

整体域上二次互反律

邹思远

学号：18307110469

专业：数学与应用数学

指导老师：姚一隽

摘要 John Tate 在 1950 年的博士毕业论文“Fourier analysis in number fields and Hecke’s zeta functions”为数论研究提供了全新的方法. 这篇学位论文将跟随他在局部域及 Adèles 环上搭建框架, 应用 Schwartz-Bruhat 函数的傅立叶变换及 Poisson 求和公式得到整体二次剩余符号的互反律, 随后将其与二次 Hilbert 符号的互反律联系起来, 最终推出代数数论语言下整体域上的二次互反律. 这篇学位论文的最后一章将用代数数论语言下的二次互反律推出 Gauss 二次互反律及函数域上类似的二次互反律的表达式.

关键字: 局部域、整体域、Adèles 环、Schwartz-Bruhat 函数、缓增广义函数、傅立叶变换、傅里叶逆变换公式、Poisson 求和公式、二次互反律

Abstract John Tate’s doctoral thesis in 1950, titled “Fourier analysis in number fields and Hecke’s zeta functions”, has provided brandnew methodology to the field of number theory. This dissertation will follow his settings on local fields and Adèles ring to enable Fourier analysis of Schwartz-Bruhat functions, and use Poisson summation formula to get reciprocity law of global quadratic residue symbol. Guaranteed that, we will be able to prove the reciprocity law for quadratic Hilbert symbol, which leads us to the result of the quadratic reciprocity law on global fields in the language of algebraic number theory. In the last chapter of this dissertation, we will use the result to deduce Gauss quadratic reciprocity law and a similar version of that on function fields.

Keywords: Local Fields, Global Fields, Adèles Ring, Schwartz-Bruhat Function, Tempered Distribution, Fourier Transform, Fourier Inversion Formula, Poisson Summation Formula, Quadratic Reciprocity Law

目录

第一章 总论	1
第二章 基本知识	2
第 1 节 局部紧拓扑群	2
第 2 节 Haar 测度	3
2.1 Haar 测度	4
2.2 积分的定义	5
2.3 Urysohn 引理	5
2.4 Riesz 表示定理	6
2.5 Haar 测度存在唯一性	6
第 3 节 商积分公式	7
第 4 节 傅里叶变换	8
第 5 节 Poisson 求和公式	9
第三章 准备工作	10
第 1 节 整体域与局部域的特点	10
1.1 局部域与整体域的定义	10
1.2 域上的赋值与完备化	10
1.3 整体域上的赋值与完备化	12
1.4 正规化的赋值	13
1.5 局部域与整体域的公理化定义	14
第 2 节 局部域上傅立叶变换	15
2.1 标准特征	15
2.2 标准测度	17
2.3 Schwartz-Bruhat 函数	17
2.4 缓增广义函数	19
第 3 节 Adèles 环	21
第 4 节 Adèles 环上傅里叶变换	23
4.1 标准特征	23
4.2 标准测度	24

4.3	Schwartz-Bruhat 函数	24
4.4	Poisson 求和公式	24
第四章	二次互反律	26
第 1 节	二次扩张	26
第 2 节	二次指数分布	27
第 3 节	二次范数剩余符号与局部积分	28
第 4 节	二次范数剩余符号的互反律	30
第 5 节	二次 Hilbert 符号的互反律	31
第 6 节	二次互反律	32
第五章	例子与应用	35
第 1 节	Gauss 二次互反律	35
第 2 节	函数域上二次互反律	36

第一章 总论

在这篇学位论文中, 我们通过在局部域上搭建傅立叶分析的框架, 并将整体域 K 离散地嵌入 $\mathbb{A}_K$ 中得到 $\mathbb{Z} \subset \mathbb{R}$ 的类比 $\mathbb{K} \subset \mathbb{A}_K$. 通过在 $\mathbb{A}_K$ 上整体地定义傅立叶变换得到其上的 Schwartz-Bruhat 函数成立 Poisson 求和公式:

$$\sum_{\kappa \in K} f(\kappa) = \sum_{\kappa \in K} \hat{f}(\kappa).$$

利用这个关键结论及傅立叶变换的技术得到整体域上二次互反律.

定理: 如果 $\pi, \varpi \in K$ 生成两个不同的奇位置, 那么有

$$\left(\frac{\pi}{\varpi}\right)_2 \left(\frac{\varpi}{\pi}\right)_2 = \prod_v (\pi, \varpi)_v,$$

其中 v 跑遍所有的偶位置或无限的位置, $(-, -)_v$ 为 Hilbert 符号.

如果 π 生成一个奇位置 v , $\alpha \in \mathfrak{o}$ 在 $\mathfrak{o}_v$ 中为单位, 那么

$$\left(\frac{\alpha}{\pi}\right)_2 = \prod_v (\pi, \alpha)_v,$$

其中 v 跑遍所有的偶位置或无限的位置, 也跑遍所有使得 α 在 $\mathfrak{o}_v$ 中不为单位的奇位置.

可以看出定理的陈述类似于 Gauss 二次互反律, 不过使用了代数数论的语言.

第二章将介绍分析基础, 即在一般的局部紧 Abel 群上进行傅立叶分析的方法, 涉及测度、积分、傅立叶逆变换公式的成立及 Poisson 求和公式.

第三章介绍如何在 Adèles 环上做傅里叶分析. 首先介绍局部域和整体域的基本知识, 在局部域上进行傅立叶分析所需的特征、测度以及将 $\mathbb{R}$ 上 Schwartz 函数及缓增广义函数的性质向局部域上推广. 随后将局部域上特征、测度、函数拼起定义在 Adèles 环上, 并且证明 $K \subset \mathbb{A}_K$ 离散, 得到 Poisson 求和公式.

第四章进入证明, 定义二次指数分布函数 $S_a(x)$, 其类似于 $e^{-\pi i x |z|^2}$, 部分地在傅立叶变换下不变, 作用了傅立叶变换后得到与二次剩余符号相关的局部积分 $\gamma(a)$. 通过 $S_a(x), \gamma(a)$ 的性质与 Poisson 求和公式得到整体二次剩余符号的互反律, 而二次剩余符号在局部与二次 Hilbert 符号等同, 故而得到二次 Hilbert 符号的互反律. 最终, 通过分类讨论得到 Legendre 符号与二次 Hilbert 符号表征的整体域上二次互反律.

第五章作为整体域上二次互反律的应用, 将推出 Gauss 二次互反律及函数域上类似的二次互反律的表达式.

在这篇学位论文中可以看出, 将分析方法引入数论研究的巨大妙用.

第二章 基本知识

由于我们将要在 Adèles 环上做傅里叶变换, 因此我们需要知道这样的积分定义在什么样的结构上, 采用什么测度, 有关 $\mathbb{R}$ 上傅里叶变换的结论可以做多大程度的推广.

第 1 节 局部紧拓扑群

一般的, 首先我们给出拓扑群的定义. 如无特别说明, e 表示群 G 的单位元.

定义 2.1. (拓扑群) 如果有一个群 G , 其上有一个拓扑, 使得群的运算在此拓扑下连续, 即:

$$G \times G \rightarrow G$$

$$(a, b) \mapsto ab$$

与

$$G \rightarrow G$$

$$g \mapsto g^{-1}$$

在此拓扑下均为连续映射, 则群 G 被称为拓扑群.

观察可以发现, 群 G 关于任何固定元素的左(右)乘法作用是 G 到自身的同胚.

命题 2.2. 对于拓扑群 G 及任何的群元素 g , 以下条件等价:

- U 为开集.
- gU 为开集.
- Ug 为开集.

特别地, 任何元素处的邻域都可以由单位元处的邻域平移得到, 这说明拓扑群局部的结构处处相同. 更进一步可以证明其为一个齐性 (homogenous) 空间.

对于大多数拓扑空间来说, 满足 Hausdorff 的条件是在其上做分析的基本要求, 对于拓扑群, 以下命题说明这样的要求是非常自然的.

命题 2.3. 如果 G 是一个拓扑群, 那么以下条件是等价的:

- 1) G 是 T_1 空间.

- 2) G 是 Hausdorff 空间.
- 3) G 的单位元是闭的.
- 4) G 的每一个点都是闭的.

命题 2.4. 如果 G 是一个拓扑群, H 是 G 的子群, 那么有:

- 1) 商空间 G/H 是齐性空间, 商映射 $\rho: G \rightarrow G/H$ 是开映射.
- 2) 商空间 G/H 是 T_1 的当且仅当 H 是闭集.
- 3) 如果 H 是正规子群, 那么商空间 G/H 在商群的群作用以及商拓扑下构成一个拓扑群.
- 4) 如果 H 是集合 $\{e\}$ 的闭包, 则 H 自然是正规子群, 那么商空间 G/H 是一个具有商群结构和商拓扑的 Hausdorff 空间.

我们略去证明, 具体可以参考 [1, 1.3, 1.4]. 这说明对于任何一个拓扑群, 只要商去 $\{e\}$ 的闭包就自动得到一个 Hausdorff 空间. 因而以下我们只考虑 Hausdorff 的拓扑群, 在此基础上, 进而考虑局部紧 Abel 群:

定义 2.5. 如果一个拓扑空间 X 中每一点都有一个紧邻域, 则称 X 为局部紧空间.

定义 2.6. 如果拓扑群 G 是作为拓扑空间是局部紧和 Hausdorff 的, 就称为局部紧群. 特别地, 如果 G 是一个 Abel 群, 则称为局部紧 Abel 群.

对于局部紧群, 2.4. 可以进一步强化.

命题 2.7. 如果 G 是一个局部紧群, H 为其闭子群, 则 G/H 为一个局部紧群.

我们略去证明, 具体可以参考 [4, 1.2.1].

局部紧 Abel 群是很重要的概念, 有理数域 $\mathbb{Q}$, 实数空间 $\mathbb{R}$, 复数空间 $\mathbb{C}$ 作为加法群都是局部紧 Abel 群, 去掉零点作为乘法群也是局部紧 Abel 群. 作为数域推广概念的整体域也具有相似的结构.

第 2 节 Haar 测度

Haar 测度是局部紧拓扑群 (不一定是 Abel 的) 上对一般拓扑空间上 Radon 测度的推广. 这一节证明 Haar 测度在局部紧拓扑群上的存在唯一性, 从中可以感受到分析方法在抽象代数结构上的妙用. 如无特别说明, G 指一个局部紧的拓扑群.

2.1 Haar 测度

类似于 Lebesgue 测度的构造, 任何一个集合 X 上都可以抽象地定义可测集, 它们是 X 的一组子集, 满足 σ -代数的结构.

定义 2.8. (σ -代数) 对于一个集合 X 的一族子集 $\mathfrak{A}$, 如果它满足以下条件:

- $X \in \mathfrak{A}$.
- 如果 $A \in \mathfrak{A}$, 则 A 的补集 $A^c \in \mathfrak{A}$.
- 如果有一列 $A_n \in \mathfrak{A} (n \geq 1)$, 令

$$A = \bigcup_{n=1}^{\infty} A_n,$$

则 $A \in \mathfrak{A}$, 则称 $\mathfrak{A}$ 为一个 σ -代数.

定义 2.9. (可测空间) 一个集合 X 与其上子集的 σ -代数 $\mathfrak{A}$ 被合称为可测空间, 记作 $(X, \mathfrak{A})$. 特别地, 如果 X 是一个拓扑空间, 那么我们可以考虑含其上所有开集的最小 σ -代数 $\mathfrak{B}$ 组成可测空间, $\mathfrak{B}$ 中的元素称为称作 **Borel 集**.

定义 2.10. (测度) 一个可测空间 $(X, \mathfrak{A})$ 上的测度 μ 为函数:

$$\mu : \mathfrak{A} \rightarrow [0, +\infty],$$

满足 $\mu(\bigsqcup A_i) = \sum \mu(A_i)$, 称 $(X, \mathfrak{A}, \mu)$ 为测度空间. 如果 $\mathfrak{A} = \mathfrak{B}$, 则称 μ 为 **Borel 测度**.

定义 2.11. (Radon 测度) Radon 测度是在紧集上取值有限的 Borel 测度, 并且

- 在 Borel 集上满足外正则性: $\mu(E) = \inf\{\mu(U) : U \supseteq E, U \text{ 为开集}\}$,
- 在开集上满足内正则性: $\mu(E) = \sup\{\mu(K) : K \subseteq E, K \text{ 为紧集}\}$.

定义 2.12. (平移不变性) 一个 Borel 测度 μ 称为左平移不变的, 如果对任何的 $g \in G$, 对任何的 Borel 集 S , 有 $\mu(S) = \mu(gS)$. 一个 Borel 测度 μ 称为右平移不变的, 如果对任何的 $g \in G$, 对任何的 Borel 集 S , 有 $\mu(S) = \mu(Sg)$.

定义 2.13. 一个 G 上的左 (右) Haar 测度即为一个 G 上非零的左 (右) 平移不变的 Radon 测度.

2.2 积分的定义

给定 $(X, \mathfrak{R}, \mu)$, 定义阶梯函数

$$f = \sum_{i=1}^n c_i \mathbb{1}_{S_i}, c_i \in \mathbb{C}, S_i \in \mathfrak{R}, \mu(S_i) < +\infty.$$

其积分定义为 $\int f = \sum_{i=1}^n c_i \mu(S_i)$.

定义 2.14. (可测函数) 在一个测度空间 $(X, \mathfrak{R}, \mu)$ 上, 如果一个函数 $f: X \rightarrow \mathbb{C}$ 成立

$$\forall S \in \mathfrak{B}(\mathbb{C}), f^{-1}(S) \in \mathfrak{R},$$

则称为可测函数.

