代数数论讲义

2021 春

作者：李加宁

组织：中国科学技术大学, 安徽省合肥市

目录

第一章 整数环以及理想

1.1 Kronecker-Weber 定理

本节利用我们所学的内容给出如下著名定理的初等证明. 我将证明分割成众多习题. 随着课程的深入, 这个定理有更简单的证明, 特别的它是我们本学期将建立的类域论的直接推论. 但历史上, 这个定理是类域论发展初期的重要结果, 给后面的发展带来很多启发. $K/\mathbb{Q}$ 是 abel 扩张指 $K/\mathbb{Q}$ 是 Galois 扩张且 Galois 群是 abel 群.

定理 1.1. Kronecker-Weber 定理

$\mathbb{Q}$ 的有限 abel 扩张均是分圆域的子域.

♡

练习 1.1 设 L/K 是数域的 Galois 扩张. $\mathfrak{p}$ 是 K 的素理想, $\mathfrak{P}$ 是 L 的 $\mathfrak{p}$ 之上的素理想. $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$. 记 $I_{\mathfrak{P}}$ 是 $\mathfrak{P}$ 的惯性群, $E = L^{I_{\mathfrak{P}}}$ 是惯性域. 对每个 $i \in \mathbb{Z}_{\geq 0}$ 定义 $I_{\mathfrak{P}}$ 的子群

$$V_i = \{\sigma \in I_{\mathfrak{P}} : \sigma(x) \equiv x \bmod \mathfrak{P}^{i+1}, \forall x \in \mathcal{O}_L\}.$$

特别地 $V_0 = I_{\mathfrak{P}}$.

(1) 证明 $L = E(\pi)$, 从而对每个 i 有

$$V_i = \{\sigma \in I_{\mathfrak{P}} : \sigma(\pi) \equiv \pi \bmod \mathfrak{P}^{i+1}\}.$$

(2) 证明 $\cap_i V_i = \{1\}$.

(3) 证明 $\sigma \mapsto \frac{\sigma(\pi)}{\pi} \bmod \mathfrak{P}$ 是 V_0 到 $(\mathcal{O}_L/\mathfrak{P})^\times$ 的群同态, 其核为 V_1, 从而诱导了单射

$$f : V_0/V_1 \hookrightarrow (\mathcal{O}_L/\mathfrak{P})^\times.$$

证明映射 f 不依赖于 π 的选取. 如果分解群 $D_{\mathfrak{P}}$ 是 abel 群, 证明 f 的像落在 $(\mathcal{O}_K/\mathfrak{p})^\times$ 里.

(4) 设 $i \geq 1$. 证明对 $\sigma \mapsto \frac{\sigma(\pi)-\pi}{\pi^{i+1}} \bmod \mathfrak{P}$ 是 V_i 到 $\mathcal{O}_L/\mathfrak{P}$ 的群同态, 其核为 V_{i+1}, 从而诱导了单射

$$V_i/V_{i+1} \hookrightarrow \mathcal{O}_L/\mathfrak{P}.$$

(5) 证明 V_1 是 V_0 的正规 Sylow p-子群.

接下来的练习中 $K/\mathbb{Q}$ 是有限 abel 扩张, p 是任意素数.

练习 1.2 说明定理1.1可约化到如下结论: (提示: 利用 Galois 理论与有限 abel 群结构定理,)

若 $[K : \mathbb{Q}] = p^k$, 则 K 是分圆域的子域.

练习 1.3

设 $[K : \mathbb{Q}]$ 等于 p 的方幂. **本题目**为证明下面的 (3) 和 (4).

(1) 设有素数 $q \neq p$ 也在 K 中分歧. 证明 q 在 K 中的分歧指数 $e_q(K/\mathbb{Q})$ 整除 $q - 1$.

(练习1.1(3).)

(2) 设 $F\subset\mathbb{Q}(\zeta_q)$ 使得 $[F:\mathbb{Q}]=e_q$. 记 $L=FK$. 对任意数域 $T\subset L$, 记 $I(T/\mathbb{Q})$ 是 q 在 $T/\mathbb{Q}$ 处的惯性群. 证明限制映射给出如下单同态

$$I(L/\mathbb{Q})\hookrightarrow I(F/\mathbb{Q})\times I(K/\mathbb{Q}).$$

证明 $I(L/\mathbb{Q})\cong I(F/\mathbb{Q})\cong I(K/\mathbb{Q})$ (利用练习1.1(3)) 以及 $KL^{I(L/\mathbb{Q})}=L$.

(3) 将定理1.1归化到如下情形:

若 $K/\mathbb{Q}$ 在 p 以外的素数非分歧, 则 K 是分圆域的子域.

(4) 利用 Minkowski 的判别式定理: " 对任何不等于 $\mathbb{Q}$ 的数域都存在素数在其中分歧", 证明:

若 $K/\mathbb{Q}$ 中分歧的素数只有 p, 则 K 是分圆域的子域.

练习 1.4 (1) 证明 $\mathbb{Q}(\zeta_{2^{k+2}})\cap\mathbb{R}$ 是 $\mathbb{Q}$ 的 2^k 次循环扩张 (循环扩张即 Galois 群为循环群的扩张).

(2) 设 $p\neq 2$. 证明 $\mathbb{Q}(\zeta_{p^{k+1}})$ 有唯一的子域 F 使得 $F/\mathbb{Q}$ 是 p^k 次循环扩张.

练习 1.5 设 $[K:\mathbb{Q}]=2^k$ 且在 K 中分歧的素数只有 2.

(1) 当 $k=1$ 时, 证明 K 是 $\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{-1})$ 或者 $\mathbb{Q}(\sqrt{-2})$, 这三个域是 $\mathbb{Q}(\zeta_8)$ 的全部非平凡子域.

(2) 当 $k>1$ 时, 设 $F\subset\mathbb{Q}(\zeta_{2^{k+2}})$ 是练习1.4(1) 中的子域. 记 $L=KF$, 令 $\sigma\in\mathrm{Gal}(L/\mathbb{Q})$ 使得 $\sigma|_F$ 是 $\mathrm{Gal}(F/\mathbb{Q})$ 的生成元. 设 E 为 L 被 σ 固定不动的域. 则证明 $E\cap F=\mathbb{Q}$, 再证明 $E\cap\mathbb{R}=\mathbb{Q}$, 以及 $E=\mathbb{Q},\mathbb{Q}(\sqrt{-1})$ 或者 $\mathbb{Q}(\sqrt{-2})$. 利用这些证明 $K\subset\mathbb{Q}(\zeta_{2^{k+2}})$.

练习 1.6 利用下面命题1.1的结论证明: 若 $p\neq 2$, $[K:\mathbb{Q}]=p^k$ 且在 K 中分歧的素数只有 p, 则 K 是分圆域的子域.

结合这些练习, Kronecker-Weber 定理的证明就差下面这个关键命题了.

命题 1.1

设 p 是奇素数, $K/\mathbb{Q}$ 是 p 次 abel 扩张且 p 是在 K 中分歧的唯一素数. 则 $K\subset\mathbb{Q}(\zeta_{p^2})$.

(题外话, 举例说明如果去掉 abel 的条件, 这个结论不对.)

引理 1.1

记 $F=\mathbb{Q}(\zeta_p)$, $\pi=1-\zeta_p$, 则 $\pi^{p-1}=p\mathcal{O}_F$. 设 $\alpha\in\mathcal{O}_F$, 我们还有

(1) 对任意 $m\in\mathbb{Z}_{\geq 1}$, 存在 $a_i\in\mathbb{Z}$ 使得 $\alpha=a_0+a_1\pi+\cdots a_{m-1}\pi^{m-1}$.

(2) 若 $\alpha\equiv 1 \bmod \pi$, 则存在 $a\in\mathbb{Z}$ 使得 $\zeta_p^a\alpha\equiv 1 \bmod \pi^2$.

(3) 若 $\alpha=\gamma^p$, $\gamma\in F$ 且 $\alpha\equiv 1 \bmod \pi$, 则 $\alpha\equiv 1 \bmod \pi^p$.

(4) 若 $\alpha\equiv 1 \bmod \pi^p$, 则 $K(\sqrt[p]{\alpha})/K$ 在 π 处非分歧.

证明 引理的证明留作练习.

证明 [命题1.1的证明] 记 $F=\mathbb{Q}(\zeta)$, $(\zeta=\zeta_p)$. 我们来证明 $L:=KF=\mathbb{Q}(\zeta_{p^2})$. 则由于 $L/\mathbb{Q}$ 处是完全分歧, 则 $\pi\mathcal{O}_F$ 在 L/F 中完全分歧, 如同上面引理, $\pi=1-\zeta$.

根据 Kummer 理论, $L=F(\sqrt[p]{\alpha})$ 是 p 次根式扩张. 我们进一步断言可选取适当 α 是 π-单位, 即 $v_{(\pi)}(\alpha)=0$. 限制映射诱导了同构

$$G:=\mathrm{Gal}(L/\mathbb{Q})\cong\mathrm{Gal}(K/\mathbb{Q})\times\mathrm{Gal}(F/\mathbb{Q}).$$

设 $\sigma\in G$ 使得 $\sigma|_F=\mathrm{id}$, $\sigma|_K$ 上是 $\mathrm{Gal}(K/\mathbb{Q})$ 的生成元, 从而 $\sigma^p=1$. 设 $\tau\in G$ 使得 $\sigma|_K=\mathrm{id}$, $\sigma|_F$ 上是 $\mathrm{Gal}(F/\mathbb{Q})$ 的生成元, 从而 $\sigma^{p-1}=1$. 因为 $\sigma(\sqrt[p]{\alpha})^p=\sigma(\alpha)=\alpha$ 且 $\sqrt[p]{\alpha}\notin F$, 所以 $\sigma(\sqrt[p]{\alpha})=\zeta\sqrt[p]{\alpha}$, $\zeta\neq1$ 是 p 次单位根. 那么利用 $\sigma\tau=\tau\sigma$, 记

$$\theta=\frac{\sigma\tau(\sqrt[p]{\alpha})}{\sqrt[p]{\alpha}},$$

则

$$\theta=\frac{\tau(\zeta)\tau(\sqrt[p]{\alpha})}{\sqrt[p]{\alpha}},\quad\sigma(\theta)=\frac{\tau(\zeta^2)\tau(\sqrt[p]{\alpha})}{\sqrt[p]{\alpha}},\quad\theta^p=\frac{\sigma(\alpha)}{\alpha}.$$

由于 $\tau(\zeta)$ 显然不等于 1, 前两个等式说明了 $\theta\notin K$, 最后一个等式说明了 $L=K(\sqrt[p]{\frac{\sigma(\alpha)}{\alpha}})$. 但由于 p 在 L 中完全分歧, 故 $\sigma((\pi))=(\pi)$, 则 $\frac{\sigma(\alpha)}{\alpha}$ 是 π 单位. 这就证明了断言.

根据中国剩余定理存在 $a\in\mathcal{O}_F$ 且 $\pi\nmid a$, 使得 $a^p\alpha\in\mathcal{O}_F$. 由于 $F(\sqrt[p]{a^p\alpha})=F(\sqrt[p]{\alpha})$, 所以我们不妨设 $\alpha\in\mathcal{O}_F$. 利用 $F(\sqrt[p]{\alpha})=F(\sqrt[p]{\alpha^{p-1}})$, 将 α 换成 α^{p-1}, 这样我们可进一步假设 $\alpha\equiv1\bmod\pi$. 根据上面引理, 取 $\alpha=\zeta_p^a\beta$ 且 $\beta\equiv1\bmod\pi^2$. 则存在 $c\in\mathbb{Z}$, $p\nmid c$, $m\geq2$ 使得

$$\beta\equiv1+c\pi^m\bmod\pi^{m+1}.$$

利用上面引理中的 $\sigma(\pi)\equiv g\pi\bmod\pi^2$, 知

$$\sigma(\beta)\equiv1+cg^m\pi^m\bmod\pi^{m+1}.$$

设 $\tau(\zeta)=\zeta^g$. 则 g 是模 p 的原根且

$$\sigma\text{ 作用}\frac{\sigma\tau(\sqrt[p]{\alpha})}{(\sqrt[p]{\alpha})^g}\text{ 不动}.$$

这说明了 $\frac{\tau(\beta)}{\beta^g}=\frac{\tau(\alpha)}{\alpha^g}\in(L^\times)^p$. 根据上面引理, 这推出了

$$\sigma(\beta)\equiv\beta^g\bmod\pi^p.\tag{1.1.1}$$

从而我们有

$$1+gc\pi^m\equiv1+cg^m\pi^m\bmod\pi^{m+1}.$$

现在我们断言 $m\geq p$. 否则 $m+1\leq p$, 则(1.1.1)推出了 $\sigma(\beta)\equiv\beta^g\bmod\pi^{m+1}$. 结合上面几个同余式得出

$$1+cg^m\pi^m\equiv(1+c\pi^m)^g\bmod\pi^{m+1}.$$

这会得出 $g^m\equiv g\bmod\pi$, 利用 g 是模 p 的原根知 $m\geq p$, 矛盾. 这样就证明了

$$\beta\equiv1\bmod\pi^p.$$

由于 $L=K(\sqrt[p]{\beta\zeta^a})$, 所以只要能证明 $\beta\in(K^\times)^p$ 就能说明 $L\subset\mathbb{Q}(\zeta_{p^2})$ 了. 反证法, 如果不是, 则域扩张 L'/K 非平凡, 这里 $L'=K(\sqrt[p]{\beta})$. 显然 $LL'\subset L(\zeta_{p^2})$, 所以 $L'/\mathbb{Q}$ 只在 p 处分歧. 根据上面引理, L'/K 在 (π) 处是非分歧的. 这样的话, $L'/\mathbb{Q}$ 关于 p 的惯性域是非平凡的, 从而它的惯性域在每个素数处都非分歧. 这与 Minkowski 定理矛盾. 所以

$L' = K$.

1.2 类域论介绍

定义 1.1. 无穷素位

设 K 是数域, 设 $\mathrm{Hom}(K, \mathbb{C})$ 是 K 到 $\mathbb{C}$ 的所有嵌入的集合. $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ 以显然的方式作用在 $\mathrm{Hom}(K, \mathbb{C})$ 上, K 的一个无穷素位指这个作用的一个轨道. 若无穷素位由实嵌入代表, 称为实素位; 否则称为复素位.

也就是说, 如果 K 有 r_1 个实嵌入, $2r_2$ 个复嵌入. 则 K 有 r_1 个实素位, r_2 个复素位.

设 L/K 是有限扩张. 设 $\sigma \in \mathrm{Hom}(K, \mathbb{C})$. 称 $\tau \in \mathrm{Hom}(L, \mathbb{C})$ 在 σ 之上是指 $\tau|_K = \sigma$, 此时也称 σ 在 τ 之下.

设 τ 是 L 的一个素位, 若 τ 本身是复素位但 τ 之下的 K 的素位是实, 则称 τ 在 L/K 中分歧, 否则称 τ 在 L/K 中完全分裂.

设 σ 是 K 的一个素位, 若 σ 实, 且存在 σ 之上 L 的素位分歧, 则称 σ 在 L/K 中分歧. 其他情形均称 σ 在 L/K 中非分歧 (也称完全分裂). ♣

$\mathcal{O}_K$ 的非零素理想也被称作 K 的有限素位 (或有限素点).

