



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9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

前言	i
第一章 代数整数	1
1.1 域扩张的线性结构	1
1.1.1 迹和范数	1
1.1.2 判别式	4
1.2 数域的整数环	6
1.2.1 整性	6
1.2.2 整基	7
1.2.3 无穷素位	9
1.2.4 分圆域的整数环	10
1.3 理想	13
1.3.1 唯一分解性	13
1.3.2 单位群和理想类群	15
1.3.3 局部化	16
1.3.4 佩尔方程	17
1.4 闵可夫斯基理论	17
1.4.1 格	18
1.4.2 闵可夫斯基空间	19
1.4.3 类群有限性	20
1.4.4 狄利克雷单位定理	22
1.5 二元二次型	25
1.5.1 等价类	25
1.5.2 表整数	27
1.5.3 与理想类群的联系	28
第二章 赋值与分歧理论	31
2.1 赋值	31
2.1.1 赋值和非阿赋值	31
2.1.2 等价赋值	32
2.1.3 完备化	34
2.2 完备离散赋值域	36
2.2.1 离散赋值	36
2.2.2 维特向量	39
2.2.3 乘法群的结构	41
2.2.4 二次曲线的有理点	42
2.2.5 有理数域上的希尔伯特符号	43

2.3 分歧理论	45
2.3.1 赋值的延拓	45
2.3.2 p 进代数闭完备域	47
2.3.3 非分歧扩张	49
2.3.4 温分歧扩张	50
2.4 整体域上的分歧理论	51
2.4.1 赋值的分歧	51
2.4.2 伽罗瓦扩张中的分歧	54
2.4.3 高阶分歧群	58
2.4.4 共轭差积和判别式	61
第三章 类域论	67
3.1 抽象类域论	67
3.1.1 射影有限群	67
3.1.2 抽象伽罗瓦理论	69
3.1.3 抽象分歧理论	69
3.1.4 互反射射	71
3.1.5 互反律	76
3.2 局部类域论	78
3.2.1 局部互反律	78
3.2.2 阿贝尔扩域	81
3.2.3 卢宾-泰特形式群	83
3.2.4 希尔伯特符号	86
3.3 整体类域论	88
3.3.1 阿代尔和伊代尔	89
3.3.2 域扩张中的伊代尔	90
3.3.3 整体域的埃尔布朗商	92
3.3.4 整体互反律	94
3.3.5 整体类域	97
3.3.6 希尔伯特符号的整体性质	100
第四章 L 函数	103
4.1 黎曼 ζ 函数和狄利克雷 L 函数	103
4.1.1 狄利克雷特征	103
4.1.2 解析延拓和函数方程	105
4.1.3 特殊值	107
4.2 戴德金 ζ 函数与赫克 L 函数	109
4.2.1 泰特的方法	109
4.2.2 解析延拓与函数方程	112
4.2.3 分圆域的 ζ 函数	113

4.2.4 二次域解析类数公式	114
4.3 模形式	115
4.3.1 庞加莱上半平面	115
4.3.2 同余子群	115
4.3.3 模形式	116
4.3.4 尖形式的 L 函数	118
4.4 椭圆曲线	121
4.4.1 代数曲线的亏格	121
4.4.2 椭圆曲线等分点	122
4.4.3 椭圆曲线的 L 函数	123
4.5 尖形式与椭圆曲线	125
4.5.1 紧黎曼面	125
4.5.2 模函数	126
4.5.3 从尖形式到椭圆曲线	127
4.5.4 模性	128
附录 A 同调代数初步	129
A.1 模	129
A.1.1 模和模同态	129
A.1.2 直和和自由模	131
A.1.3 诱导模	131
A.2 范畴	132
A.2.1 范畴与函子	132
A.2.2 加性范畴	134
A.2.3 阿贝尔范畴	136
A.2.4 正合列	137
A.2.5 正向极限和逆向极限	138
A.2.6 复形	139
A.2.7 导出函子	139
A.3 群的上同调	140
A.3.1 上同调群	140
A.3.2 同调群	142
A.3.3 泰特上同调	143
A.3.4 埃尔布朗商	143
参考文献	147

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. 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) 的迹和范数^a, 记为 $\text{Tr}_{L/K}(\alpha)$ 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

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

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

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

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

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 $\text{Tr}_{L/K}$ 和 $\mathbf{N}_{L/K}$.

固定一个 K 的代数闭包 \bar{K} . 我们记 $\text{Hom}_K(L, \bar{K})$ 为保持 K 不变的嵌入 $\tau : L \hookrightarrow \bar{K}$ 全体. 元素 $\alpha \in L^\times$ 的极小多项式是指多项式环 $K[X]$ 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.

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 $X^p - t = (X - t^{1/p})^p$.

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 $L \hookrightarrow \bar{K}$, 因此 $\text{Hom}_K(L, \bar{K})$ 的大小为 n .

命题 1.2

对于有限可分扩张 L/K , 我们有

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



证明 见 [15, Chapter I, Proposition 2.6]. 对于 $\alpha \in L$,

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

为 α 的极小多项式, 因此 $\{1, \alpha, \dots, \alpha^{m-1}\}$ 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

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

从而

$$\begin{aligned} \text{Tr}_{K(\alpha)/K}(\alpha) &= -a_{m-1} = \sum_{\tau \in \text{Hom}_K(K(\alpha), \bar{K})} \tau\alpha, \\ \mathbf{N}_{K(\alpha)/K}(\alpha) &= (-1)^m a_0 = \prod_{\tau \in \text{Hom}_K(K(\alpha), \bar{K})} \tau\alpha. \end{aligned}$$

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].

考虑 $\text{Hom}_K(L, \bar{K})$ 上等价关系: $\sigma \sim \tau \iff \sigma\alpha = \tau\alpha$. 这等价于 $\sigma^{-1}\tau \in \text{Hom}_{K(\alpha)}(L, \bar{K})$, 因此每个等价类大小均为 $d = [L : K(\alpha)]$, 共 m 个等价类. 设 τ_1, \dots, τ_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

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

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

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

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 $\text{Tr}_{K/\mathbb{Q}}(\zeta + \bar{\zeta})$ 和 $\mathbf{N}_{K/\mathbb{Q}}(\zeta + \bar{\zeta})$.

🔴 **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

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



证明 见 [23, Chapter II, §10]. 假设 M/K 可分. 考虑 $\text{Hom}_K(M, \bar{K})$ 上的等价关系: $\sigma \sim \tau \iff \sigma|_L = \tau|_L$. 这等价于 $\sigma^{-1}\tau \in \text{Hom}_L(M, \bar{K})$, 因此每个等价类大小均为 $[M : L]$, 共 $m = [L : K]$ 个等价类. 设 τ_1, \dots, τ_m 为这些等价类的一组代表元, 则 $\text{Hom}_K(L, \bar{K}) = \{\tau_i|_L : 1 \leq i \leq m\}$. 于是

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

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 $\text{Hom}_K(L, \bar{K}) = \text{Hom}_K(K^s, \bar{K})$, 于是

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

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 $\text{char}K > 0$ 的正整数次幂, 因此我们有 $\text{Tr}_{L/K} = 0$. 反之亦然.

命题 1.4 (嵌入的线性无关性)

设 $\text{Hom}_K(L, \bar{K}) = \{\tau_1, \dots, \tau_n\}$, 则 τ_1, \dots, τ_n 在 \bar{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 $\sum_{i=1}^d c_i \tau_i = 0, c_i \in \bar{K}^\times$, 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 $\alpha_1, \dots, \alpha_n \in L$ 关于 L/K 的判别式为

$$\text{disc}_{L/K}(\alpha_i)_i = \text{disc}_{L/K}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{L/K}(\alpha_i \alpha_j))_{ij}.$$



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 $\text{Hom}_K(L, \overline{K}) = \{\tau_1, \dots, \tau_n\}$, 则

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

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

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



证明

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

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

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

(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 $\text{disc}_{L/K}(\alpha_i)_i \neq 0$.

(2) K 上的双线性型

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

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



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

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

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 $\text{disc}_{L/K}(1, \theta, \dots, \theta^{n-1}) \neq 0$. 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 $\text{disc}_{L/K}(\alpha_i)_i \neq 0$. 由于双线性型 $\text{Tr}_{L/K}(xy)$ 在基 $(\alpha_i)_i$ 下的矩阵是 $(\text{Tr}_{L/K}(\alpha_i \alpha_j))_{ij}$, 它的行列式非零, 因此 $\text{Tr}_{L/K}(xy)$ 非退化. \square

由于迹配对非退化, 因此它诱导了自然同构

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

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 $\text{Tr}_{L/K}$ 的对偶基.



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

$$(\alpha_1^\vee, \dots, \alpha_n^\vee) = (\alpha_1, \dots, \alpha_n) (\text{Tr}_{L/K}(\alpha_i \alpha_j))_{ij}^{-1}.$$

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

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



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

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

由

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

知该命题成立. \square

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



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 $A[b] = A + Ab + \dots + Ab^{n-1}$. 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 $M = \sum_{i=1}^m Aa_i$. 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 $A[b_1 + b_2], A[b_1 b_2] \subseteq A[b_1, b_2]$ 也是有限生成的, 因此 $b_1 + b_2, b_1 b_2$ 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.



命题 1.13

设 A 是整闭整环, $K = \text{Frac } A$ 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 $p(X) \in A[X]$. \square

练习 1.2.2

- (1) 设 \bar{A} 是 A 在 B 中的整闭包, 则 \bar{A} 在 B 中的整闭包是 \bar{A} .
- (2) 如果 B 在 A 上代数, 则 B 的分式域等于 \bar{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** \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**.



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 $b \in \frac{1}{2} + \mathbb{Z}$, $d \equiv 1 \pmod{4}$. 故

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

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 $\text{Tr}_{K/\mathbb{Q}}$ 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

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

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 $|M^\vee/M| = |\text{disc}(\alpha_i)_i|, |M/dM| = d^n$ 均有限, 因此 \mathfrak{a} 是一个秩 n 自由交换群. \square

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**.

命题 1.16

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



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

定义 1.17 (理想的判别式)

\mathfrak{a} 的**判别式** $\Delta_{\mathfrak{a}} \in \mathbb{Z}$ 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 $d \equiv 1 \pmod{4}$ 时 $\Delta_{\mathbb{Q}(\sqrt{d})} = d$; 当 $d \equiv 2, 3 \pmod{4}$ 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 $\text{disc}(\alpha_i)_i$ 生成的理想, 其中 $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$. 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 2.4.4 小节研究它的性质.

引理 1.18 (整基判定准则)

设 $\beta_1, \dots, \beta_n \in \mathfrak{a}$ 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 $p^2 \mid \text{disc}(\beta_i)_i$ 和 $\sum_{i=1}^n x_i \beta_i \in p\mathfrak{a}, 0 \leq x_i \leq p-1, \forall i$, 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 $p^2 \mid \text{disc}(\beta_1, \dots, \beta_n) = \det(C)^2 \Delta_{\mathfrak{a}}$. 设 $\bar{C} \in M_n(\mathbb{F}_p)$ 为 C 模 p , 则存在非零列向量 $(\bar{x}_1, \dots, \bar{x}_n)^T \in \mathbb{F}_p^n$ 满足 $\bar{C}(\bar{x}_1, \dots, \bar{x}_n)^T = 0$. 设 $x_i \in \{0, 1, \dots, p-1\}$ 为 \bar{x}_i 的提升, 则

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

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

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

证明 由于 $\{\alpha^i\}_{0 \leq i \leq n-1}$ 和 $\{(\alpha+k)^i\}_{0 \leq i \leq n-1}$ 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 $\{1, \alpha, \dots, \alpha^{n-1}\}$ 不构成一组整基, 则存在素数 p 满足 $p^2 \mid \text{disc}(\alpha^i)$, 且存在不全为 p 的倍数的 x_i 满足 $x := \frac{1}{p} \sum_{i=0}^{n-1} x_i \alpha^i \in \mathcal{O}_K$. 不妨设

$0 \leq x_i \leq p-1$. 令 $j = \min \{i \mid x_i \neq 0\}$, 则

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

注意到

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

展开后为 α 的共轭元 $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$ 的初等对称函数的多项式, 且常数项为 x_j^n . 由于 $p \mid a_0, \dots, a_{n-1}$, 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 $1, \alpha, \dots, \alpha^{n-1}$ 构成一组整基. \square

例题 1.3 设 $K = \mathbb{Q}(\alpha), \alpha^3 = 2$. 则 $\text{disc}(1, \alpha, \alpha^2) = -2^2 3^3$. 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

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

又因为 $f(T+1) = T^{p-1} + \sum_{i=1}^{p-1} \binom{p}{i} T^{i-1}$ 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 $\Delta_K \equiv 0, 1 \pmod{4}$. 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 $\sigma \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, 容易看出, $\bar{\sigma} : K \xrightarrow{\sigma} \mathbb{C} \xrightarrow{\text{复共轭}} \mathbb{C}$ 也是一个嵌入.

定义 1.20 (无穷素位)

- (1) 称 σ 为**无穷素位**. 如果 $\sigma(K) \subseteq \mathbb{R}$, 即 $\bar{\sigma} = \sigma$, 称 σ 为**实嵌入**或**实素位**, 否则称之为**复嵌入**或**复素位**. 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**; 如果 K 没有实素位, 称 K 为**全虚域**.



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

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

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

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

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

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

□

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 $d \neq 0, 1$ 为无平方因子整数.
- (2) 分圆域 $\mathbb{Q}(\zeta)$, 其中 $\zeta = e^{2\pi i/n}, n \geq 3$ 为正整数.
- (3) 三次域 $\mathbb{Q}(\gamma)$.

§1.2.4 分圆域的整数环

设 $N \geq 3, \zeta_N \in \mathbb{C}$ 是 N 次本原单位根, 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 $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$.



证明 $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ 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 $\varphi: \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$.

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 $\zeta, f(T) \mid g(T^p)$. 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 $\alpha \in \mathbb{F}_p$ 是 \bar{f} 的一个根, 则 $\bar{g}(\alpha) = 0, \alpha$ 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

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

为 N 次分圆多项式. 它是 ζ_N 的极小多项式, 且

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

由默比乌斯反演²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

$$\text{disc}(1, \zeta_N, \dots, \zeta_N^{N-1}) \mid N^{\varphi(N)},$$

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

由于

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

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 $\mathbb{Z}[\zeta_{p^n}]$. □

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 $K \otimes_{\mathbb{Q}} L \rightarrow KL$ 是同构. 设 $(\alpha_1, \dots, \alpha_n)$ 和 $(\beta_1, \dots, \beta_m)$ 分别是 K 和 L 的一组整基, 则 \mathcal{O}_{KL} 中的任一元素可表为

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

²默比乌斯反演是指

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

其中默比乌斯函数

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

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 $\Delta_K x \alpha_i^\vee \in \mathcal{O}_{KL}$, 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, \dots, w_n 为 K 的一组整基, v_1, \dots, v_m 为 L 的一组整基, 则 $\{w_i v_j\}_{ij}$ 为 KL 的一组整基. 设 τ_1, \dots, τ_n 为所有嵌入 $K \hookrightarrow \overline{\mathbb{Q}}$, $\sigma_1, \dots, \sigma_m$ 为所有嵌入 $L \hookrightarrow \overline{\mathbb{Q}}$, $a_{ik} = \tau_i(w_k), b_{j\ell} = \sigma_j(v_\ell)$, 则

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

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 $\pm p^{n-1(pn-n-1)}$, 当 $p \equiv 3 \pmod{4}$ 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, $\Phi'(\zeta_{2^n}) = 2^{n-1} \zeta_{2^n}^{2^{n-1}-1}, \mathbf{N}_{\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}}(\Phi'(\zeta_{2^n})) = 2^{2^{n-1}(n-1)}$. 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

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

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.

\mathcal{O}_K 的理想的唯一分解性来源于它是一个戴德金环.

定义 1.29 (诺特环和戴德金环)

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 $I_N = I_{N+1} = I_{N+2} = \dots$, 则我们称其为**诺特环**. 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**戴德金环**. 

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 $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots, \mathfrak{a} = \bigcup_i \mathfrak{a}_i$ 是有限生成的. 设 $\mathfrak{a} = \sum_{i=1}^r Ra_i, a_i \in \mathfrak{a}_{n_i}$, 则 $\mathfrak{a} = \mathfrak{a}_n, n = \max\{n_1, \dots, n_r\}$. 因此该升链稳定. □

定理 1.31

数域的整数环 \mathcal{O}_K 是戴德金环. 

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 $f(T) \in \mathbb{Z}[T]$

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

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. \square

定理 1.32

戴德金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 1.33 (分式理想)

设 \mathcal{O} 是戴德金环. 对于 $K = \text{Frac } \mathcal{O}$ 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. 换言之, 分式理想是 K 的有限生成非零 \mathcal{O} 子模.



定理 1.32 的证明 设 \mathcal{O} 是戴德金整环, \mathfrak{a} 是它的一个非零理想. 我们断言存在非零素理想 $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ 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 $b_1, b_2 \notin \mathfrak{a}, b_1 b_2 \in \mathfrak{a}$. 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 $\frac{a}{b}\mathfrak{p} \subseteq \frac{1}{b}\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathcal{O}$, 即 $a/b \in \mathfrak{p}^{-1}$. 因此 $\mathfrak{p}^{-1} \neq \mathcal{O}$.

易知 $\mathcal{O} \subseteq \mathfrak{p}^{-1}, \mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$. 假设 $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$, 设 $\mathfrak{p} = \sum_{i=1}^r \mathcal{O}\alpha_i$, 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 $C = (c_{ij})_{1 \leq i, j \leq n}$, 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 $I \subsetneq \mathfrak{p}$. 因此 $\mathfrak{p}^{-1}I \subsetneq \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$. 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. \square

推论 1.34

数域的整数环具有素理想唯一分解性.



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 1.35

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 设 \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. \square

推论 1.36

\mathcal{O}_K 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.



§1.3.2 单位群和理想类群

形如 $(\alpha) = \alpha \mathcal{O}_K$, $\alpha \in K^\times$ 的分式理想被称为**主分式理想**, 记 \mathcal{P}_K 为主分式理想全体. 我们有群的正合列

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

其中 \mathcal{O}_K^\times 为 K 的**单位群**, 即 \mathcal{O}_K 中全体单位, $\text{Cl}_K = \mathcal{I}_K / \mathcal{P}_K$ 为 K 的理想**类群**. 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. 显然它是 \mathcal{O}_K^\times 的极大有限子群, 且它是循环群.

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.



定理 1.38 (类群有限性定理)

数域的理想类群是有限的.



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

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

而 Goldfeld [7] 通过 Gross-Zagier 公式 [8] 找到一条特殊的椭圆曲线, 给出了类数与判别式之间的大小关系, 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, 我们已经知道很多类数为 1 的实二次域 [14], 但是否有无穷多个类数为 1 的实二次域仍然是一个猜想, 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]. 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

命题 1.39

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 $s_1 \cdots s_n x$ 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 1.39 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; $\text{Cl}_{K,S}$ 为其理想类群, 称之为 S 理想类群.

命题 1.40

我们有典范的正合列

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

其中第三个箭头是

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

$v_{\mathfrak{p}}$ 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, $\text{Cl}_{K,S}$ 由所有 $S^{-1}\mathfrak{p}$ 的理想类生成, 因此它是满射. □

由此可知:

推论 1.41

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 1.42

S 理想类群 $\text{Cl}_{K,S}$ 有限.



§1.3.4 佩尔方程

设 $K = \mathbb{Q}(\sqrt{d})$ 为实二次域, $d > 1$ 为无平方因子正整数. 则 $r = 2, s = 0$, \mathcal{O}_K^\times 秩为 1, 有限部分为 $\{\pm 1\}$, 因此存在 $\varepsilon \in \mathcal{O}_K^\times$ 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**.

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 $x^2 - dy^2 = \pm 1$ 的整数解全体, P'_d 为其正整数解全体.

命题 1.43

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

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



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 $\mathbf{N}(x) = \pm 1$. 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 $n \geq 1$, 则 $u^{\pm n} - 1 \in 2\mathcal{O}_K \subseteq \mathbb{Z}[\sqrt{d}]$, $u^n \in \mathbb{Z}[\sqrt{d}]^\times$. 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 $n \geq 2$ 时,

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

故 $\varepsilon_0 = \varepsilon$. □

👉 **练习 1.3.1** $\alpha \in \mathcal{O}_K$ 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.

👉 **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 理想.

👉 **练习 1.3.4** 设 $\mathfrak{a}, \mathfrak{b}$ 为 \mathcal{O} 的分式理想.

(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.

👉 **练习 1.3.5** 分式理想全体构成一个交换群 \mathcal{I}_K , 么元为 $(1) = \mathcal{O}_K$.

👉 **练习 1.3.6** 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 $x^2 \equiv d \pmod{p}$ 无解.

👉 **练习 1.3.7** 设 \mathcal{O} 是戴德金环, \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.

👉 **练习 1.3.8** 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} 互素的整理理想代表元.

👉 **练习 1.3.9** 初步了解类群的岩泽理论.

👉 **练习 1.3.10** $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5})$ 的基本单位分别是什么?

§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 1.6 例如 \mathbb{R} 在通常拓扑下形成拓扑域, 因为 $+, -, * : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, -x : \mathbb{R} \rightarrow \mathbb{R}, x^{-1} : \mathbb{R}^\times \rightarrow \mathbb{R}^\times$ 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, \dots, v_m 线性无关^a. 如果 $m = n$, 称之为完全格. 称

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

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, \dots, v_m 扩充为 V 的一组基 v_1, \dots, 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, \dots, 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, \dots, 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, \dots, v_m 线性无关, 从而 Λ 是一个格. \square

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)

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

此时 V 上有一个平移不变的测度(哈尔测度³). 我们规定一组正交基 $\{e_1, \dots, e_n\}$ 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

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

³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.

其中 $(v_1, \dots, v_n)^T = A(e_1, \dots, e_n)^T$.

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**.



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 $\text{vol}(X) > 2^n \text{covol}(\Lambda)$, 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

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

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

§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

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

$$a \otimes z \mapsto (\tau(a)z)_{\tau}$$

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

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

$K_{\mathbb{C}}$ 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

$$f: K_{\mathbb{R}} \longrightarrow \prod_{\tau} \mathbb{R} = \mathbb{R}^n$$

$$(z_{\tau})_{\tau} \longmapsto (x_{\tau})_{\tau} \tag{1.1}$$

是一个同构, 其中对于实嵌入 $x_{\rho} = z_{\rho}$, 对于成对的复嵌入 $x_{\sigma} = \text{Re}(z_{\sigma}), x_{\bar{\sigma}} = \text{Im}(z_{\sigma})$. 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 $\text{Tr}: K_{\mathbb{C}} \rightarrow \mathbb{C}$ 为其各分量之和, 则 $\text{Tr}_{K/\mathbb{Q}} = \text{Tr} \circ j$.

§1.4.3 类群有限性

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

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

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

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



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 $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, 则 $\mathfrak{p}^i \supseteq (a) + \mathfrak{p}^{i+1} \supseteq \mathfrak{p}^{i+1}$, 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,

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

□

因此 N 满足可乘性 $N(\mathfrak{a}\mathfrak{b}) = N\mathfrak{a} \cdot N\mathfrak{b}$, 故 $N: \mathcal{I}_K \rightarrow \mathbb{R}_+^\times$ 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, $\Delta_{\mathfrak{a}} = N\mathfrak{a}^2 \Delta_K$.



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

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



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

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

另一方面,

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

因此

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

□

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, $\{c_\tau\}_{\tau \in \text{Hom}_{\mathbb{Q}}(K, \mathbb{C})}$ 为一组正实数, 满足 $c_\tau = c_{\bar{\tau}}$. 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

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



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

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

因此它的体积

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

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 $|\mathbf{N}_{K/\mathbb{Q}}(a)| \leq M_K \mathbf{N}\mathfrak{a}$, 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

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

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

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

其中 $c = \frac{n!}{n^n 2^r \pi^s}$. 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 $|\mathbf{N}_{K/\mathbb{Q}}(a)| \leq M_K \mathbf{N}\mathfrak{a}$, 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 K 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 $\mathbf{N}\mathfrak{a} \leq M$ 的理想 \mathfrak{a} 也只有有限多个.

我们断言任意理想类 $[a]$ 都存在一个代表元 a_1 使得 $\mathbf{N}a_1 \leq M_K$. 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 $|\mathbf{N}_{K/\mathbb{Q}}(a)| \leq M_K \mathbf{N}\mathfrak{a}^{-1}$. 于是 $\mathbf{N}(a\mathfrak{a}) \leq M_K$ 且 $a\mathfrak{a} \subseteq \mathcal{O}_K, a\mathfrak{a} \in [\mathfrak{a}]$. \square

例题 1.7 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 $(3) = \mathfrak{p}_3 \bar{\mathfrak{p}}_3$. 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 $\text{Cl}_K = \langle [\mathfrak{p}_3] \rangle \cong \mathbb{Z}/4\mathbb{Z}$.

例题 1.8 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

$$\begin{array}{ccccc} K^{\times} & \xrightarrow{j} & K_{\mathbb{C}}^{\times} & \xrightarrow{\ell} & \prod_{\tau} \mathbb{R} \\ \mathbf{N}_{K/\mathbb{Q}} \downarrow & & \downarrow \mathbf{N} & & \downarrow \text{Tr} \\ \mathbb{Q}^{\times} & \longrightarrow & \mathbb{C}^{\times} & \xrightarrow{\log |\cdot|} & \mathbb{R}, \end{array}$$

其中 $\mathbf{N}: K_{\mathbb{C}}^{\times} \rightarrow \mathbb{C}^{\times}$ 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.

$$\begin{array}{ccccc} \mathcal{O}_K^{\times} & \xrightarrow{j} & S & \xrightarrow{\ell} & H \\ \downarrow & & \downarrow & & \downarrow \\ K^{\times} & \xrightarrow{j} & K_{\mathbb{R}}^{\times} & \xrightarrow{\ell} & [\prod_{\tau} \mathbb{R}]^+ \\ \mathbf{N}_{K/\mathbb{Q}} \downarrow & & \downarrow \mathbf{N} & & \downarrow \text{Tr} \\ \mathbb{Q}^{\times} & \longrightarrow & \mathbb{R}^{\times} & \xrightarrow{\log |\cdot|} & \mathbb{R}, \end{array}$$

其中

$$\begin{aligned} [\prod_{\tau} \mathbb{R}]^+ &= \{(x_{\tau}) \mid x_{\tau} = x_{\bar{\tau}}\}, \\ S &= \{y \in K_{\mathbb{R}}^{\times} \mid \mathbf{N}(y) = \pm 1\} \end{aligned}$$

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

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

是 $[\prod_{\tau} \mathbb{R}]^+$ 的一个超平面.

我们固定

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

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

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 $\mu_K \subseteq \text{Ker } \lambda$. 若 $\varepsilon \in \text{Ker } \lambda$, 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 $\ker \lambda = \mu(K)$. \square

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 $c_{\tau} = c_{\bar{\tau}}$, 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 $y \in S$,

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

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 $\alpha_1, \dots, \alpha_N \in \mathcal{O}_K$ 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 $S = \bigcup_{\varepsilon \in \mathcal{O}_K^{\times}} Tj\varepsilon$. \square

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

$\text{covol}(\lambda(\mathcal{O}_K^\times)) = \sqrt{r+s}R$, 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 1.9 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 $\text{covol}(\Lambda) = \sqrt{|\det(\langle v_i, v_j \rangle)_{i,j}|}$ 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 $\text{vol}(X) = 2^n \text{covol}(\Lambda)$, 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 $\mathbf{N}((a)) = |\mathbf{N}_{K/\mathbb{Q}}(a)|, \forall a \in K^\times$.

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

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

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 $\text{vol}(X) = 2^r \pi^s \frac{t^{r+s}}{r!}$.

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 $\gamma = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$, 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 $\gamma \in \text{SL}_2(\mathbb{Z})$ 使得 G 的关联矩阵为 $\gamma^T Q \gamma$. 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 $|b| \leq |a| \leq |c|$.



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 $|b' + 2ah| \leq |a|$. 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 $|c| \geq |a|$. \square

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. \square

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

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

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 $(x, y) = \pm(1, -\text{sgn}(b))$ 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 $\gamma \in \text{SL}_2(\mathbb{Z})$ 使得

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

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

例题 1.10 列出 $-D \leq 12$ 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 $F(u, v) = n$. \square

命题 1.65

设 $n \neq 0$ 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 $D \equiv \pm 1 \pmod{8}$).



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 $D \equiv b^2 \pmod{4n}$, 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 $D \equiv 0, 1 \pmod{4}$ 知 D 模 $4n'$ 是平方; 如果 n' 是偶数, 由 $\left(\frac{D}{2}\right) = 1$ 知 $D \equiv 1 \pmod{8}$, 从而 D 模 $4n'$ 也是平方. 因此 n' 被 F 真表出, 从而 n 被 F 表出. \square

例题 1.11 设 $D = -8$, 则对应的正定既约二元二次型只有 $x^2 + 2y^2$. 由于 $\left(\frac{-2}{p}\right) = -1 \iff p \equiv 5, 7 \pmod{8}$, 因此正整数 n 可被 $x^2 + 2y^2$ 表出当且仅当 $p \equiv 5, 7 \pmod{8}$ 在 n 中的幂次为偶数.

例题 1.12 正整数 n 被 $x^2 + 5y^2$ 表出当且仅当

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

(2) 素数 $p \equiv 2, 3, 7 \pmod{20}$ 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

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

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

只能被 g 表出. 此外, 2 只能被 g 表出, 5 只能被 f 表出. 故 $p \equiv 1, 5, 9 \pmod{20}$ 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

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

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

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

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 $\text{Cl}_K^+ = \text{Cl}_K$; 如果 $D > 0$, 我们有正合列⁴

$$1 \rightarrow \mathcal{P}_K / \mathcal{P}_K^+ \rightarrow \text{Cl}_K^+ \rightarrow \text{Cl}_K \rightarrow 1.$$

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 $[\mathfrak{a}] \in \text{Cl}_K^+$.



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

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

⁴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

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

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 $f_{\alpha\omega_1, \alpha\omega_2} = f_{\omega_1, \omega_2}$. \square

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.

- $D \equiv 0 \pmod{4}$. 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

$$\frac{\sqrt{d}}{2}(1, \tau) = \pm(1, \tau) \begin{pmatrix} -b/2 & -c \\ a & -b/2 \end{pmatrix}.$$

- $D \equiv 1 \pmod{4}$. 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.

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

$$\mathbf{N}_{K/\mathbb{Q}}(\omega_1 x + \omega_2 y) = \mathbf{N}\mathfrak{b}(ax^2 + bxy + cy^2).$$

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 $\omega_2 = \tau\omega_1$, $\mathfrak{b} = (\omega_1)\mathfrak{a}$. \square

注 (1) 任意二元二次型的判别式均可唯一写成 $D = f^2 D_K$ 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 2.2.5 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 $\gamma^T Q \gamma$.

(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;
- $D \equiv 1 \pmod{4}$ 或 $D/4 \equiv 2, 3 \pmod{4}$.

👉 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).

第二章 赋值与分歧理论

内容提要

□ 赋值的定义 2.2

□ 局部分歧理论 2.3

□ 完备离散赋值域的结构 2.18, 2.21

□ 整体分歧理论 2.4



问题

设 K 为数域, $f(x_1, \dots, x_n)$ 为 K 系数次数不大于 2 的多项式. 如何判断方程 $f(x_1, \dots, x_n) = 0$ 在 K 中是否有解?



哈塞-闵可夫斯基定理告诉我们, $f(x_1, \dots, x_n) = 0$ 在 K 中有解当且仅当, 对于 K 的每个赋值 v , $f(x_1, \dots, x_n) = 0$ 在 K_v 中有解. 本章中, 我们将研究赋值的一般性质, 以及赋值在数域扩张中的变化行为.

§2.1 赋值

§2.1.1 赋值和非阿赋值

我们先来了解一般的赋值理论.

定义 2.1

全序交换群 Γ 指的是一个交换群 Γ , 其上有一个全序关系 $<$, 满足 $x < y \implies xz < yz$. 我们可以自然定义出 $\Gamma \cup \{0\}$ 上的乘法和全序: $x \cdot 0 = 0 = 0 \cdot x, 0 < x$.



👉 **练习 2.1.1** 全序交换群中没有非平凡有限阶元.

定义 2.2 (赋值)

如果域 K 上的函数 $|\cdot|: K \rightarrow \mathbb{R}_{\geq 0}$ 满足

- (1) $|x| = 0$ 当且仅当 $x = 0$;
- (2) $|xy| = |x| \cdot |y|, \forall x, y \in K$;
- (3) (三角不等式) $|x + y| \leq |x| + |y|, \forall x, y \in K$,

我们称 $|\cdot|$ 为 K 上的一个(乘性)赋值, 称 $(K, |\cdot|)$ 为赋值域. 如果 $|\cdot|$ 满足

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

则称之为非阿赋值; 否则称之为阿基米德赋值. 一般的(非阿)赋值值域可以是任意全序乘法交换群并上 0.



👉 **练习 2.1.2** 若 ζ 是 K 中的一个单位根, 则 $|\zeta| = 1$.

👉 **练习 2.1.3** 设 $|\cdot|$ 是一个非阿赋值.

- (1) 如果 $|x| \neq |y|$, 则 $|x + y| = \max\{|x|, |y|\}$.
- (2) $||x| - |y|| \leq |x - y|$.

实数域和复数域上的通常绝对值均为阿基米德赋值. 阿基米德赋值实际上等价于满足阿基米德定

理的赋值: 对于任意 $c > 0$ 和非零 x , 存在充分大的 n 使得 $|nx| > c$. 如果 $|\cdot|$ 非阿, 则 $|nx| = |x + \cdots + x| \leq |x|$ 有界; 反之, 若存在 $c > 0$ 使得 $|n| < c, \forall n \in \mathbb{Z}$,

$$\begin{aligned} |(x+y)^n| &= \left| \sum_{i=0}^n \binom{n}{i} x^i y^{n-i} \right| \leq (n+1)c \max_i \{|x|^i |y|^{n-i}\} \\ &\leq (n+1)c \max\{|x|, |y|\}^n, \end{aligned}$$

因此 $|x+y| \leq ((n+1)c)^{1/n} \max\{|x|, |y|\}$. 令 $n \rightarrow +\infty$ 可知 $|\cdot|$ 为非阿赋值.

记 Γ' 为和 Γ 相同的群, 但我们把群运算写成加法, 么元写成 0 , 序与 Γ 相反. 我们可以自然定义出 $\Gamma' \cup \{\infty\}$ 上的加法和全序: $x + \infty = \infty = \infty + x, x < \infty$. 因此非阿赋值有相应的加性版本.

定义 2.3 (加性赋值)

设 Γ 是全序加法交换群. 如果域 K 上的函数 $v: K \rightarrow \Gamma \cup \{\infty\}$, 满足

- (1) $v(x) = \infty$ 当且仅当 $x = 0$;
- (2) $v(xy) = v(x) + v(y), \forall x, y \in K$;
- (3) $v(x+y) \geq \min\{v(x), v(y)\}, \forall x, y \in K$.

则称之为加性赋值.



加性赋值和非阿赋值之间是一一对应的. 对于 $\Gamma = \mathbb{R}_{>0}$, 我们可以更直接地通过映射 $\log_a: \mathbb{R}_{>0} \rightarrow \mathbb{R}$ 构造二者之间的对应, 这里 $0 < a < 1$.

练习 2.1.4 设 \mathfrak{p} 是数域 K 的素理想, 定义 $v_{\mathfrak{p}}(x)$ 为 (x) 素理想分解中 \mathfrak{p} 的幂次, 则 $v_{\mathfrak{p}}$ 是加性赋值, $|\cdot|_{\mathfrak{p}} = \mathbf{N}\mathfrak{p}^{-v_{\mathfrak{p}}(\cdot)}$ 是乘性赋值, 称之为 \mathfrak{p} 进赋值. 特别地, 如果 $K = \mathbb{Q}, \mathfrak{p} = (p)$, v_p 是加性赋值, $|\cdot|_p = p^{-v_p(\cdot)}$ 是乘性赋值, 称之为 p 进赋值.

练习 2.1.5 证明下述函数为非阿赋值.

- (1) 设 K 为 \mathbb{C} 上的有理函数全体, $x \in \mathbb{C}$, 定义 $\text{ord}_x(f)$ 为 f 在 x 处的阶, $f \in K^\times$.
- (2) 设 k 为一个域, $k[[T]]$ 为形式幂级数环, 即

$$k[[T]] = \left\{ \sum_{n=0}^{+\infty} a_n T^n \mid a_n \in k \right\}.$$

令 $K = k((T)) = k[[T]][T^{-1}]$ 为其分式域 (为什么). 定义 $v\left(\sum_{n=m}^{+\infty} a_n T^n\right) = m, a_m \neq 0$.

(3) 设 k 为一个域, $K = k(T)$, $p(T)$ 为 K 上一不可约多项式, 则它生成 $k[[T]]$ 的素理想 \mathfrak{p} . 定义 $v_{\mathfrak{p}}(f)$ 为 $f(T)$ 的不可约分解中 $p(T)$ 的幂次, 则 $v_{\mathfrak{p}}$ 是加性赋值.

例题 2.1 固定一个素数 p . 定义 $\Gamma = \mathbb{R}_{>0} \times \gamma^{\mathbb{Z}}$ 上的序: $r\gamma^m < s\gamma^n \iff r p^{-m} < s p^{-n}$ 或 $r p^{-m} = s p^{-n}, m < n$. 设 K 是 $R = \{\sum a_n T^n \in \mathbb{Z}[[T]] : |a_n|_p \rightarrow 0\}$, 定义

$$\begin{aligned} K &\longrightarrow \Gamma \cup \{0\} \\ \sum a_n T^n &\longmapsto \sup |a_n|_p \gamma^n. \end{aligned}$$

那么它是一个非阿赋值.

§2.1.2 等价赋值

赋值将 K 变成一个度量空间, 于是定义出 K 上的一个拓扑, 其中

$$U(a, r) = \{x \in K : |x - a| < r\}, \quad a \in K, r > 0$$

构成一组拓扑基. 在该拓扑下, K 是一个拓扑域. 显然 $\mathbf{1}_{K^\times}$ 是一个平凡赋值, 它给出了离散拓扑. 我们排除这种情形.

对任意正实数 c , $|\cdot|^c$ 显然也是一个赋值, 我们称 $|\cdot|$ 和 $|\cdot|^c$ 是等价赋值.

命题 2.4

下述命题等价:

- (1) $|\cdot|$ 和 $|\cdot|'$ 等价;
- (2) 对任意 $x \in K$, $|x| < 1$ 当且仅当 $|x|' < 1$;
- (3) $|\cdot|$ 和 $|\cdot|'$ 给出相同的拓扑;
- (4) 存在 $c_1, c_2 > 0$ 使得 $|\cdot|^{c_1} \leq |\cdot|' \leq |\cdot|^{c_2}$;
- (5) 对任意 $a, b \in K$, $|a| \leq |b|$ 当且仅当 $|a|' \leq |b|'$.



证明 显然 (1) 蕴含其它所有命题.

(3) \implies (2). 由于 $|x| < 1$ 等价于 $\{x^n\}_{n \geq 0}$ 趋于 0, 从而 $|x| < 1$ 当且仅当 $|x|' < 1$.

(4) \implies (2). 显然.

(5) \implies (2). 令 $b = 1, a = x$ 即可.

(2) \implies (1). 设 $|y| > 1$, 则对于 $x \neq 0$, $|x| = |y|^s, s \in \mathbb{R}$. 设 $\{m_i/n_i\}_i$ 是一串极限为 s 且大于 s 的有理数, $n_i > 0$. 我们有 $|x| < |y|^{m_i/n_i}$, 即

$$\left| \frac{x^{n_i}}{y^{m_i}} \right| < 1.$$

反推可知 $|x|' < |y|^{m_i/n_i}$, 故 $|x|' \leq |y|^s$. 若我们考虑一串极限为 s 且小于 s 的有理数, 则我们有 $|x|' \geq |y|^s$. 从而 $|x|' = |y|^s$. 令 $c = \log |y|' / \log |y|$, 则 $c = \log |x|' / \log |x|$, 因此 $|\cdot|' = |\cdot|^c$. \square

定理 2.5

\mathbb{Q} 上的赋值等价类只有 $|\cdot|_{\mathbb{R}}$ 和 $|\cdot|_p$.



证明 对于非阿赋值 $|\cdot|, |n| \leq 1$. 如果对于所有素数 $p, |p| = 1$, 则容易推出该赋值是平凡赋值. 因此存在 p 使得 $|p| < 1$. 考虑

$$\mathfrak{a} = \{a \in \mathbb{Z} : |a| < 1\}.$$

则 \mathfrak{a} 是一个理想, 且 $p\mathbb{Z} \subseteq \mathfrak{a} \neq \mathbb{Z}$, 因此 $\mathfrak{a} = p\mathbb{Z}$. 根据赋值的可乘性, 该赋值等价于 $|\cdot|_p$.

如果 $|\cdot|$ 是阿基米德赋值, 则对于正整数 $m, n > 1$, 如果 $|n| \geq 1$,

$$m = a_0 + a_1 n + \cdots + a_r n^r, a_i \in \{0, 1, \dots, n-1\}, a_r > 0,$$

则 $r \leq \ln m / \ln n$,

$$|m| \leq \sum |a_i| \cdot |n|^i \leq \sum |a_i| \cdot |n|^r \leq \left(1 + \frac{\ln m}{\ln n}\right) n \cdot |n|^{\frac{\ln m}{\ln n}}.$$

将 m 换成 m^k 并令 $k \rightarrow +\infty$, 则

$$|m| \leq |n|^{\frac{\ln m}{\ln n}}, \quad |m|^{\frac{1}{\ln m}} \leq |n|^{\frac{1}{\ln n}}.$$

由对称性可知存在 $c > 0$ 使得当 $|n| \geq 1$ 时, $|n| = c^{\ln n} = |n|_{\mathbb{R}}^s, s = \ln c$. 由阿基米德性质知对任意 m , 存在 $k > 0$ 使得 $|k| > 1/|m|, |km| > 1$, 因此 $|km| = |km|_{\mathbb{R}}^s$. 又因为对任意 $m, |m| \leq |m|_{\mathbb{R}}^s$, 因此 $|m| = |m|_{\mathbb{R}}^s$ 等价于 $|\cdot|_{\mathbb{R}}$. \square

定义 2.6 (赋值环)

设 R 是域 K 的一个子环. 如果对于任意非零元 $x \in K$, 均有 $x \in R$ 或 $x^{-1} \in R$, 则称 R 为一个赋值环. 通过自然的商映射, 它给出了 K 的一个赋值

$$|\cdot|: K \rightarrow \Gamma \cup \{0\},$$

其中 $\Gamma = K^\times/R^\times$ 的序为: $x \leq y \iff xy^{-1} \in R$. 我们称其为克鲁尔赋值. 显然

$$R = D(0, 1) := \{x \in K : |x| \leq 1\}.$$

这给出了非阿赋值的等价类和赋值环的一一对应.



练习 2.1.6 计算习题 2.1.5 中的赋值环.

练习 2.1.7 设 k 为一个域, $K = k(T)$, 则 $v_\infty(f) = -\deg f$ 是加性赋值. 它的赋值环是什么?

练习 2.1.8 证明习题 2.1.5(3) 和 2.1.7 中的赋值是 $k(T)$ 上所有赋值.

对于不等价的赋值, 我们有如下的逼近定理.

命题 2.7 (逼近定理)

设 $|\cdot|_1, \dots, |\cdot|_n$ 为互不等价的赋值, $\alpha_1, \dots, \alpha_n \in K$. 对于任意 $\varepsilon > 0$, 存在 $\alpha \in K$ 使得 $|\alpha - \alpha_i|_i < \varepsilon, i = 1, \dots, n$.



证明 由命题 2.4 知存在 $\alpha, \beta \in K$ 使得 $|\alpha|_1 < 1 \leq |\alpha|_n, |\beta|_1 \geq 1 > |\beta|_n$. 设 $y = \beta/\alpha$, 则 $|y|_1 > 1, |y|_n < 1$.

我们归纳地证明存在 $z \in K$ 使得

$$|z|_1 > 1, |z|_j < 1, j = 2, \dots, n.$$

$n = 2$ 已成立. 设 x 满足 $|x|_1 > 1, |x|_j < 1, j = 2, \dots, n-1$. 如果 $|x|_n \leq 1$, 则对于充分大的 $m, z = x^m y$ 满足我们的要求. 如果 $|x|_n > 1$, 则对于充分大的 $m, z = yx^m/(1+x^m)$ 满足我们的要求.

我们看到, 我们所取的 z 使得 $z^m/(1+z^m)$ 在 $|\cdot|_1$ 下趋于 1, 在其它赋值趋于 0. 类似地, 我们构造 z_i 在 $|\cdot|_i$ 下趋于 1, 在其它赋值趋于 0. 最后取 $\alpha = \sum \alpha_i z_i$ 即可. \square

§2.1.3 完备化

命题 2.8

(1) 域 K 在一个赋值下 $|\cdot|$ 的完备化 \widehat{K} 仍然是一个域, 且赋值可以延拓至 \widehat{K} . 记为 $(\widehat{K}, |\cdot|_{\widehat{K}})$, 则它同构意义下唯一.

(2) \widehat{K} 是完备的, 且 K 在 \widehat{K} 中稠密.

(3) 如果 $K \hookrightarrow L$ 是赋值域的连续嵌入, 则该嵌入可延拓至 $\widehat{K} \hookrightarrow \widehat{L}$.



证明 实际上, \widehat{K} 是 K 上等价的柯西列全体构成的集合. \widehat{K} 的存在性、唯一性以及 K 在其中稠密均是标准的分析学内容, 这里我们省略. 设柯西列 $(x_n)_{n \geq 1}$ 代表了 $x \in \widehat{K}$, 则 $(|x_n|)_{n \geq 1}$ 也是柯西列, 我们将其极限定义成 $|x|_{\widehat{K}}$. 易知它是良定的且延拓了 $|\cdot|$.

我们可以自然地在 \widehat{K} 上定义加法和乘法. 如果 $a = (a_n)_{n \geq 1}$ 是一个非零柯西列, 则存在整数 $N \geq 1$

以及常数 $C > 0$ 使得 $n \geq N$ 时 $|a_n| \geq C$. 定义

$$b_n = \begin{cases} 1 & 1 \leq n \leq N-1; \\ a_n^{-1} & n \geq N, \end{cases}$$

则 $|b_n - b_m| = |a_n a_m|^{-1} |a_n - a_m| \leq C^{-2} |a_n - a_m|$. 从而 $b = (b_n)_{n \geq 1}$ 是一个柯西列, 且 $ab = 1$. 因此 \widehat{K} 是一个域.

设 $f: K \hookrightarrow L$ 为题述嵌入. 对于 $x = \lim_{n \rightarrow +\infty} x_n \in \widehat{K}$, $x_n \in K$, 定义 $\hat{f}(x) = \lim_{n \rightarrow +\infty} f(x_n)$. 则 \hat{f} 是良定的且是我们要的延拓. 由连续性知它是唯一的. \square

练习 2.1.9 对于非阿赋值域, $\{x_k\}_{k \geq 1}$ 是柯西列当且仅当 $|x_{k+1} - x_k| \rightarrow 0$. 换言之, 完备非阿赋值域中 $\sum_{k=1}^{\infty} a_k$ 收敛当且仅当 $a_k \rightarrow 0$.

命题 2.9

设 K 为非阿赋值域, R_K 为其赋值环.

(1) R_K 是整闭的, 且 $\mathfrak{p} = \{x \in K : |x| < 1\}$ 是极大理想.

(2) 设 $0 < |\pi| < 1$, 则 \widehat{K} 的赋值环为

$$R_{\widehat{K}} = \varprojlim_n R_K / \pi^n R_K = \left\{ (x_n)_n \in \prod_{n \geq 1} R_K / \pi^n R_K \mid x_{n+1} \equiv x_n \pmod{\pi^n} \right\}.$$



证明 (1) 设 $x \in K$ 被 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R_K[x]$ 零化. 如果 $|x| > 1$, 则 $|a_i x^i| = |a_i| \cdot |x|^i < |x|^n$. 于是 $0 = |f(x)| = |x|^n > 1$, 矛盾. 因此 R_K 是整闭的. 对于任意 $u \in R_K - \mathfrak{p}$, $|u^{-1}| = |u|^{-1} = 1$, 因此 $u^{-1} \in R_K$, \mathfrak{p} 是极大理想.

(2) 由于 K 在 \widehat{K} 中稠密, 因此 R_K 的闭包是 $R_{\widehat{K}}$. 对于任意 $x = (x_n)_{n \geq 1} \in R := \varprojlim_n R_K / \pi^n$, 令 $\tilde{x}_n \in R_K$ 为 x_n 的任一提升, 则 $|\tilde{x}_n - \tilde{x}_m| \leq |\pi|^m, \forall n \geq m$. 由于 $|\pi| < 1$, 因此 $\{\tilde{x}_n\}_n$ 是一个柯西列, 令 $\phi(x)$ 为其极限, 则我们定义了映射 $\phi: R \rightarrow R_{\widehat{K}}$. 反之, 对于任意 $a \in R_{\widehat{K}}$, 设序列 $\{a_n \in R_K\}_n$ 的极限为 a , 定义 $\psi(x) = (\tilde{x}_n)_n \in R$. 容易验证 ϕ 和 ψ 互逆. \square

命题 2.10

非阿赋值域全不连通, 即对任意 $x \neq y$, 存在既开又闭的两个不交集合 U, V , 其中 $x \in U, y \notin U, y \in V, x \notin V$.



证明 设 Γ 为该赋值域赋值对应的全序乘法交换群. 对任意 $r \in \Gamma$, 我们有

$$D(a, r) = U(a, r) \cup \bigcup_{|s-a|=r} U(s, r).$$

从而 $D(a, r)$ 是开集. 对于任意 $x \notin D(a, r)$, $|x - a| > r$. 设 $0 < t < |x - a| - r$, 则对于 $y \in U(x, t)$, $|y - a| \geq |x - a| - |x - y| > |x - a| - t > r$, 因此 $U(x, t) \cap D(a, r) = \emptyset$. 从而 $D(a, r)$ 既开又闭. 对于 $x \neq y$,

$$D(x, r) \cap D(y, r) = \emptyset, \quad r < |x - y|,$$

因此命题成立. \square

例题 2.2 数域 K 上的 \mathfrak{p} 进赋值的赋值环为

$$\mathcal{O}_{K, \mathfrak{p}} = (\mathcal{O}_K - \mathfrak{p})^{-1} \mathcal{O}_K.$$

它的极大理想为 $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}}$, 剩余域为 $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} \cong \mathcal{O}_K/\mathfrak{p}$. 相应的完备化为

$$\mathcal{O}_{K_{\mathfrak{p}}} := \varprojlim_n \mathcal{O}_K/\mathfrak{p}^n \mathcal{O}_K$$

的分式域 $K_{\mathfrak{p}} = \mathcal{O}_{K_{\mathfrak{p}}}[\frac{1}{\mathfrak{p}}]$, 其中 $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

特别地, \mathbb{Q} 上的 p 进赋值的赋值环为

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b \right\},$$

它的极大理想为 $p\mathbb{Z}_{(p)}$, 剩余域为 $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p$. \mathbb{Q} 在该赋值下的完备化为

$$\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n \mathbb{Z}$$

的分式域 $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$.

练习 2.1.10 给出习题 2.1.5 中赋值环的一个素元并计算剩余域.

练习 2.1.11 设 $x \in 1 + p\mathbb{Z}_p$.

(1) 证明 $x^{p^n} \in 1 + p^{n+1}\mathbb{Z}_p$.

(2) 如果整数序列 $(s_n)_{n \geq 1}$ 在 \mathbb{Z}_p 中收敛到 s , 则 $(x^{s^n})_{n \geq 1}$ 也收敛. 记为 x^s .

(3) $s \in \mathbb{Z}_p$ 在乘法群 $1 + p\mathbb{Z}_p$ 的作用 $x \mapsto x^s$ 将其变成了一个 \mathbb{Z}_p 模.

练习 2.1.12 (1) \mathbb{Q}_p 和 \mathbb{R} 不同构.

(2) 当素数 $p \neq q$ 时, 域 \mathbb{Q}_p 和 \mathbb{Q}_q 不同构.

练习 2.1.13 \mathbb{Q}_p 的代数闭包是无限次的.

§2.2 完备离散赋值域

§2.2.1 离散赋值

练习 2.2.1 \mathbb{R} 的离散子群为 $r\mathbb{Z}, r \in \mathbb{R}$.

定义 2.11 (离散赋值)

如果 $v(K^\times)$ 是 \mathbb{R} 的离散子群, 称 v 是离散赋值, 称 K 为离散赋值域, 对应的赋值环为离散赋值环. 显然, 离散赋值存在等价赋值 v' 使得 $v'(K^\times) = \mathbb{Z}$, 称之为规范化离散赋值.



例题 2.3 p 进赋值和习题 2.1.5 中的赋值均为离散赋值.

