代数数论讲义*

代数理论I：整体域与局部域†

伍海亮(Hai-Liang Wu)

*我们的主线任务是介绍学习算术几何所需的基本内容.

Dedicated to My Wife, Li Yang

前言

写这份代数数论讲义是为了方便自己平时的研究工作. 讲义共有五个部分：(i) 整体域与局部域(Global Fields and Local Fields), (ii) 类域论(Class Field Theory), (iii) 椭圆曲线(Elliptic Curves), (iv) 模形式(Modular Forms), (v) 算术几何(Arithmetic Geometry).

在此我要感谢我的导师南京大学数学系孙智伟教授. 老师对数论的热情一直激励着我.

我也要感谢我的师兄潘颢教授一直以来的支持与鼓励, 感谢我的同门好友王李远副教授, 师姐尼贺霞副教授, 师弟佘跃峰博士, 我们一起合作完成了许多工作.

我也十分感谢我的学生李宇博, 未宁柳, 李洁, 彭威峰, 季筱涵, 吉敬寒, 李宇豪, 龚洋炀, 吴德浩, 黄帅豪, 与大家相处的时光是充实并愉快的.

希望自己可以在代数数论与算术几何领域做出一些有价值的成果.

伍海亮

2025年3月

目录

1 整性

1.1 整性的定义与基本性质

我们首先给出如下定义.

定义 1.1. 设$A \subseteq B$为两个交换幺环. 对于$b \in B$, 如果b满足某个首一的多项式方程

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0,$$

(其中$n \in \mathbb{Z}_{\geq 1}$, $a_0, a_1, \cdots, a_{n-1} \in A$), 则称$b$在$A$上整. 如果$B$中每个元素都在$A$上整, 则称$B$在$A$上整.

下面的结论可以用来判断元素的整性.

定理 1.1. 设$A \subseteq B$为两个交换幺环, $b_1, b_2, \cdots, b_n \in B$. 则$b_1, b_2, \cdots, b_n$在$A$上整当且仅当$A[b_1, b_2, \cdots, b_n]$为有限生成$A$模.

证明: "⇐". 假设$A[b_1, b_2, \cdots, b_n] = Ax_1 + Ax_2 + \cdots + Ax_m$为有限生成$A$模, 其中$x_1, \cdots, x_m \in B$. 下面我们证明一个更强的结论: $A[b_1, b_2, \cdots, b_n]$在A上整. 事实上, 对任意的$b \in A[b_1, b_2, \cdots, b_n]$与$1 \leq i \leq m$, 设

$$bx_i = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{im}x_m,$$

其中$a_{ij} \in A$. 则有

$$(bI_m - M)\,\boldsymbol{x} = \mathbf{0},$$

其中I_m为m阶单位矩阵, $M = (a_{ij})_{1 \leq i,j \leq m}$, $\boldsymbol{x} = (x_1, x_2, \cdots, x_m)^T$. 上式两边同时从左侧乘上$bI_m - M$的伴随矩阵$\mathrm{adj}(bI_m - M)$得到

$$\det(bI_m - M) \cdot \boldsymbol{x} = \mathbf{0},$$

即$\det(bI_m - M)\, x_i = 0\ (\forall 1 \leq i \leq m)$. 因为1可以表示成$x_1, x_2, \cdots, x_m$的$A$线性组合, 我们有$\det(bI_m - M) = 0$. 因此$b$在$A$上整.

"⇒". 我们对n归纳. 当$n = 1$时, 因为b_1在A上整, 可以设b_1满足方程

$$b_1^r + a_{r-1}b_1^{r-1} + \cdots + a_1 b_1 + a_0 = 0\ (r \in \mathbb{Z}_{\geq 1}, a_0, \cdots, a_{r-1} \in A).$$

这说明$A[b_1] = A + Ab_1 + \cdots + Ab_1^{r-1}$为有限生成$A$模. 假设$n \geq 2$并且结论对$n-1$成立. 则$b_1, b_2, \cdots, b_n$在$A$上整$\Rightarrow$ b_n在$A[b_1, \cdots, b_{n-1}]$上整. 由$n = 1$时

的结论, $A[b_1,\cdots,b_{n-1},b_n]=A[b_1,\cdots,b_{n-1}][b_n]$为有限生成$A[b_1,\cdots,b_{n-1}]$模. 由归纳假设, $A[b_1,\cdots,b_{n-1}]$是有限生成A模. 这些说明$A[b_1,\cdots,b_{n-1},b_n]$是有限生成$A$模.

综上, 我们完成了证明. □

注记 1.1. 由定理的证明我们发现

$$\begin{aligned} b_1,\cdots,b_n\text{在}A\text{上整} &\Rightarrow A[b_1,\cdots,b_n]\text{为有限生成}A\text{模} \\ &\Rightarrow \text{任意的}b\in A[b_1,\cdots,b_n]\text{均在}A\text{上整}. \end{aligned}$$

这说明集合

$$\bar{A}:=\{b\in B:\ b\text{在}A\text{上整}\}$$

中任意两个元素的和, 差, 积均在A上整, 即$\bar{A}$是B的子环. 我们将其称作A在B上的整闭包.

下面我们给出整闭整环的定义.

定义 1.2. 设A为整环, $\mathrm{frac}(A)=K$. 如果

$$\{x\in K:\ x\text{在}A\text{上整}\}=A,$$

则称A为整闭整环.

例如, 唯一因子分解整环(ufd)就是一个整闭整环. 事实上, 设A为唯一因子分解整环, $\mathrm{frac}(A)=K$. 对任意的$x\in K$, 设$x=y/z$, 其中$y,z\in A$, $z\neq 0$且$\gcd(y,z)=1$. 如果x在A上整, 则x满足某个方程

$$x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0\ (n\in\mathbb{Z}_{\geq 1},a_0,\cdots,a_{n-1}\in A).$$

上式两边同时乘上z^n得到$y^n\equiv 0\ (\mathrm{mod}\ zA)$. 因为$\gcd(y,z)=1$, 我们有$y\equiv 0\ (\mathrm{mod}\ zA)$. 因此$x=y/z\in A$, 即$A$为整闭整环.

关于整闭整环, 我们有如下结果.

命题 1.1. 设A为整闭整环, $\mathrm{frac}(A)=K$, L/K为域的有限扩张. 则下列结论成立:

(i) 设B为A在L中的整闭包. 则

$$L=\left\{\frac{b}{a}:\ b\in B,a\in A\setminus\{0\}\right\}.$$

(ii) 对任意的$x \in L$, 设$p_x(t)$为x在K上的极小多项式. 则

$$x在A上整 \Leftrightarrow p_x(t) \in A[t].$$

证明: (i) 对任意的$y \in L$, 因为L/K为域的有限扩张, y为K上的代数元, 不妨设y满足方程

$$y^n + \frac{a_{n-1}}{a}y^{n-1} + \cdots + \frac{a_1}{a}y + \frac{a_0}{a} = 0,$$

其中$n \in \mathbb{Z}_{\geq 1}, a, a_0, \cdots, a_{n-1} \in A$且$a \neq 0$. 上式两边同时乘上$a^n$得到

$$(ay)^n + a_{n-1}(ay)^{n-1} + \cdots + a_1 a^{n-2}(ay) + a_0 a^{n-1} = 0.$$

这说明$ay \in B$, 即$y \in \frac{1}{a}B$. 因此(i)成立.

(ii) "⇒". 设x在A上整. 则存在一个首一多项式$f(t) \in A[t]$使得$\deg(f) \geq 1$且$f(x) = 0$. 因此$f(t) \equiv 0 \pmod{p_x(t)A[t]}$. 这说明$p_x(t)$在$K^{\mathrm{alg}}$中的所有零点均在$A$上整. 因为$p_x(t)$的系数可以表示成这些零点的多项式, 由注记1.1, 多项式$p_x(t)$的系数均在A上整. 注意到$p_x(t) \in K[t]$且A为整闭整环, 由上面的结果可以得到$p_x(t) \in A[t]$.

"⇐". 显然成立.

综上, 我们完成了证明. □

1.2 元素的迹与范数

我们首先给出元素的迹与范数的一般定义.

定义 1.3. 设L/K为域的有限扩张. 对任意的$x \in L$, 设K-线性变换T_x为

$$T_x(y) = xy \ (\forall y \in L).$$

则将T_x的迹称为元素x的迹, 记作$\mathrm{Tr}_{L/K}(x)$; 将T_x的行列式称为元素x的范数, 记作$\mathrm{N}_{L/K}(x)$.

关于迹与范数, 我们有如下注记.

注记 1.2. (i) 线性变换在不同基下的矩阵是相似的, 因此元素的迹与范数的定义是合理的.

(ii) 设$[L : K] = n$, 设

$$f_x(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

为T_x的特征多项式. 则

$$\mathrm{Tr}_{L/K}(x) = -a_{n-1} \in K,\ \mathrm{N}_{L/K}(x) = (-1)^n a_0 \in K.$$

(iii) 对任意的$x, y \in L$, 显然有

$$T_x + T_y = T_{x+y},\ T_x \circ T_y = T_{xy}.$$

因此,

$$\mathrm{Tr}_{L/K}(x+y = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y),\ \mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y).$$

注意到当$x \neq 0$时, T_x是可逆的线性变换. 因此$\mathrm{N}_{L/K}(x) \neq 0 (\forall x \neq 0)$. 由上面的讨论,

$$\mathrm{Tr}_{L/K}(\cdot):\ L \to K \text{为加法群同态},$$

$$\mathrm{N}_{L/K}(\cdot):\ L^\times \to K^\times \text{为乘法群同态}.$$

(iv) 对任意的$x \in K$显然有

$$\mathrm{Tr}_{L/K}(x) = x\mathrm{Tr}_{L/K}(1) = [L:K]x,$$

$$\mathrm{N}_{L/K}(x) = x^{[L:K]}\mathrm{N}_{L/K}(1) = x^{[L:K]}.$$

我们下面考虑有限可分域扩张情形下的迹与范数.

命题 1.2. 设L/K为域的有限扩张. 对任意的$x \in L$, 设$f_x(t)$为T_x的特征多项式, $p_x(t)$为x在K上的极小多项式. 则

$$f_x(t) = p_x(t)^{[L:K(x)]}.$$

更进一步, 如果L/K还为域的有限可分扩张, 则

$$f_x(t) = \prod_{\sigma \in \mathrm{Hom}_K(L, K^{\mathrm{alg}})} (t - \sigma(x)).$$

并且因此

$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \mathrm{Hom}_K(L, K^{\mathrm{alg}})} \sigma(x),$$

$$\mathrm{N}_{L/K}(x) = \prod_{\sigma \in \mathrm{Hom}_K(L, K^{\mathrm{alg}})} \sigma(x).$$

证明: 设$[K(x):K]=m,[L:K(x)]=n,x$在K上的极小多项式

$$p_x(t)=t^m+c_{m-1}t^{m-1}+\cdots+c_1t+c_0.$$

设$y_1,y_2,\cdots,y_n\in L$为$L/K(x)$的一组基. 则

$$y_1,y_1x,\cdots,y_1x^{m-1},y_2,y_2x,\cdots,y_2x^{m-1},\cdots,y_n,y_nx,\cdots,y_nx^{m-1}$$

为L/K的一组基. 容易验证T_x在这组基的下的矩阵为分块对角矩阵

$$M_x=\operatorname{diag}(C,C,\cdots,C),$$

其中

$$C=\begin{pmatrix}0&0&\cdots&0&-c_0\\1&0&\cdots&0&-c_1\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&1&-c_{m-2}\\0&0&\cdots&0&-c_{m-1}\end{pmatrix}.$$

因此,

$$f_x(t)=\det(tI_{mn}-M_x)=(\det(tI_m-C))^n=p_x(t)^n.$$

下面进一步假设L/K为域的有限可分扩张. 此时$\mathrm{Hom}_K(K(x),K^{\mathrm{alg}})$中每个元素恰好有$[L:K(x)]=n$种方式延拓为$\mathrm{Hom}_K(L,K^{\mathrm{alg}})$中的元素. 因此, 由上面的结果可以得到

$$\begin{aligned}f_x(t)=p_x(t)^n&=\prod_{\sigma\in\mathrm{Hom}_K(K(x),K^{\mathrm{alg}})}(t-\sigma(x))^n\\&=\prod_{\rho\in\mathrm{Hom}_K(L,K^{\mathrm{alg}})}(t-\rho(x)).\end{aligned}$$

由此以及注记1.2(ii)可以得到$\mathrm{Tr}_{L/K}(x)$与$\mathrm{N}_{L/K}(x)$的表达式.

综上, 我们完成了证明. □

下面的结论说明迹与范数具有传递性.

命题 1.3. *设$K\subseteq L\subseteq M$为域的有限可分扩张. 则对任意的$x\in M$,*

$$\mathrm{Tr}_{M/K}(x)=\mathrm{Tr}_{L/K}\left(\mathrm{Tr}_{M/L}(x)\right),\ \mathrm{N}_{M/K}(x)=\mathrm{N}_{L/K}\left(\mathrm{N}_{M/L}(x)\right).$$

证明: 我们仅对迹证明该结果, 范数的情形是类似的. 在$\mathrm{Hom}_K(M,K^{\mathrm{alg}})$上定义等价关系"$\sim$"为

$$\sigma\sim\tau\Leftrightarrow\sigma|_L=\tau|_L\ (\forall\sigma,\tau\in\mathrm{Hom}_K(M,K^{\mathrm{alg}})).$$

设$\mathcal{R}$为$\mathrm{Hom}_K(M,K^{\mathrm{alg}})$在该等价关系下的一个代表元系. 则容易验证

$$\mathrm{Hom}_K(L,K^{\mathrm{alg}})=\{\sigma|_L:\ \sigma\in\mathcal{R}\}.$$

另一方面, 对任意的$\sigma\in\mathcal{R}$, 注意到

$$\left\{\tau\sigma^{-1}:\ \tau\sim\sigma\right\}=\mathrm{Hom}_{\sigma(L)}(\sigma(M),K^{\mathrm{alg}}).$$

由上面的结果与命题1.2, 可以得到

$$\begin{aligned}\mathrm{Tr}_{M/K}(x)&=\sum_{\sigma\in\mathrm{Hom}_K(M,K^{\mathrm{alg}})}\sigma(x)\\&=\sum_{\sigma\in\mathcal{R}}\sum_{\tau\sim\sigma}\tau(x)\\&=\sum_{\sigma\in\mathcal{R}}\sum_{\tau\sim\sigma}\tau\sigma^{-1}\sigma(x)\\&=\sum_{\sigma\in\mathcal{R}}\sum_{\rho\in\mathrm{Hom}_{\sigma(L)}(\sigma(M),K^{\mathrm{alg}})}\rho\sigma(x)\\&=\sum_{\sigma\in\mathcal{R}}\mathrm{Tr}_{\sigma(M)/\sigma(L)}\sigma(x)\\&=\sum_{\sigma\in\mathcal{R}}\sigma|_L\left(\mathrm{Tr}_{M/L}(x)\right)\\&=\sum_{\psi\in\mathrm{Hom}_K(L,K^{\mathrm{alg}})}\psi\left(\mathrm{Tr}_{M/L}(x)\right)\\&=\mathrm{Tr}_{L/K}\left(\mathrm{Tr}_{M/L}(x)\right).\end{aligned}$$

综上, 我们完成了证明. □

下面给出基的判别式的定义.

定义 1.4. *设L/K为域的n次有限可分扩张, $\mathrm{Hom}_K(L,K^{\mathrm{alg}})=\{\sigma_1,\cdots,\sigma_n\}$. 则对$L/K$的任意一组基$x_1,x_2,\cdots,x_n$, 将其判别式定义为*

$$d(x_1,x_2,\cdots,x_n)=\left(\det\left[\sigma_i(x_j)\right]_{1\leq i,j\leq n}\right)^2.$$

关于基的判别式, 我们有如下注记.

注记 1.3. 设$X=[\sigma_i(x_j)]_{1\leq i,j\leq n}$. 则容易验证

$$d(x_1,x_2,\cdots,x_n)=(\det X)^2=\det(X^TX)=\det\left[\mathrm{Tr}_{L/K}(x_ix_j)\right]_{1\leq i,j\leq n}.$$

由此与注记1.2(iii), 可以得到$d(x_1,x_2,\cdots,x_n)\in K$.

下面我们来说明基的判别式不为零. 为此, 我们介绍经典的Dedekind无关性引理.

引理 1.1. 设G为乘法群, L为域, $\sigma_1,\sigma_2,\cdots,\sigma_n\in\mathrm{Hom}(G,L^\times)$为两两不同的群同态. 如果存在$c_1,c_2,\cdots,c_n\in L$使得

$$c_1\sigma_1+c_2\sigma_2+\cdots+c_n\sigma_n$$

为$G\to L$的零函数, 则$c_1=c_2=\cdots=c_n=0$.

证明: 使用反证法. 假设存在不全为0的$c_1,c_2,\cdots,c_n\in L$使得$c_1\sigma_1+\cdots+c_n\sigma_n=0$, 其中0表示$G\to L$的零函数. 则集合

$$\left\{k\in\mathbb{Z}^+:\text{存在}x_{i_1},\cdots,x_{i_k}\in L^\times(i_1<\cdots<i_k)\text{使得}x_{i_1}\sigma_{i_1}+\cdots+x_{i_k}\sigma_{i_k}=0\right\}$$

非空. 设r为该集合中最小的元素. 通过给这些σ_i重新编号, 不妨设

$$x_1\sigma_1+\cdots+x_r\sigma_r=0\ (x_1,\cdots,x_r\in L^\times).$$

因为这些σ_i均不为零函数, 此时必有$r\geq 2$. 又因为$\sigma_1\neq\sigma_2$, 存在$g_0\in G$使得$\sigma_1(g_0)\neq\sigma_2(g_0)$. 由上面的结果, 对任意的$g\in G$, 可以得到下面两个等式:

$$\begin{aligned}x_1\sigma_1(g_0)\sigma_1(g)+x_2\sigma_2(g_0)\sigma_2(g)+\cdots+x_n\sigma_n(g_0)\sigma_n(g)=0,\\ x_1\sigma_1(g_0)\sigma_1(g)+x_2\sigma_1(g_0)\sigma_2(g)+\cdots+x_n\sigma_1(g_0)\sigma_n(g)=0.\end{aligned}$$

两式相减得到

$$x_2\left(\sigma_2(g_0)-\sigma_1(g_0)\right)\sigma_2(g)+\cdots+x_n\left(\sigma_n(g_0)-\sigma_1(g_0)\right)\sigma_n(g)=0,$$

即

$$x_2\left(\sigma_2(g_0)-\sigma_1(g_0)\right)\sigma_2+\cdots+x_n\left(\sigma_n(g_0)-\sigma_1(g_0)\right)\sigma_n=0.$$

因为$\sigma_2(g_0)-\sigma_1(g_0)\neq 0$, 上式与$r$的最小性矛盾.

综上, 我们完成了证明. □

命题 1.4. 设L/K为域的有限可分扩张, $x_1, x_2, \cdots, x_n$为L/K的一组基. 则

$$d(x_1, x_2, \cdots, x_n) \neq 0.$$

证明: 使用反证法. 假设$d(x_1, x_2, \cdots, x_n) = 0$. 则矩阵$X = [\sigma_i(x_j)]_{1\leq i,j\leq n}$的行向量组在$L$上线性相关, 其中 $\{\sigma_1, \cdots, \sigma_n\} = \mathrm{Hom}_K(L, K^{\mathrm{alg}})$. 因此存在不全为0的$c_1, c_2, \cdots, c_n \in L$使得

$$c_1\sigma_1(x_j) + c_2\sigma_2(x_j) + \cdots + c_n\sigma_n(x_j) = 0 \ (\forall 1 \leq j \leq n).$$

因为$x_1, \cdots, x_n$为L/K的一组基, 上式说明

$$c_1\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_n\sigma_n(x) = 0 \ (\forall x \in L^\times).$$

这与Dedekind无关性引理矛盾.

综上, 我们完成了证明. □

1.3 整基的定义

我们首先给出整基的定义.

定义 1.5. 设A为整闭整环, $\mathrm{frac}(A) = K$. 设L/K为域的有限可分扩张,

$$B = \{x \in L : \ x在A上整\}$$

为A在L中的整闭包. 如果存在$\omega_1, \omega_2, \cdots, \omega_n \in B$使得$B$中的每个元素$b$都可以唯一表示成

$$b = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n \ (a_1, a_2, \cdots, a_n \in A)$$

的形式, 则称$\omega_1, \omega_2, \cdots, \omega_n$为$B$在$A$上的一组整基.

对于一般的整闭整环A, 整闭包B在A上的整基不一定存在. 但是当A为主理想整环(pid)时, 可以证明整基一定存在. 为此我们需要下面两个引理.

引理 1.2. 设A为整闭整环, $\mathrm{frac}(A) = K$. 设L/K为域的有限可分扩张,

$$B = \{x \in L : \ x在A上整\}$$

为A在L中的整闭包. 则对任意的$b \in B$都有$\mathrm{Tr}_{L/K}(b) \in A$与$\mathrm{N}_{L/K}(b) \in A$.

证明: 设$p_b(t)$为b在K上的极小多项式. 则由命题1.1(ii), 多项式$p_b(t) \in A[t]$. 由此以及命题1.2, 线性变换T_b的特征多项式

$$f_b(t) = p_b(t)^{[L:K(x)]} \in A[t].$$

再由注记1.2(ii), $\mathrm{Tr}_{L/K}(b) \in A$, $\mathrm{N}_{L/K}(b) \in A$.

综上, 我们完成了证明. □

下面的引理是非常有用的结论.

引理 1.3. *设A为整闭整环, $\mathrm{frac}(A) = K$. 设L/K为域的有限可分扩张,*

$$B = \{x \in L : \ x在A上整\}$$

为A在L中的整闭包. 设$b_1, b_2, \cdots, b_n \in B$为$L/K$的一组基(由命题1.1(i)这样的基是存在的). 则

$$d(b_1, b_2, \cdots, b_n)B \subseteq Ab_1 + Ab_2 + \cdots + Ab_n.$$

证明: 对任意的$b \in B$, 因为$b_1, b_2, \cdots, b_n \in B$为$L/K$的一组基, 可以设

$$b = x_1b_1 + x_2b_2 + \cdots + x_nb_n \ (x_1, x_2, \cdots, x_n \in K).$$

则对任意的$1 \leq i \leq n$,

$$bb_i = x_1b_ib_1 + x_2b_ib_2 + \cdots + x_nb_ib_n.$$

因此,

$$\mathrm{Tr}_{L/K}(bb_i) = \sum_{1 \leq j \leq n} x_j \mathrm{Tr}_{L/K}(b_ib_j).$$

由Cramer法则与引理1.2, 对任意的$1 \leq j \leq n$,

$$d(b_1, b_2, \cdots, b_n)x_j = \det\left[\mathrm{Tr}_{L/K}(b_ib_j)\right]_{1 \leq i,j \leq n} x_j \in A.$$

因此,

$$d(b_1, b_2, \cdots, b_n)B \subseteq Ab_1 + Ab_2 + \cdots + Ab_n.$$

综上, 我们完成了证明. □

注记 1.4. *由引理1.2与命题1.4,*

$$d(b_1, b_2, \cdots, b_n) = \det\left[\mathrm{Tr}_{L/K}(b_ib_j)\right]_{1 \leq i,j \leq n} \in A \setminus \{0\}.$$

下面我们介绍这一节的核心定理.

定理 1.2. 设A为主理想整环, $\mathrm{frac}(A)=K$. 设L/K为域的有限可分扩张,

$$B=\{x\in L:\ x在A上整\}$$

为A在L中的整闭包. 则L中任意的有限生成非零B模M是秩为$[L:K]$的自由A模. 特别地, B在A上的整基是存在的.

证明: 设$b_1,b_2,\cdots,b_n\in B$为L/K的一组基, $d=d(b_1,b_2,\cdots,b_n)\in A\setminus\{0\}$为其判别式. 设$M=Bx_1+Bx_2+\cdots+Bx_m$为$L$上的有限生成非零$B$模, 其中$x_1\neq 0$. 首先, 由命题1.1(i), 存在$a\in A\setminus\{0\}$使得$ax_i\in B$ ($\forall 1\leq i\leq n$). 因此, 利用引理1.3可以得到

$$adM\subseteq Ab_1+Ab_2+\cdots+Ab_n.$$

由此与主理想整环上自由模子模的性质我们知道M是自由A模.

下面考虑$\mathrm{rank}_A(M)$. 由于

$$b_1,b_2,\cdots,b_n\in B\subseteq\frac{1}{d}\left(Ab_1+Ab_2+\cdots+Ab_n\right),$$

我们有$\mathrm{rank}_A(B)=n$. 另一方面, 因为

$$B\subseteq x_1^{-1}M\subseteq\frac{1}{ad}\left(Ab_1+Ab_2+\cdots+Ab_n\right),$$

我们得到$\mathrm{rank}_A(M)=n$.

综上, 我们完成了证明. □

下面我们给出代数整数与代数数域的定义.

定义 1.6. 对任意的$x\in\mathbb{Q}^{\mathrm{alg}}$, 如果$x$在$\mathbb{Z}$上整, 则称$x$为一个代数整数. 如果$K/\mathbb{Q}$为域的有限扩张, 则称$K$为一个代数数域. 并且称

$$\mathcal{O}_K=\{x\in K:\ x在\mathbb{Z}上整\}$$

为K的代数整数环.

注记 1.5. (i) 由定理1.2, 代数数域K上任意有限生成的非零$\mathcal{O}_K$模M是一个秩为$[K:\mathbb{Q}]$的自由$\mathbb{Z}$模. 特别地, $\mathcal{O}_K$在$\mathbb{Z}$上的整基是存在的.

(ii) 设M为代数数域K上的有限生成非零$\mathcal{O}_K$模, $x_1,\cdots,x_n$与$y_1,\cdots,y_n$分别为M的两组$\mathbb{Z}$基. 设

$$(x_1,x_2,\cdots,x_n)=(y_1,y_2,\cdots,y_n)T,$$

其中$T\in M_{n\times n}(\mathbb{Z})$为两组$\mathbb{Z}$基之间的过渡矩阵(注意此时$\det T=\pm 1$). 如果设

$$\{\sigma_1,\sigma_2,\cdots,\sigma_n\}=\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{Q}^{\mathrm{alg}}),$$

则容易验证

$$[\sigma_i(x_j)]_{1\leq i,j\leq n}=[\sigma_i(y_j)]_{1\leq i,j\leq n}\,T.$$

由此得到

$$d(x_1,\cdots,x_n)=d(y_1,\cdots,y_n),$$

即M的任意一组$\mathbb{Z}$基的判别式均相同.

由上面的注记, 我们给出如下定义.

定义 1.7. 设K为代数数域, M为K上有限生成的非零$\mathcal{O}_K$模. 则M的任意一组$\mathbb{Z}$基的判别式均相同, 我们将这个量称为M的绝对判别式, 记作$d(M)$. 特别地, 将$d(\mathcal{O}_K)$简记为$d(K)$, 并称其为代数数域K的绝对判别式.

我们以下面这个非常有用的结论来结束这一节的内容. 在下一节, 我们将利用它给出二次代数数域的整基.

命题 1.5. 设K为代数数域, $M\subseteq M'$为K上两个有限生成的非零$\mathcal{O}_K$模. 则

$$d(M)=[M':M]^2\cdot d(M').$$

证明: 由主理想整环上自由模子模的性质, 存在M'的一组$\mathbb{Z}$基$\omega_1,\cdots,\omega_n$以及正整数$r_1,\cdots,r_n$使得

$$M'=\mathbb{Z}\omega_1+\mathbb{Z}\omega_2+\cdots+\mathbb{Z}\omega_n,$$
$$M=\mathbb{Z}r_1\omega_1+\mathbb{Z}r_2\omega_2+\cdots+\mathbb{Z}r_n\omega_n.$$

因此,

$$\begin{aligned}d(M)&=\det\left[\mathrm{Tr}_{K/\mathbb{Q}}(r_ir_j\omega_i\omega_j)\right]_{1\leq i,j\leq n}\\&=(r_1r_2\cdots r_n)^2\det\left[\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j)\right]_{1\leq i,j\leq n}\\&=[M':M]^2\cdot d(M').\end{aligned}$$

综上, 我们完成了证明. □

1.4 二次域的整基与绝对判别式

二次代数数域的整基与绝对判别式是容易得到的.

定理 1.3. 设$d \in \mathbb{Z} \setminus \{0,1\}$为无平方因子整数, $K = \mathbb{Q}(\sqrt{d})$为二次域. 则

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

并且因此,

$$d(K) = \begin{cases} 4d & \text{如果 } d \equiv 2,3 \pmod 4, \\ d & \text{如果 } d \equiv 1 \pmod 4. \end{cases}$$

证明: 显然$1, \sqrt{d} \in \mathcal{O}_K$, 因此$M = \mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq \mathcal{O}_K$. 由命题1.5,

$$4d = d(M) = [\mathcal{O}_K : M]^2 \cdot d(K).$$

因为$d \in \mathbb{Z} \setminus \{0,1\}$为无平方因子整数, 上式说明$[\mathcal{O}_K : M] \in \{1,2\}$. 因此, $2\mathcal{O}_K \subseteq M$, 即

$$\mathcal{O}_K \subseteq \mathbb{Z}\frac{1}{2} + \mathbb{Z}\frac{\sqrt{d}}{2}.$$

由命题1.1(ii)我们知道$1/2 \notin \mathcal{O}_K$, $\sqrt{d}/2 \notin \mathcal{O}_K$. 由此与上式可以得到

$$\mathcal{O}_K \subseteq \left\{ \frac{1}{2}x + \frac{\sqrt{d}}{2}y : \ x,y \in \mathbb{Z}\text{且}x \equiv y \pmod{2\mathbb{Z}} \right\},$$

以及

$$\mathcal{O}_K = \left\{ \frac{1}{2}x + \frac{\sqrt{d}}{2}y : \ x,y \in \mathbb{Z}\text{且}x \equiv y \pmod{2\mathbb{Z}} \right\} \Leftrightarrow \frac{1}{2} + \frac{\sqrt{d}}{2} \in \mathcal{O}_K,$$

$$\mathcal{O}_K = M \Leftrightarrow \frac{1}{2} + \frac{\sqrt{d}}{2} \notin \mathcal{O}_K.$$

注意到$\frac{1}{2} + \frac{\sqrt{d}}{2}$在$\mathbb{Q}$上的极小多项式为

$$t^2 - t + \frac{1-d}{4}.$$

利用命题1.1(ii)与上面的结果, 可以得到

$$\mathcal{O}_K = \left\{ \frac{1}{2}x + \frac{\sqrt{d}}{2}y : \ x,y \in \mathbb{Z}\text{且}x \equiv y \pmod{2\mathbb{Z}} \right\} \Leftrightarrow d \equiv 1 \pmod 4,$$

以及

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d} \Leftrightarrow d \equiv 2, 3 \pmod 4.$$

由此容易验证

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

以及

$$d(K) = \begin{cases} 4d & \text{如果 } d \equiv 2, 3 \pmod 4, \\ d & \text{如果 } d \equiv 1 \pmod 4. \end{cases}$$

综上, 我们完成了证明. □

2 Dedekind环

2.1 Dedekind环上分式理想的素理想分解

我们首先给出Dedekind环的定义.

定义 2.1. 设A为整环. 如果A满足以下三个条件: (i) A为诺特环; (ii) A整闭; (iii) A的每个非零素理想都是极大理想, 则称A为一个*Dedekind*环.

下面我们来说明代数数域K的代数整数环就是一个Dedekind环. 为此, 我们需要下面这的引理.

引理 2.1. 设$A \subseteq B$为两个整环. 如果B在A上整, 则

$$A\text{为域} \Leftrightarrow B\text{为域}.$$

证明: "⇐". 假设B为域. 要证明A为域仅需说明: 对任意的$x \in A \setminus \{0\}$, 都有$1/x \in A$. 事实上, 因为B为域且在A上整, 元素$1/x \in B$且满足某个首一的多项式方程

$$\left(\frac{1}{x}\right)^n + a_{n-1}\left(\frac{1}{x}\right)^{n-1} + \cdots + a_1\frac{1}{x} + a_0 = 0,$$

其中$n \in \mathbb{Z}^+, a_0, a_1, \cdots, a_{n-1} \in A$. 上式两边同时乘上$x^{n-1}$可以得到

$$\frac{1}{x} = -\left(a_{n-1} + \cdots + a_1 x^{n-2} + a_0 x^{n-1}\right) \in A.$$

因此A为域.

"⇒". 假设A为域. 要说明B为域仅需说明: 对任意的$y \in B \setminus \{0\}$, 都有$1/y \in B$. 因为y在A上整, 可以设

$$p_y(t) = t^m + a'_{m-1}t^{m-1} + \cdots + a'_1 t + a'_0$$

为y在域A上的极小多项式. 注意到$a'_0 \neq 0$. 在$p_y(b) = 0$的两边同时乘上$(a'_0 b)^{-1}$可以得到

$$\frac{1}{b} = -\frac{1}{a'_0}\left(b^{m-1} + a'_{m-1}b^{m-2} + \cdots + a'_1\right) \in B.$$

因此B为域.

综上, 我们完成了证明. □

定理 2.1. *设K为代数数域. 则$\mathcal{O}_K$为Dedekind环.*

证明: 由$\mathcal{O}_K$的定义, $\mathcal{O}_K$本身是整闭整环. 因此下面仅需说明$\mathcal{O}_K$是诺特环并且非零素理想都是极大理想.

设$\omega_1, \omega_2, \cdots, \omega_n$为$\mathcal{O}_K$在$\mathbb{Z}$上的整基. 由主理想整环上自由模子模的性质, $\mathcal{O}_K$的每个理想也均为有限生成$\mathbb{Z}$模, 自然也是有限生成$\mathcal{O}_K$模. 因此, $\mathcal{O}_K$为诺特环.

设$\mathfrak{p}$为$\mathcal{O}_K$的非零素理想. 先说明$\mathfrak{p}\cap\mathbb{Z}$是$\mathbb{Z}$上的非零素理想. 事实上, 取$x \in \mathfrak{p}\setminus\{0\}$, 设

$$p_x(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

为x在$\mathbb{Q}$上的极小多项式. 则由命题1.1(ii), 多项式$p_x(t) \in \mathbb{Z}[t]$. 又因为$p_x(t)$是极小多项式, 常数项$a_0 \in A\setminus\{0\}$. 因此

$$a_0 = -(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x) \in \mathfrak{p}\cap\mathbb{Z}.$$

这说明$\mathfrak{p}\cap\mathbb{Z}$是$\mathbb{Z}$上的非零素理想. 因为$\mathbb{Z}$是主理想整环, 存在素数$p$使得$\mathfrak{p}\cap\mathbb{Z} = p\mathbb{Z}$. 注意到

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}$$

且$\mathcal{O}_K/\mathfrak{p}$在有限域$\mathbb{Z}/p\mathbb{Z}$上整. 由引理2.1, $\mathcal{O}_K/\mathfrak{p}$是域. 因此$\mathfrak{p}$为$\mathcal{O}_K$的极大理想.

综上, 我们证明了$\mathcal{O}_K$为Dedekind环. □

下面回到一般的Dedekind环. 我们将证明Dedekind环上的非零理想一定可以唯一分解为素理想的乘积. 为此, 我们介绍下面几个引理.

引理 2.2. *设A为诺特环. 则对A的任意非零理想$\mathfrak{a}$, 一定存在有限个非零素理想$\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_r$(可以出现相同的素理想)使得*

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r \subseteq \mathfrak{a}.$$

证明: 使用反证法. 假设

$$\Omega = \{0 \neq \mathfrak{a} \trianglelefteq A : \text{任意有限个非零素理想的乘积均不包含在}\mathfrak{a}\text{中}\} \neq \emptyset.$$

因为A为诺特环, Ω中存在极大元$\mathfrak{a}$. 显然$\mathfrak{a} \neq A$且$\mathfrak{a}$不为素理想. 因此存在$x, y \in A\setminus\mathfrak{a}$使得$xy \in \mathfrak{a}$. 这说明$\mathfrak{a} \subsetneq \mathfrak{a} + xA \notin \Omega$, $\mathfrak{a} \subsetneq \mathfrak{a} + yA \notin \Omega$. 因此存在有限个素理想$\mathfrak{p}_1, \cdots, \mathfrak{p}_r, \mathfrak{q}_1, \cdots, \mathfrak{q}_s$使得

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r \subseteq \mathfrak{a} + xA,\ \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s \subseteq \mathfrak{a} + yA.$$

由此,

$$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s\subseteq(\mathfrak{a}+xA)(\mathfrak{a}+yA)\subseteq\mathfrak{a}.$$

这与$\mathfrak{a}\in\Omega$矛盾.

综上, 我们完成了证明. □

引理 2.3. *设A为Dedekind环, $\mathrm{frac}(A)=K$, $\mathfrak{p}$为A的非零素理想. 设*

$$\mathfrak{p}^{-1}:=\{x\in K:\ x\mathfrak{p}\subseteq A\}.$$

则对K上任意的有限生成非零A模M, 都有$M\subsetneq\mathfrak{p}^{-1}M$.

证明: 容易验证$\mathfrak{p}^{-1}$是A模且$A\subseteq\mathfrak{p}^{-1}$. 首先说明$A\subsetneq\mathfrak{p}^{-1}$. 取$x\in\mathfrak{p}\setminus\{0\}$. 由引理2.2, 集合

$$\left\{m\in\mathbb{Z}^+:\ 存在m个非零素理想使得它们的乘积包含在xA中\right\}$$

不为空集. 设r为该集合的最小元素, 并且设

$$\mathfrak{p}_1\cdots\mathfrak{p}_r\subseteq xA\subseteq\mathfrak{p}.$$

下面分两种情况讨论.

情形1. $r=1$. 此时, $\mathfrak{p}_1=xA\subseteq\mathfrak{p}$. 因为$A$的每个非零素理想都是极大理想, 我们得到 $\mathfrak{p}_1=\mathfrak{p}$, 并且因此$xA=\mathfrak{p}$. 这说明$\frac{1}{x}\in\mathfrak{p}^{-1}\setminus A$, 即$A\subsetneq\mathfrak{p}^{-1}$.

情形2. $r\geq 2$. 注意到$\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r\subseteq\mathfrak{p}\Rightarrow\mathfrak{p}_1,\cdots,\mathfrak{p}_r$中至少有一个素理想包含在$\mathfrak{p}$中(否则对任意的$1\leq i\leq r$, 取$x_i\in\mathfrak{p}_i\setminus\mathfrak{p}$, 元素$x_1\cdots x_r\in\mathfrak{p}_1\cdots\mathfrak{p}_r\setminus\mathfrak{p}$). 不妨设$\mathfrak{p}_1\subseteq\mathfrak{p}$. 又因为$A$的每个非零素理想都是极大理想, 我们有$\mathfrak{p}_1=\mathfrak{p}$. 由$r$的最小性, $\mathfrak{p}_2\cdots\mathfrak{p}_r\not\subseteq xA$. 取$y\in\mathfrak{p}_2\cdots\mathfrak{p}_r\setminus xA$. 注意到$y/x\notin A$, 但

$$\frac{y}{x}\mathfrak{p}\subseteq\frac{1}{x}\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r\subseteq\frac{1}{x}xA=A,$$

即$y/x\in\mathfrak{p}^{-1}\setminus A$. 因此$A\subsetneq\mathfrak{p}^{-1}$.

对K上任意的有限生成非零A模M, 如果$\mathfrak{p}^{-1}M=M$, 则利用与定理1.1充分性的证明中类似的办法, 可以说明$\mathfrak{p}^{-1}$在A上整. 又因为A整闭, 我们得到$\mathfrak{p}^{-1}\subseteq A$. 这与$A\subsetneq\mathfrak{p}^{-1}$矛盾. 因此, $M\subsetneq\mathfrak{p}^{-1}M$.

综上, 我们完成了证明. □

注记 2.1. *由该引理, $\mathfrak{p}\subsetneq\mathfrak{p}\mathfrak{p}^{-1}\subseteq A$. 又因为$\mathfrak{p}$是极大理想, 我们有$\mathfrak{p}\mathfrak{p}^{-1}=A$.*

下面我们叙述核心定理.

定理 2.2. *设A为Dedekind环. 则A的任意非零真理想可以分解为有限个非零素理想的乘积. 并且在不考虑顺序的情况下, 这种分解是唯一的.*

证明: 先使用反证法证明素理想分解的存在性. 假设

$$\Omega = \{0 \neq \mathfrak{a} \lhd A : \mathfrak{a}\text{为真理想且不能表示为有限个素理想的乘积}\} \neq \emptyset.$$

因为A为诺特环, Ω中存在极大元$\mathfrak{a}$. 显然$\mathfrak{a}$不是极大理想. 因此存在A的一个极大理想$\mathfrak{p}$使得$\mathfrak{a} \subsetneq \mathfrak{p}$. 由引理2.3与注记2.1, $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} = A$. 这说明非零真理性$\mathfrak{a}\mathfrak{p}^{-1} \notin \Omega$. 因此存在有限个非零素理想$\mathfrak{p}_1, \cdots, \mathfrak{p}_r$使得

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r.$$

在上式两边同时乘上$\mathfrak{p}$并注意到$\mathfrak{p}\mathfrak{p}^{-1} = A$, 我们得到

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

这与$\mathfrak{a} \in \Omega$矛盾. 综上, 我们证明了素理想分解的存在性.

下面来证明唯一性. 设

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

为$\mathfrak{a}$的两个素理想分解. 类似于在引理2.3证明中遇到的情况, 在Dedeind环A中, $\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq \mathfrak{q}_1 \Rightarrow \mathfrak{p}_1, \mathfrak{p}_2 \cdots, \mathfrak{p}_r$中至少有一个素理想恰好等于$\mathfrak{q}_1$. 不妨设$\mathfrak{p}_1 = \mathfrak{q}_1$. 在上面的素理想分解式中乘上$\mathfrak{p}_1^{-1}$可以得到

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

不断重复上述步骤就可以证明分解的唯一性.

综上, 我们完成了证明. □

我们给出分式理想的定义.

定义 2.2. *设A为Dedekind环, $\mathrm{frac}(A) = K$. K上的有限生成非零A模称为A的一个分式理想. A的所有分式理想构成的集合记作$J(A)$. 同时, 将A的非零理想称为A的整理想.*

注记 2.2. *设A为Dedekind环, $\mathrm{frac}(A) = K$, $M \subseteq K$为非零A模. 则显然有*

$$M \in J(A) \Leftrightarrow \text{存在} a \in A \setminus \{0\} \text{使得} aM \text{为} A \text{的整理想}.$$

下面的结论说明在分式理想的乘法下$J(A)$具有群结构.

定理 2.3. *设A为Dedekind环, $\mathrm{frac}(A)=K$. 则$J(A)$在分式理想的乘法下构成乘法交换群. 其单位元为A, 并且对于任意的$\mathfrak{a}\in J(A)$, 分式理想$\mathfrak{a}$的逆元为*

$$\mathfrak{a}^{-1}=\{x\in K:\ x\mathfrak{a}\subseteq A\}.$$

证明: 要证明该定理仅需说明: 对任意的分式理想$\mathfrak{a}$, $\mathfrak{a}^{-1}$也是分式理想且$\mathfrak{a}\mathfrak{a}^{-1}=A$. 先说明$\mathfrak{a}^{-1}\in J(A)$. 显然$\mathfrak{a}^{-1}$是$A$模. 由注记2.2, 存在$x\in A\setminus\{0\}$使得$x\mathfrak{a}$为$A$的整理想. 取$y\in x\mathfrak{a}\setminus\{0\}\subseteq A\setminus\{0\}$. 则$y\mathfrak{a}^{-1}\subseteq\mathfrak{a}\mathfrak{a}^{-1}\subseteq A$为整理想. 因此由注记2.2, $\mathfrak{a}^{-1}\in J(A)$.

下面来说明$\mathfrak{a}\mathfrak{a}^{-1}=A$. 使用反证法. 假设$\mathfrak{a}\mathfrak{a}^{-1}\subsetneq A$. 因为$\mathfrak{a}\mathfrak{a}^{-1}$是$A$的整理想, 存在$A$的极大理想$\mathfrak{p}$使得$\mathfrak{a}\mathfrak{a}^{-1}\subseteq\mathfrak{p}\subsetneq A$. 这得到

$$\mathfrak{a}\mathfrak{a}^{-1}\mathfrak{p}^{-1}\subseteq\mathfrak{p}\mathfrak{p}^{-1}=A.$$

因此$\mathfrak{a}^{-1}\mathfrak{p}^{-1}\subseteq\mathfrak{a}^{-1}$. 这与引理2.3矛盾.

综上, 我们完成了证明. □

由定理2.3可以得到如下结果.

定理 2.4. *设A为Dedekind环. 则$J(A)$中的每个分式理想$\mathfrak{a}$都可以唯一的表示为*

$$\mathfrak{a}=\prod_{\mathfrak{p}}\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})}$$

的形式, 其中$\mathfrak{p}$取遍A的所有非零素理想, $\mathrm{ord}_{\mathfrak{p}}\in\mathbb{Z}$并且对几乎所有的$\mathfrak{p}$都有$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})=0$. 我们将$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$称为分式理想$\mathfrak{a}$的$\mathfrak{p}$-adic order.

由该定理我们发现分式理想完全由其在每个非零素理想$\mathfrak{p}$处的$\mathfrak{p}$-adic order所确定. 我们给出关于$\mathfrak{p}$-adic order的注记.

注记 2.3. (i) 对于理想A, $\mathrm{ord}_{\mathfrak{p}}(A)=0\ (\forall\mathfrak{p})$. 另外补充定义$\mathrm{ord}_{\mathfrak{p}}(0)=+\infty\ (\forall\mathfrak{p})$.

(ii) 设$\mathfrak{a},\mathfrak{b}\in J(A)$. 则容易验证

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b})=\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})+\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}),$$
$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b})=\min\{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}),\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})\},$$
$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}\cap\mathfrak{b})=\max\{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}),\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})\}.$$

(iii) 对任意的$x\in\mathrm{frac}(A)$, 定义元素x的$\mathfrak{p}$-adic order为

$$\mathrm{ord}_{\mathfrak{p}}(x):=\mathrm{ord}_{\mathfrak{p}}(xA).$$

我们有如下的强三角不等式.

