeta)$ $\zeta = \omega + \omega^{-1} + \omega^4 + \omega^{-4}$

p 在 K 中分裂性 $\Leftrightarrow p^f \equiv 3^0, 3^4, 3^8, 3^{12} \pmod{17}$ 的最小 f 为 4

$\Leftrightarrow p \equiv \pm 3, \pm 5, \pm 6, \pm 7 \pmod{17}$

p 在 K 中不分裂 $\Leftrightarrow p \equiv \pm 2, \pm 9 \pmod{17}$

p 完全分裂 $\Leftrightarrow p \equiv \pm 1, \pm 4 \pmod{17}$

Chap3 理想类群 单位群

3.1 类群与类数

对 H 为 $\mathbb{R}^n$ 中的格 $\{\alpha_1, \dots, \alpha_n\}$ 为基 $P(\alpha_1, \dots, \alpha_n) = \{ \sum_{i=1}^n a_i \alpha_i \mid 0 \leq a_i < 1 \}$
 $\mu(P(\alpha_1, \dots, \alpha_n))$ 与 $\{\alpha_1, \dots, \alpha_n\}$ 选取无关, 记 $V(H)$

Lemma (1) H, H' 为 $\mathbb{R}^n$ 中的格. $H \supseteq H'$. 则 H/H' 有限. 且 $|H/H'| = \frac{V(H')}{V(H)}$

(2) $\mathbb{R}^n$ 中的格为 $\mathbb{R}^n$ 的高散子群

(3) $\mathbb{R}^n$ 中的高散子群必为某个 r 维子空间的格

Thm (Minkowski) H 为 $\mathbb{R}^n$ 中的格. S 为 $\mathbb{R}^n$ 中可测集

(1) 若 $\mu(S) > V(H)$. 则 $\exists s, s' \in S$ s.t. $s - s' \in H$

(2) 若 S 关于原点对称. 则若 $\mu(S) > 2^n V(H)$: $S \cap H$ 中有非零向量

(3) 若 $\dots$ 则 $\dots$

现在对数域 K . O_K 的全部非零理想类记为 $I^0(K)$

有消主律的乘法群 M
(则 $G = \{ \frac{A}{B} \mid A, B \in M \}$ 为群 $(\frac{A}{B} \sim \frac{C}{D} \Leftrightarrow AD = BC)$)

故对 $I \subseteq K$ 称 I 为分式理想 若 $\exists 0 \neq \mu \in O_K$ s.t. $\mu I \subseteq O_K$

$I(K)$ 为分式理想全体

(一般简记分式理想为理想 O_K 中理想为整理想)

对分式理想 $I = \frac{A}{B}$ 定义 $N_K(I) = \frac{N_K(A)}{N_K(B)}$

$$A, B \in I(K) \text{ 则 } A \times B = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in A, b_i \in B \right\}$$

→ i 为分式理想群

Thm (a) $I(K)$ 为群 且 $I^0(K)$ 为 $I(K)$ 的子群. 即分式理想群可表示为互素理想之商

(b) $I(K)$ 自由 Abelian 群. O_K 的非零素理想为基

$\alpha \in K \quad \alpha O_K$: 主分式理想 $\leadsto$ 主分式理想群 $P(K)$

Def. $C(K) = I(K)/P(K)$: (分式理想类群) 元素称为(分式)理想类

将 $C(K)$ 有限 Abelian. $h(K) = |C(K)|$ 类数

$$h(K) = 1 \Leftrightarrow I(K) = P(K) \Leftrightarrow O_K \text{ 为 PID} \Leftrightarrow O_K \text{ 为 UFD}$$

$$(13) \quad h(O(\mathbb{Q}_p)) = 1 \quad p \neq 2 \text{ (素)}$$

对 n -数域 K 有 r_1 个实嵌入 r_2 对复嵌入

$$G: K \rightarrow \mathbb{R}^n$$

$$\alpha \mapsto (G_1(\alpha), \dots, G_r(\alpha), \operatorname{Re}(G_{r+1}(\alpha)), \dots, \operatorname{Re}(G_{r+r_2}(\alpha)), \operatorname{Im}(G_{r+1}(\alpha)), \dots, \operatorname{Im}(G_{r+r_2}(\alpha)))$$

正实嵌入

引理. α 为 n -数域 K 中非零整理想. 则 $G(\alpha)$ 为 $\mathbb{R}^n$ 中的格

$$\text{且 } V(G(\alpha)) = 2^{-r_2} N(\alpha) |d(K)|^{\frac{1}{2}}$$

Let α 为 K 中非零理想. $[K:\mathbb{Q}] = n = r_1 + 2r_2$

$$\text{则 (a) } \exists 0 \neq x \in \alpha, \text{ s.t. } |N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d(K)|^{\frac{1}{2}} N(\alpha)$$

(b) K 的每个理想类 C 中 都有理想 β s.t.

$$N(\beta) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d(K)|^{\frac{1}{2}}$$

pf. (a) 对 $y = (y_1, y_2) \in \mathbb{R}^n$ 定义 $\lambda(y) = \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} (y_{r_1+j}^2 + y_{r_1+n+j}^2)^{\frac{1}{2}}$

对 $t > 0$ 定义 $B_t = \{y \in \mathbb{R}^n : \lambda(y) \leq t\}$ 关于原点对称. 紧. $|\cdot|$

$$\text{且 } \mu(B_t) = \int_{\lambda(y) \leq t} dy_1 \dots dy_n = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$$

$$\text{取 } t = \left(\frac{4}{\pi}\right)^{r_2} N(\alpha) |d(K)|^{\frac{1}{2}} n! \beta t. \mu(B_t) = 2^n V(\sigma(\alpha))$$

由 Minkowski 原理. $\exists 0 \neq x \in \alpha$ $\sigma(x) \in B_t$ 且 $\lambda(\sigma(x)) \leq t$

$$\Rightarrow |N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^n |\sigma_i(x)| \leq \left(\frac{1}{n} \sum_{i=1}^n |\sigma_i(x)|\right)^n = \frac{1}{n^n} \lambda(\sigma(x))^n \quad \checkmark$$

(b) 对 $\alpha \in C$. 已知 $\alpha = \alpha'^{-1}$ 为理想. 由 (a).

$\exists 0 \neq x \in \alpha$ s.t. $N(x) \leq \dots$ $\alpha \beta = x \alpha'$ 为理想

$$\text{且 } N(\beta) = N(x) N(\alpha)^{-1} \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d(K)|^{\frac{1}{2}} \quad \checkmark$$

$$\text{Cor. } n = [K:\mathbb{Q}] \geq 2 \text{ 时 } |d(K)| \geq \frac{\pi}{3} \left(\frac{3}{4}\right)^{n-1} \Rightarrow \exists N \text{ s.t. } \frac{n}{\log |d(K)|} \leq N$$

Thm (Minkowski) $\forall K \neq \mathbb{C}$ 均 $|d(K)| > 1$ 则存在一个非零数在 K 中绝对值

Thm (Dirichlet) $h(K) < +\infty$

pf. $\forall q \in \mathbb{Z}, q \geq 1$ 有 $N(\alpha) = q \Rightarrow \bar{q} = \bar{0} \in \mathcal{O}_K / \alpha \Rightarrow \alpha | q \mathcal{O}_K$