设 K 是完备离散赋值域, 则满足 $v(\pi) = 1$ 的元素是素元. 设 $\mathcal{O}_K, \pi, \mathfrak{p}, \kappa := \mathcal{O}_K/\mathfrak{p}, v$ 分别为 K 的赋值环、素元、极大理想、剩余域和规范化离散赋值. 我们有

$$\mathcal{O}_K = \varprojlim_n \mathcal{O}_K/\pi^n \mathcal{O}_K.$$

命题 2.12

如果 K 是完备离散赋值域, 则 \mathfrak{p} 是主理想且 \mathcal{O}_K 的所有非零理想为 $\{\mathfrak{p}^n\}_{n \geq 0}$. 特别地, \mathcal{O}_K 只有素理想 $(0), \mathfrak{p}$, 且 $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ 是一维 κ 向量空间.



证明 对任意 $x \in \mathfrak{p}$, $v(x\pi^{-1}) \geq 0$, 因此 $x\pi^{-1} \in \mathcal{O}_K$, $\mathfrak{p} = (\pi)$. 对于任意非零理想 $I \subseteq \mathcal{O}_K$, 设 $n = \min\{v(x) \mid x \in I\}$. 设 $x \in I$ 满足 $v(x) = n$, 则 $x^{-1}\pi^n \in \mathcal{O}_K$, $\pi^n = (x^{-1}\pi^n)x \in I$. 又因为对任意 $y \in I$, $v(y) \geq n$, $y\pi^{-n} \in \mathcal{O}_K$, 因此 $I = (\pi^n) = \mathfrak{p}^n$. \square

由此可知:

命题 2.13

设 S 是 κ 在 \mathcal{O}_K 的一组代表元, 则任一元素 $x \in \mathcal{O}_K$ 均可唯一表为

$$x = \sum_{i \geq 0} s_i \pi^i, \quad s_i \in S,$$

任一元素 $x \in K$ 均可唯一表为

$$x = \sum_{i \geq -n} s_i \pi^i, \quad s_i \in S.$$



根据域本身的特征和剩余域的特征, 可以将完备离散赋值域分为 $(0, 0)$, (p, p) , $(0, p)$ 三种情形. 我们将会证明前两种情形 (等特征) 情形是相对简单的.

定义 2.14 (本原多项式)

对于 $f(T) = \sum_{i=0}^n a_i T^i \in K[T]$, 定义

$$|f| := \max_i \{|a_i|\}.$$

如果 $f(T) \in \mathcal{O}_K[T]$ 满足 $f(T) \not\equiv 0 \pmod{\pi}$, 即 $|f| = 1$, 则称其为本原多项式.



引理 2.15 (亨泽尔引理)

如果本原多项式 $f(T)$ 模 π 可以分解为

$$f(T) \equiv \bar{g}(T)\bar{h}(T) \pmod{\pi},$$

其中 $\bar{g}, \bar{h} \in \kappa[x]$ 互素, 则存在分解

$$f(T) = g(T)h(T),$$

其中 $g, h \in \mathcal{O}_K[T]$, $\deg(g) = \deg(\bar{g})$ 且

$$g(T) \equiv \bar{g}(T) \pmod{\pi}, \quad h(T) \equiv \bar{h}(T) \pmod{\pi}.$$



证明 设 $d = \deg(f)$, $m = \deg(\bar{g})$. 任取 \bar{g}, \bar{h} 的提升 $g_0, h_0 \in \mathcal{O}_K[T]$ 使得 $\deg g_0 = m$, $\deg h_0 \leq d - m$. 我们将归纳地构造一系列 $g_n, h_n \in \mathcal{O}_K[T]$ 满足

- $\deg g_n = m$, $\deg h_n \leq d - m$;
- $g_n \equiv g_{n-1}, h_n \equiv h_{n-1} \pmod{\pi^n}$
- $f \equiv g_n h_n \pmod{\pi^{n+1}}$.

设 $f = g_{n-1}h_{n-1} + \pi^n f_n$, $\deg f_n \leq \deg f$. 设 $g_n = g_{n-1} + \pi^n p_n$, $h_n = h_{n-1} + \pi^n q_n$, 则

$$\begin{aligned} g_n h_n &\equiv g_{n-1} h_{n-1} + \pi^n (p_n h_{n-1} + g_{n-1} q_n) \\ &\equiv f + \pi^n (p_n h_0 + g_0 q_n - f_n) \pmod{\pi^{n+1}}. \end{aligned}$$

我们希望找到 p_n, q_n 满足 $p_n h_0 + g_0 q_n \equiv f_n \pmod{\pi}$. 由于 $(\bar{g}, \bar{h}) = 1$, 存在 $a, b \in \mathcal{O}_K[T]$ 使得 $ag_0 + bh_0 \equiv 1 \pmod{\pi}$, 因此 $af_n g_0 + bf_n h_0 \equiv f_n \pmod{\pi}$. 根据带余除法, 存在 $bf_n = ug_0 + v$, $\deg v \leq \deg g_0 - 1$. 注意到 g 首项系数是一个单位, 因此 $u, v \in \mathcal{O}_K[T]$. 令 $p_n = v, q_n$ 为 $af_n + uh_0$ 的次数小于 $d - m$ 的部分, 则它们满足我们需要的性质. 最后令 $n \rightarrow \infty$ 即可. \square

例题 2.4 假设 K 的剩余域 $\kappa = \mathbb{F}_q$ 有限. 我们知道 $T^{q-1} - 1 \in \mathcal{O}_K[T]$ 满足 $T^{q-1} - 1 \equiv \prod_{a \in \mathbb{F}_q^\times} (T - a) \pmod{\pi}$,

因此它在 $\mathcal{O}_K[T]$ 也可以分解为 $q-1$ 个不同的一次多项式乘积, 换言之, $\mu_{q-1} \subseteq \mathcal{O}_K$.

练习 2.2.2 (魏尔斯特拉斯预备定理) 任何一个非零的幂级数

$$f(T) = \sum_{n=0}^{\infty} a_n T^n \in \mathbb{Z}_p[[T]]$$

可以唯一地写成

$$f(T) = p^\mu P(T)u(T),$$

其中 $U(T) \in \mathbb{Z}_p[[T]]^\times$, $P(T) \in \mathbb{Z}_p[T]$ 首一且满足 $P(T) \equiv T^\lambda \pmod{p}$, $\lambda = \deg P$.

练习 2.2.3 在 \mathbb{Q}_7 中 $\sum_{n \geq 0} \binom{\frac{1}{2}}{n} \left(\frac{7}{9}\right)^n$ 是多少?

命题 2.16

如果完备离散赋值域 K 的剩余域 κ 是特征 p 的完全域, 则对于自然映射 $\mathcal{O}_K \rightarrow \kappa$, 存在唯一一个具有可乘性的自然的提升 $r: \kappa \rightarrow \mathcal{O}_K$.



证明 设 $a \in \kappa$. 对于任意 $n \geq 0$, 存在 $a_n \in \kappa$ 使得 $a_n^{p^n} = a$, $a_{n+1}^p = a_n$. 设 $\hat{a}_n \in \mathcal{O}_K$ 为其任一提升. 由于 $\hat{a}_{n+1}^p \equiv \hat{a}_n \pmod{\mathfrak{p}}$, 易知 $\hat{a}_{n+1}^{p^{n+1}} \equiv \hat{a}_n^{p^n} \pmod{\mathfrak{p}^{n+1}}$. 因此 $r(a) := \lim_{n \rightarrow \infty} \hat{a}_n^{p^n}$ 收敛. 容易知道, $r(a)$ 不依赖于提升的选取, 且满足可乘性. 如果 t 也满足相应性质, 则取 $\hat{a}_n = t(a_n)$,

$$r(a) = \lim_{n \rightarrow \infty} \hat{a}_n^{p^n} = \lim_{n \rightarrow \infty} t(a_n)^{p^n} = t(a).$$

因此 r 是唯一的. □

定义 2.17 (泰希米勒提升)

$r(a)$ 被称为 a 的泰希米勒提升, 记为 $[a]$.



当 K 特征 p 时, 容易看出 r 诱导了环嵌入 $\kappa \rightarrow \mathcal{O}_K$, 此时我们知道 $\mathcal{O}_K = \kappa[[\pi]]$, $K = \kappa((\pi))$. 实际上, 对于等特征情形, K 都具有这种形式.

定理 2.18

如果 K 是等特征的完备离散赋值域, 则 $\mathcal{O}_K = \kappa[[\pi]]$, $K = \kappa((\pi))$.



证明 当 κ 特征零时, 映射 $\mathbb{Z} \hookrightarrow \mathcal{O}_K \rightarrow \kappa$ 是单射, 因此 $\mathbb{Z} - \{0\}$ 在 \mathcal{O}_K 中可逆, $\mathbb{Q} \subset \mathcal{O}_K$. 由佐恩引理, \mathcal{O}_K 中存在极大子域 S . 设 \bar{S} 是它在 κ 中的像, 则 $S \xrightarrow{\sim} \bar{S}$. 我们断言 $\bar{S} = k$.

首先 κ 在 \bar{S} 上代数. 若不然, 存在 $a \in \mathcal{O}_K$ 使得 \bar{a} 在 \bar{S} 上超越, 所以 a 在 S 上超越, $S[a] \simeq \bar{S}[\bar{a}] \simeq S[T]$, $S[a] \cap \mathfrak{p} = 0$. 因此 $S(a) \subset \mathcal{O}_K$, 这与 S 极大矛盾, 因此 κ 在 \bar{S} 上代数.

对于任意 $\alpha \in \kappa$, 令 $\bar{f} \in \bar{S}[x]$ 是它的极小多项式. 由于 κ 特征零, \bar{f} 可分, α 是 \bar{f} 的单根. 由亨泽尔引理, 存在 $x \in \mathcal{O}_K$, $f(x) = 0$, $\bar{x} = \alpha$. 因此 $\bar{S}[\alpha]$ 可以提升为 $S[x]$. 由 S 极大知 $x \in S$, $\kappa = \bar{S}$.

一般情形, 我们由 Cohen 结构定理 [2] 知, 存在 \mathcal{O}_K 的子环 Λ , 使得自然映射 $\Lambda \rightarrow \kappa$ 是同构. 由此可知该命题成立. □

§2.2.2 维特向量

对于混合特征情形, $\text{char } K = 0, \text{char } \kappa = p$, 我们需要维特向量来描述完备离散赋值域的结构. 设 $\mathbf{X} = (X_0, \dots, X_n)$,

$$W_n(\mathbf{X}) = X_0^{p^n} + pX_1^{p^{n-1}} + \dots + p^n X_n \in \mathbb{Z}[\mathbf{X}] = \mathbb{Z}[X_0, \dots, X_n].$$

引理 2.19

对于任意 $\Phi \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]$, 存在多项式

$$\Phi_i \in \mathbb{Z}[X_0, \dots, X_i, Y_0, \dots, Y_i], \quad i = 0, 1, \dots, n$$

使得

$$W_n(\Phi_0, \Phi_1, \dots, \Phi_n) = \Phi(W_n(X_0, X_1, \dots, X_n), W_n(Y_0, Y_1, \dots, Y_n)).$$



证明 显然 $\Phi_0 = \Phi(X_0, Y_0)$. 归纳地定义

$$\Phi_n(\mathbf{X}, \mathbf{Y}) = \frac{1}{p^n} \left(\Phi \left(\sum_{i=0}^n p^i X_i^{p^{n-i}}, \sum_{i=0}^n p^i Y_i^{p^{n-i}} \right) - \sum_{i=0}^{n-1} p^i \Phi_i(\mathbf{X}, \mathbf{Y})^{p^{n-i}} \right).$$

我们只需要证明它是整系数的, 我们利用归纳法证明

$$\Phi \left(\sum_{i=0}^n p^i X_i^{p^{n-i}}, \sum_{i=0}^n p^i Y_i^{p^{n-i}} \right) \equiv \sum_{i=0}^{n-1} p^i \Phi_i(\mathbf{X}, \mathbf{Y})^{p^{n-i}} \pmod{p^n}.$$

由归纳假设, $\Phi_i \in \mathbb{Z}[\mathbf{X}, \mathbf{Y}]$, 因此

$$\Phi_i(\mathbf{X}^p, \mathbf{Y}^p) \equiv (\Phi_i(\mathbf{X}, \mathbf{Y}))^p \pmod{p}.$$

于是 $p^i \Phi_i(\mathbf{X}^p, \mathbf{Y}^p)^{p^{n-1-i}} \equiv p^i \Phi_i(\mathbf{X}, \mathbf{Y})^{p^{n-i}} \pmod{p^n}$,

$$\begin{aligned} \text{左边} &\equiv \Phi \left(\sum_{i=0}^{n-1} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n-1} p^i Y_i^{p^{n-i}} \right) \\ &\equiv \sum_{i=0}^{n-1} p^i \Phi_i(\mathbf{X}^p, \mathbf{Y}^p)^{p^{n-1-i}} \equiv \text{右边} \pmod{p^n}. \end{aligned}$$

因此命题得证. □

对于 $n \geq 1$ 和任意交换环 A , 令 $W_n(A) = A^n$. 令 S_i, P_i 分别为对应 $X + Y, XY$ 的 Φ_i . 对于任意 $a = (a_0, \dots, a_{n-1}), b = (b_0, \dots, b_{n-1}) \in W_n(A)$, 令

$$s_i = S_i(a_0, \dots, a_i, b_0, \dots, b_i), \quad p_i = P_i(a_0, \dots, a_i, b_0, \dots, b_i).$$

定义

$$a + b = (s_0, s_1, \dots, s_{n-1}), \quad a \cdot b = (p_0, p_1, \dots, p_{n-1}).$$

考虑

$$\begin{aligned} \rho: W_n(A) &\longrightarrow A^n \\ (a_0, a_1, \dots, a_{n-1}) &\longmapsto (w_0, w_1, \dots, w_{n-1}), \end{aligned}$$

其中 $w_i = W_i(a) = a_0^{p^{n-i}} + pa_1^{p^{n-i-1}} + \dots + p^i a_i$. 则

$$w_i(a+b) = w_i(a) + w_i(b), \quad w_i(ab) = w_i(a)w_i(b).$$

- 如果 p 可逆, 则 ρ 是双射, $W_n(A)$ 是一个环;

- 如果 A 没有 p 阶元, 则 $W_n(A) \subseteq W_n(A[\frac{1}{p}])$ 是一个子环;
- 一般情形, 存在 $I \subseteq R$ 使得 $A = R/I$, R 没有 p 阶元, $W_n(A) = W_n(R)/W_n(I)$.

因此 $W_n(A)$ 是环. 考虑满同态

$$\begin{aligned} W_{n+1}(A) &\longrightarrow W_n(A) \\ (a_0, a_1, \dots, a_n) &\longmapsto (a_0, a_1, \dots, a_{n-1}), \end{aligned}$$

定义

$$W(A) = \varprojlim_n W_n(A),$$

其中每个 $W_n(A)$ 赋予离散拓扑, 则我们得到一个拓扑环 (由直积拓扑限制得到), 称之为 A 的**维特环**, 其中元素被称为**维特向量**. 相应的 $W_n(A)$ 被称为长度为 n 的维特环, 其中元素被称为长度为 n 的维特向量.

例题 2.5 $W(\mathbb{F}_p) = \mathbb{Z}_p$. 考虑映射

$$\begin{aligned} \varphi : W(\mathbb{F}_p) &\longrightarrow \mathbb{Z}_p \\ (a_0, a_1, \dots) &\longmapsto \sum_{n \geq 0} p^n [a_n], \end{aligned}$$

我们想要说明这是环同构, 则需要验证

$$\sum_{i=0}^n (p^i [a_i] + p^i [b_i]) = \sum_{i=0}^n p^i [s_n],$$

而根据泰希米勒提升的构造, 这等价于


$$\sum_{i=0}^n p^i (\tilde{a}_i^{p^{n-i}} + \tilde{b}_i^{p^{n-i}} - \tilde{s}_i^{p^{n-i}}) \equiv 0 \pmod{p^n}, \quad \tilde{x} \in \mathbb{Z} \text{ 是 } x \in \mathbb{F}_p \text{ 的提升,}$$

这由 Φ 的构造可以看出. 乘法的验证是类似的.

一般地, 设 $S = \mathbb{F}_p[X_\alpha^{p^{-\infty}}]$ 为完全环, X_α 是一些不定元, 则 $W(S) = \widehat{\mathbb{Z}_p[X_\alpha^{p^{-\infty}}]}$, $W(S)/pW(S) = S$. 同理可知 $W(S)$ 中的元素均可表为

$$x = \sum_{n \geq 0} p^n [x_n^{p^{-n}}], \quad x_n \in S.$$

对于完全域 κ , 存在形如 $\mathbb{F}_p[X_\alpha^{p^{-n}}]$ 的 S 和满射 $h : S \rightarrow \kappa$. 对于 $a, b \in W(S)$, 我们记 $a \sim b$ 表示它们相应的 x_n 在 h 下的像相同, 则 $H = W(\kappa) = W(S)/\sim$ 是特征零完备离散赋值域, p 为素元, κ 为剩余域.

 **练习 2.2.4** 证明 $W(\mathbb{F}_p)$ 和 \mathbb{Z}_p 作为拓扑环是同构的.

定义 2.20 (绝对分歧指数)

设完备离散赋值域 K 是混合特征 $(0, p)$ 的, v 是它的规范化离散赋值. 称 $e = v(p)$ 为其**绝对分歧指数**. 若 $e = 1$, 即 p 是它的一个素元, 称之为**绝对非分歧**.



定理 2.21

设 κ 是特征 p 的完全域, 则 $W(\kappa)$ 是唯一的剩余域为 κ 的绝对非分歧特征零完备离散赋值域. 设完备离散赋值域 K 是混合特征 $(0, p)$ 的, e 为其绝对分歧指数. 如果 K 的剩余域 κ 是完全域, 则

存在唯一的同态 $\psi: W(\kappa) \rightarrow K$ 使得

$$\begin{array}{ccc} W(\kappa) & \xrightarrow{\psi} & K \\ & \searrow & \swarrow \\ & \kappa & \end{array}$$

而且 ψ 是单射, 其诱导了剩余域上的同构, \mathcal{O}_K 是秩 e 的自由 $W(\kappa)$ 模.



证明 见 [6, Theorem 0.40]. 我们简要说明下 \mathcal{O}_K 是秩 e 的自由 $W(\kappa)$ 模. 设 π 是 \mathcal{O}_K 的素元, 则任意 $a \in \mathcal{O}_K$ 可唯一表为

$$a = \sum_{n \geq 0} [\alpha_n] \pi^n, \quad \alpha_n \in \kappa.$$

而我们知道 π^e 和 p 只相差一个单位, 因此 a 可唯一表为

$$a = \sum_{n \geq 0} \sum_{j=0}^{e-1} [\alpha_{ij}] \pi^j p^i, \quad \alpha_{ij} \in \kappa.$$

因此 $\{1, \pi, \dots, \pi^{e-1}\}$ 是 \mathcal{O}_K 作为 $W(\kappa)$ 模的一组基. □

注 对于 κ 不是完全域的情形, 我们有所谓的 Cohen 环作为唯一的剩余域为 κ 的绝对非分歧特征零完备离散赋值域, 且仍然有单同态 ψ , 其诱导了剩余域上的同构, 尽管 ψ 可能不再唯一, 见 [6, § 0.2.4].

§2.2.3 乘法群的结构

设 $\mathcal{O}_K, \pi, \mathfrak{p}, \kappa, v$ 为完备离散赋值域 K 的赋值环、素元、极大理想、剩余域和规范化离散赋值.

定义 2.22 (高阶单位群)

称

$$U^{(n)} = 1 + \mathfrak{p}^n = \{x \in K^\times \mid v(x-1) \geq n\}, \quad n \geq 0$$

为 K 的 n 阶单位群. 它们形成一个递减的群序列

$$\mathcal{O}_K^\times = U^{(0)} \supseteq U^{(1)} \supseteq \dots$$



命题 2.23

我们有

$$\mathcal{O}_K^\times / U^{(n)} \cong (\mathcal{O}_K / \mathfrak{p}^n)^\times, \quad U^{(n)} / U^{(n+1)} \cong \mathcal{O}_K / \mathfrak{p},$$

以及

$$\mathcal{O}_K^\times \cong \varprojlim_n \mathcal{O}_K^\times / U^{(n)}.$$



练习 2.2.5 证明上述命题.

命题 2.24

如果 $\kappa = \mathbb{F}_q$ 有限, 则我们有分解

$$K^\times = \pi^{\mathbb{Z}} \times \mu_{q-1} \times U^{(1)}.$$



练习 2.2.6 证明上述命题.

练习 2.2.7 设 K 的特征为 0. 如果其剩余域特征为 0, 令 $\epsilon = 1$; 如果其剩余特征为 p , 令 $\epsilon = |p|^{\frac{1}{p-1}}$. 则

$$\exp(x) := \sum_{n=0}^{+\infty} \frac{x^n}{n!}$$

的收敛区域为 $U(0, \epsilon)$,

$$\log(x) := \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} (t-1)^n$$

的收敛区域为 $U(1, 1)$. 于是我们有群同构

$$\exp : U(0, \epsilon) \xrightarrow{\sim} U(1, \epsilon),$$

其逆为 \log .

命题 2.25

设 K 是剩余域 $\kappa = \mathbb{F}_q$ 有限的完备离散赋值域, 则 K 是 \mathbb{Q}_p 或 $\mathbb{F}_p[[t]]$ 的有限扩张, 且

(1) K 特征为 0 时, 我们有连续的群同构

$$K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d,$$

这里 $a \geq 0, d = [K : \mathbb{Q}_p]$.

(2) K 特征为 p 时, 我们有连续的群同构

$$K^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}_p^{\mathbb{N}}.$$



证明 见 [15, Proposition 2.5.7]. 我们粗略证明下 K 特征 0 情形, 此时 $\mathbb{Q} \subseteq K, v$ 限制在 \mathbb{Q} 上等价于 p 进赋值, 因此 $\mathbb{Q}_p \subseteq K$. 而 $\mathbb{Q}_p \subseteq \text{Frac } W(\kappa) \subseteq K$ 均为有限扩张, 因此 K/\mathbb{Q}_p 有限. 当 n 充分大时,

$$\log : U^{(n)} \rightarrow \pi^n \mathcal{O}_K \cong \mathcal{O}_K.$$

我们将会 在定理 2.33 中证明 \mathcal{O}_K 是 \mathbb{Z}_p 在 K 中的整闭包, 由注记 1.2.2 知 \mathcal{O}_K 是秩 n 的自由 \mathbb{Z}_p 模. $[U^{(1)} : U^{(n)}]$ 有限, 因此 $U^{(1)}$ 作为有限生成 \mathbb{Z}_p 模分解为有限部分和自由部分. 但有限部分只能是 K^\times 的单位根的 p 部分, 它是个循环群. \square

特别地, 如果 $K = \mathbb{Q}_p$, 当 $p > 2$ 时,

$$\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p) \cong \mathbb{Z} \oplus \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p,$$

\mathbb{Q}_p^\times 中的平方元为 $p^{2k}a, p \nmid a, a \pmod p$ 是平方数. 当 $p = 2$ 时,

$$\mathbb{Q}_2^\times = 2^{\mathbb{Z}} \times (\mathbb{Z}/4\mathbb{Z})^\times \times (1 + 4\mathbb{Z}_2) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}_2,$$

\mathbb{Q}_2^\times 中的平方元为 $2^{2k}a, 2 \nmid a, a \equiv 1 \pmod 8$.

§2.2.4 二次曲线的有理点

本节中我们将研究二次方程

$$f(x, y) = ax^2 + by^2 - c = 0, \quad a, b, c \in \mathbb{Q}, a, b \text{ 不全为零}, (x, y) \in \mathbb{Q}^2.$$

记 $V(f)$ 为 f 的所有有理根全体. 我们不加区分地使用方程的根和对应曲线的点这两种说法.

令 $\mathbb{P}^n(\mathbb{Q})$ 为 n 维射影曲线, 即 \mathbb{Q}^n 中所有过原点的直线全体. 其中的元素我们可以记为 $[x_0 : \cdots :$

$x_n], (x_0, \dots, x_n)$ 为该直线上任意一非零点. 显然 $[x_0 : \dots : x_n] = [\lambda x_0 : \dots : \lambda x_n], \lambda \in \mathbb{Q}^\times$. 因此

$$\mathbb{P}^n(\mathbb{Q}) = (\mathbb{Q}^n - \{0\})/\mathbb{Q}^\times.$$

特别地我们可以记 $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

假设 $V(f) \neq \emptyset$, 设 $P_0 = (x_0, y_0) \in V(f)$, 则对于任意其它有理点 $P = (x, y)$, 设 $(\alpha, \beta) = (x, y) - (x_0, y_0)$, 则 $[\alpha, \beta] \in \mathbb{P}^1(\mathbb{Q})$. 反之, 对于任意 $[\alpha, \beta] \in \mathbb{P}^1(\mathbb{Q})$, 直线

$$\alpha(y - y_0) = \beta(x - x_0),$$

其与 $f(x, y) = 0$ 联立后得到 x 的一个二次方程

$$(a\alpha^2 + b\beta^2)x^2 - 2b\beta(\alpha y_0 - \beta x_0)x + b(\beta x_0 - \alpha y_0)^2 - c\alpha^2 = 0.$$

如果该二次方程首项系数非零, 由于其中一个根 x_0 是有理数, 因此另一个根也是有理数, 对应的点是有理点. 这里注意有一个 $[\alpha, \beta]$ 对应的是 P 的切线. 由此我们得到

$$V(f) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q}) - \{\text{至多两个点}\}.$$

练习 2.2.8 令 $f(x, y) = x^2 + y^2 - 1, P_0 = (-1, 0)$, 计算 $V(f)$. 由此得到 $x^2 + y^2 = z^2$ 的所有整数解.

考虑 f 的齐次化版本

$$g(x, y, z) = ax^2 + by^2 - cz^2.$$

令 $V(g) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{Q}) \mid g(x, y, z) = 0\}$. 显然该定义是良好的. 则有可能排除掉的点对应于 $[b : \sqrt{-ab} : 0]$. 因此

$$V(g) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q}).$$

实际上, 如果令 $U = \mathbb{P}^2(\mathbb{Q}) - V(z)$, 即所有 $z \neq 0$ 的点, 则 $U \simeq \mathbb{Q}^2, V(f) = V(g) \cap U$.

练习 2.2.9 令 $g(x, y, z) = x^2 + y^2 - 5z^2$, 计算 $V(g)$.

命题 2.26

记号同前文. 则 $V(f) \neq \emptyset$ 当且仅当 $V(g) \neq \emptyset$.



证明 $V(f) \neq \emptyset$ 显然推出 $V(g) \neq \emptyset$. 反之, 对于 $[x : y : z] \in V(g)$, 若 $z \neq 0$, 则 $(x/z, y/z) \in V(f)$; 若 $z = 0$, 不妨设 $x \neq 0$, 则 $(y/x, z/x) \in V(a + bY^2 - cZ^2) \neq \emptyset$, 因此 $a + bY^2 - cZ^2 = 0$ 有无穷多有理点, 特别地, 存在 $Z \neq 0$ 的有理点, 即 g 存在 $z \neq 0$ 的有理点. \square

实际上, 上述讨论对于任意特征零的域都是成立的. 现在的问题是, 如何判断一个二次方程是否存在有理数点? 设 K 是一个数域, v 是其上一个赋值, 记 K_v 为 K 在该赋值下的完备化.

定理 2.27 (哈塞-闵可夫斯基定理)

设 K 为数域, $f(x_1, \dots, x_n)$ 为 K 系数次数不大于 2 的多项式, 则 $f(x_1, \dots, x_n) = 0$ 在 K 中有解当且仅当, 对于 K 的每个赋值 $v, f(x_1, \dots, x_n) = 0$ 在 K_v 中有解.



证明 见 [16, Theorem 66.4]. \square

§2.2.5 有理数域上的希尔伯特符号

我们将使用 \mathbb{Q} 上的希尔伯特符号来回答 2.2.4 节提出的问题.

定义 2.28 (希尔伯特符号)

设 $a, b \in \mathbb{Q}^\times$. 如果方程 $ax^2 + by^2 = 1$ 在 \mathbb{Q}_v 上有解, 则定义 $(a, b)_v = 1$, 否则 $(a, b)_v = -1$.



由命题 2.26 可知, $(a, b)_v = 1$ 当且仅当 $ax^2 + by^2 - z^2 = 0$ 在 $\mathbb{P}^2(\mathbb{Q}_v)$ 上有解.

练习 2.2.10 (1) 证明 $(a, b)_v = (b, a)_v, (a, -a)_v = (a, 1-a)_v = 1$.

(2) 证明 $(a, b)_\infty = 1$ 当且仅当 $a > 0$ 或 $b > 0$.

不妨设 $a, b \in \mathbb{Z}$. 当 $v = p > 2$ 时, 回忆 \mathbb{Q}_p^\times 中一个数是平方当且仅当其赋值为偶数且模 p 是二次剩余. 如果 $p \nmid ab$, 则 a 或 b 是模 p 二次剩余时, 显然有解. 如果 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$, 则

$$ax^2 = 1 - by^2, \quad (ax)^2 = a(1 - by^2).$$

当 $y = 0, \dots, \frac{p-1}{2}$ 时, $1 - by^2$ 两两不同且均不被 p 整除, 因此其中至少有一个二次非剩余, 于是

$$\left(\frac{a(1 - by^2)}{p}\right) = 1,$$

方程有解. 也就是说 $(a, b) = 1$.

练习 2.2.11 如果 $p \nmid ab$, 则 $(a, pb)_p = \left(\frac{a}{p}\right), (pa, pb)_p = (-ab, p)_p$.

当 $v = 2$ 时, 回忆 \mathbb{Q}_2^\times 中一个数是平方当且仅当其赋值为偶数且模 8 同余 1. 类似地, 若 $2 \nmid ab$, 我们有 $(2, 2)_2 = 1$,

$$(a, b)_2 = \begin{cases} 1 & a \equiv 1 \pmod{4} \text{ 或 } b \equiv 1 \pmod{4} \\ -1 & a \equiv b \equiv -1 \pmod{4}, \end{cases}$$

$$(a, 2b)_2 = \begin{cases} 1 & a \equiv 1 \pmod{8} \text{ 或 } a \equiv 1 - 2b \pmod{8} \\ -1 & \text{其它情形} \end{cases}$$

通过我们的分析, 我们发现:

命题 2.29

我们有 $(a, b)_v(a, c)_v = (a, bc)_v$.



定理 2.30 (乘积公式)

设 $a, b \in \mathbb{Q}^\times$, 则除去有限个 v 外, $(a, b)_v = 1$, 且

$$\prod_v (a, b)_v = 1.$$



证明 当 $v = p$ 不出现在 a 和 b 的分子或分母的素因子中时, 我们有 $(a, b)_v = 1$. 由于希尔伯特符号的可乘性, 我们只需要验证下列情形:

(1) $a = b = -1$. 此时 $(-1, -1)_\infty = (-1, -1)_2 = -1$, 其它 v 处为 1. 这也推出 $\prod_v (a, a)_v = \prod_v (a, -1)_v = 1$.

(2) $a = -1, b = 2$. 此时 $a + b - 1 = 0$, 因此 $(-1, 2)_v = 1$.

(3) $a = -1, b = p > 2$. 此时 $(-1, p)_\infty = 1, (-1, p)_2 = (-1)^{(p-1)/2} = \left(\frac{-1}{p}\right) = (-1, p)_p$. 由此可知乘积公式对于 $(-1, n)$ 成立, 因此对于 (n, n) 也成立.

(4) $a = 2, b = p > 2$. 此时 $(2, p)_\infty = 1, (2, p)_2 = (-1)^{(p^2-1)/8} = \left(\frac{2}{p}\right) = (2, p)_p$.

(5) $a = p, b = q \neq p$. 此时

$$\prod_v (p, q)_v = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = 1,$$

即二次互反律. □

例题 2.6 我们来看 $x^2 + 5y^2 = n \neq 0$. 由 $(-5, n)_2 = 1$ 知 $n \equiv 1 \pmod{4}$ 或 $n \equiv 6 \pmod{8}$; 由 $(-5, n)_5 = 1$ 知 $n = m$ 或 $5m, m \equiv \pm 1 \pmod{5}$; 对于奇素数 $q \mid n, q \neq 5$, 由 $(-5, n)_q = 1$ 知 $\left(\frac{-5}{q}\right) = 1, q \equiv 1, 3, 7, 9 \pmod{20}$. 因此

$$n = p_1 \dots p_{2k} q_1 \dots q_m \lambda^2,$$

素数 $p_i \equiv 2, 3, 7 \pmod{20}, q_i \equiv 1, 5, 9 \pmod{20}, \lambda$ 为任意正整数.

👉 **练习 2.2.12** 何时 $x^2 + 7y^2 = n \neq 0$ 有有理点? 这等价于 $x^2 + 7y^2 = n$ 有整数解吗?

👉 **练习 2.2.13** 何时 $x^2 + 26y^2 = n \neq 0$ 有有理点?

§2.3 分歧理论

我们已经知道了 \mathbb{Q} 的所有素位. 对于数域 K 而言, 它的赋值 w 限制在 \mathbb{Q} 上是 \mathbb{Q} 的一个赋值 v , 我们记 $w|v$. 如果 $v = \infty$, 则 w 是一个阿基米德赋值, 它的等价类是 K 的一个无穷素位. 如果 $v = p$, 我们称 w 为有限素位. 不妨设 w 是归一化离散赋值, 则

$$\mathfrak{p} = \{x \in \mathcal{O}_K \mid w(x) \geq 1\}$$

是 \mathcal{O}_K 的素理想, 且 $p\mathcal{O}_K \subset \mathfrak{p}$. 因此作为理想 $\mathfrak{p} \mid p\mathcal{O}_K$. 反之, 任一 \mathcal{O}_K 的素理想 \mathfrak{p} 诱导了 K 的赋值

$$w(x) = \min \{n \mid x \in \mathfrak{p}^n\}.$$

因此 K 的有限素位和它的素理想一一对应. 我们不加区分地用 \mathfrak{p} 来表示素理想或素位.

设 L/K 是数域的有限扩张, 则同样的分析告诉我们 $\mathfrak{P} \mid \mathfrak{p}$ 当且仅当 \mathfrak{p} 诱导的 K 上赋值是 \mathfrak{P} 诱导的 L 上赋值的限制 (等价意义下). 因此 $\mathfrak{P} \mid \mathfrak{p}$ 既可以表示理想的整除也可以表示素位的延拓. 本节中我们将研究完备域扩张下的素位变化行为.

§2.3.1 赋值的延拓

定理 2.31 (奥斯特洛斯基定理)

完备阿基米德赋值域只有 \mathbb{R} 和 \mathbb{C} .



证明 由于 $\mathbb{Q} \subseteq K$, 因此不妨设 $\mathbb{R} \subseteq K$ 且 $|\cdot|$ 延拓 $|\cdot|_{\mathbb{R}}$. 对任意 $\xi \in K$, 定义

$$f: \mathbb{C} \rightarrow \mathbb{R} \\ z \mapsto |\xi^2 - (z + \bar{z})\xi + z\bar{z}|.$$

由阿基米德性质知 $z \rightarrow \infty$ 时, $f(z) \rightarrow \infty$. 因此 f 的下确界 $m \geq 0$ 是可达的. 如果 $m > 0, S = \{z \in \mathbb{C} \mid f(z) = m\}$ 为有界闭子集, 因此存在 $z_0 \in S$ 使得 $|z_0| \geq |z|, \forall z \in S$. 设

$$g(x) = x^2 - (z_0 + \bar{z}_0)x + z_0\bar{z}_0 + \varepsilon, \quad 0 < \varepsilon < m$$

的根为 z_1, \bar{z}_1 , 则 $z_1\bar{z}_1 = z_0\bar{z}_0 + \varepsilon, |z_1| > |z_0|$.

考虑多项式

$$G(x) = [g(x) - \varepsilon]^n - (-\varepsilon)^n \in \mathbb{R}[x].$$

设它的根为 $\alpha_1 = z_1, \alpha_2, \dots, \alpha_{2n} \in \mathbb{C}$, 则

$$G(x)^2 = \prod_{i=1}^{2n} (x^2 - (\alpha_i + \bar{\alpha}_i)x + \alpha_i \bar{\alpha}_i),$$

$$|G(\xi)|^2 = \prod_{i=1}^{2n} f(\alpha_i) \geq m^{2n} \cdot \frac{f(z_1)}{m}.$$

另一方面,

$$|G(\xi)| \leq f(z_0)^n + \varepsilon^n = m^n + \varepsilon^n,$$

因此 $f(z_1)/m \leq (1 + (\frac{\varepsilon}{m})^n)^2$. 令 $n \rightarrow \infty$, $f(z_1) \leq m$, 这与 $|z_1| > |z_0|$ 矛盾. 因此 $m = 0$, K 中元素均为 \mathbb{R} 上二次多项式的根. \square

命题 2.32

设 K 是完备非阿赋值域. 如果 $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$ 不可约, $a_0 a_n \neq 0$, 则

$$|f| = \max\{|a_0|, |a_n|\}.$$

特别地, 如果 $a_n = 1, a_0 \in \mathcal{O}_K$, 则 $f \in \mathcal{O}_K[x]$.



证明 不妨设 $f \in \mathcal{O}_K[x], |f| = 1$. 设 $r = \min\{r : |a_r| = 1\}$, 则

$$f(x) \equiv x^r (a_r + a_{r+1}x + \dots + a_n x^{n-r}) \pmod{\pi}.$$

如果 $|a_0|, |a_n| < 1$, 则 $0 < r < n$, 由亨泽尔引理 2.15, f 可约, 矛盾! \square

由此, 我们有如下定理

定理 2.33

完备非阿赋值域 K 上赋值 $|\cdot|$ 可以唯一延拓至 K 的有限次扩张 L ,

$$|\alpha| = |\mathbf{N}_{L/K}(\alpha)|^{1/[L:K]},$$

且 L 在该赋值下完备.



证明 如果是阿基米德赋值, 则由定理 2.31 知 $K = \mathbb{R}, \mathbb{C}$. 假设 K 是非阿赋值域, \mathcal{O}_L 是 \mathcal{O}_K 在 L 中的整闭包. 对于 $\alpha \in L$, 如果 $\mathbf{N}_{L/K}(\alpha) \in \mathcal{O}_K$, 则由命题 2.32 知其极小多项式属于 $\mathcal{O}_K[x]$, 因此

$$\mathcal{O}_L = \{x \in L \mid \mathbf{N}_{L/K}(x) \in \mathcal{O}_K\}.$$

我们需要证明强三角不等式 $|x + y| \leq \max\{|x|, |y|\}$, 换言之, 如果 $|x| \leq 1$, 则 $|x + 1| \leq 1$, 即 $x \in \mathcal{O}_L \implies x + 1 \in \mathcal{O}_L$. 最后, 显然 \mathcal{O}_L 是延拓后的赋值的赋值环.

唯一性由赋范线性空间上范数的唯一性可得. 容易知道 L 作为 K 上线性空间在最大模下是完备的, 因此它是完备赋值域. \square

完备非阿赋值域上的多项式的在其分裂域上的根的赋值可以由所谓的**牛顿折线**确定. 设 $f(x) = \sum_{i=0}^n a_i x^i \in K[x]$, 点集

$$\{(i, v(a_i)) \mid 0 \leq i \leq n\}$$

的下凸包络被称为 f 的牛顿折线. 换言之, 它是定义在区间 $[0, n]$ 上的分段线性函数, 折点为上述点集中的点, 斜率递增, 且上述点集中没有点落在它图像的下方.

命题 2.34

设 $a_0 a_n \neq 0$. 多项式 f 在它的分裂域上的根的赋值的相反数和它的牛顿折线在每个 $[i, i+1]$ 上的斜率一一对应.



证明 不妨设 $a_n = 1$, w 为 f 分裂域上延拓 v 的赋值. 设 f 的根中

$$\begin{aligned} w(\alpha_1), \dots, w(\alpha_{s_1}) &= m_1, \\ w(\alpha_{s_1+1}), \dots, w(\alpha_{s_2}) &= m_2, \\ &\vdots \\ w(\alpha_{s_{t-1}+1}), \dots, w(\alpha_{s_t}) &= m_t, \end{aligned}$$

其中 $m_1 < m_2 < \dots < m_t$, $s_t = n$. 于是

$$\begin{aligned} v(a_{n-1}) &\geq \min \{w(\alpha_i)\} = m_1, \\ v(a_{n-2}) &\geq \min \{w(\alpha_i \alpha_j)\} = 2m_1, \\ &\vdots \\ v(a_{n-s_1}) &= \min \{w(\alpha_{i_1} \cdots \alpha_{i_{s_1}})\} = s_1 m_1. \end{aligned}$$

同样,

$$\begin{aligned} v(a_{n-s_1-1}) &\geq \min \{w(\alpha_{i_1} \cdots \alpha_{i_{s_1+1}})\} = s_1 m_1 + m_2, \\ v(a_{n-s_1-2}) &\geq \min \{w(\alpha_{i_1} \cdots \alpha_{i_{s_1+2}})\} = s_1 m_1 + 2m_2, \\ &\vdots \\ v(a_{n-s_2}) &= \min \{w(\alpha_{i_1} \cdots \alpha_{i_{s_2}})\} = s_1 m_1 + (s_2 - s_1) m_2. \end{aligned}$$

依次下去可知 f 的牛顿折线为

$$(n, 0), (n - s_1, s_1 m_1), (n - s_2, s_1 m_1 + (s_2 - s_1) m_2), \dots$$

的连线, 从而命题得证. □

练习 2.3.1 如果首一多项式 $f(T) = \sum_{i=0}^n a_i x^{n-i} \in \mathbb{Z}[T]$ 满足 $\gcd(v_p(a_n), p) = 1$ 以及 $v(a_i) \geq i v(a_n)/n$, 则称之为关于 p 的**广义艾森斯坦多项式**. 这样的多项式一定是不可约的.

§2.3.2 p 进代数闭完备域

我们来了解下 p 进世界的复数域. 由于 \mathbb{Q}_p 上的赋值可以唯一延拓至其任一有限代数扩张上, 因此可以延拓至 $\overline{\mathbb{Q}_p}$ 上. 令

$$|\gamma|_p := |\mathbf{N}_{\mathbb{Q}_p(\gamma)/\mathbb{Q}_p}(\gamma)|_p^{1/[\mathbb{Q}_p(\gamma):\mathbb{Q}_p]},$$

则它是 \mathbb{Q}_p 上赋值在 $\overline{\mathbb{Q}_p}$ 上的延拓. 我们知道 $\mathbb{Q}_\infty = \mathbb{R}, \overline{\mathbb{Q}_\infty} = \mathbb{C}$ 是完备的, 然而 $\overline{\mathbb{Q}_p}$ 却不是完备的. 记 $\overline{\mathbb{Q}_p}$ 的完备化记为 \mathbb{C}_p .

练习 2.3.2 证明 $\overline{\mathbb{Q}}$ 在 $\overline{\mathbb{Q}_p}$ 中稠密且 $\overline{\mathbb{Q}_p}$ 不是完备的.

定理 2.35

\mathbb{C}_p 是代数闭域.



引理 2.36 (克拉斯纳引理)

设 F 为完备非阿赋值域, $E \subseteq F$ 是一个闭子域. 假设 $\alpha, \beta \in F$ 满足对 α 的任意共轭元 $\alpha' \neq \alpha$, 有 $|\beta - \alpha| < |\alpha' - \alpha|$, 且 α 在 E 上可分, 则 $\alpha \in E(\beta)$.



证明 令 $E' = E(\beta)$, $\gamma = \beta - \alpha$. 则 $E'(\gamma) = E'(\alpha)$. 由于 $\gamma' = \beta - \alpha'$ 为 γ 在 E' 上的共轭, $|\gamma'| = |\gamma|$. 因此

$$|\beta - \alpha| = |\gamma| \geq |\gamma' - \gamma| = |\alpha' - \alpha|,$$

这迫使 $\alpha' = \alpha$, $\gamma' = \gamma \in E'$, 因此 $\alpha \in E'$. □

定理 2.35 的证明 设

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = \prod_{i=1}^n (x - \alpha_i) \in \mathbb{C}_p[x].$$

不妨设 $f(x) \in \mathcal{O}_{\mathbb{C}_p}[x]$. 令 $C' = \mathbb{C}_p(\alpha_1, \dots, \alpha_n)$ 为 f 的分裂域, $r = \max_{i \neq j} \{v(\alpha_i - \alpha_j)\}$. 由 \mathbb{C}_p 的完备性, 存在 $b_i \in \overline{\mathbb{Q}}$ 使得 $v(a_i - b_i) > nr$. 令

$$g = x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in \overline{\mathbb{Q}}[x].$$

设 $\beta \in \overline{\mathbb{Q}}$ 为 g 的一个根. 令 $\alpha \in C'$ 为 f 的根当中 $v(\beta - \alpha)$ 最大的一个根, 即 $v(\beta - \alpha) \geq v(\beta - \alpha_i)$. 由

$$\sum_{i=1}^n v(\beta - \alpha_i) = v(f(\beta)) = v(f(\beta) - g(\beta)) > nr$$

知 $v(\beta - \alpha) > r$. 由克拉斯纳引理, $\alpha \in \mathbb{C}_p(\beta) = \mathbb{C}_p$. □

定义 2.37 (球完备)

如果一个完备度量空间中下降的闭球套交均非空, 则称其为球完备的.



🔗 **练习 2.3.3** 例如 \mathbb{C} 和 \mathbb{Q}_p 均是球完备的.

命题 2.38

\mathbb{C}_p 不是球完备的.



证明 令 $\{r_n\}$ 为严格递减的有理数序列, 其极限为 $r = \lim r_n > 0$. 球 $B(0, r_0)$ 中存在两个不交的半径为 r_1 的球, 记为 B_0 和 B_1 . 同样, 球 B_i 中存在两个不交的半径为 r_2 的球, 记为 B_{i0} 和 B_{i1} . 依次下去我们对于每一个序列 $(i_0, i_1, \dots) \in \{0, 1\}^{\mathbb{N}}$, 都对应一个闭球套序列

$$B_{i_0} \supset B_{i_0 i_1} \supset \cdots$$

它们的交两两不同. 如果它们的交非空, 则易知交为半径为 r 的闭球. 但 $B(0, r_0)$ 中一个可数稠密子集均与每一个这样的交相交, 因此这样交出来的非空集合只有至多可数个不同的闭球. 而这样的序列数量是不可数的, 因此至少有一个闭球套交为空集. □

🔗 **练习 2.3.4** 如果完备度量空间中闭球套的半径趋于 0, 则闭球套的交非空.

对于 p 进分析感兴趣的可以阅读 [3, 17].

§2.3.3 非分歧扩张

设 $\mathcal{O}_K, \mathfrak{p}, \pi, v, \kappa$ 为完备离散赋值域 K 的赋值环、极大理想、素元、规范化离散赋值、剩余域. 设 L 为 K 的 n 次可分扩张, 则 v 可以唯一延拓为 L 上赋值 w ,

$$w(\alpha) = \frac{1}{n}v(\mathbf{N}_{L/K}(\alpha)).$$

设 $\mathcal{O}_L, \mathfrak{P}, \Pi, \kappa_L$ 为 L 的赋值环、极大理想、素元、剩余域. 称

$$e = e(L/K) = [w(L^\times) : v(K^\times)] = w(\Pi)$$

为 L/K 的**分歧指数**, 显然 $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e$. 剩余域的扩张次数

$$f = f(L/K) = [\kappa_L : \kappa]$$

被称为**惯性指数**.

命题 2.39

我们有 $ef = [L : K]$.



证明 由于主理想整环上的有限生成无挠模均为自由模, 因此 \mathcal{O}_L 是秩 n 自由 \mathcal{O}_K 模,

$$\begin{aligned} n &= \dim_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\mathfrak{p}) = \dim_{\mathcal{O}_K/\mathfrak{p}}(\mathcal{O}_L/\Pi^e\mathcal{O}_L) \\ &= \sum_{i=0}^{e-1} \dim_{\mathcal{O}_K/\mathfrak{p}}(\Pi^i\mathcal{O}_L/\Pi^{i+1}\mathcal{O}_L) = \sum_{i=0}^{e-1} f = ef. \end{aligned}$$

命题得证. □

如果 $e = 1, f = [L : K]$, 且 κ_L/κ 可分, 称 L/K **非分歧(惯性)**. 如果 $e = [L : K], f = 1$, 称 L/K **完全分歧**. 显然非分歧扩张的子扩张非分歧.

命题 2.40

设 $L, K' \subseteq \bar{K}$ 为 K 的有限扩张. 如果 L/K 非分歧, 则 LK'/K' 非分歧.



证明 设 $\mathfrak{p}', \mathfrak{P}'$ 是 $K', L' = LK'$ 的极大理想. 由于 κ_L/κ 可分, 存在 $\bar{\alpha} \in \kappa_L$ 使得 $\kappa_L = \kappa(\bar{\alpha})$. 设 $\bar{f}(x) \in \kappa[x]$ 为 $\bar{\alpha}$ 的极小多项式, 设 $f(x) \in \mathcal{O}_K[x]$ 为 \bar{f} 的首一提升, 则由亨泽尔引理, 存在 f 的一个根 $\alpha \in \mathcal{O}_L$ 提升 $\bar{\alpha}$. 显然 f 是 α 的极小多项式. 于是

$$f_{L/K} = \deg \bar{f} = \deg f = [K(\alpha) : K] \leq [L : K] = f_{L/K},$$

因此 $L = K(\alpha)$.

现在 $L' = K'(\alpha)$. 设 α 在 K' 上的极小多项式为 $g(x) \in \mathcal{O}_{K'}[x], \bar{g} = g \bmod \mathfrak{p}' \in \kappa_{K'}[x]$. 由于 $\bar{g} \mid \bar{f}$, 因此 \bar{g} 可分. 由亨泽尔引理, \bar{g} 不可约. 因此

$$f_{L'/K'} \leq [L' : K'] = \deg g = \deg \bar{g} = [\kappa_{K'}(\bar{\alpha}) : \kappa_{K'}] \leq f_{L'/K'},$$

这意味着 $f_{L'/K'} = [L' : K'], L'/K'$ 非分歧. □

推论 2.41

非分歧扩张的复合仍然是非分歧的.



由此, 如果一个无限扩张的任一子扩张均非分歧, 我们称该扩张是**非分歧的**.

定义 2.42 (极大非分歧扩张)

设 L/K 为代数扩张, 则所有 L 中 K 的非分歧子扩张的复合构成 K 在 L 中极大非分歧扩张 T .

**命题 2.43**

T 的剩余域是 κ 在 κ_L 中的可分闭包 κ^s .



证明 设 λ 是 T 的剩余域, $\bar{\alpha} \in \kappa_L$ 在 κ 中可分. 由命题 2.40 的证明中可以看出, $[K(\alpha) : K] = f_{K(\alpha)/K}$, $K(\alpha)/K$ 非分歧. 因此 $K(\alpha) \subseteq T$, $\bar{\alpha} \in \lambda$. \square

命题 2.44

如果 L/K 是混合特征完备离散赋值域的有限扩张, 且 κ_L 是完全域, 则 $KW(\kappa_L)$ 是 K 在 L 中极大非分歧扩张.



证明 由于 κ_L 是完全域, κ_L/\mathbb{F}_p 可分, 于是 $\text{Frac } W(\kappa_L) \subseteq L$ 是剩余域为 κ_L 的 \mathbb{Q}_p 的非分歧扩张, 因此 $KW(\kappa_L)$ 是 K 的非分歧扩张. 又因为 $KW(\kappa_L)$ 的剩余域和 L 相同, 因此命题成立. \square

练习 2.3.5 设 K 是完备离散赋值域, 剩余域为 κ . 设 K^{ur} 是 K 在 \bar{K} 中的极大非分歧扩张, κ^s 是 κ 的可分闭包. 证明 K^{ur}/K 的所有子扩张和 κ^s/κ 的所有子扩张一一对应.

§2.3.4 温分歧扩张

设 K 是完备离散赋值域, L 为 K 的有限可分扩张. 我们假设 $p = \text{char } \kappa > 0$.

定义 2.45 (温分歧)

如果 L/K 的分歧指数和 p 互素, 且 κ_L/κ 可分, 称 L/K 温分歧. 特别地, 非分歧扩张是温分歧的.

**命题 2.46**

设 $L, L' \subseteq \bar{K}$ 为 K 的有限扩张. 如果 L/K 温分歧, 则 LK'/K' 温分歧.



该命题可以直接由如下引理得到.

引理 2.47

L/K 温分歧当且仅当 L/T 形如

$$L = T(\sqrt[m_1]{a_1}, \dots, \sqrt[m_r]{a_r}), \quad p \nmid m_i.$$



证明 不妨设 $K = T$, $n = [L : K]$. 设 $\omega_1, \dots, \omega_r$ 是 $w(L^\times)/v(K^\times)$ 的一组代表元, m_i 是 ω_i 在 $w(L^\times)/v(K^\times)$ 的阶. 由于 $w(L^\times) = \frac{1}{n}v(\mathbf{N}_{L/K}(L^\times)) \subseteq \frac{1}{n}v(K^\times)$, 因此 $m_i \mid n$. 设 $\gamma_i \in L^\times$, $w(\gamma_i) = \omega_i$, 则存在 $c_i \in K^\times$ 使得 $w(\alpha_i^{m_i}) = v(c_i)$, 因此 $\gamma_i^{m_i} = c_i \epsilon_i$, $\epsilon_i \in \mathcal{O}_L^\times$. 由于 $\kappa = \kappa_L$, 存在 $b_i \in \mathcal{O}_K^\times$ 使得 $\epsilon_i = b_i u_i$, $\bar{u}_i = 1 \in \kappa_L$. 由亨泽尔引理, $x^m - u_i = 0$ 在 L 中有解 β_i . 令 $\alpha_i = \gamma_i \beta_i^{-1}$, 则 $w(\alpha_i) = \omega_i$, $\alpha_i^{m_i} = b_i c_i \in K$, 因此 $K(\sqrt[m_1]{a_1}, \dots, \sqrt[m_r]{a_r}) \subseteq L$. 而二者的剩余域和赋值的像相同, 因此二者相同. \square

推论 2.48

温分歧扩张的复合仍然是温分歧的.