定义 2.15. (可积函数) 如果有一个可测函数 f 在相差一个零测集的情况下为一列阶梯函数 f_i 的逐点收敛极限, 那么定义

$$\int f = \lim_{i \rightarrow \infty} \int f_i, \quad (2.1)$$

可以证明这是良定义的, 这样的可测函数被称为可积函数.

可积函数全体按照范数 $\|f\| = \int |f|$ 组成 Banach 空间 $L^1(X)$.

2.3 Urysohn 引理

一个局部紧 Hausdorff 空间满足更好的分离条件, 这是局部紧拓扑群的拓扑性质.

命题 2.16. 如果 G 是局部紧拓扑群, 则对于一个紧集 K 和包含它的开集 O , 存在一个开集 V , 成立

$$K \subset V \subset \overline{V} \subset O, \text{ 其中 } \overline{V} \text{ 是紧的.}$$

满足这样性质的拓扑空间成立 Urysohn 引理.

引理 2.17. (Urysohn 引理) 对于一个紧集 K 和包含它的开集 O , 存在一个函数 $f \in C_c(G)$, 成立

$$f(x) = \begin{cases} 1 & x \in K \\ t, t \in [0, 1] & x \in O \setminus K \\ 0 & x \in G \setminus O \end{cases}$$

其中, $C_c(G)$ 代表 G 上所有连续的, 具有紧支集的函数.

我们略去证明, 具体可以参考 [2, 21.1].

2.4 Riesz 表示定理

定理 2.18. 如果 X 是一个局部紧的 Hausdorff 空间, 给定 $C_c(X)$ 上的正线性泛函 I , 存在唯一一个 X 上的 Randon 测度 $\mu: \mathcal{B} \rightarrow [0, +\infty]$ 与之对应:

$$I(f) = \int_X f d\mu, \forall f \in C_c(X). \quad (2.2)$$

我们略去证明, 具体可以参考 [4, Theorem B.2.2].

2.5 Haar 测度存在唯一性

证明的策略是在局部紧拓扑群上用正次线性泛函逼近一个正线性泛函, 这个正次线性泛函的定义依赖于单位元 e 附近的小邻域, 相当于给小邻域的面积赋值. 可以想像当邻域越来越小得到一个线性泛函.

定义 2.19. (Haar 覆盖数) 对于给定的 $\phi \in C_c^+(G)$, 可以用它覆盖任意的 $f \in C_c^+(G)$. 记 $U = \{x: \phi(x) > \frac{\|\phi\|_{\sup}}{2}\}$, 因为 f 的支集是紧的, 则 $\text{Supp} f \subset \bigcup_{i=1}^n s_i U$, $s_i \in G$. 这说明

$$f \leq \frac{2\|f\|_{\sup}}{\|\phi\|} \sum_{i=1}^n L_{s_i} \phi. \quad (2.3)$$

因此, 定义 Haar 覆盖数为 $(f: \phi) = \inf \left\{ \sum_{i=1}^n c_i : f \leq \sum_{i=1}^n c_i L_{s_i} \phi, c_i > 0, s_i \in G \right\}$. 因为对所有的 $f \in C_c^+(G)$, $\|f\|_{\sup} > 0$, 可见覆盖数是一个有限正数.

覆盖数满足一些性质, 如

- $(cf: \phi) = c(f: \phi)$, $c > 0$.
- $(f: \phi) = (L_s f: \phi)$, $\forall s \in G$.
- $(f_1 + f_2: \phi) \leq (f_1: \phi) + (f_2: \phi)$.
- $(f: \phi) \leq (f: f_0)(f_0: \phi)$.

选定某 $f_0 \in C_c^+(G)$, 利用 Haar 覆盖数的次线性性定义次线性泛函 $I_\phi(f) = \frac{(f: \phi)}{(f_0: \phi)}$. 可以验证其为左不变次线性的, 并且对 f 的取值在区间 $\left[\frac{1}{(f_0: f)}, (f: f_0) \right]$ 内. 以下引理表明, 其次线性程度可以被控制.

引理 2.20. 对于任意的 $\epsilon > 0$, 给定 $f_1, f_2 \in C_c^+(G)$, 有 e 的邻域 U , 如果 $\text{Supp} \phi \subset U$, 则

$$I_\phi(f_1 + f_2) < I_\phi(f_1) + I_\phi(f_2) + \epsilon.$$

我们略去证明, 具体可以参考 [1, 1.10].

接下来构造一个空间, 利用次线性泛函逼近一个线性泛函. 令

$$X = \prod_{f \in C_c^+(G)} \left[\frac{1}{(f_0 : f)}, (f : f_0) \right],$$

采用乘积拓扑使其为紧空间. 将 I_ϕ 作为 $\prod_{f \in C_c^+(G)} I_\phi(f)$ 嵌入, 取 e 的紧邻域 U , 得到相关联的闭集 $K_U = \overline{\{I_\phi : \text{Supp } \phi \subset U\}}$. 由于

$$\bigcap_{i=1}^n K_{U_i} \supset K_{\bigcap_{i=1}^n U_i},$$

则由 2.17.Urysohn 引理可以构造 $I_{\phi_0} \in K_{\bigcap_{i=1}^n U_i}$. $\{K_U\}$ 为一族有限交非空的闭集, 由 X 的紧性, 存在 $\prod_{f \in C_c^+(G)} I(f) \in \bigcap K_U$, I 即为我们得到的线性泛函.

命题 2.21. 上述定义的 I 为 G 上的一个线性泛函, 由 2.18. 知其对应一个 G 上的 Haar 测度 μ , 可以证明 μ 在相差一个常数相乘的意义下唯一.

我们略去证明, 具体可以参考 [1, P15-19].

第 3 节 商积分公式

拥有群结构的拓扑空间可以做商, 我们讨论商结构和积分的相容性, 为接下来的讨论做准备.

对于一个局部紧的拓扑群 G 及其闭子群 H , 由 2.7., 商群 G/H 也为局部紧的拓扑群. 如果 H 为闭子群, 对于 $f \in C_c(G)$, 固定 $x \in G$, 可以定义 H 上函数 $f(xh)$. 因为 $f \in C_c(G)$, 所以 $\text{Supp } f(xh) \subset x^{-1}\text{Supp } f \cap H$ 为紧的, $f(xh)$ 显然是连续的, 故而 $f(xh) \in C_c(H)$. 因此可以定函数 $f^H(x) = \int_H f(xh)dh$, 对于 $[x_1] = [x_2] \in G/H$ 有 $f^H(x_1) = f^H(x_2)$, $f^H(x)$ 也可以看作是在 G/H 上的函数.

引理 2.22. 这样定义的 $f^H(x) \in C_c(G/H)$, 并且映射

$$f \mapsto f^H$$

为 $C_c(G)$ 到 $C_c(G/H)$ 的满射.

我们略去证明, 具体可以参考 [4, 1.5.1].

定理 2.23. 如果有一个局部紧的拓扑群 G , H 为其闭子群, 给定 G 上 Haar 测度, H 上取子测度, 存在 G/H 上唯一的 Haar 测度 ν , 使得对所有的 $f \in C_c(G)$ 成立

$$\int_G f(x)dx = \int_{G/H} \int_H f(xh)dhdx, \quad (2.4)$$

ν 被称作商测度. 事实上, 对于 $f \in L^1(G)$ 该式仍然成立.

我们略去证明, 具体可以参考 [4, 1.5.3].

第 4 节 傅里叶变换

定义 2.24. (酉特征) 局部紧 Abel 群 A 上一个连续的群同态: $\chi: A \rightarrow \mathbb{T}$, $\mathbb{T} = \{x \in \mathbb{C} : |x| = 1\}$, 为 A 上一个酉特征 (Unitary Character), 有些文献也直接称作特征 (Character).

酉特征全体赋予合适的拓扑可以得到一个局部紧 Abel 群.

定义 2.25. (紧开拓扑) 对于一个局部紧 Abel 群 A , 定义集合

$$W(K, U) = \{\chi : \chi(K) \subset U\}.$$

其中, χ 是 A 上酉特征, K 为 A 中紧集, U 为 $\mathbb{T}$ 中开集. 则紧开拓扑由所有可能的集合 $W(K, U)$ 生成, 用 $\hat{A}$ 表示 A 上赋予了紧开拓扑的酉特征全体.

注 2.1 $W(K, U)$ 在 1 处形成拓扑基, 但一般的, 它们只能成为该拓扑空间的子基 (Subbase), 即, 其有限交全体构成拓扑基.

$\hat{A}$ 的群结构为: $(\chi_1 \chi_2)(x) = \chi_1(x) \chi_2(x)$, 可以验证 $\hat{A}$ 由此成为一个 Abel 群.

命题 2.26. $\hat{A}$ 是局部紧 Abel 群.

我们略去证明, 具体可以参考 [4, 3.2.1].

当 $\hat{A}$ 也具有局部紧 Abel 群结构后, 可以得到其上 Haar 测度, 因此可以定义其上的函数以及积分.

定义 2.27. (卷积) 对于函数 $f, g \in L^1(A)$, 定义 $f * g$ 为

$$f * g(x) = \int_A f(y)g(x-y)dy. \quad (2.5)$$

命题 2.28. $f * g \in L^1(A)$, 并且 $f * g = g * f$.

我们略去证明, 具体可以参考 [4, 1.6.2, 1.6.4].

定义 2.29. (傅里叶变换) 对于 $f \in L^1(A)$, 其傅里叶变换为一个函数 $\hat{f}: \hat{A} \rightarrow \mathbb{C}$:

$$\hat{f}(\chi) = \int_A f(x) \overline{\chi(x)} dx. \quad (2.6)$$

由于 $f \in L^1(A)$, $|\overline{\chi(x)}| \leq 1$, $\hat{f}(\chi)$ 总是存在的.

定理 2.30. (Pontryagin 对偶) Pontryagin 映射 $\delta: A \rightarrow \hat{\hat{A}}$:

$$x \mapsto \delta_x,$$

其中 $\delta_x(\chi) = \chi(x)$, 构成两个局部紧 Abel 群间同构.

我们略去证明, 具体可以参考 [4, 3.5.5].

定理 2.31. (傅里叶逆变换公式) 对于一个局部紧 Abel 群 A , dx 为其上 Haar 测度, 那么存在唯一的 $\hat{A}$ 上对偶测度 $d\chi$, 使得如果 $f \in L^1(A)$, 有 $\hat{f} \in L^1(\hat{A})$, 那么对于几乎所有的 $x \in A$, 有

$$f(x) = \hat{f}(\delta_{x^{-1}}) = \int_{\hat{A}} \hat{f}(\chi) \chi(x) d\chi. \quad (2.7)$$

特别的, 如果 f 连续, 那么对所有的 $x \in A$, (2.7) 都成立.

我们略去证明, 具体可以参考 [4, 3.5.8].

第 5 节 Poisson 求和公式

Poisson 求和公式反映了一个局部紧 Abel 群 A 与其商群 A/B 的关系, 这里 B 为 A 的一个闭子群.

命题 2.32. 如果有局部紧 Abel 群的正合列

$$1 \rightarrow B \xrightarrow{i} A \xrightarrow{p} A/B \rightarrow 1, \quad (2.8)$$

那么

$$1 \rightarrow \widehat{A/B} \rightarrow \hat{A} \rightarrow \hat{B} \rightarrow 1 \quad (2.9)$$

也是局部紧 Abel 群的正合列.

证明. 这是因为: $B^\perp = \{\chi \in \hat{A} : \chi(x) = 1, \forall x \in B\} \simeq \widehat{A/B}$. 对任何的 $\chi \in B^\perp$, 可以定义 $\tilde{\chi}(xB) = \chi(x)$ 得到 $\tilde{\chi} \in \widehat{A/B}$; 反之也可以从 $\tilde{\chi}$ 得到 $\chi \in B^\perp$.

另一方面, $\hat{A}/B^\perp \simeq \hat{B}$. 这是因为对于 $\chi \cdot B^\perp \in \hat{A}/B^\perp$ 可以得到 $\chi|_{B^\perp} \in \hat{B}$; 反之也可以从 $\chi \in \hat{B}$ 得到 $\chi \cdot B^\perp \in \hat{A}/B^\perp$. $\square$

定理 2.33. (Poisson 求和公式) A 为局部紧 Abel 群, B 是它的闭子群, 对于 $f \in L^1(A)$, 定义 $f^B(xB) = \int_B f(xb)db$, $f^B \in L^1(A/B)$. 由于 $\widehat{A/B} \simeq B^\perp$, 则有 $\widehat{f^B} = \hat{f}|_{B^\perp}$. 如果 $\hat{f}|_{B^\perp} \in L^1(B^\perp)$, 那么

$$\int_B f(xb)db = \int_{B^\perp} \hat{f}(\chi) \chi(x) d\chi. \quad (2.10)$$

我们略去证明, 具体可以参考 [4, 3.6.3].

例子 2.34. 令 $A = \mathbb{R}$, $B = \mathbb{Z}$, 由于 $\mathbb{R}$ 到 $\widehat{\mathbb{R}}$ 的映射 $\phi: x \mapsto \chi(y) = e^{-2\pi ixy}$ 给出同构 $\mathbb{R} \simeq \widehat{\mathbb{R}}$, 则可以看出 $\mathbb{Z}^\perp \simeq \mathbb{Z}$. 若 $f \in L^1(\mathbb{R})$, $\hat{f}|_{\mathbb{Z}} \in L^1(\mathbb{Z})$, 则有

$$\sum_{k \in \mathbb{Z}} f(x+k) = \sum_{k \in \mathbb{Z}} \hat{f}(k) e^{2\pi i k x}. \quad (2.11)$$

第三章 准备工作

第 1 节 整体域与局部域的特点

1.1 局部域与整体域的定义

定义 3.1. 整体域是 $\mathbb{Q}$ 的有限扩张或 $\mathbb{F}_p((t))$ (p 为素数) 的有限扩张. 我们也称前者为数域, 后者为整体函数域.

