代数数论讲义

李加宁
中国科学技术大学

日期：2021 年 4 月 8 日

1 第一讲 (2021,03,08) 数域和代数整数环

本课程以自编讲义为主, 主要参考书目：冯克勤-代数数论. Neukrich-代数数论. 加藤和也(等)-数论 I.

注: 相比今日课堂内容, 我以 $\mathbb{Z}$ 为例增加了一些欧几里得环、主理想整环、唯一分解整环的内容. 虽然这些内容在不同阶段如小学、中学、大学抽象代数课上都可能接触过, 在这里温顾一下对学习代数数论以及课程的自封闭性是有好处的. 对于后面的课程, 我建议去温习代数学中的有限生成 *abel* 群结构定理.

我们从整数环 $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$ 说起. 一个大于等于 2 的整数的正因子只有 1 和其本身的话, 称其为**素数**. 我们来回顾所谓算术基本定理及其证明:

简记: 主理想整环 = PID (Principal Ideal Domain). 唯一分解整环 = UFD (Unique Factorization Domain)

定理 1.1. *(1) (带余除法) 对任意整数 $a, b \in \mathbb{Z}$, $b \neq 0$, 存在 $q, r \in \mathbb{Z}$, $0 \leq r \leq b-1$, 使得 $a = qb + r$. ($\mathbb{Z}$ 是欧几里得环.)*

(2) ($\mathbb{Z}$ 是 PID) 环 $\mathbb{Z}$ 的每个理想都是主理想.

(3) ($\mathbb{Z}$ 是 UFD) 每个正整数都能唯一的写成素数的乘积.

证明. (1) 先设 $b > 0$. 因 a/b 是有理数, 存在 $q \in \mathbb{Z}$ 使得 $q \leq a/b < q+1$, 令 $r = b(a/b - q) = a - bq$, 则 r, q 即是所需; 若 $b < 0$, 取 q 使得 $q - 1 \leq a/b \leq q$ 即可.

(2) 设 I 是 $\mathbb{Z}$ 的非零理想, 在 $I \setminus \{0\}$ 中, 取 $0 < b \in I$ 使得其绝对值 $|b|$ 最小. 则 $I = (b)$, 这是因为任意 $a \in I$, 由带余除法知存在 q, r, $0 \leq r < b$ 使得 $a = qb + r$, 即 $r \in I$. 根据 b 的极小性, 知 $r = 0$, 从而 $a = qb \in (b)$. 这说明了 $I = (b)$ 是主理想.

(3) 存在性: 设 $n \in \mathbb{Z}_{>0}$, 若 n 不可分解, 则无需证; 否则 n 可继续分解, 我们需证明 n 进过有限步后, n 分解成了素数的乘积. 反证法, 若任意有限步分解不能停止, 我们将得到一个无限的理想升链:

$$(n) \subsetneq (n_1) \subsetneq (n_2) \subsetneq \cdots$$

另一方面, 这些理想的并 $\cup(n_i)$ 也是 $\mathbb{Z}$ 的理想, 那么它是主理想 (d), 且对某个 k 有 $d \in (n_k)$, 这就说明这个升链是有限的, 矛盾.

唯一性: 容易看出唯一性由如下重要结论推出: 若 $p \mid ab$, $a, b \in \mathbb{Z}$, 则 $p \mid a$ 或 $p \mid b$. 换句话说 $(p) = p\mathbb{Z}$ 是 $\mathbb{Z}$ 的素理想.

现在我们来证明这个性质. 考虑理想 (p,a), 根据 (2), $(p,a)=(d)$, $d\in\mathbb{Z}$. 由素数的定义看出 (d) 只能等于 (1) 或 (p), 若 $(p,a)=(p)$ 即 $p\mid a$, 这是我们想要的. 若 $(p,a)=(1)$, 即存在 $x,y\in\mathbb{Z}$ 使得 $px+ay=1$, 两边同乘 b 得 $pxb+aby=b$. 由于 $p\mid ab$, 我们就得到了 $p\mid b$. □

回顾整环中不可约元、素元、欧几里得环、主理想整环、唯一分解整环等基本定义. 请确信以上讨论实际上证明了

$$\{\text{欧几里得环}\}\subset\{\text{主理想整环}\}\subset\{\text{唯一分解整环}\}.$$

思考题: 试举例说明以上两个包含号实为真包含.

习题: 证明在 UFD 中, 不可约元和素元是一回事. (回忆所谓素元指其生成的主理想为素理想.)

引理 1.2. *设 R 是 UFD, $\alpha,\beta\in R$ 且没有非平凡公因子. 若 $\alpha\beta=\gamma^n$, 则存在 $u,v\in R^\times$, $x,y\in R$, 使得 $\alpha=ux^n,\beta=vy^n$.*

证明. 将 $\alpha\beta=\gamma^n$ 左右两端都分解为不可约元的乘积, 再利用分解的唯一性即可看出. □

接下来, 我们从解一个整数不定方程谈起

$$y^2+1=x^3. \tag{1.1}$$

若以代数数论方法来看, 在环 $\mathbb{Z}[i]$ 中, 可将左端分解为 $(x+i)(x-i)$, 这里 $i=\sqrt{-1}$. 若用此法, 我们需了解环 $\mathbb{Z}[i]$ 的性质. 实际上 $\mathbb{Z}[i]$ 是欧几里得整环. 环中任一元素 α 均可写为 $a+bi(a,b\in\mathbb{Z})$ 的形状 (为什么?). $\mathbb{Z}[i]$ 的分式域是 $\mathbb{Q}(i)$. 我们定义 $\mathbb{Q}(i)$ 上的范数:

$$N:\mathbb{Q}(i)\to\mathbb{Q},\quad x+yi\mapsto x^2+y^2.$$

容易验证,$N(\alpha\beta)=N(\alpha)N(\beta)$ 对任意 $\alpha,\beta\in\mathbb{Q}(i)$. 现在我们来说明 N 限制在 $\mathbb{Z}[i]$ 上 (仍记作 N) 会使 $\mathbb{Z}[i]$ 成为一个欧几里得整环. 即存在带余除法: 对任意 $\alpha,0\neq\beta\in\mathbb{Z}[i]$, 存在 $\gamma,\delta\in\mathbb{Z}[i]$ 使得

$$\alpha=\beta\gamma+\delta \text{ 且} 0\le N(\delta)<N(\beta).$$

证明. $\mathbb{Z}[i]$ 的分式域 $\mathbb{Q}(i)$. 记 $\alpha/\beta=m+ni,m,n\in\mathbb{Q}$. 对有理数 q, 我们令 $[q]'$ 为距离 q 最近的整数, 则 $q:=q-[q]'$ 的绝对值小于等于 $1/2$. 则 $\alpha/\beta=([m]'+[n]'i)+(m+ni)$ 且 $N(m+ni)\le 1/2$. 令 $\gamma=[m]'+[n]'i\in\mathbb{Z}[i]$, $\delta=\beta(m+ni)$, 则 $N(\delta)=N(\beta)N(m+ni)<N(\beta)$. □

所以 $\mathbb{Z}[i]$ 也是 PID 和 UFD. 环 $\mathbb{Z}[i]$ 的单位群亦重要, 若 $\alpha=a+bi$ 是单位, 显然 $\bar\alpha:=a-bi$ 也是, 故 $N(\alpha)=\alpha\bar\alpha=a^2+b^2$ 也是单位, 这推出 $N(\alpha)=\pm1$. 由此易知 $\mathbb{Z}[i]^\times=\{1,-1,i,-i\}=\langle i\rangle\cong\mathbb{Z}/4\mathbb{Z}$.

现在我们可以来证明方程(1.1)的整数解只有 $(x,y)=(1,0)$ 了. 假设 (x,y) 是一组整数解, 则在 $\mathbb{Z}[i]$ 中有

$$(y+i)(y-i)=x^3 \tag{1.2}$$

利用自然环同态 $\mathbb{Z}\to\mathbb{Z}/4\mathbb{Z}$, 即模 4 看, 知 $2\mid x,2\nmid y$. 由此知 $(y+i,y-i)$ 生成的理想为 1, 因为 y^2+1 和 2 都属于这个理想, 故 1 也属于这个理想 (这里我们利用了环 $\mathbb{Z}$ 是 PID). 那么 $y+i$ 和 $y-i$ 在 $\mathbb{Z}[i]$ 中没有公因子, 再利用 $\mathbb{Z}[i]$ 是唯一分解环, 由引理1.2和(1.2)得出 $y+i$ 等于一个单位乘以一

个元素的立方, 由于 $\mathbb{Z}[i]$ 中的单位均可写成某个单位的立方, 我们可以得出存在 $\alpha = a+bi \in \mathbb{Z}[i]$ $(a, b \in \mathbb{Z})$ 使得 $y + i = (a + bi)^3$. 由此比较 i 的系数会得出 $(x, y) = (1, 0)$.

总结: 在整个论证过程中, $\mathbb{Z}[i]$ 是 PID 以及对于它单位群的了解都起了重要的作用.

现考虑另一方程的整数解,

$$y^2 + 5 = x^3. \tag{1.3}$$

将左边在 $\mathbb{Z}[\sqrt{-5}]$ 中分解为 $(y + \sqrt{-5})(y - \sqrt{-5})$. 容易计算环 $\mathbb{Z}[\sqrt{-5}]$ 的单位群是 $\{\pm 1\}$ (习题). 但这时会碰到一个麻烦的问题, 上面证明 $\mathbb{Z}[i]$ 是 PID 的关键一步: 构造" 适当的范数 N 作带余除法" (请同学们在此先作尝试) 在 $\mathbb{Z}[\sqrt{-5}]$ 中将不复存在. 实际上 $\mathbb{Z}[\sqrt{-5}]$ 根本就不是 UFD, 比如 6 就有两种分解为不可约元的方法 (请自行验证 $2, 3, 1 \pm \sqrt{-5}$ 均为不可约元, 且均不是素元):

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

然所幸, $\mathbb{Z}[\sqrt{-5}]$ 这个环有下面两个非常好的性质最终能帮助我们解上面的方程（我们将在两周后证明这两个事实):

(1) $\mathbb{Z}[\sqrt{-5}]$ 中任何一个非零理想都可以唯一地分解为素理想的乘积; 举例而言: $(6) = 6\mathbb{Z}[\sqrt{-5}]$ 的素理想分解式为

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

(验证右边的这三个理想都是极大理想.)

若不熟悉理想的运算, 请看 Atiyah-Macdonad 交换代数导引第一章.

由这条性质可推出, 如果两个理想 I_1, I_2 互素 (即 $I_1 + I_2$ 是单位理想) 且 $I_1 I_2$ 是某个理想的 n 次方, 则 $I_i (i = 1, 2)$ 自身也是某个理想的 n 次方.

(2) 对 $\mathbb{Z}[\sqrt{-5}]$ 中的任一理想 I, I^2 都是主理想.

利用这条性质, 我们可得出如果一个理想 I 的立方是主理想, 那么 I 本身就是主理想. (见习题) 有这两样性质后, 我们变可证明 $y^2 + 5 = x^3$ 没有整数解, 留作练习.

环 $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-5}]$ 是我们将要讲述的代数整数环的例子, 它们的分式域分别是 $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-5})$. 这样的域是 $\mathbb{Q}$ 的有限扩张. 一般地, 有理数域的有限扩张称为 (代数) 数域.

定义 1.3. (1) 如果 $\alpha \in \mathbb{C}$ 是某个首一整系数多项式的根, 我们称 α 是代数整数. 全体代数整数形成的环我们记作 $\bar{\mathbb{Z}}$. (我们将很快看到这的确是个环)

(2) 设 K 是数域, K 的 (代数) 整数环 $\mathcal{O}_K$ 指 K 中所有代数整数所构成的环. (我们将很快看到这的确是个环)

在前两周的课程中, 我们的任务是学习 $\mathcal{O}_K$ 这个环的性质, 就像我们去了解 $\mathbb{Z}[i], \mathbb{Z}[\sqrt{-5}]$ 那样.

例如: $\sqrt{2}, \zeta_N = e^{2\pi i/N}$ 均是代数整数, 因它们分别是 $x^2 - 2, x^N - 1$ 的根. 由定义看, 一个不太显然的事实是 $\sqrt{2} + e^{2\pi i/N}$ 也是代数整数.

任何 $\mathbb{Q} \setminus \mathbb{Z}$ 中的数都**不是**代数整数,(这从定义初始也并不算很明显.)

可将代数整数的概念推广到如下一般情形:

定义 1.4. 设 $R \subset S$ 是两个交换环, 对于 $\alpha \in S$, 如果存在首一多项式 $f(T) \in R[T]$ 使得 $f(\alpha) = 0$, 我们称 α 在 R 上整. 如果 S 的每个元素均在 R 上整, 称 S 在 R 上整.

所谓 R 在 S 中的整闭包, 顾名思义, 即指 S 中全体在 R 上整的元素所成之集合, 马上将看到这个整闭包是 S 的子环. 若 R 是整环, 记 $F(R)$ 为 R 的分式域, 如果 R 在 $F(R)$ 中的整闭包是 R 自身, 我们称 R 是整闭的.

考虑环 $\mathbb{Z} \subset \mathbb{C}$, 则 $\alpha \in \mathbb{C}$ 是代数整数可重新表述为 α 在 $\mathbb{Z}$ 上整,$\bar{\mathbb{Z}}$ 即是 $\mathbb{Z}$ 在 $\mathbb{C}$ 中的整闭包. 若 K 是数域, 其整数环 $\mathcal{O}_K$ 就是 $\mathbb{Z}$ 在 K 中的整闭包.

如下论断和证明与课堂所讲并无任何本质差别, 这里写成一般的情形为方便以后使用

命题 1.5. *设 $R \subset S$ 是两个交换环. 设 $\alpha \in S$, 则以下两条等价: (1) α 在 R 上整; (2) $R[\alpha]$ 的是有限生成的 R-模;*

证明. "(1) 推 (2)": 设 α 是 $T^n + a_{n-1}T^{n-1} + \cdots a_0 \in R[T]$ 的根, 则 α^n 可由 $1, \alpha, \cdots, \alpha^{n-1}$ 作为 R-模生成, 归纳可知对任何正整数 m, $\alpha^m \in R + R\alpha + \cdots R\alpha^{n-1}$. 从而 $R[\alpha]$ 可由 $1, \alpha, \cdots, \alpha n - 1$ 作为 R-模生成.

"(2) 推 (1)": 设 $\alpha_1, \cdots, \alpha_n$ 是 $R[\alpha]$ 的一组 R-模生成元. 则存在 R 上的 n 阶矩阵 A 使得 $\alpha(\alpha_1, \cdots, \alpha_n = (\alpha_1, \cdots, \alpha_n)A$. 则 $\alpha I_n - A$, (作为 $R[\alpha]$ 上的矩阵), 有 $(\alpha_1, \cdots, \alpha_n)(\alpha I_n - A) = 0$. 右乘 $\alpha I_n - A$ 的伴随矩阵知每个 α_i 被行列式 $|\alpha I_n - A| \in R[\alpha]$ 零化, 特别的 $1 \in R[\alpha]$ 被其零化, 故 $|\alpha I_n - A| = 0$, 故 α 是首一多项式 $|TI_n - A| \in R[T]$ 的根. 也就是说, α 在 R 上整.

□

推论. *(1) 设 $R \subset S$, 则 R 在 S 中的整闭包是 S 的子环.*

(2)(整的传递性) 设 $R_1 \subset R_2 \subset R_3$, 若 $\alpha \in R_3$ 在 R_2 上整, 而 R_2 在 R_1 上整, 则 α 在 R_1 上整.

证明. (1) 只需证明若 $\alpha, \beta \in S$ 在 R 上整, 则 $\alpha + \beta, \alpha\beta$ 也在 R 上整. 注意到 $R[\alpha, \beta]$ 是有限生成的 R-模即可, 它可由 $\alpha^i\beta^j$ $0 \le i \le n, 0 \le j \le m$ 生成, 这里 n 和 m 分别是零化 α,β 的首一多 R-系数项式的次数.

(2) 由条件知存在首一多项式 $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in R_2[T]$ 使得 $f(\alpha) = 0$. 故 α 在 $R_1[a_0, a_1, \cdots, a_{n-1}]$ 上整, 又由于 a_i 在 R_1 上整, 知 $R_1[a_0, a_1, \cdots, a_{n-1}]$ 是有限生成的 R_1-模, 设生成元是 $\alpha_1, \cdots, \alpha_m$, 则 $R_1[a_0, a_1, \cdots, a_{n-1}, \alpha]$ 作为 R_1-模可由 $c^i\alpha_j$ $(0 \le i \le n-1, 1 \le j \le m)$ 生成. □

命题 1.6. *$\mathbb{Z}$ 是整闭的, 换句话说 $\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. 更一般地, UFD 都是整闭的.*

证明. (我们以 $\mathbb{Z}$ 来证) 设 $r/s \in \mathbb{Q}$, 其中 $r, s \in \mathbb{Z}$, 且 r, s 无非平凡公因子, 若 r/s 在 $\mathbb{Z}$ 上整, 则存在首一整系数多项式 $f(T) = T^n + a_{n-1}T^{n-1} + \cdots a_0 \in \mathbb{Z}[T]$ 使得有等式 $f(r/s) = 0$. 在此式两边同乘 s^n, 得

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_0s^n = 0$$

若 $r/s \notin \mathbb{Z}$, 则存在一素数 p 使得 $p \mid s$, 则由上面式子知 p 将整除 r^n, 故而 $p \mid r$. 这与 r, s 没有公因子矛盾.

请确信这个证明原封不动的适用于论断: UFD 是整闭的. □

引理 1.7 (Gauss 引理)**.** *设 $f(T) \in \mathbb{Z}[T]$ 是首一整系数多项式, 则 $f(T)$ 在 $\mathbb{Q}[T]$ 中不可约当且仅当在其在 $\mathbb{Z}[T]$ 中不可约.*

这显然能推出: 若 $\alpha \in \bar{\mathbb{Z}}$, α 在 $\mathbb{Q}$ 上的首一极小多项式是整系数的.

证明. 设 $f(T)$ 在 $\mathbb{Q}[T]$ 可约, 记其分解式为 $f(T) = g(T)h(T)$, $g(T), h(T) \in \mathbb{Q}[T]$ 且首一我们需证明 $g(T), h(T) \in \mathbb{Z}[T]$. $g(T)$ 的根也是 $f(T)$ 的根, 所以都是代数整数, 而 $g(T)$ 的各项系数为一些代数整数的加和乘, 故仍是代数整数, 又 $g(T) \in \mathbb{Q}[T]$. 根据 $\mathbb{Z}$ 在 $\mathbb{Q}$ 中整闭得出 $g(T) \in \mathbb{Z}[T]$. 整闭. □

下节课中, 我们来证明所谓的整基存在性定理:

命题 1.8. *设 K 是数域, 则 $\mathcal{O}_K$ 的加法群是秩为 $n = [K : \mathbb{Q}]$ 的自由 abel 群.*

2 第二讲 (2021,03,10): 整数环 $\mathcal{O}_K$ 的性质, Dedekind 整环

本节课的目标是证明整基的存在性, 即命题1.8. 在我们回顾一些有限可分扩张的知识后, 我们将其应用到 $K/\mathbb{Q}$ 上, 证明将是水到渠成且对计算整基也有一定的启发性.

2.1 回顾有限可分扩张的基本性质

设 L/K 是一般域的有限可分扩张, 记 $n = [L : K]$ 是扩张次数. 设 $\bar{K}$ 为 K 的一个代数闭域, 令

$$\mathrm{Hom}_K(L, \bar{K}) = \{\sigma : L \hookrightarrow \bar{K} \text{ 是域嵌入} : \sigma|_K = \mathrm{id}\}.$$

我们有 $\#\mathrm{Hom}_K(L, \bar{K}) = n$. 任意的 $\alpha \in L$ 通过左乘诱导了 L 上的线性变换 $\mathcal{A}_\alpha$, 即

$$\mathcal{A}_\alpha : L \to L, \quad x \mapsto \alpha x.$$

记 α 在 K 上的极小多项式为 $f(T) = T^d + a_{d-1}T^{d-1} + \cdots a_0$。由域论知

$$f(T) = \prod_{\sigma \in \mathrm{Hom}_K(K(\alpha), \bar{K})} (T - \sigma(\alpha)).$$

易见子域 $K(\alpha) \subset L$ 实际上是 $\mathcal{A}_\alpha$ 的不变子空间, 而 $f(T)$ 是 $\mathcal{A}_\alpha$ 限制在 $K(\alpha)$ 上的特征多项式. 分别记 $\mathrm{char}_{L/K}(\alpha)$, $\mathrm{Tr}_{L/K}(\alpha)$, $N_{L/K}(\alpha)$ 为线性变换 $\mathcal{A}_\alpha$ 的特征多项式, 迹, 范数, 则

$$\mathrm{char}_{L/K}(\alpha) = \prod_\sigma (T - \sigma(\alpha)) = f(T)^{n/d},$$

$$\mathrm{Tr}_{L/K}(\alpha) := \sum_\sigma \sigma(\alpha) = \frac{n}{d}(-a_{d-1}),$$

$$N_{L/K}(\alpha) = \prod_\sigma \sigma(\alpha) = (-1)^n a_0^{n/d}.$$

在上面的求和与求积号中,σ 都跑遍 $\mathrm{Hom}_K(L, \bar{K})$.

迹 Tr 还诱导了 L 上的双线性映射:

$$\langle , \rangle : L \times L \to K, \quad (\alpha, \beta) \mapsto \mathrm{Tr}_{L/K}(\alpha\beta).$$

这个双线性配对是非退化的, 根据线性代数, 这等价于说这个双线性配对在一组基（从而在任意一组基）下的度量矩阵的行列式非零. 下面说明此配对是非退化的.

