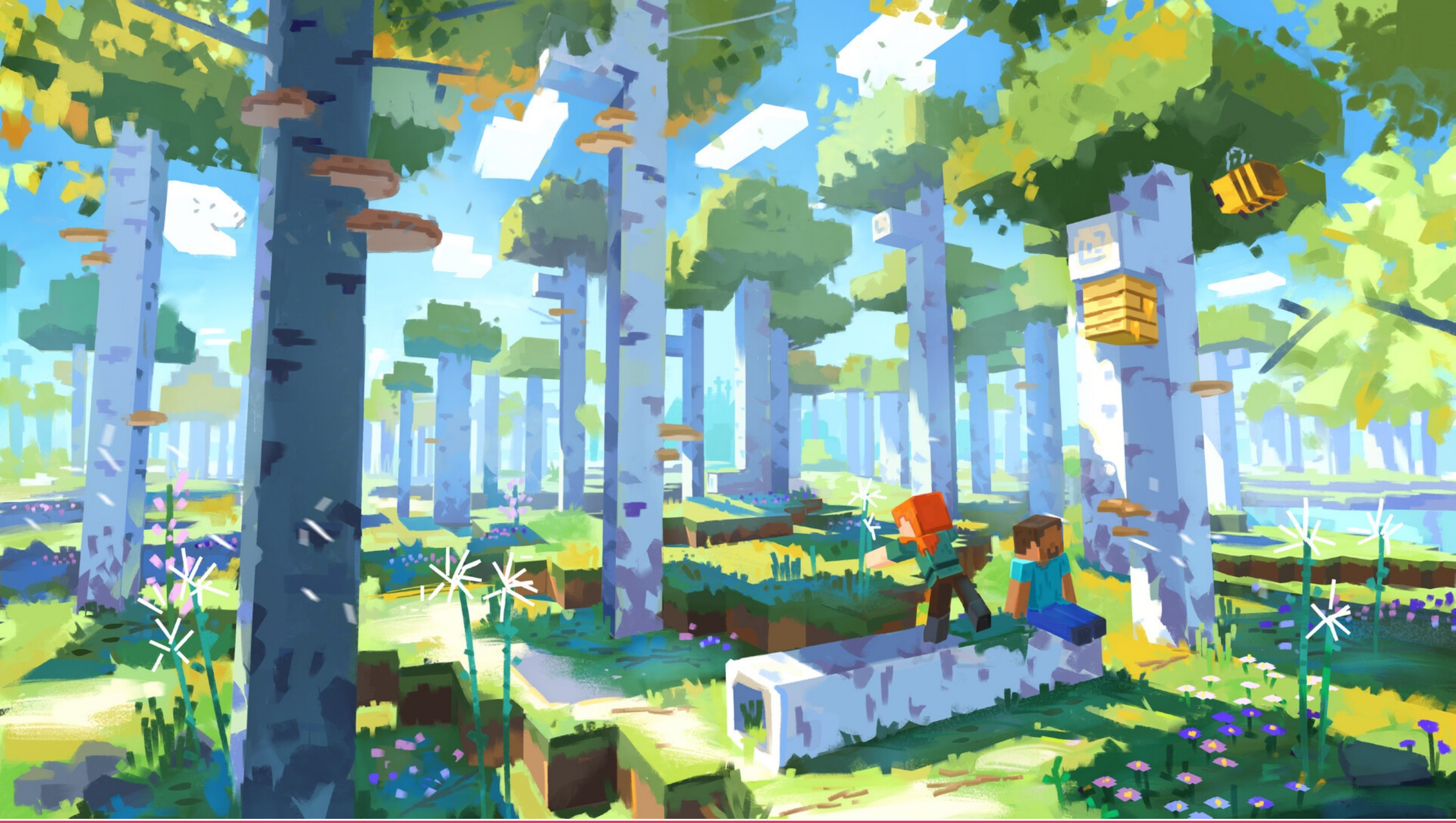

代数数论讲义

作者：张神星

组织：合肥工业大学

时间：2024 年 1 月 11 日

版本：v2.5.0.0

前言

本文为 2020 年春作者在中国科学技术大学教授代数数论 (MA05109) 的课程讲义. 本文主要沿着 [15] 的脉络进行的, 对部分章节进行了增减. 本课程需要的前置内容包括线性代数、抽象代数和伽罗瓦理论.

2020 年, 开年就是新型冠状病毒疫情, 这也导致学校的教学首次安排在线上教学. 现在, 在家中码字的我只希望, 人们能够早日战胜疫病, 加油!

张神星

2020 年 2 月 7 日

Bib 格式:

```
@misc{ZhangNotes2021,
  AUTHOR = {张神星},
  KEY = {zhang2 shen4 xing2},
  TITLE = {代数数论讲义 (v2.3)},
  YEAR = {2021},
  PAGES = {vi+163},
  HOWPUBLISHED = {Course Notes},
  URL = {https://zhangshenxing.gitee.io/teaching/代数数论讲义.pdf},
  LANGUAGE = {Chinese}
}
```

目录

第一章 代数整数

内容提要

- 整数环的结构 1.15
- 整基的判定 1.18
- 分圆域的整数环 1.27
- 类群有限性 1.53
- 狄利克雷单位定理 1.56
- 整二元二次型 1.65, 1.69

问题

什么样的正整数能够写成两个整数的平方和?

在初等数论中我们知道, 一个正整数可以写成两个整数的平方和当且仅当其素数分解中, 模 4 余 3 的素数的幂次是偶数. 证明这个结论最直接的做法是在环 $\mathbb{Z}[i]$ 中研究它们的分解. 由此可见, 即便是研究整数环 $\mathbb{Z}$ 和有理数域 $\mathbb{Q}$ 上的算术问题, 对其代数扩张的研究也是十分有必要的.

代数数域 number field 指的是有理数域 $\mathbb{Q}$ 的有限扩张. 正如整数环 $\mathbb{Z}$ 的算术性质对于 $\mathbb{Q}$ 的重要性, 本章中我们将对数域的整数环 $\mathcal{O}_K$ 进行研究, 这包括 $\mathcal{O}_K$ 的线性结构、唯一分解性、单位群的结构等内容, 并利用其回答整二元二次型表整数问题.

设 $\mathbb{F}_q$ 为 q 元有限域, t 为一未定元. 我们称 $\mathbb{F}_q[t]$ 的有限扩张为函数域 function field. 由于函数域与数域有很多相似的性质, 因此在很多情形我们可以把它们放在一起来研究.

§1.1 域扩张的线性结构

设 L/K 为域的 n 次扩张, 则 L 可以看成 K 上 n 维线性空间. 我们来研究它的线性结构.

§1.1.1 迹和范数

对于 $\alpha \in L$, 映射 $T_\alpha : x \mapsto \alpha x$ 给出了 K 线性空间 L 到自身的线性变换. 由于迹和行列式在线性代数中的重要地位, 我们给出如下定义.

定义 1.1 (迹和范数)

分别称线性映射 T_α 的迹和行列式为 α (在扩张 L/K 下) 的迹 trace 和范数 norm[a], 记为 $\mathrm{Tr}_{L/K}(\alpha)$ 和 $\mathbf{N}_{L/K}(\alpha)$.

[a]注意这不是泛函分析中的范数.

练习 1.1.1 对于 $\alpha, \beta \in L$, 证明

$$\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta), \quad \mathbf{N}_{L/K}(\alpha\beta) = \mathbf{N}_{L/K}(\alpha)\mathbf{N}_{L/K}(\beta).$$

因此 $\mathrm{Tr}_{L/K} : L \to K$ 和 $\mathbf{N}_{L/K} : L^\times \to K^\times$ 是群同态.

练习 1.1.2 对于 $\alpha \in L, \lambda \in K$, 证明

$$\mathrm{Tr}_{L/K}(\lambda\alpha) = \lambda \mathrm{Tr}_{L/K}(\alpha), \quad \mathbf{N}_{L/K}(\lambda\alpha) = \lambda^n \mathbf{N}_{L/K}(\alpha).$$

练习 1.1.3 设 L/K 是一个二次扩张. 是否总能找到 $\theta \in L$ 使得 $\theta^2 \in K$ 且 $L = K(\theta)$? 试着用 L 的一个合适的生成元 θ 来表示 $\mathrm{Tr}_{L/K}$ 和 $\mathbf{N}_{L/K}$.

固定一个 K 的代数闭包 $\overline{K}$. 我们记 $\mathrm{Hom}_K(L, \overline{K})$ 为保持 K 不变的嵌入 $\tau : L \hookrightarrow \overline{K}$ 全体. 元素 $\alpha \in L^\times$ 的极小多项式 (minimal polynomial) 是指多项式环 $K[X]$ 中零化 α 的次数最小的首一多项式, 也就是线性映射 T_α 的极小多项式. 如果 $L^\times$ 中所有元素的极小多项式均无重根, 称 L/K 可分 (separable).

例题 1.1

(1) 如果 K 的特征为零, 则 L/K 总是可分的. 这是因为如果 f 是 $\alpha \in L$ 的极小多项式, 则 f 在 $K[X]$ 中不可约. 如果 f 有重根 β, 则 f 与 f' 的最大公因子零化 β, 这意味着 f 整除 f'. 这在特征零情形是不可能的.

(2) 如果 K 的特征为素数 p, $\alpha \in L$ 不可分, 那么由前述推理可知对于 α 的极小多项式 f, 有 $f' = 0$. 因此存在 $f_1(X) \in K[X]$ 使得 $f(X) = f_1(X^p)$. 注意到 f_1 是 α^p 的极小多项式. 因此归纳可知 f 可表为 $K[X]$ 中一可分多项式的某个 p^m 次幂, $m \geq 0$. 设 t 是未定元, 则 $K(t^{1/p})/K(t)$ 中 $t^{1/p}$ 的极小多项式为 $X^p - t = \left(X - t^{1/p}\right)^p$.

设 L/K 可分. 我们知道, 有限可分扩张都是单扩张[1], 即存在 $\theta \in L$ 使得 $L = K(\theta)$. 设 θ 的极小多项式为

$$f(X) = \prod_{i=1}^{n}(X - \theta_i),$$

则 $\theta \mapsto \theta_i$ 诱导了所有的 $L \hookrightarrow \overline{K}$, 因此 $\mathrm{Hom}_K(L, \overline{K})$ 的大小为 n.

命题 1.2

对于有限可分扩张 L/K, 我们有

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{\tau \in \mathrm{Hom}_K(L,\overline{K})} \tau\alpha, \quad \mathbf{N}_{L/K}(\alpha) = \prod_{\tau \in \mathrm{Hom}_K(L,\overline{K})} \tau\alpha.$$

证明 见 [15, Chapter I, Proposition2.6]. 对于 $\alpha \in L$,

$$p(X) := \prod_{\tau \in \mathrm{Hom}_K(K(\alpha),\overline{K})} (X - \tau\alpha) = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in K[X]$$

为 α 的极小多项式, 因此 $\{1, \alpha, \ldots, \alpha^{m-1}\}$ 构成 K 向量空间 $K(\alpha)$ 的一组基. 在这个基下 T_α 的变换矩阵为

$$A = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{m-2} \\ & & & 1 & -a_{m-1} \end{pmatrix},$$

[1] 只需对 $L = K(\alpha, \beta)$ 情形证明, 一般情形归纳即可. 设 $f(X), g(X) \in K[X]$ 分别为 α, β 的极小多项式, c 为一充分大的正整数, 使得 $\alpha_i + c\beta_j$ 两两不同, 其中 α_i, β_j 分别是 α, β 的共轭元.
设 $\gamma = \alpha + c\beta$. 由于 L/K 可分, g 没有重根. 考虑多项式 $f(\gamma - cX) \in K(\gamma)[X]$ 和 $g(X) \in K[X]$. 由 c 的选择不难看出二者只有一个公共零点 β, 从而它们的最大公因子 $x - \beta \in K(\gamma)[X]$, 即 $\beta \in K(\gamma)$, 从而 $\alpha = \gamma - c\beta \in K(\gamma)$. 见 [4, §3.2 定理 2].

从而

$$\mathrm{Tr}_{K(\alpha)/K}(\alpha) = -a_{m-1} = \sum_{\tau\in\mathrm{Hom}_K(K(\alpha),\overline{K})} \tau\alpha,$$

$$\mathbf{N}_{K(\alpha)/K}(\alpha) = (-1)^m a_0 = \prod_{\tau\in\mathrm{Hom}_K(K(\alpha),\overline{K})} \tau\alpha.$$

考虑 $\mathrm{Hom}_K(L,\overline{K})$ 上等价关系: $\sigma\sim\tau \iff \sigma\alpha=\tau\alpha$. 这等价于 $\sigma^{-1}\tau\in\mathrm{Hom}_{K(\alpha)}(L,\overline{K})$, 因此每个等价类大小均为 $d=[L:K(\alpha)]$, 共 m 个等价类. 设 $\tau_1,\dots,\tau_m$ 为这些等价类的一组代表元, $\alpha_1,\dots,\alpha_d$ 为 $L/K(\alpha)$ 的一组基, 则 T_α 在基

$$\alpha_1,\alpha_1\alpha,\dots,\alpha_1\alpha^{m-1},\quad \dots\quad ,\alpha_d,\alpha_d\alpha,\dots,\alpha_d\alpha^{m-1}$$

下的矩阵为 $\mathrm{diag}\,\{A,\dots,A\}$. 因此 T_α 的特征多项式为

$$p(X)^d = \prod_{i=1}^m \prod_{\tau\sim\tau_i}(X-\tau\alpha) = \prod_{\tau\in\mathrm{Hom}_K(L,\overline{K})}(X-\tau\alpha).$$

故原命题成立. □

练习 1.1.4 求 $\alpha=\sqrt{-2}+\sqrt{3}$ 在域扩张 $K/\mathbb{Q}(\sqrt{3})$, $K/\mathbb{Q}(\sqrt{-6})$ 和 $K/\mathbb{Q}$ 下的迹和范数.

练习 1.1.5 设 $K=\mathbb{Q}(\zeta)$, 其中 $\zeta=e^{2\pi i/p}$ 是 p 次本原单位根, $p>2$ 是奇素数. 计算 $\mathrm{Tr}_{K/\mathbb{Q}}(\zeta+\overline{\zeta})$ 和 $\mathbf{N}_{K/\mathbb{Q}}(\zeta+\overline{\zeta})$.

练习 1.1.6 设 $\alpha\in\mathbb{C}$ 满足 $\alpha^3-3\alpha-1=0$. 计算 $\beta=3\alpha^2+7\alpha+5$ 的迹和范数.

推论 1.3

对于有限域扩张 $K\subseteq L\subseteq M$, 我们有

$$\mathrm{Tr}_{M/K}=\mathrm{Tr}_{L/K}\circ\mathrm{Tr}_{M/L},\quad \mathbf{N}_{M/K}=\mathbf{N}_{L/K}\circ\mathbf{N}_{M/L}.$$

证明 见 [23, Chapter II, §10]. 假设 M/K 可分. 考虑 $\mathrm{Hom}_K(M,\overline{K})$ 上的等价关系: $\sigma\sim\tau \iff \sigma|_L=\tau|_L$. 这等价于 $\sigma^{-1}\tau\in\mathrm{Hom}_L(M,\overline{K})$, 因此每个等价类大小均为 $[M:L]$, 共 $m=[L:K]$ 个等价类. 设 $\tau_1,\dots,\tau_m$ 为这些等价类的一组代表元, 则 $\mathrm{Hom}_K(L,\overline{K})=\{\tau_i|_L : 1\le i\le m\}$. 于是

$$\begin{aligned}\mathrm{Tr}_{M/K}(\alpha) &= \sum_{i=1}^m\sum_{\tau\sim\tau_i}\tau\alpha = \sum_{i=1}^m \mathrm{Tr}_{\tau_i M/\tau_i L}(\tau_i\alpha)\\ &= \sum_{i=1}^m \tau_i\mathrm{Tr}_{M/L}(\alpha) = \mathrm{Tr}_{L/K}\big(\mathrm{Tr}_{M/L}(\alpha)\big).\end{aligned}$$

对于一般情形, 设 K^s 为 K 在 L 中极大可分扩张, $[L:K]_i:=[L:K^s]$. 我们有 $\mathrm{Hom}_K(L,\overline{K})=\mathrm{Hom}_K(K^s,\overline{K})$, 于是

$$\mathrm{Tr}_{L/K}(\alpha)=[L:K]_i\sum_{\tau\in\mathrm{Hom}_K(L,\overline{K})}\tau\alpha.$$

由于 $[M:K]_i=[M:L]_i[L:K]_i$, 仿照上述证明可知原命题成立.

范数的情形类似. □

注 实际上, 如果 L/K 不可分, 则 $[L:K]_i$ 是 $\mathrm{char}K>0$ 的正整数次幂, 因此我们有 $\mathrm{Tr}_{L/K}=0$. 反之亦然.

命题 1.4 (嵌入的线性无关性)

设 $\mathrm{Hom}_K(L,\overline{K})=\{\tau_1,\ldots,\tau_n\}$, 则 $\tau_1,\ldots,\tau_n$ 在 $\overline{K}$ 上线性无关.

证明 $n=1$ 时显然. 对于 $n\geq 2$, 如果命题不成立, 我们可不妨设 $\sum_{i=1}^d c_i\tau_i=0, c_i\in\overline{K}^\times$, 其中 $d\geq 2$ 最小. 不妨设 $c_1=1$. 选取 $\beta\in L$ 使得 $\tau_1(\beta)\neq\tau_2(\beta)$, 则对任意 $\alpha\in L$, $\sum_{i=1}^d c_i\tau_i(\alpha\beta)=\sum_{i=1}^d c_i\tau_i(\alpha)\tau_i(\beta)=0$. 因此

$$\sum_{i=2}^d(\tau_i(\beta)-\tau_1(\beta))\tau_i(\alpha)=0,\quad\forall\alpha\in L.$$

这与 d 的最小性矛盾! 因此原命题成立. □

§1.1.2 判别式

现在我们来研究 K 线性空间 L 的基.

定义 1.5 (判别式)

定义 $\alpha_1,\ldots,\alpha_n\in L$ 关于 L/K 的判别式 (discriminant) 为

$$\mathrm{disc}_{L/K}(\alpha_i)_i=\mathrm{disc}_{L/K}(\alpha_1,\ldots,\alpha_n)=\det\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{ij}.$$

对于不可分扩张, 判别式总是 0. 因此本小节剩余部分总假设 L/K 可分.

引理 1.6

(1) 若 $\mathrm{Hom}_K(L,\overline{K})=\{\tau_1,\ldots,\tau_n\}$, 则

$$\mathrm{disc}_{L/K}(\alpha_i)_i=\det(\tau_i\alpha_j)_{ij}^2.$$

(2) 若存在矩阵 $C\in M_n(K)$ 使得 $(\beta_i)_i=(\alpha_i)_iC$, 则

$$\mathrm{disc}_{L/K}(\beta_i)_i=\mathrm{disc}_{L/K}(\alpha_i)_i\cdot\det(C)^2.$$

证明

(1) 由于 $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)=\sum_k(\tau_k\alpha_i)(\tau_k\alpha_j)$, 我们有

$$\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{ij}=(\tau_i\alpha_j)_{ij}^{\mathrm{T}}(\tau_i\alpha_j)_{ij},$$

因此 $\det\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)_{ij}=\det(\tau_i\alpha_j)_{ij}^2$.

(2) 由 $(\tau_i\beta_j)_{ij}=(\tau_i\alpha_j)_{ij}C$ 可得.

□

命题 1.7 (有限可分扩张的迹配对非退化)

(1) $(\alpha_i)_i$ 构成 K 向量空间 L 的一组基当且仅当 $\mathrm{disc}_{L/K}(\alpha_i)_i\neq 0$.

(2) K 上的双线性型

$$\begin{aligned}L\times L&\longrightarrow K\\(x,y)&\longmapsto\mathrm{Tr}_{L/K}(xy)\end{aligned}$$

非退化, 即 $\mathrm{Tr}_{L/K}(xy)=0,\forall y\in L$ 当且仅当 $x=0$.

证明 设 $\theta \in L$ 使得 $L = K(\theta)$, 则 $1, \theta, \ldots, \theta^{n-1}$ 构成一组基. 设

$$\mathrm{Hom}_K(L, \overline{K}) = \{\tau_1, \ldots, \tau_n\}, \quad \theta_i = \tau_i \theta,$$

则 $(\tau_i \theta^j)_{ij} = (\theta_i^j)_{ij}$ 是一个范德蒙矩阵, 其行列式为

$$\det(\theta_i^j)_{ij} = \prod_{i>j} (\theta_i - \theta_j) \neq 0,$$

因此 $\mathrm{disc}_{L/K}(1, \theta, \ldots, \theta^{n-1}) \neq 0$. 由引理 1.6(2) 可知 $(\alpha_i)_i$ 构成 K 向量空间 L 的一组基当且仅当 $\mathrm{disc}_{L/K}(\alpha_i)_i \neq 0$. 由于双线性型 $\mathrm{Tr}_{L/K}(xy)$ 在基 $(\alpha_i)_i$ 下的矩阵是 $\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{ij}$, 它的行列式非零, 因此 $\mathrm{Tr}_{L/K}(xy)$ 非退化. □

由于迹配对非退化, 因此它诱导了自然同构

$$\begin{aligned} L &\xrightarrow{\sim} L^\vee = \mathrm{Hom}_{\mathsf{Vect}/K}(L, K) \\ x &\longmapsto \mathrm{Tr}_{L/K}(x \cdot). \end{aligned}$$

定义 1.8 (对偶基)

对于 L/K 的一组基 $(\alpha_i)_i$, 令 $(\alpha_i^\vee)_i$ 为其对偶基在自然同构 $L \cong L^\vee$ 下的原像, 我们称之为 $(\alpha_i)_i$ 关于 $\mathrm{Tr}_{L/K}$ 的对偶基 (dual basis).

换言之, $\mathrm{Tr}_{L/K}(\alpha_i \alpha_j^\vee) = \delta_{ij}$, 因此对于 $\forall x \in L$, 我们有 $x = \sum_i \mathrm{Tr}(x\alpha_i)\alpha_i^\vee = \sum_i \mathrm{Tr}(x\alpha_i^\vee)\alpha_i$. 从而

$$(\alpha_1^\vee, \ldots, \alpha_n^\vee) = (\alpha_1, \ldots, \alpha_n) \left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)_{ij}^{-1}.$$

我们将会在后面的内容中用到下述命题.

命题 1.9

设 $\alpha \in L$ 的极小多项式为 $f(T) \in K[T]$. 则

$$\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \begin{cases} 0, & \text{若 } \deg f < n; \\ (-1)^{\frac{n(n-1)}{2}} \mathbf{N}_{L/K}(f'(\alpha)), & \text{若 } \deg f = n. \end{cases}$$

证明 $\deg f < n$ 时其不构成 K 的一组基, 因此 $\mathrm{disc} = 0$. 设 $\deg f = n$, 则由范德蒙行列式知

$$\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \det\left(\sigma_i(\alpha^{j-1})_{i,j}\right)^2 = \prod_{i<j} \left(\sigma_i(\alpha) - \sigma_j(\alpha)\right)^2.$$

由

$$\mathbf{N}_{K/\mathbb{Q}}\left(f'(\alpha)\right) = \prod_{i=1}^{n} \sigma\left(f'(\alpha)\right) = \prod_{i=1}^{n} \prod_{j \neq i} \left(\sigma_i(\alpha) - \sigma_j(\alpha)\right)$$

知该命题成立. □

练习 1.1.7 计算 $\{1, \alpha, \alpha + \alpha^2\}$ 关于 $\mathbb{Q}(\alpha)/\mathbb{Q}$ 的判别式, 其中 $\alpha^3 - \alpha - 4 = 0$. 它构成一组基吗? 如果是的话, 它的对偶基是什么?

练习 1.1.8 设

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in K[x]$$

是域 K 上的多项式, 其中 $\alpha_i \in \overline{K}, n \geq 1$. 称 $d(f) = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2$ 为多项式 $f(x)$ 的判别式. 显然 $f(x)$ 有重根当且仅当 $d(f) = 0$.

(1) 证明 $d(f)=(-1)^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}f'(\alpha_i)\in K$.

(2) 如果 $f(x)=x^n+a$, 求 $d(f)$.

(3) 如果 $f(x)=x^n+ax+b$, 求 $d(f)$.