将数域与函数域放在一起考虑是因为它们具有相似的结构:

- 整数环 (ring of integers) $\mathcal{O}$, 通常为 $\mathbb{Z}$, $\mathbb{F}_p[t]$ 或 $\mathbb{F}_p[1/t]$ 的整闭包 (integral closure).
- 整数环 $\mathcal{O}$ 中素理想 $\mathfrak{p}$ 诱导的不同度量.

定义 3.2. 局部域为 $\mathbb{R}$, $\mathbb{Q}_p$ 或 $\mathbb{F}_p((t))$ (p 为素数) 的有限可分扩张.

1.2 域上的赋值与完备化

这一小节引入赋值的定义. 通过不同的赋值, 从整体域出发可以得到许多局部域, 对局部域的研究放在一起就能得到整体域上的信息.

定义 3.3. (赋值) 设 K 是一个域, 如果 $|\cdot|: K \rightarrow [0, +\infty)$ 成立

- 1) $|x| \geq 0$, $|x| = 0$ 当且仅当 $x = 0$.
- 2) $|xy| = |x||y|$.
- 3) $|x + y| \leq |x| + |y|$.

那么称 $|\cdot|$ 为 K 上一个赋值 (valuation), 也叫做绝对值 (absolute value).

平凡赋值是使得对所有的 $x \in K$, $|x| = 0$ 的赋值, 研究这样的赋值意义不大, 本文接下来谈论的所有赋值都假定为非平凡赋值.

定义 3.4. (阿基米德性) 如果一个赋值 $|\cdot|$ 使得 $\{|n|\}_{n \in \mathbb{N}}$ 有上界, 则称该赋值是非阿基米德的 (nonarchimedean), 否则是阿基米德的 (Archimedean).

命题 3.5. 一个赋值 $|\cdot|$ 为非阿基米德赋值当且仅当满足强三角不等式 (strong triangle inequality):

$$|x + y| \leq \max\{|x|, |y|\}.$$

我们略去证明, 具体可以参考 [5, 3.6]. $\mathbb{R}, \mathbb{C}$ 上的绝对值或模长即为赋值, 它们具有阿基米德性, 而一般的赋值不一定具备. 对于非阿基米德赋值 $|\cdot|$, 令 $v(x) = -\log|x|$, $x \neq 0$, $v(0) = \infty$, 则得到了一个指数赋值 (exponential valuation).

定义 3.6. (指数赋值) 如果有一个域 K , $v: K \rightarrow \mathbb{R} \cup \{\infty\}$ 成立

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

则称 v 为 K 上一个指数赋值. 如果有非阿基米德赋值 $|\cdot|$, 可以验证 $v(\cdot) = -\log|\cdot|$ 为一个指数赋值, $|\cdot|$ 也称作 v 相伴的乘性赋值 (multiplicative valuation), 写作 $|\cdot|_v$.

对于非阿基米德赋值, 我们统称乘性赋值和指数赋值为赋值, 并可能使用 v 与 $|\cdot|_v$ 指代同一赋值.

赋值诱导 K 上的度量 (metric): $d(x, y) = |x - y|$. 因此一个有非平凡赋值的域 K 不仅有代数结构, 也因此获得了拓扑结构, 而等价的赋值诱导相同的拓扑.

命题 3.7. K 上两个赋值 $|\cdot|_1, |\cdot|_2$ 等价当且仅当存在一个实数 $s > 0$ 使得对所有的 $x \in K$, 有

$$|x|_1 = |x|_2^s.$$

我们略去证明, 具体可以参考 [5, Ch2, 3.3].

定义 3.8. K 上一个非平凡赋值的等价类称为 K 上一个位置 (place), 记为 v . 记 $|\cdot|_v$ 为其等价类中的某一赋值, K_v 为其完备化. 如果 v 是非阿基米德的, v 本身也可以作为赋值的符号. 记 K 上所有位置组成的集合为 M_K .

因此, 我们可以对一个有赋值的域在每一个位置上做**完备化** (completion), 得到一个完备的域. 由于等价的赋值诱导相同的完备化, 所以 K 上的赋值的等价类与 K 的完备化一一对应. 事实上, 阿基米德赋值的完备化是很好研究的, 因为我们有以下定理:

定理 3.9. (Ostrowski) 如果 K 是一个在阿基米德赋值 $|\cdot|$ 下完备的域, 那么存在一个从 K 到 $\mathbb{R}$ 或 $\mathbb{C}$ 的同构 σ , 对所有的 $x \in K$ 满足,

$$|x| = |\sigma x|^s,$$

其中常数 $s \in (0, 1]$.

我们略去证明, 具体可以参考 [5, Ch2, 4.2]. 这说明任何域在阿基米德赋值下的完备化在代数和拓扑结构上都同构于 $\mathbb{R}$ 或 $\mathbb{C}$.

1.3 整体域上的赋值与完备化

整体域上赋值与其整数环的素理想相关, 数域上的结论与函数域上的结论可以分别在 [5] 和 [10] 中找到.

定义 3.10. (Dedekind 整环) 如果一个环是诺特的 (noetherian)、整闭的 (integrally closed) 且每个非零素理想都是极大理想, 那么称其为 **Dedekind 整环** (Dedekind domain).

定理 3.11. 对于一个整体域 K , 其整数环 $\mathcal{O}_K$ 为一个 Dedekind 整环.

我们略去证明, 具体可以参考 [5, Ch1, 3.1] 与 [10, 5.7].

不同于 UFD, $\mathcal{O}_K$ 的元素并不能唯一 (相差一个单位 (unit) 的意义下) 分解为素元 (prime element) 的乘积, 但是其理想满足类似的“唯一分解”性质.

定理 3.12. 对于一个 Dedekind 整环 $\mathcal{O}$, 每一个真理想 $\mathfrak{a}$ 都可以分解为非零素理想的乘积, 即

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$

该分解在相差一个置换下唯一.

我们略去证明, 具体可以参考 [5, Ch1, 3.3].

整数环的唯一分解性质说明不同的素理想可以诱导不同的 (非阿基米德的) 赋值, 以 $\mathbb{Q}$ 为例.

例子 3.13. 我们考虑平凡整体域 $\mathbb{Q}$, $M_{\mathbb{Q}}$ 中的元素为:

- 所有素理想 (p) 诱导的非阿基米德赋值 v_p . v_p 满足对于 $\mathbb{Q}$ 中的元素 $x = p^t \frac{n}{m}$, $t \in \mathbb{Z}$, $(m, n, p) = 1$, 有 $v_p(x) = t$.
- 通常的绝对值 $|\cdot|$, 是唯一的阿基米德赋值.

可以证明这些赋值互不等价, 并且代表了 $\mathbb{Q}$ 上全部的赋值, 证明参考 [5, Ch2, 3.7]. $\mathbb{Q}$ 在所有非阿基米德赋值上的完备化记作 $\mathbb{Q}_p$, 在阿基米德赋值上的完备化即为实数全体 $\mathbb{R}$.

因此, 对于一个数域 K , $\mathbb{Z}$ 中的素理想 (p) “上升到” $\mathcal{O}_K$ 中可能分裂成不同素理想的乘积, 也即意味着位置 v_p 在 $\mathcal{O}_K$ 可能分裂成不同的赋值.

定义 3.14. 对于整体域扩张 K/k , k 中整数环的素理想 $\mathfrak{p}$ 满足

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

$\mathfrak{P}_i$ 为 $\mathcal{O}$ 中不同的素理想. 如果 $e_i = 1 (\forall i)$, 则称 $\mathfrak{p}$ 对应的位置 v 在 K 中不分歧 (unramified); 反之则称其分歧 (ramified).

一般整体域上由素理想定义非阿基米德赋值的方式需要引入更多的定义, 但是本质上与 $\mathbb{Q}$ 类似.

对于一个整体域 K , 其在不同赋值上完备化得到的域即为局部域. 由于其在阿基米德赋值上完备的局部域只有两种结构情况, 因而我们研究的重点是在非阿基米德赋值上完备的局部域 K_v . 它们有一些相似的结构:

- 赋值环 (valuation ring), 即 $\mathcal{O}_v = \{x \in K : v(x) \geq 0\}$. 可以证明 $\mathcal{O}_v$ 为一个局部环, 同时也为主理想整环 (P.I.D).
- 赋值环的唯一极大理想 $\mathfrak{p}_v$.
- 一致化子 (uniformizer) π , 为 $\mathfrak{p}_v$ 的生成元, 其为一个素元.
- 剩余类域 (redidue (class) field) $\mathfrak{f}_v = \mathcal{O}_v / \mathfrak{p}_v$.
- $\mathcal{O}_v$ 中元素 x 的表达式为 $u\pi^n$, 其中 $u \in \mathcal{O}_v^\times$, $n \in \mathbb{Z}_{\geq 0}$.
- K_v 在加法意义下为局部紧 Abel 群, 赋值环 $\mathcal{O}_v$ 是一个紧开球.

1.4 正规化的赋值

在 $\mathbb{Q}$ 的例子中选择的赋值是一类标准定义的赋值, 对于一般的局部域也有标准赋值.

定义 3.15. (正规化的赋值) 对于一个局部域 F , 有正规化的赋值 (Normalized Valuation) $|\cdot|_v$ 如下:

- $F \cong \mathbb{R}$, $|\cdot|_v$ 即为通常的绝对值.
- $F \cong \mathbb{C}$, $|\cdot|_v$ 即为通常的模长的平方.
- $F \cong K_v$ 是非阿基米德的, 对于 $x \in K_v$, $|x|_v = (\#\mathfrak{f}_v)^{-v(a)}$.

正规化的赋值在考虑进分析方法后有良好的相容性质.

命题 3.16. 对于一个非阿基米德的局部域 K_v , μ 为 K_v 上非平凡的 Haar 测度, $|\cdot|_v$ 为正规化的赋值, 则对于所有的 $x \in K_v$, S 为一个可测集, 有

$$\mu(xS) = |x|_v \mu(S). \quad (*)$$

在此意义下, $|\cdot|_v$ 是唯一的与 K_v 拓扑相容的赋值.

证明. 显然 $x = 0$ 时成立, 以下假设 $x \neq 0$. 记 K_v 上可测集全体为 $\mathcal{M}$. $\mu : \mathcal{M} \rightarrow [0, +\infty]$ 为一个 Haar 测度,

$$\begin{aligned}\mu_x : \mathcal{M} &\rightarrow [0, +\infty] \\ S &\mapsto \mu(xS)\end{aligned}$$

也为一个 Haar 测度. 由 Haar 测度的唯一性, 存在一个与 x 相关的常数 c_x 成立 $\mu_x = c_x \mu$. 任取 S 使得 $\mu(S) \neq 0$, 对于 $x, y \in K_v$ 有

$$c_{xy} = \frac{\mu_{xy}(S)}{\mu(S)} = \frac{c_x \mu_y(S)}{\mu(S)} = c_x c_y.$$

因此, 映射

$$\begin{aligned}K_v^\times &\rightarrow \mathbb{C}^\times \\ x &\mapsto c_x\end{aligned}$$

为一个群同态. 因为 $\mathcal{O}_v$ 是紧的, 由 Haar 测度的定义有 $\mu(\mathcal{O}_v) < \infty$, 故而

$$c_x = \frac{\mu(x\mathcal{O}_v)}{\mu(\mathcal{O}_v)},$$

而

$$\mu(\mathcal{O}_v) = [\mathcal{O}_v : x\mathcal{O}_v] \mu(x\mathcal{O}_v) = (\#\mathcal{O}_v/\mathfrak{p}_v)^{v(x)} \mu(x\mathcal{O}_v),$$

这说明 $c_x = |x|_v$.

假设有另一赋值 $|\cdot|_{v'}$ 也使得 (*) 成立并且与 K_v 的拓扑相容, 那么 $|\cdot|_{v'}$ 与 $|\cdot|_v$ 等价, 即存在常数 $s > 0$ ($s \neq 0$) 使得 $|\cdot|_{v'}^s = |\cdot|_v$. 这说明对于任何的 $x \in K_v, S \in \mathcal{M}$, 有

$$\left(\frac{\mu(xS)}{\mu(S)} \right)^s = \frac{\mu(xS)}{\mu(S)},$$

取 $v(x) = 1, S = \mathcal{O}_v$ 即知矛盾, 唯一性得证.

□

1.5 局部域与整体域的公理化定义

在上述讨论中可以利用赋值抽象出局部域和整体域的一些性质, 这些抽象性质完全刻画了它们.

首先注意到对于非阿基米德的局部域 K_v , 它的正规化赋值 v 满足 $v(K_v^\times) = \mathbb{Z}$, 这是非阿基米德局部域的重要性质.

定义 3.17. (离散赋值) 一个域 K 上的赋值 v 的像集如果有最小正数 s , 则称为离散赋值.

在这个情况下, 可以验证 $v(K^\times) = s\mathbb{Z}$.

定义 3.18. 局部域的另一等价定义是 $\mathbb{R}, \mathbb{C}$ 或具有有限剩余类域的完备离散赋值环的分式域 (fraction field of discrete valuation ring with finite residue field).

定义等价的证明参考 [5, Ch2, 5.2].