例 1.1 无穷素位的例子:

- $\mathbb{Q}(\sqrt[3]{2})$ 有一个由 $\sqrt[3]{2} \mapsto \sqrt[3]{2} \in \mathbb{R}$ 决定的实素位, 一个复素位 = 一对共轭的复嵌入 (由 $\sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}$ 或 $\bar{\zeta}_3\sqrt[3]{2}$ 决定.) 所以 $\mathbb{Q}$ 的唯一的无穷素位在 $\mathbb{Q}(\sqrt[3]{2})$ 中分歧.
- 在 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 中, $\mathbb{Q}$ 的无穷素位不分歧.
- 在 $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ 中, $\mathbb{Q}$ 的无穷素位分歧.
- 练习: 在 $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ 中, 哪些 $\mathbb{Q}(\sqrt{2})$ 的无穷素位分歧?
- 练习: 若 L/K 是 Galois 扩张, 则 K 的实素位 σ 之上的 L 的素位要么全是实的, 要么全是复的.

例 1.2 无穷素位的分歧对于素理想分解影响的两个例子:

- $p\mathbb{Z}$ 在 $\mathbb{Q}(\sqrt{2})$ 中分裂当且仅当 $p \equiv \pm 1 \bmod 8$, 即当且仅当 $p\mathbb{Z}$ 中存在一个生成元 $\equiv 1 \bmod 8$.
- $p\mathbb{Z}$ 在 $\mathbb{Q}(\sqrt{-1})$ 中分裂当且仅当 $p \equiv 1 \bmod 4$ 当且仅当 $p\mathbb{Z}$ 中存在一个**正**生成元 $\equiv 1 \bmod 4$.

以上两个例子将纳入一般的类域论现象.

定义 1.2

K 的一个 modulus 是指" 形式乘积" $\mathfrak{m}_o\mathfrak{m}_\infty$, 其中 $\mathfrak{m}_o$ 是 K 的整理想, $\mathfrak{m}_\infty$ 是 K 的一些不同的实素位的" 形式乘积". 给定两个 modulus $\mathfrak{m}_1, \mathfrak{m}_2$, 我们说 $\mathfrak{m}_1$ 整除 $\mathfrak{m}_2$ (记作 $\mathfrak{m}_1 \mid \mathfrak{m}_2$) 是指存在 modulus $\mathfrak{m}_3$ 使得 $\mathfrak{m}_2 = \mathfrak{m}_1\mathfrak{m}_3$.

比如在 $K = \mathbb{Q}(\sqrt{2})$, 记 ∞_1, ∞_2 是 K 的实素位. 则 $\mathfrak{m}_1 = (3+\sqrt{2})\infty_1$, $\mathfrak{m}_2 = (7)\infty_1\infty_2$ 就是一些 modulus 的例子, 其中 $\mathfrak{m}_1 \mid \mathfrak{m}_2$.

对 $\alpha \in K$, 符号 $\alpha \equiv 1 \bmod {}^+\mathfrak{m}$ 指

$$v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_o) \quad \forall \mathfrak{p} \mid \mathfrak{m}_o, \qquad 且 \sigma(\alpha) > 0 \quad \forall \sigma \mid \mathfrak{m}_\infty.$$

这里 $\mathfrak{p}$ 是 K 的素理想, $v_\mathfrak{p}(\mathfrak{m}_o)$ 指 $\mathfrak{m}_o$ 做素理想分解后 $\mathfrak{p}$ 出现的指数, $v_\mathfrak{p}(\alpha) = v_\mathfrak{p}((\alpha))$. ♣

定义 1.3. 射线理想类群

设 $\mathfrak{m}$ 是 K 的一个 modulus. 令 I_K 表示 K 的分式理想群. 记

$$I_K^\mathfrak{m} = \{\mathfrak{a} \in I_K : v_\mathfrak{p}(\mathfrak{a}) = 0 \quad \forall \mathfrak{p} \mid \mathfrak{m}_0\}.$$

换言之, $I_K^\mathfrak{m}$ 是由与 $\mathfrak{m}_o$ 互素的素理想生成的 I_K 的子群. 记

$$K_{\mathfrak{m},1} = \{\alpha \in K : \alpha \equiv 1 \bmod {}^+\mathfrak{m}\}.$$

我们记 $i : K^\times \to I_K, \alpha \mapsto (\alpha)$. 关于 modulus $\mathfrak{m}$ 的射线理想类群 $\mathrm{Cl}(K, \mathfrak{m})$ 为

$$\mathrm{Cl}(K, \mathfrak{m}) := I_K^\mathfrak{m} / i(K_{\mathfrak{m},1}).$$

特别的, $\mathrm{Cl}(K, (1))$ 就是理想类群 $\mathrm{Cl}(K)$; ♣

例 1.3 (1) $K = \mathbb{Q}$. $\mathfrak{m} = N\infty$. 则 $(\mathbb{Z}/N\mathbb{Z})^\times \cong \mathrm{Cl}(K, \mathfrak{m})$. 同构映射由 $a \bmod N \mapsto a\mathbb{Z}$ 诱导. (细节留作练习, 或者见下面一般情形.)

(2) 设 $\mathfrak{m}$ 为所有实素位的乘积. $I_K^\mathfrak{m} = I_K$, $K_{\mathfrak{m},1} = K^+ := \{\alpha \in K : \sigma(\alpha) > 0, 对每个实嵌入\sigma\}$, K^+ 中的元素称作在 K 中全正. (如果 K 没有实素位, 则称 $K = K_{\mathfrak{m},1}$ 中元素都是全正的, 比如 -1 在 $\mathbb{Q}(\sqrt{-1})$ 中是全正的.) 则 $\mathrm{Cl}(K, \mathfrak{m}) = I_K / i(K^+)$.

命题 1.2

$\mathrm{Cl}(K, \mathfrak{m})$ 是有限的. ♠

证明 证明是通过考察 $\mathrm{Cl}(K, \mathfrak{m}) \to \mathrm{Cl}(K)$ 的自然映射得到的. 留作练习. 我们后面讲完局部理论时会对这个事实有更清楚的了解.

定义 1.4. Artin 映射

设 L/K 是 abel 扩张, 设 S 是 K 的素理想的有限集且包含所有分歧的素理想. 若 K 的素理想 $\mathfrak{p} \notin S$, 我们有 $\mathrm{Frob}_\mathfrak{p} = \mathrm{Frob}_{\mathfrak{p},L/K} \in G$. 所谓 Artin 映射就是将 Frobenieus 映射延拓为如下群同态:

$$\psi_{L/K} : I_K^S \to \mathrm{Gal}(L/K), \quad \prod_\mathfrak{p} \mathfrak{p}^{a_\mathfrak{p}} \mapsto \prod_\mathfrak{p} (\mathrm{Frob}_\mathfrak{p})^{a_\mathfrak{p}}.$$

这里 I_K^S 是由 K 中不属于 S 的素理想生成的 I_K 的子群.

在陈述类域论主定理之前, 我们先总结下分圆域的性质.

- 在 $\mathbb{Q}(\zeta)/\mathbb{Q}, \mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}, \zeta=\zeta_N$ 的情形, 有如下交换图:

$$\begin{tikzcd} \mathrm{Cl}(\mathbb{Q}, N\infty) \arrow[r, "\cong"] \arrow[dr, "\cong", "\psi_{\mathbb{Q}(\zeta)/\mathbb{Q}}"'] & (\mathbb{Z}/N\mathbb{Z})^\times \arrow[d, "\cong"] \\ & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \end{tikzcd}$$

$$\begin{tikzcd} \mathrm{Cl}(\mathbb{Q}, N) \arrow[r, "\cong"] \arrow[dr, "\cong", "\psi_{\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}}"'] & (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\} \arrow[d, "\cong"] \\ & \mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}) \end{tikzcd}$$

- 设 $v=p\mathbb{Z}$ 或者 ∞, 则 $v\nmid N\infty$ 时, v 在 $\mathbb{Q}(\zeta_N)$ 中非分歧; $v\nmid N$ 时, v 在 $\mathbb{Q}(\zeta_N+\zeta_N^{-1})$ 中非分歧.
- 特别的, $p\mathbb{Z}$ 在 $\mathbb{Q}(\zeta)$ 中完全分裂当且仅当 $p\mathbb{Z}\in i(\mathbb{Q}_{(N)\infty,1})$, 即 $p\equiv 1 \bmod N$;
- $p\mathbb{Z}$ 在 $\mathbb{Q}(\zeta+\zeta^{-1})$ 中完全分裂当且仅当 $p\mathbb{Z}\in i(\mathbb{Q}_{(N),1})$, 即 $p\equiv \pm 1 \bmod N$;
- 根据 Kroncker-Weber 定理, 若 $F/\mathbb{Q}$ 是有限 abel 扩张, 且 ∞ 在 F 中分歧, 则 $F\subset \mathbb{Q}(\zeta_N)$ 对某个 N;
- 若 $F/\mathbb{Q}$ 是有限 abel 扩张, 且 ∞ 在 F 中非分歧, 即 $F\subset\mathbb{R}$, 则 $F\subset\mathbb{Q}(\zeta_N+\zeta_N^{-1})$ 对某个 N.
- 若 $M\mid N$, 则 $\mathbb{Q}(\zeta_M)\subset\mathbb{Q}(\zeta_N), \mathbb{Q}(\zeta_M+\zeta_M^{-1})\subset\mathbb{Q}(\zeta_N+\zeta_N^{-1})$.

下面用理想语言来陈述类域论的主要结论. 本课程的一大目的是理解好类域论的陈述和应用.

定理 1.2. 类域论

对任何 K 的 modulus $\mathfrak{m}$, 存在唯一的有限 abel 扩张 $K(\mathfrak{m})/K$ 使得
(1) 对任何 $\mathfrak{p}\nmid\mathfrak{m}$, $\mathfrak{p}$ 在 $K(\mathfrak{m})/K$ 中不分歧;
(2) $\psi_{K(\mathfrak{m})/K}$ 诱导了同构 $\mathrm{Cl}(K,\mathfrak{m})\cong\mathrm{Gal}(L/K)$.
而且
(3) 给定两个 modulus $\mathfrak{m}_1,\mathfrak{m}_2$, 若 $\mathfrak{m}_1\mid\mathfrak{m}_2$ 则 $K(\mathfrak{m}_1)\subset K(\mathfrak{m}_2)$.
(4) 设 L 是 K 的有限 abel 扩张, 则存在 $\mathfrak{m}$ 使得 $L\subset K(\mathfrak{m})$. 而且, 存在 $\mathfrak{m}$ 使得 $L\subset K(\mathfrak{m})$ 且若 $L\subset K(\mathfrak{m}')$, 则 $\mathfrak{m}\mid\mathfrak{m}'$; 此时, K 的素位 v(有限或无限) 在 L 中分歧当且仅当 $v\mid\mathfrak{m}$. (这个 $\mathfrak{m}$ 称作 L/K 的导子.)

例 1.4 在 $K=\mathbb{Q}$ 的情形, 说明 $\mathbb{Q}((N)\infty)=\mathbb{Q}(\zeta_N), \mathbb{Q}((N))=\mathbb{Q}(\zeta_N+\zeta_N^{-1})$.

命题 1.3

设 K 是二次域, $d=|d_K|$. 则 $\mathbb{Q}(\zeta_d)$ 是包含 K 的最小分圆域. 这推出了 K 是实二次域时, K 的导子是 (d_K); 当 K 是虚二次域时, K 的导子是 $(d_K)\infty$.

这个证明留作练习.

1.2.1 Hilbert 类域

当 K 的 modulus 为 (1) 时, 则 $\mathrm{Cl}(K,\mathfrak{m})=\mathrm{Cl}(K)$. 根据类域论, 记 $K(1):=K((1))$ 为其对应的射线类域, 由于历史的原因, 这个域也称作 K 的 Hilbert 类域.

推论 1.1

(1) $K(1)$ 是 K 的极大 abel 且在每个素位 (包括无穷素位) 都非分歧的扩张;

(2) Artin 映射诱导了同构 $\mathrm{Cl}(K)\cong \mathrm{Gal}(K(1)/K)$.

证明 (1) 由定理1.2(4), (2) 是定理1.2(2) 特殊情形.

由于类群是有限的, 所以这个结论告诉我们 K 的极大 abel 非分歧扩张是 K 的有限扩张, 定理1.2还推出

$$K\text{ 的素理想}\mathfrak{p}\text{ 是主理想}\Leftrightarrow \mathfrak{p}\text{ 在}K(1)\text{ 中完全分裂.}$$

练习: 若 $K/\mathbb{Q}$ 是 Galois 扩张, 则 $K(1)/\mathbb{Q}$ 也是.

例 1.5

- $K=\mathbb{Q}(\sqrt{-5})$, $\mathrm{Cl}(K)\cong\mathbb{Z}/2\mathbb{Z}$, $K(1)=K(\sqrt{5})=\mathbb{Q}(\sqrt{-5},\sqrt{-1})$;
- $K=\mathbb{Q}(\sqrt{-14})$, $\mathrm{Cl}(K)\cong\mathbb{Z}/4\mathbb{Z}$, 验证 $K(1)=K(\sqrt{2\sqrt{2}-1})$;
- $K=\mathbb{Q}(\sqrt{-23})$, $\mathrm{Cl}(K)\cong\mathbb{Z}/3\mathbb{Z}$, 验证 $K(1)=K(\alpha)$, α 是 T^3-T-1 的一个根.

给定 $d\in\mathbb{Z}$, 历史上, 人们关心什么样的素数 p 可表示为 x^2+dy^2, $x,y\in\mathbb{Z}$. 这个问题可由类域论描述, 我们讲一个容易叙述的情形.

命题 1.4

设整数 $d\equiv 2,3 \bmod 4$ 且无平方因子, $K=\mathbb{Q}(\sqrt{d})$. 设素数 $p\nmid 2d$. 下面等价:

(1) 存在 $x,y\in\mathbb{Z}$ 使得 $\pm p=x^2-dy^2$;

(2) $p\mathbb{Z}$ 在 K 中分裂为两个主理想相乘;

(3) $p\mathbb{Z}$ 在 $K(1)$ 中完全分裂.

证明 (1) 和 (2) 等价是显然的. (2) 和 (3) 等价是由 Hilbert 类域的性质.

如果 $K(1)$ 恰好也是 $\mathbb{Q}$ 的 abel 扩张时, 则上面等价条件中的 (3) 可进一步用 $p\equiv a \bmod N$ 这样的同余条件描述.

例 1.6

- $p=x^2+5y^2$ 当且仅当 p 在 $K(1)=\mathbb{Q}(\sqrt{-5},\sqrt{-1})$ 中分裂, 这里 $K=\mathbb{Q}(\sqrt{-5})$. 此时由于 $K(1)\subset\mathbb{Q}(\zeta_{20})$. 在同构 $\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/\mathbb{Q})\cong(\mathbb{Z}/20\mathbb{Z})^\times$ 下, 有

  $$\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/K(1))\cong\{1 \bmod 20, 9 \bmod 20\}.$$

  所以 p 在 $K(1)$ 中完全分裂当且仅当 $\mathrm{Frob}_{p,\mathbb{Q}(\zeta_{20})/\mathbb{Q}}\in\mathrm{Gal}(\mathbb{Q}(\zeta_{20})/K(1))$ 当且仅当 $p\equiv 1,9 \bmod 20$. (也可以利用 p 在 $K(1)=\mathbb{Q}(\sqrt{5},\sqrt{-1})$ 中完全分裂当且仅当 p 同时在 $\mathbb{Q}(\sqrt{5})$ 和 $\mathbb{Q}(\sqrt{-1})$ 中完全分裂这个事实来得到 $p\equiv 1,9 \bmod 20$.)

- 由于 $K=\mathbb{Q}(\sqrt{-14})$ 时, $K(1)/\mathbb{Q}$ 不是 abel 的, 我们将在后面的课程中证明 p 在 $K(1)$ 中完全分裂将不能由形如 $p\equiv a \bmod N$ 之类的同余条件刻画, 从而 $p=x^2+14y^2$ 也不能由这样的同余条件刻画.