(4) 设 $f(x)\in\mathbb{R}[x]$ 为 3 次多项式. 证明: 如果 $d(f)>0$, 则 $f(x)$ 有三个实根; 如果 $d(f)<0$, 则 $f(x)$ 只有一个实根.

§1.2 数域的整数环

本节我们将研究 K 的整数环 $\mathcal{O}_K$ 的群结构. 请先行自学附录 A.1.

§1.2.1 整性

我们先来了解一般的整性的概念.

定义 1.10 (整)

设 $A\subseteq B$ 是两个含幺交换环. 如果 $b\in B$ 被一个 A 系数首一多项式零化, 称 b 在 A 上整 (integral). 这样的元素全体称为 A 在 B 中的整闭包 (integral closure).

命题 1.11

$b_1,\dots,b_n$ 在 A 上整当且仅当 $B=A[b_1,\dots,b_n]$ 是有限生成 A 模. 换言之, 存在 $\beta_1,\dots,\beta_k\in B$, 使得 B 中任一元素均可表为 $\sum_{i=1}^{k}a_i\beta_i, a_i\in A$.

证明 如果 b 在 A 上整, 设首一多项式 $f(X)\in A[X]$ 零化 b. 由于 f 首一, 对于任意多项式 $g(X)\in A[X]$, 存在 $q(X),r(X)\in A[X]$ 使得

$$g(X)=f(X)q(X)+r(X),\quad \deg r<\deg f.$$

因此 $A[b]$ 中的每个元素都可表为 $1,b,\dots,b^{n-1}$ 的 A 系数组合, 即 $A[b]=A+Ab+\cdots+Ab^{n-1}$. 从而 $A[b]$ 是有限生成 A 模. 由于 b_i 在 $A[b_1,\dots,b_{i-1}]$ 上整, 因此 $A[b_1,\dots,b_i]$ 是有限生成 $A[b_1,\dots,b_{i-1}]$ 模. 归纳可知 $A[b_1,\dots,b_n]$ 是有限生成 A 模.

反之, 若 $M=A[b_1,\dots,b_n]$ 是有限生成 A 模, 设 $M=\sum\limits_{i=1}^{m}Aa_i$. 对于 $b\in M$, 我们有

$$ba_i=\sum_{j=1}^{m}c_{ij}a_j,\quad c_{ij}\in A.$$

因此

$$(bI_n-(c_{ij})_{ij})\begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix}=O.$$

左乘 $C:=bI_n-(c_{ij})_{ij}$ 的伴随矩阵, 我们得到 $\det(C)a_i=0,\forall i$. 而 1 可以表为 a_i 的 A 系数组合, 故 $\det(C)=0$. 而 $\det(C)$ 是 b 的首一零化多项式, 因此 b 在 A 上整. $\square$

如果 b_1,b_2 在 A 上整, 则 $A[b_1+b_2],A[b_1b_2]\subseteq A[b_1,b_2]$ 也是有限生成的, 因此 b_1+b_2,b_1b_2 均在 A 上整. 从而 A 在 B 中的整闭包构成一个环.

练习 1.2.1 对于 $A \subseteq B \subseteq C$, 如果 B 在 A 上整 (即其中每个元素在 A 上整), C 在 B 上整, 则 C 在 A 上整.

定义 1.12 (整闭)

如果整环 A 在其分式域中的整闭包为自身, 称其为整闭的 (integral closed).

命题 1.13

设 A 是整闭整环, $K = \operatorname{Frac} A$ 为其分式域. 设 L/K 是代数扩张, 则 $b \in L$ 在 A 上整当且仅当其极小多项式 $p(X) \in K[X]$ 是 A 系数的.

证明 设首一多项式 $g(X) \in A[X]$ 零化 b, 则在 $K[X]$ 中 $p(X) \mid g(X)$. 于是 $p(X)$ 的所有根都在 A 上整, 它的所有系数也在 A 上整. 由于 A 是整闭的, 因此 $p(X) \in A[X]$. □

练习 1.2.2

(1) 设 $\overline{A}$ 是 A 在 B 中的整闭包, 则 $\overline{A}$ 在 B 中的整闭包是 $\overline{A}$.

(2) 如果 B 在 A 上代数, 则 B 的分式域等于 $\overline{A}$ 的分式域.

练习 1.2.3 (1) 证明 $\mathbb{Z}, \mathbb{Z}[i], \mathbb{F}_p[T]$ 是整闭的.

(2) 证明 $\mathbb{Z}[\sqrt{5}]$ 不是整闭的. 它在其分式域中的整闭包是什么?

§1.2.2 整基

现在我们来研究 K 的整数环的群结构.

定义 1.14 (整数环)

数域 K 的整数环 (ring of integers) $\mathcal{O}_K$ 指的是 $\mathbb{Z}$ 在 K 中的整闭包, 其中的元素被称为代数整数 (algebraic integers).

换言之, 代数整数是整系数多项式的根.

例题 1.2 考虑 $K = \mathbb{Q}(\sqrt{d}), d \neq 0, 1$ 是无平方因子整数. 由命题1.13可知, $\mathcal{O}_K$ 中的有理数只能是整数; 如果 $a + b\sqrt{d} \in \mathcal{O}_K$, 则

$$f(X) = X^2 - 2aX + a^2 - db^2 \in \mathbb{Z}[X]$$

是它的极小多项式, 因此 $2a, 2b$ 是整数. 如果 $a \in \frac{1}{2} + \mathbb{Z}$, 则 $b \in \frac{1}{2} + \mathbb{Z}$, $d \equiv 1 \bmod 4$. 故

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

练习 1.2.4 设 L/K 是数域扩张. 证明 $\mathcal{O}_K$ 在 L 中的整闭包是 $\mathcal{O}_L$.

设 K 是 n 次数域, 即 $n = [K : \mathbb{Q}]$.

定理 1.15

$\mathcal{O}_K$ 的任意非零理想 $\mathfrak{a}$ 是秩 n 自由交换群.

证明 任取 $K/\mathbb{Q}$ 的一组基 $(\alpha_i)_i$, 通过乘以一个正整数, 我们可以不妨设 $\alpha_i \in \mathcal{O}_K$. 记其生成的子群为 $M = \sum_i \mathbb{Z}\alpha_i$. 令 $(\alpha_i^\vee)_i$ 为其关于 $\operatorname{Tr}_{K/\mathbb{Q}}$ 的对偶基, 其生成 K 的一个子群 $M^\vee = \sum_i \mathbb{Z}\alpha_i^\vee$. 容易看出

$$M^\vee = \left\{x \in K \mid \operatorname{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z}, \forall y \in M\right\}.$$

因此 $M \subseteq \mathcal{O}_K \subseteq M^\vee$. 对任意非零理想 $\mathfrak{a}$, 设 d 是其中任一非零元素的范数, 则 $d \in \mathfrak{a}, d\mathcal{O}_K \subseteq \mathfrak{a}$, 因此 $dM \subseteq \mathfrak{a} \subseteq M^\vee$. 又因为 $|M^\vee/M| = |\mathrm{disc}(\alpha_i)_i|, |M/dM| = d^n$ 均有限, 因此 $\mathfrak{a}$ 是一个秩 n 自由交换群. □

注 如果 A 是诺特 (定义 1.29) 整闭整环, K 为其分式域, L/K 是一个有限可分扩张, B 是 A 在 L 中的整闭包, 那么 B 是有限生成 A 模. 特别地, 如果 A 是主理想整环, 则 B 是自由 A 模, 它的秩只能是 $[L:K]$. 这对于 B 的非零理想也成立. 见 [11, I §2, Theorem 1].

一个自然的问题是: 何时 K 中一组元素能够构成 $\mathfrak{a}$ 的一组基, 即所谓的整基 (integral basis).

命题 1.16

如果 $(\alpha_i)_i, (\beta_i)_i$ 是 $\mathfrak{a}$ 的两组整基, 则 $\mathrm{disc}(\alpha_i)_i = \mathrm{disc}(\beta_i)_i$.

证明 存在矩阵 $C \in M_n(\mathbb{Z})$ 使得 $(\beta_i)_i = (\alpha_i)_i C$, 因此 $\mathrm{disc}(\beta_i)_i = \mathrm{disc}(\alpha_i)_i \det(C)^2$, $\mathrm{disc}(\beta_i)_i$ 是 $\mathrm{disc}(\alpha_i)_i$ 的正整数倍. 反之亦然, 因此 $\mathrm{disc}(\beta_i)_i = \mathrm{disc}(\alpha_i)_i$. □

定义 1.17 (理想的判别式)

$\mathfrak{a}$ 的判别式 (discriminant) $\Delta_{\mathfrak{a}} \in \mathbb{Z}$ 是指它的任意一组整基的判别式. 特别地, 如果 $\mathfrak{a} = \mathcal{O}_K$, 我们也称它的整基为 K 的整基, 它的判别式为 K 的判别式 Δ_K.

练习 1.2.5 设 $d \neq 0, 1$ 是无平方因子整数. 当 $d \equiv 1 \bmod 4$ 时 $\Delta_{\mathbb{Q}(\sqrt{d})} = d$; 当 $d \equiv 2, 3 \bmod 4$ 时 $\Delta_{\mathbb{Q}(\sqrt{d})} = 4d$.

注 对于一般的数域的有限扩张 L/K, $\mathcal{O}_L$ 未必是自由 $\mathcal{O}_K$ 模. 我们定义判别式 $\mathfrak{d}_{L/K}$ 为 $\mathrm{disc}(\alpha_i)_i$ 生成的理想, 其中 $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_L$. 即使 $\mathcal{O}_K$ 是主理想整环, 不同的基的判别式也可能会相差一个单位. 特别地, $\mathfrak{d}_{K/\mathbb{Q}} = (\Delta_K)$. 我们将在 **??** 小节研究它的性质.

引理 1.18 (整基判定准则)

设 $\beta_1, \ldots, \beta_n \in \mathfrak{a}$ 是 $K/\mathbb{Q}$ 的一组基. $(\beta_i)_i$ 构成 $\mathfrak{a}$ 一组整基当且仅当: 如果素数 p 满足 $p^2 \mid \mathrm{disc}(\beta_i)_i$ 和 $\sum\limits_{i=1}^n x_i\beta_i \in p\mathfrak{a}, 0 \leq x_i \leq p-1, \forall i$, 则 $x_i = 0, \forall i$.

证明 设 $(\alpha_i)_i$ 为一组整基, 令 $(\beta_i)_i = (\alpha_i)_i C, C \in M_n(\mathbb{Z})$. 假设 $(\beta_i)_i$ 不是一组整基, 则存在素数 $p \mid \det(C)$. 因此 $p^2 \mid \mathrm{disc}(\beta_1, \ldots, \beta_n) = \det(C)^2 \Delta_{\mathfrak{a}}$. 设 $\overline{C} \in M_n(\mathbb{F}_p)$ 为 C 模 p, 则存在非零列向量 $(\bar{x}_1, \ldots, \bar{x}_n)^{\mathrm{T}} \in \mathbb{F}_p^n$ 满足 $\overline{C}(\bar{x}_1, \ldots, \bar{x}_n)^{\mathrm{T}} = 0$. 设 $x_i \in \{0, 1, \ldots, p-1\}$ 为 $\bar{x}_i$ 的提升, 则

$$\sum_{i=1}^n x_i\beta_i = (\alpha_1, \ldots, \alpha_n) C (x_1, \ldots, x_n)^{\mathrm{T}} \in p\mathfrak{a}.$$

反之, 若存在不全为零的整数 $0 \leq x_i \leq p-1, \forall i$ 使得 $\sum\limits_{i=1}^n x_i\beta_i \in p\mathfrak{a}$, 则 $\overline{C}(\bar{x}_1, \ldots, \bar{x}_n)^{\mathrm{T}} = 0$, $\det(C)$ 是 p 的倍数, 因此 $(\beta_1, \ldots, \beta_n)$ 不是整基. □

命题 1.19

设 $\alpha \in \mathcal{O}_K, K = \mathbb{Q}(\alpha), f(T) \in \mathbb{Z}[T]$ 为 α 的极小多项式. 如果对任意满足 $p^2 \mid \mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$ 的素数 p, 存在整数 k 使得 $f(T+k)$ 是关于 p 的艾森斯坦多项式, 则 $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

关于 p 的艾森斯坦多项式(Eisenstein polynomial) 指的是首一多项式 $f(T)=T^n+a_{n-1}T^{n-1}+\cdots+a_0\in\mathbb{Z}[T]$ 满足 $p\mid a_{n-1},\ldots,a_0$ 且 $p^2\nmid a_0$. 通过分解 $f(T)\bmod p$ 不难看出艾森斯坦多项式总是不可约的.

证明 由于 $\{\alpha^i\}_{0\le i\le n-1}$ 和 $\{(\alpha+k)^i\}_{0\le i\le n-1}$ 只相差一个行列式为 1 的整系数矩阵, 它们生成相同的交换群, 因此我们不妨设 $f(T)$ 本身就是关于 p 的艾森斯坦多项式. 假如 $\{1,\alpha,\ldots,\alpha^{n-1}\}$ 不构成一组整基, 则存在素数 p 满足 $p^2\mid \operatorname{disc}(\alpha^i)$, 且存在不全为 p 的倍数的 x_i 满足 $x:=\frac{1}{p}\sum\limits_{i=0}^{n-1}x_i\alpha^i\in\mathcal{O}_K$. 不妨设 $0\le x_i\le p-1$. 令 $j=\min\{i\mid x_i\neq 0\}$, 则

$$\mathbf{N}_{K/\mathbb{Q}}(x)=\frac{\mathbf{N}_{K/\mathbb{Q}}(\alpha)^j}{p^n}\mathbf{N}_{K/\mathbb{Q}}(\sum_{i=j}^{n-1}x_i\alpha^{i-j}).$$

注意到

$$\mathbf{N}_{K/\mathbb{Q}}(\sum_{i=j}^{n-1}x_i\alpha^{i-j})=\prod_{k=1}^{n}(x_j+x_{j+1}\sigma_k(\alpha)+\cdots+x_{n-1}\sigma_k(\alpha)^{n-1-j}).$$

展开后为 α 的共轭元 $\sigma_1(\alpha),\ldots,\sigma_n(\alpha)$ 的初等对称函数的多项式, 且常数项为 x_j^n. 由于 $p\mid a_0,\ldots,a_{n-1}$, 因此其模 p 同余于 x_j^n. 而 p 整除但 p^2 不整除 $\mathbf{N}_{K/\mathbb{Q}}(\alpha)=(-1)^n a_n$, 因此 $\mathbf{N}_{K/\mathbb{Q}}(x)\notin\mathbb{Z}, x\notin\mathcal{O}_K$, 矛盾! 因此 $1,\alpha,\ldots,\alpha^{n-1}$ 构成一组整基. $\square$

例题 1.3 设 $K=\mathbb{Q}(\alpha),\alpha^3=2$. 则 $\operatorname{disc}(1,\alpha,\alpha^2)=-2^2 3^3$. 而 $f(T)=T^3-2$ 关于 2 是艾森斯坦的, $f(T-1)=T^3-3T^2+3T-3$ 关于 3 是艾森斯坦的, 因此 $\mathcal{O}_K=\mathbb{Z}[\alpha]$.

例题 1.4 设 p 为奇素数, $K=\mathbb{Q}(\zeta),\zeta=e^{2\pi i/p}$ 的极小多项式为

$$f(T)=\frac{T^p-1}{T-1}=T^{p-1}+\cdots+1=\prod_{i=1}^{p-1}(T-\zeta^i),$$

因此

$$\begin{aligned}\operatorname{disc}(1,\zeta,\ldots,\zeta^{p-2})&=(-1)^{\frac{p(p-1)}{2}}\prod_{\substack{i,j=1\\ i\neq j}}^{p-1}(\zeta^i-\zeta^j)\\&=(-1)^{\frac{(p-1)(p-2)}{2}}\prod_{j=1}^{p-1}\prod_{\substack{i=1\\ i\neq -j}}^{p-1}(1-\zeta^i)\\&=(-1)^{\frac{(p-1)(p-2)}{2}}\left(\prod_{i=1}^{p-1}(1-\zeta^i)\right)^{p-2}\\&=(-1)^{\frac{(p-1)(p-2)}{2}}f(1)^{p-2}=(-1)^{\frac{(p-1)(p-2)}{2}}p^{p-2}.\end{aligned}$$

又因为 $f(T+1)=T^{p-1}+\sum\limits_{i=1}^{p-1}\binom{p}{i}T^{i-1}$ 是艾森斯坦的, 因此 $\mathcal{O}_K=\mathbb{Z}[\zeta_p]$.

✍ **练习 1.2.6** 证明 $1,\alpha,\frac{1}{2}(\alpha+\alpha^2)$ 是数域 $\mathbb{Q}(\alpha)$ 的一组整基, 其中 $\alpha^3-\alpha-4=0$.

✍ **练习 1.2.7** (Stickelberger 判别式关系) 证明 $\Delta_K\equiv 0,1 \bmod 4$. 提示: 设 P,N 分别为行列式 $\det(\tau_i\omega_j)_{ij}$ 中符号为正/负的置换对应的项之和, 则 $\Delta_K=(P-N)^2, P+N, PN$ 是整数.

§1.2.3 无穷素位

我们来研究下判别式的符号. 设 K 是 n 次数域. 考虑嵌入 $\sigma\in\operatorname{Hom}_{\mathbb{Q}}(K,\mathbb{C})$, 容易看出, $\overline{\sigma}: K\xrightarrow{\sigma}\mathbb{C}\xrightarrow{\text{复共轭}}\mathbb{C}$ 也是一个嵌入.

定义 1.20 (无穷素位)

(1) 称 σ 为无穷素位 (infinity place). 如果 $\sigma(K) \subseteq \mathbb{R}$, 即 $\overline{\sigma} = \sigma$, 称 σ 为实嵌入 (real embedding) 或实素位 (real place), 否则称之为复嵌入 (complex embedding) 或复素位 (complex place). 我们视一对复嵌入为同一个复素位.

(2) 如果 K 没有复素位, 称 K 为全实域 (totally real field); 如果 K 没有实素位, 称 K 为全虚域 (totally imaginary field).

设 K 有 r 个实嵌入和 s 对复嵌入, 那么

$$r + 2s = n.$$

如果 $K = \mathbb{Q}(\gamma)$, 则 γ 的共轭根中有 r 个实数和 s 对复数. 如果 $K/\mathbb{Q}$ 是伽罗瓦扩张, 那么由于 K 的共轭域均为其自身, 因此 K 必为全实域或全虚域.

命题 1.21

判别式 Δ_K 的符号为 $(-1)^s$.

证明 设 $\alpha_1, \ldots, \alpha_n$ 是 K 的一组整基. 设

$$\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C}) = \Big\{ \underbrace{\sigma_1, \ldots, \sigma_r}_{\text{实嵌入}}, \underbrace{\sigma_{r+1}, \ldots, \sigma_n}_{\text{复嵌入}} \Big\},$$

且 $\sigma_{r+2i} = \overline{\sigma}_{r+2i-1}, 1 \le i \le s$, 则

$$\overline{\det\big(\sigma_i(\alpha_j)\big)_{i,j}} = \det\big(\overline{\sigma}_i(\alpha_j)\big)_{i,j} = (-1)^s \det\big(\sigma_i(\alpha_j)\big)_{i,j},$$

这里我们交换了 s 对 $\big(\overline{\sigma}_i(\alpha_j)\big)_{i,j}$ 的行向量. 于是

$$(-1)^s \Delta_K = (-1)^s \big|\det\big(\sigma_i(\alpha_j)\big)_{i,j}\big|^2 > 0.$$

□

✍ **练习 1.2.8** 研究下列域的无穷素位:

(1) 二次域 $\mathbb{Q}(\sqrt{d})$, 其中 $d \ne 0, 1$ 为无平方因子整数.

(2) 分圆域 $\mathbb{Q}(\zeta)$, 其中 $\zeta = e^{2\pi i/n}$, $n \ge 3$ 为正整数.

(3) 三次域 $\mathbb{Q}(\gamma)$.

§1.2.4 分圆域的整数环

设 $N \ge 3, \zeta_N \in \mathbb{C}$ 是 N 次本原 (primitive) 单位根, 即 $\zeta_N = e^{2c\pi i/N}, \gcd(c, N) = 1$.

命题 1.22 (分圆域的伽罗瓦群)

我们有同构 $\mathrm{Gal}\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$.

证明 $\sigma \in \mathrm{Gal}\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big)$ 总将 ζ_N 映为 N 次本原单位根 $\zeta_N^a, \gcd(a, N) = 1$, 设 $\varphi(\sigma) = a$, 则有单同态 $\varphi : \mathrm{Gal}\big(\mathbb{Q}(\zeta_N)/\mathbb{Q}\big) \hookrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$.

我们将证明如下事实: 对于素数 p 和 N 次本原单位根 ζ, ζ^p 和 ζ 共轭. 这样, 任意与 N 互素的正整数 a 可以表达成一些素数的乘积, 从而 ζ_N^a 与 ζ_N 共轭, φ 满. 设 $f(T) \in \mathbb{Z}[T]$ 是 ζ 的极小多项式, $T^N - 1 = f(T)g(T)$. 如果 ζ^p 不是 ζ 的共轭元, 则 $g(\zeta^p) = 0$, 即 $g(T^p)$ 零化 ζ, $f(T) \mid g(T^p)$. 设 $\bar{f}, \bar{g} \in \mathbb{F}_p[x]$ 为 f, g 模 p 的像, 则 $\bar{f}(T) \mid \bar{g}(T^p) = \bar{g}(T)^p$. 设 $\alpha \in \overline{\mathbb{F}}_p$ 是 $\bar{f}$ 的一个根, 则 $\bar{g}(\alpha) = 0$, α 是

$\bar{F}(T)=\bar{f}(T)\bar{g}(T)$ 的一个重根. 而 $\bar{F}'(\alpha)=N\alpha^{N-1}\neq 0$, $\bar{F}'$ 无重根, 矛盾! □

推论 1.23

设 $N,M\geq 2$, $\gcd(N,M)=1$, 则 $\mathbb{Q}(\zeta_N)\cap\mathbb{Q}(\zeta_M)=\mathbb{Q}$.

证明 由于 $\mathbb{Q}(\zeta_{NM})=\mathbb{Q}(\zeta_N)\mathbb{Q}(\zeta_M)$,

$$[\mathbb{Q}(\zeta_M):\mathbb{Q}(\zeta_N)\cap\mathbb{Q}(\zeta_M)]=[\mathbb{Q}(\zeta_{NM}):\mathbb{Q}(\zeta_N)]=\frac{\varphi(MN)}{\varphi(N)}=\varphi(M)=[\mathbb{Q}(\zeta_M):\mathbb{Q}],$$

因此命题成立. □

称

$$\Phi_N(T)=\prod_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}(T-\zeta_N^a)\in\mathbb{Z}[T],$$

N-th cyclotomic polynomial
为 N 次分圆多项式. 它是 ζ_N 的极小多项式, 且

$$T^N-1=\prod_{a\in\mathbb{Z}/N\mathbb{Z}}(T-\zeta_N^a)=\prod_{d|N}\Phi_N(T),$$

Möbius inverse formula
由默比乌斯反演[1]可知

$$\Phi_N(T)=\prod_{d|N}(T^d-1)^{\mu(N/d)}.$$

命题 1.24

$\mathbb{Q}(\zeta_N)$ 的判别式整除 $N^{\varphi(N)}$. 由此可知, 如果 p 是素数, 则 $\mathbb{Q}(\zeta_{p^n})$ 的整数环为 $\mathbb{Z}[\zeta_{p^n}]$.

证明 设 $T^N-1=\Phi_N(T)F(T)$, 则

$$NT^{N-1}=\Phi_N'(T)F(T)+\Phi_N(T)F'(T),$$
$$N\zeta_N^{N-1}=\Phi_N'(\zeta_N)F(\zeta_N).$$

因此 $\mathbf{N}_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(\Phi_N'(\zeta_N))$ 整除 $\mathbf{N}_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(N\zeta_N^{N-1})=N^{\varphi(N)}$. 由命题 1.9 可知

$$\operatorname{disc}(1,\zeta_N,\ldots,\zeta_N^{N-1})\mid N^{\varphi(N)},$$

因此 $\mathbb{Q}(\zeta_N)$ 的判别式也整除 $N^{\phi(N)}$.