$\Rightarrow \alpha$ 只有有限个

又由 Lem(b). 每个理想类中都有 β s.t. $N(\beta) \leq M \Rightarrow$ 只有有限个类

Thm(Hermite) $\forall d \in \mathbb{Z}$ 只有有限个数域 K s.t. $d(K)=d$

Pf. n 有界, r_1, r_2 有限, 故只需对固定 n, r_1, r_2 证明

$r_1 > 0$ 时 令 $B = \left\{ y: \begin{aligned} &1 \leq |y_i| \leq 2^{n-1} \left(\frac{\pi}{2}\right)^{-r_1} |d|^{\frac{1}{2}} \\ &|y_i| \leq \frac{1}{2} (2 \leq i \leq r_1) \\ &(y_{r_1+j}^2 + y_{r_1+r_2+j}^2) \leq \frac{1}{2} (1 \leq j \leq r_2) \end{aligned} \right\}$

$\Rightarrow \mu(B) = 2^{n-r_2} |d|^{\frac{1}{2}}$

$r_1 = 0$ 时 令 $B = \left\{ y: \begin{aligned} &1 \leq |y_1| \leq \frac{1}{2} \\ &1 \leq |y_{r_2+1}| \leq 2^n \left(\frac{\pi}{2}\right)^{-r_2} |d|^{\frac{1}{2}} \\ &(y_j^2 + y_{r_2+j}^2) \leq \frac{1}{2} (2 \leq j \leq r_2) \end{aligned} \right\}$

$\wedge V(\mathcal{O}_K) = 2^{-r_2} |d|^{\frac{1}{2}} \Rightarrow \exists 0 \neq x \in \mathcal{O}_K, G(x) \in B$

$r_1 > 0$ 时 $|N(x)| \geq 1 \Rightarrow |G_i(x)| \geq 1 \Rightarrow G_i(x) (1 \leq i \leq n)$ 两两不同

$r_1 = 0$ 时 $\exists x$ 有 n 个不同的共轭元素 即 x 的极小多项式 $\geq n$ 次
 $\Rightarrow$ 配 $K = \mathbb{Q}(x)$

又 x 的极小多项式的系数为 $G_i(x)$ 的对称函数 $\Rightarrow$ 系数有上界

又 $x \in \mathcal{O}_K \Rightarrow$ 系数 $\in \mathbb{Z} \Rightarrow$ 有限个 $\checkmark$

例 $K = \mathbb{Q}(\sqrt{d})$ $d > 0$ 无平方因子 $\Rightarrow n=2, r_2=0$ $M(K) = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d(K)|^{\frac{1}{2}}$
 $= \frac{1}{2} |d(K)|^{\frac{1}{2}}$

$K = \mathbb{Q}(\sqrt{5}) \Rightarrow d(K)=5, M(K) < 2$ 则 K 的理想类均有主理想 $A, N_K(A)=1$
 $\Rightarrow h(K)=1, \mathcal{O}_K = \mathbb{O}(\frac{1+\sqrt{5}}{2})$ 为 PID UFD $\hookrightarrow A = \mathcal{O}_K$

$d(K)=40$
 $K = \mathbb{Q}(\sqrt{10}) \quad M(K) = \frac{1}{2} \sqrt{40} < 4 \quad 2\mathcal{O}_K = \mathcal{P}_2^2 \quad N(\mathcal{P}_2) = 2$
 $3\mathcal{O}_K = \mathcal{P}_3 \mathcal{P}_3 \quad N(\mathcal{P}_3) = N(\overline{\mathcal{P}_3}) = 3$

$[\mathcal{P}_2] = 1 \Leftrightarrow \mathcal{P}_2$ 为主理想 $\Leftrightarrow 2 = N(\mathcal{P}_2) = |N(\alpha)|$
 $\alpha = a + b\sqrt{10}$
 $\Leftrightarrow a^2 - 10b^2 = \pm 2 \quad X$

故 $[\mathcal{P}_2] \neq 1 \Rightarrow \mathcal{P}_2$ 为 2 阶元
 $([\mathcal{P}_2]^2) = [\mathcal{O}_K] = 1$

$$\text{例- 例 } \alpha = 2 + \sqrt{10} \in \mathcal{O}_K \quad N(\alpha) = 6 \Rightarrow (\alpha) = \mathfrak{p}_2 \mathfrak{p}_3 \text{ 或 } \mathfrak{p}_3^2$$

$\Rightarrow \mathbb{C}(K)$ 由 $\mathbb{C}(\sqrt{10})$ 生成

$$h(K) = 2$$

$$\text{例 } K = \mathbb{Q}(\sqrt{-23}) \quad \mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right] \quad M(K) = \frac{2}{\pi}\sqrt{23} < 4$$

$$\text{由 } \left(\frac{-23}{3}\right) = 1 \quad -23 \equiv 1 \pmod{3} \Rightarrow 2, 3 \text{ 分 } \mathfrak{p}_2$$

$$2\mathcal{O}_K = \mathfrak{p}_2 \bar{\mathfrak{p}}_2 \quad [\bar{\mathfrak{p}}_2] = [\mathfrak{p}_2]^{-1} \quad \mathbb{C}(K) \text{ 由 } \mathbb{C}(\sqrt{-23}) \text{ 生成}$$

$$3\mathcal{O}_K = \mathfrak{p}_3 \bar{\mathfrak{p}}_3 \quad [\bar{\mathfrak{p}}_3] = [\mathfrak{p}_3]^{-1}$$

类似有 $[\mathfrak{p}_2] \neq 1$

$$\text{主理想 } \alpha = \frac{1}{2}(1+\sqrt{-23}) \in \mathcal{O}_K \quad N(\alpha) = 6$$

$$(\alpha) \sim \mathfrak{p}_2^3, \mathfrak{p}_2^2 \bar{\mathfrak{p}}_2, \mathfrak{p}_2 \bar{\mathfrak{p}}_2^2, \bar{\mathfrak{p}}_2^3$$

$$\text{又 } \mathfrak{p}_2 \bar{\mathfrak{p}}_2 = (2) \nmid (\alpha) \Rightarrow (\alpha) = \mathfrak{p}_2^3 \text{ 或 } \bar{\mathfrak{p}}_2^3 \Rightarrow \mathfrak{p}_2 \text{ 为 } 3 \text{ 阶元}$$

$$\text{再对 } \beta = \frac{1}{2}(1+\sqrt{-23}) \in \mathcal{O}_K \quad N(\beta) = 6$$

$$(\beta) \sim \mathfrak{p}_2 \mathfrak{p}_3, \bar{\mathfrak{p}}_2 \mathfrak{p}_3, \mathfrak{p}_2 \bar{\mathfrak{p}}_3, \bar{\mathfrak{p}}_2 \bar{\mathfrak{p}}_3$$

$$\text{故 } \mathbb{C}(K) \text{ 由 } \mathbb{C}(\sqrt{-23}) \text{ 生成. } h(K) = 3$$

Causs 猜想: 虚二次域 $\mathbb{Q}(\sqrt{-d})$ 中只有 $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$

$$\text{使得 } h(K) = 1$$

Baker, Stark: 证明了这是对的

3.2 Dirichlet 单位定理

U_K : O_K 的单位群

回忆 K 中单位根全体 W_K 为有限循环群 $\Rightarrow U_K = W_K \times \underbrace{U_K}_{\text{自由Abel (无扭)}}$
 $\text{tor}(U_K)$

Lemma. K 为 n 次数域. $\sigma_1, \dots, \sigma_n$ 为 n 个 K -嵌入. $u \in O_K$ 则

$$(a) u \in U_K \Leftrightarrow N_{K/\mathbb{Q}}(u) = \pm 1$$

$$(b) u \in W_K \Leftrightarrow |\sigma_i(u)| = 1 \quad (\forall 1 \leq i \leq n)$$

pf (a) $\Rightarrow N(u)N(u^{-1}) = 1$ 则 $N(u) = \pm 1$

$\Leftarrow$ u 为首一多项式 $f(x) = \prod_{i=1}^n (x - \sigma_i(u)) = x^n + a_{n-1}x^{n-1} + \dots \pm 1 \in \mathbb{Z}[x]$ 根