1.3 理想的范

设 L/K 是数域的扩张. 我们推广之前理想的绝对范的定义.

定义 1.5. 理想的 (相对) 范

设 $\mathfrak{P}$ 是 L 的一个素理想. 定义

$$\mathbf{N}_{L/K}(\mathfrak{P})=\mathfrak{p}^f,\quad \mathfrak{p}=\mathfrak{P}\cap K, f=f(\mathfrak{P}/\mathfrak{p}).$$

对 L 的一个分式理想 $\mathfrak{A}$, 若 $\mathfrak{A}$ 的素理想分解为 $\prod\mathfrak{P}^{a_{\mathfrak{P}}}$, 则定义

$$\mathbf{N}_{L/K}(\mathfrak{A})=\prod\mathbf{N}_{L/K}(\mathfrak{P})^{a_{\mathfrak{P}}}.$$

♣

命题 1.5

记 I_L 和 I_K 分别为 L 和 K 的分式理想群. 则我们有如下交换图:

$$\begin{tikzcd} L^\times \arrow[r] \arrow[d, "N_{L/K}"'] & I_L \arrow[d, "\mathbf{N}_{L/K}"] \\ K^\times \arrow[r] & I_K \end{tikzcd}$$

♠

证明 先证明 L/K 是 Galois 扩张的情形. 此时, $\mathbf{N}_{L/K}(\mathfrak{P})\mathcal{O}_L=\mathfrak{p}^f\mathcal{O}_L=\prod_{\sigma\in G}\sigma(\mathfrak{P})$, 进而对一般的理想 $\mathfrak{A}$, 有 $\mathbf{N}_{L/K}(\mathfrak{A})=\prod_{\sigma\in G}\sigma(\mathfrak{A})$. 而对 $x\in L$, 熟知 $N_{L/K}(x)=\prod_{\sigma\in G}\sigma(x)$. 所以交换图成立.

一般情形, 设 M 是 K 的正规扩张且 $M\supset L$. 记 $G=\mathrm{Gal}(M/K)$. 对 $x\in L$, 我们有

$$\mathbf{N}_{M/K}(x\mathcal{O}_M)=(x\mathcal{O}_L)^{[M:L]}$$

以及

$$\mathbf{N}_{M/K}(x\mathcal{O}_M)=N_{M/K}(x)\mathcal{O}_K=N_{L/K}(x)^{[M:L]}\mathcal{O}_K.$$

由此推出 $\mathbf{N}_{L/K}(x\mathcal{O}_L)=N_{L/K}(x)\mathcal{O}_K$.

第二章 赋值

2.1 赋值的定义

设 A 是 Dedekind 整环, K 是分式域. $\mathfrak{p}$ 是 A 的非零素理想. 定义所谓 $\mathfrak{p}$-进赋值 $v_{\mathfrak{p}}(x)$ 为分式理想 (x) 做分解时 $\mathfrak{p}$ 出现的指数, 再定义 $v_{\mathfrak{p}}(0)=\infty$. 容易验证有

$$v_{\mathfrak{p}}(xy)=v_{\mathfrak{p}}(x)+v_{\mathfrak{p}}(y), \qquad v_{\mathfrak{p}}(x+y)\geq \min\{v_{\mathfrak{p}}(x),v_{\mathfrak{p}}(y)\}. \tag{2.1.1}$$

我们着重考虑 $A=\mathbb{Z}, K=\mathbb{Q}$ 的情形. 简记 $v_{(p)}$ 为 v_p.

先回顾域上绝对值的定义.

定义 2.1

对任意域 K, 一个 (乘性) 赋值或绝对值是指满足下面三条的函数 $|\cdot|: K\to\mathbb{R}_{\geq 0}$:

(1) $|x|=0$ 当且仅当 $x=0$;

(2) $|xy|=|x|\cdot|y|$ 对任意 $x,y\in K$;

(3) (三角不等式)$|x+y|\leq|x|+|y|$ 对任意 $x,y\in K$.

称赋值 $|\cdot|$ 是非阿基米德赋值 (简称非阿赋值) 如进一步满足

(3')(强三角不等式) $|x+y|\leq\max\{|x|,|y|\}$, 对任意 $x,y\in K$.

否则称 $|\cdot|$ 是阿基米德赋值. ♣

对每个域, 都存在平凡绝对值: 它将所有非零元的绝对值定义为 1. 若 $\zeta\in K$ 是个单位根, 即存在 $n\in\mathbb{Z}$ 使得 $\zeta^n=1$, 则 ζ 在任何绝对值下都等于 1.

引理 2.1

$|\cdot|$ 是非阿赋值当且仅当对每个 $m\in\mathbb{Z}$, $|m|\leq 1$. 特别的, 若 K 特征大于 0, 则 K 上的所有赋值都是非阿. ♡

证明 若 $|\cdot|$ 非阿, 则根据强三角不等式知 $|m|\leq 1$ 对每个 $m\in\mathbb{Z}$. 反过来, 对 $x,y\in K$, $N\in\mathbb{Z}_{\geq 1}$, 我们有

$$|(x+y)^N|\leq\sum_{i=0}^{N}|x^iy^{N-i}|\leq(N+1)\max\{|x|^N,|y|^N\}.$$

由此知, 对每个 N,

$$|x+y|\leq\sqrt[N]{N+1}\max\{|x|,|y|\}.$$

令 $N\to\infty$, 熟知 $\sqrt[N]{N+1}\to 1$, 由此强三角不等式成立. 最后如果 K 的特征是 $p>0$, 则 $|1|=|2|=\cdots|p-1|=1$, 因为它们都是 $p-1$ 次单位根, 所以 $|\cdot|$ 是非阿的.

定义 2.2

设 $(K,|\cdot|)$ 是赋值域, 则 K 称为自然度量空间, 特别的 K 是自然的拓扑空间. 称 K 上两个绝对值等价是指它们诱导了相同的度量拓扑. ♣

引理 2.2

设 $|\cdot|, |\cdot|'$ 是域 K 上两个绝对值, 则以下几条等价:

(1) $|\cdot|$ 与 $|\cdot|'$ 等价;

(2) $|x| \le 1$ 当且仅当 $|x|' \le 1$.

(3) $|x| < 1$ 当且仅当 $|x|' < 1$.

(4) 存在 $c > 0$ 使得 $|x|' = |x|^c$ 对每个 $x \in F$ 成立;

证明 留作练习.

2.2 p 进数

$\mathbb{Q}$ 上的 p-进 (加法) 赋值 v_p 可给出 p-进 (乘法) 赋值 (或叫作 p-进绝对值)$|\cdot|_p$:

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\ge 0}, \quad x \mapsto p^{-v_p(x)}.$$

由(2.1.1) 知 $|\cdot|_p$ 是 $\mathbb{Q}$ 上的非阿赋值. 将其完备化 (柯西列的等价类) 记作 $\mathbb{Q}_p$, 称 $\mathbb{Q}_p$ 为 **p-进数域**. 由于 $|\mathbb{Q}|_p := \{|x|_p : x \in \mathbb{Q}\} = \{0, p^{\pm 1}, p^{\pm 2}, \cdots\}$ 是 $\mathbb{R}$ 的闭集, 所以 $|\mathbb{Q}_p|_p = |\mathbb{Q}|_p$, 特别的 $|\mathbb{Q}^\times|_p = |\mathbb{Q}_p^\times|_p$ 在 $\mathbb{R}$ 中还是离散的. 类似的, v_p 也延拓为 $\mathbb{Q}_p$ 的函数, 且仍旧满足(2.1.1).

定义

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \le 1\} = \{x \in \mathbb{Q}_p : v_p(x) \ge 0\}.$$

利用强三角不等式知 $\mathbb{Z}_p$ 是 $\mathbb{Q}_p$ 的子环, 我们称 $\mathbb{Z}_p$ 为 **p-进整数环**.

定义 2.3

同时是 Dedekind 整环和局部环的环被称作离散赋值环.

由前面 Dedekind 整环一节知, 只有有限个素理想的 Dedekind 整环是主理想整环. 所以离散赋值环也可定义为同时是主理想整环和局部环.

命题 2.1

(1) $\mathbb{Z}_p$ 是离散赋值环, 它的极大理想是 $p\mathbb{Z}_p$, 它的单位群是 $\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p : |x|_p = 1\}$. $\mathbb{Z}_p$ 的所有非零理想都形如 $p^n\mathbb{Z}_p$, $n \in \mathbb{Z}_{\ge 0}$. 而且 $p^n\mathbb{Z}_p$ 是 0 的一组邻域基. 我们有 $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$, 特别的 $\mathbb{Q}_p$ 是 $\mathbb{Z}_p$ 的分式域.

(2) $\mathbb{Z}$ 在 $\mathbb{Z}_p$ 中稠密;

(3) 自然包含 $\mathbb{Z} \subset \mathbb{Z}_p$ 诱导了同构

$$\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p/p^n\mathbb{Z}_p.$$

证明 (1) 关于 $\mathbb{Z}_p$ 是局部环, 以及它的单位群的断言是显然的. 它的极大理想是

$$\{x \in \mathbb{Z}_p : |x|_p < 1\} = \{x \in \mathbb{Z}_p : |x|_p \le p^{-1}\} = p\mathbb{Z}_p.$$

其中第一个等式是利用了延拓后赋值仍旧是离散的, 第二个等式是显然的. 设 $\mathfrak{a} \subset \mathbb{Z}_p$ 是非零理想, 则取 $a \in \mathfrak{a}$ 使得 $|a|_p = p^{-n}$ 最大 (即 $v_p(a)$ 最小). 则 $\mathfrak{a} = \{x \in \mathbb{Z}_p : |x|_p \le$

$p^{-n}\} = p^n\mathbb{Z}_p$. (1) 中最后两句话的断言是显然的.

(2) 任取 $x \in \mathbb{Z}_p$, 则存在某个 n 使得 $x = p^n u, u \in \mathbb{Z}_p^\times$. 则根据完备化的定义存在一列有理数 $\frac{a_n}{b_n}$ 使得其在 $|\cdot|_p$ 下的极限是 u. 因为 $u \in \mathbb{Z}_p^\times$, 所以对充分大的 n, 我们有 $|\frac{a_n}{b_n}|_p = 1$, 即 $p \nmid a_n b_n$, 那么存在 $c_n \in \mathbb{Z}$ 使得 $b_n c_n \equiv 1 \bmod p^n$. 则

$$\lim_{n\to\infty} a_n c_n - \frac{a_n}{b_n} = \lim_{n\to\infty} a_n \left(\frac{b_n c_n - 1}{b_n}\right) = 0.$$

这就证明了

$$u = \lim_{n\to\infty} a_n c_n \quad \text{从而} \quad x = \lim_{n\to\infty} p^n a_n c_n.$$

所以 $\mathbb{Z}$ 在 $\mathbb{Z}_p$ 中稠密.

(3) 显然 $\mathbb{Z} \cap p^n\mathbb{Z}_p = p^n\mathbb{Z}$, 即 (3) 中映射是单射. 任取 $x \in \mathbb{Z}_p$, 由 $\mathbb{Z}$ 的稠密性知存在 $a \in \mathbb{Z}$ 使得 $|x-a|_p \leq p^{-n}$, 即 $x \equiv a \bmod p^n\mathbb{Z}_p$. 这就证明了满射.

2.2.1 p 进指数和对数函数

这部分内容完全包含于《数论 I, 2.5 节》, 请直接阅读这部分, 注意教材中 ord_p 是课堂上的 v_p. 我把教材中略去的一个证明补在这里.

证明 [数论 I, 引理 2.14(1) 的证明]

1 至 n 内被 p^k 整除的数恰是 $p^k, 2p^k, \cdots, \left[\frac{n}{p^k}\right] p^k$. 所以

$$\#\{1 \leq a \leq n : a \in \mathbb{Z}, v_p(a) = k\} = \left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right].$$

于是,

$$v_p(n!) = \sum_{k=1}^{\infty} k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right) = \sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right].$$

2.3 完备域上的有限维线性空间

本节我们证明一个分析学中的结论.

定义 2.4

设 $(K, |\cdot|)$ 是赋值域, 且在此赋值下完备. 设 V 是 K 上的有限维线性空间. 如果函数 $||\cdot|| : V \to \mathbb{R}_{\geq 0}$ 满足下面三条, 称它为 V 上的一个范数:

(1) $||\alpha|| = 0$ 当且仅当 $\alpha = 0$;

(2) 对 $x \in K, \alpha \in V$, $||x\alpha|| = |x| \cdot ||\alpha||$;

(3) 对 $\alpha, \beta \in V$, $||\alpha + \beta|| \leq ||\alpha|| + ||\beta||$.

V 上两个范数 $||\cdot||_1, ||\cdot||_2$ 等价是指存在常数 $C_1, C_2 > 0$ 使得

$$C_1||\alpha||_1 \leq ||\alpha||_2 \leq C_2||\alpha||_1, \quad \forall \alpha \in V.$$

♣

例 2.1 固定 V 的一组基 $e_1, \cdots, e_n$. 对任意 $\alpha = x_1e_1 + \cdots x_ne_n \in V, x_i \in K$, 如下定义的 $||\cdot||_{\max}$ 是一个范数

$$||\alpha||_{\max} = \max\{|x_1|, \cdots, |x_n|\}.$$

若 K 完备, 则 V 在 $||\cdot||_{\max}$ 下也是完备的.

定理 2.1

设 K 完备. 设 $||\cdot||$ 是 V 上任意一个范数, 则 $||\cdot||$ 与 $||\cdot||_{\max}$ 等价, 特别的 V 在任意范数下都是完备的. ♡

证明 我们沿用上面例子中的记号. 令 $C_2 = n\max\{||e_1||, \cdots, ||e_n||\}$. 则对任意 $\alpha \in V$,

$$||\alpha|| \leq \sum |x_i|||e_i|| \leq C_2||\alpha||_{\max}.$$

下面用归纳法来证明存在 $C_1 > 0$ 使得对每个 $\alpha \in V$ 有 $||\alpha|| \geq C_1||\alpha||_{\max}$. 当 $n = 1$ 时结论显然成立. 假设结论对 $n-1$ 维空间成立. 对每个 i, 考虑 $n-1$ 维空间

$$V_i = Ke_1 + \cdots Ke_{i-1} + Ke_{i+1} + \cdots Ke_n.$$

由归纳假设 V_i 在 $||\cdot||$ 下完备, 特别的 V_i 在 V 中是闭集, 从而 $W_i := e_i + V_i$ 也是 V 的闭集. 由于 $0 \notin W_i$, 故存在如下半径为 $r_i > 0$ 的 0 的邻域与 W_i 不交

$$\{\beta \in V : ||\beta|| \leq r_i.\}$$

我们取 $C_1 = \min\{r_1, \cdots, r_n\}$. 任取 V 中非零元 $\alpha = x_1e_1 + \cdots + x_ne_n$, 不妨设 $||\alpha||_{\max} = |x_j|$ 则 $x_j \neq 0$. 由于 $x_j^{-1}\alpha \in W_j$, 所以

$$||\alpha|| = |x_j| \cdot ||x_j^{-1}\alpha|| \geq r_j||\alpha||_{\max} \geq C_1||\alpha||_{\max}.$$

推论 2.1

设 $K, |\cdot|$ 完备, L/K 是有限扩张. 则 L 上延拓 $|\cdot|$ 的赋值 (若存在) 则是唯一的, 且 L 在这个赋值下完备. ♡

证明 若 L 上一个赋值延拓了 $|\cdot|$, 则它显然是 L 作为 K 线性空间的范数. 若有两个不同的赋值延拓 $|\cdot|_L$ 和 $|\cdot|'_L$, 则它们作为范数是等价的, 从而作为赋值也是等价的因为它们定义了相同的拓扑. 所以存在 $c > 0$ 使得 $|\cdot|_L^c = |\cdot|'_L$. 又它们限制在 K 上相同, 所以 $c = 1$. L 的完备性是定理的直接推论.