由于

$$\Phi_{p^n}(T+1)\cdot\left((T+1)^{p^{n-1}}-1\right)=(T+1)^{p^n}-1,$$

两边展开模 p 可知 $\Phi_{p^n}(T+1)$ 除了首项外系数均被 p 整除. 容易知道 $\Phi_{p^n}(T+1)$ 常数项为 p, 因此它是艾森斯坦多项式, 根据命题 1.19 可知 $\mathbb{Q}(\zeta_{p^n})$ 的整数环为 $\mathbb{Z}[\zeta_{p^n}]$. □

---

[1] 默比乌斯反演是指

$$a_n=\sum_{d|n}b_d\implies b_n=\sum_{d|n}\mu(\frac{n}{d})a_d,$$

Möbius function
其中默比乌斯函数

$$\mu(n)=\begin{cases}1, & n=1;\\ (-1)^k, & n=p_1\cdots p_k\text{ 为 }k\text{ 个不同素数乘积;}\\ 0, & n\text{ 有平方因子.}\end{cases}$$

引理 1.25

对于数域 K, L, 如果 $[KL:\mathbb{Q}]=[K:\mathbb{Q}][L:\mathbb{Q}]$, 则 $\mathcal{O}_{KL}\subseteq\frac{1}{d}\mathcal{O}_K\mathcal{O}_L, d=\gcd(\Delta_K,\Delta_L)$. 特别地, 如果 $\gcd(\Delta_K,\Delta_L)=1$, 则 $\mathcal{O}_{KL}=\mathcal{O}_K\mathcal{O}_L$.

证明 显然有 $\mathcal{O}_K\mathcal{O}_L\subseteq\mathcal{O}_{KL}$. 由假设可知 $K\otimes_{\mathbb{Q}}L\to KL$ 是同构. 设 $(\alpha_1,\ldots,\alpha_n)$ 和 $(\beta_1,\ldots,\beta_m)$ 分别是 K 和 L 的一组整基, 则 $\mathcal{O}_{KL}$ 中的任一元素可表为

$$x=\sum_{i,j}\frac{x_{i,j}}{r}\alpha_i\beta_j,\quad x_{i,j},r\in\mathbb{Z},\gcd(x_{1,1},\ldots,x_{n,m},r)=1.$$

令 $(\alpha_i^\vee)_i$ 为 $(\alpha_i)_i$ 的对偶基, 则

$$\mathrm{Tr}_{KL/L}(x\alpha_i^\vee)=\sum_{k,l}\frac{x_{k,l}}{r}\mathrm{Tr}_{KL/L}(\alpha_k\beta_l\alpha_i^\vee)=\sum_{l}\frac{x_{i,l}}{r}\beta_l,$$

这里 $\mathrm{Tr}_{KL/L}(\alpha_k\alpha_i^\vee)=\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_k\alpha_i^\vee)=1$. 由对偶基的定义可知 $\Delta_K\alpha_i^\vee\in\mathcal{O}_K$, 因此 $\Delta_Kx\alpha_i^\vee\in\mathcal{O}_{KL}$, 于是我们有

$$\mathrm{Tr}_{KL/L}\left(\sum_j\Delta_K\cdot\frac{x_{i,j}}{r}\beta_j\right)=\Delta_K\mathrm{Tr}_{KL/L}(x\alpha_i^\vee)\in\mathrm{Tr}_{KL/L}(\mathcal{O}_{KL})\subseteq\mathcal{O}_L.$$

由于 $(\beta_j)_j$ 是 $\mathcal{O}_L$ 的一组整基, 因此 $\Delta_K\cdot\frac{x_{i,j}}{r}\in\mathbb{Z}, r\mid\Delta_K$. 由对称性, $r\mid\Delta_L$, 因此 $r\mid d$. □

推论 1.26

对于 n 次数域 K 和 m 次数域 L, 如果 $[KL:\mathbb{Q}]=mn$ 且 $\gcd(\Delta_K,\Delta_L)=1$, 则 $\Delta_{KL}=\Delta_K^m\Delta_L^n$.

证明 设 $w_1,\ldots,w_n$ 为 K 的一组整基, $v_1,\ldots,v_m$ 为 L 的一组整基, 则 $\{w_iv_j\}_{ij}$ 为 KL 的一组整基. 设 $\tau_1,\ldots,\tau_n$ 为所有嵌入 $K\hookrightarrow\overline{\mathbb{Q}}$, $\sigma_1,\ldots,\sigma_m$ 为所有嵌入 $L\hookrightarrow\overline{\mathbb{Q}}$, $a_{ik}=\tau_i(w_k), b_{j\ell}=\sigma_j(v_\ell)$, 则

$$\Delta_K=\det\big((a_{ik})_{ik}\big)^2,\ \Delta_L=\det\big((b_{j\ell})_{j\ell}\big)^2,\ \Delta_{KL}=\det\big((a_{ik}b_{j\ell})_{(i,j),(k,\ell)}\big)^2.$$

记这三个矩阵分别为 $A,B,A\otimes B$, 则我们需要证明 $\det(A\otimes B)=\det(A)^m\det(B)^n$. 我们将 A 写成初等矩阵的乘积, 而对于初等矩阵该等式是容易验证的. 因此该命题成立. □

定理 1.27 (分圆域的整数环)

$\mathbb{Q}(\zeta_N)$ 的整数环为 $\mathbb{Z}[\zeta_N]$.

证明 我们对 N 的素因子个数进行归纳. 若 N 只有一个素因子, 由命题 1.24 已得. 若不然, 设 $N=nm, n,m>1,\gcd(n,m)=1$, 由推论 1.23、命题 1.24 和引理 1.25 以及归纳假设可知

$$\mathcal{O}_{\mathbb{Q}(\zeta_N)}=\mathcal{O}_{\mathbb{Q}(\zeta_m)}\mathcal{O}_{\mathbb{Q}(\zeta_n)}=\mathbb{Z}[\zeta_n,\zeta_m]=\mathbb{Z}[\zeta_N].$$

□

命题 1.28 (分圆域的判别式)

$\Delta_{\mathbb{Q}(\zeta_{p^n})}$ 的判别式为 $\pm p^{p^{n-1}(pn-n-1)}$, 当 $p\equiv 3\bmod 4$ 或 $p^n=4$ 时符号为 $-$, 其余情形符号为 $+$.

证明 符号由命题 1.21 得到. 我们知道 ζ_{p^n} 的极小多项式为

$$\Phi(T)=\frac{T^{p^n}-1}{T^{p^{n-1}}-1}=\sum_{i=0}^{p-1}T^{p^{n-1}i}.$$

当 $p=2$ 时, $\Phi'(\zeta_{2^n})=2^{n-1}\zeta_{2^n}^{2^{n-1}-1}$, $\mathbf{N}_{\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}}\big(\Phi'(\zeta_{2^n})\big)=2^{2^{n-1}(n-1)}$. 当 $p\geq 3$ 时,

$$\begin{aligned}\Phi'(\zeta_{p^n})&=\sum_{i=1}^{p-1}p^{n-1}i\zeta_{p^n}^{p^{n-1}i-1}\\&=p^{n-1}\zeta_{p^n}^{p^{n-1}-1}\sum_{i=1}^{p-1}i\zeta_{p^n}^{p^{n-1}(i-1)}\\&=p^{n-1}\zeta_{p^n}^{p^{n-1}-1}\sum_{i=1}^{p-1}i\zeta_{p}^{i-1}\\&=p^{n-1}\zeta_{p^n}^{p^{n-1}-1}\Phi_p'(\zeta_p)\end{aligned}$$

由习题 1.4 知 $\mathbf{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p)=\pm p^{p-2}$, 于是

$$\mathbf{N}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}\big(\Phi'(\zeta_{p^n})\big)=\pm p^{p^{n-1}(p-1)(n-1)}p^{(p-2)p^{n-1}}=\pm p^{p^{n-1}(np-p-1)}.$$

由命题 1.9 可知结论成立. □

练习 1.2.9 证明 $\mathbb{Q}(\mu_n)$ 的判别式为

$$(-1)^{\varphi(n)/2}\frac{n^{\varphi(n)}}{\prod_{p|n}p^{\varphi(n)/(p-1)}}.$$

§1.3 理想

§1.3.1 唯一分解性

例题 1.5 设 $K=\mathbb{Q}(\sqrt{-5})$. 在 $\mathcal{O}_K=\mathbb{Z}[\sqrt{-5}]$ 中,

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

容易验证 $2,3,1\pm\sqrt{-5}$ 都是不可约元, 因此 $\mathcal{O}_K$ 不是唯一因子分解整环. 然而, 令

$$\mathfrak{a}=(2,1+\sqrt{-5})=(2,1-\sqrt{-5}),$$
$$\mathfrak{b}=(3,1+\sqrt{-5}),\quad \bar{\mathfrak{b}}=(3,1-\sqrt{-5}),$$

则 $\mathcal{O}_K/\mathfrak{a}\cong\mathbb{F}_2,\mathcal{O}_K/\mathfrak{b}\cong\mathcal{O}_K/\bar{\mathfrak{b}}\cong\mathbb{F}_3$, 因此 $\mathfrak{a},\mathfrak{b},\bar{\mathfrak{b}}$ 均是素理想, 且

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

因此 $(6)=\mathfrak{a}^2\mathfrak{b}\bar{\mathfrak{b}}$. 实际上, 作为 $\mathcal{O}_K$ 理想, (6) 的素理想分解是唯一的.

练习 1.3.1 给定数域 K, 我们总简记 $\mathbf{N}=\mathbf{N}_{K/\mathbb{Q}}$. 证明 $\alpha\in\mathcal{O}_K$ 是一个单位当且仅当 $\mathbf{N}(\alpha)=\pm 1$. 如果 $\pm\mathbf{N}(\alpha)$ 是一个素数, 则 α 是一个素元.

$\mathcal{O}_K$ 的理想的唯一分解性来源于它是一个戴德金整环.

定义 1.29 (诺特环和戴德金整环)

如果一个交换环的任意上升的理想链

$$0\subseteq I_1\subseteq I_2\subseteq\dots$$

均稳定, 即存在 $N>0$ 使得 $I_N=I_{N+1}=I_{N+2}=\cdots$, 则我们称其为诺特环 (noetherian ring). 如果一个诺特整环是整闭的, 且任意非零素理想都是极大理想, 则称其为戴德金整环 (Dedekind domain).

练习 1.3.2 举一个不是诺特环的例子.

练习 1.3.3 (希尔伯特基定理) 如果 R 是诺特环, 则 $R[x]$ 也是诺特环. 提示: 考虑 $R[x]$ 非零理想 $\mathfrak{a}$ 所有最高次项次数构成的 R 的理想.

练习 1.3.4 设 $\mathcal{O}$ 是戴德金整环, $\mathfrak{a}$ 是非零理想, 则 $\mathcal{O}/\mathfrak{a}$ 是主理想整环. 由此证明 $\mathfrak{a}$ 可以由两个元素生成.

命题 1.30

交换环 R 是诺特环当且仅当 R 的每个理想是有限生成的 R 模.

证明 设 $\mathfrak{a}$ 是诺特环 R 的理想, S 是所有包含在 $\mathfrak{a}$ 中有限生成理想的集合. 如果 S 没有极大元, 则任取 $\mathfrak{a}_1 \in S$, 存在 $\mathfrak{a}_2 \supsetneq \mathfrak{a}_1$, 依次下去可以得到一个无限严格递增的理想链, 这与 R 诺特矛盾. 因此 S 有极大元. 如果 S 的极大元 $\mathfrak{b} \neq \mathfrak{a}$, 设 $x \in \mathfrak{a} - \mathfrak{b}$, 则 $\mathfrak{b} + (x)$ 仍然是有限生成的, 矛盾! 因此 $\mathfrak{a}$ 是有限生成的.

反之, 如果 R 的每个理想都是有限生成的, 则对于任意理想升链 $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$, $\mathfrak{a} = \bigcup_i \mathfrak{a}_i$ 是有限生成的. 设 $\mathfrak{a} = \sum\limits_{i=1}^{r} Ra_i$, $a_i \in \mathfrak{a}_{n_i}$, 则 $\mathfrak{a} = \mathfrak{a}_n, n = \max\{n_1, \ldots, n_r\}$. 因此该升链稳定. □

定理 1.31

戴德金整环具有素理想唯一分解性, 即任意非零理想可唯一分解为有限个素理想的乘积.

我们将理想的概念稍做扩充.

定义 1.32 (分式理想)

设 $\mathcal{O}$ 是戴德金整环. 对于 $K = \operatorname{Frac}\mathcal{O}$ 的非零子集 $\mathfrak{a}$, 如果存在 $\mathcal{O}$ 中的非零元 c 使得 $c\mathfrak{a}$ 为 $\mathcal{O}$ 的理想, 则称 $\mathfrak{a}$ 为 $\mathcal{O}$ 的一个分式理想 (fractional ideal). 换言之, 分式理想是 K 的有限生成非零 $\mathcal{O}$ 子模.

定理 1.31 的证明 我们断言, 对于 $\mathcal{O}$ 的任意一个非零理想 $\mathfrak{a}$, 均存在非零素理想 $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ 使得

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

设 S 为所有不满足该性质的非零理想的集合. 假设 S 非空. 由于 $\mathcal{O}$ 是诺特的, S 中的元素关于包含关系拥有极大元 $\mathfrak{a}$. $\mathfrak{a}$ 不是素理想, 因此存在 $b_1, b_2 \in \mathcal{O}$ 使得 $b_1, b_2 \notin \mathfrak{a}, b_1b_2 \in \mathfrak{a}$. 设 $\mathfrak{a}_i = \mathfrak{a} + (b_i)$, 则 $\mathfrak{a} \subsetneq \mathfrak{a}_i, \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$. 由 $\mathfrak{a}$ 的极大性, $\mathfrak{a}_1, \mathfrak{a}_2 \notin S$, 因此它们包含素理想的乘积, 由此推出 $\mathfrak{a}$ 也包含, 矛盾!

设 $\mathfrak{p}$ 是一个素理想. 任取 $0 \neq b \in \mathfrak{p}$, 设 r 为满足 $(b) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$ 的最小的 r, 其中 $\mathfrak{p}_i$ 为素理想. 由于 $\mathfrak{p}$ 是素理想, 它必须包含某个 $\mathfrak{p}_i$. 不妨设 $\mathfrak{p} \supseteq \mathfrak{p}_1$, 由于 $\mathfrak{p}_i$ 是极大理想, $\mathfrak{p} = \mathfrak{p}_1$, $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (b)$. 于是存在 $a \in \mathfrak{p}_2 \cdots \mathfrak{p}_r, a \notin (b)$. 因此 $ab^{-1}\mathfrak{p} \subseteq b^{-1}\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathcal{O}$. 记

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathcal{O}\},$$

则 $ab^{-1} \in \mathfrak{p}^{-1}$. 因此 $\mathfrak{p}^{-1} \neq \mathcal{O}$.

显然 $\mathcal{O} \subseteq \mathfrak{p}^{-1}$, $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$. 假设 $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$, 设 $\mathfrak{p} = \sum\limits_{i=1}^{r} \mathcal{O}\alpha_i$, 则对于任一 $x \in \mathfrak{p}^{-1}, x \notin \mathcal{O}$,

$$x\alpha_i = \sum_j c_{ij}\alpha_j, \quad c_{ij} \in \mathcal{O}.$$

设 $C = (c_{ij})_{ij}$, 则 $\det(xI_r - C) = 0$, x 在 $\mathcal{O}$ 上整, 于是 $x \in \mathcal{O}$, 矛盾! 因此 $\mathfrak{p} \neq \mathfrak{p}\mathfrak{p}^{-1}$. 由于 $\mathfrak{p}$ 是极大理想, $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.

设 T 是所有不能写成有限多个素理想乘积的理想全体. 如果 T 非空, 则存在极大元 I. 由于 I 不是素理想, 存在素理想 $\mathfrak{p}$ 使得 $I \subsetneq \mathfrak{p}$. 由于 $\mathfrak{p}^{-1}\mathfrak{p} = A$, 因此 $\mathfrak{p}^{-1}I \subsetneq \mathcal{O}$ 是理想. 由 I 的极大性知 $\mathfrak{p}^{-1}I =$

$\prod_i \mathfrak{p}_i, I = \mathfrak{p}\prod_i \mathfrak{p}_i$, 矛盾! 因此每个非零理想均可表为有限多个素理想乘积.

假设 $\prod_{i=1}^{r}\mathfrak{p}_i = \prod_{j=1}^{s}\mathfrak{q}_j$. 如果 $r \geq 1$, $\mathfrak{p}_1 \supseteq \prod_{j=1}^{s}\mathfrak{q}_j$, 因此 $\mathfrak{p}_1$ 包含某个 $\mathfrak{q}_j$. 不妨设 $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$, 则 $\mathfrak{p}_1 = \mathfrak{q}_1$, $\prod_{i=2}^{r}\mathfrak{p}_i = \prod_{j=2}^{s}\mathfrak{q}_j$. 归纳可知该分解唯一. □

练习 1.3.5 设 $\mathfrak{a}, \mathfrak{b}$ 为 $\mathcal{O}$ 的分式理想. 证明

(1) $\mathfrak{a}\mathfrak{b} = \left\{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\right\}$ 是一个分式理想.

(2) $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}$ 是一个分式理想.

推论 1.33

数域的整数环具有素理想唯一分解性.

推论 1.34

戴德金整环 $\mathcal{O}$ 的分式理想 $\mathfrak{a}$ 可唯一分解为

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}},$$

其中 $\mathfrak{p}$ 为素理想, $e_{\mathfrak{p}} \in \mathbb{Z}$ 只有有限多非零项.

定理 1.35

数域的整数环 $\mathcal{O}_K$ 是戴德金整环.

主理想整环如 $\mathbb{Z}, \mathbb{F}_p[T], \mathbb{C}[T]$ 都是唯一因子分解整环, 同样可知它们都是戴德金整环.

推论 1.36

戴德金整环 $\mathcal{O}$ 是唯一因子分解整环当且仅当它是主理想整环.

证明 充分性显然, 下证必要性. 设戴德金整环 $\mathcal{O}$ 是唯一因子分解整环, $\mathfrak{p}$ 是 $\mathcal{O}$ 的非零素理想, $0 \neq x \in \mathfrak{p}$. 设 $x = p_1 \cdots p_r$ 是素元分解, 则 $\mathfrak{p} \mid (x) = \prod (p_i)$, $\mathfrak{p} \mid (p_i)$. 由于 (p_i) 是极大理想, 因此 $\mathfrak{p} = (p_i)$ 是主理想. □

证明 根据定理 1.15, $\mathcal{O}_K$ 的理想 $\mathfrak{a}$ 是有限生成 $\mathbb{Z}$ 模, 自然也是有限生成 $\mathcal{O}_K$ 模. 由命题 1.13, $\mathcal{O}_K$ 作为 $\mathbb{Z}$ 在 K 中整闭包, 它是整闭的. 设 $\mathfrak{p}$ 是 $\mathcal{O}_K$ 的非零素理想, 则对于任意 $0 \neq x \in \mathfrak{p}$, 设首一多项式

$$f(T) = T^n + a_1 T^{n-1} + \cdots + a_n \in \mathbb{Z}[T],$$

是 x 的极小多项式, 则 $0 \neq a_n \in \mathfrak{p} \cap \mathbb{Z}$, 因此 $\mathfrak{p} \cap \mathbb{Z}$ 是 $\mathbb{Z}$ 的非零理想. 显然它是素理想, 因此 $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. 由于 $\mathcal{O}_K/\mathfrak{p}$ 是域 $\mathbb{Z}/p\mathbb{Z}$ 添加若干代数元得到, 因此它是一个域, $\mathfrak{p}$ 是极大理想. □

练习 1.3.6 分式理想全体构成一个交换群 $\mathcal{I}_K$, 幺元为 $(1) = \mathcal{O}_K$.

练习 1.3.7 设 $d \neq 0, 1$ 是平方自由的整数, $K = \mathbb{Q}(\sqrt{d})$. 对于素数 p, $p\mathcal{O}_K$ 是素理想当且仅当 $x^2 \equiv d \bmod p$ 无解.

§1.3.2 单位群和理想类群

我们将形如 $(\alpha)=\alpha\mathcal{O}_K,\alpha\in K^\times$ 的分式理想称为主分式理想 (principal fractional ideal), 记 $\mathcal{P}_K$ 为主分式理想全体构成的群. 我们有群的正合列[1]

$$1\longrightarrow\mathcal{O}_K^\times\longrightarrow K^\times\xrightarrow{\alpha\mapsto(\alpha)}\mathcal{I}_K\longrightarrow\mathrm{Cl}_K\longrightarrow 1\,,$$

其中 $\mathcal{O}_K^\times$ 为 K 的单位群 (group of units), 即 $\mathcal{O}_K$ 中全体单位, $\mathrm{Cl}_K=\mathcal{I}_K/\mathcal{P}_K$ 为 K 的理想类群 (class group). 可以看出, 单位群和类群描述的是 "数和理想的差异", 特别地, 类群表达了 "素元分解成立的程度".

记 μ_K 为 K 中单位根全体.

✍ **练习 1.3.8** 证明 μ_K 是 $\mathcal{O}_K^\times$ 的极大有限子群, 且它是循环群.

✍ **练习 1.3.9** 求所有二次域的单位根群.

✍ **练习 1.3.10** 设 $\mathfrak{m}$ 是 $\mathcal{O}_K$ 的非零理想. 对于任意 Cl_K 中的理想类, 均存在一个与 $\mathfrak{m}$ 互素的整理想代表元.

定理 1.37 (狄利克雷单位定理)

$\mathcal{O}_K^\times$ 为有限生成交换群, 秩为 $r+s-1$, 即

$$\mathcal{O}_K^\times\cong\mu_K\times\mathbb{Z}^{r+s-1},$$

其中 r,s 分别为 K 的实素位和复素位的个数.

例题 1.6 设 $K=\mathbb{Q}(\sqrt{2})$, 则 $r=2,s=0,\mu_K=\{\pm1\}$,

$$\mathcal{O}_K^\times=\left\{\pm(1+\sqrt{2})^n\mid n\in\mathbb{Z}\right\}\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}.$$

一般地, 设 $K=\mathbb{Q}(\sqrt{d})$ 为实二次域, $d>1$ 为无平方因子正整数. 存在 $\varepsilon\in\mathcal{O}_K^\times$ 使得

$$\mathcal{O}_K^\times=\{\pm\varepsilon^n\mid n\in\mathbb{Z}\}\,.$$

这样的 ε 被称为实二次域 K 的基本单位 (fundamental unit).

我们来看狄利克雷单位定理的一个应用. 设 $d>1$ 无平方因子, $K=\mathbb{Q}(\sqrt{d})$, P_d 为佩尔方程 $x^2-dy^2=\pm1$ 的整数解全体, P_d' 为其正整数解全体.

推论 1.38

设 (x_0,y_0) 是 P_d' 中 x,y 最小的元素, $\varepsilon=x_0+y_0\sqrt{d}$, 则

$$P_d=\left\{(x,y)\mid x+y\sqrt{d}=\pm\varepsilon^n,n\in\mathbb{Z}\right\}.$$

证明 对于任意元素 $\alpha=x+y\sqrt{d}\in\mathbb{Z}[\sqrt{d}]\subseteq\mathcal{O}_K$, $\mathbf{N}(\alpha)=x^2-dy^2$. 如果 $x\in\mathbb{Z}[\sqrt{d}]^\times$, 则 $\mathbf{N}(x)$ 也可逆, 即 $\mathbf{N}(x)=\pm1$. 反之亦然, 因此 $\mathbb{Z}[\sqrt{d}]^\times\xrightarrow{\sim}P_d$.

由狄利克雷单位定理, $\mathcal{O}_K^\times$ 秩为 1. 设 u 为任一无限阶元, 则 u 在 $\mathcal{O}_K/2\mathcal{O}_K$ 中的像可逆. 假设它的阶为 $n\geq1$, 则 $u^{\pm n}-1\in2\mathcal{O}_K\subseteq\mathbb{Z}[\sqrt{d}]$, $u^n\in\mathbb{Z}[\sqrt{d}]^\times$. 于是 $\mathbb{Z}[\sqrt{d}]^\times$ 是无限群, 显然它有限部分为 ±1, 因此存在 $\varepsilon_0\in\mathbb{Z}[\sqrt{d}]$ 使得 $\mathbb{Z}[\sqrt{d}]^\times=\{\pm\varepsilon_0^n\mid n\in\mathbb{Z}\}$. 由于 $\pm\varepsilon_0,\pm\varepsilon_0^{-1}$ 均可替代其地位, 不妨设 $\varepsilon_0=x_1+y_1\sqrt{d},x_1,y_1>0$. 于是 $n\geq2$ 时,

$$\varepsilon_0^n=x'+y'\sqrt{d},\quad x'>x,y'>y,$$

[1] 见定义 A.33.