若 $\alpha_1,\cdots,\alpha_n$ 是 L 的一组 K-基, 则由上面的公式知 $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)=\sum_\sigma \sigma(\alpha_i)\sigma(\alpha_j)$. 由此得到如下度量矩阵的分解. 记 $\mathrm{Hom}_K(L,\bar{K})=\{\sigma_1,\cdots,\sigma_n\}$, 则

$$(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{i,j}=(\sigma_i(\alpha_j)_{i,j}(\sigma_i(\alpha_j)_{i,j})^t. \quad \text{右上角的}t\text{ 表示矩阵转置.}$$

熟知有限可分扩张为单扩张, 即存在 $\theta\in L$ 使 $L=K(\theta)$, 那么 $1,\theta,\cdots,\theta^{n-1}$ 为 K-线性空间 L 的一组基. 通过计算一个范德蒙德行列式, 我们知配对 $\langle,\rangle$ 在这组基下的度量矩阵的行列式等于

$$\prod_{i\neq j}(\sigma_i(\theta)-\sigma_j(\theta))^2.$$

由于 L/K 可分, 即 θ 的极小多形式没有重根也就是说 $\sigma_i(\theta)\neq\sigma_j(\theta)$ $(i\neq j$ 时), 故右式不等于 0, 根据线性代数, 配对 $\langle,\rangle$ 非退化. 那么由于配对 $<,>$ 非退化, 对任意一组基 $\alpha_1,\cdots,\alpha_n$, 存在**对偶基** $\check{\alpha}_1,\cdots,\check{\alpha}_n\in L$ 使得

$$Tr_{L/K}(\alpha_i\check{\alpha}_j)=\begin{cases}1, & \text{如果}i=j\\ 0, & \text{如果}i\neq j\end{cases}$$

注 2.1. (1) 实际上, 有限扩张 L/K 为可分当且仅当由迹诱导的配对 $\langle,\rangle$ 非退化. 感兴趣的同学请尝试证明.

(2) 当然, 如果域 K 的特征为 0, (比如 L/K 是数域扩张的情形), 非退化性有更简单直接的证明, 因为如果 $\alpha\neq 0$, 取 $\beta=\alpha^{-1}$, 则 $\mathrm{Tr}_{L/K}(\alpha\beta)=[L:K]\neq 0$.

若 $\alpha_1,\cdots,\alpha_n\in L$, 我们称配对 $\langle,\rangle$ 在这组元素下度量矩阵的判别式称作这组元素的**判别式**, 记作 $d_{L/K}(\alpha_1,\cdots,\alpha_n)$, 即

$$d_{L/K}(\alpha_1,\cdots,\alpha_n)=|\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)_{i,j}|, \quad \text{也等于}|\sigma_i(\alpha_j)_{i,j}|^2.$$

根据线性代数, $\alpha_1,\cdots,\alpha_n$ 是 L 作为 K-线性空间的一组基当且仅当 $d_{L/K}\neq 0$.

如下是一个帮助计算判别式的习题:

习题 2.1. 设 $L=K(\alpha)$, $f(T)\in K[T]$ 是 α 在 K 上的首一极小多项式, 记 $f'(T)$ 为 $f(T)$ 的导数. 证明

$$d_{L/K}(1,\alpha,\cdots,\alpha^{n-1})=(-1)^{\frac{n(n-1)}{2}}N_{L/K}(f'(\alpha)).$$

2.2 Dedekind 整环

现在我们回到数域的情形. 数域的扩张 L/K 是有限可分扩张.

引理 2.2. *(1) 对每个代数数 α, 存在整数 a 使得 $a\alpha\in\bar{\mathbb{Z}}$. (2) 设 L/K 是数域的扩张 (特别的这是有限扩张), 则 $\mathrm{Tr}_{L/K}(\mathcal{O}_L)\subset\mathcal{O}_K$, $N_{L/K}(\mathcal{O}_L)\subset\mathcal{O}_K$.*

这两个结论的证明留作练习.

命题1.8的证明. 先设 $\alpha_1,\cdots,\alpha_n$ 是 K 作为 $\mathbb{Q}$-线性空间的一组基, 根据引理2.2, 我们可以要求每个 $\alpha_i\in\mathcal{O}_K$. 显然 $\mathbb{Z}\alpha_1+\cdots+\mathbb{Z}\alpha_n$ 是包含于 $\mathcal{O}_K$ 的一个秩为 n 的自由 $\mathbb{Z}$-模. 令 $\check{\alpha}_1,\cdots,\check{\alpha}_n$ 是在非退化双线性映射 $K\times K\to\mathbb{Q}$, $(x,y)\mapsto\mathrm{Tr}_{K/\mathbb{Q}}(xy)$ 下的对偶基. 则存在 $a_1,\cdots,a_n\in\mathbb{Q}$ 使得 $\alpha=a_1\check{\alpha}_1+\cdots a_n\check{\alpha}_n$. 现在用 α_k 乘以该式然后用 $\mathrm{Tr}_{K/\mathbb{Q}}$ 同时作用两边得

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_k\alpha)=a_k.$$

由于 $\alpha_k, \alpha \in \mathcal{O}_K$, 我们有 $a_k \in \mathbb{Z}$. 这就证明了 $\mathcal{O}_K$ 包含于秩为 n 的自由 $\mathbb{Z}$-模 $\subset \mathbb{Z}\check{\alpha}_1 + \cdots \mathbb{Z}\check{\alpha_n}$. 根据有限生成的 $\mathbb{Z}$-模理论, 我们有 $\mathcal{O}_K \cong \mathbb{Z}^n$. □

这个论证过程的关键是迹诱导的配对是非退化的使得我们可以去到一组对偶基, 所以请确信它证明了下面这样一个稍微一般的结论:

命题 2.3. *设 A 是个诺特整环, K 是它的分式域. 设 L/K 是 n 次有限可分扩张, B 是 A 在 L 中的整闭包. 则存在 L 的两个秩为 n 的自由 A 子模 M, M' 使得 $M \subset \mathcal{O} \subset M'$. 特别的, 根据 A 是诺特, 我们知道 $\mathcal{O}$ 是有限生成的 A 模. (再特别的, 若 A 是 PID, 根据 PID 上有限生成模的结论, 知 $\mathcal{O}$ 必定也是秩为 n 的自由 A 模)*

一点花絮: 对任何整环, 主理想总是一个秩为 1d 自由 R 模. 在 $\mathbb{Z}[\sqrt{-5}]$ 中, $(2, 1+\sqrt{-5})$ 被包在两个秩为 1 的自由模中间: $(2) \subset (2, 1+\sqrt{-5}) \subset (1)$, 但 $(2, 1+\sqrt{-5})$ 不是自由模.

我们这样就证明了对任何数域 K, 存在 $\alpha_1, \cdots, \alpha_n$ 使得 $\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \alpha_n$. 这样一组元素称作 $\mathcal{O}_K$ 也称作是 K 的整基.

定义 2.4. 设 K 是数域, 设 $\alpha_1, \cdots, \alpha_n$ 是其一组整基, 则这组元素的判别式 $d_K := d_{K/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n)$ 称作数域 K 的 (绝对) 判别式.

如果换一组整基 $\beta_1, \cdots, \beta_n$, 则其过渡矩阵是一个 $\mathbb{Z}$-系数可逆矩阵 C, 即 $(\beta_1, \cdots, \beta_n) = (\alpha_1, \cdots, \alpha_n)C$. 那么 $d_{K/\mathbb{Q}}(\beta_1, \cdots, \beta_n) = |C|^2 d_{K/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n)$. 由于 C 的行列式为 ± 1, 故我们判别式的定义不依赖于整基的选取.

总结: 数域 K 的判别式是其整基在双线性配对 ($\langle x, y\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$) 下的度量矩阵的行列式.

对于数域的整基存在性, 请试着用如下思路来给出一个新的证明: 若 $\alpha_1, \cdots, \alpha_n \in \mathcal{O}_K$ 是使得其判别式在所有的 n 元 (代数) 整数组里是绝对值最小的那一组, 证明这组元素可以生成 $\mathcal{O}_K$.

例 2.1. 任何一个二次域 K(二次域指 $\mathbb{Q}$ 的二次扩张) 可写成 $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$, $d \neq 0, 1$ 且 d 无平方因子. (为什么?) 我们有

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{如果} d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{如果} d \equiv 1 \bmod 4. \end{cases}$$

设 $a + b\sqrt{d} \in K$ ($a, b \in \mathbb{Q}$), 则 $a + b\sqrt{d} \in \mathcal{O}_K$ 当且仅当其迹和范都属于 $\mathbb{Z}$, 也就是 $2a, a^2 - b^2 d \in \mathbb{Z}$. 则 $a \in \mathbb{Z}/2$. d 无平方因子以及 $a^2 - b^2 d \in \mathbb{Z}$ 给出了 $b \in \mathbb{Z}/2$. 且 $a \in \frac{1}{2} + \mathbb{Z}$ 当且仅当 $b \in \frac{1}{2} + \mathbb{Z}$, 而且容易看出这种情况发生当且仅当 $d \equiv 1 \bmod 4$.

利用这组整基, 可计算二次域的判别式: 当 $d \equiv 1 \bmod 4$ 时, $d_K = d$; 当 $d \equiv 2, 3 \bmod 4$ 时, $d_K = 4d$.

定义 2.5. R 称作是 Dedekind 整环, 如果 R 是诺特, 整闭, 非零素理想均为极大理想的整环.

习题: 证明 PID 是 Dedekind 整环. 特别的域上的一元多项式环是 Dedekind 整环.

定理 2.6. *设 K 是数域, 则 $\mathcal{O}_K$ 是 Dedekind 整环.*

证明. (1) 诺特性可由整基定理推出. 具体来说, 设 I 是 $\mathcal{O}_K$ 的一个非零理想, 取非零元 $\alpha \in I$, 设 $f(T) = T^d + a_{d-1}T^{d-1} + \cdots a_0 \in \mathbb{Z}[T]$ 是 α 的极小多项式, 则 $a_0 \neq 0$. 另一方面因为 $f(\alpha) = 0$, 且 I 是理想知道 $a_0 \in \mathfrak{p} \cap \mathbb{Z}$. 特别的 $a_0\mathcal{O}_K \subset I$. 故理想 I 也是秩为 $[K : \mathbb{Q}]$ 的自由 $\mathbb{Z}$-模, 那么自动是有限生成的 $\mathcal{O}_K$-模.

(2) 整闭可由整的传递性推出. 具体来说, 首先根据引理2.2知 K 确实是 $\mathcal{O}_K$ 的分式域. 设 $\alpha \in K$ 在 $\mathcal{O}_K$ 上整, 则因为 $\mathcal{O}_K/\mathbb{Z}$ 整, 知 α 在 $\mathbb{Z}$ 上整, 知 $\alpha \in \mathcal{O}_K$.

(3) 非零素理想为极大可由整基定理推出. 设 $\mathfrak{p}$ 是 $\mathcal{O}_K$ 的非零素理想, 则 $\mathfrak{p} \cap \mathbb{Z}$ 是 $\mathbb{Z}$ 的一个素理想, 由 (1) 的讨论知这是个非零素理想, 故而是 $\mathbb{Z}$ 的一个极大理想 $p\mathbb{Z}$. 因为 $\mathcal{O}_K/\mathbb{Z}$ 整, 这会给出 $\mathcal{O}_K/\mathfrak{p}$ 在 $\mathbb{Z}/p\mathbb{Z}$ 上整, 但 $\mathbb{Z}/p\mathbb{Z}$ 是域, 所以 $\mathcal{O}_K/\mathfrak{p}$ 是 $\mathbb{Z}/p\mathbb{Z}$ 添加代数元得到, 故而也是域. 这就说明了 $\mathfrak{p}$ 是 $\mathcal{O}_K$ 的极大理想. (实际上, 因为整基的存在性知 $\mathcal{O}_K$ 可由 $\mathbb{Z}$ 添加有限个元素得到, 故 $\mathcal{O}_K/\mathfrak{p}$ 也可由 $\mathbb{Z}/p\mathbb{Z}$ 添加有限个元素得到, 所以 $\mathcal{O}_K/\mathfrak{p}$ 是有限域. 当然这也能从 $p\mathcal{O}_K \subset \mathfrak{p} \subset \mathcal{O}_K$ 看出 $\mathcal{O}_K/\mathfrak{p}$ 是有限域, 其大小不超过 $p^n = [\mathcal{O}_K : p\mathcal{O}_K], n = [K : \mathbb{Q}]$. □

注 2.7. 请确信上面的论证过程实际证明了这样稍微一般的结论:

设 A 是诺特整环且其每个非零素理想都是极大理想, K 是 A 的分式域. 设 L/K 是 n 次有限可分扩张, $\mathcal{O}$ 是 A 在 L 中的整闭包. 则 $\mathcal{O}$ 是 Dedekind 整环.

我们知道 $\mathbb{Z}[\sqrt{-5}]$ 是 $\mathbb{Q}(\sqrt{-5})$ 的整数环, 前面看到过它不是 PID, 所以它是一个 Dedekind 整环但不是 PID 的例子. 对我们而言, 最重要的是 Dedekind 整环的如下性质: (历史上, 是 Dedekind 引入了理想的概念, 并对数域的整数环证明了这条性质)

定理 2.8. *[理想唯一分解定理] 设 R 是 Dedekind 整环, 则 R 的每个非零理想都可唯一分解成素理想的乘积.*

定义 2.9. 设 R 是一个诺特整环, 其分式域记为 K. 我们称 $I \subset K$ 是一个 R 的**分式理想**, 如果 I 是有限生成的 R-模; 对两个分式理想 I, J 我们 (像通常理想那样去) 定义它们的加法和乘法:

$$I + J = \{a + b : a \in I, b \in J\} \qquad IJ = \text{ 由}\{ab : a \in I, b \in J\} \text{ 生成的}R\text{模}.$$

非零分式理想 I 的逆定义为

$$I^{-1} := \{\alpha \in K : \alpha I \subset R\}.$$

(I^{-1} 也是分式理想, 留作练习), 若 $II^{-1} = R$, 我们称 I 可逆.

分式理想 I 可逆等价于存在分式理想 J 使得 $IJ = R$. (练习: 证明这句话.)

首先注意到我们要求分式理想作为 R 模是有限生成的, 比如 $R = \mathbb{Z}$ 时, 所有的分式理想都形如 $\frac{a}{b}\mathbb{Z}$ 注意: 我课堂这有笔误, 写成了 $\frac{1}{d}\mathbb{Z}, d \in \mathbb{Z}$, 而诸如 $\mathbb{Q}, \mathbb{Z}[1/2]$ 等虽然也是 $\mathbb{Z}$ 模, 但它们不是有限生成的, 故不是 R 的分式理想.

再者, 如果分式理想 $I \subset R$, 那么 I 就是我们通常意义下 R 的理想. 所以分式理想这个概念推广了理想, 其上的加和乘也推广了通常理想的运算. 经过一点计算便知 (留作练习), I 是分式理想当且仅当存在 $\alpha \in R$ 使得 αI 是 R 的理想. 换句话说, 每个分式理想都形如 $\frac{I}{\alpha} = \{\beta/\alpha : \beta \in I\}$, 其中 $I \subset R$ 是 R 的理想,$\alpha \in R$. (根据这条性质, " 分式理想" 这个名字便很形象了). 为避免歧义或为了强调, 我们有时将 R 通常的理想称作整理想.)

再谈谈可逆理想, 第一个重要的观察是所有可逆理想构成群, 单位理想 $R=(1)$ 是这个群的单位元. 第二个观察是非零主分式理想总是可逆的, 所有非零主理想作成所有可逆理想的一个子群. 如下给出个不可逆理想的例子, 这将说明对一般的诺特整环, 其所有非零分式理想一般来说不作成群. 考虑 $R=\mathbb{Z}[\sqrt{-3}]$. (观察到此环不是 PID 的一个角度是其不整闭, 其整闭包是 $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, 故其不是 UFD (因为 UFD 是整闭的, 见第一讲), 也就不是 PID. 考虑其上的理想 $\mathfrak{m}=(2,1+\sqrt{-3})$, 它是个极大理想. 计算得 $\mathfrak{m}^2=(2)\mathfrak{m}$. 若 I 可逆, 我们两边同乘 $\mathfrak{m}^{-1}$, 会得到 $I=(2)$ 是个矛盾, 所以 I 不是可逆的. 事实上, 通过直接计算能得出 $\mathfrak{m}\mathfrak{m}^{-1}=\mathfrak{m}$. 这些计算留作练习.

再回到 Dedekind 整环.

定理 2.10. *[理想可逆定理] 设 R 是 Dedekind 整环, 则 R 的每个非零分式理想都是可逆的.*

此定理的第一个重要推论是

推论 (分式理想群的定义)**.** *Dedekind 整环的所有非零分式理想在乘法下作成群, 称这个群为此环的分式理想群.*

这也是引入分式理想的一大好处, 如果不引入, 只能说所有的非零分式理想作成幺半群, 且对非零理想 $I\subset R$, 存在理想 $J\subset R$ 使得 IJ 是主理想. 定理2.10的另一推论是, 在 Dedekind 整环的理想里, 像整数环 $\mathbb{Z}$ 的理想那样, 有所谓的" 包含即整除":

推论 (包含即整除)**.** *设 R 是 Dedekind 整环, I,J 是非零分式理想. 则 $I\subset J$ 当且仅当存在 R 的 (整) 理想 $T\subset R$ 使得 $I=JT$ (后半句简单来说就是 J 整除 I, 记作 $J\mid I$).*

证明. 若 $I=JT$, 则 $I\subset JR=J$. 反过来, 若 $I\subset J$, 显然有 $T:=IJ^{-1}\subset R$ 和 $I=TJ$. □

利用定理2.10还可轻松愉快的推出 Dedekind 整环的理想唯一分解性, 即定理2.8. 反过来, 用唯一分解性定理也能推出每个理想可逆.

定理2.10推定理2.8. 回忆环 R 是诺特的一个等价刻画是: 任意非空的理想集合都存在极大元.

存在性: 反证, 如果存在非零理想 I 不能写成素理想的乘积, 根据诺特性, 我们可以不妨设 I 是拥有这个性质的极大的那个理想. 首先 I 是包含在某个极大理想 $\mathfrak{p}$ 里. 根据上面的" 包含即整除" 性质, $\mathfrak{p}\mid I$. 所以 $I\mathfrak{p}^{-1}\subset R$ 也是整理想. 注意到 $I\subset I\mathfrak{p}^{-1}$ 且它们是不相等的理想. 因为如果相等, 利用 I 是可逆的, 我们就得到 $\mathfrak{p}^{-1}=R$, 但显然 $\mathfrak{p}R=\mathfrak{p}\neq R$. 那么 $I\mathfrak{p}^{-1}$ 就可以写成素理想的乘积了. 两边同时乘以 $\mathfrak{p}$, 就推出 I 也能写成素理想的乘积, 矛盾.

唯一性: 设 $\mathfrak{p}_1\cdots\mathfrak{p}_r=\mathfrak{q}_1\cdots\mathfrak{q}_s$, 其中 $\mathfrak{p}_i,\mathfrak{q}_j$ 都是非零素理想. 则 $\mathfrak{p}_1\supset\mathfrak{q}_1\cdots\mathfrak{q}_s$, 根据素理想的定义容易推出 $\mathfrak{p}_i$ 包含某个 $\mathfrak{q}_j$. 但 Dedekind 整环中非零素理想都是极大理想, 故 $\mathfrak{p}_1=\mathfrak{q}_j$. 然后两边同时乘以 $\mathfrak{p}_1^{-1}$, 再重复这个论证即可. □

现在我们来证关键的定理2.10. 先准备如下重要引理.

引理 2.11. *设 R 是诺特环, $I\subset R$ 是理想. 则 I 包含有限个非零素理想的乘积.* 我课堂上好像忘记说非零了

证明. 反证法: 假设不满足结论的理想的集合非空. 根据诺特性, 我们取出这个集合中的极大元 I. 则 I 显然不是素理想, 那么存在 $a, b \notin R$ 使得 $ab \in I$. 特别的 $I + (a), I + (b)$ 都是真包含 I 的理想, 所以它们各自都包含有限个素理想的乘积, 特别的, 它们的乘积 $(I + (a))(I + (b))$ 也是. 但它们的乘积等于 I, 矛盾. □

引理 2.12. *设 R 是诺特整环, 且其所有非零素理想都是极大理想. 则对任意理想 $I \subset R$, 有 $I^{-1} \supsetneq R$.*

证明. 熟知存在极大理想 $\mathfrak{p}$ 使得 $I \subset \mathfrak{p}$, 则 $I^{-1} \supset \mathfrak{p}^{-1}$. 故我们只需证明 $\mathfrak{p}^{-1} \supsetneq R$. 现取 $0 \neq a \in \mathfrak{p}$. 根据引理2.11, 存在 r 个非零素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ 使得

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (a)$$

我们设 r 是极小的. 于是, 我们有

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset \mathfrak{p}.$$

但 $\mathfrak{p}$ 是素理想, 我们知道 $\mathfrak{p}$ 包含某个 $\mathfrak{p}_i$, 不妨设 $i = 1$. 即 $\mathfrak{p} \supset \mathfrak{p}_1$, 又 R 中的非零素理想都是极大理想, 所以 $\mathfrak{p} = \mathfrak{p}_1$. 另一方面, 由 r 的极小性,

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subset (a).$$

所以存在 $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ 但 $b \notin (a)$. 则 $\frac{b}{a} \notin R$, 而且

$$\frac{b}{a}\mathfrak{p} = \frac{b}{a}\mathfrak{p}_1 \subset (\frac{1}{a})\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset (\frac{1}{a})(a) = R,$$

也就是说 $\frac{b}{a} \in \mathfrak{p}^{-1}$. 这就证明了 $\mathfrak{p}^{-1} \supsetneq R$. □

> 引理2.12的例子和" 非例子": 例如 $R = \mathbb{Z}[\sqrt{-3}]$ 就是满足引理条件的环, 但它不整闭, 所以不是 Dedekind. 若有兴趣, 可动手验算一下下面这个 R 分式理想的等式
>
> $$(2, 1 + \sqrt{-3})^{-1} = (1, \frac{1 + \sqrt{-3}}{2}) \supsetneq R.$$
>
> 以及 $(2, 1 + \sqrt{-3})$ 不可逆. 这里 (a, b) 指由 a, b 生成的在 R 分式域 $\mathbb{Q}(\sqrt{-3})$ 中的子模, 故它是个分式理想.
>
> 另外, 若 k 是域, 则二元多项式环 $R = k[T_1, T_2]$ 是诺特, 整闭, 但它存在不是极大理想的非零素理想, 试着去说明 $(x, y)^{-1} = R$.