而对于整体域, 在 $\mathbb{Q}$ 的例子中可以看出, 选取正规化的赋值有

$$\forall v \in M_{\mathbb{Q}}, x \neq 0, \prod_{v \in M_{\mathbb{Q}}} |x|_v = \prod_{v_p \in M_{\mathbb{Q}}} |x|_{v_p} \times |x| = 1.$$

这是描述整体域的重要性质.

命题 3.19. (乘法公式) 对于一个整体域 K , 其在每个位置 v 上完备化得到的局部域记为 K_v , 选取正规化的赋值 v 有乘法公式 (product formula) 成立:

$$\forall x \neq 0, x \in K, \prod_{v \in M_K} |x|_v = 1. \quad (3.1)$$

定义 3.20. 整体域的另一等价定义是一个至少有一个非平凡赋值的域 K , 其满足在每个位置 v 上的完备化都为局部域 K_v , 并且正规化的赋值 v 满足乘法公式 (product formula).

定义等价的证明参考 [8].

第 2 节 局部域上傅立叶变换

对于阿基米德的局部域上傅立叶变换的结论我们已经很熟悉, 这一节将在非阿基米德的局部域上推广.

2.1 标准特征

将局部域看作加法群, 局部域 F 上可以取**标准特征** (Standard Character) χ_F .

- 如果 $F_0 = \mathbb{R}$, 则取 $\chi_{F_0}(x) = e^{-2\pi i x}$.
- 如果 $F_0 = \mathbb{Q}_p$, 对于 $x = \sum_{n \geq k} a_n p^n$, $0 < a_n \leq p-1$, 定义

$$\lambda_{F_0}(x) = \begin{cases} \sum_{n \geq k}^{-1} a_n p^n & k \leq -1 \\ 0 & k \geq 0 \end{cases}, \chi_{F_0}(x) = e^{2\pi i \lambda_{F_0}(x)}.$$

- 如果 $F_0 = \mathbb{F}_p((t))$, 对于 $x = \sum_{n \geq k} a_n t^n$, 定义

$$\lambda_{F_0}(x) = \begin{cases} \frac{a_{-1}}{p} & k \leq -1 \\ 0 & k \geq 0 \end{cases}, \chi_{F_0}(x) = e^{2\pi i \lambda_{F_0}(x)}.$$

- 如果 F 是上述 F_0 的有限扩张, 定义

$$\chi_F(x) = e^{2\pi i \lambda_{F_0}(\text{Tr}_{F/F_0}(x))}.$$

命题 3.21. 对任何局部域 F 上的非平凡特征 χ , 对任何的 $a \in F$, 定义 $\chi_a(x) = \chi(ax)$, 则有局部紧 Abel 群同构 $F \cong \widehat{F}$:

$$\begin{aligned} \Psi : F &\rightarrow \widehat{F} \\ a &\mapsto \chi_a. \end{aligned}$$

我们略去证明, 具体可以参考 [7, Theorem 4.4].

命题 3.22. 对于一个整体域 K , 其在除了有限个位置上的完备化 K_v 有局部紧 Abel 群同构 $\mathcal{O}_v \cong \mathcal{O}_v^\perp$:

$$\begin{aligned} \Phi : \mathcal{O}_v &\rightarrow \widehat{K_v/\mathcal{O}_v} \cong \mathcal{O}_v^\perp \\ a &\mapsto \chi_a, \end{aligned}$$

注意此同构是在命题3.21.的意义下.

证明. 这是由于对于整体域 $K/\mathbb{Q}$ 或 $\mathbb{F}_p(T)$ 为有限可分扩张, 只有有限个位置在 K 中分歧 ([5, Ch1, 8.4]). 对于不分歧的局部域扩张 F/F_0 , 定义

$$\mathcal{D}^{-1} = \{x \in K_v : \text{Tr}(xy) \text{ 在 } F_0 \text{ 的赋值环中, 对所有的 } y \in \mathcal{O}_v\},$$

可以证明 $\mathcal{D}^{-1} = \mathcal{O}_v$.

在这些不分歧的位置 v 上, 首先对于 $a \in \mathcal{O}_v$, χ_a 作为 K_v 的特征, $\chi_a|_{\mathcal{O}_v} = 1$ 说明 $\chi_a \in \widehat{K_v/\mathcal{O}_v}$.

另一方面, 对任何的 $a \notin \mathcal{O}_v$, 由于 $\mathcal{D} = \mathcal{O}_v$, 总可以选取合适的 $b \in \mathcal{O}_v$ 使得 $\chi_{K_v}(ab) \neq 1$, 由命题3.21.的结论知即意味着 $\chi_a \notin \widehat{K_v/\mathcal{O}_v}$. 最后, $\widehat{K_v/\mathcal{O}_v} \cong \mathcal{O}_v^\perp$ 由命题2.32.的证明得到. $\square$

2.2 标准测度

由定理2.31.知道, 给定局部域 F 上一个 Haar 测度 dx , 有唯一的对偶测度 $d\chi$ 使得 $L^1(F)$ 上傅立叶逆变换成立:

$$f(x) = \hat{\hat{f}}(\delta_{-x}) = \int_{\hat{F}} \hat{f}(\chi) \chi(x) d\chi.$$

而由命题3.21.知 χ_F 诱导同构 $F \cong \hat{F}$, 因而由 Haar 测度唯一性, 有 $d\chi = r dx$, r 为常数. 通过对 dx 进行调整, 不妨取 dx 为自对偶的, 即 $d\chi = dx$.

定义 3.23. 记 dx_F 为 F 上相对于标准特征自对偶的 Haar 测度, 则 dx_F 为 F 上的标准测度 (Standard Measure).

因此, 给定 F 上一个自对偶的 Haar 测度 dx_F , 有傅里叶逆变换公式成立:

$$f(x_F) = \hat{\hat{f}}(-x_F) = \int_F \hat{f}(y_F) \chi_F(y_F x_F) dy_F. \quad f \in L^1(F), \hat{f} \in L^1(F) \quad (3.2)$$

可以证明, 局部域 F 上的标准测度为:

- 如果 $F = \mathbb{R}$ 或 $\mathbb{C}$, 则 dx_F 为 Lebesgue 测度.
- 如果 $F \cong K_v$ 是非阿基米德的, 赋值环为 $\mathcal{O}_v$, 那么定义

$$\mathcal{D} = \{x \in K_v : \text{Tr}(xy) \text{ 在 } F_0 \text{ 的赋值环中, 对所有的 } y \in \mathcal{O}_v\}^{-1},$$

可以证明 $\mathcal{D}$ 为 $\mathcal{O}_v$ 中的一个理想. 标准测度 dx_F 为使得 $\text{Vol}(\mathcal{O}_v)$ 取值 $\#(\mathcal{O}_v/\mathcal{D})^{-\frac{1}{2}}$ 的测度.

2.3 Schwartz-Bruhat 函数

定义 3.24. 对于 $\mathbb{R}^n$, 如果 f 满足 $f \in C^\infty(\mathbb{R}^n)$, 且对任何 $\alpha, \beta \in \mathbb{N}^n$, f 的导数成立 $\sup_{x \in \mathbb{R}^n} \left| x^\alpha \frac{d^\beta f(x)}{dx^\beta} \right| < +\infty$, 则称其为 $\mathbb{R}^n$ 上的 **Schwartz 函数**. 将 $\mathbb{R}^n$ 上所有的 Schwartz 函数记为 $\mathcal{S}(\mathbb{R}^n)$.

通过 $\mathbb{R}^n$ 上傅里叶变换的理论, 可以知道对于 $f \in \mathcal{S}(\mathbb{R}^n)$, 有 $\hat{f} \in \mathcal{S}(\mathbb{R}^n)$, 且傅里叶逆变换的成立说明 Schwartz 函数在傅里叶变换下不变.

定义 3.25. (光滑函数) 对于一个非阿基米德的局部域 F , 由于 F 上的函数不能求导, 如果 $f : F \rightarrow \mathbb{C}$ 为局部常值的, 那么称 f 为 F 上的光滑函数 (Smooth Function). 将 F 上所有的光滑函数记为 $C^\infty(F)$.

定义 3.26. (Schwartz-Bruhat 函数) 对于局部域 F ,

- 若 $F = \mathbb{R}, \mathbb{C}$, $f \in \mathcal{S}(F)$,

- 若 F 是非阿基米德的, $f \in C_c^\infty(F)$,

则统称其为局部域 F 上的 **Schwartz-Bruhat** 函数. 将 F 上所有的 Schwartz-Bruhat 函数记为 $\mathcal{S}(F)$.

命题 3.27. 对于一个非阿基米德的局部域 F , $\mathcal{S}(F)$ 中的函数为形如 $\mathbb{1}_{D_\alpha}$ (D_α 为 F 中紧开球) 函数的 $\mathbb{C}$ -线性组合.

证明. 对于 $f \in \mathcal{S}(F)$, $\text{Supp} f$ 被紧开球 $\{D_i\}_{i=1}^n$ 覆盖, f 在 D_i 上为常值 c_i , 注意到在 F 的拓扑中任何相交的开球必然相互包含, 合并得到

$$f = \sum_{j=1}^m c_j \mathbb{1}_{D_j}.$$

□

命题 3.28. 对于一个局部域 F , 取标准测度 dx_F 使得傅里叶逆变换成立, 那么对于 $f \in \mathcal{S}(F)$, 有 $\hat{f} \in \mathcal{S}(F)$.

证明. 只需要对 F 为非阿基米德的局部域证明. 此时 $F = K_v$, 有赋值环 $\mathcal{O}_v$.

断言: 如果 $f = \mathbb{1}_{\mathcal{O}_v}$, 那么 $\hat{f} = \text{Vol}(\mathcal{O}_v)f$.

证明. 对于

$$\hat{f}(\chi) = \int_{K_v} f(x) \chi(x) dx = \int_{\mathcal{O}_v} \chi(x) dx,$$

若 $\chi|_{\mathcal{O}_v} \neq 1$, 则存在 $y_0 \in \mathcal{O}_v$ 使得 $\chi(y_0) \neq 1$. 那么

$$\begin{aligned} \hat{f}(\chi) &= \int_{\mathcal{O}_v} \chi(x) dx \\ &= \int_{\mathcal{O}_v - y_0} \chi(x + y_0) d(x + y_0) \\ &= \chi(y_0) \int_{\mathcal{O}_v} \chi(x) dx, \end{aligned}$$

这说明 $\hat{f}(\chi) = 0$.

而对于 $\chi|_{\mathcal{O}_v} = 1$, $\hat{f}(\chi) = \text{Vol}(\mathcal{O}_v)$, 这说明 $\hat{f} = \text{Vol}(\mathcal{O}_v) \mathbb{1}_{\mathcal{O}_v^\perp}$. □

由于一般的 f 为 $\mathbb{1}_{D_\alpha}$ (D_α 形如 $y + \pi^n \mathcal{O}_v$, $y \in K_v$, π 为 $\mathcal{O}_v$ 中素理想 $\mathfrak{p}_v$ 的一致化子) 的 $\mathbb{C}$ -线性组合, 其证明是类似的, 可以参考 [9, P141-144] (该证明只对 $\mathbb{Q}_p$ 证明, 但事实上适用于所有非阿基米德的局部域). □

命题 3.29. 对于局部域 F 上的 Schwartz-Bruhat 函数 f, g , 有

$$\widehat{f * g} = \hat{f} \hat{g}. \quad (3.3)$$

证明. 可以直接证明.

$$\begin{aligned}
\widehat{f * g}(z) &= \int_F f(y)g(x-y)dy \chi_F(zx)dx \\
&= \int_F f(y)g(x)\chi_F(zx+zy)dydx && x-y \text{ 替代 } x \\
&= \int_F f(y)\chi_F(zy)dy \int_F g(x)\chi_F(zx)dx && \text{Fubini 定理} \\
&= \hat{f}(z)\hat{g}(z).
\end{aligned}$$

□

定义 3.30. (Schwartz-Bruhat 函数收敛) 对于一个阿基米德的局部域 F , 有一列 $\{f_n\} \subset \mathcal{S}(F)$, $f \in \mathcal{S}(F)$, 如果 f_n, f 的支集都包含在同一个紧集当中, 有

$$\frac{d^\alpha f_n}{dx^\alpha} \Rightarrow \frac{d^\alpha f}{dx^\alpha}, \quad \forall \alpha \in \mathbb{N}^i, i = 1, 2$$

则称 $\{f_n\}$ 收敛于 f .

对于一个非阿基米德的局部域 F , 有一列 $\{f_n\} \subset \mathcal{S}(F)$, $f \in \mathcal{S}(F)$, 如果存在 $a, b \in F$, f_n, f 的支集都包含在同一个紧集 $a\mathcal{O}_v$ 当中, 且 $a\mathcal{O}_v$ 为 $b\mathcal{O}_v$ -不变的, 有

$$f_n(x) \rightarrow f(x), \quad \forall x \in F$$

则称 $\{f_n\}$ 收敛于 f .

命题 3.31. 对于一个局部域 F , 傅立叶变换 $\mathcal{F} : \mathcal{S}(F) \rightarrow \mathcal{S}(F)$ 是同胚映射, 即 $\mathcal{F}$ 与 $\mathcal{F}^{-1}$ 均连续.

我们略去证明, 具体可以参考 [11, Theorem 3.2].

Schwartz-Bruhat 函数是对 Schwartz 函数定义的延拓, 也是我们将要做变换的主要对象.

2.4 缓增广义函数

这一小节讨论的结论对于 $\mathbb{R}^n$ 都成立, 因此只对 F 是非阿基米德的局部域进行证明.

定义 3.32. 对于一个局部域 F , 其上的缓增广义函数 (tempered distribution) 为 $\mathcal{S}(F)$ 的连续线性泛函全体. 将 F 上所有的缓增广义函数记为 $\mathcal{S}'(F)$.