故 $\varepsilon_0 = \varepsilon$. □

练习 1.3.11 $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5})$ 的基本单位分别是什么?

例题 1.7 设 $K = \mathbb{Q}(\sqrt[3]{2})$, 则 $r = 1, s = 1$,

$$\mathcal{O}_K^\times = \left\{\pm(1-\sqrt[3]{2})^n \mid n \in \mathbb{Z}\right\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

练习 1.3.12 证明 $x^3 + 3y^3 + 9z^3 - 9xyz = 1$ 有无穷多整数解.

例题 1.8 如果 $\mathcal{O}_K^\times$ 有限, 则 $r + s = 1$, $(r, s) = (1, 0)$ 或 $(0, 1)$, 即 $K = \mathbb{Q}$ 或为虚二次域.

定理 1.39 (类群有限性定理)

数域的理想类群是有限的.

我们将在下一节证明这两个定理.

类群的大小被称为类数 (class number) h_K. 类数为 1 即指 $\mathcal{O}_K$ 为主理想整环. 对于虚二次域 $\mathbb{Q}(\sqrt{d}), d < 0$, 高斯猜想并由贝克 [1, p. I] 和 Stark [20] 证明它的类数等于 1 当且仅当

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Goldfeld [7] 通过 Gross-Zagier 公式 [8] 找到一条特殊的椭圆曲线, 并利用它给出了类数的一个下界 (d 的函数), 从而可以有效地得到类数为给定值的所有虚二次域. 对于实二次域而言, 高斯猜想有无穷多个类数为 1 的实二次域. 尽管我们已经知道了很多类数为 1 的实二次域 [14], 但该猜想仍未解决, 甚至我们不知道是否有无穷多类数为 1 的数域.

对于分圆域而言, 如果 $p \nmid h_{\mathbb{Q}(\zeta_p)}, p \geq 3$, 库默尔证明了

$$x^p + y^p = z^p, \quad xyz \neq 0$$

无整数解, 见 [12, Chapter 1]. 这也是库默尔引出 “理想” 这一概念的源头. 该方程即著名的费马大定理, 它由怀尔斯 [21, 22] 于 1994 年完全证明.

§1.3.3 局部化

有时候我们需要考虑 K 的整数环 $\mathcal{O}_K$ 的一些类比, 这些类比往往具有和 $\mathcal{O}_K$ 类似的性质, 例如它的局部化.

命题 1.40

戴德金整环的局部化仍然是戴德金整环.

证明 设 $\mathcal{O}$ 是戴德金整环, $S \subseteq \mathcal{O} \setminus \{0\}$ 为一乘法集. 设 $\mathfrak{A}$ 是 $S^{-1}\mathcal{O}$ 的理想, $\mathfrak{a} = \mathfrak{A} \cap \mathcal{O}$, 则 $\mathfrak{A} = S^{-1}\mathfrak{a}$. 由于 $\mathfrak{a}$ 有限生成, 因此 $\mathfrak{A}$ 也是有限生成的, 故 $S^{-1}\mathcal{O}$ 是诺特的. 由于 $S^{-1}\mathcal{O}$ 的素理想为 $S^{-1}\mathfrak{p}$, 其中 $\mathfrak{p}$ 是 $\mathcal{O}$ 的素理想且 $\mathfrak{p} \cap S = \emptyset$, 因此它是极大理想. 最后, 如果 $x \in K$ 满足方程

$$x^n + \frac{a_1}{s_1}x^{n-1} + \cdots + \frac{a_n}{s_n} = 0, \quad a_i \in \mathcal{O}, s_i \in S,$$

则 $s_1 \ldots s_n x$ 在 $\mathcal{O}$ 上整, 从而属于 $\mathcal{O}$, $x \in S^{-1}\mathcal{O}$. 综上所述, $S^{-1}\mathcal{O}$ 是戴德金的. □

设 S 是 $\mathcal{O}_K$ 的有限多个素理想构成的集合, 定义

$$\mathcal{O}_{K,S} = \left\{\frac{f}{g} \mid f, g, \in \mathcal{O}_K, g \notin \mathfrak{p}, \forall \mathfrak{p} \notin S\right\},$$

即 K 中分母的素理想分解仅出现 S 的素理想的全体. 由命题 1.40可知它是戴德金整环, 记 $\mathcal{O}_{K,S}^\times$ 为其单

位群, 其中的元素被称为 S 单位 (S-unit); $\mathrm{Cl}_{K,S}$ 为其理想类群, 称之为 S 理想类群 (S-class group).

命题 1.41

我们有典范的正合列

$$1 \to \mathcal{O}_K^\times \to \mathcal{O}_{K,S}^\times \to \mathbb{Z}^{\#S} \to \mathrm{Cl}_K \to \mathrm{Cl}_{K,S} \to 1,$$

其中第三个箭头是

$$x \mapsto \big(v_\mathfrak{p}(x)\big)_{\mathfrak{p}\in S},$$

$v_\mathfrak{p}$ 为其素理想分解中 $\mathfrak{p}$ 的幂次; 第四个箭头是

$$(e_\mathfrak{p})_{\mathfrak{p}\in S} \mapsto \prod_{\mathfrak{p}\in S} \mathfrak{p}^{e_\mathfrak{p}}.$$

证明 容易知道, $\mathcal{O}_{K,S}^\times = \{x \in K \mid v_\mathfrak{p}(x) = 0, \forall \mathfrak{p} \notin S\}$. 如果 $x \in \mathcal{O}_{K,S}^\times$ 满足 $v_\mathfrak{p}(x) = 0, \forall \mathfrak{p} \in S$, 则 (x) 的素理想分解中所有幂次为零, 即 $x \in \mathcal{O}_K^\times$. 因此在 $\mathcal{O}_{K,S}^\times$ 处正合. 如果 $\prod_{\mathfrak{p}\in S}\mathfrak{p}^{e_\mathfrak{p}} = (x)$ 是主理想, 则 $x \in \mathcal{O}_{K,S}^\times$. 因此在 $\mathbb{Z}^{\#S}$ 处正合. 如果 $\mathcal{O}_K$ 的非零理想 $\mathfrak{a}$ 满足 $S^{-1}\mathfrak{a} = (a/s)$, 则 $v_\mathfrak{p}(\mathfrak{a}) \geq 0, \forall \mathfrak{a} \notin S$. 从而它是第三个箭头的像. 而对于 $\mathfrak{p} \in S$, $S^{-1}\mathfrak{p} = (1)$ 是主理想, 因此在 Cl_K 处正合. 容易验证第四个箭头是良定的. 由于 Cl_K 由所有素理想 $\mathfrak{p}$ 的理想类生成, $\mathrm{Cl}_{K,S}$ 由所有 $S^{-1}\mathfrak{p}$ 的理想类生成, 因此它是满射. $\square$

由此可知:

推论 1.42

我们有同构

$$\mathcal{O}_{K,S}^\times \cong \mu_K \times \mathbb{Z}^{\#S+r+s-1},$$

其中 r, s 分别为 K 的实素位和复素位的个数.

推论 1.43

S 理想类群 $\mathrm{Cl}_{K,S}$ 有限.

✍ **练习 1.3.13** 初步了解类群的岩泽理论.

§1.4 闵可夫斯基理论

我们将利用闵可夫斯基理论证明狄利克雷单位定理和类群有限定理.

§1.4.1 格

我们称一个群 (环、域) 为拓扑群 (环、域)，如果它有拓扑结构，且相应的运算是连续的.

例题 1.9 例如 $\mathbb{R}$ 在通常拓扑下形成拓扑域, 因为 $+, -, * : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$, $-x : \mathbb{R} \to \mathbb{R}$, $x^{-1} : \mathbb{R}^\times \to \mathbb{R}^\times$ 是连续的.

定义 1.44 (格)

设 V 是 n 维实向量空间. V 的一个子群

$$\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$$

被称为 V 的一个格, 其中 $v_1, \ldots, v_m$ 线性无关[a]. 如果 $m = n$, 称之为完全格. 称

$$\Phi = \{x_1v_1 + \cdots + x_nv_n \mid 0 \le x_i < 1, x_i \in \mathbb{R}\}$$

为它的一个基本区域.

[a]一般情形下, 设 F^+ 是拓扑域 F 的一个离散子群, 则我们可以类似定义 F^+ 格.

作为实向量空间, $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ 的维数为 m. 如果 Λ 是完全格, 则 $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = V$. 注意格与有限生成子群的差异, 例如 $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq \mathbb{C}$ 就不是一个格.

命题 1.45

V 的子群是一个格当且仅当它是离散的, 即对于任意 $\gamma \in \Lambda$, 存在开集 $U \ni \gamma$ 使得 $\Lambda \cap U = \{\gamma\}$.

证明 沿用之前的记号, 我们将 $v_1, \ldots, v_m$ 扩充为 V 的一组基 $v_1, \ldots, v_n$. 设 Φ_1 是 $\Lambda_1 = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ 关于这组基的基本区域, 则 $(\gamma + \Phi_1) \cap \Lambda = \{\gamma\}$. 因此 Λ 是离散的.

反之, 设 Λ 是一个离散子群. 我们来说明 Λ 是闭的. 设 U 是 0 的一个邻域使得 $\Lambda \cap U = \{0\}$. 由减法的连续性可知存在邻域 $U' \subset U$ 使得对任意 $x, y \in U', x - y \in U$. 若存在 $x \notin \Lambda$ 但 x 属于 Λ 的闭包中, 则 x 的任一邻域 $x + U'$ 中存在无穷多元素属于 Λ. 设 $\gamma_1 \neq \gamma_2 \in (x + U') \cap \Lambda$, 则 $\gamma_1 - \gamma_2 \in U \cap \Lambda = \{0\}$, 矛盾! 因此这样的 x 不存在, Λ 是闭的.

设 Λ 生成 m 维空间 $V_0 \subseteq V$, 则 V_0 存在一组由 Λ 中元素 $u_1, \ldots, u_m$ 构成的基. 设

$$\Lambda_0 = \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subseteq \Lambda,$$

它是 V_0 的一个完全格, Φ_0 为相应的基本区域. 对于 V 中任意元素 x, 存在 $\gamma \in \Lambda_0$ 使得 $x - \gamma \in \Phi_0$. 特别地, 我们可以选择陪集 Λ/Λ_0 的一组代表元, 它们均落在 Φ_0 中. 由于 Φ_0 的闭包是有界闭集, 它和闭集 Λ 的交既紧又离散, 从而只能是有限集, 即 Λ/Λ_0 有限.

设 $q = (\Lambda : \Lambda_0)$, 则 $\Lambda_0 \subseteq \Lambda \subseteq \frac{1}{q}\Lambda_0$. 由有限生成交换群的结构定理, Λ 是秩 m 的自由交换群, 从而存在 $v_1, \ldots, v_m$ 使得 $\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$. 而 $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = V_0$, 故 $v_1, \ldots, v_m$ 线性无关, 从而 Λ 是一个格. □

设 V 是一个欧式空间, 即 V 是一个有限维实向量空间, 其上有一个对称正定双线性型 (内积)

$$\langle\, , \rangle : V \times V \to \mathbb{R}.$$

此时 V 上有一个平移不变的测度 (哈尔测度[1]). 我们规定一组正交基 $\{e_1, \ldots, e_n\}$ 张成的平行多面体的体积为 1. 对于完全格 $\Lambda = \sum \mathbb{Z}v_i$, 有

$$\mathrm{covol}(\Lambda) := \mathrm{vol}(\Phi) = |\det A|,$$

其中 $(v_1, \ldots, v_n)^{\mathrm{T}} = A(e_1, \ldots, e_n)^{\mathrm{T}}$.

定义 1.46 (凸集)

设 X 是 V 的一个子集. 如果 $x \in X \implies -x \in X$, 称 X 是对称的. 如果 $x, y \in X \implies tx + (1-t)y \in X, \forall t \in [0,1]$, 称 X 是凸集.

[1]对于豪斯多夫局部紧群, 左 (右) 哈尔测度总是存在的. 交换群的情形下二者一致, 称为哈尔测度.

定理 1.47 (闵可夫斯基格点定理)

设 Λ 是欧式空间 V 的完全格, X 是 V 的一个对称凸子集. 如果 $\mathrm{vol}(X) > 2^n\mathrm{covol}(\Lambda)$, 则存在非零 $\gamma \in \Lambda$ 使得 $\gamma \in X$.

证明 我们只需证明存在不同的 $\gamma_1, \gamma_2 \in \Lambda$ 使得

$$\left(\frac{1}{2}X + \gamma_1\right) \cap \left(\frac{1}{2}X + \gamma_2\right) \neq \emptyset.$$

实际上, 设 $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$, 则 $\gamma = \gamma_1 - \gamma_2 = \frac{1}{2}(x_2 - x_1)$ 落在 $-x_1$ 和 x_2 构成的线段上, 因此 $\gamma \in \Lambda \cap X$.

如果所有的 $\frac{1}{2}X + \gamma$ 都两两不交, 则 $\Phi \cap (\frac{1}{2}X + \gamma)$ 也是如此, 因此

$$\mathrm{vol}(\Phi) \geq \sum_{\gamma\in\Lambda} \mathrm{vol}\big(\Phi \cap (\frac{1}{2}X + \gamma)\big) = \sum_{\gamma\in\Lambda} \mathrm{vol}\big((\Phi - \gamma) \cap \frac{1}{2}X\big).$$

由于 $\Phi - \gamma$ 覆盖整个空间, 因此右侧等于 $\mathrm{vol}(\frac{1}{2}X) = \frac{1}{2^n}\mathrm{vol}(X)$. 这和假设矛盾. □

§1.4.2 闵可夫斯基空间

$\mathbb{C}$ 上的复共轭诱导了 $K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C}$ 上的共轭作用 F, 则在同构

$$K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C} = \prod_{\tau\in\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})} \mathbb{C}$$

$$a \otimes z \mapsto \big(\tau(a)z\big)_\tau$$

下, $F\big((z_\tau)_\tau\big) = (\bar{z}_{\bar{\tau}})_\tau$. 显然

$$K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} = K_{\mathbb{C}}^{F=\mathrm{id}}.$$

$K_{\mathbb{C}}$ 有一个厄米特双线性型

$$\langle x, y\rangle = \sum_\tau x_\tau \bar{y}_\tau.$$

易知 $\langle Fx, Fy\rangle = \overline{\langle x, y\rangle}$. 对于 $x, y \in K_{\mathbb{R}}$, $\overline{\langle x, y\rangle} = \langle Fx, Fy\rangle = \langle x, y\rangle$, 因此 $\langle x, y\rangle \in \mathbb{R}$, $\langle x, y\rangle = \overline{\langle x, y\rangle} = \langle y, x\rangle$. 显然 $\langle x, x\rangle > 0, \forall x \neq 0$, 因此 $K_{\mathbb{R}}$ 上的 $\langle\, ,\rangle$ 是一个正定双线性型. 我们称欧式空间 $K_{\mathbb{R}}$ 为闵可夫斯基空间.

由定义容易看出

$$\begin{aligned} f : K_{\mathbb{R}} &\longrightarrow \prod_\tau \mathbb{R} = \mathbb{R}^n \\ (z_\tau)_\tau &\longmapsto (x_\tau)_\tau \end{aligned} \tag{1.1}$$

是一个同构, 其中对于实嵌入 $x_\rho = z_\rho$, 对于成对的复嵌入 $x_\sigma = \mathrm{Re}(z_\sigma), x_{\bar{\sigma}} = \mathrm{Im}\,(z_\sigma)$. 此同构诱导了右侧的内积

$$\langle x, y\rangle = \sum_\tau \alpha_\tau x_\tau y_\tau, \tag{1.2}$$

对于实嵌入, $\alpha_\tau = 1$; 对于复嵌入, $\alpha_\tau = 2$. 从而该测度是 $\mathbb{R}^n$ 上勒贝格测度的 2^s 倍.

我们有自然嵌入

$$j : K \hookrightarrow K_{\mathbb{R}} \hookrightarrow K_{\mathbb{C}}.$$

定义 $\mathrm{Tr} : K_{\mathbb{C}} \to \mathbb{C}$ 为其各分量之和, 则 $\mathrm{Tr}_{K/\mathbb{Q}} = \mathrm{Tr} \circ j$.

§1.4.3 类群有限性

对于 $\mathcal{O}_K$ 的非零理想 $\mathfrak{a}$, 定义

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

定理 1.48

如果 $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ 为素理想分解, 则

$$\mathbf{N}\mathfrak{a} = (\mathbf{N}\mathfrak{p}_1)^{e_1} \cdots (\mathbf{N}\mathfrak{p}_r)^{e_r}.$$

证明 由中国剩余定理

$$\mathcal{O}_K/\mathfrak{a} = \bigoplus_{i=1}^{r} \mathcal{O}_K/\mathfrak{p}_i^{e_i}.$$

因此我们只需要证明 $\mathfrak{a} = \mathfrak{p}^e$ 的情形. 由唯一分解定理, $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$. 设 $a \in \mathfrak{p}^i \backslash \mathfrak{p}^{i+1}$, 则 $\mathfrak{p}^i \supseteq (a) + \mathfrak{p}^{i+1} \supsetneq \mathfrak{p}^{i+1}$, 因此 $\mathfrak{p}^i = (a) + \mathfrak{p}^{i+1}$, $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ 作为 $\mathcal{O}_K/\mathfrak{p}$ 向量空间由 $a \bmod \mathfrak{p}^{i+1}$ 生成, 因此它是一维的,

$$\mathbf{N}\mathfrak{p}^e = (\mathcal{O}_K : \mathfrak{p}^e) = \prod_{i=0}^{e-1} (\mathfrak{p}^i : \mathfrak{p}^{i+1}) = (\mathbf{N}\mathfrak{p})^e.$$

□

因此 $\mathbf{N}$ 满足可乘性 $\mathbf{N}(\mathfrak{a}\mathfrak{b}) = \mathbf{N}\mathfrak{a} \cdot \mathbf{N}\mathfrak{b}$, 故 $\mathbf{N} : \mathcal{I}_K \to \mathbb{R}_+^\times$ 是一个群同态.

命题 1.49

设 $\mathfrak{a} \subseteq \mathfrak{b}$ 为非零理想, 则 $\Delta_\mathfrak{a} = [\mathfrak{b} : \mathfrak{a}]^2 \Delta_\mathfrak{b}$. 特别地, $\Delta_\mathfrak{a} = \mathbf{N}\mathfrak{a}^2 \Delta_K$.

证明 我们只需证明 $[\mathfrak{b} : \mathfrak{a}]$ 等于相应的整基的线性变化的行列式的绝对值, 这可以通过 $\mathbb{Z}$ 上矩阵进行初等变换来证明. □

命题 1.50

设 $\mathfrak{a} \subseteq \mathcal{O}_K$ 是非零理想. 则 $j\mathfrak{a}$ 是 $K_\mathbb{R}$ 的一个完全格, 且

$$\operatorname{covol}(j\mathfrak{a}) = \sqrt{|\Delta_K|}\mathbf{N}\mathfrak{a}.$$

证明 设 $\alpha_1, \ldots, \alpha_n$ 是 $\mathfrak{a}$ 的一组基, $\operatorname{Hom}_\mathbb{Q}(K, \mathbb{C}) = \{\tau_1, \ldots, \tau_n\}$. 设 $A = (\tau_i \alpha_k)_{ik}$, 则

$$\Delta_\mathfrak{a} = (\det A)^2 = (\mathbf{N}\mathfrak{a})^2 \Delta_K.$$

另一方面,

$$(\langle j\alpha_i, j\alpha_k \rangle)_{ik} = \Big(\sum_{l=1}^{n} \tau_l \alpha_i \overline{\tau}_l \alpha_k\Big)_{ik} = A^\mathrm{T} \overline{A}.$$

因此

$$\operatorname{covol}(\Lambda) = |\det(\langle j\alpha_i, j\alpha_k \rangle)_{ik}|^{\frac{1}{2}} = |\det A| = \sqrt{|\Delta_K|}\mathbf{N}\mathfrak{a}.$$

□

设 r, s 分别为 K 的实素位和复素位的个数.

定理 1.51

设 $\mathfrak{a}\subseteq\mathcal{O}_K$ 是非零理想, $\{c_\tau\}_{\tau\in\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})}$ 为一组正实数, 满足 $c_\tau=c_{\overline{\tau}}$. 如果

$$\prod_\tau c_\tau>\left(\frac{2}{\pi}\right)^s\sqrt{|\Delta_K|}\mathbf{N}\mathfrak{a},$$

则存在非零元 $a\in\mathfrak{a}$ 使得

$$|\tau a|<c_\tau,\quad\forall\tau\in\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C}).$$

证明 集合 $X=\{(z_\tau)\in K_{\mathbb{R}}:|z_\tau|<c_\tau\}$ 是一个对称凸集. 通过映射 (1.1), 它的像为

$$f(X)=\left\{(x_\tau)\in\prod_\tau\mathbb{R}:|x_\rho|<c_\rho,|x_\sigma^2+x_{\overline{\sigma}}^2|<c_\sigma^2\right\}.$$

因此它的体积

$$\begin{aligned}\mathrm{vol}(X)&=2^s\mathrm{vol}_{\text{勒贝格}}\big(f(X)\big)=2^s\prod_\rho(2c_\rho)\prod_\sigma(\pi c_\sigma^2)=2^{r+s}\pi^s\prod_\tau c_\tau\\&>2^{r+s}\pi^s\left(\frac{2}{\pi}\right)^s\sqrt{|\Delta_K|}\mathbf{N}\mathfrak{a}=2^n\mathrm{covol}(j\mathfrak{a}),\end{aligned}$$

由闵可夫斯基格点定理 1.47 知存在非零元 $a\in\mathfrak{a}$, $ja\in X$. □

命题 1.52

对 $\mathcal{O}_K$ 的任一非零理想 $\mathfrak{a}$, 存在非零元 $a\in\mathfrak{a}$ 使得 $|\mathbf{N}_{K/\mathbb{Q}}(a)|\le M_K\mathbf{N}\mathfrak{a}$, 其中

$$M_K=\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|\Delta_K|}$$

被称为 K 的闵可夫斯基界.

证明 设 X 为上述练习中的对称凸集. 当

$$\mathrm{vol}(X)=2^r\pi^s\frac{t^n}{n!}=2^n\sqrt{|\Delta_K|}\mathbf{N}\mathfrak{a}+\epsilon,\quad\epsilon>0,$$

时, 由闵可夫斯基格点定理 1.47 知存在非零元 $a\in\mathfrak{a}$, $ja\in X$. 于是

$$|\mathbf{N}_{K/\mathbb{Q}}(a)|=\prod|\tau a|\le\left(\frac{\sum|\tau a|}{n}\right)^n\le\left(\frac{t}{n}\right)^n=M_K\mathbf{N}\mathfrak{a}+c\epsilon,$$

其中 $c=\frac{n!}{n^n2^r\pi^s}$. 我们取 ϵ 充分小, 使得 $M_K\mathbf{N}\mathfrak{a}$ 和 $M_K\mathbf{N}\mathfrak{a}+c\epsilon$ 向下取整相同. 由 $\mathbf{N}_{K/\mathbb{Q}}(a)$ 是整数可知 $|\mathbf{N}_{K/\mathbb{Q}}(a)|\le M_K\mathbf{N}\mathfrak{a}$, 命题得证. □

注 实际上习题 1.4.6 中的界对于证明类群有限也是足够的, 但是闵可夫斯基界在很多情况下是一个更好的界, 这对于计算具体的类群是有必要的.

定理 1.53

数域的类群是有限的.

证明 如果 $\mathfrak{p}$ 是非零素理想, 则 $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$, $\mathcal{O}_K/\mathfrak{p}$ 是 $\mathbb{F}_p$ 的有限扩张. 设扩张次数为 f, 则 $\mathbf{N}\mathfrak{p}=p^f$. 任给素数 p, $p\mathcal{O}_K$ 的素理想分解只有有限多个, 因此只有有限多 $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$. 于是 $\mathbf{N}$ 有界的素理想只有有限多个. 根据 $\mathbf{N}$ 的可乘性, 满足 $\mathbf{N}\mathfrak{a}\le M$ 的理想 $\mathfrak{a}$ 也只有有限多个.