由此, 如果一个无限扩张的任一子扩张均温分歧, 我们称该扩张是温分歧的.

定义 2.49 (极大温分歧扩张)

设 L/K 为代数扩张, 则所有 L 中 K 的温分歧子扩张的复合构成 K 在 L 中极大温分歧扩张 V .



令 $w(L^\times)^{(p)}$ 为 $w(L^\times)$ 中在 $w(L^\times)/v(K^\times)$ 中的像阶与 p 互素的元素构成.

命题 2.50

V 的剩余域是 κ 在 κ_L 中的可分闭包 κ^s 且 $w(V^\times) = w(L^\times)^{(p)}$.



证明 不妨设 L/K 有限, 且 $T = K$. 此时, $p \nmid e(V/K) = \#w(V^\times)/v(K^\times)$, 因此 $w(V^\times) \subseteq w(L^\times)^{(p)}$. 反之, 对任意 $\omega \in w(L^\times)^{(p)}$, 存在 $\alpha \in L, a = \alpha^m \in K, (m, p) = 1$ 使得 $w(\alpha) = \omega$, 因此 $\alpha \in V, \omega \in w(V^\times)$.

□

我们总结一下 L/K 中子扩张的剩余域和赋值群的变化

$$\begin{aligned} K &\subseteq T \subseteq V \subseteq L \\ \kappa &\subseteq \kappa^s = \kappa^s \subseteq \kappa_L \\ v(K^\times) &= w(T^\times) \subseteq w(L^\times)^{(p)} \subseteq w(L^\times). \end{aligned}$$

设 $e(L/K) = e'p^a, p \nmid e'$, 则 $e' = e(V/K)$. 如果 $L \neq V$, 称 L/K 野分歧.

练习 2.3.6 设 L/K 是一个完全分歧且是温分歧的扩张, $w|_v$ 是 L 和 K 的赋值. 证明 L/K 的所有子扩张和 $w(L^\times)/v(K^\times)$ 的所有子群一一对应.

§2.4 整体域上的分歧理论

§2.4.1 赋值的分歧

回忆数域 K 上的任何一个嵌入 $\tau: K \hookrightarrow \mathbb{C}$ 诱导了 K 上的一个赋值, 其中 τ 和 τ' 诱导了相同的赋值当且仅当 $\tau' = \tau \circ \sigma, \sigma \in G(\mathbb{C}/\mathbb{R})$. 这样的赋值等价类我们称之为无穷素位.

我们考虑一般的有限可分域扩张 $L/K, v$ 是 K 的一个赋值. v 可以唯一地延拓到 \overline{K}_v 上, 记为 \bar{v} . 任一嵌入

$$\tau \in \text{Hom}_K(L, \overline{K}_v)$$

均诱导了 L 的赋值 $w = \bar{v} \circ \tau$, 它可以唯一连续地延拓至 L_w 上. 对于任意 $\sigma \in G(\overline{K}_v/K_v), \sigma \circ \tau: L \hookrightarrow \overline{K}_v$ 也是一个嵌入, 我们称 τ 和 $\sigma \circ \tau$ 是共轭的. 我们可以看出, 这里的 \overline{K}_v 相当于无穷素位中 \mathbb{C} 的地位. 我们有如下命题来判断何时不同的嵌入对应同一素位.

命题 2.51

设 L/K 为有限可分域扩张, v 是 K 的一个赋值.

- (1) 任一 v 在 L 上的延拓均来自 $w = \bar{v} \circ \tau, \tau: L \hookrightarrow \overline{K}_v$.
- (2) $\bar{v} \circ \tau$ 和 $\bar{v} \circ \tau'$ 等价当且仅当 τ, τ' 共轭.



证明 (1) 设 w 是 v 在 L 上的延拓, L_w 为相应的完备化, w 在 L_w 上的延拓仍记为 w . 则 w 是 v 从 K_v 到 L_w 的唯一延拓. 任取一个嵌入 $\tau: L_w \hookrightarrow \overline{K}_v$, 则 $\bar{v} \circ \tau = w$. τ 在 L 上的限制诱导了 L 上的 $\bar{v} \circ \tau = w$.

(2) 设 τ 和 $\sigma \circ \tau$ 是两个共轭嵌入 $L \hookrightarrow \overline{K}_v$. 由于 v 在 \overline{K}_v 上的延拓唯一, 因此 $\bar{v} = \bar{v} \circ \sigma, \bar{v} \circ \tau = \bar{v} \circ \sigma \circ \tau$. 反之, 若 $\bar{v} \circ \tau = \bar{v} \circ \tau'$. 设 $\sigma: \tau L \xrightarrow{\sim} \tau' L$ 为保持 K 不动的同构, 即 $\sigma = \tau' \circ \tau^{-1}$. 则 σ 可以延拓为保持

K_v 不动的同构

$$\sigma : \tau L \cdot K_v \rightarrow \tau' L \cdot K_v.$$

实际上, 由于 τL 在 $\tau L \cdot K_v$ 中稠密, 任意 $x \in \tau L \cdot K_v$ 可表为

$$x = \lim_{n \rightarrow \infty} \tau x_n, \quad x_n \in L.$$

由于 $\bar{v} \circ \tau = \bar{v} \circ \tau'$, 因此 $\tau' x_n = \sigma \tau x_n$ 收敛至 $\sigma x \in \tau' L \cdot K_v$. 因此我们得到了 σ 的延拓. 我们将 σ 延拓为 \bar{K}_v 上的自同构 $\tilde{\sigma}$, 则 $\tau' = \tilde{\sigma} \circ \tau$, 因此 τ, τ' 共轭. \square

设 $L = K(\theta)$, $f(x) \in K[x]$ 为 θ 的极小多项式. 设 $f(x)$ 在 $K_v[x]$ 上分解为

$$f(x) = f_1(x)^{m_1} \cdots f_r(x)^{m_r}.$$

由于 L/K 可分, $m_i = 1$. 对于每一个嵌入 $\tau : L \hookrightarrow \bar{K}_v$, $\tau(\theta)$ 是 $f(x)$ 在 \bar{K}_v 中的一个根. 如果两个嵌入 τ, τ' 共轭, 则 $\tau(\theta), \tau'(\theta) \in \bar{K}_v$ 在 K_v 之上共轭, 即它们是同一个不可约多项式 $f_i(x)$ 的根. 因此

命题 2.52

K 的有限可分扩张 $L = K(\theta)$ 在 v 之上的赋值一一对应于 θ 的极小多项式 $f(x)$ 在 $K_v[x]$ 中分解出的不可约因子.



对每一个 f_i , 设 $\theta_i \in \bar{K}_v$ 为其一个根, 令

$$\tau_i : L \rightarrow \bar{K}_v, \quad \theta \mapsto \theta_i$$

为其对应的嵌入. 则 $w_i = \bar{v} \circ \tau_i$ 为其对应的赋值, τ_i 可以延拓为 $L_{w_i} \xrightarrow{\sim} K_v(\theta_i)$.

我们记 $w|v$ 表示 L 的赋值 w 是 K 的赋值 v 的一个延拓. 每一个 $L \hookrightarrow L_w$ 诱导了 $L \otimes_K K_v \rightarrow L_w$, 因此有

$$\varphi : L \otimes_K K_v \rightarrow \prod_{w|v} L_w.$$

命题 2.53

如果 L/K 有限可分, 则 $L \otimes_K K_v \xrightarrow{\sim} \prod_{w|v} L_w$.



证明 对每一个 w , 固定 $L_w \hookrightarrow \bar{K}_v$. 记 f_w, α_w 为其对应的 f 在 $K_v[X]$ 中的因式和 θ 在 $L \hookrightarrow L_w$ 下的像. 我们有交换图

$$\begin{array}{ccc} K_v[X]/(f) & \longrightarrow & \prod_{w|v} K_v[X]/(f_w) \\ \downarrow X \mapsto \theta \otimes 1 \simeq & & \simeq \downarrow X \mapsto \theta_w \\ L \otimes_K K_v & \longrightarrow & \prod_{w|v} L_w, \end{array}$$

其中第一行由中国剩余定理给出. \square

由此可得如下推论:

推论 2.54

如果 L/K 有限可分, 则

$$[L : K] = \sum_{w|v} [L_w : K_v]$$

且

$$\mathbf{N}_{L/K}(\alpha) = \prod_{w|v} \mathbf{N}_{L_w/K_v}(\alpha), \quad \mathrm{Tr}_{L/K}(\alpha) = \prod_{w|v} \mathrm{Tr}_{L_w/K_v}(\alpha).$$



命题 2.55

如果 v 非阿, e_w, f_w 为 L_w/K_v 的分歧指数和惯性指数, 则

$$[L : K] = \sum_{w|v} e_w f_w.$$



考虑数域 K , 回忆 $\mathbf{N}a = [\mathcal{O}_K : a]$. 对于有限素位 \mathfrak{p} , $\mathbf{N}\mathfrak{p} = \#\kappa(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$. 定义

$$|a|_{\mathfrak{p}} = \mathbf{N}\mathfrak{p}^{-v_{\mathfrak{p}}(a)},$$

其中 $v_{\mathfrak{p}}$ 是 $K_{\mathfrak{p}}$ 的归一化赋值. 对于无穷素位 $\tau : K \hookrightarrow \mathbb{C}$,

$$|a|_{\mathbb{R}} = |\tau a|, \quad |a|_{\mathbb{C}} = |\tau a|^2.$$

命题 2.56 (乘积公式)

对于任意 $a \in K^{\times}$, 对几乎所有素位 v , $|a|_v = 1$, 且

$$\prod_v |a|_v = 1.$$



证明 由推论 2.54 可知

$$\mathbf{N}_{K/\mathbb{Q}}(a) = \prod_{w|v} \mathbf{N}_{K_w/\mathbb{Q}_v}(a).$$

而 $|a|_w = |\mathbf{N}_{K_w/\mathbb{Q}_v}(a)|_v$, 因此该命题可以约化到 \mathbb{Q} 的情形, 而这是显然的. \square

我们来看数域情形. 设 L/K 是数域的 n 次有限扩张. 对于 K 的有限素位 $v = \mathfrak{p}$, 如果 $w = \mathfrak{P} | v$, 则 $\mathfrak{p} \subset \mathfrak{P}$, $\mathfrak{P} = \mathfrak{P}_i$, 其中

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

其中 $e_i = e(\mathfrak{P}_i/\mathfrak{p}) = e(L_{\mathfrak{P}_i}/K_{\mathfrak{p}})$.

设 $L = K(\theta)$, $\theta \in \mathcal{O}_L$, $f(x) \in \mathcal{O}_K[x]$ 为 θ 的极小多项式. 考虑分解

$$\bar{f}(x) = \bar{p}_1(x)^{e_1} \cdots \bar{p}_r(x)^{e_r} \in \mathcal{O}_K/\mathfrak{p}[x].$$

注意这里 $p_i(x)^{e_i} \equiv f_i(x) \pmod{\mathfrak{p}}$. 设 $\mathcal{O} := \mathcal{O}_K[\theta] \subset \mathcal{O}_L$, 我们假设 \mathfrak{p} 与

$$\mathfrak{F} = \{\alpha \in \mathcal{O}_L \mid \alpha\mathcal{O}_L \subset \mathcal{O}[\theta]\}$$

互素. 设 p_i 是 \bar{p}_i 的首一提升, 则我们有

$$\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + p_i(\theta)\mathcal{O}_L,$$

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

证明 设 $\mathcal{O} = \mathcal{O}_K[\theta], \kappa = \mathcal{O}_K/\mathfrak{p}$, 则

$$R := \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \simeq \mathcal{O}/\mathfrak{p}\mathcal{O} \cong \kappa[x]/(\bar{f}(x)).$$

实际上, 由于 $\mathfrak{p}\mathcal{O}_L + \mathfrak{F} = \mathcal{O}_L$, 而 $\mathfrak{F} \subseteq \mathcal{O}$, 因此 $\mathcal{O}/\mathfrak{p}\mathcal{O} \rightarrow \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ 是满射. 它的核为 $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O} = (\mathfrak{p}\mathcal{O}_L + \mathfrak{F})(\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}) \subseteq \mathfrak{p}\mathcal{O} \subseteq \mathfrak{p}\mathcal{O}_L \cap \mathcal{O}$, 因此它是单射. 第二个同构是显然的, 因为两边都是 $\mathcal{O}_K[\theta]/(\mathfrak{p}, \bar{f}(x))$.

由中国剩余定理可知

$$\kappa[x]/(\bar{f}(x)) \cong \bigoplus_{i=1}^r \kappa[x]/(\bar{p}_i(x)^{e_i}).$$

因此 R 的非零素理想为 \bar{p}_i 生成的主理想, 且 $[R/\bar{p}_i : \kappa] = \deg \bar{p}_i$. 我们有

$$(0) = (\bar{f}) = \bigcap_{i=1}^r (\bar{p}_i)^{e_i}.$$

我们将它们通过映射 $\mathcal{O}_L \rightarrow \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = R$ 提升为

$$\mathfrak{p}\mathcal{O}_L \supseteq \bigcap_{i=1}^r \mathfrak{P}_i^{e_i},$$

其中 $\mathfrak{P}_i = p_i(\theta)\mathcal{O}_L + \mathfrak{p}\mathcal{O}_L$ 是所有整除 $\mathfrak{p}\mathcal{O}_L$ 的素理想. 由于 $\sum e_i f_i = n$, 因此两边的大小相等, 故 $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$. \square

如果 $r = e_1 = 1$, 称 \mathfrak{p} 惯性. 如果所有的 $e_i = f_i = 1$, 即 $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_n$, 我们称 \mathfrak{p} 在 L 中完全分裂. 如果 $e_i = 1$, 我们称 \mathfrak{P}_i 在 K 上非分歧, 注意此时剩余域扩张可分自动满足; 否则称之为分歧. 如果 $r = f_1 = 1, e_1 = n$, 称 \mathfrak{P}_1 完全分歧.

命题 2.57

设 L/K 是数域的有限扩张, 则只有有限多个 K 的素理想在 L 中分歧.



证明 设 $L = K(\theta), \theta \in \mathcal{O}_L, d = \text{disc}(1, \theta, \dots, \theta^{n-1}) \in \mathcal{O}_K$. 则对于与 $d\mathfrak{F}$ 互素的素理想 $\mathfrak{p}, \bar{f}(x) \in \mathcal{O}_K/\mathfrak{p}[x]$ 的判别式非零, 因此它没有重根, $e_i = 1$, 从而 \mathfrak{p} 非分歧. \square

注 实际上 L/K 中素理想分歧当且仅当 \mathfrak{p} 整除 L/K 的判别式.

练习 2.4.1 (1) 对于任意数域 K 的有限个素理想 $\mathfrak{p}_1, \dots, \mathfrak{p}_r$, 存在 n 次扩张 L/K 使得 $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ 惯性.

(2) 构造 \mathbb{Q} 的无限代数扩张 L 使得对于每个 p 之上的素理想 \mathfrak{p} , 存在数域 $K \subset L$ 使得 \mathfrak{p} 在 L/K 惯性.

(3) L 的整数环 \mathcal{O}_L 是一个戴德金环.

例题 2.7 设 $K = \mathbb{Q}(\sqrt{d})$ 为二次域, $d \neq 0, 1$ 无平方因子. 当 $d \equiv 2, 3 \pmod{4}$ 时, $\mathcal{O}_K = \mathbb{Q}[\theta], \theta = \sqrt{d}$ 的极小多项式为 $x^2 - d$. 如果素数 $p \mid 2d$, 则 $r = 1, e = 2, \mathfrak{p}\mathcal{O}_K = (\sqrt{d}, p)^2$ 或 $2\mathcal{O}_K = (\sqrt{d} + 1, 2)^2$ ($2 \nmid d$ 时) 完全分歧. 如果素数 $p \nmid 2d$, 当 $\left(\frac{d}{p}\right) = 1$ 时, $x^2 - d$ 在 \mathbb{F}_p 上有两个不同的根 $\pm \bar{a}$, 于是 $\mathfrak{p}\mathcal{O}_K = (\sqrt{d} + a, p)(\sqrt{d} - a, p)$ 完全分裂; 当 $\left(\frac{d}{p}\right) = -1$ 时, p 惯性.

练习 2.4.2 考虑 $d \equiv 1 \pmod{4}$ 时, $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ 中素理想分解情况.

§2.4.2 伽罗瓦扩张中的分歧

设 L/K 是有限伽罗瓦扩张, $G = G(L/K)$ 为它的伽罗瓦群.

命题 2.58

G 在所有的 $w \mid v$ 上作用是传递的.



证明 设 w, w' 是 v 的两个延拓. 如果 w 和 w' 不共轭, 则

$$\{w \circ \sigma \mid \sigma \in G\}, \quad \{w' \circ \sigma \mid \sigma \in G\}$$

不交. 由逼近定理 2.7, 存在 $x \in L$ 使得

$$|\sigma x|_w < 1, \quad |\sigma x|_{w'} > 1, \quad \forall \sigma \in G.$$

于是 $\mathbf{N}_{L/K}(x)$ 满足 $|\alpha|_v = \prod_{\sigma} |\sigma x|_w < 1$. 同理 $|\alpha|_v > 1$, 矛盾! 因此 w, w' 共轭. □

特别地, 如果 $v = \mathfrak{p}$ 非阿, 则 $e = e_{\mathfrak{p}_i/\mathfrak{p}}$ 均相等, $f = f_{\mathfrak{p}_i/\mathfrak{p}}$ 均相等.

定义 2.59 (分解群, 惯性群和分歧群)

定义 w 的分解群为

$$G_w(L/K) = \{\sigma \in G \mid w \circ \sigma = w\}.$$

如果 $w = \mathfrak{P}$ 是非阿赋值, 设 B 为 \mathfrak{P} 的赋值环. 定义其惯性群为

$$I_w(L/K) = \{\sigma \in G_w \mid \sigma x \equiv x \pmod{\mathfrak{P}}, \forall x \in B\},$$

分歧群为

$$R_w(L/K) = \left\{ \sigma \in G_w \mid \frac{\sigma x}{x} \equiv 1 \pmod{\mathfrak{P}}, \forall x \in L^\times \right\}.$$

称它们的固定子域分别为分解域 Z_w , 惯性域 T_w , 分歧域 V_w .



显然

$$G \supseteq G_w \supseteq I_w \supseteq R_w \supseteq \{1\}, \quad K \subseteq Z_w \subseteq T_w \subseteq V_w \subseteq L.$$

我们将说明, Z_w 是 w 完全分裂的最大的子域, T_w, V_w 分别是 L/Z_w 的极大非分歧扩张和极大温分歧扩张.

这些群和它们所对应的的完备域扩张的相应群是一致的.

命题 2.60

$$G_w(L/K) \cong G(L_w/K_v),$$

$$I_w(L/K) \cong I(L_w/K_v),$$

$$R_w(L/K) \cong R(L_w/K_v).$$



证明 分解群 G_w 由那些在 w 下连续的自同构构成. 根据赋值诱导的拓扑的定义, $\sigma \in G_w$ 显然是连续的. 反之, 若 $\sigma \in G$ 连续, 则对于 $|x|_w < 1$, $x^n \rightarrow 0$, 因此 $\sigma x^n \rightarrow 0$, $|\sigma x|_w = |x|_{w \circ \sigma} < 1$. 因此 w 和 $w \circ \sigma$ 等价.

由于 L 在 L_w 中稠密, 任意 $\sigma \in G_w(L/K)$ 可以唯一地延拓为 L_w 的连续的 K_v 自同构 $\tilde{\sigma}$. 容易知道当 $\sigma \in I_w, R_w$ 时 $\tilde{\sigma} \in I_w(L_w/K_v), R_w(L_w/K_v)$. □

设 W_v 为 v 之上的所有素位, 则

$$G_w \backslash G \xrightarrow{\sim} W_v$$

$$G_w \sigma \mapsto w\sigma.$$

一般情形下, 设 N 为 L/K 的伽罗瓦闭包,

$$G = G(N/K), H = G(N/L), G_w = G_w(N/K),$$

则

$$G_w \backslash G/H \xrightarrow{\sim} W_v$$

$$G_w \sigma H \mapsto w \circ \sigma|_L.$$

命题 2.61

(1) $w_Z := w|_{Z_w}$ 可以唯一地延拓到 L 上.

(2) $Z_w = L \cap K_v \subseteq L_w$.

(3) 如果 v 有限, 则 w_Z 和 v 剩余域相同.



证明 (1) 如果 w' 是 w_Z 在 L 上的延拓, 则 $w' = w \circ \sigma, \sigma \in G(L/Z_w) = G_w$, 因此 $w' = w$.

(2) 由于 $G_w(L/K) = G(L_w/K_v)$, 因此 $Z_w = L \cap K_v \subseteq L_w$.

(3) 由于 K, Z_w 的剩余域和 K_v 相同, 因此 w_Z 和 v 剩余域相同. \square

现在我们来考虑惯性群. 设 $w = \mathfrak{p}$ 非阿. 由于 $G(L/Z_w) \cong G(L_w/K_v)$, 因此我们在考虑 L/Z_w 子扩张时, 可以将其放在 L_w/K_v 中看. 设 $B, \kappa_{\mathfrak{p}}$ 为 L 的赋值环和剩余域. 对于 $\sigma \in I_w$, 由于 $\sigma\mathfrak{p} = \mathfrak{p}, \sigma B = B$, 因此它诱导了 $v = \mathfrak{p}$ 剩余域 κ 上的自同构

$$\bar{\sigma} : B/\mathfrak{p} \longrightarrow B/\mathfrak{p}$$

$$x \bmod \mathfrak{p} \longmapsto \sigma x \bmod \mathfrak{p}.$$

因此我们有群同态 $G_w \rightarrow \text{Aut}_{\kappa}(\kappa_{\mathfrak{p}})$.

命题 2.62

$\kappa_{\mathfrak{p}}/\kappa$ 是正规扩张且我们有正合列

$$1 \rightarrow I_w \rightarrow G_w \rightarrow G(\kappa_{\mathfrak{p}}/\kappa) \rightarrow 1.$$

因此 $G(T_w/Z_w) \cong G(\kappa_{\mathfrak{p}}/\kappa)$, 且 T_w 是 L/Z_w 的极大非分歧扩张.



证明 设 $v = \mathfrak{p}, w = \mathfrak{p}, \mathfrak{p}_Z := \mathfrak{p} \cap Z_{\mathfrak{p}}$. 由于 \mathfrak{p}_Z 之上的素理想为 $\sigma\mathfrak{p} = \mathfrak{p}, \sigma \in G(L/Z_{\mathfrak{p}}) = D_{\mathfrak{p}}$, 因此 \mathfrak{p}_Z 之上的素理想只有 \mathfrak{p} . 由于 G 在 $w|v$ 上传递, 因此 $n = efr, r$ 为 $w|v$ 个数, e, f 为任意一个的分歧指数和惯性指数. 而 $r = (G : D_{\mathfrak{p}})$, 因此 $ef = [L : Z_{\mathfrak{p}}]$. 我们不妨设 $K = Z_w$, 设 $\theta \in B$ 是 $\bar{\theta} \in \kappa$ 的提升, 它们的极小多项式为 $f(x), \bar{g}(x)$. 显然 $\bar{g} | \bar{f}$. 由于 L/K 是正规扩张, 因此 f 在 L 上分解为一次多项式乘积, 从而 \bar{f}, \bar{g} 也是如此, 故 $\kappa_{\mathfrak{p}}/\kappa$ 正规.

设 $\bar{\theta}$ 是 $\kappa_{\mathfrak{p}}/\kappa$ 的极大可分子扩张的生成元, $\bar{\sigma} \in G(\kappa_{\mathfrak{p}}/\kappa) = G(\kappa(\bar{\theta})/\kappa)$. 因此 $\bar{\sigma}\bar{\theta}$ 是 \bar{g} 的根, 从而是 \bar{f} 的根. 因此存在 f 的根 θ' 使得 $\theta' \equiv \bar{\sigma}\bar{\theta} \bmod \mathfrak{p}, \theta'$ 是 θ 的共轭元, 即 $\theta' = \sigma\theta, \sigma \in G(L/K)$ 是 $\bar{\sigma}$ 的一个原像, 因此该映射是满射. 它的核为 I_w .

最后, 设 T 为 L/Z_w 极大非分歧扩张. 我们对 T/Z_w 应用上述结论, 则 $G(T/Z_w) \rightarrow G(\kappa_L/\kappa_K)$ 是满射. 由于非分歧扩张分歧指数为 1, 因此这是一个同构, 从而 $T = T_w$. \square

如果 \mathfrak{P} 非分歧, 则 $I_w = 1$, $G_w \cong G(\kappa_{\mathfrak{P}}/\kappa) = \langle \varphi \rangle$, 其中 $\varphi(x) = x^{\#\kappa}$. 从而存在一个元素

$$\left(\frac{L/K}{\mathfrak{P}}\right) \in \text{Gal}(L/K)$$

使得 $\left(\frac{L/K}{\mathfrak{P}}\right)(x) \equiv x^{\#\kappa} \pmod{\mathfrak{P}}$. 对于 $\sigma \in \text{Gal}(L/K)$, 我们有

$$\left(\frac{L/K}{\sigma\mathfrak{P}}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}.$$

记 $\left(\frac{L/K}{\mathfrak{p}}\right)$ 为 $\left(\frac{L/K}{\mathfrak{P}}\right)$ 所在的共轭类.

定理 2.63 (切博塔廖夫密度定理)

设 $c \subset G$ 是一个共轭类, 则 $\left(\frac{L/K}{\mathfrak{p}}\right) = c$ 的全体 \mathfrak{p} 在所有素理想中的密度为 $\#c/\#G$. 这里的密度是指狄利克雷密度

$$\rho(\mathcal{S}) = \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in \mathcal{S}} \mathbf{N}\mathfrak{p}^{-s}}{\sum_{\mathfrak{p} \in \mathcal{P}} \mathbf{N}\mathfrak{p}^{-s}},$$


其中 \mathcal{P} 为所有素理想集合.



现在我们来考虑分歧群. 设 $\chi(L/K) = \text{Hom}(w(L^\times)/v(K^\times), \kappa_L^\times)$, 定义

$$\begin{aligned} I_w &\longrightarrow \chi(L/K) \\ \sigma &\longmapsto (w(x) \mapsto \frac{\sigma x}{x} \pmod{\mathfrak{P}}), \end{aligned}$$

该映射的核为分歧群 R_w .

 **练习 2.4.3** 验证该映射良定义且是群同态.

命题 2.64

R_w 是 I_w 的唯一的希洛夫 p 子群且我们有正合列

$$1 \rightarrow R_w \rightarrow I_w \rightarrow \chi(L/K) \rightarrow 1.$$

因此 V_w 是 L/Z_w 的极大温分歧扩张.



证明 我们不妨设 L/K 是完备域的扩张. 如果 R_w 不是 p 群, 则存在 $\sigma \in R_w$ 阶为素数 $\ell \neq p$. 设 K' 是 σ 的固定子域, κ' 为其剩余域. 由于 $R_w \subset I_w$, $K' \supseteq T$, 因此 κ 在 κ_L 中的可分闭包包含在 κ' 中, κ_L/κ' 纯不可分, 从而 κ_L/κ' 扩张次数是 p 的幂次. 设 σ 是 $\bar{\sigma} \in \kappa_L$ 的提升, $f \in K'[x], \bar{g} \in \kappa'[x]$ 为它们的极小多项式, 则 $\bar{f} = \bar{g}^m$ 的次数为 1 或 ℓ . 这迫使 $\kappa' = \kappa_L$. 而 L/K' 是温分歧扩张, 存在 $a \in K'$ 使得 $L = K'(\alpha), \alpha = \sqrt[\ell]{a}$. 于是 $\sigma\alpha = \zeta\alpha$, 其中 $\zeta \in L$ 是 ℓ 次本原单位根. 由于 $\sigma \in R_w, \zeta = \sigma\alpha/\alpha \equiv 1 \pmod{\mathfrak{P}}$, 这意味着 $\zeta = 1$, 矛盾! 因此 R_w 是 p 群.

由于 κ_L 特征 p, κ_L^\times 中元素的阶与 p 互素, 从而 $\chi(L/K)$ 也是如此. 因此 R_w 是 I_w 的希洛夫 p 子群, V_w 为 L/T 的所有与 p 互素次扩张的并, 因此 V_w 包含 L/Z_w 的极大温分歧扩张 V . 由于 V_w/V 扩张次数与 p 互素, V_w/V 的剩余域扩张可分, 从而 V_w/V 是温分歧扩张, $V_w = V$.

最后我们来证明满. 由于 T_w/K 是 V_w/K 的极大非分歧扩张, V_w/T_w 惯性指数为 1, 因此

$$[V_w : T_w] = (w(V_w^\times) : w(T_w^\times)) = (w(V_w^\times) : v(K^\times)).$$

由于 $w(V_w^\times) = w(L^\times)^{(p)}$, 因此上式等于商群 $w(L^\times)/v(K^\times)$ 中与 p 互素的部分大小. 若 $w(L^\times)^{(p)}/v(K^\times)$

包含 m 阶元, 则我们知道 κ_L^\times 包含 m 阶元, 因此


$$\#\chi(L/K) = \#\text{Hom}(w(L^\times)^{(p)}/v(K^\times), \kappa_L^\times) = \#w(L^\times)^{(p)}/v(K^\times).$$

□

例题 2.8 设 L/K 是数域的伽罗瓦扩张, $w = \infty' | v = \infty$ 分别为它们的无穷素位. 如果 ∞, ∞' 同为实素位或复素位, 则 $L_{\infty'} = K_\infty, G_w(L/K) = 1$, 因此 ∞ 在 L 中完全分裂为 n 个无穷素位.

如果 ∞ 是实素位而 ∞' 为复素位, 则 $G_w(L/K) = G(\mathbb{C}/\mathbb{R})$, 因此存在 L 的一个二阶子域 L' , 使得 ∞ 在 L'/K 完全分裂, 而 $\infty'|_{L'}$ 在 L'/L' 中惯性. 特别地, 如果 $K = \mathbb{Q}$, 则 L' 是 L 的极大实子域, L'/L 是二次扩张.

例题 2.9 设 $K = \mathbb{Q}(i, \sqrt{p})$. 当 $q \equiv 1 \pmod{4}$ 时, q 在 $\mathbb{Q}(i)$ 中分裂为 $q_1 q_2$, 它们的剩余域均为 \mathbb{F}_q . 如果 $q \neq p$, 则 q 在 $\mathbb{Q}(\sqrt{p})$ 中非分歧, 从而在 K 上非分歧. 若 $\left(\frac{p}{q}\right) = 1$, 则 \sqrt{p} 的极小多项式在 $\mathbb{F}_p[x]$ 中分解为两个不同的多项式的乘积, 因此 q 在 K 上完全分裂, $G_w = 1$. 若不然, 则 q 在 $\mathbb{Q}(\sqrt{p})$ 中惯性, 从而 q_1, q_2 在 K 中惯性, $G_w = G(K/\mathbb{Q}(i)), I_w = 1$. 如果 $q = p$, 则 q 在 $\mathbb{Q}(\sqrt{p})$ 中分歧, 从而在 K 中分歧, 因此 $G_w = I_w = G(K/\mathbb{Q}(i)), R_w = 1$.

 **练习 2.4.4** $q \equiv -1 \pmod{4}$ 或 $q = 2$ 时, q 之上的素位的分解群、惯性群、分歧群分别是什么?

§2.4.3 高阶分歧群

为了研究伽罗瓦扩张的子扩张和其本身的分歧群之间的联系, 我们将考虑更多的分歧群. 我们假设 $K = Z_w$, 即 L/K 中 v 之上的素位只有 w . 设 A, B 分别为 K, L 在 v, w 的赋值环. 我们假设 L/K 的剩余域扩张 κ_w/κ 可分.

引理 2.65

存在 $a \in B$ 使得 $B = A[a]$.



证明 由于 κ_w/κ 可分, 存在 \bar{a} 使得 $\kappa_L = \kappa[\bar{a}]$. 设 $f(x) \in A[x]$ 是 \bar{a} 的极小多项式 \bar{f} 的一个首一提升, 则存在 \bar{a} 的一个提升 $a \in B$ 使得 $f(a)$ 是一个素元. 实际上, 设 a 为任一提升, $v_L(f(a)) \geq 1$. 如果 $v_L(f(a)) \geq 2$, 则 $v_L(f(a + \Pi)) = 1$. 这是因为

$$f(a + \Pi) = f(a) + f'(a)\Pi + O(\Pi^2),$$

而 $f'(\bar{a}) \neq 0, f'(a) \in B^\times$. 所以 $a^i f(a)^j, 0 \leq i \leq f-1, 0 \leq j \leq e-1$ 形成 B/\mathfrak{p} 的一组 κ 基. 设 M 为它们生成的子 A 模, N 为 a^i 生成的子 A 模, 则 $M = N + Nf(a) + \cdots + Nf(a)^{e-1}$,

$$B = N + f(a)B = \cdots = M + f(a)^e B = M + \mathfrak{p}B,$$

由中山引理, $B = M$, 即 $B = A[a]$. □

定义 2.66 (高阶分歧群)

设 L/K 是有限伽罗瓦扩张, v 是 K 上规范化离散赋值, w 为 v 之上 L 的一个规范化离散赋值. 对于任意实数 $s \geq -1$, 定义 s 阶分歧群为

$$G_s = G_s(L/K) = \{\sigma \in G \mid v_L(\sigma a - a) \geq s + 1, \forall a \in B\}.$$



容易知道 $G_{-1} = G, G_0 = I_w$ 为惯性群, $G_1 = R_w$ 为分歧群. 由于

$$v_L(\tau^{-1}\sigma\tau a - a) = v_L(\sigma\tau a - \tau a),$$

且 $\tau B = B$, 因此这些分歧群都是 G 的正规子群, 它们形成一个正规子群的下降链

$$G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots.$$

命题 2.67

设 Π 是 B 的一个素元. 对于任意整数 $s \geq 0$,

$$\begin{aligned} G_s/G_{s+1} &\longrightarrow U_L^{(s)}/U_L^{(s+1)} \\ \sigma &\longmapsto \frac{\sigma\Pi}{\Pi} \end{aligned}$$

是不依赖于 Π 的选取的单同态.



练习 2.4.5 证明该命题.

注意到 $s \geq 1$ 时, $U^{(0)}/U^{(1)} \cong \kappa_L^\times$, $U^{(s)}/U^{(s+1)} \cong \kappa_L$, 因此 G_s/G_{s+1} 是 p 群, G_0/G_1 阶与 p 互素. 我们在上一节已经知道, R_w 是 I_w 的希洛夫 p 子群.

命题 2.68

设 K' 是 L/K 的中间域, 则

$$G_s(L/K') = G_s(L/K) \cap G(L/K').$$



练习 2.4.6 证明该命题.

而 L/K 的分歧群和它的伽罗瓦子扩张 L'/K 的分歧群的联系更为复杂. 通过商映射 $G(L/K) \rightarrow G(L'/K)$, L/K 的分歧群确实映为 L'/K 的分歧群, 但是指标发生了改变.

我们记

$$i_{L/K}(\sigma) = v_L(\sigma a - a) = \min v_L(\sigma b - b \mid b \in B),$$

则

$$G_s(L/K) = \{\sigma \in G \mid i_{L/K}(\sigma) \geq s + 1\}.$$

命题 2.69

设 $e = e(L/L')$ 为伽罗瓦子扩张 L/L' 的分歧指数, 则

$$i_{L'/K}(\sigma') = \frac{1}{e'} \sum_{\sigma|_{L'}=\sigma'} i_{L/K}(\sigma).$$



证明 $\sigma' = 1$ 时两边均为无穷. 设 $\sigma' \neq 1$, B' 为 $w|_{L'}$ 的赋值环. 存在 $b \in B'$ 使得 $B' = A[b]$. 我们有

$$e' i_{L'/K}(\sigma') = v_L(\sigma' b - b).$$

固定一个 $\sigma \in G$ 使得 $\sigma|_{L'} = \sigma'$, 则所有限制在 L' 上为 σ' 的元素为 $\sigma\tau$, $\tau \in H = G(L/L')$. 我们只需证 $u = \sigma b - b$ 和 $v = \prod_{\tau \in H} (\sigma\tau a - a)$ 的赋值相同.

设 $f(x) \in B'[x]$ 是 a 的极小多项式, 则 $f(x) = \prod_{\tau \in H} (x - \tau a)$, $\sigma f(x) = \prod_{\tau \in G} (x - \sigma\tau a)$, 这里 σ 作用在系数上. 显然 $\sigma f - f$ 的系数被 $u = \sigma b - b$ 整除, 因此 u 整除 $(\sigma f - f)(a) = \pm v$.

反之, 存在多项式 $g(x) \in A[x]$ 使得 $b = g(a)$. 于是

$$g(x) - b = f(x)h(x), \quad h(x) \in B'[x].$$

令 σ 作用在两边系数上, 并取 $x = a$, 我们得到

$$u = \sigma b - b = (\sigma f)(a)(\sigma h)(a) = \pm v \cdot (\sigma h)(a).$$

因此 $v \mid u$. □

我们将证明 $G_s(L/K)$ 的像为 $G_t(L'/K)$, 其中

$$t = \eta_{L/K}(s) = \int_0^s \frac{dx}{(G_0 : G_x)}.$$

这里 $-1 < s \leq 0$ 时, $(G_0 : G_s) = (G_{-s} : G_0)^{-1} = 1$. 显然这是一个连续的分段线性函数, 其中 $0 \leq m \leq s \leq m+1$ 时,

$$\eta_{L/K}(s) = \frac{1}{g_0}(g_1 + g_2 + \cdots + g_m + (s-m)g_{m+1}), \quad g_i = \#G_i.$$

命题 2.70

证明

$$\eta_{L/K}(s) = \frac{1}{g_0} \sum_{\sigma \in G} \min \{i_{L/K}(\sigma), s+1\} - 1.$$



证明 设右端为 $\theta(s)$, 显然它也是连续的分段线性函数. 我们有 $\theta(0) = \eta_{L/K}(0) = 0$. 如果 $-1 \leq m < s < m+1$,

$$\theta'(s) = \frac{1}{g_0} \# \{ \sigma \in G \mid i_{L/K}(\sigma) \geq m+2 \} = \frac{1}{(G_0 : G_{m+1})} = \eta'_{L/K}(s).$$

因此二者相等. □

定理 2.71 (埃尔布朗定理)

设 L'/K 是 L/K 的伽罗瓦子扩张, $H = G(L/L')$. 我们有

$$G_s(L/K)H/H = G_t(L'/K),$$

其中 $t = \eta_{L/L'}(s)$.



证明 设 $G = G(L/K)$, $G' = G(L'/K)$. 对于任意 $\sigma' \in G'$, 设 $\sigma \in G$ 是它的一个原像, 其具有最大的 $i_{L/K}(\sigma)$. 那么我们只需要说明

$$i_{L'/K}(\sigma') - 1 = \eta_{L/L'}(i_{L/K}(\sigma) - 1).$$

这是因为, $\sigma' \in G_s H/H \iff i_{L/K}(\sigma) - 1 \geq s \iff i_{L'/K}(\sigma') - 1 \geq \eta_{L/L'}(s) \iff \sigma' \in G'_t$.

设 $m = i_{L/K}(\sigma)$. 如果 $\tau \in H$ 属于 $H_{m-1} = G_{m-1}(L/L')$, 则 $i_{L/K}(\tau) \geq m$, $i_{L/K}(\sigma\tau) = m$. 如果 $\tau \notin H_{m-1}$, 则 $i_{L/K}(\tau) < m$, $i_{L/K}(\sigma\tau) = i_{L/K}(\tau)$. 因此 $i_{L/K}(\sigma\tau) = \min \{i_{L/K}(\tau), m\}$. 于是由命题 2.69 知

$$i_{L'/K}(\sigma') = \frac{1}{e'} \sum_{\tau \in H} \{i_{L/K}(\tau), m\}.$$

由命题 2.70 知我们所需的关系式成立, $e' = \#G_0(L/L')$. □

我们记 $\eta_{L/K}$ 的逆为 $\psi_{L/K}$, 并定义

$$G^t(L/K) := G_{\psi_{L/K}(t)}(L/K).$$

命题 2.72

记号同上, $\eta_{L/K} = \eta_{L'/K} \circ \eta_{L/L'}$, $\psi_{L/K} = \psi_{L/L'} \circ \psi_{L'/K}$. 因此 $G^t(L/K)H/H = G^t(L'/K)$.



证明 我们有 $e = e_{L'/K}e'$. 由于 $G_s/H_s = (G/H)_t$, $t = \eta_{L/L'}(s)$, 我们有

$$\frac{1}{e} \# G_s = \frac{1}{e_{L'/K}} \# (G/H)_t \frac{1}{e'} \# H_s,$$

此即

$$\eta'_{L/K}(s) = \eta'_{L'/K}(t) \eta'_{L/L'}(s) = (\eta_{L'/K} \circ \eta_{L/L'})'(s).$$

又因为它们均经过原点, 因此二者相等. □

§2.4.4 共轭差积和判别式

设 B/A 是戴德金整环的有限扩张, 且 $L = \text{Frac } B$ 是 $K = \text{Frac } A$ 的可分扩张. 我们假设 B/A 的每个剩余域上的扩张都是可分的.

定义 2.73 (共轭差积)

称分式理想

$$\mathfrak{D}_{B/A}^{-1} = \{x \in L \mid \text{Tr}(xB) \subseteq A\}$$

的逆为 B/A 的共轭差积.



练习 2.4.7 设 S 是 A 的乘法集, 则 $\mathfrak{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}_{B/A}$.

命题 2.74

(1) 设 $A \subseteq B \subseteq C$ 是戴德金环的有限扩张塔, 则 $\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B}\mathfrak{D}_{B/A}$.

(2) 如果 \mathfrak{P} 是 B 的素理想, $\mathfrak{p} = \mathfrak{P} \cap A$, 则 $\mathfrak{D}_{B/A}\mathcal{O}_{\mathfrak{P}} = \mathfrak{D}_{B_{\mathfrak{P}}/A_{\mathfrak{p}}}$.



证明 (1) 由于

$$\text{Tr}_{C/A}(\mathfrak{D}_{C/B}^{-1}\mathfrak{D}_{B/A}^{-1}C) \subseteq A,$$

因此 $\mathfrak{D}_{C/B}^{-1}\mathfrak{D}_{B/A}^{-1} \subseteq \mathfrak{D}_{C/A}^{-1}$, 即 $\mathfrak{D}_{C/B}\mathfrak{D}_{B/A} \supseteq \mathfrak{D}_{C/A}$. 由于

$$A \supseteq \text{Tr}_{C/A}(\mathfrak{D}_{C/A}^{-1}C) = \text{Tr}_{B/A}(\text{Tr}_{C/B}(\mathfrak{D}_{C/A}^{-1}C)B),$$

因此 $\text{Tr}_{C/B}(\mathfrak{D}_{C/A}^{-1}C) \subseteq \mathfrak{D}_{B/A}^{-1}$,

$$\text{Tr}_{C/B}(\mathfrak{D}_{B/A}\mathfrak{D}_{C/A}^{-1}C) \subseteq \mathfrak{D}_{B/A}\text{Tr}_{C/B}(\mathfrak{D}_{C/A}^{-1}C) \subseteq B,$$

所以 $\mathfrak{D}_{B/A}\mathfrak{D}_{C/A}^{-1} \subseteq \mathfrak{D}_{C/B}^{-1}$, 即 $\mathfrak{D}_{C/B}\mathfrak{D}_{B/A} \subseteq \mathfrak{D}_{C/A}$.

(2) 不妨设 A 是离散赋值环. 根据推论 2.54,

$$\text{Tr}_{L/K} = \sum_{\mathfrak{P}|\mathfrak{p}} \text{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}.$$

由命题 2.7, 存在 $\eta \in L$ 在 $|\cdot|_{\mathfrak{P}}$ 下接近 $y \in B_{\mathfrak{P}}$, 在其它 $|\cdot|_{\mathfrak{P}'}, \mathfrak{P}' \mid \mathfrak{p}, \mathfrak{P}' \neq \mathfrak{P}$ 下接近 0. 对于 $x \in \mathfrak{D}_{B/A}^{-1}$,

$$\text{Tr}_{L/K}(x\eta) = \text{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x\eta) + \sum_{\mathfrak{P}' \neq \mathfrak{P}} \text{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(x\eta) \in A_{\mathfrak{p}}.$$

而 $\text{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(x\eta)$ 接近 0, 因此也属于 $A_{\mathfrak{p}}$, 所以 $\text{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x\eta) \in A_{\mathfrak{p}}$. 故 $\mathfrak{D}_{B/A}^{-1} \subseteq \mathfrak{D}_{B_{\mathfrak{P}}/A_{\mathfrak{p}}}$.

通过同样的证明方法, 如果 $x \in \mathfrak{D}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}$, $\xi \in L$ 在 $|\cdot|_{\mathfrak{p}}$ 下接近 x , 在其它 $|\cdot|_{\mathfrak{p}'}$ 下接近 0, 则 $\xi \in \mathfrak{D}_{B/A}$. 因此 $\mathfrak{D}_{B/A}^{-1}$ 在 $\mathfrak{D}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}^{-1}$ 中稠密, 换言之 $\mathfrak{D}_{B/A}^{-1}B_{\mathfrak{p}} = \mathfrak{D}_{B_{\mathfrak{p}}/A_{\mathfrak{p}}}^{-1}$. \square

定义 2.75 (元素的共轭差积)

设 $f(X) \in A[X]$ 是 $\alpha \in B$ 的极小多项式. 定义 α 的共轭差积为

$$\delta_{B/A}(\alpha) = \begin{cases} f'(\alpha), & L = K(\alpha), \\ 0, & L \neq K(\alpha). \end{cases}$$



定理 2.76

如果 $B = A[\alpha]$, 则 $\mathfrak{D}_{B/A} = (\delta_{B/A}(\alpha))$. 一般地, $\mathfrak{D}_{B/A}$ 为所有 $\delta_{B/A}(\alpha)$ 生成的理想.



证明 设 $B = A[\alpha]$. 设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in A[x]$ 是 α 的极小多项式, α_i 是 α 的所有共轭根. 容易证明如下恒等式

$$\frac{1}{f(x)} = \sum_{i=1}^n \frac{1}{f'(\alpha_i)(x - \alpha_i)}.$$

两边关于 $\frac{1}{x}$ 做幂级数展开, 我们得到其第 $k \leq n$ 项系数为

$$0 = \sum_{i=1}^n \alpha_i^k / f'(\alpha_i) = \text{Tr}(\alpha^k / f'(\alpha)),$$

除了常数项为 0. 特别地, $a_{ij} = \text{Tr}(\alpha^{i+j} / f'(\alpha)), 0 \leq i, j \leq n-1$ 形成的矩阵为三角阵, 因此它的行列式为 ± 1 , $x^j / f'(x)$ 形成 $\mathfrak{D}_{B/A}^{-1}$ 的一组基, $\mathfrak{D}_{B/A} = (f'(\alpha))$.

一般情形下, 设 $L = K(\alpha), \alpha \in B$. 考虑 $A[\alpha]$ 的导子

$$\mathfrak{f} = \mathfrak{f}_{A[\alpha]} = \{x \in L \mid xB \subseteq A[\alpha]\}.$$

对于 $b = f'(\alpha), x \in L$,

$$\begin{aligned} x \in \mathfrak{f} &\iff xB \subseteq A[\alpha] \iff b^{-1}xB \subseteq b^{-1}A[\alpha] \iff \text{Tr}(b^{-1}xB) \subseteq A \\ &\iff b^{-1}x \in \mathfrak{D}_{B/A}^{-1} \iff x \in b\mathfrak{D}_{B/A}^{-1}. \end{aligned}$$

因此 $(f'(\alpha)) = \mathfrak{f}\mathfrak{D}_{B/A}, f'(\alpha) \in \mathfrak{D}_{B/A}$.

要证明 $\mathfrak{D}_{B/A}$ 是所有 $\delta(\alpha)$ 的最大公因子, 我们只需要对任意 \mathfrak{p} 证明存在 α 使得 $v_{\mathfrak{p}}(\mathfrak{D}_{B/A}) = v_{\mathfrak{p}}(f'(\alpha))$ 即可. 设 $L_{\mathfrak{p}}, K_{\mathfrak{p}}$ 为相应的完备化, $\mathcal{O}_{\mathfrak{p}}, \mathcal{O}_{\mathfrak{p}}$ 为其赋值环. 我们知道存在 $a, \mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[a]$, 而且 a 可以替换为任意一个和 a 足够接近的元素 b . 因此

$$v_{\mathfrak{p}}(\mathfrak{D}_{B/A}) = v_{\mathfrak{p}}(\mathfrak{D}_{\mathcal{O}_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}}) = v_{\mathfrak{p}}(\delta_{\mathcal{O}_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}}(b)).$$

所以我们只需要构造 $b \in B$ 且 $L = K(b), v_{\mathfrak{p}}(\delta_{\mathcal{O}_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}}(b)) = v_{\mathfrak{p}}(\delta_{B/A}(b))$. 设 $\sigma_i : L \rightarrow \overline{K}_{\mathfrak{p}}$ 给出所有 \mathfrak{p} 之上素位 $\mathfrak{p} = \mathfrak{p}_1, \dots, \mathfrak{p}_r$. 设 $\alpha = 0$ 或 1 满足

$$|\tau a - \alpha| = 1, \quad \forall \tau \in G(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}}).$$

由中国剩余定理, 存在 $b \in B$ 使得 $|b - a|, |\sigma_i b - \alpha|$ 都充分小. 我们不妨设 $L = K(b)$, 若不然, 由克拉斯纳引理 2.36, $L = K(b + \pi^n \gamma), L = K(\gamma), n$ 充分大即可. 又因为 $\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}[b]$, 则

$$\delta_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(b) = \prod_{1 \neq \tau \in \text{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{p}}, \overline{K}_{\mathfrak{p}})} (b - \tau b),$$

$$\delta_{B/A}(b) = \prod_{1 \neq \sigma \in \text{Hom}_K(L, \bar{K})} (b - \sigma b) = \prod_{1 \neq \tau} (b - \tau b) \prod_{i=2}^r \prod_j (b - \tau_{ij} \sigma_i b).$$

而 $|b - \tau_{ij} \sigma_i b| = |\tau_{ij}^{-1} b - \alpha + \alpha - \sigma_i b| = 1$. 因此二者赋值相同. \square

下述定理表明, 在域扩张 L/K 中, 共轭差积刻画了 L 的各个素位的分歧程度.

定理 2.77

L 的素理想 \mathfrak{P} 在 K 上分歧当且仅当 $\mathfrak{P} \mid \mathfrak{D}_{L/K}$. 设 $s = v_{\mathfrak{P}}(\mathfrak{D}_{L/K})$, 则 \mathfrak{P} 温分歧时 $s = e - 1$, 野分歧时 $e \leq s \leq e - 1 + v_{\mathfrak{P}}(e)$.



证明 不妨设 A 为完备离散赋值环, 极大理想为 \mathfrak{p} , 则 $B = A[a]$, $v_{\mathfrak{P}}(f'(a)) = s$. 如果 L/K 非分歧, 则 $\bar{a} = a \bmod \mathfrak{P}$ 是 $\bar{f} = f \bmod \mathfrak{p}$ 的单根, 因此 $f'(\alpha) \in A^\times$, $s = 0 = e - 1$.

根据命题 2.74, 我们只需考虑 L/K 完全分歧的情形. 此时 a 可以取为 B 的素元. 此时

$$f(x) = c_e x^e + c_{e-1} x^{e-1} + \cdots + c_1 x + c_0, \quad c_e = 1$$

是艾森斯坦多项式,

$$f'(x) = e x^{e-1} + (e-1) c_{e-1} x^{e-2} + \cdots + 2c_2 x + c_1.$$

对于 $1 \leq i \leq e$,

$$v_{\mathfrak{P}}(i c_i a^{i-1}) \equiv i - 1 \pmod{e}.$$

因此

$$s = v_{\mathfrak{P}}(f'(a)) = \min_{0 \leq i \leq e} v_{\mathfrak{P}}(i c_i a^{i-1}).$$

如果 L/K 温分歧, $s = v_{\mathfrak{P}}(e c_e a^{e-1}) = e - 1$. 如果 L/K 野分歧, $e \leq s \leq v_{\mathfrak{P}}(e) + e - 1$. \square

共轭差积和微分的联系十分密切. 设 B/A 是交换环的扩张, 定义

$$\Omega_{B/A}^1 = \frac{\langle db \mid b \in B \rangle}{\{d(xy) - y dx - x dy, da = 0, \forall a \in A\}}$$

为所有 $db, b \in B$ 生成的 B 模, 且满足莱布尼茨法则以及在 A 上为 0. 我们称之为 B/A 的**微分模**, 其中的元素被称为**微分**. 称

$$d: B \rightarrow \Omega_{B/A}^1$$

为 B/A 的**导数**.