定义 3.33. (缓增广义函数收敛) 如果有一列 $\{F_n\} \in \mathcal{S}'(F)$, $F \in \mathcal{S}'(F)$, 对于所有的 $f \in \mathcal{S}(F)$ 有

$$F_n(\varphi) \rightarrow F(\varphi), \text{ 对所有的 } \varphi \in \mathcal{S}(F),$$

则称 $\{F_n\}$ 在缓增广义函数的意义下收敛于 F .

对于光滑函数 $\varphi \in C^\infty(F)$, $f \in \mathcal{S}(F)$, 如果定义

$$\varphi(f) := \int_F \varphi(x)f(x)dx, \quad (3.4)$$

则有光滑函数全体 $C^\infty(F) \subset \mathcal{S}'(F)$.

对于 F 上的 Schwartz-Bruhat 函数 f 与光滑函数 φ 有

$$(\varphi * f)(x) = \int_F \varphi(y)f(x-y)dy,$$

若将 φ 看作缓增广义函数, 定义符号 L_y , L_y 作用在 f 上成立

$$L_y f(x) = f(x-y).$$

又定义符号 θ , θ 作用在函数 f 上成立

$$\theta f(x) = f(-x),$$

则上式可以写成

$$(\varphi * f)(x) = \varphi(L_x \theta f). \quad (3.5)$$

由于此时 $\varphi * f$ 也为光滑函数, 也可以看作缓增广义函数, 则

$$(\varphi * f)(g) = \varphi(\theta f * g). \quad g \in \mathcal{S}(F)$$

定义 3.34. (缓增广义函数卷积) 对于一个局部域 F , $u \in \mathcal{S}'(F)$, $f \in \mathcal{S}(F)$, 定义 $u * f$ 为

$$(u * f)(g) := u(\theta f * g). \quad g \in \mathcal{S}(F)$$

可以看出, 如果该缓增广义函数 u 为一个函数 φ , 那么缓增广义函数卷积与通常的函数卷积相容.

注意到由 Fubini 定理, 对于 $f, g \in \mathcal{S}(F)$ 有乘法等式 (multiplication identity) 成立:

$$\int_F \hat{\varphi}(x)f(x)dx = \int_F \varphi(x)\hat{f}(x)dx. \quad (3.6)$$

定义 3.35. (缓增广义函数的傅立叶变换) 对于一个局部域 F , $u \in \mathcal{S}'(F)$, 定义 $\hat{u}$ 为

$$\hat{u}(f) = u(\hat{f}), \quad f \in \mathcal{S}(F).$$

可以看出, 由于 $\mathcal{F}$ 为 $\mathcal{S}(F)$ 上的拓扑同构, $\hat{u}$ 仍属于 $\mathcal{S}'(F)$, 并且 $\mathcal{F} : \mathcal{S}'(F) \rightarrow \mathcal{S}'(F)$ 在缓增广义函数的意义下连续.

引理 3.36. (p -进版本) 对于一个非阿基米德的局部域 F , $f \in \mathcal{S}(F)$, $\varphi \in C^\infty(F)$, 有

$$\widehat{\varphi f} = \hat{\varphi} * \hat{f}.$$

证明. 取 $\{U_\alpha\}$ 为 K_v 中所有越来越大的紧开子群, 将 φ 看作缓增广义函数, 因为对于足够大的 U_α , 由于 f 是紧支的,

$$\int_{U_\alpha} \varphi(x)f(x)dx = \int_{K_v} \varphi(x)f(x)dx,$$

故而在缓增广义函数的意义下 $\mathbb{1}_{U_\alpha}\varphi \rightarrow \varphi$. 由傅里叶变换的连续性,

$$\lim_{U_\alpha} \widehat{\mathbb{1}_{U_\alpha}\varphi} = \widehat{\varphi}. \quad (3.7)$$

因此,

$$\begin{aligned} \hat{\varphi} * \hat{f}(x) &= (\hat{\varphi})(L_x \theta \hat{f}) & (3.5) \\ &= (\lim_{U_\alpha} \widehat{\mathbb{1}_{U_\alpha}\varphi})(L_x \theta \hat{f}) & (\varphi \text{ 作为缓增广义函数}) \\ &= \lim_{U_\alpha} (\widehat{\mathbb{1}_{U_\alpha}\varphi})(L_x \theta \hat{f}) & (\text{缓增广义函数收敛}) \\ &= \lim_{U_\alpha} (\widehat{\mathbb{1}_{U_\alpha}\varphi * \hat{f}})(x) & (3.5) \\ &= \lim_{U_\alpha} \widehat{\mathbb{1}_{U_\alpha}\varphi f}(x) & (\mathbb{1}_{U_\alpha}\varphi \text{ 作为 Schwartz-Bruhat 函数满足 (3.3)}) \\ &= \widehat{\varphi f}(x). & (\mathcal{F} \text{ 连续}) \end{aligned}$$

□

这一小节对缓增广义函数定义的运算是函数上运算的自然延拓, 因此如果将一个函数看作缓增广义函数, 二者的理论是相容的.

第 3 节 Adèles 环

给定一个整体域 K , 我们记

- K_v 为 K 在位置 v 完备化得到的局部域,
- $\mathcal{O}_v$ 是 K_v 的赋值环或者 K_v 本身 (v 为阿基米德赋值),
- $\mathfrak{p}_v$ 为 $\mathcal{O}_v$ 的极大理想,
- k_v 为剩余域 $\mathcal{O}_v/\mathfrak{p}_v$,
- $|\cdot|_v$ 为正规化的绝对值.

在此基础上, K 的 Adèles 环将 K 在所有位置上完备化的信息都收集起来.

定义 3.37. (Adèles 环) 整体域 K 的 **Adèles 环** (Adèles Ring) $\mathbb{A}$ 为 $(K_v, \mathcal{O}_v)$ 的限制乘积 (restricted product), 即

$$\mathbb{A} = \prod'_{v \in M_K} (K_v, \mathcal{O}_v),$$

对于 $\mathbb{A}$ 中的元素 $\prod_{v \in M_K} x_v$, 只有有限个 $x_v \in K_v$, 其余的 x_v 均属于 $\mathcal{O}_v$. 这也说明

$$\mathbb{A} = \bigcup_{S \subset M_K, |S| < +\infty} \prod_{v \in S} K_v \prod_{v \notin S} \mathcal{O}_v.$$

其中, $\mathbb{A}^S$ 定义为

$$\mathbb{A}^S = \prod_{v \in S} K_v \prod_{v \notin S} \mathcal{O}_v,$$

则

$$\mathbb{A} = \bigcup_{S \subset M_K, |S| < +\infty} \mathbb{A}^S.$$

对于 $\mathbb{A}$ 来说, K 以 $\prod_v k$ 的形式嵌入 $\mathbb{A}$.

定义 3.38. (Idèle 群) 整体域 K 的 **Idèle 群** (Idèle Group) $\mathbb{I}$ 为 $(K_v^\times, \mathcal{O}_v^\times)$ 的限制乘积 (restricted product), 即

$$\mathbb{I} = \prod'_{v \in M_K} (K_v^\times, \mathcal{O}_v^\times),$$

对于 $\mathbb{I}$ 中的元素 $\prod_{v \in M_K} x_v$, 只有有限个 $x_v \in K_v^\times$, 其余的 x_v 均属于 $\mathcal{O}_v^\times$. 这也说明

$$\mathbb{I} = \bigcup_{S \subset M_K, |S| < +\infty} \prod_{v \in S} K_v^\times \prod_{v \notin S} \mathcal{O}_v^\times.$$

其中, $\mathbb{I}^S$ 定义为

$$\mathbb{I}^S = \prod_{v \in S} K_v^\times \prod_{v \notin S} \mathcal{O}_v^\times,$$

则

$$\mathbb{I} = \bigcup_{S \subset M_K, |S| < +\infty} \mathbb{I}^S.$$

可以直接验证 Idèles 群的另一等价定义是

$$\mathbb{I} = \mathbb{A}^\times.$$

对于 $\mathbb{I}$ 来说, $K^\times$ 以 $\prod_v k$ 的形式嵌入 $\mathbb{I}$.

命题 3.39. $\mathbb{A}$ 是局部紧 Abel 群.

这是由于 $\mathbb{A}^S$ 均为局部紧 Abel 群.

命题 3.40. K 嵌入 $\mathbb{A}$ 的像是离散的, 仍把其记作 K , $\mathbb{A}/K$ 在商拓扑下是紧的.

我们略去证明, 具体可以参考 [6, P64]. 由此, 我们得到 $\mathbb{Z} \subset \mathbb{R}$ 的类比 $K \subset \mathbb{A}$.

第 4 节 Adèles 环上傅里叶变换

如无特别说明, $\mathbb{A}$ 指一个固定的整体域 K 上的 Adèles 环.

4.1 标准特征

给定整体域 K , $\mathbb{A}$ 上特征为 K_v 上特征拼成.

命题 3.41. 我们有同构 $\widehat{\mathbb{A}} \simeq \prod'_{v \in M_K} (\widehat{K_v}, \widehat{K_v/\mathcal{O}_v})$, 由以下映射给出:

$$\begin{aligned} \widehat{\mathbb{A}} &\simeq \prod'_{v \in M_K} (\widehat{K_v}, \widehat{K_v/\mathcal{O}_v}) \\ \chi &\mapsto (\chi|_{K_v}) \\ \prod \chi_v &\mapsto (\chi_v) \end{aligned}$$

这也说明, $\mathbb{A}$ 上特征 χ 是给定 (χ_v) 拼成的, 其中 χ_v 为 K_v 上特征, 且除有限多个 v 外, $\chi_v|_{\mathcal{O}_v} = 1$.

我们略去证明, 具体可以结合 [6, Chapter.XV, Theorem 3.2.1] 与命题 3.22 的证明.

定义 3.42. 记 χ_0 为诸 K_v 上标准特征 χ_{K_v} 拼成的, 则 χ_0 为 $\mathbb{A}$ 上标准特征 (Standard Character).

命题 3.43. 对任何的 $a \in \mathbb{I}$, 定义 $\chi_a(x) = \chi_0(ax)$, 那么有同构 $\mathbb{A} \cong \widehat{\mathbb{A}}$, 由以下映射给出:

$$\begin{aligned} \Psi : \mathbb{A} &\rightarrow \widehat{\mathbb{A}} \\ a &\mapsto \chi_a. \end{aligned}$$

我们略去证明, 具体可以参考 [6, Chapter.XV, Theorem 4.1.1].

命题 3.44. $\mathbb{A}$ 上标准特征 χ_0 满足 $\chi_0|_K = 1$.

我们略去证明, 具体可以参考 [6, Chapter.XV, Theorem 4.1.5].

命题 3.45. 由命题 3.43., 有局部紧 Abel 群同构 $K \cong K^\perp$:

$$\begin{aligned} \Phi : K &\rightarrow \widehat{\mathbb{A}/K} \cong K^\perp \\ a &\mapsto \chi_a. \end{aligned}$$

我们略去证明, 具体可以参考 [6, Chapter.XV, Theorem 4.1.4].

命题 2.32. 与命题 3.45. 说明正合列

$$1 \rightarrow K \xrightarrow{i} \mathbb{A} \xrightarrow{p} \mathbb{A}/K \rightarrow 1, \quad (3.8)$$

与正合列

$$1 \rightarrow \widehat{\mathbb{A}/K} \rightarrow \widehat{\mathbb{A}} \rightarrow \widehat{K} \rightarrow 1 \quad (3.9)$$

是同构的.

4.2 标准测度

定义 3.46. 记 $dx = \prod dx_{K_v}$, 对 $\mathbb{A}$ 中所有开集 $\prod U_v$ 有

$$\int_{\prod U_v} dx = \prod \int_{U_v} dx_{K_v},$$

则 dx 为 $\mathbb{A}$ 上标准测度 (Standard Measure).

命题 3.47. 在标准测度下, 成立 $\text{Vol}(\mathbb{A}/K) = 1$.

我们略去证明, 具体可以参考 [7, Proposition 5.5].

4.3 Schwartz-Bruhat 函数

定义 3.48. 对于一个 Adèles 环 $\mathbb{A}$, 如果对于有限个位置 v 取 $f_v \in \mathcal{S}(K_v)$, 其余的位置取 $f = \mathbb{1}_{\mathcal{O}_v}$, 那么 $\prod f_v : \mathbb{A} \rightarrow \mathbb{C}$ 为 $\mathbb{A}$ 上一个定义好的函数. 如果 $\mathbb{A}$ 上一个函数 f 为有限个这样的函数的 $\mathbb{C}$ -线性组合, 则称其为 $\mathbb{A}$ 上的 **Schwartz-Bruhat 函数**. 将 $\mathbb{A}$ 上所有的 Schwartz-Bruhat 函数记为 $\mathcal{S}(\mathbb{A})$.

命题 3.49. 对于一个 Adèles 环 $\mathbb{A}$, 取标准测度 dx 使得傅里叶逆变换成立, 那么对于 $f \in \mathcal{S}(\mathbb{A})$, 有 $\hat{f} \in \mathcal{S}(\mathbb{A})$.

证明. 不妨只考虑 $f = \prod f_v$ 的情况, 对其做傅立叶变换相当于在每个位置 v 的分量上做傅里叶变换.

对于一个局部域 F , 相对于其上的标准特征 χ_F 做傅立叶变换, 并取标准测度 dx_F , 由命题 3.28 知上述 $\hat{f} \in \mathcal{S}(F)$.