定理2.10的证明. 先对非零素理想, 也就是极大理想 $\mathfrak{p}$ 来证明它可逆. 显然我们有 $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset R$. 由于 $\mathfrak{p}$ 是极大理想, $\mathfrak{p}\mathfrak{p}^{-1}$ 要么是 R 要么是 $\mathfrak{p}$. 反证: 假设 $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$. 具体来说, 设 $\alpha_1, \cdots, \alpha_n$ 是 $\mathfrak{p}$ 的一组生成元, 取 $\alpha \in \mathfrak{p}^{-1}$, 则存在 R 系数的矩阵 A 使得 $\alpha(\alpha_1, \cdots, \alpha_n)A$, 因此 $(\alpha I_n - A)(\alpha_1, \cdots, \alpha_n)$. 因为 $\alpha_1, \cdots, \alpha_n$ 不全为 0, 根据线性代数行列式 $|\alpha I_n - A| = 0$, 所以 α 在 R 上整, 根据 R 的整闭性知 $\alpha \in R$. 这就说明了 $\mathfrak{p}^{-1} \subset R$, 即 $\mathfrak{p}^{-1} = R$. 另一方面根据引理2.12知, $\mathfrak{p}^{-1} \supsetneq R$, 得到矛盾. 这就说明了 $\mathfrak{p}\mathfrak{p}^{-1} \neq \mathfrak{p}$, 故 $\mathfrak{p}\mathfrak{p}^{-1} = R$.

现在对任意的 (整) 理想 $I \subset R$ 来证明其可逆. 根据引理2.11知, I 包含有限个素理想的乘积. 我们归纳的证明包含 r 个素理想乘积的理想都可逆. 根据上一段的论证, $r = 1$ 时成立. 假设对

$r-1$ 成立. 现在设 $I \neq (1)$ 是包含 r 非零素理想 $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ 的乘积的一个理想. 取 $\mathfrak{p}$ 极大, $I \subset \mathfrak{p}$. 于是我们有

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset I \subset \mathfrak{p}.$$

由于 $\mathfrak{p}$ 是素理想, 知道 $\mathfrak{p}$ 包含某个 $\mathfrak{p}_i$, 不妨设 $i = 1$. 这时两边同时乘以 $\mathfrak{p}^{-1}$, 由 $\mathfrak{p}$ 可逆, 得到

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \subset I\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = (1).$$

根据归纳法 $J := I\mathfrak{p}^{-1}$ 可逆, 因为 J 包含 $r-1$ 个素理想的乘积. 于是 $I = J\mathfrak{p}$, 以及 $IJ^{-1}\mathfrak{p} = (1)$. 这就说明了 I 可逆.

最后如果 $I = J/(\alpha)$ 是个分式理想, 其中 $J \subset R$ 是 (整) 理想, $\alpha \in R$, 利用 J 可逆以, 显然我们有 $I\alpha J^{-1} = (1)$. 故 I 可逆. □

3 第三讲: 理想类群的定义, 理想的 (绝对) 范, 数域的无穷素位

显然, Dedekind 整环的理想唯一分解性可重新叙述为:

定理 3.1. *设 R 是 Dedekind 整环, 则其非零分式理想群是由 R 的所有非零素理想自由生成的 abel 群:*

$$\oplus_{0 \neq \mathfrak{p} \text{ 素}} \mathfrak{p}^{\mathbb{Z}}.$$

引理 3.2. *设 R 是 Dedekind 整环, K 是其分式域. (1)$v_\mathfrak{p}(I+J) = \min\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\}$; $v_\mathfrak{p}(I \cap J) = \max\{v_\mathfrak{p}(I), v_\mathfrak{p}(J)\}$. (即"加"是"最大公因子", "交"是"最小公倍数理想")*

(2) 若 $\alpha, \beta \in K^\times$, $v_\mathfrak{p}(\alpha+\beta) \geq \min\{v_\mathfrak{p}(\alpha), v_\mathfrak{p}(\beta)\}$; 且 $v_\mathfrak{p}(\alpha) \neq v_\mathfrak{p}(\beta)$ 时, 成立等号.

证明. 见习题. □

定理 3.3 (中国剩余定理)**.** *设 R 是 Dedekind 整环, $I \subset R$ 是理想. 设 $I = \prod_{1 \leq i \leq g} \mathfrak{p}^{e_i}$ 是其素理想分解. 则*

$$R/I \cong \prod_{1 \leq i \leq g} R/\mathfrak{p}^{e_i}.$$

证明. 见习题. □

命题 3.4. *设 R 是 Dedekind 整环. 设 $\mathfrak{p} \subset R$ 是非零素理想. 则作为 R-模, 对 $n \in \mathbb{Z}$ 有 $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong R/\mathfrak{p}$. (也就是说, $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ 是一维的 $R/\mathfrak{p}$ 线性空间.)*

证明. 首先注意到 $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong R/\mathfrak{p}$ 是自然的 $R/\mathfrak{p}$-线性空间. 由 Dedekind 整环的理想唯一分解性知 $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$, 取 $\alpha \in \mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$. $\alpha \bmod \mathfrak{p}^{n+1} \in \mathfrak{p}^n/\mathfrak{p}^{n+1}$ 生成的子空间是 $((\alpha)+\mathfrak{p}^{n+1})/\mathfrak{p}^{n+1}$. 根据引理3.2, $(\alpha)+\mathfrak{p}^{n+1}) = \mathfrak{p}^n$, 即 $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ 是由 $\alpha \bmod \mathfrak{p}^{n+1}$ 生成的一维 $R/\mathfrak{p}$-线性空间, 故同构于 $R/\mathfrak{p}$. □

证明了任何Dedekind整环的理想都可以唯一的写成素理想的乘积了. 先把定理用在 $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ 的情形试试吧. 在 $\mathbb{Z}[\sqrt{-5}]$ 中, 验算下面几个素理想分解:

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

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

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

下面的定义刻画了 Dedekind 整环中的理想与主理想的距离.

定义 3.5. 设 R 是 Dedekind 整环, K 是其分式域. R(或 K) 的**理想类群**定义为 R 的非零分式理想群商其非零主分式理想子群所得的商群.

如果 K 是 R 的分式域, 通常还会将 R 的非零分式理想群也称作是 K 的非零分式理想群, 记作 $\mathcal{I}_K$. 我们有自然同态 $i : K^\times \to \mathcal{I}_K$, $a \mapsto (a)$, 这个同态的像就是 R 的非零主分式理想群, i 的核易见是 R 的单位群 $R^\times$. 也就是说有群的正合列:

$$1 \to R^\times \to K^\times \to \mathcal{I}_K \to \mathrm{Cl}_K \to 1.$$

我们现在知道 $\mathcal{I}_K$ 是个以 R 的所有非零素理想为基的自由 abel 群 (也就是说是个相对好理解、简单的群), 但人们往往对 $K^\times$ 这个群更感兴趣, 那么映射 i 的核与余核就对了解 $K^\times$ 有着重要的意义了. 接下来, 我们就回到数域的整数环这类特殊的 Dedekind 整环, 对它们的单位群与其理想类群的描述是本课程第一阶段最重要的定理.

4 第三讲: 从无穷远处看数域, 理想类群与单位群

所谓登高望远, 今天我们就从" 无穷远处" 来看数域 K. 若域嵌入 $\sigma : K \hookrightarrow \mathbb{C}$ 的像 $\sigma(K) \subset \mathbb{R}$, 称 σ 是实嵌入, 实嵌入的个数记为 r_1. 若 $\sigma(K) \not\subset \mathbb{R}$, 称 σ 是复嵌入. 注意到如果 τ 是复嵌入, 则它和复共轭 $\mathbb{C} \to \mathbb{C}$ 的复合 $\bar{\tau}$ 又是一个新的复嵌入, 所以复共轭是成对出现的, K 的复嵌入对数记为 r_2 对. 所以

$$[K : \mathbb{Q}] = r_1 + 2r_2.$$

(若数域 $K = \mathbb{Q}(\alpha)$, 设 $f(T)$ 是 α 在 $\mathbb{Q}$ 上的极小多项式. 则 r_1 是 $f(T)$ 的实根的个数, r_2 是 $f(T)$ 复根 (非实根) 的对数.)

在本节中, 我们**固定** r_2 个互不 (复) 共轭的复嵌入 $\tau_1, \cdots, \tau_{r_2}$, 与 r_1 个实嵌入 $\rho_1, \cdots, \rho_{r_1}$ 作成集合 S_∞:

$$S_\infty = \{\rho_1, \cdots, \rho_{r_1}, \tau_1, \cdots, \tau_{r_2}\}.$$

对任意 $\sigma \in S_\infty$, 令 $K_\sigma = \sigma(K)$ 在$\mathbb{C}$中的 (拓扑) 闭包, 也就是说 (请自行验证下面式子)

$$K_\sigma = \begin{cases} \mathbb{R}, & \text{如果}\sigma \text{ 是实嵌入} \\ \mathbb{C}, & \text{如果}\sigma \text{ 是复嵌入.} \end{cases}$$

记

$$K_\infty = \prod_{\sigma \in S_\infty} K_\sigma = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}. \tag{4.1}$$

定义 4.1. 我们对每个 $\sigma \in S_\infty$, 定义绝对值 $|\cdot|_\sigma : K_\sigma \to \mathbb{R}_{\geq 0}$ 如下:

$$|x|_\sigma = \begin{cases} |x| & \text{如果} K_\sigma = \mathbb{R}; \\ x\bar{x} & \text{如果} K_\sigma = \mathbb{C}. \end{cases}$$

定义 K_∞ 上的绝对值 $|\cdot|_\infty : K_\infty \to \mathbb{R}_{\geq 0}$:

$$|.|_\infty : (x_\sigma)_{\sigma \in S_\infty} \mapsto \prod_{\sigma \in S_\infty} |x_\sigma|_\sigma.$$

现在考虑嵌入:

$$K \hookrightarrow K_\infty, \quad x \mapsto (\sigma(x))_{\sigma \in S_\infty}.$$

K_∞ 作为 $\mathbb{R}$-代数, 其上的任何元素通过左乘给出了 K_∞ 上的线性变换, 因而我们可以定义范映射 $N_\mathbb{R}$ 与迹映射. 验证有如下交换图 (练习):

$$\begin{array}{ccccc} K & \longrightarrow & K_\infty & & \\ {\scriptstyle N=N_{K/\mathbb{Q}}}\downarrow & & \downarrow{\scriptstyle N_\mathbb{R}} & \searrow^{|\cdot|_\infty} & \\ \mathbb{Q} & \longrightarrow & \mathbb{R} & \xrightarrow[|\cdot|]{} & \mathbb{R}_{\geq 0} \end{array}$$

后面要进行一些体积计算, 所以我们先约定测度的取法. 通过映射 $z \mapsto (\mathrm{Re}(z), \mathrm{Im}(z))$ 固定 $\mathbb{C}$ 与 $\mathbb{R}^2$ 的同构, $\mathbb{R}^2$ 上通常的 Lebesuge 测度就给出了 $\mathbb{C}$ 的测度, 例如

$$\mu(\{z \in \mathbb{C} | 0 \leq \mathrm{Re}(z) < 1, 0 \leq \mathrm{Im}(z) < 1\}) = 1.$$

我们在 K_∞ 上取乘积测度. 最后给出 K_∞ 的一组基: 对 $\sigma \in S_\infty$, 考虑

$$(0, \cdots, 0, \underset{\sigma}{1}, 0, \cdots, 0) \quad \sigma \in S_\infty, \quad (0, \cdots, 0, \underset{\sigma}{i}, 0, \cdots, 0), \quad \text{当}\sigma \text{ 复}. \tag{4.2}$$

这 n 个元素显然是 K_∞ 一组基. 它们生成的格的基本区域的测度是 1, 格与基本区域的定义见下节.

5 第四讲, 类群有限

引理 5.1 (格的定义)**.** *设 Γ 是 n-维实线性空间 V 的子集. 则下面的 (1) 与 (2) 等价, (i) 与 (ii) 等价. 若满足 (1) 或 (2), 称 Γ 是 V 的***格***, 若满足 (i) 或 (ii), 称 Γ 是 V 的***满格***或***完全格***.*

(1)Γ 是 V 的离散子群;

(2) 存在线性无关的向量 $\alpha_1, \cdots, \alpha_k$ 使得 $\Gamma = \mathbb{Z}\alpha_1 + \cdots \mathbb{Z}\alpha_k$.

(i) Γ 是 V 的离散子群且 V/Γ 紧;

(ii) 存在线性无关的向量 $\alpha_1, \cdots, \alpha_n$ 使得 $\Gamma = \mathbb{Z}\alpha_1 + \cdots \mathbb{Z}\alpha_n$.

注 5.2. 若 $\Gamma = \mathbb{Z}\alpha_1 + \cdots \mathbb{Z}\alpha_n$ 是满格, 称 $\mathcal{F} := \{\sum a_i\alpha_i | 0 \leq a_i < 1\}$ 是 Γ 的一个基本区域. 对任意 $v \in V$, 存在唯一的元素 $v_0 \in \mathcal{F}$ 使 $v - v_0 \in \Gamma$. 记 μ 是 V 上的 Lebesgue 测度. 尽管基本区域依赖于 Γ 的一组 $\mathbb{Z}$-基的选取, 但其测度是不变的, 我们把这个测度 (也称作是 Γ 的体积), 记作 $\mathrm{vol}(\Gamma) := \mu(\mathcal{F})$.

证明. 见习题. □

定理 5.3 (Minkowski)**.** *设 X 是 n 维实线性空间 V 中可测集, Γ 是 V 的一个满格.*

(1) 若 $\mu(X) > \mathrm{vol}(X)$, 存在 $x_1, x_2 \in X$ 使得 $0 \neq x_1 - x_2 \in \Gamma$;

(2) 设 X 是对称的凸集. 若 $\mu(X) > 2^n \mathrm{vol}(\Gamma)$, 存在 $0 \neq x \in X \cap \Gamma$;

(3) 设 X 是对称的凸闭集. 若 $\mu(X) \geq 2^n \mathrm{vol}(\Gamma)$, 存在 $0 \neq x \in X \cap \Gamma$.

证明. (1) 令 $\mathcal{F}$ 是 Γ 的一个基本区域. 则 V 可以写成无交并

$$V = \bigcup_{\gamma \in \Gamma} \gamma + \mathcal{F}.$$

从而,

$$\mu(X) = \sum_{\gamma \in \Gamma} \mu(X \cap (-\gamma + \mathcal{F})) = \sum_{\gamma \in \Gamma} \mu((\gamma + X) \cap \mathcal{F}).$$

如果 (1) 不成立, $(\gamma + X) \cap \mathcal{F}, (\gamma \in \Gamma)$ 是两两不交的 $\mathcal{F}$ 的子集. 则上式右端小于等于 $\mu(\mathcal{F})$, 即 $\mathrm{vol}(\Gamma)$. 这与条件矛盾.

(2) 由条件知 $\mu(X/2) > \mathrm{vol}(\Gamma)$. 根据 (1), 我们可以取 $x_1, x_2 \in X/2$ 使得 $0 \neq \frac{x_1 - x_2}{2} \in \Gamma$. 又因为 X 是对称凸集, 我们有 $\frac{x_1 - x_2}{2} \in X$.

(3) 令 $X_n = (1 + \frac{1}{n})X$, 则根据 (2), 存在 $0 \neq x_n \in X_n \cap \Gamma$. 由 X 是闭知存在 $0 \neq x \in X \cap \Gamma$. □

引理 5.4 (微积分习题, 留作练习)**.** *对 $t \geq 0$, 令*

$$X_t = \{(x_\sigma)_{\sigma \in S_\infty} \in K_\infty : \sum_{\sigma \text{实}} |x_\sigma|_\sigma + \sum_{\sigma \text{复}} 2\sqrt{|x_\sigma|_\sigma} \leq t\}.$$

(课堂上, 我将 X_t 写成了如下, 两者是一回事)

$X_t = \{(x_1, \cdots, x_{r_1}, z_1, \cdots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : |x_1| + \cdots + |x_{r_1}| + 2|z_1| + \cdots + 2|z_{r_2}| \leq t$ （这个式子里$|z| = \sqrt{z\bar{z}}$).

则 $\mu(X) = 2^{r_1}(\frac{\pi}{2})^{r_2}(\frac{t^n}{n!})$.

下面我们将 K 与它在嵌入 $K \hookrightarrow K_\infty$ 下的像做等同. 数域的整数环有如下重要性质:

命题 5.5. *(1) $\mathcal{O}_K$ 在 K_∞ 中离散且 $K_\infty/\mathcal{O}_K$ 紧. (也就是说, $\mathcal{O}_K$ 是 K_∞ 的一个满格.)*

(2) $\mathcal{O}_K$ 的基本区域的测度是 $2^{-r_2}\sqrt{|d_K|}$.

证明. 设 $\alpha_1, \cdots, \alpha_n$ 是 $\mathcal{O}_K$ 的一组整基, 见命题1.8. 则在 K_∞ 中, $\alpha_i = (\sigma(\alpha_i))_{\sigma \in S_\infty}$. 则 $\alpha_1, \cdots, \alpha_n$ 在 K_∞ 的标准基(4.2)下的矩阵 A 可逆, 经过初等变换可看出, A 的行列式

$$|A| = 2^{-r_2}|(\sigma(\alpha_j))|_{\sigma \in \mathrm{Hom}(K,\mathbb{C}), 1 \leq j \leq n} = 2^{-r_2}\sqrt{|d_K|}.$$

这里我们回忆 d_K 是域 K 的判别式, 它是个非零的整数. 这就推出了 $\alpha_1, \cdots, \alpha_n$ 是一组线性无关的向量, 从而 $\mathcal{O}_K$ 是格, 且它的基本区域的测度是 $2^{-r_2}d_K$. □

如上的证明中我们用到了整基的存在性结论, 我们还可以反过来利用代数整数的特性首先推出 $\mathcal{O}_K$ 是满格, 从而给出了整基存在性的又一证明, 这也算是从" 无穷远处" 看 K 的一个" 风景" 了. 细节如下:

整基存在性即命题1.8另证. 首先来证明 $\mathcal{O}_K$ 是 K_∞ 的离散子群. 这只需说明对任意 $M > 0$, 球 $B(0, M) = \{(x_\sigma)_\sigma \in K_\infty : |x|_\sigma < M \text{ 对每个} \sigma \in S_\infty\}$ 与 $\mathcal{O}_K$ 的交集是有限的. 设 α 属于它俩的交, 考虑 α 在 $\mathbb{Q}$ 上首一极小多项式

$$f(T) := T^d + a_{d-1}T^{d-1} + \cdots + a_0.$$

对 $\sigma \in S_\infty$, 每个 $\sigma(\alpha)$ 都是 $f(T)$ 的根. 那么由根与系数的关系知 $f(T)$ 的系数 $a_{d-1}, \cdots, a_0$ 都只有有限种取法. 另一方面, 因为 $\alpha \in K$, 所以 d 小于等于数域 K 的次数 n. 故只有有限个多项式使得 α 以它为极小多项式. 这就证明了 $\mathcal{O}_K \cap B(0, M)$ 是有限的, 从而 $\mathcal{O}_K$ 在 K_∞ 中离散. 根据引理5.1, $\mathcal{O}_K$ 作为 abel 群是自由群且秩小于等于 n.