$\Rightarrow u^{-1}$ 为 $x \pm (a_1x^{n-1} + \dots + a_{n-1}x + 1)$ 的根 $\Rightarrow u^{-1} \in O_K$

$$(b) \Rightarrow u^m = 1 \Rightarrow \sigma_i(u)^m = 1$$

$\Leftarrow u^j$ 为 $g(x) = \prod_{i=1}^n (x - \sigma_i(u^j)) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ 的根

只有有限个这样的多项式 $\Rightarrow \exists u^j = u^k \quad (|a_i| \leq C_i)$

Thm (Dirichlet 单位定理) U_K 秩为 $r = r_1 + r_2 - 1$ 的自由Abel群

pf. $\iota: U_K \rightarrow \mathbb{R}^{r_1+r_2}$

$$\eta \mapsto (\lambda_1 \log |\eta^{(1)}|, \dots, \lambda_{r_1+r_2} \log |\eta^{(r_1+r_2)}|)$$

$$\lambda_i = \begin{cases} 1, & 1 \leq i \leq r_1 \\ 2, & r_1+1 \leq i \leq r_1+r_2 \end{cases}$$

$$\eta^{(i)} = \sigma_i(\eta)$$

$$\eta \in \ker \iota \Leftrightarrow |\eta^{(i)}| = 1 \stackrel{\text{Lemma}}{\Leftrightarrow} \eta \in W_K$$

$$\Rightarrow U_K \subseteq \iota(U_K)$$

$$\text{又 } \sum_{i=1}^{r_1+r_2} \lambda_i \log |\eta^{(i)}| = \sum_{i=1}^n \log |\eta^{(i)}| = \log |N(\eta)| \stackrel{\text{Lemma 0}}{=} 0$$

$$\Rightarrow \iota(U_K) \subseteq H = \{a \in \mathbb{R}^{r_1+r_2} \mid a_1 + \dots + a_{r_1+r_2} = 0\}$$

则 $\iota(U_K)$ 有界. 若 $\iota(\eta) \in B \Rightarrow |\eta^{(i)}| \leq e^M$

$\Rightarrow \prod_{i=1}^n (x - \eta^{(i)})$ 系数有界 $\Rightarrow$ 有限个

$\mathcal{O}_K \cap \mathcal{O}_K \cap B$ 有限 $\Rightarrow \rho(U_K)$ 为某个子空间的格

$$\Rightarrow \text{rank } V_K \leq r_1 + r_2 - 1$$

再记“ $\geq$ ”即得 同构

$$(r = r_1 + r_2 - 1)$$

定理也可表述为 $\exists \underbrace{\gamma_1, \dots, \gamma_r}_{\text{基本单位组}} \in U_K$ s.t. $\forall \eta \in U_K$ 有唯一表示 $\eta = w \gamma_1^{a_1} \dots \gamma_r^{a_r}$
 $(w \in W_K, a_i \in \mathbb{Z})$

若还有另一基本单位组 $\{\varepsilon_1, \dots, \varepsilon_r\} \Rightarrow \varepsilon_i = w_i \prod_{j=1}^r \gamma_j^{a_{ij}} \quad \det(a_{ij}) = \pm 1$

若 $\rho(\gamma_i) = (y_{i1}, \dots, y_{i, r+1})$ 定义 $R(\gamma_1, \dots, \gamma_r) = |\det(y_{ij})_{1 \leq i, j \leq r}|$

$$\text{则 } R(\varepsilon_1, \dots, \varepsilon_r) = |\det(\lambda_i \log \varepsilon_i^{(i)})|$$

$$= 2^{\max(r_2-1, 0)} |\det(\log \varepsilon_i^{(i)})| = R(\gamma_1, \dots, \gamma_r)$$

$\leadsto$ 不变量! $R(K)$ regulator

例 $K = \mathbb{Q}(\sqrt{d}) \quad d > 0 \quad \begin{matrix} r_1=2 \\ r_2=0 \end{matrix} \Rightarrow r=1$ 则基本单位组仅一个元素 ε

$W_K = \{\pm 1\} \Rightarrow U_K = \{\pm \varepsilon^n \mid n \in \mathbb{Z}\} \Rightarrow$ 显然 $\pm \varepsilon^{-1}$ 可为基本单位

进而 $\varepsilon > 1$ 的基本单位唯一

$$d \equiv 2, 3 \pmod{4}: \quad \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$$

$$a + b\sqrt{d} \text{ 单位} \Leftrightarrow a^2 - b^2d = \pm 1 \quad \text{Pell 方程}$$

Prop $\varepsilon > 1 \quad \varepsilon^n = a_n + b_n \sqrt{d}$ 则

(a) 若 $N(\varepsilon) = 1$ 则 $x^2 - dy^2 = -1$ 无 $\mathbb{Z}$ -解

$x^2 - dy^2 = 1$ 的全部 $\mathbb{Z}$ -解为 $(\pm a_n, \pm b_n) / n \in \mathbb{Z}$

(b) $N(\varepsilon) = -1$

$-1 \dots$

$(\pm a_{2n+1}, \pm b_{2n+1}) / n \in \mathbb{Z}$

$1 \dots$

$\pm a_{2n} \pm b_{2n}$

Pell方程最小解 $\leadsto$ 基本单位

$$d \equiv 1 \pmod{4}: \quad \omega = \frac{1+\sqrt{d}}{2} \quad \mathcal{O}_K = \mathbb{Z}[\omega]$$

$$\varepsilon = \frac{1}{2}(A+B\sqrt{d}) \text{ 单位} \Leftrightarrow A^2-dB^2 = \pm 4 \quad \text{再讨论}$$

例 $K = \mathbb{Q}(\alpha)$ 实二次域

$$\bar{f}(x) = x^3 + kx - 1 \quad k \geq 1, k \in \mathbb{Z} \quad (\text{此时 } r_1 = r_2 = 1)$$

若 $4k^2+27$ 无平方因子, 则 $\alpha+k$ 为基本单位

例 分圆域 $K = \mathbb{Q}(\omega)$ $\omega = \zeta_p$ 的每个单位均为实单位和单位根的乘积

Chap 4. $\zeta(s)$, $L(s, \chi)$ 和 $\zeta_K(s)$

4.1 Dirichlet级数理论

$f: \mathcal{P} \rightarrow R$ 数论函数

$\{1, 2, 3, \dots\}$ 自然数环

卷积

$$h(n) = \sum_{d|n} f(d)g(\frac{n}{d})$$

Dirichlet级数 $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$

(D-级数)

$\rightarrow D(R)$ 形式D-级数环

IS 乘法 $\Leftrightarrow$ 卷积

$R^{\mathcal{P}}$ R 上数论函数环

Lem (1) R 整环 $\Rightarrow D(R)$ 整环

(2) $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ 为 $D(R)$ 中单位 $\Leftrightarrow a_1$ 为 R 中单位

(3) f 积性 $\Leftrightarrow F(s)$ 有 Euler 展开 $F(s) = \prod_p (1 + f(p)p^{-s} + f(p^2)p^{-2s} + \dots)$
 $= \prod_p \sum_{n=0}^{\infty} \frac{f(p^n)}{p^{ns}}$

(4) 类似 $\Leftrightarrow F(s) = \prod_p (1 - f(p)p^{-s})^{-1}$

例: $f=1 \rightarrow$ Zeta 级数 $\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p (1 - p^{-s})^{-1}$