练习 2.4.8 设 k 是一个域, 计算 $\Omega_{A/k}^1$, 其中 $A = k[x, y], k[x]/(x^2 + 1), k[x, y]/(xy - 1), k(x)$.

练习 2.4.9 证明对于任意交换的 A 代数 A' , $\Omega_{B \otimes_A A'/A'}^1 = \Omega_{B/A}^1 \otimes_A A'$. 因此微分模和局部化和完备化相匹配.

命题 2.78

$\mathfrak{D}_{B/A}$ 是 B 模 $\Omega_{B/A}^1$ 的零化子, 即

$$\mathfrak{D}_{B/A} = \{x \in B \mid x dy = 0, \forall y \in B\}.$$



证明 由习题 2.4.9, 我们只需考虑 A 是完备离散赋值环的情形. 由于 B/A 的剩余域扩张 κ_B/κ_A 是可分的, 存在 $\bar{x} \in \kappa_B, \kappa_B = \kappa_A(\bar{x})$. 设 $\bar{f}(X) \in \kappa_A[X]$ 是它的极小多项式, $f(X) \in A[X]$ 是它的一个提升. 任取 \bar{x} 的一个提升, $v_L(f(x)) \geq 1$. 如果 $v_L(f(x)) \geq 2$, 由于 $\bar{f}'(\bar{x}) \neq 0, f'(x) \in B^\times, f(x + \pi_L) \equiv$

$f(x) + f'(x)\pi_L^e \pmod{\pi_L^2}$ 的赋值为 1. 因此我们总可以找到 \bar{x} 的一个提升 x 使得 $f(x)$ 是 B 的一个素元. 因此 $\{x^i f(x)^j\}_{0 \leq i \leq e-1, 0 \leq j \leq f-1}$ 构成 B/A 的一组整基, $B = A[x]$. 设 $g(x)$ 是 x 的零化多项式. 则 $\Omega_{B/A} = B dx$ 的零化子为 $(f'(x))$. \square

回忆判别式 $\mathfrak{d}_{B/A}$ 为 $\text{disc}(\alpha_i)_i$ 生成的理想, 其中 $\alpha_1, \dots, \alpha_n \in B$. 如果 A 是主理想整环, 判别式就是 B 的一组 A 基的判别式生成的理想, 但是不同的基的判别式并不一定相同. 特别地, $\mathfrak{d}_{\mathcal{O}_K/\mathbb{Z}} = (\Delta_K)$.

练习 2.4.10 如果 $S \subset A$ 是一个乘法集, 则 $\mathfrak{d}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{d}_{B/A}$.

练习 2.4.11 如果戴德金环 R 只有有限多个素理想, 则 R 是主理想整环.

定理 2.79

$$\mathfrak{d}_{B/A} = \mathbf{N}_{L/K}(\mathfrak{D}_{B/A}).$$



证明 由于 $\mathfrak{d}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{d}_{B/A}$, $\mathfrak{D}_{S^{-1}B/S^{-1}A} = S^{-1}\mathfrak{D}_{B/A}$, 通过考虑 $S^{-1}B/S^{-1}A$, 我们可以不妨设 A 是离散赋值环, 从而 A 是主理想整环. 此时 B 只有有限多个素理想, 从而 B 也是主理想整环. 由注记 1.2.2, B 是有限生成自由 A 模, 从而存在一组基 $\alpha_1, \dots, \alpha_n$, $\mathfrak{d}_{B/A} = (\text{disc}(\alpha_i)_i)$. 我们知道 $\mathfrak{D}_{B/A}^{-1}$ 作为 A 模由 $\alpha_1, \dots, \alpha_n$ 的对偶基 $\alpha_1^\vee, \dots, \alpha_n^\vee$ 生成. 设 $\mathfrak{D}_{B/A}^{-1}$ 作为理想由 β 生成, 则 $\beta\alpha_1, \dots, \beta\alpha_n$ 也是它作为 A 模的一组生成元, 因此

$$(\text{disc}(\alpha_i^\vee)_i) = \mathbf{N}_{L/K}(\beta)^2 (\text{disc}(\alpha_i)_i).$$

由于 $\text{disc}(\alpha_i)_i = \det((\sigma_i \alpha_j)_{ij})^2$, 因此 (α_i) 和 (α_i^\vee) 的判别式互逆, 从而

$$\mathfrak{d}_{B/A} = (\text{disc}(\alpha_i)_i) = (\mathbf{N}_{L/K}(\beta))^{-1} = \mathbf{N}_{L/K}(\mathfrak{D}_{B/A}).$$

\square

推论 2.80

对于戴德金环的扩张塔 $A \subseteq B \subseteq C$, 设 $K \subseteq L \subseteq M$ 为对应的域扩张, 则

$$\mathfrak{d}_{C/A} = \mathfrak{d}_{B/A}^{[M:L]} \mathbf{N}_{L/K}(\mathfrak{d}_{C/B}).$$



推论 2.81

$$\mathfrak{d} = \prod_{\mathfrak{p}} \mathfrak{d}_{\mathfrak{p}}.$$



由此可以看出, 在域扩张 L/K 中, 判别式刻画了 K 的各个素位的分歧程度. 特别地, 如果 $\mathfrak{d} = 1$, 则 L/K 处处非分歧.

练习 2.4.12 (1) 证明 $f(x) = x^3 + x^2 - 2x + 8 \in \mathbb{Q}[x]$ 是不可约多项式. 令 θ 是它的一个根, $K = \mathbb{Q}(\theta)$.

(2) 证明 2 在 K 中完全分解.

(3) 对每个 $\alpha \in \mathcal{O}_K$, $\{1, \alpha, \alpha^2\}$ 的判别式是偶数, 因此它不可能是一组整基.

定理 2.82

设 K 是一个数域, S 是它的素位的一个有限集, 则只有有限多 n 次扩张 L/K 在 S 外不分歧.



证明 如果 L/K 是 n 次扩张且在 S 外不分歧, 则 $\mathfrak{d}_{L/K}$ 整除一个固定的整理想. 因此我们只需证明具有这样的判别式的 n 次扩张 L/K 只有有限多个. 由于此时 L/\mathbb{Q} 是一个 $n[K:\mathbb{Q}]$ 次扩张, 且 $\mathfrak{d}_{L/\mathbb{Q}} = \mathfrak{d}_{K/\mathbb{Q}}^n \mathbf{N}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})$, 因此我们只需要对 $K = \mathbb{Q}$ 情形证明即可. 最后 $L(\sqrt{-1}) \neq L$ 时, $L(\sqrt{-1})/\mathbb{Q}$ 的判别式和 L/\mathbb{Q} 的判别式的平方差 $\mathbf{N}_{L/\mathbb{Q}}(\mathfrak{d}_{L(\sqrt{-1})/L})$. 注意到 $\mathcal{O}_L + \mathcal{O}_L\sqrt{-1} \subseteq \mathcal{O}_{L(\sqrt{-1})}$, 因此 $\mathfrak{d}_{L(\sqrt{-1})/L} \mid 4$

有界. 所以我们只需证明给定判别式的 n 次含 $\sqrt{-1}$ 的数域 K 只有有限多个. 这样的数域只有复嵌入, 任选一个 $\tau_0: K \hookrightarrow \mathbb{C}$. 考虑闵可夫斯基空间 $K_{\mathbb{R}} = K_{\mathbb{C}}^{F=\text{id}}$ 中一个对称凸集

$$X = \left\{ (z_{\tau}) \in K_{\mathbb{R}} : |\text{Im}(z_{\tau_0})| < C\sqrt{|\Delta_K|}, |\text{Re}(z_{\tau_0})| < 1, |z_{\tau}| < 1, \tau \neq \tau_0, \bar{\tau}_0 \right\}.$$

我们取充分大的 C (只依赖于 n) 使得 $\text{vol}(X) > 2^n \sqrt{|\Delta_K|} = 2^n \text{covol}(\mathcal{O}_K)$, 则存在非零 $\alpha \in \mathcal{O}_L$ 使得 $ja = (\tau\alpha) \in X$. 由于 $|\mathbf{N}_{K/\mathbb{Q}}(\alpha)| \geq 1, |\tau_0\alpha| > 1, \text{Im}(\tau_0\alpha) \neq 0$, 因此 $\tau_0\alpha \neq \bar{\tau}_0\alpha$. 又因为 $\tau_0\alpha \neq \tau\alpha, \tau \neq \tau_0$, 因此 $K = \mathbb{Q}(\alpha)$, 否则存在 $\tau'|_{\mathbb{Q}(\alpha)} = \tau|_{\mathbb{Q}(\alpha)}$, 这导致 $\tau'\alpha = \tau\alpha$.

由于 Δ_K 和 n 固定时, $\tau\alpha$ 是有界的, 因此 α 的极小多项式的系数也都是有界的, 从而只有有限多这样的 α , 于是只有有限多这样的 K . \square

由习题 1.4.9 可知:

定理 2.83

\mathbb{Q} 的非分歧扩张只有它自身.



对于这些命题, 我们有着高维的推广. 设 X/K 是数域上的一条完备光滑代数曲线, 即射影空间中光滑的多项式给出的曲线. 那么在每个素位, 相应的约化曲线如果仍然光滑, 我们称之为好约化. \mathbb{Q} 的非分歧扩张只有它自身也有着相应的高维推广: 方丹证明了 \mathbb{Q} 上没有处处都是好约化的完备光滑代数曲线, 见 [5].

在素位有限集 S 外都是好约化的亏格为 g 的 K 上完备光滑代数曲线只有有限多条. 在此基础上法尔廷斯证明了任意 K 上亏格 $g > 1$ 的完备光滑代数曲线只有有限多个有理点. 前文中所说的二次曲线均是亏格 0 的情形, 我们对其有理点已经有明确刻画. 最后剩下 $g = 1$ 的, 即椭圆曲线, 其有理点形成一个有限生成交换群. 椭圆曲线的算术性质仍是目前数论前沿的主要研究对象之一.

第三章 类域论

内容提要

□ 抽象类域论 3.1

□ 整体类域论 3.3

□ 局部类域论 3.2



我们称伽罗瓦群为交换群的扩张为阿贝尔扩张.

问题 3.1

给定数域 K , 如何确定它的所有阿贝尔扩张?



类域论的主要目的是为了分类给定域 K 的所有阿贝尔扩张, 这些扩张应当由 K 自身的结构所导出. 它建立了这些扩张和与 K 有关的交换群 A_K 的子群的一一对应. 在局部域的情形 $A_K = K^\times$, 在整体域的情形 A_K 是理想类群的变种——伊代尔类群. 类域论的核心是互反映射

$$r : G(L/K)^{\text{ab}} \xrightarrow{\sim} A_K / \mathbf{N}_{L/K} A_L.$$

我们先研究抽象的类域论, 然后再应用到具体情形.

§3.1 抽象类域论

抽象类域论又称 class formation. 它的目的是为了统一地处理各种类域论. 在阅读过程中, 我们可以先代入局部类域论的情形来理解.

§3.1.1 射影有限群

为了研究无限伽罗瓦扩张, 我们需要学习射影有限群.

命题 3.2

射影有限群是指有限群的逆向极限, 每个分量赋予离散拓扑. 这等价于一个紧豪斯多夫群, 且存在由正规子群形成么元的一组邻域基.



证明 设 G 是一个紧豪斯多夫群, 正规子群 $\{N_i\}$ 形成 $1 \in G$ 的一组邻域基. 则 N_i 的陪集形成 G 的一组开覆盖, 因此 G/N_i 有限. 设

$$f : G \rightarrow \varprojlim G_i, \quad G_i = G/N_i.$$

由于 G 是豪斯多夫, G_i 都是离散的. 由于 $\cap N_i = \{1\}$, 因此 f 单. 对于 $\varprojlim G_i$ 的开集

$$U_S = \prod_{i \in S} \{1_{G_i}\} \times \prod_{i \notin S} \varprojlim G_i, \quad \#S < \infty,$$

$f^{-1}(U_S) = \cap_{i \in S} N_i$ 开, 因此 f 连续. 对于任意 $x = (x_i) \in \varprojlim G_i$ 和邻域 xU_S , 令 $N = \cap_{i \in S} N_i$, 则存在 $y \in G$ 使得 $x_i = y \bmod N_i$, 因此 $f(y) \in xU_S$, f 是稠密的. 由于 G 紧, f 将闭集映为闭集, 开集映为开集, 因此 f 是满的.

反之则可以直验证得到. □

练习 3.1.1 拓扑群的开子群是闭子群, 有限指标的闭子群是开子群.

例题 3.1 设 Ω/k 是任意伽罗瓦扩张, $G = G(\Omega/k)$ 为其伽罗瓦群. 我们有¹

$$G(\Omega/k) \cong \varprojlim G(K/k),$$

其中 K 取遍 k 的有限伽罗瓦子扩张.

例题 3.2 设 \mathcal{O} 是一个剩余域有限的完备离散赋值环, \mathfrak{p} 是极大理想, 则

$$\mathcal{O} = \varprojlim_n \mathcal{O}/\mathfrak{p}^n, \quad \mathcal{O}^\times = \varprojlim_n \mathcal{O}^\times/U^{(n)}.$$

例题 3.3 令

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

则 $\widehat{\mathbb{Z}}/n\widehat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$ 且

$$\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p.$$

我们有自然的嵌入 $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}$, 它是稠密的.

例题 3.4 我们有

$$G(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}, \quad \varphi_q \mapsto 1,$$

其中 $\varphi_q(x) = x^q$ 是弗罗贝尼乌斯. 因此

$$G(\overline{\mathbb{F}}_q/\mathbb{F}_q) \cong \widehat{\mathbb{Z}}.$$

例题 3.5 如果 K 是一个完备离散赋值域, 且剩余域 κ 有限. 则我们知道 $K^{\text{ur}} = KW(\overline{\kappa})$ 是它的极大非分歧扩张, 且

$$G(K^{\text{ur}}/K) \cong G(\overline{\kappa}/\kappa) \cong \widehat{\mathbb{Z}}.$$

例题 3.6 设 $\mathbb{Q}^{\text{cyc}} = \cup_n \mathbb{Q}(\zeta_n)$, 则

$$G(\mathbb{Q}^{\text{cyc}}/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = \widehat{\mathbb{Z}}^\times \cong \prod_p \mathbb{Z}_p^\times.$$

例题 3.7 如果一个射影有限群 G 由一个元素 $\sigma \in G$ 拓扑生成, 即 $G = \overline{\langle \sigma \rangle}$, 则称之为射影循环群. 它的开子群一定形如 G^n . 例如 $G = \mathbb{Z}_p, \widehat{\mathbb{Z}}$ 均是射影循环群.

例题 3.8 设 A 是一个交换挠群, 定义它的庞特里亚金对偶为

$$A^\vee = \text{Hom}(A, \mathbb{Q}/\mathbb{Z}).$$

如果 $A = \cup_i A_i$ 是一些有限子群的并, 则

$$A^\vee = \varprojlim A_i^\vee$$

是射影有限群. 例如 $A = \mathbb{Q}/\mathbb{Z} = \cup_n \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, 则 $(\frac{1}{n}\mathbb{Z}/\mathbb{Z})^\vee = \mathbb{Z}/n\mathbb{Z}$,

$$A^\vee = \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}.$$

例题 3.9 对于任意群 G , N 取遍它的有限指标的正规子群. 定义

$$\widehat{G} = \varprojlim_N G/N$$

¹称该拓扑为克鲁尔拓扑.

为它的射影完备化. 例如 \mathbb{Z} 的射影完备化就是 $\widehat{\mathbb{Z}}$.

练习 3.1.2 射影有限 (乘法) 群 G 均可视为 $\widehat{\mathbb{Z}}$ 模, 即对于任意 $\sigma \in G, a, b \in \widehat{\mathbb{Z}}, (\sigma^a)^b = \sigma^{ab}, \sigma^{a+b} = \sigma^a \sigma^b$. 其作用限制在 \mathbb{Z} 就是通常的 \mathbb{Z} 作用.

练习 3.1.3 如果 $G = \varprojlim_i G_i$ 是射影有限的, 则 $G^{\text{ab}} = \varprojlim_i G_i^{\text{ab}}$.

§3.1.2 抽象伽罗瓦理论

设 G 是一个射影有限群. $\{G_E\}_{E \in X}$ 是它的闭子群构成的一个集族, 且其中包含 G 和 $\{1\}$. 我们把指标 E 叫做 (抽象) 域. 那么存在域 k 和 \bar{k} 满足 $G_k = G, G_{\bar{k}} = 1$.

如果 $G_L \subseteq G_K$, 我们记 $K \subseteq L$ 或 L/K , 并称之为域扩张. 如果 $n = [G_K : G_L]$ 有限, 称 L/K 为 n 次有限扩张, 此时 G_L 是 G_K 的开子群. 如果 $G_L \triangleleft G_K$ 是正规子群, 称 L/K 为正规扩张或伽罗瓦扩张, 并定义 $G(L/K) = G_K/G_L$. 不难证明

$$G = \varprojlim_{[K:k] < \infty} G(K/k),$$

其中 K 取遍 k 的所有有限伽罗瓦扩张. 类似地, 我们可以定义域之交、复合、共轭以及循环扩张、阿贝尔扩张等概念, 即对应的 G_E 复合、交、共轭以及 $G(L/K)$ 是循环群、阿贝尔群等.

例题 3.10 设 E 是一个域, Ω 是它的一个伽罗瓦扩张, $G = G(\Omega/E)$, X 为所有包含在 Ω 的 E 的有限扩张 F 以及 $\Omega, G_F = G(\Omega/F)$. 特别地, 我们可以取 $\Omega = E^{\text{sep}}$.

设 A 是一个拓扑 G 模 (A 赋予离散拓扑), 即 G 在 A 上的作用 $G \times A \rightarrow A$ 连续, 则对于任意 $a \in A$, 存在 $(1, a) \in G \times A$ 的一个邻域 $G_K \times \{a\}$ 落在它的原像, 即 $a \in A_K = A^{G_K}$. 因此

$$A = \bigcup_{[K:k] < \infty} A_K.$$

定义范映射

$$\begin{aligned} \mathbf{N}_{L/K} : A_L &\longrightarrow A_K \\ a &\longmapsto \prod_{\sigma} a^{\sigma}, \end{aligned}$$

其中 σ 取遍 $G_K \setminus G_L$ 的一组代表元. 对于伽罗瓦扩张, A_L 是 $G(L/K)$ 模且 $A_L^{G(L/K)} = A_K$. 因此相应的泰特上同调为

$$\begin{aligned} \mathbf{H}^0(G(L/K), A_L) &= A_K / \mathbf{N}_{L/K} A_L, \\ \mathbf{H}^{-1}(G(L/K), A_L) &= A_L^{\mathbf{N}=1} / I_{G(L/K)} A_L. \end{aligned}$$

§3.1.3 抽象分歧理论

固定一个满射

$$d : G \rightarrow \widehat{\mathbb{Z}}.$$

记 \tilde{k} 为 $I = \ker d$ 的固定域, 则 $G(\tilde{k}/k) \cong \widehat{\mathbb{Z}}$. 对于任意域 K , 称

$$I_K = G_K \cap I = G_K \cap G_{\tilde{k}} = G_{K\tilde{k}},$$

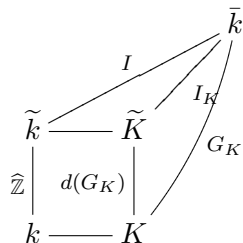
为 K 的惯性群, 它是 $\tilde{K} := K\tilde{k}$ 的固定域, 称之为 K 的极大非分歧扩张. 令

$$f_K = [\widehat{\mathbb{Z}} : d(G_K)], \quad e_K = [I : I_K].$$

如果 f_K 有限, 则我们有满同态

$$d_K = \frac{1}{f_K} d : G_K \rightarrow \widehat{\mathbb{Z}},$$

核为 I_K , 因此 $d_K : G(\tilde{K}/K) \xrightarrow{\sim} \widehat{\mathbb{Z}}$.



定义 3.3 (弗罗贝尼乌斯)

称 $G(\tilde{K}/K)$ 的拓扑生成元 $\varphi_K = d_K^{-1}(1)$ 为 K 的弗罗贝尼乌斯.



对于域扩张 L/K , 定义惯性指数 $f_{L/K} = [d(G_K) : d(G_L)]$, $e_{L/K} = [I_K : I_L]$. 我们有 $\tilde{L} = L\tilde{K}$, 于是 $f_{L/K} = [L \cap \tilde{K} : K]$. 对于域扩张 $K \subseteq L \subseteq M$, 显然

$$f_{M/K} = f_{L/K} f_{M/L}, \quad e_{M/K} = e_{L/K} e_{M/L}.$$

命题 3.4

我们有 $[L : K] = f_{L/K} e_{L/K}$.



证明 考虑交换图表

$$\begin{array}{ccccccc} 1 & \longrightarrow & I_L & \longrightarrow & G_L & \longrightarrow & d(G_L) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & I_K & \longrightarrow & G_K & \longrightarrow & d(G_K) \longrightarrow 1. \end{array}$$

如果 L/K 伽罗瓦, 则

$$1 \rightarrow I_K/I_L \rightarrow G(L/K) \rightarrow d(G_K)/d(G_L) \rightarrow 1$$

正合. 如果 L/K 不是伽罗瓦, 考虑它的伽罗瓦闭包 M/K , 然后利用 e, f 关于扩张的可乘性即可. \square

如果 $f_{L/K} = 1$, 称之为完全分歧, 即 $L \cap \tilde{K} = K$. 如果 $e_{L/K} = 1$, 称之为非分歧, 即 $L \subseteq \tilde{K}$. 此时,

$$G(\tilde{K}/K) \rightarrow G(L/K)$$

是满射. 若 f_K 有限, 称 φ_K 的像 $\varphi_{L/K}$ 为 L/K 的弗罗贝尼乌斯.

定义 3.5 (亨泽尔赋值)

A_k 的一个亨泽尔赋值是指同态

$$v : A_k \rightarrow \widehat{\mathbb{Z}},$$

满足

- (1) $v(A_k) = Z \supseteq \mathbb{Z}$ 和 $\mathbb{Z}/n\mathbb{Z} \cong Z/nZ, \forall n \in \mathbb{N}$,
- (2) $v(\mathbf{N}_{K/k} A_K) = f_k Z$.



命题 3.6

对有限扩张 K/k ,

$$v_K = \frac{1}{f_K} v \circ \mathbf{N}_{K/k} : A_K \rightarrow Z$$

定义了一个满同态, 且

- (1) $v_K = v_{K^\sigma} \circ \sigma, \forall \sigma \in G$,
- (2) 对于有限扩张 L/K ,

$$\begin{array}{ccc} A_L & \xrightarrow{v_L} & \widehat{Z} \\ \mathbf{N}_{L/K} \downarrow & & \downarrow f_{L/K} \\ A_K & \xrightarrow{v_K} & \widehat{Z}. \end{array}$$



证明 (1) 设 τ 取遍 G_k/G_K 的一组代表元, 则 $\sigma^{-1}\tau\sigma$ 取遍 $G_k/\sigma^{-1}G_K\sigma = G_k/G_{K^\sigma}$ 的一组代表元. 因此

$$v_{K^\sigma}(a^\sigma) = \frac{1}{f_{K^\sigma}} v \left(\prod_{\tau} a^{\tau\sigma} \right) = \frac{1}{f_K} v \left(\prod_{\tau} a^\tau \right) = v_K(a).$$

(2) 由范数关于域扩张 $L/K/k$ 的分解性得到. □

定义 3.7 (素元)

A_K 的素元是指满足 $v_K(\pi_K) = 1$ 的 $\pi_K \in A_K$. 记

$$U_K = \{u \in A_K \mid v_K(u) = 0\}.$$



容易知道, 当 L/K 非分歧时, K 的素元仍然是 L 的素元; 当 L/K 完全分歧时, L 素元的范数是 K 的素元.

§3.1.4 互反映射

对于抽象的伽罗瓦群 G 和一个 G 模 A , 我们固定了

$$d : G \rightarrow \widehat{Z}, \quad v : A_k \rightarrow \widehat{Z}.$$

我们现在只考虑有限扩张 K/k . 我们要求 G 和 A 满足如下的类域论公理:

公理 3.8 (类域论公理)

对于任意循环扩张 L/K ,

$$\#H^0(G(L/K), A_L) = [L : K], \quad H^{-1}(G(L/K), A_L) = 1.$$

**命题 3.9**

对于任意非分歧扩张 L/K ,

$$H^0(G(L/K), U_L) = H^{-1}(G(L/K), U_L) = 1.$$



证明 由于 L/K 非分歧, 因此 π_K 是 L 的素元. 由于 $H^{-1}(G(L/K), A_L) = 1$, 因此对于任意 $u \in U_L^{\mathbf{N}=1}$, 存在 $a \in A_L$ 使得 $u = a^{\sigma-1}$. 设 $a = \varepsilon \pi_K^m, \varepsilon \in U_L$, 则 $u = \varepsilon^{\sigma-1}$. 因此 $H^{-1}(G(L/K), U_L) = 1$.

满同态 $v_K : A_K \rightarrow Z$ 诱导了满同态

$$v_K : A_K/\mathbf{N}A_L \rightarrow Z/nZ \cong \mathbb{Z}/n\mathbb{Z}, \quad n = f_{L/K} = [L : K].$$

由于 $\#A_K/\mathbf{N}A_L = n$, 因此这是一个同构. 对于 $u \in U_K, v_K(u) = 0$, 因此存在 $a \in A_L$ 使得 $u = \mathbf{N}a$. 而 $v_K(u) = nv_L(a)$, 因此 $a \in U_L, H^0(G(L/K), U_L) = 1$. \square

对于无限扩张 L/K , 我们令

$$\mathbf{N}_{L/K}A_L := \bigcap_M \mathbf{N}_{M/K}A_M,$$

其中 M/K 取遍 L/K 的所有有限子扩张. 所谓的互反映射指的是如下的一个典范同态

$$r_{L/K} : G(L/K) \rightarrow A_K/\mathbf{N}_{L/K}A_L.$$

考虑 \tilde{L}/K , 则 $G_{\tilde{L}} = I_L \subseteq I_K$. 因此 $d_K : G_K \rightarrow \hat{\mathbb{Z}}$ 诱导了 $d_K : G(\tilde{L}/K) \rightarrow \hat{\mathbb{Z}}$. 定义

$$\text{Frob}(\tilde{L}/K) = \left\{ \sigma \in G(\tilde{L}/K) \mid d_K(\sigma) \in \mathbb{N}^+ \right\}.$$

定理 3.10 (互反映射)

定义

$$\begin{aligned} r_{\tilde{L}/K} : \text{Frob}(\tilde{L}/K) &\longrightarrow A_K/\mathbf{N}_{\tilde{L}/K}A_{\tilde{L}} \\ \sigma &\longmapsto \mathbf{N}_{\Sigma/K}(\pi_\Sigma) \bmod \mathbf{N}_{\tilde{L}/K}A_{\tilde{L}}, \end{aligned}$$

其中 Σ 是 σ 的固定域, π_Σ 是它的一个素元. 它可以下降为

$$r_{L/K} : G(L/K) \rightarrow A_K/\mathbf{N}_{L/K}A_L.$$



引理 3.11

设 Σ 是 $\sigma \in \text{Frob}(\tilde{L}/K)$ 的固定域, 则

$$f_{\Sigma/K} = d_K(\sigma), \quad [\Sigma : K] < \infty, \quad \tilde{\Sigma} = \tilde{L}, \quad \sigma = \varphi_\Sigma.$$



证明 (1) 由于 $\Sigma \cap \tilde{K}$ 是 $\sigma|_{\tilde{K}} = \varphi_K^{d_K(\sigma)}$ 的固定域, 因此

$$f_{\Sigma/K} = [\Sigma \cap \tilde{K} : K] = d_K(\sigma).$$

(2) 由 $\tilde{K} \subseteq \Sigma\tilde{K} = \tilde{\Sigma} \subseteq \tilde{L}$ 知

$$e_{\Sigma/K} = (I_K : I_\Sigma) = \#G(\tilde{\Sigma}/\tilde{K}) \leq \#G(\tilde{L}/\tilde{K})$$

有限, 因此 $[\Sigma : K] = f_{\Sigma/K}e_{\Sigma/K}$ 有限.

(3) 由于 $\Gamma = G(\tilde{L}/\Sigma) = \langle \sigma \rangle$ 是射影循环群, $(\Gamma : \Gamma^n) \leq n$. 因此满射 $\Gamma \rightarrow G(\tilde{\Sigma}/\Sigma) \cong \tilde{\mathbb{Z}}$ 诱导了双射 $\Gamma/\Gamma^n \cong \tilde{\mathbb{Z}}/n\tilde{\mathbb{Z}}$, 从而 $\Gamma \cong G(\tilde{\Sigma}/\Sigma), \tilde{\Sigma} = \tilde{L}$.

(4) 由于 $f_{\Sigma/K}d_\Sigma(\sigma) = d_K(\sigma) = f_{\Sigma/K}$, 因此 $d_\Sigma(\tilde{\sigma}) = 1, \sigma = \varphi_\Sigma$. \square

定理 3.10 的证明 先考虑有限伽罗瓦扩张.

第一步. 对于有限伽罗瓦扩张 L/K ,

$$\begin{aligned} \text{Frob}(\tilde{L}/K) &\longrightarrow G(L/K) \\ \sigma &\longmapsto \sigma|_L \end{aligned}$$

是满射. 设 $\varphi \in G(\tilde{L}/K)$ 是 φ_K 的一个提升, 即 $\varphi|_{\tilde{K}} = \varphi_K$ 且 $d_K(\varphi) = 1$. 由于 $L \cap \tilde{K}/K$ 非分歧, 因此 $\varphi|_{L \cap \tilde{K}} = \varphi_{L \cap \tilde{K}/K}$. 对于任意 $\sigma \in G(L/K)$, σ 在 $L \cap \tilde{K}$ 上的限制是生成元 $\varphi_{L \cap \tilde{K}/K}$ 的一个幂次, 不妨设 $\sigma|_{L \cap \tilde{K}} = \varphi_{L \cap \tilde{K}/K}^n, n \in \mathbb{N}^+$. 由于 $\tilde{L} = L\tilde{K}$, 因此

$$G(\tilde{L}/\tilde{K}) \cong G(L/L \cap \tilde{K}).$$

设 $\tau \in G(\tilde{L}/\tilde{K})$ 是 $\sigma\varphi^{-n}|_L$ 的原像, 则 $\tilde{\sigma} = \tau\varphi^n$ 满足 $\tilde{\sigma}|_L = \sigma$ 和 $\tilde{\sigma}|_{\tilde{K}} = \varphi_K^n$, 即 $d_K(\tilde{\sigma}) = n$.

第二步. $r_{\tilde{L}/K}$ 不依赖于 π_Σ 的选取. 设 $u \in U_\Sigma$, 对于任意 $\Sigma \subseteq M \subseteq \tilde{\Sigma} = \tilde{L}$, 由类域论公理, 存在 $\varepsilon \in U_M$ 使得 $u = \mathbf{N}_{M/\Sigma}(\varepsilon)$, 因此 $\mathbf{N}_{\Sigma/K}(u) = \mathbf{N}_{M/K}(\varepsilon) \in \mathbf{N}_{M/K}A_M$. 从而 $\mathbf{N}_{\Sigma/K}(u) \in \mathbf{N}_{\tilde{L}/K}A_{\tilde{L}}$, 因此 $r_{\tilde{L}/K}$ 不依赖于素元的选取.

第三步. $r_{\tilde{L}/K}$ 具有可乘性. 对于任意 $\varphi \in G(\tilde{L}/K)$, 考虑自同态

$$\begin{aligned} \varphi - 1 : A_{\tilde{L}} &\rightarrow A_{\tilde{L}}, & a &\mapsto a^\varphi/a, \\ \varphi_n : A_{\tilde{L}} &\rightarrow A_{\tilde{L}}, & a &\mapsto \prod_{i=0}^{n-1} a^{\varphi^i}. \end{aligned}$$

显然 $(\varphi - 1) \circ \varphi_n = \varphi_n \circ (\varphi - 1) = \varphi^n - 1$. 设 $\sigma_1 = \sigma_2\sigma_3 \in \text{Frob}(\tilde{L}/K)$, $n_i = d_K(\tilde{\sigma}_i)$, Σ_i 为 σ_i 的固定域, $\pi_i \in A_{\Sigma_i}$ 是素元. 固定 $\varphi \in G(\tilde{L}/K)$ 使得 $d_K(\varphi) = 1$, 令 $\tau_i = \sigma_i^{-1}\varphi^{n_i} \in G(\tilde{L}/\tilde{K})$. 我们知道 $n_3 = n_1 + n_2$,

$$\tau_3 = \sigma_2^{-1}\sigma_1^{-1}\varphi^{n_1+n_2} = (\sigma_2^{-1}\varphi^{n_2})(\varphi^{-n_2}\sigma_1\varphi^{n_2})^{-1}\varphi^{n_1}.$$

令 $\sigma_4 = \varphi^{-n_2}\sigma_1\varphi^{n_2}$, $n_4 = d_K(\sigma_4) = n_1$, $\Sigma_4 = \Sigma_1^{\varphi^{n_2}}$, $\pi_4 = \pi_1^{\varphi^{n_2}} \in A_{\Sigma_4}$, $\tau_4 = \sigma_4^{-1}\varphi^{n_4}$, 则 $\tau_3 = \tau_2\tau_4$ 且 $\mathbf{N}_{\Sigma_4/K}(\pi_4) = \mathbf{N}_{\Sigma_1/K}(\pi_1)$. 我们只需证明

$$\mathbf{N}_{\Sigma_3/K}(\pi_3) \equiv \mathbf{N}_{\Sigma_2/K}(\pi_2)\mathbf{N}_{\Sigma_4/K}(\pi_4) \pmod{\mathbf{N}_{\tilde{L}/K}A_{\tilde{L}}}.$$

引理 3.12

设 $\varphi, \sigma \in \text{Frob}(\tilde{L}/K)$, $d_K(\varphi) = 1$, $d_K(\sigma) = n$. 若 Σ 是 σ 的固定域, $a \in A_\Sigma$, 则

$$\mathbf{N}_{\Sigma/K}(a) = (\mathbf{N} \circ \varphi_n)(a) = (\varphi_n \circ \mathbf{N})(a),$$

其中 $\mathbf{N} = \mathbf{N}_{\tilde{L}/\tilde{K}}$.



证明 K 在 Σ 的极大非分歧扩张 $\Sigma^0 = \tilde{K} \cap \sigma/K$ 的扩张次数为 n , 伽罗瓦群 $G(\Sigma^0/K)$ 由 $\varphi_{\Sigma^0/K} = \varphi_K|_{\Sigma^0} = \varphi|_{\Sigma^0}$. 因此 $\mathbf{N}_{\Sigma^0/K} = \varphi_n|_{A_{\Sigma^0}}$. 又因为 $\Sigma\tilde{K} = \tilde{\Sigma}$, $\Sigma \cap \tilde{K} = \Sigma^0$, $\mathbf{N}_{\Sigma/\Sigma^0} = \mathbf{N}|_{A_\Sigma}$. 对于 $a \in A_\Sigma$,

$$\mathbf{N}_{\Sigma/K}(a) = \mathbf{N}_{\Sigma^0/K}(\mathbf{N}_{\Sigma/\Sigma^0}(a)) = \mathbf{N}(a)^{\varphi_n} = \mathbf{N}(a^{\varphi_n}).$$

最后由 φ 正规化 $G(\tilde{L}/\tilde{K})$ 可知第二个等式成立. \square

现在我们知道 $\mathbf{N}_{\Sigma_i/K}(\pi_i) = \mathbf{N}(\pi_i^{\varphi^{n_i}})$. 因此我们只需证明 $\mathbf{N}(u) \in \mathbf{N}_{\tilde{L}/K}A_{\tilde{L}}$, $u = \pi_3^{\varphi^{n_3}}\pi_4^{-\varphi^{n_4}}\pi_2^{-\varphi^{n_2}}$. 注意到 $I_{G(\tilde{L}/\tilde{K})}U_{\tilde{L}}$ 中的元素在 \mathbf{N} 下的像为 1, 因此 \mathbf{N} 诱导了同态 $H_0(G(\tilde{L}/\tilde{K}), U_{\tilde{L}}) \rightarrow U_{\tilde{K}}$.

引理 3.13

如果 $x \in H_0(G(\tilde{L}/\tilde{K}), U_{\tilde{L}})$ 被 $\varphi \in G(\tilde{L}/K)$ 固定, 且 $d_K(\varphi) = 1$, 则 $\mathbf{N}(x) \in \mathbf{N}_{\tilde{L}/K}U_{\tilde{L}}$.



证明 设 $x = u \pmod{I_{G(\tilde{L}/\tilde{K})}U_{\tilde{L}}}$, 则

$$u^{\varphi-1} = \prod_{i=1}^r u_i^{\tau_i-1}, \quad \tau_i \in G(\tilde{L}/\tilde{K}), u_i \in U_{\tilde{L}}.$$

设 M/K 是 \tilde{L}/K 的有限伽罗瓦子扩张, 不妨设 $u, u_i \in M$ 且 $L \subseteq M$. 设 $n = [M : K]$, $\sigma = \varphi^n \in G(\tilde{L}/M)$, Σ 是 σ 的固定域, Σ_n 是 $\sigma^n = \varphi_n^n$ 的固定域, 则 Σ_n/Σ 是 n 次非分歧扩张. 由类域论公理, 存在 $\tilde{u}, \tilde{u}_i \in U_{\Sigma_n}$ 使得

$$u = \mathbf{N}_{\Sigma_n/\Sigma}(\tilde{u}) = \tilde{u}^{\sigma^n}, \quad u_i = \mathbf{N}_{\Sigma_n/\Sigma}(\tilde{u}_i) = \tilde{u}_i^{\sigma^n}.$$

因此 $\tilde{u}^{\varphi-1}$ 和 $\prod_i \tilde{u}_i^{\varphi-1}$ 仅相差一个 $\tilde{x} \in U_{\Sigma_n}$ 满足 $\mathbf{N}_{\Sigma_n/\Sigma}(\tilde{x}) = 1$. 再次由类域论公理, 存在 $\tilde{y} \in U_{\Sigma_n}, \tilde{x} = \tilde{y}^{\sigma-1} = \tilde{y}^{\varphi_n(\varphi-1)}$. 从而

$$\mathbf{N}(\tilde{u})^{\varphi-1} = \mathbf{N}(\tilde{y}^{\varphi_n})^{\varphi-1}, \quad \mathbf{N}(\tilde{u}) = \mathbf{N}(\tilde{y}^{\varphi_n})z,$$

其中 $z \in U_{\tilde{K}}, z^{\varphi-1} = 1$, 即 $z \in U_K$. 设 $y = \tilde{y}^{\sigma_n} = \mathbf{N}_{\Sigma_n/\Sigma}(\tilde{y}) \in U_{\Sigma}$,

$$\mathbf{N}(u) = \mathbf{N}(\tilde{u})^{\sigma_n} = \mathbf{N}(\tilde{y}^{\varphi_n})^{\sigma_n} z^{\sigma_n} = \mathbf{N}(y^{\varphi_n})z^n = \mathbf{N}_{\Sigma/K}(y)\mathbf{N}_{M/K}(z)$$

属于 $\mathbf{N}_{M/K}U_M$. □

现在返回到原命题. 由于 $\varphi_{n_i} \circ (\varphi - 1) = \varphi^{n_i} - 1, \pi_i^{\varphi_{n_i}-1} = \pi_i^{\tau_i-1}$, 因此

$$u^{\varphi-1} = \pi_3^{\tau_3-1} \pi_4^{1-\tau_4} \pi_2^{1-\tau_2}.$$

由于 $\tau_3 = \tau_2\tau_4$ 知道 $(\tau_3 - 1) + (1 - \tau_2) + (1 - \tau_4) = (1 - \tau_2)(1 - \tau_4)$. 设

$$\pi_3 = u_3\pi_4, \quad \pi_2 = u_2^{-1}\pi_4, \quad \pi_4^{\tau_2} = u_4\pi_4,$$

则 $u^{\varphi-1} = \prod_{i=2}^4 u_i^{\tau_i-1}$, 从而 $\mathbf{N}(u) \in \mathbf{N}_{\tilde{L}/K}A_{\tilde{L}}$.

第四步. 互反映射 $r_{L/K}$ 良定. 由于 $\text{Frob}(\tilde{L}/K) \rightarrow G(L/K)$ 是满射, 且 $\mathbf{N}_{\tilde{L}/K}A_{\tilde{L}} \subseteq \mathbf{N}_{L/K}A_L$, 因此 $r_{\tilde{L}/K} : \text{Frob}(\tilde{L}/K) \rightarrow A_K/\mathbf{N}_{\tilde{L}/K}A_{\tilde{L}}$ 可以下降为

$$r_{L/K} : G(L/K) \rightarrow A_K/\mathbf{N}_{L/K}A_L.$$

我们只需说明该定义不依赖于 $\sigma \in G(L/K)$ 在 $\text{Frob}(\tilde{L}/K)$ 中提升 $\tilde{\sigma}$ 的选取. 设 $\tilde{\sigma}'$ 也提升 $\sigma, \Sigma, \pi_{\Sigma'} \in A_{\Sigma'}$ 是素元. 如果 $d_K(\tilde{\sigma}) = d_K(\tilde{\sigma}')$, 则二者在 \tilde{K} 和 L 上均相同, 从而二者相同. 如果 $d_K(\tilde{\sigma}) < d_K(\tilde{\sigma}')$, 则存在 $\tilde{\tau} \in \text{Frob}(\tilde{L}/K)$ 使得 $\tilde{\sigma}' = \tilde{\sigma}\tilde{\tau}$ 且 $\tilde{\tau}|_L = 1$. 因此 $\tilde{\tau}$ 的固定域 Σ'' 包含 L , 从而 $r_{\tilde{L}/K}(\tilde{\tau}) \equiv \mathbf{N}_{\Sigma''/K}(\pi_{\Sigma''}) \equiv 1 \pmod{\mathbf{N}_{L/K}A_L}$, 因此 $r_{\tilde{L}/K}(\tilde{\sigma}') = r_{\tilde{L}/K}(\tilde{\sigma})$.

第五步. 根据定义不难证明互反映射满足下列函子性质. 从而可知命题对于无限伽罗瓦扩张 L/K 也成立. □

命题 3.14

对于有限伽罗瓦扩张 $L/K, L'/K'$, 如果 $K \subseteq K', L \subseteq L', \sigma \in G(L/K)$, 则下列图表交换

$$\begin{array}{ccc} G(L'/K') & \xrightarrow{r_{L'/K'}} & A_{K'}/\mathbf{N}_{L'/K'}A_{L'} \\ \downarrow & & \downarrow \mathbf{N}_{K'/K} \\ G(L/K) & \xrightarrow{r_{L/K}} & A_K/\mathbf{N}_{L/K}A_L \end{array}$$

其中左垂直箭头为限制在 L 上,

$$\begin{array}{ccc} G(L/K) & \xrightarrow{r_{L/K}} & A_K/\mathbf{N}_{L/K}A_L \\ \downarrow & & \downarrow \sigma \\ G(L^\sigma/K^\sigma) & \xrightarrow{r_{L^\sigma/K^\sigma}} & A_{K^\sigma}/\mathbf{N}_{L^\sigma/K^\sigma}A_{L^\sigma} \end{array}$$

其中左垂直箭头为 σ 共轭作用.



如果 $L = L'$, 则有自然的嵌入 $A_K/\mathbf{N}_{L/K}A_L \hookrightarrow A_{K'}/\mathbf{N}_{L'/K'}A_{L'}$, 它在伽罗瓦群的反映为变换映射(Verlagerung). 设 H 是 G 的指标有限的子群, 则我们可以定义典范的同态

$$\text{Ver} : G^{\text{ab}} \rightarrow H^{\text{ab}}.$$

对于 $\sigma \in G$, 我们有双倍集分解

$$G = \bigsqcup_{\tau} \langle \sigma \rangle \tau H.$$

对于任意 τ , 设 $f(\tau)$ 是最小的正整数使得 $\sigma_{\tau} = (\tau^{-1}\sigma\tau)^{f(\tau)} \in H$, 定义

$$\text{Ver}(\sigma \bmod G') = \prod_{\tau} \sigma_{\tau} \bmod H'.$$

 **练习 3.1.4** 证明 Ver 是一个良定义的同态.

命题 3.15

对于有限伽罗瓦扩张 L/K 的中间域 K' , 我们有交换图表

$$\begin{array}{ccc} G(L/K')^{\text{ab}} & \xrightarrow{r_{L/K'}} & A_{K'}/\mathbf{N}_{L/K'}A_L \\ \text{Ver} \uparrow & & \uparrow \\ G(L/K)^{\text{ab}} & \xrightarrow{r_{L/K}} & A_K/\mathbf{N}_{L/K}A_L \end{array}$$

其中右侧由嵌入诱导.



证明 我们暂时记 $G = G(\tilde{L}/K)$, $H = G(\tilde{L}/K')$. 设 $\sigma \in G(L/K)$, $\tilde{\sigma} \in \text{Frob}(\tilde{L}/K)$ 是 σ 的原像, Σ 为固定域, $S = G(\tilde{L}/\Sigma) = \langle \tilde{\sigma} \rangle$. 考虑双倍集分解

$$G = \bigsqcup_{\tau} S\tau H.$$

令 $S_{\tau} = \tau^{-1}S\tau \cap H$, $\tilde{\sigma}_{\tau} = \tau^{-1}\tilde{\sigma}^{f(\tau)}\tau$. 令

$$\bar{G} = G(L/K), \bar{H} = G(L/K'), \bar{S} = \langle \sigma \rangle, \bar{\tau} = \tau|_L, \sigma_{\tau} = \tilde{\sigma}_{\tau}|_L,$$

则显然有双倍集分解

$$\bar{G} = \bigsqcup_{\tau} \bar{S}\bar{\tau}\bar{H}.$$

因此

$$\text{Ver}(\sigma \bmod G(L/K)') = \prod_{\tau} \sigma_{\tau} \bmod G(L/K)'.$$

对于任意 τ , 设有陪集分解

$$H = \bigsqcup_{\omega_{\tau}} S_{\tau}\omega_{\tau}, \quad G = \bigsqcup_{\tau, \omega_{\tau}} S\tau\omega_{\tau}.$$

设 Σ_{τ} 是 $\tilde{\sigma}_{\tau}$ 的固定域, Σ^{τ} 是 $\tau^{-1}\tilde{\sigma}\tau$ 的固定域, 则 $\Sigma_{\tau}/\Sigma^{\tau}$ 是 $f(\tau)$ 次非分歧扩张. 如果 $\pi \in A_{\Sigma}$ 是 Σ 的素元, 则 $\pi^{\tau} \in A_{\Sigma^{\tau}}$ 是 Σ^{τ} 的素元, 因此也是 Σ_{τ} 的素元. 从而,

$$\begin{aligned} \mathbf{N}_{\Sigma/K}(\pi) &= \prod_{\tau, \omega_{\tau}} \pi^{\tau\omega_{\tau}} = \prod_{\tau} \mathbf{N}_{\Sigma_{\tau}/K'}(\pi^{\tau}), \\ r_{L/K}(\sigma) &\equiv \prod_{\tau} r_{L/K'}(\sigma_{\tau}) \equiv r_{L/K'}\left(\prod_{\tau} \sigma_{\tau}\right) \equiv r_{L/K'}\left(\text{Ver}(\sigma \bmod G(L/K)')\right). \end{aligned}$$

□

命题 3.16

如果 L/K 非分歧, 则 $r_{L/K}$ 由 $r_{L/K}(\varphi_{L/K}) = \pi_K \bmod \mathbf{N}_{L/K}A_L$ 确定, 此时 $r_{L/K}$ 是同构.



证明 此时 $\tilde{L} = \tilde{K}$, $\varphi_K \in G(\tilde{K}/K)$ 是 $\varphi_{L/K}$ 的原像, 固定域为 K , 因此 $r_{L/K}$ 由此给出. 赋值 v_K 诱导了同构 $A_K/\mathbf{N}_{L/K}A_L \xrightarrow{\sim} Z/nZ \cong \mathbb{Z}/n\mathbb{Z}$, 这是因为对于 $v_K(a) \equiv \text{mod } nZ$, $a = u\pi_K^{dn}$, 而 $u = \mathbf{N}_{L/K}(\varepsilon)$, $\varepsilon \in U_L$, 从而 $a = \mathbf{N}_{L/K}(\varepsilon\pi_K^d)$. 最后由于生成元 $\varphi_{L/K}$ 的像为素元 π_K , 即生成元相互对应, 从而 $r_{L/K}$ 是同构. \square

§3.1.5 互反律

类域论的主定理如下所述:

定理 3.17 (互反律)

对于任意有限伽罗瓦扩张 L/K , 互反映射

$$r_{L/K} : G(L/K)^{\text{ab}} \rightarrow A_L/\mathbf{N}_{L/K}A_K$$

是同构.



证明 设 M/K 是 L/K 的伽罗瓦子扩张, 则我们有交换图表

$$\begin{array}{ccccccc} 1 & \longrightarrow & G(L/M) & \longrightarrow & G(L/K) & \longrightarrow & G(M/K) \longrightarrow 1 \\ & & \downarrow r_{L/M} & & \downarrow r_{L/K} & & \downarrow r_{M/K} \\ & & A_M/\mathbf{N}_{L/M}A_L & \xrightarrow{\mathbf{N}_{M/K}} & A_K/\mathbf{N}_{L/K}A_L & \longrightarrow & A_K/\mathbf{N}_{M/K}A_M \longrightarrow 1. \end{array}$$

第一步. 约化到 $G(L/K)$ 是交换群情形. 若此时已成立, 则取 $M = L^{\text{ab}}/K$ 为其极大阿贝尔子扩张, 即 $G(M/K) = G(L/K)^{\text{ab}}$. 此时 $G(L/M)$ 是 $r_{L/K}$ 的核, 因此 $r_{L/K}$ 是单射. 要证明满射, 我们对次数进行归纳. 当 $G(L/K)$ 是可解群时, $M = L$ 或 $[L : M] < [L : K]$, 如果 $r_{L/M}$ 和 $r_{M/K}$ 都是满射, 则 $r_{L/K}$ 也是满射. 一般情形下, 设 M 是 $G(L/K)$ 的一个希洛夫 p 子群的固定域, 则我们只需证明 $\mathbf{N}_{M/K}$ 的像是 $A_K/\mathbf{N}_{L/K}A_L$ 的希洛夫 p 子群 S_p 即可, 这诱导了 $r_{L/K}$ 是满射. 嵌入 $A_K \hookrightarrow A_M$ 诱导了

$$i : A_K/\mathbf{N}_{L/K}A_L \rightarrow A_M/\mathbf{N}_{L/M}A_L,$$

他满足 $\mathbf{N}_{M/K} \circ i = [M : K]$. 由于 $p \nmid [M : K]$, 因此 $[M : K] : S_p \rightarrow S_p$ 是同构, 从而 S_p 落在 $\mathbf{N}_{M/K}$ 的像, 因此 $r_{L/K}$ 是满射.

第二步. 约化到循环扩张情形. 若 M/K 取遍所有循环子扩张, $r_{L/K}$ 的核落在 $G(L/K) \rightarrow \prod G(M/K)$ 的核中. 由于 $G(L/K)$ 是交换群, 该映射是单的, 因此 $r_{L/K}$ 是单射. 由于此时 $G(L/K)$ 是可解的, 因此对次数进行和第一步相同的归纳可知 $r_{L/K}$ 是满射.

第三步. 设 L/K 是循环扩张. 不妨设 $f_{L/K} = 1$. 实际上, 设 $M = L \cap \tilde{K}$, 则 $f_{L/M} = 1$, $r_{M/K}$ 是同构. 由类域论公理可知图表中下面一行的群的阶, 从而它是正合的, 因此 $r_{L/M}$ 是同构蕴含 $r_{L/K}$ 是同构.

设 L/K 是循环完全分歧扩张. 设 $G(L/K) = \langle \sigma \rangle$. 我们把 σ 在 $G(L/K) \cong G(\tilde{L}/\tilde{K})$ 下的像仍记为 σ , 则 $\tilde{\sigma} = \sigma\varphi_L \in \text{Frob}(\tilde{L}/\tilde{K})$ 是 σ 的一个原像, 且 $d_K(\tilde{\sigma}) = 1 = f_{L/K}$. 设 Σ 是 $\tilde{\sigma}$ 的固定域, 则 $f_{\Sigma/K} = 1$, 因此 $\Sigma \cap \tilde{K} = K$. 设 M/K 是 \tilde{L}/\tilde{K} 的伽罗瓦子扩张, 包含 ΣL , $M^0 = M \cap \tilde{K}$. 令 $\mathbf{N} = \mathbf{N}_{M/M^0}$, 则 $\mathbf{N}_{A_\Sigma} = \mathbf{N}_{\Sigma/K}$, $\mathbf{N}_{A_L} = \mathbf{N}_{L/K}$.