另一方面, 若 $\alpha_1, \cdots, \alpha_n$ 是 K 的一组 $\mathbb{Q}$-线性空间的基, 熟知乘以这组元素一个适当的整数会使它们都属于 $\mathcal{O}_K$. 由此知 $\mathcal{O}_K$ 包含一个秩 n 的自由 abel 群. 由上段的结论知 $\mathcal{O}_K \cong \mathbb{Z}^n$. 这就证明了整基的存在性. □

定义 5.6 (理想的 (绝对) 范)**.** 设 K 是数域, $\mathfrak{a} \subset \mathcal{O}_K$ 是整理想. 定义理想 $\mathfrak{a}$ 的 **(绝对) 范**:

$$\mathbf{N}(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}].$$

若 $\alpha_1, \cdots, \alpha_n$ 是 $\mathcal{O}_K$ 的一组整基, $\beta_1, \cdots, \beta_n$ 是 $\mathfrak{a}$ 的一组 $\mathbb{Z}$-基, 设 $C \in M_{n\times n}(\mathbb{Z})$ 使得 $(\beta_1, \cdots, \beta_n) = (\alpha_1, \cdots, \alpha_n)C$. 则根据有限生成 abel 群理论知

$$\mathbf{N}(\mathfrak{a}) = |\det C|, \quad d_K(\beta_1, \cdots, \beta_n) = (\det C)^2 d_K.$$

显然 $\mathfrak{a}$ 也是 K_∞ 的满格. 而且命题5.5的论证过程结合有限生成 abel 群的结论证明了

$$\mathrm{vol}(\mathfrak{a}) = 2^{-r_2}\mathbf{N}(\mathfrak{a})\sqrt{|d_K|}. \tag{5.1}$$

引理 5.7. *(1) 设 $\mathfrak{a}, \mathfrak{b}$ 是两个整理想. 则 $\mathbf{N}(\mathfrak{ab}) = \mathbf{N}(\mathfrak{a})\mathbf{N}(\mathfrak{b})$.*

(2) 若 $0 \neq \alpha \in \mathcal{O}_K$, 我们有 $|\mathbf{N}(\alpha)| = |N(\alpha)|$.

证明. 根据中国剩余定理与命题3.4立得 (1).

(2) 可由有限生成 abel 群的理论推出. □

上面只能算牛刀小试, " 从无穷远处看到的真正风景" 是如下定理以及后面要讲的 Dirichlet 单位定理:

定理 5.8. *设 K 是数域. 则 K 的 (理想) 类群 Cl_K 有限.*

下次的目标是通过证明如下重要结论来证明类群有限.

定理 5.9. *令 $M_K = \frac{n!}{n^n}(\frac{4}{\pi})^{r_2}\sqrt{|d_K|}$. 则对每个非零理想 $\mathfrak{a} \subset \mathcal{O}_K$, 存在 $0 \neq \alpha \in \mathfrak{a}$ 使得*

$$|N(\alpha)| \leq M_K \mathbf{N}(\mathfrak{a}).$$

证明. 我们知道 $\mathrm{vol}(\mathfrak{a}) = 2^{-r_2}\sqrt{|d_K|}\mathbf{N}(\mathfrak{a})$. 令 X 如同引理5.4中, 取 t 使得 $\mu(X) = 2^n \mathrm{vol}(\mathfrak{a})$, 即 $t^n = 2^n \frac{\mathbf{N}(\mathfrak{a})\sqrt{|d_K|}}{2^{r_1}(2\pi)^{r_2}} n!$. 根据 Minkowski 定理, 存在 $0 \neq \alpha \in \mathfrak{a} \cap X$ 使

$$|N(\alpha)| = \prod_{\sigma\in S_\infty} |\sigma(\alpha)|_\sigma \leq \left(\frac{\sum_{\sigma\text{实}} |\sigma(\alpha)|_\sigma + \sum_{\sigma\text{复}} 2\sqrt{|\sigma(\alpha)|_\sigma}}{n}\right)^n \leq \frac{t^n}{n^n} \leq M_K \mathbf{N}(\mathfrak{a}).$$

□

我们来看如何用此定理证明类群有限.

引理 5.10. *给定任意的整数 $d \geq 1$, 范小于等于 d 的 ($\mathcal{O}_K$-) 整理想只有有限个.*

证明. 若整理想 $\mathfrak{a}$ 的范是 d, 则 $d \in \mathfrak{a}$, 因为 $d * 1 \subset d\mathcal{O}_K \subset \mathfrak{a}$. 根据环同态基本定理, 包含 (d) 的 $\mathcal{O}_K$ 理想一一对应于商环 $\mathcal{O}_K/(d)$ 的理想, 而由整基定理知 $\mathcal{O}_K/(d) \cong (\mathbb{Z}/d\mathbb{Z})^n$ 是有限环, 从而只有有限个理想.

另证: 若整理想 $\mathfrak{a}$ 的范是 d, 则 $d \in \mathfrak{a}$, 因为 $\mathcal{O}_K$ 是 Dedekind 整环, 利用" 包含即整除" 性质, 知作为理想 $\mathfrak{a} \mid (d)$, 由理想唯一分解定理知 $\mathfrak{a}$ 只有有限种取法. □

定理5.8的证明. 任取 K 的一个理想类 $\mathfrak{C} \in \mathrm{Cl}_K$, 我们可以取一个整理想 $\mathfrak{a}$ 代表. 根据定理8, 存在 $0 \neq \alpha \in \mathfrak{a}$ 使得 $N(\alpha) \leq M_K \mathbf{N}(\mathfrak{a})$. 则 $(\alpha)\mathfrak{a}^{-1}$ 是整理想属于理想类 $\mathfrak{C}^{-1}$, 且 $\mathbf{N}(\alpha\mathfrak{a}^{-1}) \leq M_K$. 这就证明了在每个理想类中, 可以取到一个整理想代表元使其范小于等于 M_K, 因为当 $\mathfrak{C}$ 跑遍 Cl_K 时, $\mathfrak{C}^{-1}$ 也跑遍. □

类群方面的历史 (冯克勤 < 代数数论, 科学出版社 2000>102 页) Kummer 研究 Fermat 大定理即 $x^p + y^p = z^p$ (p 素数), 提出理想数的概念, 他实际证明了 $\mathbb{Q}(\zeta_p)$ 理想类群是有限的. 并证明了若 $p \nmid h_{\mathbb{Q}(\zeta_p)}$, 则 Fermat 大定理正确. Dedekind 后来定义了一般的代数整数环以及理想, 并证明了理想的唯一分解性, 然后定义了理想类群并证明它是有限的. 我们再讲讲 Dedekind 的证明:

Dedekind 关于定理5.8的证明. 令 $\alpha_1, \cdots, \alpha_n$ 是 $\mathcal{O}_K$ 的一组整基. 令

$$D = \prod_{\sigma \in S_\infty} |\sum_{i=1}^{n} \sigma(\alpha_i)|_\sigma.$$

我们现在来证明对每个 $\mathcal{O}_K$ 的非零整理想 $\mathfrak{a}$, 都存在 $0 \neq \alpha \in \mathfrak{a}$ 使得 $|N(\alpha)| \leq D\mathbf{N}(\mathfrak{a})$. 给定 $\mathfrak{a}$, 取整数 $N \geq 1$ 使得 $N^n \leq \mathbf{N}(\mathfrak{a}) < (N+1)^n$. 考虑有限集合

$$A = \{\sum_{i=1}^{n} r_i \alpha_i : r_i \in \mathbb{Z}, 0 \leq r_i \leq N\}.$$

因为 A 有 $(N+1)^n$ 个元素, 所以存在两个不同的 $\beta, \beta' \in A$ 使得 $\beta \equiv \beta' \bmod \mathfrak{a}$. 记 $\alpha = \beta - \beta' = \sum_{i=1}^{n} a_i \alpha_i$. 则 $0 \neq \alpha \in \mathfrak{a}$, 以及 $|a_i| \leq N$. 那么

$$|N(\alpha)| = \prod_{\sigma \in S_\infty} |\sigma(\alpha)|_\sigma = \prod_{\sigma \in S_\infty} |\sum_{i=1}^{n} a_i \sigma(\alpha_i)|_\sigma \leq N^n \prod_{\sigma \in S_\infty} |\sum_{i=1}^{n} \sigma(\alpha_i)|_\sigma \leq D\mathbf{N}(\mathfrak{a}).$$

接下来, 就可以按照定理5.8的证明的讨论来得出类群的有限性了. □

Dedekind 证明非常简短, 但 Minkowski 的界 M_K 在实际计算时更为方便. 现在我们可以完成第一节课留下的关于 $\mathbb{Z}(\sqrt{-5})$ 的断言了: 任何 $\mathbb{Z}[\sqrt{-5}]$ 的理想的平方都是主理想.

例 5.1. $K = \mathbb{Q}(\sqrt{-5})$, 则 $r_2 = 1, d_K = -20$. 故 $M_K = \frac{2}{\pi}\sqrt{20} < 3$. 范等于 2 整理想只有一个 $(2, 1+\sqrt{-5})$. 细节: 若 $\mathbf{N}(\mathfrak{a}) = 2$, 则 $\mathcal{O}_K/\mathfrak{a} \cong \mathbb{F}_2$ 知 $\mathfrak{a}$ 是极大理想. 由于 $(2) \subset \mathfrak{a}$, 根据环同态基本定理, $\mathfrak{a}$ 对应 $\mathcal{O}_K/2\mathcal{O}_K$ 的极大理想.

$$\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{Z}[T]/(2, T^2+5) \cong \mathbb{F}_2[T]/((T+1)^2).$$

$\mathbb{F}_2[T]/((T+1)^2)$ 唯一的极大理想是由 $(T+1)$ 生成, 对应回去就是 $(2, 1+\sqrt{-5})$. 范是 1 的整理想是 (1). 由于 $(2, 1+\sqrt{-5})$ 不是主理想. 这推出了 $\mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$. 故任何理想的平方都是主理想.

现在我们利用这一点来证明 $y^2 + 5 = x^3$ 没有 $\mathbb{Z}$-解. 反证法: 设 x, y 是一组 $\mathbb{Z}$-解. 则 $5 \nmid xy$. 模 8 知 $2 \mid x, 2 \parallel y$. 在 $\mathcal{O}_K$ 中,

$$(y + \sqrt{-5})(y - \sqrt{-5}) = x^3.$$

注意到 $(y+\sqrt{-5})$ 与 $(y-\sqrt{-5})$ 互素 (即, 它们在 $\mathbb{Z}[\sqrt{-5}]$ 中生成单位理想), 这是因为 x, y 显然是两个互素的整数以及 $2 \nmid x$, 故 $(1) = (2y, x^3) \subset (y+\sqrt{-5}, y-\sqrt{-5})$. 根据理想唯一分解定理知存在理想 $\mathfrak{a} \subset \mathcal{O}_K$ 使

$$(y+\sqrt{-5}) = \mathfrak{a}^3.$$

由于 $\mathrm{Cl}_K \cong \mathbb{Z}/2\mathbb{Z}$, 推出 $\mathfrak{a}$ 本身是主理想, 设其生成元是 $a+b\sqrt{-5}$ $(a, b \in \mathbb{Z})$. 由于 $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$, 我们有

$$y+\sqrt{-5} = \pm(a+b\sqrt{-5})^3.$$

比较 $\sqrt{-5}$ 的系数得矛盾.

6 第五讲: Dirichlet 单位定理

对数域 K, 记 $\mu(K) = \{x \in K^\times : \text{存在} n \in \mathbb{Z} \text{ 使} x^n = 1\}$. 注意到 $\mu(K)$ 就是 $\mathcal{O}_K^\times$ 的扭子群, 我们称它为 K 的**单位根群**. 本节课的目标是证明 Dirichlet 单位定理, 定理6.3

与前面一样, 我们会等同 K 与它在嵌入 $K \hookrightarrow K_\infty = \prod_{\sigma \in S_\infty} K_\sigma = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ 下的像.

引理 6.1. *设 $u \in \mathcal{O}_K$. (1) $u \in \mathcal{O}_K^\times$ 当且仅当 $N(u) = \pm 1$ 当且仅当 $|u|_\infty = 1$.*

$|\cdot|_\infty$ 的定义在第三讲开始.

(2) 设 $u \in \mathcal{O}_K$, $u \in \mu(K)$ 当且仅当 $|\sigma(u)|_\sigma = 1$ 对每个 $\sigma \in S_\infty$.

(3) $\mu(K)$ 是有限循环群.

证明. (1) 若 u 是单位, 则 $N(u)$ 与 $N(u^{-1}) = N(u)^{-1}$ 都属于 $\mathbb{Z}$, 则 $N(u) \in \mathbb{Z}^\times = \{\pm 1\}$. 若 $N(u) = \pm 1$, 设 u 在 $\mathbb{Q}$ 上的极小多项式 $T^d + a_{d-1}T^{d-1} + \cdots + a_0$, 显然 a_0 属于 (u). 则由范的基本性质知

$$N(u) = \pm(a_0)^{\frac{n}{d}}.$$

推出 $a_0 = \pm 1$, 这推出 $(u) = (1)$, 即 u 是单位.

" 反过来的方向" 另证: $\pm 1/u = N(u)/u$ 是一些 $\sigma(u)$ 的乘积, $\sigma \in \mathrm{Hom}(K, \mathbb{C})$. 它们显然都是代数整数, 故 $\pm 1/u \in \overline{\mathbb{Z}} \cap K = \mathcal{O}_K$, 推出 u 是单位.

(1) 另另证: 由于 $u \in \mathcal{O}_K$, (u) 是整理想. 则 u 是单位当且仅当 $(u) = (1)$ 当且仅当 $\mathbf{N}((u)) = 1$ 当且仅当 $N(u) = \pm 1$. 最后一步用到了理想范的性质, 见引理5.7.

(2) 若 $u \in \mu(K)$, 对每个 $\sigma \in S_\infty$, 显然 $|\sigma(u)|_\sigma = 1$. 反过来, 若对每个 $\sigma \in S_\infty$ 有 $|\sigma(u)|_\sigma = 1$, 由 (1) 知 $u \in \mathcal{O}_K^\times$. 记 $\langle u \rangle$ 为 u 生成的子群. 在嵌入 $K \to K_\infty$ 下, $\langle u \rangle$ 中的元素都落在 K_∞ 的紧子集 $\{(z_\sigma)_\sigma : |z_\sigma|_\sigma = 1\} = \{\pm 1\}^{r_1} \times (\mathbb{S}^1)^{r_2}$ 上. 根据命题5.5, $\mathcal{O}_K$ 在 K_∞ 中离散, 从而 $\langle u \subset \mathcal{O}_K \cap \{\pm 1\}^{r_1} \times (\mathbb{S}^1)^{r_2}$ 是有限集. 这就推出了 $u \in \mu(K)$.

(3) 刚才说明了 $\mu(K) \subset \mathcal{O}_K \cap \{\pm 1\}^{r_1} \times (\mathbb{S}^1)^{r_2}$, 由 $\mathcal{O}_K$ 在 K_∞ 中离散知 $\mu(K)$ 有限. 熟知域的有限乘法子群均为循环群, 证毕. □

记 $\log : \mathbb{R}_{>0} \to \mathbb{R}$ 为通常的对数映射. 定义映射

$$\iota : K_\infty^\times \to \mathbb{R}^{r_1+r_2}, \quad (x_\sigma)_\sigma \mapsto \log |x_\sigma|_\sigma.$$

回忆如果 σ 是复嵌入, $|\cdot|_\sigma$ 是通常模长的平方, 等于我课堂上的 $|\cdot|_{\mathbb{C}}$. 记

$$K_\infty^1 = \{x = (x_\sigma)_\sigma \in K_\infty^\times : |x|_\infty = 1\};$$
$$\{\pm 1\}^{r_1} \times (\mathbb{S}^1)^{r_2} = \{(x_\sigma)_{\sigma\in S_\infty} \in K_\infty^1 : |x_\sigma|_\sigma = 1, \sigma \in S_\infty\};$$
$$(\mathbb{R}^{r_1+r_2})^0 = \{(x_1, \cdots, x_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} : \sum_{i=1}^{r_1+r_2} x_i = 0\}.$$

根据 ι 的定义以及引理6.1, 我们有如下交换图且其中每行正合, 竖箭头为嵌入映射:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu(K) & \longrightarrow & \mathcal{O}_K^\times & \xrightarrow{\iota} & \iota(\mathcal{O}_K^\times) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \{\pm 1\}^{r_1} \times \mathbb{S}^{1r_2} & \longrightarrow & K_\infty^1 & \xrightarrow{\iota} & (\mathbb{R}^{r_1+r_2})^0 & \longrightarrow & 1. \end{array} \tag{6.1}$$

定理 6.2 (Dirichlet 单位定理 (拓扑描述))**.** *设 K 是数域, 我们有*

(1) $\mathcal{O}_K^\times$ 在 K_∞^1 中离散且 $K_\infty^1/\mathcal{O}_K^\times$ 紧.

(2) $\iota(\mathcal{O}_K^\times)$ 在 $(\mathbb{R}^{r_1+r_2})^0$ 中离散且 $(\mathbb{R}^{r_1+r_2})^0/\iota(\mathcal{O}_K^\times)$ 紧.

由上述定理的 (2) 知 $\iota(\mathcal{O}_K^\times)$ 是 $(\mathbb{R}^{r_1+r_2})^0$ 的满格. 特别地, $\iota(\mathcal{O}_K^\times) \cong \mathbb{Z}^{r_1+r_2-1}$. 根据正合列(6.1)的第一行以及引理6.1(3) 我们得出:

定理 6.3 (Dirichlet 单位定理)**.** *设 K 是数域, 记 $w = \#\mu(K)$. 我们有*

$$\mathcal{O}_K^\times \cong \mathbb{Z}^{r_1+r_2-1} \times \mathbb{Z}/w\mathbb{Z}.$$

定理6.2的证明仍旧是使用 Minkowski 定理.

定理6.2的证明. (1) 中的离散性. 根据命题5.5, $\mathcal{O}_K$ 在 K_∞ 中离散. 特别的, $\mathcal{O}_K^\times$ 在 K_∞^1 中离散.

(2) 中的离散性. 设 $M \subset (\mathbb{R}^{r_1+r_2})^0$ 是有界集, 显然 $\#\iota(\mathcal{O}_K^\times) \cap M \le \#\mathcal{O}_K^\times \cap \iota^{-1}(M)$. 注意到 $\iota^{-1}(M)$ 也是有界集. 故 $\iota^{-1}(M) \cap \mathcal{O}_K^\times$ 有限, 这就证明了 $\iota(\mathcal{O}_K^\times) \cap M$ 有限, 从而 $\iota(\mathcal{O}_K^\times)$ 在 $(\mathbb{R}^{r_1+r_2})^0$ 中离散.

注意: 离散性已经说明了 $\iota(\mathcal{O}_K^\times) \cong \mathbb{Z}^k$, $k \le r_1 + r_2 - 1$.

(1) 中的余紧性. (**这一条是整个定理的关键**, 这推出了上式中的 $r = r_1 + r_2 - 1$.)

取 $X \subset K_\infty$ 是紧、对称、凸、可测、且 $\mu(X) \ge 2^n \mathrm{vol}(\mathcal{O}_K)$. 由紧 (即有界闭) 性知, 存在 C 使得对任意 $x \in X$ 有 $|x|_\infty \le C$. 设范小于等于 C 的所有 $\mathcal{O}_K$ 的非零整理想为 $(\beta_1), \cdots, (\beta_t)$, 这样的理想只有有限个是因为范小于等于 C 的整理想的个数也是有限的, 见引理5.7. 任取 $z \in K_\infty^1$, 则 Xz 也是对称、凸、可测、有界且 $\mu(Xz^{-1}) = \mu(X)$. 用 Minkowski 定理知存在 $0 \ne \gamma \in \mathcal{O}_K \cap Xz^{-1}$. 则 $|N(\gamma)| = \mathbf{N}((\gamma)) \le N$, 故 (γ) 是某个 (β_i), 则存在 $u \in \mathcal{O}_K^\times$ 使得 $\gamma = u^{-1}\beta_i$. 这就推出了 $u^{-1}\beta_i \in Xz^{-1}$, 也就是说 $z \in X\beta_i^{-1}u$. 令

$$X' = \cup_{i=1}^t X\beta_i^{-1} \cap K_\infty^1.$$

则我们证明了自然映射 $X' \to K_\infty^1/\mathcal{O}_K^\times$ 是满射. 由于 X 紧, X' 也紧, 而这个映射连续, 我们知道 $K_\infty^1/\mathcal{O}_K^\times$ 紧, 因为紧集的连续像紧.

(2) 中的余紧性. 这其实是上面一条的推论: 首先看出 (由蛇形引理) 交换图6.1诱导了下面的正合列, 且其中每个箭头都是连续映射:

$$1 \to (\{\pm 1\}^{r_1} \times \mathbb{S}^{1^{r_2}})/\mu(K) \to K_\infty^1/\mathcal{O}_K^\times \to (\mathbb{R}^{r_1+r_2})^0/\iota(\mathcal{O}_K^\times) \to 1. \tag{6.2}$$

我们证明了中间一项是紧的, 从而它的像也是紧的, 证毕.

□

定义 6.4. 上面证明了 $\iota(\mathcal{O}_F^\times)$ 是 $(\mathbb{R}^{r_1+r_2})^0$ 的满格. $\iota(\mathcal{O}_F^\times)$ 与单位向量 $(\frac{1}{\sqrt{r_1+r_2}}, \cdots, \frac{1}{\sqrt{r_1+r_2}}) \in \mathbb{R}^{r_1+r_2}$ 正交, 所以它们生成 $\mathbb{R}^{r_1+r_2}$ 的一个满格. 定义 K 的**规范子** R_K 为 $\frac{1}{\sqrt{r_1+r_2}}$ 乘以这个满格的体积.