2.4 Hensel 引理, 非阿赋值的延拓

定义 2.5. 完备离散赋值域

设 $(K, |\cdot|)$ 是非阿赋值域. 记 $A = \{x \in K : |x| \leq 1\}$ 为 K 的赋值环.

称 K 是完备离散赋值域指 A 是离散赋值环且 K 是完备的. ♣

例 2.2 若 $\mathfrak{p}$ 是某 Dedekind 整环的非零素理想. 则其分式域 K 在 $\mathfrak{p}$ 诱导的赋值下的完备化是完备离散赋值域. 特别的前面介绍的 $\mathbb{Q}_p$ 是完备离散赋值域.

在本节中, K 总表示完备离散赋值域. 由于其赋值环 A 是离散赋值环 (特别的是 Dedekind 整环), 记 π 是其极大理想 $\mathfrak{p}$ 的一个生成元. K 中每个非零元都可写成 $\pi^m u$, $m \in \mathbb{Z}, u \in A^\times$ 的形式. 将素理想 $\mathfrak{p} = (\pi)$ 诱导的加法赋值记作 $v_\mathfrak{p}$, 则 $v_\mathfrak{p}(\pi^m u) = m$. 对于 $f, g \in A[T]$, 记号 $f \equiv g \bmod \pi^k$ 表示 $f - g$ 的每个系数在 $\mathfrak{p}^k = (\pi^k)$ 中. 记号 $\bar{f}$ 表示 f 在

剩余类域多项式环 $A/\mathfrak{p}[T]$ 中的像.

定理 2.2. Hensel 引理

设 $f(T)\in A[T], x_0\in A, n=v_{\mathfrak{p}}(f(x_0)), k=v_{\mathfrak{p}}(f'(x_0))$. 若 $n>2k$, 则存在 $x\in A$ 使得 $f(x)=0$ 且 $x\equiv x_0 \bmod \pi^{n-k}$.

证明 我们断言存在 x_1 满足

$$x_1\equiv x_0 \bmod \pi^{n-k},\quad f(x_1)\equiv 0 \bmod \pi^{n+1},\quad v_{\mathfrak{p}}(f'(x_1))=k.$$

设 $a\in A$ 记 $x_1=x_0+\pi^{n-k}a$. 由二项式展开

$$f(x_1)\equiv f(x_0)+f'(x_0)\pi^{n-k}a \bmod \pi^{2n-2k}.$$

由于 $2n-2k\geq n+1$, 上面同余式对模 π^{n+1} 也成立. 根据条件 $f'(x_0)/\pi^k\in A^\times$, 从而可取 a 满足下面同余式,

$$\frac{f(x_0)}{\pi^n}+\frac{f'(x_0)}{\pi^k}a\equiv 0 \bmod \pi.$$

此时便有 $f(x_1)\equiv 0 \bmod \pi^{n+1}$. 再由二项式展开知

$$f'(x_1)\equiv f'(x_0)+f''(x_0)\pi^{n-k}a \bmod \pi^{2n-2k}.$$

利用 $n-k>k$ 以及 $2n-2k>k$ 知 $v_{\mathfrak{p}}(f'(x_1))=k$. 这就证明了断言.

以此类推, 可用归纳法证明对每个 $m\in\mathbb{Z}_{\geq 1}$, 存在 x_m 使得

$$x_m\equiv x_{m-1} \bmod \pi^{n+m-1-k},\quad f(x_n)\equiv 0 \bmod \pi^{n+m}A,\quad v_{\mathfrak{p}}(f'(x_1))=k.$$

显然 $\{x_m\}$ 是柯西列, 设 x 是其极限. 则 $f(x)=0$. 由于每个 $x_m\equiv x_0 \bmod \pi^{n-k}$, 所以 $x\equiv x_0 \bmod \pi^{n-k}$.

推论 2.2

设 $f(T)\in A[T], x_0\in A$. 若 $f(x_0)\equiv 0 \bmod \pi$, $f'(x_0)\not\equiv 0 \bmod \pi$, 则存在唯一的 $x\in A$ 使得 $f(x)=0$ 且 $x\equiv x_0 \bmod \pi$.

证明 这是 $n=1,k=0$ 的情形. 唯一性由 x_0 是 $\bar{f}(T)\in A/\mathfrak{p}[T]$ 的单根得出.

例 2.3 考虑 $A=\mathbb{Z}_p$ 的情形. 设 $p>2$, $f(T)=T^{p-1}-1$, 由 Hensel 引理知对每个 $a\in\mathbb{F}_p^\times$, 存在唯一的 $x\in A$ 使得 $f(x)=1$ 且 $x\equiv a \bmod p$.

例 2.4 $A=\mathbb{Z}_2$. 考虑老例子 $f(T)=T^3-T^2-2T-8\in\mathbb{Z}_2[T]$. 计算知

$$f(0)\equiv f(2)\equiv f(4)\equiv f(6)\equiv f(7)\equiv 0 \bmod 8.$$

以及

$$v_2(f'(0))=v_2(f'(2))=v_2(f'(4))=v_2(f'(6))=1,\quad v_2(f'(7))=0.$$

根据 Hensel 引理, 存在 $x,y,z\in\mathbb{Z}_2$ 使得

$$f(x)=f(y)=f(z)=0 \text{ 且} x\equiv 0 \bmod 4, y\equiv 2 \bmod 4, z\equiv 7 \bmod 8.$$

这说明了 $f(T)$ 在 $\mathbb{Z}_2[T]$ 中分解为三个不同的一次因式的乘积. 后面将看到这件事情与我们之前证明的 2 在 $\mathbb{Q}(T)/(f)$ 这个数域中完全分裂这件事之前的关系.

定理 2.3. Hensel 引理’

设 $f \in A[T]$. 若 $\bar{f} = \phi\psi$ 且 $\phi, \psi \in A/\mathfrak{p}[T]$ 互素. 则存在唯一的 $g, h \in A[T]$ 使得 $f = gh$ 且 $\bar{g} = \phi, \bar{h} = \psi$ 以及 $\deg g = \deg \phi$.

证明 对每个 $n \geq 1$, 我们将归纳构造 $g_n, h_n \in A[T]$ 满足如下性质:

$$g_{n+1} \equiv g_n \bmod \pi^n \quad h_{n+1} \equiv h_n \bmod \pi^n, \tag{2.4.1}$$

$$f \equiv g_n h_n \bmod \pi^n, \quad \deg g_n = \deg \phi. \tag{2.4.2}$$

显然 $\{g_n\}, \{h_n\}$ 是两个收敛的多项式序列. 令 $g = \lim g_n$, $h = \lim h_n$, 则 g, h 满足定理的要求. 唯一性是显然的.

对 $n = 1$, $g_1, h_1 \in A[T]$ 分别取 ϕ, ψ 的任意提升且满足 $\deg g_1 = \deg \phi$. 假设对小于等于 n 时均已构造处满足上面要求的 g_n 和 h_n. 令 $g_{n+1} = g_n + \pi^n u$, $h_{n+1} = h_n\pi^n v$, $u, v \in A[T]$. 则 g_{n+1}, h_{n+1} 满足上面行间公式的第一条要求. 由于

$$g_{n+1}h_{n+1} \equiv g_n h_n + \pi^n(g_n v + h_n u) \bmod \pi^n,$$

则 $f \equiv g_{n+1}h_{n+1} \bmod \pi^{n+1}$ 当且仅当

$$\frac{f - g_n h_n}{\pi^n} + (g_n v + h_n u) \equiv 0 \bmod \pi. \tag{2.4.3}$$

注意根据归纳假设, 上式左边第一项属于 $A[T]$. 由于 $g_n \equiv \phi \bmod \pi, h_n \equiv \psi \bmod \pi$, 且 ϕ, ψ 在 $A/\mathfrak{p}[T]$ 中互素, 满足(2.4.3)的 u, v 显然是存在的, 且可要求 $\deg u < \deg g_n = \deg \phi$, 因为若 $\deg u > \deg \phi$, 则 $u \equiv \phi q + r \bmod \pi$, 这里 $q, r \in A[T]$ 且 $\deg r < \deg \phi$, 将原来的 (u, v) 换成 $(r, v + h_n q)$ 即可.

推论 2.3

设 $f(T) = T^d + a_{d-1}T^{d-1} + \cdots a_0 \in K[T]$ 是首一不可约多项式, 若 $a_0 \in A$, 则每个系数 a_i 也属于 A.

证明 如若不然, 则存在 $k \in \mathbb{Z}_{\geq 1}$ 使得 $\pi^k f(T) \in A[T]$ 但 $\pi^k f(T) \not\equiv 0 \bmod \pi$. 我们有

$$\pi^k f(T) \equiv T^i g(T) \bmod \pi \quad g(T) \in A[T], \text{ 且} 1 \leq i \leq d-1.$$

根据 Hensel 引理’ 知 $f(T)$ 不是不可约多项式. 矛盾.

现在利用 Hensel 引理来证明本节的主要结果.

定理 2.4. 完备离散赋值域的延拓

设 K 是完备离散赋值域, A 是其赋值环. 设 L/K 是有限扩张.

(1) 存在唯一的 L 上的赋值 $|\cdot|_L$ 延拓了 $(K, |\cdot|)$. 这个赋值是

$$|\alpha|_L = |N_{L/K}(\alpha)|^{\frac{1}{[L:K]}}, \quad \alpha \in L.$$

(2) L 的赋值环 $\{\alpha \in L : |\alpha|_L \leq 1\}$ 等于 A 在 L 中的整闭包.

(3) B 是完备离散赋值环, L 是完备离散赋值域.

证明 (1) 延拓的唯一性由推论2.1知. 现来证 (2) 中的等式. 记 B 为 A 在 L 中的整闭包. 若 $\alpha \in B$, 熟知 $N_{L/K}(\alpha) \in A$, 故 $|\alpha|_L \leq 1$. 反过来, 若 $N_{L/K}(\alpha) \in A$, 则 α 在 K 的极小

多项式的常数项也属于 A. 根据上面 Hensel 引理的推论知 α 的极小多项式属于 $A[T]$, 则 $\alpha \in B$. 这就证明了 (2) 中的等式. 特别的 $\{\alpha \in L : |\alpha|_L \leq 1\}$ 是环, 因为 B 是环.

现证 $|\cdot|_L$ 是赋值. $|\cdot|_L$ 的" 非零性" 与" 乘性" 根据范数的性质显然. 关于强三角不等式, 我们只需证明 $|\alpha|_L \leq 1 \Rightarrow |\alpha+1|_L \leq 1$. 而这也是显然成立的因为 B 是环! 这就证明了 (1) 和 (2).

(3) 根据推论2.1知, L 是完备的. 从而 L 的赋值环 B 是完备赋值环. 赋值的离散性从 $|\cdot|_L$ 的定义可得出. 这就证明了本定理.

(当 L/K 可分时 (3) 的另证) 由 $|\cdot|_L$ 的定义可看出 $|\cdot|_L$ 也是离散赋值. 从而 B 是离散赋值环. 又 B 是 A 在 L 中的整闭包, 依据第一章 Dedekind 整环的结论知 B 是有限生成的 A 模, 从而由 A 是主理想整环知 $B \cong A^n, n=[L:K]$. 再利用 A 是完备的知

$$A \cong \varprojlim A/\mathfrak{p}^n \quad \text{从而} \quad B \cong \varprojlim B/\mathfrak{p}^n B.$$

注意到 $\mathfrak{p}^n B$ 是 B 的一组邻域基, 所以 B 是完备的. 取 $\Pi \in B$ 是 B 极大理想的生成元, 则 $L = B[\Pi^{-1}]$. 由此得 L 也是完备的.

延拓的唯一性的另证: 如果 $(L, |\cdot|'_L)$ 是 $(K, |\cdot|)$ 的另一种延拓, 则 $|\cdot|'_L$ 也是非阿赋值. 那么记 $B', \mathfrak{p}'$ 分别为 $(L, |\cdot|'_L)$ 的赋值环和其极大理想. 我们先断言 $B \subset B'$. 否则取 $\alpha \in B \setminus B'$, 由于 α 在 A 上整, 设 $f = T^d + a_{d-1}T^{d-1} + \cdots + a_0 \in A[T]$ 是 α 在 K 上的极小多项式. 则

$$\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_0 = 0.$$

两边同时除以 α^d, 利用 $A \subset B'$ 得 $1 \in \mathfrak{m}'_L$, 矛盾. 说明 $B \subset B'$, 即 $|x|_L \leq 1 \Rightarrow |x|'_L \leq 1$.

类似的可证明 $\mathfrak{p} \subset \mathfrak{p}'$, 即 $|x|_L < 1 \Rightarrow |x|'_L < 1$. (否则取 $\alpha \in \mathfrak{m} \setminus \mathfrak{m}'$, 则由 Hensel 引理知上面 α 极小多项式的每个系数 $a_i \in \mathfrak{p}$ (为什么, 留作习题), 然后两边除以 α^d 得出 $1 \in \mathfrak{m}'_L$ 的矛盾.)

现在若 $|x|_L > 1$, 则 $|x^{-1}|_L < 1$, 则 $|x^{-1}|'_L < 1$ 从而 $|x|'_L > 1$. 根据赋值等价性的等价条件知 $|\cdot|_L \sim |\cdot|'_L$, 但它们限制在 K 上相等, 说明 $|\cdot|_L = |\cdot|'_L$. 这就证明了唯一性.

推论 2.4

设 $\overline{K}$ 是 K 的代数闭域. 其上存在唯一的赋值 (仍记作)$|\cdot|$ 延拓 $(K, |\cdot|)$.
特别的取 $(K, |\cdot|) = (\mathbb{Q}_p, |\cdot|_p)$ 时, $\overline{\mathbb{Q}}_p$ 上存在唯一的赋值 (仍记作)$|\cdot|_p$ 延拓 $(\mathbb{Q}_p, |\cdot|_p)$. ♡

证明 唯一性是上面定理的推论. 存在性: 对任意 $\alpha \in \overline{K}$. 定义

$$|\alpha| = |N_{K(\alpha)/K}(\alpha)|^{\frac{1}{[K(\alpha):K]}}.$$

如果 L 是含有 α 的 K 的有限扩张, 利用如下范映射的事实, 再由上面定理知 $|\cdot|$ 是赋值.

$$N_{L/K}(\alpha) = (N_{K(\alpha)/K}(\alpha))^{[L:K(\alpha)]}.$$

2.5 嵌入, 非阿赋值, 素理想, 在数域中的应用

本节中 K 总表示数域.

2.5.1 素理想与非阿赋值

先回顾下素理想与非阿赋值之间的关系. 设 $\mathfrak{p}$ 是 $\mathcal{O}_K$ 的非零素理想. 如前面所讲可定义 K 上的 (加法) 赋值 $v_{\mathfrak{p}}$. 其 (乘法) 赋值 $|\cdot|_v$ 可定义为,

$$|x|_v = C^{-v_{\mathfrak{p}}(x)} \quad C > 1.$$

取不同的 C 定义的是等价的赋值. 由此得到一个从 $\mathcal{O}_K$ 的素理想到 K 的非阿赋值等价类的映射, 这里将 0 理想对应到平凡赋值.

反过来, 对于 K 上一个非阿赋值 $|\cdot|$, 令 A 是其赋值环, $\{x \in A : |x| < 1\}$ 是 A 的极大理想. (注意到两个等价的非阿赋值给出的赋值环和极大理想是相同的.) 由下面引理知 $\mathcal{O}_K \subset A$, 那么 $\{x \in A : |x| < 1\} \cap \mathcal{O}_K$ 是 $\mathcal{O}_K$ 的素理想. 特别的, 若 $|\cdot|$ 是平凡赋值, 则 $\{x \in A : |x| < 1\} \cap \mathcal{O}_K$ 是 0 理想.