设 $r_{L/K}(\sigma^k) = 1$, $0 \leq k < n = [L : K]$. 由于 π_Σ 和 π_L 都是 M 的素元, 因此 $\pi_\Sigma^k = u\pi_L^k$, $u \in U_M$, 于是

$$r_{L/K}(\sigma^k) \equiv \mathbf{N}(\pi_\Sigma^k) \equiv \mathbf{N}(u)\mathbf{N}(\pi_L^k) \equiv \mathbf{N}(u) \text{ mod } \mathbf{N}_{L/K}A_L.$$

由 $r_{L/K}(\sigma^k) = 1$ 知存在 $v \in U_L$ 使得 $\mathbf{N}(uv^{-1}) = 1, uv^{-1} = a^{\sigma^{-1}}, a \in A_M$, 从而

$$(\pi_L^k v)^{\sigma^{-1}} = (\pi_L^k v)^{\tilde{\sigma}^{-1}} = (\pi_{\Sigma}^k u^{-1} v)^{\tilde{\sigma}^{-1}} = (a^{\sigma^{-1}})^{\tilde{\sigma}^{-1}} = (a^{\tilde{\sigma}^{-1}})^{\sigma^{-1}},$$

因此 $x = \pi_L^k v a^{1-\tilde{\sigma}} \in A_{M^0}$. 由于 $nv_{M^0}(x) = v_M(x) = k$, 因此 $k = 0$, $r_{L/K}$ 是单射. 由类域论公理知 $\#A_K/\mathbf{N}_{L/K}A_L = n$, 因此 $r_{L/K}$ 是同构. \square

我们考虑互反映射的逆诱导的同态

$$(\cdot, L/K) : A_K \rightarrow G(L/K)^{\text{ab}},$$

它的核是 $\mathbf{N}_{L/K}A_L$, 我们称该映射为**范剩余符号**. 由互反映射的函子性我们自然有范剩余符号的函子性. 对于无限伽罗瓦扩张 L/K ,

$$G(L/K)^{\text{ab}} = \varprojlim_i G(L_i/K)^{\text{ab}},$$

其中 L_i/K 取遍所有有限子扩张. 由于 $(a, L'/K)|_{L^{\text{ab}}} = (a, L/K)$, 因此这定义出 $G(L/K)^{\text{ab}}$ 的一个元素, 即此时也有范剩余符号.

命题 3.18

我们有

$$(a, \tilde{K}/K) = \varphi_K^{v_K(a)}, \quad d_K \circ (\cdot, \tilde{K}/K) = v_K.$$



证明 考虑它的有限 f 次子扩张 L/K , 则 $v_K(a) = n + fz, n \in \mathbb{Z}, z \in \mathbb{Z}$, 即 $a = u\pi_K^n b^f, u \in U_K, b \in A_K$. 于是

$$(a, \tilde{K}/K)|_L = (a, L/K) = (\pi_K, L/K)^n (b, L/K)^f = \varphi_{L/K}^n = \varphi_K^{v_K(a)}|_L.$$

从而 $(a, \tilde{K}/K) = \varphi_K^{v_K(a)}$. \square

对于任意 K , 我们赋予 A_K 拓扑为 $\mathbf{N}_{L/K}A_L$ 形成单位元的邻域基, 其中 L/K 取遍有限伽罗瓦扩张, 我们称之为**范数拓扑**.

命题 3.19

- (1) A_K 的开子群是它的有限指标闭子群.
- (2) $v_K : A_K \rightarrow \widehat{\mathbb{Z}}$ 是连续的.
- (3) 对于有限扩张 $L/K, \mathbf{N}_{L/K} : A_L \rightarrow A_K$ 是连续的.
- (4) A_K 是豪斯多夫的当且仅当 $A_K^0 = \bigcap_L \mathbf{N}_{L/K}A_L = 0$.



证明 (1) 根据习题 3.1.1, 我们只需说明开子群是有限指标的, 而这由它包含某个 $\mathbf{N}_{L/K}A_L$ 可知.

(2) $f\widehat{\mathbb{Z}}, f \geq 1$ 形成 $0 \in \widehat{\mathbb{Z}}$ 的邻域基. 设 L/K 是 f 次非分歧扩张, 则 $v_K(\mathbf{N}_{L/K}A_L) = f v_L(A_L) \subset f\widehat{\mathbb{Z}}$, 因此 v_K 连续.

(3) 由于 $\mathbf{N}_{M/K}A_M$ 形成 $a \in A_K$ 的邻域基, 而它的原像包含 $\mathbf{N}_{M/L}A_M$, 因此 $\mathbf{N}_{L/K}$ 连续.

(4) 显然. \square

通过互反律, 我们可以给出 K 的有限阿贝尔扩张的一种刻画.

定理 3.20

映射

$$L \mapsto \mathcal{N}_L = \mathbf{N}_{L/K}A_L$$

给出了有限阿贝尔扩张 L/K 和 A_K 的开子群间的一一对应。



证明 证明是比较直接的, 见 [15, Theorem 4.6.7]. □

我们称 A_K 的开子群 \mathcal{N} 对应 L 为其对应的类域, 则

$$G(L/K) \cong A_K/\mathcal{N}.$$

§3.2 局部类域论

§3.2.1 局部互反律

对于任意域 k , $G = G(k^{\text{sep}}/k)$, $A = (k^{\text{sep}})^{\times}$, 我们都有如下结论:

定理 3.21 (希尔伯特 90)

对于有限循环扩张 L/K , $H^{-1}(G(L/K), L^{\times}) = 1$.



命题 3.22 (诺特)

对于有限伽罗瓦扩张 L/K , $H^1(G(L/K), L^{\times}) = 1$.



由于循环扩张情形, $H^1 = H^{-1}$, 因此这蕴含希尔伯特 90.

证明 设 $f: G \rightarrow L^{\times}$ 是一个 1 余循环. 对于 $c \in L^{\times}$, 令

$$\alpha = \sum_{\sigma \in G(L/K)} f(\sigma)c^{\sigma}.$$

由 $1, \sigma, \dots, \sigma^{n-1}$ 的线性无关性 1.4, 存在 $c \in L^{\times}$ 使得 $\alpha \neq 0$. 我们有

$$\alpha^{\tau} = \sum_{\sigma} f(\sigma)^{\tau} c^{\sigma\tau} = \sum_{\sigma} f(\tau)^{-1} f(\sigma\tau) c^{\sigma\tau} = f(\tau)^{-1} \alpha,$$

因此 $f(\sigma) = (\alpha^{-1})^{\sigma-1}$ 是 1 余边界. □

设 k 是 \mathbb{Q}_p 的有限扩张.

定理 3.23

设 $G = G(\bar{k}/k)$, $A = \bar{k}^{\times}$, 则它们满足类域论公理 3.8.



证明 $H^{-1} = 1$ 由希尔伯特 90 得到. 设 $G = G(L/K)$, 则我们有 G 模正合列

$$0 \rightarrow U_L \rightarrow L^{\times} \rightarrow \mathbb{Z} \rightarrow 0,$$

于是

$$h(G, L^{\times}) = h(G, \mathbb{Z})h(G, U_L) = [L : K]h(G, U_L).$$

选取 L/K 的一组正规基 $\{\alpha^{\sigma} \mid \sigma \in G\}$, $\alpha \in \mathcal{O}_L$. 设 $M = \sum_{\sigma \in G} \mathcal{O}_K \alpha^{\sigma} \subseteq \mathcal{O}_L$. 则

$$V^n = 1 + \pi_K^n M, \quad n = 1, 2, \dots$$

形成了 $1 \in U_L$ 的一组邻域基. 由于 M 是开子群, 因此存在 N 使得 $\pi_K^N \mathcal{O}_L \subseteq M$, 于是对于 $n \geq N$,

$$(\pi_K^n M)(\pi_K^n M) = \pi_K^{2n} MM \subseteq \pi_K^{2n} \mathcal{O}_L \subseteq \pi_K^{2n-N} M \subseteq \pi_K^n M,$$

即 $V^n V^n \subseteq V^n$. 显然 V^n 包含其中元素的逆. 我们有 G 模同构

$$\begin{aligned} V^n/V^{n+1} &\xrightarrow{\sim} M/\pi_K M \\ 1 + \pi_K^n \alpha &\mapsto \alpha \bmod \pi_K M. \end{aligned}$$

而

$$M/\pi_K M = \bigoplus_{\sigma \in G} (\mathcal{O}_K/\pi_K) \alpha^\sigma = \text{Ind}_G^1(\mathcal{O}_K/\pi_K),$$

由命题 A.45, $H^i(G, V^n/V^{n+1}) = 1, i = 0, -1$. 设 $a \in (V^n)^G$, 则存在 $b_0 \in V^n, a_1 \in (V^{n+1})^G$ 使得 $a = (\mathbf{N}b_0)b_1$. 归纳地, 我们得到一串 $b_i \in V^{n+i}$ 使得 $a = \mathbf{N}(\prod_{i=0}^{\infty} b_i)$, 这里这个乘积是收敛的. 因此 $H^0(G, V^n) = 1$. 同理可得 $H^{-1}(G, V^n) = 1$, 因此 $h(G, V^n) = 1$. 而 U_L/V^n 有限, 因此

$$h(G, U_L) = h(G, U_L/V^n)h(G, V^n) = 1.$$

□

设 κ 为 k 的剩余域, \tilde{k} 为 k 的极大非分歧扩张, 则

$$G(\tilde{k}/k) \cong G(\bar{\kappa}/\kappa) \cong \hat{\mathbb{Z}}.$$

设 $q = \#\kappa$, 则 $1 \in \hat{\mathbb{Z}}$ 对应弗罗贝尼乌斯 $x \mapsto x^q$. 于是 $\varphi_k \in G(\tilde{k}/k)$ 由

$$a^{\varphi_k} \equiv a^q \bmod \mathfrak{p}_{\tilde{k}}, \quad a \in \mathcal{O}_{\tilde{k}}$$

决定. 我们有自然的满同态

$$d: G \rightarrow \hat{\mathbb{Z}}.$$

设 $v_K: K^\times \rightarrow \mathbb{Z}$ 为 K 的归一化赋值. 对于任意有限扩张 K/k , $\frac{1}{e_K}v_K$ 是 v_k 在 K^\times 上的延拓. 我们有

$$\frac{1}{e_K}v_K = \frac{1}{[K:k]}v_k \circ \mathbf{N}_{K/k},$$

因此 $v_K(\mathbf{N}_{K/k}K^\times) = f_K v_K(K^\times) = f_K \mathbb{Z}$, 即 v_k 是一个亨泽尔赋值,

$$d: G \rightarrow \hat{\mathbb{Z}}, \quad v_k: k^\times \rightarrow \mathbb{Z}$$

满足类域论的假设. 因此我们有局部域的互反律定理 3.17 和阿贝尔扩张刻画定理 3.20.

定理 3.24

对于任意局部域的有限伽罗瓦扩张,

$$r_{L/K}: G(L/K)^{\text{ab}} \rightarrow L^\times / \mathbf{N}_{L/K} K^\times$$

是同构.



定理 3.25

$$L \mapsto \mathcal{N}_L = \mathbf{N}_{L/K} L^\times$$

给出了局部域的有限阿贝尔扩张 L/K 和 K^\times 的有限指标开子群间的一一对应.



证明 这里需要证明赋值给出的拓扑中有限指标开子群和范数拓扑的开子群一致, 见 [15, Theorem 5.1.4]. 由范数拓扑下开子群包含 $\mathbf{N}_{L/K} U_L = U_K$ 知道它是开的, 显然它是有限指标的. 反之, 我们需要考虑库默尔理论.

设 $\varphi: A \rightarrow A$ 是 G 模满同态, 核 μ_φ 为 n 阶循环群. 在我们的情形, $a^\varphi := a^n$ 即可. 设 $K \supseteq \mu_\varphi$. 对

于集合 $B \subseteq A$, 记 $K(B)$ 为

$$H = \{\sigma \in G_K \mid \sigma b = b, \forall b \in B\}$$

的固定域. 显然如果 B 是 G_K 不变的, $K(B)/K$ 是伽罗瓦的. 库默尔扩张是指形如 $K(\wp^{-1}(\Delta))/K$ 的扩张, 其中 $\Delta \subseteq A_K$.

命题 3.26

库默尔扩张和 K 的指数为 n 的阿贝尔扩张一一对应. 设 L/K 是指数为 n 的阿贝尔扩张, 则

$$L = K(\wp^{-1}(\Delta)), \quad \Delta = A_L^\wp \cap A_K.$$

特别地, 如果 L/K 是循环扩张, 则存在 $\alpha^\wp \in A_K$ 使得 $L = K(\alpha)$.



证明 我们有单射

$$G(K(\wp^{-1}(a))/K) \hookrightarrow \mu_\wp \quad \sigma \mapsto \alpha^{\sigma-1},$$

其中 $\wp(\alpha) = a$. 由于 $\mu_\wp \subseteq A_K$, 因此该映射不依赖于 α 的选取. 从而

$$G(L/K) \hookrightarrow \prod_{a \in \Delta} G(K(\wp^{-1}(a))/K) \hookrightarrow \mu_\wp^\Delta$$

是单射.

反之我们有 $\wp^{-1}(\Delta) \subseteq A_L$. 由于 L/K 是它循环子扩张的合成, 考虑 M/K 是其中之一. 我们只需证 $M \subseteq K(\wp^{-1}(\Delta))$. 设 σ 生成 $G(M/K)$, ζ_\wp 生成 μ_\wp , $d = [M : K]$, $d' = n/d$, $\xi = \zeta_\wp^{n/d}$. 由于 $\mathbf{N}_{M/K}(\xi) = \xi^d = 1$, 由类域论公理存在 $\alpha \in A_M$ 使得 $\xi = \alpha^{\sigma-1}$, 因此 $K \subseteq K(\alpha) \subseteq M$. 由于 $\alpha^{\sigma^i} = \xi^i \alpha$, 因此 $\alpha^{\sigma^i} = \alpha$ 当且仅当 $d \mid i$, 所以 $M = K(\alpha)$. 最后 $(\alpha^\wp)^{\sigma-1} = \xi^\wp = 1$, $a = \alpha^\wp \in A_K$, 即 $\alpha \in \wp^{-1}(\Delta)$, 从而 $M \subseteq K(\wp^{-1}(\Delta))$. \square

定理 3.27

映射

$$\Delta \mapsto L = K(\wp^{-1}(\Delta))$$

给出了群 $A_K^\wp \subseteq \Delta \subseteq A_K$ 和指数为 n 的阿贝尔扩张 L/K 的一一对应, 其中 $\Delta = A_L^\wp \cap A_K$. 此时,

$$\Delta/A_K^\wp \cong \text{Hom}(G(L/K), \mu_\wp), \quad a \bmod A_K^\wp \mapsto \chi_a,$$

其中 $\chi_a(\sigma) = \alpha^{\sigma-1}$, $\alpha \in \wp^{-1}(a)$.



证明 考虑

$$\Delta \rightarrow \text{Hom}(L/K, \mu_\wp), \quad a \mapsto \chi_a.$$

$\chi_a = 1$ 当且仅当 $\alpha^{\sigma-1} = 1, \forall \sigma$, 从而 $\alpha \in A_K, a \in A_K^\wp$. 因此定理中映射为单射. 要证明满射, 任一 χ 的核的固定域 M/K 是 d 次循环扩张, 且诱导了 $\bar{\chi} : G(M/K) \rightarrow \mu_\wp$. 设 σ 生成 $G(M/K)$, 则 $\mathbf{N}_{M/K}(\bar{\chi}(\sigma)) = \bar{\chi}(\sigma)^d = 1$, 从而存在 $\alpha \in A_M, \bar{\chi}(\sigma) = \alpha^{\sigma-1}$. 很明显, $a = \alpha^\wp \in \Delta = A_L^\wp \cap A_K$. 对于 $\tau \in G(L/K)$, $\chi(\tau) = \bar{\chi}(\tau|_M) = \alpha^{\tau-1} = \chi_a(\tau)$, 即 $\chi = \chi_a$. 从而

$$\Delta/A_K^\wp \cong \text{Hom}(G(L/K), \mu_\wp).$$

根据这个对应可知, 如果 Δ 对应 L , 则它的大小是确定的,

最后我们来说明一一对应. 设 $A_K^\wp \subseteq \Delta \subseteq A_K$, 且 $L = K(\wp^{-1}(\Delta))$, 则 $\Delta \subseteq \Delta' = A_L^\wp \cap A_K$. 因此

$$\Delta'/A_K^\wp \cong \text{Hom}(G(L/K), \mu_\wp)$$

的子群对应

$$\Delta/A_K^\wp \cong \text{Hom}(G(L/K)/H, \mu_\wp),$$

其中

$$H = \{\sigma \in G(L/K) \mid \chi_a(\sigma) = 1, \forall a \in \Delta\}.$$

由于 $\chi_a(\sigma) = \sigma^{a-1}$, 因此 H 固定 $\wp^{-1}(\Delta)$, 从而固定 L , 即 $H = 1, \Delta = \Delta'$. \square

现在返回到局部类域论. 设 \mathcal{N} 是指标为 n 的子群, 则 $K^{\times n} \subset \mathcal{N}$. 我们可不妨设 $\mu_n \subseteq K^\times$, 不然令 $K_1 = K(\mu_n)$. 若 K_1 包含 $\mathbf{N}_{L_1/K_1} L_1^\times$, L/K 是包含 L_1 的伽罗瓦扩张, 则 $\mathbf{N}_{L/K} L^\times \subseteq K^\times$.

现在设 $\mu_n \subseteq K, L = K(\sqrt[n]{K^\times})$ 是 K 的极大指数 n 阿贝尔扩张, 则

$$K^\times / \mathbf{N}_{L/K} L^\times \cong \text{Hom}(G(L/K), \mu_n) \cong K^\times / K^{\times n}.$$

而根据 K^\times 的结构, 它是有限的, 从而 L/K 有限. 由于 $K^\times / \mathbf{N}_{L/K} L^\times \cong G(L/K)$ 指数 n , 因此 $K^{\times n} \subseteq \mathbf{N}_{L/K} L^\times$. 比较指数大小可知二者一致. \square

§3.2.2 阿贝尔扩域

定义 3.28 (导子)

设 L/K 是有限阿贝尔扩张, n 为最小的满足 $U_K^{(n)} \subseteq \mathbf{N}_{L/K} L^\times$ 的正整数. 称 $f_{L/K} = \mathfrak{p}_K^n$ 为 L/K 的导子.



命题 3.29

有限阿贝尔扩张 L/K 非分歧当且仅当 $f_{L/K} = 1$.



证明 如果 L/K 非分歧, 则 $U_K = \mathbf{N}_{L/K} U_L, f = 1$. 如果 $f = 1$, 则 $U_K \subseteq \mathbf{N}_{L/K} U_L, \pi_K^n \in \mathbf{N}_{L/K} L^\times$, 其中 $n = (K^\times : \mathbf{N}_{L/K} L^\times)$. 设 M/K 是 n 次非分歧扩张, 则 $\mathbf{N}_{M/K} M^\times = \pi_K^{n\mathbb{Z}} \times U_K \subseteq \mathbf{N}_{L/K} L^\times$, 因此 $M \supseteq L, L/K$ 非分歧. \square

任何 K^\times 的有限指标开子群都包含某个有限指标开子群 $\pi^{f\mathbb{Z}} \times U_K^{(n)}$. 因此每个有限阿贝尔扩张 L/K 都包含在某个 $\pi^{f\mathbb{Z}} \times U_K^{(n)}$ 对应的类域. 换言之, 这样的类域对于研究 K 的阿贝尔扩张是至关重要的. 现在我们考虑 \mathbb{Q}_p 的情形.

命题 3.30

$\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ 的范数群为 $p^{\mathbb{Z}} \times U_{\mathbb{Q}_p}^\times$.



证明 设 $K = \mathbb{Q}_p, L = \mathbb{Q}_p(\mu_{p^n})$. 由于 $\zeta = \zeta_{p^n}$ 的极小多项式为 $\Phi(x) = x^{p^{n-1}(p-1)} + \dots + x^{p^{n-1}} + 1$, 因此

$$\mathbf{N}_{L/K}(1 - \zeta) = \prod_{\sigma} (1 - \sigma\zeta) = \Phi(1) = p.$$

如果 v_L 延拓 v_K , 则 $v_L(\zeta) = \frac{1}{p^{n-1}(p-1)} v_K(p) = \frac{1}{p^{n-1}(p-1)}, p\mathcal{O}_L = (1 - \zeta)^{p^{n-1}(p-1)}, p$ 完全分歧. 考虑

$$\exp : \mathfrak{p}_K^\nu \rightarrow U_K^{(\nu)},$$

其中 $\nu = v_p(2p) = 1$ 或 2 . 由于

$$\begin{aligned} \mathfrak{p}_K^\nu &\longrightarrow \mathfrak{p}_K^{\nu+s-1} \\ a &\longmapsto p^{s-1}(p-1)a \end{aligned}$$

是一个同构, 它诱导了 $(U_K^{(1)})^{p^{n-1}(p-1)} = U_K^{(n)}, p \geq 3$ 和 $(U_K^{(2)})^{2^{n-2}} = U_K^{(n)}, p = 2$. 因此, $p \geq 3$ 时 $U_K^{(n)} \subseteq \mathbf{N}_{L/K}L^\times; p = 2$ 时

$$\begin{aligned} U_K^{(2)} &= U_K^{(3)} \cup 5U_K^{(3)} = (U_K^{(2)})^2 \cup 5(U_K^{(2)})^2, \\ U_K^{(n)} &= (U_K^{(2)})^{2^{n-1}} \cup 5^{2^{n-2}}(U_K^{(2)})^{2^{n-1}}. \end{aligned}$$

而 $5^{2^{n-2}} = \mathbf{N}_{L/K}(2+i)$, 因此 $U_K^{(n)} \subseteq \mathbf{N}_{L/K}L^\times$. 从而 $p^{\mathbb{Z}} \times U_K^{(n)} \subseteq \mathbf{N}_{L/K}L^\times$. 又因为二者在 K^\times 中的指标相同, 因此二者相等. \square

推论 3.31

\mathbb{Q}_p 的任意有限阿贝尔扩张都包含在某个 $\mathbb{Q}_p(\mu_n)$ 中. 特别地 $\mathbb{Q}_p^{\text{ab}} = \mathbb{Q}_p(\mu_\infty)$.



证明 设 $\zeta = \zeta_n, p \nmid n, \Phi(X)$ 为其极小多项式, $L = \mathbb{Q}_p(\zeta_n)$. 由于 $\bar{\Phi} \mid X^n - 1$ 可分, 由亨泽尔引理它不可约, 从而 $\bar{\Phi}(x)$ 是 $\bar{\zeta} \equiv \zeta \pmod{\mathfrak{p}_L}$ 在 \mathbb{F}_p 上的极小多项式, $[L : \mathbb{Q}_p] = \deg \Phi = \deg \bar{\Phi} = f, L/\mathbb{Q}_p$ 非分歧, $X^n - 1$ 在剩余域 κ_L 上完全分解为一次多项式乘积, 从而 $\kappa_L = \mathbb{F}_{p^f}$ 由 μ_n 生成, 即 $n \mid p^f - 1$. 因此 $\mathbb{Q}_p(\mu_{p^f-1})/\mathbb{Q}_p$ 是 f 次非分歧扩张.

对于一般的阿贝尔扩张 M , 设 $p^{f\mathbb{Z}} \times U_{\mathbb{Q}_p}^{(n)} \subseteq \mathbf{N}_{M/K}M^\times$, 则 M 包含在

$$p^{f\mathbb{Z}} \times U_{\mathbb{Q}_p}^{(n)} = (p^{f\mathbb{Z}} \times U_{\mathbb{Q}_p}) \cap (p^{\mathbb{Z}} \times U_{\mathbb{Q}_p}^{(n)})$$

对应的类域 $L\mathbb{Q}_p(\mu_{p^n}) = \mathbb{Q}_p(\mu_{(p^f-1)p^n})$ 中. \square

定理 3.32 (克罗内克-韦伯)

\mathbb{Q} 的任意有限阿贝尔扩张都包含在某个 $\mathbb{Q}(\mu_n)$ 中. 特别地 $\mathbb{Q}^{\text{ab}} = \mathbb{Q}(\mu_\infty)$.



证明 设 L/\mathbb{Q} 是阿贝尔扩张, S 包含所有在 L 中分歧的素数, $\mathfrak{p} \mid p$, 则 $L_{\mathfrak{p}}/\mathbb{Q}_p$ 是阿贝尔扩张, 从而 $L_{\mathfrak{p}} \subseteq \mathbb{Q}_p(\mu_{n_p})$. 设 $e_p = v_p(n_p)$,

$$n = \prod_{p \in S} p^{e_p},$$

$M = L(\mu_n)$, 则 M/\mathbb{Q} 是阿贝尔扩张且分歧的有限素位均包含在 S 中. 设 $\mathfrak{P} \mid \mathfrak{p}$,

$$M_{\mathfrak{P}} = L_{\mathfrak{p}}(\mu_n) = \mathbb{Q}_p(\mu_{p^{e_p}n'}) = \mathbb{Q}_p(\mu_{p^{e_p}})\mathbb{Q}_p(\mu_{n'}), p \nmid n',$$

由于 $\mathbb{Q}_p(\mu_{n'})$ 是 $M_{\mathfrak{P}}/\mathbb{Q}_p$ 的极大非分歧子扩张, 其惯性群

$$I_{\mathfrak{p}} = G(\mathbb{Q}_p(\mu_{p^{e_p}})/\mathbb{Q}_p)$$

大小为 $\varphi(p^{e_p})$. 设 $I \subseteq G(M/\mathbb{Q})$ 由所有惯性群 $I_{\mathfrak{p}}, p \in S$ 生成, 则 I 的固定域非分歧, 它只能是 \mathbb{Q} . 由此

$$\#I \leq \prod_{\mathfrak{p}} \#I_{\mathfrak{p}} = \prod_{\mathfrak{p}} \varphi(p^{e_p}) = \varphi(n) = [\mathbb{Q}(\mu_n) : \mathbb{Q}],$$

$[M : \mathbb{Q}] = [\mathbb{Q}(\mu_n) : \mathbb{Q}]$, 即 $M = \mathbb{Q}(\mu_n)$. \square

§3.2.3 卢宾-泰特形式群

对于一般的局部域, 我们需要利用卢宾-泰特形式群来描述其阿贝尔扩域.

定义 3.33 (形式群)

环 R 上的形式群指的是满足如下条件的形式幂级数 $\mathcal{F}(X, Y) \in R[[X, Y]]^a$

- (1) $\mathcal{F}(X, Y) \equiv X + Y \pmod{\deg 2}$;
- (2) $\mathcal{F}(X, Y) = \mathcal{F}(Y, X)$;
- (3) $\mathcal{F}(X, \mathcal{F}(Y, Z)) = \mathcal{F}(\mathcal{F}(X, Y), Z)$.

我们记 $X +_{\mathcal{F}} Y := \mathcal{F}(X, Y)$.

^a高维的形式群也可以类似地定义.



练习 3.2.1 (1) 验证 $\mathbb{G}_a(X, Y) = X + Y$ 是形式群, 称为形式加法群.

(2) 验证 $\mathbb{G}_m(X, Y) = X + Y + XY$ 是形式群, 称为形式乘法群.

(3) 设 $f(X) = a_1X + a_2X^2 + \cdots \in R[[X]]$, $a_1 \in R^\times$, 则存在 $f^{-1}(X) \in R[[X]]$ 使得 $f(f^{-1}(X)) = f^{-1}(f(X)) = X$. 此时 $\mathcal{F}(X, Y) = f^{-1}(f(X) + f(Y))$ 是形式群, f 称为 \mathcal{F} 的对数.

设 \mathcal{F}, \mathcal{G} 是形式群. 如果 $f \in XR[[X]]$ 满足

$$f(\mathcal{F}(X, Y)) = \mathcal{G}(f(X), f(Y)),$$

称之为形式群的同态 $f: \mathcal{F} \rightarrow \mathcal{G}$. 如果 $f \in R[[X]]^\times$, 即存在 $f^{-1}: \mathcal{G} \rightarrow \mathcal{F}$, 称之为同构. 容易验证 \mathcal{F} 的自同态全体在加法和复合意义下构成环 $\text{End}_R(\mathcal{F})$.

练习 3.2.2 设 R 是 \mathbb{Q} 代数. 对于任意 R 上形式群 \mathcal{F} , 存在唯一的形式群同构 $\log_{\mathcal{F}}: \mathcal{F} \xrightarrow{\sim} \mathbb{G}_a$, 使得 $\log_{\mathcal{F}}(X) \equiv X \pmod{\deg 2}$, 称之为 \mathcal{F} 的对数.

练习 3.2.3 $\log_{\mathbb{G}_m} = \log(1 + X) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{X^n}{n}$.

定义 3.34 (形式模)

设 \mathcal{F} 是 R 上的形式群. 如果环同态

$$\begin{aligned} R &\longrightarrow \text{End}_R(\mathcal{F}) \\ a &\longmapsto [a]_{\mathcal{F}}(X) \end{aligned}$$

满足 $[a]_{\mathcal{F}}(X) \equiv aX \pmod{\deg 2}$, 称之为形式 R 模, 或简称 \mathcal{F} 为形式 R 模. 自然地, 形式模之间的同态为满足 $f([a]_{\mathcal{F}}(X)) = [a]_{\mathcal{G}}(f(X))$ 的形式群同态 $f: \mathcal{F} \rightarrow \mathcal{G}$.



设 K 是一个局部环, π 为其素元, $q = \#k$.

定义 3.35 (卢宾-泰特级数)

如果 $e(X) \in \mathcal{O}_K[[X]]$ 满足

$$e(X) \equiv \pi X \pmod{\deg 2} \quad e(X) \equiv X^q \pmod{\pi},$$

称之为关于 π 的卢宾-泰特级数.



定理 3.36

(1) 对于任意卢宾-泰特级数 $e(X)$, 存在唯一的形式 \mathcal{O}_K 模 \mathcal{F} 使得

$$e \in \text{End}_{\mathcal{O}_K}(\mathcal{F}), \quad [\pi]_{\mathcal{F}}(X) = e(X),$$

称之为卢宾-泰特形式群.

(2) 如果 $e'(X)$ 也是关于 π 的卢宾-泰特级数, 则存在 $[a]_{\mathcal{F}, \mathcal{F}'}(X) \in \mathcal{O}_K[[X]]$ 使得

$$[a]_{\mathcal{F}, \mathcal{F}'} : \mathcal{F} \rightarrow \mathcal{F}'$$

是形式 \mathcal{O}_K 模同态. 如果 a 是一个单位, 它是形式模同构.



例题 3.11 设 $K = \mathbb{Q}_p$, $e(X) = (1 + X)^p - 1$, 则

$$\mathbb{Z}_p \longrightarrow \text{End}_{\mathbb{Z}_p}(\mathbb{G}_m)$$

$$a \longmapsto [a]_{\mathbb{G}_m}(X) = (1 + X)^a - 1$$

使得 \mathbb{G}_m 成为对应的形式 \mathbb{Z}_p 模.

命题 3.37

设 e, e' 分别是关于素元 π, π' 的卢宾-泰特级数, φ 是弗罗贝尼乌斯的一个提升, $\check{K} = \widehat{K}$. 如果 $a_i \in \mathcal{O}_{\check{K}}$ 满足 $\pi a_i = \pi' \varphi(a_i)$, $L(X_1, \dots, X_n) = \sum_{i=1}^n a_i X_i$, 则存在唯一的幂级数

$$\mathcal{F}(X_1, \dots, X_n) \in \mathcal{O}_{\check{K}}[[X_1, \dots, X_n]]$$

满足

$$\mathcal{F} \equiv L \pmod{\deg 2}, \quad e \circ \mathcal{F} = \mathcal{F}^\varphi \circ e'.$$



该命题可归纳地解出 \mathcal{F} 的每一个齐次项, 这里不做详解. 当 $\pi = \pi', a_i \in \mathcal{O}_K$ 时, \mathcal{F} 还是 \mathcal{O}_K 系数的. 由此可得前述定理, 且同一个 π 对应的卢宾-泰特形式群是同构的,

如果 R 是一个完备赋值环, \mathfrak{p} 是其极大理想, 则

$$x +_{\mathcal{F}} y := \mathcal{F}(x, y)$$

定义了 \mathfrak{p} 上一个交换群的结构. 如果 \mathcal{F} 还是一个形式 R 模, 则 \mathfrak{p} 成为 R 模.

设 \bar{K} 为局部域 K 的代数闭包, $\bar{\mathfrak{p}}$ 为其极大理想, π 为 K 的一个素元, \mathcal{LT} 为其关联的一个卢宾-泰特形式群, 它在同构下是唯一的. 定义

$$\mathcal{LT}[\pi^n] = \{\lambda \in \bar{\mathfrak{p}} \mid [\pi^n]_{\mathcal{LT}}(\lambda) = 0\} = \ker[\pi^n]_{\mathcal{LT}}$$

为其 π^n 等分点群. 易知它是一个 $\mathcal{O}_K/\pi^n \mathcal{O}_K$ 模.

命题 3.38

$\mathcal{LT}[\pi^n]$ 是秩为 1 的自由 $\mathcal{O}_K/\pi^n \mathcal{O}_K$ 模. 因此 $[\]_{\mathcal{F}}$ 定义了同构

$$\mathcal{O}_K/\pi^n \mathcal{O}_K \xrightarrow{\sim} \text{End}_{\mathcal{O}_K}(\mathcal{LT}[\pi^n]), \quad U_K/U_K^{(n)} \xrightarrow{\sim} \text{Aut}_{\mathcal{O}_K}(\mathcal{LT}[\pi^n]).$$



证明 不妨设 $e(X) = X^q + \pi X = [\pi]_{\mathcal{F}}(X)$, 则 $\mathcal{LT}[\pi^n]$ 是 $e^n(X) = 0$ 的根, 归纳可知它是可分多项式. 设 $\lambda_n \in \mathcal{LT}[\pi^n] - \mathcal{LT}[\pi^{n-1}]$, 则

$$\mathcal{O}_K \rightarrow \mathcal{LT}[\pi^n], \quad a \mapsto [a]_{\mathcal{F}}(\lambda_n)$$

诱导了 \mathcal{O}_K 模同构 $\mathcal{O}_K/\pi^n \mathcal{O}_K \xrightarrow{\sim} \mathcal{LT}[\pi^n]$. □

设 $L_n = K(\mathcal{LT}[\pi^n])$. 由于不同的卢宾-泰特形式群之间是同构的, $f: \mathcal{F} \rightarrow \mathcal{G}$, 因此 $\mathcal{G}[\pi^n] = f(\mathcal{F}[\pi^n])$, $K(\mathcal{G}[\pi^n]) \subseteq K(\mathcal{F}[\pi^n])$, L_n 不依赖于 \mathcal{LT} 的选取.

例题 3.12 如果 $K = \mathbb{Q}_p$, $e(X) = (1 + X)^p - 1$, 则

$$\mathcal{LT}[\pi^n] = \{\zeta - 1 \mid \zeta \in \mu_{p^n}\},$$

于是 $L_n = \mathbb{Q}_p(\mu_{p^n})$.

定理 3.39

L_n/K 是完全分歧的 $q^{n-1}(q-1)$ 次阿贝尔扩张, 伽罗瓦群为

$$G(L_n/K) \cong \text{Aut}_{\mathcal{O}_K}(\mathcal{LT}[\pi^n]) \cong U_K/U_K^{(n)},$$

其中

$$\sigma \mapsto u \bmod U_K^{(n)}, \quad \lambda^\sigma = [u]_F(\lambda), \lambda \in \mathcal{LT}[\pi^n].$$

如果 $\lambda_n \in \mathcal{LT}[\pi^n] - \mathcal{LT}[\pi^{n-1}]$, 则 $L_n = K(\lambda_n)$ 是 L_n 的素元, 且

$$\phi_n(X) = \frac{e^n(X)}{e^{n-1}(X)} = X^{q^{n-1}(q-1)} + \cdots + \pi \in \mathcal{O}_X[X]$$

是它的极小多项式, $\mathbf{N}_{L_n/K}(-\lambda_n) = \pi$.



证明 如果

$$e(X) = X^q + \pi(a_{q-1}X^{q-1} + \cdots + a_2X^2) + \pi X,$$

则

$$\phi_n(X) = e^{n-1}(X)^{q-1} + \pi(a_{q-1}X^{q-2} + \cdots + a_2X) + \pi$$

是艾森斯坦多项式, 从而是 λ_n 的极小多项式. 于是 λ_n 是完全分歧扩张 $K(\lambda_n)/K$ 的素元. 任一 $\sigma \in G(L_n/K)$ 诱导了 $\mathcal{LT}[\pi^n]$ 的自同构, 从而

$$G(L_n/K) \rightarrow \text{Aut}_{\mathcal{O}_K}(\mathcal{LT}[\pi^n]) \cong U_K/U_K^{(n)}.$$

由于 L_n 由 $\mathcal{LT}[\pi^n]$ 生成, 它是单的. 而

$$\#G(L_n/K) \geq [K(\lambda_n) : K] = q^{n-1}(q-1) = \#U_K/U_K^{(n)},$$

因此它是同构. □

定理 3.40

设 $a = u\pi^{v_K(a)} \in K^\times$, $u \in U_K$, 则

$$(a, L_n/K)\lambda = [u^{-1}]_{\mathcal{LT}}(\lambda), \quad \lambda \in \mathcal{LT}[\pi^n].$$



证明 设 $\sigma \in G(L_n/K)$ 对应 $u \in U_K$, $\tilde{\sigma} \in \text{Frob}(\tilde{L}_n/K)$ 是 σ 的提升且满足 $d_K(\tilde{\sigma}) = 1$. 我们将 $\tilde{\sigma}$ 视为 $\check{L}_n = L_n\check{K}$ 的自同构. 设 Σ 是 $\tilde{\sigma}$ 的固定域, 则 $f_{\Sigma/K} = d_K(\tilde{\sigma}) = 1$, Σ/K 完全分歧. 由于 $\Sigma \cap \check{K} = K$, $\tilde{\Sigma} = \Sigma\check{K} = \tilde{L}_n$, 因此 $[\Sigma : K] = [\tilde{L}_n : \check{K}] = [L_n : K] = q^{n-1}(q-1)$.

设 e, e' 分别为对应 π, π' 的卢宾-泰特级数, $\pi = u\pi'$, $\mathcal{F}, \mathcal{F}'$ 为 e, e' 对应的卢宾-泰特形式群. 则存在 $\theta = \varepsilon X + O(X^2) \in \mathcal{O}_{\check{K}}[[X]]$, 使得 $\varepsilon \in U_{\check{K}}$,

$$\theta^\varphi = \theta \circ [u]_{\mathcal{F}'}, \quad \theta^\varphi \circ e' = e \circ \theta, \quad \varphi = \varphi_K.$$

设 $\lambda_n \in \mathcal{F}[\pi^n] - \mathcal{F}[\pi^{n-1}]$, $\pi_\Sigma = \theta(\lambda_n)$. 则

$$\pi_{\tilde{\Sigma}} = \theta^\varphi(\lambda_n^\sigma) = \theta^\varphi([u^{-1}]_{\mathcal{F}}(\lambda_n)) = \theta(\lambda_n) = \pi_\Sigma.$$

由于 $i = n$ 时, $e^{i^i}(\theta(\lambda_n)) = \theta^{\varphi^i}(e^i(\lambda_n)) = 0$, $i = n - 1$ 时, 它非零. 因此 $\pi_\Sigma \in \mathcal{F}'[\pi^n] - \mathcal{F}'[\pi^{n-1}]$, $\Sigma = K(\pi_\Sigma)$, $\mathbf{N}_{\Sigma/K}(-\pi_\Sigma) = \pi' = u\pi$,

$$r_{L_n/K}(\sigma) = \mathbf{N}_{\Sigma/K}(-\pi_\Sigma) = \pi' \equiv u \pmod{\mathbf{N}_{L_n/K}L_n^\times},$$

因此

$$(a, L_n/K) = (\pi^{v_K(a)}, L_n/K)(u, L_n/K) = (u, L_n/K) = \sigma.$$

□

例题 3.13 当 $K = \mathbb{Q}$, $\mathcal{LT} = \mathbb{G}_m$ 时, $a = up^{v_p(a)} \in \mathbb{Q}_p^\times$, $u \in \mathbb{Z}_p^\times$, $\lambda = \zeta - 1$, 其中 ζ 是本原 p^n 次单位根, 则

$$(a, \mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p)\zeta = \zeta^{u^{-1}}.$$

定理 3.41

L_n/K 的范数群为 $(\pi) \times U_K^{(n)}$. 因此, $K^{\text{ab}} = \tilde{K}(\mathcal{LT}[\pi^\infty])$ 为 K 的极大阿贝尔扩张.



证明 由于 $a = u\pi^{v_K(a)}$ 时, $a \in \mathbf{N}_{L_n/K}L_n^\times$ 当且仅当 $[u^{-1}]_{\mathcal{LT}} = \text{id}_{\mathcal{LT}[\pi^n]}$, 即 $u \in U_K^{(n)}$. 设 L/K 是有限阿贝尔扩张, 则 $\pi^{f\mathbb{Z}} \times U_K^{(n)} \in \mathbf{N}_{L/K}L^\times$. 和分圆域情形类似, 此时 $\pi^{f\mathbb{Z}}$ 对应的是非分歧扩张, 因此 $L \subseteq \tilde{K}(\mathcal{LT}[\pi^\infty])$. □

对于 K^\times 的高阶单位群, 它在范剩余符号下的像是 $G(L/K)$ 的高阶分歧群.

定理 3.42

设 L/K 是有限阿贝尔扩张, 范剩余符号

$$(\cdot, L/K) : K^\times \rightarrow G(L/K)$$

将 $U_K^{(n)}$ 映为 $G^n(L/K)$. 特别地, $\{G^t(L/K)\}_{t \geq -1}$ 仅在整数处有跳跃.



证明 见 [15, Chapter V, §6], 这里省略. □

§3.2.4 希尔伯特符号

我们称互反映射的逆

$$(\cdot, L/K) : K^\times \rightarrow G(L/K)^{\text{ab}}$$

为局部范数剩余符号. 对于 \mathbb{C}/\mathbb{R} 情形, $(a, \mathbb{C}/\mathbb{R}) = \text{sgn}(a) \in G(\mathbb{C}/\mathbb{R})$.

假设 $K \supseteq \mu_n$. 设 $L = K(\sqrt[n]{K^\times})$, 则 $\mathbf{N}_{L/K}L^\times = K^{\times n}$, 因此

$$G(L/K) \cong K^\times / K^{\times n}.$$

另一方面, 我们有自然同构

$$\text{Hom}(G(L/K), \mu_n) \cong K^\times / K^{\times n}$$

$$\left(\sigma \mapsto \frac{(\sqrt[n]{a})^\sigma}{\sqrt[n]{a}} \right) \leftarrow a.$$

因此双线性映射

$$G(L/K) \times \text{Hom}(G(L/K), \mu_n) \longrightarrow \mu_n$$

$$(\sigma, \chi) \longmapsto \chi(\sigma)$$

诱导了

$$\left(\frac{\cdot}{\mathfrak{p}}\right) : K^\times / K^{\times n} \times K^\times / K^{\times n} \rightarrow \mu_n.$$

称之为 n 次希尔伯特符号.

由定义我们有:

命题 3.43

对于 $a, b \in K^\times$,

$$(a, K(\sqrt[n]{b})/K) \sqrt[n]{b} = \left(\frac{a, b}{\mathfrak{p}}\right) \sqrt[n]{b}.$$



一般的希尔伯特符号和我们在2.2.5节中接触的二次希尔伯特符号一样,也有着一系列易于计算的性质.

命题 3.44

- (1) $\left(\frac{aa', b}{\mathfrak{p}}\right) = \left(\frac{a, b}{\mathfrak{p}}\right) \left(\frac{a', b}{\mathfrak{p}}\right), \left(\frac{a, bb'}{\mathfrak{p}}\right) = \left(\frac{a, b}{\mathfrak{p}}\right) \left(\frac{a, b'}{\mathfrak{p}}\right);$
- (2) $\left(\frac{a, b}{\mathfrak{p}}\right) = 1 \iff a \in \mathbf{N}_{K(\sqrt[n]{b})/K} K(\sqrt[n]{b})^\times;$
- (3) $\left(\frac{a, b}{\mathfrak{p}}\right) = 1, \forall b \implies a \in K^{\times n};$
- (4) $\left(\frac{a, b}{\mathfrak{p}}\right) = \left(\frac{b, a}{\mathfrak{p}}\right)^{-1};$
- (5) $\left(\frac{a, -a}{\mathfrak{p}}\right) = \left(\frac{a, 1-a}{\mathfrak{p}}\right) = 1.$



证明 (1-3) 由定义和互反映射的性质可得. 设 $b \in K^\times, x \in K$ 使得 $x^n - b \neq 0$, 设 d 是 n 的最大的因子使得 $\sqrt[n]{b} \in K$. 设 $\beta^n = b$, 则 $K(\beta)/K$ 是 $m = n/d$ 次循环扩张且 $i \equiv j \pmod{d}$ 时, $x - \zeta^i \beta$ 是 $x - \zeta^j \beta$ 的共轭元, 其中 ζ 是一个 n 次本原单位根. 于是

$$x^n - b = \prod_{i=0}^{d-1} \mathbf{N}_{K(\beta)/K}(x - \zeta^i \beta)$$

是 $K(\sqrt[n]{b})/K$ 的一个范数, 因此

$$\left(\frac{x^n - b, b}{\mathfrak{p}}\right) = 1.$$

由此可得 (5). 最后

$$1 = \left(\frac{ab, -ab}{\mathfrak{p}}\right) = \left(\frac{a, b}{\mathfrak{p}}\right) \left(\frac{a, -a}{\mathfrak{p}}\right) \left(\frac{b, a}{\mathfrak{p}}\right) \left(\frac{b, -b}{\mathfrak{p}}\right) = \left(\frac{a, b}{\mathfrak{p}}\right) \left(\frac{b, a}{\mathfrak{p}}\right)$$

得到 (4). □

练习 3.2.4 对于 $\mathbb{C}/\mathbb{R}, n = 2$, 证明 $\left(\frac{a, b}{\infty}\right) = (-1)^{\frac{\text{sgn}a-1}{2} \cdot \frac{\text{sgn}b-1}{2}}$.

设 $K(\neq \mathbb{R}, \mathbb{C})$ 的剩余特征为 p , 假设 $p \nmid n$. 我们来计算该情形即所谓的温希尔伯特符号. 由于 K 的单位根群为 μ_{q-1} , 因此 $n \mid q - 1$.

引理 3.45

设 $p \nmid n, x \in K^\times$, 则 $K(\sqrt[n]{x})/K$ 非分歧当且仅当 $x \in U_K K^{\times n}$.



证明 设 $x = uy^n, u \in U_K, y \in K^\times$, 则 $K(\sqrt[n]{x}) = K(\sqrt[n]{u})$. 设 κ' 为 $X^n - u$ 在 κ 上的分裂域, K'/K 是非分歧扩张且 κ' 是 K' 的剩余域. 由亨泽尔引理, $X^n - u$ 在 K' 上完全分解, 因此 $K(\sqrt[n]{u}) \subseteq K'$ 非分歧. 反之, 若 $L = K(\sqrt[n]{x})$ 非分歧, 令 $x = u\pi^r, u \in U_K, \pi$ 是素元, 则 $v_L(\sqrt[n]{u\pi^r}) = r/n \in \mathbb{Z}$, 从而 $n \mid r$. \square

由于 $U_K = \mu_{q-1} \times U_K^{(1)}$, 因此任一 $u \in U_K$ 可分解为

$$u = \omega(u)\langle u \rangle,$$

其中 $\omega(u) \in \mu_{q-1}, \langle u \rangle \in U_K^{(1)}$.

命题 3.46

设 $p \nmid n, a, b \in K^\times$, 则

$$\left(\frac{a, b}{\mathfrak{p}}\right) = \omega\left(\left(-1\right)^{\alpha\beta} \frac{b^\alpha}{a^\beta}\right)^{(q-1)/n},$$

其中 $\alpha = v_K(a), \beta = v_K(b)$.



证明 由于右侧是双线性的, 因此我们只需证明 $a = \pi, b = -\pi u, u \in U_K$ 的情形. 而 $\left(\frac{\pi, -\pi}{\mathfrak{p}}\right) = 1$, 因此只需证 $a = \pi, b = u$ 的情形. 设 $y = \sqrt[n]{u}, K' = K(y)$, 则 $K(y)/K$ 非分歧, 因此 $(\pi, K(y)/K)$ 是弗罗贝尼乌斯映射 $\varphi = \varphi_{K(y)/K}$, 于是

$$\left(\frac{\pi, u}{\mathfrak{p}}\right) = \frac{\varphi y}{y} \equiv y^{q-1} \equiv u^{(q-1)/n} \equiv \omega(u)^{(q-1)/n} \pmod{\mathfrak{p}}.$$

由于 $\mu_n \subseteq \mu_{q-1} = \kappa^\times$, 因此两侧相等. \square

我们可以看出 $\left(\frac{\pi, u}{\mathfrak{p}}\right)$ 不依赖于 π 的选取, 定义勒让德符号(或 n 次剩余符号)

$$\left(\frac{u}{\mathfrak{p}}\right) := \left(\frac{\pi, u}{\mathfrak{p}}\right) = \omega(u)^{(q-1)/n}.$$

练习 3.2.5 $\left(\frac{u}{\mathfrak{p}}\right) = 1$ 当且仅当 $u \pmod{\mathfrak{p}}$ 是一个 n 次方.

我们来证明本节定义的希尔伯特符号和 2.2.5 节定义的一致. 我们只需证明 $K = \mathbb{Q}_2, n = 2$ 时,

$$\left(\frac{2, a}{2}\right) = (-1)^{(a^2-1)/8}, \quad \left(\frac{a, b}{2}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}, \quad a, b \in U_{\mathbb{Q}_2}.$$

由于 $U_{\mathbb{Q}_2}/U_{\mathbb{Q}_2}^2 = \langle -1, 5 \rangle$, 我们只需要考虑 $a, b = -1$ 或 5 . $\left(\frac{-1, x}{2}\right) = 1$ 当且仅当 $x \in \mathbf{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}$, 因此 $\left(\frac{-1, 2}{2}\right) = \left(\frac{-1, 5}{2}\right) = 1$. 但是 -1 不是个平方, 因此 $\left(\frac{-1, -1}{2}\right) = -1$. 由于 $\left(\frac{2, 2}{2}\right) = \left(\frac{2, -1}{2}\right) = 1$, 而 2 不是个平方, 这迫使 $\left(\frac{2, 5}{2}\right) = -1$.

练习 3.2.6 证明 $U_{\mathbb{Q}_2}/U_{\mathbb{Q}_2}^2 = \langle -1, 5 \rangle$.

可以看出, $p \mid n$ 的情形(野希尔伯特符号)相对而言更复杂. 具体的结果由 Brückner 于 1964 年给出, 见 [15, Theorem 5.3.7].

练习 3.2.7 了解和学习整体函数域情形的局部类域论.

§3.3 整体类域论

整体类域论中的 G 模 A 是所谓的伊代尔类群.

§3.3.1 阿代尔和伊代尔

定义 3.47 (阿代尔环)

称

$$\mathbb{A}_K := \prod'_v K_v$$

为数域 K 的阿代尔环. 这里的 $'$ 表示相对于 \mathcal{O}_v 的限制直积, 即除有限多个素位外, $\alpha_v \in \mathcal{O}_v^a$. 它的拓扑定义为相应的乘积拓扑的限制拓扑. 其中的元素被称为 K 的阿代尔 (adèle).

^a一般地, 给出一族局部紧群 (G_λ) , 对除有限多个 λ 外给了一个紧开子群 U_λ , 则其直积中满足除有限多个 λ 外, $x_\lambda \in U_\lambda$ 的元素称之为限制直积.



定义 3.48 (伊代尔群)

称阿代尔环的乘法群

$$\mathbb{I}_K = \mathbb{A}_K^\times = \prod'_v K_v^\times$$

为 K 的伊代尔群, 其中的元素被称为伊代尔 (idèle). 容易看出, 伊代尔群是 K_v^\times 相对于 \mathcal{O}_v^\times 的限制直积.



嵌入 $K \hookrightarrow K_v$ 诱导了对角嵌入

$$K^\times \hookrightarrow \mathbb{I}_K.$$

我们称 K^\times 的像为主伊代尔.

定义 3.49 (伊代尔类群)

商群 $C_K = \mathbb{I}_K / K^\times$ 被称为 K 的伊代尔类群.



对于 $v \mid \infty$, 定义

$$\mathcal{O}_v = \begin{cases} \mathbb{R}_{\geq 0}, & v \text{ 是实素位;} \\ \mathbb{C}, & v \text{ 是复素位.} \end{cases}$$

设 S 是 K 的素位的一个有限集合, 我们记 \mathbb{I}_K^S 为 S 以外的素位处都属于 \mathcal{O}_v^\times 的伊代尔构成的子群. 显然

$$\mathbb{I}_K = \bigcup_S \mathbb{I}_K^S.$$

记

$$K^S = K^\times \cap \mathbb{I}_K^S.$$

如果 $S_\infty = \{v \mid \infty\}$ 包含所有无穷素位, 则 $K^{S_\infty} = \mathcal{O}_K^\times$.