在正合列(6.2)中, 如果能证明第三项是紧的, 那么由下面拓扑群的一般结论知中间一项也紧. 下面我们对于(6.2)中第三项紧给一个" 稍微不同" 的证明. 取 $c = (c_\sigma)_\sigma \in S_\infty$ ($c_\sigma > 0$), 满足

$$X_0 = \{(x_\sigma)_{\sigma\in S_\infty} \in K_\infty : |x_\sigma|_\sigma \le c_\sigma\} = 2^n \mathrm{vol}(\mathcal{O}_K).$$

我们有 $\mu(X_0) = \prod_{\sigma实}(2c_\sigma)\prod_{\sigma复}(\pi c_\sigma) = 2^n\mathrm{vol}(\mathcal{O}_K)$, 以及对任意 $x \in X$,

$$|x|_\infty \le \prod_{\sigma\in S_\infty} c_\sigma = \frac{2^n\mathrm{vol}(\mathcal{O}_K)}{2^{r_1}\pi^{r_2}} =: C. \tag{6.3}$$

那么根据 Minkowski 定理, 存在 $0 \ne \alpha_0 \in \mathcal{O}_K \cap X_0$ 且

$$|N(\alpha_0)| = |\alpha_0|_\infty \le C$$

现在对某个固定的 $\sigma_0 \in S_\infty$, 我们定义

$$X_1 = \{(x_\sigma)_{\sigma\in S_\infty} \in K_\infty : \text{ 当}\sigma \ne \sigma_0 \text{ 时}, |x_\sigma|_\sigma \le \frac{|\sigma(\alpha_0)|_\sigma}{2}, |x_{\sigma_0}|_{\sigma_0} \le C_1, \}$$

这里 $C_1 \in \mathbb{R}$ 使得 $\mu(X_1) = 2^n\mathrm{vol}(\mathcal{O}_K)$. 那么对任意的 $x \in X_1$, 仍旧有(6.3)的不等式成立. 再根据 Minkowski 定理, 我们得到 $0 \ne \alpha_1 \in \mathcal{O}_K \cap X_1$, 且 α_1 满足

$$|N(\alpha_1)| \le C,$$

$$\text{当}\sigma \ne \sigma_0 \text{ 时}, |\sigma(\alpha_1)|_\sigma < |\sigma(\alpha_0)|_\sigma.$$

依此下去, 我们可以得到一列 $\alpha_0, \alpha_1, \cdots$, 满足对每个 i

$$|N(\alpha_i)| \le C,$$

$$\text{当}\sigma \ne \sigma_0 \text{ 时}, |\sigma(\alpha_i)|_\sigma < |\sigma(\alpha_{i-1})|_\sigma.$$

但是范小于等于 C 的主 (整) 理想只有有限个, 所以存在 $i < j$ 使得 $(\alpha_i) = (\alpha_j)$. 令

$$u_{\sigma_0} = \alpha_i/\alpha_j.$$

则 u_{σ_0} 是单位且满足

$$|u_{\sigma_0}|_{\sigma_0} > 1 \text{ 以及} |u_\sigma|_\sigma < 1 \text{ 对任意}\sigma \ne \sigma_0.$$

也就是说 $\iota(u)$ 这个向量在 σ_0 处是正的, 在其他处是负的, 且所有分量之和是 0:

$$\iota(u_{\sigma_0}) = (-, \cdots, -, \underset{\sigma_0}{+}, -\cdots, -).$$

当 σ_0 取遍 S_∞ 时, 我们得到了 $r_1 + r_2 - 1$ 个单位 $\{u_\sigma : \sigma \in S_\infty\}$. 根据下面的引理 $\iota(\sigma), (\sigma \in S_\infty)$ 生成了 $(\mathbb{R}^{r_1+r_2-1})^0$. 这就证明了 $\iota(\mathcal{O}_K^\times)$ 是 $(\mathbb{R}^{r_1+r_2})^0$ 中的满格, 从而(6.2)中的第三项是紧的.

引理 6.5. *设 G 是拓扑群, H 是 G 的紧子群使得 G/H 紧. 则 G 紧.*

证明. 留给感兴趣的同学. □

引理 6.6. *若一个 m 阶实数方阵的每行之和是 0, 对角线元素均正, 其他元素均负. 则此阵的秩是 $m-1$.*

证明. 练习. □

7 第六讲: 素理想分解

设 K 是 n 次数域, p 是素数. 我们考虑 $(p)=p\mathcal{O}_K$ 的素理想分解:

$$p\mathcal{O}_K=\prod_{i=1}^{g}\mathfrak{p}^{e_i}.$$

$\mathbb{Z}\subset\mathcal{O}_K$ 诱导了域嵌入 $\mathbb{Z}/p\mathbb{Z}\hookrightarrow\mathcal{O}_K/\mathfrak{p}_i$. 因为 $\mathcal{O}_K$ 是有限生成的 $\mathbb{Z}$ 模, $\mathcal{O}_K/\mathfrak{p}$ 是 $\mathbb{Z}/p\mathbb{Z}$ 的有限扩张. 这是个有限域的扩张 (练习), 记 $f_i=f(\mathfrak{p}_i/p)$ 为扩张次数, 称为 $\mathfrak{p}_i$ 关于 p 的**剩余类域次数** (或者**惯性指数**). $e_i=e(\mathfrak{p}_i/p)$ 称作**分歧指数**.

定理 7.1.

$$\sum_{i=1}^{g}e_if_i=n.$$

证明. 根据中国剩余定理, 我们有 $\mathbb{F}_p$-代数同构:

$$\mathcal{O}_K/p\mathcal{O}_K\cong\prod_{i=1}^{g}\mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

由于 $\mathcal{O}_K\cong\mathbb{Z}^n$, 故左边同构于 $(\mathbb{Z}/p\mathbb{Z})^n$, 即左边的 $\mathbb{F}_p$ 维数是 n.

所以我们只需证明右边每一项的 $\mathbb{F}_p$ 维数是 e_if_i. 由命题3.4知 $\mathfrak{p}_i^k/\mathfrak{p}_i^{k+1}$ 是一维的 $\mathcal{O}_K/\mathfrak{p}_i$ 空间, 所以是 f_i 维的 $\mathbb{F}_p$ 空间. 现在考虑

$$\mathcal{O}_K\supset\mathfrak{p}_i\supset\cdots\supset\mathfrak{p}_i^{e_i}.$$

我们有 $\dim\mathcal{O}_K/\mathfrak{p}_i^{e_i}=\dim\mathcal{O}_K/\mathfrak{p}_i+\cdots+\dim\mathfrak{p}_i^{e_i-1}/\mathfrak{p}_i^{e_i}=e_i\dim\mathcal{O}_K/\mathfrak{p}_i=e_if_i$. 证毕. □

定理 7.2. *设 $\alpha\in\mathcal{O}_K$ 使得 $K=\mathbb{Q}(\alpha)$ 且 $p\nmid[\mathcal{O}_K:\mathbb{Z}[\alpha]]$. 记 $f(T)\in\mathbb{Z}[T]$ 是 α 在 $\mathbb{Q}$ 上的极小多项式. 设 $\overline{f(T)}:=f(T)\bmod(p)$ 在 $\mathbb{F}_p[T]$ 中的素因子分解为*

$$\overline{f(T)}=\overline{f_1(T)}^{e_1}\cdots\overline{f_g(T)}^{e_g}.$$

则 $(p,f_i(\alpha)):=p\mathcal{O}_K+f_i(\alpha)\mathcal{O}_K$ $(i=1,\cdots,g)$ 是 $\mathcal{O}_K$ 的两两不同的素理想且

$$p\mathcal{O}_K=(p,f_1(\alpha))^{e_1}\cdots(p,f_g(\alpha))^{e_g},$$

以及 $e(\mathfrak{p}_i/p)=e_i$, $f(\mathfrak{p}_i/p)=f_i$.

证明. 显然 $\mathcal{O}_K$ 与 $\mathbb{Z}[\alpha]$ 都是秩为 n 的有限 abel 群, 故商群 $\mathcal{O}_K/\mathbb{Z}[\alpha]$ 是有限 abel 群, 且由条件知 p 不整除它的阶故而 p 倍映射是同构:

$$\mathcal{O}_K/\mathbb{Z}[\alpha]\to\mathcal{O}_K/\mathbb{Z}[\alpha],\quad x\bmod\mathbb{Z}[\alpha]\mapsto px\bmod\mathbb{Z}[\alpha].$$

满射给出了 $\mathcal{O}_K=\mathbb{Z}[\alpha]+p\mathcal{O}_K$ 单射给出了 $\mathbb{Z}[\alpha]\cap p\mathcal{O}_K=p\mathbb{Z}[\alpha]$. 那么自然嵌入 $\mathbb{Z}[\alpha]\hookrightarrow\mathcal{O}_K$ 诱导了同构

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]\cong\mathcal{O}_K/p\mathcal{O}_K.$$

由环同态基本定理和中国剩余定理知

$$\mathbb{Z}[\alpha]/p\mathbb{Z}[\alpha]\cong\mathbb{Z}[T]/(p,f(T))\cong\mathbb{F}_p[T]/(\overline{f(T)})\cong\prod_{i=1}^{g}\mathbb{F}_p[T]/(\overline{f_i(T)}^{e_i}).$$

上面的同构诱导了

$$\mathcal{O}_K/\mathfrak{p}_i\cong\mathbb{F}_p[T]/(\overline{f_i(T)}),$$

由于 $(\overline{f_i(T)})$ $(i=1,\cdots,g)$ 是 $\mathbb{F}_p[T]$ 包含 $(\overline{f(T)})$ 两两不同的极大理想, $\mathfrak{p}_i=(p,f_i(\alpha)),(i=1,\cdots,g)$ 是 $\mathcal{O}_K$ 的两两不同的极大理想. 且 $\mathfrak{p}_i$ 的剩余类域次数等于 $\deg f_i(T)$.

下面来证明 $p\mathcal{O}_K=\prod\mathfrak{p}_i^{e_i}$. 利用上面的同构和对应知

$$\mathcal{O}_K/(p,f_i^{e_i}(\alpha))\cong\mathbb{F}_p[T]/(\overline{f_i(T)}^{e_i}), \tag{7.1}$$

进而

$$\mathcal{O}_K/p\mathcal{O}_K\cong\prod_{i=1}^{g}\mathcal{O}_K/(p,f_i^{e_i}(\alpha)).$$

这推出了

$$p\mathcal{O}_K\supset\bigcap_{i=1}^{g}(p,f_i^{e_i}(\alpha))$$

利用显然的包含 $(p,f_i^{e_i}(\alpha))\supset\mathfrak{p}_i^{e_i}$. 我们有

$$p\mathcal{O}_K\supset\bigcap_{i=1}^{g}\mathfrak{p}_i^{e_i}=\prod_{i=1}^{g}\mathfrak{p}_i^{e_i}.$$

最后一步利用了 $\mathfrak{p}_i$ $(i=1,\cdots,g)$ 两两不同. 另一方面, $\mathcal{O}_K/p\mathcal{O}_K$ 的 $\mathbb{F}_p$-维数是 n, 由(7.1)知 $\mathcal{O}_K/\mathfrak{p}_i^{e_i}$ 的 $\mathbb{F}_p$ 维数等于 $e_i\deg f_i(T)$, 故 $\prod_i\mathfrak{p}_i^{e_i}$ 的 $\mathbb{F}_p$ 维数是 $\sum e_i\deg f_i(T)=\deg f(T)=n$. 这就证明了上述包含是等号. □

8 第七讲: Eisenstein 多项式, Dedekind 判别式定理及应用

引理 8.1. *设 $\alpha,\beta\in K$, $\mathfrak{p}$ 是素理想, 约定 $v_\mathfrak{p}(0)=\infty$. 则 $v_\mathfrak{p}(\alpha+\beta)\geq\min\{v_\mathfrak{p}(\alpha),v_\mathfrak{p}(\beta)\}$, 且当 $v_\mathfrak{p}(\alpha)\neq v_\mathfrak{p}(\beta)$ 时等号成立.*

证明. 由于 $\alpha+\beta\in(\alpha)+(\beta)$, 根据课后习题知引理中的不等式成立. 若 $v_\mathfrak{p}(\alpha)\neq v_\mathfrak{p}(\beta)$, 先设 $\alpha,\beta\in\mathcal{O}_K$, 以及 $r:=v_\mathfrak{p}(\alpha)>s:=v_\mathfrak{p}(\beta)$. 则 $\alpha+\beta\equiv0\bmod\mathfrak{p}^s$ 但 $\alpha+\beta\equiv\beta\not\equiv0\bmod\mathfrak{p}^{s+1}$, 也就是说 $v_\mathfrak{p}(\alpha+\beta)=s$. 一般情形, 取 $0\neq\gamma\in\mathcal{O}_K$ 使得 $\gamma\alpha,\gamma\beta\in\mathcal{O}_K$, 利用 $v_\mathfrak{p}(ab)=v_\mathfrak{p}(a)+v_\mathfrak{p}(b)$ 知等式显然. □

命题 8.2. *设 $f(T)\in\mathbb{Z}[T]$ 是关于素数 p 的 Eisenstein 多项式, π 是 $f(T)$ 的一个根. 记 $K=\mathbb{Q}(\pi)$, 则 $p\nmid[\mathcal{O}_K:\mathbb{Z}[\pi]]$.*

回顾: 首一 n 次整系数多项式 $f(T)\in\mathbb{Z}[T]$ 称作是关于素数 p 的 Eisenstein 多项式, 指 $f(T)\equiv T^n\bmod p$, 且 $p^2\nmid f(0)$. 这样的 $f(T)$ 在 $\mathbb{Z}[T]$ 中不可约; 若可约 $f(T)=g(T)h(T)$, 则 $g(T)\equiv T^i\bmod p, h(T)\equiv T^j\bmod p$, 则 $g(T)h(T)$ 的常数项将被 p^2 整除, 矛盾.

证明. 设 $\mathfrak{p}$ 是整除 p 的一个素理想, 显然 $\pi\in\mathfrak{p}$, 即 $v_\mathfrak{p}(\pi)>0$. 利用 $f(T)$ 是 Eisenstein 形式以及引理8.1知

$$v_\mathfrak{p}(\pi^n)=v_\mathfrak{p}(p).$$

根据定理7.1, $v_\mathfrak{p}(p)\leq n$, 所以 $v_\mathfrak{p}(\pi)$ 必须等于 1, 即 p 在 K 中完全分歧:

$$(p)=\mathfrak{p}^n.$$

现在来证明 $p \nmid [\mathcal{O}_K : \mathbb{Z}[\pi]]$. 若不成立, 则存在 $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}[\pi]$ 使 $p\alpha \in \mathbb{Z}[\pi]$. 那么存在 $a_0, \cdots, a_{n-1} \in \mathbb{Z}$ 且不全被 p 整除使得

$$p\alpha = a_0 + a_1\pi + \cdots a_{n-1}\pi^{n-1}.$$

注意到右边的 n 项的 $\mathfrak{p}$ 赋值各不相同, 故其 $\mathfrak{p}$ 赋值等于最小的那个, 即 $v_\mathfrak{p}(a_i\pi^i)$ 这里 i 是 $0, 1, \cdots, n-1$ 中最小使得 $p \nmid a_i$. 而 $v_\mathfrak{p}(a_i\pi^i) = v_\mathfrak{p}(\pi^i) = i < v_\mathfrak{p}(p) = n$, 矛盾. □

引理 8.3. 设 $K = \mathbb{Q}(\alpha)$, $\alpha \in \mathcal{O}_K$ 使得 $p^2 \nmid \operatorname{disc}(1, \alpha, \cdots, \alpha^{n-1})$. 则 $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

证明. 设 $\alpha_1, \cdots, \alpha_n$ 是 $\mathcal{O}_K$ 的一组整基, 则存在整系数矩阵 C 使得 $(1, \alpha, \cdots, \alpha^{n-1}) = (\alpha_1, \cdots, \alpha_n)C$. 根据有限生成 abel 群的理论知

$$|\det C| = [\mathcal{O}_K : \mathbb{Z}[\alpha]].$$

根据线性代数知

$$\operatorname{disc}(1, \alpha, \cdots, \alpha^{n-1}) = \operatorname{disc}(\alpha_1, \cdots, \alpha_n) \det C^2.$$

由此结论显然. □

命题 8.4. 设 $\zeta = \zeta_{p^k}$ 是 p^k 次本原单位根, 则 $K = \mathbb{Q}(\zeta)$ 是 $\phi(p^k)$ 次数域, p 在 K 中完全分歧, $\mathcal{O}_K = \mathbb{Z}[\zeta]$, $d_K = (-1)^{\phi(p^k)} p^{k\phi(p^k) - p^{k-1}}$.

证明. 如下是 $1 - \zeta$ 的零化多项式

$$f(T) := \frac{(1+T)^{p^k} - 1}{(1+T)^{p^{k-1}} - 1}.$$

这是个关于 p 的 Eisenstein 多项式, 所以不可约. 故 $[K : \mathbb{Q}] = \phi(p^k)$. 利用习题的计算判别式公式可得 (留作练习)

$$\operatorname{disc}(f) = (-1)^{\phi(p^k)/2} p^{k\phi(p^k) - p^{k-1}}.$$

根据上面引理和命题8.2知 $[\mathcal{O}_K : \mathbb{Z}[\zeta]] = 1$. 从而 $d_K = \operatorname{disc}(f)$. □

对奇素数 p, $\mathbb{Q}(\zeta_p)$ 的判别式就是 $(-1)^{\frac{p-1}{2}} p$. 这给出如下有趣的推论. 对 $m \geq 1$, 称 $\mathbb{Q}(\zeta_m)$ 是 m 阶**分圆域**.

推论. *(1) 对奇素数 p, $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p}) \subset \mathbb{Q}(\zeta_p)$;*

(2) 任何二次域都是分圆域的子域.

证明. 对任意 n 次数域 K, 如果 $K/\mathbb{Q}$ 是正规扩张, 即对每个 $\sigma_i : K \to \overline{\mathbb{Q}}$ $(i = 1, \cdots, n)$, 都有 $\sigma_i(K) = K$. 我们知道 K 中一组元素的判别式

$$\operatorname{disc}(\alpha_1, \cdots, \alpha_n) = \det(\sigma_i(\alpha_j)_{i,j})^2,$$

所以 $\operatorname{disc}(\alpha_1, \cdots, \alpha_n)$ 是 K 中的平方元. 分圆域显然是正规扩张, 根据命题8.4的计算知 $d_{\mathbb{Q}(\zeta_p)} = (-1)^{\frac{p-1}{2}} p^{p-2}$, 由此推出 (1).

对于 (2), 首先注意到 $(\zeta_8 + \zeta_8^{-1})^2 = 2$, 由此 $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$. 那么对任意无平方因子的整数 $d = \pm p_1, \cdots, p_k$, p_i 是素数,

$$\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_8, \zeta_{p_1}, \cdots, \zeta_{p_k}) \subset \mathbb{Q}(\zeta_{8|d|}).$$

□

练习: 加强上面的 (2) 为: 若二次域 K 的判别式是 d, 则 $K \subset \mathbb{Q}(\zeta_{|d|})$.

下面回到一般的数域 K. 迹映射 $\mathrm{Tr} : \mathcal{O}_K \to \mathbb{Z}$ 诱导了线性映射 (我们仍用 Tr 表示)

$$\mathrm{Tr} : \mathcal{O}_K/p\mathcal{O}_K \to \mathbb{F}_p.$$

它又给出了双线性型 $\langle , \rangle$:

$$\mathcal{O}_K/p\mathcal{O}_K \times \mathcal{O}_K/p\mathcal{O}_K \to \mathbb{F}_p, \quad \langle \bar{\alpha}, \bar{\beta} \rangle = \mathrm{Tr}(\bar{\alpha\beta})$$

类似的我们也可以定义 $\mathcal{O}_K/p\mathcal{O}_K$ 中 n 个元素的判别式为 $\langle , \rangle$ 的度量矩阵的行列式. 若 $\alpha_1, \cdots, \alpha_n$ 是 K 的一组整基, 则 $\overline{\alpha}_1, \cdots, \overline{\alpha}_n$ 是 $\mathcal{O}_K/p\mathcal{O}_K$ 的一组 $\mathbb{F}_p$-基. 那么

$$d_K \bmod p = \mathrm{disc}(\overline{\alpha}_1, \cdots, \overline{\alpha}_n).$$

定理 8.5. *设 K 是数域. p 在 K 中分歧当且仅当 $p \mid d_K$.*

证明. 由中国剩余定理,

$$\mathcal{O}_K/p\mathcal{O}_K \cong \prod_{i=1}^{g} \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

如果 p 分歧, 则存在 $e = e_i > 1$. 取 $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, 易见 $0 \neq \bar{\pi}$ 是个幂零元. 则对任意 $\bar{\alpha} \in \mathcal{O}_K/p\mathcal{O}_K$, $\overline{\alpha\pi}$ 也是幂零元, 从而 $\mathrm{Tr}(\alpha\pi) = 0$. 这就说明了 $\langle , \rangle$ 是退化的. 根据线性代数, $p \mid d_K$.