引理 2.3

若 $|\cdot|$ 是 K 上的非阿赋值, 设 $A = \{x \in K : |x| \leq 1\}$ 是其赋值环. 则 $\mathcal{O}_K \subset A$.

证明 设 $\alpha \in \mathcal{O}_K$. 则存在 $a_0, \cdots, a_{n-1} \in \mathbb{Z}$ 使得 $\alpha^n = a_{n-1}\alpha^{n-1} + \cdots a_1\alpha + a_0$. 根据非阿赋值的强三角不等式性质以及 $k \in \mathbb{Z} \Rightarrow |k| \leq 1$ 的性质知存在 $0 \leq i \leq n-1$ 使得

$$|\alpha^n| \leq |a_i\alpha^i| \leq |\alpha^i|.$$

由此 $\alpha \in A$.

命题 2.2

我们有一一对应:

$$\{\mathcal{O}_K \text{ 的素理想}\} \quad \overset{1-1}{\longleftrightarrow} \quad \{K \text{ 的非阿赋值}\}/\sim$$

$$\mathfrak{p} \mapsto |\cdot|_v$$

$$\{x \in K : |x| < 1\} \cap \mathcal{O}_K \leftarrow\!\shortmid |\cdot|$$

证明 这两个映射显然互逆.

接下来设 L/K 是有限扩张. 设 $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_g\}$ 是 L 的 $\mathfrak{p}$ 之上的素理想. 对 $\mathfrak{P} = \mathfrak{P}_i$, 可定义 L 上的加法赋值 $w_{\mathfrak{P}}$. 其相应的 (乘法) 赋值 $|\cdot|_w$ 定义为

$$|x|_w = C^{-\frac{w_{\mathfrak{P}}(x)}{e}}, \quad e = e(\mathfrak{P}/\mathfrak{p}).$$

则 $(L, |\cdot|_w)$ 是 $(K, |\cdot|_v)$ 的延拓.

命题 2.3

设 $|\cdot|_v$ 是 $\mathfrak{p}$ 诱导的 K 上的赋值. 有一一对应:

$$\{\mathcal{O}_L \text{ 的} \mathfrak{p} \text{ 之上的素理想}\} \quad \overset{1-1}{\longleftrightarrow} \quad \{L \text{ 的延拓} (K, |\cdot|_v) \text{ 的赋值}\}$$

证明 这是由前一命题推出来的. 再注意到若 $|\cdot|, |\cdot|'$ 是两个延拓, 则 $|\cdot| \sim |\cdot|'$ 等价于

$|\cdot| = |\cdot|'$, 因为它们限制在 K 上相同.

用域嵌入的方式也可以给出 L 上延拓 $(K, |\cdot|_v)$ 的赋值. 记 K_v 是 K 在 $|\cdot|_v$ 的完备化. 记 $\overline{K}_v$ 是 K_v 的代数闭包, 在上一节中我们证明了 $|\cdot|_v$ 可唯一的延拓到 $\overline{K}_v$ 上. 任给 $\sigma \in \mathrm{Hom}_K(L, \overline{K}_v)$, 可得到 L 的一个延拓 $(K, |\cdot|_v)$ 的赋值:

$$|x|_\sigma := |\sigma(x)|_v.$$

定义 2.6

对 $\sigma, \tau \in \mathrm{Hom}_K(L, \overline{K}_v)$, 称 σ 与 τ 共轭 (记作 $\sigma \sim \tau$) 指存在 $s \in \mathrm{Gal}(\overline{K}_v/K_v)$ 使得 $\sigma = s \circ \tau$, 即使得下图交换

$$\begin{tikzcd} L \arrow[r, "\tau"] \arrow[dr, "\sigma"'] & \overline{K}_v \arrow[d, "s"] \\ & \overline{K}_v \end{tikzcd}$$

换句话讲, 若 $L = K(\alpha)$, 则 σ 与 τ 共轭当且仅当 $\sigma(\alpha)$ 与 $\tau(\alpha)$ 是在 K_v 上共轭的两个元素. ♣

例 2.5 设 $L/K = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, $K_v = \mathbb{Q}_5$. 根据 $T^3 - 2$ 模 5 的不可约分解得出在 $\mathbb{Q}_5[T]$ 中的不可约分解为

$$T^3 - 2 = (T - 3 + O(5))(T^2 + (3 + O(5))T + 4 + O(5)).$$

从而在 $\overline{\mathbb{Q}}_5[T]$ 中,

$$T^3 - 2 = (T - \alpha)(T - \beta_1)(T - \beta_2), \quad \text{其中}\alpha \in 3 + 5\mathbb{Z}_5, \beta_1, \beta_2 \notin \mathbb{Q}_5.$$

我们有

$$\mathrm{Hom}(\mathbb{Q}(\sqrt[3]{2}, \overline{\mathbb{Q}}_5) = \{\sigma, \tau_1, \tau_2\},$$

这三个域嵌入由 $\sigma(\sqrt[3]{2}) = \alpha, \tau_i(\sqrt[3]{2}) = \beta_i\ (i = 1, 2)$ 决定. 则 τ_1 与 τ_2 是共轭的, σ 与 τ_i 是不共轭的.

虽然之前讨论的 v 是非阿的, 但下面的定理对 v 是阿基米德赋值也成立. (详见下一小节对无穷素位的补充)

定理 2.5. 延拓定理

设 $|\cdot|_v$ 是数域 K 的赋值.

(1) L 的每个延拓 $(K, |\cdot|_v)$ 的赋值都等于某 $|\cdot|_\sigma, \sigma \in \mathrm{Hom}_K(L, \overline{K}_v)$;

(2) 对 $\sigma, \tau \in \mathrm{Hom}_K(L, \overline{K}_v), |\cdot|_\sigma \sim |\cdot|_\tau$ 当且仅当 σ 与 τ 共轭. ♡

上述定理可表述成

定理 2.6. 延拓定理等价描述

有一一对应:

$$\mathrm{Hom}_K(L,\overline{K}_v)/\sim\ \xleftrightarrow{1-1}\ \{L\text{ 的延拓}(K,|\cdot|_v)\text{ 的非阿赋值}\}$$
$$\sigma\longmapsto|\cdot|_\sigma.$$

证明 (1) 设 $|\cdot|_w$ 是 L 的一个赋值且延拓 $|\cdot|_v$. 记 L_w 是 $(L,|\cdot|_w)$ 的完备化. 则 K 在 L_w 中的闭包是 K 的完备化 K_v. 所以 $L_w\supset LK_v$. 由于 LK_v 是 K_v 的有限扩张, 根据定理2.1, LK_v 是完备的. 根据完备化的唯一性知,

$$L_w=LK_v.$$

从而 L_w/K_v 是有限扩张特别的是代数扩张. 所以 $\mathrm{Hom}_{K_v}(L_w,\overline{K}_v)$ 非空.

任取 $\sigma\in\mathrm{Hom}_{K_v}(L_w,\overline{K}_v)$. 利用这个 σ, 我们又可得到 L_w 的一个赋值: $x\mapsto|\sigma(x)|_v$ 且延拓 $|\cdot|_v$. 由于 K_v 是完备的, 根据延拓的唯一性, (定理2.1) 知 $|x|_w=|\sigma(x)|_v$ 对任意 $x\in L_w$, 特别的等式对 $x\in L$ 成立. 最后注意到 $\sigma|_L\in\mathrm{Hom}_K(L,\overline{K}_v)$. 所以 L 上的赋值 $|\cdot|_w$ 是由 σ_L 诱导来的. 这就证明了 (1). 从这个证明中还得出 (后面会用到)

$$L_w\cong\sigma(L_w)=K_v\sigma(L),\tag{2.5.1}$$

(2) 若 σ 与 τ 共轭, 则根据赋值延拓的唯一性知 $|\cdot|_\sigma=|\cdot|_\tau$. 反之, 设 $|\cdot|_\sigma=|\cdot|_\tau$. 断言: $\tau(L)K_v$ 是 $\tau(L)$ 的完备化. 一方面由于 $\tau(L)K_v$ 是 K_v 的有限扩张, 故是完备的, 所以它包含 $\tau(L)$ 的完备化; 另一方面 $\tau(L)$ 的完备化要包含 $\tau(K)=K$ 的完备化 K_v 以及 $\tau(L)$. 这就证明了断言. 所以 $\tau(L)L_v$ 中的元素都形如 $\lim\tau(x_n)$, $\tau(x_n)$ 是柯西列 $x_n\in L$. 类似的结论当然对 $\sigma(L)$ 也成立.

定义

$$s:\tau(L)K_v\to\sigma(L)K_v,\quad \lim\tau(x_n)\to\lim\sigma(x_n).$$

这里 $\tau(x_n)$ 是 $\tau(L)K_v\subset\overline{K}_v$ 中的柯西列. 由于 $|\cdot|_\sigma=|\cdot|_\tau$, $\sigma(x_n)$ 也是 $\sigma(L)K_v\subset\overline{K}_v$ 中的柯西列, 所以 $\lim\sigma(x_n)\in\sigma(L)K_v$.

请读者自行验证 s 不依赖于代表柯西列的选取以及 σ 是域嵌入. 由于 $\tau|_K=\sigma|_K$, 所以根据 s 的定义, s 限制在 K_v 上也是恒等. 根据域论 s 可延拓为 $\overline{K}_v$ 到 $\overline{K}_v$ 的自同构. 这就证明了 $\sigma\sim\tau$.

设

$$\mathfrak{p}\mathcal{O}_L=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}.$$

设 $L=K(\alpha)$, $f(T)\in K[T]$ 是 α 在 K 上的极小多项式. 设 $f(T)$ 在 $K_v[T]$ 上的不可约分解为:

$$f(T)=f_1(T)\cdots f_u(T)\quad(\text{马上会看到}u=g).$$

对每个 $\beta\in\overline{K}_v$ 是 $f(T)$ 的根, 都存在域嵌入 $L\hookrightarrow\overline{K}_v$ 将 α 映为 β.

反过来, 给定 $\sigma,\tau\in\mathrm{Hom}_K(L,\overline{K}_v)$, $\sigma(\alpha)$ 和 $\tau(\alpha)$ 也分别是某 f_i 和 f_j 的根. 又根据域论, σ 与 τ 共轭当且仅当 $\sigma(\alpha)$ 与 $\tau(\alpha)$ 都是某个 f_i 的根. 特别的, $u=g$. 所以我们有一一

对应

$$\mathrm{Hom}_K(L,\overline{K}_v)/\sim \quad \xleftrightarrow{1-1} \quad \{f_1,\cdots,f_g\}. \tag{2.5.2}$$

设 L 在 $|\cdot|_\sigma$ 的完备化为 L_w, 显然 σ 可延拓为 $\mathrm{Hom}_{K_v}(L_w,\overline{K}_v)$ 中的元素. 由上面的证明公式(2.5.1)知 $\sigma(L_w)=K_v(\sigma(\alpha))\cong K_v[T]/(f_i)$, 利用 $L_w\cong\sigma(L_w)$ 知 $L_w\cong K_v[T]/(f_i)$.

如果 $|\cdot|_w$ 是 $|\cdot|_v$ 的延拓, 我们记作 $w\mid v$.

定理 2.7

设 $\alpha,f,f_1,\cdots,f_g$ 如上面, 我们有 K_v-代数同构:

$$L\otimes_K K_v\cong K_v[T]/(f)\cong\prod_{i=1}^{g}K_v[T]/(f_i)\cong\prod_{w|v}L_w.$$

♡

证明 其中第一个同构利用 $L\cong K[T]/(f)$ 以及张量积的基本性质. 第二个同构是中国剩余定理, 第三个同构是根据上面的讨论.

推论 2.5

$\mathfrak{p}$ 在 L 中完全分裂当且仅当 $f(T)$ 在 K_v 中分解为一次多项式的乘积.

♡

例 2.6 前面用 Hensel 引理知 $f(T)=T^3-T^2-2T-8$ 在 $\mathbb{Q}_2$ 中分解为三个不同的一次因式乘积; 在第一章中用理想语言证明了 2 在 $\mathbb{Q}(\alpha)$ 中完全分裂 ($f(\alpha)=0$); 这个例子中产生的现象便是上面定理的一个特例.

推论 2.6

设 $N_{L/K}:L\to K,\mathrm{Tr}_{L/K}:L\to K$ 分别是范和迹映射. 我们有

$$N_{L/K}=\prod_{w|v}N_{L_w/K_v}\quad 以及\quad \mathrm{Tr}_{L/K}=\prod_{w|v}\mathrm{Tr}_{L_w/K_v}.$$

♡

证明 设 $e_1,\cdots,e_n$ 是 L 的一组 K 基. 则 $e_1\otimes 1,\cdots,e_n\otimes 1$ 是 $L\otimes K_v$ 的一组 K_v 基. 对任意 $L\to L$ 的 K 线性变换 $\mathcal{A}$, $\mathcal{A}\otimes 1$ 给出了 $L\otimes K_v\to L\otimes K_v$ 的 K_v 线性变换, 且这两个线性变换在上面两组基下的矩阵是相同的. 特别的, 对 $\alpha\in L$,

$$N_{L/K}(\alpha)=N_{L\otimes K_v/K_v}(\alpha\otimes 1),\quad \mathrm{Tr}_{L/K}(\alpha)=\mathrm{Tr}_{L\otimes K_v/K_v}(\alpha\otimes 1).$$

本推论随后由上面定理的同构得出.

2.5.2 关于无穷素位的简短补充

定理 2.8. Ostrowkski

(1) $\mathbb{Q}$ 的阿基米德赋值等价于通常的绝对值.

(2) 更一般的, 设 K 是数域.

$$\{K\text{ 的阿基米德赋值}\}/\sim \quad \stackrel{1-1}{\longleftrightarrow} \quad \mathrm{Hom}(K,\mathbb{C})/\sim$$

♡

证明 (1) 设 $||\cdot||$ 是 $\mathbb{Q}$ 的一个阿基米德赋值. 设 m_0 是大于 1 的两个整数. 对每个 $N\in\mathbb{Z}_{\geq 1}$, 存在正整数 k 以及 $a_i\in\{0,1\cdots,m_0-1\}$ 使得

$$m^N=a_0+a_1m_0+\cdots a_km_0^{k-1},\quad m_0^{k-1}\leq m^N<m_0^k.$$

则 $k\leq N\frac{\log m}{\log m_0}+1$. 记 $A=\max\{||1||,||2||,\cdots,||m_0-1||\}$. 则对每个 N,

$$||m||=\sqrt[N]{||m||^N}\leq\sqrt[N]{A(1+||m_0||+\cdots+||m_0^{k-1}||)}. \tag{2.5.3}$$

若 $||m_0||\leq 1$, 令 N 趋于无穷大可得 $||m||\leq 1$, 从而 $||\cdot||$ 是非阿赋值, 矛盾. 由于 m_0 是任意选取的, 所以每个大于 1 的整数的 $||\cdot||$ 都大于 1. 由(2.5.3)得

$$||m||\leq\sqrt[N]{kA\cdot||m_0^{k-1}||}.$$

令 N 趋于无穷得,

$$||m||\leq||m_0||^{\frac{\log m}{\log m_0}}$$

调换 m 与 m_0 的位置重复上面的证明得

$$||m_0||\leq||m||^{\frac{\log m_0}{\log m}}.$$

若记 $||m_0||=m_0^c$, 则 $c>0$, 则上式说明了 $||m||=m^c$. 因为 m 是任意的以及 $||-1||=1$, 利用赋值的乘性知对任意 $x\in\mathbb{Q}$ 有 $||x||=|x|^c$. 这就证明了 $||\cdot||$ 与通常的绝对值 $|\cdot|$ 是等价的.