命题 2.1. *设A为Dedekind环, $\mathrm{frac}(A)=K$, $\mathfrak{p}$为A的非零素理想. 对任意$x,y\in K$, 强三角不等式*

$$\mathrm{ord}_{\mathfrak{p}}(x+y)\geq \min\{\mathrm{ord}_{\mathfrak{p}}(x),\mathrm{ord}_{\mathfrak{p}}(y)\}$$

成立. 并且当$\mathrm{ord}_{\mathfrak{p}}(x)\neq \mathrm{ord}_{\mathfrak{p}}(y)$时,

$$\mathrm{ord}_{\mathfrak{p}}(x+y)=\min\{\mathrm{ord}_{\mathfrak{p}}(x),\mathrm{ord}_{\mathfrak{p}}(y)\}.$$

证明: 因为$(x+y)A\subseteq xA+yA$, 由注记2.3(ii),

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}}(x+y)&=\mathrm{ord}_{\mathfrak{p}}\left((x+y)A\right)\\&\geq \mathrm{ord}_{\mathfrak{p}}\left(xA+yA\right)\\&=\min\{\mathrm{ord}_{\mathfrak{p}}(xA),\mathrm{ord}_{\mathfrak{p}}(yA)\}\\&=\min\{\mathrm{ord}_{\mathfrak{p}}(x),\mathrm{ord}_{\mathfrak{p}}(y)\}.\end{aligned}$$

当$\mathrm{ord}_{\mathfrak{p}}(x)\neq \mathrm{ord}_{\mathfrak{p}}(y)$时, 不妨设$\mathrm{ord}_{\mathfrak{p}}(x)<\mathrm{ord}_{\mathfrak{p}}(y)$. 则由上面的结果

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}}(x+y)\geq \mathrm{ord}_{\mathfrak{p}}(x)&=\mathrm{ord}_{\mathfrak{p}}(x+y-y)\\&\geq \min\{\mathrm{ord}_{\mathfrak{p}}(x+y),\mathrm{ord}_{\mathfrak{p}}(-y)\}\\&=\min\{\mathrm{ord}_{\mathfrak{p}}(x+y),\mathrm{ord}_{\mathfrak{p}}(y)\}\\&=\mathrm{ord}_{\mathfrak{p}}(x+y).\end{aligned}$$

因此$\mathrm{ord}_{\mathfrak{p}}(x+y)=\mathrm{ord}_{\mathfrak{p}}(x)$.

综上, 我们完成了证明. □

为了更好地利用地利用$\mathfrak{p}$-adic order来处理Dedekind环上的分式理想, 我们引入$\mathfrak{p}$-adic 赋值的定义(我们会在第七章详细地介绍赋值).

定义 2.3. *设A为Dedekind环, $\mathrm{frac}(A)=K$, $\mathfrak{p}$为非零素理想, $0<\lambda<1$为实数. 对任意的$\mathfrak{a}\in J(A)$, 定义分式理想$\mathfrak{a}$的$\mathfrak{p}$-adic范数为*

$$|\mathfrak{a}|_{\mathfrak{p}}:=\lambda^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})},$$

并补充定义零理想的$\mathfrak{p}$-adic范数$|0|_{\mathfrak{p}}=0$. 同时, 对任意$x\in K$, 定义元素x的$\mathfrak{p}$-adic范数为

$$|x|_{\mathfrak{p}}=|xA|_{\mathfrak{p}}.$$

由注记2.3容易得到下面的结论.

命题 2.2. 设A为*Dedekind*环, $\mathrm{frac}(A)=K$, $\mathfrak{p}$为非零素理想. 则下列结论成立.

(i) 对任意的$\mathfrak{a},\mathfrak{b}\in J(A)$,

$$|\mathfrak{ab}|_{\mathfrak{p}}=|\mathfrak{a}|_{\mathfrak{p}}|\mathfrak{b}|_{\mathfrak{p}},$$
$$|\mathfrak{a}+\mathfrak{b}|_{\mathfrak{p}}=\max\{|\mathfrak{a}|_{\mathfrak{p}},|\mathfrak{b}|_{\mathfrak{p}}\},$$
$$|\mathfrak{a}\cap\mathfrak{b}|_{\mathfrak{p}}=\min\{|\mathfrak{a}|_{\mathfrak{p}},|\mathfrak{b}|_{\mathfrak{p}}\}.$$

(ii) 对任意的$x,y\in K$,

$$|x+y|_{\mathfrak{p}}\leq\max\{|x|_{\mathfrak{p}},|y|_{\mathfrak{p}}\},$$

并且当$|x|_{\mathfrak{p}}\neq|y|_{\mathfrak{p}}$时, 我们有(称作*domination principle*)

$$|x+y|_{\mathfrak{p}}=\max\{|x|_{\mathfrak{p}},|y|_{\mathfrak{p}}\}.$$

2.2 Dedekind环上的强逼近定理

我们介绍Dedekind环上非常重要的强逼近定理.

定理 2.5. 设A为*Dedekind*环, $\mathrm{frac}(A)=K$, $\mathcal{T}$是由有限个A的非零素理想构成的集合. 对任意的$\mathfrak{p}\in\mathcal{T}$, 固定一个$a_{\mathfrak{p}}\in K$. 则对任意的$\varepsilon>0$, 存在$x\in K$使得

$$\begin{cases}|x-a_{\mathfrak{p}}|_{\mathfrak{p}}<\varepsilon & (\forall\mathfrak{p}\in\mathcal{T}),\\ |x|_{\mathfrak{p}}\leq 1 & (\forall\mathfrak{p}\notin\mathcal{T}).\end{cases}$$

证明: 不妨设$0<\varepsilon<1$. 首先, 在$\mathcal{T}$中增加有限个非零素理想, 将其扩大为$\mathcal{T}'$使得

$$|a_{\mathfrak{p}}|_{\mathfrak{q}}\leq 1\ (\forall\mathfrak{p}\in\mathcal{T},\forall\mathfrak{q}\notin\mathcal{T}').$$

并且对于任意的$\mathfrak{p}'\in\mathcal{T}'\setminus\mathcal{T}$, 补充定义$a_{\mathfrak{p}'}=0$.

对任意的$\mathfrak{p}\in\mathcal{T}'$与充分大的正整数$N$, 由中国剩余定理, 存在$b_{\mathfrak{p}}\in A$使得

$$\begin{cases}b_{\mathfrak{p}}\equiv 1\ (\mathrm{mod}\ \mathfrak{p}^N),\\ b_{\mathfrak{p}}\equiv 0\ (\mathrm{mod}\ \mathfrak{q}^N)\ (\forall\mathfrak{q}\in\mathcal{T}'\setminus\{\mathfrak{p}\}),\end{cases}$$

即$|b_{\mathfrak{p}}-1|_{\mathfrak{p}}$与$|b_{\mathfrak{p}}|_{\mathfrak{q}}$均充分小$(\forall\mathfrak{q}\in\mathcal{T}'\setminus\{\mathfrak{p}\})$. 令

$$x=\sum_{\mathfrak{p}\in\mathcal{T}'}a_{\mathfrak{p}}b_{\mathfrak{p}}.$$

则由$\mathcal{T}'$的构造以及$b_{\mathfrak{p}} \in A$ $(\forall \mathfrak{p} \in \mathcal{T}')$, 容易验证

$$|x|_{\mathfrak{q}} \leq 1 \ (\forall \mathfrak{q} \notin \mathcal{T}').$$

对任意的$\mathfrak{p} \in \mathcal{T}'$, 我们有

$$\begin{aligned} |x - a_{\mathfrak{p}}|_{\mathfrak{p}} &= \left| (b_{\mathfrak{p}} - 1)a_{\mathfrak{p}} + \sum_{\mathfrak{q} \in \mathcal{T}' \setminus \{\mathfrak{p}\}} a_{\mathfrak{q}} b_{\mathfrak{q}} \right|_{\mathfrak{p}} \\ &\leq \max\left\{ |(b_{\mathfrak{p}} - 1)a_{\mathfrak{p}}|_{\mathfrak{p}}, \max\left\{ |a_{\mathfrak{q}} b_{\mathfrak{q}}|_{\mathfrak{p}} : \ q \in \mathcal{T}' \setminus \{\mathfrak{p}\} \right\} \right\} \\ &< \varepsilon. \end{aligned}$$

并且注意到对任意的$\mathfrak{p} \in \mathcal{T}' \setminus \mathcal{T}$,

$$|x|_{\mathfrak{p}} = |x - a_{\mathfrak{p}}|_{\mathfrak{p}} < \varepsilon < 1.$$

综上, 我们完成了证明. □

利用强逼近定理, 我们可以得到下面两个结果.

命题 2.3. *设A为Dedekind环, $\mathrm{frac}(A) = K$. 则对任意的$\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in J(A)$, 存在$x, y \in K^{\times}$使得*

$$\mathfrak{c} = x\mathfrak{a} + y\mathfrak{b}.$$

证明: 取$y \in \mathfrak{c}\mathfrak{b}^{-1} \setminus \{0\}$. 令$\mathcal{T}$为有限个非零素理想构成的集合并满足条件

$$|y|_{\mathfrak{q}} = |\mathfrak{a}|_{\mathfrak{q}} = |\mathfrak{b}|_{\mathfrak{q}} = |\mathfrak{c}|_{\mathfrak{q}} = 1 \ (\forall \mathfrak{q} \notin \mathcal{T}).$$

对任意的$\mathfrak{p} \in \mathcal{T}$, 固定元素

$$a_{\mathfrak{p}} \in \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}^{-1}\mathfrak{c})} \setminus \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}^{-1}\mathfrak{c})+1}.$$

由定理2.5, 存在$x \in K$使得

$$\begin{cases} |x - a_{\mathfrak{p}}|_{\mathfrak{p}}\text{充分小} & (\forall \mathfrak{p} \in \mathcal{T}), \\ |x|_{\mathfrak{q}} \leq 1 & (\forall \mathfrak{q} \notin \mathcal{T}). \end{cases}$$

由命题2.2(ii),

$$|x|_{\mathfrak{p}} = |a_{\mathfrak{p}}|_{\mathfrak{p}} = |\mathfrak{a}^{-1}\mathfrak{c}|_{\mathfrak{p}} \ (\forall \mathfrak{p} \in \mathcal{T}).$$

注意到$|y\mathfrak{b}|_{\mathfrak{p}} \leq |\mathfrak{c}|_{\mathfrak{p}}$ $(\forall \mathfrak{p})$, 由上容易验证

$$|x\mathfrak{a} + y\mathfrak{b}|_{\mathfrak{p}} = \max\{|x\mathfrak{a}|_{\mathfrak{p}}, |y\mathfrak{b}|_{\mathfrak{p}}\} = \max\{|c|_{\mathfrak{p}}, |y\mathfrak{b}|_{\mathfrak{p}}\} = |\mathfrak{c}|_{\mathfrak{p}} \ (\forall \mathfrak{p} \in \mathcal{T}),$$

并且

$$|x\mathfrak{a}+y\mathfrak{b}|_{\mathfrak{q}}=\max\{|x\mathfrak{a}|_{\mathfrak{q}},|y\mathfrak{b}|_{\mathfrak{q}}\}=1=|\mathfrak{c}|_{\mathfrak{q}}\ (\forall\mathfrak{q}\notin\mathcal{T}).$$

因此, $x\mathfrak{a}+y\mathfrak{b}=\mathfrak{c}$.

综上, 我们完成了证明. □

下面的结果非常有用, 我们后面会经常使用它.

定理 2.6. *设A为Dedekind环. 若A仅有有限个非零素理想, 则A是主理想整环.*

证明: 如果Dedekind环A没有非零素理想, 则显然A为域. 此时结论成立. 下面假设A存在非零素理想, 并且设$\mathfrak{p}_1,\cdots,\mathfrak{p}_r$恰好为$A$的全部非零素理想. 对任意的$\mathfrak{a}\in J(A)$以及$1\leq i\leq r$, 固定元素$a_i\in\mathfrak{p}_i^{\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{a})}\setminus\mathfrak{p}_i^{\mathrm{ord}_{\mathfrak{p}_i}(\mathfrak{a})+1}$. 则由定理2.5, 存在$x\in\mathrm{frac}(A)$使得 $|x-a_i|_{\mathfrak{p}_i}$充分小($\forall 1\leq i\leq r$). 由命题2.2(ii), 上式说明$|x|_{\mathfrak{p}_i}=|\mathfrak{a}|_{\mathfrak{p}_i}$ ($\forall 1\leq i\leq r$). 因此, $\mathfrak{a}=xA$, 即A是主理想整环.

综上, 我们完成了证明. □

3 局部化与离散赋值环

3.1 分式化的定义与基本性质

我们这里仅讨论整环上的分式化. 首先给出乘法子集的定义.

定义 3.1. 设A为整环, $\emptyset \neq S \subseteq A$. 如果$S$满足

(i) $1 \in S$且$0 \notin S$;

(ii) 对任意的$x, y \in S$都有$xy \in S$,

则称S为A的一个乘法子集.

下面给出分式环的定义.

定义 3.2. 设A为整环, S为A的一个乘法子集. 则

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

在$\mathrm{frac}(A)$的运算下构成一个子环. 我们称其为分式环.

对于分式环, 我们有下面几个有用的结论.

命题 3.1. 设$A \subseteq B$为两个整环, $S \subseteq A$为乘法子集. 如果$\bar{A}$为A在B中的整闭包, 则$S^{-1}\bar{A}$为$S^{-1}A$在$S^{-1}B$中的整闭包.

证明: 对任意的$x/s \in S^{-1}\bar{A}$ $(x \in \bar{A}, s \in S)$, 因为$x \in \bar{A}$, 不妨设

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

其中$n \in \mathbb{Z}^+, a_0, a_1, \cdots, a_{n-1} \in A$. 上式两边同时乘以$\frac{1}{s^n}$得到

$$\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_1}{s^{n-1}}\left(\frac{x}{s}\right) + \frac{a_0}{s^n} = 0.$$

这说明x/s在$S^{-1}A$上整, 即$S^{-1}\bar{A}$包含在$S^{-1}A$在$S^{-1}B$中的整闭包中.

反过来, 设$y/t \in S^{-1}B$ $(y \in B, t \in S)$在$S^{-1}A$上整. 则存在$m \in \mathbb{Z}^+$, $s_0 \in S$以及$a_0', a_1', \cdots, a_{m-1}'$使得

$$\left(\frac{y}{t}\right)^m + \frac{a_{m-1}'}{s_0}\left(\frac{y}{t}\right)^{m-1} + \cdots + \frac{a_1'}{s_0}\left(\frac{y}{t}\right) + \frac{a_0'}{s_0} = 0.$$

上式两边同时乘以$(s_0 t)^m$得到

$$(s_0 y)^m + t a_{m-1}'(s_0 y)^{m-1} + \cdots + s_0^{m-2} t^{m-1} a_1'(s_0 y) + s_0^{m-1} t^m a_0' = 0.$$

这说明$s_0y \in \bar{A}$. 因此

$$\frac{y}{t} = \frac{s_0y}{s_0t} \in S^{-1}\bar{A},$$

即$S^{-1}A$在$S^{-1}B$中的整闭包包含在$S^{-1}\bar{A}$中.

综上, 我们证明了$S^{-1}A$在$S^{-1}B$中的整闭包恰好为$S^{-1}\bar{A}$. □

下面的命题说明分式环上的理想均为扩理想.

命题 3.2. *设A为整环, S为A的一个乘法子集. 则对$S^{-1}A$的任意理想$\tilde{\mathfrak{a}}$, 我们有*

$$\tilde{\mathfrak{a}} = S^{-1}(\tilde{\mathfrak{a}} \cap A).$$

证明: 首先显然$S^{-1}(\tilde{\mathfrak{a}} \cap A) \subseteq \tilde{\mathfrak{a}}$. 反过来, 对任意$x = \frac{y}{s} \in \tilde{\mathfrak{a}}$ $(y \in A, s \in S)$, 我们有$y = sx \in \tilde{\mathfrak{a}} \cap A$. 因此, $x \in S^{-1}(\tilde{\mathfrak{a}} \cap A)$, 即$\tilde{\mathfrak{a}} \subseteq S^{-1}(\tilde{\mathfrak{a}} \cap A)$.

综上, 我们证明了$\tilde{\mathfrak{a}} = S^{-1}(\tilde{\mathfrak{a}} \cap A)$. □

命题 3.3. *设A为整环, S为A的一个乘法子集,*

$$\Omega_1 = \{\mathfrak{p} : \mathfrak{p}\text{为}A\text{的素理想且}\mathfrak{p} \cap S = \emptyset\},$$
$$\Omega_2 = \left\{\tilde{\mathfrak{p}} : \tilde{\mathfrak{p}}\text{为}S^{-1}A\text{的素理想}\right\}.$$

则$\varphi : \mathfrak{p} \mapsto S^{-1}\mathfrak{p}$是$\Omega_1 \to \Omega_2$的一个双射, 并且$\varphi$的逆映射$\varphi^{-1}$为$\tilde{\mathfrak{p}} \mapsto \tilde{\mathfrak{p}} \cap A$.

证明: 我们先说明对任意的$\mathfrak{p} \in \Omega_1$, 扩理想$S^{-1}\mathfrak{p} \in \Omega_2$. 事实上, 因为$S \cap \mathfrak{p} = \emptyset$, 我们有$1 \notin S^{-1}\mathfrak{p}$, 即$S^{-1}\mathfrak{p} \neq S^{-1}A$. 设$x/s_1, y/s_2 \in S^{-1}A$ $(s_1, s_2 \in S, x, y \in A)$使得$\frac{x}{s_1} \cdot \frac{y}{s_2} \in S^{-1}\mathfrak{p}$. 则存在$s_3 \in S, p \in \mathfrak{p}$使得

$$\frac{x}{s_1} \cdot \frac{y}{s_2} = \frac{p}{s_3}.$$

这说明$s_3xy = ps_1s_2 \in \mathfrak{p}$. 注意到$s_3 \notin \mathfrak{p}$, 上式得到$x \in \mathfrak{p}$或者$y \in \mathfrak{p}$, 即$x/s_1 \in S^{-1}\mathfrak{p}$或者$y/s_2 \in S^{-1}\mathfrak{p}$. 综上, $S^{-1}\mathfrak{p} \in \Omega_2$.

另一方面, 对任意的$\tilde{\mathfrak{p}} \in \Omega_2$, 素理想$(\tilde{\mathfrak{p}} \cap A) \cap S = \emptyset$. 再由命题3.2,

$$\tilde{\mathfrak{p}} = S^{-1}\left(\tilde{\mathfrak{p}} \cap A\right).$$

这些说明$\varphi : \Omega_1 \to \Omega_2$是满射.

下面我们来说明φ为单射. 为此, 仅需说明对任意的$\mathfrak{p} \in \Omega_1$都有

$$S^{-1}\mathfrak{p} \cap A = \mathfrak{p}.$$

首先显然$\mathfrak{p} \subseteq S^{-1}\mathfrak{p} \cap A$. 反过来, 对任意的$x = \frac{z}{s} \in S^{-1}\mathfrak{p} \cap A$ ($s \in S, z \in \mathfrak{p}$), 由$sx = z \in \mathfrak{p}$以及$s \notin \mathfrak{p}$, 我们得到$x \in \mathfrak{p}$, 即$S^{-1}\mathfrak{p} \cap A \subseteq \mathfrak{p}$. 这些说明$S^{-1}\mathfrak{p} \cap A = \mathfrak{p}$.

综上, 我们完成了证明. □

下面我们给出局部化的定义.

定义 3.3. *设A为整环, X为A上一些素理想构成的非空集合. 则容易验证*

$$S = A \setminus \bigcup_{\mathfrak{p} \in X} \mathfrak{p}$$

为A的乘法子集. 定义

$$A(X) := S^{-1}A = \left\{ \frac{f}{g} : \ f, g \in A \text{且} g \not\equiv 0 \pmod{\mathfrak{p}} \ \forall \mathfrak{p} \in X \right\}.$$

特别地, 当$X = \{\mathfrak{p}\}$时, 定义

$$A_{\mathfrak{p}} := \left\{ \frac{x}{s} : \ s, x \in A \text{且} s \not\equiv 0 \pmod{\mathfrak{p}} \right\}.$$

我们将其称作A在素理想$\mathfrak{p}$处的局部化.

局部化是研究Dedekind环的重要方法. 我们先介绍如下结果.

命题 3.4. *设A为Dedekind环, S为A的乘法子集. 则$S^{-1}A$也为Dedekind环. 特别地, A在每个非零素理想$\mathfrak{p}$处的局部化$A_{\mathfrak{p}}$为Dedekind环.*

证明: 由命题3.2, 分式环$S^{-1}A$的理想$\tilde{\mathfrak{a}}$均为扩理想$S^{-1}(\tilde{\mathfrak{a}} \cap A)$. 因为$A$为诺特环, A的理想$(\tilde{\mathfrak{a}} \cap A)$是有限生成$A$模. 由此$\tilde{\mathfrak{a}} = S^{-1}(\tilde{\mathfrak{a}} \cap A)$是有限生成$S^{-1}A$模. 这说明$S^{-1}A$是诺特环.

设$\mathrm{frac}(A) = K$. 因为A整闭, A在K中的整闭包$\bar{A} = A$. 由命题3.1, 分式环$S^{-1}A$在K中的整闭包为$S^{-1}\bar{A} = S^{-1}A$, 即$S^{-1}A$为整闭整环.

最后, 由命题3.3, 分式环$S^{-1}A$的非零素理想均形如$S^{-1}\mathfrak{p}$, 并且

$$S^{-1}\mathfrak{p} \cap A = \mathfrak{p},$$

其中$\mathfrak{p}$为A中与S不交的素理想. 由此以及注意到A的非零素理想均为极大理想, 我们得到$S^{-1}A$的非零素理想也均为极大理想.

综上, 我们证明了$S^{-1}A$为Dedekind环. □

注记 3.1. 设A为*Dedekind*环, $\mathfrak{a}$为A的一个分式理想. 则由第二章的内容, 要研究$\mathfrak{a}$的素理想分解, 仅需弄清楚$\mathfrak{a}$在每个非零素理想$\mathfrak{p}$处的$\mathfrak{p}$-*adic order*.

局部化是处理该问题的有效方法. 事实上, 由命题*3.4*, 我们知道分式环$A_{\mathfrak{p}}$是*Dedekind*环. 由命题*3.3*, 扩理想$\mathfrak{p}A_{\mathfrak{p}}$是*Dedekind*环$A_{\mathfrak{p}}$唯一的非零素理想. 因此由定理*2.6*, 分式环$A_{\mathfrak{p}}$为主理想整环. 设$\pi_{\mathfrak{p}}$为$A_{\mathfrak{p}}$的一个素元, 即$\pi_{\mathfrak{p}}A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$.

对A的任意一个不等于$\mathfrak{p}$的非零素理想$\mathfrak{q}$, 显然有$\mathfrak{p} + \mathfrak{q} = A$. 因此存在$p \in \mathfrak{p}, q \in \mathfrak{q}$使得$p + q = 1$(注意此时$q = 1 - p \in A \setminus \mathfrak{p}$). 由此, 对任意的$n \in \mathbb{Z}_{\geq 0}$,

$$1 = q^n \cdot \frac{1}{q^n} \in \mathfrak{q}^n A_{\mathfrak{p}},$$

以及

$$1 = q^{-n} \cdot \frac{q^n}{1} \in \mathfrak{q}^{-n} A_{\mathfrak{p}}.$$

这说明$\mathfrak{q}^m A_{\mathfrak{p}} = A_{\mathfrak{p}}$ $(\forall m \in \mathbb{Z})$. 因此,

$$\mathfrak{a}A_{\mathfrak{p}} = \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})} A_{\mathfrak{p}} = (\mathfrak{p}A_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})} = \pi_{\mathfrak{p}}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})} A_{\mathfrak{p}}.$$

这样不仅去掉了其它的素理想, 而且把问题转换到了结构简单的环$A_{\mathfrak{p}}$上(我们下一节会看到, $A_{\mathfrak{p}}$其实是一个离散赋值环).

我们以下面的定理来结束本节.

定理 3.1. 设A为整环, $\mathfrak{p}$为A的非零素理想. 则有嵌入

$$A/\mathfrak{p} \hookrightarrow A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}.$$

更进一步, 如果$\mathfrak{p}$还是A的极大理想, 则对任意的$n \in \mathbb{Z}^+$, 我们有环同构

$$A/\mathfrak{p}^n \cong A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}.$$

证明: 由命题3.3, $\mathfrak{p}A_{\mathfrak{p}} \cap A = \mathfrak{p}$. 由此显然有嵌入

$$A/\mathfrak{p} \hookrightarrow A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}.$$

进一步假设$\mathfrak{p}$为极大理想. 对任意的$s \in A \setminus \mathfrak{p}$, 我们断言理想

$$sA + \mathfrak{p}^n = A. \tag{3.1}$$

事实上, 假设$sA+\mathfrak{p}^n \subsetneq A$. 则存在素理想$\mathfrak{q}$使得$sA+\mathfrak{p}^n \subseteq \mathfrak{q}$. 这得到$\mathfrak{p}^n \subseteq \mathfrak{q}$. 因此$\mathfrak{p} \subseteq \mathfrak{q}$. 注意到$\mathfrak{p}$为极大理想, 我们有$\mathfrak{q}=\mathfrak{p}$. 这与$s \notin \mathfrak{p}$矛盾. 因此, 上述断言成立.

先说明同态$x \mapsto x \bmod \mathfrak{p}^n A_{\mathfrak{p}}$是$A \to A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}$的满同态. 对任意的$x/s \in A_{\mathfrak{p}}$ $(x \in A, s \in S)$, 由(3.1)存在$a \in A$以及$y \in \mathfrak{p}^n$使得

$$sa+y=1.$$

这得到

$$\frac{1}{s} \equiv a \ (\mathrm{mod}\ \mathfrak{p}^n A_{\mathfrak{p}}).$$

因此$x/s \equiv ax \ (\mathrm{mod}\ \mathfrak{p}^n A_{\mathfrak{p}})$. 这说明上述同态为满同态.

下面来说明这个满同态的核为$\mathfrak{p}^n$. 也就是说要说明$\mathfrak{p}^n A_{\mathfrak{p}} \cap A = \mathfrak{p}^n$. 显然$\mathfrak{p}^n \subseteq \mathfrak{p}^n A_{\mathfrak{p}}$. 反过来, 对任意的$u=\frac{z}{t} \in \mathfrak{p}^n A_{\mathfrak{p}} \cap A$ $(z \in \mathfrak{p}^n, t \in S)$, 再由(3.1), 存在$v \in A, w \in \mathfrak{p}^n$使得

$$tv+w=1.$$

因此

$$u=utv+uw=zv+uw \in \mathfrak{p}^n.$$

这说明$\mathfrak{p}^n A_{\mathfrak{p}} \cap A \subseteq \mathfrak{p}^n$. 因此该满同态的核恰好为$\mathfrak{p}^n$. 则由同构定理我们得到

$$A/\mathfrak{p}^n \cong A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}}.$$

综上, 我们完成了证明. □

3.2 离散赋值环

这一节我们将介绍离散赋值环. 首先我们给出赋值环的定义.

定义 3.4. *设A为整环, $\mathrm{frac}(A)=K$. 如果对任意的$x \in K^\times$都有$x \in A$或者$1/x \in A$, 则称A为一个赋值环.*

赋值环有如下性质.

命题 3.5. *设A为赋值环. 则A整闭. 同时, A为局部环, 并且*

$$\mathfrak{m}=\{x \in A:\ x=0\text{或者}1/x \notin A\}$$

为A唯一的极大理想.

证明: 设$\mathrm{frac}(A)=K$. 使用反证法来说明A整闭. 假设存在$x\in K^\times\setminus A$使得x在A上整. 不妨设x满足

$$x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0,$$

其中$n\in\mathbb{Z}^+,a_0,\cdots,a_{n-1}\in A$. 由赋值环的定义, 此时$1/x\in A$. 在上式两边同时乘以$(1/x)^{n-1}$得到

$$x=-\left(a_{n-1}+\cdots+a_1\left(\frac{1}{x}\right)^{n-2}+a_0\left(\frac{1}{x}\right)^{n-1}\right)\in A.$$

这与$x\notin A$矛盾. 因此A整闭.

下面来说明A为局部环. 此时仅需说明$\mathfrak{m}$为A模. 也就是要说明, 对任意的$x,y\in\mathfrak{m}$以及任意的$r\in A$, 都有$x+y\in\mathfrak{m}$与$rx\in\mathfrak{m}$. 我们继续使用反证法. 假设存在$u,v\in\mathfrak{m}$使得$u+v\notin\mathfrak{m}$. 则$u,v\neq0$且$u+v\in A^\times$. 由此得到

$$\begin{cases}\frac{v}{u} &=\frac{1}{u}(u+v)-1\notin A,\\ \frac{u}{v} &=\frac{1}{v}(u+v)-1\notin A.\end{cases}$$

这与赋值环的定义矛盾. 再假设存在$w\in\mathfrak{m}$以及$a\in A$使得$aw\notin\mathfrak{m}$. 则$a\neq0,w\neq0$且$aw\in A^\times$. 由此得到

$$\frac{1}{w}=a\left(\frac{1}{aw}\right)\in A.$$

这与$w\in\mathfrak{m}$矛盾. 上面的讨论说明$\mathfrak{m}$为A模. 因此A为局部环且$\mathfrak{m}$为其唯一的极大理想.

综上, 我们完成了证明. □

下面我们给出离散赋值环的定义.

定义 3.5. *设A为整环. 如果A为主理想整环且仅有唯一的非零极大理想, 则称A为一个离散赋值环. 我们常用*dvr*来表示离散赋值环.*

注记 3.2. *容易说明离散赋值环是一个赋值环. 事实上, 设$\pi\in A$为A的一个素元. 则显然$\mathfrak{m}=\pi A$为离散赋值环A唯一的极大理想. 并且对任意的$x\in\mathrm{frac}(A)^\times$, 存在唯一的$r\in\mathbb{Z}$以及$\varepsilon\in A^\times$使得*

$$x=\pi^r\cdot\varepsilon.$$

另一方面由Dedekind环的定义, A显然是一个Dedekind环, $r=\mathrm{ord}_{\mathfrak{m}}(x)$并且

$$A=\{x\in\mathrm{frac}(A):\ \mathrm{ord}_{\mathfrak{m}}(x)\geq0\},$$

这里我们认为$\mathrm{ord}_{\mathfrak{m}}(0)=+\infty>0$. 由上面的讨论容易得到$A$是一个赋值环.

下面的结果说明, 除域以外, 离散赋值环是结构最简单的整环.

命题 3.6. 设A为离散赋值环, $\mathrm{frac}(A)=K$, $B\subseteq K$为交换幺环. 如果$A\subsetneq B\subseteq K$, 则$B=K$.

证明: 设$\mathfrak{m}$为A唯一的极大理想. 因为$A\subsetneq B$, 存在$b_0\in B\setminus A$. 由注记3.2, 我们得到$\mathrm{ord}_{\mathfrak{m}}(1/b_0)=r_0\in\mathbb{Z}^+$. 因此对任意的$x\in K$, 存在充分大的正整数$N$使得

$$\mathrm{ord}_{\mathfrak{m}}\left(\left(\frac{1}{b_0}\right)^N x\right)>0,$$

即(由注记3.2)

$$\left(\frac{1}{b_0}\right)^N x\in A.$$

这说明$x\in b_0^N\cdot A\subseteq B$. 因此$K=B$.

综上, 我们完成了证明. □

利用定理2.6, 我们容易得到下面的结果.

命题 3.7. 设A为整环. 则A为离散赋值环当且仅当A为整闭的诺特环且A有唯一的非零极大理想.

下面我们的定理说明Dedekind环在非零素理想处的局部化为离散赋值环.

定理 3.2. 设A为诺特整环. 则A为*Dedekind*环当且仅当A在每个非零素理想$\mathfrak{p}$处的局部化$A_{\mathfrak{p}}$为离散赋值环.

证明: "⇒". 由注记3.1, 结论显然成立.

"⇐". 假设A在每个非零素理想$\mathfrak{p}$处的局部化$A_{\mathfrak{p}}$为离散赋值环. 我们首先证明

$$A=\bigcap_{\mathfrak{p}}A_{\mathfrak{p}}. \tag{3.2}$$

左边包含于右边是显然的. 反过来, 对任意的$x\in\cap_{\mathfrak{p}}A_{\mathfrak{p}}$, 设

$$I_x=\{a\in A:\ ax\in A\}.$$

则显然I_x为A的理想, 并且对任意的非零素理想$\mathfrak{p}$, 存在$s\in A\setminus\mathfrak{p}$使得$sx\in A$, 即$I_x\not\subseteq\mathfrak{p}$ $(\forall\mathfrak{p})$. 因此$I_x=A$. 这说明$x=1x\in A$. 由上面的讨论, (3.2)成立.

下面说明A为Dedekind环. 为此仅需说明A整闭以及A的非零素理想$\mathfrak{p}$均为极大理想. 先说明A整闭. 设$x \in \mathrm{frac}(A)$且x在A上整. 则x也在$A_\mathfrak{p}$上整$(\forall \mathfrak{p})$. 因为$A_\mathfrak{p}$整闭, 由(3.2)我们得到

$$x \in \bigcap_\mathfrak{p} A_\mathfrak{p} = A.$$

因此A整闭. 下面说明A的非零素理想均为极大理想. 使用反证法. 假设存在非零素理想$\mathfrak{p}$使得$\mathfrak{p} \subsetneq \mathfrak{m}$, 其中$\mathfrak{m}$为$A$的极大理想. 则由命题3.3, $\mathfrak{p}A_\mathfrak{m} \subsetneq \mathfrak{m}A_\mathfrak{m}$为主理想整环$A_\mathfrak{m}$上的两个非零素理想, 这与主理想整环上的非零素理想均为极大理想的性质矛盾. 因此, A的非零素理想均为极大理想. 上面的讨论说明A为Dedekind环.

综上, 我们完成了证明. □

注记 3.3. *证明的核心是等式(3.2). 利用类似的方法, 对Dedekind环A的任意分式理想$\mathfrak{a}$, 我们可以得到*

$$\mathfrak{a} = \bigcap_\mathfrak{p} \mathfrak{a}A_\mathfrak{p}.$$

4 Dedekind环上素理想的扩理想

4.1 分歧指数与惯性次数

我们首先从下面的定理出发.

定理 4.1. *设A为Dedekind环, $\mathrm{frac}(A)=K$, L/K为域的有限可分扩张. 则A在域L中的整闭包B也是Dedekind环.*

证明: 由命题1.1, 可以设$b_1,b_2,\cdots,b_n\in B$为L/K的一组基. 令d为这组基的判别式. 则由引理1.3与命题1.4,

$$B\subseteq A\frac{b_1}{d}+A\frac{b_2}{d}+\cdots+A\frac{b_n}{d}.$$

这说明B的每个理想都是一个有限生成诺特A模的子模. 由有限生成诺特模的子模的性质, B的理想均为有限生成A模, 那自然也为有限生成B模. 因此B为诺特环.

下面来说明B的任意非零素理想$\mathfrak{P}$为极大理想. 事实上, 利用与定理2.1的证明中类似的方法可以说明$\mathfrak{P}\cap A=\mathfrak{p}$为$A$的一个非零素理想. 注意到$A/\mathfrak{p}\hookrightarrow B/\mathfrak{P}$且$B/\mathfrak{P}$在$A/\mathfrak{p}$上整. 由引理2.1, 我们得到$B/\mathfrak{P}$为域. 因此$\mathfrak{P}$为极大理想.

而由B的定义, B整闭.

综上, 我们证明了B为Dedekind环. □

注记 4.1. *事实上, 这个定理中的条件可以减弱许多. 我们不加证明地给出经典的Akizuki-Krull定理.*

定理 4.2. *设A为整环且A的每个非零素理想均为极大理想, $\mathrm{frac}(A)=K$, L/K为域的有限扩张. 则A在L中的整闭包B是Dedekind环.*

设A为Dedekind环, $\mathrm{frac}(A)=K$, L/K为域的有限可分扩张, B为A在L中的整闭包. 这一节的主要任务是研究A的非零素理想$\mathfrak{p}$在B上的扩理想$\mathfrak{p}B$. 为此, 我们首先介绍经典的中山引理(the Nakayama Lemma).

引理 4.1. *设A为局部环, $\mathfrak{m}$为其唯一的非零极大理想, M为有限生成A模. 如果$\mathfrak{m}M=M$, 则$M=0$.*

证明: 因为M为有限生成A模, 集合

$$\left\{k\in\mathbb{Z}^+:\ \text{存在}x_1,\cdots,x_k\text{使得}M=Ax_1+\cdots+Ax_k\right\}$$

不为空集. 设r为该集合中最小的元素, 并且设

$$M = Ay_1 + \cdots + Ay_r.$$

如果$r = 1$, 则存在$m_1 \in \mathfrak{m}$使得$y_1 = m_1 y_1$. 因为A为局部环, $(1 - m_1) \in A^\times$. 因此由$y_1 = m_1 y_1$可以得到$y_1 = 0$, 即$M = 0$. 如果$r \geq 2$, 则存在$t_1, \cdots, t_r \in \mathfrak{m}$使得

$$x_1 = t_1 x_1 + t_2 x_2 + \cdots + t_r x_r.$$

注意到$(1 - t_1) \in A^\times$, 由上式我们得到$x_1 \in Ax_2 + \cdots + Ax_r$. 因此

$$M = Ax_2 + \cdots + Ax_r.$$

这与r的最小性矛盾. 由上面的讨论, 我们得到$r = 1$并且因此$M = 0$.

综上, 我们完成了证明. □

利用中山引理, 我们可以得到下面的结果.

引理 4.2. *设A为Dedekind环, $\mathrm{frac}(A) = K$, L/K为域的有限可分扩张, B为A在域L中的整闭包. 对A的任意非零素理想$\mathfrak{p}$, 我们有$\mathfrak{p}B \neq B$.*

证明: 设$S = A \setminus \mathfrak{p}$, $A_\mathfrak{p}$为A在$\mathfrak{p}$处的局部化, $B_\mathfrak{p} := S^{-1}B$为分式环. 使用反证法. 假设$\mathfrak{p}B = B$. 则由命题3.2, 我们得到

$$B_\mathfrak{p} = S^{-1}B = S^{-1}(\mathfrak{p}B) = S^{-1}\mathfrak{p}S^{-1}B = \mathfrak{p}A_\mathfrak{p}B_\mathfrak{p}. \tag{4.1}$$

由定理3.2我们知道$A_\mathfrak{p}$为离散赋值环. 由命题3.1, $A_\mathfrak{p}$在L中的整闭包恰好为$B_\mathfrak{p}$. 因此, 由定理1.2, 我们得到$B_\mathfrak{p}$为有限生成$A_\mathfrak{p}$模. 将这些与(4.1)以及引理4.1结合起来, 我们得到$B_\mathfrak{p} = 0$. 这显然矛盾.

综上, 我们证明了$\mathfrak{p}B \neq B$. □

由引理4.2与定理4.1, 我们知道对A的任意非零素理想$\mathfrak{p}$, 扩理想$\mathfrak{p}B$可以分解为Dedekind环B上一些素理想的乘积. 我们给出如下定义.

定义 4.1. *设A为Dedekind环, $\mathrm{frac}(A) = K$, L/K为域的有限可分扩张, B为A在域L中的整闭包. 对A的任意非零素理想$\mathfrak{p}$, 设*

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r}$$

为$\mathfrak{p}B$在Dedekind环B上的素理想分解, 其中$\mathfrak{P}_1, \cdots, \mathfrak{P}_r$为$B$的两两不同的非零素理想, $e_1, \cdots, e_r \in \mathbb{Z}^+$. 将$e_i$称作$\mathfrak{P}_i$在$\mathfrak{p}$上的分歧指数(ramification index),

并记作$e(\mathfrak{P}_i|\mathfrak{p})$. 将剩余类域的扩张次数$[B/\mathfrak{P}_i : A/\mathfrak{p}]$称作$\mathfrak{P}_i$在$\mathfrak{p}$上惯性次数inertia degree, 并记作$f(\mathfrak{P}_i|\mathfrak{p})$.

关于分歧指数与惯性次数, 我们有如下结果.

定理 4.3. 记号如上. 则

$$\sum_{i=1}^{r} e\left(\mathfrak{P}_i|\mathfrak{p}\right) \cdot f\left(\mathfrak{P}_i|\mathfrak{p}\right) = [L:K].$$

证明: 利用Dedekind环上B上的$\mathfrak{P}$-adic order, 对任意的$1 \leq i \neq j \leq r$以及B的任意非零素理想$\mathfrak{P}$, 容易得到

$$\mathrm{ord}_{\mathfrak{P}}\left(\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j}\right) = \min\left\{\mathrm{ord}_{\mathfrak{P}}\left(\mathfrak{P}_i^{e_i}\right), \mathrm{ord}_{\mathfrak{P}}\left(\mathfrak{P}_j^{e_j}\right)\right\} = 0,$$

即$P_i^{e_i} + \mathfrak{P}_j^{e_j} = B$. 这说明这些$\mathfrak{P}_i^{e_i}$两两互素. 因此, 由中国剩余定理,

$$B/\mathfrak{p}B \cong \bigoplus_{1\leq i\leq r} B/\mathfrak{P}_i^{e_i}. \tag{4.2}$$

注意到上式两边均为$A/\mathfrak{p}$模. 为了证明定理, 我们仅需说明

$$\dim_{A/\mathfrak{p}}\left(B/\mathfrak{p}B\right) = [L:K], \tag{4.3}$$

以及

$$\dim_{A/\mathfrak{p}}\left(B/\mathfrak{P}_i^{e_i}\right) = e\left(\mathfrak{P}_i|\mathfrak{p}\right) \cdot f\left(\mathfrak{P}_i|\mathfrak{p}\right). \tag{4.4}$$

我们采用局部化的方法来证明(4.3). 为此, 先证明如下的$A/\mathfrak{p}$模同构

$$B/\mathfrak{p}B \cong B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}. \tag{4.5}$$

考虑$B \to B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$的同态$h : b \mapsto b \bmod \mathfrak{p}B_{\mathfrak{p}}$. 先说明$h$为满同态. 对任意的$b/s \in B_{\mathfrak{p}}$ $(b \in B, s \in S = A \setminus \mathfrak{p})$, 容易验证

$$sA + \mathfrak{p} = A.$$

因此$sB + \mathfrak{p}B = B$. 由此存在$x \in B, u \in \mathfrak{p}B$使得$sx + u = 1$. 这说明

$$\frac{b}{s} \equiv xb \ (\mathrm{mod}\ \mathfrak{p}B_{\mathfrak{p}}).$$

因此h为满同态.

下面考虑$\ker h$. 显然$\ker h = \mathfrak{p}B_{\mathfrak{p}} \cap B$. 我们断言$\ker h = \mathfrak{p}B_{\mathfrak{p}} \cap B = \mathfrak{p}B$. 显然$\mathfrak{p}B \subseteq \mathfrak{p}B_{\mathfrak{p}} \cap B$. 反过来, 对任意的$y = z/t \in \mathfrak{p}B_{\mathfrak{p}} \cap B$ ($z \in \mathfrak{p}B, t \in S$), 利用和上面类似的办法容易得到

$$tB + \mathfrak{p}B = B.$$

因此, 存在$v \in B, w \in \mathfrak{p}B$使得

$$tv + w = 1.$$

由此, $y = ytv + yw = zv + yw \in \mathfrak{p}B$, 即$\mathfrak{p}B_{\mathfrak{p}} \cap B \subseteq \mathfrak{p}B$. 由上面的讨论, 我们得到$\ker h = \mathfrak{p}B$. 综上, 同构(4.5)成立. 再由定理3.1, 我们有$A/\mathfrak{p} \cong A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. 因此,

$$\dim_{A/\mathfrak{p}} (B/\mathfrak{p}B) = \dim_{A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}} (B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}).$$

由定理3.2, $A_{\mathfrak{p}}$为离散赋值环. 由命题3.1, $A_{\mathfrak{p}}$在L中的整闭包恰好为$B_{\mathfrak{p}}$. 由这些与定理1.2, $B_{\mathfrak{p}}$关于$A_{\mathfrak{p}}$的整基是存在的, 不妨设为$\omega_1, \cdots, \omega_n$, 其中$n = [L : K]$. 设$\bar{\omega}_i = \omega_i \bmod \mathfrak{p}B_{\mathfrak{p}}$. 对任意的$x \in A_{\mathfrak{p}}$, 设$\bar{x} = x \bmod \mathfrak{p}A_{\mathfrak{p}}$. 则对任意的$x_1, \cdots, x_n \in A_{\mathfrak{p}}$, 如果

$$\sum_{1 \leq i \leq n} \bar{x}_i \bar{\omega}_i = 0,$$

则

$$\sum_{1 \leq i \leq n} x_i \omega_i \equiv 0 \ (\mathrm{mod}\ \mathfrak{p}B_{\mathfrak{p}}).$$

因为这些ω_i为整基, 我们得到$x_i \in \mathfrak{p}A_{\mathfrak{p}}$ ($\forall 1 \leq i \leq n$), 即$\bar{x}_i = 0$ ($\forall 1 \leq i \leq n$). 注意到这些$\bar{\omega}_i$可以$A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$线性表示$B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$中的任意元素. 由上面的讨论, $\bar{\omega}_1, \cdots, \bar{\omega}_n$恰好为$B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$的一组$(A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})$-基. 因此,

$$\dim_{A/\mathfrak{p}} (B/\mathfrak{p}B) = \dim_{A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}} (B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}) = [L : K],$$

即(4.3)成立.

下面考虑(4.4). 首先, 对任意的$m \in \mathbb{Z}_{\geq 0}$, 容易得到正合列

$$0 \to \mathfrak{P}_i^m/\mathfrak{P}_i^{m+1} \to B/\mathfrak{P}_i^{m+1} \to B/\mathfrak{P}_i^m \to 0, \tag{4.6}$$

其中我们定义$\mathfrak{P}_i^0 = B$. 另一方面, 对任意的$m \in \mathbb{Z}_{\geq 0}$, 我们断言有如下的$A/\mathfrak{p}$模同构

$$B/\mathfrak{P}_i \cong \mathfrak{P}_i^m/\mathfrak{P}_i^{m+1}. \tag{4.7}$$

事实上, 取$x_m \in \mathfrak{P}_i^m \setminus \mathfrak{P}_i^{m+1}$. 考虑理想$x_m B + \mathfrak{P}_i^{m+1}$. 对$B$的任意非零素理想$\mathfrak{P}$, 容易验证

$$\mathrm{ord}_{\mathfrak{P}}\left(x_m B + \mathfrak{P}_i^{m+1}\right) = \begin{cases} 0 & \text{如果 } \mathfrak{P} \neq \mathfrak{P}_i, \\ m & \text{如果 } \mathfrak{P} = \mathfrak{P}_i. \end{cases}$$

因此$x_m B + \mathfrak{P}_i^{m+1} = \mathfrak{P}_i^m$. 由此, 同态$b \mapsto bx_m \bmod \mathfrak{P}_i^{m+1}$是$B \to \mathfrak{P}_i^m/\mathfrak{P}_i^{m+1}$的满同态. 并且该满同态的核显然为$\mathfrak{P}_i$. 综上, 同构(4.7)成立. 将(4.6)与(4.7)结合起来, 我们得到正合列

$$0 \to B/\mathfrak{P}_i \to B/\mathfrak{P}_i^{m+1} \to B/\mathfrak{P}_i^m \to 0.$$

因此

$$\dim_{A/\mathfrak{p}}\left(B/\mathfrak{P}_i^{m+1}\right) - \dim_{A/\mathfrak{p}}\left(B/\mathfrak{P}_i^m\right) = \dim_{A/\mathfrak{p}}\left(B/\mathfrak{P}_i\right).$$

由此我们得到

$$\dim_{A/\mathfrak{p}}\left(B/\mathfrak{P}_i^{e_i}\right) = e_i \cdot \dim_{A/\mathfrak{p}}\left(B/\mathfrak{P}_i\right) = e\left(\mathfrak{P}_i|\mathfrak{p}\right) \cdot f\left(\mathfrak{P}_i|\mathfrak{p}\right),$$

即(4.4)成立.

最后, 由(4.2), (4.3)与(4.4), 我们得到

$$\sum_{i=1}^{r} e\left(\mathfrak{P}_i|\mathfrak{p}\right) \cdot f\left(\mathfrak{P}_i|\mathfrak{p}\right) = [L:K].$$

综上, 我们完成了证明. □

4.2 Kummer分解定理

设A为Dedekind环, $\mathrm{frac}(A) = K$, L/K为域的有限可分扩张, B为A在域L中的整闭包. 因为L/K为域的有限可分扩张并且$L = \{b/a : b \in B, a \in A \setminus \{0\}\}$ (命题1.1), 存在$\theta \in B$使得$L = K(\theta)$. 显然此时$A[\theta] \subseteq B$.