如果 p 是非分歧的, 则 $\mathcal{O}_K/p\mathcal{O}_K$ 是 g 个域的直积. 根据有限可分扩张的一般理论, $\langle , \rangle$ 限制在 $\mathcal{O}_K/\mathfrak{p}_i$ 上是非退化的. 由于当 $i \neq j$ 时 $\mathcal{O}_K/\mathfrak{p}_i$ 与 $\mathcal{O}_K/\mathfrak{p}_j$ 中元素相乘等于 0, 所以 $\langle \mathcal{O}_K/\mathfrak{p}_i, \mathcal{O}_K/\mathfrak{p}_j \rangle = 0$. 由此可知, 若 $e_{i1}, \cdots, e_{it_i}$ 是 $\mathcal{O}_K/\mathfrak{p}_i$ 的一组基, 在 $\mathbb{F}_p$ 中,

$$\mathrm{disc}(e_{11}, \cdots, e_{1t_1}, \cdots, e_{g1}, \cdots, e_{gt_g}) = \prod_{i=1}^{g} \mathrm{disc}(e_{i1}, \cdots, e_{it_i}) \neq 0.$$

从而 $d_K \not\equiv 0 \bmod p$. □

利用之前的 Minkowski 界 (定理8) 可得如下关于数域的重要事实:

定理 8.6 (Minkowski)**.** *若数域 $K \neq \mathbb{Q}$, 则存在素数 p 在 K 中分歧.*

证明. 根据定理知, 对任何整理想 $\mathfrak{a}$ 都存在 $\alpha \in \mathfrak{a}$ 使得 $M_K \geq \mathbf{N}((\alpha)\mathfrak{a}^{-1}) \geq 1$. 所以

$$\sqrt{|d_K|} \geq (\frac{\pi}{4})^{r_2} \frac{n^n}{n!}.$$

简单估计知当 $n \geq 2$ 时 $|d_K| > 1$. 根据定理8.5, 存在素数 p 在 K 中分歧. □

下面考虑一般分圆域 $K = \mathbb{Q}(\zeta)$, $\zeta = \zeta_m = e^{\frac{2\pi i}{m}}$, $m \in \mathbb{Z}_{\geq 1}$. 显然 $K/\mathbb{Q}$ 是 Galois 的, 对任意 $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, 则存在 $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ 使得 $\sigma(\zeta) = \zeta^a$. 这给出了单同态:

$$\mathrm{Gal}(K/\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^\times, \quad \sigma \mapsto a \bmod m, \text{ 如果} \sigma(\zeta) = \zeta^a.$$

Gauss 证明了如下定理:

定理 8.7. *上面的同态是同构, 等价地, $[K : \mathbb{Q}] = \phi(m)$, 这里 $\phi(m) := \#(\mathbb{Z}/m\mathbb{Z})^\times$ 是欧拉函数.*

证明. (Gauss 的证明) 设 $f(T) \in \mathbb{Z}[T]$ 是 ζ 的极小多项式, 我们需要证明对任意与 m 互素的整数 a, $f(\zeta^a) = 0$. 由于 a 是由素数乘积得到的, 显然我们只需证明对任意素数 p 满足 $p \nmid m$, $f(\zeta^p) = 0$. 令 $g(T) \in \mathbb{Z}[T]$ 使得 $T^m - 1 = fg$. 如果 $f(\zeta^p) \neq 0$, 则必有 $g(\zeta^p) = 0$. 从而 $f(T) \mid g(T^p)$. 模 p

得 $\bar{f} \mid \bar{g}^p$. 从而 $\bar{f}, \bar{g}$ 在 $\mathbb{F}_p[T]$ 中有非平凡公因子. 那么 $T^m - 1$ 模 p 就有重根. 但另一方面, 由于 $p \nmid m$, $T^m - 1$ 与其导函数 mT^{m-1} 显然互素. 这就矛盾. 定理得证.

□

若 $m \equiv 2 \bmod 4$, 有 $\zeta_m = -\zeta_{m/2}$, 那么 $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{m/2})$, 所以我们假定 $m \not\equiv 2 \bmod 4$.

引理 8.8. *设 $m \not\equiv 2 \bmod 4$. 则 p 在 K 中分歧当且仅当 $p \mid m$.*

证明. 若 $p \mid m$, 则 p 在 $\mathbb{Q}(\zeta_p)$ 中分歧, 而 $\mathbb{Q}(\zeta_p) \subset K$, 易见 p 在 K 中分歧. 若 $p \nmid m$, 则 $T^m - 1$ 模 p 没有重根, 所以 p 在 K 中是非分歧的. □

现在利用 Minkowski 判别式界再给一个定理8.7的证明:

Minkowski 判别式界 + Dedekind 判别式定理. 首先证明若 M, N 是两个互素的整数, 则 $F := \mathbb{Q}(\zeta_M) \cap \mathbb{Q}(\zeta_N) = \mathbb{Q}$. 如若不然, 则根据 Minkowski 判别式界知 $|d_F| > 1$, 所以有 p 在 F 中分歧, 但根据上面引理知 p 一定同时整除 M 和 N, 而 M, N 互素, 矛盾! 再注意到当 M, N 互素时, $\mathbb{Q}(\zeta_M, \zeta_N) = \mathbb{Q}(\zeta_{MN})$. 根据 Galois 理论知限制映射诱导了同构

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{MN})/\mathbb{Q}(\zeta_M)) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}).$$

所以

$$[\mathbb{Q}(\zeta_{MN} : \mathbb{Q}] = [\mathbb{Q}(\zeta_M : \mathbb{Q}][\mathbb{Q}(\zeta_N : \mathbb{Q}].$$

这就把问题归化为 m 是素数方幂的情形, 而这是知道的. □

8.1 计算: 整基的求法

我讲课堂上所讲的例子抽象出来, 写一个对任意数域求整基与判别式的算法; 但必须强调下面这个算法实际效率不高, 对于更高效的算法见计算代数数论方面的书籍 (例如 GTM138).

实际中, 给出一个数域 K 通常是给一个 n 次首一不可约多项式 $f(T) \in \mathbb{Z}[T]$. $K = \mathbb{Q}(\alpha)$, $f(\alpha) = 0$. 对任何 $\beta \in K$, 可这样判断 β 是否整: 先求出 α 在一组基 (比如 $1, \alpha, \cdots, \alpha^{n-1}$) 下的矩阵 (这里 α 指 α 诱导的线性变换 $\mathcal{A}_\alpha : x \mapsto x\alpha$), 则对任意 $\beta = r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1}$, $r_i \in \mathbb{Q}$, 可写出 β 的矩阵, β 是代数整数当且仅当其特征多项式是整系数的. 下面给出个求整基的步骤:

- 算出 $\mathrm{disc}(f) = \mathrm{disc}(1, \alpha, \cdots, \alpha^{n-1})$; 若 $\mathrm{disc}(f)$ 平方自由, 则 $\mathcal{O}_K = \mathbb{Z}[\alpha]$, 算法终止.

  这是利用了 $\mathrm{disc}(f) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 d_K$ 得出对 $p^2 \nmid \mathrm{disc}(f)$ 的素数 p, 有 $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$.

- 对每个满足 $p^2 \mid \mathrm{disc}(f)$ 的 p, 考虑有限集合

  $$\{\frac{a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1}}{p} \in K : a_i = 0, 1, \cdots, p-1, \text{ 且不全为0}\}.$$

  对这个集合中的每个元素, 计算它是否为代数整数. 若均不是代数整数, 则 $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. 若里面某个元素

  $$\alpha' := \frac{a_0 + a_1\alpha + \cdots a_{n-1}\alpha^{n-1}}{p} \text{ 是代数整数}, a_k \neq 0,$$

则 $1, \alpha, \cdots, \alpha^{k-1}, \alpha', \alpha', \cdots, \alpha^{n-1}$ 的判别式等于 $\mathrm{disc}(f)/p^2$. 然后对这组元素重复上面的进程.

练习: 验证上面一步的合理性.

实际中算法的第二步有时可利用 *Eisenstein* 判别法优化, 比如说, 若能找到某个 $a \in \mathbb{Z}$ 使得 $f(T+a)$ 是 *p-Eisenstein* 的, 则 $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]$

例 8.1. 设 $K = \mathbb{Q}(\sqrt[3]{2})$. 因为 $\mathrm{disc}(T^3 - 2) = -4 * 27$, 所以 $[\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}]]$ 的素因子只可能有 2 和 3. 而 $T^3 - 2$ 是 2-Eisenstein 多项式, $(T-1)^3 - 2$ 是 3-Eisenstein 多项式, 所以 $\mathcal{O}_K$ 就是 $\mathbb{Z}[\sqrt[3]{2}] = \mathbb{Z}[\sqrt[3]{2}+1]$. (对这个例子如果用上面一般的算法, 很耗时.)

8.2 Dedekind 的例子 $f(T) = T^3 - T^2 - 2T - 8$.

标题中的 $f(T)$ 是不可约多项式, 因为如果可约就有一次多项式因子, 根据 Gauss 引理 $T - a$ $a \in \mathbb{Z}$ 整除 $f(T)$, 这就推出 $a = \pm 1, \pm 2, \pm 4, \pm 8$, 然而它们都不是 $f(T)$ 的根. $f(T)$ 的不可约性也能从模 3 看出: $f(0), f(1), f(2)$ 均模 3 不为 0.

令 α 是上面标题中 $f(T)$ 的根, 则 $K = \mathbb{Q}(\alpha)$ 是三次域. 计算得 $\mathrm{disc}(f) = -4 \times 503$. 所以 $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = 1$ 或者 2. 我们应用前小节的一般算法来判断. 考虑集合

$$\{\frac{a_0 + a_1\alpha + a_2\alpha^2}{2} : a_i = 0 \text{ 或1 且不全为0.}\}$$

验算里面的数是否为代数整数, 当然 1/2 显然不是, 然后我们发现 $\frac{\alpha+\alpha^2}{2} \in \mathcal{O}_K$. 实际上, $\beta := 4/\alpha$ 是如下首一整系数多项式的根

$$g(T) = \frac{T^3 f(4/T)}{-8} = T^3 + T^2 + 2T - 8.$$

且 $\beta = \frac{\alpha^2+\alpha}{2} + 1$. 这说明了 $\beta \in \mathcal{O}_K$ 且

$$\mathrm{disc}(1, \alpha, \beta) = -503 \text{ 从而} d_K = -503.$$

这推出了 $\mathcal{O}_K$ 的一组整基是 $1, \alpha, \beta$. 通过计算可知, $\alpha^2 \equiv \alpha \bmod 2\mathcal{O}_K$, $\beta^2 \equiv \beta \bmod 2\mathcal{O}_K$, 从而对任意 $\gamma \in \mathcal{O}_K$, 有 $\gamma^2 \equiv \gamma \bmod 2\mathcal{O}_K$. 由此知 $\mathrm{disc}(1, \gamma, \gamma^2) \equiv 0 \bmod 2$. 这就推出了对每个 $\gamma \in \mathcal{O}_K$, 有 $2 \mid [\mathcal{O}_K : \mathbb{Z}[\gamma]]$.

我们断言 2 在 K 中实际上是完全分裂的. 先承认这个断言. 这反过来也说明了 $\mathcal{O}_K$ 不可能等于 $\mathbb{Z}[\gamma]$. 如若不然, 根据定理7.2知 γ 的极小多项式在 $\mathbb{F}_2[T]$ 中分解成三个不相同的一次多项式的乘积, 但 $\mathbb{F}_2$ 只有两个元素, 不可能!

下面来证明这个断言. 设 $\mathbb{Z}[T, S]$ 为 $\mathbb{Z}$ 上二元多项式环. 考虑环同态:

$$\mathbb{Z}[T, S] \to \mathbb{Z}[\alpha, \beta], \quad T \mapsto \alpha, S \mapsto \beta.$$

这显然是满射, 它的核 I 包含了 α 和 β 的所有代数关系. 观察 $f(T), g(T)$ 得以下关系:

$$0 = f(\alpha) = g(\beta) = \alpha^2 - \alpha - 2 - 2\beta = \alpha\beta - 4 = \beta^2 + \beta + 2 - 2\alpha.$$

实际上 $I = (T^2 - T - 2 - 2S, TS - 4, S^2 + S + 2 - 2T)$. 这是因为 $\mathbb{Z}[T, S]/I$ 是秩 3 的自由 $\mathbb{Z}$-模,

(一组基是 $1, T, S$ 在商环中的像). 而 $\mathbb{Z}[T,S]/I \to \mathcal{O}_K \cong \mathbb{Z}^3$ 是满射, 故只能是同构. 所以就有

$$\mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2[T,S]/(T^2-T, TS, S^2+S).$$

根据中国剩余定理, 2 在 $\mathcal{O}_K$ 中完全分裂当且仅当 $\mathcal{O}_K/2\mathcal{O}_K$ 有三个极大理想. 而 $(T,S), (T,S+1), (T-1,S)$ 在右边商环中的像就是两两不同的三个极大理想. (练习: 验证这三个其实是右边的主理想.) 写成 $\mathcal{O}_K$ 中理想的形式, 我们有

$$2\mathcal{O}_K = (2,\alpha,\beta)(2,\alpha,\beta+1)(2,\alpha-1,\beta).$$

我们将在习题课上演示, 实际上 K 的类数是 1, 特别的右边这三个理想都是主理想.

9 第六讲 (一般版本): 扩张中的素理想

这部分内容是第六讲的交换代数推广.

9.1 局部化

设 A 是 (交换) 整环, 分式域是 K, $S \subset A$ 是非零乘性子集. 定义 K 的子环

$$S^{-1}A := \{\frac{a}{s} \in K : a \in A, s \in S\}.$$

显然 $A \subset S^{-1}A$. 若 $\mathfrak{a}$ 是 A 的理想, 记 $S^{-1}\mathfrak{a}$ 为 $\mathfrak{a}$ 在 $S^{-1}A$ 中生成的理想. 容易验证 $S^{-1}A$ 中的任何理想都形如 $S^{-1}\mathfrak{a}$. (留作练习). 特别的, 诺特环的局部化依旧是诺特. 这里我们只对整环定义了局部化, 一般情形参考 Atiyah.

引理 9.1. *(1) 若 $\mathfrak{p}$ 是与 S 不交的素理想, 我们有 $S^{-1}\mathfrak{p} \cap A = \mathfrak{p}$.*

(2) 我们有一一对应:

$$\{A \text{ 中与} S \text{ 不交的素理想}\} \leftrightarrow \{S^{-1}A \text{ 的素理想},\}$$

$$\mathfrak{p} \mapsto S^{-1}\mathfrak{p}.$$

证明. (1) 设 $b \in S^{-1}\mathfrak{p} \cap A$, 则 $b = \frac{a}{s}$ 其中 $a \in \mathfrak{p}$, $s \in S$. 则 $a = bs \in \mathfrak{p}$, 但由条件知 $s \notin \mathfrak{p}$, 故 $b \in \mathfrak{p}$. 另一方面我们显然有 $\mathfrak{p} \subset S^{-1}\mathfrak{p} \cap A$, 故 (1) 中等号成立.

(2) 由 (1) 显然. □

推论. *设 $\mathfrak{p}$ 是素理想, 则 $S = A \setminus \mathfrak{p}$ 是乘性子集. 此时记 $S^{-1}A = A_{\mathfrak{p}}$. 则 $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ 同构于整环 $A/\mathfrak{p}$ 的分式域; 特别的, 如果 $\mathfrak{p}$ 是极大理想, 自然映射 $A \to A_{\mathfrak{p}}$ 诱导了域同构 $A/\mathfrak{p} \cong A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$.*

证明. 根据素理想的定义知 S 是乘性子集. 设 $\bar{S}$ 是 S 在 $A/\mathfrak{p}$ 中的像, 即 $\bar{S}$ 是整环 $A/\mathfrak{p}$ 中的所有非零元之集. 则 $A/\mathfrak{p}$ 的分式域为 $\bar{S}^{-1}(A/\mathfrak{p})$. 映射

$$S^{-1}A/S^{-1}\mathfrak{p} \to \bar{S}^{-1}(A/\mathfrak{p}), \quad \frac{a}{s} \bmod S^{-1}\mathfrak{p} \mapsto \frac{\bar{a}}{\bar{s}}$$

显然是同构. □

引理 9.2. *设 $A \subset C$ 是整环. 设 B 是 A 在 C 中的整闭包. 则对任意乘性子集 $S \subset A$, $S^{-1}A$ 在 $S^{-1}C$ 中的整闭包是 $S^{-1}B$.*

证明. 第一周习题. □

定义 9.3. 整环 A 称作是离散赋值环, 如果它是局部环, 且任何理想都形如 $\mathfrak{m}^k$, $\mathfrak{m}$ 是 A 的极大理想, $k \in \mathbb{Z}_{\geq 0}$.

取 $a \in \mathfrak{m}$ 使得 $(\pi) = \mathfrak{m}^k$ 中的 k 最小, 那么 $k = 1$, 从而 $\mathfrak{m} = (\pi)$. 任何理想都形如 (π^k), 所以离散赋值环是 PID.

引理 9.4. *设 A 是 Dedekind 整环, $\mathfrak{p} \subset A$ 是非零素理想. 则 $A_\mathfrak{p}$ 是离散赋值环, 特别的 $A_\mathfrak{p}$ 是 PID.*

证明. 因为 A 是诺特整闭的, 所以 $A_\mathfrak{p}$ 也是. 而且 $A_\mathfrak{p}$ 只有一个非零素理想 $\mathfrak{p}$, 所以 $A_\mathfrak{p}$ 是 Dedekind 整环. 由 Dedekind 整环的习题知, 只有有限个素理想的 Dedekind 整环是主理想整环, 所以 $\mathfrak{p} = (\pi)$. 而 Dedekind 整环中任何理想都是素理想的乘积, 所以 $A_\mathfrak{p}$ 是离散赋值环. □

9.2 Dedekind 整环的扩张

引理 9.5. *设 $A \subset B$ 是环且 B 在 A 上整. 若 $\mathfrak{a}$ 是 A 的非平凡理想, 则 $\mathfrak{a}B \neq B$.*

在 $A = \mathbb{Z}$, $B = \mathcal{O}_K$ 或者 $\bar{\mathbb{Z}}$ 的时候, 这个结论较为显然.

证明. 若 $\mathfrak{a}B = B$, 则存在 $\alpha_1, \cdots, \alpha_t \in \mathfrak{a}$, $b_1, \cdots, b_t \in B$ 使得 $1 = \sum_i b_i \alpha_i$. 令 $B' = A[b_1, \cdots, b_t]$. 则 B' 也在 A 上整且有限生成, 故 B' 是有限生成的 A-模, 即存在 $\omega_1, \cdots, \omega_m$ 使得

$$B' = A\omega_1 + \cdots + A\omega_m \quad \text{且} \mathfrak{a}B' = B'.$$

特别的, 存在 $\mathfrak{a}$-系数的矩阵 $M = (a_{ij})_{i,j}$ 使得 $(\omega_1, \cdots, \omega_m) = (\omega_1, \cdots, \omega_m)M$. 即 $(\omega_1, \cdots, \omega_m)(I_m - M) = 0$. 两边右乘 $I_m - M$ 的伴随矩阵得 $d(\omega_1, \cdots, \omega_m)) = 0$, 这里 d 是 $I_m - M$ 的行列式, 从而 $d \cdot dB' = 0$. 将 $I_m - M$ 的行列式展开即看出 $1 \in \mathfrak{a}$, 矛盾. □

定义 9.6. *ABLK* 设 A 是 Dedekind 整环, 分式域为 K; L/K 是有限可分 n 次扩张, B 是 A 在 L 中的整闭包. 由注2.7知 B 也是 Dedekind 整环.

设 $\mathfrak{p}$ 是 A 的非零素理想, 则由引理9.5知 $\mathfrak{p}B \neq B$. 记 $\mathfrak{p}B$ 的素理想分解为

$$\mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}.$$

因为 B 是有限生成的 A 模, 故 $B/\mathfrak{P}$ 是 $A/\mathfrak{p}$ 的有限扩张, 称扩张次数为 $\mathfrak{P}$ 在 L/K 中的**剩余类域次数或惯性指数**, 记作 $f_\mathfrak{P}$ 或 $f_{\mathfrak{P}/\mathfrak{p}}$.

定理 9.7.

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_\mathfrak{P} f_\mathfrak{P} = n.$$

引理 9.8. *设 $S = A \setminus \mathfrak{p}$, 记 $A_\mathfrak{p} = S^{-1}A$, $B_\mathfrak{p} := S^{-1}B$ 分别是 A, B 关于 S 的局部化. 则*

(1) $B_\mathfrak{p}$ 是 $A_\mathfrak{p}$ 在 L 中的整闭包, 且 $B_\mathfrak{p} \cong A_\mathfrak{p}^n$;

(2) $B/\mathfrak{p}B \cong B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}$.

证明. (1) 的前半句是引理9.2(第一周习题) 的特例. 对于后半句, 我们取 $\alpha_1, \cdots, \alpha_n \in B_\mathfrak{p}$ 是 L 关于 K 的一组基, 则重复整基的存在性证明2.2知

$$A_\mathfrak{p}\alpha_1 + \cdots A_\mathfrak{p}\alpha_n \subset B_\mathfrak{p} \subset A_\mathfrak{p}\check{\alpha}_1 + \cdots + A_\mathfrak{p}\check{\alpha}_n.$$

再由引理9.4知 $A_{\mathfrak{p}}$ 是 PID, 所以 $B_{\mathfrak{p}} \cong A_{\mathfrak{p}}^n$.

(2) 满射性: 给定 $\frac{b}{s} \in B_{\mathfrak{p}}$ ($s \in A \setminus \mathfrak{p}, b \in B$), 因为 $s \notin \mathfrak{p}$ 以及 $\mathfrak{p} \subset A$ 是极大理想, 存在 $a \in A$, $a' \in \mathfrak{p}$ 使得 $as + a' = 1$. 则

$$\frac{b}{s} \equiv ab \bmod \mathfrak{p}B_{\mathfrak{p}}.$$

单射性: 取 $b = \frac{b}{s} \in B \cap \mathfrak{p}B_{\mathfrak{p}}$ ($b, b' \in B, s \in S$), 则根据理想唯一分解性及 (s) 与 $\mathfrak{p}B$ 互素知,$b \in \mathfrak{p}B$. 从而 $B \cap \mathfrak{p}B_{\mathfrak{p}} = \mathfrak{p}B$, 这就证明了单射性. □

证明. 根据中国剩余定理我们有 $k := A/\mathfrak{p}$-代数同构:

$$B/\mathfrak{p}B \cong \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}}. \tag{9.1}$$

由命题3.4知每个 $\mathfrak{P}^i/\mathfrak{P}^{i+1}$ 是一维的 $B/\mathfrak{P}$ 空间, 从而作为 k 空间是 $f_{\mathfrak{P}}$ 维的. 由

$$B \supset \mathfrak{P} \supset \cdots \supset \mathfrak{P}^{e_{\mathfrak{P}}},$$

知 $\dim B/\mathfrak{P}^{e_{\mathfrak{P}}} = e_{\mathfrak{P}} f_{\mathfrak{P}}$, 这里 dim 是作为 k 空间的维数. 从而

$$\dim \prod_{\mathfrak{P}|\mathfrak{p}} B/\mathfrak{P}^{e_{\mathfrak{P}}} = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}.$$

下面来证明左边的维数是 n.