用 (1) 的结论, (2) 可由原封不动的仿照定理2.6的证明得出.

我们将 $\mathrm{Hom}(K,\mathbb{C})/\sim$ 中的元素 σ 或者它诱导的赋值 $|\cdot|_\sigma$ 称作是 K 的一个无穷素位. 若 σ 是实 (复) 嵌入, 称 σ 是实 (复) 素位. 下面的命题也是类似得到的.

命题 2.4

设 L/K 是数域的扩张, 设 $|\cdot|_\sigma$ 是 K 的一个无穷素位, 记 $\mathrm{Hom}_\sigma(L,\mathbb{C})=\{\tau\in\mathrm{Hom}(L,\mathbb{C}):\tau|_K=\sigma\}$. 则有一一对应

$$\{L\text{ 的延拓}|\cdot|_\sigma\text{ 的赋值}\}/\sim \quad \stackrel{1-1}{\longleftrightarrow} \quad \mathrm{Hom}_\sigma(L,\mathbb{C})/\sim.$$

♠

综合前面一小节对非阿赋值的讨论, 下面三个集合有一一对应 (记 $\mathbb{Q}_\infty=\mathbb{R}$)

$$K\text{ 非平凡赋值等价类之集},\quad \mathcal{O}_K\text{ 非零素理想之集}\cup\mathrm{Hom}(K,\mathbb{C})/\sim,\quad \bigcup_{p\leq\infty}\mathrm{Hom}(K,\overline{\mathbb{Q}}_p)/\sim.$$

现在可以给出数域 K 的素位的定义:

定义 2.7

设 K 是数域, K 的一个素位 (或者素点) 是指 K 上的一个非平凡赋值的等价类. 非阿赋值对应的素位称作是有限素位, 阿基米德赋值对应的素位称作是无穷 (无限) 素位. 无歧义时, 也将在上面一一对应下另外两个集合中的元素称作是 K 的一个素位 (有限素位, 无穷素位). ♣

2.5.3 分歧

现在回到 v 是非阿的情形. 设 $K_v = K_\mathfrak{p}$ 是素理想 $\mathfrak{p}$ 诱导的完备化, $L_w = L_\mathfrak{P}$ 是 $\mathfrak{P}$ 诱导的完备化, 且 $\mathfrak{P} \mid \mathfrak{p}$, 则 L_w 是 K_v 的有限扩张. 设 $\mathcal{O}_v = \mathcal{O}_\mathfrak{p}$ 和 $\mathcal{O}_w = \mathcal{O}_\mathfrak{P}$ 分别是 K_v 和 L_w 的赋值环. 前面我们证明了 $\mathcal{O}_w$ 等于 $\mathcal{O}_v$ 在 L_w 中的整闭包. 我们有 $\mathcal{O}_v$ 的极大理想等于 $\mathfrak{p}\mathcal{O}_v$, $\mathcal{O}_w$ 的极大理想等于 $\mathfrak{P}\mathcal{O}_w$.

命题 2.5

我们有 $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}\mathcal{O}_w/\mathfrak{p}\mathcal{O}_v)$, $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}\mathcal{O}_w/\mathfrak{p}\mathcal{O}_v)$; ♠

证明 若 $\mathfrak{P}' \neq \mathfrak{P}$ 是 $\mathcal{O}_L$ 的素理想, 则 $\mathfrak{P}'\mathcal{O}_w = \mathcal{O}_w$. 记 $\mathfrak{P}_1 = \mathfrak{P}$, $e_1 = e(\mathfrak{P}/\mathfrak{p})$, 那么

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \Rightarrow \mathfrak{p}\mathcal{O}_w = \mathfrak{P}_1^{e_1}\mathcal{O}_w.$$

这就证明了关于分歧指数的断言. 对于惯性指数的断言是由于

$$\mathcal{O}_L/\mathfrak{P} \cong \mathcal{O}_w/\mathfrak{P}\mathcal{O}_w \quad \text{以及} \quad \mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_v/\mathfrak{p}\mathcal{O}_v.$$

注 记 $e = e(\mathfrak{P}/\mathfrak{p})$, $f = f(\mathfrak{P}/\mathfrak{p})$. 通过数 $\mathcal{O}_w/\mathfrak{p}\mathcal{O}_w = \mathcal{O}_w/\mathfrak{P}^e\mathcal{O}_v$ 两边的 $\mathcal{O}_v/\mathfrak{p}\mathcal{O}_v$-维数, 利用 $\mathcal{O}_v$ 是主理想整环易得

$$[L_w : K_v] = ef.$$

结合定理2.7, 这重新证明了用理想语言讲述时的等式:

$$\sum_{\mathfrak{P}} e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}) = [L : K].$$

笔记 所以要了解数域中素理想的分解行为, 我们需要学习类似 L_w/K_v 在扩张中的分歧指数与惯性指数, 由于这些域是完备离散赋值域且剩余类域是有限域, 了解它们比了解数域要简单一些.

衡量分歧的更精细的概念是共轭差积. 我们回顾所谓 $AKLB$ 记号, 即 A 是 Dedekind 整环, K 是 A 的分式域, L/K 是有限可分扩张, B 是 L 在 A 中的整闭包. 在这里 $AKLB$ 等于下面两种情况之一 (一般的讨论参考数论 I §6.3 或者 Neukrich):

$$\mathcal{O}_K, K, L, \mathcal{O}_L \quad \text{和} \quad \mathcal{O}_v, K_v, L_w, \mathcal{O}_w$$

定义 2.8

设 $AKLB$ 如上. 令

$$\boldsymbol{D}(B/A)^{-1} := \{\alpha \in L : \mathrm{Tr}_{L/K}(\alpha B) \subset A\}.$$

$\boldsymbol{D}(B/A)^{-1}$ 是 B 分式理想且包含 B (练习). 定义 $AKLB$ 的**共轭差积** (different) $\boldsymbol{D}(B/A)$ 为 $\boldsymbol{D}(B/A)^{-1}$ 的逆理想. 特别的 $\boldsymbol{D}(B/A)$ 是 B 的整理想.

$(\mathbb{Z}, \mathbb{Q}, K, \mathcal{O}_K)$ 的共轭差积被称作数域 K 的 (绝对) 共轭差积, 记作 $\boldsymbol{D}_K$.

命题 2.6

设 K 是数域, $\mathbf{N}$ 是理想的绝对范, d_K 是 K 的判别式. 则

$$\mathbf{N}(\boldsymbol{D}_K) = d_K.$$

证明 设 K 的一组整基是 $\alpha_1, \cdots, \alpha_n$. 回顾 $\mathrm{Tr}_{K/\mathbb{Q}}$ 诱导了 K 上的非退化双线性配对. 记 $\breve{\alpha}_1, \cdots, \breve{\alpha}_n$ 是对偶基. 则 $\boldsymbol{D}_K^{-1}$ 是由这组对偶基自由生成的 $\mathbb{Z}$-模. 由于

$$(\breve{\alpha}_1, \cdots, \breve{\alpha}_n) = (\alpha_1, \cdots, \alpha_n)(\mathrm{Tr}(\alpha_i \alpha_j))_{i,j}.$$

我们有

$$[\boldsymbol{D}_K^{-1} : \mathcal{O}_K] = [\mathcal{O}_K : \boldsymbol{D}_K] = \det(\mathrm{Tr}(\alpha_i \alpha_j))_{i,j} = d_K.$$

设 $|\cdot|_{\mathfrak{p}} = |\cdot|_v$ 是 K 的素位延拓了 $\mathbb{Q}, |\cdot|_p$. 对 $\mathbb{Z}_p, \mathbb{Q}_p, K_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}$. 由于 $\mathcal{O}_v$ 是有限秩的自由 $\mathbb{Z}_p$-模, 设 $\alpha_1, \cdots, \alpha_n$ 是一组基. 定义局部判别式 $d_{K_{\mathfrak{p}}}$ 为这组基在 $\mathrm{Tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p}$ 诱导的双线性配对的度量矩阵的行列式在 $\mathbb{Z}_p$ 中生成的理想. 对 $K_{\mathfrak{p}}$ 的理想 $\mathfrak{p}^k$, 定义

$$N_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\mathfrak{p}^k) = (p\mathbb{Z}_p)^{fk}, \quad f = f(\mathfrak{p}/p).$$

这个定义使得, 对 $\alpha \in K_v$, $N_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\alpha)\mathbb{Z}_p = N_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\alpha \mathcal{O}_v)$. (证明类似第一章最后一节: 理想的范.)

命题 2.7

$$N_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\boldsymbol{D}(\mathcal{O}_v/\mathbb{Z}_p)) = d_{K_{\mathfrak{p}}}.$$

如下定理将共轭差距的计算归化为" 局部" 情形.

定理 2.9

$v_{\mathfrak{P}}(\boldsymbol{D}(\mathcal{O}_L/\mathcal{O}_K)) = v_{\mathfrak{P}}(\boldsymbol{D}(\mathcal{O}_w/\mathcal{O}_v))$.

证明 设 $d \in \mathbb{Z}_{\geq 1}$, 我们需证明 $\mathfrak{P}^d \mid D(\mathcal{O}_w/\mathcal{O}_v)$ 当且仅当 $\mathfrak{P}^d \mid D(\mathcal{O}_L/\mathcal{O}_K)$. 取 $0 \neq a \in \mathcal{O}_K$ 使得 $a \in \mathfrak{P}^d$. 由中国剩余定理再结合推论2.6得下面交换图表:

$$\begin{tikzcd}
\mathfrak{P}^{-d}/\mathcal{O}_L \arrow[r, hook] \arrow[d, "\cong"] & a^{-1}\mathcal{O}_L/\mathcal{O}_L \arrow[r, "\mathrm{Tr}"] \arrow[d, "\cong"] & a^{-1}\mathcal{O}_K/\mathcal{O}_K \arrow[d, "\cong"] \\
\mathfrak{P}^{-d}\mathcal{O}_w/\mathcal{O}_w \arrow[r, hook] & \prod\limits_{\mathfrak{P}'|a} a^{-1}\mathcal{O}_{\mathfrak{P}'}/\mathcal{O}_{\mathfrak{P}'} \arrow[r, "\sum\limits_{\mathfrak{p}'|a}\mathrm{Tr}_{\mathfrak{P}'/\mathfrak{p}'}"] & \prod\limits_{\mathfrak{p}'|a} a^{-1}\mathcal{O}_{\mathfrak{p}'}/\mathcal{O}_{\mathfrak{p}'}.
\end{tikzcd}$$

其中第一行右侧的 Tr 表示由迹映射诱导的, 第二行右侧的 $\mathrm{Tr}_{\mathfrak{P}'/\mathfrak{p}'}$ 是由 $L_{\mathfrak{P}'}$ 到 $K_{\mathfrak{p}'}$ 的迹映射诱导的. 中间和右边的同构是中国剩余定理以及前面证明过的 Dedekind 整环的事实:

对非零理想 $\mathfrak{a} \subset \mathcal{O}_K$ 有 $\mathcal{O}_K/\mathfrak{a} \cong \mathfrak{a}^{-1}/\mathcal{O}_K$. 那么,

$$\begin{aligned}\mathfrak{P}^d \mid \boldsymbol{D}(\mathcal{O}_L/\mathcal{O}_K) &\Leftrightarrow \text{ 上右水平箭头零化}\mathfrak{P}^{-d}/\mathcal{O}_L \\ &\Leftrightarrow \text{ 下右水平箭头零化}\mathfrak{P}^{-d}\mathcal{O}_w/\mathcal{O}_w \\ &\Leftrightarrow \mathfrak{P}^d\mathcal{O}_w \mid \boldsymbol{D}(\mathcal{O}_w/\mathcal{O}_v).\end{aligned}$$

推论 2.7

对每个素数 p, 有 $v_p(d_K) = \sum\limits_{\mathfrak{p}|p} v_p(d_{K_\mathfrak{p}})$.

定理 2.10

$v_\mathfrak{P}(\boldsymbol{D}(\mathcal{O}_w/\mathcal{O}_v)) \geq e-1$, 等号成立当且仅当 $\mathfrak{p} \nmid e$, 这里 $e = e(\mathfrak{P}/\mathfrak{p})$.

引理 2.4

设 L_w/K_v 是完全分歧. 设 Π 是 $\mathfrak{P}\mathcal{O}_w$ 的一个生成元. 则 $\mathcal{O}_w = \mathcal{O}_v[\Pi]$.

证明 此时 Π 的极小多项式是关于 $\mathfrak{p}$ 的 Eisenstein 多项式 $f(T) = T^n + a_{n-1}T^{n-1} + \cdots a + 0$ (之前习题的结论). 根据前面 Dedekind 整环的结论知 $\mathcal{O}_w/(\mathcal{O}_v[\Pi]) \otimes \mathcal{O}_v/\mathfrak{p} = 0$. 但由于 $\mathfrak{p}$ 是 $\mathcal{O}_v$ 唯一的极大理想, 知 $\mathcal{O}_w = \mathcal{O}_v[\Pi]$. 通过乘 Π 诱导的线性映射 $L_w \to L_w$ 在基 $1, \Pi, \cdots, \Pi^{n-1}$ 下的矩阵记为 A. 则 A 是 $\mathcal{O}_v$ 系数的矩阵, 且 $A \bmod \mathfrak{p}$ 形如

$$\begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ & \ddots & \ddots & & \\ & & & & \\ & & & 1 & 0 \end{pmatrix}$$

由此易得对 $k \geq 1$, $\mathrm{Tr}(\Pi^k) = \mathrm{Tr}(A^k) \equiv 0 \bmod \mathfrak{p}$.

练习 2.1 思考题: 设 L_w/K_v 不一定完全分歧, 证明此时也存在 $\alpha \in \mathcal{O}_w$ 使得 $\mathcal{O}_w = \mathcal{O}_v[\alpha]$. 这在数域的情形是不对的, 例如 $K = \mathbb{Q}(\alpha)$, α 是 $T^3 - T^2 - 2T - 8$ 的一个根.

命题 2.8

(1) 若 L_w/K_v 是非分歧的, 则 $\boldsymbol{D}(\mathcal{O}_w/\mathcal{O}_v) = (1)$ 且 $\mathrm{Tr}(\mathcal{O}_w) = \mathcal{O}_v$.

(2) 设分歧指数 $e = e(\mathfrak{P}/\mathfrak{p}) > 1$. 则 $\mathrm{Tr}(\mathfrak{P}) \subset \mathfrak{p}$; 当 $\mathfrak{p} \nmid e$ 时 $\mathrm{Tr}(\mathcal{O}_w) = \mathcal{O}_v$; 当 $\mathfrak{p} \mid e$ 时, $\mathrm{Tr}(\mathcal{O}_w) \subset \mathfrak{p}\mathcal{O}_v$.

证明 (1) 此时 $\mathfrak{P} = \mathfrak{p}B$. 根据共轭差积的定义,

$$\begin{aligned}\mathfrak{P} \mid \boldsymbol{D}(\mathcal{O}_w/\mathcal{O}_v) &\Leftrightarrow \mathrm{Tr}(\mathfrak{P}^{-1}) = \mathrm{Tr}(\mathfrak{p}^{-1}\mathcal{O}_w) \subset \mathcal{O}_v \\ &\Leftrightarrow \mathrm{Tr}(\mathcal{O}_w) \subset \mathfrak{p}\mathcal{O}_v \\ &\Leftrightarrow \text{ 有限域的迹映射} Tr : \mathcal{O}_w/\mathfrak{p}\mathcal{O}_w \to \mathcal{O}_v/\mathfrak{p} \text{ 是 } 0 \text{ 映射.}\end{aligned}$$

熟知最后一条是不对的, 所以 $\boldsymbol{D}(\mathcal{O}_w/\mathcal{O}_v)=(1)$. 注意到 $\mathrm{Tr}(\mathcal{O}_w)$ 总是 $\mathcal{O}_v$ 的非零理想从而 $\mathrm{Tr}(\mathcal{O}_w)=\mathcal{O}_v$.