$\xrightarrow{\text{if}}$ Möbius $\mu(n) = - \sum_{d|n, d \neq n} \mu(d)$

有 $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_p (1 - p^{-s}) \Rightarrow \mu(n) = \begin{cases} 1, & n=1 \\ (-1)^r, & n \text{ 为 } r \text{ 个不同素数的积} \\ 0, & \text{其他} \end{cases}$

Möbius 反演: $f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d) \mu(\frac{n}{d})$

Thm. $F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ $a_n \cdot s \in \mathbb{C}$ $A(N) = \sum_{n=1}^N a_n$ 则

(a) $\exists -\infty \leq \sigma_0 \leq +\infty$ s.t. $\sigma > \sigma_0$ 时, $F(s)$ 收敛且半-收敛 (s = $\sigma + it$)
 $\sigma < \sigma_0$ 时 $F(s)$ 发散
收敛横坐标

(b) $F(s)$ 定义在 $\sigma > \sigma_0$ 中的正则函数 且可延拓本号

(c) 若 $A(N)$ 发散, 则 $\sigma_0 = \lim_{N \rightarrow \infty} \frac{\log A(N)}{\log N}$

Thm $a_n \geq 0$ $F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ 在 $\text{Re}(s) > c$ 中收敛. 若 $F(s)$ 在以 $s=c$ 为中心的一个
 1. 圆内解析. 则 $\exists \varepsilon > 0$ s.t. $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ 在 $\text{Re}(s) > c - \varepsilon$ 内收敛
 特别地, 若 σ_0 为收敛横坐标, 则 σ_0 为奇点

例. $a_n = 1$ $A(N) = N \rightarrow \infty$ $\sigma_0 = 1 \Rightarrow \zeta(s)$ 在 $\text{Re}(s) > 1$ 定义正则函数 $s=1$ 奇点

$a_n = (-1)^n \Rightarrow F_2(s) = \sum_{n=1}^{\infty} (-1)^n n^{-s}$ 的收敛横坐标 $\sigma_0 = 0 \Rightarrow s=1/2$ 正则

$$F_2(s) = \sum_{n=1}^{\infty} \frac{(-1)^n}{n^s} = -\sum_{n=1}^{\infty} n^{-s} + 2 \sum_{n=1}^{\infty} (2n)^{-s} \\ = -(1-2^{1-s}) \zeta(s)$$

$$\text{又 } s=1/2, 1-2^{-(s-1)} = (s-1) \log 2 + O((s-1)^2) + \dots$$

$$\Rightarrow \zeta(s) \text{ 在 } s=1 \text{ 为单极点 留数 } \text{Res}_{s=1} \zeta(s) = -\frac{F_2(1)}{\log 2} = 1$$

且 $\zeta(s)$ 的 $\text{Re}(s) > 0$ 中其它奇点只配为 $1 + \frac{2\pi i n}{\log 2}$ ($n \in \mathbb{Z}$)

Def. $\sum_{n=1}^{\infty} |a_n| n^{-s}$ 的收敛横坐标 σ_1 : $\sum_{n=1}^{\infty} a_n n^{-s}$ 的绝对收敛横坐标
 (fact: $\sigma_0 \leq \sigma_1 \leq \sigma_0 + 1$)

Thm. $f: \mathcal{P} \rightarrow \mathbb{C}$ 积性数论函数. σ_1 为绝对收敛横坐标 of $\sum f(n) n^{-s}$
 则当 $\text{Re}(s) > \sigma_1$ 时 $\prod_p (1 + \frac{f(p)}{p^s} + \dots)$ 绝对收敛, 且等于 $\sum \frac{f(n)}{n^s}$

4.2 $\zeta(s)$ 和 $L(s, \chi)$

Thm. $\zeta(s)$ 可延拓到整个 $\mathbb{C}$ 上 且满足 $\pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \pi^{-\frac{1-s}{2}} \Gamma(\frac{1-s}{2}) \zeta(1-s)$

(回忆 $\Gamma(s) = \int_0^\infty x^{s-1} e^{-x} dx$ 由 $\Gamma(s+1) = s\Gamma(s)$ 延拓到 $\mathbb{C}$)

Weierstrass 展开: $\frac{1}{\Gamma(s)} = se^{\gamma s} \prod_{n=1}^\infty (1 + \frac{s}{n}) e^{-\frac{s}{n}} \Rightarrow \frac{1}{\Gamma(s)}$ 零点为 $0, -1, -2, \dots$

$\hookrightarrow \Gamma(s)$ 在 $\mathbb{C}$ 单极点 $0, -1, -2, \dots$ $\text{res}_{s=-n} \Gamma(s) = \frac{(-1)^n}{n!}$

Poisson 求和. f 实函数. 且 $\sum_{n=-\infty}^\infty f(x+n)$ 在有限区间 (a, b) 上均一致收敛

$\int_{-\infty}^\infty |f(x)| dx$ 收敛. $\sum_{k=-\infty}^\infty |a_k|$ 收敛. 其中 $a_k = \int_{-\infty}^\infty f(x) e^{-2\pi i k x} dx$

则 $\sum_{n=-\infty}^\infty f(n) = \sum_{n=-\infty}^\infty a_n$

Pf of Thm, $\text{Re}(s) > 1$ 时

$$(\star) = \pi^{-\frac{s}{2}} \zeta(s) \Gamma(\frac{s}{2}) = \int_0^\infty \pi^{-\frac{s}{2}} \sum_{n=1}^\infty n^{-s} t^{\frac{s}{2}-1} e^{-t} dt$$

$$= \int_0^1 + \int_1^\infty t^{\frac{s}{2}-1} \sum_{n=1}^\infty e^{-\pi n^2 t} dt$$

$$= \int_1^\infty x^{\frac{s}{2}-1} w(x) + x^{-\frac{s}{2}-1} w(x^{-1}) dx \quad (w(x) = \sum_{n=1}^\infty e^{-\pi n^2 x})$$

$$\frac{1}{2} \theta(x) = \sum_{n=-\infty}^\infty e^{-\pi n^2 x} = 1 + 2w(x) \quad \text{取 } f(t) = e^{-t^2 \pi x} \Rightarrow a_n = \frac{1}{\sqrt{x}} e^{-\frac{\pi n^2}{x}}$$

$$\text{Poisson} \hookrightarrow \theta(x) = \frac{1}{\sqrt{x}} \sum_{n=-\infty}^\infty e^{-\frac{\pi n^2}{x}} = \frac{1}{\sqrt{x}} \theta\left(\frac{1}{x}\right)$$

$$\Rightarrow w\left(\frac{1}{x}\right) = -\frac{1}{2} + \frac{\sqrt{x}}{2} + \sqrt{x} w(x)$$

$$(\star) = -\frac{1}{s} - \frac{1}{1-s} + \int_1^\infty x^{\frac{s}{2}-1} w(x) + x^{\frac{1-s}{2}-1} w(x) dx \quad \text{对称性!}$$

Cor (a) $\zeta(s)$ 在 $\mathbb{C}$ 上只有一个奇点 1, 为留数为 1 的极点.