取 A 的乘性子集 $S = A \setminus \mathfrak{p}$, 则由上面引理知 $S^{-1}B \cong (A_{\mathfrak{p}})^n$. 所以

$$B_{\mathfrak{p}}/(\mathfrak{p}B_{\mathfrak{p}}) \cong (A_{\mathfrak{p}}/(\mathfrak{p}A_{\mathfrak{p}}))^n \cong k^n.$$

最后一个同构是因为引理9.1的推论. 再利用上面引理第二条就证明了 $\dim B/\mathfrak{p}B = n$. □

我们称 $e_{\mathfrak{P}} = e_{\mathfrak{P}/\mathfrak{p}}$ 为 $\mathfrak{P}$ 在 L/K 中的**分歧指数**. 如果 $e_{\mathfrak{P}} = 1$, 称 $\mathfrak{P}$ 在 L/K 中是**非分歧**的; 否则称 $\mathfrak{P}$ 在 L/K 中分歧. 如果对所有 $\mathfrak{P} \mid \mathfrak{p}$ 有 $e_{\mathfrak{P}} = 1$, 称 $\mathfrak{p}$ 在 L/K 中非分歧, 否则称 $\mathfrak{p}$ 在 L/K 中分歧. 如果对每个 $\mathfrak{P} \mid \mathfrak{p}$, $e_{\mathfrak{P}} = f_{\mathfrak{P}} = 1$, 则根据上面公式知在 B 中整除 $\mathfrak{p}$ 的素理想恰有 n 个, 此时我们称 $\mathfrak{p}$ 在 L/K 中**完全分裂**. 如果 $e_{\mathfrak{P}} = n$, 则 $\mathfrak{p}B = \mathfrak{P}^n$, 我们称 $\mathfrak{P}$ 或 $\mathfrak{p}$ 在 L/K 中 **完全分歧**. 如果 $f_{\mathfrak{P}} = n$, 则 $\mathfrak{p}B$ 是素理想, 称 $\mathfrak{p}$ 在 L/K 中**惯性**.

下面的 Kummer 引理可对一大类 $\mathfrak{p} \subset A$ 具体计算 $\mathfrak{p}B$ 的分解.

定理 9.9. *设 $\alpha \in B$ 使得 $L = K(\alpha)$. 设 $\mathfrak{p}$ 是 A 的素理想使得 $B = \mathfrak{p}B + A[\alpha]$. 若 α 的极小多项式 $f(T) \in A[T]$ 在 $A/\mathfrak{p}[T]$ 中的不可约分解为*

$$f(T) = f_1^{e_1}(T) \cdots f_g^{e_g}(T) \bmod \mathfrak{p}.$$

则 $\mathfrak{P}_i = \mathfrak{p}B + f_i(\alpha)B$ ($i = 1, \cdots, g$) 是 B 的两两不同的素理想, $\mathfrak{P}_i$ 的剩余类域等于 $\deg f_i(T)$, 且

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}. \tag{9.2}$$

证明. 记剩余类域 $A/\mathfrak{p}$ 为 k. 我们断言 $A[\alpha] \hookrightarrow B$ 诱导如下环同构

$$A[\alpha]/\mathfrak{p}A[\alpha] \cong B/\mathfrak{p}B. \tag{9.3}$$

映射显然是良定义的. 满射是由条件 $B = \mathfrak{p}B + A[\alpha]$ 保证的. 两边都是 k 代数, 故只需说明两边的 k 维数相同. 而我们在上一个定理中的证明中已经看到 $B/\mathfrak{p}B$ 的维数是 n. 由于 $A[\alpha]$ 是自由的 A-模 (比如 $1, \alpha, \cdots, \alpha^{n-1}$ 是一组基), 故

$$A[\alpha]/\mathfrak{p}A[\alpha] \cong A[\alpha] \otimes_A k \cong A^n \otimes_A k \cong k^n.$$

所以(9.3)是同构, 断言成立.

根据环同态基本定理, 我们有同构

$$A[\alpha]/\mathfrak{p}A[\alpha] \cong A[T]/(\mathfrak{p}, f(T)) \cong k[T]/(\overline{f}). \tag{9.4}$$

在同构(9.3) 和(9.4)的对应下, $\mathfrak{P}_i$ 对应于 $k[T]$ 的理想 $\overline{f_i}$ 以及

$$k[T]/(\overline{f_i}) \cong B/(\mathfrak{p}B, \bar{f}_i B).$$

熟知 $k[T]/(\overline{f_i})$ 是域, 所以 $\mathfrak{P}_i$ $(i = 1, \cdots, g)$ 是两两不同的 B 的素理想, 且 $\mathfrak{P}_i$ 的剩余类域次数显然是 $\deg f_i$. 下面来证明(9.2). 根据中国剩余定理及上面的同构我们有下面同构交换图 (且右边每一项都分别同构)

$$\begin{array}{ccc} B/\mathfrak{p}B & \xrightarrow{\cong} & B/(\mathfrak{p}B, f_1^{e_1}(\alpha)B) \times \cdots \times B/(\mathfrak{p}B, f_g^{e_g}(\alpha)B) \\ \downarrow\cong & & \downarrow\cong \\ k[T]/(\bar{f}) & \xrightarrow{\cong} & k[T]/(\overline{f_1^{e_1}}) \times \cdots \times k[T]/(\overline{f_g^{e_g}}). \end{array}$$

再注意到显然的事实 $(\mathfrak{p}B, f_i^{e_i}(\alpha)B) \supset \mathfrak{P}_i^{e_i}$, 我们有

$$\mathfrak{p}B = \bigcap_{i=1}^{g} (\mathfrak{p}B, f_i^{e_i}(\alpha)B) \supset \bigcap_{i=1}^{g} \mathfrak{P}_i^{e_i} = \prod_{i=1}^{g} \mathfrak{P}^{e_i}.$$

第一个等号是根据上面图第一行, 最后一个等号是因为 $\mathfrak{P}_i (i = 1, \cdots, g)$ 两两不同的素理想故两两互素. 注意到

$$\dim_k B/\prod_{i=1}^{g} \mathfrak{P}^{e_i} = \sum_{i=1}^{g} \dim_k B/\mathfrak{P}^{e_i} = \sum_{i=1}^{g} e_i \deg f_i = n = \dim_k B/\mathfrak{p}B,$$

我们就有 $\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}^{e_i}$. □

我们给出一些已知 A, K, L 求 B 的方法.

引理 9.10. *设 $B' \subset B$ 是环. 则 $B' = B$ 当且仅当对所有 A 的非零素理想 $\mathfrak{p}$ 有 $B'_{\mathfrak{p}} = B_{\mathfrak{p}}$, 这里 $B'_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}B'$.*

证明. 如果 $B'_{\mathfrak{p}} = B_{\mathfrak{p}}$, 我们有

$$B_{\mathfrak{p}}/B'_{\mathfrak{p}} \cong (B/B') \otimes_A A_{\mathfrak{p}} = 0.$$

那么 $B/B' = 0$, 这是交换代数中的一个一般事实.

□

定义 9.11. 设 $\mathfrak{p} \subset A$, 若首一多项式 $f(T) \in A[T]$ 满足 $f(T) \equiv T^n \bmod \mathfrak{p}$, 且 $\mathfrak{p}^2$ 不整除 $f(T)$ 的常数项 $f(0)$, 我们称 $f(T)$ 是 (关于 $\mathfrak{p}$) 的 Eisenstein 多项式.

命题 9.12. *设 A 是 Dedekind 整环, $\mathfrak{p}$ 是 A 的一个非零素理想. (1) 设 $f(T) \in A[T]$ 是关于 $\mathfrak{p}$ 的 Eisenstein 多项式. 则 $f(T)$ 在 $K[T]$ 中不可约. 设 π 是 $f(T)$ 的一个根, 令 $L = K(\pi)$, B 是 A 在 L 中的整闭包. 则 $B_{\mathfrak{p}}/A_{\mathfrak{p}}[\pi] = (B/A[\pi]) \otimes_A A/\mathfrak{p} = 0$.*

(2) 设 $f(T) \in A[T]$ 是首一不可约多项式. 设 α 是 $f(T)$ 一个根, 令 $L = K(\alpha)$, B 是 A 在 L 中的整闭包. 若 $\mathfrak{p}$ 不整除 $f(T)$ 的判别式 $\operatorname{disc} f(T)$, 则 $B_{\mathfrak{p}}/A_{\mathfrak{p}}[\alpha] = (B/A[\alpha]) \otimes_A A/\mathfrak{p} = 0$.

注意到 (1) 是命题8.2的直接推广.

证明. 由引理9.1的推论知 $A/\mathfrak{p} \cong A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$, 从而有

$$B/A[\pi] \otimes_A A/\mathfrak{p} \cong B/A[\pi] \otimes_A A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong B/A[\pi] \otimes_A A_\mathfrak{p} \otimes_A A/\mathfrak{p} \cong B_\mathfrak{p}/A_\mathfrak{p}[\pi] \otimes_A A/\mathfrak{p}.$$

现在来证明 (1): $f(T)$ 在 $K[T]$ 中不可约是由 Gauss 引理和 Eisenstein 多项式的不可约保证的. 我们来证 $B_\mathfrak{p} = A_\mathfrak{p}[\pi]$. 根据 Eisenstain 多项式的形状以及引理8.1可知 $\mathfrak{p}$ 在 B/A 中完全分歧, 记 $\mathfrak{p}B = \mathfrak{P}^n$, 则 $v_\mathfrak{P}(\pi) = 1$. 考虑 A 的局部化 $A_\mathfrak{p}$, 此时 $\mathfrak{p}A_\mathfrak{p} = \varpi A_\mathfrak{p}$ 是主理想. 记 $S = A \setminus \mathfrak{p}$, 则 $B_\mathfrak{p} := B_\mathfrak{p}$ 是 $A_\mathfrak{p}$ 在 L 中的整闭包.

如果 $B_\mathfrak{p} \neq A_\mathfrak{p}[\pi]$, 则存在 $\beta \in B_\mathfrak{p} \setminus A_\mathfrak{p}[\pi]$ 使得 $\varpi\beta \in A[\pi]$. 即存在 $a_0, \cdots, a_{n-1} \in A$, 且 a_i 不全属于 $\varpi A_\mathfrak{p}$ 使得

$$\varpi\beta = a_0 + a_1\pi + \cdots a_{n-1}\pi^{n-1}.$$

我们设 $a_0, \cdots, a_{i-1} \in \mathfrak{p}$, $a_i \in \mathfrak{p}$, 则根据引理8.1 右边的 $\mathfrak{P}$ 赋值等于 $v_\mathfrak{P}(a_i\pi^i) = i < n$, 但 $v_\mathfrak{P}(\varpi\beta) \geq v_\mathfrak{P}(\varpi) = n$. 矛盾.

(2) 还是来证明 $B_\mathfrak{p} = A_\mathfrak{p}[\alpha]$. 由于 $B_\mathfrak{p} \cong A_\mathfrak{p}^n$, 设 $B_\mathfrak{p}$ 关于 $A_\mathfrak{p}$ 的一组基是 $\beta_1, \cdots, \beta_n$. 如果 $B_\mathfrak{p} \neq A_\mathfrak{p}[\alpha]$, 则过渡 $A_\mathfrak{p}$ 系数矩阵 C 满足 $(1, \alpha, \cdots, \alpha^{n-1}) = (\beta_1, \cdots, \beta_n)C$ 且 $|C| \in \mathfrak{p}A_\mathfrak{p}$. 这样的话 $\mathrm{disc}(f) = \mathrm{disc}(1, \alpha, \cdots, \alpha^{n-1}) = |C|^2\mathrm{disc}(\beta_1, \cdots, \beta_n) \in \mathfrak{p}$, 这与条件矛盾. □

用上面这个推广版本的 Eisenstein 多项式结论, 我们再给一个 m 阶分圆域的次数是 $\phi(m)$ 的证明同时决定其整数环:

命题 9.13. *对任意 $m \in \mathbb{Z}_{\geq 1}$, m 阶分圆域 $\mathbb{Q}(\zeta_m)$ 的的代数整数环是 $\mathbb{Z}[\zeta_m]$.*

证明. 若 m 是素数方幂的情形是通常版本的 Eisenstein 多项式内容就决定的, 这不再重复. 一般地, 用归纳法, 假设小于 m 阶的分圆域次数是知道的. 记 $m = m'p^k, p \nmid m$, 则根据归纳假设 $\mathbb{Q}(\zeta_{m'})$ 是 $\phi(m')$ 次数域以及 $\mathbb{Z}[\zeta_{m'}]$ 是其整数环. 现在需证 $[K : \mathbb{Q}(\zeta_{m'})] = \phi(p^k)$ 以及 $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$, K 是 $\mathbb{Q}(\zeta_m)$. 考虑 $\zeta_{p^k} - 1$ 在 $\mathbb{Q}$ 上的极小多项式

$$f(T) = \frac{(1+T)^{p^k} - 1}{(1+T)^{p^{k-1}} - 1}.$$

设 $\mathfrak{p}$ 是 $\mathbb{Q}(\zeta_{m'})$ 的任意一个 p 之上的素理想, 则将 $f(T)$ 看作 $\mathbb{Z}[\zeta_{m'}]$ 上的多项式的话, 我们断言它是 $\mathfrak{p}$-Eisenstein 的. 这是因为 $\mathfrak{p}$ 在 $\mathbb{Q}(\zeta_{m'})/\mathbb{Q}$ 中是非分歧的, 所以对于一个整数 a, $v_\mathfrak{p}(a) = v_p(a)$. 这就说明了 $f(T)$ 是 Eisenstein 的, 那么也不可约. 根据命题9.12(1),

$$(\mathcal{O}_K)_\mathfrak{p} = \mathbb{Z}[\zeta_{m'}]_\mathfrak{p}[\zeta_{p^k}].$$

对于一个不是 p 之上的 $\mathbb{Q}(\zeta_{m'})$ 的素理想 $\mathfrak{q}$, 由于 $f(T)$ 的多项式判别式与 $\mathfrak{q}$ 互素, 根据命题9.12(2) 我们有

$$(\mathcal{O}_K)_\mathfrak{q} = \mathbb{Z}[\zeta_{m'}]_\mathfrak{q}[\zeta_{q^k}].$$

根据引理9.10知 $\mathcal{O}_K = \mathbb{Z}[\zeta_{m'}][\zeta_{p^k}] = \mathbb{Z}[\zeta_m]$. □

10 第八讲: Galois 作用

设 A 是 Dedekind 整环, K 是 A 的分式域, L/K 是有限可分扩张, B 是 A 在 L 中整闭包 (从而 B 也是 Dedekind 整环.) 在本节中我们将假定 L/K 还是正规扩张, 从而 L/K 是 Galois 扩张, 记 $G = \mathrm{Gal}(L/K)$. 接下来, $\mathfrak{p}$ 总表示 A 的非零素理想, $\mathfrak{P}$ 以及 $\mathfrak{P}_i$ 总表示 B 的整除 $\mathfrak{p}B$ 的非零素理想. **术语**: 常把 $\mathfrak{P} \mid \mathfrak{p}B$ 称为 $\mathfrak{P}$ 在 $\mathfrak{p}$ 之上, $\mathfrak{p} = \mathfrak{P} \cap A$ 称为 $\mathfrak{p}$ 在 $\mathfrak{P}$ 之下.

对 $\sigma \in G$, σ 诱导了环同构 $B \to B, b \mapsto \sigma(b)$ 以及同构

$$B/\mathfrak{P} \cong B/\sigma(\mathfrak{P}), \quad b \bmod \mathfrak{P} \mapsto \sigma(b) \bmod \sigma(\mathfrak{P}). \tag{10.1}$$

这说明了 $\sigma(\mathfrak{P})$ 也是 G 的素理想, 显然 $\sigma(\mathfrak{P}) \mid \sigma(\mathfrak{p}B) = \mathfrak{p}B$. 设 $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_g\}$ 是 B 的所有 $\mathfrak{p}$ 之上的素理想所成的集合, 则 $(\sigma, \mathfrak{P}) \mapsto \sigma(\mathfrak{P})$ 给出了 G 在这个集合上的自然作用.

命题 10.1. *这个作用是传递的. (换言之, 对任何两个 $\mathfrak{p}$ 之上的 $\mathfrak{P}, \mathfrak{P}'$, 都存在 $\sigma \in G$ 使得 $\sigma(\mathfrak{P}) = \mathfrak{P}'$.)*

证明. 否则 B 中存在两个不同 $\mathfrak{p}$ 之上的 $\mathfrak{P}, \mathfrak{P}'$ 使得对任意 $\sigma \in G$ 有 $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$. 根据中国剩余定理, 存在 $x \in B$ 使得 $x \in \mathfrak{P}'$ 且对每个 $\sigma \in G$ 有 $x \notin \sigma(\mathfrak{P})$. 那么, 对每个 σ, $\sigma^{-1}(x) \notin \mathfrak{P}$. 由于 $\mathfrak{P}$ 是素理想, 我们有

$$N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) = \prod_{\sigma \in G} \sigma^{-1}(x) \notin \mathfrak{P} \cap K = \mathfrak{p}.$$

但另一方面由 $x \in \mathfrak{P}'$ 知 $N_{L/K}(x) \in \mathfrak{P}' \cap K = \mathfrak{p}$, 矛盾! □

设 $\mathfrak{p}B$ 的素理想分解为

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}. \tag{10.2}$$

回忆剩余类域次数 $f_i = f(\mathfrak{P}_i/\mathfrak{p}) := [B/\mathfrak{P}_i : A/\mathfrak{p}]$. 命题10.1和定理7.1推出了

推论. *设 L/K 是 Galois 扩张. 则 $e_1 = \cdots = e_g, f_1 = \cdots = f_g$, 从而有 $n = efg, e = e_1, f = f_1$.*

证明. 对每个 $\mathfrak{P}_i$ 有 $\sigma_i(\mathfrak{P}_1) = \mathfrak{P}_i$. 所以(10.1)推出了 $f_1 = \cdots = f_g$. 用 σ_i 作用(10.2)两边再利用理想唯一分解性知 $e_1 = \cdots = e_g$. □

所以当 L/K 是 Galois 扩张时, 说 $\mathfrak{p}$ 在 L 中的分歧指数 $e_\mathfrak{p}$ 和剩余类域次数 $f_\mathfrak{p}$ 是没有歧义的, 它分别指某个 $\mathfrak{P} = \mathfrak{P}_i$ 的 $e(\mathfrak{P}/\mathfrak{p})$, $f(\mathfrak{P}/\mathfrak{p})$.

定义 $\mathfrak{P}$ 在 L/K 的**分解群**为

$$D_\mathfrak{P}(L/K) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

若无歧义, 用 $D_\mathfrak{P}$ 或 D 来简记这个群. 显然 $D_\mathfrak{P}(L/K)$ 就是 $\mathfrak{P}$ 在群 G 作用集合 $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_g\}$ 下的稳定子群. 由一般群作用的轨道公式以及命题10.1知

$$\#D_\mathfrak{P}(L/K) = \frac{\#G}{g} = ef. \tag{10.3}$$

若 $\sigma \in D := D_\mathfrak{P}(L/K)$, 则 σ 诱导的(10.1)中的同构变为自同构且限制在 $A/\mathfrak{p}$ 上不动, 于是(10.1)诱导了自然群同态

$$\epsilon : D \to \mathrm{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})). \tag{10.4}$$

这里 $\kappa(\mathfrak{P})=B/\mathfrak{P}, \kappa(\mathfrak{p})=A/\mathfrak{p}$. 定义 $\mathfrak{P}$ 的**惯性群**为

$$I_{\mathfrak{P}}(L/K)=\{\sigma\in D: b\equiv\sigma(b) \bmod \mathfrak{P}, \forall b\in B\}.$$

若无, 我们用 $I_{\mathfrak{P}}$ 或者 I 来记惯性群. $I_{\mathfrak{P}}$ 是同态 ϵ 的核, 特别的它是 $D_{\mathfrak{P}}$ 的正规子群. 我们有 $I_{\sigma(\mathfrak{P})}=\sigma I_{\mathfrak{P}}\sigma^{-1}$.

命题 10.2. *假设 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 是可分扩张. 我们有 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 是正规扩张, 且(10.4)中的同态 ϵ 决定了正合列:*

$$1\to I_{\mathfrak{P}}\to D_{\mathfrak{P}}\to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))\to 1.$$

特别地, $\#I_{\mathfrak{P}}$ 是 $\mathfrak{p}$ 在 L 中分歧指数.

证明. 首先来说明 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 是正规扩张. 对 $\bar{b}=b \bmod \mathfrak{P}\in\kappa(\mathfrak{P})$, 多项式 $f(T):=\prod_{\sigma\in G}(T-\sigma(b))\in K[T]$, 而且它的系数都在 A 上整, 所以由 A 在 K 中整闭知 $f(T)\in A[T]$. 那么 $\bar{f}(T):=f(T) \bmod \mathfrak{p}\in\kappa(\mathfrak{p})$ 是 $\bar{b}$ 在 $\kappa(\mathfrak{p})[T]$ 中的零化多项式. 由于 L/K 是 Galois 扩张, $\bar{f}(T)$ 的每个根 $\overline{\sigma(b)}\in\kappa(\mathfrak{P})$. 这就说明了 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 是正规扩张. (在课堂上我们考虑数域的情形, 这就是有限域扩张, 所以正规是显然的.)