(2) 记 M 是最大的 L_w/K_v 中间域使得 M/K_v 非分歧. 则 $e=[L_w:M]$. 设 M 的赋值环是 $\mathcal{O}$. 则 $\mathcal{O}$ 的极大理想是 $\mathfrak{p}\mathcal{O}$. 由上面引理 $\mathcal{O}_w=\mathcal{O}+\mathcal{O}\Pi+\cdots\mathcal{O}\Pi^{e-1}$. 我们断言当 $k\geq 1$ 时 $\mathrm{Tr}(\Pi^k)\in\mathfrak{p}$. 记 $\mathrm{Tr}_{L_w/M}$ 在 $B/\mathfrak{p}B$ 上诱导的迹映射为 T. 对 $\alpha\in\mathfrak{P}$, $\bar{\alpha}:=\alpha \bmod \mathfrak{p}B\in B/\mathfrak{p}B=B/\mathfrak{P}^eB$ 是幂零元, 所以 $T(\bar{\alpha})=0$. 换言之, $\mathrm{Tr}(\mathfrak{P})\subset\mathfrak{p}\mathcal{O}$. 特别的断言成立.

现在, $\mathrm{Tr}_{L_w/M}(1)=e\in\mathfrak{p}\mathcal{O}_M$ 当且仅当 $\mathfrak{p}\mid e$. 所以

$$\mathrm{Tr}_{L_w/M}(\mathcal{O}_w)\begin{cases}=\mathcal{O} & \text{当}\,\mathfrak{p}\nmid e,\\ \subset\mathfrak{p}\mathcal{O} & \text{当}\,\mathfrak{p}\mid e.\end{cases}$$

再利用 (1) 和迹的传递性 $\mathrm{Tr}_{L_w/K_v}=\mathrm{Tr}_{M/K_v}\circ\mathrm{Tr}_{L_w/M}$ 得所需结论.

证明 [定理2.10的证明] 当 $e=1$ 时, 这由命题2.8(1) 推出. 设 $e>1$. 则由上面命题知 $\mathrm{Tr}(\mathfrak{P})\subset\mathfrak{p}$ 所以 $\mathrm{Tr}(\mathfrak{p}^{-1}\mathfrak{P})=\mathrm{Tr}(\mathfrak{P}^{1-e})\subset\mathcal{O}_v$. 根据共轭差积的定义, 有 $\mathfrak{P}^{e-1}\mid\boldsymbol{D}(\mathcal{O}_w/\mathcal{O}_v)$. 进一步, 再根据命题2.8

$$\mathrm{Tr}(\mathfrak{P}^{-e})=\mathrm{Tr}(\mathfrak{p}^{-1}\mathcal{O}_w)=\mathfrak{p}^{-1}\mathrm{Tr}(\mathcal{O}_w)\begin{cases}=\mathfrak{p}^{-1} & \text{当}\,\mathfrak{p}\nmid e,\\ \subset\mathfrak{p}^{-1}\mathfrak{p}=\mathcal{O}_v & \text{当}\,\mathfrak{p}\mid e.\end{cases}$$

由此知 $\mathfrak{P}^e\mid\boldsymbol{D}(\mathcal{O}_w/\mathcal{O}_v)$ 当且仅当 $\mathfrak{p}\mid e$.

例 2.7 $K=\mathbb{Q}(\zeta_p)$ 时, $\boldsymbol{D}_K=(1-\zeta_p)^{p-2}$.

最后我们用这些理论来计算纯三次域的判别式和整基. 设 $K=\mathbb{Q}(\sqrt[3]{m})$, $m\in\mathbb{Z}$ 但不是立方数. K 称作是纯三次域. 显然我们可假设 $m=ab^2$, $a,b\in\mathbb{Z}_{\geq 1}$, a,b 互素且 a,b 均无平方因子. 设 $\alpha=\sqrt[3]{m}$, $\beta=\sqrt[3]{a^2b}=\frac{\alpha^2}{b}$.

命题 2.9

(1) 若 $m\not\equiv\pm 1 \bmod 9$, 则 K 一组整基是 $\{1,\alpha,\beta\}$, 判别式 $d_K=-27a^2b^2$.

(2) 若 $m\equiv\pm 1 \bmod 9$, 则 K 一组整基是 $\{\gamma,\alpha,\beta\}$, 判别式 $d_K=-3a^2b^2$, 其中 $\gamma=\frac{1+a\alpha+b\beta}{3}$.

证明 $1,\alpha,\alpha^2$ 的判别式等于 T^3-m 的判别式等于 $-27m^2$, 所以 $d_K<0$. 由此还知若 $p\nmid 3ab$, 则 p 非分歧. 特别的对这样的 p, 若 $v\mid p$, 则 $d_{K_v}=(1)$.

若 $p\mid a$ (若 $p\mid b$), 则 T^3-ab^2 (T^3-a^2b) 是 p-Eisenstein, 所以 p 完全分歧, 记为 $p\mathcal{O}_K=\mathfrak{p}^3$. 由 Eisenstein 多项式性质知 $\mathcal{O}_{\mathfrak{p}}=\mathbb{Z}_p[\alpha]$ ($\mathcal{O}_{\mathfrak{p}}=\mathbb{Z}_p[\beta]$). 总之

$$d_{K_{\mathfrak{p}}}=-27a^2b^2\mathbb{Z}_p=\begin{cases}3^5 & \text{当}\,p=3,\\ p^2 & \text{当}\,p\neq 3.\end{cases}.$$

故若 $3 \mid m$, 有

$$d_K = -3^3 a^2 b^2.$$

计算知

$$d(1, \alpha, \beta) = \frac{1}{b^2} d(1, \alpha, \alpha^2) = -27 a^2 b^2.$$

从而 $1, \alpha, \beta$ 是一组整基.

现在考虑 $3 \nmid m$ 的情形. 若 $m \not\equiv \pm 1 \bmod 9$, 则根据下面引理知, $T^3 - m$ 在 $\mathbb{Q}_3[T]$ 中不可约. 注意到 $(T \pm 1)^3 - m$ 是 3-Eisenstein 的, 所以 3 依旧完全分歧, 与上面一样的分析得想要结论.

若 $m \equiv \pm 1 \bmod 9$, 则有 $\mathbb{Z}_3[T]$ 中的不可约分解

$$T^3 - m = (T - \alpha)(T^2 + \alpha T + \alpha^2).$$

设 $\mathfrak{p}_1, \mathfrak{p}_2$ 是 K 的两个素位分别对应右边的两个多项式. 则 $K_{\mathfrak{p}_1} = \mathbb{Q}_3, K_{\mathfrak{p}_2} = \mathbb{Q}_3(\zeta_3)$. 于是 $\mathcal{O}_{\mathfrak{p}_1} = \mathbb{Z}_3, \mathcal{O}_{\mathfrak{p}_2} = \mathbb{Z}_3[\zeta_3]$. 所以

$$d_{K_{\mathfrak{p}_1}} = (1) \quad d_{K_{\mathfrak{p}_2}} = 3\mathbb{Z}_3.$$

那么当 $m \equiv 1 \bmod 9$ 时, 整合每个局部的判别式得

$$d_K = -3 a^2 b^2.$$

设 $\sigma_1, \sigma_2 \in \mathrm{Hom}(K, \overline{\mathbb{Q}}_3)$ 分别对应 $\mathfrak{p}_1, \mathfrak{p}_2$. 可不妨设 $\sigma_1(\alpha) = \alpha \in \mathbb{Z}_3, \sigma_2(\alpha) = \zeta_3 \alpha \in \mathbb{Z}_3[\zeta_3]$. 简单计算知 (下面 $+$ 对应 $+$, $-$ 对应 $-$)

$$m \equiv \pm 1 \bmod 9 \Rightarrow \alpha \equiv a \equiv \pm 1 \bmod 3.$$

由此

$$\sigma_1(1 + a\alpha + \alpha^2) \equiv 0 \bmod 3\mathbb{Z}_3, \quad \sigma_2(1 + a\alpha + \alpha^2) \equiv 1 + \zeta_3 + \zeta_3^2 \equiv 0 \bmod 3\mathbb{Z}_3.$$

这说明 $\sigma_i(\gamma) \in \mathcal{O}_{\mathfrak{p}_i} (i = 1, 2)$, 即 γ 在 $\mathfrak{p}_1, \mathfrak{p}_2$ 处的 (加法) 赋值是非负的, 而 γ 在其他素理想处的赋值显然是非负的, 所以 $\gamma \in \mathcal{O}_K$. 计算得

$$d(\gamma, \alpha, \beta) = \frac{1}{3^2} d(1, \alpha, \beta) = -3 a^2 b^2 = d_K.$$

这推出整基是 γ, α, β.

引理 2.5

$(\mathbb{Z}_3^\times)^3 = 1 + 9\mathbb{Z}_3 \times \{\pm 1\}$.

证明 习题.

第三章 阿代尔环与伊代尔群

设 K 是数域. 本章介绍 K 的阿达尔环 $\mathbb{A}_K$ 与伊代尔群 $\mathbb{A}_K^\times$. 我们将用两种方式来讲述, 第一种是从第一章理想语言所得到的结论来推导本节的主要结果. 另一种是讲述 < 数论 I> 的方式: 用局部紧群上的测度理论来建立主要结果, 由此再推导出第一章的主要结论. 这些颇为重要, 后面将看到

- $\mathbb{A}_K$ 上的 Fourier 分析会给出 K 的解析理论, 这是 Tate 博士论文的内容;
- 类域论会将 K 的极大 abel 扩张关于 K 的 Galois 群与所谓伊代尔类群 $\mathbb{A}_K^\times/K^\times$ 联系起来, 从而对伊代尔群有个好的认识会帮助我们了解 K 的 abel 扩张.

3.1 阿代尔与伊代尔的定义与拓扑

见数论 I, 第六节 a). 我们补充一点. (与书中类似, 紧和局部紧均指对 Hausdorff 空间.)

命题 3.1

$\mathbb{A}_K$ 和 $\mathbb{A}_K^\times$ 均是 Hausdorff 的局部紧群.

证明 一般的局部紧群的限制直积均是 Hausdorff 局部紧. 证明留作练习.

3.2 阿代尔与主阿代尔的关系

本小节用之前理想语言得到的结论来建立这些小标题中的关系.

定理 3.1. 强逼近定理

设 v_0 是 K 的任意素位. 则 K 在限制直积 $\prod'_{v\neq v_0} K_v$ 中稠密. 这里 v 跑遍 K 的不同于 v_0 的所有素位, 限制直积是对 $(K_v, \mathcal{O}_v)$ (当 v 有限时) 取的.

设 S 是 K 素位的有限集合且包含 K 的全部无穷素位. 定义 K 的 S-整数环

$$\mathcal{O}_S := \{x \in K : \mathrm{ord}_v(x) \geq 0 \text{ 对任意} v \notin S.$$

例 3.1 $K = \mathbb{Q}, S = \{p, \infty\}$. 则 $\mathcal{O}_S = \mathbb{Z}[\frac{1}{p}]$.

上面定理写成经典语言的话是:

定理 3.2. 强逼近定理'

设 S 是包含 K 所有无穷素位的有限集合. 任取 $v_0 \in S$, 记 $S' = S \setminus \{v_0\}$. 则 $\mathcal{O}_S$ 在 $\prod_{v\in S'} K_v$ 中稠密.

笔记 这里我详细写下定理3.1与定理3.2的等价性证明. (这纯属点集拓扑的简单讨论.)

定理3.1 "$\Rightarrow$ 定理3.2 ": 任意给定 $(a_v)_{v\in S'} \in \prod_{v\in S'} K_v$ 以及 $\epsilon > 0$. 定义 $\prod'_{v\neq v_0} K_v$ 中

元素

$$a = (a_v)_{v \neq v_0} = \begin{cases} a_v & 若 v \in S', \\ 0 & 若 v \notin S'. \end{cases}$$

在 $\prod'_{v \neq v_0} K_v$ 中取 a 的如下开邻域

$$U := \prod_{v \notin S} \mathcal{O}_v \times \prod_{v \in S} B(a_v, \epsilon), \quad 这里 B(a_v, \epsilon) = \{x \in K_v : |x - a_v|_v < \epsilon\}.$$

由定理3.1知, 存在 $x \in K \cap U$. 注意到 $K \cap U \subset \mathcal{O}_S$, 且当 $v \in S'$ 时 $|x - a_v|_v < \epsilon$. 这就证明了定理 3.2.

定理3.2 "⇒ 定理3.1 ": 任意给定 $a = (a_v)_{v \neq v_0} \in \prod'_{v \neq v_0} K_v$ 以及 a 的开邻域 U. 根据限制直积拓扑的定义, 我们可不妨设

$$U = \prod_{v \notin S} \mathcal{O}_v \times \prod_{v \in S, v \neq v_0} B(a_v, \epsilon),$$

其中 S 为包含全部无穷素位且不包含 v_0 的有限集合. 由定理3.2知, 存在 $x \in \mathcal{O}_S$ 使得当 $v \in S \setminus \{v_0\}$ 时, $x \in B(a_v, \epsilon)$. 注意到在 $\prod'_{v \neq v_0} K_v$ 中有 $x \in U$, 这就证明了定理3.1.

我们将对定理3.2给出证明. (下面这个引理可推广到一般 Dedekind 整环中).

引理 3.1

$\mathcal{O}_S$ 在 $\prod_{v \in S, v \nmid \infty} K_v$ 中稠密.

♡

证明 证明是个关于中国剩余定理的游戏. 细节如下: 记 $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$ 为 S 中有限素位的集合. 任意给定

$$(a_i)_i \in \prod_{i=1}^{r} K_{\mathfrak{p}_i} \quad 以及 \quad \epsilon > 0.$$

我们需证存在 $z \in \mathcal{O}_S$ 使得对每个 $i |z - a_i|_{\mathfrak{p}_i} < \epsilon$.

首先来说明存在 $x \in K$ 使得 $v_{\mathfrak{p}_i}(x) = v_{\mathfrak{p}_i}(a_i)$. 记 $k_i = v_{\mathfrak{p}_i}(a_i)$. 取 $\beta \in \mathfrak{p}_i^{|k_i|} \setminus \mathfrak{p}^{|k_i|+1}$. 根据中国剩余定理存在 $\alpha_i \in \mathcal{O}_K$ 满足

$$\alpha_i \equiv \beta \bmod \mathfrak{p}^{|k_i|+1},$$

$$\alpha_i \equiv 1 \bmod \mathfrak{p}_j, \ 对每个 j \neq i.$$

适当取 ± 号, 我们有 $\alpha := \prod_{i=1}^{r} \alpha_i^{\pm}$ 在每个 $\mathfrak{p}_j$ $(1 \leq j \leq r)$ 处的赋值都等于 k_j. 再次应用中国剩余定理知存在 $\gamma \in \mathcal{O}_K$ 使得对充分大的整数 N 成立

$$\gamma \equiv 0 \bmod \mathfrak{p}_i^N$$

$$\gamma \equiv 1 \bmod \mathfrak{p}_j \ 对每个 j \neq i.$$

则 $x := \gamma\alpha \in \mathcal{O}_S$ 就是所需元素.