我们断言任意理想类 $[\mathfrak{a}]$ 都存在一个代表元 $\mathfrak{a}_1$ 使得 $\mathbf{N}\mathfrak{a}_1\le M_K$. 通过乘以适当的 $\gamma\in\mathcal{O}_K$, 我们可不妨设 $\mathfrak{a}^{-1}\subseteq\mathcal{O}_K$. 由命题 1.52 知存在非零 $a\in\mathfrak{a}^{-1}$ 使得 $|\mathbf{N}_{K/\mathbb{Q}}(a)|\le M_K\mathbf{N}\mathfrak{a}^{-1}$. 于是 $\mathbf{N}(a\mathfrak{a})\le M_K$ 且

$a\mathfrak{a} \subseteq \mathcal{O}_K, a\mathfrak{a} \in [\mathfrak{a}]$. □

例题 1.10 令 $K = \mathbb{Q}(\sqrt{-14})$, 则 $n = 2, s = 1, \Delta_K = -56$,

$$M_K = \frac{4}{\pi}\sqrt{14} \approx 4.765 < 5.$$

因此 K 的每个理想类都包含一个范数不超过 4 的理想. 注意到 $(2) = \mathfrak{p}_2^2, \mathfrak{p}_2 = (2, \sqrt{-14}), \mathbf{N}\mathfrak{p}_2 = 2$. 易知 $\mathfrak{p}$ 不是主理想, 因此它的阶为 2. 设 $\mathfrak{p}_3 = (3, 1+\sqrt{-14})$, 则 $(3) = \mathfrak{p}_3\overline{\mathfrak{p}}_3$. 注意到 $\mathfrak{p}_3^2 = (9, -2+\sqrt{-14}) = (\frac{-2+\sqrt{-14}}{2})\mathfrak{p}_2$. 范数为 4 的只有 (2), 因此 $\mathrm{Cl}_K = \langle[\mathfrak{p}_3]\rangle \cong \mathbb{Z}/4\mathbb{Z}$.

例题 1.11 令 $K = \mathbb{Q}(\sqrt[3]{2})$, 则 $n = 3, s = 1, \Delta_K = -2^2 3^3$,

$$M_K = \left(\frac{4}{\pi}\right)\frac{3!}{3^3}\sqrt{3^3 2^2} \approx 2.94 < 3.$$

而范数为 2 的理想只有 $(\sqrt[3]{2})$, 因此 $\mathcal{O}_K$ 是主理想整环.

§1.4.4 狄利克雷单位定理

为了证明狄利克雷单位定理, 我们需要乘法版本的闵可夫斯基理论. 记 $K_{\mathbb{C}}$ 中每个分量非零的元素全体为 $K_{\mathbb{C}}^\times$. 我们知道 $j\mathcal{O}_K \subseteq K_{\mathbb{R}} \subseteq K_{\mathbb{C}}$ 是一个格, 因此 $j\mathcal{O}_K^\times$ 在 $K_{\mathbb{C}}^\times$ 中是离散的. 想要将 $\mathcal{O}_K^\times$ 映射为一个格, 我们可以考虑映射

$$\begin{aligned} \ell : K_{\mathbb{C}}^\times &\longrightarrow \prod_\tau \mathbb{R} \\ (z_\tau)_\tau &\longmapsto (\log|z_\tau|)_\tau \end{aligned}.$$

于是我们有交换图表

$$\begin{tikzcd} K^\times \arrow[r, "j"] \arrow[d, "\mathbf{N}_{K/\mathbb{Q}}"'] & K_{\mathbb{C}}^\times \arrow[r, "\ell"] \arrow[d, "\mathbf{N}"] & \prod_\tau \mathbb{R} \arrow[d, "\mathrm{Tr}"] \\ \mathbb{Q}^\times \arrow[r] & \mathbb{C}^\times \arrow[r, "\log|\cdot|"] & \mathbb{R}, \end{tikzcd}$$

其中 $\mathbf{N} : K_{\mathbb{C}}^\times \to \mathbb{C}^\times$ 为其各个分量的乘积. 考虑 F 在这个交换图表上的作用不动的部分, 以及其限制在 $\mathcal{O}_K^\times$ 下的映射.

$$\begin{tikzcd} \mathcal{O}_K^\times \arrow[r, "j"'] \arrow[rr, bend left, "\lambda"] \arrow[d, hook] & S \arrow[r, "\ell"'] \arrow[d, hook] & H \arrow[d, hook] \\ K^\times \arrow[r, "j"] \arrow[d, "\mathbf{N}_{K/\mathbb{Q}}"'] & K_{\mathbb{R}}^\times \arrow[r, "\ell"] \arrow[d, "\mathbf{N}"] & [\prod_\tau \mathbb{R}]^+ \arrow[d, "\mathrm{Tr}"] \\ \mathbb{Q}^\times \arrow[r] & \mathbb{R}^\times \arrow[r, "\log|\cdot|"] & \mathbb{R}, \end{tikzcd}$$

其中

$$[\prod_\tau \mathbb{R}]^+ = \{(x_\tau) \mid x_\tau = x_{\overline{\tau}}\},$$

$$S = \left\{y \in K_{\mathbb{R}}^\times \mid \mathbf{N}(y) = \pm 1\right\}$$

是 $K_{\mathbb{R}}^\times$ 的一个超曲面 (余维数为 1),

$$H = \left\{x \in [\prod_\tau \mathbb{R}]^+ \mid \mathrm{Tr}(x) = 0\right\}$$

是 $[\prod_\tau \mathbb{R}]^+$ 的一个超平面.

我们固定

$$f : [\prod_\tau \mathbb{R}]^+ \xrightarrow{\sim} \mathbb{R}^{r+s}$$

$$(x_\rho, x_\sigma, x_{\overline{\sigma}}) \mapsto (x_\rho, 2x_\sigma).$$

则 Tr 变为通常的迹, ℓ 变为 $\ell(x) = (\log|x_\rho|, \log|x_\sigma|^2)$.

命题 1.54
$\ker\lambda = \mu_K$.

证明 显然 $\mu_K \subseteq \operatorname{Ker}\lambda$. 若 $\varepsilon \in \operatorname{Ker}\lambda$, 则 $|\tau\varepsilon| = 1$, 故 $j\varepsilon$ 落在 $K_\mathbb{R}$ 的一个有界区域内. 而 $j\mathcal{O}_K$ 是一个格, 因此 $\ker\lambda$ 有限, 这迫使 $\ker\lambda = \mu(K)$. □

定理 1.55
$\Lambda = \lambda(\mathcal{O}_K^\times)$ 是 H 的一个完全格.

证明 我们首先证明 Λ 是一个格. 对于任意 $c > 0$, 我们断言

$$\left\{(x_\tau) \in \prod_\tau \mathbb{R} : |x_\tau| \leq c\right\}$$

只包含有限多个 Λ 中的元素. 该区域在 ℓ 下的原像为

$$\left\{(z_\tau) \in \prod_\tau \mathbb{C}^\times : e^{-c} \leq |z_\tau| \leq e^c\right\}.$$

由于 $j\mathcal{O}_K^\times \subset j\mathcal{O}_K$ 是一个格的子集, 因此该区域只包含有限多 $j\mathcal{O}_K^\times$ 中的元素, 从而 Λ 是离散的, 因此它是一个格.

我们将构造一个有界集 $T \subseteq S$ 使得所有 $Tj\varepsilon, \varepsilon \in \mathcal{O}_K^\times$ 覆盖整个 S. 于是 $M = \ell(T) \subseteq H$ 中元素的每个分量都是上有界的, 而 H 中元素各分量之和为 0, 因此它们也是下有界的, 即 M 有界, 由此可得 $\Lambda \subseteq H$ 是完全格. 设 $c_\tau > 0$ 满足 $c_\tau = c_{\overline{\tau}}$, 且

$$C = \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

设 $X = \{(z_\tau) \in K_\mathbb{R} : |z_\tau| < c_\tau\}$, 则对于 $y \in S$,

$$Xy^{-1} = \left\{(z_\tau) \in K_\mathbb{R} : |z_\tau| < c_\tau|y_\tau|^{-1}\right\}.$$

由定理 1.51 知存在 $0 \neq a \in \mathcal{O}_K$ 使得

$$|\mathbf{N}_{K/\mathbb{Q}}(a)| \leq C, ja \in Xy^{-1}, y \in X(ja)^{-1}.$$

我们知道范数有限的理想只有有限多个, 因此可以选取 $\alpha_1, \ldots, \alpha_N \in \mathcal{O}_K$ 使得任意满足 $|\mathbf{N}_{K/\mathbb{Q}}(\alpha)| \leq C$ 的元素 $\alpha \in \alpha_i\mathcal{O}_K^\times$. 于是

$$T = S \cap \bigcup_{i=1}^N X(j\alpha_i)^{-1}$$

是一个有界集, 且 $S = \bigcup_{\varepsilon \in \mathcal{O}_K^\times} Tj\varepsilon$. □

因此我们得到

定理 1.56 (狄利克雷单位定理)

$\mathcal{O}_K^\times$ 为有限生成交换群, 秩为 $r+s-1$, 即

$$\mathcal{O}_K^\times \cong \mu_K \times \mathbb{Z}^{r+s-1}.$$

令 $t=r+s-1$. 设 $\varepsilon_1,\dots,\varepsilon_t$ 是 $\mathcal{O}_K^\times$ 自由部分的一组生成元. 令

$$y=\frac{1}{\sqrt{r+s}}(1,\dots,1)\in\mathbb{R}^{r+s},$$

则它和 H 正交, 因此 $\lambda(\mathcal{O}_K^\times)$ 的体积等于

$$\pm\det\begin{pmatrix} y_1 & \lambda_1(\varepsilon_1) & \dots & \lambda_1(\varepsilon_t) \\ \vdots & \vdots & & \vdots \\ y_{r+s} & \lambda_{r+s}(\varepsilon_1) & \dots & \lambda_{r+s}(\varepsilon_t) \end{pmatrix}.$$

将所有行加到任意一行, 我们得到 $(\sqrt{r+s},0,\dots,0)$, 因此我们有:

命题 1.57

$\operatorname{covol}\big(\lambda(\mathcal{O}_K^\times)\big)=\sqrt{r+s}R$, 其中 R 是矩阵

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \dots & \lambda_1(\varepsilon_t) \\ \vdots & & \vdots \\ \lambda_{r+s}(\varepsilon_1) & \dots & \lambda_{r+s}(\varepsilon_t) \end{pmatrix}$$

的任一 $r+s-1$ 阶主子式的行列式的绝对值. 我们称 R 为 K 的调整子.

例题 1.12 设 $K=\mathbb{Q}(\sqrt[3]{2})$, 则

$$\mathcal{O}_K^\times=\left\{\pm(1-\sqrt[3]{2})^n \mid n\in\mathbb{Z}\right\}\cong\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}.$$

✍ **练习 1.4.1** 证明 $\operatorname{covol}(\Lambda)=\sqrt{|\det\left(\langle v_i,v_j\rangle\right)_{i,j}|}$ 且不依赖于基的选取.

✍ **练习 1.4.2** 设 Λ 是欧式空间 V 的完全格, 存在一个对称凸集 X 使得 $\operatorname{vol}(X)=2^n\operatorname{covol}(\Lambda)$, 且 $\Lambda\cap X=\{0\}$.

✍ **练习 1.4.3** 证明在等式(1.2)中, 对于实嵌入, $\alpha_\tau=1$; 对于复嵌入, $\alpha_\tau=2$.

✍ **练习 1.4.4** $\mathbf{N}\big((a)\big)=|\mathbf{N}_{K/\mathbb{Q}}(a)|,\forall a\in K^\times$.

✍ **练习 1.4.5** 证明 $\mathfrak{a}$ 所有元素的范数生成的 $\mathbb{Z}$ 的理想为 $\mathbf{N}\mathfrak{a}\mathbb{Z}$.

✍ **练习 1.4.6** 证明对 $\mathcal{O}_K$ 的任一非零理想 $\mathfrak{a}$, 存在非零元 $a\in\mathfrak{a}$ 使得

$$|\mathbf{N}_{K/\mathbb{Q}}(a)|\le\left(\frac{2}{\pi}\right)^s\sqrt{|\Delta_K|}\mathbf{N}\mathfrak{a}.$$

✍ **练习 1.4.7** 证明对称凸集

$$X=\left\{(z_\tau)\in K_\mathbb{R}\mid\sum_\tau|z_\tau|<t\right\}$$

的体积为 $\operatorname{vol}(X)=2^r\pi^s\frac{t^n}{n!}$.

✍ **练习 1.4.8** 计算 $K=\mathbb{Q}(\sqrt{d}),d=-1,-2,-3,-5,-7,2,3,5$ 的类数.

✍ **练习 1.4.9** 证明 $K\neq\mathbb{Q}$ 时, $|\Delta_K|\neq 1$.

✍ **练习 1.4.10** 证明当数域 K 的次数趋于无穷时, $|\Delta_K|$ 趋于无穷.

✍ **练习 1.4.11** 在相差一个单位的前提下, $\mathbf{N}_{K/\mathbb{Q}}(\alpha)=a$ 的 α 只有有限多个.

练习 1.4.12 虚二次域的单位群是什么?

练习 1.4.13 证明 $x^3+3y^3+9z^3-9xyz=1$ 有无穷多整数解.

§1.5 二元二次型

本节中, 我们将讨论二元二次型和类群之间的联系.

§1.5.1 等价类

定义 1.58 (二次型)

形如 $F(x,y)=ax^2+bxy+cy^2, a,b,c\in\mathbb{Z}$ 的多项式被称为 (整)二元二次型. 如果 $(a,b,c)=1$, 我们称 F 是本原的. F 的判别式是指 $D=b^2-4ac$.

容易看出, F 可以分解为两个有理系数的一次因式的乘积当且仅当 D 是个平方数. 我们总是假设 d 不是平方数.

定义 1.59

(1) 如果对于非零 (x,y), 总有 $F(x,y)>0$, 我们称 F 是正定的. 这等价于 $D<0, a>0$.

(2) 如果对于非零 (x,y), 总有 $F(x,y)<0$, 我们称 F 是负定的. 这等价于 $D<0, a<0$.

(3) 如果 F 既能取到正值也能取到负值, 我们称 F 是不定的. 这等价于 $D>0$.

对于 $\gamma=\left(\begin{smallmatrix} r & s\\ u & v\end{smallmatrix}\right)\in \mathrm{SL}_2(\mathbb{Z})$, 定义

$$G(x,y)=F(rx+sy,ux+vy).$$

我们称 F 和 G 是等价的.

我们记 $Q=\begin{pmatrix} a & b/2\\ b/2 & c\end{pmatrix}$ 为 F 的关联矩阵. 则 G 和 F 等价当且仅当存在 $\gamma\in\mathrm{SL}_2(\mathbb{Z})$ 使得 G 的关联矩阵为 $\gamma^{\mathrm{T}}Q\gamma$. 不难证明, 等价的二元二次型具有相同的判别式, 且 $F(x,y)=n$ 的解的数量和 $G(x,y)=n$ 的解的数量相同.

我们所感兴趣的是所有二元二次型的等价类.

引理 1.60

任一二元二次型可等价于 $ax^2+bxy+cy^2$, 其中 $|b|\le|a|\le|c|$.

证明 设 a 是集合 $\{F(x,y):x,y\in\mathbb{Z}\}$ 中绝对值最小的非零元. 设 $a=F(r,s), q=(r,s)$. 则

$$F\left(\frac{r}{q},\frac{s}{q}\right)=\frac{a}{q^2},$$

因此 q 只能是 1, r 与 s 互素. 于是存在 $u,v\in\mathbb{Z}$ 使得 $rv-us=1$. 记

$$F(rx+uy,sx+vy)=ax^2+b'xy+c'y^2.$$

注意到

$$a(x+hy)^2+b'(x+hy)y+c'y^2=ax^2+(b'+2ah)xy+(ah^2+b'h+c')y^2,$$

我们可以取 h 使得 $|b'+2ah|\le|a|$. 令 $b=b'+2ah, c=ah^2+b'h+c'$, 则 $c=G(0,1)$, 其中 $G(x,y)=ax^2+bxy+cy^2$ 是和 F 等价的二次型. 由 $|a|$ 的极小性可知 $|c|\ge|a|$. □

定理 1.61 (二元二次型等价类个数有限)

固定一个无平方因子的整数 D, 则只有有限多个二元二次型的等价类, 其判别式为 D.

证明 我们假设每个等价类中已选出如上述引理所描述的二元二次型. 如果 $D>0$, 则 $|ac|\geq b^2=D+4ac\geq 4ac$, 于是 $ac<0$, $4|ac|\leq D$, 从而 $|a|\leq \sqrt{D}/2$. 如果 $D<0$, 则 $|D|=4ac-b^2\geq 4a^2-a^2=3a^2$, $|a|\leq\sqrt{|D|/3}$. 无论哪种情形, a 只有有限多种可能. 于是 $|b|\leq |a|$ 也只有有限多种可能. 而 $c=(b^2-d)/4a$, 因此命题得证. □

定理 1.62

每一个正定的二元二次型等价类有如下形式的唯一代表元: $ax^2+bxy+cy^2$, $|b|\leq a\leq c$, 且若 $|b|=a$ 或 $a=c$, 有 $b\geq 0$.

注 这样的形式被称为既约的.

证明 上述定理告诉我们可不妨设 $|b|\leq a\leq c$. 若 $|b|=a$ 且 $b<0$, 我们有

$$F(x+y,y)=ax^2+axy+cy^2;$$

若 $a=c$ 且 $b<0$, 我们有

$$F(-y,y)=ax^2-bxy+ay^2.$$

因此每个题述的等价类均有这样的代表元.

我们来说明这些两两不等价. 设 $F(x,y)=ax^2+bxy+cy^2$ 既约, 则对任意 $x,y\in\mathbb{Z}$, 我们有

$$F(x,y)\geq (a+c-|b|)\min\left\{x^2,y^2\right\}.$$

实际上, 不妨设 $|x|\geq|y|$, 则

$$F(x,y)\geq (a-|b|)|xy|+cy^2\geq (a+c-|b|)y^2.$$

特别地, $xy\neq 0$ 时 $F(x,y)\geq a+c-|b|$, 且等号仅在 $(x,y)=\pm\big(1,-\mathrm{sgn}(b)\big)$ 时成立. 于是 F 可表达的非零整数中最小的三个为

$$a\leq c\leq a+c-|b|.$$

设 $G(x,y)$ 是和 $F(x,y)$ 等价的既约二元二次型, 则 $G(x,y)=ax^2+b'xy+c'y^2$.

- 如果 $a=c=b\geq 0$, 则 $-D=4ac'-b'^2\geq 4a^2-a^2=-D$, 从而 $c'=a=|b'|$. 而 G 是既约的, 从而 $b'=a$.
- 如果 $a=c>b\geq 0$, 则 $c'=a$ 或 $c'=2a-b$. 若 $c'=2a-b$, 则 $F(x,y)=a$ 有四个解, 而 $G(x,y)=a$ 只有两个解, 这不可能. 因此 $c'=a=c$, 从而 $b'=b$.
- 如果 $c>a=|b|$, 则 $a<c=a+c-|b|$, 从而 $c'=a$ 或 c. 而 $c'=a$ 时划归到前述两种情形, 这不可能, 因此 $c'=c$, $b'=b$.
- 如果 $c>a>|b|$, 则 $c'>a>|b'|$, 否则 G 化归到划归到前述两种情形, 这不可能. 从而 $a<c<a+c-|b|, a<c'<a+c'-|b'|$. 由此可知 $c'=c, |b'|=|b|$.

所以我们只需说明最后一种情形下, $b\neq 0$ 时 $F(x,y)=ax^2+bxy+cy^2$ 和 $G(x,y)=ax^2-bxy+cy^2$ 不等价. 假设存在 $\gamma\in\mathrm{SL}_2(\mathbb{Z})$ 使得

$$\gamma^{\mathrm{T}}\begin{pmatrix} a & -b/2\\ -b/2 & c\end{pmatrix}\gamma=\begin{pmatrix} a & b/2\\ b/2 & c\end{pmatrix},$$

则 $F(x,y)=G(x',y')=n$ 当且仅当 $(x,y)=(x',y')\gamma^{\mathrm{T}}$. 由 $n=a$ 时解为 $(\pm1,0)$ 和 $n=c$ 时解为 $(0,\pm1)$ 可知 $\gamma=\pm I_2$ 或 $\pm\left(\begin{smallmatrix} & 1\\ -1 & \end{smallmatrix}\right)$. 但 $\det\gamma=1$, 从而 $\gamma=\pm I_2$, $F=G$, 矛盾! □

例题 1.13 列出 $-D\le 12$ 的所有正定既约二元二次型.

§1.5.2 表整数

定义 1.63

如果 $F(x,y)=n$ 有整数解, 我们称 n 可以被 $F(x,y)$ 表出. 如果有 $(x,y)=1$ 的解, 我们称 n 被 $F(x,y)$ 真表出.

引理 1.64

整数 n 可被 $F(x,y)$ 真表出当且仅当 $F(x,y)$ 与某个 $nx^2+bxy+cy^2$ 等价.

证明 充分性显然. 若 $F(u,v)=n,(u,v)=1$, 则存在 $r,s\in\mathbb{Z}$ 使得 $us-rv=1$, 从而 $F(x,y)$ 等价于 $F(ux+ry,vx+sy)$, 且后者 x^2 项系数为 $F(u,v)=n$. □

命题 1.65

设 $n\ne0$ 和 D 是整数.

(1) 存在判别式为 D 的二元二次型真表出 n 当且仅当 D 模 $4n$ 是个平方.

(2) 存在判别式为 D 的二元二次型表出 n 当且仅当 n 中幂次为奇数的素因子 p 需要满足 $\left(\frac{D}{p}\right)=1$ (其中 $\left(\frac{D}{2}\right)=1$ 是指 $D\equiv\pm1 \bmod 8$).

证明 (1) 若 F 真表出 n, 则 F 等价于 $nx^2+bxy+cy^2$, 从而判别式 $D=b^2-4nc$ 是模 $4n$ 的平方. 反之, 存在 b 使得 $D\equiv b^2 \bmod 4n$, 令 $c=(b^2-D)/4n$, 则 $nx^2+bxy+cy^2$ 是判别式为 D 且真表出 n 的二元二次型.

(2) 这等价于存在 n' 被 F 真表出且 n/n' 是平方数. 如果 p 在 n 中的幂次是奇数, 则 $p\mid n'$, 从而 D 模 p 是平方. 反之, 若 n 中每个幂次为奇数的素因子 p 都满足 $\left(\frac{D}{p}\right)=1$, 则所有这样不同的 p 的乘积 n' 满足 D 是模 $4n'$ 的平方. 如果 n' 是奇数, 由 $D\equiv0,1 \bmod 4$ 知 D 模 $4n'$ 是平方; 如果 n' 是偶数, 由 $\left(\frac{D}{2}\right)=1$ 知 $D\equiv1 \bmod 8$, 从而 D 模 $4n'$ 也是平方. 因此 n' 被 F 真表出, 从而 n 被 F 表出. □

例题 1.14 设 $D=-8$, 则对应的正定既约二元二次型只有 x^2+2y^2. 由于 $\left(\frac{-2}{p}\right)=-1\iff p\equiv 5,7 \bmod 8$, 因此正整数 n 可被 x^2+2y^2 表出当且仅当 $p\equiv5,7 \bmod 8$ 在 n 中的幂次为偶数.

例题 1.15 正整数 n 被 x^2+5y^2 表出当且仅当

(1) 素数 $p\equiv 11,13,17,19 \bmod 20$ 在 n 中的幂次为偶数;

(2) 素数 $p\equiv 2,3,7 \bmod 20$ 在 n 中的幂次之和为偶数.