现在只需证明(10.4)是满射. 根据我们的假设 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 是可分扩张. 可设 $\bar{a}=a \bmod \mathfrak{P}$ 是 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 的一个本原元, 即使得 $\kappa(\mathfrak{P})=\kappa(\mathfrak{p})(\bar{a})$. 根据中国剩余定理, 存在 $b\in B$ 使

$$b\equiv a \bmod \mathfrak{P},\quad b\equiv 0 \bmod \sigma(\mathfrak{P})\quad \text{当}\sigma\notin D\text{ 时}.$$

考虑 $g(T):=\prod_{\sigma\in G}(T-\sigma(b))$, 显然 $g(T)$ 是首一 A 系数多项式且 $\bar{g}(T)\in\kappa(T)$ 是 $\bar{a}$ 的一个零化多项式. 但根据上面 b 的选取知存在 $k\in\mathbb{Z}$ 使得

$$\bar{g}(T)=T^k\prod_{\sigma\in D}(T-\overline{\sigma(b)}).$$

显然 $\bar{a}\neq 0$, 这就说明了 $\bar{a}$ 在 $\kappa(\mathfrak{p})$ 上的极小多项式整除 $\prod_{\sigma\in D}(T-\overline{\sigma(b)})$. 从而对任何 $\tau\in\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$, $\tau(\bar{a})$ 的共轭根都等于某个 $\overline{\sigma(b)}, \sigma\in D$. 这推出(10.4)是满射. 从而有命题中的正合列. □

命题 10.3. *我们有 $D_{\mathfrak{P}}(L/E)=D_{\mathfrak{P}}(L/K)\cap\mathrm{Gal}(L/E)$ 以及 $I_{\mathfrak{P}}(L/E)=I_{\mathfrak{P}}(L/K)\cap\mathrm{Gal}(L/E)$.*

证明. 由定义直接得. □

记 L^D 和 L^I 为 L/K 分别被 D 和 I 固定不动的中间域, 称它们为 $\mathfrak{P}$ 的**分解域**和**惯性域**. 若 E 是 L/K 的中间域, 记 $\mathfrak{P}_E=\mathfrak{P}\cap E$. 则 $\mathfrak{P}_E$ 是 $\mathfrak{p}$ 之上 E 的素理想. 如下的两个命题可看出这两个群确实" 掌管着"$\mathfrak{P}$ 在 L/K 及其中间域中的分解.

命题 10.4. *设 E 是 L/K 的中间域, 记 $D=D_{\mathfrak{P}}(L/K)$. 则以下几条等价:*

(1) $e(\mathfrak{P}_E/\mathfrak{p})=f(\mathfrak{P}_E/\mathfrak{p})=1$;

(2) $e(\mathfrak{P}/\mathfrak{P}_E)=e(\mathfrak{P}/\mathfrak{p}), f(\mathfrak{P}/\mathfrak{P}_E)=f(\mathfrak{P}/\mathfrak{p})$;

(3) $D_{\mathfrak{P}}(L/E)=D$;

(4) $E\subset L^D$; 换句话说, 分解域是最大的中间域使得 $e(\mathfrak{P}_E, E/K)=f(\mathfrak{P}_E, E/K)=1$.

(5) D 作用 E 平凡.

证明. (1) 与 (2) 的等价是由分歧指数与剩余类域次数的传递公式所得. 根据命题10.3与分解群的阶公式(10.3), (2) 等价于 (3). (3) 推 (4) 是由 Galois 对应, (4) 推 (3) 是因为一方面由 (4) 知 $\mathrm{Gal}(L/E) \supset D$, 再加命题10.3即知. (4) 等价于 (5) 是由 Galois 对应. □

注 10.5. (1) 如果 D 还是 G 的正规子群, 这时对任意 $\sigma \in G$ 有 $D_{\sigma(\mathfrak{P})} = D$. 则在上面命题中 $E = L^D$ 的情形推出

$$\mathfrak{p} \text{ 在} E \text{ 中完全分裂} \Leftrightarrow D \text{ 作用} E \text{ 平凡} \Leftrightarrow E \subset L^D.$$

这样看" 分解群和分解域更加名副其实."

(2) 可利用分解域给出(10.4)是满射的另一证明 (见冯老师书). 我们记 $\mathfrak{P}_D = \mathfrak{P} \cap L^D$. 则由命题10.4知 $\kappa(\mathfrak{P}_D) = \kappa(\mathfrak{p})$. 设 $\bar{a} \in \kappa(\mathfrak{P})$ 是 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 的本原元, 则考虑多项式 $g(T) = \prod_{\sigma \in D}(T - \sigma(a))$. 它是首一 $\mathcal{O}_{L^D}$ 系数多项式, 故 $\bar{g}(T) \bmod \mathfrak{P}_D \in \kappa(\mathfrak{P}_D)[T] = \kappa(\mathfrak{p})[T]$ 以 $\bar{a}$ 为根, 故每个 $\bar{a}$ 在 $\kappa(\mathfrak{p})$ 上的共轭根都等于某个 $\sigma(a) \bmod \mathfrak{P}$, $\sigma \in D$. 这就证明了(10.4)是满射.

命题 10.6. *设 E 是 L/K 的中间域, 记 $I = I_{\mathfrak{P}}(L/K)$. 则以下几条等价:*

(1) $e(\mathfrak{P}_E/\mathfrak{p}) = 1$;

(2) $e(\mathfrak{P}/\mathfrak{P}_E) = e(\mathfrak{P}/\mathfrak{p})$;

(3) $I_{\mathfrak{P}}(L/E) = I$;

(4) $E \subset L^I$; 换句话说, 惯性域是最大的中间域使得 $e(\mathfrak{P}_E, E/K) = 1$.

(5) I 作用 E 平凡.

证明. 证明与命题10.4相似, 留作练习. □

如下是几个经常用到的结论. 这些命题的陈述虽然看起来与 Galois 扩张、Galois 群、分解群、惯性群没有关系, 但取正规闭包后考虑这几个群的作用使得证明变得直接了当, 都成为命题10.4, 10.6的推论了. 这便是考虑 Galois 作用的一大好处.

命题 10.7. *设 F/K, M/K 是两个有限可分扩张, $\mathfrak{p}$ 是 K 的一个素理想.*

(1) 若 F 的一个 $\mathfrak{p}$ 之上素理想 $\mathfrak{p}_F$ 在 F/K 中是非分歧的, 则每个 $\mathfrak{p}_F$ 之上的 MF 素理想在 MF/M 中也是非分歧的.

(2) 若 $\mathfrak{p}$ 在 F/K 中是非分歧的, 则每个 M 的 $\mathfrak{p}$ 之上素理想在 MF/M 中也是非分歧的.

(3) 若 $\mathfrak{p}$ 在 F/K 和 M/K 中都是非分歧的, 则 $\mathfrak{p}$ 在 MF 中也是非分歧的.

(4) 若 $\mathfrak{p}$ 在 F/K 中是非分歧的, 则 $\mathfrak{p}$ 在 F/K 的正规闭包中也是非分歧的.

证明. 注意到 (1) ⇒ (2) ⇒ (3) ⇒ (4) 是容易的 (细节留作练习). 下面来证 (1):

设 $L \supset MF$ 使得 L/K 是有限 Galois 扩张. 记 $\mathfrak{P}$ 是 L 的 $\mathfrak{p}_F$ 之上的一个素理想. 根据条件知 $I_{\mathfrak{P}}(L/K)$ 作用 F 平凡. 由 $I_{\mathfrak{P}}(L/M) = I_{\mathfrak{P}}(L/K) \cap \mathrm{Gal}(T/M)$ 知 $I_{\mathfrak{P}}(L/M)$ 作用 M 和 F 都平凡即作用 MF 平凡. 所以 $\mathfrak{P}$ 在 MF/M 中非分歧. □

练习: 举例说明命题10.7的 (1) 和 (2) 反过来不对.

命题 10.8. *设 F/K, M/K 是两个有限可分扩张, $\mathfrak{p}$ 是 K 的一个素理想.*

(1) 若 F 的一个 $\mathfrak{p}$ 之上素理想 $\mathfrak{p}_F$ 在 F/K 中使得 $e(\mathfrak{p}_F/\mathfrak{p}) = f(\mathfrak{p}_F/\mathfrak{p}) = 1$, 则每个 $\mathfrak{p}_F$ 之上的 MF 素理想在 MF/M 中分歧指数与剩余类域次数也都是 1.

(2) 若 $\mathfrak{p}$ 在 F/K 中是完全分裂的, 则每个 M 的 $\mathfrak{p}$ 之上素理想在 MF/M 中也是完全分裂的.

(3) 若 $\mathfrak{p}$ 在 F/K 和 M/K 中是完全分裂的, 则 $\mathfrak{p}$ 在 MF 中也是完全分裂的.

(4) 若 $\mathfrak{p}$ 在 F/K 中是完全分裂的, 则 $\mathfrak{p}$ 在 F/K 的正规闭包中也是完全分裂的.

证明. 与命题10.7的证明是类似的, 留作练习. □

10.1 Dedekind 多项式 $T^3 - T^2 - 2T - 8$

现在通过一个具体例子来看看分解群和惯性群: 设 $K = \mathbb{Q}(\alpha), \alpha = \alpha_1$ 是 $f(T) = T^3 - T^2 - 2T - 8 = (T - \alpha_1)(T - \alpha_2)(T - \alpha_3)$ 的一个根. 计算得 $\mathrm{disc}(f) = -4 * 503$. 我们的目标是证明 2 在 K 中完全分裂. 记 $F = \mathbb{Q}(\sqrt{\mathrm{disc}(f)}) = \mathbb{Q}(\sqrt{-503})$. 则 $K/\mathbb{Q}$ 的正规闭包是 $L := KF$. 通过 σ 在 $\{\alpha_1, \alpha_2, \alpha_3\}$ 上的作用我们有同构 $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. 记 $\mathfrak{P}$ 为 L 的一个 2 之上的素理想. 记 $D = D_{\mathfrak{P}}(L/\mathbb{Q}), I = I_{\mathfrak{P}}(L/\mathbb{Q})$. 首先注意到 2 在 F 中是完全分裂的. 所以 D 作用 F 平凡, 也就是说 $D \subset \mathrm{Gal}(L/F)$. (1) 这一步证明 I 是平凡的即 $e(\mathfrak{P}/2) = 1$. 如若不然, $I = \mathrm{Gal}(L/F) = \langle\sigma\rangle$ 是 3 阶循环群. 由于 σ 轮换 $\alpha_1, \alpha_2, \alpha_3$, 根据惯性群的定义我们有

$$\alpha_1 \equiv \alpha_2 \equiv \alpha_3 \bmod \mathfrak{P}.$$

特别的 $f(T) \bmod \mathfrak{P}$ 有三重根, 但 $f(T) \equiv T(T-1)^2 \bmod \mathfrak{P}$, 矛盾!

(2) 这一步证明 I 是平凡的即 $e(\mathfrak{P}/2) = f(\mathfrak{P}/2) = 1$. 如若不然 $D = \mathrm{Gal}(L/F)$, 则 $e(\mathfrak{P}/2) = 1, f(\mathfrak{P}/2) = 3$. 又 $D_{\mathfrak{P}}(L/K) = D \cap \mathrm{Gal}(L/K) = \{1\}$, 即 $e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = 1$, 这里 $\mathfrak{p} = \mathfrak{P} \cap K$. 那么必有 $f(\mathfrak{p}/2) = 3$. 这说明 $2\mathcal{O}_K$ 是 $\mathcal{O}_K$ 的素理想. 但 $\alpha, \frac{4}{\alpha} \in \mathcal{O}_K \setminus 2\mathcal{O}_K$ 使得 $4 = \alpha \times \frac{4}{\alpha} \in 2\mathcal{O}_K$. 这说明 $2\mathcal{O}_K$ 不是素理想. 这个矛盾说明了 D 平凡, 从而 2 在 L 中完全分裂, 特别的 2 在 K 中也是完全分裂.

习题 10.1. 写出 $L/\mathbb{Q}$ 的所有中间域, 求 L 的 $3, 503$ 之上的素理想的分解域与惯性域.

10.2 Frobenieus 元

现在设 L/K 是数域的扩张. 取 $A = \mathcal{O}_K$ 则 $B = \mathcal{O}_L$. $\mathcal{O}_K$ 的剩余类域 $\kappa(\mathfrak{p})$ 是有限域, 阶为 $\mathbf{N}(\mathfrak{p})$. 根据有限域扩张的理论知, $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ 是 f 阶循环群由所谓的"Frobneieus 自同构"$x \mapsto x^{\mathbf{N}(\mathfrak{p})}$ 生成.

设 $\mathfrak{p}$ 在 L/K 中不分歧, 则 $I_{\mathfrak{P}}$ 平凡, $D_{\mathfrak{P}}(L/K) \cong \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. 所以在 G 中存在唯一的元素 $\mathrm{Frob}_{\mathfrak{P}}(L/K)$ 使得 $\mathrm{Frob}_{L/K}$ 在同构(10.4)下对应于剩余类域扩张的"Frobneieus 自同构", 即

$$\mathrm{Frob}_{\mathfrak{P}}(L/K)(x) \equiv x^{\mathbf{N}(\mathfrak{p})} \bmod \mathfrak{P}.$$

(唯一性是因为 G 中满足上面性质的元素自动属于 $D_{\mathfrak{P}}(L/K)$.) 这个元素称作 $\mathfrak{P}$ 在 L/K 中的 Frobenieus 元. 若无歧义时, 简记 $\mathrm{Frob}_{\mathfrak{P}}(L/K)$ 为 $\mathrm{Frob}_{\mathfrak{P}}$. 此时 $D_{\mathfrak{P}}$ 是由 $\mathrm{Frob}_{\mathfrak{P}}$ 生成的 $f(\mathfrak{P}/\mathfrak{p})$ 阶循环群. 所以对非分歧的 $\mathfrak{P}$, 了解清楚 $\mathrm{Frob}_{\mathfrak{P}}$ 在 G 中的阶就知道了 $\mathfrak{p}\mathcal{O}_L$ 的分解情况. 特别的, $\mathrm{Frob}_{\mathfrak{P}} = 1$ 当且仅当 $\mathfrak{p}$ 在 L/K 中完全分裂.

验证可知 $\mathrm{Frob}_{\sigma(\mathfrak{P})}(L/K)=\sigma\mathrm{Frob}_{\mathfrak{P}}(L/K)\sigma^{-1}$. 从而

$$\mathrm{Frob}_{\mathfrak{p}}:=\{\mathrm{Frob}_{\mathfrak{P}}:\mathfrak{P}\mid\mathfrak{p}\mathcal{O}_L\}\text{ 是}G\text{ 的一个共轭类.}$$

特别的若 G 是 abel 群时, $\mathrm{Frob}_{\mathfrak{p}}$ 是 G 中良定义的元素, 而且此时根据中国剩余定理, 有

$$\mathrm{Frob}_{\mathfrak{p}}(L/K)(x)\equiv x^{\mathbf{N}(\mathfrak{p})}\bmod\mathfrak{p}\mathcal{O}_L.$$

引理 10.9. *设 $\mathfrak{P}\subset\mathcal{O}_L$ 在 L/K 中不分歧, E 是 L/K 的中间域.*

(1) $\mathrm{Frob}_{\mathfrak{P}}(L/E)=\mathrm{Frob}_{\mathfrak{P}}(L/K)^{f(E/K)}$, *这里 $f(E/K)$ 是 $\mathfrak{P}\cap E$ 关于 $\mathfrak{p}$ 的剩余类域次数;*

(2) 若 E/K 是 Galois 扩张, 则 $\mathrm{Frob}_{\mathfrak{P}}(L/K)|_E=\mathrm{Frob}_{\mathfrak{P}_E}(E/K)$.

证明. 均从定义出发显然. □

10.3 分圆域

我们可用 Frobenieus 元的存在性来计算分圆域的次数, 即重新证明 Gauss 的定理8.7. 设 $\mathbb{Q}(\zeta_m)$ 是 m 阶分圆域, $m\not\equiv 2\bmod 4$. 则 p 在 $\mathbb{Q}(\zeta_m)$ 中不分歧当且仅当 $p\nmid m$. 我们考虑

$$\mathrm{Frob}_p:=\mathrm{Frob}_p(\mathbb{Q}(\zeta_m)/\mathbb{Q})\in\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}).$$

它具有性质

$$\mathrm{Frob}_p(\zeta_m)\equiv\zeta_m^p\bmod p\quad\text{以及存在}i,\quad\mathrm{Frob}_p(\zeta_m)=\zeta_m^i,(i,m)=1.$$

但由 $p\nmid m$ 易知 T^m-1 模 p 没有重根, 所以 $\zeta_m^i\equiv\zeta_m^p\bmod p$ 表明了 $\zeta_m^i=\zeta_m^p$. 即 $\mathrm{Frob}_p(\zeta_m)=\zeta_m^p$. 这就说明了 $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\to(\mathbb{Z}/m\mathbb{Z})^\times$ 是满射.

Frobenieus 元还可用来计算一个素数 p 在 $\mathbb{Q}(\zeta_m)$ 中的 e,f,g.

定理 10.10 (分圆域中的分解律)**.** *设 $K=\mathbb{Q}(\zeta_m)$, $m\not\equiv 2\bmod 4$.*

(1) 设 $p\nmid m$. 则 p 在 K 中不分歧, $f_p(K/\mathbb{Q})$ 等于 $p\bmod m$ 在 $(\mathbb{Z}/m\mathbb{Z})^\times$ 中的阶.

(2) 设 $m=p^km'$, $p\nmid m'$. 则 $e_p(K/\mathbb{Q})=\phi(p^k)$, $f_p(K/\mathbb{Q})$ 等于 $p\bmod m$ 在 $(\mathbb{Z}/m'\mathbb{Z})^\times$ 中的阶.

(3) 特别的, p 在 K 中完全分裂当且仅当 $p\equiv 1\bmod m$.

证明. (1) 当 $p\nmid m$ 时熟知 p 不分歧. 剩余类域次数等于 Frob_p 的阶等于 p 在 $(\mathbb{Z}/m\mathbb{Z})^\times$ 中的阶, 得证.

(2) 设 $\mathfrak{p}$ 为 K 的 p 之上的素理想. 因为 p 在 $K':=\mathbb{Q}(\zeta_{m'})$ 中不分歧以及 $K=K'\mathbb{Q}(\zeta_{p^k})$, 根据命题10.7知 $\mathfrak{p}$ 在 $K/\mathbb{Q}(\zeta_{p^k})$ 中不分歧. 熟知 p 在 $\mathbb{Q}(\zeta_{p^k})$ 中完全分歧. 所以 $\mathfrak{p}$ 在 K/K' 中完全分歧故在 $K/\mathbb{Q}$ 中具有分歧指数 $\phi(p^k)$. 剩下的部分由 (1) 可得.

(3) 由 (2) 立得. □

我们用分圆域的方法来证明 Gauss 的二次互反律.

定理 10.11 (Gauss 二次互反律)**.** *设 p,q 是两个不同的奇素数. 记 $p^*=(-1)^{\frac{p-1}{2}}p$.*

(1) p 在 $\mathbb{Q}(\sqrt{q})$ 中分裂当且仅当 q 在 $\mathbb{Q}(\sqrt{p^*})$ 中分裂;

(2) p 在 $\mathbb{Q}(\sqrt{2})$ 中分裂当且仅当 $p\equiv\pm1\bmod 8$;

(3) p 在 $\mathbb{Q}(\sqrt{-1})$ 中分裂当且仅当 $p\equiv 1\bmod 4$.

根据理想分解与多项式 mod p 分解的对应, 我们知道奇素数 p 在 $\mathbb{Q}(\sqrt{d})$ 中分裂当且仅当 $T^2 - d \bmod p$ 有两个不同的解, 当且仅当 d 模 p 是平方元, 用 Legendre 符号的语言来说的话, 这等价于 $\left(\frac{d}{p}\right) = 1$. 所以由定理10.11(1), (3) 就得出初等数论所看到的二次互反律表述形式:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

定理10.11的证明. 证明最重要的一点是我们在推论8算出的 $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$.

我们刚刚算出 $\mathrm{Frob}_q(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = \sigma_q$, 这里 $\sigma_q \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ 将 ζ_p 变为 ζ_p^q. 也就是说在同构 $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ 下, Frob_q 对应于 $q \bmod m$, $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p^*}))$ 对应于 $((\mathbb{Z}/p\mathbb{Z})^\times)^2$, 后面这点是因为 $(\mathbb{Z}/p\mathbb{Z})^\times$ 是循环群.

(1) q 在 $\mathbb{Q}(\sqrt{p^*})$ 中分裂 $\Leftrightarrow \mathrm{Frob}_q(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = 1 \Leftrightarrow \mathrm{Frob}_q(\mathbb{Q}(\zeta_p)/\mathbb{Q})|_{\mathbb{Q}(\sqrt{p^*})} = 1 \Leftrightarrow \mathrm{Frob}_q(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{p^*})) \Leftrightarrow q \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2 \Leftrightarrow p$ 在 $\mathbb{Q}(\sqrt{q})$ 中完全分裂.

(2) 利用 $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_8 + \zeta_8^{-1})$ 可类似证明, 留作练习.

(3) 留作练习. □