特别的, $\frac{a_i}{x} \in \mathcal{O}_{\mathfrak{p}_i}^{\times}$. 再由中国剩余定理知存在 $y \in \mathcal{O}_K$ 使得, 对每个 $i = 1, 2, \cdots, r$ 以

及充分大的整数 N 有

$$y \equiv \frac{a_i}{x} \bmod \mathfrak{p}_i^N \mathcal{O}_{\mathfrak{p}_i}.$$

则

$$z := xy \in \mathcal{O}_S \quad \text{且对每个} i \text{ 有} \quad z - a_v \in \mathfrak{p}_i^{k_i+N} \mathcal{O}_{\mathfrak{p}_i}.$$

当 N 充分大时, 显然我们有 $|z-a_i|_{\mathfrak{p}_i} < \epsilon$ 对 $1 \le i \le r$ 成立. 这就说明了 z 是所需的逼近.

Minkowski 定理在如下的证明中起到了核心作用.

证明 [定理3.2的证明]

任意给定 $(a_v)_v \in \prod_{v\in S'} K_v$ 以及 $\epsilon > 0$. 我们需证明存在 $z \in \mathcal{O}_S$ 使得 $|z-a_v| < \epsilon$, $v \in S'$. 我们将先证两种特殊情形, 最后证一般情形. 设 $\mathcal{F}$ 是 $\prod_{v|\infty} K_v$ 关于格 $\mathcal{O}_K$ 的一个基本区域. 由于 $\mathcal{F}$ 有界, 可取 $M > 0$ 使得

$$\text{对任意} (f_v)_{v|\infty} \in \mathcal{F} \ \text{有} |f_v|_v \le M. \tag{3.2.1}$$

(1) 设 $S = \{$全体无穷素位$\}$, $v_0 \in S$. 此时 $\mathcal{O}_S = \mathcal{O}_K$. 应用 Minkowski 定理知存在 $x \in \mathcal{O}_K$ 使得

$$|x|_v < \frac{\epsilon}{M}, \quad \text{对每个} v \in S'.$$

任取 $a_{v_0} \in K_{v_0}$, 因为 $\mathcal{F}$ 是基本区域, 存在 $y \in \mathcal{O}_K$ 使得在 $\prod_{v\in S} K_v$ 中,

$$y - \frac{(a_v)_{v\in S}}{x} \in \mathcal{F}.$$

根据(3.2.1)有

$$|xy - a_v|_v = |x|_v |y - \frac{a_v}{x}|_v < \epsilon \quad \text{对每个} v \in S'.$$

那么 $z = xy \in \mathcal{O}_S$ 就是所需的逼近.

(2) 设 $S' = \{$全体无穷素位$\}$, v_0 是有限素位. 设 v_0 对应的素理想是 $\mathfrak{p}_0$. 由于类群有限, 故存在 $h \in \mathbb{Z}_{\ge 0}$ 使得 $\mathfrak{p}_0^h = (\pi)$, $\pi \in \mathcal{O}_K$. 则我们有

$$\mathcal{O}_S = \mathcal{O}_K[\pi^{-1}].$$

其中右边包含于左边是显然的; 反过来的包含是因为对任意 $\alpha\mathcal{O}_S$, 显然存在 $N \in \mathbb{Z}_{\ge 0}$ 使得 $\pi^N\alpha \in \mathcal{O}_K$. 设 $0 \ne \mathfrak{a} \subset \mathcal{O}_K$ 是整理想, 则对 $m \in \mathbb{Z}_{\ge 1}$, $\mathcal{O}_K$ 的分式理想 $(\pi^{-m})\mathfrak{a}$ 作为 $\prod_{v\in S'} K_v$ 中格的体积随着 m 增大时可任意小. 应用 Minkowski 定理知存在 $x \in \mathcal{O}_S$ 使得

$$|x|_v < \frac{\epsilon}{M} \quad \text{对每个} v \in S'.$$

取 $y \in \mathcal{O}_K$ 使得

$$y - \frac{(a_v)_{v\in S'}}{x} \in \mathcal{F}.$$

根据(3.2.1)有

$$|xy - a_v|_v = |x|_v |y - \frac{a_v}{x}|_v < \epsilon \quad \text{对每个} v \in S'.$$

那么 $z = xy \in \mathcal{O}_S$ 就是所需的逼近.

注意到在上面两种特殊情形的条件下, 我们实际上成立如下更强的事实

$$N\mathcal{O}_S \text{ 在 } \prod_{v\in S'}(NK_v) = \prod_{v\in S'} K_v \text{ 中稠密}, \quad N \text{ 任意正整数}.$$

(3) 一般情形: 由引理3.1知存在 $x \in \mathcal{O}_S$ 使得

$$|x - a_v|_v < \epsilon \quad \text{对每个} v \in S' \text{ 且} v \nmid \infty. \tag{3.2.2}$$

对 $N \in \mathbb{Z}_{\geq 1}$, 由前两种特殊情形的结论知存在 $y \in N\mathcal{O}_S$ 使得

$$|y - (x - a_v)|_v < \epsilon \quad \text{对每个} v \in S' \text{ 且} v \mid \infty. \tag{3.2.3}$$

若 v_0 是有限素位, 根据情形 (2); 若 v_0 是无穷素位, 这是由情形 (1) 的结论. 现在取 N 满足对每个素理想 $\mathfrak{p} \in S$, $\mathfrak{p}$ 的足够高次方整除 N, 结合(3.2.3)可知(3.2.3)中的不等式对 S' 中的有限素位也成立. 则 $z = x - y \in \mathcal{O}_S$ 就是所需的逼近.

命题 3.2

K 在 $\mathbb{A}_K$ 中离散且闭, $\mathbb{A}_K/K$ 紧.

证明 记 $K_\infty = \prod_{v|\infty} K_v$. 由强逼近定理易知

$$K + (\prod_{v\nmid\infty} \mathcal{O}_v \times K_\infty) = \mathbb{A}_K.$$

另外我们有显然的等式

$$K \cap (\prod_{v\nmid\infty} \mathcal{O}_v \times K_\infty) = \mathcal{O}_K.$$

所以包含映射诱导了如下自然的拓扑群同构

$$(\prod_{v\nmid\infty} \mathcal{O}_v \times K_\infty)/\mathcal{O}_K \cong \mathbb{A}_K/K.$$

设 $\mathcal{F}$ 是 $\prod_{v|\infty} K_v$ 关于格 $\mathcal{O}_K$ 的基本区域, 记 $\overline{\mathcal{F}}$ 为其闭包. 显然有连续的自然满射

$$\prod_{v\nmid\infty} \mathcal{O}_v \times \overline{\mathcal{F}} \to (\prod_{v\nmid\infty} \mathcal{O}_v \times K_\infty)/\mathcal{O}_K.$$

前者作为紧空间的乘积是紧, 从而后者也是紧的. K 在 $\mathbb{A}_K$ 中的离散性由 $\mathcal{O}_K$ 在 $\prod_{v|\infty} K_v$ 中的离散性得出. (根据一般拓扑群的结论知 K 在 $\mathbb{A}_K$ 中闭).

推论 3.1

设 S 为 K 素位的有限集合且包含 K 所有无穷素位. 则 $\mathcal{O}_S$ 在 $\prod_{v\in S} K_v$ 下的像离散且余紧.

证明 由于 $\mathcal{O}_S$ 是群, 我们只需证明 $0 \in \mathcal{O}_S$ 在 $\prod_{v\in S} K_v$ 中离散. 对 $v \in S$, 设 $U_v \subset K_v$ 是 $0 \in K_v$ 的一个紧邻域. 则 U 是 0 在 $\mathbb{A}_K$ 中的紧邻域, 这里

$$U = \prod_{v\in S} U_v \times \prod_{v\notin S} \mathcal{O}_v.$$

由于 K 在 $\mathbb{A}_K$ 中闭, 所以 $K \cap U$ 紧且离散, 故而有限. 显然 $x \in K \cap U$ 当且仅当

$x \in \mathcal{O}_S \cap \prod_{v\in S} K_v$, 所以 $\mathcal{O}_S$ 在度量空间 $\prod_{v\in S} K_v$ 中离散. 由于

$$K + \prod_{v\notin S} \mathcal{O}_v \times \prod_{v\in S} K_v = \mathbb{A}_K,$$

故

$$(\prod_{v\notin S} \mathcal{O}_v \times \prod_{v\in S} K_v)/\mathcal{O}_S \cong \mathbb{A}_K/K \text{ 紧}.$$

利用如下自然投射知后者紧

$$(\prod_{v\notin S} \mathcal{O}_v \times \prod_{v\in S} K_v)/\mathcal{O}_S \to (\prod_{v\in S} K_v)/\mathcal{O}_S.$$

例 3.2 (1) $\mathbb{Z}$ 在 $\mathbb{R}$ 中离散且余紧.

(2) $\mathbb{Z}[\frac{1}{p}]$ 在 $\mathbb{R}\times\mathbb{Q}_p$ 中离散且余紧, 但分别在 $\mathbb{R}$ 和 $\mathbb{Q}_p$ 中稠密.

3.3 伊代尔与主伊代尔的关系

对 K_v 上的绝对值, 我们首先需要选择所谓" 标准" 绝对值 $|\cdot|_{K_v}$, 也简记作 $|\cdot|_v$. 若 v 是有限素位对应素理想 $\mathfrak{p}$, (仿照 < 数论 I>) 用 ord_v 来表示加法赋值 $v_{\mathfrak{p}}$, 记 q_v 是 K_v 剩余类域的阶. 定义

$$|x|_{K_v} = \begin{cases} q_v^{-\mathrm{ord}_v(x)} & \text{若} v \text{ 有限;} \\ \text{通常绝对值} & \text{若} K_v = \mathbb{R}; \\ x\bar{x} & \text{若} K_v = \mathbb{C}. \end{cases}$$

在阿代尔上定义绝对值 $\cdot|_{\mathbb{A}_K}$ (也简记为 $|\cdot|$):

$$|\cdot|_{\mathbb{A}_K} : \mathbb{A}_K \to \mathbb{R}_{\geq 0}, \quad a = (a_v)_v \mapsto \prod_v |a_v|_{K_v}.$$

由于对几乎所有的 v, $a_v \in \mathcal{O}_v$ 即 $|a_v|_{K_v} \leq 1$, 故上面乘积收敛. 如果 $(a_v)_v$ 是个伊代尔, 则对几乎所有的 v, $|a_v|_{K_v} = 1$, 故 $|(a_v)_v|_{\mathbb{A}_K}$ 是有限乘积.

命题 3.3. 乘积公式

若 $x \in K^\times$, 则 $|x|_{\mathbb{A}_K} = 1$.

证明 当 $K = \mathbb{Q}$ 时, 直接验证即可得结论. 一般情形显然由如下等式推出

$$|x|_{\mathbb{A}_K} = |N_{K/\mathbb{Q}}(x)|_{\mathbb{A}_{\mathbb{Q}}}. \tag{3.3.1}$$

为证(3.3.1), 只要说明对每个素位 v, 当 $x \in K_v$ 时成立如下等式

$$\prod_{v|p} |x|_v = |N_{K/\mathbb{Q}}(x)|_p.$$

这里 p 是 $\mathbb{Q}$ 的 v 之下的素位. 当 v 是无限素位时, 上式由范的基本性质推出. 以下设 v 是有限素位. 根据赋值理论知

$$N_{K/\mathbb{Q}}(x) = \prod_{v|p} N_{K_v/\mathbb{Q}_p}(x).$$

所以我们只需证明

$$|N_{K_v/\mathbb{Q}_p}(x)|_p = |x|_v.$$

对当 $\operatorname{ord}_v(x) = 1$ 时, (右边的事实见练习) $\operatorname{ord}_p(N_{K_v/\mathbb{Q}_p}(x)) = f(v/p)$. 利用 $q_v = p^{f(v/p)}$ 知对这样的 x 上面公式成立时, 利用乘性知对任意 $x \in K_v$ 上式也成立. 这就证明了(3.3.1).

令

$$\mathbb{A}_K^1 = \{a \in \mathbb{A}_K^\times : |a|_K = 1.\}$$

给 $\mathbb{A}_K^1$ 赋予 $\mathbb{A}_K^\times$ 的子拓扑. 命题3.3证明了 $K^\times \subset \mathbb{A}_K^1$.

定理 3.3

$K^\times$ 在 $\mathbb{A}_K^1$ 中离散且 $\mathbb{A}_K^1/K^\times$ 紧.

为证明这个定理, 定义映射 (回忆 I_K 表示 K 的分式理想群):

$$\mathbb{A}_K^\times \to I_K, \quad (a_v)_v \mapsto \prod_{v\nmid\infty} \mathfrak{p}_v^{\operatorname{ord}_v a_v}.$$

(闲谈: 由这个映射可看出伊代尔是 (分式) 理想的" 加细", 这正是名称 idéle = ideal element 的由来). 记其核为 U_K, 则

$$U_K = \prod_{v\nmid\infty} \mathcal{O}_v^\times \times \prod_{v\mid\infty} K_v^\times. \tag{3.3.2}$$

显然 I_K 的子群主分式理想群的逆像是 $K^\times U_K$, 这诱导了同构

$$\mathbb{A}_K^\times/U_K K^\times \cong \mathrm{Cl}_K.$$

引理 3.2

记 $U_K^1 = U_K \cap \mathbb{A}_K^1$. 则自然嵌入 $\mathbb{A}_K^1 \subset \mathbb{A}_K^\times$ 诱导了同构

$$\mathbb{A}_K^1/K^\times U_K^1 \cong \mathbb{A}_K^\times/U_K K^\times.$$

特别的, $\mathbb{A}_K^1/K^\times U_K^1$ 同构于类群从而是有限群.

证明 利用 $K^\times \subset \mathbb{A}_K^1$, 我们得出 $\mathbb{A}_K^1 \cap U_K K^\times = U_K^1 K^\times$. 所以只需证明

$$\mathbb{A}_K^1 U_K = \mathbb{A}_K^\times.$$

设 $a \in \mathbb{A}_K^\times$. 取一个无穷素位 v, 令

$$b = (1, \cdots, 1, b_v, 1, \cdots, 1) \in U_K \quad \text{使得} |b_v|_v = |a|_K.$$

则 $|b|_K = |a|_K$. 故 $ab^{-1} \in \mathbb{A}_K^1$ 从而 $a = (ab^{-1})b \in \mathbb{A}_K^1 U_K$. 这就证明了上面的等式.

证明 [定理3.3的证明]

记

$$K_\infty = \prod_{v\mid\infty} K_v, \quad K_\infty^1 = \{(x_v)_v \in K_\infty : \prod_{v\mid\infty} |x_v|_v = 1\}.$$

则
$$\left(\prod_{v\nmid\infty}\mathcal{O}_v^\times\times K_\infty\right)\cap K^\times=\left(\prod_{v\nmid\infty}\mathcal{O}_v^\times\times K_\infty^1\right)\cap K^\times=\mathcal{O}_K^\times.$$
从而有拓扑 abel 群的正合列:
$$1\to(\prod_{v\nmid\infty}\mathcal{O}_v^\times\times K_\infty^1)/\mathcal{O}_K^\times\to\mathbb{A}_K^1/K^\times\to\mathbb{A}_K^1/U_KK^\times\to 1.$$
因为类数有限, 故右边是有限群. 所以若能证明左边是紧群就行了. 考虑正合列
$$1\to\prod_{v\nmid\infty}\mathcal{O}_v^\times\to(\prod_{v\nmid\infty}\mathcal{O}_v^\times\times K_\infty^1)/\mathcal{O}_K^\times\to K_\infty^1/\mathcal{O}_K^\times\to 1.$$
右边的箭头由 $(a_v)_v\to(a_v)_{v|\infty}$ 诱导. 左边是紧的, 右边紧是因为 Dirichlet 单位定理, 从而中间一项也是紧的.

3.4 Haar 测度