注意到判别式为 -20 的正定二元二次型只有

$$f(x,y)=x^2+5y^2,\quad g(x,y)=2x^2+2xy+3y^2.$$

由上述命题可知与 -20 互素的素数 p 可被 f 或 g 表出当且仅当 $\left(\frac{-5}{p}\right)=1$. 由二次互反律, 我们有

$$\left(\frac{-5}{p}\right)=\begin{cases}1, & p\equiv 1,3,7,9 \bmod 20\\ -1, & p\equiv 11,13,17,19 \bmod 20.\end{cases}$$

容易看出 $f(x,y)\not\equiv -1 \bmod 4$, $g(x,y)\not\equiv 1 \bmod 4$, 从而 $p\equiv 1,9 \bmod 20$ 只能被 f 表出, $p\equiv 3,7 \bmod 20$

只能被 g 表出. 此外, 2 只能被 g 表出, 5 只能被 f 表出. 故 $p\equiv 1,5,9 \bmod 20$ 在 n 中的幂次任意. 最后, (2) 由下面这个神奇的等式得到:

$$(2x^2+2xy+3y^2)(2x^2+2xw+3w^2)=(2xz+xy+yz+3yw)^2+5(xw-yz)^2.$$

这个等式是如何得到的呢? 设 $\mathfrak{p}=(2,1+\sqrt{-5})\subseteq K=\mathbb{Q}(\sqrt{-5})$, 则 $\mathfrak{p}^2=(2)$. 我们有

$$2x^2+2xy+3y^2=\frac{\mathbf{N}_{K/\mathbb{Q}}(2x+(1\pm\sqrt{-5})y)}{\mathbf{N}\mathfrak{p}}.$$

我们对

$$(2x+(1\pm\sqrt{-5})y)(2z+(1\pm\sqrt{-5})w)=2\big((2xz+xy+yz+3yz)+(xw-yz)\sqrt{-5}\big)$$

两边取范数便得到了上述等式.

§1.5.3 与理想类群的联系

定义 1.66

设 $x\in K$. 如果对于所有实嵌入 $\sigma:K\hookrightarrow\mathbb{R}$, 有 $\sigma(x)>0$, 我们称 x 是全正的. 当 K 是全虚域时该条件总成立.

记 $\mathcal{P}_K^+\subseteq\mathcal{I}_K$ 为由全正元生成的主分式理想全体. 定义 K 的缩理想类群为

$$\mathrm{Cl}_K^+:=\mathcal{I}_K/\mathcal{P}_K^+.$$

对于全虚域, 该定义与理想类群并无差异.

设 $K=\mathbb{Q}(\sqrt{D})$ 是判别式为 D 的二次域, 记 $x\mapsto\bar{x}$ 为 $G(K/\mathbb{Q})$ 中非平凡元. 如果 $D<0$, 我们有 $\mathrm{Cl}_K^+=\mathrm{Cl}_K$; 如果 $D>0$, 我们有正合列[1]

$$1\to\mathcal{P}_K/\mathcal{P}_K^+\to\mathrm{Cl}_K^+\to\mathrm{Cl}_K\to 1.$$

定义 1.67

设 α_1,α_2 为 K 中两个 $\mathbb{Q}$ 线性无关的元素. 如果

$$\frac{\det\begin{pmatrix}\alpha_1&\alpha_2\\\bar{\alpha}_1&\bar{\alpha}_2\end{pmatrix}}{\sqrt{D}}>0,$$

我们称 (α_1,α_2) 是正向的.

显然 (α_1,α_2) 和 (α_2,α_1) 中有且仅有一个是正向的.

对于 K 的分式理想 $\mathfrak{a}$, 设 (ω_1,ω_2) 为其一组正向的 $\mathbb{Z}$ 基. 记

$$f_{\omega_1,\omega_2}(x,y)=\frac{\mathbf{N}_{K/\mathbb{Q}}(x\omega_1+y\omega_2)}{\mathbf{N}\mathfrak{a}}.$$

引理 1.68

二次型 f_{ω_1,ω_2} 是整系数的, 其判别式为 D, 且 K 是虚二次域时是正定的. 更进一步, f_{ω_1,ω_2} 的等价类只依赖于 $[\mathfrak{a}]\in\mathrm{Cl}_K^+$.

证明 对于正整数 x,y, 我们有 $f_{\omega_1,\omega_2}(x,y)\in\mathbb{Z}$. 由于它的 x^2,y^2,xy 系数分别为

$$f_{\omega_1,\omega_2}(1,0),\ f_{\omega_1,\omega_2}(0,1),\ f_{\omega_1,\omega_2}(1,1)-f_{\omega_1,\omega_2}(1,0)-f_{\omega_1,\omega_2}(0,1),$$

[1] 如果 K 有范数为 -1 的单位, 则 $\mathcal{P}_K=\mathcal{P}_K^+$; 否则它的大小为 2.

因此 f_{ω_1,ω_2} 是整系数的. 通过计算可知它的判别式为

$$\frac{(\omega_1\bar{\omega}_2-\bar{\omega}_1\omega_2)^2}{\mathbf{N}\mathfrak{a}^2}=\frac{\Delta_{\mathfrak{a}}}{\mathbf{N}\mathfrak{a}^2}=\Delta_K=D.$$

如果 K 是虚二次域, 任意数的范数均非负, 从而 f_{ω_1,ω_2} 正定.

如果 (ω_1',ω_2') 也是 $\mathfrak{a}$ 的一组正向的 $\mathbb{Z}$ 基, 则存在 $\gamma\in\mathrm{GL}_2(\mathbb{Z})$ 使得 $(\omega_1',\omega_2')=(\omega_1,\omega_2)\gamma$. 由于这两组基都是正向的, 因此 $\gamma\in\mathrm{SL}_2(\mathbb{Z})$, 从而这两个二元二次型等价.

若 $\mathfrak{b}$ 和 $\mathfrak{a}$ 在 Cl_K^+ 中位于同一个等价类, 则存在全正的 $\alpha\in K$ 使得 $\mathfrak{b}=(\alpha)\mathfrak{a}$. 于是 $(\alpha\omega_1,\alpha\omega_2)$ 是 $\mathfrak{b}$ 的一组正向的 $\mathbb{Z}$ 基, 且我们有 $f_{\alpha\omega_1,\alpha\omega_2}=f_{\omega_1,\omega_2}$. □

对于二元二次型 f, 我们记 $[f]$ 为其等价类.

定理 1.69

上述构造 $\mathfrak{a}\mapsto[f_{\omega_1,\omega_2}]$ 给出了 Cl_K^+ 到判别式为 D 的非负定的二元二次型等价类全体的双射.

证明 设 $f(x,y)=ax^2+bxy+cy^2$ 是判别式为 D 的非负定二元二次型. 我们可不妨设 $a>0$. 设 τ 是 $ax^2-bx+c=0$ 中满足 $(1,\tau)$ 是正向的那个根. 设 $\mathfrak{a}=\mathbb{Z}+\mathbb{Z}\tau\subset K$, 我们来说明它是一个分式理想.

- $D\equiv 0 \bmod 4$. 我们有 $2\mid b$ 且 $\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\frac{\sqrt{D}}{2}$. 由 $\tau=\frac{b\pm\sqrt{D}}{2a}$ 可知
$$\frac{\sqrt{d}}{2}(1,\tau)=\pm(1,\tau)\begin{pmatrix}-b/2 & -c\\ a & -b/2\end{pmatrix}.$$
- $D\equiv 1 \bmod 4$. 我们设 $\omega_D=\frac{1\pm\sqrt{D}}{2}$, 正负号与 $\tau=\frac{b\pm\sqrt{D}}{2a}$ 一致, 则 $\mathcal{O}_K=\mathbb{Z}+\mathbb{Z}\omega_D$,
$$\omega_D(1,\tau)=(1,\tau)\begin{pmatrix}(1-b)/2 & -c\\ a & (1+b)/2\end{pmatrix}.$$

从而 $\mathfrak{a}$ 是一个分式理想. 易知 $\mathrm{disc}(1,\tau)=D/a^2$, 故 $\mathbf{N}\mathfrak{a}=a^{-1}$. 由此可知

$$f_{1,\tau}=\frac{\mathbf{N}_{K/\mathbb{Q}}(x+y\tau)}{\mathbf{N}\mathfrak{a}}=ax^2+bxy+cy^2=f.$$

从而题述映射是满的.

现在我们来说明单. 设 $\mathfrak{b}$ 有一组正向基 (ω_1,ω_2) 使得 $[f_{\omega_1,\omega_2}]=[f]$. 存在 $\gamma=\left(\begin{smallmatrix} r & s\\ u & v\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$ 使得

$$f_{\omega_1,\omega_2}(rx+sy,ux+vy)=f(x,y).$$

我们将正向基 (ω_1,ω_2) 换为 $(\omega_1',\omega_2')=(\omega_1,\omega_2)\gamma$, 则我们可以不妨设 $f_{\omega_1,\omega_2}=f$. 于是

$$\mathbf{N}_{K/\mathbb{Q}}(\omega_1x+\omega_2y)=\mathbf{N}\mathfrak{b}(ax^2+bxy+cy^2).$$

注意到 $\mathbf{N}_{K/\mathbb{Q}}(\omega_1)=a\mathbf{N}\mathfrak{b}>0$, 通过将 (ω_1,ω_2) 换成 $(-\omega_1,-\omega_2)$, 我们可不妨设 ω_1 全正. 令 $(x,y)=(-\tau,1)$, 则 $\mathbf{N}_{K/\mathbb{Q}}(\omega_2-\tau\omega_1)=0$, 从而 $\omega_2=\tau\omega_1$, $\mathfrak{b}=(\omega_1)\mathfrak{a}$. □

注 (1) 任意二元二次型的判别式均可唯一写成 $D=f^2D_K$ 的形式, 其中 D_K 是某个二次域的判别式, f 是正整数. 称 f 为该二元二次型的导子. 类似地, 判别式为 D 的非负定二元二次型等价类全体和 $\mathcal{O}_K$ 的子环 $\mathcal{O}=\mathbb{Z}+f\mathcal{O}_K$ 的缩理想类群有一一对应.

(2) 由定理 1.61和1.69可以得到二次域类群的有限性. 实际上, 这还给出了虚二次域类数的一个有效算法.

(3) 上述定理还给出了二元二次型上的乘法, 称之为高斯复合律. 这由高斯于 1800 年左右首次发现, 在那个时间一般数域的理想类群的概念还尚未被提出.

(4) 如果我们只考虑 $F(x,y)=n$ 何时有有理解的话, 问题会简单得多, 见**??**小节.

练习 1.5.1 设 F,G 为两个二次型, Q 为 F 的关联矩阵.

(1) G 和 F 等价当且仅当存在 $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ 使得 G 的关联矩阵为 $\gamma^{\mathrm{T}} Q \gamma$.

(2) 若 F 和 G 等价, 则它们的判别式相同, 且 $F(x,y)=n$ 的解的数量和 $G(x,y)=n$ 的解的数量相同.

✍ **练习 1.5.2** 哪些正整数可被 x^2+3y^2 表出?

✍ **练习 1.5.3** D 是某个二次域的判别式当且仅当

- 任意奇素数在 D 中的幂次最多为一次;
- $D \equiv 1 \bmod 4$ 或 $D/4 \equiv 2,3 \bmod 4$.

✍ **练习 1.5.4** 学习高斯关于二次域缩理想类群的 2 部分的刻画 (Gauss genus theory).

附录 A 同调代数初步

该附录包含了该课程所需要的同调代数方面的内容, 其中每一节应当安排在正文相同序号的章之前. 诱导模和导出函子可以安排在第三章之前.

§A.1 模

§A.1.1 模和模同态

设 $(M,+)$ 是交换群, 记 $\mathrm{End}(M)$ 为 M 的自同态 (endomorphism) 全体, $\mathrm{Aut}(M)$ 为 M 的自同构 (automorphism) 全体, 则 $(\mathrm{End}(M),+,\circ)$ 在加法和复合意义下构成环, 它的单位群为 $\mathrm{Aut}(M)$.

定义 A.1 (模)

设 R 是 (含幺) 交换环, 称环同态 $\rho: R \to \mathrm{End}(M)$ 为 R 模 (R-module), 或简称 M 是 R 模[a]. 对于 $r\in R, a\in M$, 我们记 ra 或 $r.a=\rho(r)(a)$.

[a] 如果将 $\mathrm{End}(M)$ 上的乘法定义为 $fg=g\circ f$, 则这样的环同态被称为右 R 模 (right R-module), 原来的环同态则被称为左 R 模 (left R-module). 如果 M 既是左模又是右模且 $(ra)s=r(as)$, 则称之为 R 双模 (R-bimodule).

定义 A.2 (群模)

设 G 是群, 称群同态 $\rho: G\to \mathrm{Aut}(M)$ 为 G 模 (G-module), 或简称 M 是 G 模[a]. 对于 $s\in G, a\in M$, 我们记 sa 或 $s.a=\rho(s)(a)$. 注意 M 是 G 模等价于 M 是 $\mathbb{Z}[G]$ 模.

[a] 类似地我们有右 G 模和双模.

注 如果 M 是一个乘法群, 我们通常将 R 或 G 的作用记为 a^r 这种形式.

例题 A.1 (1) 交换群 G 是自然的 $\mathrm{End}(G)$ 模.

(2) $\mathbb{Z}$ 模就是交换群.

(3) 如果环 $A\subseteq B$, 则 B 可视为自然 A 模.

(4) 只有一个元素的群自然是 R 模, 称之为零模.

定义 A.3 (模同态)

设 M,N 为两个 R 模. 如果群同态 $f: M\to N$ 满足 $f(ra)=rf(a), \forall r\in R$, 则称之为模同态 (homomorphism). 如果 f 是群的单同态, 满同态, 同构, 则称之为模的单同态 (monomorphism), 满同态 (epimorphism), 同构 (isomorphism), 记为 $M\hookrightarrow N, M\twoheadrightarrow N, M\cong N$. 记 $\mathrm{Hom}_R(M,N)$ 为 M 到 N 的模同态全体.

定义 A.4 (子模)

如果 N 是 M 的子群, 且 $ra \in N, \forall r \in R, a \in N$, 则称 N 是 M 的子模 (submodule). 显然任意多个子模的交仍然是子模. M 有限多个子模的元素之和也形成 M 的子模. M 中包含其子集 S 最小的子模称为由 S 生成的子模 (submodule generated by S).

如果存在 $a \in M$ 使得 $M = Ra$, 即 M 由 $\{a\}$ 生成, 称之为循环模 (cyclic module). 如果存在有限集 $S \subseteq M$ 使得 S 生成 M, 则称之为有限生成模 (finitely generated module).

命题 A.5

设 N 是 M 的子模, $M/N = \{x + N \mid x \in M\}$ 为其商群. 定义 $r(a+N) = ra + N$, 则 M/N 是 R 模, 称为商模.

证明 易证. □

定义 A.6 (零化子)

对于 $a \in M$, 定义

$$\mathrm{Ann}(a) = \{r \in R \mid ra = 0\},$$

$$\mathrm{Ann}(M) = \{r \in R \mid rM = 0\}$$

为 a 和 M 的零化子, 则它们是 R 的左理想. 如果 $\mathrm{Ann}(a)$ 非零, 称 a 为挠元. 如果 M 所有元素都是挠元, 称之为挠模.

例题 A.2 (1) 群同态就是 $\mathbb{Z}$ 模同态; 群同构就是 $\mathbb{Z}$ 模同构.

(2) 有限生成 $\mathbb{Z}$ 模就是有限生成交换群.

(3) 域 F 上的模就是 F 上的向量空间, 有限生成 F 模就是有限维 F 向量空间.

(4) 环 R 的左理想是 R 的子模.

✍ **练习 A.1.1** 设 $A \subseteq B \subseteq C$ 是整环. 如果 B 是有限生成 A 模, C 是有限生成 B 模, 则 C 是有限生成 A 模.

命题 A.7 (中山引理)

设 R 是交换环, $\mathfrak{a}$ 为它的一个理想, 且 $\mathfrak{a}$ 是所有极大理想的子集. 如果有限生成 R 模 M 和它的子模 N 满足 $M = N + \mathfrak{a}M$, 则 $M = N$. 特别地, 如果 R 是局部环, $\mathfrak{a}$ 为其唯一极大理想时该命题成立. 特别地, 如果 $M = \mathfrak{a}M$, 则 $M = 0$.

证明 由于 $M/N = I \cdot M/N$, 因此我们不妨设 $N = 0$. 设 $a_1, \ldots, a_n$ 是 M 的一组生成元, 则存在 $A \in M_n(\mathfrak{a})$ 使得

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = A \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

于是

$$(I_n - A)^*(I_n - A)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \mathbf{0},$$

即 $\det(I_n - A)a_i = 0$. 而 $\det(I_n - A)$ 展开后除了对角元以外都属于理想 $\mathfrak{a}$, 因此 $\det(I_n - A) = 1 + a, a \in \mathfrak{a}$. 如果 $1 + a$ 不是单位, 则存在极大理想 $\mathfrak{m}$ 包含它, 从而 $1 = (1 + a) - a \in \mathfrak{m}$, 矛盾! 所以 $1 + a \in R^\times$, $a_i = 0, M = 0$. □

§A.1.2 直和和自由模

定义 A.8 (直积和直和)

设 $M_i, i \in I$ 是一族 R 模. 定义 $\prod_{i \in I} M_i, \bigoplus_{i \in I} M_i$ 为群的直积和直和, 则它们有自然的 R 模结构, R 通过在每个分量作用. 称之为模的直积和直和.

定义 A.9 (自由模)

如果存在一族元素 $a_i \in M, i \in I$ 使得 $M = \bigoplus_{i \in I} Ra_i$, 且 $Ra_i \cong R$, 则称之为自由模. 换言之, $M \cong \bigoplus_{i \in I} R$.

命题 A.10

主理想整环 R 上的有限生成模一定同构于

$$M \cong R^{\oplus r} \oplus \bigoplus_i R/\mathfrak{a}_i,$$

其中 $\mathfrak{a}_i$ 是 R 的非零理想.

证明 略. □

定义 A.11 (秩)

称 $r = \mathrm{rank} M$ 为 M 的秩.

例题 A.3 设 A, B 为 R 模, 令 $A \otimes B$ 为形如 $a \otimes b, a \in A, b \in B$ 的对象生成的交换群, 其中 $ra \otimes b = a \otimes rb, \forall r \in R$. 换言之,

$$A \otimes_R B = \langle (a, b) \mid a \in A, b \in B \rangle / \sim,$$

其中 $(ra, b) \sim (a, rb)$. $A \otimes B$ 可以自然地看成 R 模, 称之为 A 和 B 的张量积. 我们有

$$A \otimes B \cong B \otimes A,$$

$$(A \otimes B) \otimes C \cong A \otimes (B \otimes C) \cong A \otimes B \otimes C,$$

$$(A \oplus B) \otimes C \cong (A \otimes C) \oplus (B \otimes C),$$

$$A \otimes R \cong A.$$

§A.1.3 诱导模

定义 A.12 (诱导模)

如果 $H \leqslant G$ 是一个子群, 则对于任意 H 模 B,

$$A = \mathrm{Ind}_G^H B := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} B$$

是一个 G 模, 称为诱导模. 这里 $\mathbb{Z}[H]$ 在 $\mathbb{Z}[G]$ 通过右乘 h^{-1} 作用, G 在 A 通过左乘 g 作用.
另一种看法是将诱导模看成全体函数 $f : G \to B$, 其中 $f(gh) = f(g)^h, \forall h \in H$. 然后 G 的作用是 $f^\sigma(x) = f(\sigma^{-1}x)$. 当 $(G : H)$ 有限时这二者是同构的. 显然 $B = \mathbb{Z}[H] \otimes_{\mathbb{Z}[H]} B$ 是 A 的一个 H 子模, 且

$$\mathrm{Ind}_G^H B = \bigoplus_{\sigma H \in G/H} B^\sigma$$

是 B 模同构, 这里 σ 取遍左陪集 G/H 的一组代表元.

§A.2 范畴

§A.2.1 范畴与函子

定义 A.13 (范畴)

范畴 C 由如下三个要素构成:

- 一个类 $\mathrm{Obj}\,\mathsf{C}$, 其中的元素 $A \in \mathrm{Obj}\,\mathsf{C}$ (或简记为 $A \in \mathsf{C}$) 被称为对象;
- 对于任意对象 A, B, 存在集合 $\mathrm{Hom}(A, B)$, 其中的元素 u 被称为 A 到 B 的态射, 记为 $u : A \to B$; 不同的有序对 (A, B) 对应的态射不同;
- 对于任意对象 A, B, C, 存在映射

  $$\mathrm{Hom}(A, B) \times \mathrm{Hom}(B, C) \to \mathrm{Hom}(A, C).$$

  称 (v, u) 的像为二者的复合, 记为 $u \circ v$ 或 uv.

这些要素需要满足

- 结合律: 对于 $u : A \to B, v : B \to C, w : C \to D, w \circ (v \circ u) = (w \circ v) \circ u$;
- 对于任意 $A \in \mathsf{C}$, 存在 $\mathrm{id}_A \in \mathrm{Hom}(A, A)$ 使得对任意 $u : A \to B$, $u \circ \mathrm{id}_A = u$; 对任意 $v : B \to A$, $\mathrm{id}_A \circ v = v$.

例题 A.4 (1) 范畴的对象并不要求是一个具体的集合, 态射也不要求是集合间的映射, 尽管从主流集合论出发包括自然数, 实数等均为视为集合. 设 $(I, \leq)$ 是一个偏序集, 对于 $i, j \in I$, 当 $i \leq j$ 时, $\mathrm{Hom}(i, j)$ 为单点集; 否则 $\mathrm{Hom}(n, m)$ 为空. 这样便构造了一个范畴. 例如 $(\mathbb{N}^+, \leq)$, $(\mathbb{N}^+, |)$, 拓扑空间开集关于包含关系等, 都可以构成范畴.

(2) 范畴对象构成的一般是一个类而不是集合. 例如全体集合关于集合间的映射构成的范畴 Sets 的对象全体, 即全体集合, 就不是一个集合 (为什么).

(3) 其它例子包括: 全体群关于群同态构成范畴 Groups; 全体交换群关于群同态构成范畴 Ab; 全体环关于环同态构成范畴 Rings; 环 R 上全体模关于模同态构成范畴 Mod/R; 域 k 上全体线性空间关于线性映射构成范畴 Vect/k 等.

定义 A.14 (对偶范畴)

设 A 是一个范畴, 定义其对偶范畴 A^{op}:

- $\mathrm{Obj}\,\mathsf{A}^{\mathrm{op}} = \mathrm{Obj}\,\mathsf{A}$;
- $\mathrm{Hom}_{\mathsf{A}^{\mathrm{op}}}(A, B) = \mathrm{Hom}_{\mathsf{A}}(B, A)$.

例题 A.5 设 $(I, \leq)$ 是一个偏序集, 则 $(I, \geq)$ 也是一个偏序集, 它们对应的范畴构成对偶范畴.

定义 A.15 (函子)

范畴 A 到范畴 B 间的(共变) 函子 $\mathcal{F}$ 由如下要素构成:

- 对于任意 $A \in \mathsf{A}$, 有 $\mathcal{F}(A) \in \mathsf{B}$;
- 对于任意 A 中态射 $u : A_1 \to A_2$, 有 $\mathcal{F}(u) : \mathcal{F}(A_1) \to \mathcal{F}(A_2)$,

且满足

- $\mathcal{F}(\mathrm{id}_A) = \mathrm{id}_{\mathcal{F}(A)}$;
- $\mathcal{F}(u \circ v) = \mathcal{F}(u) \circ \mathcal{F}(v)$.

定义 A.16 (反变函子)

范畴 A 到范畴 B 间的反变函子 $\mathcal{F}$ 由如下要素构成:

- 对于任意 $A \in \mathsf{A}$, 有 $\mathcal{F}(A) \in \mathsf{B}$;
- 对于任意 A 中态射 $u : A_1 \to A_2$, 有 $\mathcal{F}(u) : \mathcal{F}(A_2) \to \mathcal{F}(A_1)$,

且满足

- $\mathcal{F}(\mathrm{id}_A) = \mathrm{id}_{\mathcal{F}(A)}$;
- $\mathcal{F}(u \circ v) = \mathcal{F}(v) \circ \mathcal{F}(u)$.

这等价于共变函子 $\mathcal{F} : \mathsf{A}^{\mathrm{op}} \to \mathsf{B}$.

例题 A.6 (1) $\mathrm{id}_{\mathsf{A}} : \mathsf{A} \to \mathsf{A}$ 将范畴 A 的所有对象和映射保持不变, 它显然是一个函子, 称为恒等函子.

(2) 设 k 是一个域对于任意集合 S, 定义 $\mathcal{F}(S)$ 为以 S 为基的 k 上线性空间, 则 $\mathcal{F} : \mathsf{Sets} \to \mathsf{Vect}/k$ 是一个函子. $\mathcal{F}$ 在态射上怎么作用?