我们首先给出如下定义.

定义 4.2. *记号如上. 称B模*

$$\mathcal{F} := \{x \in B : \ xB \subseteq A[\theta]\}$$

为$A[\theta]$在B中的导子.

注记 4.2. (i) 对任意的$x \in \mathcal{F}$, 我们有$x \cdot 1 \in xB \subseteq A[\theta]$. 因此$\mathcal{F} \subseteq A[\theta]$.

(ii) 如果设$[L : K] = n$, 则$1, \theta, \cdots, \theta^{n-1} \in B$为$L/K$的一组基. 此时这组基的判别式$d = d(1, \theta, \cdots, \theta^{n-1}) \in A \setminus \{0\}$, 并且由引理*1.3*, 我们有$dB \subseteq A[\theta]$. 这说明$\mathcal{F}$是非零理想.

为了方便, 对任意的$f(t) \in A[t]$以及A的任意非零素理想$\mathfrak{p}$, 定义$\bar{f}(t) = f(t) \bmod \mathfrak{p}A[t] \in (A/\mathfrak{p})[t]$.

下面我们给出经典的Kummer分解定理.

定理 4.4. 记号如上. 设$p_\theta(t) \in A[t]$为θ在K上的极小多项式, $\mathfrak{p}$为A的非零素理想且$\mathfrak{p}A[\theta]$与$\mathcal{F}$在$A[\theta]$中互素. 如果$\overline{p_\theta}(t)$在$(A/\mathfrak{p})[t]$中的分解式为

$$\overline{p_\theta}(t) = \overline{p_1}(t)^{e_1}\overline{p_2}(t)^{e_2}\cdots\overline{p_r}(t)^{e_r},$$

其中这些$p_i(t) \in A[t]$均为首一多项式, 这些$\overline{p_i}(t)$均为$(A/\mathfrak{p})[t]$中两两不同的不可约多项式并且$e_1, \cdots, e_r \in \mathbb{Z}^+$, 则

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r},$$

其中这些

$$\mathfrak{P}_i = \mathfrak{p}B + p_i(\theta)B$$

为B上两两不同的素理想, 并且

$$e\left(\mathfrak{P}_i|\mathfrak{p}\right) = e_i,\ f\left(\mathfrak{P}_i|\mathfrak{p}\right) = \deg(p_i(t)).$$

证明: 设$\kappa = A/\mathfrak{p}$. 我们首先证明如下的同构.

$$\kappa[t]/\overline{p_\theta}(t)\kappa[t] \underset{h_1}{\cong} A[\theta]/\mathfrak{p}A[\theta] \underset{h_2}{\cong} B/\mathfrak{p}B, \tag{4.8}$$

其中

$$h_1 : \overline{g}(t) \bmod \overline{p_\theta}(t)\kappa[t] \mapsto g(\theta) \bmod \mathfrak{p}A[\theta],$$
$$h_2 : g(\theta) \bmod \mathfrak{p}A[\theta] \mapsto g(\theta) \bmod \mathfrak{p}B.$$

容易验证$\overline{h_1}, \overline{h_2}$的定义是合理的.

考虑$\kappa[t]\to A[\theta]/\mathfrak{p}A[\theta]$的同态$h_1:\overline{g}(t)\mapsto g(\theta)\bmod \mathfrak{p}A[\theta]$. 容易验证$h_1$的定义是合理的, 并且$h_1$是满同态. 另一方面,

$$\begin{aligned}\mathrm{Ker}h_1&=\{\overline{g}(t)\in\kappa[t]:\ g(\theta)\equiv 0\ (\mathrm{mod}\ \mathfrak{p}A[\theta])\}\\&=\{\overline{g}(t)\in\kappa[t]:\ \text{存在}u(t)\in\mathfrak{p}A[t]\text{使得}g(\theta)=u(\theta)\}\\&=\{\overline{g}(t)\in\kappa[t]:\ \text{存在}u(t)\in\mathfrak{p}A[t]\text{使得}g(t)\equiv u(t)\ (\mathrm{mod}\ p_\theta(t)A[t])\}\\&=\{\overline{g}(t)\in\kappa[t]:\ \overline{g}(t)\equiv 0\ (\mathrm{mod}\ \overline{p_\theta}(t)\kappa[t])\}\\&=\overline{p_\theta}(t)\kappa[t].\end{aligned}$$

由上面的讨论, 我们得到

$$\kappa[t]/\overline{p_\theta}(t)\kappa[t]\underset{\overline{h_1}}{\cong}A[\theta]/\mathfrak{p}A[\theta].$$

考虑$A[\theta]\to B/\mathfrak{p}B$的同态$h_2:\ g(\theta)\mapsto g(\theta)\bmod\mathfrak{p}B$. 因为$\mathfrak{p}A[\theta]$与$\mathcal{F}$在$A[\theta]$中互素, 由$\mathcal{F}$的定义我们得到

$$\mathfrak{p}A[\theta]+\mathcal{F}=A[\theta]\Rightarrow\mathfrak{p}B+\mathcal{F}B=B\Rightarrow\mathfrak{p}B+A[\theta]=B.$$

这说明h_2为满同态. 下面考虑$\ker h_2=\mathfrak{p}B\cap A[\theta]$. 我们断言$\ker h_2=\mathfrak{p}B\cap A[\theta]=\mathfrak{p}A[\theta]$. 显然有$\mathfrak{p}A[\theta]\subseteq\mathfrak{p}B\cap A[\theta]$. 反过来, 因为$\mathfrak{p}A[\theta]+\mathcal{F}=A[\theta]$, 存在$v\in\mathfrak{p}A[\theta]$与$w\in\mathcal{F}$使得

$$v+w=1.$$

对任意的$g(\theta)\in\mathfrak{p}B\cap A[\theta]$, 我们有

$$g(\theta)=vg(\theta)+wg(\theta)\in\mathfrak{p}A[\theta]+\mathcal{F}\mathfrak{p}B=\mathfrak{p}A[\theta].$$

因此$\mathfrak{p}B\cap A[\theta]\subseteq\mathfrak{p}A[\theta]$. 由上面的讨论, $\ker h_2=\mathfrak{p}A[\theta]$. 由此

$$A[\theta]/\mathfrak{p}A[\theta]\underset{\overline{h_2}}{\cong}B/\mathfrak{p}B.$$

综上, 同构(4.8)成立.

由商环的性质, $\kappa[t]/\overline{p_\theta}(t)\kappa[t]$上的素理想与$\kappa[t]$上包含$\overline{p_\theta}(t)$的素理想一一对应. 因此,

$$\mathfrak{a}_i=\overline{p_i}(t)\kappa[t]/\overline{p_\theta}(t)\kappa[t]\ (i=1,2,\cdots,r)$$

恰好为$k[t]/\overline{p_\theta}(t)\kappa[t]$上的全部素理想. 由同构(4.8), 我们得到

$$\overline{h_2}\circ\overline{h_1}\left(\mathfrak{a}_i\right)=\left(p_i(\theta)B+\mathfrak{p}B\right)/\mathfrak{p}B\ (i=1,2,\cdots,r)$$

恰好为$B/\mathfrak{p}B$上的全部素理想. 再利用商环的性质,

$$\mathfrak{P}_i = p_i(\theta)B + \mathfrak{p}B \ (i = 1, 2, \cdots, r)$$

恰好就是B中包含$\mathfrak{p}B$的全部素理想.

下面考虑分歧指数与惯性次数. 注意到

$$e(\mathfrak{P}_i|\mathfrak{p}) = \max\left\{e \in \mathbb{Z}_{\geq 0} : \ \mathfrak{p} \subseteq \mathfrak{P}_i^e\right\}.$$

(补充定义$\mathfrak{P}_i^0 = B$). 由此与同构(4.8), 我们得到

$$\begin{aligned} e(\mathfrak{P}_i|\mathfrak{p}) &= \max\left\{e \in \mathbb{Z}_{\geq 0} : \ \mathfrak{p} \subseteq \mathfrak{P}_i^e\right\} \\ &= \max\left\{e \in \mathbb{Z}_{\geq 0} : \ \overline{p_\theta}(t)\kappa[t] \subseteq \overline{p_i}(t)^e\kappa[t]\right\} \\ &= e_i. \end{aligned}$$

再由同构(4.8),

$$B/\mathfrak{P}_i \cong \frac{B/\mathfrak{p}B}{\mathfrak{P}_i/\mathfrak{p}B} \cong \frac{\kappa[t]/\overline{p_\theta}(t)\kappa[t]}{\overline{p_i}(t)\kappa[t]/\overline{p_\theta}(t)\kappa[t]} \cong \kappa[t]/\overline{p_i}(t)\kappa[t].$$

因此,

$$f\left(\mathfrak{P}_i|\mathfrak{p}\right) = [B/\mathfrak{P}_i : \kappa] = [\kappa[t]/\overline{p_i}(t)\kappa[t] : \kappa] = \deg(p_i(t)).$$

综上, 我们完成了证明. □

4.3 有理素数在二次域上的素理想分解

在本节中, 我们将利用Kummer分解定理来研究有理素数在二次域上的素理想分解.

定理 4.5. *设$d \neq 0, 1$为无平方因子整数, $K = \mathbb{Q}(\sqrt{d})$. 则下列结论成立.*

(i) *当素数$p > 2$时, 我们有*

$$\begin{aligned} p\text{在}\mathcal{O}_K\text{上完全分歧} &\Leftrightarrow d \equiv 0 \ (\mathrm{mod}\ p\mathbb{Z}), \\ p\text{在}\mathcal{O}_K\text{上完全分裂} &\Leftrightarrow \left(\frac{d}{p}\right) = 1, \\ p\mathcal{O}_K\text{为素理想} &\Leftrightarrow \left(\frac{d}{p}\right) = -1. \end{aligned}$$

(ii) 当$p=2$时, 我们有

$$2\text{在}\mathcal{O}_K\text{上完全分歧} \Leftrightarrow d\equiv 2,3 \pmod 4,$$
$$2\text{在}\mathcal{O}_K\text{上完全分裂} \Leftrightarrow d\equiv 1 \pmod 8,$$
$$2\mathcal{O}_K\text{为素理想} \Leftrightarrow d\equiv 5 \pmod 8.$$

证明: (i) 当$p>2$时, 令$\mathcal{F}$为$\mathbb{Z}[\sqrt{d}]$在$\mathcal{O}_K$中的导子. 则由定理1.3, 我们有$2\mathcal{O}_K\subseteq\mathbb{Z}[\sqrt{d}]$, 即$2\in\mathcal{F}$. 因此, 显然有$p\mathbb{Z}[\sqrt{d}]$与$\mathcal{F}$互素. 由定理4.4, $p\mathcal{O}_K$的素理想分解完全取决于$\sqrt{d}$在$\mathbb{Q}$上的极小多项式t^2-d在$\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p$上的分解. 由此, 我们容易验证(i)成立.

(ii) 当$p=2$时, 我们分两种情形讨论. 如果$d\equiv 2,3 \pmod 4$, 则取$\theta=\sqrt{d}$, 并且此时$\mathbb{Z}[\sqrt{d}]$在$\mathcal{O}_K$中的导子恰好为$\mathcal{O}_K$. 因为t^2-d在$\mathbb{F}_2$中可以分解为$(t-d)^2$, 由定理4.4, 素数2在$\mathcal{O}_K$上完全分歧. 如果$d\equiv 1 \pmod 4$, 则取$\theta=(-1+\sqrt{d})/2\in\mathcal{O}_K$. 此时$\theta$在$\mathcal{O}_K$中的导子也等于$\mathcal{O}_K$. 由定理4.4, $2\mathcal{O}_K$的分解完全取决于$(-1+\sqrt{d})/2$在$\mathbb{Q}$上的极小多项式$t^2+t+\frac{1-d}{4}$在$\mathbb{F}_2$上的分解. 由此, 我们容易验证(ii)成立.

综上, 我们完成了证明. □

4.4 分圆域的代数整数环

设$n\in\mathbb{Z}_{\geq 2}$, $\zeta_n\in\mathbb{C}$为一个本原n次单位根, 即

$$\zeta_n^m=1 \Leftrightarrow m\equiv 0 \pmod{n\mathbb{Z}}.$$

分圆域$\mathbb{Q}(\zeta_n)$是代数数论的重要研究对象, 在这里我们先介绍分圆域的一些简单性质.

为了方便, 对任意的素数p与多项式$f(t)\in\mathbb{Z}[t]$, 我们使用记号$\overline{f}(t)$表示$f(t)$模p的约化$f(t) \bmod p\mathbb{Z}[t]$. 我们首先有如下定理.

定理 4.6. 记号如上. 则

$$\{\sigma(\zeta_n):\ \sigma\in \mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})\}=\left\{\zeta_n^k:\ k\in(\mathbb{Z}/n\mathbb{Z})^\times\right\}.$$

也就是说, ζ_n的全部共轭元恰好为全体本原n次单位根.

证明: 我们先证明所有的本原n次单位根均为ζ_n的共轭元. 使用反证法. 假设存在本原n次单位根ζ_n^k $(\gcd(k,n)=1)$使得

$$\sigma(\zeta_n^k)\neq\zeta_n\ (\forall\sigma\in\mathrm{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})).$$

由Dirichlet定理, 存在素数p使得$p \equiv k \pmod{n\mathbb{Z}}$. 因此, $\zeta_n^k = \zeta_n^p$.

设$p_n(t) \in \mathbb{Z}[t]$为ζ_n在$\mathbb{Q}$上的极小多项式. 则存在首一多项式$g(t) \in \mathbb{Q}[t]$使得

$$t^n - 1 = p_n(t)g(t).$$

由Gauss引理, 我们有$g(t) \in \mathbb{Z}[t]$. 因为ζ_n^p不是ζ_n的共轭元, 我们得到$g(\zeta_n^p) = 0$. 因此,

$$g(t^p) \equiv 0 \pmod{p_n(t)\mathbb{Z}[t]}.$$

考虑这些多项式在$\mathbb{F}_p$上的约化. 注意到

$$g(t^p) \equiv g(t)^p \pmod{p\mathbb{Z}[t]},$$

由上面的讨论, 我们得到

$$\overline{g}(t)^p = \overline{g}(t^p) \equiv 0 \pmod{\overline{p_n}(t)\mathbb{F}_p[t]}.$$

因为$p_n(t) \in \mathbb{Z}[t]$为首一多项式, 我们有$\deg(\overline{p_n}(t)) \geq 1$. 由此, 存在$\mathbb{F}_p[t]$上的不可约多项式$\overline{h}(t)$使得

$$\overline{g}(t)^p \equiv 0 \pmod{\overline{h}(t)\mathbb{F}_p[t]}.$$

这说明

$$\overline{g}(t) \equiv 0 \pmod{\overline{h}(t)\mathbb{F}_p[t]}.$$

由此, 多项式$t^n - 1$在$\mathbb{F}_p^{\mathrm{alg}}$上有重根. 这显然矛盾(因为$\gcd(p, n) = 1$, 多项式$t^n - 1$在$\mathbb{F}_p^{\mathrm{alg}}$中无重根). 由上面的讨论, 我们得到

$$\left\{\zeta_n^k : k \in (\mathbb{Z}/n\mathbb{Z})^\times\right\} \subseteq \{\sigma(\zeta_n) : \sigma \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)\}.$$

反过来, 设ζ_n^m为ζ_n的一个共轭元, 并且设$\sigma_0 \in \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}\right)$使得$\sigma_0(\zeta_n) = \zeta_n^m$. 假设$\gcd(m, n) = d > 1$. 则

$$1 = (\zeta_n^m)^{\frac{n}{d}} = \sigma_0(\zeta_n)^{\frac{n}{d}} = \sigma_0(\zeta_n^{\frac{n}{d}}).$$

因此,

$$\zeta_n^{\frac{n}{d}} = \sigma_0^{-1}(1) = 1.$$

这与ζ_n为本原n次单位根矛盾. 上面的讨论说明ζ_n的共轭元一定为本原n次单位根.

综上, 我们完成了证明. □

由该定理, 我们容易得到如下推论.

推论 4.1. *记号如上. 则下列结论成立.*

(i) $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\left|(\mathbb{Z}/n\mathbb{Z})^\times\right|=\varphi(n)$.

(ii) ζ_n*的极小多项式为*

$$\Phi_n(t)=\prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(t-\zeta_n^k\right).$$

我们将其称为分圆多项式.

下面我们介绍抽象代数中的一个经典结果.

引理 4.3. *设G为有限交换群, $x,y\in G$. 则存在$z\in G$使得*

$$o(z)=\operatorname{lcm}\left(o(x),o(y)\right).$$

证明: 当$o(x)=o(y)=1$时, 结论显然成立. 下面假设$o(x)>1$或者$o(y)>1$. 设$p_1,\cdots,p_r$为$o(x)o(y)$中出现的全部素因子, 并且设

$$o(x)=\prod_{1\leq i\leq r}p_i^{u_i},\ o(y)=\prod_{1\leq i\leq r}p_i^{v_i},$$

其中$u_i,v_i\in\mathbb{Z}_{\geq 0}$. 令

$$X=\{1\leq i\leq r:\ u_i\leq v_i\},\ Y=\{1\leq i\leq r:\ u_i>v_i\}.$$

则容易验证

$$o\left(x^{\prod_{i\in X}p_i^{u_i}}\right)=\prod_{i\in Y}p_i^{u_i},$$

以及

$$o\left(y^{\prod_{i\in Y}p_i^{v_i}}\right)=\prod_{i\in X}p_i^{v_i}.$$

因为G为交换群且

$$\gcd\left(o\left(x^{\prod_{i\in X}p_i^{u_i}}\right),o\left(y^{\prod_{i\in Y}p_i^{v_i}}\right)\right)=1,$$

我们得到

$$o\left(x^{\prod_{i\in X}p_i^{u_i}}\cdot y^{\prod_{i\in Y}p_i^{v_i}}\right)=\prod_{i\in Y}p_i^{u_i}\cdot\prod_{i\in X}p_i^{v_i}=\operatorname{lcm}\left(o(x),o(y)\right).$$

综上, 我们完成了证明. □

我们还需要初等数论中的一个经典结果.

引理 4.4. 设$m,n\in\mathbb{Z}_{\geq 2}$, $\mathrm{lcm}(m,n)=l$, $\gcd(m,n)=d$. 则

$$\varphi(m)\varphi(n)=\varphi(d)\varphi(l).$$

证明: 设

$$\begin{aligned}X&=\{p:p\text{为素数},p\mid m,p\mid n\},\\ Y&=\{p:p\text{为素数},p\mid m,p\nmid n\},\\ Z&=\{p:p\text{为素数},p\nmid m,p\mid n\}.\end{aligned}$$

则

$$\begin{aligned}d&=\prod_{p\in X}p^{\min\{\mathrm{ord}_p(m),\mathrm{ord}_p(n)\}},\\ l&=\prod_{p\in X}p^{\max\{\mathrm{ord}_p(m),\mathrm{ord}_p(n)\}}\cdot\prod_{p\in Y}p^{\mathrm{ord}_p(m)}\cdot\prod_{p\in Z}p^{\mathrm{ord}_p(n)}.\end{aligned}$$

由此与φ函数的计算公式, 容易得到

$$\varphi(m)\varphi(n)=\varphi(d)\varphi(l).$$

综上, 我们完成了证明. □

利用这两个引理我们可以得到如下结果.

定理 4.7. 记号如上. 则下列结论成立.

(i) 对任意的$m\in\mathbb{Z}_{\geq 2}$, 我们有

$$\mathbb{Q}(\zeta_m,\zeta_n)=\mathbb{Q}(\zeta_{\mathrm{lcm}(m,n)}),\ \mathbb{Q}(\zeta_m)\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{\gcd(m,n)}).$$

(ii) 当$n\geq 2$为奇数时, $\mathbb{Q}(\zeta_n)=\mathbb{Q}(\zeta_{2n})$. 当$n\geq 2$为偶数时, 分圆域$\mathbb{Q}(\zeta_n)$中的所有单位根恰好为全体$n$次单位根.

证明: (i) 设$\mathrm{lcm}(m,n)=l$. 考虑由ζ_n,ζ_m生成的有限乘法交换群

$$G=\left\{\zeta_n^i\zeta_m^j:\ 0\leq i\leq n-1,0\leq j\leq m-1\right\}.$$

由引理4.3, 存在一个本原l次单位根$\zeta_l\in G$. 因此$\mathbb{Q}(\zeta_l)\subseteq\mathbb{Q}(\zeta_m,\zeta_n)$. 另一方面, 因为$n\mid l$, 单位根$\zeta_l^{\frac{l}{n}}$是一个本原$n$次单位根. 由定理4.6, 存在$k\in\mathbb{Z}$且$\gcd(k,n)=1$使得

$$\left(\zeta_l^{\frac{l}{n}}\right)^k=\zeta_n.$$

这说明$\zeta_n \in \mathbb{Q}(\zeta_l)$. 类似地, $\zeta_m \in \mathbb{Q}(\zeta_l)$. 由上面的讨论我们得到

$$\mathbb{Q}(\zeta_l) \subseteq \mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_l),$$

即$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{\mathrm{lcm}(m,n)})$.

设$d = \gcd(m, n)$. 因为$d \mid m, d \mid n$, 利用与上面类似的方法可以得到

$$\mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n).$$

另一方面, 由上面的讨论与Galois定理,

$$[\mathbb{Q}(\zeta_l) : \mathbb{Q}] = [\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_m) : \mathbb{Q}]\,[\mathbb{Q}(\zeta_n) : \mathbb{Q}]}{[(\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)) : \mathbb{Q}]}.$$

由此与引理4.4,

$$[(\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)) : \mathbb{Q}] = \frac{\varphi(m)\varphi(n)}{\varphi(l)} = \varphi(d) = [\mathbb{Q}(\zeta_d) : \mathbb{Q}]\,.$$

由上面的讨论我们得到

$$\mathbb{Q}(\zeta_d) = \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n).$$

(ii) 当$n \geq 2$为奇数时, $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{2n})$并且

$$[\mathbb{Q}(\zeta_{2n} : \mathbb{Q})] = \varphi(2n) = \varphi(n) = [\mathbb{Q}(\zeta_n : \mathbb{Q})]\,.$$

因此$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$.

当$n \geq 2$为偶数时, 设$\zeta_m \in \mathbb{Q}(\zeta_n)$为一个本原$m$次单位根, $l = \mathrm{lcm}(m, n)$. 由(i), 我们得到

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_l).$$

因此, $\varphi(n) = \varphi(l)$. 设$p_1, \cdots, p_r$恰好为所有整除n的素数且$p_1 = 2$. 因为$n \mid l$, 不妨设

$$n = p_1^{u_1} \cdots p_r^{u_r},$$
$$l = p_1^{v_1} \cdots p_r^{v_r} l',$$

其中$1 \leq u_i \leq v_i$, $l' \in \mathbb{Z}^+$且$\gcd(l', p_1 p_2 \cdots p_r) = 1$. 注意到$l'$为奇数, 由$\varphi$函数

的计算公式, 我们得到

$$\begin{aligned}
&\varphi(n)=\varphi(l)\\
\Rightarrow&\prod_{1\leq i\leq r}\left(1-\frac{1}{p}\right)p^{u_i}=\prod_{1\leq i\leq r}\left(1-\frac{1}{p}\right)p^{v_i}\cdot\varphi(l')\\
\Rightarrow&\prod_{1\leq i\leq r}p_i^{u_i-v_i}=\varphi(l')\\
\Rightarrow&\varphi(l')=1\text{并且}u_i=v_i\ (\forall i=1,2,\cdots,r)\\
\Rightarrow&n=l\\
\Rightarrow&m\mid n.
\end{aligned}$$

因此ζ_m是n次单位根.

综上, 我们完成了证明. □

当n为素数幂次时, 分圆域$\mathbb{Q}(\zeta_n)$的代数整数环是容易确定的.

引理 4.5. 设$n=p^r$, 其中p为素数, $r\in\mathbb{Z}^+$. 考虑分圆域$K=\mathbb{Q}(\zeta_n)$. 则下列结论成立.

(i) $\mathfrak{p}=(1-\zeta_n)\mathcal{O}_K$为$\mathcal{O}_K$上唯一包含素数$p$的素理想, 并且

$$p\mathcal{O}_K=(1-\zeta_n)^{\varphi(n)}\mathcal{O}_K.$$

(ii) $d(1,\zeta_n,\cdots,\zeta_n^{\varphi(n)-1})=\pm p^s$, 其中$s=p^{r-1}(rp-r-1)$.

(iii) $\mathcal{O}_K=\mathbb{Z}[\zeta_n]$.

证明: (i) 由定理4.6, ζ_n的极小多项式为

$$\Phi_n(t)=\prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(t-\zeta_n^k\right)=\frac{t^{p^r}-1}{t^{p^{r-1}}-1}=1+t^{p^{r-1}}+\cdots+t^{p^{r-1}(p-1)}.$$

令$t=1$, 我们得到

$$p=\prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(1-\zeta_n^k\right). \tag{4.9}$$

对任意的$k_1,k_2\in(\mathbb{Z}/n\mathbb{Z})^\times$, 可以取正整数$m$使得$k_2\cdot(m \bmod \mathfrak{n}\mathbb{Z})=k_1$. 因此

$$\frac{1-\zeta_n^{k_1}}{1-\zeta_n^{k_2}}=\frac{1-\zeta_n^{k_2m}}{1-\zeta_n^{k_2}}\in\mathbb{Z}[\zeta_n]\subseteq\mathcal{O}_K.$$

这说明对任意的$k_1,k_2\in(\mathbb{Z}/n\mathbb{Z})^\times$,

$$\frac{1-\zeta_n^{k_1}}{1-\zeta_n^{k_2}}\in\mathcal{O}_K^\times.$$

由此与(4.9), 我们得到

$$p\mathcal{O}_K = \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times} \left(1-\zeta_n^k\right)\mathcal{O}_K = (1-\zeta_n)^{\varphi(n)}\,\mathcal{O}_K.$$

注意到$[K:\mathbb{Q}]=\varphi(n)$, 利用定理4.3, 上式说明$\mathfrak{p}=(1-\zeta_n)\mathcal{O}_K$恰好为唯一包含$p$的素理想, 且$e(\mathfrak{p}|p)=\varphi(n)$, $f(\mathfrak{p}|p)=1$.

(ii) 为了方便, 我们设$m=\varphi(n)$, 并且设

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1,\cdots,\sigma_m\}.$$

则由判别式的定义,

$$\begin{aligned} d(1,\zeta_n,\cdots,\zeta_n^{\varphi(n)-1}) &= \det\left[\sigma_i(\zeta_n^{j-1})\right]_{1\le i,j\le m}^2 \\ &= \prod_{1\le i<j\le m}(\sigma_j(\zeta_n)-\sigma_i(\zeta_n)) \\ &= \pm\prod_{1\le i\ne j\le m}(\sigma_j(\zeta_n)-\sigma_i(\zeta_n)) \\ &= \pm\prod_{1\le j\le m}\prod_{i\ne j}(\sigma_j(\zeta_n)-\sigma_i(\zeta_n)) \\ &= \pm\prod_{1\le j\le m}\sigma_j\left(\Phi_n'(\zeta_n)\right) \\ &= \pm\mathrm{N}_{K/\mathbb{Q}}\left(\Phi_n'(\zeta_n)\right). \end{aligned} \tag{4.10}$$

在等式

$$\left(t^{p^{r-1}}-1\right)\Phi_n(t) = t^{p^r}-1$$

两边同时对t求导, 我们得到

$$\left(\zeta_n^{p^{r-1}}-1\right)\Phi_n'(\zeta_n) = p^r\zeta_n^{-1}.$$

注意到$\zeta_n^{p^{r-1}}$是一个本原p次单位根. 为了方便, 我们将其记作ζ_p. 由上式我们容易验证

$$\mathrm{N}_{K/\mathbb{Q}}\left(\Phi_n'(\zeta_n)\right) = \mathrm{N}_{K/\mathbb{Q}}\left(\frac{p^r}{\zeta_n(\zeta_p-1)}\right) = p^{rm}\cdot\mathrm{N}_{K/\mathbb{Q}}\left(\frac{1}{\zeta_n(\zeta_p-1)}\right). \tag{4.11}$$

由定理4.6与命题1.2,

$$\mathrm{N}_{K/\mathbb{Q}}(\zeta_n) = \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}\zeta_n^k = \pm\Phi_n(0) = \pm 1. \tag{4.12}$$

由命题1.3,

$$\begin{aligned}\mathrm{N}_{K/\mathbb{Q}}(\zeta_p-1)&=\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\mathrm{N}_{K/\mathbb{Q}(\zeta_p)}\left(\zeta_p-1\right)\right)\\&=\mathrm{N}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\left(\zeta_p-1\right)^{p^{r-1}}\\&=\pm p^{p^{r-1}}.\end{aligned}\tag{4.13}$$

将(4.10)–(4.13)结合起来, 我们得到

$$d(1,\zeta_n,\cdots,\zeta_n^{\varphi(n)-1})=\pm p^s,$$

其中$s=p^{r-1}(rp-r-1)$.

(iii) 沿用(ii)中的记号. 因为$f(\mathfrak{p}|p)=1$, 我们有$\mathbb{Z}/p\mathbb{Z}\cong\mathcal{O}_K/\mathfrak{p}$. 因此, $\mathbb{Z}+\mathfrak{p}=\mathcal{O}_K$. 这说明

$$\mathbb{Z}[\zeta_n]+(1-\zeta_n)\mathcal{O}_K=\mathcal{O}_K.\tag{4.14}$$

上式两边同时乘以$(1-\zeta_n)$得到

$$(1-\zeta_n)\mathcal{O}_K=(1-\zeta_n)\mathbb{Z}[\zeta_n]+(1-\zeta_n)^2\mathcal{O}_K.$$

由此与(4.14), 我们有

$$\mathbb{Z}[\zeta_n]+(1-\zeta_n)^2\mathcal{O}_K=\mathcal{O}_K.$$

重复上面的操作, 容易验证对任意的正整数t都有

$$\mathbb{Z}[\zeta_n]+(1-\zeta_n)^t\mathcal{O}_K=\mathcal{O}_K.$$

特别地, 当$t=ms$时$(m,s$均为(ii)中定义的数), 由(i),(ii)以及引理1.3我们得到

$$\begin{aligned}\mathcal{O}_K&=\mathbb{Z}[\zeta_n]+(1-\zeta_n)^{ms}\mathcal{O}_K\\&=\mathbb{Z}[\zeta_n]+p^s\mathcal{O}_K\\&=\mathbb{Z}[\zeta_n]+d(1,\zeta_n,\cdots,\zeta_n^{m-1})\mathcal{O}_K\\&\subseteq\mathbb{Z}[\zeta_n]\subseteq\mathcal{O}_K.\end{aligned}$$

因此$\mathcal{O}_K=\mathbb{Z}[\zeta_n]$.

综上, 我们完成了证明. □

对一般的$n\in\mathbb{Z}^+$, 下面我们来确定分圆域$\mathbb{Q}(\zeta_n)$的代数整数环. 为此, 我们首先介绍如下定理.

定理 4.8. 设A为整闭整环, $\mathrm{frac}(A)=K$, $L/K, L'/K$均为域的有限*Galois*扩张且$L\cap L'=K$. 设$\mathcal{O}_M$为A在LL'/K的中间域M上的整闭包.

假设$\mathcal{O}_L$与$\mathcal{O}_{L'}$关于A的整基均存在, 且分别设为$x_1,\cdots,x_n$与$y_1,\cdots,y_m$. 如果$d=d(x_1,\cdots,x_n)$与$d'=d(y_1,\cdots,y_m)$在A上互素, 则

$$x_iy_j\ (1\leq i\leq n, 1\leq j\leq m)$$

恰好为$\mathcal{O}_{LL'}$关于A的整基, 并且此时这组整基的判别式为$d^md'^n$.

证明: 首先由Galois定理与$L\cap L'=K$, 我们得到

$$[LL':K]=\frac{[L:K]\,[L':K]}{[L\cap L':K]}=[L:K]\,[L':K]\,. \tag{4.15}$$

注意到

$$LL'=K(x_1,\cdots,x_n)K(y_1,\cdots,y_m).$$

这说明LL'中的元素都可以表示为这些x_iy_j的K线性组合. 由此与(4.15), 这些x_iy_j恰好为LL'/K的一组基. 由此, 我们下面仅需证明$\mathcal{O}_{LL'}$中的任意元素均可表示为这些x_iy_j的A线性组合.

设$z\in\mathcal{O}_{LL'}$. 则存在$a_{ij}\in K\ (1\leq i\leq n, 1\leq j\leq m)$使得

$$z=\sum_{1\leq i\leq n}\sum_{1\leq j\leq m}a_{ij}x_iy_j=\sum_{1\leq i\leq n}M_ix_i, \tag{4.16}$$

其中

$$M_i=\sum_{1\leq j\leq m}a_{ij}y_j\in L'.$$

因为$L\cap L'=K$, 设

$$\mathrm{Gal}\,(LL'/L')\cong\mathrm{Gal}\,(L/K)=\{\sigma_1,\sigma_2,\cdots,\sigma_n\}\,.$$

由(4.16)得到线性方程组

$$\sigma_i(z)=\sum_{1\leq j\leq n}\sigma_j(x_i)M_i\ (1\leq j\leq n).$$

由Cramer法则, 对任意的$1\leq i\leq n$,

$$M_i\in\frac{1}{\det\left[\sigma_j(x_i)\right]_{1\leq i,j\leq n}}\mathcal{O}_{LL'}.$$

由此我们得到

$$d \cdot M_i = \sum_{1\leq j\leq m} da_{ij}y_j \in \mathcal{O}_{LL'} \cap L' = \mathcal{O}_{L'}.$$

因为这些y_j为$\mathcal{O}_{L'}$在A上的整基, 我们有$da_{ij} \in A$ $(\forall 1 \leq i \leq n, 1 \leq j \leq m)$. 类似地, 我们也有$d'a_{rj} \in A$ $(\forall 1 \leq i \leq n, 1 \leq j \leq m)$. 因为$d, d'$在$A$上互素, 存在$u, v \in A$使得

$$du + d'v = 1.$$

这说明对任意的$1 \leq i \leq n, 1 \leq j \leq m$,

$$a_{ij} = da_{ij}u + d'a_{ij}v \in A.$$

综上, 我们证明了这些x_iy_j恰好为$\mathcal{O}_{LL'}$关于A的整基.

下面考虑这组整基的判别式. 设

$$N = [\tau_i(y_j)]_{1\leq i,\leq m},$$

其中

$$\{\tau_1, \cdots, \tau_m\} = \mathrm{Gal}\left(L'/K\right).$$

因为$L \cap L' = K$, 我们有

$$\mathrm{Gal}\left(LL'/K\right) \cong \mathrm{Gal}(L/K) \oplus \mathrm{Gal}(L'/K).$$

由这些与判别式的定义, 这组整基的判别式恰好等于

$$\det \begin{bmatrix} \sigma_1(x_1)N & \sigma_1(x_2)N & \cdots & \sigma_1(x_n)N \\ \sigma_1(x_2)N & \sigma_2(x_2)N & \cdots & \sigma_2(x_n)N \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(x_1)N & \sigma_n(x_2)N & \cdots & \sigma_n(x_n)N \end{bmatrix}^2 = d^m d'^n.$$

综上, 我们完成了证明. □

最后, 我们介绍这一节的核心定理.

定理 4.9. 设$n \in \mathbb{Z}^+$. 则代数数域$K = \mathbb{Q}(\zeta_n)$的代数整数环为$\mathbb{Z}[\zeta_n]$.

证明: 由引理4.5, 当$n = 1$或者n为素数幂次时, 结论成立. 因此我们不妨设

$$n = p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s},$$

其中$s \geq 2, p_1, \cdots, p_s$为两两不同的素数, 并且$r_1, \cdots, r_s \in \mathbb{Z}^+$. 由定理4.7,

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{r_1}}, \zeta_{p_2^{r_2}}, \cdots, \zeta_{p_s^{r_s}}).$$

由定理4.7与引理4.5, 对任意的$1 \leq i < j \leq s$, 我们有

$$\mathbb{Q}(\zeta_{p_i^{r_i}}) \cap \mathbb{Q}(\zeta_{p_j^{r_j}}) = \mathbb{Q},$$

以及

$$\gcd\left(d(\mathbb{Q}(\zeta_{p_i^{r_i}})), d(\mathbb{Q}(\zeta_{p_j^{r_j}}))\right) = 1.$$

由上面的讨论, 利用定理4.8, 我们得到

$$\mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_K = \mathbb{Z}[\zeta_{p_1^{r_1}}, \zeta_{p_2^{r_2}}, \cdots, \zeta_{p_s^{r_s}}] \subseteq \mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_K.$$

因此, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$.

综上, 我们完成了证明. □

4.5 有理素数在分圆域上的素理想分解

本节我们利用Kummer分解定理研究有理素数在分圆域上的素理想分解.

定理 4.10. *设$n \in \mathbb{Z}_{\geq 2}$, $K = \mathbb{Q}(\zeta_n)$. 对任意的有理素数p, 设*

$$f_p := \min\left\{k \in \mathbb{Z}^+ : \ p^k \equiv 1 \ (\mathrm{mod}\ n/p^{\mathrm{ord}_p(n)})\right\}.$$

则

$$p\mathcal{O}_K = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r)^{\varphi(p^{\mathrm{ord}_p(n)})},$$

其中$\mathfrak{p}_1, \cdots, \mathfrak{p}_r$为$\mathcal{O}_K$上两两不同的素理想. 并且对任意的$1 \leq i \leq r$, 我们有$f(\mathfrak{p}_i|p) = f_p$.

证明: 首先考虑$p \nmid n$的情形. 设$\mathfrak{p}$为$\mathcal{O}_K$上一个包含p的素理想. 我们有

$$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subseteq \mathcal{O}_K/\mathfrak{p} \subseteq \mathbb{F}_p^{\mathrm{alg}}.$$

设

$$U_n(\mathbb{C}) = \{x \in \mathbb{C} : \ x^n = 1\}, \ U_n(\mathbb{F}_p^{\mathrm{alg}}) = \{x \in \mathbb{F}_p^{\mathrm{alg}} : \ x^n = 1\}.$$

因为$p \nmid n$, 多项式$t^n - 1$在$\mathbb{F}_p^{\mathrm{alg}}$上无重根. 因此, $x \mapsto x \bmod \mathfrak{p}$为$U_n(\mathbb{C}) \to U_n(\mathbb{F}_p^{\mathrm{alg}})$的同构. 注意到

$$\mathbb{F}_p\left(U_n(\mathbb{F}_p^{\mathrm{alg}})\right) = \mathbb{F}_{p^{f_p}}.$$

因此, 对$\mathbb{F}_p^{\mathrm{alg}}$中任意的本原$n$次单位根$x$, 我们有$[\mathbb{F}_p(x):\mathbb{F}_p] = f_p$, 并且$\overline{\Phi_n}(t) = \Phi_n(t) \bmod p\mathbb{Z}[t]$在$\mathbb{F}_{p^{f_p}}[t]$上完全分解为

$$\overline{\Phi_n}(t) = \prod_{x\in\mathbb{F}_p^{\mathrm{alg}}\text{为本原}n\text{次单位根}} (t-x).$$

因为t^n-1在$\mathbb{F}_p$上无重根, 我们可以设$\overline{\Phi_n}(t)$在$\mathbb{F}_p$上分解为

$$\overline{\Phi_n}(t) = \overline{p_1}(t)\overline{p_2}(t)\cdots\overline{p_r}(t),$$

其中$p_i(t) \in \mathbb{Z}[t]$为首一多项式, $\overline{p_i}(t) = p_i(t) \bmod p\mathbb{Z}[t]$为$\mathbb{F}_p[t]$上两两不同的不可约多项式. 注意到这些不可约多项式$\overline{p_i}(t)$均为$\mathbb{F}_p^{\mathrm{alg}}$中本原$n$次单位根在$\mathbb{F}_p$上的不可约多项式. 我们得到

$$\deg(p_i(t)) = f_p.$$

因为$\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, 由定理4.4, 我们有

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r,$$

其中这些$\mathfrak{p}_i = p\mathcal{O}_K + p_i(\zeta_n)\mathcal{O}_K$为$\mathcal{O}_K$上两两不同的素理想, 并且$f(\mathfrak{p}|p) = \deg(p_i) = f_p$.

下面我们考虑$p \mid n$的情形. 此时我们设$n = p^{\mathrm{ord}_p(n)}n'$, 并取$\mathcal{O}_K$上的一个素理想$\mathfrak{p}$使得 $(1-\zeta_{p^{\mathrm{ord}_p(n)}}) \in \mathfrak{p}$ (由引理4.5, 元素$(1-\zeta_{p^{\mathrm{ord}_p(n)}}) \notin \mathcal{O}_K$, 因此这样的$\mathfrak{p}$是存在的). 因为$\gcd(p^{\mathrm{ord}_p(n)}, n') = 1$,

$$\left(\mathbb{Z}/p^{\mathrm{ord}_p(n)}\mathbb{Z}\right)^\times \oplus (\mathbb{Z}/n'\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

这得到

$$\left\{\zeta_{p^{\mathrm{ord}_p(n)}}^i\zeta_{n'}^j : i \in (\mathbb{Z}/p^{\mathrm{ord}_p(n)})^\times, j \in (\mathbb{Z}/n'\mathbb{Z})^\times\right\} = \left\{\zeta_n^i : i \in (Z/n\mathbb{Z})^\times\right\}.$$

因此,

$$\Phi_n(t) = \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}\left(t-\zeta_n^k\right) = \prod_{i\in(\mathbb{Z}/p^{\mathrm{ord}_p(n)})^\times}\prod_{j\in(\mathbb{Z}/n'\mathbb{Z})^\times}\left(t-\zeta_{p^{\mathrm{ord}_p(n)}}^i\zeta_{n'}^j\right).$$

因为$\zeta_{p^{\mathrm{ord}_p(n)}} \equiv 1 \pmod{\mathfrak{p}}$, 上式可以得到

$$\Phi_n(t) \equiv \prod_{i\in(\mathbb{Z}/p^{\mathrm{ord}_p(n)}\mathbb{Z})^\times} \prod_{j\in(\mathbb{Z}/n'\mathbb{Z})^\times} (t-\zeta_{p^{\mathrm{ord}_p(n)}}^i) \equiv \Phi_{n'}(t)^{\varphi(p^{\mathrm{ord}_p(n)})} \pmod{\mathfrak{p}\mathcal{O}_K[t]}.$$

注意到$\Phi_n(t), \Phi_{n'}(t) \in \mathbb{Z}[t]$, 上面的同余式说明

$$\Phi_n(t) \equiv \Phi_{n'}(t)^{\varphi(p^{\mathrm{ord}_p(n)})} \pmod{p\mathbb{Z}[t]}.$$

也就是说, $\Phi_n(t) \bmod p\mathbb{Z}[t]$在$\mathbb{F}_p[t]$上的分解完全取决于$\Phi_{n'}(t) \bmod p\mathbb{Z}[t]$在$\mathbb{F}_p[t]$上的分解. 因为$p \nmid n'$, 利用前面的讨论, 我们容易得到

$$p\mathcal{O}_K = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r)^{\varphi(p^{\mathrm{ord}_p(n)})},$$

其中$\mathfrak{p}_1, \cdots, \mathfrak{p}_r$为$\mathcal{O}_K$上两两不同的素理想. 并且对任意的$1 \leq i \leq r$, 我们有

$$f(\mathfrak{p}_i|p) = \min\left\{k \in \mathbb{Z}^+ : \ p^k \equiv 1 \pmod{n'}\right\}.$$

综上, 我们完成了证明. □

5 Hilbert分歧理论

在本章中, 如果没有特殊说明, 我们总是设A为Dedekind环, $\mathrm{frac}(A)=K$, L/K为有限Galois扩张, B为A在L中的整闭包. 对A的任意非零素理想$\mathfrak{p}$, 令

$$\Omega_{\mathfrak{p}}=\{\mathfrak{P}:\ \mathfrak{P}\text{为}B\text{的素理想且}\mathfrak{p}\subseteq\mathfrak{P}\}.$$

5.1 分解群与惯性群

我们从下面的结果开始.

命题 5.1. *设$\mathfrak{p}$为A的非零素理想. 则对任意的$\mathfrak{P}_0\in\Omega_{\mathfrak{p}}$, 我们有*

$$\{\sigma(\mathfrak{P}_0):\ \sigma\in\mathrm{Gal}(L/K)\}=\Omega_{\mathfrak{p}}.$$

也就是说, $\mathrm{Gal}(L/K)$在$\Omega_{\mathfrak{p}}$上的作用是可迁的.

证明: 使用反证法. 假设存在$\mathfrak{P}_1\in\Omega_{\mathfrak{p}}$使得

$$\mathfrak{P}_1\notin\{\sigma(\mathfrak{P}_0):\ \sigma\in\mathrm{Gal}(L/K)\}.$$

则由中国剩余定理, 存在$x\in B$使得

$$\begin{cases}x\equiv 0\ (\mathrm{mod}\ \mathfrak{P}_1),\\ x\equiv 1\ (\mathrm{mod}\ \sigma^{-1}(\mathfrak{P}_0))\ (\forall\sigma\in\mathrm{Gal}(L/K)).\end{cases}$$

由此,

$$\mathrm{N}_{L/K}(x)=\prod_{\sigma\in\mathrm{Gal}(L/K)}\sigma(x)\equiv 1\ (\mathrm{mod}\ \mathfrak{P}_0).$$

因为$\mathrm{N}_{L/K}(x)\in A$, 上式得到$\mathrm{N}_{L/K}(x)\equiv 1\ (\mathrm{mod}\ \mathfrak{p})$. 另一方面,

$$\mathrm{N}_{L/K}(x)=x\cdot\prod_{\sigma\in\mathrm{Gal}(L/K)\setminus\{\mathrm{id}\}}\sigma(x)\equiv 0\ (\mathrm{mod}\ \mathfrak{P}_1).$$

因此, $\mathrm{N}_{L/K}(x)\equiv 0\ (\mathrm{mod}\ \mathfrak{p})$. 这与$\mathrm{N}_{L/K}(x)\equiv 1\ (\mathrm{mod}\ \mathfrak{p})$矛盾.

综上, 我们完成了证明. □

由该命题, 我们容易得到如下推论.

推论 5.1. *设$\mathfrak{p}$为A的非零素理想. 则对任意的$\mathfrak{P}_i,\mathfrak{P}_j\in\Omega_{\mathfrak{p}}$都有*

$$e\left(\mathfrak{P}_i|\mathfrak{p}\right)=e\left(\mathfrak{P}_j|\mathfrak{p}\right),$$

以及

$$f\left(\mathfrak{P}_i|\mathfrak{p}\right)=f\left(\mathfrak{P}_j|\mathfrak{p}\right).$$

为了方便, 将这些相同的$e\left(\mathfrak{P}_i|\mathfrak{p}\right)$简记为$e_{\mathfrak{p}}$, 将这些相同的$f\left(\mathfrak{P}_i|\mathfrak{p}\right)$简记为$f_{\mathfrak{p}}$.

下面我们给出分解群以及分解域的定义.