(b) $s = -2, -4, -6, \dots$ 为 $\zeta(s)$ 的单零点 (平凡零点) 其他零点均在

$0 < \text{Re}(s) < 1$ 中. 且关于 $\text{Re}(s) = \frac{1}{2}$ 对称

公. 有限 Abel G 的特记集合

$\hat{G}$ 与 G 正则同构

$$\chi: G \rightarrow \mathbb{C}^* \text{ 同构}$$

回忆正交关系

$$\sum_{g \in G} \chi(g) = \begin{cases} n, & \chi = \chi_0 \\ 0, & \text{其他} \end{cases}$$

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} n, & g = 1_G \\ 0, & \text{其他} \end{cases}$$

$\mathbb{Z}/m\mathbb{Z}$ 加法群 $\rightarrow$ 模 m 加法特记 为 $\{\chi^a \mid 0 \leq a \leq m-1\}$ $\chi^a(n) = e^{\frac{2\pi i n a}{m}}$

$(\mathbb{Z}/m\mathbb{Z})^*$ 乘法群 $\rightarrow$... 乘 $\cdot$ 正 $\cdot$ 模 m 的本原 D-特记

$\chi(-1) = 1$: 偶特记

$\chi(-1) = -1$: 奇特记

$$\downarrow$$

$$(\mathbb{Z}/m\mathbb{Z})^* \text{ (乘法群)}$$

$$\text{CRT} \\ (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_r^{a_r}\mathbb{Z})^*$$

$p \geq 3$: $(\mathbb{Z}/p^a\mathbb{Z})^*$ 为 $\varphi(p^a)$ 阶循环群 1 特记生成

$$p=2: (\mathbb{Z}/2^a\mathbb{Z})^* = \langle -1 \rangle \times \underbrace{\langle 1 \rangle}_{2^{a-2} \text{ 阶循环群}} \quad (a \geq 3)$$

Lem. χ 为模 m 的本原 D-特记 $d \mid m$ 则 $\exists \chi' \in \hat{G}$

$$(a) \exists \text{ 模 } d \text{ 的 } \dots \chi' \quad \text{s.t. } (m, a) = 1 \text{ 时 } \chi(a) = \chi'(a)$$

$$(b) (a, m) = 1 \quad a \equiv 1 \pmod{d} \Rightarrow \chi(a) = 1$$

$$(c) (a, m) = (a', m) = 1 \quad a \equiv a' \pmod{d} \Rightarrow \chi(a) = \chi(a')$$

若上两成立且 $d \neq m$ 则 χ 为模 m 的非本原 D-特记

这样的最大的 d 称为 χ 的 $\text{cond}(\chi)$

Lem. χ 为模 m D-特记. $\text{cond}(\chi) = d$. 则 χ 由模 d 的本原 D-特记诱导

Def $G(k, \chi) = \sum_{n=0}^{m-1} \chi(n) e^{\frac{2\pi i n k}{m}}$ 模 m 的 Gauss 和 $\mapsto G(k, \chi) = \sum_{n=0}^{m-1} \chi(n) e^{\frac{2\pi i n k}{m}}$
 $\downarrow$ m -加特征 $\downarrow$ m -乘特征 $(n, m) > 1$ 时规定 $\chi(n) = 0$

Thm (a) $(k, m) = 1 \Rightarrow G(k, \chi) = \bar{\chi}(k) G(1, \chi)$

(b) χ 为模 m 非平凡 D-特征. 则 $|G(1, \chi)| = \sqrt{m}$ 当 $(k, m) > 1$ 时 $G(k, \chi) = 0$

pf. (a) $G(k, \chi) = \sum_{n=0}^{m-1} \bar{\chi}(k) \chi(nk) e^{\frac{2\pi i n k}{m}}$
 $= \sum_{n=0}^{m-1} \bar{\chi}(k) \chi(n) e^{\frac{2\pi i n k}{m}} = \bar{\chi}(k) G(1, \chi)$

(b) 若 $(k, m) = d > 1$ $k' = \frac{k}{d}$ $m' = \frac{m}{d} < m \Rightarrow \exists r \equiv 1 \pmod{m'}$ 且 $\chi(r) \neq 1$
 $(d, m) = 1$

则 $G(k, \chi) = \sum_{n=0}^{m-1} \chi(n) e^{\frac{2\pi i n k}{m}} = \sum_{\lambda=0}^{m'-1} e^{\frac{2\pi i k' \lambda}{m'}} \sum_{\substack{n=0 \\ n \equiv \lambda \pmod{m'}}}^{m-1} \chi(n)$

$= \sum_{\lambda=0}^{m'-1} e^{\frac{2\pi i k' \lambda}{m'}} \sum_{n=0}^{m-1} \chi(n) = \sum_{n=0}^{m-1} \chi(n) G(k', \chi) \Rightarrow G(k, \chi) = 0$
 $\chi(n) = \chi(rn) = \chi(r) \chi(n)$

另一方面 $|G(1, \chi)|^2 = G(1, \chi) \sum_{n=0}^{m-1} \bar{\chi}(n) e^{-\frac{2\pi i n}{m}}$
 $\stackrel{(a)}{=} \sum_{n=0}^{m-1} G(n, \chi) e^{-\frac{2\pi i n}{m}} = \sum_{n, n'=0}^{m-1} \chi(n') e^{\frac{2\pi i n' n - 2\pi i n}{m}}$
 $= m \chi(1) = m$

Dirichlet L-函数 $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$

$\chi \neq \chi_0$ 时 χ 收敛于 0. $G_1 = 1$

$\Rightarrow \operatorname{Re}(s) > 1$ 时 $L(s, \chi) = \prod_p (1 - \chi(p) p^{-s})^{-1}$

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

若 $\operatorname{cond}(\chi) = m'/m$ $\prod_p (1 - \chi(p) p^{-s})^{-1} \cdot \prod_{p|m} (1 - \chi'(p) p^{-s})$

则 $\chi \mapsto \chi'$

$= L(s, \chi') \underbrace{\prod_{p|m} (1 - \chi'(p) p^{-s})}_{\text{有理化}}$

故只须考虑本原 D-特征.

Thm. χ 为本原 D-特征 令 $\delta(\chi) = \delta = \begin{cases} 0, & \chi(-1)=1 \\ 1, & \chi(-1)=-1 \end{cases}$

$$\xi(s, \chi) = \left(\frac{N}{\pi}\right)^{\frac{s}{2}} \Gamma\left(\frac{s+\delta}{2}\right) L(s, \chi)$$

则 $L(s, \chi)$ 可解析延拓到 $\mathbb{C}$ 上. 且满足 $\xi(s, \chi) = \frac{G(\chi)}{i\delta\sqrt{N}} \xi(1-s, \bar{\chi})$

Lem. χ 为本原 D-特征. 则 $\forall t \in \mathbb{R}, L(1+it, \chi) \neq 0$

与 ξ 类似. 略

Cor. $\chi \cdots, N \geq 2$. 则 $L(s, \chi)$ 为 $\mathbb{C}$ 上解析函数. 且

$s = -\delta(\chi) - 2n$ 为单零点 (平凡零点). 其他零点均在 $0 < \operatorname{Re}(s) < 1/2$ 内

Thm. $a_n \in \mathbb{C}$ $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ has $\sigma_0 < +\infty$

令 $f(t) = \sum_{n=1}^{\infty} a_n e^{-nt}$ 则 $f(t)$ 在 $t \rightarrow 0$ 时收敛. 且

(a) 若 $t \rightarrow 0$ 时 $f(t) \sim b_0 + b_1 t + b_2 t^2 + \cdots$ 则 F 可延拓为 $\mathbb{C}$ 上全纯. 且

$$F(-n) = (-1)^n n! b_n$$

(b) 若 $t \rightarrow 0$ 时 $f(t) \sim \frac{b_{-1}}{t} + b_0 + \cdots$ 则 F 可延拓到 $\mathbb{C}$ 上

$$F(s) = \frac{b_{-1}}{s-1} \text{ 全纯. 且 } F(-n) = (-1)^n n! b_n$$

Pf. $A(N) = \sum_{n=1}^N a_n = O(N^{\sigma_0 + \varepsilon}) \Rightarrow a_n = O(n^{\sigma_0 + \varepsilon}) \Rightarrow f(t) \rightarrow 0$ 收敛.