(3) 对于任意群 G, 定义 $\mathcal{F}(G)$ 为其对应的集合, 则 $\mathcal{F} : \mathsf{Groups} \to \mathsf{Sets}$ 是一个函子, 称之为遗忘函子. 同理我们有遗忘函子 $\mathsf{Mod}/R \to \mathsf{Ab}$ 等.

(4) 设 A 是一个范畴, $A, M, N \in \mathsf{C}$. 定义 $\mathrm{Hom}(A, -)(M) = \mathrm{Hom}(A, M)$, 则 $\mathrm{Hom}(A, -) : \mathsf{A} \to \mathsf{Sets}$ 是一个函子, 其中对于 $u : M \to N$,

$$\begin{aligned} \mathrm{Hom}(A, -)(u) : \mathrm{Hom}(A, M) &\longrightarrow \mathrm{Hom}(A, N) \\ v &\longmapsto u \circ v. \end{aligned}$$

(5) 设 A 是一个范畴, $A, M, N \in \mathsf{C}$. 定义 $\mathrm{Hom}(-, A)(M) = \mathrm{Hom}(M, A)$, 则 $\mathrm{Hom}(-, A) : \mathsf{A} \to \mathsf{Sets}$ 是一个反变函子, 其中对于 $u : M \to N$,

$$\begin{aligned} \mathrm{Hom}(-, A)(u) : \mathrm{Hom}(N, A) &\longrightarrow \mathrm{Hom}(M, A) \\ v &\longmapsto v \circ u. \end{aligned}$$

我们称 $\mathrm{Hom}(A, -), \mathrm{Hom}(-, A)$ 为 Hom 函子.

(6) 设 H 是 G 的一个子群, 则 $\mathrm{Ind}_G^H : \mathsf{Mod}/H \to \mathsf{Mod}/G$ 和 $\mathrm{Res}_G^H : \mathsf{Mod}/G \to \mathsf{Mod}/H$ 是函子, 其

中 $\mathrm{Res}_G^H(M)=M$. 它们互为伴随, 即

$$\mathrm{Hom}_G(\mathrm{Ind}_G^H M,N)=\mathrm{Hom}_H(M,\mathrm{Res}_G^H N).$$

(7) 设 G 是一个群, $G^{\mathrm{ab}}=G/[G,G]$ 为其极大阿贝尔商, 则 $(\ )^{\mathrm{ab}}:\mathsf{Groups}\to\mathsf{Ab}$ 是一个函子.

定义 A.17 (范畴的同构)

设 $u:A\to B$. 如果存在 $v:B\to A$ 使得 $v\circ u=\mathrm{id}_A, u\circ v=\mathrm{id}_B$, 则称 u 是同构.

定义 A.18 (自然变换与范畴等价)

设 $\mathcal{F},\mathcal{G}:\mathsf{A}\to\mathsf{B}$ 是两个函子. 称 f 为 $\mathcal{F}$ 到 $\mathcal{G}$ 的自然变换, 如果对于任意 $A\in\mathsf{A}$, 存在 $f_A:\mathcal{F}(A)\to\mathcal{G}(A)$, 且满足对任意态射 $u:A_1\to B_2$,

$$\begin{array}{ccc}\mathcal{F}(A_1) & \xrightarrow{\mathcal{F}(u)} & \mathcal{F}(A_2)\\ {\scriptstyle f_{A_1}}\downarrow & & \downarrow{\scriptstyle f_{A_2}}\\ \mathcal{G}(A_1) & \xrightarrow{\mathcal{G}(u)} & \mathcal{G}(A_2)\end{array}$$

交换. 特别地, 我们有自然变换 $\mathrm{id}_{\mathcal{F}}:\mathcal{F}\to\mathcal{F}$, 其中 $(\mathrm{id}_{\mathcal{F}})_A=\mathrm{id}_{\mathcal{F}(A)}$. 如果 A 是一个小范畴, 即 $\mathrm{Obj}\,\mathsf{A}$ 是一个集合, 则 $\mathsf{A}\to\mathsf{B}$ 间的函子以及函子的自然变换构成范畴 $\mathsf{Func}(\mathsf{A},\mathsf{B})$. 对于反变函子, 我们也可以类似定义自然变换.

如果存在自然变换 $f:\mathcal{F}\to\mathcal{G}, g:\mathcal{G}\to\mathcal{F}$ 使得 $g\circ f=\mathrm{id}_{\mathcal{F}}, f\circ g=\mathrm{id}_{\mathcal{G}}$, 则称 $\mathcal{F}$ 和 $\mathcal{G}$ 同构. 换言之, $\mathcal{F},\mathcal{G}$ 在 $\mathsf{Func}(\mathsf{A},\mathsf{B})$ 中同构. 这也等价于对任意 $A\in\mathsf{A}$, $f_A:\mathcal{F}(A)\to\mathcal{G}(A)$ 是同构.

如果存在 $\mathcal{F}:\mathsf{A}\to\mathsf{B}, \mathcal{G}:\mathsf{B}\to\mathsf{A}$ 使得 $\mathcal{G}\circ\mathcal{F}$ 和 id_{A} 同构, $\mathcal{F}\circ\mathcal{G}$ 和 id_{B} 同构, 则称 $\mathcal{F},\mathcal{G}$ 诱导了 A 和 B 的范畴等价. 这不同于范畴同构, 后者是指范畴的对象的态射完全一一对应, 即 $\mathcal{F}\circ\mathcal{G}=\mathrm{id}_{\mathsf{B}}, \mathcal{G}\circ\mathcal{F}=\mathrm{id}_{\mathsf{A}}$. 但是范畴等价意味着两个范畴的对象在同构意义下是一一对应的, 特别地, 二者的骨架范畴是同构的, 其中骨架范畴是指范畴的每个对象的同构等价类中只选取一个对象.

§A.2.2 加性范畴

范畴论中大量概念都是通过泛性质来定义的.

定义 A.19 (始对象)

如果范畴 A 中的对象 I 满足:

- 对于任意对象 A, $\mathrm{Hom}(I,A)=\{i_A\}$ 是单点集;
- 对于任意态射 $u:A\to B$, $u\circ i_A=i_B$,

则称 I 为 A 的始对象.

定义 A.20 (终对象)

如果范畴 A 中的对象 F 满足:

- 对于任意对象 A, $\mathrm{Hom}(A,F)=\{j_A\}$ 是单点集;
- 对于任意态射 $u:A\to B$, $j_B\circ u=j_A$,

则称 F 为 A 的终对象.

定义 A.21 (零对象)

如果一个对象既是始对象也是终对象，称之为零对象，通常记为 0，并记 $\mathrm{Hom}(A,0)=\{0\}, \mathrm{Hom}(0,A)=\{0\}$.

命题 A.22

始对象在同构意义下是唯一的; 终对象在同构意义下是唯一的.

证明 设 I, I' 是始对象, 则 $\mathrm{Hom}(I,I')=\{i_{I'}\}, \mathrm{Hom}(I',I)=\{i'_I\}$, 因此 $i_{I'}\circ i'_I: I\to I$. 由于 $\mathrm{Hom}(I,I)=\{\mathrm{id}_I\}$, 因此 $i_{I'}\circ i'_I=\mathrm{id}_I$. 同理 $i'_I\circ i_{I'}=\mathrm{id}_{I'}$, 所以 $i_{I'}: I\to I'$ 是同构. 类似地, 终对象在同构意义下也是唯一的. □

设 $A_i, i\in I$ 是范畴 A 中的一族对象.

定义 A.23 (直和)

如果对象 A 以及一族态射 $\alpha_i: A_i\to A$, 满足对于任意对象 M 和一族态射 $u_i: A_i\to M$, 存在唯一的 $v: A\to M$ 使得下图交换

$$\begin{tikzcd} A_i \arrow[d, "\alpha_i"'] \arrow[dr, "\forall u_i"] & \\ A \arrow[r, dotted, "\exists! v"'] & M \end{tikzcd}$$

则称 (A,α_i) 为 A_i 的直和, 记为 $\oplus_i A_i$.

定义 A.24 (直积)

如果对象 A 以及一族态射 $\beta_i: A\to A_i$, 满足对于任意对象 M 和一族态射 $u_i: M\to A_i$, 存在唯一的 $v: M\to A$ 使得下图交换

$$\begin{tikzcd} M \arrow[r, dotted, "\exists! v"] \arrow[dr, "u_i"'] & A \arrow[d, "\beta_i"] \\ & A_i \end{tikzcd}$$

则称 (A,β_i) 为 A_i 的直积, 记为 $\prod_i A_i$.

命题 A.25

直和和直积是同构意义下唯一的.

证明 易证. □

对于 $\mathsf{Ab}, \mathsf{Mod}/R$ 等范畴, 我们可以发现 $\mathrm{Hom}(A,B)$ 均构成交换群且有有限直和, 有限直积, 核, 像等概念. 由此出发, 我们可以定义加性范畴和阿贝尔范畴.

定义 A.26 (加性范畴)

如果范畴 C 满足

- 对于任意对象 A, B, C, $\mathrm{Hom}(A,B)$ 具有交换群结构, 且态射复合

$$\mathrm{Hom}(A,B)\times\mathrm{Hom}(B,C)\to\mathrm{Hom}(A,C)$$

是双线性的;

- 存在零对象 0;
- 对于任意对象 A, B, 存在直和 $A \oplus B$ 和直积 $A \times B$,

我们称之为加性范畴.

命题 A.27

对于加性范畴的对象 A, B, 我们有同构 $A \oplus B \xrightarrow{\sim} A \times B$.

证明 考虑 $\mathrm{id}_A : A \to A, 0 : A \to B$, 存在 $(\mathrm{id}_A, 0) : A \to A \times B$. 同理存在 $(0, \mathrm{id}_B) : B \to A \times B$. 因此存在态射 $i : A \oplus B \to A \times B$, 使得下图交换

$$\begin{tikzcd}
A \arrow[d, "\alpha_A"'] \arrow[dr, "(\mathrm{id}_A,0)"] & \\
A \oplus B \arrow[r, "i"] & A \times B \\
B \arrow[u, "\alpha_B"] \arrow[ur, "(0,\mathrm{id}_B)"'] &
\end{tikzcd}$$

容易验证 $\alpha_A \circ \beta_A + \alpha_B \circ \alpha_A : A \times B \to A \oplus B$ 是它的逆. □

定义 A.28 (加性函子)

如果加性范畴间的函子 $\mathcal{F} : \mathsf{A} \to \mathsf{B}$ 满足

- $\mathcal{F}(0) = 0$;
- 自然态射 $\mathcal{F}(A_1) \oplus \mathcal{F}(A_2) \to \mathcal{F}(A_1 \oplus A_2)$ 是同构,

称之为加性函子. 这等价于对任意 $A, B, \mathcal{F} : \mathrm{Hom}(A, B) \to \mathrm{Hom}\big(\mathcal{F}(A), \mathcal{F}(B)\big)$ 是群同态.

例题 A.7 (1) 加性范畴的对偶仍然是加性的.

(2) Ab 是加性范畴, 其上的 Hom 函子是加性函子.

§A.2.3 阿贝尔范畴

设 $u : A \to B$ 是加性范畴 A 上的一个态射.

定义 A.29 (核)

如果对象 C 和态射 $i : C \to B$ 满足对于任意对象 M 和态射 $v : M \to A$, 若 $u \circ v = 0$, 则存在唯一的态射 $w : M \to C$ 使得下图交换

$$\begin{tikzcd}
M \arrow[d, dotted, "\exists ! w"'] \arrow[dr, "\forall v"] \arrow[drr, "0"] & & \\
C \arrow[r, "i"'] & A \arrow[r, "u"'] & B
\end{tikzcd}$$

则称 (C, i) 为 u 的核, 记为 $\ker u$. 若 $\ker u = 0$, 称 u 为单态射.

定义 A.30 (余核)

如果对象 D 和态射 $j: B \to D$ 满足对于任意对象 M 和态射 $v: B \to M$, 若 $v \circ u = 0$, 则存在唯一的态射 $w: D \to M$ 使得下图交换

$$\begin{tikzcd} A \arrow[r, "u"] \arrow[drr, "0"'] & B \arrow[r, "j"] \arrow[dr, "\forall v"] & D \arrow[d, dotted, "\exists! w"] \\ & & M \end{tikzcd}$$

则称 (D, j) 为 u 的余核, 记为 $\operatorname{coker} u$. 若 $\operatorname{coker} u = 0$, 称 u 为满态射.

定义 A.31 (像和余像)

称余核的核 $\ker(\operatorname{coker} u)$ 为 u 的像 $\operatorname{im} u$; 称核的余核 $\operatorname{coker}(\ker u)$ 为 u 的余像 $\operatorname{coim} u$.

我们将它们对应的对象记为 Ker, Coker, Im, CoIm.

定义 A.32 (阿贝尔范畴)

如果加性范畴 A 满足

- 任意态射均有核和余核;
- 对于任意态射 $u: A \to B$, 自然映射 $\operatorname{CoIm} u \to \operatorname{Im} u$ 是同构,

则称 A 为阿贝尔范畴. 这等价于既满又单的态射是同构.

例题 A.8 (1) 阿贝尔范畴的对偶仍然是阿贝尔的.

(2) Ab, Mod/R 是阿贝尔范畴.

(3) (Mitchell 嵌入定理) 任何一个小阿贝尔范畴 A 可正合嵌入为一个模范畴 Mod/R 的全子范畴, 即存在函子 $\mathcal{F}: \mathsf{A} \to \mathsf{Mod}/R$, 使得 $\mathcal{F}$ 诱导了

$$\operatorname{Obj} \mathsf{A} \hookrightarrow \operatorname{Obj} \mathsf{Mod}/R,$$
$$\operatorname{Hom}_{\mathsf{A}}(A, B) = \operatorname{Hom}_{\mathsf{Mod}/R}\big(\mathcal{F}(A), \mathcal{F}(B)\big),$$

且保持核和余核.

§A.2.4 正合列

定义 A.33 (正合)

设 A 为阿贝尔范畴, $A, B, C \in \mathsf{A}$. 称 $A \xrightarrow{u} B \xrightarrow{v} C$ 正合, 如果自然映射 $\operatorname{Ker} v \simeq \operatorname{Im} u$ 是同构. 由于它们都可以看成是 B 的子对象 (存在到 B 的单态射), 此时 $\operatorname{Ker} v = \operatorname{Im} u$. 由此可知

$$0 \to A \xrightarrow{u} B \xrightarrow{v} C \to 0$$

正合当且仅当 $\operatorname{Ker} u = 0, \operatorname{Im} u = \operatorname{Ker} v, \operatorname{Im} v = C$, 这样的序列被称为短正合列.

命题 A.34 (蛇形引理)

考虑阿贝尔范畴 A 中的交换图

$$\begin{tikzcd} & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B \arrow[r] & C & \end{tikzcd}$$

其中每行都是正合的, 则存在唯一的态射

$$\delta : \operatorname{Ker}\gamma \to \operatorname{Coker}\alpha$$

使得下图交换

$$\begin{tikzcd} B \times_C \operatorname{Ker}\gamma \arrow[r] \arrow[d] & \operatorname{Ker}\gamma \arrow[d, "\delta"] \\ A' \arrow[r] & \operatorname{Coker}\alpha \end{tikzcd}$$

其中左竖直态射由 β 诱导, 而且我们有正合列

$$\operatorname{Ker}\alpha \to \operatorname{Ker}\beta \to \operatorname{Ker}\gamma \xrightarrow{\delta} \operatorname{Coker}\alpha \to \operatorname{Coker}\beta \to \operatorname{Coker}\gamma.$$

对于模范畴情形, 我们可以直接验证.

推论 A.35 (五引理)

考虑交换图表

$$\begin{tikzcd} A^1 \arrow[r] \arrow[d, "u^1"] & A^2 \arrow[r] \arrow[d, "u^2"] & A^3 \arrow[r] \arrow[d, "u^3"] & A^4 \arrow[r] \arrow[d, "u^4"] & A^5 \arrow[d, "u^5"] \\ B^1 \arrow[r] & B^2 \arrow[r] & B^3 \arrow[r] & B^4 \arrow[r] & B^5, \end{tikzcd}$$

其中每行都正合. 如果 u^1, u^2, u^4, u^5 是同构, 则 u^3 也是同构.

§A.2.5 正向极限和逆向极限

定义 A.36 (正向极限)

设 I 是一个偏序集. 对于范畴 A 中的一族对象 $A_i, i \in I$, 以及 $i \leq j$ 时态射 $\alpha_{ij} : A_i \to A_j$, 如果对象 A 以及一族态射 $\alpha_i : A_i \to A$, 满足对任意 $i \leq j$, $\alpha_j \circ \alpha_{ij} = \alpha_i$, 以及对于任意对象 M 和一族态射 $u_i : A_i \to M$, 如果 $u_j \circ \alpha_{ij} = u_i$, 存在唯一的 $v : A \to M$ 使得下图交换

$$\begin{tikzcd} A_i \arrow[r, "\alpha_{ij}"] \arrow[dr, "\alpha_i"] \arrow[ddr, bend right, "\forall u_i"'] & A_j \arrow[d, "\alpha_j"] \arrow[dd, bend left, "u_j"] \\ & A \arrow[d, dotted, "\exists! v"] \\ & M \end{tikzcd}$$

则称 (A, α_i) 为 A_i 的正向极限, 记为 $\varinjlim_i A_i$.

定义 A.37 (逆向极限)

对于范畴 A 中的一族对象 $A_i, i \in I$, 以及 $i \leq j$ 时态射 $\alpha_{ij} : A_i \to A_j$, 如果对象 A 以及一族态射 $\alpha_i : A_i \to A$, 满足对任意 $i \leq j, \alpha_j \circ \alpha_{ij} = \alpha_i$, 以及对于任意对象 M 和一族态射 $u_i : A_i \to M$, 如果 $u_j \circ \alpha_{ij} = u_i$, 存在唯一的 $v : A \to M$ 使得下图交换

$$\begin{tikzcd}
M \arrow[d, dotted, "\exists ! v"] \arrow[dd, bend right, "\forall u_i"'] \arrow[ddr, bend left, "\forall u_j"] & \\
A \arrow[d, "\alpha_i"] \arrow[dr, "\alpha_j"] & \\
A_i \arrow[r, "\alpha_{ij}"'] & A_j
\end{tikzcd}$$

则称 (A, α_i) 为 A_i 的逆向极限, 记为 $\varprojlim_i A_i$.

命题 A.38

正向极限和逆向极限是同构意义下唯一的.

证明 易证. □

我们考虑模范畴情形. 对于正向系 $A_i, i \in I$, 设 $A = \varinjlim_i A_i$, 则存在映射 $u : \bigoplus_i A_i \to A$. 考虑 $\bigoplus_i A_i$ 中由 $a_j - u_{ij}(a_i)$ 生成的子模 M, 则

$$\varinjlim_i A_i = \frac{\bigoplus_i A_i}{M},$$

所以正向极限是直和的商模. 同理, 设 $B = \varprojlim_i A_i$, 则存在映射 $u : B \to \prod_i A_i$. 考虑 $\prod_i A_i$ 中由满足 $a_j = u_{ij}(a_i)$ 的元素 $(a_i)_i$ 全体 N, 则 N 是 $\prod_i A_i$ 的子模, 它就是 $\varprojlim_i A_i$.

§A.2.6 复形

设 A 是一个阿贝尔范畴. A 上的复形 $L = L^\bullet$ 是指一族对象 $L^i, i \in \mathbb{Z}$, 以及态射 $d = d^i : L^i \to L^{i+1}$, 使得 $d \circ d = 0$. 我们记为

$$L = (\cdots \to L^i \to L^{i+1} \to \cdots).$$

其中 d 被称为 L 的微分, L^i 被称为 i 次分量. 复形的态射 $u : L \to M$ 是指一族 $u^i : L^i \to M^i$, 使得 $d_M \circ u^i = u^{i+1} \circ d_L$. A 上复形全体构成阿贝尔范畴 C(A).

定义

$$Z^i L = \operatorname{Ker} d^i : L^i \to L^{i+1}, \quad B^i L = \operatorname{Im} d^{i-1} : L^{i-1} \to L^i,$$

$$\mathrm{H}^i = Z^i / B^i,$$

为 L 的循环, 边界, 上同调.

定义 A.39 (拟同构)

设 $u : L \to M$ 是复形的态射. 如果 $\mathrm{H}^i(u) : \mathrm{H}^i L \to \mathrm{H}^i M$ 是同构, $\forall i$, 则称 u 是拟同构.

显然任意 $A \in$ A 可以看做 0 处是 A, 其它地方是 0 的复形.

定义 A.40 (解出)

设 $A \in \mathsf{A}, L, M \in \mathsf{C}(\mathsf{A})$. 称 $u : L \to E$ 是一个左解出, 如果 $L^i = 0, i > 0$. 这等价于给出正合列

$$\cdots \to L^2 \to L^1 \to L^0 \to A \to 0.$$

类似地, 称 $u : A \to M$ 是一个右解出, 如果 $M^i = 0, i < 0$. 这等价于给出正合列

$$0 \to A \to M^0 \to M^1 \to M^2 \to \cdots.$$

§A.2.7 导出函子

定义 A.41 (导出函子)

设 $\mathcal{F} : \mathsf{A} \to \mathsf{B}$ 是加性范畴间的加性函子. 如果对于任意正合列

$$0 \to A_1 \to A_2 \to A_3 \to 0,$$

序列

$$0 \to \mathcal{F}(A_1) \to \mathcal{F}(A_2) \to \mathcal{F}(A_3)$$

(或 $\mathcal{F}(A_1) \to \mathcal{F}(A_2) \to \mathcal{F}(A_3) \to 0$) 也正合, 则称 $\mathcal{F}$ 是左正合(或右正合). 如果 $\mathcal{F}$ 既左正合也右正合, 则称其正合. 对于反变函子 $\mathcal{G} : \mathsf{A} \to \mathsf{B}$, 我们称其左正合 (或右正合) 是指其对应的共变函子 $\mathcal{G}^{\mathrm{op}} : \mathsf{A}^{\mathrm{op}} \to \mathsf{B}$ 左正合 (或右正合).

例题 A.9 设 $M \in \mathsf{Mod}/R$. 函子 $\mathrm{Hom}(M, -) : \mathsf{Mod}/R \to \mathsf{Mod}/R$ 是左正合的. 设

$$0 \longrightarrow A \xrightarrow{u} B \xrightarrow{v} C$$

正合, 则

$$0 \longrightarrow \mathrm{Hom}(M, A) \longrightarrow \mathrm{Hom}(M, B) \longrightarrow \mathrm{Hom}(M, C)$$

正合. 显然该序列构成复形. 设 $f \in \mathrm{Hom}(M, A)$ 使得 $u \circ f = 0$, 由于 u 是单射, 因此 $f = 0$. 设 $g \in \mathrm{Hom}(M, B)$ 使得 $v \circ g = 0$, 对任意 $m \in M$, $g(m) \in \mathrm{Ker}\, v = \mathrm{Im}\, u$, 因此存在唯一的 $a \in A$ 使得 $u(a) = g(m)$. 定义 $h : M \to A, h(m) = a$, 则容易看出 h 是模同态且 $u \circ h = g$.

类似地, 反变函子 $\mathrm{Hom}(-, M) : \mathsf{Mod}/R \to \mathsf{Mod}/R$ 左正合.

例题 A.10 设 $M \in \mathsf{Mod}/R$, 则函子 $M \otimes - : \mathsf{Mod}/R \to \mathsf{Mod}/R$ 是右正合的.

定义 A.42 (内射和投射)

设 A 是阿贝尔范畴. 如果 $\mathrm{Hom}(-, M)$ 正合, 我们称 M 是内射的. 我们称 A 有足够多的内射对象, 是指对任意 $L \in \mathsf{A}$, 存在内射 $L' \in \mathsf{A}$ 和单态射 $L \to L'$.

如果 $\mathrm{Hom}(M, -)$ 正合, 我们称 M 是投射的. 我们称 A 有足够多的投射对象, 是指对任意 $L \in \mathsf{A}$, 存在投射 $L' \in \mathsf{A}$ 和满态射 $L' \to L$.