定义 5.1. 设$\mathfrak{p}$为A的非零素理想. 对任意的$\mathfrak{P}\in\Omega_{\mathfrak{p}}$, 称子群

$$G_{\mathfrak{P}}:=\{\sigma\in\mathrm{Gal}(L/K):\ \sigma(\mathfrak{P})=\mathfrak{P}\}$$

为$\mathfrak{P}$在K上的分解群(decomposition group). 同时, 将$G_{\mathfrak{P}}$的不动点域

$$Z_{\mathfrak{P}}:=\{x\in L:\ \sigma(x)=x\ \forall\sigma\in G_{\mathfrak{P}}\}$$

称为$\mathfrak{P}$在K上的分解域(decomposition field).

关于$G_{\mathfrak{P}}$, 我们有如下注记.

注记 5.1. (i) 对任意的$\sigma\in\mathrm{Gal}(L/K)$, 我们有

$$G_{\sigma(\mathfrak{P})}=\sigma\circ G_{\mathfrak{P}}\circ\sigma^{-1}.$$

(ii) 由群作用的性质与定理*4.3*,

$$[\mathrm{Gal}(L/K):G_{\mathfrak{P}}]=|\Omega_{\mathfrak{p}}|=\frac{[L:K]}{e_{\mathfrak{p}}f_{\mathfrak{p}}}.$$

因此, $|G_{\mathfrak{P}}|=e_{\mathfrak{p}}f_{\mathfrak{p}}$.

为了方便, 对B的任意非零素理想$\mathfrak{P}$以及任意的中间域$K\subseteq M\subseteq L$, 记号$\mathfrak{P}_M$表示$B\cap M$上的素理想$\mathfrak{P}\cap M$. 我们有如下定理.

定理 5.1. 设$\mathfrak{P}$为B的非零素理想, $\mathfrak{p}=\mathfrak{P}\cap A$. 则下列结论成立.

(i) $\mathfrak{P}$为B上唯一包含$\mathfrak{P}_{Z_{\mathfrak{P}}}$的素理想.

(ii) $e(\mathfrak{P}_{Z_{\mathfrak{P}}}|\mathfrak{p})=f(\mathfrak{P}_{Z_{\mathfrak{P}}}|\mathfrak{p})=1$.

(iii) 设集合

$$X=\{M:\ M\text{为}L/K\text{的中间域且}\mathfrak{P}\text{为}B\text{上唯一包含}\mathfrak{P}_M\text{的素理想}\}.$$

则对任意的$M\in X$都有$Z_{\mathfrak{P}}\subseteq M$, 即$Z_{\mathfrak{P}}$为$X$中最小的中间域.

(iv) 设集合

$$Y=\{M:\ M\text{为}L/K\text{的中间域且}e(\mathfrak{P}_M|\mathfrak{p})=f(\mathfrak{P}_M|\mathfrak{p})=1\}.$$

则对任意的$M\in Y$都有$M\subseteq Z_{\mathfrak{P}}$, 即$Z_{\mathfrak{P}}$为$Y$中最大的中间域.

证明: (i) 因为$L/Z_{\mathfrak{P}}$也为Galois扩张, 由命题5.1, 集合

$$\{\sigma(\mathfrak{P}):\ \sigma\in \mathrm{Gal}(L/Z_{\mathfrak{P}})=G_{\mathfrak{P}}\}$$

中的全部素理想恰好为B上包含$\mathfrak{P}_{Z_{\mathfrak{P}}}$的全体素理想. 因此$\mathfrak{P}$为$B$上唯一包含$\mathfrak{P}_{Z_{\mathfrak{P}}}$的素理想.

(ii) 容易验证$\mathfrak{P}$在$Z_{\mathfrak{P}}$上的分解群恰好为$G_{\mathfrak{P}}$. 因此, 由注记5.1我们得到

$$e(\mathfrak{P}|\mathfrak{P}_{Z_{\mathfrak{P}}})\cdot f(\mathfrak{P}|\mathfrak{P}_{Z_{\mathfrak{P}}})=|G_{\mathfrak{P}}|=e(\mathfrak{P}|\mathfrak{p})\cdot f(\mathfrak{P}|\mathfrak{p}).$$

由此$e(\mathfrak{P}_{Z_{\mathfrak{P}}}|\mathfrak{p})=f(\mathfrak{P}_{Z_{\mathfrak{P}}}|\mathfrak{p})=1$.

(iii) 对任意的$M\in X$, 由分解群的定义, $\mathfrak{P}$在M上的分解群为

$$\{\sigma\in \mathrm{Gal}(L/M):\ \sigma(\mathfrak{P})=\mathfrak{P}\}=G_{\mathfrak{P}}\cap \mathrm{Gal}(L/M).$$

由Galois对应, $\mathfrak{P}$在M上的分解域恰好为$Z_{\mathfrak{P}}M$. 因为$\mathfrak{P}$为B上唯一包含$\mathfrak{P}_M$的素理想, 由(ii)与定理4.3, 我们得到

$$[L:M]=e\left(\mathfrak{P}|\mathfrak{P}_M\right)\cdot f\left(\mathfrak{P}|\mathfrak{P}_M\right)=e\left(\mathfrak{P}|\mathfrak{P}_{Z_{\mathfrak{P}}M}\right)\cdot f\left(\mathfrak{P}|\mathfrak{P}_{Z_{\mathfrak{P}}M}\right)=[L:Z_{\mathfrak{P}}M].$$

因此, $M=Z_{\mathfrak{P}}M$, 即$Z_{\mathfrak{P}}\subseteq M$.

(iv) 对任意的$M\in Y$, 类似于(iii)的证明, $\mathfrak{P}$在M上的分解域恰好为$Z_{\mathfrak{P}}M$. 因为$e(\mathfrak{P}_M|\mathfrak{p})=f(\mathfrak{P}_M|\mathfrak{p})=1$, 由(ii)与定理4.3, 我们得到

$$\begin{aligned}[L:Z_{\mathfrak{P}}M]&=e(\mathfrak{P}|\mathfrak{P}_{Z_{\mathfrak{P}}M})\cdot f(\mathfrak{P}|\mathfrak{P}_{Z_{\mathfrak{P}}M})\\&=e(\mathfrak{P}|\mathfrak{P}_M)\cdot f(\mathfrak{P}|\mathfrak{P}_M)\\&=e(\mathfrak{P}|\mathfrak{p})\cdot f(\mathfrak{P}|\mathfrak{p})\\&=[L:Z_{\mathfrak{P}}].\end{aligned}$$

因此, $Z_{\mathfrak{P}}M=Z_{\mathfrak{P}}$, 即$M\subseteq Z_{\mathfrak{P}}$.

综上, 我们完成了证明. □

为了给出惯性群的定义, 我们需要下面几个结果.

引理 5.1. *设$\mathfrak{P}$为B的非零素理想, $\mathfrak{p}=\mathfrak{P}\cap A$, $\lambda=B/\mathfrak{P}$, $\kappa=A/\mathfrak{p}$. 则剩余类域的扩张λ/κ为正规扩张.*

证明: 对任意的$\bar{x}=x \bmod \mathfrak{P}\in\lambda$ (其中$x\in B$), 设$p_x(t)\in A[t]$为x在K上的极小多项式, $\overline{h}_x(t)\in\kappa[t]$为$\bar{x}$在$\kappa$上的极小多项式. 显然在$\kappa[t]$中, $\overline{h}_x(t)$可以

整除$\overline{p_x}(t) = p_x(t) \bmod \mathfrak{p}A[t]$. 因为$L/K$为Galois扩张, $p_x(t)$在$B[t]$中完全分解. 因此,$\overline{p_x}(t)$在$\kappa[t]$中完全分解. 由上面的讨论, $\overline{h}_x(t)$在$\kappa[t]$中完全分解. 因此, λ/κ是正规扩张.

综上, 我们完成了证明. □

我们给出如下定理.

定理 5.2. *记号如上. 假设λ/κ为可分扩张. 考虑$G_{\mathfrak{P}} \to \mathrm{Gal}(\lambda/\kappa)$的同态$\pi : \sigma \mapsto \overline{\sigma}$, 其中*

$$\overline{\sigma}\left(x \bmod \mathfrak{P}\right) = \sigma(x) \bmod \mathfrak{P} \ (\forall x \in B).$$

则π为满同态.

证明: 由定理5.1,

$$\left(B \cap Z_{\mathfrak{P}}\right) / \mathfrak{P}_{Z_{\mathfrak{P}}} \cong A/\mathfrak{p}.$$

因此, 我们不妨设$K = Z_{\mathfrak{P}}$. 此时有$\mathrm{Gal}(L/K) = G_{\mathfrak{P}}$. 因为$\lambda/\kappa$为有限可分扩张, 存在$x \in B$使得$\lambda = \kappa(\bar{x})$, 其中$\bar{x} = x \bmod \mathfrak{P}$. 设$p_x(t)$为$x$在$K$上的极小多项式, $\overline{h}_x(t)$为$\bar{x}$在κ上的极小多项式. 则对任意的$\tau \in \mathrm{Gal}(\lambda/\kappa)$, 自同构$\tau$完全由$\tau(\bar{x})$所决定. 在$\kappa[t]$中, $\overline{h}_x(t)$可以整除$\overline{p_x}(t) = p_x(t) \bmod \mathfrak{p}A[t]$. 由上面的讨论, 存在$\sigma \in \mathrm{Hom}_K(K(x), L)$使得

$$\sigma(x) \bmod \mathfrak{P} = \tau(\bar{x}).$$

将σ延拓为$\mathrm{Gal}(L/K)$中的自同构σ_0. 则$\pi(\sigma_0) = \tau$. 因此, π为满同态.

综上, 我们完成了证明. □

注记 5.2. *将λ/κ为可分扩张的条件去掉, 结论依然成立. 我们在这里就不详细讨论了.*

下面我们给出惯性群以及惯性域的定义.

定义 5.2. *记号如上. 将满同态$\pi : G_{\mathfrak{P}} \to \mathrm{Gal}(\lambda/\kappa)$的核$\mathrm{Ker}\pi$称为$\mathfrak{P}$在$K$上的惯性群(inertia group), 记作$I_{\mathfrak{P}}$. 将$I_{\mathfrak{P}}$的不动点域*

$$T_{\mathfrak{P}} = \{x \in L : \ \sigma(x) = x \ \forall \sigma \in I_{\mathfrak{P}}\}$$

称为$\mathfrak{P}$在K上的惯性域(inertia field).

关于惯性群我们有如下注记.

注记 5.3. (i) 由满同态π的定义, 容易验证

$$\begin{aligned} I_{\mathfrak{P}} &= \{\sigma \in G_{\mathfrak{P}} : \ \sigma(x) \equiv x \ (\mathrm{mod}\ \mathfrak{P}) \ \forall x \in B\} \\ &= \{\sigma \in \mathrm{Gal}(L/K) : \ \sigma(x) \equiv x \ (\mathrm{mod}\ \mathfrak{P}) \ \forall x \in B\}. \end{aligned}$$

最后一个等式成立是因为$\sigma(x) \equiv x \ (\mathrm{mod}\ \mathfrak{P}) \ (\forall x \in B) \Rightarrow \sigma \in G_{\mathfrak{P}}$.

(ii) 因为$G_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\lambda/\kappa)$, 我们得到$|I_{\mathfrak{P}}| = e(\mathfrak{P}|\mathfrak{p})$. 因此, 当$\mathfrak{p}$在$L$上不分歧时,

$$G_{\mathfrak{P}} \cong \mathrm{Gal}(\lambda/\kappa).$$

关于惯性群与惯性域, 我们有如下定理.

定理 5.3. 设$\mathfrak{P}$为B的非零素理想, $\mathfrak{p} = \mathfrak{P} \cap A$. 则下列结论成立.

(i) $\mathfrak{P}_{T_{\mathfrak{P}}}$在$L$上完全分歧, 即$[L : T_{\mathfrak{P}}] = e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{P}_{T_{\mathfrak{P}}})$.

(ii) $f(\mathfrak{P}_{T_{\mathfrak{P}}}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p})$以及$e(\mathfrak{P}_{T_{\mathfrak{P}}}|\mathfrak{p}) = 1$.

(iii) 设集合

$$U = \{M : \ M\text{为}L/K\text{的中间域且}\mathfrak{P}_M\text{在}L\text{上完全分歧}\}.$$

则对任意的$M \in U$都有$T_{\mathfrak{P}} \subseteq M$, 即$T_{\mathfrak{P}}$为$U$中最小的中间域.

(iv) 设集合

$$V = \{M : \ M\text{为}L/K\text{的中间域且}e(\mathfrak{P}_M|\mathfrak{p}) = 1\}.$$

则对任意的$M \in V$都有$M \subseteq T_{\mathfrak{P}}$, 即$T_{\mathfrak{P}}$为$V$中最大的中间域.

证明: (i) 由注记5.3, 素理想$\mathfrak{P}$在$T_{\mathfrak{P}}$上的惯性群为

$$\{\sigma \in \mathrm{Gal}(L/T_{\mathfrak{P}}) : \ \sigma(x) \equiv x \ (\mathrm{mod}\ \mathfrak{P}) \ \forall x \in B\} = I_{\mathfrak{P}} \cap \mathrm{Gal}(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}.$$

因此, 再由注记5.3, 我们得到

$$e(\mathfrak{P}|\mathfrak{P}_{T_{\mathfrak{P}}}) = |I_{\mathfrak{P}}| = e(\mathfrak{P}|\mathfrak{p}) = [L : T_{\mathfrak{P}}]. \tag{5.1}$$

这说明$\mathfrak{P}_{T_{\mathfrak{P}}}$在$L$上完全分歧.

(ii) 由(5.1), 我们有$e(\mathfrak{P}_{T_{\mathfrak{P}}}|\mathfrak{p}) = 1$. 另一方面, 容易验证$\mathfrak{P}$在$T_{\mathfrak{P}}$上的分解群为

$$G_{\mathfrak{P}} \cap \mathrm{Gal}(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}.$$

因此, 由注记5.1与(5.1), 我们有

$$e(\mathfrak{P}|\mathfrak{P}_{T_\mathfrak{P}}) = |I_\mathfrak{P}| = e(\mathfrak{P}|\mathfrak{P}_{T_\mathfrak{P}}) \cdot f(\mathfrak{P}|\mathfrak{P}_{T_\mathfrak{P}}).$$

因此, $f(\mathfrak{P}|\mathfrak{P}_{T_\mathfrak{P}}) = 1$, 即$f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}_{T_\mathfrak{P}}|\mathfrak{p})$.

(iii) 对任意的$M \in U$, 类似于定理5.1的证明, 容易说明$MT_\mathfrak{P}$恰好为$\mathfrak{P}$在M上的惯性域. 注意到$[L : M] = e(\mathfrak{P}|\mathfrak{P}_M)$, 由(i), 我们得到

$$[L : MT_\mathfrak{P}] = e(\mathfrak{P}|\mathfrak{P}_{MT_\mathfrak{P}}) = e(\mathfrak{P}|\mathfrak{P}_M) = [L : M].$$

因此, $MT_\mathfrak{P} = M$, 即$T_\mathfrak{P} \subseteq M$.

(iv) 对任意的$M \in V$, 类似于上面的讨论, $MT_\mathfrak{P}$恰好为$\mathfrak{P}$在M上的惯性域. 由(i)以及$e(\mathfrak{P}_M|\mathfrak{p}) = 1$, 我们得到

$$[L : MT_\mathfrak{P}] = e(\mathfrak{P}|\mathfrak{P}_{MT_\mathfrak{P}}) = e(\mathfrak{P}|\mathfrak{P}_M) = e(\mathfrak{P}|\mathfrak{p}) = [L : T_\mathfrak{P}].$$

这说明$MT_\mathfrak{P} = T_\mathfrak{P}$, 即$M \subseteq T_\mathfrak{P}$.

综上, 我们完成了证明. □

注记 5.4. *由定理5.1与定理5.3, $\mathfrak{p}$在B中素理想分解的过程可以由下面的图来描述*

$$\underset{\mathfrak{p}}{K} \xrightarrow[\text{分裂过程}]{} \underset{\mathfrak{P}_{Z_\mathfrak{P}}}{Z_\mathfrak{P}} \xrightarrow[\text{惯性次数改变过程}]{} \underset{\mathfrak{P}_{T_\mathfrak{P}}}{T_\mathfrak{P}} \xrightarrow[\text{分歧过程}]{} \underset{\mathfrak{P}}{L}.$$

利用定理5.1与定理5.3, 我们可以得到如下推论.

推论 5.2. *设A为Dedekind环, $\mathrm{frac}(A) = K$, 域L_1, L_2均为K的有限可分扩张, $\mathcal{O}_{L_1}$为A在L_1中的整闭包. 则对A的任意非零素理想$\mathfrak{p}$, 下列结论成立.*

(i) 如果$\mathfrak{p}$在L_1, L_2上都不分歧, 则$\mathfrak{p}$在L_1L_2上也不分歧.

(ii) 如果$\mathfrak{p}$在L_1, L_2上完全分裂, 则$\mathfrak{p}$在L_1L_2上也完全分裂.

(iii) 假设L_2/K为有限Galois扩张. 如果$\mathfrak{p}$在L_2上不分歧(或者完全分裂), 则$\mathcal{O}_{L_1}$上任意包含$\mathfrak{p}$的素理想$\mathfrak{P}_{L_1}$在L_1L_2上也不分歧(或者完全分裂).

证明: 我们只证明(iii)中不分歧的情形, 其余命题的证明是类似的. 设N为有限可分扩张L_1L_2/K的Galois闭包, $\mathcal{O}_N$为A在N中的整闭包, $\mathfrak{P}$为$\mathcal{O}_N$上任意一个包含$\mathfrak{p}$的素理想. 因为$\mathfrak{p}$在L_2上不分歧, 由定理5.3, 我们有$L_2 \subseteq T_\mathfrak{P}$. 另一方面, 由前面定理的证明可知, $\mathfrak{P}$在L_1上的惯性域恰好为$L_1T_\mathfrak{P}$. 因此, $L_1L_2 \subseteq L_1T_\mathfrak{P}$. 由定理5.3, 我们有$e(\mathfrak{P}_{L_1L_2}|\mathfrak{p}) = 1$. 由$\mathfrak{P}$选取的任意性, $\mathcal{O}_{L_1}$上任意包含$\mathfrak{p}$的素理想$\mathfrak{P}_{L_1}$在L_1L_2上也不分歧.

综上, 我们完成了证明. □

5.2 Frobenius自同构

设$\mathfrak{P}$为B的非零素理想, $\mathfrak{p}=\mathfrak{P}\cap A$, $\lambda=B/\mathfrak{P}$, $\kappa=A/\mathfrak{p}$. 这一节中, 我们总假定κ为有限域并且λ/κ为有限可分扩张. 如果$e(\mathfrak{P}|\mathfrak{p})=1$, 即$\mathfrak{p}$在$L$上不分歧时, 则由定理5.2, 我们有同构

$$G_{\mathfrak{P}}\cong \mathrm{Gal}\left(\lambda/\kappa\right).$$

我们给出Frobenius自同构的定义.

定义 5.3. *记号如上. 如果$e(\mathfrak{P}|\mathfrak{p})=1$, 则存在唯一的自同构$\sigma_{\mathfrak{P}}\in G_{\mathfrak{P}}$使得*

$$\sigma_{\mathfrak{P}}(x)\equiv x^{|\kappa|}\ (\mathrm{mod}\ \mathfrak{P})\ (\forall x\in B).$$

我们将其称为$\mathfrak{P}$在K上的Frobenius自同构.

关于Frobenius自同构, 我们有如下注记.

注记 5.5. (i) *定义中的条件可以修改为$\sigma_{\mathfrak{P}}\in \mathrm{Gal}(L/K)$. 这是因为 $\sigma_{\mathfrak{P}}(x)\equiv x^{|\kappa|}\ (\mathrm{mod}\ \mathfrak{P})\ (\forall x\in B)\Rightarrow \sigma_{\mathfrak{P}}\in G_{\mathfrak{P}}$.*

(ii) *$\sigma_{\mathfrak{P}}$在$\mathrm{Gal}\left(\lambda/\kappa\right)$中的像恰好为循环群$\mathrm{Gal}\left(\lambda/\kappa\right)$的生成元. 因此, $\sigma_{\mathfrak{P}}$是循环群$G_{\mathfrak{P}}$的生成元, 即$o(\sigma_{\mathfrak{P}})=f(\mathfrak{P}|\mathfrak{p})$.*

(iii) *对任意的$\tau\in\mathrm{Gal}(L/K)$, 素理想$\tau(\mathfrak{P})$在K上的Frobenius自同构为*

$$\sigma_{\tau(\mathfrak{P})}=\tau\circ\sigma_{\mathfrak{P}}\circ\tau^{-1}.$$

特别地, 当L/K为阿贝尔扩张时, $\sigma_{\mathfrak{P}}$仅与$\mathfrak{P}\cap A=\mathfrak{p}$有关. 此时, 我们将$\sigma_{\mathfrak{P}}$简记为$\sigma_{\mathfrak{p}}$.

下面我们介绍分圆域与二次域上Frobenius自同构的例子.

(1) 分圆域上的Frobenius自同构.

设$n\in\mathbb{Z}_{\geq 2}$, $\zeta_n\in\mathbb{C}$为一个本原n次单位根, 素数p满足

$$\begin{cases}\mathrm{ord}_p(n)=0 & \text{如果 } p>2,\\ \mathrm{ord}_p(n)=0,1 & \text{如果 } p=2.\end{cases}$$

则由定理4.10, p在$\mathbb{Q}(\zeta_n)$上不分歧. 此时我们断言$\mathrm{Gal}(\mathbb{Q}(\zeta_n/\mathbb{Q}))$中使得

$$\sigma_p(\zeta_n)=\zeta_n^p$$

的自同构σ_p就是Frobenius自同构. 事实上, 设$\mathfrak{p}$为$\mathbb{Z}[\zeta_n]$上一个包含p的素理想. 则对任意的

$$x = a_0 + a_1\zeta_n + \cdots + a_{m-1}\zeta_n^{m-1} \in \mathbb{Z}[\zeta_n]$$

(其中$m = \varphi(n), a_0, \cdots, a_{m-1} \in \mathbb{Z}$), 我们有

$$\begin{aligned}\sigma_p(x) &= a_0 + a_1\zeta_n^p + \cdots + a_{m-1}\zeta_n^{p(m-1)}\\ &\equiv a_0^p + a_1^p\zeta_n^p + \cdots + a_{m-1}^p\zeta_n^{p(m-1)}\\ &\equiv (a_0 + a_1\zeta_n + \cdots + a_{m-1}\zeta_n^{m-1})^p\\ &\equiv x^p \pmod{\mathfrak{p}}.\end{aligned}$$

这说明σ_p就是Frobenius自同构.

(2) 二次域上的Frobenius自同构.

设$d \neq 0, 1$为无平方因子整数. 对于奇素数$p \nmid d$, 由定理4.5, p在$\mathbb{Q}(\sqrt{d})$上不分歧. 此时, 利用定理4.5, 容易验证$\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$使得

$$\sigma_p(\sqrt{d}) = \begin{cases}\sqrt{d} & \text{如果 } (\frac{d}{p}) = 1,\\ -\sqrt{d} & \text{如果 } (\frac{d}{p}) = -1.\end{cases}$$

当$d \equiv 1 \pmod 4$且$p = 2$时, 我们知道2在$\mathbb{Q}(\sqrt{d})$不分歧. 此时容易验证

$$\sigma_2(\sqrt{d}) = \begin{cases}\sqrt{d} & \text{如果 } d \equiv 1 \pmod 8,\\ -\sqrt{d} & \text{如果 } d \equiv 5 \pmod 8.\end{cases}$$

6 Hasse-Davenport公式

首先介绍本章将要使用的记号. 设p为素数, $q=p^f(f\in\mathbb{Z}_{\geq 1})$, m为$q-1$的一个正因子. 设$\zeta_p,\zeta_{q-1},\zeta_m\in\mathbb{C}$分别为本原$p$次单位根, 本原$q-1$次单位根与本原$m$次单位根. 设$L=\mathbb{Q}(\zeta_{q-1},\zeta_p)$, $L_m=\mathbb{Q}(\zeta_m,\zeta_p)$, $K=\mathbb{Q}(\zeta_p)$, $K_{q-1}=\mathbb{Q}(\zeta_{q-1})$, $K_m=\mathbb{Q}(\zeta_m)$. 设$\mathfrak{P}$为$\mathcal{O}_L$的非零素理想且$p\in\mathfrak{P}$, 设$\mathfrak{P}_m=\mathfrak{P}\cap L_m$, $\mathfrak{p}=\mathfrak{P}\cap K$, $\mathfrak{p}_{q-1}=\mathfrak{P}\cap K_{q-1}$, $\mathfrak{p}_m=\mathfrak{P}\cap K_m$.

因为这里记号比较多, 我们用下面的图来展示这些记号.

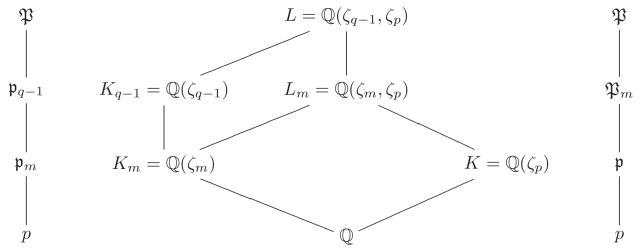

图 1: 本章中出现的分圆域与素理想

$\mathbb{F}_q$上所有乘法特征构成的循环群记作$\widehat{\mathbb{F}_q^\times}$. ε表示平方特征. 对任意的$\psi\in\widehat{\mathbb{F}_q^\times}$, 补充定义$\psi(0)=0$. 另外, $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$表示$\mathbb{F}_q\to\mathbb{F}_p$的迹映射.

6.1 Stickelberger同余式

我们首先介绍素理想$\mathfrak{P}$的Teichümuller特征. 由定理4.10, 我们有$f(\mathfrak{P}|p)=f$. 因此

$$\mathcal{O}_L/\mathfrak{P}\cong\mathbb{F}_q.$$

在本章后面的内容中, 如果没有特殊说明, 则我们总是认为$\mathcal{O}_L/\mathfrak{P}=\mathbb{F}_q$. 类似于定理4.10的证明, 容易验证同态$x\mapsto x \bmod \mathfrak{P}$为

$$U_{q-1}(\mathbb{F}_q^{\mathrm{alg}})=\mathbb{F}_q^\times=(\mathcal{O}_L/\mathfrak{P})^\times\to U_{q-1}(\mathbb{C})=\left\{x\in\mathbb{C}:\ x^{q-1}=1\right\}$$

的同构. 由此, 我们给出如下定义.

定义 6.1. 记号如上. 设$\mathbb{F}_q^\times\to U_{q-1}(\mathbb{C})$的映射$\omega_{\mathfrak{P}}$满足

$$\omega_{\mathfrak{P}}(x \bmod \mathfrak{P})\equiv x \pmod{\mathfrak{P}}\ (\forall x\in\mathcal{O}_L).$$

容易说明$\omega_{\mathfrak{P}}$为$\mathbb{F}_q$上的乘法特征. 我们将其称作素理想$\mathfrak{P}$的Teichümuller特征.

我们有如下注记.

注记 6.1. (i) 取$x_0 \in \mathcal{O}_L^\times$使得$x_0 \bmod \mathfrak{P}$为$(\mathcal{O}_L/\mathfrak{P})^\times$的生成元. 由Teichümuller特征的定义, $\omega_{\mathfrak{P}}(x_0 \bmod \mathfrak{P})$为一个本原$(q-1)$次单位根. 因此, $o(\omega_{\mathfrak{P}}) = q-1$, 即$\omega_{\mathfrak{P}}$为$\widehat{\mathbb{F}_q^\times}$的一个生成元.

(ii) 我们将在后面的内容中用*p-adic*的语言重新介绍Teichümuller特征.

下面我们将利用前面5章的内容来证明经典的Stickelberger同余式(在后面的章节中, 我们将会用Gross-Koblitz公式给出一个简单的证明). 我们从下面的引理开始.

引理 6.1. 记号如上. 对任意的$0 \leq a, b \leq q-2$, 我们有同余式

$$J_q(\omega_{\mathfrak{P}}^{-a}, \omega_{\mathfrak{P}}^{-b}) \equiv -\binom{a+b}{a} \equiv -\frac{(a+b)!}{a!b!} \pmod{\mathfrak{P}}.$$

特别地, 当$a+b \geq q$时,

$$J_q(\omega_{\mathfrak{P}}^{-a}, \omega_{\mathfrak{P}}^{-b}) \equiv 0 \pmod{\mathfrak{P}}.$$

证明: 由Teichümuller特征的定义, 容易验证

$$\begin{aligned} J_q(\omega_{\mathfrak{P}}^{-a}, \omega_{\mathfrak{P}}^{-b}) \bmod \mathfrak{P} &= \sum_{x \in \mathbb{F}_q} \omega_{\mathfrak{P}}^{q-1-a}(x)\omega_{\mathfrak{P}}^{q-1-b}(1-x) \bmod \mathfrak{P} \\ &= \sum_{x \in \mathbb{F}_q} x^{q-1-a}(1-x)^{q-1-b} \\ &= \sum_{x \in \mathbb{F}_q} x^{q-1-a} \sum_{r=0}^{q-1-b} \binom{q-1-b}{r} (-1)^r x^r \\ &= \sum_{r=0}^{q-1-b} \binom{q-1-b}{r} (-1)^r \sum_{x \in \mathbb{F}_q^\times} x^{q-1-a+r}. \end{aligned} \tag{6.1}$$

注意到

$$\sum_{x \in \mathbb{F}_q^\times} x^{q-1-a+r} = \begin{cases} 0 & \text{如果 } r \not\equiv a \pmod{(q-1)\mathbb{Z}}, \\ -1 & \text{如果 } r \equiv a \pmod{(q-1)\mathbb{Z}}, \end{cases}$$

以及$0 \leq a, b \leq q-2$. 因此当$a \notin [0, q-1-b]$时, 即$a+b \geq q$时, 由(6.1),

$$J_q(\omega_{\mathfrak{P}}^{-a}, \omega_{\mathfrak{P}}^{-b}) \equiv 0 \pmod{\mathfrak{P}}.$$

当$a \in [0, q-1-b]$时, 再由(6.1), 我们得到

$$J_q(\omega_{\mathfrak{P}}^{-a}, \omega_{\mathfrak{P}}^{-b}) \equiv (-1)^{a+1}\binom{q-1-b}{a} \equiv -\binom{a+b}{a} \pmod{\mathfrak{P}},$$

其中最后一个同余式成立是因为

$$(-1)^{a+1}\binom{q-1-b}{a} = (-1)^{a+1}\frac{(q-1-b)(q-2-b)\cdots(q-a-b)}{a!}$$
$$\equiv -\binom{a+b}{a} \pmod{p\mathbb{Z}}.$$

综上, 我们完成了证明. □

下面我们介绍两个非常重要的定义. 在介绍p-adic分析的内容时, 我们还会遇到它们.

定义 6.2. 设$0 \leq r' \leq q-2$为整数, r'的p进展开为

$$r' = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1},$$

其中$0 \leq a_0, \cdots, a_{f-1} \leq p-1$. 定义

$$s(r') := \sum_{i=0}^{f-1} a_i,$$

以及

$$t(r') := \prod_{i=0}^{f-1} (a_i!)\,.$$

对于一般的整数r, 设r'为r模$q-1$的最小非负剩余. 我们定义 $s(r) := s(r')$以及$t(r) = t(r')$.

下面我们介绍经典的Stickelberger同余式.

定理 6.1. 对任意的整数r, 考虑$\mathbb{F}_q$上的*Gauss*和

$$G_q(\omega_{\mathfrak{P}}^{-r}) := \sum_{x\in\mathbb{F}_q} \omega_{\mathfrak{P}}(x)^{-r}\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}.$$

则

$$\frac{G_q(\omega_{\mathfrak{P}})}{(\zeta_p-1)^{s(r)}} \equiv -\frac{1}{t(r)} \pmod{\mathfrak{P}(\mathcal{O}_L)_{\mathfrak{P}}}.$$

证明: 由$s(r)$与$t(r)$的定义, 在下面的证明中仅需考虑$0 \leq r \leq q-2$的情形. 下面对$s(r)$进行归纳. 当$s(r) = 0$, 即$r = 0$时, 利用$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$为$\mathbb{F}_q \to \mathbb{F}_p$的满同

态, 容易验证

$$\begin{aligned}\sum_{x\in\mathbb{F}_q}\varepsilon(x)\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)} &= -1+\sum_{x\in\mathbb{F}_q}\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}\\ &= -1+\sum_{x\in\mathbb{F}_p}|\mathrm{Ker}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}|\cdot\zeta_p^x\\ &= -1\\ &= G_q(\varepsilon).\end{aligned}$$

因此当$s(r)=0$时, 结论成立. 当$s(r)=1$, 即$r=p^j$ $(0\leq j\leq f-1)$时, 因为$\omega_{\mathfrak{P}}^{-p^j}\neq\varepsilon$, 我们有

$$\begin{aligned}G_q(\omega_{\mathfrak{P}}^{-p^j}) &= \sum_{x\in\mathbb{F}_q}\omega_{\mathfrak{P}}(x)^{-p^j}\left(\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}-1\right)+\sum_{x\in\mathbb{F}_q}\omega_{\mathfrak{P}}(x)^{-p^j}\\ &= \sum_{x\in\mathbb{F}_q}\omega_{\mathfrak{P}}(x)^{-p^j}\left(\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}-1\right)\end{aligned}$$

由此, 容易验证

$$\begin{aligned}\frac{G_q(\omega_{\mathfrak{P}}^{-r})}{\zeta_p-1}\ \mathrm{mod}\ \mathfrak{P}(\mathcal{O}_L)_{\mathfrak{P}} &= \sum_{x\in\mathbb{F}_q\setminus\mathrm{Ker}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}}\omega_{\mathfrak{P}}^{-p^j}(x)\left(\frac{\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}-1}{\zeta_p-1}\right)\ \mathrm{mod}\ \mathfrak{P}(\mathcal{O}_L)_{\mathfrak{P}}\\ &= \sum_{x\in\mathbb{F}_q\setminus\mathrm{Ker}\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}}x^{-p^j}\cdot\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)\\ &= \sum_{x\in\mathbb{F}_q^\times}x^{-p^j}\left(x+x^p+\cdots+x^{p^{f-1}}\right)\\ &= -1\\ &= -\frac{1}{t(r)}\ \mathrm{mod}\ \mathfrak{P}(\mathcal{O}_L)_{\mathfrak{P}}.\end{aligned}$$

因此当$s(r)=1$时, 结论成立. 下面设$s(r)\geq 2$, 并且假设当$s(r')<s(r)$时结论对r'成立. 下面分两种情况讨论.

情况1. $r\not\equiv 0\ (\mathrm{mod}\ p\mathbb{Z})$. 注意此时$s(r-1)=s(r)-1$, 且$\omega_{\mathfrak{P}}^{-r}\neq\varepsilon$. 则由Gauss和与Jacobi和的转换公式,

$$\frac{G_q(\omega_{\mathfrak{P}}^{-r})}{(\zeta_p-1)^{s(r)}}=\frac{G_q(\omega_{\mathfrak{P}}^{-(r-1)})\cdot G_q(\omega_{\mathfrak{P}}^{-1})}{J_q(\omega_{\mathfrak{P}}^{-(r-1)},\omega_{\mathfrak{P}}^{-1})\cdot(\zeta_p-1)^{s(r-1)}\cdot(\zeta_p-1)}.\tag{6.2}$$

设r的p进展开为

$$a_0+a_1p+\cdots+a_{f-1}p^{f-1},$$

其中$0 \leq a_0, \cdots, a_{f-1} \leq p-1$且$a_0 \neq 0$. 则由引理6.1,

$$J_q(\omega_{\mathfrak{P}}^{-(r-1)}, \omega_{\mathfrak{P}}^{-1}) \equiv -\binom{r}{1} \equiv -r \equiv -a_0 \pmod{\mathfrak{P}}. \tag{6.3}$$

因此, $J_q(\omega_{\mathfrak{P}}^{-(r-1)}, \omega_{\mathfrak{P}}^{-1}) \in (\mathcal{O}_L)_{\mathfrak{P}}^{\times}$. 由(6.2),(6.3)以及归纳假设, 我们得到

$$\frac{G_q(\omega_{\mathfrak{P}}^{-r})}{(\zeta_p-1)^{s(r)}} \equiv -\frac{1}{a_0 \cdot t(r-1) \cdot t(1)} \equiv -\frac{1}{t(r)} \pmod{\mathfrak{P}(\mathcal{O}_L)_{\mathfrak{P}}}.$$

情况2. $r \equiv 0 \pmod{p\mathbb{Z}}$. 此时不妨设$r = pr_0$. 则此时

$$\begin{aligned} G_q(\omega_{\mathfrak{P}}^{-r}) &= \sum_{x \in \mathbb{F}_q} \omega_{\mathfrak{P}}^{-r_0 p}(x) \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)} \\ &= \sum_{x \in \mathbb{F}_q} \omega_{\mathfrak{P}}^{-r_0}(x^p) \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x^p)} \\ &= \sum_{x \in \mathbb{F}_q} \omega_{\mathfrak{P}}^{-r_0}(x) \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)} \\ &= G_q(\omega_{\mathfrak{P}}^{-r_0}). \end{aligned}$$

由此并注意到$s(r) = s(r_0), t(r) = t(r_0)$, 我们有

$$\frac{G_q(\omega_{\mathfrak{P}}^{-r})}{(\zeta_p-1)^{s(r)}} = \frac{G_q(\omega_{\mathfrak{P}}^{-r_0})}{(\zeta_p-1)^{s(r_0)}}.$$

设$r' = \frac{r}{p^{\mathrm{ord}_p(r)}}$. 重复上面的操作, 最终可以得到

$$\frac{G_q(\omega_{\mathfrak{P}}^{-r})}{(\zeta_p-1)^{s(r)}} = \frac{G_q(\omega_{\mathfrak{P}}^{-r'})}{(\zeta_p-1)^{s(r')}}. \tag{6.4}$$

利用(6.4), 我们可以回到情况1.

综上, 我们完成了证明. □

注记 6.2. (i) 由引理*4.5*与定理*4.10*, 我们知道p在$\mathbb{Q}(\zeta_{q-1})$不分歧, 在$\mathbb{Q}(\zeta_p)$上完全分歧, 并且$(\zeta_p-1)\mathbb{Z}[\zeta_p]$是$\mathbb{Z}[\zeta_p]$上唯一包含$p$的素理想. 在由推论*5.2*, $\mathbb{Z}[\zeta_p]$上的素理想$(\zeta_p-1)\mathbb{Z}[\zeta_p]$在$\mathcal{O}_L$不分歧. 由此与定理*6.1*, 我们得到

$$\mathrm{ord}_{\mathfrak{P}}\left(G_q(\omega_{\mathfrak{P}}^{-r})\right) = s(r) \cdot \mathrm{ord}_{\mathfrak{P}}\left(\zeta_p - 1\right) = s(r).$$

(ii) 注意到当$\psi \in \widehat{\mathbb{F}_q^{\times}}$为非平凡特征时,

$$G_q(\psi) \cdot \overline{G_q(\psi)} = q = p^f.$$

因此, 出现在理想$G_q(\psi)\mathcal{O}_L$分解式中的素理想一定包含素数p.

6.2 乘积公式与提升公式

在本节中继续使用上一节的记号, 并且对任意的实数x, 记号$\{x\}$表示x的小数部分.

我们将利用前5章的结论来证明经典的Hasse-Davenport乘积公式与提升公式(在后面的章节中, 我们将会用Gross-Koblitz公式给出一个简单的证明). 我们从下面的引理开始.

引理 6.2. *对任意的整数r, 我们有*

$$s(r) = (p-1) \cdot \sum_{0 \leq i \leq f-1} \left\{ \frac{p^i r}{q-1} \right\}. \tag{6.5}$$

当$0 \leq r \leq q-2$时,

$$t(r) \equiv \frac{r!}{(-p)^{\mathrm{ord}_p(r!)}} \pmod{p\mathbb{Z}}.$$

证明: 注意到(6.5)两边均为周期为$q-1$的函数. 因此仅需考虑$0 \leq r \leq q-2$的情形. 设r的p进展开为

$$r = a_0 + a_1 p + \cdots + a_{f-1} p^{f-1},$$

其中$0 \leq a_0, \cdots, a_{f-1} \leq p-1$. 注意到$p^f \equiv 1 \pmod{(q-1)\mathbb{Z}}$. 因此, 对任意的$1 \leq i \leq f-1$,

$$p^i r = a_0 p^i + a_1 p^{i+1} + \cdots + a_{f-1-i} p^{f-1} + a_{f-i} p^f + \cdots + a_{f-1} p^{f-1+i}$$

模$(q-1)$的最小非负剩余为

$$a_0 p^i + a_1 p^{i+1} + \cdots + a_{f-1-i} p^{f-1} + a_{f-i} + a_{f-i+1} p \cdots + a_{f-1} p^{i-1}.$$

当$i = 0$时, $p^i r$模$(q-1)$的最小非负剩余恰好为r. 由上面的讨论, 我们得到

$$(p-1) \cdot \sum_{0 \leq i \leq f-1} \left\{ \frac{p^i r}{q-1} \right\} = \frac{p-1}{q-1} \sum_{0 \leq i \leq f-1} a_i \sum_{0 \leq j \leq f-1} p^j = s(r).$$

下面来考虑$t(r)$的同余式. 对r进行归纳. 当$r = 0$时结论显然成立. 设$1 \leq r \leq q-2$, 并假设结论对任意的$0 \leq r' < r$均成立. 我们分两种情况讨论.

情况1. $r \not\equiv 0 \pmod{p\mathbb{Z}}$. 此时, r的p进展开为

$$r = a_0 + a_1 p + \cdots + a_{f-1} p^{f-1},$$

其中$0 \leq a_0, \cdots, a_{f-1} \leq p-1$且$a_0 \neq 0$. 因此, $r-1$的p进展开为

$$r-1 = (a_0 - 1) + a_1 p + \cdots + a_{f-1} p^{f-1}.$$

则由归纳假设以及$r \equiv a_0 \neq 0 \pmod{p\mathbb{Z}}$, 我们得到

$$\begin{aligned} t(r) = \prod_{i=0}^{f-1} (a_i!) &= a_0 \cdot t(r-1) \\ &\equiv r \cdot \frac{(r-1)!}{(-p)^{\mathrm{ord}_p((r-1)!)}} \\ &\equiv \frac{r!}{(-p)^{\mathrm{ord}_p(r!)}} \pmod{p\mathbb{Z}}. \end{aligned}$$

情况2. $r \equiv 0 \pmod{p\mathbb{Z}}$. 设$r = pr_0$. 注意到$t(r) = t(r_0)$. 由归纳假设, 容易验证

$$\begin{aligned} \frac{r!}{(-p)^{\mathrm{ord}_p(r!)}} &= (-1)^{r_0 + \mathrm{ord}_p(r_0!)} \frac{(pr_0)!}{p^{r_0 + \mathrm{ord}_p(r_0!)}} \\ &\equiv (-1)^{r_0 + \mathrm{ord}_p(r_0!)} \cdot ((p-1)!)^{r_0} \cdot \frac{r_0!}{p^{\mathrm{ord}_p(r_0!)}} \\ &\equiv \frac{r_0!}{(-p)^{\mathrm{ord}_p(r_0!)}} \\ &\equiv t(r_0) \\ &\equiv t(r) \pmod{p\mathbb{Z}}. \end{aligned}$$

综上, 我们完成了证明. □

引理 6.3. 设$k \in \mathbb{Z}$, $m \in \mathbb{Z}^+$并且$\gcd(k, a) = 1$. 则对任意的$z \in \mathbb{R}$,

$$\sum_{a \in \mathbb{Z}/m\mathbb{Z}} \left\{ \frac{ka + z}{m} \right\} = \frac{m-1}{2} + \{z\}.$$

证明: 因为$\gcd(k, a) = 1$, 我们容易验证

$$\begin{aligned} \sum_{a \in \mathbb{Z}/m\mathbb{Z}} \left\{ \frac{ka + z}{m} \right\} &= \sum_{a \in \mathbb{Z}/m\mathbb{Z}} \left\{ \frac{ka + \lfloor z \rfloor + \{z\}}{m} \right\} \\ &= \sum_{0 \leq a \leq m-1} \frac{a + \{z\}}{m} \\ &= \frac{m-1}{2} + \{z\}. \end{aligned}$$

综上, 我们完成了证明. □

下面的引理是我们证明乘积公式与提升公式的核心.

引理 6.4. 设$m \in \mathbb{Z}^+$为$q-1$的因子, $d=(q-1)/m$. 则对任意的$b \in \mathbb{Z}$, 下列命题成立.

(i)
$$\sum_{a=0}^{m-1} s(da+b) - \sum_{a=0}^{m-1} s(da) = s(mb),$$
并且
$$\sum_{a=0}^{m-1} s(da) = (p-1)(m-1)f/2.$$

(ii)
$$\frac{m^{mb} \cdot \prod_{0\leq a\leq m-1} t(da+b)}{t(mb)\prod_{0\leq a\leq m-1} t(da)} \equiv 1 \pmod{p\mathbb{Z}_p}.$$

证明: (i) 由引理6.2与引理6.3, 容易验证
$$\begin{aligned}
\sum_{a=0}^{m-1} s(da+b) &= \sum_{a=0}^{m-1}(p-1)\sum_{i=0}^{f-1}\left\{\frac{p^i(da+b)}{q-1}\right\} \\
&= \sum_{i=0}^{f-1}(p-1)\sum_{a=0}^{m-1}\left\{\frac{p^ia+p^ib/d}{m}\right\} \\
&= \sum_{i=0}^{f-1}(p-1)\left(\frac{m-1}{2}+\left\{\frac{p^ib}{d}\right\}\right) \\
&= \frac{(p-1)(m-1)f}{2} + \sum_{i=0}^{f-1}(p-1)\left\{\frac{p^imb}{q-1}\right\} \\
&= \frac{(p-1)(m-1)f}{2} + s(mb).
\end{aligned}$$

令$b=0$, 由上式得到
$$\sum_{a=0}^{m-1} s(da) = (p-1)(m-1)f/2,$$
并且
$$\sum_{a=0}^{m-1} s(da+b) - \sum_{a=0}^{m-1} s(da) = s(mb).$$
因此(i)成立.

(ii) 由$t(r)$的定义, 不妨设$0 \leq b \leq d-1$. 下面对b归纳. 当$b=0$时, 结论显然成立. 设$1 \leq b \leq q-1$且结论对$b-1$成立. 设
$$F(b) = \frac{m^{mb} \cdot \prod_{0\leq a\leq m-1} t(da+b)}{t(mb)\prod_{0\leq a\leq m-1} t(da)}.$$

注意到$F(b), F(b-1) \in \mathbb{Z}_p^\times$, 由引理6.2我们得到

$$\begin{aligned}\frac{F(b)}{F(b-1)} &= \frac{m^m \cdot t(mb-m)}{t(mb)} \prod_{0\leq a\leq m-1} \frac{t(da+b)}{t(da+b-1)} \\ &\equiv \frac{m^m \cdot (mb-m)!}{(mb)!} \prod_{0\leq a\leq m-1} (da+b) \\ &\equiv \prod_{0\leq a\leq m-1} \frac{mb-a+q}{mb-a} \pmod{p\mathbb{Z}_p}. \end{aligned} \tag{6.6}$$

因为$1 \leq mb-a \leq q-1 = p^f - 1$, 我们有$\mathrm{ord}_p(mb-a) < \mathrm{ord}_p(q) = f$. 因此$\mathrm{ord}_p(mb-a) = \mathrm{ord}_p(mb-a+q)$. 注意到$mb-a \equiv mb-a+q \pmod{p\mathbb{Z}}$. 由上面的讨论, 我们得到$\frac{mb-a+q}{mb-a} \in \mathbb{Z}_p^\times$并且

$$\frac{mb-a+q}{mb-a} \equiv 1 \pmod{p\mathbb{Z}_p}.$$

由此, (6.6)与归纳假设, 我们得到

$$\frac{m^{mb} \cdot \prod_{0\leq a\leq m-1} t(da+b)}{t(mb)\prod_{0\leq a\leq m-1} t(da)} \equiv 1 \pmod{p\mathbb{Z}_p}.$$

因此(ii)成立.