对 $\operatorname{Re}(s) > \sigma_0 + 1$, 有

$$\begin{aligned} \Gamma(s) F(s) &= \int_0^{\infty} t^{s-1} e^{-t} \sum_{n=1}^{\infty} \frac{a_n}{n^s} dt = \int_0^{\infty} t^{s-1} \sum_{n=1}^{\infty} a_n e^{-nt} dt \\ &= \int_0^1 + \int_1^{\infty} t^{s-1} f(t) dt \\ &\quad \quad \quad \downarrow \text{全纯} \end{aligned}$$

$$f(t) = \sum_{n \in \mathbb{N}} b_n t^n + o(t^N)$$

$$\int_0^1 f(t) t^{s-1} dt = \sum_{n \in \mathbb{N}} \frac{b_n}{s+n} + \int_0^1 \underbrace{\left(\sum_{n \in \mathbb{N}} b_n t^n + f(t) \right)}_{\text{valid when } \operatorname{Re}(s) > -N} t^{s-1} dt$$

$$\text{故 } \Gamma(s) F(s) = \sum_{n \in \mathbb{N}} \frac{b_n}{s+n} + G(s)$$

$\hookrightarrow \operatorname{Re}(s) > -N$ 中成立

又 N 任意大 $\checkmark$

(a)(b) 中计算显然.

Def Bernoulli 数 $\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n$

$$\hookrightarrow B_n(x) = \sum_{k=0}^n \binom{n}{k} B_{n-k} x^k$$

对 χ 为模 N 的特征. 定义

$$\text{广义 Bernoulli 数 } B_n, \chi = N^{n-1} \sum_{m=1}^N \chi(m) B_n\left(\frac{m}{N}\right)$$

Thm (a) $(1+B)^n = \sum_{k=0}^n \binom{n}{k} B_k$ (对 $n \geq 2$ 时 $(1+B)^n = B_n$)

$$\Rightarrow -n B_{n-1} = B_0 + \binom{n}{1} B_1 + \dots + \binom{n}{n-2} B_{n-2}$$

(b) $\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} t^n$

$$\frac{t}{e^N t - 1} \sum_{m=1}^N \chi(m) e^{mt} = \sum_{n=0}^{\infty} \frac{B_n, \chi}{n!} t^n$$

(c) $B_1 = -\frac{1}{2}$. 对 $n \geq 3$ 时 $B_n = 0$

若 $\chi \neq \chi_0$. 对 $\delta(\chi) + n \equiv 1 \pmod{2}$ 时 $B_n, \chi = 0$

Pf. (a) $t = \left(\sum_{n=0}^{\infty} \frac{t^n}{n!} \right) \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} t^n \right) = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n$

$$= \sum_{n=0}^{\infty} t^n \sum_{k+l=n} \frac{B_k}{k! l!} = \dots$$

$$= \sum_{n=0}^{\infty} \frac{t^n (1+B)^n}{n!} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n$$

比较 t^n 系数.

$$(b) \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} t^n = \sum_{n=0}^{\infty} \frac{t^n}{n!} \sum_{k=0}^n C_n^k B_k x^{n-k}$$

$$= \sum_{n=0}^{\infty} \sum_{k+l=n} \frac{B_k t^k}{k!} \frac{x^l t^l}{l!} = \frac{t e^{xt}}{e^t - 1}$$

$$\sum_{n=0}^{\infty} \frac{B_n(x)}{n!} t^n = \sum_{n=0}^{\infty} \frac{t^n}{n!} N^{n-1} \sum_{m=1}^N \chi(m) B_n\left(\frac{m}{N}\right)$$

$$= \frac{1}{N} \sum_{m=1}^N \chi(m) \sum_{n=0}^{\infty} \frac{B_n\left(\frac{m}{N}\right)}{n!} (tN)^n = \frac{t}{e^{tN} - 1} \sum_{m=1}^N \chi(m) e^{mt}$$

$$(c) 2 \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} t^n = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} t^n + \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} (-t)^n$$

$$= \frac{t}{e^{tN} - 1} \sum_{m=1}^N \chi(m) (e^{nt} - e^{-nt})$$

$\delta=1$ 时为 0 $\Rightarrow$ $2\chi(n)$ 时 $B_n \chi = 0$ $\delta=0$ 时类似

Thm. (a) $\zeta(s) - \frac{1}{s-1}$ 可延拓为 $\mathbb{C}$ 上解析函数. 且 $\zeta(0) = -\frac{1}{2}$ $\zeta(-n) = -\frac{B_{n+1}}{n+1}$ ($n \geq 1$)

(b) χ 为模 N 的 Dirichlet 特征. 则 $L(s, \chi)$ 可延拓为 $\mathbb{C}$ 上亚纯.

$\forall \chi \neq \chi_0$. $L(s, \chi)$ 全纯

$\forall \chi = \chi_0$. $L(s, \chi)$ 在 $s=1$ 为唯一极点. $\text{res}_{s=1} L(s, \chi_0) = \frac{\varphi(N)}{N}$

$$L(-n, \chi) = -\frac{B_{n+1} \chi}{n+1}$$

pf. (a) $a_n = 1$ $F(s) = \zeta(s)$ $f(t) = \sum_{n=1}^{\infty} a_n e^{-nt} = \frac{1}{e^t - 1}$

$$= \frac{1}{t} + \sum_{n=0}^{\infty} \frac{B_{n+1}}{(n+1)!} t^n$$

(b) $a_n = \chi(n)$ $f(t) = \sum_{n=1}^{\infty} \chi(n) e^{-nt}$

$$= \sum_{m=1}^N \chi(m) \sum_{k=0}^{\infty} e^{-(m+Nk)t}$$

$$= \sum_{m=1}^N \chi(m) \frac{e^{-mt}}{1 - e^{-Nt}}$$

$$= \sum_{m=1}^N \chi(m) \left(\sum_{k=0}^{\infty} (-1)^k \frac{m^k}{k!} t^k \right) \left(\sum_{r=0}^{\infty} \frac{(-1)^r B_r}{r!} (Nt)^{r-1} \right)$$

$$\Rightarrow b_n = \sum_{m=1}^N \chi(m) \sum_{k+r=n+1} \frac{(-1)^{n+1} m^k N^{r-1} B_r}{k! r!} = \frac{1}{N} \sum_{m=1}^N \chi(m) = \begin{cases} 0 & \chi \neq \chi_0 \\ \frac{\varphi(N)}{N} & \chi = \chi_0 \end{cases}$$

$$\stackrel{n \geq 0}{=} \frac{(-1)^{n+1}}{(n+1)!} N^n \sum_{m=1}^N \chi(m) \sum_{k=0}^{n+1} C_{n+1}^k \left(\frac{m}{N}\right)^k B_{n+1-k}$$

$$= \frac{(-1)^{n+1}}{(n+1)!} B_{n+1} \chi$$

✓

4.3 $\zeta_K(s)$

$$\zeta_K(s) = \sum_{\alpha} N(\alpha)^{-s} \quad \alpha: K \text{ 的非零整理想}$$

Dedekind zeta 函数

(定义 zeta 函数)

Thm (a) $\zeta_K(s)$ 在 $\text{Re}(s) > 1$ 中收敛. 且在 $\text{Re}(s) > 1$ 的每个子域中一致绝对收敛 (*)

$$(b) \text{Re}(s) > 1 \text{ 时 有 } \zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1} \quad \mathfrak{p}: \mathcal{O}_K \text{ 素理想}$$

