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

1 整数环以及理想 **1**

1.1 Kronecker-Weber 定理 1

1.2 类域论介绍 4

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 $\alpha = \gamma^p, \gamma \in \mathcal{O}_F$, 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 $v_{(\pi)}(\alpha) = 0$. 利用 $[L : \mathbb{Q}] = p^- p$ 知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 $\sigma(\sqrt[p]{\alpha}) = \zeta\sqrt[p]{\alpha}$, $\zeta \neq 1$ 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 $\alpha \equiv 1 \bmod \pi$. 根据上面引理, 取 $\alpha = \zeta_p^a\beta$ 且 $\beta \equiv 1 \bmod \pi^2$. 则存在 $c \in \mathbb{Z}$, $p \nmid c$, $m \geq 2$ 使得

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

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

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

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

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

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

$$\beta \equiv 1 \bmod \pi^p.$$

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

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

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

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. $I_K^\mathfrak{m} = I_K$, $K_{\mathfrak{m},1} = K^+ := \{\alpha \in K : \sigma(\alpha) > 0, \text{对每个实嵌入} \sigma\}$, 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 Frobenius 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:

$$\begin{array}{ccc} \mathrm{Cl}(\mathbb{Q}, N\infty) & \xrightarrow{\cong} & (\mathbb{Z}/N\mathbb{Z})^\times \\ & \overset{\psi_{\mathbb{Q}(\zeta)/\mathbb{Q}}}{\searrow^{\cong}} & \downarrow{\scriptstyle\cong} \\ & & \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \end{array}$$

$$\begin{array}{ccc} \mathrm{Cl}(\mathbb{Q}, N) & \xrightarrow{\cong} & (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\} \\ & \overset{\psi_{\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}}}{\searrow^{\cong}} & \downarrow{\scriptstyle\cong} \\ & & \mathrm{Gal}(\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}) \end{array}$$

- 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, 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

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.

参考文献