综上, 我们完成了证明. □

下面我们来介绍Hasse-Davenport乘积公式.

定理 6.2. *设非平凡特征$\rho \in \widehat{\mathbb{F}_q^\times}$且$o(\rho) = m > 1$. 则对任意的$\psi \in \widehat{\mathbb{F}_q^\times}$,*

$$\prod_{a=0}^{m-1} G_q(\psi\rho^a) = -\psi^{-m}(m) \cdot G_q(\psi^m) \cdot \prod_{a=0}^{m-1} G_q(\rho^a).$$

证明: 这里我们仅讨论$\mathrm{char}(\mathbb{F}_q) = p > 2$的情况. 首先, 当$\psi \in \{\rho^k : k \in \mathbb{Z}\}$时结论显然成立. 下面假设$\psi \notin \{\rho^k : k \in \mathbb{Z}\}$. 令

$$x = \frac{-\psi^m(m)}{G_q(\psi^m)} \cdot \prod_{a=0}^{m-1} \frac{G_q(\psi\rho^a)}{G_q(\rho^a)} \in L = \mathbb{Q}(\zeta_{q-1}, \zeta_p).$$

要证明该定理, 仅需证明$x = 1$.

我们首先证明$x \in \mathcal{O}_L^\times$. 为此仅需说明对$\mathcal{O}_L$的任意非零素理想$\mathfrak{P}$, 都有$\mathrm{ord}_{\mathfrak{P}}(x) = 0$. 由注记6.2(ii), 仅需说明对$\mathcal{O}_L$上所有包含素数$p$的素理想$\mathfrak{P}$, 都有$\mathrm{ord}_{\mathfrak{P}}(x) = 0$. 设$p \in \mathfrak{P}$为$\mathcal{O}_L$上的素理想. 暂时将$\mathbb{F}_q$与$\mathcal{O}_L/\mathfrak{P}$等同起来. 由注记6.1, 素理想$\mathfrak{P}$的Teichümuller特征$\omega_{\mathfrak{P}}$为$\widehat{\mathbb{F}_q^\times}$的生成元. 因此不妨设$\psi =$

$\omega_{\mathfrak{P}}^{-b}, \rho = \omega_{\mathfrak{P}}^{-dr}$, 其中$d = (q-1)/m, r \in \mathbb{Z}$且$\gcd(r, m) = 1$. 则由注记6.2(i)与引理6.4(i), 我们有

$$\begin{aligned}\mathrm{ord}_{\mathfrak{P}}(x) &= \sum_{a=0}^{m-1} s(dra + b) - \sum_{a=0}^{m-1} s(dra) - s(mb)\\ &= \sum_{a=0}^{m-1} s(da + b) - \sum_{a=0}^{m-1} s(da) - s(mb)\\ &= 0.\end{aligned}$$

由此, $x \in \mathcal{O}_L^{\times}$.

下面我们再证明$x \in U_{q-1}(\mathbb{C})$. 事实上, 因为$\psi \notin \{\rho^k : k \in \mathbb{Z}\}$且$\rho \neq \varepsilon$, 利用Gauss和与Jacobi和的转换公式, 我们得到

$$\begin{aligned}x &= \frac{-\psi^m(m) \cdot J_q(\psi, \psi\rho, \cdots, \psi\rho^{m-1}) \cdot G_q(\psi^m \rho^{m(m-1)/2})}{-J_q(\psi^m, \rho, \cdots, \rho^{m-1}) \cdot G_q(\psi^m \rho^{m(m-1)/2})}\\ &= \frac{\psi^m(m) \cdot J_q(\psi, \psi\rho, \cdots, \psi\rho^{m-1})}{J_q(\psi^m, \rho, \cdots, \rho^{m-1})} \in \mathbb{Q}(\zeta_{q-1}) \cap \mathcal{O}_L = \mathbb{Z}[\zeta_{q-1}].\end{aligned}$$

对任意的$\sigma_s \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})$, 其中$\gcd(s, q-1) = 1$且$\sigma_s(\zeta_{q-1}) = \zeta_{q-1}^s$, 容易验证

$$\sigma_s(x) = \frac{\psi^{sm}(m) \cdot J_q(\psi^s, \psi^s\rho^s, \cdots, \psi^s\rho^{s(m-1)})}{J_q(\psi^{sm}, \rho, \cdots, \rho^{s(m-1)})}.$$

注意到上式分子与分母出现的Jacobi和中的特征均为非平凡特征, 并且它们的乘积也均不是平凡特征. 由此,

$$|\sigma_s(x)| = \frac{\sqrt{q}}{\sqrt{q}} = 1.$$

这说明

$$x \in X = \{y \in \mathbb{Z}[\zeta_{q-1}] : |\sigma(y)| = 1 \ \forall \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q})\}.$$

设X中任意元素y在$\mathbb{Q}$上的极小多项式为$p_y(t) \in \mathbb{Z}[t]$. 利用根与系数的关系, 我们得到$\deg(p_y(t)) \leq \varphi(q-1)$并且$p_y(t)$中$t^i$的系数的绝对值小于等于$\binom{\varphi(q-1)}{i}$. 因为$y \in \mathbb{Z}[\zeta_{q-1}]$, 上面的讨论说明

$$|\{p_y(t) : y \in X\}| < \infty.$$

由此, X是有限集. 注意到$x, x^2, x^3, \cdots, x^k, \cdots \in X$. 因此, 一定存在$1 \leq i < j$使得$x^i = x^j$. 又因为$x \neq 0$, 上式说明$x \in \mathbb{Q}(\zeta_{q-1})$是一个单位根. 因为$q-1 \equiv 0 \pmod 2$, 由定理4.7, 我们有$x \in U_{q-1}(\mathbb{C})$.

最后, 我们来说明$x=1$. 固定$\mathcal{O}_L$上的一个素理想$\mathfrak{P}$使得$p\in\mathfrak{P}$. 注意到同态$x\mapsto x \bmod \mathfrak{P}$是$U_{q-1}(\mathbb{C})\to U_{q-1}(\mathbb{F}_q)$的同构(这里我们将$\mathcal{O}_L/\mathfrak{P}$等同于$\mathbb{F}_q$). 因此, 要说明$x=1$, 我们仅需证明$x\equiv 1 \pmod{\mathfrak{P}}$. 设$\psi=\omega_{\mathfrak{P}}^{-b},\rho=\omega_{\mathfrak{P}}^{-dr}$, 其中$d=(q-1)/m, r\in\mathbb{Z}$且$\gcd(r,m)=1$. 则由定理6.1, 引理6.4并注意到$x\in\mathcal{O}_L^\times$, 我们有

$$\begin{aligned} x &= \frac{-\omega_{\mathfrak{P}}^{-bm}(m)}{G_q(\omega_{\mathfrak{P}}^{-bm})}\cdot\prod_{a=0}^{m-1}\frac{G_q(\omega_{\mathfrak{P}}^{-dra-b})}{G_q(\omega_{\mathfrak{P}}^{-dra})}\\ &\equiv \frac{t(mb)}{m^{mb}}\cdot\prod_{a=0}^{m-1}\frac{t(dra)}{t(dra+b)}\\ &\equiv \frac{t(mb)}{m^{mb}}\cdot\prod_{a=0}^{m-1}\frac{t(da)}{t(da+b)}\\ &\equiv 1 \pmod{\mathfrak{P}}. \end{aligned}$$

综上, 我们完成了证明. □

为了叙述提升定理, 我们给出如下定义.

定义 6.3. 设$n\in\mathbb{Z}^+$. 对任意$\psi\in\widehat{\mathbb{F}_q^\times}$, 定义$\psi_{(n)}\in\widehat{\mathbb{F}_{q^n}^\times}$为

$$\psi_{(n)}=\psi\circ \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}.$$

注记 6.3. 对任意$\psi\in\widehat{\mathbb{F}_q^\times}$, 容易说明

$$\psi\text{为平凡特征}\Leftrightarrow\psi_{(n)}\text{为平凡特征}.$$

事实上, "⇒"显然成立. 对于" ⇐ ", 注意到$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$为$\mathbb{F}_{q^n}\to\mathbb{F}_q$的满射, 我们容易说明充分性也成立.

下面我们介绍Hasse-Davenport提升公式.

定理 6.3. 设$n\in\mathbb{Z}^+$. 对任意$\psi\in\widehat{\mathbb{F}_q^\times}$, 我们有

$$G_q(\psi)^n=(-1)^{n-1}\cdot G_{q^n}(\psi_{(n)}).$$

证明: 我们仅考虑$\mathrm{char}(\mathbb{F}_q)=p>2$的情形. 令

$$x=\frac{(-1)^{n-1}\cdot G_q(\psi)^n}{G_{q^n}(\psi_{(n)})}\in L.$$

为了证明该定理, 仅需说明$x=1$.

我们先证明$x \in \mathcal{O}_L^\times$. 设$L_{(n)} = \mathbb{Q}(\zeta_{q^n-1}, \zeta_p)$. 类似于定理6.2的证明, 要说明$x \in \mathcal{O}_L^\times$, 仅需说明对$\mathcal{O}_{L_{(n)}}$上任意包含$p$的素理想$\mathfrak{P}_{(n)}$, 都有$\mathrm{ord}_{\mathfrak{P}_{(n)}}(x) = 0$. 为了区分记号$s(r)$, 对于$q^n-1$, 我们用记号$s_{(n)}(r)$, 并且设$\mathfrak{P} = \mathfrak{P}_{(n)} \cap \mathcal{O}_L$. 此时, 对于$\mathfrak{P}_{(n)}$的Teichümuller特征$\omega_{\mathfrak{P}_{(n)}}$, 容易验证

$$\omega_{\mathfrak{P}_{(n)}}|_{\mathbb{F}_q} = \omega_{\mathfrak{P}},$$

这里我们认为

$$\mathbb{F}_q = \mathcal{O}_L/\mathfrak{P} \subseteq \mathcal{O}_{L_{(n)}}/\mathfrak{P}_{(n)} = \mathbb{F}_{q^n}.$$

设$\psi = \omega_{\mathfrak{P}}^{-b} = \omega_{\mathfrak{P}_{(n)}}^{-b}|_{\mathbb{F}_q}$, 其中$(0 \leq b \leq q-2)$. 则

$$\begin{aligned}
G_{q^n}(\psi_{(n)}) &= \sum_{x \in \mathbb{F}_{q^n}} \psi_{(n)}(x)\zeta_p^{\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(x)} \\
&= \sum_{x \in \mathbb{F}_{q^n}} \psi\left(x^{\frac{q^n-1}{q-1}}\right)\zeta_p^{\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(x)} \\
&= \sum_{x \in \mathbb{F}_{q^n}} \omega_{\mathfrak{P}_{(n)}}^{-b}\left(x^{\frac{q^n-1}{q-1}}\right)\zeta_p^{\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(x)} \\
&= \sum_{x \in \mathbb{F}_{q^n}} \omega_{\mathfrak{P}_{(n)}}^{-b\frac{q^n-1}{q-1}}(x)\zeta_p^{\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(x)} \\
&= G_{q^n}\left(\omega_{\mathfrak{P}_{(n)}}^{-b\frac{q^n-1}{q-1}}\right).
\end{aligned}$$

注意到$e(\mathfrak{P}_{(n)}|\mathfrak{P}) = 1$. 则由注记6.2以及上面的讨论, 我们得到

$$\begin{aligned}
\mathrm{ord}_{\mathfrak{P}_{(n)}}(x) &= \mathrm{ord}_{\mathfrak{P}}\left(G_q(\psi)^n\right) - \mathrm{ord}_{\mathfrak{P}_{(n)}}\left(G_{q^n}(\psi_{(n)})\right) \\
&= n \cdot s(b) - s_{(n)}\left(b \cdot \frac{q^n-1}{q-1}\right).
\end{aligned} \tag{6.7}$$

因为$0 \leq b \leq q-2$, 我们有

$$s_{(n)}\left(b \cdot \frac{q^n-1}{q-1}\right) = s_{(n)}\left(b + bq + \cdots + bq^{n-1}\right) = n \cdot s(b).$$

由此与(6.7), 我们有$\mathrm{ord}_{\mathfrak{P}_{(n)}}(x) = 0$. 因此$x \in \mathcal{O}_L^\times$.

下面我们证明$x \in U_{q-1}(\mathbb{C})$. 事实上, 对任意的$\sigma_s \in \mathrm{Gal}(L/\mathbb{Q}(\zeta_{q-1})) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, 其中$s \in \mathbb{F}_p^\times$并且$\sigma_s(\zeta_{q-1}) = \zeta_{q-1}$, $\sigma_s(\zeta_p) = \zeta_p^s$, 我们有

$$\sigma_s(x) = x \cdot \frac{\psi(s^{-1})^n}{\psi_{(n)}(s^{-1})} = x.$$

因此, 由Galois对应, $x \in \mathbb{Q}(\zeta_{q-1})$. 另一方面, 对任意的$\tau_r \in \mathrm{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$, 其中$r \in (\mathbb{Z}/(q-1)\mathbb{Z})^\times$并且$\tau_r(\zeta_{q-1}) = \zeta_{q-1}^r$, $\tau_r(\zeta_p) = \zeta_p$, 由注记6.3, 我们有

$$|\tau_r(x)| = \frac{|G_q(\psi^r)|^n}{\left|G_{q^n}(\psi_{(n)}^r)\right|} = 1.$$

因此, 利用与定理6.2证明中类似的方法并注意到$q-1 \equiv 0 \pmod 2$, 容易说明$x \in U_{q-1}(\mathbb{C})$.

最后我们来说明$x = 1$. 固定$\mathcal{O}_{L_{(n)}}$上一个包含p的素理想$\mathfrak{P}_{(n)}$. 类似于定理6.2的证明, 仅需说明$x \equiv 1 \pmod{\mathfrak{P}_{(n)}}$. 为了区分记号$t(r)$, 对于$q^n-1$, 我们用记号$t_{(n)}(r)$. 设$\psi = \omega_{\mathfrak{P}}^{-b} = \omega_{\mathfrak{P}_{(n)}}^{-b}|_{\mathbb{F}_q}$, 其中$0 \leq b \leq q-2$. 则由上面的讨论, 我们知道

$$G_{q^n}(\psi_{(n)}) = G_{q^n}\left(\omega_{\mathfrak{P}_{(n)}}^{-b\frac{q^n-1}{q-1}}\right).$$

由此以及定理6.1, 并注意到$x \in \mathcal{O}_L^\times$, 我们有

$$\begin{aligned} x &= (-1)^{n-1} \cdot \frac{G_q\left(\omega_{\mathfrak{P}}^{-b}\right)^n}{G_{q^n}\left(\omega_{\mathfrak{P}_{(n)}}^{-b\frac{q^n-1}{q-1}}\right)} \\ &\equiv \frac{t_{(n)}\left(b \cdot \frac{q^n-1}{q-1}\right)}{t(b)^n} \\ &\equiv 1 \pmod{\mathfrak{P}_{(n)}}. \end{aligned}$$

综上, 我们完成了证明. □

设素数$p > 2$, Gauss首先证明了二次Gauss和

$$\sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) e^{2\pi \mathbf{i}/p} = \begin{cases} \sqrt{p} & \text{如果 } p \equiv 1 \pmod 4, \\ \mathbf{i}\sqrt{p} & \text{如果 } p \equiv 3 \pmod 4. \end{cases}$$

由注记6.3, 对任意的$n \in \mathbb{Z}^+$, 特征

$$\phi := \left(\frac{\cdot}{p}\right)_{(n)} = \left(\frac{\cdot}{p}\right) \circ \mathrm{N}_{\mathbb{F}_{p^n}/\mathbb{F}_p}$$

是$\mathbb{F}_{p^n}$上唯一的二次乘法特征. 由定理6.3, 我们可以得到一般有限域上二次Gauss和的精确值.

推论 6.1. 记号如上. 则

$$\sum_{x \in \mathbb{F}_{p^n}} \phi(x) e^{2\pi \mathbf{i} \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(x)/p} = \begin{cases} (-1)^{n-1}\sqrt{q} & \text{如果 } q \equiv 1 \pmod 4, \\ (-1)^{n-1}\mathbf{i}^n\sqrt{q} & \text{如果 } q \equiv 3 \pmod 4. \end{cases}$$

7 赋值域

7.1 赋值的基本性质

我们首先给出赋值的定义.

定义 7.1. 设K为域. 如果函数$|\cdot|: K \to \mathbb{R}$满足以下三条性质:

(i) 对任意的$x \in K$都有$|x| \geq 0$, 并且$|x| = 0 \Leftrightarrow x = 0$,

(ii) 对任意的$x, y \in K$都有$|xy| = |x||y|$,

(iii) 对任意的$x, y \in K$, 三角不等式成立, 即

$$|x + y| \leq |x| + |y|,$$

则我们称$|\cdot|$为域K上的一个赋值.

关于赋值我们有如下注记.

注记 7.1. (i) 定义函数$|\cdot|_0: K \to \mathbb{R}$为

$$|x|_0 = \begin{cases} 1 & \text{如果 } x \neq 0, \\ 0 & \text{如果 } x = 0. \end{cases}$$

由赋值的定义, $|\cdot|_0$为域K上的一个赋值. 我们将其称作平凡赋值. **在本讲义中, 如果没有特殊说明, 则默认讨论的赋值均为非平凡赋值.**

(ii) 设$|\cdot|$为K上的一个赋值. 定义K上的距离为

$$d(x, y) := |x - y| \ (\forall x, y \in K).$$

则K在此距离决定的拓扑下成为了一个拓扑域, 记作$(K, |\cdot|)$.

我们给出等价赋值的定义.

定义 7.2. 设$|\cdot|_1$与$|\cdot|_2$为域K上的两个赋值. 如果$|\cdot|_1$与$|\cdot|_2$在K上定义的拓扑相同, 则称$|\cdot|_1$与$|\cdot|_2$等价.

命题 7.1. 设$|\cdot|_1$与$|\cdot|_2$为域K上的两个赋值. 则$|\cdot|_1$与$|\cdot|_2$等价当且仅当存在实数$s > 0$使得$|\cdot|_1 = |\cdot|_2^s$.

证明: "$\Leftarrow$". 设存在实数$s > 0$使得$|\cdot|_1 = |\cdot|_2^s$. 对任意的$\varepsilon > 0$, 定义

$$U_\varepsilon^{(1)} := \{x \in K : \ |x|_1 < \varepsilon\}.$$

则$\{U_\varepsilon^{(1)}:\varepsilon\in\mathbb{R}_{>0}\}$恰好为$(K,|\cdot|_1)$中, 0的开邻域基. 因为$K$为拓扑域, 我们得到

$$\mathcal{T}_1=\left\{U\subseteq K:\text{对任意的}x\in K\text{存在}\varepsilon>0\text{使得}x+U_\varepsilon^{(1)}\subseteq U\right\}$$

中的集合恰好为$(K,|\cdot|_1)$中的全部开集. 类似地, 我们可以定义$U_\varepsilon^{(2)}$与$\mathcal{T}_2$.

注意到

$$x\in U_\varepsilon^{(1)}\Leftrightarrow|x|_1<\varepsilon\Leftrightarrow|x|_2^s<\varepsilon\Leftrightarrow x\in U_{\varepsilon^{1/s}}^{(2)}.$$

我们有$U_\varepsilon^{(1)}=U_{\varepsilon^{1/s}}^{(2)}$. 因此$\mathcal{T}_1=\mathcal{T}_2$.

"⇒". 设$(K,|\cdot|_1)=(K,|\cdot|_2)$. 因为$|\cdot|_1$为非平凡赋值, 存在$y_0\in K^\times$使得$|y_0|_1>1$. 注意到序列$\{(1/y)^n\}_{n=1}^\infty$在$(K,|\cdot|_1)$中收敛到0, 由$(K,|\cdot|_1)=(K,|\cdot|_2)$, 序列$\{(1/y)^n\}_{n=1}^\infty$在$(K,|\cdot|_2)$中也收敛到0. 因此$|y_0|_2>1$.

对任意的$x\in K^\times$. 设$|x|_1=|y_0|_1^\alpha$. 取有理数序列$\{\frac{n_i}{m_i}\}_{i=1}^\infty$(其中$n_i\in\mathbb{Z},m_i\in\mathbb{Z}^+$)使得$\frac{n_i}{m_i}\geq\alpha\ (\forall i\in\mathbb{Z}^+)$并且

$$\lim_{i\to+\infty}\frac{n_i}{m_i}=\alpha.$$

因为$|y_0|_1>1$以及$m_i\in\mathbb{Z}^+$, 利用上面说明$|y_0|_2>1$的方法, 容易验证

$$|y_0|_1^{\frac{n_i}{m_i}}\geq|y_0|_1^\alpha=|x|_1\Rightarrow|y_0|_1^{n_i}\geq|x|_1^{m_i}\Rightarrow\left|\frac{y_0^{n_i}}{x^{m_i}}\right|_1\geq1\Rightarrow\left|\frac{y_0^{n_i}}{x^{m_i}}\right|_2\geq1.$$

因此$|y_0|_2^{\frac{n_i}{m_i}}\geq|x|_2$. 令$i\to+\infty$我们有

$$|y_0|_2^\alpha\geq|x|_2.$$

再取一个有理数序列从小于α的方向收敛到α, 利用类似的方法我们得到

$$|y_0|_2^\alpha\leq|x|_2.$$

通过上面的讨论, 对任意的$x\in K^\times$,

$$\begin{cases}|x|_1&=|y_0|_1^\alpha,\\|x|_2&=|y_0|_2^\alpha.\end{cases}$$

因为$|y_0|_1>1,|y_0|_2>1$, 上式得到

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

其中

$$s=\frac{\log|y_0|_1}{\log|y_0|_2}>0.$$

综上, 我们完成了证明. □

注记 7.2. (i) 从命题的证明中, 我们可以得到一个判定两个非平凡赋值等价的简单准则:

$$|\cdot|_1\text{与}|\cdot|_2\text{等价}\Leftrightarrow|x|_1<1\Rightarrow|x|_2<1.$$

事实上, "⇒"显然成立. 对于"⇐", 令$y_0=1/x$, 利用上面证明中的方法容易说明存在$s\in\mathbb{R}_{>0}$使得$|\cdot|_1=|\cdot|_2^s$. 因此两个赋值等价.

(ii) 利用这个准则, 我们还可以得到

$$|\cdot|_1\text{与}|\cdot|_2\text{不等价}\Leftrightarrow\text{存在}x_0\in K\text{使得}|x_0|_1<1\text{且}|x_0|_2>1.$$

事实上, "⇐"显然成立. 对于"⇒", 因为$|\cdot|_1$与$|\cdot|_2$不等价, 存在$z_0\in K$使得$|z_0|_1<1,|z_0|_2\geq1$, 还存在$w_0\in K$使得$|w_0|_1\geq1,|w_0|_2<1$. 此时令$x_0=z_0/w_0$. 则有$|x_0|_1<1$且$|x_0|_2>1$.

下面我们介绍赋值域上的弱逼近定理.

定理 7.1. 设K为域, $n\in\mathbb{Z}_{\geq2}$, $|\cdot|_1,\cdots,|\cdot|_n$为$K$上两两不等价的非平凡赋值. 固定元素$a_1,\cdots,a_n\in K$. 则对任意的$\varepsilon>0$, 存在$\alpha\in K$使得对任意的$1\leq i\leq n$都有

$$|\alpha-a_i|_i<\varepsilon.$$

证明: 我们首先断言: 存在$\beta\in K$使得

$$\begin{cases}|\beta|_1>1\\|\beta|_i<1\ (\forall 2\leq i\leq n)\end{cases}.$$

对n归纳. 当$n=2$时, 由注记7.2, 结论成立. 下面假设$n\geq3$并且结论对$n-1$成立. 则由归纳假设存在$\beta_0\in K$使得$|\beta_0|_1>1$且$|\beta_0|_i<1(\forall2\leq i\leq n-1)$. 下面我们分三种情况讨论.

情况1. $|\beta_0|_n<1$. 则此时令$\beta=\beta_0$即可.

情况2. $|\beta_0|_n=1$. 取$y_0\in K$使得$|y_0|_1>1,|y_0|_n<1$. 再取一个充分大的整数N_0. 此时令$\beta=\beta_0^{N_0}\cdot y_0$即可.

情况3. $|\beta_0|_n > 1$. 取$y_0 \in K$使得$|y_0|_1 > 1, |y_0|_n < 1$. 注意到在$(K, |\cdot|_1)$以及在$(K, |\cdot|_n)$中,

$$\lim_{m\to+\infty} \frac{\beta_0^m}{1+\beta_0^m} = 1.$$

当$2 \leq i \leq n-1$时, 在$(K, |\cdot|_i)$中我们有

$$\lim_{m\to+\infty} \frac{\beta_0^m}{1+\beta_0^m} = 0.$$

因此, 此时取一个充分大的整数N_1. 令

$$\beta_0 = \frac{\beta_0^{N_1}}{1+\beta_0^{N_1}}$$

即可.

综上, 上述断言成立. 因此, 对任意的$1 \leq i \leq n$, 存在$\beta_i \in K$使得

$$\begin{cases} |\beta_i|_i > 1 \\ |\beta_i|_j < 1 \ (\forall j \neq i) \end{cases}$$

与上面类似, 设

$$x_i = \frac{\beta_i^N}{1+\beta_i^N},$$

其中N为一个充分大的整数使得

$$\begin{cases} |x_i - 1|_i \text{充分小}, \\ |x_i|_j \text{充分小} \ (\forall 2 \leq j \leq n). \end{cases}$$

此时容易验证

$$\alpha = \sum_{i=1}^{n} a_i x_i$$

满足定理的要求.

综上, 我们完成了证明. □

下面介绍一类我们后面主要研究的赋值.

定义 7.3. 设K为域, $|\cdot|$为K上的非平凡赋值. 如果$|\cdot|$满足强三角不等式

$$|x+y| \leq \max\{|x|, |y|\} \ (\forall x, y \in K),$$

则我们称$|\cdot|$为K上的一个非阿基米德赋值. 否则, 我们称$|\cdot|$为K上的一个阿基米德赋值.

我们在第二章中介绍的p-adic赋值就是一个非阿基米德赋值. 关于非阿基米德赋值, 我们有一个简单却很有用的结论(一般将其称为domination principle).

命题 7.2. *设K为域, $|\cdot|$为K上的一个非阿基米德赋值. 如果$|x|<|y|$, 则*

$$|x+y|=|y|.$$

证明: 因为$|x|<|y|$, 由强三角不等式,

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

这完成了证明. □

判断一个非平凡赋值是否为非阿基米德赋值有一个很简单的准则.

命题 7.3. *设K为域, $|\cdot|$为K上的非平凡赋值. 则$|\cdot|$为K上的一个非阿基米德赋值当且仅当*

$$\{|n|:\ n=1,2,\cdots\}$$

为有界集.

证明: "⇒". 设$|\cdot|$为非阿基米德赋值. 则由强三角不等式

$$|n|=|1+1+\cdots+1|\leq|1|=1.$$

"⇐". 设$M\in\mathbb{R}_{>0}$使得对任意的$n=1,2,\cdots$,都有$|n|\leq M$. 则对任意的$x,y\in K$以及任意的$N\in\mathbb{Z}^+$, 我们有

$$\begin{aligned}|x+y|^N=|(x+y)^N|&=\left|\sum_{i=0}^{N}\binom{N}{i}x^iy^{N-i}\right|\\&\leq\sum_{i=0}^{N}\left|\binom{N}{i}x^iy^{N-i}\right|\\&\leq(N+1)\cdot M\cdot\max\{|x|^N,|y|^N\}.\end{aligned}$$

因此,

$$|x+y|\leq(N+1)^{1/N}\cdot M^{1/N}\cdot\max\{|x|,|y|\}.$$

上式两边令$N\to+\infty$得到

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

综上, 我们证明了$|\cdot|$为非阿基米德赋值. □

设$|\cdot|$为K上的一个非阿基米德赋值. 我们容易将其延拓到函数域$K(t)$上.

命题 7.4. 设$|\cdot|$为K上的一个非阿基米德赋值. 对任意的

$$f(t)=a_nt^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0\in K[t]$$

我们定义

$$|f|:=\max\{|a_i|:\ 0\leq i\leq n\}.$$

对于任意的$\frac{h(t)}{g(t)}\in K(t)$ (其中$h(t),g(t)\in K[t]$且$g(t)\neq 0$), 我们定义

$$\left|\frac{h(t)}{g(t)}\right|:=\frac{|h(t)|}{|g(t)|}.$$

则$|\cdot|$为$K(t)$上的一个非阿基米德赋值.

证明: 首先对任意的$\frac{h(t)}{g(t)}\in K(t)$ (其中$h(t),g(t)\in K[t]$且$g(t)\neq 0$), 显然有

$$\left|\frac{h(t)}{g(t)}\right|\geq 0,\ \text{并且}\ \left|\frac{h(t)}{g(t)}\right|=0\Leftrightarrow\frac{h(t)}{g(t)}=0.$$

下面证明$|\cdot|$在$K(t)^\times$上的限制映射为$K(t)^\times\to\mathbb{R}_{>0}$的乘法群同态. 为此, 我们先考虑$K[t]$上的情形. 设

$$\begin{aligned}f_1(t)&=b_nt^n+b_{n-1}t^{n-1}+\cdots+b_1t+b_0\in K[t]\setminus\{0\},\\ f_2(t)&=c_mt^m+c_{m-1}t^{m-1}+\cdots+c_1t+c_0\in K[t]\setminus\{0\}.\end{aligned}$$

为了方便, 当$i\in\mathbb{Z}\setminus[0,n]$时, 设$b_i=0$. 当$j\in\mathbb{Z}\setminus[0,m]$时, 设$c_j=0$. 因为$|\cdot|$为非阿基米德赋值, 显然有

$$\begin{aligned}|f_1(t)f_2(t)|&=\max\left\{\left|\sum_{i=0}^n c_ib_{r-i}\right|:\ 0\leq r\leq m+n\right\}\\ &\leq\max\{|b_i|:\ 0\leq i\leq n\}\cdot\max\{|c_j|:\ 0\leq j\leq m\}\\ &=|f_1(t)|\cdot|f_2(t)|.\end{aligned}$$

反过来, 设$|f_1|=|b_s|$, $|f_2|=|c_t|$, 其中$|b_i|<|b_s|$ $(\forall 0\leq i<s)$并且$|c_j|<|c_t|$ $(\forall 0\leq j<t)$. 则f_1f_2中t^{s+t}的系数d_{s+t}为

$$d_{s+t}=\sum_{i=0}^{s+t}b_ic_{s+t-i}.$$

由s,t的定义, 利用命题7.2, 容易验证

$$|d_{s+t}|=|b_sc_t|=|f_1(t)f_2(t)|.$$

这说明$|f_1(t)f_2(t)| \geq |f_1(t)| \cdot |f_2(t)|$. 结合上面的讨论我们得到

$$|f_1(t)f_2(t)| = |f_1(t)| \cdot |f_2(t)|.$$

因此对任意的$\frac{h(t)}{g(t)}, \frac{h_1(t)}{g_1(t)} \in K(t)$ $(h(t), g(t), h_1(t), g_1(t) \in K[t]$且$g(t)g_1(t) \neq 0)$, 容易验证

$$\begin{aligned}\left|\frac{h(t)}{g(t)} \cdot \frac{h_1(t)}{g_1(t)}\right| &= \frac{|h(t)h_1(t)|}{|g(t)g_1(t)|} \\ &= \frac{|h(t)| \cdot |h_1(t)|}{|g(t)| \cdot |g_1(t)|} \\ &= \left|\frac{h(t)}{g(t)}\right| \cdot \left|\frac{h_1(t)}{g_1(t)}\right|.\end{aligned}$$

最后我们来证明强三角不等式. 记号如上, 对任意的$f_1(t), f_2(t) \in K[t]$, 容易说明

$$|f_1(t) + f_2(t)| \leq \max\{|f_1(t)|, |f_2(t)|\}.$$

因此对任意的$\frac{h(t)}{g(t)}, \frac{h_1(t)}{g_1(t)} \in K(t)$ $(h(t), g(t), h_1(t), g_1(t) \in K[t]$且$g(t)g_1(t) \neq 0)$, 容易验证

$$\begin{aligned}\left|\frac{h(t)}{g(t)} + \frac{h_1(t)}{g_1(t)}\right| &= \left|\frac{h(t)g_1(t) + h_1(t)g(t)}{g(t)g_1(t)}\right| \\ &= \frac{|h(t)g_1(t) + h_1(t)g(t)|}{|g(t)g_1(t)|} \\ &\leq \frac{\max\{|h(t)g_1(t)|, |h_1(t)g(t)|\}}{|g(t)g_1(t)|} \\ &= \max\left\{\left|\frac{h(t)}{g(t)}\right|, \left|\frac{h_1(t)}{g_1(t)}\right|\right\}.\end{aligned}$$

综上, 我们完成了证明. □

利用该命题, 我们容易证明经典的Gauss引理.

命题 7.5. *设$f(t) \in \mathbb{Z}[t]$为首一多项式. 如果存在两个首一多项式$g(t), h(t) \in \mathbb{Q}[t]$使得$f(t) = g(t)h(t)$, 则$g(t), h(t) \in \mathbb{Z}[t]$.*

证明: 对任意的素数p, 考虑$\mathbb{Q}$上的p-adic赋值$|\cdot|_p$. 由命题7.4, 我们得到

$$1 = |f(t)|_p = |g(t)h(t)|_p = |g(t)|_p \cdot |h(t)|_p.$$

因为$g(t), h(t) \in \mathbb{Q}[t]$为首一多项式, 我们有$|g(t)|_p \geq 1$, $|h(t)|_p \geq 1$. 结合上面的讨论, 对任意的素数p,

$$|g(t)|_p = |h(t)|_p = 1.$$

这说明$g(t), h(t)$的每一项系数均属于

$$\bigcap_p \mathbb{Z}_p = \mathbb{Z}.$$

因此, $g(t), h(t) \in \mathbb{Z}[t]$.

综上, 我们完成了证明. □

对于非阿基米德赋值, 为了使用方便, 我们给出如下定义.

定义 7.4. 设$|\cdot|$为域K上的一个非阿基米德赋值. 定义$\nu: K \to \mathbb{R} \cup \{+\infty\}$为

$$\nu(x) = \begin{cases} -\log|x| & \text{如果 } x \neq 0, \\ +\infty & \text{如果 } x = 0, \end{cases}$$

并将其称作非阿基米德赋值$|\cdot|$对应的指数赋值(exponential valuation).

注记 7.3. (i) 容易验证指数赋值$\nu: K \to \mathbb{R} \cup \{+\infty\}$满足以下三个条件

- $\nu(x) = +\infty \Leftrightarrow x = 0$.
- $\nu(xy) = \nu(x) + \nu(y)$ $(\forall x, y \in K)$.
- $\nu(x+y) \geq \min\{\nu(x), \nu(y)\}$并且当$\nu(x) < \nu(y)$时, 我们有

$$\nu(x+y) = \nu(x).$$

(ii) 固定实数$0 < \lambda < 1$, 容易说明

$$|x|' := \lambda^{\nu(x)}$$

为K上一个与$|\cdot|$等价的赋值.

(iii) 对任意的正实数$s > 0$, 对非阿基米德赋值$|\cdot|$, 容易说明$|\cdot|^s$也是一个非阿基米德赋值(但是, 该结论对于阿基米德赋值并不成立. 例如, 对于绝对值赋值$|\cdot|_\infty$, 函数$|\cdot|_\infty^2$不满足三角不等式, 因此它并不是一个赋值). 由此, 容易说明两个指数赋值ν_1, ν_2等价当且仅当存在实数$s > 0$使得$\nu_1 = s \cdot \nu_2$.

定义 7.5. 设K为域, $|\cdot|$为K上的一个非阿基米德赋值, ν为其对应的指数赋值. 容易验证

$$\mathcal{O} = \{x \in K: |x| \leq 1\} = \{x \in K: \nu(x) \geq 0\}$$

为一个赋值环, 其中

$$\mathfrak{p} = \{x \in K : |x| < 1\} = \{x \in K : \nu(x) > 0\}$$

为其唯一的非零极大理想,

$$\mathcal{O}^\times = \{x \in K : |x| = 1\} = \{x \in K : \nu(x) = 0\}$$

为其可逆元构成的乘法子群.

注记 7.4. 由注记7.2, 容易证明K上的两个赋值$|\cdot|_1$与$|\cdot|_2$等价当且仅当它们的赋值环相同.

下面我们给出离散赋值的定义.

定义 7.6. 设ν为域K上的一个指数赋值. 如果存在正实数$s > 0$使得

$$\nu(K^\times) := \left\{\nu(x) : x \in K^\times\right\} = s \cdot \mathbb{Z},$$

则称ν为一个离散赋值. 特别地, 如果$\nu(K^\times) = \mathbb{Z}$, 则称$\nu$为正则的离散赋值.

离散赋值与我们在第三章中介绍的离散赋值环密切相关.

命题 7.6. 设ν为域K上的一个离散赋值. 则其赋值环

$$\mathcal{O} = \{x \in K : \nu(x) \geq 0\}$$

为离散赋值环. 更进一步, 如果ν为正则的离散赋值, 则对任意的正整数n都有

$$\mathfrak{p}^n = \{x \in K : \nu(x) \geq n\}.$$

并且此时有加法群同构

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p}.$$

证明: 由命题3.5, 我们知道赋值环是整闭整环并且有唯一的非零极大理想. 下面只要证明$\mathcal{O}$为主理想整环即可. 因为ν为离散赋值, 存在$s > 0$使得$\nu(K^\times) = s \cdot \mathbb{Z}$. 取$\pi \in \mathcal{O}$使得$\nu(\pi) = s$. 对$\mathcal{O}$的任意非零$\mathfrak{a}$, 令

$$r = \min\left\{\frac{\nu(x)}{s} : x \in \mathfrak{a}\right\},$$

令$x_0 \in \mathfrak{a}$使得$\nu(x_0) = sr$. 则对任意的$y \in \mathfrak{a}$, 我们有

$$\nu\left(\frac{y}{x_0}\right) = \nu(y) - \nu(x_0) = \nu(y) - sr \geq 0.$$

这说明$y/x_0 \in \mathcal{O}$. 因此$\mathfrak{a} = x_0\mathcal{O}$, 即$\mathcal{O}$为主理想整环. 结合上面的讨论, $\mathcal{O}$是离散赋值环. 利用第三章中介绍的离散赋值环的性质容易证明第二个结论.

综上, 我们完成了证明. □

设ν为域K上正则的离散赋值, π为离散赋值环$\mathcal{O}$的一个素元. 容易说明

$$\left\{\mathfrak{p}^n : n \in \mathbb{Z}^+\right\}$$

为0的一组开邻域基,

$$\left\{U^{(n)} = 1 + \mathfrak{p}^n : n \in \mathbb{Z}^+\right\}$$

为1的一组开邻域基. 并且, 对任意的$1 + \pi^n y \in U^{(n)}$ ($y \in \mathcal{O}$), 因为$\mathcal{O}$为局部环, $1 + \pi^n y$一定为$\mathcal{O}$上的可逆元. 因此存在$z \in \mathcal{O}$使得

$$(1 + \pi^n y)z = 1.$$

这得到

$$(1 + \pi^n y)^{-1} = z = 1 - \pi^n yz \in U^{(n)}.$$

这说明$U^{(n)}$是$\mathcal{O}^\times$的乘法子群.

命题 7.7. *记号如上. 设ν为域K上正则的离散赋值, $n \in \mathbb{Z}^+$. 则有群同构*

(i) $\mathcal{O}^\times/U^{(n)} \cong (\mathcal{O}/\mathfrak{p}^n)^\times$.

(ii) $U^{(n)}/U^{(n+1)} \cong \mathcal{O}/\mathfrak{p}$.

证明: (i) 设$x \in \mathcal{O}$使得$x \bmod \mathfrak{p}^n \in (\mathcal{O}/\mathfrak{p}^n)^\times$. 则存在$y \in \mathcal{O}$使得

$$xy \equiv 1 \pmod{\mathfrak{p}^n}.$$

因为$\mathcal{O}$为局部环, 上式说明$x \in \mathcal{O}^\times$. 因此$h(x) = x \bmod \mathfrak{p}^n$是$\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{p}^n)^\times$的满同态, 并且显然$\ker h = U^{(n)}$. 由同构定理, 同构(i)成立.

(ii) 因为ν为正则的离散赋值, 由命题7.6, $\mathcal{O}$为离散赋值环. 取π为$\mathcal{O}$的一个素元. 则同态 $g(x) = 1 + \pi^n x \bmod U^{(n+1)}$显然是$\mathcal{O} \to U^{(n)}/U^{(n+1)}$的满同态且$\mathrm{Ker} g = \mathfrak{p}$. 因此同构(ii)成立.

综上, 我们完成了证明. □

作为本节的结束, 我们来介绍$\mathbb{Q}$上的Ostrowski定理. 我们将在后面的章节中介绍一般代数数域上的Ostrowski定理.

定理 7.2. 设$|\cdot|$为$\mathbb{Q}$上的一个非平凡赋值. 当$|\cdot|$为非阿基米德赋值时, $|\cdot|$与某个p-*adic*赋值$|\cdot|_p$等价. 当$|\cdot|$为阿基米德赋值时, $|\cdot|$与绝对值赋值$|\cdot|_\infty$等价.

证明: (i) 设$|\cdot|$为非阿基米德赋值. 注意到此时, 对任意的$n\in\mathbb{Z}$都有$|n|\leq 1$. 我们断言: 存在素数p使得$|p|<1$. 事实上, 如果假设对每个素数p都有$|p|=1$. 则对任意的$x\in\mathbb{Q}^\times$, 我们有

$$|x|=\prod_p\left|p^{\mathrm{ord}_p(x)}\right|=1.$$

这说明$|\cdot|$为平凡赋值, 显然矛盾. 因此, 存在素数p使得$|p|<1$. 对任意的素数$q\neq p$, 我们知道存在$a,b\in\mathbb{Z}$使得$aq+bp=1$. 由命题7.2,

$$1\geq|q|\geq|aq|=|1-bp|=|1|=1,$$

即$|q|=1$. 这说明对任意的$x\in\mathbb{Q}^\times$, 我们有

$$|x|=\left|p^{\mathrm{ord}_p(x)}\right|\cdot\prod_{q\neq p}\left|q^{\mathrm{ord}_q(x)}\right|=\left|p^{\mathrm{ord}_p(x)}\right|=|p|^{\mathrm{ord}_p(x)}=|x|_p^s,$$

其中

$$s=\frac{\log|p|}{\log|p|_p}>0.$$

由命题7.1, 赋值$|\cdot|$与$|\cdot|_p$等价.

(ii) 下面设$|\cdot|$为阿基米德赋值. 我们断言: 对任意的$n\in\mathbb{Z}_{\geq 2}$, 都有$|n|>1$. 事实上, 假设存在$n_0\in\mathbb{Z}_{\geq 2}$使得$|n_0|\leq 1$. 对任意的$m\in\mathbb{Z}_{\geq 2}$以及任意的$N\in\mathbb{Z}^+$, 设

$$m^N=a_0+a_1n_0+\cdots+a_rn_0^r$$

为m^N的n_0进制展开, 其中$0\leq a_i\leq n_0-1$且$a_r\neq 0$. 则

$$|m|^N\leq\sum_{i=0}^r|a_in_0^i|\leq\sum_{i=0}^r|a_i|\leq(r+1)n_0\leq\left(1+\frac{N\log m}{\log n_0}\right)\cdot n_0.$$

因此,

$$|m|\leq\left(1+\frac{N\log m}{\log n_0}\right)^{1/N}\cdot n_0^{1/N}.$$

令$N\to+\infty$得到$|m|\leq 1$. 由此以及命题7.3, 我们得到$|\cdot|$为非阿基米德赋值, 这显然矛盾. 因此, 上述断言成立.

对任意的$m,n\in\mathbb{Z}_{\geq 2}$以及任意的$N\in\mathbb{Z}^+$, 设

$$m^N=b_0+b_1n+\cdots+b_rn^r$$

为m^N的n进制展开, 其中$0 \leq b_i \leq n-1$且$b_r \neq 0$. 因为$|n| > 1$, 容易验证

$$|m|^N \leq \sum_{i=0}^{r} |b_i n^i| \leq (r+1) \cdot n \cdot |n|^r \leq \left(1 + \frac{N \log m}{\log n}\right) \cdot n \cdot |n|^{\frac{N \log m}{\log n}}.$$

因此,

$$|m| \leq \left(1 + \frac{N \log m}{\log n}\right)^{1/N} \cdot n^{1/N} \cdot |n|^{\frac{\log m}{\log n}}.$$

令$n \to \infty$得到

$$|m| \leq |n|^{\frac{\log m}{\log n}}.$$

将m, n换个位置得到

$$|n| \leq |m|^{\frac{\log n}{\log m}}.$$

结合上面的讨论, 对任意的$m, n \in \mathbb{Z}_{\geq 2}$,

$$\frac{\log |n|}{\log |m|} = \frac{\log n}{\log m}.$$

这说明

$$|n| = |n|_\infty^s, \tag{7.1}$$

其中

$$s = \frac{\log |2|}{\log 2} > 0.$$

因为$|-n| = n$且$|1| = 1$, 等式(7.1)对任意的整数n均成立. 由此, 对任意的$x/y \in \mathbb{Q}(x, y \in \mathbb{Z}$且$y \neq 0)$, 我们有

$$\left|\frac{x}{y}\right| = \frac{|x|}{|y|} = \frac{|x|_\infty^s}{|y|_\infty^s} = \left|\frac{x}{y}\right|_\infty^s.$$

由此与命题7.1, 赋值$|\cdot|$与绝对值赋值$|\cdot|_\infty$等价.

综上, 我们完成了证明. □

7.2 赋值域的完备化

首先, 我们给出完备赋值域的定义.

定义 7.7. *设K为域, $|\cdot|$为K上的非平凡赋值. 如果对$(K, |\cdot|)$中任意的Cauchy序列$\{a_n\}_{n=1}^{\infty}$, 存在$a \in K$使得*

$$\lim_{n \to +\infty} a_n = a,$$

则称$(K, |\cdot|)$是一个完备的赋值域.