考虑群同态

$$\begin{aligned} (\cdot) : \mathbb{I}_K &\longrightarrow \mathcal{I}_K \\ \alpha &\longmapsto (\alpha) = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}. \end{aligned}$$

它的核是

$$\mathbb{I}_K^{S_\infty} = \prod_{\mathfrak{p}|\infty} \mathcal{O}_{\mathfrak{p}}^\times \times \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^\times.$$

这诱导了群同态

$$C_K \rightarrow \text{Cl}_K,$$

核为 $\mathbb{I}_K^{S_\infty} K^\times / K^\times$.

命题 3.50

K^\times 是 \mathbb{I}_K 的离散闭子群.



证明 只需证明 1 有一个不包含其它主伊代尔的开集即可. 取

$$U = \{\alpha \in \mathbb{I}_K \mid v \nmid \infty \text{ 时, } \alpha_v \in \mathcal{O}_v^\times; v \mid \infty \text{ 时, } |\alpha_v - 1|_v < 1.\}$$

如果 $1 \neq x \in U$ 是一个主伊代尔, 则

$$1 = \prod_v |x - 1|_v < \prod_{v \nmid \infty} |x - 1|_v \leq \prod_{v \nmid \infty} \max\{|x|_v, 1\} = 1,$$

矛盾.

由于 $(x, y) \mapsto xy^{-1}$ 是连续的, 存在 1 的一个开邻域 V 使得 $VV^{-1} \subseteq U$. 对于任意 $y \in \mathbb{I}_K$, 如果 yV 包含两个不同的主伊代尔 $x_1 = yv_1, x_2 = yv_2 \in K^\times$, 则 $x_1x_2^{-1} = v_1v_2^{-1} \in U$, 矛盾! 因此 yV 里只有至多一个主伊代尔, 因此 K^\times 是闭子群. \square

练习 3.3.1 (1) $\mathbb{A}_{\mathbb{Q}} = (\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}) \times \mathbb{R}$.

(2) $\mathbb{A}_{\mathbb{Q}}/\mathbb{Z}$ 是紧的, 连通的.

(3) $\mathbb{A}_{\mathbb{Q}}/\mathbb{Z}$ 任意唯一可除, 即对于任意 $y \in \mathbb{A}_{\mathbb{Q}}/\mathbb{Z}, n \in \mathbb{Z}$, 存在唯一的 $x \in \mathbb{Z}_{\mathbb{Q}}/\mathbb{Z}$ 使得 $nx = y$.

§3.3.2 域扩张中的伊代尔

设 L/K 是数域的有限扩张. 我们记

$$L_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}} = L \otimes_K K_{\mathfrak{p}}.$$

它是 $[L : K]$ 次 $K_{\mathfrak{p}}$ 代数. 自然的对角嵌入 $K_{\mathfrak{p}} \hookrightarrow L_{\mathfrak{p}}$ 诱导了 $\mathbb{A}_K \hookrightarrow \mathbb{A}_L$ 以及

$$\begin{aligned} \mathbb{I}_K &\longrightarrow \mathbb{I}_L \\ \alpha &\longmapsto \alpha', \end{aligned}$$

其中 $\alpha'_{\mathfrak{P}} = \alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}^\times \subseteq L_{\mathfrak{P}}^\times, \mathfrak{P} \mid \mathfrak{p}$.

设 $\sigma : L \xrightarrow{\sim} \sigma L$ 是一个同构, 则它同样诱导了同构 $\sigma : \mathbb{I}_L \rightarrow \mathbb{I}_{\sigma L}$. 对于 L 的任一素位 \mathfrak{P} , 设 $\alpha \in L_{\mathfrak{P}}$ 是 $\{\alpha_i \in L\}$ 在 $|\cdot|_{\mathfrak{P}}$ 下的极限, 令 $\sigma\alpha \in (\sigma L)_{\sigma\mathfrak{P}}$ 是 $\{\sigma\alpha_i \in \sigma L\}$ 在 $|\cdot|_{\sigma\mathfrak{P}}$ 下的极限, 则 $\sigma : L_{\mathfrak{P}} \xrightarrow{\sim} (\sigma L)_{\sigma\mathfrak{P}}$. 对于 $\alpha \in \mathbb{I}_L$, 我们有 $(\sigma\alpha)_{\sigma\mathfrak{P}} = \sigma\alpha_{\mathfrak{P}} \in (\sigma L)_{\sigma\mathfrak{P}}$. 如果 L/K 是伽罗瓦扩张, 则任一 $\sigma \in G = G(L/K)$ 诱导了同构 $\sigma : \mathbb{I}_L \rightarrow \mathbb{I}_L$, 因此 \mathbb{I}_L 是 G 模.

命题 3.51

如果 L/K 是有限伽罗瓦扩张, 则 $\mathbb{I}_L^G = \mathbb{I}_K$.



证明 对于 $\alpha \in \mathbb{I}_L, \sigma \in G$ 诱导了 $K_{\mathfrak{p}}$ 同构 $\sigma : L_{\mathfrak{p}} \rightarrow L_{\sigma\mathfrak{p}}, \mathfrak{p} | \mathfrak{p}$. 因此

$$(\sigma\alpha)_{\sigma\mathfrak{p}} = \sigma\alpha_{\mathfrak{p}} = \alpha_{\mathfrak{p}} = \alpha_{\sigma\mathfrak{p}},$$

即 $\sigma\alpha = \alpha, \alpha \in \mathbb{I}_L^G$. 反之, 若 $\alpha \in \mathbb{I}_L^G$, 则

$$(\sigma\alpha)_{\sigma\mathfrak{p}} = \sigma\alpha_{\mathfrak{p}} = \alpha_{\sigma\mathfrak{p}}.$$

如果 $\sigma \in G_{\mathfrak{p}} = G(L_{\mathfrak{p}}/K_{\mathfrak{p}})$, 则 $\sigma\mathfrak{p} = \mathfrak{p}, \sigma\alpha_{\mathfrak{p}} = \alpha_{\mathfrak{p}}, \alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}^{\times}$. 一般地, $\alpha_{\mathfrak{p}} = \sigma\alpha_{\mathfrak{p}} = \alpha_{\sigma\mathfrak{p}}$. 而 G 在 $\{\mathfrak{p} | \mathfrak{p}\}$ 上传递, 因此 $\alpha \in \mathbb{I}_K$. \square

任一 $\alpha_{\mathfrak{p}} \in L_{\mathfrak{p}}^{\times}$ 诱导了 $K_{\mathfrak{p}}$ 向量空间 $L_{\mathfrak{p}}$ 上的自同构

$$\begin{aligned} \alpha_{\mathfrak{p}} : L_{\mathfrak{p}} &\longrightarrow L_{\mathfrak{p}} \\ x &\longmapsto \alpha_{\mathfrak{p}}x, \end{aligned}$$

它的行列式记为 $\mathbf{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(\alpha_{\mathfrak{p}})$. 由此定义了群同态

$$\mathbf{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}} : L_{\mathfrak{p}}^{\times} \rightarrow K_{\mathfrak{p}}^{\times}$$

以及

$$\mathbf{N}_{L/K} : \mathbb{I}_L \rightarrow \mathbb{I}_K.$$

显然, $\alpha_{\mathfrak{p}} = (\alpha_{\mathfrak{p}})$ 诱导的同构是 $\alpha_{\mathfrak{p}} : L_{\mathfrak{p}} \rightarrow L_{\mathfrak{p}}$ 的直和, 因此

$$\mathbf{N}_{L/K}(\alpha)_{\mathfrak{p}} = \prod_{\mathfrak{p}|p} \mathbf{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(\alpha_{\mathfrak{p}}).$$

命题 3.52

- (1) 对于 $K \subseteq L \subseteq M, \mathbf{N}_{M/K} = \mathbf{N}_{L/K} \circ \mathbf{N}_{M/L}$.
- (2) 如果 M/K 是伽罗瓦扩张, L 是中间域, $G = G(M/K), H = G(M/L)$, 则对于 $x \in \mathbb{I}_L$, $\mathbf{N}_{L/K}(\alpha) = \prod_{\sigma \in G/H} \sigma\alpha$.
- (3) $\mathbf{N}_{L/K}(\alpha) = \alpha^{[L:K]}, \alpha \in \mathbb{I}_K$.
- (4) 主伊代尔 $x \in L^{\times}$ 的范数是 $\mathbf{N}_{L/K}(x)$ 对应的主伊代尔.



证明 类似域扩张情形. \square

由于 $\mathbf{N}_{L/K} : \mathbb{I}_L \rightarrow \mathbb{I}_K$ 将主伊代尔映为主伊代尔, 因此它诱导了 $\mathbf{N}_{L/K} : C_L \rightarrow C_K$.

现在我们考虑域扩张下伊代尔类群的关系.

命题 3.53

设 L/K 是有限扩张, 则 $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$ 诱导了嵌入 $C_K \rightarrow C_L$.



证明 我们只需证明 $\mathbb{I}_K \cap L^{\times} = K^{\times}$. 设 M 是 L/K 的伽罗瓦闭包, $G = G(M/K)$,

$$\mathbb{I}_K \cap L^{\times} \subseteq \mathbb{I}_K \cap M^{\times} = (\mathbb{I}_K \cap M^{\times})^G = \mathbb{I}_K \cap M^{\times G} = \mathbb{I}_K \cap K^{\times} = K^{\times}.$$

\square

命题 3.54

设 L/K 是有限伽罗瓦扩张, $G = G(L/K)$, 则 C_L 是自然的 G 模且 $C_L^G = C_K$.



证明 L^\times 是 \mathbb{I}_L 的 G 子模, 因此 C_L 是自然的商模. 我们有 G 模短正合列

$$1 \rightarrow L^\times \rightarrow \mathbb{I}_L \rightarrow C_L \rightarrow 1,$$

这诱导了长正合列

$$1 \rightarrow L^{\times G} \rightarrow \mathbb{I}_L^G \rightarrow C_L^G \rightarrow H^1(G, L^\times)$$

由命题 3.22 知 $H^1(G, L^\times) = 1$, 因此 $C_L^G = \mathbb{I}_L^G / L^{\times G} = \mathbb{I}_K / K^\times = C_K$. □

§3.3.3 整体域的埃尔布朗商

设 L/K 是数域的有限伽罗瓦扩张, $G = G(L/K)$. 设 $\mathfrak{p} \mid \mathfrak{p}$, $G_{\mathfrak{p}} = G(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \subseteq G$ 是其分解群. 我们有

$$L_{\mathfrak{p}} = \prod_{\sigma \in G/G_{\mathfrak{p}}} L_{\sigma\mathfrak{p}} = \prod_{\sigma \in G/G_{\mathfrak{p}}} \sigma(L_{\mathfrak{p}}),$$

因此

$$L_{\mathfrak{p}}^\times = \text{Ind}_G^{G_{\mathfrak{p}}} L_{\mathfrak{p}}^\times, \quad U_{L,\mathfrak{p}} = \text{Ind}_G^{G_{\mathfrak{p}}} U_{\mathfrak{p}}$$

是诱导模. 由诱导模性质知

$$H^i(G, L_{\mathfrak{p}}^\times) \cong H^i(G_{\mathfrak{p}}, L_{\mathfrak{p}}^\times), \quad H^i(G, U_{L,\mathfrak{p}}) = H^i(G_{\mathfrak{p}}, U_{\mathfrak{p}}).$$

命题 3.55

设 L/K 是数域循环扩张, S 包含 K 的所有在 L 中分歧的素位, 则对于 $i = 0, -1$,

$$H^i(G, \mathbb{I}_L^S) \cong \bigoplus_{\mathfrak{p} \in S} H^i(G_{\mathfrak{p}}, L_{\mathfrak{p}}^\times), \quad H^i(G, \mathbb{I}_L) \cong \bigoplus_{\mathfrak{p}} H^i(G_{\mathfrak{p}}, L_{\mathfrak{p}}^\times).$$

这里, 每个 \mathfrak{p} 之上选取一个 \mathfrak{p} .



证明 由于 $\mathbb{I}_L^S = (\bigoplus_{\mathfrak{p} \in S} L_{\mathfrak{p}}^\times) \oplus V$, $V = \prod_{\mathfrak{p} \notin S} U_{L,\mathfrak{p}}$, 因此我们有

$$H^i(G, \mathbb{I}_L^S) \cong \bigoplus_{\mathfrak{p} \in S} H^i(G, L_{\mathfrak{p}}^\times) \oplus H^i(G, V),$$

以及单射

$$H^i(G, V) \hookrightarrow \prod_{\mathfrak{p} \notin S} H^i(G, U_{L,\mathfrak{p}}).$$

对于 $\mathfrak{p} \notin S$, $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ 非分歧, 因此 $H^i(G, U_{L,\mathfrak{p}}) = H^i(G_{\mathfrak{p}}, U_{\mathfrak{p}}) = 1$. 由此我们得到第一个同构. 第二个由

$$H^i(G, \mathbb{I}_L) = \varinjlim_S H^i(G, \mathbb{I}_L^S) \cong \varinjlim_S \bigoplus_{\mathfrak{p} \in S} H^i(G_{\mathfrak{p}}, L_{\mathfrak{p}}^\times) = \bigoplus_{\mathfrak{p}} H^i(G_{\mathfrak{p}}, L_{\mathfrak{p}}^\times)$$

可得. □

注 对于 $G = G(\mathbb{C}/\mathbb{R})$, 我们有

$$H^{-1}(G, \mathbb{C}^\times) = 1, \quad \#H^0(G, \mathbb{C}^\times) = 2.$$

因此在无穷素位的相应上调也满足类域论公理.

练习 3.3.2 设 $i = 0, -1$.

(1) 对于任意多个 G 模 A_k , $H^i(G, \bigoplus_k A_k) = \prod_k H^i(G, A_k)$.

(2) 对于任意多个 G 模 A_k , $H^i(G, \prod_k A_k) \hookrightarrow \prod_k H^i(G, A_k)$ 是单射.

(3) 对于 G 模正向系 A_k , $H^i(G, \varinjlim_k A_k) = \varinjlim_k H^i(G, A_k)$.

根据希尔伯特 90, $H^{-1}(G_{\mathfrak{p}}, L_{\mathfrak{p}}^{\times}) = 1$, 因此 $H^{-1}(G, \mathbb{I}_L) = 1$. 换言之, 一个伊代尔是范当且仅当在每个局部如此.

设 $n_{\mathfrak{p}} = [L_{\mathfrak{p}} : K_{\mathfrak{p}}]$, 则由上述结论可知:

命题 3.56

设 L/K 是循环扩张, S 包含 K 的所有在 L 中分歧的素位, 则

$$H^{-1}(G, \mathbb{I}_L^S) = 1, \quad h(G, \mathbb{I}_L^S) = \prod_{\mathfrak{p} \in S} n_{\mathfrak{p}}.$$



命题 3.57

设 L/K 是 n 次循环扩张, S 包含 K 的所有在 L 中分歧的素位, 则

$$h(G, L^S) = \frac{1}{n} \prod_{\mathfrak{p} \in S} n_{\mathfrak{p}}.$$



证明 设 \bar{S} 是 L 中 S 之上的素位全体, $\{e_{\mathfrak{p}}\}$ 是 $V = \prod_{\mathfrak{p} \in \bar{S}} \mathbb{R}$ 的标准基, 则同态

$$\lambda : L^S \rightarrow V, \quad \lambda(a) = \sum_{\mathfrak{p} \in \bar{S}} \log |a|_{\mathfrak{p}} e_{\mathfrak{p}}$$

的核为 $\mu(L)$, 像为 $(s-1)$ 维格, $s = \#\bar{S}$. 考虑 G 在 V 上的作用 $\sigma e_{\mathfrak{p}} = e_{\sigma\mathfrak{p}}$, 则 λ 是 G 模同态. 因此 $e_0 = \sum_{\mathfrak{p}} e_{\mathfrak{p}}$ 和 $\lambda(L^S)$ 生成 G 不变的完全格 Γ . 由于作为 G 模, $\mathbb{Z}e_0 \cong \mathbb{Z}$, 我们有

$$0 \rightarrow \mathbb{Z}e_0 \rightarrow \Gamma \rightarrow \Gamma/\mathbb{Z}e_0 \rightarrow 0,$$

$\Gamma/\mathbb{Z}e_0 = \lambda(L^S)$, 因此

$$h(G, L^S) = h(G, \lambda(L^S)) = h(G, \mathbb{Z})^{-1} h(G, \Gamma) = \frac{1}{n} h(G, \Gamma).$$

我们断言, 存在子完全格 $\Gamma' \subseteq \Gamma$ 使得

$$\Gamma' = \sum \mathbb{Z}w_{\mathfrak{p}},$$

$\sigma w_{\mathfrak{p}} = w_{\sigma\mathfrak{p}}$. 设 $|\sum a_{\mathfrak{p}} e_{\mathfrak{p}}| = \max_{\mathfrak{p}} |a_{\mathfrak{p}}|$. 存在 $b > 0$ 使得对任意 $x \in V, \gamma \in \Gamma, |x - \gamma| < b$. 选取充分大的 $t \in \mathbb{R}$ 和 $\gamma \in \Gamma$, 使得 $y = te_{\mathfrak{p}_0} - \gamma$ 满足 $|y| < b$. 定义 $w_{\mathfrak{p}} = \sum_{\sigma\mathfrak{p}_0=\mathfrak{p}} \sigma\gamma$, 则 $\sigma w_{\mathfrak{p}} = w_{\sigma\mathfrak{p}}$. 我们来说明它们线性无关. 如果 $\sum c_{\mathfrak{p}} w_{\mathfrak{p}} = 0$ 系数不全为零, 不妨设 $|c_{\mathfrak{p}}| \leq 1$ 且存在 $c_{\mathfrak{p}} = 1$, 则

$$w_{\mathfrak{p}} = \sum_{\sigma\mathfrak{p}_0=\mathfrak{p}} \sigma\gamma = tn_{\mathfrak{p}}e_{\mathfrak{p}} - y_{\mathfrak{p}},$$

其中 $|y_{\mathfrak{p}}| \leq gb, g = \#G$. 因此

$$0 = \sum c_{\mathfrak{p}} w_{\mathfrak{p}} = t \sum c_{\mathfrak{p}} n_{\mathfrak{p}} e_{\mathfrak{p}} - z, \quad |z| \leq sgb.$$

而 t 充分大时这不可能成立, 因此 $w_{\mathfrak{p}}$ 线性无关.

现在

$$\Gamma' = \bigoplus_{\mathfrak{p}} \mathbb{Z}w_{\mathfrak{p}} = \bigoplus_{\mathfrak{p} \in S} \bigoplus_{\mathfrak{p}|\mathfrak{p}} \mathbb{Z}w_{\mathfrak{p}} = \bigoplus_{\mathfrak{p} \in S} \Gamma'_{\mathfrak{p}}.$$

而 $\Gamma'_p = \text{Ind}_G^{G_p} \mathbb{Z}w_{\mathfrak{p}_0}$ 是诱导模, Γ' 在 Γ 中有限指标, 从而

$$h(G, L^S) = \frac{1}{n} h(G, \Gamma') = \frac{1}{n} \prod_{\mathfrak{p} \in S} (G_p, \mathbb{Z}w_{\mathfrak{p}_0}) = \frac{1}{n} \prod_{\mathfrak{p}} n_{\mathfrak{p}}.$$

□

定理 3.58

设 L/K 是 n 次循环扩张, 则

$$h(G, C_L) = n.$$



证明 设 $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ 是 Cl_L 的一组代表元, S 为包含分歧、无穷素位以及 \mathfrak{a}_i 在 K 中分解的素因子的一个素位的有限集合, 则 $\mathbb{I}_L = \mathbb{I}_L^S L^\times$. 实际上, 对于任意 $\alpha \in \mathbb{I}_L$, 设 $(\alpha) = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}$ 为对应的分式理想. 设 $(\alpha) = \mathfrak{a}_i(a), a \in L^\times, \alpha' = \alpha a^{-1}$. 对于 $\mathfrak{p} \notin \overline{S}, v_{\mathfrak{p}}(\alpha') = 0, \alpha'_{\mathfrak{p}} \in U_{\mathfrak{p}}$, 因此 $\alpha' \in \mathbb{I}_L^S$, 从而 $\mathbb{I}_L = \mathbb{I}_L^S L^\times$. 由正合列

$$1 \rightarrow L^S \rightarrow \mathbb{I}_L^S \rightarrow \mathbb{I}_L^S L^\times / L^\times \rightarrow 1$$

可知 $h(G, C_L) = h(G, \mathbb{I}_L^S) / h(G, L^S) = n$.

□

推论 3.59

如果 L/K 是 $n = p^v$ 次循环扩张, 则有无穷多 K 的素位在 L 中不分裂.



证明 假设不分裂的素位集合 S 有限. 设 M/K 是 p 次子扩张. 对于任意 $\mathfrak{p} \notin S$, 相应的分解群 $G_{\mathfrak{p}} \neq G$. 因此 $G_{\mathfrak{p}} \subseteq G(L/M)$, 即所有 $\mathfrak{p} \notin S$ 在 M/K 中完全分裂.

对于任意 $\alpha \in \mathbb{I}_K$, 由逼近定理, 存在 $a \in K^\times$ 使得对任意 $\mathfrak{p} \in S, \alpha_{\mathfrak{p}} a^{-1}$ 包含在 $\mathbf{N}_{M_{\mathfrak{p}}/K_{\mathfrak{p}}} M_{\mathfrak{p}}^\times$ 的一个开子群中. 而 $\mathfrak{p} \notin S$ 时 $M_{\mathfrak{p}} = K_{\mathfrak{p}}$, 因此 $\alpha_{\mathfrak{p}} a^{-1}$ 自然落在 $\mathbf{N}_{M_{\mathfrak{p}}/K_{\mathfrak{p}}} M_{\mathfrak{p}}^\times$ 中. 因此 αa^{-1} 局部处处是范, 从而它是 \mathbb{I}_M 的范, α 在 C_K 中的类落在 $\mathbf{N}_{M/K} C_M$ 中. 故 $C_K = \mathbf{N}_{M/K} C_M$, 这与 $h(G(M/K), C_M) = p$ 矛盾!

□

推论 3.60

设 L/K 是数域的有限扩张. 如果 K 几乎所有的素位都在 L 中完全分裂, 则 $L = K$.



证明 设 M/K 是其伽罗瓦闭包, $G = G(M/K), H = G(M/L)$. 设 $\mathfrak{p} | \mathfrak{p}$ 是 M 的素位, 则 L 中 \mathfrak{p} 之上的素位个数为双陪集 $H \backslash G / G_{\mathfrak{p}}$ 的大小. 因此 \mathfrak{p} 在 L 中完全分裂当且仅当 $\#H \backslash G / G_{\mathfrak{p}} = [L : K] = \#H \backslash G$, 这意味着 $G_{\mathfrak{p}} = 1$, 即 \mathfrak{p} 在 M 中完全分裂.

设 $\sigma \in G(M/K)$ 为素数阶元, 固定域为 K' , 则 K' 几乎所有的素位在 M 中完全分裂, 这与前述推论矛盾! 因此 $M = K, L = K$.

□

§3.3.4 整体互反律

现在我们知道循环扩张 L/K 中 C_L 的埃尔布朗商为 $n = [L : K]$, 因此我们只需要说明 H^0 的大小等于 n 即可得到类域论公理. 我们略去证明过程.

定理 3.61

设 L/K 是 n 次循环扩张, 则

$$\#H^0(G(L/K), C_L) = n, \quad H^{-1}(G(L/K), C_L) = 1.$$

**推论 3.62**

设 L/K 是循环扩张, 则 K 中元素是 L 的范当且仅当在每个局部如此.



证明 设 $G = G(L/K)$. 由于

$$1 \rightarrow L^\times \rightarrow \mathbb{I}_L \rightarrow C_L \rightarrow 1$$

正合, 我们有正合列

$$1 = H^{-1}(G, C_L) \rightarrow H^0(G, L^\times) \rightarrow H^0(G, \mathbb{I}_L).$$

由于 $H^0(G, \mathbb{I}_L) = \bigoplus_{\mathfrak{p}} H^0(G_{\mathfrak{p}}, L_{\mathfrak{p}}^\times)$, 因此该命题成立. □

命题 3.63

设 T 是 $G(\mathbb{Q}(\mu_\infty)/\mathbb{Q})$ 的挠部分, 则 T 的固定子域 $\tilde{\mathbb{Q}}$ 是 \mathbb{Q} 的 $\hat{\mathbb{Z}}$ 扩张.



证明 由于

$$G(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) = \varprojlim_n G(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times = \hat{\mathbb{Z}}^\times,$$

而 $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p, \mathbb{Z}_p^\times \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}, p \neq 2$ 或 $\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}, p = 2$. 因此

$$G(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times \cong \hat{\mathbb{Z}} \times \hat{T}, \quad \hat{T} = \prod_{p \neq 2} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

而 $T = \bigoplus_{p \neq 2} \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 的闭包是 \hat{T} , 因此 T 和 \hat{T} 的固定域相同, $G(\tilde{\mathbb{Q}}/\mathbb{Q}) = G(\mathbb{Q}(\mu_\infty)/\mathbb{Q})/\hat{T} \cong \hat{\mathbb{Z}}$. □

固定 $G(\tilde{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\sim} \hat{\mathbb{Z}}$, 则我们有一个连续的满同态

$$d: G_{\mathbb{Q}} \rightarrow \hat{\mathbb{Z}}.$$

对于数域 K , 令 $f_K = [K \cap \tilde{\mathbb{Q}} : \mathbb{Q}]$, 则我们有满同态

$$d_K = \frac{1}{f_K} d: G_K \rightarrow \hat{\mathbb{Z}}.$$

这给出了一个 $\hat{\mathbb{Z}}$ 扩张 $\tilde{K} = K\tilde{\mathbb{Q}}/K$, 称之为 K 的**分圆扩张**.

对于有限次阿贝尔扩张 L/K , 定义

$$\begin{aligned} [\cdot, L/K]: \mathbb{I}_K &\longrightarrow G(L/K) \\ \alpha &\longmapsto \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}). \end{aligned}$$

由于对几乎所有的素位 \mathfrak{p} , $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ 非分歧, 因此 $\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}$ 的像是 1, 从而右侧乘积有意义.

和局部类域论类似, 我们可以对于无穷次阿贝尔扩张定义范剩余符号, 且范剩余符号满足相应的函数性. 我们不做详解.

命题 3.64

对于任一单位根 ζ 和主伊代尔 $a \in K^\times$, $[a, K(\zeta)/K] = 1$.



证明 由函子性我们有 $[\mathbf{N}_{K/\mathbb{Q}}(a), \mathbb{Q}(\zeta)/\mathbb{Q}] = [a, K(\zeta)/K]_{\mathbb{Q}(\zeta)}$. 因此我们只需对 $K = \mathbb{Q}$ 情形证明即可. 出于同样的理由, 我们可以不妨设 ζ 是 $\ell^m \neq 2$ 阶. 对于 $a \in \mathbb{Q}^\times$, 设 $a = u_p p^{v_p(a)}$. 对于 $p \neq \ell, \infty$, $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ 非分歧, $(p, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ 是弗罗贝尼乌斯 $\varphi_p: \zeta \mapsto \zeta^p$. 由局部类域论可知

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\zeta = \zeta^{n_p}, \quad n_p = \begin{cases} p^{v_p(a)}, & p \neq \ell, \infty, \\ u_p^{-1}, & p = \ell, \\ \text{sgn}(a), & p = \infty. \end{cases}$$

因此

$$[a, \mathbb{Q}(\zeta)/\mathbb{Q}]\zeta = \zeta^\alpha,$$

其中

$$\alpha = \prod_p n_p = \text{sgn}(a) \prod_{p \neq \ell, \infty} p^{v_p(a)} u_\ell^{-1} = 1.$$

□

由此可知 $[a, \tilde{K}/K] = 1, \forall a \in K^\times$. 因此我们有

$$[\cdot, \tilde{K}/K]: C_K \rightarrow G(\tilde{K}/K).$$

通过复合 $d_K: G(\tilde{K}/K) \rightarrow \hat{\mathbb{Z}}$, 我们得到

$$v_K: C_K \rightarrow \hat{\mathbb{Z}}.$$

命题 3.65

v_K 是满同态且是亨泽尔的.



证明 我们对有限伽罗瓦子扩张 L/K 来证明 $[\cdot, L/K]$ 是满射. 由于在每个局部范剩余符号是满的, 因此 $[\mathbb{I}_K, L/K]$ 包含所有的分解群, 从而它的固定域 M 上所有 \mathfrak{p} 完全分裂, 这意味着 $M = K$, $[\mathbb{I}_K, L/K] = G(L/K)$. 所以 $[\mathbb{I}_K, \tilde{K}/K] = [C_K, \tilde{K}/K]$ 在 $G(\tilde{K}/K)$ 中稠密.

对于任意 $\alpha \in \mathbb{I}_K$, 定义

$$|\alpha| = \prod_{\mathfrak{p}} |\alpha_{\mathfrak{p}}|_{\mathfrak{p}}^{-1}.$$

由乘积公式可知 $|\cdot|$ 在主伊代尔上平凡, 因此它诱导了连续同态 $|\cdot|: C_K \rightarrow \mathbb{R}_+^\times$. 我们不加证明地断言它的核 C_K^0 是紧的. 通过将 \mathbb{R}_+^\times 看成一个无穷素位处完备化的正实数部分, 我们固定一个 $|\cdot|$ 的截面, 从而 $C_K = C_K^0 \times \mathbb{R}_+^\times$. 而 \mathbb{R}_+^\times 的像是平凡的, 因此 C_K 和 C_K^0 的像相同, 它是一个闭集, 因此它的像等于它的闭包 $G(\tilde{K}/K)$. 故 v_K 是满的.

对于有限扩张 L/K , 由函子性我们有

$$\begin{aligned} v_K(\mathbf{N}_{L/K} C_L) &= v_K(\mathbf{N}_{L/K} \mathbb{I}_L) = d_K[\mathbf{N}_{L/K} \mathbb{I}_L, \tilde{K}/K] \\ &= f_{L/K} d_L[\mathbb{I}_L, \tilde{L}/L] = f_{L/K} v_L(C_L) = f_{L/K} \hat{\mathbb{Z}}. \end{aligned}$$

□

于是

$$d_{\mathbb{Q}}: G_{\mathbb{Q}} \rightarrow \hat{\mathbb{Z}}, \quad v_{\mathbb{Q}}: C_{\mathbb{Q}} \rightarrow \hat{\mathbb{Z}}$$

满足类域论公理. 我们有

定理 3.66

设 L/K 是数域的伽罗瓦扩张, 我们有典范同构

$$r_{L/K} : G(L/K)^{\text{ab}} \xrightarrow{\sim} C_K / \mathbf{N}_{L/K} C_L.$$



它的逆

$$(\cdot, L/K) : C_K \rightarrow G(L/K)^{\text{ab}}$$

被称为整体范剩余符号.

命题 3.67 (乘积公式)

设 L/K 是数域的伽罗瓦扩张, 我们有典范同构

$$(a, L/K) = \prod_{\mathfrak{p}} (a_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}), \quad a \in \mathbb{A}_K^{\times}.$$

特别地, 对于主伊代尔 $a \in K^{\times}$, 我们有乘积公式

$$\prod_{\mathfrak{p}} (a, L_{\mathfrak{p}}/K_{\mathfrak{p}}) = 1.$$



证明 见 [15, Chapter VI, Proposition 5.6, Corollary 5.7], 这里省略. □

§3.3.5 整体类域

定理 3.68

$L \mapsto \mathcal{N}_L = \mathbf{N}_{L/K} C_L$ 给出了 K 的有限阿贝尔扩张 L 和 C_K 的有限指标闭子群的一一对应.



证明 我们需要证明范拓扑下开子群和通常拓扑下有限指标闭子群一致. 我们省略. □

设 $\mathfrak{m} = \prod_{\mathfrak{p}|\infty} \mathfrak{p}^{n_{\mathfrak{p}}}$ 为 K 的理想, 记

$$\mathbb{I}_K^{\mathfrak{m}} = \prod_{\mathfrak{p}}' U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}.$$

定义 3.69 (同余子群和射线类群)

称

$$C_K^{\mathfrak{m}} = \mathbb{I}_K^{\mathfrak{m}} K^{\times} / K^{\times}$$

为模 \mathfrak{m} 的同余子群, 称 $C_K / C_K^{\mathfrak{m}}$ 为模 \mathfrak{m} 的射线类群.



命题 3.70

C_K 的子群是有限指标闭子群当且仅当其包含一个同余子群.



证明 由于 $\mathbb{I}_K^{\mathfrak{m}} \subseteq \mathbb{I}_K$ 开, 因此 $C_K^{\mathfrak{m}}$ 是开子群. 由于 $\mathbb{I}_K^{\mathfrak{m}} \subseteq \mathbb{I}_K^{S_{\infty}}$, 而 $(C_K : \mathbb{I}_K^{S_{\infty}} K^{\times} / K^{\times}) = h_K < \infty$, 因此

$$\begin{aligned} (C_K : C_K^{\mathfrak{m}}) &= h_K (\mathbb{I}_K^{S_{\infty}} K^{\times} : \mathbb{I}_K^{\mathfrak{m}} K^{\times}) \leq h (\mathbb{I}_K^{S_{\infty}} : \mathbb{I}_K^{\mathfrak{m}}) \\ &= h_K \prod_{\mathfrak{p}|\mathfrak{m}} (U_{\mathfrak{p}} : U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}) 2^{r_1} \end{aligned}$$

有限. 从而 C_K^m 是有限指标闭子群, 包含 C_K^m 的子群是有限多个陪集的不交并, 也是有限指标闭子群.

反之, 设 \mathcal{N} 是有限指标闭子群, 则 \mathcal{N} 是开子群. 于是它在 \mathbb{I}_K 中的原像 U 是开集, 它包含某个

$$W = \prod_{\mathfrak{p} \in S - S_\infty} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \times \prod_{\mathfrak{p} \in S \cap S_\infty} W_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}},$$

其中 $\mathfrak{p} \in S \cap S_\infty$ 时, $W_{\mathfrak{p}} \subset K_{\mathfrak{p}}^\times$ 是开集, 它必然生成整个 $U_{\mathfrak{p}}$, 从而 U 包含某个 \mathbb{I}_K^m , $\mathcal{N} \supseteq C_K^m$. \square

设 \mathcal{I}_K^m 为所有和 \mathfrak{m} 互素的分式理想, \mathcal{P}_K^m 为所有主分式理想 (a) , 其中 $a \equiv 1 \pmod{\mathfrak{m}}$ 且 a 全正 (即在所有实嵌入下的像大于 0). 令

$$\text{Cl}_K^m = \mathcal{I}_K^m / \mathcal{P}_K^m.$$

命题 3.71

自然同态 $(\cdot) : \mathbb{I}_K \rightarrow \mathcal{I}_K$ 诱导了同构 $C_K / C_K^m \cong \text{Cl}_K^m$. 特别地, $\text{Cl}_{\mathbb{Q}}^m \cong (\mathbb{Z}/m\mathbb{Z})^\times$.



证明 记

$$\mathbb{I}_K^{(m)} = \left\{ \alpha \in \mathbb{I}_K \mid \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}, \mathfrak{p} \mid m \infty \right\}.$$

我们有 $\mathbb{I}_K = \mathbb{I}_K^{(m)} K^\times$, 这是因为对于 $\alpha \in \mathbb{I}_K$, 由逼近定理, 存在 $a \in K^\times$ 使得 $\alpha_{\mathfrak{p}} a \equiv 1 \pmod{\mathfrak{p}^{n_{\mathfrak{p}}}}$, $\mathfrak{p} \mid m$ 以及 $\alpha_{\mathfrak{p}} a > 0$, \mathfrak{p} 是实素位. 因此 $\beta = \alpha a \in \mathbb{I}_K^{(m)}$, $\alpha = \beta a^{-1} \in \mathbb{I}_K^{(m)} K^\times$. 显然 $\mathbb{I}_K^{(m)} \cap K^\times$ 对应的 \mathcal{P}_K^m 中的理想, 因此我们有满同态

$$C_K = \mathbb{I}_K^{(m)} K^\times / K^\times = \mathbb{I}_K^{(m)} / \mathbb{I}_K^{(m)} \cap K^\times \rightarrow \mathcal{I}_K^m / \mathcal{P}_K^m.$$

显然 $C_K^m = \mathbb{I}_K^m K^\times / K^\times$ 在核中. 如果 $[\alpha]$ 在核中, $\alpha \in \mathbb{I}_K^{(m)}$, 则存在 $(a) \in \mathcal{P}_K^m$ 使得 $(\alpha) = (a)$. 由于 $a \in \mathbb{I}_K^{(m)} \cap K^\times$, 因此 $\beta = \alpha a^{-1} \in \mathbb{I}_K^m$, $[\alpha] = [\beta] \in C_K^m$, 核为 C_K^m .

对每个 $\text{Cl}_{\mathbb{Q}}^m$ 中的代表元, 我们选择其正生成元, 则我们得到满同态 $\mathcal{I}_{\mathbb{Q}}^m \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times$, 显然它的核是 $a \equiv m, a > 0$ 生成的理想. \square

称 C_K^m 对应的类域 K^m 为射线类域, K 的任意有限阿贝尔扩张均包含在其中. 当 $K = \mathbb{Q}$ 时, 模 m 的射线类域就是 $\mathbb{Q}(\mu_m)$, 换言之, 射线类域是分圆域的推广.

对于一个有限阿贝尔扩张, 想要判断它落在哪个射线类域中, 我们需要引入导子.

定义 3.72 (导子)

有限阿贝尔扩张 L/K 的导子 f 为满足 $L \subseteq K^f$ 的最小的 f .



命题 3.73

$$f_{L/K} = \prod_{\mathfrak{p}} f_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}.$$



证明 设 $\mathcal{N} = \mathbf{N}_{L/K} C_L$, 则对于 $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$,

$$C_K^m \subseteq \mathcal{N} \iff f \mid \mathfrak{m}, \quad \prod_{\mathfrak{p}} f_{\mathfrak{p}} \mid \mathfrak{m} \iff \mathfrak{p} \mid \mathfrak{p}^{n_{\mathfrak{p}}}, \forall \mathfrak{p}$$

因此我们只需证 $C_K^m \subseteq \mathcal{N} \iff f_{\mathfrak{p}} \mid \mathfrak{p}^{n_{\mathfrak{p}}}, \forall \mathfrak{p}$. 我们知道一个伊代尔是范当且仅当每个局部是范, 因此 $C_K^m \subseteq \mathcal{N}$ 当且仅当每个局部 $U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \subseteq \mathbf{N}L_{\mathfrak{p}}^\times$, 即 $f_{\mathfrak{p}} \mid \mathfrak{p}^{n_{\mathfrak{p}}}$. \square

推论 3.74

对于有限阿贝尔扩张 L/K , \mathfrak{p} 分歧当且仅当 $\mathfrak{p} \mid f_{L/K}$.



令 $m = 1$, 我们称 K^1 为 K 的大希尔伯特类域, 它是 K 的极大非分歧阿贝尔扩张.

命题 3.75

我们有正合列

$$1 \rightarrow \mathcal{O}^\times / \mathcal{O}_+^\times \rightarrow \prod_{\text{实素位 } \mathfrak{p}} \mathbb{R}^\times / \mathbb{R}_+^\times \rightarrow \text{Cl}_K^1 \rightarrow \text{Cl}_K \rightarrow 1,$$

其中 \mathcal{O}_+^\times 表示所有的全正单位.



证明 显然我们有

$$1 \rightarrow \mathbb{I}_K^{S_\infty} K^\times / \mathbb{I}_K^1 K^\times \rightarrow \text{Cl}_K^1 \rightarrow \text{Cl}_K \rightarrow 1,$$

另一方面

$$1 \rightarrow \mathbb{I}_K^{S_\infty} \cap K^\times / \mathbb{I}_K^1 \cap K^\times \rightarrow \mathbb{I}_K^{S_\infty} / \mathbb{I}_K^1 \rightarrow \mathbb{I}_K^{S_\infty} K^\times / \mathbb{I}_K^1 K^\times \rightarrow 1.$$

由 $\mathbb{I}_K^{S_\infty} \cap K^\times = \mathcal{O}^\times$, $\mathbb{I}_K^1 \cap K^\times = \mathcal{O}_+^\times$, $\mathbb{I}_K^{S_\infty} / \mathbb{I}_K^1 = \prod_{\mathfrak{p} | \infty} K_\mathfrak{p}^\times / U_\mathfrak{p} = \prod_{\text{实素位 } \mathfrak{p}} \mathbb{R}^\times / \mathbb{R}_+^\times$ 知该命题成立. \square

K^1 中无穷素位完全分裂 (即实素位变成实素位) 的极大子扩张被称为 K 的希尔伯特类域.

命题 3.76

$$G(H_K/K) \cong \text{Cl}_K.$$



证明 H_K/K 是所有 $G(K_\mathfrak{p}^1/K_\mathfrak{p})$, $\mathfrak{p} | \infty$ 生成的子群 G_∞ 的固定域, 它在范剩余符号下的像为所有 $K_\mathfrak{p}^\times$ 在 $G(K^1/K) \cong \mathbb{I}_K / \mathbb{I}_K^1 K^\times$ 中生成的子群, 即

$$\left(\prod_{\mathfrak{p} | \infty} K_\mathfrak{p}^\times \right) \mathbb{I}_K^1 K^\times / \mathbb{I}_K^1 K^\times = \mathbb{I}_K^{S_\infty} K^\times / \mathbb{I}_K^1 K^\times,$$

因此

$$G(H_K/K) = G(K^1/K) / G_\infty \cong \mathbb{I}_K / \mathbb{I}_K^{S_\infty} K^\times \cong \text{Cl}_K.$$

\square

我们知道 \mathbb{Q} 的射线类域由单位根生成, 那么对于一般的数域而言, 是否可以通过添加解析函数的特殊值来得到呢? 目前为止, 人们仅知道虚二次域的情形. 该情形下, 射线类域由添加理想类的 j 函数值得到, 在此不做详解.

设 L/K 是 n 次阿贝尔扩张, \mathfrak{p} 非分歧, 则

$$\varphi_\mathfrak{p} = (\pi_\mathfrak{p}, L_\mathfrak{p}/K_\mathfrak{p})$$

不依赖于 $\pi_\mathfrak{p}$ 的选取, 且生成 $G_\mathfrak{p} = G(L_\mathfrak{p}/K_\mathfrak{p})$. 记

$$\left(\frac{L/K}{\mathfrak{p}} \right) := \varphi_\mathfrak{p}.$$

设 $L \subseteq K^m$, 即 $f | m$, 则 $\mathfrak{p} \nmid m$ 时 \mathfrak{p} 非分歧, 定义阿廷符号

$$\left(\frac{L/K}{\mathfrak{p}} \right) : \mathcal{I}_K^m \rightarrow G(L/K)$$

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_\mathfrak{p}} \mapsto \prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}} \right)^{v_\mathfrak{p}}.$$

显然

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \left(\prod_{\mathfrak{p}} \langle \pi_{\mathfrak{p}} \rangle^{\nu_{\mathfrak{p}}}, L/K\right),$$

因此它在 $\mathcal{P}_K^{\mathfrak{m}}$ 上平凡.

定理 3.77

设 L/K 是 n 次阿贝尔扩张, $f \mid m$, 则我们有满射

$$\left(\frac{L/K}{\cdot}\right) : \text{Cl}_K^{\mathfrak{m}}/H^{\mathfrak{m}} \rightarrow G(L/K),$$

它的核为 $H^{\mathfrak{m}}/\mathcal{P}_K^{\mathfrak{m}}$, 其中 $H^{\mathfrak{m}} = (\mathbf{N}_{L/K}\mathcal{I}_L^{\mathfrak{m}})\mathcal{P}_K^{\mathfrak{m}}$, 且我们有正合列的交换图

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathbf{N}_{L/K}C_L & \longrightarrow & C_K & \xrightarrow{(\cdot, L/K)} & G(L/K) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \parallel \\ 1 & \longrightarrow & H^{\mathfrak{m}}/\mathcal{P}_K^{\mathfrak{m}} & \longrightarrow & \text{Cl}_K^{\mathfrak{m}} & \xrightarrow{(\cdot, L/K)} & G(L/K) \longrightarrow 1. \end{array}$$

换言之, 我们有同构

$$\left(\frac{L/K}{\cdot}\right) : \mathcal{I}_K^{\mathfrak{m}}/H^{\mathfrak{m}} \rightarrow G(L/K).$$



定理 3.78

设 L/K 是 n 次阿贝尔扩张, $f \mid m$, \mathfrak{p} 非分歧. 设 \mathfrak{p} 在 $\mathcal{I}_K^{\mathfrak{m}}/H^{\mathfrak{m}}$ 中的阶为 f , 则 \mathfrak{p} 在 L 中分解为 n/f 个不同素理想的乘积. 特别地, 完全分解的素理想为 H^f 中的素理想全体.



证明 这是因为 $\mathfrak{P} \mid \mathfrak{p}$ 的分解群的大小为弗罗贝尼乌斯 $\varphi_{\mathfrak{p}}$ 的阶, 即 \mathfrak{p} 在 $\mathcal{I}_K^{\mathfrak{m}}/H^{\mathfrak{m}}$ 中的阶. □

例题 3.14 当 $K = \mathbb{Q}$ 时, p 在 $\mathbb{Q}(\mu_m)/\mathbb{Q}$ 中分解为 $\varphi(m)/f$ 个不同素理想乘积, 其中 f 为 $p \bmod m$ 的阶. 特别地, 当且仅当 $p \equiv 1 \pmod m$ 时, p 完全分解.

我们知道 $G(H_K/K) = \text{Cl}_K = \mathcal{I}_K/\mathcal{P}_K$, 因此该扩张对应的 $H^1 = \mathcal{P}_K$.

推论 3.79

K 中素理想在希尔伯特类域中完全分解当且仅当它是主理想.



定理 3.80

K 中任一理想在希尔伯特类域中变成主理想.



证明 见 [15, Chapter VI, Proposition 7.5], 这里省略. □

一般而言, K 的希尔伯特类域类数不为 1. 一个自然的问题是,

$$K = K_0 \subseteq K_1 \subseteq \dots$$

是否会在某一层停止? 其中 $K_{i+1} = H_{K_i}$. 答案是否定的, E. S. Golod 和沙法列维奇证明了存在 K 使得这个扩张塔可以一直增长下去.

§3.3.6 希尔伯特符号的整体性质

设 K 包含 n 次单位根.

命题 3.81

对于 $a, b \in K^\times$,

$$\prod_{\mathfrak{p}} \left(\frac{a, b}{\mathfrak{p}} \right) = 1.$$



对于与 n 互素的理想 $\mathfrak{b} = \prod_{\mathfrak{p} \nmid n} \mathfrak{p}^{\nu_{\mathfrak{p}}}$, 以及和 \mathfrak{b} 互素的元素 a , 定义 n 次剩余符号

$$\left(\frac{a}{\mathfrak{b}} \right) = \prod_{\mathfrak{p} \nmid n} \left(\frac{a}{\mathfrak{p}} \right)^{\nu_{\mathfrak{p}}}.$$


定理 3.82


如果 $a, b \in K^\times$ 互素且均和 n 互素, 则

$$\left(\frac{a}{\mathfrak{b}} \right) \left(\frac{b}{\mathfrak{a}} \right)^{-1} = \prod_{\mathfrak{p} | n_\infty} \left(\frac{a, b}{\mathfrak{p}} \right).$$



当我们取 $n = 2, K = \mathbb{Q}$ 时, 这就是高斯的二次互反律.

 **练习 3.3.3** 了解和学习整体函数域情形的整体类域论.

 **练习 3.3.4** 了解和学习几何类域论.

第四章 L 函数

内容提要

□ 狄利克雷 L 函数 4.1

□ 模形式 4.3

□ 赫克 L 函数 4.24

□ 椭圆曲线 4.4

□ 解析类数公式 4.23



问题 4.1

是否有分析手段来研究数域的代数行为?



数论中人们关心的很多对象,例如类群、方程的解的结构等,都与某些分析对象有关,这些分析对象我们可以使用很多分析工具来处理,因此构建算术和分析之间的联系是现代数论的主要研究目的.

§4.1 黎曼 ζ 函数和狄利克雷 L 函数

§4.1.1 狄利克雷特征

定义 4.2 (狄利克雷特征)

设 N 是正整数,模 N 的狄利克雷特征是指群同态

$$\chi: (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow S^1.$$

其中 $S^1 = \{z \in \mathbb{C} : |z| = 1\}$. 我们可以扩充定义 $\chi: \mathbb{Z} \rightarrow \mathbb{C}$, 使得 $(n, N) > 1$ 时 $\chi(n) = 0$.



定义 4.3 (导子和本原)

对于 N 的正因子 d , 一个模 d 的狄利克雷特征 χ_1 诱导了模 N 的狄利克雷特征 $(\mathbb{Z}/N\mathbb{Z})^\times \rightarrow (\mathbb{Z}/d\mathbb{Z})^\times \xrightarrow{\chi_1} S^1$. 对于狄利克雷特征 χ , 这样的最小的 d 我们称之为 χ 的导子 f_χ . 记 $\chi^{\text{prim}} = \chi_1$, 则 $f_{\chi^{\text{prim}}} = f_\chi = d$. 如果 $f_\chi = N, \chi^{\text{prim}} = \chi$, 我们称之为本原的; 否则称之为非本原的.



例题 4.1 (1) 设 $\chi: (\mathbb{Z}/8\mathbb{Z})^\times \rightarrow S^1, \chi(1) = \chi(5) = 1, \chi(3) = \chi(7) = -1$, 则 $\chi(a+4) = \chi(a)$, 从而 $f_\chi = 4$.

(2) 设 p 是奇素数. 勒让德符号 $\left(\frac{\cdot}{p}\right)$ 是导子为 p 的狄利克雷特征.

练习 4.1.1 设 n 是正整数. 证明雅克比符号 $\left(\frac{\cdot}{n}\right)$ 是狄利克雷特征. 计算它的导子.

定义 4.4 (狄利克雷特征的 L 函数)

称

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s} = \prod_p (1 - \chi(p)p^{-s})^{-1}, \quad \text{Re}(s) > 1$$

为 χ 的 L 函数, 其中右侧的乘积被称为欧拉乘积. 特别地, $\chi = 1$ 时,

$$\zeta(s) := L(s, 1) = \sum_{n=1}^{\infty} n^{-s} = \prod_p (1 - p^{-s})^{-1}$$

被称为黎曼 ζ 函数. 容易看出 χ 非本原时, $L(s, \chi)$ 和 $L(s, \chi^{\text{prim}})$ 仅相差有限个欧拉因子.



我们将证明 $L(s, \chi)$ 可以解析延拓.

练习 4.1.2 设 $N = 4$, $\chi(1 + 2k) = (-1)^k$, 证明 $L(1, \chi) = \frac{\pi}{4}$.

设 χ 是模 N 的本原特征, $\zeta = \zeta_N = e^{2\pi i/N}$. 定义高斯和

$$\tau(\chi) = \sum_{n \bmod N} \chi(n)\zeta^n. \quad (4.1)$$

引理 4.5

$$\sum_{n \bmod N} \chi(n)\zeta^{nm} = \bar{\chi}(m)\tau(\chi).$$



证明 如果 $(m, N) = 1$,

$$\begin{aligned} \sum_{n \bmod N} \chi(n)\zeta^{nm} &= \bar{\chi}(m) \sum_{n \bmod N} \chi(nm)\zeta^{nm} \\ &= \bar{\chi}(m) \sum_{n \bmod N} \chi(n)\zeta^n = \bar{\chi}(m)\tau(\chi). \end{aligned}$$

一般地, 设 $d = (m, N)$, $m = dm_1$, $N = dN_1$. 由本原性, 存在 $c \equiv 1 \pmod{N_1}$ 使得 $\chi(c) \neq 1$, 于是

$$\sum_{n \equiv r \pmod{N_1}} \chi(n) = \sum_{n \equiv r \pmod{N_1}} \chi(cn) = \chi(c) \sum_{n \equiv r \pmod{N_1}} \chi(n)$$

为 0,

$$\begin{aligned} \sum_{n \bmod N} \chi(n)\zeta^{nm} &= \sum_{n \bmod N} \chi(n)\zeta_{N_1}^{nm_1} \\ &= \sum_{r=0}^{N_1-1} \sum_{n \equiv r \pmod{N_1}} \chi(n)\zeta_{N_1}^{nm_1} = \sum_{r=0}^{N_1-1} \zeta_{N_1}^{rm_1} \sum_{n \equiv r \pmod{N_1}} \chi(n) = 0, \end{aligned}$$

命题得证. □

引理 4.6

$$|\tau(\chi)| = \sqrt{N}. \text{ 特别地, } \tau(\chi) \neq 0.$$



证明 注意到

$$\left| \sum_{n \bmod N} \chi(n)\zeta^{nm} \right|^2 = \sum_{\substack{n_1, n_2 \bmod N \\ (n_1 n_2, N) = 1}} \chi(n_1 - n_2)\zeta^{(n_1 - n_2)m}.$$

对 $m \bmod N$ 求和, 我们得到

$$\varphi(N)|\tau(\chi)|^2 = \sum_{m \bmod N} \sum_{\substack{n_1, n_2 \bmod N \\ (n_1 n_2, N) = 1}} \chi(n_1 - n_2)\zeta^{(n_1 - n_2)m} = \varphi(N)N,$$

因此 $|\tau(\chi)| = \sqrt{N}$. □

练习 4.1.3 证明 $\tau(\chi)\tau(\bar{\chi}) = \chi(-1)N$.