Pf (a) $n = [K:\mathbb{Q}]$. 又 $\forall \mathfrak{p}$ 素数在 K 中至多 $g \leq \frac{n}{f} \leq n$ 个素理想因子

$$\text{则 } s > 1 \text{ 时 } \sum_{N(\mathfrak{p}) \leq x} N(\mathfrak{p})^{-s} \leq \sum_{p \leq x} \sum_{\mathfrak{p} | p} N(\mathfrak{p})^{-s} \\ \leq n \sum_{p \leq x} p^{-s} \leq n \sum_{m \leq x} m^{-s}$$

由 (*) $N(\mathfrak{p})^{-s}$ 满足 (*)

$$\text{另外由 } \sum_{N(\mathfrak{p}) \leq x} \sum_{m=1}^{\infty} N(\mathfrak{p})^{-ms} = \sum_{N(\mathfrak{p}) \leq x} N(\mathfrak{p})^{-s} (1 - N(\mathfrak{p})^{-s})^{-1} \\ \leq 2 \sum_{N(\mathfrak{p}) \leq x} N(\mathfrak{p})^{-s} \Rightarrow \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} N(\mathfrak{p})^{-ms} \text{ 满足 (*)}$$

由 $\mathcal{O}_K$ 素理想分解性

$$\sum_{N(\alpha) \leq x} N(\alpha)^{-s} \leq \prod_{N(\mathfrak{p}) \leq x} (1 + N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{-2s} + \dots) \leq \prod_{N(\mathfrak{p}) \leq x} (1 - N(\mathfrak{p})^{-s})^{-1} \\ \Rightarrow \text{满足 (*)}$$

$$\text{对 } C \text{ 为理想类 } \zeta_K(C, s) = \sum_{\alpha \in C} N(\alpha)^{-s} = \sum_{n=1}^{\infty} a_n(C) n^{-s} \\ \zeta_K(s) = \sum_{C \in \text{Cl}(K)} \zeta_K(C, s) \quad C \text{ 中元素为 } n \text{ 个理想数}$$

Thm. C 理想类 $n = [K:\mathbb{Q}]$ 令 $f(C, x) = \sum_{n \leq x} a_n(C) = \sum_{N(\alpha) \leq x} 1$

$$\text{则 } x \rightarrow \infty \text{ 时 } f(C, x) = \rho_K x + O(x^{1-\frac{1}{n}})$$

$$\rho_K = \frac{2^{r_1} (2\pi)^{r_2} R_K}{w_K \sqrt{|d_K|}} \rightarrow \text{regulator}$$

$\downarrow$
 $|W_K|$

Pf. 任取理想 β in C^{-1} . 若 α 为 C 中理想 $\Rightarrow \alpha\beta = (a) \quad a \in \beta$

$$N(a) = N(\alpha)N(\beta) \leq xN(\beta)$$

反之若 $a \in \beta \quad N(a) \leq xN(\beta)$. $\exists \alpha = (a)\beta^{-1} \nmid \mathfrak{o}$ 且 $N(\alpha) \leq x$

$$\Rightarrow f(C, x) = |\{(\alpha) \mid \alpha \in \beta, N(\alpha) \leq xN(\beta)\}|$$

$$= \# \{ \alpha \bmod \mathfrak{U}_1 \mid a \in \beta, N(\alpha) \leq xN(\beta) \}$$

取 β 的基 $\alpha_1, \dots, \alpha_n$

$$\varphi: \beta \rightarrow \mathbb{R}^n$$

$\varphi(\beta)$ 为格

$$\alpha \mapsto (m_i)$$

$$\sum m_i d_i$$

$$f(C, x) = \# \{ (x_1, \dots, x_n) \in \mathbb{Z}^n \mid \alpha = \sum x_i d_i \bmod \mathfrak{U}_1, 0 < N(\alpha) \leq xN(\beta) \}$$

取 V_K 的基 $\varepsilon_1, \dots, \varepsilon_r$

$$K^* \xrightarrow{\sigma} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\iota} \mathbb{R}^{r_1+r_2}$$

$$\alpha \mapsto (\sigma(\alpha), \dots, \sigma_{r_1+r_2}(\alpha))$$

$$(y_1, \dots, y_{r_1+r_2}) \mapsto (n_1 \log |y_1|, \dots, n_{r_1+r_2} \log |y_{r_1+r_2}|)$$

$$n_i = \begin{cases} 1, & 1 \leq i \leq r_1 \\ 2, & r_1 < i \leq r_1+r_2 \end{cases}$$

回忆 $\text{Ker}(\iota \circ \sigma) = W_K$

$\iota \circ \sigma(V_K)$ 为 $\mathbb{R}^{r_1+r_2}$ 的超平面 $H = \{x_1 + \dots + x_{r_1+r_2} = 0\}$ 的格

$$\exists t = (n_1, \dots, n_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \quad \text{s.t. } t \notin H \Rightarrow$$

$$\mathbb{R}^{r_1+r_2} = \mathbb{R}t \oplus \mathbb{R}(\iota \circ \sigma(\varepsilon_1)) \oplus \dots \oplus \mathbb{R}(\iota \circ \sigma(\varepsilon_r))$$

$\forall \alpha \in K^*$

$$\iota \circ \sigma(\alpha) = c t + \sum c_i \iota \circ \sigma(\varepsilon_i)$$

$$u \in \mathfrak{U}_K$$

$$\Rightarrow \iota \circ \sigma(u\alpha) = c t + \sum (c_i + a_i) \iota \circ \sigma(\varepsilon_i)$$

$$\begin{aligned} & \parallel: a_1, \dots, a_r \\ & \text{w.r.t. } \varepsilon_1, \dots, \varepsilon_r \\ & \sim \\ & \mathfrak{U}_K \end{aligned}$$

$\mathbb{R} \setminus \{0\} = \{\sum x_i \alpha_i \in \mathcal{B} - \{0\} \mid x_i \in \mathbb{Z}\}$. 在 $\mathcal{U}_K$ 中可取恰 w_K 个 α 且 w_K
 s.t. $0 \leq c_i + a_i < 1 \ (1 \leq i \leq r)$

故 $w_K f(C, x) = \# \{ (x_1, \dots, x_n) \in \mathbb{Z}^n \mid \alpha = \sum x_i \alpha_i, \ 0 < N(\alpha) \leq x N(\beta) \}$
 $\left. \begin{aligned} & (0 \leq c_i) = c + \sum_{i=1}^r c_i (0 \leq c_i) \end{aligned} \right\}$
 $0 \leq c_i \leq 1$

对 $y = (y_1, \dots, y_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. $\lambda N(y) = |y_1 \cdots y_{r_1} y_{r_1+1}^2 \cdots y_{r_1+r_2}^2|$

$\Rightarrow N(\sigma(\alpha)) = N(\sum x_i \sigma(\alpha_i))$

$\Gamma_0 \triangleq \{ (x_1, \dots, x_n) \in \mathbb{R}^n \mid 0 < N(\sum x_i \sigma(\alpha_i)) \leq 1 \mid (\sum x_i \sigma(\alpha_i)) = c + \sum_{i=1}^r c_i (0 \leq c_i \leq 1) \}$

$\Rightarrow w_K f(C, x)$ 为 $(x N(\beta))^{\frac{1}{n}}$ Γ_0 中整点个数

$\downarrow x \rightarrow \infty$ (误差阶 $x^{1-\frac{1}{n}}$)

$\text{Vol}((x N(\beta))^{\frac{1}{n}} \Gamma_0) = x N(\beta) V(\Gamma_0)$

$\lambda \sum x_i \sigma(\alpha_i) = (y_1 \cdots y_{r_1} y_{r_1+1} + i y_{r_1+r_2+1}, \dots, y_{r_1+r_2} + i y_n)$