我们知道有许多不完备的赋值域$(K,|\cdot|)$. 例如, $(\mathbb{Q},|\cdot|_\infty)$以及$(\mathbb{Q},|\cdot|_p)$. 下面我们介绍赋值域的完备化过程. 设$\mathcal{R}$为$(K,|\cdot|)$上所有Cauchy序列构成的集合, 并且令

$$\mathfrak{m}=\left\{\{a_n\}_{n=1}^\infty\in\mathcal{R}:\lim_{n\to+\infty}a_n=0\right\}.$$

在序列的加法与乘法运算下, 容易说明$\mathfrak{m}$是$\mathcal{R}$的极大理想. 令$\widehat{K}:=\mathcal{R}/\mathfrak{m}$. 对任意的$x\in K$, 将$a$等同于常数序列$\{a\}_{n=1}^\infty$. 则显然有$K\hookrightarrow\widehat{K}$. 对任意的$\{a_n\}_{n=1}^\infty \bmod \mathfrak{m}\in\widehat{K}$, 因为$\{a_n\}_{n=1}^\infty$为Cauchy列以及不等式

$$||a_s|-|a_t||\leq|a_s-a_t|,$$

我们得到$\{|a_n|\}_{n=1}^\infty$是$\mathbb{R}$上的Cauchy列. 因此$\lim_{n\to+\infty}|a_n|$存在. 并且容易验证当

$$\{a_n\}_{n=1}^\infty\equiv\{b_n\}_{n=1}^\infty\ (\mathrm{mod}\ \mathfrak{m})$$

时, 必有

$$\lim_{n\to+\infty}|a_n|=\lim_{n\to+\infty}|b_n|.$$

定义函数$|\cdot|_*:\widehat{K}\to\mathbb{R}$为

$$|\{a_n\}_{n=1}^\infty \bmod \mathfrak{m}|_*:=\lim_{n\to+\infty}|a_n|.$$

由上面的讨论, 我们容易验证$|\cdot|_*$的定义是合理的. 利用赋值的定义也容易说明$|\cdot|_*$是$\widehat{K}$上的赋值并且$|a|_*=|a|\ (\forall a\in K)$. 同时, 也容易验证$K$在赋值域$(\widehat{K},|\cdot|_*)$中是稠密的.

下面我们来说明$(\widehat{K},|\cdot|_*)$是完备的.

定理 7.3. *记号如上. 则$(\widehat{K},|\cdot|_*)$是完备的赋值域.*

证明: 设$\{x_n\}_{n=1}^\infty$为$(\widehat{K},|\cdot|_*)$上的任意一个Cauchy列, 其中

$$x_n=\{a_i^{(n)}\}_{i=1}^\infty \bmod \mathfrak{m}.$$

当$n=1$时, 存在$k_1\in\mathbb{Z}^+$使得对任意的$i,i'\geq k_1$都有

$$|a_i^{(1)}-a_{i'}^{(1)}|<1.$$

利用递推构造, 对任意的$n\geq 2$, 存在正整数$k_n>k_{n-1}$使得对任意的$i,i'\geq k_n$都有

$$|a_i^{(n)}-a_{i'}^{(n)}|<\frac{1}{n}.$$

考虑序列$\{a_{k_n}^{(n)}\}_{n=1}^{\infty}$. 先说明该序列为$(K,|\cdot|)$上的Cauchy列. 事实上, 对任意的$\varepsilon>0$, 因为$\{x_n\}_{n=1}^{\infty}$为$(\widehat{K},|\cdot|_*)$上的Cauchy列, 存在$N_0(\varepsilon)$使得对任意的$m,n\geq N_0(\varepsilon)$都有

$$|x_n-x_m|_*=\lim_{i\to+\infty}|a_i^{(n)}-a_i^{(m)}|<\frac{\varepsilon}{6}.$$

因此, 存在$N_1(\varepsilon)$使得对任意的$i\geq N_1(\varepsilon)$都有

$$|a_i^{(n)}-a_i^{(m)}|<\frac{\varepsilon}{6}.$$

令

$$N(\varepsilon)=\max\left\{N_0(\varepsilon),N_1(\varepsilon),1+\lfloor\varepsilon/6\rfloor\right\}.$$

则对任意的$m\geq n\geq N(\varepsilon)$, 我们有

$$\begin{aligned}\left|a_{k_n}^{(n)}-a_{k_m}^{(m)}\right|&=\left|a_{k_n}^{(n)}-a_{k_m}^{(n)}+a_{k_m}^{(n)}-a_{k_m}^{(m)}\right|\\&\leq\left|a_{k_n}^{(n)}-a_{k_m}^{(n)}\right|+\left|a_{k_m}^{(n)}-a_{k_m}^{(m)}\right|\\&\leq\frac{1}{n}+\frac{\varepsilon}{6}\\&<\varepsilon/3.\end{aligned}$$

因此, $\{a_{k_n}^{(n)}\}_{n=1}^{\infty}$为$(K,|\cdot|)$上的Cauchy列.

令$x=\{a_{k_n}^{(n)}\}_{n=1}^{\infty}\bmod\mathfrak{m}\in\widehat{K}$. 记号如上. 则当$n\geq N(\varepsilon)$时, 我们有

$$\begin{aligned}|x_n-x|_*&=\lim_{i\to+\infty}\left|a_i^{(n)}-a_{k_i}^{(i)}\right|\\&\leq\lim_{i\to+\infty}\left|a_i^{(n)}-a_{k_i}^{(n)}\right|+\lim_{i\to+\infty}\left|a_{k_i}^{(n)}-a_{k_n}^{(n)}\right|+\lim_{i\to+\infty}\left|a_{k_n}^{(n)}-a_{k_i}^{(i)}\right|\\&\leq\frac{1}{n}+\frac{1}{n}+\frac{\varepsilon}{3}\\&<\varepsilon.\end{aligned}$$

因此,

$$\lim_{n\to+\infty}x_n=x.$$

综上, 我们证明了$(\widehat{K},|\cdot|_*)$是完备的赋值域. □

注记 7.5. (i) 当$|\cdot|$是K上的非阿基米德赋值时, 我们断言对任意的$\{a_n\}_{n=1}^{\infty}\in\mathcal{R}\setminus\mathfrak{m}$, 一定存在$N\in\mathbb{Z}^+$使得

$$|a_n|=|a_N|\ (\forall n\geq N).$$

事实上, 因为$\{a_n\}_{n=1}^{\infty}$不收敛到0, 存在$\varepsilon_0 > 0$使得对任意的$N_1 \in \mathbb{Z}^+$, 存在$n(N_1) \geq N_1$使得$|a_{n(N_1)}| > \varepsilon_0$. 另一方面, 因为$\{a_n\}_{n=1}^{\infty}$是*Cauchy*列, 存在$N_2$使得对任意的$m, n \geq N_2$都有$|a_m - a_n| < \varepsilon_0/2$. 令$N = n(N_2)$. 则由命题*7.2*, 对任意的$n \geq N$,

$$|a_n| = |(a_n - a_N) + a_N| = |a_N|.$$

因此, 上述断言成立. 注意当$\{a_n\}_{n=1}^{\infty}$收敛到0时, 上述结论并不成立. 例如, $(\mathbb{Q}, |\cdot|_p)$的*Cauchy*序列$\{p^n\}_{n=1}^{\infty}$中每一项的*p-adic*赋值互不相同.

由上面的讨论, 当$|\cdot|$是K上的非阿基米德赋值时,

$$|K| := \{|x| : x \in K\} = \{|x|_* : x \in \widehat{K}\} = |\widehat{K}|_*.$$

(ii) 对于阿基米德赋值的情形, 我们不加证明地给出如下定理(它的证明主要涉及分析的技巧, 这里就不赘述了).

定理 7.4. 设$(K, |\cdot|)$为一个完备的阿基米德赋值域. 则

$$(K, |\cdot|) \underset{topological}{\cong} (\mathbb{R}, |\cdot|_\infty),$$

或者

$$(K, |\cdot|) \underset{topological}{\cong} (\mathbb{C}, |\cdot|_\infty),$$

其中记号$\underset{topological}{\cong}$表示这两个赋值域之间存在一个域同构$\varphi$, 并且作为拓扑空间之间的映射, φ还是一个同胚.

(iii) 从现在开始, 将$\mathbb{Q}$在*p-adic*赋值下的完备化记作$\mathbb{Q}_p$, 将其赋值环记作$\mathbb{Z}_p$(注意在这章之前, 记号$\mathbb{Z}_p$指的是$\mathbb{Z}$在p处的局部化). 我们后面会详细介绍它们.

下面我们给出完备化的一般定义.

定义 7.8. 设$(K, |\cdot|)$为一个赋值域. 如果赋值域$(\widehat{K}, \widehat{|\cdot|})$满足以下三个条件

(i) $(\widehat{K}, \widehat{|\cdot|})$是完备的,

(ii) $K \subseteq \widehat{K}$并且$\widehat{|\cdot|}$在K上的限制与$|\cdot|$等价,

(iii) K在$(\widehat{K}, \widehat{|\cdot|})$中稠密,

则将$(\widehat{K}, \widehat{|\cdot|})$称为$(K, |\cdot|)$的一个完备化.

关于赋值域的完备化, 我们首先介绍下面的延拓定理.

定理 7.5. 设$(K,|\cdot|)$为赋值域, $(\widehat{K},\widehat{|\cdot|})$为其完备化, $(M,|\cdot|_M)$为一个完备的赋值域. 设拓扑嵌入(topological injection)

$$f:\ (K,|\cdot|)\underset{topological}{\hookrightarrow}(M,|\cdot|_M),$$

其中记号$\underset{topological}{\hookrightarrow}$表示$f$为域嵌入, 并且作为拓扑空间之间的映射, K与$f(K)$是同胚的(这里$f(K)$上的拓扑为子空间拓扑). 则存在f唯一的延拓$\hat{f}$使得

$$\hat{f}:\ (\widehat{K},\widehat{|\cdot|})\underset{topological}{\hookrightarrow}(M,|\cdot|_M).$$

换句话说, 存在f唯一的延拓$\hat{f}$使得使得下面的交换图成立

$$\begin{array}{ccc} K & \xrightarrow{f} & M \\ \downarrow & \nearrow_{\hat{f}} & \\ \widehat{K} & & \end{array}$$

证明: 因为$\widehat{|\cdot|}$在K上的限制与$|\cdot|$等价, 为了方便, 由命题7.1, 不妨设$\widehat{|\cdot|}$在K上的限制恰好等于$|\cdot|$.

先证明延拓的存在性. 因为K在$(\widehat{K},\widehat{|\cdot|})$中稠密, 对任意的$x\in\widehat{K}$, 存在$K$上的Cauchy列$\{x_n\}_{n=1}^{\infty}$使得

$$\lim_{n\to+\infty}x_n=x.$$

因为$f:\ (K,|\cdot|)\underset{topological}{\hookrightarrow}(M,|\cdot|_M)$, 序列$\{f(x_n)\}_{n=1}^{\infty}$为$M$上的Cauchy列. 定义

$$\hat{f}(x):=\lim_{n\to+\infty}f(x_n).$$

容易验证这个定理是合理的并且$\hat{f}$是域嵌入. 下面我们来说明

$$\hat{f}:\ (\widehat{K},\widehat{|\cdot|})\underset{topological}{\hookrightarrow}(M,|\cdot|_M).$$

为此, 仅需证明$\widehat{|\cdot|}$与$|\cdot|_M\circ\hat{f}$是等价的赋值. 对任意的$y\in\{x\in\widehat{K}:\ \widehat{|x|}<1\}$, 取$K$上收敛到$y$的Cauchy列$\{y_n\}_{n=1}^{\infty}$. 设$\widehat{|y|}<r_0<1$. 则当$n$充分大时,

$$|y_n|=\widehat{|y_n|}\leq\widehat{|y_n-y|}+\widehat{|y|}<r_0.$$

因为f是拓扑嵌入, 当n充分大时, $|f(y_n)|_M<1$. 由此

$$|\hat{f}(y)|_M=\left|\lim_{n\to+\infty}f(y_n)\right|_M=\lim_{n\to+\infty}|f(y_n)|_M\leq r_0<1.$$

这说明

$$\widehat{|y|} < 1 \Rightarrow |\hat{f}(y)|_M < 1.$$

由此与注记7.2, 赋值$\widehat{|\cdot|}$与赋值$|\cdot|_M \circ \hat{f}$是等价的. 因此, $\hat{f}$是拓扑嵌入.

最后来证明延拓的唯一性. 设$\hat{g}: \widehat{K} \underset{topological}{\hookrightarrow} M$为$f$的一个延拓. 对任意的$x \in \widehat{K}$, 取$K$上收敛到$x$的Cauchy列$\{x_n\}_{n=1}^{\infty}$. 则

$$\hat{g}(x) = \hat{g}\left(\lim_{n\to+\infty} x_n\right) = \lim_{n\to+\infty} \hat{g}(x_n) = \lim_{n\to+\infty} f(x_n) = \hat{f}(x).$$

因此$\hat{f} = \hat{g}$.

综上, 我们完成了证明. □

由该延拓定理, 我们容易得到下面的推论.

推论 7.1. *设$(K, |\cdot|)$为赋值域, $(M_1, |\cdot|_1)$与$(M_2, |\cdot|_2)$均为$(K, |\cdot|)$的完备化. 则存在拓扑同构*

$$\varphi: (M_1, |\cdot|_1) \underset{topological}{\cong} (M_2, |\cdot|_2).$$

并且$\varphi|_K = \mathrm{id}$.

7.3 完备的离散赋值域与反向极限

由定理7.4, 阿基米德赋值域的完备化本质就是$(\mathbb{R}, |\cdot|_\infty)$或者$(\mathbb{C}, |\cdot|_\infty)$. 因此, 我们下面主要关注非阿基米德赋值域的完备化, 尤其是离散赋值域的完备化.

命题 7.8. *设$(K, |\cdot|)$为非阿基米德赋值域, $\mathcal{O}$为其赋值环, $\mathfrak{p}$为$\mathcal{O}$的极大理想. 设$(\widehat{K}, \widehat{|\cdot|})$为$K$的完备化, $\widehat{\mathcal{O}}$为其赋值环, $\widehat{\mathfrak{p}}$为$\widehat{\mathcal{O}}$的极大理想. 则$\mathcal{O}$在$(\widehat{K}, \widehat{|\cdot|})$中的闭包恰好为$\widehat{\mathcal{O}}$, 并且*

$$\mathcal{O}/\mathfrak{p} \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}.$$

更进一步, 如果$|\cdot|$对应的指数赋值是离散赋值, 则对任意的$n \in \mathbb{Z}^+$,

$$\mathcal{O}/\mathfrak{p}^n \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n.$$

证明: 因为$\widehat{|\cdot|}$在K上的限制与$|\cdot|$等价, 为了方便, 由命题7.1, 不妨设$\widehat{|\cdot|}$在K上的限制恰好等于$|\cdot|$. 注意到, 由注记7.4, 两个等价的赋值有着相同的赋值环. 因此, 这样的操作并不影响命题的结果.

(i) 对任意的$x \in \widehat{\mathcal{O}}$, 取$K$上收敛到$x$的Cauchy列$\{x_n\}_{n=1}^{\infty}$. 则当$n$充分大时, 必有

$$|x_n| = \widehat{|x_n|} \leq \max\{\widehat{|x_n - x|}, \widehat{|x|}\} \leq 1.$$

这说明当n充分大时, $x_n \in \mathcal{O}$. 注意到$\{x + \widehat{\mathfrak{p}}^n : n \in \mathbb{Z}^+\}$是$x$在$(\widehat{K}, \widehat{|\cdot|})$中的一组开邻域基, 上面的讨论说明

$$\left(x + \widehat{\mathfrak{p}}^n\right) \cap \mathcal{O} \neq \emptyset \ (\forall n \in \mathbb{Z}^+). \tag{7.2}$$

设$\mathcal{O}$在$(\widehat{K}, \widehat{|\cdot|})$中的闭包为$C$. 则上式说明$x \in C$, 即$\widehat{\mathcal{O}} \subseteq C$. 注意到$\widehat{\mathcal{O}}$是闭集, 我们有$\widehat{\mathcal{O}} = C$.

由(7.2), 同态$y \mapsto y \bmod \widehat{\mathfrak{p}}$是$\mathcal{O} \to \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$的满同态. 显然该满同态的核为

$$\widehat{\mathfrak{p}} \cap \mathcal{O} = \mathfrak{p}.$$

因此,

$$\mathcal{O}/\mathfrak{p} \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}.$$

(ii) 设$|\cdot|$对应的指数赋值ν为离散赋值. 由注记7.3, 不妨设ν为正则的离散赋值. 对任意的$n \in \mathbb{Z}^+$, 由(7.2), 同态$f_n : y \mapsto y \bmod \widehat{\mathfrak{p}}^n$是$\mathcal{O} \to \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n$的满同态. 并且

$$\ker f_n = \widehat{\mathfrak{p}}^n \cap \mathcal{O} = \{x \in \mathcal{O} : \nu(x) \geq n\} = \mathfrak{p}^n.$$

因此,

$$\mathcal{O}/\mathfrak{p}^n \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n.$$

综上, 我们完成了证明.

利用该命题, 我们可以得到下面这个非常重要的结论.

定理 7.6. *设(K, ν)为离散赋值域, $\mathcal{O}$为其赋值环, $\mathfrak{p}$为$\mathcal{O}$的极大理想, π为$\mathcal{O}$上的素元. 设$(\widehat{K}, \widehat{\nu})$为$K$的完备化, $\widehat{\mathcal{O}}$为其赋值环, $\widehat{\mathfrak{p}}$为$\widehat{\mathcal{O}}$的极大理想, R为$\mathcal{O}/\mathfrak{p}$的一个代表元系并且$0 \in R$. 则$\widehat{K}^\times$中的每个元素x均可唯一表示为*

$$x = \pi^m \cdot \sum_{i=0}^{\infty} a_i \pi^i,$$

其中$m = \mathrm{ord}_{\widehat{\mathfrak{p}}}(x)$, $a_i \in R$并且$a_0 \neq 0$.

证明: 类似于前面的证明, 我们不妨设ν是一个正则的离散赋值. 因为$\widehat{\nu}$在K上的限制与ν等价, 为了方便, 由命题7.1, 不妨设$\widehat{\nu}$在K上的限制恰好等于ν. 再由注记7.5,

$$\nu(K) = \widehat{\nu}(\widehat{K}) = \mathbb{Z} \cup \{\infty\}.$$

因此, $\widehat{\nu}(\pi) = \nu(\pi) = 1$, 即$\pi$也是$\widehat{\mathcal{O}}$上的素元. 由命题7.6, $\widehat{\mathcal{O}}$是离散赋值环. 因此, 对任意的$x \in \widehat{K}^{\times}$, 元素$x$可以唯一表示为

$$x = \pi^m \cdot \varepsilon,$$

其中$m = \mathrm{ord}_{\widehat{\mathfrak{p}}}(x)$并且$\varepsilon \in \widehat{\mathcal{O}}^{\times}$. 由命题7.8, $\mathcal{O}/\mathfrak{p} \cong \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$. 因此, 存在唯一的$a_0 \in R \setminus \{0\}$使得$\varepsilon \equiv a_0 \pmod{\pi\widehat{\mathcal{O}}}$. 由此, 设$\varepsilon - a_0 = \pi x_1$, 其中$x_1 \in \widehat{\mathcal{O}}$. 对$x_1$进行类似的讨论并且不断重复上面的操作, 就可以把$x$表示为

$$x = \pi^m \cdot \sum_{i=0}^{\infty} a_i \pi^i,$$

其中$m = \mathrm{ord}_{\widehat{\mathfrak{p}}}(x), a_i \in R$并且$a_0 \neq 0$的形式(此时, 级数$\sum_{i=0}^{\infty} a_i\pi^i$在$(\widehat{K}, \widehat{|\cdot|})$显然收敛). 而唯一性的证明几乎是平凡的.

综上, 我们完成了证明. □

为了更好地理解完备的离散赋值域的拓扑结构, 需要介绍一些涉及反向极限的简单理论. 我们首先给出一些定义.

定义 7.9. *设$\mathcal{I}$为非空指标集. 如果对任意的$i, j \in \mathcal{I}$, 存在$k \in \mathcal{I}$使得$i \leq k$且$j \leq k$, 则称$\mathcal{I}$为正向指标集*(directed indexing set).

定义 7.10. *设$\mathcal{I}$为正向指标集, 对任意的$i \in \mathcal{I}$, X_i为拓扑空间. 对任意的$i \leq j$, 映射f_{ji}为$X_j \to X_i$的连续映射. 如果对于任意的$i \leq j \leq k$, 都有交换图*

$$\begin{array}{ccc} X_k & \xrightarrow{f_{kj}} & X_j \\ {\scriptstyle f_{ki}}\downarrow & \swarrow{\scriptstyle f_{ji}} & \\ X_i & & \end{array}$$

则称

$$\{(X_i, f_{ji}) : i, j \in \mathcal{I}且i \leq j\}$$

为一个反向系统.

同调代数中往往利用"泛性质"来定义反向极限, 但在这里暂时并不需要这样做, 我们直接给出如下定义.

定义 7.11. 设$\mathcal{I}$为正向指标集, $\{(X_i, f_{ji}) : i, j \in \mathcal{I}且i \leq j\}$为一个反向系统. 则该反向系统的反向极限定义为乘积空间$\prod_{i\in\mathcal{I}} X_i$的子空间

$$\left\{(x_i)_{i\in\mathcal{I}} \in \prod_{i\in\mathcal{I}} X_i : \ f_{ji}(x_j) = x_i \ \forall i \leq j\right\}.$$

将其记作$\varprojlim_{i\in\mathcal{I}} X_i$.

下面我们来研究反向极限的拓扑性质. 为此, 我们需要一些引理.

引理 7.1. 设X, Y为拓扑空间, 且Y为Hausdorff空间, f, g为$X \to Y$的连续映射. 则

$$C = \{x \in X : \ f(x) = g(x)\}$$

为X的闭子集.

证明: 仅需证明$X \setminus C$为开集. 对任意的$x \in X \setminus C$, 因为Y为Hausdorff空间, 存在$f(x)$的开邻域$V_{f(x)}$以及$g(x)$的开邻域$V_{g(x)}$使得

$$V_{f(x)} \cap V_{g(x)} = \emptyset.$$

因为f, g为连续映射, $U_1 = f^{-1}(V_{f(x)})$以及$U_2 = g^{-1}(V_{g(x)})$均为x的开邻域. 容易验证$U = U_1 \cap U_2$为x的开邻域且$f(z) \neq g(z)$ $(\forall z \in U)$. 这说明$U \subseteq X \setminus C$. 因此$X \setminus C$为开集.

综上, 我们完成了证明. □

利用这个引理, 我们可以得到下面的结果.

命题 7.9. 设$\mathcal{I}$为正向指标集, $\{(X_i, f_{ji}) : i, j \in \mathcal{I}且i \leq j\}$为一个反向系统. 如果每个拓扑空间$X_i$均为Hausdorff空间, 则$\varprojlim_{i\in\mathcal{I}} X_i$为闭子集.

证明: 对任意的$i \in \mathcal{I}$, 设p_i为乘积空间$\prod_{i\in\mathcal{I}} X_i$到$X_i$的自然投射. 对任意的$i \leq j$, 由引理7.1,

$$X_{ji} := \left\{x \in \prod_{i\in\mathcal{I}} X_i : \ p_i(x) = f_{ji} \circ p_j(x)\right\}$$

为闭子集. 因此

$$\varprojlim_{i\in\mathcal{I}} X_i = \bigcap_{i\leq j} X_{ji}$$

也为闭子集.

综上, 我们完成了证明. □

下面的一般性定理可以在后面帮助我们更好地理解完备的离散赋值域的拓扑结构.

定理 7.7. *设$\mathcal{I}$为正向指标集, $\{(X_i, f_{ji}) : i, j \in \mathcal{I}且i \leq j\}$为一个反向系统. 如果每个拓扑空间$X_i$均为非空的紧的Hausdorff空间, 则$\varprojlim_{i\in\mathcal{I}} X_i$为非空紧空间.*

证明: 先说明反向极限非空. 因为X_i均为紧空间, 由Tykhonov定理, 乘积空间$\prod_{i\in\mathcal{I}} X_i$为紧空间. 使用命题7.9证明中的记号. 我们有

$$\varprojlim_{i\in\mathcal{I}} X_i = \bigcap_{i\leq j} X_{ji}.$$

假设$\varprojlim_{i\in\mathcal{I}} X_i = \emptyset$. 因为这些$X_{ji}$为闭子集, 由紧空间中闭子集的有限交性质, 存在有限组$i_1 \leq j_1, i_2 \leq j_2, \cdots, i_n \leq j_n$使得

$$\bigcap_{1\leq r\leq n} X_{j_r i_r} = \emptyset. \tag{7.3}$$

因为$\mathcal{I}$为正向指标集, 取$k \in \mathcal{I}$使得对任意的$1 \leq r \leq n$, 都有$i_r \leq k$且$j_r \leq k$. 此时, 固定X_k中的一个元素y_k. 取乘积空间中的一个元素y使得y的在指标k处的分量为y_k, 在每个指标i_r与j_r处的分量分别为$f_{ki_r}(y_k)$与$f_{kj_r}(y_k)$ $(\forall 1 \leq r \leq n)$. 由反向系统的定义, 容易验证

$$y \in \bigcap_{1\leq r\leq n} X_{j_r i_r}.$$

这与(7.3)矛盾. 因此, 我们得到

$$\varprojlim_{i\in\mathcal{I}} X_i \neq \emptyset.$$

由此以及命题7.9, 反向极限$\varprojlim_{i\in\mathcal{I}} X_i$是紧空间的一个非空闭子集. 因此, 反向极限为非空紧子集.

综上, 我们完成了证明. □

下面我们利用上面的结论来研究完备的离散赋值域. 设(K, ν)为一个完备的离散赋值域, 其中ν为正则的离散赋值, $\mathcal{O}$为其赋值环, $\mathfrak{p}$为$\mathcal{O}$的极大理想.

对任意的$n \in \mathbb{Z}^+$, 商环$\mathcal{O}/\mathfrak{p}^n$上的拓扑为自然满同态$f_n : \mathcal{O} \twoheadrightarrow \mathcal{O}/\mathfrak{p}^n$所确定的商拓扑. 也就是说,

$$V \subseteq \mathcal{O}/\mathfrak{p}^n为开集 \Leftrightarrow f_n^{-1}(V)为子空间\mathcal{O}中的开集.$$

注意到

$$f_n^{-1}(0 \bmod \mathfrak{p}^n) = \mathfrak{p}^n$$

为开集. 因此这些商空间$\mathcal{O}/\mathfrak{p}^n$均为离散空间. 对于任意的正整数$i \leq j$, 定义同态

$$f_{ji} : \mathcal{O}/\mathfrak{p}^j \to \mathcal{O}/\mathfrak{p}^i$$

为$f_{ji}(x \bmod \mathfrak{p}^j) = x \bmod \mathfrak{p}^i$. 容易验证$f_{ji}$的定义是合理的, 并且因为$\mathcal{O}/\mathfrak{p}^j$为离散空间, 这些同态$f_{ji}$是连续映射. 由上面的讨论,

$$\left\{(\mathcal{O}/\mathfrak{p}^n, f_{mn}) : m, n \in \mathbb{Z}^+ \text{且} n \leq m\right\}$$

构成了一个反向系统. 并且此时, $\varprojlim_{n\in\mathbb{Z}^+} \mathcal{O}/\mathfrak{p}^n$有一个显然的环结构. 类似地,

$$\left\{\left(\mathcal{O}^\times/U^{(n)}, g_{mn}\right) : m, n \in \mathbb{Z}^+ \text{且} n \leq m\right\},$$

也为一个反向系统, 其中$U^{(n)} = 1 + \mathfrak{p}^n$,

$$g_{mn}(x \bmod U^{(m)}) = x \bmod U^{(n)}.$$

我们有下面的定理.

定理 7.8. *记号如上. 则下列拓扑同构成立.*

(i) $\mathcal{O} \underset{topological}{\cong} \varprojlim_{n\in\mathbb{Z}^+} \mathcal{O}/\mathfrak{p}^n$.

(ii) $\mathcal{O}^\times \underset{topological}{\cong} \varprojlim_{n\in\mathbb{Z}^+} \mathcal{O}^\times/U^{(n)}$.

证明: 我们只证明(i). (ii)的证明是类似的. 设同态

$$\varphi : \mathcal{O} \to \varprojlim_{n\in\mathbb{Z}^+} \mathcal{O}/\mathfrak{p}^n$$

为$\varphi(x) = (x \bmod \mathfrak{p}^n)_{n\in\mathbb{Z}^+}$. 下面说明$\varphi$是一个拓扑同构.

首先, 因为

$$\bigcap_{n\in\mathbb{Z}^+} \mathfrak{p}^n = \{0\},$$

同态φ为单同态. 设π为$\mathcal{O}$的一个素元. 对于任意的$(x_n \bmod \mathfrak{p}^n)_{n\in\mathbb{Z}^+} \in \varprojlim_{n\in\mathbb{Z}^+} \mathcal{O}/\mathfrak{p}^n$, 因为

$$x_n \equiv x_{n-1} \pmod{\pi^n\mathcal{O}} \ (\forall n \in \mathbb{Z}_{\geq 2}),$$

存在$\mathcal{O}$中的元素$a_0, a_1, \cdots, a_n, \cdots$使得

$$x_n = a_0 + a_1\pi + a_2\pi^2 + \cdots + a_{n-1}\pi^{n-1} \ (\forall n \in \mathbb{Z}^+).$$

因为(K, ν)是完备的并且$\mathcal{O}$是闭子集, 赋值环$\mathcal{O}$是完备的. 因此

$$x = \sum_{i=0}^{\infty} a_i \pi^i \in \mathcal{O}$$

使得$\varphi(x) = (x_n \bmod \mathfrak{p}^n)_{n\in\mathbb{Z}^+}$, 即$\varphi$为满同态.

下面我们来说明φ是同胚. 先说明φ是连续映射. 对任意的非空有限集$I \subseteq \mathbb{Z}^+$, 令

$$U_I := \left(\prod_{n\in I} \{0 \bmod \mathfrak{p}^n\} \times \prod_{n\in\mathbb{Z}^+\setminus I} \mathcal{O}/\mathfrak{p}^n \right) \bigcap \varprojlim_{n\in\mathbb{Z}^+} \mathcal{O}/\mathfrak{p}^n.$$

则这些U_I恰好为$\varprojlim\limits_{n\in\mathbb{Z}^+} \mathcal{O}/\mathfrak{p}^n$中零元素的一组开邻域基. 容易验证

$$\varphi^{-1}(U_I) = \mathfrak{p}^r,$$

其中$r = \max I$. 注意到$\varprojlim\limits_{n\in\mathbb{Z}^+} \mathcal{O}/\mathfrak{p}^n$是拓扑环, 上式说明$\varphi$是连续映射. 由上面的讨论, 要证明$\varphi$是同胚, 现在仅需说明$\varphi$是开映射即可. 对任意的$n \in \mathbb{Z}^+$, 容易验证

$$\varphi(\mathfrak{p}^n) = U_{I_n},$$

其中$I_n = \{1, 2, \cdots, n\}$. 注意到这些$\mathfrak{p}^n$为0的一组开邻域基并且$\mathcal{O}$是拓扑环, 上式说明$\varphi$是开映射. 结合上面的讨论, φ是同胚.

综上, 我们完成了证明. □

7.4 Hensel引理

Hensel引理是研究完备的非阿基米德赋值域的一个重要工具. 我们在这里介绍两个结论, 一个与赋值环上的多项式分解有关, 另一个与赋值环上多元多项式的零点有关.

定理 7.9. *设$(K, |\cdot|)$为完备的非阿基米德赋值域, $\mathcal{O}$为其赋值环, $\mathfrak{p}$为$\mathcal{O}$的极大理想. 设多项式$f(t) \in \mathcal{O}[t]$并且$|f| = 1$, 设*

$$\overline{f}(t) = f(t) \bmod \mathfrak{p} \in (\mathcal{O}/\mathfrak{p})[t]$$

为$f(t)$模$\mathfrak{p}$的约化. 如果存在$(\mathcal{O}/\mathfrak{p})[t]$上互素的多项式$\tilde{g}(t)$与$\tilde{h}(t)$使得

$$\overline{f}(t)=\tilde{g}(t)\cdot\tilde{h}(t),$$

则存在$g(t),h(t)\in\mathcal{O}[t]$使得

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

$\deg(g(t))=\deg(\tilde{g}(t))$, $g(t)\bmod\mathfrak{p}=\tilde{g}(t)$并且$h(t)\bmod\mathfrak{p}=\tilde{h}(t)$.

证明: 采用递推构造的方法.

取多项式$g_0(t),h_0(t)\in\mathcal{O}[t]$使得$\deg(g_0(t))=\deg(\tilde{g}(t))$, $\deg(h_0(t))\leq\deg(f(t))-\deg(g_0(t))$, $g_0(t)\bmod\mathfrak{p}=\tilde{g}(t)$并且$h_0(t)\bmod\mathfrak{p}=\tilde{h}(t)$. 此时显然有

$$f(t)\equiv g_0(t)h_0(t)\ (\mathrm{mod}\ \mathfrak{p}).$$

如果$f(t)-g_0(t)h_0(t)=0$, 则直接令$g(t)=g_0(t),h=h_0(t)$即可.

下面假设$f(t)-g_0(t)h_0(t)\neq 0$. 因为$\tilde{g}$与$\tilde{h}$在$(\mathcal{O}/\mathfrak{p})[t]$上互素, 存在多项式$a(t),b(t)\in\mathcal{O}[t]$使得

$$a(t)g_0(t)+b(t)h_0(t)-1\equiv 0\ (\mathrm{mod}\ \mathfrak{p}).$$

令$f(t)-g_0(t)h_0(t)$以及$a(t)g_0(t)+b(t)h_0(t)-1$的所有非零系数中, 乘积赋值最小的系数为π.

对任意的正整数$n\geq 1$, 假设我们已经构造了多项式

$$g_{n-1}(t)=g_0(t)+\pi p_1(t)+\cdots+\pi^{n-1}p_{n-1}(t),$$

以及

$$h_{n-1}(t)=h_0(t)+\pi q_1(t)+\cdots+\pi^{n-1}q_{n-1}(t),$$

其中这些$p_i(t),q_i(t)\in\mathcal{O}[t]$, $\deg(p_i(t))<\deg(g_0(t))=\deg(\tilde{g}(t))$, $\deg(q_i(t))\leq\deg(f(t))-\deg(g_0(t))$, 并且

$$g_{n-1}(t)h_{n-1}(t)\equiv f(t)\ (\mathrm{mod}\ \pi^n\mathcal{O}[t]).$$

下面来构造$g_n(t)$与$h_n(t)$. 首先设

$$f(t)-g_{n-1}(t)h_{n-1}(t)=\pi^n\Delta_n(t),$$

其中$\Delta_n(t) \in \mathcal{O}[t]$并且$\deg(\Delta_n(t)) \leq \deg(f)$. 设

$$g_n(t) = g_{n-1}(t) + \pi^n p_n^*(t),$$

$$h_n(t) = h_{n-1}(t) + \pi^n q_n^*(t)$$

(其中$p_n^*(t), q_n^*(t) \in \mathcal{O}[t]$待定)使得

$$g_n(t)h_n(t) \equiv f(t) \pmod{\pi^{n+1}\mathcal{O}[t]}. \tag{7.4}$$

由简单的计算, (7.4)等价于

$$g_{n-1}(t)q_n^*(t) + h_{n-1}(t)p_n^* \equiv \Delta_n(t) \pmod{\pi\mathcal{O}[t]}. \tag{7.5}$$

注意到π是$f(t) - g_0(t)h_0(t)$以及$a(t)g_0(t) + b(t)h_0(t) - 1$的所有非零系数中, 乘积赋值最小的. 由$g_{n-1}(t)$与$h_{n-1}(t)$的构造, 我们得到

$$g_{n-1}(t)a(t) + h_{n-1}(t)b(t) \equiv 1 \pmod{\pi\mathcal{O}[t]}.$$

这说明存在$p_n^*(t), q_n^*(t) \in \mathcal{O}[t]$使得(7.5)成立. 设

$$p_n^*(t) = x_n(t)g_{n-1}(t) + p_n(t),$$

其中$p_n(t) = 0$或者$\deg(p_n(t)) < \deg(g_{n-1}(t)) = \deg(g_0(t))$. 将其带入(7.5), 我们得到

$$g_{n-1}(t)q_n(t) + h_{n-1}(t)p_n(t) \equiv \Delta_n(t) \pmod{\pi\mathcal{O}[t]},$$

其中$\deg(p_n(t)) < \deg(g_0(t))$, 并且$q_n(t)$为去掉$q_n^*(t) + h_{n-1}(t)x_n(t)$中那些系数在$\pi\mathcal{O}$中的项后得到的多项式. 则此时$\deg(q_n) = \deg(q_n \bmod \pi\mathcal{O})$. 由上面的讨论容易验证

$$\begin{aligned}\deg(g_{n-1} \bmod \pi\mathcal{O}) + \deg(q_n) &= \deg\left((\Delta_n - h_{n-1}p_n) \bmod \pi\mathcal{O}[t]\right) \\ &\leq \deg(f).\end{aligned}$$

这说明$\deg(q_n) \leq \deg(f) - \deg(g_{n-1}) = \deg(f) - \deg(\tilde{g})$. 这样就完成了构造. 也就是说, 对任意的整数$n \geq 0$, 假设存在多项式

$$g_n(t) = g_0(t) + \pi p_1(t) + \cdots + \pi^n p_n(t),$$

以及

$$h_n(t) = h_0(t) + \pi q_1(t) + \cdots + \pi^n q_n(t)$$

(其中这些$p_i(t), q_i(t) \in \mathcal{O}[t], \deg(p_i(t)) < \deg(g_0(t)) = \deg(\tilde{g}(t)), \deg(q_i(t)) \leq \deg(f(t)) - \deg(g_0(t))$使得

$$g_n(t)h_n(t) \equiv f(t) \pmod{\pi^{n+1}\mathcal{O}[t]}.$$

因为$(K, |\cdot|)$是完备的非阿基米德赋值域并且赋值环$\mathcal{O}$是闭子集, 我们得到$\mathcal{O}$是完备的. 因此,

$$g(t) = \lim_{n\to+\infty} g_n(t),\ h(t) = \lim_{n\to+\infty} h_n(t)$$

就是满足定理条件的多项式.

综上, 我们完成了证明. □

注记 7.6. 这个形式的Hensel引理说明, 在完备的非阿基米德赋值域上, 可以通过讨论多项式在剩余类域$\mathcal{O}/\mathfrak{p}$上的分解来研究多项式在$\mathcal{O}[t]$上的分解.

定理7.9有一个非常有用的推论.

推论 7.2. 设$(K, |\cdot|)$为完备的非阿基米德赋值域, $\mathcal{O}$为其赋值环, $\mathfrak{p}$为$\mathcal{O}$的极大理想. 如果

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n \in K[t]$$

为不可约多项式(其中$a_0 a_n \neq 0$). 则

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

证明: 使用反证法. 假设$|f| > \max\{|a_0|, |a_n|\}$. 则存在$0 < i < n$使得

$$|f| = |a_i|,\ \text{并且} |a_j| < |a_i|\ (\forall 0 \leq j < i).$$

注意$a_i \neq 0$并且此时$\frac{1}{a_i} f \bmod \mathfrak{p}$在剩余类域$\mathcal{O}/\mathfrak{p}$上可以分解为两个互素的多项式乘积, 并且其中一个多项式的次数为i. 由定理7.9, 多项式$\frac{1}{a_i} f$在$\mathcal{O}[t]$上可约. 这显然矛盾.

综上, 我们完成了证明.

下面我们介绍另外一种形式的Hensel引理, 它与赋值环上多元多项式的零点有关.

定理 7.10. 设(K,ν)为一个完备的离散赋值域, ν是正则的离散赋值, $\mathcal{O}$为其赋值环, $\mathfrak{p}$为$\mathcal{O}$的极大理想. 设$f(t_1,t_2,\cdots,t_n)\in\mathcal{O}[t_1,t_2,\cdots,t_n]$为一个$n$元多项式. 如果存在$a_1,a_2,\cdots,a_n\in\mathcal{O}$, $\delta\in\mathbb{Z}_{\geq 0}$以及某个$1\leq i\leq n$使得

$$\begin{cases} F(a_1,a_2,\cdots,a_n) & \equiv 0\ (\mathrm{mod}\ \mathfrak{p}^{2\delta+1}),\\ \frac{\partial F}{\partial t_i}(a_1,a_2,\cdots,a_n) & \equiv 0\ (\mathrm{mod}\ \mathfrak{p}^{\delta}),\\ \frac{\partial F}{\partial t_i}(a_1,a_2,\cdots,a_n) & \not\equiv 0\ (\mathrm{mod}\ \mathfrak{p}^{\delta+1}) \end{cases}$$

(约定$\mathfrak{p}^0=\mathcal{O}$), 则存在$\theta_1,\theta_2,\cdots,\theta_n\in\mathcal{O}$使得

$$F(\theta_1,\theta_2,\cdots,\theta_n)=0,$$

并且

$$\theta_j\equiv a_j\ (\mathrm{mod}\ \mathfrak{p}^{\delta+1})\ (\forall 1\leq j\leq n).$$

证明: 使用递推构造的方法. 设

$$f(t)=F(a_1,\cdots,a_{i-1},t,a_{i+1},\cdots,a_n).$$

设π为$\mathcal{O}$的素元. 下面我们来构造一个$\mathcal{O}$上的Cauchy序列$\{\alpha_m\}_{m=0}^{\infty}$使得

$$f(\alpha_m)\equiv 0\ (\mathrm{mod}\ \pi^{2\delta+1+m}),$$

并且$\alpha_m\equiv a_i\ (\mathrm{mod}\ \pi^{\delta+1}\mathcal{O})\ (\forall m\in\mathbb{Z}_{\geq 0})$. 令$\alpha_0=a_i$. 假设$m\geq 1$并且满足要求的$\alpha_{m-1}$已经构造完成. 下面来构造$\alpha_m$. 设

$$f(t)=f(\alpha_{m-1})+f'(\alpha_{m-1})(t-\alpha_{m-1})t+\text{高次项},$$

由归纳假设, 存在$b_0\in\mathcal{O}$使得$f(\alpha_{m-1})=\pi^{2\delta+m}b_0$. 因为$\alpha_{m-1}\equiv a_i\ (\mathrm{mod}\ \mathfrak{p}^{\delta+1})$, 我们有

$$\begin{aligned} f'(\alpha_{m-1})\equiv f'(a_i)=\frac{\partial F}{\partial t_i}(a_1,a_2,\cdots,a_n)\equiv 0\ (\mathrm{mod}\ \mathfrak{p}^{\delta}),\\ f'(\alpha_{m-1})\equiv f'(a_i)=\frac{\partial F}{\partial t_i}(a_1,a_2,\cdots,a_n)\not\equiv 0\ (\mathrm{mod}\ \mathfrak{p}^{\delta+1}). \end{aligned}$$

因此, 存在$b_1\in\mathcal{O}^{\times}$使得$f'(\alpha_{m-1})=\pi^{\delta}b_1$. 令$x=\alpha_{m-1}+\xi_m\pi^{\delta+m}$, 其中$\xi_m\in\mathcal{O}$待定. 则由上面的讨论

$$f(x)\equiv 0\ (\mathrm{mod}\ \pi^{2\delta+1+m}\mathcal{O})\Leftrightarrow b_0+b_1\xi\equiv 0\ (\mathrm{mod}\ \pi\mathcal{O}).$$

此时, 令$\xi_m = -b_1^{-1}b_0 \in \mathcal{O}$, 并且设

$$\alpha_m = \alpha_{m-1} + \xi_m \pi^{m+\delta}.$$

则容易验证

$$\begin{cases} f(\alpha_m) & \equiv 0 \ (\mathrm{mod}\ \pi^{2\delta+1+m}\mathcal{O}), \\ \alpha_m - \alpha_{m-1} & \equiv 0 \ (\mathrm{mod}\ \pi^{m+\delta}\mathcal{O}), \\ \alpha_m & \equiv a_i \ (\mathrm{mod}\ \pi^{\delta+1}\mathcal{O}). \end{cases}$$

显然$\{\alpha_m\}_{m=0}^{\infty}$为完备的拓扑空间$\mathcal{O}$上的Cauchy列. 令

$$\begin{cases} \theta_i = \lim\limits_{m\to\infty} \alpha_m, \\ \theta_j = a_j \ (\forall j \neq i). \end{cases}$$

则有

$$F(\theta_1, \theta_2, \cdots, \theta_n) = f(\theta_i) = \lim_{m\to+\infty} f(\alpha_m) = 0,$$

并且$\theta_j \equiv a_j \ (\mathrm{mod}\ \mathfrak{p}^{\delta+1})\ (\forall 1 \leq j \leq n)$.

综上, 我们完成了证明. □

7.5 赋值的延拓

在本节中, 我们来研究赋值的延拓. 首先考虑完备的赋值域上赋值的延拓. 我们从下面的命题开始.

命题 7.10. *设$(K, |\cdot|)$是完备的赋值域(阿基米德与非阿基米德均可), V为K上的n维向量空间. 固定V上的一组基$\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_n$. 对任意的$\boldsymbol{x} = x_1\boldsymbol{v}_1 + \cdots + x_n\boldsymbol{v}_n \in V$, 定义$V$上的范数$||\cdot||_\infty$为*

$$||x||_\infty := \max\{|x_i| : \ 1 \leq i \leq n\}.$$

则V上任意范数$||\cdot||$均与$||\cdot||_\infty$等价. 并且此时

$$V \underset{topological}{\cong} K^n$$

是一个完备的赋范线性空间.

证明: 命题第二部分的结论是显然的. 我们仅需证明$||\cdot||$与$||\cdot||_\infty$等价, 即存在$a, b > 0$使得

$$a||\boldsymbol{x}||_\infty \leq ||\boldsymbol{x}|| \leq b||\boldsymbol{x}||_\infty \ (\forall \boldsymbol{x} \in V).$$

首先b是容易确定的. 事实上, 对任意的$\boldsymbol{x}=x_1\boldsymbol{v}_1+\cdots+x_n\boldsymbol{v}_n\in V$,

$$||\boldsymbol{x}||\leq\sum_{i=1}^{n}|x_i|\cdot||\boldsymbol{v}_i||\leq\left(\sum_{i=1}^{n}||\boldsymbol{v}_i||\right)\cdot||\boldsymbol{x}||_\infty.$$

因此, 我们可以取

$$b=\sum_{i=1}^{n}||\boldsymbol{v}_i||.$$

下面我们通过对n归纳来证明正实数a的存在性. 当$n=1$时, 令$a=||\boldsymbol{v}_1||$即可. 下面假设$n\geq 2$, 并且对于K的任意$n-1$维赋范线性空间, 我们都可以找到这样的a. 由此以及上面的讨论, K的任意$n-1$维赋范线性空间均是完备的. 对任意的$1\leq i\leq n$, 定义于K的任意$n-1$维赋范线性空间

$$V_i=K\boldsymbol{v}_1+\cdots+K\boldsymbol{v}_{i-1}+K\boldsymbol{v}_{i+1}+\cdots+K\boldsymbol{v}_n.$$

因为这些V_i是完备的, 集合

$$\bigcup_{i=1}^{n}(V_i+\boldsymbol{v}_i)$$

是闭集. 由此以及

$$\boldsymbol{0}\notin\bigcup_{i=1}^{n}(V_i+\boldsymbol{v}_i),$$

我们得到存在正常数$a>0$使得

$$B(\boldsymbol{0},a)\bigcap\left(\bigcup_{i=1}^{n}(V_i+\boldsymbol{v}_i)\right)=\emptyset,$$

其中

$$B(\boldsymbol{0},a)=\{\boldsymbol{x}\in V:\ ||\boldsymbol{x}||<a\}.$$

此时, 对任意的$\boldsymbol{x}=x_1\boldsymbol{v}_1+\cdots+x_n\boldsymbol{v}_n\in V\setminus\{\boldsymbol{0}\}$, 不妨设$|x_i|=||\boldsymbol{x}||_\infty>0$. 则$\frac{1}{x_i}\boldsymbol{x}\in V_i$. 因此

$$\left|\left|\frac{1}{x_i}\boldsymbol{x}\right|\right|\geq a.$$

这说明

$$a||\boldsymbol{x}||_\infty\leq||\boldsymbol{x}||\ (\forall\boldsymbol{x}\in V).$$

因此, 正常数a是存在的. 由上面的讨论, 范数$||\cdot||$与$||\cdot||_\infty$等价.