而对于 $f = \mathbb{1}_{\mathcal{O}_v}$, 由命题 3.22 及标准测度的表达式知道在除了有限个位置 v 上都有 $\mathcal{O}_v^\perp \cong \mathcal{O}_v$ 且 $\text{Vol}(\mathcal{O}_v) = 1$, 即由命题 3.28 的证明得到 $\hat{f} = \mathbb{1}_{\mathcal{O}_v}$.

故而 $\hat{f} = \prod \hat{f}_v$, 诸 $\hat{f}_v \in \mathcal{S}(K_v)$, 且除了有限个位置之外 $\hat{f}_v = \mathbb{1}_{\mathcal{O}_v}$, 则 $\hat{f} \in \mathcal{S}(\mathbb{A})$. $\square$

4.4 Poisson 求和公式

引理 3.50. 对于一个 Adèles 环 $\mathbb{A}$, 如果 $f \in \mathcal{S}(\mathbb{A})$, 那么 $\sum_{\kappa \in K} f(x + \kappa)$ 在紧集上绝对且一致收敛为一个 K -周期函数.

我们略去证明, 具体可以参考 [7, Lemma 5.6]

定理 3.51. ($\mathbb{A}$ 相对于 K 的 Poisson 求和公式) 对于一个 Adèles 环 $\mathbb{A}$, 如果 $f \in \mathcal{S}(\mathbb{A})$, 那么有

$$\sum_{\kappa \in K} f(\kappa) = \sum_{\kappa \in K} \hat{f}(\kappa).$$

证明. 这个定理可以直接由定理2.33得到. 我们同样可以给出一个技巧性的证明, 与 $\mathbb{R}$ 相对于 $\mathbb{Z}$ 的 Poisson 求和公式可以给出的证明一样, 即对函数

$$F(x) := \sum_{\kappa \in K} f(x + \kappa)$$

应用傅里叶逆变换公式.

由于 F 可以看作 $\mathbb{A}/K$ 上的函数, 那么 $\widehat{F}$ 作为 $\widehat{\mathbb{A}/K}$ 上的函数, 由于同构 $\widehat{\mathbb{A}/K} \cong K$ 可以看作 K 上的函数. 对于 $\kappa \in K$,

$$\begin{aligned} \widehat{F}(\kappa) &= \int_{\widehat{\mathbb{A}/K}} \sum_{l \in K} f(x + l) \chi_0(\kappa x) dx \\ &= \sum_{l \in K} \int_{\widehat{\mathbb{A}/K}} f(x + l) \chi_0(\kappa x) dx && \sum_{l \in K} f(x + l) \text{ 在紧集上绝对且一致收敛} \\ &= \sum_{l \in K} \int_{\widehat{\mathbb{A}/K+l}} f(x) \chi_0(\kappa(x - l)) dx && x + l \text{ 替代 } x \\ &= \sum_{l \in K} \int_{\widehat{\mathbb{A}/K+l}} f(x) \chi_0(\kappa x) dx && \chi_0(-l) = 1 \\ &= \int_{\mathbb{A}} f(x) \chi_0(\kappa x) dx \\ &= \widehat{f}(\kappa). \end{aligned}$$

由傅里叶逆变换公式 (2.7)(注意到 $\widehat{F} = \widehat{f} \in L^1(K)$)

$$F(x) = \sum_{\kappa \in K} \widehat{F}(\kappa) \chi_0(\kappa x),$$

令 $x = 0$ 有

$$\sum_{\kappa \in K} f(\kappa) = \sum_{\kappa \in K} \widehat{f}(\kappa).$$

□

第四章 二次互反律

这一节中涉及的局部域上赋值均取为标准赋值, 因此有命题3.16.与乘法公式 (3.1) 成立.

第 1 节 二次扩张

给定一个特征不为 2 的整体域 k , k 在每个位置 v 的完备化记为 k_v . 在每个 k_v 上取标准特征 χ_{k_v} 与标准测度 dx_{k_v} 拼成 $\mathbb{A}_k$ 上的标准特征 χ_1 与标准测度 dx_1 , 由命题3.44.知 $\chi_1|_k$ 为 k 上平凡特征, 由命题3.47.知在标准测度下 $\mathbb{A}_k/k$ 的体积为 1.

现在, 考虑 K 为 k 的二次扩张, 对于 k 的一个位置 v 定义

$$K_v = K \otimes_k k_v,$$

由于 k 的位置 v 在扩张 K 中的不同分歧情况,

$$K_v \cong \begin{cases} K_w & (w|v, v \text{ 不分歧}) \\ \prod_w K_w & (w|v, v \text{ 分歧}) \end{cases},$$

即 K_v 在 v 不分歧的情况下为域, 否则仅为一个局部紧 Abel 群.

事实上, 如果 v 分歧, 由于 $[K : k] = 2 = \sum_{w|v} [K_w : k_v]$, 那么有 $w = v$, $K_w \cong k_v$, $K_v \cong k_v \times k_v$, 该同构是将 K_v 看作 $k_v[X] \bmod (X^2 - t)$, ($t \in k_v$) 的 2 维 k_v - 向量空间.

由于 k 含 1 的 2 次根, 故而域扩张 K/k 是 Galois 的, 考虑非平凡 $\sigma \in \text{Gal}(K/k)$, 在 K 上定义 k -二次型 $\langle -, - \rangle$, 使得对于 $\alpha, \beta \in K$,

$$\langle \alpha, \beta \rangle = \text{Tr}_{K/k}(\alpha\sigma(\beta)) = \alpha\sigma(\beta) + \sigma(\alpha)\beta,$$

并延拓定义成 K_v 上的 k_v -二次型, 使得对于 $\tilde{\alpha} = \alpha \otimes a, \tilde{\beta} = \beta \otimes b \in K_v$

$$\langle \tilde{\alpha}, \tilde{\beta} \rangle = \text{Tr}_{K_v/k_v}(\tilde{\alpha}\sigma(\tilde{\beta})) = ab\langle \alpha, \beta \rangle,$$

注意到此时的 σ 延拓定义在 K_v/k_v 上, 可以看出 $\langle \tilde{\alpha}, \tilde{\beta} \rangle = \langle \tilde{\beta}, \tilde{\alpha} \rangle$.

利用映射 $\Phi : x \mapsto \chi_{k_v}(\langle x, - \rangle)$ 得到同构 $K_v \cong \widehat{K_v}$, 选取自对偶测度 dx , 则 K_v 上 Schwartz-Bruhat 函数的傅立叶变换为

$$\hat{f}(x) = \int_{K_v} f(y) \overline{\chi_{k_v}(\langle x, y \rangle)} dy,$$

且有傅里叶逆变换公式成立.

第 2 节 二次指数分布

定义 4.1. 对于 $a \in k_v^\times$, 定义 K_v 上的二次指数分布函数为

$$S_a(x) = \chi_{k_v} \left(\frac{a}{2} \langle x, x \rangle \right). \quad (4.1)$$

二次指数分布函数是局部常值的, 因此可以被看作缓增广义函数, 以下两个引理蕴含了二次互反律的核心.

引理 4.2. (p -进版本) 二次指数分布的傅立叶变换满足

$$\widehat{S_a}(x) = \gamma(a) S_{-a^{-1}}(x), \quad (4.2)$$

其中

$$\gamma(a) = \lim_{U_\alpha} \int_{U_\alpha} \chi_{k_v} \left(\frac{a}{2} \langle y, y \rangle \right) dy, \quad (4.3)$$

$\{U_\alpha\}$ 为 K_v 中所有越来越大的紧开子群.

证明. 如果将 S_a 看作缓增广义函数, 那么

$$\widehat{S_a(f)} = S_a(\hat{f}) = \int_{K_v} S_a(x) \hat{f}(x) dx.$$

由于 $\hat{f}$ 仍为 Schwartz-Bruhat 函数, 因此对于 K_v 中足够大的紧开集 U , 有

$$\int_{K_v} S_a(x) \hat{f}(x) dx = \int_{K_v} S_a(x) \mathbb{1}_U(x) \hat{f}(x) dx.$$

此时, $S_a \mathbb{1}_U$ 为紧支集光滑函数, 即成为了一个 Schwartz-Bruhat 函数, 因此由乘法等式 (3.6) 有

$$\widehat{S_a(f)} = \int_{K_v} \widehat{S_a \mathbb{1}_U}(x) f(x) dx.$$

考虑

$$\widehat{S_a \mathbb{1}_U}(x) = \int_U S_a(y) \overline{\chi_{k_v}(\langle x, y \rangle)} dy,$$

因为 $\chi_{k_v}(\langle x, y \rangle) = \chi_{k_v}(\langle y, x \rangle)$, 故有

$$\begin{aligned} \widehat{S_a \mathbb{1}_U}(x) &= \int_U \chi_{k_v} \left(\frac{a}{2} \langle y, y \rangle - \frac{1}{2} \langle x, y \rangle - \frac{1}{2} \langle y, x \rangle \right) dy, \\ &= \int_U \chi_{k_v} \left(\frac{a}{2} \langle y - a^{-1}x, y - a^{-1}x \rangle - \frac{a^{-1}}{2} \langle x, x \rangle \right) dy. \end{aligned}$$

对于固定的 a , 上述积分中用 $y + a^{-1}x$ 替换 y 做变量平移得到

$$\begin{aligned} \widehat{S_a \mathbb{1}_U}(x) &= \int_U \chi_{k_v} \left(\frac{a}{2} \langle y, y \rangle - \frac{a^{-1}}{2} \langle x, x \rangle \right) dy \quad (U \text{ 为紧开子群}) \\ &= S_{-a^{-1}}(x) \int_U \chi_{k_v} \left(\frac{a}{2} \langle y, y \rangle \right) dy, \end{aligned}$$

即由 (3.7) 有

$$\widehat{S}_a(x) = S_{-a^{-1}}(x) \lim_{U_\alpha} \int_{U_\alpha} \chi_{k_v}(\frac{a}{2}\langle y, y \rangle) dy.$$

□

引理 4.3. 如果有一个 K_v 上的 Schwartz-Bruhat 函数 f , 对于 $a \in k_v^*$, $x \in K_v$, 有

$$(S_a * f)(x) = S_a(x) \widehat{S}_a f(ax). \quad (4.4)$$

证明. 由命题 2.28 有

$$\begin{aligned} (S_a * f)(x) &= (f * S_a)(x) = \int_{K_v} S_a(x-y) f(y) dy \\ &= \int_{K_v} \chi_{k_v}(\frac{a}{2}\langle x, x \rangle - a\langle x, y \rangle + \frac{a}{2}\langle y, y \rangle) f(y) dy \\ &= S_a(x) \int_{K_v} \overline{\chi_{k_v}(\langle ax, y \rangle)} S_a(y) f(y) dy \\ &= S_a(x) \widehat{S}_a f(ax). \end{aligned}$$

□

第 3 节 二次范数剩余符号与局部积分

定义 4.4. 如下定义二次范数剩余符号 $\nu_v : k_v^\times \rightarrow \pm 1$:

$$\nu_v(a) = \begin{cases} 1 & K_v \text{ 不是一个域} \\ 1 & K_v \text{ 是一个域且 } a \text{ 为 } K_v \text{ 中某元素的范数} \\ -1 & \text{其余情况} \end{cases}$$

事实上, 如果 K_v 是 k_v 的可分二次扩张, 那么 K 在 v 不分歧, $k_v^\times$ 中 K_v 的范数构成 $k_v^\times$ 中指标为 2 的子群, 因此二次范数剩余符号 ν_v 是一个群同态.

引理 4.5. (p -进版本) 对于 (4.3) 中的 γ 有

$$\gamma(a) = \nu_v(a) |a|_{k_v}^{-1} \gamma(1). \quad (a \in k_v^\times) \quad (4.5)$$

证明. 由定义, 有

$$\gamma(a) = \lim_{U_\alpha} \int_{U_\alpha} \chi_{k_v}(ay\sigma(y)) dy.$$

如果 a 是一个局部范数, 例如 $a = x_0\sigma(x_0)$, 那么在上式中用 yx_0^{-1} 替换 y 得到

$$\gamma(a) = |x_0|_{K_v}^{-1} \lim_{U_\alpha} \int_{x_0 U_\alpha} \chi_{k_v}(y\sigma(y)) dy, \quad x_0 U_\alpha \text{ 仍为一个紧开子群}$$

由于我们采用的是正规化的赋值, 因此成立

$$|a|_{k_v} = |x_0\sigma(x_0)|_{k_v} = |x_0|_{K_v},$$

故而此时 (4.5) 成立.