例题 4.2 设 $\chi(n) = \left(\frac{n}{p}\right)$, 则 $\tau(\chi) = \sqrt{(-1)^{(p-1)/2}p}$, 见 [11, Chapter IV, §3].

现在我们有

$$\chi(n) = \frac{1}{\tau(\bar{\chi})} \sum_{m \bmod N} \bar{\chi}(m)\zeta^{nm} = \frac{\chi(-1)\tau(\chi)}{N} \sum_{m \bmod N} \bar{\chi}(m)\zeta^{nm}.$$

于是我们可以将 χ 延拓至整个 \mathbb{R} 上.

§4.1.2 解析延拓和函数方程

设 f 是 \mathbb{R} 上足够好函数¹. 定义

$$\widehat{f}(x) = \int_{-\infty}^{\infty} f(y)e^{2\pi ixy} dy$$

为其傅里叶变换, 则 \widehat{f} 的傅里叶变换为 $f(-x)$.

命题 4.7 (泊松求和公式)

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \widehat{f}(n).$$



证明 考虑 $F(x) = \sum_{n \in \mathbb{Z}} f(x+n)$ 的傅里叶展开

$$F(x) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n x}, \quad a_n = \int_0^1 F(x) e^{-2\pi i n x} dx,$$

则

$$\sum_{n \in \mathbb{Z}} f(n) = F(0) = \sum_{n \in \mathbb{Z}} a_n = \sum_{n \in \mathbb{Z}} \widehat{f}(n).$$

□

命题 4.8

设 χ 是本原模 N 特征,

$$\sum_{n \in \mathbb{Z}} \chi(n) f(n) = \frac{\chi(-1)\tau(\chi)}{N} \sum_{n \in \mathbb{Z}} \bar{\chi}(n) \widehat{f}\left(\frac{n}{N}\right).$$



证明 设

$$f_1(x) = \chi(x)f(x) = \frac{\chi(-1)\tau(\chi)}{N} \sum_{m \bmod N} \bar{\chi}(m) \zeta^{mx} f(x),$$

则

$$\widehat{f}_1(x) = \frac{\chi(-1)\tau(\chi)}{N} \sum_{m \bmod N} \bar{\chi}(m) \widehat{f}\left(\frac{Nx+m}{N}\right).$$

因此

$$\begin{aligned} \sum_{n \in \mathbb{Z}} \chi(n) f(n) &= \frac{\chi(-1)\tau(\chi)}{N} \sum_{m \bmod N} \sum_{n \in \mathbb{Z}} \bar{\chi}(m) \widehat{f}\left(\frac{Nx+m}{N}\right) \\ &= \frac{\chi(-1)\tau(\chi)}{N} \sum_{n \in \mathbb{Z}} \bar{\chi}(n) \widehat{f}\left(\frac{n}{N}\right), \end{aligned}$$

命题得证. □

对于实部大于 0 的复数 t , 令

$$f_{t,\varepsilon} = x^\varepsilon e^{-\pi t x^2}, \quad \varepsilon = 0, 1.$$

练习 4.1.4 证明

$$\widehat{f}_{t,\varepsilon} = i^\varepsilon t^{-\frac{1}{2}-\varepsilon} f_{\frac{1}{t},\varepsilon}.$$

¹只有有限多间断点的分段连续函数, 全变分有界, 在间断点的值为左右极限的平均值, 且存在 $c_1 > 0, c_2 > 1, |f(x)| < c_1 \min(1, x^{-c_2})$.

设 χ 是本原模 N 特征, 且 $\chi(-1) = (-1)^\varepsilon$, 定义 θ 函数

$$\theta_\chi(t) = \frac{1}{2} \sum_{n \in \mathbb{Z}} \chi(n) f_{t,\varepsilon}(n) = \frac{\chi(0)}{2} + \sum_{n=1}^{\infty} n^\varepsilon \chi(n) e^{-\pi n^2 t}.$$

练习 4.1.5 对 $f_{t,\varepsilon}$ 应用命题 4.8, 证明

$$\theta_\chi(t) = \frac{(-i)^\varepsilon \tau(\chi)}{N^{\varepsilon+1} t^{\varepsilon+\frac{1}{2}}} \theta_{\bar{\chi}}\left(\frac{1}{N^2 t}\right).$$

称

$$\Gamma(s) = \int_0^\infty e^{-y} y^s \frac{dy}{y}$$

为 Γ 函数.

练习 4.1.6 (1) $\Gamma(s+1) = s\Gamma(s)$, 因此 $\Gamma(n+1) = n!, n \in \mathbb{N}$.

$$(2) \Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}.$$

命题 4.9

Γ 可以亚纯延拓至复平面, 处处非零, 仅在 $s = 0, -1, -2, \dots$ 处有单极点, 留数为 $\frac{(-1)^s}{(-s)!}$. Γ 满足函数方程

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}, \quad \Gamma(s)\Gamma\left(s + \frac{1}{2}\right) = \frac{2\sqrt{\pi}}{2^{2s}} \Gamma(2s).$$



定理 4.10

令

$$\Lambda(s, \chi) = \pi^{-\frac{s+\varepsilon}{2}} \Gamma\left(\frac{s+\varepsilon}{2}\right) L(s, \chi),$$

则 $\Lambda(s, \chi)$ 可以亚纯延拓至整个复平面. 当 $\chi \neq 1$ 时, 它是全纯的; 当 $\chi = 1$ 时, 它有单极点 $s = 0, 1$ 且留数为 ∓ 1 . 我们有函数方程

$$\Lambda(s, \chi) = (-i)^\varepsilon \tau(\chi) N^{-s} \Lambda(1-s, \bar{\chi}).$$



证明 如果 $\chi \neq 1, \chi(0) = 0$. 当 $\operatorname{Re}(s) > 0$ 时,

$$\int_0^\infty e^{-\pi t n^2} t^{\frac{s+\varepsilon}{2}} \frac{dt}{t} = \pi^{-\frac{s+\varepsilon}{2}} \Gamma\left(\frac{s+\varepsilon}{2}\right) n^{-s-\varepsilon},$$

因此

$$\Lambda(s, \chi) = \int_0^\infty \theta_\chi(t) t^{\frac{s+\varepsilon}{2}} \frac{dt}{t}.$$

当 $t \rightarrow \infty$ 时 θ 函数是急减的. 根据 θ 函数的函数方程, 当 $t \rightarrow 0$ 它也是急减的. 因此右侧积分在整个复平面收敛. 于是我们得到 $\Lambda(s, \chi)$ 的延拓. 利用 θ 函数的函数方程我们可以得到 $\Lambda(s, \chi)$ 的函数方程.

如果 $\chi = 1, \theta(t) = \frac{1}{2} + \sum_{n=1}^{\infty} e^{-\pi n^2 t}$. 此时

$$\widehat{\zeta}(s) = \Lambda(s, 1) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \int_0^\infty \left(\theta(t) - \frac{1}{2}\right) t^{\frac{s}{2}} \frac{dt}{t}.$$


当 $\operatorname{Re} s > 1$ 时,

$$\begin{aligned} & \int_0^1 \left(\theta(t) - \frac{1}{2} \right) t^{\frac{s}{2}} \frac{dt}{t} = \int_0^1 \theta(t) t^{\frac{s}{2}} \frac{dt}{t} - \frac{1}{s} \\ & = \int_1^\infty \theta\left(\frac{1}{t}\right) t^{-\frac{s}{2}} \frac{dt}{t} - \frac{1}{s} = \int_1^\infty \theta(t) t^{\frac{1-s}{2}} \frac{dt}{t} - \frac{1}{s} \\ & = \int_1^\infty \left(\theta(t) - \frac{1}{2} \right) t^{\frac{1-s}{2}} \frac{dt}{t} - \left(\frac{1}{1-s} + \frac{1}{s} \right), \end{aligned}$$

因此

$$\widehat{\zeta}(s) = \int_1^\infty \left(\theta(t) - \frac{1}{2} \right) (t^{\frac{s}{2}} + t^{\frac{1-s}{2}}) \frac{dt}{t} - \left(\frac{1}{s} + \frac{1}{1-s} \right).$$

当 $t \rightarrow \infty$ 时, $\theta(t) - \frac{1}{2}$ 是急减的, 因此该积分在 $s \neq 0, 1$ 处收敛, 故 $\Lambda(s)$ 可以全纯延拓至 $\mathbb{C} - \{0, 1\}$. 显然 $\Lambda(s) = \Lambda(1-s)$ 且 $\Lambda(s)$ 在 $s = 0, 1$ 处有单极点, 留数为 1. \square

 **练习 4.1.7** 如果 χ 是实特征, 即 $\chi: (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \{\pm 1\}$, 则 $\tau(\chi) = i^\varepsilon \sqrt{N}$.

推论 4.11

$\zeta(s)$ 可以解析延拓至 $\mathbb{C} - \{1\}$, 且在 $s = 1$ 处有单极点, 留数为 1. $\zeta(s)$ 满足函数方程

$$\zeta(1-s) = 2(2\pi)^{-s} \Gamma(s) \cos\left(\frac{\pi s}{2}\right) \zeta(s).$$



 **练习 4.1.8** 证明上述推论.

§4.1.3 特殊值

我们称泰勒展开

$$F(t) = \frac{te^t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!} = 1 + \frac{1}{2}t + \frac{1}{6} \frac{t^2}{2} - \frac{1}{30} \frac{t^4}{4!} + \frac{1}{42} \frac{t^6}{6!} + \dots$$

中的 B_k 称为伯努利数. 由于 $F(-t) = F(t) - t$, 因此 $B_{2k+1} = 0, k \geq 1$.

命题 4.12

对于正整数 k ,

$$\zeta(1-k) = -\frac{B_k}{k}.$$

因此对于正整数 k ,

$$\zeta(2k) = (-1)^{k+1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k}.$$



对于狄利克雷特征 $\chi \neq 1$, 考虑

$$F_\chi(t) = \sum_{a=1}^N \chi(a) \frac{te^{at}}{e^{Nt} - 1} = \sum_{k=0}^{\infty} B_{k,\chi} \frac{t^k}{k!}.$$

我们有 $F_\chi(-t) = \chi(-1)F_\chi(t)$, 因此 $B_{2k+\varepsilon,\chi} = 0, k \geq 0$.

命题 4.13

对于正整数 k ,

$$L(1-k, \chi) = -\frac{B_{k,\chi}}{k}.$$

因此对于正整数 $k \equiv \varepsilon \pmod{2}$,

$$L(k, \chi) = (-1)^{1+(k-\varepsilon)/2} \tau(\chi) \frac{(2\pi/N)^k}{2i^\varepsilon k!} B_{k, \bar{\chi}}.$$



我们知道 ζ 函数在负偶数处为零, 这样的零点被称为 ζ 函数的平凡零点, 其它的被称为非平凡零点. ζ 函数的非平凡零点和素数分布有关. 设 $\pi(x)$ 为不超过 x 的素数个数, 则通过证明 ζ 的非平凡零点位于 $0 < \operatorname{Re}(s) < 1$, 可以得到

$$\pi(x) \sim \int_0^x \frac{dt}{\ln t} \sim \frac{x}{\ln x},$$

而更精确的零点信息可以得到余项信息. 著名的黎曼猜想

$$\zeta \text{ 的非平凡零点位于 } \operatorname{Re}(s) = \frac{1}{2}$$

等价于

$$\pi(x) = \int_0^x \frac{dt}{\ln t} + O(x^{1/2} \ln x).$$

对于 L 函数, 人们也猜测它的非平凡零点位于函数方程的对称轴上 (广义黎曼猜想). 对于狄利克雷 L 函数, 对称轴为 $\operatorname{Re}(s) = \frac{1}{2}$.

定理 4.14

设 χ 是导子 $N > 3$ 的狄利克雷特征, 则 χ 是偶特征时,

$$L(1, \chi) = -\frac{\tau(\chi)}{N} \sum_{a=1}^{N-1} \bar{\chi}(a) \log |1 - \zeta^a| = -\frac{\tau(\chi)}{N} \sum_{a=1}^{N-1} \bar{\chi}(a) \log \left(\sin \frac{\pi a}{N} \right);$$

χ 是奇特征时,

$$L(1, \chi) = \frac{\tau(\chi)\pi i}{N^2} \sum_{a=1}^{N-1} \bar{\chi}(a)a.$$



证明 对于 $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, 考虑

$$\sum_{n=1}^{+\infty} \zeta^{an} n^{-s}, \quad \operatorname{Re}(s) > 1.$$

通过收敛性估计, 我们可以得知 $s \rightarrow 1^+$ 时它的极限为

$$\sum_{n=1}^{+\infty} \zeta^{an} n^{-1} = -\log(1 - \zeta^a).$$

这里我们选择将正实数映为正实数的 \log 的一个分支. 于是

$$\sum_{a=1}^{N-1} \bar{\chi}(a) \sum_{n=1}^{+\infty} \zeta^{an} n^{-s} = \tau(\bar{\chi}) \sum_{n=1}^{\infty} \chi(n) n^{-s},$$

因此

$$L(1, \chi) = -\frac{\chi(-1)\tau(\chi)}{N} \sum_{a=1}^{N-1} \bar{\chi}(a) \log(1 - \zeta^a).$$

注意到

$$\log(1 - \zeta^a) = \log |1 - \zeta^a| + \pi i \left(\frac{a}{N} - \frac{1}{2} \right).$$

当 χ 是奇特征时, $|1 - \zeta^a| = |1 - \zeta^{-a}|$, 于是

$$\begin{aligned} \sum_{a=1}^{N-1} \bar{\chi}(a) \log(1 - \zeta^a) &= \sum_{a=1}^{N-1} \bar{\chi}(-a) \log(1 - \zeta^a) \\ &= - \sum_{a=1}^{N-1} \bar{\chi}(a) \log(1 - \zeta^a) = 0. \end{aligned}$$

因此

$$L(1, \chi) = \frac{\tau(\chi)}{N} \sum_{a=1}^{N-1} \bar{\chi}(a) \pi i \left(\frac{a}{N} - \frac{1}{2} \right) = \frac{\tau(\chi) \pi i}{N^2} \sum_{a=1}^{N-1} \bar{\chi}(a) a.$$

当 χ 是偶特征时,

$$\begin{aligned} \sum_{a=1}^{N-1} \bar{\chi}(a) \left(\frac{a}{N} - \frac{1}{2} \right) &= \sum_{a=1}^{N-1} \bar{\chi}(a) \left(\frac{-a}{N} - \frac{1}{2} \right) \\ &= -\frac{1}{2} \sum_{a=1}^{N-1} \bar{\chi}(a) = 0. \end{aligned}$$

因此

$$L(1, \chi) = -\frac{\tau(\chi)}{N} \sum_{a=1}^{N-1} \bar{\chi}(a) \log(1 - \zeta^a) = -\frac{\tau(\chi)}{N} \sum_{a=1}^{N-1} \bar{\chi}(a) \log \left(\sin \frac{\pi a}{f} \right).$$

命题得证. □

§4.2 戴德金 ζ 函数与赫克 L 函数

现在我们来考虑一般数域 K . 定义戴德金 ζ 函数

$$\zeta_K(s) = \sum_{\mathfrak{a}} \mathbf{N}\mathfrak{a}^{-s},$$

其中 \mathfrak{a} 取遍 \mathcal{O}_K 的所有非零理想. 容易证明 $\zeta_K(s)$ 在 $\operatorname{Re}(s) > 1$ 收敛且有欧拉乘积

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - \mathbf{N}\mathfrak{p}^{-s})^{-1}.$$

定义 4.15 (赫克特征)

称连续同态 $\chi: C_K \rightarrow \mathbb{C}^\times$ 为拟赫克特征. 如果它的像落在 S^1 中, 则称之为(酉)赫克特征.



狄利克雷 L 函数在一般数域上的推广为赫克 L 函数. 设 χ 为赫克特征, 定义

$$L(s, \chi) = \prod_{v \neq \infty} (1 - \chi(v) \mathbf{N}\mathfrak{p}^{-s})^{-1}$$

为其赫克 L 函数, 其中在映射 $K_v^\times \rightarrow C_K \rightarrow S^1$ 下 $\chi(\mathcal{O}_v^\times) = 1$ 时, $\chi(v) := \chi(\pi_v)$; 否则定义为 0. 通过乘以适当的 Γ 函数和判别式、导子等, 我们可以定义完备的赫克 L 函数 $\Lambda(s, \chi)$.

我们将使用泰特的方法来得到它们的函数方程.

§4.2.1 泰特的方法

设 k 是一局部域, 即 \mathbb{R}, \mathbb{C} 或 \mathbb{Q}_p 的有限扩张.

定义 4.16 (施瓦兹函数)

$k = \mathbb{R}$ 或 \mathbb{C} 上的施瓦兹函数是指急减光滑函数; k/\mathbb{Q}_p 上的施瓦兹函数是紧支撑的局部常值函数. 记 $\mathcal{S}(k, \mathbb{C})$ 为 k 上复值施瓦兹函数全体.



我们选取 k 上的哈尔测度

- k/\mathbb{Q}_p 时, dx 满足

$$\int_{\mathcal{O}_k} dx = \Delta_{k/\mathbb{Q}_p}^{-1/2};$$

- $k = \mathbb{R}$ 时为通常的勒贝格测度;
- $k = \mathbb{C}$ 时为通常的勒贝格测度的 2 倍.

于是

$$d^\times x = \begin{cases} \frac{dx}{|x|}, & k = \mathbb{R} \text{ 或 } \mathbb{C} \\ \frac{1}{1-Np^{-1}} \cdot \frac{dx}{|x|}, & k/\mathbb{Q}_p \end{cases}$$

是 k^\times 上的哈尔测度. 注意 $k = \mathbb{C}$ 时 $|x| = x\bar{x}$.

定义 4.17

连续的群同态 $\chi: k^\times \rightarrow \mathbb{C}^\times$ 被称为拟特征. 如果它的像落在 S^1 中, 则称之为(酉)特征.



练习 4.2.1 拟特征一定可以表为 $\chi = \chi_0 |\cdot|^s$, 其中 χ_0 是酉特征, $s \in \mathbb{C}$. 我们记 $\text{Re}(\chi) = \text{Re}(s)$.

对于 $f \in \mathcal{S}(k, \mathbb{C})$ 和拟特征 $\chi = \chi_0 |\cdot|^s$, 定义局部 ζ 函数

$$\zeta(f, \chi) := \int_{k^\times} f(x) \chi(x) d^\times x.$$

练习 4.2.2 证明 $\zeta(f, \chi)$ 在 $\text{Re}(\chi) > 0$ 处绝对收敛.

定义 $f \in \mathcal{S}(k, \mathbb{C})$ 的傅里叶变换为

$$\hat{f}(x) = \int_k f(y) \psi(xy) dy,$$

则 $\hat{f} \in \mathcal{S}(k, \mathbb{C})$, 且 \hat{f} 的傅里叶变换为 $f(-x)$. 对于拟特征 χ , 定义

$$\hat{\chi}(x) = |x| \chi^{-1}(x).$$

引理 4.18

设 $f, g \in \mathcal{S}(k, \mathbb{C})$, $0 < \text{Re}(\chi) < 1$. 我们有函数方程

$$\zeta(f, \chi) \zeta(\hat{g}, \hat{\chi}) = \zeta(\hat{f}, \hat{\chi}) \zeta(g, \chi).$$



证明 将左式写为

$$\iint f(x) \hat{g}(y) \chi(xy^{-1}) |y| d^\times x d^\times y,$$

然后做变量替换 $(x, y) \rightarrow (x, xy)$, 则我们得到

$$\iint f(x) \hat{g}(xy) \chi(y^{-1}) |xy| d^\times x d^\times y.$$

展开,

$$\iiint f(x) g(z) \chi(y^{-1}) |xy| \psi(xyz) d^\times x d^\times y d^\times z.$$

这关于 f, g 是对称的, 因此我们得到右式. □

如果存在 f 使得 $\zeta(\hat{f}, \hat{\chi}) \neq 0$, 则我们可定义 $w(\chi) = \zeta(f, \chi) / \zeta(\hat{f}, \hat{\chi})$. 具体的 f 和计算可见 [11, Chapter XIV, §4].

定理 4.19

函数 $\zeta(f, \chi)$ 可以亚纯延拓至复平面, 且满足函数方程

$$\zeta(f, \chi) = w(\chi)\zeta(\hat{f}, \hat{\chi}).$$

这里 $w(\chi)$ 在 $0 < \operatorname{Re}(\chi) < 1$ 上有定义, 并可亚纯延拓至复平面.



练习 4.2.3 根据函数方程我们有

- $w(\chi)w(\hat{\chi}) = \chi(-1)$;
- $w(\bar{\chi}) = \chi(-1)\overline{w(\chi)}$;
- 如果 $\operatorname{Re}(\chi) = \frac{1}{2}$, 则 $|w(\chi)| = 1$.

现在考虑数域 K .

定义 4.20 (施瓦兹函数)

\mathbb{A}_K 上的**施瓦兹函数**是指所有形如 $f = \otimes_v f_v, f_v \in \mathcal{S}(K_v, \mathbb{C})$ 的函数的线性组合, 其中对几乎所有的 $v, f_v = \mathbf{1}_{\mathcal{O}_v}$.



注意到对几乎所有的 v, \mathcal{O}_v 的体积为 1. 因此局部的哈尔测度给出了 \mathbb{A}_K 上的哈尔测度 $= dx = \prod_v dx_v$, 它诱导了 \mathbb{A}_K/K 上的哈尔测度 dx , 见 [11, Chapter XIV, §5]. 我们有

$$\int_{\mathbb{A}_K} f(x) dx = \prod_v \int_{K_v} f_v(x_v) dx_v,$$

且 f 相对

$$\langle x, y \rangle = \prod_v \psi_v(x_v y_v)$$

的傅里叶变换为 $\hat{f} = \otimes_v \hat{f}_v$.

练习 4.2.4 拟赫克特征一定可以表为 $\chi = \chi_0 |\cdot|^s$, 其中 χ_0 是特征, $s \in \mathbb{C}, |\cdot|$ 为伊代尔上的范数. 我们记 $\operatorname{Re}(\chi) = \operatorname{Re}(s)$.

对于 $f \in \mathcal{S}(K, \mathbb{C})$ 和拟赫克特征 $\chi = \chi_0 |\cdot|^s$, 定义 ζ 函数

$$\zeta(f, \chi) := \int_{\mathbb{I}_K} f(x)\chi(x) d^\times x.$$

类似于狄利克雷 L 函数, 该函数可以表为某种 s 与 $1-s$ 对称的形式, 从而可以得到它的亚纯延拓. 通过局部的计算, 我们可以得到整体的函数方程.

定理 4.21

$\zeta(f, \chi)$ 可以亚纯延拓至复平面, 且满足函数方程

$$\zeta(f, \chi) = \zeta(\hat{f}, \hat{\chi}).$$

仅当 $\chi = |\cdot|^s$ 时 $\zeta(f, \chi)$ 有极点, 分别为 $s = 0$ 和 1 的单极点, 留数为

$$-\operatorname{Res}_{s=0}\zeta(f, \chi) = \operatorname{Res}_{s=1}\zeta(f, \chi) = f(0) \frac{2^{r_1+r_2} \pi^{r_2} h R}{w|\Delta_K|^{\frac{1}{2}}},$$

其中 h 为 K 的类数, R 为调整子, w 为 $\mu(K)$ 大小, Δ_K 为判别式, r_1, r_2 分别为 K 的实素位和复

素位的个数.



令

$$f_v(x) = \begin{cases} \mathbf{1}_{\mathcal{O}_k}(x), & v \nmid \infty; \\ \exp(-\pi x^2), & K_v = \mathbb{R}; \\ \exp(-\pi x\bar{x}), & K_v = \mathbb{C}, \end{cases}$$

则我们可得戴德金 ζ 函数与赫克 L 函数的解析延拓和函数方程. 具体细节可参考 [9, §7.5] 和 [10, §11.2].

§4.2.2 解析延拓与函数方程

令

$$\widehat{\zeta}_K(s) = |\Delta_K|^{\frac{s}{2}} 2^{(1-s)r_2} \pi^{-\frac{ns}{2}} \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} \zeta_K(s).$$

定理 4.22

$\widehat{\zeta}_K(s)$ 可以解析延拓至 $\mathbb{C} - \{0, 1\}$ 且有函数方程

$$\widehat{\zeta}_K(s) = \widehat{\zeta}_K(1-s).$$

它在 $s = 0, 1$ 处有单极点, 留数为 $\mp \frac{2^{r_1+r_2} h R}{w}$, 其中 h 为 K 的类数, R 为调整子, w 为 $\mu(K)$ 大小.



推论 4.23

$\zeta_K(s)$ 可以解析延拓至 $\mathbb{C} - \{1\}$, 在 $s = 1$ 处有单极点且

$$\text{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2}}{w |\Delta_K|^{\frac{1}{2}}} h R.$$

$\zeta_K(s)$ 满足函数方程

$$\zeta_K(s) = |\Delta_K|^{s-\frac{1}{2}} \left(\cos \frac{\pi s}{2}\right)^{r_1+r_2} \left(\sin \frac{\pi s}{2}\right)^{r_2} 2^n (2\pi)^{-ns} \Gamma(s)^n \zeta_K(1-s).$$

ζ_K 在 $s = 0$ 处为 $r_1 + r_2 - 1$ 阶零点, 且

$$\lim_{s \rightarrow 0} s^{-r_1-r_2+1} \zeta_K(s) = -\frac{hR}{w}.$$



练习 4.2.5 证明该推论.

这个公式意味着我们可以通过估计 L 函数来达到计算类数的目的, 因此该公式被称为解析类数公式.

完备的赫克 L 函数 $\Lambda(s, \chi)$ 可以参考 [9, §7.5], 我们在次省略.

定理 4.24

赫克 L 函数 $L(s, \chi)$ 可以亚纯延拓至整个复平面, 且仅在 $\chi|_{\mathbb{A}_K^1/K^\times} = 1$ 时才有极点, 此时 $\chi(a) = |a|^{it}$, $L(s, \chi) = \zeta_K(s+it)$, $t \in \mathbb{R}$. 这里 \mathbb{A}_K^1 表示范数为 1 的伊代尔全体. 我们有函数方程 $\Lambda(s, \chi) = W(s, \chi) \Lambda(1-s, \bar{\chi})$, $|W(\frac{1}{2}, \chi)| = 1$.



设 L 为 K 的有限阿贝尔扩张, 则 L 对应于 C_K 的指数有限的开子群 H .

定理 4.25

我们有

$$\zeta_L(s) = \prod_{\chi} L(s, \chi),$$

其中 χ 取遍 C_K/H 的所有特征.

**§4.2.3 分圆域的 ζ 函数****推论 4.26**

如果 $K = \mathbb{Q}(\zeta_m)$, 则

$$\zeta_K(s) = G(s) \prod_{\chi} L(s, \chi),$$

其中 χ 取遍模 m 的狄利克雷特征,

$$G(s) = \prod_{p|m} (1 - \mathbf{N}p^{-s})^{-1}.$$



我们知道 $\zeta_K(s)$ 和 $\zeta(s) = L(1, s)$ 均只在 $s = 1$ 处有单极点, 因此

命题 4.27

χ 非平凡时, $L(1, \chi) \neq 0$.

**定理 4.28 (狄利克雷素数定理)**

对于任意互素的整数 $a, m > 0$, $a + m\mathbb{Z}$ 中有无穷多素数.



证明 设 χ 是模 m 的狄利克雷特征. 当 $\operatorname{Re}(s) > 1$ 时,

$$\log L(s, \chi) = - \sum_p \log(1 - \chi(p)p^{-s}) = \sum_p \sum_{m=1}^{\infty} \frac{\chi(p^m)}{mp^{ms}} = \sum_p \frac{\chi(p)}{p^s} + g_{\chi}(s).$$

通过估计可知 $g_{\chi}(s)$ 在 $\operatorname{Re}(s) > \frac{1}{2}$ 全纯. 两边同时乘以 $\chi(a^{-1})$ 并对所有模 m 特征求和

$$\begin{aligned} \sum_{\chi} \chi(a^{-1}) \log L(s, \chi) &= \sum_{\chi} \sum_p \frac{\chi(a^{-1}p)}{p^s} + g(s) \\ &= \sum_{b=1}^m \sum_{\chi} \chi(a^{-1}b) \sum_{p \equiv b \pmod{m}} \frac{1}{p^s} + g(s) \\ &= \sum_{p \equiv a \pmod{m}} \frac{\varphi(m)}{p^s} + g(s). \end{aligned}$$

设 $\chi_0 : (\mathbb{Z}/m\mathbb{Z})^{\times} \rightarrow S^1$ 为平凡特征. 当 $s \rightarrow 1$ 时, 对于 $\chi \neq \chi_0$, $\log L(s, \chi)$ 有界, 而 $\log L(s, \chi_0) = -\sum_{p|m} \log(1 - p^{-s}) + \log \zeta(s)$ 趋于无穷, 因此等式右侧也趋于无穷. 这意味着右侧的求和不可能只有有限多项. \square

注 实际上狄利克雷证明了这样的素数全体的密度为 $1/\varphi(m)$, 切博塔廖夫密度定理 2.63 是它的推广.

§4.2.4 二次域解析类数公式

设 $K = \mathbb{Q}(\sqrt{\Delta_K})$ 为二次域. 设 $N = |\Delta_K|$. 我们有分解

$$\zeta_K(s) = \zeta(s)L(s, \chi_{\Delta_K}),$$

其中 $\chi_{\Delta_K} : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \{\pm 1\}$ 为非平凡特征, 它满足 $\chi_{\Delta_K}(p) = \left(\frac{\Delta_K}{p}\right)$, p 为奇素数. 容易知道 $\chi(-1) = \text{sgn}(\Delta_K)$.

当 K 为实二次域时,

$$\text{Res}_{s=1}\zeta_K(s) = \frac{2}{|\Delta_K|^{\frac{1}{2}}}hR, \quad \lim_{s \rightarrow 0} s^{-1}\zeta_K(s) = \frac{2hR}{w}.$$

因此

$$h = |\Delta_K|^{\frac{1}{2}} \frac{L(1, \chi_{\Delta_K})}{2R} = \frac{L'(0, \chi_{\Delta_K})}{R}.$$

当 K 为虚二次域时,

$$\text{Res}_{s=1}\zeta_K(s) = \frac{2\pi}{w|\Delta_K|^{\frac{1}{2}}}h, \quad \zeta_K(0) = \frac{2hR}{w}.$$

因此

$$h = \frac{w}{2\pi} |\Delta_K|^{\frac{1}{2}} L(1, \chi_{\Delta_K}) = \frac{w}{2} L(0, \chi_{\Delta_K}).$$

由定理 4.14, 我们得到二次域的解析类数公式.

定理 4.29

设 K 为二次域. 如果 $\Delta_K < 0$, 则

$$h = -\frac{w_k}{2|\Delta_K|} \sum_{a=1}^{|\Delta_K|-1} \chi_{\Delta_K}(a)a.$$

如果 $\Delta_K > 0$, 则

$$h = -\frac{1}{\log \varepsilon} \sum_{a=1}^{[\Delta_K/2]} \chi_{\Delta_K}(a) \log\left(\sin \frac{\pi a}{\Delta_K}\right),$$

其中 $\varepsilon > 1$ 是 K 的基本单位.



例题 4.3 (1) $K = \mathbb{Q}(\sqrt{2})$, $\varepsilon = \sqrt{2} + 1$,

$$h_K = -\frac{1}{\log(\sqrt{2} + 1)} \left(\log \sin \frac{\pi}{8} - \log \sin \frac{3\pi}{8} \right) = 1.$$

(2) $K = \mathbb{Q}(\sqrt{-56})$. 对于奇素数 p , 易知

$$\chi_{-56}(p) = 1 \iff p \equiv 3, 5, 13, 19, 23 \pmod{56}.$$

注意到

$$\sum_{a=1}^{N-1} \chi(a)a = \sum_{a=1}^{[\frac{N}{2}]} \chi(a)a - \chi(a)(N-a) = 2 \sum_{a=1}^{[\frac{N}{2}]} \chi(a)a - N \sum_{a=1}^{[\frac{N}{2}]} \chi(a).$$

因此 $\sum_{a=1}^{55} \chi_{-56}(a)a = 2 \times 112 - 56 \times 8 = -224$, $h = 4$.

练习 4.2.6 计算虚二次域 $K = \mathbb{Q}(\sqrt{m})$ 的类数, 其中 $m = -1, -2, -3, -5, -6, -10, -26$.

§4.3 模形式

最后,我们将极其简要地介绍谷山-志村-韦伊关于椭圆曲线的猜想,它最终由怀尔斯证明,并由此得到费马大定理.

§4.3.1 庞加莱上半平面

设

$$\mathcal{H} = \{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$$

为庞加莱上半平面. 我们考虑 $\text{GL}(2, \mathbb{R})^+$ 在 $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \infty$ 的作用

$$\gamma \cdot \tau := \frac{a\tau + b}{c\tau + d}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}(2, \mathbb{R})^+.$$

这里 $+$ 表示行列式为正的实矩阵. 这种作用可以看成是 $\text{PGL}(2, \mathbb{R})$ 在 $\mathbb{P}^1(\mathbb{C}) \supseteq \mathcal{H}^*$ 上的自然线性作用诱导而来.

命题 4.30

- (1) $d(\gamma \cdot \tau) = \det \gamma \cdot (c\tau + d)^{-2} d\tau$.
- (2) $\text{Im}(\gamma \cdot \tau) = \det \gamma \cdot |c\tau + d|^{-2} \text{Im}(\tau)$.



证明 直接验证即可. □

考虑 \mathcal{H} 上的度量

$$\frac{dx^2 + dy^2}{y^2} = \frac{|d\tau|^2}{(\text{Im} \tau)^2}.$$

由上述命题可知该度量在 $\text{GL}(2, \mathbb{R})^+$ 作用下不动. 该度量下的测地线是圆心在实轴上的半圆, 以及和实轴垂直的射线.

§4.3.2 同余子群


定义 4.31 (同余子群)

对于正整数 N , 定义


$$\Gamma(N) = \{\gamma \in \text{SL}(2, \mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \pmod{N}\},$$

$$\Gamma_1(N) = \{\gamma \in \text{SL}(2, \mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} \pmod{N}\},$$


$$\Gamma_0(N) = \{\gamma \in \text{SL}(2, \mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} * & * \\ & * \end{pmatrix} \pmod{N}\}.$$

称 $\Gamma(N)$ 为**主同余子群**. 任何包含某个 $\Gamma(N)$ 的 $\text{SL}(2, \mathbb{Z})$ 的子群 Γ 被称为**同余子群**. 易知同余子群都是指标有限的. 

定义 4.32 (尖点)

称同余子群 Γ 在 $\mathbb{P}^1(\mathbb{Q}) \subseteq \mathcal{H}^*$ 上的作用的等价类为它的**尖点**. 

命题 4.33

$\text{SL}(2, \mathbb{Z})$ 只有一个尖点 ∞ , 一般的同余子群 Γ 只有有限多个尖点. 

证明 对于互素的 $a, c \in \mathbb{Z}$, 存在 $b, d \in \mathbb{Z}$ 使得 $ad - bc = 1$, 于是 $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = a/c$, 因此只有一个轨道. 一般地, $\mathrm{SL}(2, \mathbb{Z}) = \sqcup_{i=1}^k \Gamma g_i$, 因此只有有限多个尖点 $g_i \infty$. \square

Γ 在 \mathfrak{H} 上的作用得到一个开的黎曼面, 通过添加尖点可以将其紧化, 从而得到一个紧黎曼面. 具体如何边界点处的坐标卡此处不做详解, 感兴趣的可以阅读 [13].

我们记 $X_\Gamma = (\Gamma \backslash \mathfrak{H})^*$ 为相应的紧化, 称之为**模曲线**. 记 $X(N), X_1(N), X_0(N)$ 为相应的同余子群对应的模曲线.

§4.3.3 模形式

设 f 为上半平面的全纯函数. 如果 f 满足 $f(\tau + N) = f(\tau)$, 则通过 $q_N = e^{2\pi i \tau / N} : \mathcal{H} \rightarrow U(0, 1)$, f 在 $z = 0 \in U(0, 1)$ 的展开拉回变成

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q_N^n.$$

若 $a_n = 0, \forall n < 0$, 称 f 在 ∞ **全纯**; 若 $a_n = 0, \forall n \leq 0$, 称 f 在 ∞ **消没**.

考虑 $r \in \mathbb{Q}$, 则存在 $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ 使得 $\gamma \infty = r$. 如果 $f(\gamma z)$ 在 ∞ 全纯/消没, 则称 f 在 r 处全纯/消没.

对于 $k \in \mathbb{Z}, \gamma \in \mathrm{GL}(2, \mathbb{R})^+$, 定义

$$f|_k \gamma(\tau) = (\det \gamma)^{k/2} (c\tau + d)^{-k} f(\gamma\tau).$$

命题 4.34

$$f|_k(\gamma_1 \gamma_2) = (f|_k \gamma_1)|_k \gamma_2.$$



定义 4.35 (模形式)

设 k 是整数. 如果上半平面的全纯函数 f 满足对任意 $\gamma \in \Gamma_0(N)$, $f|_k \gamma = f$, 且在所有的尖点处全纯, 则称 f 为**权 k , 级 $\Gamma_0(N)$ 的模形式**. 若 f 在所有的尖点处消没, 则称 f 为**尖点形式**. 分别记相应的空间为 $M_k(\Gamma), S_k(\Gamma)$. 当 $\Gamma = \mathrm{SL}(2, \mathbb{Z})$ 时我们省略 Γ .



如果 $-I \in \Gamma$, 则容易知道仅当 $k \in 2\mathbb{Z}$ 时存在权 k 级 Γ 的非零模形式.

考虑 $f d\tau^{\otimes k}$. 任意 $\alpha \in \mathrm{GL}(2, \mathbb{R})^+$ 都给出了 \mathcal{H} 上的全纯自同构, 从而诱导了微分形式的拉回 α^* ,

$$\alpha^*(f d\tau^{\otimes k}) = (f \circ \alpha)(d\alpha\tau)^{\otimes k} = (f|_{2k} \alpha) d\tau^{\otimes k}.$$

因此 f 是权 $2k$ 级 Γ 的模形式当且仅当 $f d\tau^{\otimes k}$ 在 Γ 作用下不变.

例题 4.4 设 k 为正整数, $\Gamma \subseteq \mathbb{C}$ 为一个格. 定义

$$G_{2k}(\Lambda) = \sum_{0 \neq \omega \in \Lambda} \omega^{-2k}.$$

定义 $G_{2k}(\tau) = G_{2k}(\mathbb{Z} + \mathbb{Z}\tau), \tau \in \mathcal{H}$. 容易看出 $k \geq 2$ 时它绝对收敛.

命题 4.36

当 $k \geq 2$ 时,

$$G_{2k}(\tau) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n, \quad q = e^{2\pi i \tau},$$

其中 $\sigma_\ell(n) = \sum_{0 < d|n} d^\ell$. 因此 $G_{2k} \in M_{2k}(\Gamma(1))$.



证明 通过对

$$\frac{\sin(\pi s)}{\pi s} = \prod_{n=1}^{\infty} \left(1 - \frac{s^2}{n^2}\right)$$

两边同时取 $\frac{d \log}{ds}$ 得到恒等式

$$\pi \cot \pi \tau = \frac{1}{\tau} + \sum_{m=1}^{\infty} \left(\frac{1}{\tau + m} + \frac{1}{\tau - m} \right),$$

其中右侧在紧集上一致收敛. 令 $q = e^{2\pi i \tau}$, 则 $|q| < 1$,

$$\pi \cot \pi \tau = i\pi \frac{q+1}{q-1} = i\pi - \frac{2\pi i}{1-q} = i\pi - 2\pi i \sum_{d=0}^{\infty} q^d.$$

因此

$$\frac{1}{\tau} + \sum_{m=1}^{\infty} \left(\frac{1}{\tau + m} + \frac{1}{\tau - m} \right) = i\pi - 2\pi i \sum_{d=0}^{\infty} q^d,$$

两边求 $2k-1$ 次导数,

$$\sum_{m=-\infty}^{\infty} \frac{1}{(\tau + m)^{2k}} = \frac{1}{(2k-1)!} (2\pi i)^{2k} \sum_{d=1}^{\infty} d^{2k-1} q^d.$$

因此

$$\begin{aligned} G_{2k}(\tau) &= \sum_{(m,n) \neq (0,0)} (n\tau + m)^{-2k} \\ &= \sum_{m \neq 0} m^{-2k} + \sum_{n \neq 0} \sum_{m=-\infty}^{\infty} (n\tau + m)^{-2k} \\ &= 2\zeta(2k) + 2 \sum_{n=1}^{\infty} \sum_{m=-\infty}^{\infty} (n\tau + m)^{-2k} \\ &= 2\zeta(2k) + 2 \frac{1}{(2k-1)!} (2\pi i)^{2k} \sum_{d=1}^{\infty} \sum_{a=1}^{\infty} d^{2k-1} q^{da} \\ &= 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n. \end{aligned}$$

命题得证. □

定义 4.37 (艾森斯坦级数)

定义

$$E_{2k}(\tau) = \frac{1}{2} \sum_{(c,d)=1} (c\tau + d)^{-2k}.$$

容易证明 $G_{2k} = 2\zeta(2k)E_{2k}$, 因此 E_{2k} 的傅里叶展开常数项为 1.



命题 4.38

我们有

$$E_{2k}(\tau) = 1 - \frac{2k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n.$$



定义 4.39 (拉马努金 Δ 函数)

定义

$$\Delta = \frac{(2\pi)^{12}}{1728}(E_4^3 - E_6^2) = (2\pi)^{12}(q - 24q^2 + 252q^3 - 1472q^4 + \cdots) \in S_{12}(\Gamma(1)).$$



定理 4.40

设 $M = \bigoplus_k M_k$ 为模形式形成的分次代数, 则 $M = \mathbb{C}[E_4, E_6]$. 特别地, $k < 0$ 时 $M_k = 0$; $k \geq 0$ 时,

$$\dim M_k = \begin{cases} \left[\frac{k}{12}\right] + 1, & k \not\equiv 2 \pmod{12}; \\ \left[\frac{k}{12}\right], & k \equiv 2 \pmod{12}. \end{cases}$$



命题 4.41

我们有

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

§4.3.4 尖形式的 L 函数

设 $f \in S_k$ 是一个尖形式, 它的傅里叶展开为

$$f(\tau) = \sum_{n=1}^{\infty} c_n q^n.$$

定义 f 的 L 函数为

$$L(s, f) := \sum_{n=1}^{\infty} c_n n^{-s}.$$

定义 4.42 (梅林变换)

函数 $F: (0, \infty) \rightarrow \mathbb{C}$ 的梅林变换为

$$g(s) = \int_0^{\infty} F(t) t^s \frac{dt}{t}.$$



设 $\tau = \rho + i\sigma$. 考虑 $f(i\sigma)$ 的梅林变换, 我们暂时不考虑收敛性的问题. 此时它的梅林变换为

$$\begin{aligned} g(s) &:= \int_0^{\infty} f(i\sigma) \sigma^s \frac{d\sigma}{\sigma} = \int_0^{\infty} \sum_{n=1}^{\infty} c_n e^{-2\pi n\sigma} \sigma^s \frac{d\sigma}{\sigma} \\ &= \sum_{n=1}^{\infty} c_n \int_0^{\infty} e^{-t(2\pi n)^{-s}} t^s \frac{dt}{t} \\ &= (2\pi)^{-s} \Gamma(s) \sum_{n=1}^{\infty} c_n n^{-s} = (2\pi)^{-s} \Gamma(s) L(s, f). \end{aligned}$$

引理 4.43

$\varphi(\tau) = |f(\tau)|\sigma^{k/2}$ 在 \mathcal{H} 上有界且在 $SL(2, \mathbb{Z})$ 作用下不变. 由此可知 $|c_n| \leq Cn^{k/2}$.



证明 由 $|q| < 1$ 时 $f(\tau) = \sum_{n=0}^{\infty} c_n q^n$ 收敛可知 $|c_n| < C(3/4)^n/4$, 因此当 $|q| < \frac{1}{2}$ 时, $|f(\tau)| \leq C|q|$, 即

$$|f(\tau)| \leq C e^{-2\pi\sigma}, \quad \sigma \geq \frac{1}{2\pi} \log 2.$$

因此当 τ 在 $\mathrm{SL}(2, \mathbb{Z})$ 基本区域 R 中趋于 ∞ 时, $\varphi(\tau) = |f(\tau)|\sigma^{k/2} \rightarrow 0$. 而 φ 是连续的, R 中 $\sigma \leq \frac{1}{2\pi} \log 2$ 部分是紧的, 因此 φ 在 R 上有界. 容易验证 φ 是 $\mathrm{SL}(2, \mathbb{Z})$ 不变的, 因此 φ 在 \mathcal{H} 上有界.

我们有 $c_n = \int_{-\frac{1}{2}}^{\frac{1}{2}} f(\tau) e^{-2\pi i n \tau} d\rho$, 因此 $|c_n| \leq C \sigma^{-k/2} e^{2\pi n \sigma}$, $\forall \sigma > 0$. 取 $\sigma = 1/n$, 则 $|c_n| \leq C e^{2\pi} n^{k/2}$.

□

定理 4.44

若 $f \in S_k$, 则 $L(s, f)$ 在 $\mathrm{Res} > k/2 + 1$ 上收敛, 且可以解析延拓至复平面. 我们有函数方程

$$\Lambda(s, f) = (-1)^{k/2} \Lambda(k - s, f),$$

其中 $\Lambda(s, f) = (2\pi)^{-s} \Gamma(s) L(s, f)$.



证明 由 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ 可知 $f(-1/\tau) = \tau^k f(\tau)$, 因此

$$f(i/\sigma) = i^k \sigma^k f(i\sigma).$$

由 $|c_n| \leq n^{k/2}$ 知

$$\Lambda(s, f) = \int_0^\infty f(i\sigma) \sigma^{s-1} d\sigma$$

在 $\mathrm{Res} > k/2 + 1$ 时收敛. 和狄利克雷特征的 L 函数情形类似,

$$\int_1^\infty f(i\sigma) \sigma^{s-1} d\sigma$$

对任意 s 收敛, 且

$$\int_0^1 f(i\sigma) \sigma^{s-1} d\sigma = i^k \int_1^\infty f(i\sigma) \sigma^{k-s-1} d\sigma$$

右侧对任意 s 收敛. 因此我们得到了 $\Lambda(s, f)$ 的解析延拓和函数方程. 由于 Γ 没有零点, 因此 $L(s, f)$ 全纯. □

设 $f \in S_k(\Gamma_0(N))$ 是一个级 N 的尖形式, 它的傅里叶展开为

$$f(\tau) = \sum_{n=1}^{\infty} c_n q^n.$$

定义 f 的 L 函数为

$$L(s, f) := \sum_{n=1}^{\infty} c_n n^{-s}.$$

同样的, 我们有

$$\int_0^\infty f(i\sigma) \sigma^s \frac{d\sigma}{\sigma} = (2\pi)^{-s} \Gamma(s) L(s, f).$$

引理 4.45

$\varphi(\tau) = |f(\tau)|\sigma^{k/2}$ 在 \mathcal{H} 上有界且在 $\Gamma_0(N)$ 作用下不变. 由此可知 $|c_n| \leq C n^{k/2}$.



证明 考虑 $\Gamma_0(N)$ 的基本区域 R_N , 其中的尖点为 $\beta^{-1}\infty$. 显然

$$\beta^{-1} \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \beta \in \Gamma_0(N),$$

因此 $f|_k \beta^{-1} \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \beta = f$, 即

$$f|_k \beta^{-1}(\tau + N) = f|_k \beta^{-1}(\tau),$$

于是我们有傅里叶展开

$$f|_k\beta^{-1}(\tau) = \sum_{n=1}^{\infty} c_n^{(\beta)} q_N^n.$$

和上一节情形类似, $\varphi(\beta^{-1}\tau) = |f|_k\beta^{-1}(\tau)|(\operatorname{Im}\tau)^{k/2}$ 在 $\operatorname{Im}\tau \geq 2$ 上有界. 而 R_N 去掉每个尖点的一个小领域是紧集, 从而 $\varphi(\tau)$ 在整个 R_N 上有界. 容易验证 φ 是 $\Gamma_0(N)$ 不变的, 因此 φ 在 \mathcal{H} 上有界. 其余部分同上一节. \square

定义 4.46 (Atkin-Lehner 算子)

设 $\alpha_N = \begin{pmatrix} 0 & 1 \\ N & 0 \end{pmatrix}$. 设 $f \in M_k(\Gamma_0(N))$, 我们称 $w_N f = f|_k\alpha_N$ 为 **Atkin-Lehner 算子**.



对于 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\alpha_N \gamma \alpha_N^{-1} = \begin{pmatrix} d & -c/N \\ -Nb & a \end{pmatrix}$. 因此

$$\alpha_N \Gamma_0(N) \alpha_N^{-1} \subseteq \Gamma_0(N).$$

对于 $\gamma \in \Gamma_0(N)$,

$$(f|_k\alpha_N)|_k\gamma = (f|_k\alpha_N^{-1}\gamma\alpha_N^{-1})|_k\alpha_N = f|_k\alpha_N,$$

因此 $w_N f$ 也是权 k 级 N 的函数.

命题 4.47

w_N 将 $M_k(\Gamma_0(N))$ 映到 $M_k(\Gamma_0(N))$, $S_k(\Gamma_0(N))$ 映到 $S_k(\Gamma_0(N))$.



证明 直接计算可知

$$\begin{pmatrix} 1 & N^2 \\ & 1 \end{pmatrix} \in \beta \alpha_N^{-1} \Gamma_0(N) \alpha_N \beta^{-1}, \quad \beta \in \operatorname{SL}(2, \mathbb{Z}).$$

因此

$$(w_N f)|_k\beta^{-1}(\tau) = \sum_{n=0}^{\infty} c_n^{(\beta)} q_{N^2}^n.$$

但 $w_N f$ 实际上是权 k 级 N 的全纯函数, 因此 $c_n^{(\beta)} = 0, N \nmid n$. 于是 $w_N f$ 在 $\beta^{-1}\infty$ 全纯, 从而它是模形式. 同理可知 $w_N : S_k(\Gamma_0(N)) \rightarrow S_k(\Gamma_0(N))$. \square

显然 $w_N^2 = 1$, 因此 w_N 是一个内卷, 从而它诱导了分解

$$S_k(\Gamma_0(N)) = S_k^+(\Gamma_0(N)) \oplus S_k^-(\Gamma_0(N)),$$

其中 $S_k^\pm(\Gamma_0(N))$ 上 w_N 特征值为 ± 1 .

定理 4.48

若 $f \in S_k^\varepsilon(\Gamma_0(N))$, 则 $L(s, f)$ 在 $\operatorname{Res} > k/2 + 1$ 上收敛, 且可以解析延拓至复平面. 我们有函数方程

$$\Lambda(s, f) = \varepsilon(-1)^{k/2} \Lambda(k-s, f),$$

其中 $\Lambda(s, f) = N^{s/2} (2\pi)^{-s} \Gamma(s) L(s, f)$.



证明 和上一节类似, 由 c_n 的估计可知 $L(s, f)$ 在 $\operatorname{Res} > k/2 + 1$ 时收敛. 由于 $w_N f = \varepsilon f$,

$$f\left(\frac{i}{N\sigma}\right) = \varepsilon N^{k/2} i^k \sigma^k f(i\sigma).$$

我们有

$$\Lambda(s, f) = N^{s/2} \int_0^\infty f(i\sigma)\sigma^{s-1} d\sigma.$$

我们知道

$$\int_{1/\sqrt{N}}^\infty f(i\sigma)\sigma^{s-1} d\sigma$$

对任意 s 收敛, 且


$$\int_0^{1/\sqrt{N}} f(i\sigma)\sigma^{s-1} d\sigma = \varepsilon N^{k/2-s} i^k \int_{1/\sqrt{N}}^\infty f(i\sigma)\sigma^{k-s-1} d\sigma$$

右侧对任意 s 收敛. 因此我们得到了 $\Lambda(s, f)$ 的解析延拓和函数方程. □


§4.4 椭圆曲线

§4.4.1 代数曲线的亏格

定义 4.49 (代数曲线)

所谓的代数闭域 \bar{K} 上的**代数曲线**, 是指 \bar{K} 上有限多个多项式的公共零点, 且其在 \bar{K} 之上的有理函数全体 $\bar{K}(C)$ 的超越维数为 1. 如果我们考虑的是射影空间, 则是指有限多个齐次多项式的公共零点, 且其交某个 $\mathbb{A}^n \subset \mathbb{P}^n$ 为 \mathbb{A}^n 中的曲线. 