综上, 我们完成了证明. □

完备的赋值域上赋值的延拓是容易的. 我们有如下定理.

定理 7.11. 设$(K,|\cdot|)$是完备的赋值域(阿基米德与非阿基米德均可). 对K的任意代数扩张L(有限扩张与无限扩张均可), 赋值$|\cdot|$有且仅有一种方式延拓到L上. 特别地, 当L/K为有限代数扩张时, 该延拓为

$$|x| = |\mathrm{N}_{L/K}(x)|^{\frac{1}{[L:K]}} \ (\forall x \in L).$$

并且此时, 有限扩张L在此赋值定义的拓扑下是一个完备的赋值域.

证明: 当$(K,|\cdot|)$是完备的阿基米德赋值域时, 由定理7.4, 结论显然成立.

下面设$(K,|\cdot|)$是完备的非阿基米德赋值域. 因为

$$L = \prod_{\substack{K\subseteq M\subseteq L \\ M/K\text{为有限扩张}}} M,$$

仅需考虑L/K为有限扩张的情形. 设$\mathcal{O}_K$为$|\cdot|$在K上的赋值环, B为$\mathcal{O}_K$在L中的整闭包. 我们断言

$$B = \left\{x \in L : \ \left|\mathrm{N}_{L/K}(x)\right| \leq 1\right\}. \tag{7.6}$$

事实上, 对任意的$x \in L$, 设

$$p_x(t) = t^m + a_{m-1}t^{m-1} + \cdots + a_1 t + a_0 \in K[t]$$

为x在K上的极小多项式. 因为$\mathcal{O}_K$为整闭整环, 由命题1.1,

$$x \in B \Leftrightarrow p_x(t) \in \mathcal{O}_K[t].$$

再由推论7.2, 对于不可约多项式$p_x(t)$, 我们有

$$|p_x(t)| = \max\{1, |a_0|\}.$$

由上面的讨论, 并注意到$\mathrm{N}_{L/K}(x) = \pm a_0^{[L:K(x)]}$ (命题1.2), 我们得到

$$x \in B \Leftrightarrow p_x(t) \in \mathcal{O}_K[t] \Leftrightarrow |a_0| \leq 1 \Leftrightarrow \left|\mathrm{N}_{L/K}(x)\right| \leq 1.$$

因此, (7.6)成立.

设$[L:K] = n$. 下面来说明$|\cdot|^{\frac{1}{n}} \circ \mathrm{N}_{L/K}$是$L$上的赋值. 此时, 仅需说明其满足强三角不等式. 对任意的$x, y \in L^\times$, 不妨设

$$|\mathrm{N}_{L/K}(x)|^{\frac{1}{n}} \leq |\mathrm{N}_{L/K}(y)|^{\frac{1}{n}}.$$

注意到此时$|\mathrm{N}_{L/K}(x/y)| \leq 1$. 则由(7.6), 元素$x/y \in B$. 注意到$B$是环. 我们有$1 + x/y \in B$. 再由(7.6),

$$\left|\mathrm{N}_{L/K}\left(1+\frac{x}{y}\right)\right|^{\frac{1}{n}} \leq 1.$$

这说明,

$$\left|\mathrm{N}_{L/K}(x+y)\right|^{\frac{1}{n}} \leq \left|\mathrm{N}_{L/K}(y)\right|^{\frac{1}{n}} = \max\left\{\left|\mathrm{N}_{L/K}(x)\right|^{\frac{1}{n}}, \left|\mathrm{N}_{L/K}(y)\right|^{\frac{1}{n}}\right\},$$

即强三角不等式成立. 因此, $|\cdot|^{\frac{1}{n}} \circ \mathrm{N}_{L/K}$是$L$上的赋值. 并且利用范数的性质, 容易说明其是$|\cdot|$在$L$上的延拓.

下面来说明延拓的唯一性. 设$|\cdot|_*$是$|\cdot|$在L上的一个延拓. 对任意的

$$y \in \{z \in L : |z|_* \leq 1\},$$

设

$$p_y(t) = t^r + b_{r-1}t^{r-1} + \cdots + b_1 t + b_0 \in K[t]$$

为y在K上的极小多项式. 由推论7.2,

$$|p_y(t)| = \max\{1, |b_0|\}.$$

如果$|b_0| > 1$, 则由命题7.2,

$$0 = \left|y^r + b_{r-1}y^{r-1} + \cdots + b_1 y + b_0\right|_* = |b_0| > 1,$$

这显然矛盾. 因此$|b_0| \leq 1$, 即$p_y(t) \in \mathcal{O}_K[t]$. 由(7.6), 我们得到

$$|y|_* \leq 1 \Rightarrow y \in B \Rightarrow \left|\mathrm{N}_{L/K}(y)\right|^{1/n} \leq 1.$$

因此, 由注记7.2, 赋值$|\cdot|_*$与$|\cdot|^{\frac{1}{n}} \circ \mathrm{N}_{L/K}$等价. 注意到它们在$K$上的限制为相同的非平凡赋值. 由命题7.1, 我们得到

$$|\cdot|_* = |\cdot|^{\frac{1}{n}} \circ \mathrm{N}_{L/K}.$$

再由命题7.10, 当L/K为有限扩张时, L必为完备的赋范线性空间.

综上, 我们完成了证明. □

注记 7.7. (i) 当L/K为无限代数扩张时, L不一定是完备的. 例如$\mathbb{Q}_p^{\mathrm{alg}}$就是一个不完备的赋值域(我们后面会详细介绍).

(ii) 定理的证明中蕴藏了一个今后我们会经常使用的结果. 事实上, 当赋值域$(K,|\cdot|)$是完备的非阿基米德赋值域时, 由(7.6), 对于有限扩张L/K, 我们得到$|\cdot|^{\frac{1}{n}}\circ \mathrm{N}_{L/K}$在$L$上的赋值环恰好是$\mathcal{O}_K$在$L$中的整闭包.

下面介绍两个后面经常会遇到的量.

定义 7.12. 设(K,ν)为离散赋值域, L/K为域的有限扩张, ω为L的赋值满足$\omega|K=\nu$. 定义ω对ν的分歧指数

$$e(\omega|\nu):=\left[\omega(L^\times):\nu(K^\times)\right].$$

设$\mathcal{O}_K,\mathcal{O}_L$分别为$\nu$在$K$上与$\omega$在$L$上的赋值环, $\mathfrak{p}_K,\mathfrak{P}_L$分别为$\mathcal{O}_K$与$\mathcal{O}_L$上的极大理想. 定义$\omega$对$\nu$的惯性次数

$$f(\omega|\nu):=\left[\mathcal{O}_L/\mathfrak{P}_L:\mathcal{O}_K/\mathfrak{p}_K\right].$$

关于e与f我们有如下结果.

命题 7.11. 设(K,ν)为离散赋值域, L/K为域的有限扩张, ω为L上的赋值并且满足$\omega|K=\nu$. 则

$$[L:K]\geq e(\omega|\nu)\cdot f(\omega|\nu).$$

更进一步, 如果(K,ν)为完备的离散赋值域并且L/K为域的有限可分扩张, 则

$$[L:K]=e(\omega|\nu)\cdot f(\omega|\nu).$$

证明: 首先我们说明当$[L:K]<\infty$时, 必有$f(\omega|\nu)<\infty$. 设$x_1,x_2,\cdots,x_m\in\mathcal{O}_L$使得这些$\bar{x}_i:=x_i \bmod \mathfrak{P}_L$在$\mathcal{O}_K/\mathfrak{p}_K$上线性无关. 我们断言这些$x_i$一定$K$线性无关. 事实上, 假设存在$K$中不全为0的元素$a_1,a_2,\cdots,a_m$使得

$$a_1x_1+a_2x_2+\cdots+a_mx_m=0.$$

设

$$|a_r|=\max\{|a_i|:\ 1\leq i\leq m\}>0.$$

则由上式, 存在$b_1,\cdots,b_{r-1},b_{r+1},\cdots,b_m\in\mathcal{O}_K$使得

$$b_1x_1+\cdots+b_{r-1}x_{r-1}+x_r+b_{r+1}x_{r+1}+\cdots+b_mx_m=0.$$

上式两边模$\mathfrak{P}_L$得到这些$\bar{x}_i$在$\mathcal{O}_K/\mathfrak{p}_K$上线性相关. 这显然矛盾. 由上面的讨论, 我们得到$f(\omega|\nu)<\infty$.

设

$$\pi_1, \cdots, \pi_e \in L^\times$$

使得这些$\omega(\pi_i)$为$\omega(L^\times)/\nu(K^\times)$的一个代表元系. 设

$$x_1, x_2, \cdots, x_f \in \mathcal{O}_L$$

使得这些$\bar{x}_j$恰好为$\mathcal{O}_L/\mathfrak{P}_L$的一组$\mathcal{O}_K/\mathfrak{p}_K$-基.

(i) 下面来证明第一个不等式. 为此仅需说明这些$\pi_i x_j (1 \leq i \leq e, 1 \leq j \leq f)$在$K$上线性无关. 假设存在不全为的$a_{ij} \in K$ $(1 \leq i \leq e, 1 \leq j \leq f)$使得

$$\sum_{1 \leq i \leq e} \sum_{1 \leq j \leq f} a_{ij} \pi_i x_j = \sum_{1 \leq i \leq e} c_i \pi_i = 0,$$

其中

$$c_i = \sum_{1 \leq j \leq f} a_{ij} x_j.$$

由一开始的讨论, 这些x_j在K上线性无关. 因此, 当a_{ij}不全为0时, 这些c_i也不全为0. 并且, 当$c_s \neq 0$时, 设

$$|a_{sr}| = \max\{|a_{sj}| : 1 \leq j \leq f\} > 0.$$

因为这些$\bar{x}_j$为恰好为$\mathcal{O}_L/\mathfrak{P}_L$的一组$\mathcal{O}_K/\mathfrak{p}_K$-基, 我们得到

$$\sum_{1 \leq j \leq f} \frac{a_{sj}}{a_{sr}} x_j \not\equiv 0 \pmod{\mathfrak{P}_L},$$

即

$$\sum_{1 \leq j \leq f} \frac{a_{sj}}{a_{sr}} x_j \in \mathcal{O}_L^\times.$$

由此,

$$\omega(c_s) = \omega(a_{sr}) \cdot \omega\left(\sum_{1 \leq j \leq f} \frac{a_{sj}}{a_{sr}} x_j\right) = \nu(a_{sr}) \in \nu(K^\times).$$

另一方面, 因为

$$\sum_{1 \leq i \leq e} c_i \pi_i = 0$$

并且这些c_i不全为0, 由命题7.2, 存在$1 \leq s_1 < s_2 \leq e$使得$c_{s_1} c_{s_2} \neq 0$并且

$$\omega(c_{s_1} \pi_{s_1}) = \omega(c_{s_2} \pi_{s_2}).$$

由上面的讨论, 我们得到

$$\omega(\pi_{s_1}) - \omega(\pi_{s_2}) = \omega\left(c_{s_1}/c_{s_2}\right) \in \nu(K^\times).$$

这与这些π_i的定义矛盾. 因此, $\pi_i x_j (1 \leq i \leq e, 1 \leq j \leq f)$在$K$上线性无关. 这说明

$$[L : K] \geq e(\omega|\nu) \cdot f(\omega|\nu).$$

(ii) 下面假设(K, ν)是完备的赋值域且L/K为域的有限可分扩张. 为了方便, 不妨设此时ν为K上的正则离散赋值并且$[L : K] = n$. 由定理7.11, 对任意的$x \in L$,

$$\omega(x) = \frac{1}{n} \cdot \nu\left(\mathrm{N}_{L/K}(x)\right) \in \frac{1}{n}\mathbb{Z}.$$

由此以及$\mathbb{Z} = \nu(K^\times) \subseteq \omega(L^\times)$, 我们得到$\omega(L^\times)$是$\frac{1}{n}\mathbb{Z}$的秩为1的子$\mathbb{Z}$模. 这说明$\omega$是一个离散赋值. 因此, 设$\pi_L$为$\mathcal{O}_L$的素元. 则容易验证

$$\omega(L^\times) = \{\omega(\pi_L)^r : \ r \in \mathbb{Z}\}.$$

设

$$\pi_L^0, \pi_L^1, \cdots, \pi_L^{e-1}$$

使得这些$\omega(\pi_L^i)$为$\omega(L^\times)/\nu(K^\times)$的一个代表元系. 注意此时

$$\omega(\pi_L) = \frac{1}{e}.$$

设

$$x_1, x_2, \cdots, x_f \in \mathcal{O}_L$$

使得这些$\bar{x}_j$为$\mathcal{O}_L/\mathfrak{P}_L$的一组$\mathcal{O}_K/\mathfrak{p}_K$-基. 由(i)的证明, 这些$\pi_L^i x_j$在$K$上线性无关. 下面来说明这些$\pi_L^i x_j$恰好为$\mathcal{O}_L$关于$\mathcal{O}_K$的一组整基. 设$\pi_K$为$\mathcal{O}_K$的素元,

$$M := \sum_{i=0}^{e-1} \sum_{j=1}^{f} \mathcal{O}_K \pi_L^i x_j = \mathcal{O}_L,$$

以及

$$N := \sum_{1 \leq j \leq f} \mathcal{O}_K x_j.$$

则

$$M = N + \pi_L N + \cdots + \pi_L^{e-1} N.$$

因为这些$\bar{x}_j$为恰好为$\mathcal{O}_L/\mathfrak{P}_L$的一组$\mathcal{O}_K/\mathfrak{p}_K$-基, 我们得到

$$\mathcal{O}_L = N + \pi_L \mathcal{O}_L.$$

重复利用这个式子, 我们得到

$$\begin{aligned}\mathcal{O}_L = N + \pi_L \mathcal{O}_L &= N + \pi_L N + \pi_L^2 \mathcal{O}_L \\ &= \cdots \\ &= N + \pi_L N + \pi_L^2 N + \cdots + \pi_L^{e-1} N + \pi_L^e \mathcal{O}_L \\ &= M + \pi_K \mathcal{O}_L,\end{aligned}$$

其中最后一个等式成立是因为

$$\pi_L^e \in \pi_K \cdot \mathcal{O}_L^\times.$$

由注记7.7, 赋值环$\mathcal{O}_L$恰好为$\mathcal{O}_K$在L中的整闭包. 因为$\mathcal{O}_K$为离散赋值环且L/K为有限可分扩张, 由定理1.2, 我们知道$\mathcal{O}_L$是有限生成$\mathcal{O}_K$模. 由上面的讨论以及引理4.1(中山引理),

$$M + \pi_K \mathcal{O}_L = \mathcal{O}_L \Rightarrow M = \mathcal{O}_L.$$

因此, 当(K, ν)为完备的离散赋值域并且L/K为域的有限可分扩张时,

$$[L : K] = e(\omega|\nu) \cdot f(\omega|\nu).$$

综上, 我们完成了证明. □

注记 7.8. *在上述证明中, 我们得到了一个很有用的结论: 设(K, ν)为完备的离散赋值域并且L/K为域的有限可分扩张, π_L为$\mathcal{O}_L$的素元, $x_1, x_2, \cdots, x_f \in \mathcal{O}_L$ 使得这些$\bar{x}_j$为$\mathcal{O}_L/\mathfrak{P}_L$的一组$\mathcal{O}_K/\mathfrak{p}_K$-基. 则此时这些*

$$\pi_L^i x_j \ (0 \leq i \leq e-1, 1 \leq j \leq f)$$

恰好为$\mathcal{O}_L$关于$\mathcal{O}_K$的一组整基.

设$(K, |\cdot|_v)$为一个赋值域(阿基米德或者非阿基米德均可), L/K为域的有限扩张. 我们下面揭示如何将$|\cdot|_v$延拓为L上的赋值. 为此, 首先介绍下面的引理.

引理 7.2. 设$(K,|\cdot|_K)$为完备的赋值域, L/K为域的有限扩张, $|\cdot|_L$为$|\cdot|_K$在L上唯一的延拓. 设$(M,|\cdot|_M)$为赋值域, $\varphi:L\to M$为域嵌入. 如果$\varphi|_K$是拓扑嵌入, 则φ本身也是拓扑嵌入.

注记 7.9. 下图可以清晰地说明该引理表达的内容.

$$\begin{array}{ccc} K & & \\ \big\downarrow & \searrow^{\varphi|_K\ topological} & \\ L & \xrightarrow[\varphi]{} & M \end{array} \Rightarrow \varphi:\ L \underset{topological}{\hookrightarrow} M.$$

证明: 因为$\varphi|_K$是拓扑嵌入, $(K,|\cdot|_M\circ\varphi|_K)$是完备的. 因为$|\cdot|_M\circ\varphi$显然是$|\cdot|_M\circ\varphi|_K$在$L$上的延拓, 由定理7.11, 赋值域$(L,|\cdot|_M\circ\varphi)$是完备的. 由命题7.10, 容易验证

$$\begin{aligned}(L,|\cdot|_L) &\underset{topological}{\cong} (K,|\cdot|_K)\times\cdots\times(K,|\cdot|_K)\\ &\underset{topological}{\cong} (K,|\cdot|_M\circ\varphi|_K)\times\cdots\times(K,|\cdot|_M\circ\varphi|_K)\\ &\underset{topological}{\cong} (L,|\cdot|_M\circ\varphi)\,.\end{aligned}$$

这说明φ本身是拓扑嵌入.

综上, 我们完成了证明. □

下面介绍如何将$|\cdot|_v$延拓为L上的赋值. 设$(K_v,|\cdot|_{v_*})$为$(K,|\cdot|_v)$的一个完备化, 其中$|\cdot|_{v_*}|_K=|\cdot|_v$. 考虑代数扩张$K_v^{\mathrm{alg}}/K_v$. 由定理7.11, 赋值$|\cdot|_{v_*}$可以唯一地延拓为$K_v^{\mathrm{alg}}$上的赋值$|\cdot|_{\bar{v}}$. 对任意的$\tau\in\mathrm{Hom}_K(L,K_v^{\mathrm{alg}})$, 显然赋值$|\cdot|_{\bar{v}}\circ\tau$为$|\cdot|_v$在$L$上的一个延拓.

下面的定理说明$|\cdot|_v$在L上的任何一个延拓都是通过这种方式得到的.

定理 7.12. 记号如上. 则下列结论成立.

(i) 对$|\cdot|_v$在L上的任意延拓$|\cdot|_w$, 存在$\tau\in\mathrm{Hom}_K(L,K_v^{\mathrm{alg}})$使得

$$|\cdot|_w=|\cdot|_{\bar{v}}\circ\tau.$$

(ii) 对任意的$\tau_1,\tau_2\in\mathrm{Hom}_K(L,K_v^{\mathrm{alg}})$, 我们有

$$|\cdot|_{\bar{v}}\circ\tau_1=|\cdot|_{\bar{v}}\circ\tau_2 \Leftrightarrow \text{存在}\sigma\in\mathrm{Hom}_{K_v}\left(K_v^{\mathrm{alg}},K_v^{\mathrm{alg}}\right)\text{使得}\tau_2=\sigma\circ\tau_1.$$

证明: (i) 设$(L_w,|\cdot|_{w_*})$为$(L,|\cdot|_w)$的一个完备化且$|\cdot|_{w_*}|_L=|\cdot|_w$. 此时$K$在$(L_w,|\cdot|_{w_*})$的闭包显然也为$(K,|\cdot|_v)$的一个完备化. 由推论7.1, 我们可以将$K_v$等同于$K$在$(L_w,|\cdot|_{w_*})$的闭包. 则对任意的$\tilde{\tau}\in\mathrm{Hom}_{K_v}(L_w,K_v^{\mathrm{alg}})$, 我们有下面的交换图

$$\begin{array}{ccc} K_v & & \\ \big\downarrow & \searrow^{\tilde{\tau}|_{K_v}=\mathrm{id}} & \\ L_w & \xrightarrow[\tilde{\tau}]{} & K_v^{\mathrm{alg}} \end{array}$$

则由引理7.2, 我们得到$\tilde{\tau}$是拓扑嵌入. 因此, 赋值$|\cdot|_{w_*}$与$|\cdot|_{\bar{v}}\circ\tilde{\tau}$等价. 又因为它们在$K_v$上的限制为相同的非平凡赋值, 我们有$|\cdot|_{w_*}=|\cdot|_{\bar{v}}\circ\tilde{\tau}$. 令$\tau=\tilde{\tau}|_L\in\mathrm{Hom}_K(L,K_v^{\mathrm{alg}})$. 则有

$$|\cdot|_w=|\cdot|_{w_*}|_L=|\cdot|_{\bar{v}}\circ\tau.$$

因此, (i)成立.

(ii) "⇐". 假设存在$\sigma\in\mathrm{Hom}_{K_v}\left(K_v^{\mathrm{alg}},K_v^{\mathrm{alg}}\right)$使得$\tau_2=\sigma\circ\tau_1$. 因为$|\cdot|_{\bar{v}}\circ\sigma$与$|\cdot|_{\bar{v}}$均为$|\cdot|_{v_*}$在$K_v^{\mathrm{alg}}$的延拓, 由定理7.11, 我们有

$$|\cdot|_{\bar{v}}\circ\sigma=|\cdot|_{\bar{v}}.$$

因此对任意的$x\in L$,

$$|\tau_2(x)|_{\bar{v}}=|\sigma\circ\tau_1(x)|_{\bar{v}}=|\tau_1(x)|_{\bar{v}},$$

即

$$|\cdot|_{\bar{v}}\circ\tau_1=|\cdot|_{\bar{v}}\circ\tau_2.$$

"⇒". 假设$|\cdot|_{\bar{v}}\circ\tau_1=|\cdot|_{\bar{v}}\circ\tau_2$. 则显然有

$$(\tau_1(L),|\cdot|_{\bar{v}})\xrightarrow[topological]{\tau_2\circ\tau_1^{-1}}(\tau_2(L),|\cdot|_{\bar{v}}).$$

此时仅需将$\tau_2\circ\tau_1^{-1}$延拓为$\mathrm{Hom}_{K_v}\left(K_v^{\mathrm{alg}},K_v^{\mathrm{alg}}\right)$上的一个元素$\sigma$即可.

综上, 我们完成了证明. □

当L/K为单扩张, 即存在$\alpha\in L$使得$L=K(\alpha)$时, 我们来介绍如何利用定理7.12来得到赋值$|\cdot|_v$在L上的全部延拓(这是我们后面最常遇到的情形).

设$p_\alpha(t)$为α在K上的极小多项式. 设$p_\alpha(t)$在$K_v[t]$的分解为

$$p_\alpha(t)=f_1(t)^{e_1}f_2(t)^{e_2}\cdots f_r(t)^{e_r},$$

其中这些$f_i(t)$为$K_v[t]$上两两不同的首一不可约多项式并且这些$e_i \in \mathbb{Z}^+$. 对任意的$1 \leq i \leq r$, 设$\alpha_i \in K_v^{\mathrm{alg}}$为$f_i(t)$的一个零点. 则由定理7.12, 赋值$|\cdot|_v$在$L$上的延拓完全取决于$\tau \in \mathrm{Hom}_K(L, K_v^{\mathrm{alg}})$. 因此$|\cdot|_v$在$L$上的延拓完全取决于$\tau(\alpha)$. 再利用定理7.12, 我们得到$\tau_1, \tau_2 \in \mathrm{Hom}_K(L, K_v^{\mathrm{alg}})$决定同一个延拓当且仅当$\tau_1(\alpha)$与$\tau_2(\alpha)$均是某个不可约因式$f_i(t)$的零点. 由上面的讨论, $|\cdot|_v$恰好有r种方式延拓为L上的赋值. 此时, 如果设$|\cdot|_{w_i}$是由$\tau(\alpha) = \alpha_i$确定的延拓, 则

$$L_{w_i} \underset{topological}{\cong} K_v(\alpha_i).$$

下面的定理及其推论会揭示"整体与局部"之间的联系. 为了方便, 对于L上的赋值$|\cdot|_w$, 记号$w \mid v$表示$|\cdot|_w$在K上的限制为$|\cdot|_v$.

定理 7.13. 设L/K为域的有限可分扩张, $|\cdot|_v$为K上一个非平凡赋值. 则有域同构

$$L \otimes_K K_v \cong \bigoplus_{w|v} L_w.$$

证明: 因为L/K为有限可分扩张, 存在$\alpha \in L$使得$L = K(\alpha)$. 设$p_\alpha(t)$为α在K上的极小多项式. 设$p_\alpha(t)$在$K_v[t]$的分解为

$$p_\alpha(t) = f_1(t) f_2(t) \cdots f_r(t),$$

其中这些$f_i(t)$为$K_v[t]$上两两不同的首一不可约多项式. 对任意的$1 \leq i \leq r$, 设$\alpha_i \in K_v^{\mathrm{alg}}$为$f_i(t)$的一个零点. 因为$L \cong K[t]/p_\alpha(t)K[t]$, 我们有正合列

$$0 \to p_\alpha(t)K[t] \to K[t] \to L \to 0.$$

注意到$\otimes_K$为右正合函子, 我们有正合列

$$p_\alpha(t)K[t] \otimes_K K_v \to K[t] \otimes_K K_v \to L \otimes_K K_v \to 0.$$

由此以及上面的讨论,

$$\begin{aligned} L\otimes_K K_v &\cong (K[t]\otimes_K K_v)/(p_\alpha(t)K[t]\otimes_K K_v)\\ &\cong K_v[t]/p_\alpha(t)K_v[t]\\ &\cong \bigoplus_{1\leq i\leq r} K_v[t]/f_i(t)K_v[t]\\ &\cong \bigoplus_{1\leq i\leq r} K_v(\alpha_i)\\ &\cong \bigoplus_{w|v} L_w. \end{aligned}$$

综上, 我们完成了证明. □

由该定理, 我们容易得到如下推论.

推论 7.3. *设L/K为域的有限可分扩张, $|\cdot|_v$为K上一个非平凡赋值. 则下列结论成立.*

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

(ii) *对任意的$x\in L$, 我们有*

$$\mathrm{N}_{L/K}(x)=\prod_{w|v}\mathrm{N}_{L_w/K_v}(x),$$

以及

$$\mathrm{Tr}_{L/K}(x)=\sum_{w|v}\mathrm{Tr}_{L_w/K_v}(x).$$

(iii) *如果$|\cdot|_v$对应的指数赋值ν是离散赋值, 则*

$$[L:K]=\sum_{w|v}e(w|v)\cdot f(w|v).$$

证明: (i) 由定理7.13,

$$L\otimes_K K_v\cong\bigoplus_{w|v}L_w.$$

注意到两边均为K_v上的向量空间, 我们得到

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

(ii) 设$y_1,\cdots,y_n$为L的一组K基. 则$y_1\otimes_K 1,\cdots,y_n\otimes_K 1$恰好为$L\otimes_K K_v$的一组$K_v$基. 因此, 对任意的$x\in L$, 显然有

$$\mathrm{N}_{L/K}(x)=\mathrm{N}_{L\otimes_K K_v/K_v}(x).$$

另一方面, 对任意的$w|v$, 设$x_1^{(w)},\cdots,x_{n_w}^{(w)}$为$L_w$的一组$K_v$基. 由同构

$$L\otimes_K K_v\cong\bigoplus_{w|v}L_w,$$

将这些基合起来就得到了$L\otimes_K K_v$的一组K_v基. 因此,

$$\mathrm{N}_{L\otimes_K K_v/K_v}(x)=\prod_{w|v}\mathrm{N}_{L_w/K_v}(x).$$

将上面的讨论结合起来, 我们得到

$$\mathrm{N}_{L/K}(x)=\prod_{w|v}\mathrm{N}_{L_w/K_v}(x).$$

同理, 我们也可以证明迹函数也满足这种类似的性质.

(iii) 假设$|\cdot|_v$对应的指数赋值ν是离散赋值. 则由注记7.5, 我们不妨设(K,ν)的完备化K_v上的指数赋值依旧为ν, (L,ω)的完备化L_w上的指数赋值依旧为ω, 其中ω为$|\cdot|_w$对应的指数赋值. 将命题7.11与(i)结合起来, 我们得到

$$[L:K]=\sum_{w|v}[L_w:K_v]=\sum_{w|v}e(w|v)\cdot f(w|v).$$

综上, 我们完成了证明. □

现在我们来介绍代数数域上的Ostrowski定理.

定理 7.14. 设K为代数数域. 则K上非阿基米德赋值的等价类与$\mathcal{O}_K$的非零素理想$\mathfrak{p}$一一对应. 设$\rho_1,\cdots,\rho_r$恰好为$K\to\mathbb{C}$的全部实嵌入, $\tau_1,\overline{\tau}_1,\cdots,\tau_s,\overline{\tau}_s$恰好为$K\to\mathbb{C}$的全部非实嵌入. 则$K$上阿基米德赋值的等价类与

$$\rho_1,\cdots,\rho_r,\tau_1,\tau_2,\cdots,\tau_s$$

一一对应.

证明: 我们首先说明K上任意的非平凡赋值$|\cdot|$在$\mathbb{Q}$上的限制均为非平凡赋值. 事实上, 取$x\in K$使得$|x|<1$. 设x在$\mathbb{Q}$上的极小多项式为

$$p_x(t)=t^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0$$

(注意此时$a_0\neq 0$). 如果$|\cdot|$在$\mathbb{Q}$上的限制为平凡赋值, 则由命题7.2,

$$0=|0|=|x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0|=|a_0|=1,$$

这显然矛盾. 因此, K上任意的非平凡赋值$|\cdot|$在$\mathbb{Q}$上的限制均为非平凡赋值.

(i) 我们先考虑非阿基米德的情形. 设$|\cdot|$为K上一个非阿基米德赋值, ω为其对应的指数赋值. 则由上面的讨论, $|\cdot|$在$\mathbb{Q}$上的限制为$\mathbb{Q}$上的非阿基米德赋值. 由定理7.2, 存在有理素数p使得$\omega|_Q$与p-adic指数赋值ord_p等价. 由注记7.3(iii), 不妨设$\omega|_Q = \mathrm{ord}_p$. 设

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

其中这些$\mathfrak{p}_i$为$\mathcal{O}_K$上两两不同的素理想并且这些$e_i \in \mathbb{Z}^+$. 此时, 对任意的$1 \leq i \leq r$, 离散赋值

$$\omega_i := \frac{1}{e_i}\mathrm{ord}_{\mathfrak{p}_i}$$

均为ord_p在K上的延拓. 并且$e(\omega_i|\mathrm{ord}_p) = e_i = e(\mathfrak{p}_i|p)$,

$$f(\omega_i|\mathrm{ord}_p) = [(\mathcal{O}_K)_{\mathfrak{p}}/\mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}} : \mathbb{F}_p] = [\mathcal{O}_K/\mathfrak{p} : \mathbb{F}_p] = f(\mathfrak{p}_i|p).$$

由定理4.3, 我们得到

$$\sum_{i=1}^{r} e(\omega_i|\mathrm{ord}_p)\cdot f(\omega_i|\mathrm{ord}_p) = \sum_{i=1}^{r} e(\mathfrak{p}_i|p)\cdot f(\mathfrak{p}_i|p) = [L:K]. \tag{7.7}$$

另一方面, 由推论7.3(iii),

$$\sum_{\omega|\mathrm{ord}_p} e(\omega|\mathrm{ord}_p)\cdot f(\omega|\mathrm{ord}_p) = [L:K]. \tag{7.8}$$

将(7.7)与(7.8)结合起来, 我们发现这些$\omega_i(1 \leq i \leq r)$恰好就是$\mathrm{ord}_p$在$K$上的全部延拓. 这说明此时$\omega$一定等于某个$\omega_i$. 因此, K上非阿基米德赋值的等价类与$\mathcal{O}_K$的非零素理想$\mathfrak{p}$一一对应.

(ii) 我们再考虑阿基米德的情形. 设$|\cdot|$为K上一个阿基米德赋值. 类似于(i)的证明, 由定理7.2, 赋值$|\cdot|$在$\mathbb{Q}$上的限制与$|\cdot|_\infty$等价. 由命题7.1, 存在实数$s > 0$使得$|\cdot|$在$\mathbb{Q}$上的限制等于$|\cdot|_\infty^s$. 也就是说, $|\cdot|$是$|\cdot|_\infty^s$在K中的一个延拓. 另一方面, 由定理7.12, $|\cdot|_\infty^s$在K中的延拓完全由$\tau \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$所确定(注意此时$(\mathbb{Q}, |\cdot|_\infty^s)$的完备化为$\mathbb{R}$), 并且$\tau_1, \tau_2 \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$所确定的延拓相同当且仅当$\tau_1 = \overline{\tau_2}$. 由上面的讨论, $|\cdot|$所在的等价类完全由两两不共轭的嵌入$\rho_1,\cdots,\rho_r,\tau_1,\tau_2,\cdots,\tau_s$所确定. 因此, K上阿基米德赋值的等价类与

$$\rho_1,\cdots,\rho_r,\tau_1,\tau_2,\cdots,\tau_s$$

一一对应.

综上, 我们完成了证明. □

注记 7.10. 设

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r},$$

其中这些$\mathfrak{p}_i$为$\mathcal{O}_K$上两两不同的素理想并且这些$e_i \in \mathbb{Z}^+$. 在证明的过程中, 我们发现这些离散赋值

$$\omega_i := \frac{1}{e_i}\mathrm{ord}_{\mathfrak{p}_i}$$

恰好就是$\mathbb{Q}$上p-adic指数赋值ord_p在K上的全部延拓. 并且此时, $e(\omega_i|\mathrm{ord}_p) = e(\mathfrak{p}_i|p)$, $f(\omega_i|\mathrm{ord}_p) = f(\mathfrak{p}_i|p)$.

为了更好地理解上述结果, 作为本节的结束, 我们来讨论一个具体的例子. 考虑实二次域$K = \mathbb{Q}(\sqrt{5})$上的赋值等价类.

首先, $\mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{C})$中有且仅有两个嵌入$a+b\sqrt{5} \mapsto a+b\sqrt{5}$与$a+b\sqrt{5} \mapsto a-b\sqrt{5}$. 因此, $\mathbb{Q}$上的绝对值赋值$|\cdot|_\infty$在K上仅有两个延拓:

$$|a+b\sqrt{5}|_1 = |a+b\sqrt{5}|_\infty,\ |a+b\sqrt{5}|_2 = |a-b\sqrt{5}|_\infty,$$

其中$|\cdot|_\infty$为$\mathbb{R}$上的绝对值赋值.

再看$\mathbb{Q}$上p-adic赋值$|\cdot|_p$在K上的延拓. 由定理7.14, 赋值$|\cdot|_p$在K上的延拓取决于p在$\mathcal{O}_K$上的素理想分解. 下面分几种情况考虑.

情况 1. $p > 2$且$(\frac{5}{p}) = 1$. 此时, 由定理4.5,

$$p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2,$$

其中$\mathfrak{p}_1, \mathfrak{p}_2$为$\mathcal{O}_K$的不同素理想. 因此, $|\cdot|_p$在K恰好有两个延拓. 再利用定理7.12, 不妨设延拓$|\cdot|_i$是由$\tau_i \in \mathrm{Hom}_{\mathbb{Q}}(K,\mathbb{Q}_p^{\mathrm{alg}})$确定的, 其中 $\tau_1 = \mathrm{id}$, $\tau_2(a+b\sqrt{5}) = a-b\sqrt{5}$. 由定理7.5并注意到此时$\sqrt{5} \in \mathbb{Q}_p$(定理7.10或者推论7.3), 我们得到

$$|a+b\sqrt{5}|_1 = \left|\mathrm{N}_{\mathbb{Q}_p(\sqrt{5})/\mathbb{Q}_p}(a+b\sqrt{5})\right|^{\frac{1}{[\mathbb{Q}_p(\sqrt{5}):\mathbb{Q}_p]}} = |a+b\sqrt{5}|_p,$$

以及

$$|a+b\sqrt{5}|_2 = \left|\mathrm{N}_{\mathbb{Q}_p(\sqrt{5})/\mathbb{Q}_p}(a-b\sqrt{5})\right|^{\frac{1}{[\mathbb{Q}_p(\sqrt{5}):\mathbb{Q}_p]}} = |a-b\sqrt{5}|_p,$$

其中$|\cdot|_p$为$\mathbb{Q}_p$上的p-adic赋值.

情况 2. $p > 2$且$(\frac{5}{p}) = -1$. 此时, 由定理4.5, 理想$p\mathcal{O}_K = \mathfrak{p}$为$\mathcal{O}_K$上的素理想. 因此, $|\cdot|_p$在K有且仅有一个延拓$|\cdot|_1$. 再由定理7.12, 延拓$|\cdot|_1$是

由$\mathrm{id} \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q}_p^{\mathrm{alg}})$确定的. 由定理7.5并且注意到$[\mathbb{Q}_p(\sqrt{5}) : \mathbb{Q}_p] = 2$(推论7.3), 我们得到

$$|a+b\sqrt{5}|_1 = \left|\mathrm{N}_{\mathbb{Q}_p(\sqrt{5})/\mathbb{Q}_p}(a+b\sqrt{5})\right|^{\frac{1}{[\mathbb{Q}_p(\sqrt{5}):\mathbb{Q}_p]}} = |a^2-5b^2|_p^{1/2},$$

其中$|\cdot|_p$为$\mathbb{Q}_p$上的p-adic赋值.

情况 3. $p \in \{2, 5\}$. 此时, 由定理4.5,

$$p\mathcal{O}_K = \mathfrak{p}^2,$$

其中$\mathfrak{p}$为$\mathcal{O}_K$的素理想. 因此, $|\cdot|_p$在K有且仅有一个延拓$|\cdot|_1$. 再由定理7.12, 延拓$|\cdot|_1$是由$\mathrm{id} \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q}_p^{\mathrm{alg}})$确定的. 由定理7.5并且注意到$[\mathbb{Q}_p(\sqrt{5}) : \mathbb{Q}_p] = 2$(推论7.3), 我们得到

$$|a+b\sqrt{5}|_1 = \left|\mathrm{N}_{\mathbb{Q}_p(\sqrt{5})/\mathbb{Q}_p}(a+b\sqrt{5})\right|^{\frac{1}{[\mathbb{Q}_p(\sqrt{5}):\mathbb{Q}_p]}} = |a^2-5b^2|_p^{1/2},$$

其中$|\cdot|_p$为$\mathbb{Q}_p$上的p-adic赋值.

7.6 局部域

这一节我们将利用前面介绍的理论来研究一类非常重要的赋值域: 局部域. 我们先介绍本节的记号. 设(K, ν)为一个非阿基米德赋值域, $\mathcal{O}_K$为其赋值环, $\mathfrak{p}_K$为$\mathcal{O}_K$的极大理想, $\kappa = \mathcal{O}_K/\mathfrak{p}_K$为$\mathcal{O}_K$的剩余类域.

定义 7.13. 设(K, ν)为一个非阿基米德赋值域. 如果(K, ν)是完备的离散赋值域并且其赋值环的剩余类域κ为有限域, 则称(K, ν)为一个局部域.

注记 7.11. (i) 此时设$q = |\kappa|$. 则称赋值

$$|x|_{\mathfrak{p}_K} := \left(\frac{1}{q}\right)^{\mathrm{ord}_{\mathfrak{p}_K}(x)}$$

为正则的$\mathfrak{p}_K$-*adic*赋值.

(ii) 由定理*7.8*, 我们有

$$\mathcal{O}_K \underset{topological}{\cong} \varprojlim_{n\in\mathbb{Z}^+} \mathcal{O}_K/\mathfrak{p}_K^n.$$

注意到此时对任意的$n \in \mathbb{Z}^+$, 商空间$\mathcal{O}_K/\mathfrak{p}_K^n$为离散空间且

$$|\mathcal{O}_K/\mathfrak{p}_K^n| = |\mathcal{O}_K/\mathfrak{p}_K|^n < \infty.$$

这说明$\mathcal{O}_K/\mathfrak{p}_K^n$为紧空间. 由此与定理*7.7*, 赋值环$\mathcal{O}_K$为紧空间.

局部域上非零元构成的乘法群的代数结构是简单的.

定理 7.15. *设(K,ν)为局部域, π为$\mathcal{O}_K$的素元, $|\kappa|=q$. 则*

$$K^\times \cong \langle\pi\rangle \times U_{q-1}(K) \times U^{(1)},$$

其中

$$U_{q-1}(K)=\{x\in K:\ x^{q-1}=1\},$$

并且$U^{(1)}=1+\mathfrak{p}_K$.

证明: 我们知道$K^\times$中任意的非零元x可以唯一表示为$\pi^{\mathrm{ord}_{\mathfrak{p}_K}(x)}\cdot\varepsilon$, 其中$\varepsilon\in\mathcal{O}_K^\times$. 因此, 下面仅需证明

$$\mathcal{O}_K^\times \cong U_{q-1}(K)\times U^{(1)}.$$

因为$\kappa=\mathbb{F}_q$, 由定理7.9, 多项式$t^{q-1}-1$在$\mathcal{O}_K[t]$上完全分裂. 因此

$$|U_{q-1}(K)|=q-1.$$

也就是说, K^{alg}中的所有$q-1$次单位根都落在K中. 类似于定理4.10的证明, 容易说明

$$U_{q-1}(K)\underset{f}{\cong}(\mathcal{O}_K/\mathfrak{p}_K)^\times=\mathbb{F}_q^\times,$$

其中$f(x)=x \bmod \mathfrak{p}_K$. 由此以及命题7.7, 我们得到同构

$$\mathcal{O}_K^\times/U^{(1)}\cong(\mathcal{O}_K/\mathfrak{p}_K)^\times\cong U_{q-1}(K).$$

因此,

$$\mathcal{O}_K^\times = U_{q-1}(K)\times U^{(1)}.$$

综上, 我们完成了证明. □

下面的定理说明, 在拓扑同构的意义下, 局部域本质上仅有两类.

定理 7.16. *在拓扑同构的意义下, 局部域(K,ν)本质上仅有两类. 一类为p-adic数域$\mathbb{Q}_p$的有限扩张, 另一类为形式洛朗级数域$\mathbb{F}_p((t))$的有限扩张.*

证明: 首先说明$\mathbb{Q}_p$以及$\mathbb{F}_p((t))$均为局部域. 前者显然为局部域. 我们主要考虑$\mathbb{F}_p((t))$. 考虑函数域$\mathbb{F}_p(t)$在t-adic赋值下的完备化. $\mathbb{F}_p(t)$在t-adic赋值下的

赋值环恰好为$\mathbb{F}_p[t]$在t处的局部化, 并且剩余类域恰好为$\mathbb{F}_p$. 由此与定理7.6, 函数域$\mathbb{F}_p(t)$在t-adic赋值下的完备化

$$\widehat{\mathbb{F}_p(t)} = \mathbb{F}_p((t)),$$

并且由命题7.8, 此时$\mathbb{F}_p((t))$赋值环的剩余类域也为$\mathbb{F}_p$. 因此, $\mathbb{F}_p((t))$为局部域. 再由定理7.5以及命题7.11, 局部域$\mathbb{Q}_p$以及$\mathbb{F}_p((t))$的有限扩张仍为局部域.

下面我们来说明, 局部域在拓扑同构的意义下, 仅有上面两类. 设(K,ν)为局部域. 分两种情况讨论.

情况 1. $\mathrm{char}(K)=0$. 此时设$\mathrm{char}(\kappa)=p$. 由此$\nu(p)>0$. 这说明$\nu|_{\mathbb{Q}}$为非阿基米德赋值. 由定理7.2以及此$\nu(p)>0$, 赋值明$\nu|_{\mathbb{Q}}$与p-adic指数赋值ord_p等价. 因此, 在拓扑同构的意义下, $\mathbb{Q}_p\subseteq K$. 再由命题7.11,

$$[K:\mathbb{Q}] = e(\nu|\mathrm{ord}_p)\cdot f(\nu|\mathrm{ord}_p) < \infty.$$

因此, K为$\mathbb{Q}_p$的有限扩张.

情况 2. $\mathrm{char}(K)=p>0$. 此时显然有$\mathrm{char}(\kappa)=p$. 因为$|\kappa|<\infty$, 不妨设$\kappa=\mathbb{F}_q$, 其中q为素数p的正整数幂次. 设t为$\mathcal{O}_K$的素元. 则由定理7.6,

$$K = \mathbb{F}_q((t)).$$

下面说明t为$\mathbb{F}_q$上的超越元. 假设t为$\mathbb{F}_q$上的代数元. 则 $\mathbb{F}_q((t)) = \mathbb{F}_q(t)$为有限域. 但是, 有限域上的赋值一定为平凡赋值, 这与ν为离散赋值矛盾. 因此, K为形式洛朗级数域$\mathbb{F}_p((t))$的有限扩张.

综上, 我们完成了证明. □

下面介绍局部域的非分歧扩张, 其它类型的扩张将在讲义的第二部分(类域论)详细介绍. 首先介绍一些记号. 设(K,ν_K)为局部域, L/K为有限扩张. 对L/K的任意中间域M, 设ν_M为ν_K在M上唯一的延拓, $\mathcal{O}_M$为ν_M在M上的赋值环, $\mathfrak{p}_M$为$\mathcal{O}_M$的极大理想, 剩余类域$\mathcal{O}_M/\mathfrak{p}_K$记作$\lambda_M$. 特别地, 当$M=K$时, 将$\lambda_K$记为$\kappa$, 当$M=L$时, 将$\lambda_L$记作$\lambda$.

定义 7.14. *设(K,ν_K)为局部域, L/K为有限扩张. 如果*

$$[L:K] = [\lambda:\kappa],$$

则称L/K为不分歧扩张.

关于局部域的非分歧扩张, 我们有下面一些简单的结果. 我们将会看到, 这个结果的证明展示了Hensel引理第一形式(定理7.9)的使用技巧.