如果 a 不是一个局部范数, 那么只有可能在 K_v 是一个域的情况下, 用 Θ 表示 $K_v^\times$ 中范数为 1 的子群, 它是紧的. 如果令 U_α 为越来越大的 Θ -不变的紧开子群, 那么有

$$\begin{aligned}\gamma(a) &= \lim_{U_\alpha} \int_{U_\alpha} \chi_{k_v}(ay\sigma(y))dy \\ &= \lim_{U_\alpha} \int_{U_\alpha/\Theta} \int_{\Theta} \chi_{k_v}(ay\theta\sigma(\theta)\sigma(y))d\theta dy \quad (\text{商积分公式}) \\ &= \lim_{U_\alpha} \int_{U_\alpha/\Theta} \chi_{k_v}(ay\sigma(y))dy. \quad (\text{取子群测度使得 Vol}(\Theta) = 1)\end{aligned}$$

注意到 $K_v^\times/\Theta$ 在范数映射下同构于其在 $k_v^\times$ 中的像, 且

$$d^\times y = |y|_{K_v}^{-1} dy, \quad d^\times b = |b|_{k_v}^{-1} db$$

为 $K_v^\times/\Theta, k_v^\times$ 上与范数映射相容的乘性 Haar 测度, 那么

$$\begin{aligned}\gamma(a) &= \lim_{U_\alpha} \int_{U_\alpha/\Theta} \chi_{k_v}(ay\sigma(y))dy \\ &= \lim_{U'_\alpha} \int_{U'_\alpha/\Theta} \chi_{k_v}(ay\sigma(y))|y|_{K_v} d^\times y \quad (U'_\alpha = U_\alpha \setminus \{0\}) \\ &= \lim_{V_\alpha} \int_{V_\alpha} \chi_{k_v}(ab)|b|_{k_v} d^\times b, \quad (V_\alpha = \text{Nr}(U'_\alpha))\end{aligned}$$

将 b 用 ba^{-1} 代替有

$$\gamma(a) = |a|_{k_v}^{-1} \lim_{V_\alpha} \int_{aV_\alpha} \chi_{k_v}(b)|b|_{k_v} d^\times b.$$

由于 K_v 的范数构成 $k_v^\times$ 中指标为 2 的子群, 且 a 不为局部范数, 那么

$$\left(\lim_{V_\alpha} \int_{V_\alpha} + \lim_{V_\alpha} \int_{aV_\alpha} \right) \chi_{k_v}(b)|b|_{k_v} d^\times b = \lim_{W_\alpha} \int_{W_\alpha} \chi_{k_v}(b)|b|_{k_v} d^\times b, \quad (\text{忽略}\{0\}\text{做积分})$$

W_α 跑遍 k_v 中一族越来越大的紧开子群 (加性子群). 类似于命题 3.28 中的证明, 由于 χ_{k_v} 在非常大的子群 W_α 上非平凡, 选取 $b_0 \in W_\alpha$ 使得 $\chi_{k_v}(b_0) \neq 1$, 通过变量代换有

$$\lim_{W_\alpha} \int_{W_\alpha} \chi_{k_v}(b)|b|_{k_v} d^\times b = \lim_{W_\alpha} \int_{W_\alpha} \chi_{k_v}(b)db = 0. \quad (4.6)$$

那么

$$\lim_{V_\alpha} \int_{aV_\alpha} \chi_{k_v}(b)|b|_{k_v} d^\times b = - \lim_{V_\alpha} \int_{V_\alpha} \chi_{k_v}(b)|b|_{k_v} d^\times b,$$

则说明

$$\gamma(a) = -|a|_{k_v}^{-1} \gamma(1) = \nu_v(a) |a|_{k_v}^{-1} \gamma(1).$$

□

第 4 节 二次范数剩余符号的互反律

定义 4.6. 对于 $a = (a_v) \in \mathbb{I}_k$, 整体范数剩余符号

$$\nu_{K/k}(a) = \prod_v \nu_v(a_v).$$

定理 4.7. (二次范数剩余符号的互反律) 整体的范数剩余符号在 $k^\times$ 上平凡.

证明. 整体的结论需要使用整体的结论, 证明中使用了 Poisson 求和公式. 对于 $f \in \mathcal{S}(\mathbb{A}_K)$, $a \in k^\times$, $x = \{x_v\} \in \mathbb{A}_K$, 记 (4.1) 中的 S_a 为 S_a^v , (4.3) 中 γ 为 γ_v , 令

$$\gamma(a) = \prod_v \gamma_v(a)$$

且

$$S_a(x) = \prod_v S_a^v(x_v),$$

引理 4.5 仍然成立. 如果 $x = \{x\} \in K$, 那么

$$S_a(x) = \prod_v \chi_{k_v}(a \text{Nr}_{K/k} x),$$

$\chi_0 = \prod_v \chi_{k_v}$ 在 K 上平凡, 故 S_a 在 K 上平凡. 有

$$\begin{aligned} \sum_{x \in K} f(x) &= \sum_{x \in K} S_a(x) f(x) \\ &= \sum_{x \in K} \widehat{S_a f}(x) && \text{(Poisson 求和公式)} \\ &= \sum_{x \in K} \widehat{S_a}(x) * \hat{f}(x) && \text{(命题 3.36.)} \\ &= \gamma(a) \sum_{x \in K} (S_{-a^{-1}} * \hat{f}(x)) && \text{(引理 4.2.)} \\ &= \gamma(a) \sum_{x \in K} S_{-a^{-1}}(x) \widehat{S_{-a^{-1}} \hat{f}}(-a^{-1}x) && \text{(引理 4.3.)} \\ &= \gamma(a) \sum_{x \in K} \widehat{S_{-a^{-1}} \hat{f}}(-a^{-1}x), && (S_{-a^{-1}}|_K = 1) \end{aligned}$$

由 Poisson 求和公式, 上式为

$$\begin{aligned}
 \sum_{x \in K} f(x) &= \gamma(a) \sum_{x \in K} S_{-a^{-1}}(-a^{-1}x) \hat{f}(-a^{-1}x) \\
 &= \gamma(a) \sum_{x \in K} S_{-a^{-1}}(x) \hat{f}(x) && (-ax \text{ 替代 } x) \\
 &= \gamma(a) \sum_{x \in K} \hat{f}(x) && (S_{-a^{-1}}|_K = 1) \\
 &= \gamma(a) \sum_{x \in K} f(x). && (\text{Poisson 求和公式})
 \end{aligned}$$

因此得到 $\sum_{x \in K} f(x) = \gamma(a) \sum_{x \in K} f(x)$. 总可以选取合适的 f 使得

$$\sum_{x \in K} f(x) \neq 0,$$

故而得到

$$\gamma(a) = 1 \quad (\text{对所有的 } a \in k^\times).$$

因此, 对于 $a \in k^\times$ 有

$$\begin{aligned}
 1 &= \gamma(a) = \prod_v \gamma_v(a) \\
 &= \prod_v |a|_{k_v}^{-1} \nu_v(a) \gamma_v(1) && (\text{引理 4.5.}) \\
 &= \prod_v \nu_v(a) \gamma_v(1) && (\text{乘法公式}) \\
 &= \nu(a) \gamma(1) = \nu(a). && (\gamma(1) = 1)
 \end{aligned}$$

这说明 ν 在 $k^\times$ 上平凡.

□

第 5 节 二次 Hilbert 符号的互反律

定义 4.8. 对于 $a, b \in k_v$, 二次 Hilbert 符号

$$(a, b)_v \begin{cases} 1 & ax^2 + by^2 = z^2 \text{ 在 } k_v \text{ 中有非平凡解} \\ -1 & \text{其余情况} \end{cases}.$$

定理 4.9. (Hilbert 符号的互反律) 对于 $a, b \in k^\times$,

$$\prod_v (a, b)_v = 1. \quad (4.7)$$

证明. 证明使用了二次范数剩余符号在 $k^\times$ 上平凡的结论.

首先, 如果 a 或 b 为 k 中平方数, 那么

$$ax^2 + by^2 = z^2$$

在 k 中有平凡解, 自然在每个 k_v 中都有平凡解, 则 $(a, b)_v = 1$, 有 $\prod_v (a, b)_v = 1$.

如果 a, b 之一不是 k 中平方数, 不妨假设是 b , 令 $K = k(\sqrt{b})$, 那么可以将每个位置 v 处的方程写为

$$ax^2 = z^2 - bx^2 = \text{Nr}_{K_v/k_v}(z + y\sqrt{b}). \quad (4.8)$$

对于 k 的每个位置 v , 其在 K 中的分裂情况可能不同:

- v 在 K 中分歧, 分裂成两个不同的位置, 使得 K_v 不是域, 范数映射 $\text{Nr}_{K_v/k_v} : K_v \rightarrow k_v$ 是满射, $\nu_v \equiv 1$.
- v 在 K 中不分歧, 使得 K_v 是域, 那么方程 (4.8) 中只有 $x \neq 0$ 才可能有非平凡解. 将方程改写为

$$a = \text{Nr}_{K_v/k_v}(z' + y'\sqrt{b}),$$

这说明方程有非平凡解当且仅当 a 是 K_v 中某元素的范数.

以上讨论说明 $(a, b)_v$ 的值与 $\nu_v(a)$ 相对于域扩张 $K(\sqrt{b})/k$ 的值相等. 因此, 由二次范数剩余符号的互反律有 $\prod_v (a, b)_v = \prod_v \nu_v(a) = 1$. $\square$

注 4.1 事实上, 我们证明了一个更强的局部结论: 对任何 $a, b \in k_v^\times$, 二次 Hilbert 符号 $(a, b)_v$ 的值等于 $\nu_v(a)$ 相对于域扩张 $k_v(\sqrt{b})/k_v$ 的值, 只要在 b 为 k_v 中平方数时, 将 $k_v(\sqrt{b})$ 看作

$$k_v[X] \mod (X^2 - b),$$

即为一个 2 维 k_v -向量空间.

第 6 节 二次互反律

这一节从定理 4.9 推出经典版本的二次互反律. 我们将会给出二次互反律主要部分和补充部分的陈述, 但只对主要部分进行证明. 记整体域 k 的整数环为 $\mathfrak{o}$.

定义 4.10. (二次符号) 对于 k 的一个非阿基米德的位置 v , $a \in \mathfrak{o}$, 二次符号

$$\left(\frac{a}{v}\right)_2 = \begin{cases} 1 & (a \bmod v \text{ 为非零平方数}) \\ 0 & (a \equiv 0 \bmod v) \\ -1 & (a \bmod v \text{ 为非零非平方数}) \end{cases},$$

其中, $a \bmod v$ 为 a 在 $\mathfrak{o}_v$ 中展开式

$$a = \sum_{n \geq 0} a_n \pi^n$$

的零阶系数 $a_0 \in \mathfrak{f}_v$.

由于每个非阿基米德的位置 v 由 $\mathfrak{o}$ 中的素理想 $\mathfrak{P}$ 诱导, 如果 $\mathfrak{P}$ 由 $\pi \in \mathfrak{o}$ 生成, 此时也可以说 v 是 π 生成的, 将 $\left(\frac{x}{v}\right)_2$ 写作 $\left(\frac{x}{\pi}\right)_2$.

如果一个非阿基米德的位置 v 的剩余类域是 $\mathbb{F}_p$ 的有限扩张, p 为奇数, 则称位置 v 是**奇的** (odd), 否则是**偶的** (even). 对于一个阿基米德的位置 v , 由于其没有有限剩余类域, 则称其为**无限的** (infinite).

定理 4.11. (二次互反律的主要部分) 如果 π 和 ϖ 生成两个不同的奇位置, 那么有

$$\left(\frac{\pi}{\varpi}\right)_2 \left(\frac{\varpi}{\pi}\right)_2 = \prod_v (\pi, \varpi)_v, \quad (4.9)$$

其中 v 跑遍所有的偶位置或无限的位置, $(-, -)_v$ 为 Hilbert 符号.

定理 4.12. (二次互反律的补充部分) 如果 π 生成一个奇位置 v , $\alpha \in \mathfrak{o}$ 在 $\mathfrak{o}_v$ 中为单位, 那么

$$\left(\frac{\alpha}{\pi}\right)_2 = \prod_v (\pi, \alpha)_v, \quad (4.10)$$

其中 v 跑遍所有的偶位置或无限的位置, 也跑遍所有使得 α 在 $\mathfrak{o}_v$ 中不为单位的奇位置.

主要部分的证明. 断言: 对于 π, ϖ 生成两个不同的奇位置, 有

$$(\pi, \varpi)_v = \begin{cases} \left(\frac{\varpi}{\pi}\right)_2 & v \text{ 由 } \pi \text{ 生成} \\ \left(\frac{\pi}{\varpi}\right)_2 & v \text{ 由 } \varpi \text{ 生成} \\ 1 & v \text{ 为其余不同的奇位置时} \end{cases}.$$

证明. 对于 v 由 π 生成的情况, 假设方程

$$\pi x^2 + \varpi y^2 = z^2$$

在 k_v 中有非平凡解 (x_0, y_0, z_0) , 这说明

$$\min\{1 + 2v(x_0), 2v(y_0)\} = 2v(z_0),$$

由奇偶性知 $k = v(y_0) = v(z_0) \leq v(x_0)$. 因此, $\pi^{-k}(x_0, y_0, z_0)$ 仍为方程的非平凡解, 且此时

$$\varpi \equiv \left(\frac{z_0}{y_0}\right)^2 \pmod{v},$$

即 $(\pi, \varpi)_v = \left(\frac{\varpi}{\pi}\right)_2 = 1$.

另一方面, 如果 $\varpi \bmod v$ 为平方数, 即存在 $\alpha_0 \in k_v$ 使得 $\alpha_0^2 \equiv \varpi \bmod v$. 那么由 Hensel 引理, 令 $f(x) = x^2 - \varpi$, 此时 α_0 满足

$$|f(\alpha_0)|_v = |\varpi - \alpha_0^2|_v \leq (\#\mathfrak{f}_v)^{-1} < |f'(\alpha_0)|_v^2 = |2\alpha_0|_v = 1,$$

由序列

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}, \quad i \in \mathbb{N}$$

收敛到 f 的根 $\alpha \in k_v$. 因此方程在 k_v 中有非平凡解 $(0, 1, \alpha)$. 此时 $\left(\frac{\varpi}{\pi}\right)_2 = (\pi, \varpi)_v = 1$.

对于 v 由 ϖ 生成的情况是类似的.

考虑 v 为其余不同的奇位置时, 如果 ϖ 为 k_v 中的平方数, 那么方程有非平凡解 $(0, 1, \sqrt{\varpi})$, $(\pi, \varpi)_v = 1$.