设 A 是有足够多的内射对象的阿贝尔范畴. 对于任意 $A \in \mathsf{A}$, 存在内射 I^0 和单态射 $A \to I^0$. 对其余核进行同样的操作 $\mathrm{Coker}\,(A \to I^0) \to I^1$, 反复操作下去, 我们便可得到 A 的一个内射右解出

$$0 \to A \to I^0 \to I^1 \to \cdots.$$

对于左正合函子 $\mathcal{F} : \mathsf{A} \to \mathsf{B}$, 复形

$$0 \to \mathcal{F}(I^0) \to \mathcal{F}(I^1) \to \cdots$$

的上同调 $R^i\mathcal{F}(A)$ 称为 $\mathcal{F}$ 的右导出函子 $R^i\mathcal{F}:\mathsf{A}\to\mathsf{B}$. 显然 $R^0\mathcal{F}=\mathcal{F}$.

类似地, 设 A 是有足够多的投射对象的阿贝尔范畴. 对于任意 $A\in\mathsf{A}$, 存在投射左解出

$$\cdots\to P^1\to P^0\to A\to 0.$$

对于右正合函子 $\mathcal{F}:\mathsf{A}\to\mathsf{B}$, 复形

$$\cdots\to\mathcal{F}(P^1)\to\mathcal{F}(P^0)\to 0$$

的同调 $L^i\mathcal{F}(A):=\mathrm{H}^{-i}\big(\mathcal{F}(P^\bullet)\big)$ 称为 $\mathcal{F}$ 的左导出函子 $L^i\mathcal{F}:\mathsf{A}\to\mathsf{B}$. 显然 $L^0\mathcal{F}=\mathcal{F}$.

对于反变函子, 考虑其对应的共变函子即可.

§A.3 群的上同调

§A.3.1 上同调群

设 A 是一个 G 模, 定义 $\mathcal{F}(A)=A^G$ 为 A 中被 G 固定的部分, 则这诱导了 G 模范畴到交换群范畴的一个函子. $\mathcal{F}$ 是左正合的, 即如果

$$0\to A\to B\to C$$

是 G 模正合列 ($A\to B$ 是单射, $A\to B$ 的像等于 $B\to C$ 的核), 则

$$0\to\mathcal{F}(A)\to\mathcal{F}(B)\to\mathcal{F}(C)$$

是交换群的正合列.

✍ **练习 A.3.1** 证明 $A\mapsto A^G$ 是左正合的.

基于范畴的一般理论, $\mathcal{F}$ 有所谓右导出函子 $\mathrm{H}^i(G,-)=R^i\mathcal{F}$, 它们可以通过下述方式得到. 我们可以构造 $\mathbb{Z}$ 的左解出序列

$$\cdots\to P_2\to P_1\to P_0\to\mathbb{Z}\to 0,$$

其中 P_i 都是自由 G 模. 于是 $K^i=\mathrm{Hom}_G(P_i,A)$ 构成余链复形

$$0\to K_0\to K_1\to K_2\to K_3\to\cdots,$$

即连续的两个映射的复合是 0, 定义

$$\mathrm{H}^q(G,A)=\mathrm{H}^q(K)=\frac{\mathrm{Ker}\,(K^q\to K^{q+1})}{\mathrm{Im}\,(K^{q-1}\to K^q)}.$$

实际上, 我们可以取 $P_i=\mathbb{Z}[G\times\cdots\times G]$, 其中一共有 $i+1$ 个 G, G 通过对角作用, 即

$$s.(g_0,\ldots,g_i)=(sg_0,\ldots,sg_i).$$

映射为

$$d(g_0,\ldots,g_1)=\sum_{j=0}^{i}(-1)^j(g_0,\ldots,\hat{g}_j,\ldots,g_i),$$

其中 $\hat{g}_j$ 表示去除该项. 特别地 $d:P_0\to\mathbb{Z}$ 为 $d(g_0)=1$.

✍ **练习 A.3.2** 验证 $\cdots\to P_2\to P_1\to P_0\to\mathbb{Z}\to 0$ 是正合的.

于是 $K^i=\mathrm{Hom}_G(P_i,A)$ 可以看成 $G\times\cdots\times G$ 上满足

$$h(s.g_0,\ldots,s.g_i)=s.h(g_0,\ldots,g_i)$$

的函数全体. 由此也可以看出 h 完全由函数

$$f(g_1,\dots,g_i)=h(1,g_1,g_1g_2,\dots,g_1\dots g_i)$$

确定. 通过这种非齐次的表达式, d 变为了

$$\begin{aligned}df(g_1,\dots,g_{i+1})=&g_1.f(g_2,\dots,g_{i+1})\\&+\sum_{j=1}^{i}(-1)^jf(g_1,\dots,g_jg_{j+1},\dots,g_{i+1})\\&+(-1)^{i+1}f(g_1,\dots,g_i).\end{aligned}$$

特别地, 1 余循环 $\operatorname{Ker}(K^1\to K^2)$ 由满足

$$f(gg')=g.f(g')+f(g)$$

的函数构成, 1 余边界 $\operatorname{Im}(K^0\to K^1)$ 由 $f(g)=g.a-a$ 形式的函数构成. 显然, 如果 G 的作用是平凡的, 则 $\mathrm{H}^1(G,A)=\operatorname{Hom}(G,A)$.

✍ **练习 A.3.3** 2 余循环满足什么条件?

由导出函子的性质, 我们有

$$0\to A\to B\to C\to 0$$

正合, 则

$$\cdots\to\mathrm{H}^q(G,B)\to\mathrm{H}^q(G,C)\xrightarrow{\delta}\mathrm{H}^{q+1}(G,A)\to\mathrm{H}^{q+1}(G,B)\to\cdots$$

正合, 其中 δ 被称为连接映射.

§A.3.2 同调群

设 A 是一个 G 模, DA 为 A 中 $s.a-a, s\in G$ 生成的子模, 考虑 $\mathcal{F}(A)=A_G:=A/DA$, 它是 A 被 G 作用平凡的极大商.

✍ **练习 A.3.4** 证明 $A\mapsto A_G$ 是右正合的.

基于范畴的一般理论, $\mathcal{F}$ 有所谓左导出函子 $\mathrm{H}_i(G,-)=L^i\mathcal{F}$, 它们可以通过下述方式得到. 类似地, 我们可以构造 $\mathbb{Z}$ 的左解出序列

$$\cdots\to P_2\to P_1\to P_0\to\mathbb{Z}\to 0,$$

其中 $P_i=\mathbb{Z}[G\times\cdots\times G]$. 于是 $\mathrm{H}_q(G,A)$ 为链复形

$$\cdots\to P_2\otimes_G A\to P_1\otimes_G A\to P_0\otimes_G A\to 0$$

其中的元素可视为函数 $x(g_1,\dots,g_q)$. 类似地, d 为

$$\begin{aligned}dx(g_1,\dots,g_{q-1})=&\sum_{g\in G}g^{-1}.f(g,g_1,\dots,g_{q-1})\\&+\sum_{j=1}^{q-1}(-1)^j\sum_{g\in G}x(g_1,\dots,g_jg,g^{-1},\dots,g_{q-1})\\&+(-1)^qf(g_1,\dots,g_{q-1},q).\end{aligned}$$

我们有类似的长正合列.

若 $A=\mathbb{Z}$, G 为平凡作用, 则 $\mathrm{H}_1(G,\mathbb{Z})=G^{\mathrm{ab}}$. 实际上, 设 $\pi:\mathbb{Z}[G]\to\mathbb{Z}$ 为增广映射, 即 $\sum n_gg\mapsto$

$\sum n_g$. 令 I_G 为其核, 即增广理想, 它由 $g-1$ 生成. 由定义, $\mathrm{H}_0(G,A)=A/I_GA$. 考虑

$$0\to I_G\to\mathbb{Z}[G]\xrightarrow{\pi}\mathbb{Z}\to 0.$$

我们有 $\mathrm{H}_0(G,I_G)=I_G/I_G^2$ 且其在 $\mathrm{H}_0(G,\mathbb{Z}[G])$ 中的像为 0. 而 $\mathbb{Z}[G]$ 是自由模, 它的同调为 0, 因此同调的上正合列诱导了同构

$$d:\mathrm{H}_1(G,Z)\to\mathrm{H}_0(G,I_G)=I_G/I_G^2.$$

容易验证 $s\mapsto s-1$ 诱导了同构 $G^{\mathrm{ab}}\simeq I_G/I_G^2$. 因此 $\mathrm{H}_1(G,\mathbb{Z})=G^{\mathrm{ab}}$.

由导出函子的性质, 我们有

$$0\to A\to B\to C\to 0$$

正合, 则

$$\cdots\to\mathrm{H}_{q+1}(G,B)\to\mathrm{H}_{q+1}(G,C)\xrightarrow{\delta}\mathrm{H}_q(G,A)\to\mathrm{H}_q(G,B)\to\cdots$$

正合, 其中 δ 被称为连接映射.

§A.3.3 泰特上同调

我们希望将群的上同调和同调统一起来. 设 G 有限群. 记

$$\mathbf{N}=\sum_{g\in G}g\in\mathbb{Z}[G]$$

为它的范数,

$$I_G=\langle g-1\mid g\in G\rangle\subseteq\mathbb{Z}[G]$$

为增广理想. $\mathbf{N}$ 在 A 上的作用满足

$$I_GA\subseteq A^{\mathbf{N}=0}=\ker\mathbf{N},\quad \mathbf{N}A=\operatorname{im}\mathbf{N}\subseteq A^G.$$

定义泰特上同调

$$\begin{aligned}\widehat{\mathrm{H}}^n(G,A)&=\mathrm{H}^n(G,A),\quad n\geq 1\\ \widehat{\mathrm{H}}^0(G,A)&=A^G/\mathbf{N}A,\\ \widehat{\mathrm{H}}^{-1}(G,A)&=A^{\mathbf{N}=1}/I_GA,\\ \widehat{\mathrm{H}}^{-n}(G,A)&=\mathrm{H}_{n-1}(G,A),\quad n\geq 2\end{aligned}$$

则对于正合列

$$0\to A\to B\to C\to 0,$$

我们有长正合列

$$\cdots\to\widehat{\mathrm{H}}^{q-1}(G,C)\to\widehat{\mathrm{H}}^q(G,A)\to\widehat{\mathrm{H}}^q(G,B)\to\widehat{\mathrm{H}}^q(G,C)\to\widehat{\mathrm{H}}^{q+1}(G,A)\to\cdots$$

后文中我们将简记 $\mathrm{H}^n=\widehat{\mathrm{H}}^n, n\in\mathbb{Z}$.

§A.3.4 埃尔布朗商

为了计算类域的上同调, 我们需要埃尔布朗商. 设 G 有限群, A 是 G 模, 则

$$\begin{aligned}\mathrm{H}^0(G,A) &= A^G/\mathbf{N}A,\\ \mathrm{H}^{-1}(G,A) &= A^{\mathbf{N}=1}/I_G A,\\ \mathrm{H}^1(G,A) &= Z^1/B^1,\end{aligned}$$

其中

$$\begin{aligned}Z^1 &:= \left\{f : G \to A \mid f(gh) = f(g)^h f(h)\right\},\\ B^1 &:= \left\{f_a : G \to A \mid f_a(g) = a^{g-1}, a \in A\right\}.\end{aligned}$$

命题 A.43

如果 $G = \langle\sigma\rangle$ 是循环群, 则 $\mathrm{H}^1(G,A) = \mathrm{H}^{-1}(G,A)$. 对于 G 模的正合列

$$1 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 1$$

我们有正合六边形

$$\begin{tikzcd}
 & \mathrm{H}^0(G,A) \arrow[r, "f_1"] & \mathrm{H}^0(G,B) \arrow[dr, "f_2"] & \\
\mathrm{H}^{-1}(G,C) \arrow[ur, "f_6"] & & & \mathrm{H}^0(G,C) \arrow[dl, "f_3"] \\
 & \mathrm{H}^{-1}(G,B) \arrow[ul, "f_5"] & \mathrm{H}^{-1}(G,A) \arrow[l, "f_4"'] &
\end{tikzcd}$$

该命题可以利用此情形下泰特上同调和复形

$$\cdots \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\mathbf{N}} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\mathbf{N}} \mathbb{Z}[G] \xrightarrow{\sigma-1} \cdots$$

的上同调一致得到, 见 [18, §8.4]. 由此可知 $\mathrm{H}^n(G,A)$ 只与 n 的奇偶性有关, 从而由上同调的长正合列得到该命题. 也可以直接证明, 见 [15, Proposition 4.3.7, Proposition 4.7.1], 其中 $f_3(c) = \left(j^{-1}(c)\right)^{\sigma-1}$, $f_6(c) = \mathbf{N}\left(j^{-1}(c)\right)$.

✍ **练习 A.3.5** 验证 f_3, f_6 是良定义的, 并由此证明该命题.

定义 A.44 (埃尔布朗商)

定义

$$h(G,A) = \frac{\#\mathrm{H}^0(G,A)}{\#\mathrm{H}^{-1}(G,A)}$$

为 A 的埃尔布朗商. 这里它只在两个上同调都有限的情形才有定义.

由正合六边形,

$$0 \to \mathrm{Im}\, f_6 \to \mathrm{H}^0(G,A) \to \mathrm{Im}\, f_1 \to 0$$

正合, 因此 $\#\mathrm{H}^0(G,A) = \#\mathrm{Im}\, f_6 \cdot \#\mathrm{Im}\, f_1$. 类似地, 对其它上同调也有这样的形式, 因此

$$h(G,B) = h(G,A)h(G,C).$$

✍ **练习 A.3.6** 证明有限模的埃尔布朗商是 1.

命题 A.45

如果 G 是有限循环群, 则

$$\mathrm{H}^i(G, \mathrm{Ind}_G^H B) \cong \mathrm{H}^i(H, B).$$

证明 设 $A = \mathrm{Ind}_G^H B$. 设 R 是 G/H 的一组代表元. 考虑 H 模同态

$$\pi : A \to B, \quad f \mapsto f(1),$$
$$\nu : A \to B, \quad f \mapsto \prod_{\tau \in R} f(\tau).$$

容易看出

$$s : B \to A, \quad b \mapsto f_b(h) = \begin{cases} b^h, & \text{如果} h \in H, \\ 1, & \text{如果} h \notin H \end{cases}$$

满足 $\pi \circ s = \nu \circ s = \mathrm{id}$. 我们还有

$$\pi \circ \mathbf{N}_G = \mathbf{N}_H \circ v.$$

很明显, π 诱导了同构 $A^G \to B^H$, 而且

$$\pi(\mathbf{N}_G A) = \mathbf{N}_H(\nu A) \subseteq \mathbf{N}_H B, \ \mathbf{N}_H B = \mathbf{N}_H(\nu s B) = \pi\big(\mathbf{N}_G(sB)\big) \subseteq \pi(\mathbf{N}_G A).$$

因此 $\mathrm{H}^0(G, A) = \mathrm{H}^0(H, B)$. $i = -1$ 情形留作习题. □

✍ **练习 A.3.7** 证明 G 是有限循环群时, $\mathrm{H}^{-1}(G, \mathrm{Ind}_G^H B) \cong \mathrm{H}^{-1}(H, B)$.

✍ **练习 A.3.8** 如果 G 是有限群, H 是正规子群, 则 $\mathrm{H}^1(G, \mathrm{Ind}_G^H B) \cong \mathrm{H}^1(H, B)$.

参考文献

[1] A. Baker. “Linear forms in the logarithms of algebraic numbers. I, II, III”. In: *Mathematika* 13 (1966), 204–216, ibid. 14 (1967), 102–107, ibid. 14 (1967), 220–228. ISSN: 0025-5793. DOI: 10.1112/s0025579300003843. URL: https://doi.org/10.1112/s0025579300003843.

[2] I. S. Cohen. “On the structure and ideal theory of complete local rings”. In: *Trans. Amer. Math. Soc.* 59 (1946), pp. 54–106. ISSN: 0002-9947. DOI: 10.2307/1990313. URL: https://doi.org/10.2307/1990313.

[3] Pierre Colmez. *Fontaine’s rings and p-adic L-functions*. Notes from a course given at Tsinghua University. 2004. URL: http://staff.ustc.edu.cn/~yiouyang/colmez.pdf.

[4] 冯克勤, 李尚志, 章璞. 近世代数引论. 3 版. 中国科学技术大学精品教材. 中国科学技术大学出版社, 2009, p. 186. ISBN: 978-7-312-02292-0.

[5] Jean-Marc Fontaine. “Il n’y a pas de variété abélienne sur **Z**”. In: *Invent. Math.* 81.3 (1985), pp. 515–538. ISSN: 0020-9910. DOI: 10.1007/BF01388584. URL: https://doi.org/10.1007/BF01388584.

[6] Jean-Marc Fontaine and Yi Ouyang. *Theory of p-adic Galois representations*. second draft, a book in preparation. 2021. URL: http://staff.ustc.edu.cn/~yiouyang/galoisrep.pdf.

[7] Dorian Goldfeld. “Gauss’s class number problem for imaginary quadratic fields”. In: *Bull. Amer. Math. Soc. (N.S.)* 13.1 (1985), pp. 23–37. ISSN: 0273-0979. DOI: 10.1090/S0273-0979-1985-15352-2. URL: https://doi.org/10.1090/S0273-0979-1985-15352-2.

[8] Benedict H. Gross and Don B. Zagier. “Heegner points and derivatives of L-series”. In: *Invent. Math.* 84.2 (1986), pp. 225–320. ISSN: 0020-9910. DOI: 10.1007/BF01388809. URL: https://doi.org/10.1007/BF01388809.

[9] 加藤和也, 黑川信重, and 斋藤毅. *数论 I——Fermat 的梦想和类域论*. Chinese. Vol. 12. 现代数学基础. 胥鸣伟, 印林生译. 高等教育出版社, 2009, p. 298. ISBN: 978-7-04-026360-2.

[10] 黑川信重, 栗原将人, and 斋藤毅. *数论 II——岩泽理论和自守形式*. Chinese. Vol. 13. 现代数学基础. 印林生, 胥鸣伟译. 高等教育出版社, 2009, p. 180. ISBN: 978-7-04-026361-9.

[11] Serge Lang. *Algebraic number theory*. Second. Vol. 110. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+357. ISBN: 0-387-94225-4. DOI: 10.1007/978-1-4612-0853-2. URL: https://doi.org/10.1007/978-1-4612-0853-2.

[12] Serge Lang. *Cyclotomic fields I and II*. second. Vol. 121. Graduate Texts in Mathematics. With an appendix by Karl Rubin. Springer-Verlag, New York, 1990, pp. xviii+433. ISBN: 0-387-96671-4. DOI: 10.1007/978-1-4612-0987-4. URL: https://doi.org/10.1007/978-1-4612-0987-4.

[13] 李文威. *模形式初步*. Chinese. 现代数学基础丛书. 科学出版社, 2020, p. 382. ISBN: 978-7-030-64531-9. URL: https://www.wwli.asia/downloads/books/Modulform.pdf.

[14] R. A. Mollin and H. C. Williams. "On a determination of real quadratic fields of class number one and related continued fraction period length less than 25". In: *Proc. Japan Acad. Ser. A Math. Sci.* 67.1 (1991), pp. 20–25. ISSN: 0386-2194. URL: http://projecteuclid.org/euclid.pja/1195512263.

[15] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. ISBN: 3-540-65399-6. DOI: 10.1007/978-3-662-03983-0. URL: https://doi.org/10.1007/978-3-662-03983-0.

[16] O. Timothy O'Meara. *Introduction to quadratic forms*. Classics in Mathematics. Reprint of the 1973 edition. Springer-Verlag, Berlin, 2000, pp. xiv+342. ISBN: 3-540-66564-1.

[17] Alain M. Robert. *A course in p-adic analysis*. Vol. 198. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, pp. xvi+437. ISBN: 0-387-98669-3. DOI: 10.1007/978-1-4757-3254-2. URL: https://doi.org/10.1007/978-1-4757-3254-2.

[18] Jean-Pierre Serre. *Local fields*. Vol. 67. Graduate Texts in Mathematics. Translated from the French by Marvin Jay Greenberg. Springer-Verlag, New York-Berlin, 1979, pp. viii+241. ISBN: 0-387-90424-7.

[19] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

[20] H. M. Stark. "A complete determination of the complex quadratic fields of class-number one". In: *Michigan Math. J.* 14 (1967), p. 27. ISSN: 0026-2285. URL: http://projecteuclid.org/euclid.mmj/1028999653.

[21] Richard Taylor and Andrew Wiles. "Ring-theoretic properties of certain Hecke algebras". In: *Ann. of Math. (2)* 141.3 (1995), pp. 553–572. ISSN: 0003-486X. DOI: 10.2307/2118560. URL: https://doi.org/10.2307/2118560.

[22] Andrew Wiles. "Modular elliptic curves and Fermat's last theorem". In: *Ann. of Math. (2)* 141.3 (1995), pp. 443–551. ISSN: 0003-486X. DOI: 10.2307/2118559. URL: https://doi.org/10.2307/2118559.

[23] Oscar Zariski and Pierre Samuel. *Commutative algebra, Volume I*. The University Series in Higher Mathematics. With the cooperation of I. S. Cohen. D. Van Nostrand Company, Inc., Princeton, New Jersey, 1958, pp. xi+329.

中外人名对照表

阿贝尔	Niels Henrik Abel, 1802–1829
阿基米德	Ἀρχιμήδης, 公元前 287–前 212
埃尔布朗	Jacques Herbrand, 1908–1931
艾森斯坦	Ferdinand Gotthold Max Eisenstein, 1823–1852
奥斯特洛斯基	Олександр Маркович Островський, 1893–1986
贝克	Alan Baker, 1939–2018
伯奇	Bryan John Birch, 1931–
泊松	Siméon Denis Poisson, 1781–1840
戴德金	Julius Wilhelm Richard Dedekind, 1831–1916
狄利克雷	Johann Peter Gustav Lejeune Dirichlet, 1805–1859
法尔廷斯	Gerd Faltings, 1954–
方丹	Jean-Marc Fontaine, 1944–2019
费马	Pierre de Fermat, 1601–1665
傅里叶	Jean-Baptiste Joseph Fourier, 1768–1830
弗罗贝尼乌斯	Ferdinand Georg Frobenius, 1849–1917
伽罗瓦	Évariste Galois, 1811-1832
高斯	Johann Carl Friedrich Gauß, 1777–1855
谷山丰	谷山豊, 1927–1953
哈尔	Alfréd Haar, 1885–1933
哈塞	Helmut Hasse, 1898–1979
豪斯多夫	Felix Hausdorff, 1868–1942
赫克	Erich Hecke, 1887–1947
亨泽尔	Kurt Hensel, 1861–1941
怀尔斯	Sir Andrew John Wiles, 1953–
克拉斯纳	Marc Krasner, 1912–1985
克鲁尔	Wolfgang Krull, 1899–1971
克罗内克	Leopold Kronecker, 1823–1891
柯西	Augustin-Louis Cauchy, 1789–1857
库默尔	Ernst Eduard Kummer, 1810–1893
莱布尼茨	Gottfried Wilhelm Freiherr von Leibniz, 1646–1716
勒让德	Adrien-Marie Legendre, 1752–1833
黎曼	Georg Friedrich Bernhard Riemann, 1826–1866
卢宾	Jonathan Darby Lubin, 1936–
闵可夫斯基	Hermann Minkowski, 1864–1909
默比乌斯	August Ferdinand Möbius, 1790–1868

牛顿	Sir Isaac Newton, 1643–1727
诺特	Amalie Emmy Noether, 1882–1935
欧拉	Leonhardus Eulerus, 1707–1783
庞特里亚金	Лев Семёнович Понтря́гин, 1908–1988
佩尔	John Pell, 1611–1685
切博塔廖夫	Мико́ла Григо́рович Чеботарьо́в, 1894–1947
塞尔	Jean-Pierre Serre, 1926–
施瓦兹	Laurent-Moïse Schwartz, 1915–2002
斯温纳顿-戴尔	Sir Henry Peter Francis Swinnerton-Dyer, 1927–2018
沙法列维奇	И́горь Ростисла́вович Шафаре́вич, 1923–2017
泰勒	Brook Taylor, 1685–1731
泰特	John Torrence Tate, 1925–2019
泰希米勒	Paul Julius Oswald Teichmüller, 1913–1943
韦伯	Wilhelm Eduard Weber, 1804–1891
魏尔斯特拉斯	Karl Theodor Wilhelm Weierstraß, 1815–1897
维特	Ernst Witt, 1911–1991
韦伊	André Weil, 1906–1998
希尔伯特	David Hilbert, 1862–1943
伯努利	Jacques Bernoulli, 1654–1705
岩泽健吉	岩澤健吉, 1917–1998
志村五郎	志村五郎, 1930–2019