$\mathbb{R} \setminus \Gamma_0 = \left\{ (y_1, \dots, y_n) \in \mathbb{R}^n \mid \begin{aligned} & 0 < |y_1 \cdots y_{r_1} (y_{r_1+1}^2 + y_{r_1+r_2+1}^2) \cdots (y_{r_1+r_2}^2 + y_n^2)| \leq 1 \\ & (\log |y_1|, \dots, \log |y_{r_1}|, \log |y_{r_1+1}^2 + y_{r_1+r_2+1}^2|, \dots, \log |y_{r_1+r_2}^2 + y_n^2|) \\ & = c + \sum_{i=1}^r c_i (0 \leq c_i \leq 1) \end{aligned} \right\}$

$V(\Gamma_0) = 2^{r_2} \int_{\mathbb{R}} |\sigma| dy_1 \cdots dy_n \quad \Gamma = \Gamma_0 \cap \{ y_i \neq 0, 1 \leq i \leq r_1 \} \quad 0 \leq c_i \leq 1$

$\frac{\partial y_k}{\partial x_j} = \begin{cases} \sigma_k(\alpha_j), & 1 \leq k \leq r_1 \\ \text{Re}(\sigma_k(\alpha_j)), & r_1+1 \leq k \leq r_1+r_2 \\ \text{Im}(\sigma_k(\alpha_j)), & r_1+r_2+1 \leq k \leq n \end{cases} \Rightarrow |\sigma| = 2^{-r_2} |\det(\sigma_i(\alpha_j))|$
 $= 2^{-r_2} d(\alpha_1 \cdots \alpha_n)^{\frac{1}{2}}$
 $= 2^{-r_2} N(\beta) d(K)^{\frac{1}{2}}$

$\Rightarrow V(\Gamma_0) = \frac{2^{r_1+r_2}}{N(\beta) |d(K)|^{\frac{1}{2}}} V(\Gamma)$

$$\text{对 } \begin{cases} p_i = y_i \\ p_{r_1+j} e^{i\theta_j} = y_{r_1+j} + i y_{r_1+r_2+j} \end{cases} \Rightarrow \Gamma = \{(p, \theta) \mid \begin{aligned} &0 \leq p = p_1 \cdots p_{r_1+r_2} \leq 1 \\ &0 \leq \theta_j < 2\pi \quad (1 \leq j \leq r_2) \\ &\log p_i = \frac{\log p}{n} + \sum c_j \log |\xi_j^{(i)}| \\ &(1) \text{ 到 } (n) \quad c = \frac{\log p}{n} \quad 0 \leq c_j \leq 1 \end{aligned}\}$$

$$J\left(\frac{y_1 \cdots y_n}{p, \theta}\right) = p_{r_1+1} \cdots p_{r_1+r_2}$$

$$\Rightarrow V(\Gamma) = \int_{p, \theta} p_{r_1+1} \cdots p_{r_1+r_2} dp d\theta = (2\pi)^{r_2} \int_p p_{r_1+1} \cdots p_{r_1+r_2} dp$$

$$\bar{A}(p_1, \dots, p_{r_1+r_2}) \rightarrow (p, c_1, \dots, c_{r_2}) \quad \frac{\partial p_i}{\partial p} = \frac{p_i \partial \log p}{\partial p} = \frac{p_i}{np}$$

$$\frac{\partial p_i}{\partial c_j} = p_i \log |\xi_j^{(i)}|$$

$$\hookrightarrow J = \frac{p_1 \cdots p_{r_1+r_2}}{np 2^{r_2}} R_K \cdot n$$

$$\text{所以 } V(\Gamma) = (2\pi)^{r_2} \int_{0 \leq p, c_1, \dots, c_{r_2} \leq 1} p_1 \cdots p_{r_1} p_{r_1+1}^2 \cdots p_{r_1+r_2}^2 \frac{R_K \cdot n}{np 2^{r_2}} dp dc$$

$$= \pi^{r_2} R_K \quad \checkmark$$

Thm $\zeta_K(C, s)$ 与 $\zeta_K(s)$ 均可解析延拓到 $\operatorname{Re}(s) > 1 - \frac{1}{n}$ 仅在 $s=1$ 处单极点.

$$\operatorname{res}_{s=1} \zeta_K(C, s) = P_K \quad \operatorname{res}_{s=1} \zeta_K(s) = h_K P_K$$

pf. $\zeta_K(C, s) = P_K \zeta(s) + \sum_{n=1}^{\infty} (a_n(C) - P_K) n^{-s}$

$$N \rightarrow \infty \text{ 时 } \sum_{n=1}^N (a_n(C) - P_K) \neq f(C, N) - P_K N = O(N^{1-\frac{1}{n}})$$

$$\Rightarrow \text{在 } \operatorname{Re}(s) > 1 - \frac{1}{n} \text{ 正则}$$

$$\text{又 } \zeta(s) \text{ 在 } s=1 \text{ 单极点} \Rightarrow \operatorname{res}_{s=1} \zeta_K(C, s) = P_K \operatorname{res}_{s=1} \zeta(s) = P_K$$

$$\operatorname{res}_{s=1} \zeta_K(s) = h_K P_K \quad \checkmark$$

希望延拓到 $\mathbb{C}$ 上. 仍然考虑函数方程

$$\text{Thm. } \Phi(s) = \left(\frac{|d(K)|}{4^{r_2} \pi^n} \right)^{\frac{s}{2}} \Gamma\left(\frac{s}{2}\right)^r \Gamma(s)^{r_2} \zeta_K(s)$$

$$\text{则 } \Phi(s) = W \Phi(1-s) \quad |W|=1. \quad W \text{ 只取决于 } K$$

(记号)

Lemma $\zeta_K(1+it) \neq 0 \quad (t \in \mathbb{R})$

Cor (a) $\zeta_K(s)$ 只有 $s=1$ 为奇点. 留数为 $h_K \rho_K$

(b) $\zeta_K(s)$ 在 $s=0$ 为 r 阶零点. $s=-2, -4, \dots$ $r+1$ 阶零点 (平凡零点)
 $s=-1, -3, \dots$ r_2 阶零点

其他零点均在 $0 < \text{Re}(s) < 1$ 中 且关于 $\text{Re}(s) = \frac{1}{2}$ 对称

Riemann 猜想的推广. 是否 $\zeta_K(s)$ 的非平凡零点在 $\text{Re}(s) = \frac{1}{2}$ 上?

Hasse 对 Abel 域建立了如下函数方程

$$(a) \quad K \text{ 为 } n \text{ 次 Abelian} \quad \text{则 } R_K h_K = \prod_{\chi \in K} \left| \sum_{1 \leq k < \frac{f_K}{2}} \chi(k) \log \sin \frac{k\pi}{f_K} \right|$$

$$(b) \quad K \text{ 为 } 2r \text{ 次 Abelian} \quad \text{则 } R_K h_K = \prod_{\substack{\chi \in K \\ \chi(-1)=1}} \left| \sum_{1 \leq k < \frac{f_K}{2}} \chi(k) \log \sin \frac{k\pi}{f_K} \right|$$

K^+ : K 的极大实子域

f_K : K 的导数

K : K 的特征群

(即 $\text{Gal}(K/\mathbb{Q})$ 的特征群)

$$\frac{R_K h_K}{R_{K^+} h_{K^+}} = \frac{w_K}{2} \prod_{\substack{\chi \in K \\ \chi(-1)=-1}} \frac{1}{|\chi(2)-2|} \left| \sum_{1 \leq k < \frac{f_K}{2}} \chi(k) \right|$$

由此可计算二次域. 分圆域的类数