如果 ϖ 不为 k_v 中的平方数, 那么 $k(\sqrt{\varpi})$ 为 k 的二次扩张, 且在 v 处不分歧, 可以证明任何 k_v 中的单位都是 $k_v(\sqrt{\varpi})$ 中某单位的范数, 即存在 $y_0, z_0 \in k_v$ 成立

$$\pi = \text{Nr}_{k_v(\sqrt{\varpi})/k_v}(z_0 + y_0\sqrt{\varpi}) = z_0^2 - \varpi y_0^2.$$

这说明 $(\pi, \varpi)_v = 1$. □

因此, 由 Hilbert 符号的互反律有

$$\prod_v (\pi, \varpi)_v = \left(\frac{\pi}{\varpi}\right)_2 \left(\frac{\varpi}{\pi}\right)_2 \prod_{v \text{ 偶或无限}} (\pi, \varpi)_v = 1,$$

由于 $\prod_{v \text{ 偶或无限}} (\pi, \varpi)_v$ 只可能取值 ± 1 , 故而 $\prod_{v \text{ 偶或无限}} (\pi, \varpi)_v^2 = 1$, 有

$$\left(\frac{\pi}{\varpi}\right)_2 \left(\frac{\varpi}{\pi}\right)_2 = \prod_{v \text{ 偶或无限}} (\pi, \varpi)_v.$$

□

补充部分的证明. 只需要证明断言: 对于 π 生成一个奇位置 v , $\alpha \in \mathfrak{o}$ 在 $\mathfrak{o}_v$ 中为单位,

$$(\pi, \alpha)_v = \begin{cases} \left(\frac{\alpha}{\pi}\right)_2 & v \text{ 由 } \pi \text{ 生成} \\ 1 & v \text{ 为其余使得 } \alpha \in \mathfrak{o}_v \text{ 为单位的奇位置} \end{cases}.$$

讨论是完全类似的, □

第五章 例子与应用

这一节从定理4.11.推出经典的、与素数 (而非素理想) 相关的二次互反律.

第 1 节 Gauss 二次互反律

例子 5.1. (Gauss 二次互反律) 给定两个不同的奇素数 $p, q \in \mathbb{Z}$, 有

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 = (-1)^{\frac{(p-1)(q-1)}{4}}. \quad (5.1)$$

证明. 由定理4.11.有

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 = (p, q)_2 (p, q)_\infty.$$

由于 $\mathbb{Q}_\infty \cong \mathbb{R}$,

$$px^2 + qy^2 = z^2 \quad (5.2)$$

显然在 $\mathbb{R}$ 中有非平凡的解, 那么 $(p, q)_\infty = 1$, 则得到

$$\left(\frac{q}{p}\right)_2 \left(\frac{p}{q}\right)_2 = (p, q)_2,$$

其中 $(p, q)_2$ 代表方程 (5.2) 在 $\mathbb{Q}_2$ 中有无非平凡解的情况.

事实上, 如果方程 (5.2) 有非平凡解, 可以通过在等式两边乘以 $2^{2k}, k \in \mathbb{Z}$ 使得解在 $\mathbb{Z}_2$ 中, 且 $\max\{|x|_2, |y|_2, |z|_2\} = 1$. 由于 $\mathbb{Z}_2$ 中平方数都形如 $4^l(1 + 8\mathbb{Z}_2), l \in \mathbb{Z}$, 则平方数模 8 取值为 0, 1, 4, 经过简单计算即有

$$px^2 + qy^2 = z^2$$

的解为 $p \equiv 1 \pmod{8}, q \equiv 1 \pmod{8}$ 或 $p, q \pmod{8}$ 分别为 3, 5, 那么有 $(p, q)_2 = 1 = (-1)^{\frac{(p-1)(q-1)}{4}}$.

另一方面, 若 $(-1)^{\frac{(p-1)(q-1)}{4}} = 1$, 则说明

$$(p-1)(q-1) \equiv 0 \pmod{8},$$

由于 $p \pmod{8}, q \pmod{8}$ 取值为 1, 3, 5, 7, 故而要么二者之一取值为 1, 要么取值分别为 3, 5. 断言: 若整数 $n \equiv 1 \pmod{8}$, 则其为 $\mathbb{Z}_2$ 中的平方数.

证明. 如果 $n = 1 + 8a$ ($a \in \mathbb{Z}$) 为 $\mathbb{Z}_2$ 中的平方数, 那么存在 $x \in \mathbb{Z}_2$ 使得

$$(1 + 2x)^2 = n = 1 + 8a.$$

而由 Hensel 引理, 本原多项式 $f(x) = x^2 + x - 2a$ 在 $\mathbb{Z}_2$ 中有解 α , 故而 $n = (1 + 2\alpha)^2$. $\square$

因此, 如果 $p \equiv 1 \pmod{8}$, 方程 (5.2) 有非平凡解 $(1, 0, (1 + 2\sqrt{p}))$, $q \equiv 1 \pmod{8}$ 的情况也一样, 有 $(p, q)_2 = 1$. 对于最后一种情况, 不妨设 $p \equiv 3 \pmod{8}$, $q \equiv 5 \pmod{8}$, 则有 $q + 4p \equiv 1 \pmod{8}$, 故而方程 (5.2) 有非平凡解 $(1, 2, \sqrt{q + 4p})$, 有 $(p, q)_2 = 1$.

因此, $(p, q)_2 = (-1)^{\frac{(p-1)(q-1)}{4}}$, 即得到 Gauss 二次互反律的经典结果. $\square$

第 2 节 函数域上二次互反律

例子 5.2. (函数域上二次互反律) 对于 $\mathbb{F}_q[T]$, q 为奇数, 给定两个不同的首一不可约多项式 $\pi, \varpi \in \mathbb{F}_q[T]$, 有

$$\left(\frac{\pi}{\varpi}\right)_2 \left(\frac{\varpi}{\pi}\right)_2 = \left(\frac{-1}{\mathbb{F}_q}\right)_2^{(\deg \pi)(\deg \varpi)}, \quad (5.3)$$

其中, $\left(\frac{-1}{\mathbb{F}_q}\right)_2$ 的正负性取决于 -1 在 $\mathbb{F}_q$ 中是否为平方数.

证明. 首一不可约多项式 π, ϖ 生成素理想, 因此上式有意义. 注意到 q 为奇数, 因此 $\mathbb{F}_q(T)$ 没有偶位置, 由定理 4.11 的结论及上例的讨论有

$$\left(\frac{\pi}{\varpi}\right)_2 \left(\frac{\varpi}{\pi}\right)_2 = (\pi, \varpi)_\infty,$$

∞ 是 $\mathbb{F}_q(T)$ 上唯一的无限位置:

$$\begin{aligned} \mathbb{F}_q(T) &\rightarrow [0, \infty) \\ P &\mapsto q^{\deg P}, \end{aligned}$$

$\mathbb{F}_q(T)$ 在 ∞ 完备化得到 $\mathbb{F}_q((t_\infty))$, $t_\infty = T^{-1}$, 赋值环为 $\mathbb{F}_q[[t_\infty]]$.

首先, 如果 π 或 ϖ 之一的 $\deg$ 为偶数, 不妨假设为 π , 那么

$$\pi = t_\infty^{-\deg \pi} (1 + t_\infty(\cdots)),$$

由 Hensel 引理, 与定理 4.11 中类似地证明 $(1 + t_\infty(\cdots))$ 在 $\mathbb{F}_q[[t_\infty]]$ 中为平方数, 即 π 在 $\mathbb{F}_q((t_\infty))$ 中是平方数, 方程

$$\pi x^2 + \varpi y^2 = z^2$$

在 $\mathbb{F}_q((t_\infty))$ 中有非平凡解 $(1, 0, \sqrt{\pi})$, 这说明 $(\pi, \varpi)_\infty = 1$.

如果 π 和 ϖ 在 $\mathbb{F}_q((t_\infty))$ 中都不为平方数, 即它们的 $\deg$ 为奇数, 那么不妨讨论方程

$$t_\infty(x^2 + y^2) = z^2$$

在 $\mathbb{F}_q((t_\infty))$ 中是否有非平凡解.

如果 $\sqrt{-1}$ 在 $\mathbb{F}_q((t_\infty))$ 中, 那么 $(1, \sqrt{-1}, 0)$ 为方程在 $\mathbb{F}_q((t_\infty))$ 中的非平凡解.

如果 $\sqrt{-1}$ 不在 $\mathbb{F}_q((t_\infty))$ 中, 如果方程有非平凡解 (x_0, y_0, z_0) , 那么 $x_0^2 + y_0^2$ 实际上是域扩张 $\mathbb{F}_q((T))(\sqrt{-1})/\mathbb{F}_q((T))$ 中元素 $x_0 + \sqrt{-1}y_0$ 的范数, 该扩张在 ∞ 不分歧. 因此 $\deg(x_0 + \sqrt{-1}y_0) = \deg(x_0 - \sqrt{-1}y_0)$, 故 $\deg(x_0 + \sqrt{-1}y_0)$ 是偶数. 这说明 $\deg(t_\infty(x_0^2 + y_0^2))$ 是奇数, 与 $\deg z_0^2$ 为偶数矛盾, 因此方程在 $\mathbb{F}_q((t_\infty))$ 中没有非平凡解.

综合以上讨论可以得到

$$\left(\frac{\pi}{\varpi}\right)_2 \left(\frac{\varpi}{\pi}\right)_2 = \left(\frac{-1}{\mathbb{F}_q}\right)_2^{(\deg \pi)(\deg \varpi)}.$$

□

附录

这里介绍一些正文中承认了的定理或引理.

Fubini 定理

定理： 对于两个局部紧 *Abel* 群 A, B 及其上的测度 da, db , f 是 $A \times B$ 上的可测函数, 如果

$$\int_A \int_B |f(a, b)| db da \text{ 或 } \int_B \int_A |f(a, b)| da db$$

有限, 那么

$$\int_A \int_B f(a, b) db da = \int_B \int_A f(a, b) da db.$$

参考 [4, Appendix B.3].

分歧定理

定理： 如果 K/k 是整体域的有限可分扩张, v 为 k 的一个位置, 那么

$$K \otimes_k k_v \cong \prod_{w|v} L_w,$$

同构通过 $x \otimes a \mapsto (xa, \dots, xa)$ 实现.

参考 [5, Ch2, 8.3].

定理： 如果 K/k 是整体域的有限可分扩张, v 为 k 的一个非阿基米德的位置, 那么

$$[K : k] = \sum_{w|v} [K_w : k_v].$$

参考 [5, Ch2, 8.4].

Hensel 引理

引理： (Hensel 引理) 如果 $K = (K, |\cdot|)$ 是一个有非阿基米德赋值的完备域, A 是它的赋值环 $\{a \in K \mid |a| \leq 1\}$, 且 $f(x) \in A[x]$. 假设有 $\alpha_0 \in A$ 使得

$$|f(\alpha_0)| < |f'(\alpha_0)|^2.$$

那么, 序列

$$\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}, \quad i \in \mathbb{N}$$

收敛到 f 的一个根 α , 且 α 满足

$$|\alpha - \alpha_0| \leq \frac{|f(\alpha_0)|}{|f'(\alpha_0)|} < 1.$$

事实上, 这是 f 唯一一个满足此式的根.

参考<https://math.berkeley.edu/~vojta/254a/ho4.pdf>.

另有一个常用版本的 Hensel 引理:

引理: (Hensel 引理') 如果 $K = (K, |\cdot|)$ 是一个有非阿基米德赋值的完备域, A 是它的赋值环 $\{a \in K \mid |a| \leq 1\}$, $\mathfrak{p}$ 是 A 的素理想, $k = A/\mathfrak{p}$. 若 $f(x) \in A[x]$, $f \not\equiv 0 \pmod{\mathfrak{p}}$,

$$f(x) \equiv \bar{g}(x)\bar{h}(x) \pmod{\mathfrak{p}},$$

$\bar{g}(x), \bar{h}(x)$ 在 $k[x]$ 中互素, 那么

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

$\deg(g) = \deg(\bar{g})$, 且

$$g(x) \equiv \bar{g}(x) \pmod{\mathfrak{p}}, h(x) \equiv \bar{h}(x) \pmod{\mathfrak{p}}.$$

参考 [5, Ch2, 4.6].

参考文献

- [1] Dinakar Ramakrishnan and Robert J. Valenza, Fourier Analysis on Number Fields, Springer-Verlag, 1999.
- [2] H.L. Royden and P.M. Fitzpatrick, Real Analysis (Fourth Edition), China Machine Press, 2020
- [3] Walter Rudin, Real and Complex Analysis (Third Edition), McGraw-Hill Book Company, 1987.
- [4] Anton Deitmar and Siegfried Echterhoff, Principles of Harmonic Analysis, Second Edition, Springer-Verlag, 2009.
- [5] Jürgen Neukirch, Algebraic Number Theory, Springer-Verlag, 1999.
- [6] J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory (Second Edition), London Mathematical Society, 2010.
- [7] Bjorn Poonen, "Tate's Thesis", <https://math.mit.edu/~poonen/786/notes.pdf>
- [8] Artin Emil and Whaples George (1946), "A note on axiomatic characterization of fields", Bull. Amer. Math. Soc., 52: P 245-247
- [9] Paul Garrett, "Number theory notes 2011-21", https://www-users.cse.umn.edu/~garrett/m/number_theory/Notes_2011-12.pdf
- [10] Gabriel Daniel Villa Salvador, Topics in the Theory of Algebraic Function Fields, Birkhauser Boston, 2006
- [11] A. Wawrzyńczyk, "On tempered distributions and Bochner-Schwartz theorem on arbitrary locally compact abelian groups", Colloquium Mathematicae (1968), Volume: 19, Issue: 2, P 305-318