定义 4.50 (光滑和奇异)

设曲线 C 由 $\bar{K}[X_1, \dots, X_n]$ 上的方程给出, 则零化 C 的多项式全体构成 $\bar{K}[X_1, \dots, X_n]$ 的理想 I . 如果 I 可以由 K 上的多项式生成, 称 C 定义在 K 上. 设 f_1, \dots, f_m 生成 I , 则曲线 C 在点 P 处**光滑**是指 $\left(\frac{\partial f_i}{\partial X_j}\right)_{ij}$ 的秩为 $n-1$. 不光滑的点称之为**奇异点**. 若 C 无奇异点, 称 C 光滑. 

例题 4.5 设 $C: y^2 = x^3 + x$, 则 C 的奇异点满足 $2y = 3x^2 + 1 = 0$, 因此当 K 特征为 2 时, $(1, 0)$ 是奇异点; 其它情形 C 是光滑的.

设 C 是一条射影光滑曲线, P 是 C 上一个点. 称

$$\bar{K}[V]_P = \{f/g \in \bar{K}(V) \mid g(P) \neq 0\}$$

为 P 处**局部环**, 它是一个离散赋值环, 因此我们有规范化赋值

$$\text{ord}_P: \bar{K}(C) \rightarrow \mathbb{Z} \cup \{\infty\}.$$

我们称形式有限和 $\sum_P n_P(P)$ 为**除子**. 记

$$\text{div}(f) = \sum_P \text{ord}_P(f)(P), \quad f \neq 0$$

是其对应的除子, 称之为**主除子**. 对于射影曲线, 其上处处全纯的函数只可能是常值函数, 换言之 $\text{div}(f) \geq 0 \iff f \in \bar{K}^\times$. 这个 \geq 表示每个系数都 \geq .

考虑 $\omega \in \Omega_{\bar{K}(C)/\bar{K}}$, 则在每个 P 处, 设 t 是它的局部环的素元, 则存在 f 使得 $\omega = f dt$, 定义

$$\text{ord}_P(\omega) := \text{ord}_P(f), \quad \text{div}(\omega) := \sum_P \text{ord}_P(\omega)(P).$$

如果 $\text{div}(\omega) \geq 0$, 称 ω 是**全纯微分**. 全纯微分全体构成有限维 \bar{K} 向量空间, 其维数被称为 C 的**亏格**, 记

为 $g = g_C$.

例 4.6 (1) $C = \mathbb{P}^1$. 当 $P = \alpha \in \overline{K}$ 时, $t - \alpha$ 是素元, 从而 $dt = d(t - \alpha)$ 阶为 0. 当 $P = \infty$ 时, $1/t$ 是素元, $dt = -t^{-2}d(1/t)$ 阶为 -2 . 因此

$$\operatorname{div}(dt) = -2(\infty).$$

(2) $C: y^2 = (x - e_1)(x - e_2)(x - e_3)$, e_i 两两不同. 当 $P = P_i = (e_i, 0)$ 时, $\operatorname{ord}(y) = 1, \operatorname{ord}(x - e_i) = 2$, 从而 $dx = d(x - e_i)$ 阶为 1. 当 $P = \infty = [0:1:0]$ 时, $\operatorname{ord}(y) = -3, \operatorname{ord}(x) = -2, \operatorname{ord}(x/y) = 1$, 从而 dx 阶为 3. 因此

$$\operatorname{div}(dx) = (P_1) + (P_2) + (P_3) - 3(\infty).$$

由此可知 dx/y 是全纯微分, 实际上此时全纯微分是一维的, 即 $g = 1$.

§4.4.2 椭圆曲线等分点

定义 4.51 (椭圆曲线)

K 上的椭圆曲线 (E, O) 是指 K 上的亏格 1 的光滑曲线 E 和一个点 $O \in E(K)$.



记 $\mathcal{L}(D) = \{f \mid \operatorname{div}(f) \geq D\} \cup \{0\}$, 则通过黎曼-Roch 定理可知

$$\dim \mathcal{L}(n(O)) = n.$$

设 $1, x$ 生成 $\mathcal{L}(2(O))$, $1, x, y$ 生成 $\mathcal{L}(3(O))$, 则 $1, x, y, x^2, xy, y^2, x^3$ 生成 $\mathcal{L}(6(O))$, 因此它们线性相关. 从而 $(x, y): E \rightarrow \mathbb{P}^2$ 且

$$E: y^2 + a_1y + a_3 = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K.$$

该形式被称为魏尔斯特拉斯方程. 此时 O 对应 $[0:1:0] \in \mathbb{P}^2$, 具体见 [19, §III.3]. 由于 E 是光滑的, 因此其判别式 Δ 非零.

容易看出 $E(\mathbb{R})$ 拥有 1 或 2 个连通分支. 我们来考虑 $E(\mathbb{C})$. 设 $\Lambda \subseteq \mathbb{C}$ 为复平面上一个格. 定义

$$\begin{aligned} g_2(\Lambda) &= 60G_4(\Lambda), \quad g_3(\Lambda) = 140G_6(\Lambda), \\ \wp(z, \Lambda) &= \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right), \end{aligned}$$

则 \wp 是 Λ 周期的, 且极点为 $\omega \in \Lambda$.

定理 4.52

对于椭圆曲线 $E/\mathbb{C}: y^2 = 4x^3 - g_2x - g_3$, 存在格 Λ 使得 $g_2 = g_2(\Lambda), g_3 = g_3(\Lambda)$, 且我们有连续同构

$$\begin{aligned} \mathbb{C}/\Lambda &\xrightarrow{\sim} E(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)) = [\wp(z) : \wp'(z) : 1]. \end{aligned}$$

容易看出 0 映为 $\mathbb{P}^2(\mathbb{C})$ 的无穷远点 $\infty = [0:1:0] \in E(\mathbb{C})$.



显然 \mathbb{C}/Λ 有一个自然地群结构, 这给出了 $E(\mathbb{C})$ 上的群结构. 在魏尔斯特拉斯方程下, 设 $A, B \in E(\mathbb{C})$, 则 $C = A + B$ 关于 x 轴的对称点 $-C$ 和 AB 在同一条直线上. AB 重合时取切线, AB 垂直 x 轴时 $A + B = O = \infty$. 这种加法定义方式对于任何域上的椭圆曲线都是良定的, 即 $E(K)$ 总形成一个交

换群.

如果我们换一个 K 点 O' , 则 $(E, O) \xrightarrow{\sim} (E, O')$, $P \mapsto P + O' - O$ 是群同构, 所以我们可以任取一个 $E(K)$ 点, 这并不影响 E 本质的结构.

$E(\mathbb{C})$ 和环面 \mathbb{C}/Λ 同构, 从而它的 n 等分点

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

很容易看出 $E[n]$ 的坐标均为代数数, 换言之 $E[n] \subseteq E(\overline{\mathbb{Q}})$. 实际上, $\text{char}K \nmid n$ 时, 总有 $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^{\oplus 2}$.

设 p 为素数, 考虑 p 倍映射 $E[p^{n+1}] \rightarrow E[p^n]$, 则我们称

$$T_p(E) = \varprojlim E[p^n]$$

为 E 的泰特模, 它是秩为 2 的自由 \mathbb{Z}_p 模. 固定它的一组基 e_1, e_2 , 则 $G_{\mathbb{Q}}$ 的作用在这组基下的矩阵形式给出了表示

$$\rho_p : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{Z}_p).$$

定理 4.53

设 K_{p^∞} 为包含 $E[p^\infty]$ 的最小的域, 即 $\text{Ker } \rho_p$ 的固定域. 设 E 在素数 $\ell \neq p$ 处为好约化, 则 ℓ 在 K_{p^∞}/\mathbb{Q} 非分歧. 设 Frob_ℓ 为 ℓ 的弗罗贝尼乌斯共轭类, 则

$$\det(\rho_p(\text{Frob}_\ell)) = \ell.$$

设 $a_\ell = \text{Tr}(\rho_p(\text{Frob}_\ell))$, 则

$$\#E(\mathbb{F}_\ell) = \ell + 1 - a_\ell.$$

我们有 $|a_\ell| \leq 2\sqrt{\ell}$.



我们在下一节中叙述约化的定义.

定理 4.54 (Mordell 定理)

$E(\mathbb{Q})$ 是有限生成交换群.



$E(\mathbb{Q})$ 的有限部分只可能是 $\mathbb{Z}/n\mathbb{Z}$, $1 \leq n \leq 10$ 或 $n = 12$; $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $n = 2, 4, 6, 8$. $E(\mathbb{Q})$ 的秩被称为 E 的秩.

§4.4.3 椭圆曲线的 L 函数

同一条椭圆曲线对应的魏尔斯特拉斯方程可以 (也只可能) 相差 F 上的线性变换. 当 $F = \mathbb{Q}$ 是有理函数域时, 在不同的表达形式中, 存在判别式的绝对值最小的那个整系数方程, 我们称之为极小魏尔斯特拉斯模型 (Néron). 例如 $y^2 = x^3 - x$, $y^2 + y = x^3 - x^2$.

考虑有理数域上椭圆曲线 E 的极小魏尔斯特拉斯模型和相应的判别式 Δ . 对于任意素数 p , 我们将该方程系数看成是 \mathbb{F}_p 上, 则 $p \nmid \Delta$ 时该曲线是仍然是光滑的, 它是 \mathbb{F}_p 上的椭圆曲线, 我们称之为好约化; 否则称之为坏约化. 假设 E 在 p 处有坏约化, 如果在奇点处只有一条切线 (尖点), 称之为加性约化; 如果有两条不同切线 (结点), 称之为乘性约化, 此时若切线斜率位于 \mathbb{F}_p , 称之为分裂乘性约化, 否则称之为非分裂乘性约化.

命题 4.55

若 p 为加性约化, $E_{\text{ns}}(\mathbb{F}_p) \cong \mathbb{F}_p$; 若 p 为分裂乘性约化, $E_{\text{ns}}(\mathbb{F}_p) \cong \mathbb{F}_p^\times$; 若 p 为非分裂乘性约化, $E_{\text{ns}}(\mathbb{F}_p) \cong \mathbb{F}_{p^2}^{\mathbb{N}=1}$. 这里 E_{ns} 表示光滑部分.



例题 4.7 $y^2 = x^3 - x$ 在 $p = 2$ 处为加性约化, 其余素数处为好约化. $y^2 + y = x^3 - x$ 在 $p = 11$ 处为分裂乘性约化, 其余素数处为好约化.

对于 \mathbb{Q} 上的椭圆曲线 E , 定义

$$L_p(s, E) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1}, & \text{如果 } p \text{ 处为好约化;} \\ (1 - p^{-s})^{-1}, & \text{如果 } p \text{ 处为分裂乘性约化;} \\ (1 + p^{-s})^{-1}, & \text{如果 } p \text{ 处为非分裂乘性约化;} \\ 1, & \text{如果 } p \text{ 处为加性约化.} \end{cases}$$

实际上, 在坏约化处 $L_p(s, E) = (1 - a_p p^{-s})^{-1}$, $a_p = p + 1 - \#E(\mathbb{F}_p)$. 定义

$$L(s, E) = \prod_p L_p(s, E).$$

命题 4.56

$L(s, E)$ 在 $\text{Re}(s) > 3/2$ 时绝对收敛.



证明 对于好约化 p , 由于 $|a_p| \leq 2\sqrt{p}$, 因此 $X^2 - a_p X + p = 0$ 的根复共轭, 设为 $\alpha_p, \bar{\alpha}_p$. 设

$$L(s, E) = \sum_{n=1}^{\infty} a_n n^{-s},$$

则 $a_p^k = \sum_{i=0}^k \alpha_p^i \bar{\alpha}_p^{k-i}$, $|a_p^k| \leq (k+1)p^{k/2}$. 显然这对坏约化也成立, 于是

$$|a_n| \leq \sqrt{n} \prod_p (e_p + 1) \leq n^{\frac{1}{2} + \varepsilon}, \quad n \rightarrow \infty.$$

由此可知 $\text{Re}(s) > 3/2$ 时, $L(s, E)$ 绝对收敛. □

它可以解析延拓至 \mathbb{C} 且具有函数方程 $s \leftrightarrow 2 - s$, 这些依赖于它的模性, 我们将在下一节叙述.

著名的伯奇-斯温纳顿-戴尔猜想断言

$$\text{ord}_{s=1} L(s, E) = \text{rank}_{\mathbb{Z}} E(\mathbb{Q}).$$

我们可以将其视为

$$\text{ord}_{s=0} \zeta_K(s) = \text{rank } \mathcal{O}_K^\times$$

的一种类比. 同时他们还给出了 $L(s, E)$ 在 $s = 1$ 处泰勒展开的首项系数与椭圆曲线的算术量之间的联系. 解析秩 (左端) 为 0 和 1 的情形人们已经基本完全解决了, 但大于等于 2 的情形人们知之甚少.

§4.5 尖形式与椭圆曲线

§4.5.1 紧黎曼面

设 $f \in S_2(\Gamma_0(N))$, 则 $f(\zeta) d\zeta$ 是 $\Gamma_0(N)$ 不变的. 固定 $\tau_0 \in \mathcal{H}$, 定义

$$F(\tau) = \int_{\tau_0}^{\tau} f(\zeta) d\zeta.$$

由于 f 是全纯的, 因此该积分不依赖于路径的选取. 对于 $\gamma \in \Gamma_0(N)$, 我们有

$$F(\gamma(\tau)) = F(\tau) + \int_{\tau_0}^{\gamma\tau_0} f(\zeta) d\zeta.$$

令

$$\Phi_f(\gamma) = \int_{\tau_0}^{\gamma\tau_0} f(\zeta) d\zeta.$$

由 $f(\zeta) d\zeta$ 的不变性易知 $\Phi_f(\gamma)$ 不依赖于 τ_0 的选取.

命题 4.57

对于 $f \in S_2(\Gamma_0(N))$, Φ_f 是 $\Gamma_0(N)$ 到 \mathbb{C} 的群同态.



证明

$$\Phi_f(\gamma_1\gamma_2) = \int_{\tau_0}^{\gamma_1\gamma_2\tau_0} f(\zeta) d\zeta = \int_{\tau_0}^{\gamma_1\tau_0} f(\zeta) d\zeta + \int_{\gamma_1\tau_0}^{\gamma_1\gamma_2\tau_0} f(\zeta) d\zeta = \Phi_f(\gamma_1) + \Phi_f(\gamma_2).$$

□

一般地, 设 X 是紧黎曼面, 亏格为 $g \geq 1$, 则 $H_1(X, \mathbb{Z})$ 是秩 $2g$ 的自由交换群. 设 $a_1, \dots, a_g, b_1, \dots, b_g$ 为其中一组基并满足特定的相交条件.

命题 4.58

设 X 是紧黎曼面, 亏格为 $g \geq 1$, $\omega_1, \dots, \omega_g$ 是 X 上全纯微分的一组基, 则向量

$$\begin{pmatrix} \int_{c_k} \omega_1 \\ \vdots \\ \int_{c_k} \omega_g \end{pmatrix} \in \mathbb{C}^g$$

在 \mathbb{R} 上线性无关.



因此它们生成 \mathbb{C}^g 中的一个完全格 $\Lambda(X)$, 显然这不依赖 $\{c_k\}$ 的选取. 如果换一组基 $\{\omega_j\}$, 则 $\Lambda(X)$ 会相差一个 $\text{GL}(g, \mathbb{C})$ 的作用.

X 的雅克比簇是指 g 维复环面 $J(X) = \mathbb{C}^g / \Lambda(X)$. 固定一个点 $x_0 \in X$, 令

$$\Phi : X \rightarrow J(X), \quad \Phi(x) = \left\{ \int_{x_0}^x \omega_j \right\}_{j=1}^g.$$

对于 $X = X_0(N)$, Φ 就是 $\{\Phi_f\}$, 其中 f 是 $S_2(\Gamma_0(N))$ 的一组基.

由于 $J(X)$ 是一个群, 容易将 Φ 线性扩充到 X 的除子上, 即 $\Phi : \text{Div}(X) \rightarrow J(X)$. 我们定义

$$\deg\left(\sum n_P(P)\right) = \sum n_P,$$

则 $\deg(\text{div}(f)) = 0$.

定理 4.59 (阿贝尔定理)

设 X 是紧黎曼面, 亏格为 $g \geq 1$. 除子 D 是主除子当且仅当 $\deg(D) = 0$ 且 $\Phi(D) = 0 \in J(X)$.

**推论 4.60**

- (1) 如果 $g = 1$, 则 $\Phi: X \rightarrow J(X)$ 是双全纯同构.
 (2) 如果 $g > 1$, 则 $\Phi: X \rightarrow J(X)$ 是单全纯映射, 它的像是 $J(X)$ 的子流形.



记 $K(X)$ 为 X 上亚纯函数全体.

定理 4.61

设 X 是紧黎曼面, 亏格为 $g \geq 0$, $x \in K(X)$ 非常值, 则存在 $y \in K(X)$ 非常值, 以及不可约多项式 $P(x, y) = 0$, 使得

$$K(X) \cong \mathbb{C}(x)[y]/(P(x, y)).$$

因此 X/\mathbb{C} 是代数曲线.

**§4.5.2 模函数**

设

$$j(\tau) = \frac{1728g_2(\tau)^3}{\Delta(\tau)} = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c_n q^n,$$

则它是权 0 的模函数, 因此 $j \in K(X_0(N))$. 由于

$$\Delta(\tau) = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24},$$

因此 Δ 在 \mathcal{H} 上无零点, 从而 j 在 \mathcal{H} 上全纯.

命题 4.62

$j: \mathrm{SL}(2, \mathbb{Z}) \backslash \mathcal{H} \rightarrow \mathbb{C}$ 是满射.



证明 固定 $z_0 \in \mathbb{C}$, 则 $\deg(\mathrm{div}(j - z_0)) = 0$. 由于 $\pi(\infty)$ 是它唯一的极点, $\pi: \mathcal{H}^* \rightarrow X(1)$, 因此

$$\mathrm{div}(j - z_0) = p - \pi(\infty).$$

从而 $j(p) = z_0$, j 是满射. □

引理 4.63

如果 f 权 0 且在 \mathcal{H} 上全纯, 设 $f(\tau) = \sum_{n=-M}^{\infty} c_n q^n$. 则 f 是 j 的多项式, 且系数落在 $\mathbb{Z}[c_n: n \in \mathbb{Z}]$ 中.



证明 若 $M = 0$, 则 f 是常数. 假设对 $M - 1$ 命题成立, 则 $f - c_{-M}j^M$ 在 $\pi(\infty)$ 是至多 $M - 1$ 阶极点, 从而由归纳假设可知命题成立. □

定理 4.64

$K(X_0(1)) = \mathbb{C}(j)$.



证明 由于 $f \in K(X_0(1))$ 只有有限多极点, 因此

$$f(\tau) \cdot \prod_{\text{ord}_P(f) < 0} (j(\tau) - j(p))^{-\text{ord}_P(f)}$$

仅在 $\pi(\infty)$ 有极点, 从而它是 j 的多项式. □

对于一般的 N , 令 $j_N = j \circ \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$, 则我们有

定理 4.65

$$K(X_0(N)) = \mathbb{C}(j, j_N).$$



实际上, j, j_N 满足的多项式可以为 \mathbb{Q} 系数的, 从而 $X_0(N)$ 可以视为 \mathbb{Q} 上的代数曲线.

§4.5.3 从尖形式到椭圆曲线

设 $M(n)$ 为行列式为 n 的整矩阵全体,

$$M(n, N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = n, N \mid c, (a, N) = 1 \right\}.$$

设 $\{\alpha_i\}$ 为 $\Gamma_0(N)$ 关于 $M(n, N)$ 的右陪集代表元. 对于 $f \in M_k(\Gamma_0(N))$, 定义

$$T_k(n)f = n^{k/2-1} \sum_i f|_k \alpha_i.$$

称

$$T_k(n) : M_k(\Gamma_0(N)) \rightarrow M_k(\Gamma_0(N))$$

为赫克算子.

定理 4.66 (赫克定理)

在 $M_k(\Gamma_0(N))$ 上, 我们有

(1) 若 $p \nmid N$,

$$T_k(p^r)T_k(p) = T_k(p^{r+1}) + p^{k-1}T_k(p^{r-1}).$$

(2) 若 $p \mid N$,

$$T_k(p^r) = T_k(p)^r.$$

(3) 若 $(m, n) = 1$, 则 $T_k(m)T_k(n) = T_k(mn)$.

(4) $T_k(n), n \geq 1$ 生成的代数可以由 $T_k(p)$ 生成, 它是交换代数.

$(n, N) = 1$ 时, $T_k(n)$ 将尖形式映为尖形式.



命题 4.67

如果 $f \in S_k(\Gamma_0(N))$ 是所有 $T_k(n)$ 的特征形式, $T_k(n)f = \lambda(n)f$, 则其傅里叶系数

$$c_n = \lambda(n)c_1.$$



假设 $c_1 = 1$, 则由赫克算子的运算性质可知

$$L(s, f) = \prod_{p \mid N} (1 - c_p p^{-s})^{-1} \prod_{p \nmid N} (1 - c_p^{-s} + p^{k-1-2s})^{-1}, \quad \text{Re}(s) > k/2 + 1.$$

对于 $f \in S_k(\Gamma_0(N/r)), 1 < r \mid N$, 我们有 $f(\tau), f(r\tau) \in S_k(\Gamma_0(N))$. 所谓的**新形式**, 是指不从上述方式

得到的赫克算子的特征尖形式. 如果两个特征形式的特征值均相同, 称之**等价**.

定理 4.68 (Atkin-Lehner 定理)

如果 $f \in S_k(\Gamma_0(N))$ 是新形式, 则它的等价类是一维的.



定理 4.69

设 $f(\tau) = \sum_{n=1}^{\infty} c_n e^{2\pi i n \tau} \in S_2(\Gamma_0(N))$ 是新形式且 $c_1 = 1$. 假设 $c_n \in \mathbb{Z}, \forall c_n$, 则存在椭圆曲线 E 和满同态 $\nu: J_0(N) \rightarrow E$ 使得

- (1) 设 $\Lambda_f \subseteq \mathbb{C}$ 是 Φ_f 的像, 则 $\mathbb{C}/\Lambda_f \cong E(\mathbb{C})$,
- (2) $L(s, E) = L(s, f)$ 除去至多有限个素数外, 具有相同的欧拉因子.



由此可得非常值 (满) 映射 $\nu \circ \Phi: X_0(N) \rightarrow E$.

§4.5.4 模性

定理 4.70 (谷山-韦伊-志村猜想, 怀尔斯, Breuil-Conrad-Diamond-泰勒)

设 E/\mathbb{Q} 是椭圆曲线, 则存在正整数 N 使得存在非常值映射 $F: X_0(N) \rightarrow E$.



设 ω 是 E 上非常值全纯微分, 则 $F^*\omega = f(\tau) d\tau, f \in S_2(\Gamma_0(N))$ 是特征形式, 且

$$L(s, f) = L(s, E).$$

定理 4.71

设 E/\mathbb{Q} 是椭圆曲线, 则存在正整数 N 使得 $L(s, E)$ 可以全纯延拓且

$$\Lambda(s, E) = N^{s/2} (2\pi)^{-s} \Gamma(s) L(s, E)$$

满足函数方程

$$\Lambda(s, E) = -\varepsilon \Lambda(2-s, E).$$



Frey, 塞尔, Ribet 的工作显示, 如果

$$\alpha^\ell + \beta^\ell = \gamma^\ell, \ell \geq 5, \alpha\beta\gamma \neq 0$$

则

$$E: y^2 = x(x - \alpha^\ell)(x - \beta^\ell)$$

只可能对应特征形式 $f \in S_2(\Gamma_0(2))$. 然而这是零空间, 因此如果 E 具有模性, 则费马大定理

$$\alpha^\ell + \beta^\ell = \gamma^\ell, \ell \geq 5, \alpha\beta\gamma = 0$$

成立.

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 $\text{End}(M)$ 为 M 的自同态全体, $\text{Aut}(M)$ 为 M 的自同构全体, 则 $(\text{End}(M), +, \circ)$ 在加法和复合意义下构成环, 它的单位群为 $\text{Aut}(M)$.

定义 A.1 (模)

设 R 是(含幺)交换环, 称环同态 $\rho: R \rightarrow \text{End}(M)$ 为 R 模, 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 $\text{End}(M)$ 上的乘法定义为 $fg = g \circ f$, 则这样的环同态被称为右 R 模, 原来的环同态则被称为左 R 模. 如果 M 既是左模又是右模且 $(ra)s = r(as)$, 则称之为 R 双模.



定义 A.2 (群模)

设 G 是群, 称群同态 $\rho: G \rightarrow \text{Aut}(M)$ 为 G 模, 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 $\text{End}(G)$ 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 $f: M \rightarrow N$ 满足 $f(ra) = rf(a), \forall r \in R$, 则称之为模同态. 如果 f 是群的单同态, 满同态, 同构, 则称之为模的单同态, 满同态, 同构, 记为 $M \hookrightarrow N, M \twoheadrightarrow N, M \cong N$. 记 $\text{Hom}_R(M, N)$ 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. 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.

如果存在 $a \in M$ 使得 $M = Ra$, 即 M 由 $\{a\}$ 生成, 称之为循环模. 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.

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

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

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

为 a 和 M 的零化子, 则它们是 R 的左理想. 如果 $\text{Ann}(a)$ 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, \dots, 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 $r = \text{rank} M$ 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 $H \leq G$ 是一个子群, 则对于任意 H 模 B ,

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

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 $f: G \rightarrow B$, 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

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

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 \mathcal{C} 由如下三个要素构成:

- 一个类 $\text{Obj } \mathcal{C}$, 其中的元素 $A \in \text{Obj } \mathcal{C}$ (或简记为 $A \in \mathcal{C}$) 被称为对象;
- 对于任意对象 A, B , 存在集合 $\text{Hom}(A, B)$, 其中的元素 u 被称为 A 到 B 的态射, 记为 $u : A \rightarrow B$; 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

$$\text{Hom}(A, B) \times \text{Hom}(B, C) \rightarrow \text{Hom}(A, C).$$

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 $u : A \rightarrow B, v : B \rightarrow C, w : C \rightarrow D, w \circ (v \circ u) = (w \circ v) \circ u$;
- 对于任意 $A \in \mathcal{C}$, 存在 $\text{id}_A \in \text{Hom}(A, A)$ 使得对任意 $u : A \rightarrow B, u \circ \text{id}_A = u$; 对任意 $v : B \rightarrow A, \text{id}_A \circ v = v$.



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, 实数等均视为集合. 设 (I, \leq) 是一个偏序集, 对于 $i, j \in I$, 当 $i \leq j$ 时, $\text{Hom}(i, j)$ 为单点集; 否则 $\text{Hom}(i, j)$ 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 \mathcal{A} 是一个范畴, 定义其对偶范畴 \mathcal{A}^{op} :

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



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

且满足

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



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

且满足

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

这等价于共变函子 $\mathcal{F} : A^{\text{op}} \rightarrow B$.



例题 A.6 (1) $\text{id}_A : A \rightarrow A$ 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 $\mathcal{F} : \text{Sets} \rightarrow \text{Vect}/k$ 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 $\mathcal{F} : \text{Groups} \rightarrow \text{Sets}$ 是一个函子, 称之为**遗忘函子**. 同理我们有遗忘函子 $\text{Mod}/R \rightarrow \text{Ab}$ 等.

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

$$\text{Hom}(A, -)(u) : \text{Hom}(A, M) \longrightarrow \text{Hom}(A, N)$$

$$v \longmapsto u \circ v.$$

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

$$\text{Hom}(-, A)(u) : \text{Hom}(N, A) \longrightarrow \text{Hom}(M, A)$$

$$v \longmapsto v \circ u.$$

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

(6) 设 H 是 G 的一个子群, 则 $\text{Ind}_G^H : \text{Mod}/H \rightarrow \text{Mod}/G$ 和 $\text{Res}_G^H : \text{Mod}/G \rightarrow \text{Mod}/H$ 是函子, 其中 $\text{Res}_G^H(M) = M$. 它们互为**伴随**, 即

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

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

定义 A.17 (范畴的同构)

设 $u : A \rightarrow B$. 如果存在 $v : B \rightarrow A$ 使得 $v \circ u = \text{id}_A, u \circ v = \text{id}_B$, 则称 u 是**同构**.



定义 A.18 (自然变换与范畴等价)

设 $\mathcal{F}, \mathcal{G} : \mathcal{A} \rightarrow \mathcal{B}$ 是两个函子. 称 f 为 \mathcal{F} 到 \mathcal{G} 的**自然变换**, 如果对于任意 $A \in \mathcal{A}$, 存在 $f_A : \mathcal{F}(A) \rightarrow \mathcal{G}(A)$, 且满足对任意态射 $u : A_1 \rightarrow A_2$,

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

交换. 特别地, 我们有自然变换 $\text{id}_{\mathcal{F}} : \mathcal{F} \rightarrow \mathcal{F}$, 其中 $(\text{id}_{\mathcal{F}})_A = \text{id}_{\mathcal{F}(A)}$. 如果 \mathcal{A} 是一个**小范畴**, 即 $\text{Obj } \mathcal{A}$ 是一个集合, 则 $\mathcal{A} \rightarrow \mathcal{B}$ 间的函子以及函子的自然变换构成范畴 $\text{Func}(\mathcal{A}, \mathcal{B})$. 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 $f : \mathcal{F} \rightarrow \mathcal{G}, g : \mathcal{G} \rightarrow \mathcal{F}$ 使得 $g \circ f = \text{id}_{\mathcal{F}}, f \circ g = \text{id}_{\mathcal{G}}$, 则称 \mathcal{F} 和 \mathcal{G} **同构**. 换言之, \mathcal{F}, \mathcal{G} 在 $\text{Func}(\mathcal{A}, \mathcal{B})$ 中同构. 这也等价于对任意 $A \in \mathcal{A}, f_A : \mathcal{F}(A) \rightarrow \mathcal{G}(A)$ 是同构.

如果存在 $\mathcal{F} : \mathcal{A} \rightarrow \mathcal{B}, \mathcal{G} : \mathcal{B} \rightarrow \mathcal{A}$ 使得 $\mathcal{G} \circ \mathcal{F}$ 和 $\text{id}_{\mathcal{A}}$ 同构, $\mathcal{F} \circ \mathcal{G}$ 和 $\text{id}_{\mathcal{B}}$ 同构, 则称 \mathcal{F}, \mathcal{G} 诱导了 \mathcal{A} 和 \mathcal{B} 的**范畴等价**. 这不同于范畴同构, 后者是指范畴的对象的状态射完全一一对应, 即 $\mathcal{F} \circ \mathcal{G} = \text{id}_{\mathcal{B}}, \mathcal{G} \circ \mathcal{F} = \text{id}_{\mathcal{A}}$. 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 \mathcal{A} 中的对象 I 满足:

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

则称 I 为 \mathcal{A} 的**始对象**.

**定义 A.20 (终对象)**

如果范畴 \mathcal{A} 中的对象 F 满足:

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

则称 F 为 \mathcal{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 $\text{Hom}(A, 0) = \{0\}, \text{Hom}(0, A) = \{0\}$.

**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 $\text{Hom}(I, I') = \{i_{I'}\}, \text{Hom}(I', I) = \{i'_I\}$, 因此 $i_{I'} \circ i'_I : I \rightarrow I$. 由于 $\text{Hom}(I, I) = \{\text{id}_I\}$, 因此 $i_{I'} \circ i'_I = \text{id}_I$. 同理 $i'_I \circ i_{I'} = \text{id}_{I'}$, 所以 $i_{I'} : I \rightarrow I'$ 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 \mathcal{A} 中的一族对象.

定义 A.23 (直和)

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


$$\begin{array}{ccc} A_i & & \\ \alpha_i \downarrow & \searrow \forall u_i & \\ A & \xrightarrow{\exists! v} & M \end{array}$$

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


定义 A.24 (直积)

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

$$\begin{array}{ccc} M & \xrightarrow{\exists! v} & A \\ & \searrow u_i & \downarrow \beta_i \\ & & A_i \end{array}$$

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 $\text{Ab}, \text{Mod}/R$ 等范畴, 我们可以发现 $\text{Hom}(A, B)$ 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 \mathcal{C} 满足

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


$$\text{Hom}(A, B) \times \text{Hom}(B, C) \rightarrow \text{Hom}(A, C)$$

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 $\text{id}_A : A \rightarrow A, 0 : A \rightarrow B$, 存在 $(\text{id}_A, 0) : A \rightarrow A \times B$. 同理存在 $(0, \text{id}_B) : B \rightarrow A \times B$. 因此

存在态射 $i: A \oplus B \rightarrow A \times B$, 使得下图交换

$$\begin{array}{ccc}
 A & & \\
 \alpha_A \downarrow & \searrow^{(id_A, 0)} & \\
 A \oplus B & \xrightarrow{i} & A \times B \\
 \alpha_B \uparrow & \nearrow_{(0, id_B)} & \\
 B & &
 \end{array}$$

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

定义 A.28 (加性函子)

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

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

称之为**加性函子**. 这等价于对任意 $A, B, \mathcal{F}: \text{Hom}(A, B) \rightarrow \text{Hom}(\mathcal{F}(A), \mathcal{F}(B))$ 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 $u: A \rightarrow B$ 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 $i: C \rightarrow A$ 满足对于任意对象 M 和态射 $v: M \rightarrow A$, 若 $u \circ v = 0$, 则存在唯一的态射 $w: M \rightarrow C$ 使得下图交换

$$\begin{array}{ccccc}
 M & & & & \\
 \exists! w \downarrow & \searrow^0 & & & \\
 C & \xrightarrow{i} & A & \xrightarrow{u} & B \\
 & & \forall v & &
 \end{array}$$

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

$$\begin{array}{ccccc}
 A & \xrightarrow{u} & B & \xrightarrow{j} & D \\
 & \searrow^0 & \forall v & \downarrow \exists! w & \\
 & & & & M
 \end{array}$$

则称 (D, j) 为 u 的**余核**, 记为 $\text{coker } u$. 若 $\text{coker } u = 0$, 称 u 为**满态射**.



定义 A.31 (像和余像)

称余核的核 $\ker(\text{coker } u)$ 为 u 的**像** $\text{im } u$; 称核的余核 $\text{coker}(\ker u)$ 为 u 的**余像** $\text{coim } u$.



我们将它们对应的对象记为 $\text{Ker}, \text{Coker}, \text{Im}, \text{CoIm}$.

定义 A.32 (阿贝尔范畴)

如果加性范畴 \mathcal{A} 满足

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

则称 \mathcal{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) $\text{Ab}, \text{Mod}/R$ 是阿贝尔范畴.

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

$$\text{Obj } \mathcal{A} \hookrightarrow \text{Obj } \text{Mod}/R,$$

$$\text{Hom}_{\mathcal{A}}(A, B) = \text{Hom}_{\text{Mod}/R}(\mathcal{F}(A), \mathcal{F}(B)),$$

且保持核和余核.

§A.2.4 正合列

定义 A.33 (正合)

设 \mathcal{A} 为阿贝尔范畴, $A, B, C \in \mathcal{A}$. 称 $A \xrightarrow{u} B \xrightarrow{v} C$ 正合, 如果自然映射 $\text{Ker } v \simeq \text{Im } u$ 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 $\text{Ker } v = \text{Im } u$. 由此可知

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

正合当且仅当 $\text{Ker } u = 0, \text{Im } u = \text{Ker } v, \text{Im } v = C$, 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 \mathcal{A} 中的交换图

$$\begin{array}{ccccccc} A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 0 & \longrightarrow & A' & \longrightarrow & B & \longrightarrow & C \end{array}$$

其中每行都是正合的, 则存在唯一的态射

$$\delta : \text{Ker } \gamma \rightarrow \text{Coker } \alpha$$

使得下图交换

$$\begin{array}{ccc} B \times_C \text{Ker } \gamma & \longrightarrow & \text{Ker } \gamma \\ \downarrow & & \downarrow \delta \\ A' & \longrightarrow & \text{Coker } \alpha \end{array}$$

其中左竖直态射由 β 诱导, 而且我们有正合列

$$\text{Ker } \alpha \rightarrow \text{Ker } \beta \rightarrow \text{Ker } \gamma \xrightarrow{\delta} \text{Coker } \alpha \rightarrow \text{Coker } \beta \rightarrow \text{Coker } \gamma.$$



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

$$\begin{array}{ccccccccc} A^1 & \longrightarrow & A^2 & \longrightarrow & A^3 & \longrightarrow & A^4 & \longrightarrow & A^5 \\ \downarrow u^1 & & \downarrow u^2 & & \downarrow u^3 & & \downarrow u^4 & & \downarrow u^5 \\ B^1 & \longrightarrow & B^2 & \longrightarrow & B^3 & \longrightarrow & B^4 & \longrightarrow & B^5, \end{array}$$

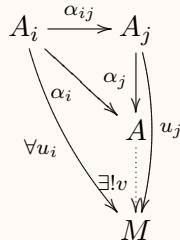
其中每行都正合. 如果 u^1, u^2, u^4, u^5 是同构, 则 u^3 也是同构.



§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 \mathbf{A} 中的一族对象 $A_i, i \in I$, 以及 $i \leq j$ 时态射 $\alpha_{ij} : A_i \rightarrow A_j$, 如果对象 A 以及一族态射 $\alpha_i : A_i \rightarrow A$, 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 $u_i : A_i \rightarrow M$, 如果 $u_j \circ \alpha_{ij} = u_i$, 存在唯一的 $v : A \rightarrow M$ 使得下图交换

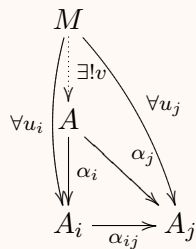


则称 (A, α_i) 为 A_i 的**正向极限**, 记为 $\varinjlim A_i$.



定义 A.37 (逆向极限)

对于范畴 \mathbf{A} 中的一族对象 $A_i, i \in I$, 以及 $i \leq j$ 时态射 $\alpha_{ij} : A_i \rightarrow A_j$, 如果对象 A 以及一族态射 $\alpha_i : A_i \rightarrow A$, 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 $u_i : A_i \rightarrow M$, 如果 $u_j \circ \alpha_{ij} = u_i$, 存在唯一的 $v : A \rightarrow M$ 使得下图交换



则称 (A, α_i) 为 A_i 的**逆向极限**, 记为 $\varprojlim A_i$.



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 $A = \varinjlim A_i$, 则存在映射 $u : \bigoplus_i A_i \rightarrow A$. 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 $u : B \rightarrow \prod_i A_i$. 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 \mathbf{A} 是一个阿贝尔范畴. \mathbf{A} 上的复形 $L = L^\bullet$ 是指一族对象 $L^i, i \in \mathbb{Z}$, 以及态射 $d = d^i : L^i \rightarrow L^{i+1}$, 使得 $d \circ d = 0$. 我们记为

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

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

定义

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

$$H^i = Z^i / B^i,$$

为 L 的循环, 边界, 上同调.

定义 A.39 (拟同构)

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



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

定义 A.40 (解出)

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

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

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

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



§A.2.7 导出函子

定义 A.41 (导出函子)

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

$$0 \rightarrow A_1 \rightarrow A_2 \rightarrow A_3 \rightarrow 0,$$

序列

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

(或 $\mathcal{F}(A_1) \rightarrow \mathcal{F}(A_2) \rightarrow \mathcal{F}(A_3) \rightarrow 0$) 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 $\mathcal{G} : \mathbf{A} \rightarrow \mathbf{B}$, 我们称其左正合(或右正合)是指其对应的共变函子



$\mathcal{G}^{\text{op}} : \mathbf{A}^{\text{op}} \rightarrow \mathbf{B}$ 左正合 (或右正合).

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

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

正合, 则

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

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

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

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

定义 A.42 (内射和投射)

设 \mathbf{A} 是阿贝尔范畴. 如果 $\text{Hom}(-, M)$ 正合, 我们称 M 是**内射**的. 我们称 \mathbf{A} 有足够多的内射对象, 是指对任意 $L \in \mathbf{A}$, 存在内射 $L' \in \mathbf{A}$ 和单态射 $L \rightarrow L'$.

如果 $\text{Hom}(M, -)$ 正合, 我们称 M 是**投射**的. 我们称 \mathbf{A} 有足够多的投射对象, 是指对任意 $L \in \mathbf{A}$, 存在投射 $L' \in \mathbf{A}$ 和满态射 $L' \rightarrow L$.



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

$$0 \rightarrow A \rightarrow I^0 \rightarrow I^1 \rightarrow \dots$$

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

$$0 \rightarrow \mathcal{F}(I^0) \rightarrow \mathcal{F}(I^1) \rightarrow \dots$$

的上同调 $R^i \mathcal{F}(A)$ 称为 \mathcal{F} 的**右导出函子** $R^i \mathcal{F} : \mathbf{A} \rightarrow \mathbf{B}$. 显然 $R^0 \mathcal{F} = \mathcal{F}$.

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

$$\dots \rightarrow P^1 \rightarrow P^0 \rightarrow A \rightarrow 0.$$

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

$$\dots \rightarrow \mathcal{F}(P^1) \rightarrow \mathcal{F}(P^0) \rightarrow 0$$

的同调 $L^i \mathcal{F}(A) := H^{-i}(\mathcal{F}(P^\bullet))$ 称为 \mathcal{F} 的**左导出函子** $L^i \mathcal{F} : \mathbf{A} \rightarrow \mathbf{B}$. 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

$$0 \rightarrow A \rightarrow B \rightarrow C$$

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

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

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 $H^i(G, -) = R^i\mathcal{F}$, 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

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

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

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

即连续的两个映射的复合是 0, 定义

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

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

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

映射为

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

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

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

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

$$h(s \cdot g_0, \dots, s \cdot g_i) = s \cdot h(g_0, \dots, g_i)$$

的函数全体. 由此也可以看出 h 完全由函数

$$f(g_1, \dots, g_i) = h(1, g_1, g_1 g_2, \dots, g_1 \cdots g_i)$$

确定. 通过这种非齐次的表达式, d 变为了

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

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

$$f(gg') = g \cdot f(g') + f(g)$$

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

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

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

正合, 则

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

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 $H_i(G, -) = L^i \mathcal{F}$, 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

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

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

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

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

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

我们有类似的长正合列.

若 $A = \mathbb{Z}$, G 为平凡作用, 则 $H_1(G, \mathbb{Z}) = G^{\text{ab}}$. 实际上, 设 $\pi: \mathbb{Z}[G] \rightarrow \mathbb{Z}$ 为增广映射, 即 $\sum n_g g \mapsto \sum n_g$. 令 I_G 为其核, 即增广理想, 它由 $g - 1$ 生成. 由定义, $H_0(G, A) = A/I_G A$. 考虑

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

我们有 $H_0(G, I_G) = I_G/I_G^2$ 且其在 $H_0(G, \mathbb{Z}[G])$ 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

$$d: H_1(G, \mathbb{Z}) \rightarrow H_0(G, I_G) = I_G/I_G^2.$$

容易验证 $s \mapsto s - 1$ 诱导了同构 $G^{\text{ab}} \simeq I_G/I_G^2$. 因此 $H_1(G, \mathbb{Z}) = G^{\text{ab}}$.

由导出函子的性质, 我们有

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

正合, 则

$$\cdots \rightarrow H_{q+1}(G, B) \rightarrow H_{q+1}(G, C) \xrightarrow{\delta} H_q(G, A) \rightarrow H_q(G, B) \rightarrow \cdots$$

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

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

定义泰特上同调

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

则对于正合列

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0,$$

我们有长正合列

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

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

§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

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

其中

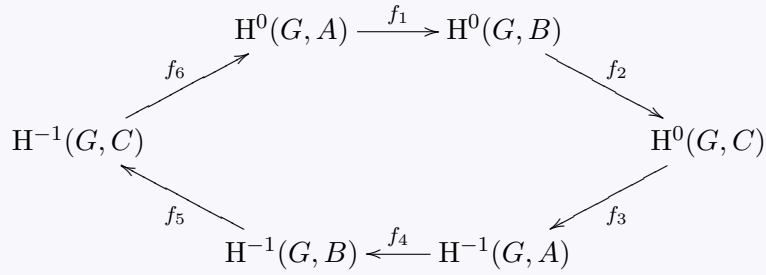
$$\begin{aligned} Z^1 &:= \{f : G \rightarrow A \mid f(gh) = f(g)^h f(h)\}, \\ B^1 &:= \{f_a : G \rightarrow A \mid f_a(g) = a^{g-1}, a \in A\}. \end{aligned}$$

命题 A.43

如果 $G = \langle \sigma \rangle$ 是循环群, 则 $H^1(G, A) = H^{-1}(G, A)$. 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



该命题可以利用此情形下泰特上同调和复形

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

的上同调一致得到, 见 [18, §8.4]. 由此可知 $H^n(G, A)$ 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 $f_3(c) = (j^{-1}(c))^{\sigma^{-1}}$, $f_6(c) = \mathbf{N}(j^{-1}(c))$.

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

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

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,

$$0 \rightarrow \text{Im } f_6 \rightarrow H^0(G, A) \rightarrow \text{Im } f_1 \rightarrow 0$$

正合, 因此 $\#H^0(G, A) = \#\text{Im } f_6 \cdot \#\text{Im } f_1$. 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

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

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

$$\begin{aligned} \pi : A &\rightarrow B, & f &\mapsto f(1), \\ \nu : A &\rightarrow B, & f &\mapsto \prod_{\tau \in R} f(\tau). \end{aligned}$$

容易看出

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

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

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

很明显, π 诱导了同构 $A^G \rightarrow B^H$, 而且

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

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

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

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

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](https://doi.org/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](https://doi.org/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 \mathbf{Z} ”. In: *Invent. Math.* 81.3 (1985), pp. 515–538. ISSN: 0020-9910. DOI: [10.1007/BF01388584](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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.wvli.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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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](https://doi.org/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 Понтрягин, 1908–1988
佩尔	John Pell, 1611–1685
切博塔廖夫	Мико́ла Григо́рович Чеботарьов, 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 Шафа́рэвич, 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

索引

- \mathbb{A}_K , 89
- \mathbb{A}_K^\times , 89
- adèle, 89
- Atkin-Lehner 算子, 120

- C_K , 89
- Cl_K , 15

- Δ_a , 8
- Δ_K , 8
- disc, 4

- Γ 函数, 106

- $\text{Hom}_K(L, \overline{K})$, 2
- Hom 函子, 133

- \mathbb{I}_K , 89
- \mathcal{I}_K , 17
- idèle, 89
- \mathbb{I}_K^S , 89

- \overline{K} , 2

- L 函数, 103

- μ_K , 15

- $\mathbf{N}_{L/K}$, 1
- N 次分圆多项式, 11
- n 次剩余符号, 88, 101
- n 阶单位群, 41

- \mathcal{O}_K^\times , 15
- \mathcal{O}_K , 7

- \mathcal{P}_K , 15
- p 进赋值, 32
- \mathfrak{p} 进赋值, 32

- S 单位, 16
- S 理想类群, 16

- θ 函数, 106

- Tr, 20
- $\text{Tr}_{L/K}$, 1

- ζ 函数, 111

- 上同调, 139
- 主伊代尔, 89
- 主分式理想, 15
- 主同余子群, 115
- 主除子, 121
- 乘性约化, 123
- 二元二次型, 25
 - 不定的, 25
 - 判别式, 25
 - 导子, 29
 - 既约的, 26
 - 本原, 25
 - 正定的, 25
 - 等价的, 25
 - 负定的, 25
- 亏格, 121
- 互反律, 76
- 互反射射, 72
- 亨泽尔赋值, 70
- 代数整数, 7
- 代数曲线, 121
- 伊代尔, 89
- 伊代尔类群, 89
- 伊代尔群, 89
- 伯努利数, 107
- 伴随, 133
- 伽罗瓦扩张, 69
- 余像, 136
- 余核, 136

- 傅里叶变换, 105, 110
- 像, 136
- 光滑, 121
- 克鲁尔拓扑, 68

- 克鲁尔赋值, 34
全不连通, 35
全实域, 9
全序交换群, 31
全正, 28
全纯, 116
全纯微分, 121
全虚域, 9
共轭差积, 61, 62
共轭的, 51
内射, 140
凸集, 19
函子
 共变函子, 133
 反变函子, 133
函数域, 1
分圆扩张, 95
分式理想, 14
分歧, 54
 分歧域, 55
 分歧指数, 49
 分歧群, 55
分裂乘性约化, 123
分解域, 55
分解群, 55
判别式, 4, 8
加性函子, 136
加性约化, 123
加性范畴, 135
加性赋值, 32
勒让德符号, 88
单位群, 15
单同态, 129
单态射, 136
卢宾-泰特形式群, 84
卢宾-泰特级数, 83
变换映射, 74
可分, 2
右导出函子, 140, 141
右正合, 139
右解出, 139
同余子群, 97, 115
同态, 83
同构, 83, 129, 133, 134
哈尔测度, 18
商模, 130
坏约化, 123
埃尔布朗商, 144
域, 69
域扩张, 69
基本区域, 18
基本单位, 17
增广映射, 142
增广理想, 142, 143
复嵌入, 9
复形, 139
复素位, 9
大希尔伯特类域, 99
奇异, 121
好约化, 123
始对象, 134
子模, 129
完全分歧, 49, 54, 70
完全分裂, 54
完全格, 18
实嵌入, 9
实素位, 9
对偶基, 5
对偶范畴, 132
对数, 83
对称, 19
对象, 132
导子, 81, 98, 103
导数, 63
射影完备化, 69
射影循环群, 68
射影曲线, 43
射影有限群, 67

- 射线类域, 98
 射线类群, 97
 小范畴, 134
 尖点, 115
 尖点形式, 116
 局部 ζ 函数, 110
 局部环, 121
 局部范数剩余符号, 86
 左导出函子, 140, 142
 左正合, 139
 左解出, 139
 希尔伯特符号, 87
 希尔伯特类域, 99
 平凡赋值, 33
 广义艾森斯坦多项式, 47
 库默尔扩张, 80
 庞加莱上半平面, 115
 庞特里亚金对偶, 68
 弗罗贝尼乌斯, 70
 张量积, 131
 形式群, 83
 - 形式 R 模, 83
 - 形式乘法群, 83
 - 形式加法群, 83
 循环, 139
 循环模, 130
 微分, 63, 139
 微分模, 63

 态射, 132, 139
 恒等函子, 133
 惯性, 49, 54
 - 惯性域, 55
 - 惯性指数, 49, 70
 - 惯性群, 55, 69
 戴德金 ζ 函数, 109
 戴德金环, 13
 投射, 140
 拟同构, 139
 拟特征, 110

 拟赫克特征, 109
 挠元, 130
 挠模, 130
 数域, 1
 整, 6
 整体范剩余符号, 97
 整基, 8
 整数环, 7
 整闭包, 6
 整闭的, 6
 新形式, 127
 施瓦兹函数, 110, 111
 无穷素位, 9
 有限扩张, 69
 有限素位, 45
 本原, 103
 本原多项式, 37
 权, 116
 极大分歧扩张, 51
 极大非分歧扩张, 50, 69
 极小多项式, 2
 极小魏尔斯特拉斯模型, 123
 核, 136
 格, 18
 梅林变换, 118
 模, 129
 模同态, 129
 模形式, 116
 模曲线, 116
 欧式空间, 18
 欧拉乘积, 103
 正合, 137, 139
 正向, 28
 正向极限, 138
 正规扩张, 69
 泛性质, 134
 泰希米勒提升, 38
 泰特上同调, 143
 消没, 116

- 温分歧, 50, 51
 温希尔伯特符号, 87
 满同态, 129
 满态射, 136

 牛顿折线, 47
 特征, 110
 狄利克雷特征, 103
 球完备, 48
 理想类群
 缩理想类群, 28
 生成的子模, 129
 直和, 131, 135
 直积, 131, 135
 短正合列, 137
 离散赋值, 36
 离散赋值域, 36
 离散赋值环, 36
 规范化离散赋值, 36
 秩, 123
 等价, 128
 等价赋值, 33
 类域, 78
 类域论公理, 71
 类数, 15
 类群, 15
 素元, 71
 级, 116
 终对象, 134
 绝对分歧指数, 40
 绝对非分歧, 40
 维特向量, 40
 维特环, 40

 自然变换, 134
 自由模, 131
 艾森斯坦多项式, 8
 范剩余符号, 77
 范数, 1, 143
 范数拓扑, 77
 范畴, 132

 范畴等价, 134
 表出, 27
 真表出, 27
 解析类数公式, 112
 诱导模, 131
 诺特环, 13
 调整子, 24
 赋值, 31
 赋值域, 31
 赋值环, 34
 赫克 L 函数, 109
 赫克特征, 109
 赫克算子, 127
 边界, 139
 连接映射, 142
 迹, 1

 逆向极限, 138
 遗忘函子, 133
 野分歧, 51
 野希尔伯特符号, 88
 闵可夫斯基界, 21
 闵可夫斯基空间, 19
 阿代尔, 89
 阿代尔环, 89
 阿基米德赋值, 31
 阿廷符号, 99
 阿贝尔扩张, 67
 阿贝尔范畴, 137
 限制直积, 89
 除子, 121
 雅克比簇, 125
 零化子, 130
 零对象, 134
 非分歧, 49, 50, 54, 70
 非分裂乘性约化, 123
 非本原, 103
 非阿赋值, 31
 骨架范畴, 134
 高斯和, 104

- 高斯复合律, 29
高阶分歧群, 58
魏尔斯特拉斯方程, 122
黎曼 ζ 函数, 103
默比乌斯函数, 11
默比乌斯反演, 11