命题 7.12. *设(K,ν_K)为局部域, L/K为有限扩张, L_1,L_2均为L/K的中间域. 如果L_1/K为非分歧扩张, 则L_1L_2/L_2也为非分歧扩张.*

证明: 因为L_1/K为分分歧扩张, $[\lambda_{L_1}:\kappa]=[L_1:K]<\infty$. 又因为$\kappa$为有限域, 我们得到$\lambda_{L_1}/\kappa$为有限可分扩张. 因此, 存在$\alpha\in\mathcal{O}_{L_1}$使得

$$\lambda_{L_1}=\kappa(\bar{\alpha}),$$

其中$\bar{\alpha}=\alpha \bmod \mathfrak{p}_{L_1}\in\lambda_{L_1}$. 设$p_\alpha(t)\in\mathcal{O}_K[t]$为$\alpha$在$K$上的极小多项式, $\tilde{h}_{\bar{\alpha}}(t)\in\kappa[t]$为$\bar{\alpha}$在$\kappa$上的极小多项式. 则

$$\overline{p_\alpha(t)}\equiv 0\ (\mathrm{mod}\ \tilde{h}_{\bar{\alpha}}(t)\kappa[t]),$$

其中$\overline{p_\alpha(t)}=p_\alpha(t)\bmod\mathfrak{p}_K$. 由定理7.9, 多项式$\overline{p_\alpha(t)}$在$\kappa[t]$中的不可约因子仅有$\tilde{h}_{\bar{\alpha}}(t)$(否则, $p_\alpha(t)$在$\mathcal{O}_K[t]$上可约). 因此, 存在正整数m使得

$$\overline{p_\alpha(t)}=\tilde{h}_{\bar{\alpha}}(t)^m.$$

因为L_1/K为分分歧扩张, 由上面的讨论容易验证

$$\begin{aligned}\deg\left(\tilde{h}_{\bar{\alpha}}(t)\right)=[\lambda_{L_1}:\kappa]=[L_1:K]&\geq[K(\alpha):K]\\&=\deg\left(p_\alpha(t)\right)\\&=\deg\left(\overline{p_\alpha(t)}\right)\\&=m\cdot\deg\left(\tilde{h}_{\bar{\alpha}}(t)\right).\end{aligned}$$

这说明$m=1$. 因此, $[K(\alpha):K]=[L_1:K]$, 即$K(\alpha)=L_1$.

由上面的讨论, $L_1L_2=L_2(\alpha)$. 下面来说明$L_2(\alpha)/L_2$是非分歧扩张. 设$g_\alpha(t)\in\mathcal{O}_{L_2}[t]$为$\alpha$在$L_2$上的极小多项式. 则

$$p_\alpha[t]\equiv 0\ (\mathrm{mod}\ g_\alpha(t)\mathcal{O}_{L_2}[t]).$$

注意到$\overline{p_\alpha(t)}=\tilde{h}_{\bar{\alpha}}(t)$, 我们有

$$\tilde{h}_{\bar{\alpha}}(t)\equiv 0\ (\mathrm{mod}\ \overline{g_\alpha(t)}\lambda_{L_2}[t]),$$

其中$\overline{g_\alpha(t)} = g_\alpha(t) \bmod \mathfrak{p}_{L_2}$. 因为$\kappa$为有限域, 我们得到$\kappa$上的不可约多项式$\tilde{h}_{\bar{\alpha}}(t)$在$\kappa^{\mathrm{alg}}$中无重根. 再由上面的讨论, $\overline{g_\alpha(t)}$在κ^{alg}中也无重根. 因此, 由定理7.9, 多项式$\overline{g_\alpha(t)}$为λ_{L_2}上的不可约多项式. 由上面的讨论与命题7.11, 容易验证

$$\begin{aligned}[\lambda_{L_1L_2} : \lambda_{L_2}] \geq [\lambda_{L_2}(\bar{\alpha}) : \lambda_{L_2}] &= \deg\left(\overline{g_\alpha(t)}\right) \\ &= \deg\left(g_\alpha(t)\right) \\ &= [L_2(\alpha) : L_2] \\ &= [L_1L_2 : L_2] \\ &\geq [\lambda_{L_1L_2} : \lambda_{L_2}].\end{aligned}$$

因此, $[L_1L_2 : L_2] = [\lambda_{L_1L_2} : \lambda_{L_2}]$, 即$L_1L_2/L_2$为非分歧扩张.

综上, 我们完成了证明. □

利用这个结果, 我们容易得到下面的推论.

推论 7.4. *设(K, ν_K)为局部域, L/K为有限扩张, L_1, L_2均为L/K的中间域. 则下列结论成立.*

(i) *如果L/K为非分歧扩张, 则对L/K的任意中间域M, M/K也为非分歧扩张.*

(ii) *如果$L_1/K, L_2/K$均为非分歧扩张, 则L_1L_2/K也为非分歧扩张.*

7.7 p-adic分圆域

作为本章的结束, 我们简单介绍一下p-adic分圆域. 我们将在讲义的第二部分(类域论)详细地研究它.

定理 7.17. *设K为局部域, 剩余类域$\kappa = \mathbb{F}_q$, 其中q为素数p的正整数幂次. 对任意的$n \in \mathbb{Z}^+$满足$\gcd(n, p) = 1$, 设$\zeta_n \in K^{\mathrm{alg}}$为一个本原$n$次单位根, $L = K(\zeta_n)$, $\mathcal{O}_L$为其赋值环(由注记7.7, $\mathcal{O}_L$也是$\mathcal{O}_K$在L上的整闭包). 则下列结论成立.*

(i) *L/K为非分歧扩张且*

$$[L : K] = \min\{r \in \mathbb{Z}^+ : \ q^r \equiv 1 \ (\mathrm{mod}\ n\mathbb{Z})\}.$$

(ii) $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\lambda_L/\kappa)$.

(iii) $\mathcal{O}_L = \mathcal{O}_K[\zeta_n]$.

证明: (i) 设$p_n(t) \in \mathcal{O}_K[t]$为$\zeta_n$在$K$上的极小多项式, $\overline{p_n(t)} = p_n(t) \bmod \mathfrak{p}_K$. 因为

$$t^n - 1 \equiv 0 \,(\mathrm{mod}\, p_n(t)\mathcal{O}_K[t]),$$

我们有

$$t^n - 1 \equiv 0 \,(\mathrm{mod}\, \overline{p_n(t)}\kappa[t]).$$

因为$\gcd(n,p) = 1$, 多项式$t^n - 1$在κ中无重根. 因此上式说明$\overline{p_n(t)}$在κ中也无重根. 再由定理7.9, 多项式$\overline{p_n(t)}$在κ上不可约. 由此以及命题7.11,

$$\begin{aligned}[\lambda_L : \kappa] \geq [\kappa(\overline{\zeta_n})] &= \deg(\overline{p_n(t)}) \\ &= \deg(p_n(t)) \\ &= [L:K] \\ &\geq [\lambda_L : \kappa],\end{aligned}$$

其中$\overline{\zeta_n} = \zeta_n \bmod \mathfrak{p}_L$. 这说明$[L:K] = [\lambda_L : \kappa]$, 即$L/K$为非分歧扩张. 下面考虑扩张次数. 因为$\gcd(n,p) = 1$, 类似于定理4.10的证明, 我们有

$$U_n(K^{\mathrm{alg}}) \cong U_n(\mathbb{F}_q^{\mathrm{alg}}) = U_n(\kappa^{\mathrm{alg}}).$$

因此,

$$[\lambda_L : \kappa] = [\kappa(\overline{\zeta_n}) : \kappa] = [\mathbb{F}_q(U_n(\mathbb{F}_q^{\mathrm{alg}})) : \mathbb{F}_q] = \min\{r \in \mathbb{Z}^+ :\, q^r \equiv 1 \,(\mathrm{mod}\, n\mathbb{Z})\}.$$

这得到$[L:K] = [\lambda_L : \kappa] = \min\{r \in \mathbb{Z}^+ :\, q^r \equiv 1 \,(\mathrm{mod}\, n\mathbb{Z})\}$.

(ii) 因为K与L均为局部域, 我们得到$\mathfrak{p}_L$在K上的分解群

$$G_{\mathfrak{p}_L} = \mathrm{Gal}(L/K).$$

另一方面, 设$\mathfrak{p}_K\mathcal{O}_L = \mathfrak{p}_L^e$. 则$\frac{1}{e} \cdot \mathrm{ord}_{\mathfrak{p}_L}$显然为指数赋值$\mathrm{ord}_{\mathfrak{p}_K}$在$L$上的唯一延拓. 此时素理想的分歧指数$e = e(\mathfrak{p}_L|\mathfrak{p}_K)$恰好等于赋值之间的分歧指数. 因为$L/K$为非分歧扩张, 我们得到$e = 1$. 因此, 由上面的讨论以及注记5.3(ii),

$$\mathrm{Gal}(L/K) = G_{\mathfrak{p}_L} \cong \mathrm{Gal}(\lambda_L/\kappa).$$

(iii) 首先由注记7.7, 赋值$\mathrm{ord}_{\mathfrak{p}_L}$在$L$上的赋值环$\mathcal{O}_L$恰好为$\mathcal{O}_K$在$L$上的整闭包. 因为$L/K$为非分歧扩张且$\kappa(\overline{\zeta_n}) = \lambda_L$, 由注记7.8, 我们知道

$$1, \zeta_n, \cdots, \zeta_n^{[\lambda_L:\kappa]-1}$$

恰好为$\mathcal{O}_L$关于$\mathcal{O}_K$的一组整基. 因此, $\mathcal{O}_L = \mathcal{O}_K[\zeta_n]$.

综上, 我们完成了证明. □

注记 7.12. 在(ii)的证明中, 我们发现这里的理论与第五章的内容有联系. 下面来研究这种联系.

回顾一下第五章的记号. 设A为Dedekind环, $\mathrm{frac}(A) = K$, L/K为有限Galois扩张, B为A在L中的整闭包. 对A的任意非零素理想$\mathfrak{p}$, 设$\mathfrak{P}$为B上一个包含$\mathfrak{p}$的素理想, $G_{\mathfrak{P}}$为$\mathfrak{P}$在K上的分解群, $L_{\mathfrak{P}}$为L在$\mathfrak{P}$-adic赋值下的完备化, $K_{\mathfrak{p}}$为K在$\mathfrak{p}$-adic赋值下的完备化. 在拓扑同构的意义下, 我们认为$K_{\mathfrak{p}} \subseteq L_{\mathfrak{P}}$. 并且, 此时容易验证$L_{\mathfrak{P}}/K_p$也为有限Galois扩张.

我们首先需要下面这个深刻的引理.

引理 7.3. 记号如上. 则

$$G_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma\text{为}(L, |\cdot|_{\mathfrak{P}}) \to (L, |\cdot|_{\mathfrak{P}})\text{的连续映射}\}.$$

证明: 先证明左边包含于右边. 对任意的$\sigma \in G_{\mathfrak{P}}$以及任意的$n \in \mathbb{Z}^+$, 显然有

$$x \equiv 0 \ (\mathrm{mod}\ \mathfrak{P}^n) \Rightarrow \sigma(x) \equiv 0 \ (\mathrm{mod}\ \mathfrak{P}^n).$$

这说明σ在0处连续. 又因为$(L, |\cdot|_{\mathfrak{P}})$为拓扑域, σ为$(L, |\cdot|_{\mathfrak{P}}) \to (L, |\cdot|_{\mathfrak{P}})$的连续映射. 因此, 左边包含于右边.

再证明右边包含于左边. 对任意的$\sigma \in \mathrm{Gal}(L/K)$使得$\sigma$为$(L, |\cdot|_{\mathfrak{P}}) \to (L, |\cdot|_{\mathfrak{P}})$的连续映射. 对任意的$x \in \mathfrak{P}$(即$|x|_{\mathfrak{P}} < 1$), 当正整数$N$充分大时, 容易验证

$$|x^N|_{\mathfrak{P}}\text{充分小} \Rightarrow |\sigma(x^N)|_{\mathfrak{P}} < 1 \Rightarrow |\sigma(x)|_{\mathfrak{P}}^N < 1 \Rightarrow |\sigma(x)|_{\mathfrak{P}} < 1 \Rightarrow \sigma(x) \in \mathfrak{P}.$$

这说明$\sigma(\mathfrak{P}) = \mathfrak{P}$, 即$\sigma \in G_{\mathfrak{P}}$. 因此, 右边包含于左边.

综上, 我们完成了证明. □

下面的定理可以让我们对分解群$G_{\mathfrak{P}}$有更深刻的理解.

定理 7.18. 记号如上. 则$G_{\mathfrak{P}} \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

证明: 对任意的$\sigma \in G_{\mathfrak{P}}$, 因为$L$在$L_{\mathfrak{P}}$中稠密且$\sigma$在$(L|\cdot|_{\mathfrak{P}})$上连续(引理7.3), 可以将$\sigma$唯一延拓为$\mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$中的自同构$\hat{\sigma}$. 并且, 容易验证$\sigma \mapsto \hat{\sigma}$是一个单的群同态.

下面来证明上述群同态为满同态. 对任意的$\tau \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$, 考虑下面的交换图

$$\begin{array}{ccc} K_{\mathfrak{p}} & & \\ \downarrow & \searrow^{\tau|_{K_{\mathfrak{p}}}=\mathrm{id}\ topological} & \\ L_{\mathfrak{P}} & \xrightarrow[\tau]{} & L_{\mathfrak{P}} \end{array}$$

由引理7.2, 我们得到τ为$L_{\mathfrak{P}} \to L_{\mathfrak{P}}$的拓扑同构. 因此, 对任意的$x \in \mathfrak{P}$(即$|x|_{\mathfrak{P}} < 1$), 我们有$|\tau(x)|_{\mathfrak{P}} < 1$. 这说明$\tau|_L \in G_{\mathfrak{P}}$. 此时显然有

$$\widehat{\tau|_L} = \tau.$$

因此, 证$\sigma \mapsto \hat{\sigma}$是满同态.

综上, $\sigma \mapsto \hat{\sigma}$是群同构. 这完成了证明. □

回到p-adic分圆域. 定理7.17考虑了非分歧的局部分圆域. 我们下面来考虑完全分歧的p-adic分圆域.

定理 7.19. *设p为素数, $m \in \mathbb{Z}^+$, $\zeta_{p^m} \in \mathbb{Q}_p^{\mathrm{alg}}$为一个本原$p^m$次单位根. 则下列结论成立.*

(i) $\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p$为完全分歧扩张并且

$$[\mathbb{Q}_p(\zeta_{p^m}) : \mathbb{Q}_p] = \varphi(p^m).$$

(ii) $\mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p\right) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$.

(iii) $\mathbb{Z}_p$在$\mathbb{Q}_p(\zeta_{p^m})$中的整闭包为$\mathbb{Z}_p[\zeta_{p^m}]$.

(iv) $(1-\zeta_{p^m})$为$\mathbb{Z}_p[\zeta_{p^m}]$上的素元.

证明: 设$L = \mathbb{Q}_p(\zeta_{p^m})$, 记号$\mathrm{ord}_p$表示$\mathbb{Q}_p$上的指数$p$-adic赋值在$\mathbb{Q}_p(\zeta_{p^m})$上的延拓, $\mathcal{O}_L$为ord_p在L上的赋值环(由注记7.7, $\mathcal{O}_L$也是$\mathbb{Z}_p$在L上的整闭包).

(i)与(ii) 由定理4.10, 素数p在$\mathbb{Z}[\zeta_{p^m}]$上完全分歧. 因此, 由定理7.14(数域上的Ostrowski定理)以及注记7.10, 赋值ord_p在$\mathbb{Q}(\zeta_{p^m})$恰好仅有一种延拓并且此时局部域的扩张为完全分歧扩张, 即

$$p\mathcal{O}_L = \mathfrak{p}^{[L:\mathbb{Q}_p]} = \mathfrak{p}^{\varphi(p^m)},$$

其中$\mathfrak{p}$为$\mathcal{O}_L$上素理想.

由推论4.1与推论7.3,

$$\varphi(p^m) = [\mathbb{Q}(\zeta_{p^m}) : \mathbb{Q}] = [\mathbb{Q}_p(\zeta_{p^m}) : \mathbb{Q}_p].$$

这不仅说明了$[\mathbb{Q}_p(\zeta_{p^m}):\mathbb{Q}_p]=\varphi(p^m)$, 还说明了分圆多项式

$$\begin{aligned}\Phi_{p^m}(t)&=\prod_{r\in(\mathbb{Z}/p^m\mathbb{Z})^\times}\left(t-\zeta_{p^m}^r\right)\\&=\frac{t^{p^m}-1}{t^{p^{m-1}}-1}\\&=t^{p^{m-1}(p-1)}+t^{p^{m-1}(p-2)}+\cdots+t^{p^{m-1}}+1\end{aligned}$$

是$\mathbb{Q}_p$上的不可约多项式. 因此,

$$\mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p\right)\cong\left(\mathbb{Z}/p^m\mathbb{Z}\right)^\times.$$

(iii)与(iv) 注意到

$$p=\Phi_{p^m}(1)=\prod_{r\in(\mathbb{Z}/p^m\mathbb{Z})^\times}\left(1-\zeta_{p^m}^r\right)=\mathrm{N}_{\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p}\left(1-\zeta_{p^m}\right).$$

注意此时

$$\mathrm{ord}_p=\frac{1}{\varphi(p^m)}\mathrm{ord}_{\mathfrak{p}}.$$

由上面的讨论与定理7.5,

$$\begin{aligned}\frac{1}{\varphi(p^m)}\mathrm{ord}_{\mathfrak{p}}\left(1-\zeta_{p^m}\right)&=\mathrm{ord}_p\left(1-\zeta_{p^m}\right)\\&=\frac{1}{\varphi(p^m)}\mathrm{ord}_p\left(\mathrm{N}_{\mathbb{Q}_p(\zeta_{p^m})/\mathbb{Q}_p}\left(1-\zeta_{p^m}\right)\right)\\&=\frac{1}{\varphi(p^m)}\mathrm{ord}_p(p)\\&=\frac{1}{\varphi(p^m)}.\end{aligned}$$

这说明$\mathrm{ord}_{\mathfrak{p}}\left(1-\zeta_{p^m}\right)=1$, 即$1-\zeta_{p^m}$为$\mathcal{O}_L$上的素元. 则由注记7.8, 我们得到

$$\mathcal{O}_L=\mathbb{Z}_p[1-\zeta_{p^m}]=\mathbb{Z}_p[\zeta_{p^m}].$$

综上, 我们完成了证明. □

把定理7.17与定理7.19结合起来, 我们可以得到下面的定理.

定理 7.20. 设p为素数, $n\in\mathbb{Z}_{\geq 2}$且$n=n'\cdot p^{\mathrm{ord}_p(n)}$. 设$\zeta_n,\zeta_{n'},\zeta_{p^{\mathrm{ord}_p(n)}}\in\mathbb{Q}_p^{\mathrm{alg}}$分别为本原$n$次单位根, 本原$n'$次单位根以及本原$p^{\mathrm{ord}_p(n)}$次单位根. 则下列结论成立.

(i) $\mathbb{Q}_p(\zeta_n)=\mathbb{Q}_p(\zeta_{n'},\zeta_{p^{\mathrm{ord}_p(n)}})$并且$\mathbb{Q}_p(\zeta_{n'})\cap\mathbb{Q}_p(\zeta_{p^{\mathrm{ord}_p(n)}})=\mathbb{Q}_p$.

(ii) 关于Galois群, 我们有

$$\mathrm{Gal}\left(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p\right) \cong \mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{n'})/\mathbb{Q}_p\right) \times \mathrm{Gal}\left(\mathbb{Q}_p(\zeta_{p^{\mathrm{ord}_p(n)}})/\mathbb{Q}_p\right).$$

(iii) $\mathbb{Z}_p$在$\mathbb{Q}_p(\zeta_n)$上整闭包恰好为$\mathbb{Z}_p[\zeta_n]$.

证明: (i) $\mathbb{Q}_p(\zeta_{n'}, \zeta_{p^{\mathrm{ord}_p(n)}}) \subseteq \mathbb{Q}_p(\zeta_n)$是显然的. 反过来, 由引理4.3, 分圆域$\mathbb{Q}_p(\zeta_{n'}, \zeta_{p^{\mathrm{ord}_p(n)}})$中存在本原$n$次单位根. 这说明$\mathbb{Q}_p(\zeta_n) \subseteq \mathbb{Q}_p(\zeta_{n'}, \zeta_{p^{\mathrm{ord}_p(n)}})$. 结合上面的讨论, $\mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_{n'}, \zeta_{p^{\mathrm{ord}_p(n)}})$. 由定理7.17, 素数$p$在$\mathbb{Q}_p(\zeta_{n'})$上不分歧. 由定理7.19, p在$\mathbb{Q}_p(\zeta_{p^{\mathrm{ord}_p(n)}})$上完全分歧. 因此, $\mathbb{Q}_p(\zeta_{n'}) \cap \mathbb{Q}_p(\zeta_{p^{\mathrm{ord}_p(n)}}) = \mathbb{Q}_p$.

(ii) 因为$\mathbb{Q}_p(\zeta_{n'}) \cap \mathbb{Q}_p(\zeta_{p^{\mathrm{ord}_p(n)}}) = \mathbb{Q}_p$, 由Galois定理, (ii)显然成立.

(iii) 设$K = \mathbb{Q}_p(\zeta_{p^{\mathrm{ord}_p(n)}})$. 由定理7.19, $\mathcal{O}_K = \mathbb{Z}_p[\zeta_{p^{\mathrm{ord}_p(n)}}]$. 由(i), 我们有$\mathbb{Q}_p(\zeta_n) = K(\zeta_{n'})$. 再利用定理7.17, $\mathcal{O}_K$在$\mathbb{Q}_p(\zeta_n)$上的整闭包为

$$\mathcal{O}_K[\zeta_{n'}] = \mathbb{Z}_p[\zeta_{n'}, \zeta_{p^{\mathrm{ord}_p(n)}}] = \mathbb{Z}_p[\zeta_n].$$

由注记7.7, 我们知道$\mathcal{O}_K$在$\mathbb{Q}_p(\zeta_n)$上的整闭包恰好是$\mathbb{Q}_p(\zeta_n)$的赋值环. 再利用注记7.7, $\mathbb{Q}_p(\zeta_n)$的赋值环恰好就是$\mathbb{Z}_p$在$\mathbb{Q}_p(\zeta_n)$上的整闭包. 因此, (iii)成立.

综上, 我们完成了证明. □

8 微分与判别式

8.1 微分

我们将利用前面介绍的局部域理论来研究一般Dedekind环的微分与判别式.

除非特别说明, 本章中我们设$\mathcal{O}_K$为Dedekind环, $\mathrm{frac}(\mathcal{O}_K)=K$, L/K为域的有限可分扩张. 对于L/K的任意中间域M, 记号$\mathcal{O}_M$表示$\mathcal{O}_K$在M上的整闭包. 对$\mathcal{O}_L$的任意非零素理想$\mathfrak{P}$, 总假定剩余类域扩张$(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$为有限可分扩张, 其中$\mathfrak{p}=\mathfrak{P}\cap\mathcal{O}_K$.

L在$\mathfrak{P}$-adic赋值下的完备化记作$L_{\mathfrak{P}}$, 其赋值环记作$\widehat{\mathcal{O}_{\mathfrak{P}}}$. K在$\mathfrak{p}$-adic赋值下的完备化记作$K_{\mathfrak{p}}$, 其赋值环记作$\widehat{\mathcal{O}_{\mathfrak{p}}}$. 为了方便, 在拓扑同构的意义下, 设$K_{\mathfrak{p}}\subseteq L_{\mathfrak{P}}$.

我们首先给出如下定义.

定义 8.1. *设$I\in J(\mathcal{O}_L)$为$\mathcal{O}_L$的分式理想. 定义I的对偶$\mathcal{O}_L$模为*

$$I^*:=\left\{x\in L:\ \mathrm{Tr}_{L/K}(xI)\subseteq\mathcal{O}_K\right\}.$$

显然$I^*\subseteq L$为$\mathcal{O}_L$模. 并且, 因为$I\in J(\mathcal{O}_L)$, 存在$t\neq\mathcal{O}_L\setminus\{0\}$使得$tI\subseteq\mathcal{O}_L$. 注意到

$$\mathrm{Tr}_{L/K}(tI)\subseteq\mathrm{Tr}_{L/K}(\mathcal{O}_L)\subseteq\mathcal{O}_K,$$

我们有$I^*\subseteq L$为非零$\mathcal{O}_L$模. 更进一步, 下面的结论成立.

命题 8.1. *记号如上. I^*为$\mathcal{O}_L$的分式理想.*

证明: 首先, 我们断言$I\cap\mathcal{O}_K\neq\{0\}$. 事实上, 因为$I\in J(\mathcal{O}_L)$, 由注记2.2, 存在$c\in\mathcal{O}_L\setminus\{0\}$使得$cI\subseteq\mathcal{O}_L$. 容易验证对任意的$x\in cI\setminus\{0\}$,

$$\mathrm{N}_{L/K}(x)\in(cI\cap\mathcal{O}_K)\setminus\{0\}\subseteq(I\cap\mathcal{O}_K)\setminus\{0\}.$$

因此, 上述断言成立.

设$b_1,b_2,\cdots,b_n\in\mathcal{O}_L$为$L/K$的一组基, $d=d(b_1,b_2,\cdots,b_n)\neq0$. 对任意的$x\in I^*$, 设

$$x=x_1b_1+x_2b_2+\cdots+x_nb_n,$$

其中$x_1, x_2, \cdots, x_n \in K$. 固定一个$a \in (I \cap \mathcal{O}_K) \setminus \{0\}$. 对任意的$1 \leq i \leq n$, 在上式两边同时乘以$ab_i$, 我们得到

$$axb_i = \sum_{j=1}^{n} ax_j b_i b_j.$$

因此我们得到线性方程组

$$\mathrm{Tr}_{L/K}(axb_i) = \sum_{j=1}^{n} ax_j \mathrm{Tr}_{L/K}(b_i b_j),\ (1 \leq i \leq n).$$

注意到

$$\mathrm{Tr}_{L/K}(axb_i) \in \mathrm{Tr}_{L/K}(xI) \subseteq \mathcal{O}_K,$$

由Cramer法则, 对任意的$1 \leq j \leq n$,

$$ax_j \in \frac{1}{d}\mathcal{O}_K.$$

因此

$$adx = \sum_{j=1}^{n} adx_j b_j \in \mathcal{O}_L,$$

即$adI^* \subseteq \mathcal{O}_L$. 由注记2.2以及$I^* \subseteq L$为非零$\mathcal{O}_L$模, 上式说明$I^*$为$\mathcal{O}_L$的分式理想.

综上, 我们完成了证明. □

下面我们给出微分的定义.

定义 8.2. 记号如上. 令

$$\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K} := \mathcal{O}_L^* = \left\{x \in L :\ \mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\right\}.$$

我们称

$$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K} := \mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}^{-1}$$

为$\mathcal{O}_L$关于$\mathcal{O}_K$的微分.

注记 8.1. 因为$\mathcal{O}_L \subseteq \mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}$, 微分$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K} \subseteq \mathcal{O}_L$是$\mathcal{O}_L$的整理想.

为了介绍微分的性质, 我们首先需要下面这个非常有用的引理.

引理 8.1. 设A为*Dedekind*环, $\mathrm{frac}(A) = K$. 对A的非零素理想$\mathfrak{p}$, 设$K_{\mathfrak{p}}$为K在$\mathfrak{p}$-*adic*赋值下的完备化, $\widehat{A_{\mathfrak{p}}}$为其赋值环. 则$A$的任意分式理想$\mathfrak{a}$在$K_{\mathfrak{p}}$中的闭包恰好为$\mathfrak{a}\widehat{A_{\mathfrak{p}}}$.

证明: 设A在$\mathfrak{p}$处的局部化为$A_{\mathfrak{p}}$. 由定理3.2, $A_{\mathfrak{p}}$是离散赋值环. 设π为$A_{\mathfrak{p}}$的一个素元. 则由定理7.6, 元素π也为$\widehat{A_{\mathfrak{p}}}$的素元, 即

$$\widehat{\mathfrak{p}} = \pi\widehat{A_{\mathfrak{p}}} = \mathfrak{p}\widehat{A_{\mathfrak{p}}}$$

为离散赋值环$\widehat{A_{\mathfrak{p}}}$的唯一极大理想.

由上面的讨论,

$$\mathfrak{a}\widehat{A_{\mathfrak{p}}} = \left\{x \in K_{\mathfrak{p}} : \operatorname{ord}_{\widehat{\mathfrak{p}}}(x) \geq \operatorname{ord}_{\widehat{\mathfrak{p}}}(\mathfrak{a}\widehat{A_{\mathfrak{p}}}) = \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a})\right\}$$

为一个包含$\mathfrak{a}$的闭集. 因此, $C \subseteq \mathfrak{a}\widehat{A_{\mathfrak{p}}}$. 另一方面, 由命题7.8我们知道$A_{\mathfrak{p}}$在$\widehat{A_{\mathfrak{p}}}$中稠密. 因此, $\mathfrak{a}$在$\mathfrak{a}\widehat{A_{\mathfrak{p}}}$中也稠密. 结合上面的讨论, $\mathfrak{a}$在$K_{\mathfrak{p}}$中的闭包恰好为$\mathfrak{a}\widehat{A_{\mathfrak{p}}}$.

综上, 我们完成了证明. □

关于这个引理, 我们给出如下注记.

注记 8.2. 从引理的证明中我们发现, A中素理想$\mathfrak{p}$在$\widehat{A_{\mathfrak{p}}}$中的扩理想$\mathfrak{p}\widehat{A_{\mathfrak{p}}}$恰好就是$\widehat{A_{\mathfrak{p}}}$的唯一非零素理想. 因此$\operatorname{ord}_{\widehat{\mathfrak{p}}}$恰好就是$\operatorname{ord}_{\mathfrak{p}}$在$K_{\mathfrak{p}}$上的延拓. 为了减少记号, 将$\operatorname{ord}_{\widehat{\mathfrak{p}}}$简记为$\operatorname{ord}_{\mathfrak{p}}$, 将$K_{\mathfrak{p}}$上的$\widehat{\mathfrak{p}}$-*adic*赋值$|\cdot|_{\widehat{\mathfrak{p}}}$简记为$|\cdot|_{\mathfrak{p}}$.

关于微分我们有下面的结论.

定理 8.1. 记号如上. 则下列结论成立.

(i) 对L/K的任意中间域M,

$$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K} = \mathcal{D}_{\mathcal{O}_L/\mathcal{O}_M}\mathcal{D}_{\mathcal{O}_M/\mathcal{O}_K}\mathcal{O}_L.$$

(ii) 设$S \subseteq \mathcal{O}_K$为乘法子集. 则

$$S^{-1}\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K} = \mathcal{D}_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}.$$

(iii) 设$\mathfrak{P}$为$\mathcal{O}_L$的非零素理想, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_L$. 则

$$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}\widehat{\mathcal{O}_{\mathfrak{P}}} = \mathcal{D}_{\widehat{\mathcal{O}_{\mathfrak{P}}}/\widehat{\mathcal{O}_{\mathfrak{p}}}}.$$

证明: (i) 由微分的定义, 我们仅需证明

$$\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K} = \mathcal{C}_{\mathcal{O}_L/\mathcal{O}_M}\mathcal{C}_{\mathcal{O}_M/\mathcal{O}_K}\mathcal{O}_L.$$

首先, 容易验证

$$\begin{aligned}\mathrm{Tr}_{L/K}\left(\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_M}\mathcal{C}_{\mathcal{O}_M/\mathcal{O}_K}\mathcal{O}_L\mathcal{O}_L\right) &= \mathrm{Tr}_{M/K}\circ\mathrm{Tr}_{L/M}\left(\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_M}\mathcal{C}_{\mathcal{O}_M/\mathcal{O}_K}\mathcal{O}_L\mathcal{O}_L\right)\\ &= \mathrm{Tr}_{M/K}\left(\mathcal{C}_{\mathcal{O}_M/\mathcal{O}_K}\mathrm{Tr}_{L/M}\left(\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_M}\mathcal{O}_L\right)\right)\\ &\subseteq \mathrm{Tr}_{M/K}\left(\mathcal{C}_{\mathcal{O}_M/\mathcal{O}_K}\mathcal{O}_M\right)\\ &\subseteq \mathcal{O}_K.\end{aligned}$$

因此, $\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_M}\mathcal{C}_{\mathcal{O}_M/\mathcal{O}_K}\mathcal{O}_L\subseteq\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}$. 反过来, 因为

$$\begin{aligned}\mathrm{Tr}_{M/K}\left(\mathrm{Tr}_{L/M}\left(\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{O}_L\right)\mathcal{O}_M\right) &= \mathrm{Tr}_{L/K}\left(\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{O}_L\mathcal{O}_M\right)\\ &= \mathrm{Tr}_{L/K}\left(\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{O}_L\right)\\ &\subseteq \mathcal{O}_K,\end{aligned}$$

我们得到

$$\begin{aligned}&\mathrm{Tr}_{L/M}\left(\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{O}_L\right)\subseteq\mathcal{C}_{\mathcal{O}_M/\mathcal{O}_K}\\ \Rightarrow\ &\mathrm{Tr}_{L/M}\left(\mathcal{C}^{-1}_{\mathcal{O}_M/\mathcal{O}_K}\mathcal{O}_L\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{O}_L\right)\subseteq\mathcal{O}_M\\ \Rightarrow\ &\mathcal{C}^{-1}_{\mathcal{O}_M/\mathcal{O}_K}\mathcal{O}_L\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\subseteq\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_M}\\ \Rightarrow\ &\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\subseteq\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_M}\mathcal{C}_{\mathcal{O}_M/\mathcal{O}_K}\mathcal{O}_L.\end{aligned}$$

结合上面的讨论, (i)成立.

(ii) 此时仅需证明

$$S^{-1}\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}=\mathcal{C}_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}.$$

首先, 容易验证

$$\begin{aligned}\mathrm{Tr}_{L/K}\left(S^{-1}\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}S^{-1}\mathcal{O}_L\right) &= S^{-1}\mathrm{Tr}_{L/K}\left(\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\mathcal{O}_L\right)\\ &\subseteq S^{-1}\mathcal{O}_K.\end{aligned}$$

这说明$S^{-1}\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\subseteq\mathcal{C}_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}$. 反过来, 设$b_1,\cdots,b_n\in\mathcal{O}_L$为$L/K$的一组基, $d=d(b_1,b_2,\cdots,b_n)\neq 0$. 由引理1.3,

$$d\mathcal{O}_L\subseteq\mathcal{O}_Kb_1+\mathcal{O}_Kb_2+\cdots+\mathcal{O}_Kb_n.$$

这说明$\mathcal{O}_L$是诺特$\mathcal{O}_K$模的子模. 因此, $\mathcal{O}_L$是有限生成$\mathcal{O}_K$模. 不妨设

$$\mathcal{O}_L=\mathcal{O}_Kx_1+\mathcal{O}_Kx_2+\cdots+\mathcal{O}_Kx_m,$$

其中$x_1,\cdots,x_m\in\mathcal{O}_L$. 则对任意的$x\in\mathcal{C}_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}$, 容易验证

$$\begin{aligned}x\in\mathcal{C}_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}&\Rightarrow \mathrm{Tr}_{L/K}(x\mathcal{O}_L)\subseteq\mathrm{Tr}_{L/K}(xS^{-1}\mathcal{O}_L)\subseteq S^{-1}\mathcal{O}_K\\&\Rightarrow \mathrm{Tr}_{L/K}(xx_i)\in S^{-1}\mathcal{O}_K\ (\forall 1\leq i\leq m)\\&\Rightarrow \text{存在}s_i\in S\text{使得}\mathrm{Tr}_{L/K}(xx_i)\in\frac{1}{s_i}\mathcal{O}_K\ (\forall 1\leq i\leq m).\end{aligned}$$

令$s=s_1s_2\cdots s_n\in S$. 则由上面的讨论,

$$\mathrm{Tr}_{L/K}(sx\mathcal{O}_L)=\sum_{i=1}^m\mathrm{Tr}_{L/K}(sx_i\mathcal{O}_K)\in\mathcal{O}_K.$$

这说$x\in S^{-1}\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}$, 即

$$\mathcal{C}_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}\subseteq S^{-1}\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}.$$

结合前面的讨论, 我们得到

$$\mathcal{C}_{S^{-1}\mathcal{O}_L/S^{-1}\mathcal{O}_K}=S^{-1}\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}.$$

综上, (ii)成立.

(iii) 此时仅需证明

$$\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\widehat{\mathcal{O}_\mathfrak{P}}=\mathcal{C}_{\widehat{\mathcal{O}_\mathfrak{P}}/\widehat{\mathcal{O}_\mathfrak{p}}}.$$

设$S=\mathcal{O}_K\setminus\mathfrak{p}$, $(\mathcal{O}_L)_\mathfrak{p}=S^{-1}\mathcal{O}_L$. 注意到$S\in\widehat{\mathcal{O}_\mathfrak{P}}^\times$, 由(ii)得到

$$\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\widehat{\mathcal{O}_\mathfrak{P}}=S^{-1}\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}\widehat{\mathcal{O}_\mathfrak{P}}=\mathcal{C}_{(\mathcal{O}_L)_\mathfrak{p}/(\mathcal{O}_K)_\mathfrak{p}}\widehat{\mathcal{O}_\mathfrak{p}}.$$

下面仅需证明

$$\mathcal{C}_{(\mathcal{O}_L)_\mathfrak{p}/(\mathcal{O}_K)_\mathfrak{p}}\widehat{\mathcal{O}_\mathfrak{p}}=\mathcal{C}_{\widehat{\mathcal{O}_\mathfrak{P}}/\widehat{\mathcal{O}_\mathfrak{p}}}.$$

为此, 先说明$\mathcal{C}_{(\mathcal{O}_L)_\mathfrak{p}/(\mathcal{O}_K)_\mathfrak{p}}\subseteq\mathcal{C}_{\widehat{\mathcal{O}_\mathfrak{P}}/\widehat{\mathcal{O}_\mathfrak{p}}}$. 对任意的$x\in\mathcal{C}_{(\mathcal{O}_L)_\mathfrak{p}/(\mathcal{O}_K)_\mathfrak{p}}$以及任意的$y\in\widehat{\mathcal{O}_\mathfrak{P}}$, 因为$\mathcal{O}_L$在$\mathfrak{P}$处的局部化$(\mathcal{O}_L)_\mathfrak{P}$在$\widehat{\mathcal{O}_\mathfrak{P}}$中稠密(命题7.8) 存在$y'\in(\mathcal{O}_L)_\mathfrak{P}$使得$|y-y'|_\mathfrak{P}$充分小. 设

$$\Omega_\mathfrak{p}=\{\mathfrak{P}'\lhd\mathcal{O}_L:\ \mathfrak{P}'\text{为素理想且}\mathfrak{p}\subseteq\mathfrak{P}'\}.$$

则由定理7.1, 存在$\xi\in L$使得 $|\xi-y'|_\mathfrak{P}$以及$|\xi|_{\mathfrak{P}'}(\forall\mathfrak{P}'\in\Omega_\mathfrak{p}\setminus\{\mathfrak{P}\})$都充分小. 并且因此$\xi\in(\mathcal{O}_L)_\mathfrak{p}$. 再由$y'$的取法, $|\xi-y|_\mathfrak{P}$也充分小. 类似于定理7.14的证明, 容易说明这些指数赋值

$$\frac{1}{e(\mathfrak{P}'|\mathfrak{p})}\mathrm{ord}_{\mathfrak{P}'}\ (\mathfrak{P}'\in\Omega_\mathfrak{p})$$

恰好就是K上的指数赋值$\mathrm{ord}_{\mathfrak{p}}$在$L$上的全部延拓. 由推论7.3,

$$\mathrm{Tr}_{L/K}(x\xi)=\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x\xi)+\sum_{\mathfrak{P}'\in\Omega_{\mathfrak{p}}\setminus\{\mathfrak{P}\}}\mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(x\xi). \tag{8.1}$$

因为$|\xi|_{\mathfrak{P}'}$充分小, 如果令$|\cdot|_{\mathfrak{p}}$为$\mathfrak{p}$-adic赋值在$L_{\mathfrak{P}'}$上的延拓, 则

$$\begin{aligned}\left|\mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(x\xi)\right|_{\mathfrak{p}}&=\left|\sum_{\sigma\in\mathrm{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}'},K_{\mathfrak{p}}^{\mathrm{alg}})}\sigma(x\xi)\right|_{\mathfrak{p}}\\&\leq\max\left\{|\sigma(x\xi)|_{\mathfrak{p}}:\ \sigma\in\mathrm{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}'},K_{\mathfrak{p}}^{\mathrm{alg}})\right\}.\end{aligned} \tag{8.2}$$

注意到对任意的$\sigma\in\mathrm{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}'},K_{\mathfrak{p}}^{\mathrm{alg}})$, 赋值$|\cdot|_{\mathfrak{p}}\circ\sigma$也是$K_{\mathfrak{p}}$上的$\mathfrak{p}$-adic赋值在$L_{\mathfrak{P}'}$上的延拓, 由定理7.11有$|\cdot|_{\mathfrak{p}}\circ\sigma=|\cdot|_{\mathfrak{p}}$. 因此, 由(8.2), 对任意的$\mathfrak{P}'\in\Omega_{\mathfrak{p}}\setminus\{\mathfrak{P}\}$, 都有$|\mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(x\xi)|_{\mathfrak{p}}$充分小, 即$\mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(x\xi)\in\widehat{\mathcal{O}_{\mathfrak{p}}}$. 由此并注意到$\mathrm{Tr}_{L/K}(x\xi)\in(\mathcal{O}_K)_{\mathfrak{p}}\subseteq\widehat{\mathcal{O}_{\mathfrak{p}}}$, 由(8.1)有$\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x\xi)\in\widehat{\mathcal{O}_{\mathfrak{p}}}$. 利用与(8.2)类似的方法, 可以说明$|\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x(\xi-y))|_{\mathfrak{p}}$也充分小, 即$\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x(\xi-y))\in\widehat{\mathcal{O}_{\mathfrak{p}}}$. 利用上面的讨论,

$$\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(xy)=\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x\xi)-\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(x(\xi-y))\in\widehat{\mathcal{O}_{\mathfrak{p}}}.$$

这说明$\mathcal{C}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}}\subseteq\mathcal{C}_{\widehat{\mathcal{O}_{\mathfrak{P}}}/\widehat{\mathcal{O}_{\mathfrak{p}}}}$.

下面来说明$\mathcal{C}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}}$在$\mathcal{C}_{\widehat{\mathcal{O}_{\mathfrak{P}}}/\widehat{\mathcal{O}_{\mathfrak{p}}}}$中是稠密的. 对任意的$\gamma\in\mathcal{C}_{\widehat{\mathcal{O}_{\mathfrak{P}}}/\widehat{\mathcal{O}_{\mathfrak{p}}}}$, 类似于上面的证明, 存在$\alpha\in L$使得$|\alpha-\gamma|_{\mathfrak{P}}$以及$|\alpha|_{\mathfrak{P}'}(\forall\mathfrak{P}'\in\Omega_{\mathfrak{p}}\setminus\{\mathfrak{P}\})$都充分小. 我们断言$\alpha\in\mathcal{C}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}}$. 事实上, 对任意的$z\in(\mathcal{O}_L)_{\mathfrak{p}}$, 由推论7.3

$$\mathrm{Tr}_{L/K}(\alpha z)=\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}((\alpha-\gamma)z)+\mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\gamma z)+\sum_{\mathfrak{P}'\in\Omega_{\mathfrak{p}}\setminus\{\mathfrak{P}\}}\mathrm{Tr}_{L_{\mathfrak{P}'}/K_{\mathfrak{p}}}(\alpha z).$$

由此并利用与上面证明类似的方法容易得到$\mathrm{Tr}_{L/K}(\alpha z)\in(\mathcal{O}_K)_{\mathfrak{p}}$. 由上面的讨论, $\mathcal{C}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}}$在$\mathcal{C}_{\widehat{\mathcal{O}_{\mathfrak{P}}}/\widehat{\mathcal{O}_{\mathfrak{p}}}}$中稠密. 因此, 由引理8.1得到

$$\mathcal{C}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}}\widehat{\mathcal{O}_{\mathfrak{p}}}=\mathcal{C}_{\widehat{\mathcal{O}_{\mathfrak{P}}}/\widehat{\mathcal{O}_{\mathfrak{p}}}}.$$

综上, 我们完成了证明. □

下面我们来解释将$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$称为微分的原因. 为此, 我们给出如下定义.

定义 8.3. 记号如上. 对任意的$x\in\mathcal{O}_L$, 设$f(t)\in\mathcal{O}_K[t]$为x在K上的极小多项式. 定义元素x的微分为

$$\delta_{L/K}(x):=\begin{cases}f'(x) & \text{如果 } L=K(\alpha),\\ 0 & \text{如果 } L\neq K(\alpha).\end{cases}$$

当$\mathcal{O}_L$关于$\mathcal{O}_K$存在幂元整基时, 微分是容易计算的.

命题 8.2. 记号如上. 如果存在$x \in \mathcal{O}_L$使得$\mathcal{O}_L = \mathcal{O}_K[x]$, 则

$$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K} = \delta_{L/K}(x)\mathcal{O}_L.$$

证明: 设

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in \mathcal{O}_K[t]$$

为x在K上的极小多项式, 设

$$\frac{f(t)}{t-x} = b_{n-1}t^{n-1} + b_{n-2}t^{n-2} + \cdots + b_1 t + b_0 \in \mathcal{O}_L[t], \tag{8.3}$$

并且容易验证

$$b_{n-1} = 1, b_{n-2} = x + a_{n-1}, \cdots, b_0 = x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1.$$

这说明$1, x, \cdots, x^{n-1} \in \mathcal{O}_K b_0 + \mathcal{O}_K b_1 + \cdots + \mathcal{O}_K b_{n-1}$. 因此

$$\mathcal{O}_K b_0 + \mathcal{O}_K b_1 + \cdots + \mathcal{O}_K b_{n-1} = \mathcal{O}_K[x] = \mathcal{O}_L. \tag{8.4}$$

设$x_1, x_2, \cdots, x_n$为$f(t)$在K^{alg}上全部零点, 其中$x_1 = x$. 因为L/K为有限可分扩张, 这些x_i两两不同. 对任意的$0 \leq r \leq n-1$, 注意到对任意的$1 \leq j \leq n$都有

$$x_j^r = \sum_{i=1}^{n} \frac{x_i^r}{f'(x_i)} \cdot \frac{f(x_j)}{x_j - x_i}.$$

因此, 对任意的$0 \leq r \leq n-1$都有

$$t^r = \sum_{i=1}^{n} \frac{x_i^r}{f'(x_i)} \cdot \frac{f(t)}{t - x_i}. \tag{8.5}$$

将(8.3)代入(8.5)可以得到

$$\mathrm{Tr}_{L/K}\left(\frac{b_l}{f'(x)}x^r\right) = \begin{cases} 1 & \text{如果 } l = r, \\ 0 & \text{如果 } l \neq r. \end{cases}$$

这说明基$1, x, \cdots, x^{n-1}$在非退化对称双线性型$\mathrm{Tr}_{L/K}(\cdot)$下的对偶基恰好为

$$\frac{b_0}{f'(x)}, \frac{b_1}{f'(x)}, \cdots, \frac{b_{n-1}}{f'(x)}.$$

因此, 容易验证

$$\begin{aligned}\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K} &= \left\{y \in L:\ \mathrm{Tr}_{L/K}(y\mathcal{O}_L) \subseteq \mathcal{O}_K\right\}\\ &= \left\{y \in L:\ \mathrm{Tr}_{L/K}(yx^i) \in \mathcal{O}_K\ \forall 0 \leq i \leq n-1\right\}\\ &= \mathcal{O}_K\frac{b_0}{f'(x)} + \mathcal{O}_K\frac{b_1}{f'(x)} + \cdots + \mathcal{O}_K\frac{b_{n-1}}{f'(x)}.\end{aligned}$$

由(8.4), 上式说明

$$\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K} = \frac{1}{f'(x)}\left(\mathcal{O}_K b_0 + \mathcal{O}_K b_1 + \cdots + \mathcal{O}_K b_{n-1}\right) = \frac{1}{f'(x)}\mathcal{O}_L. \tag{8.6}$$

因此,

$$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K} = f'(x)\mathcal{O}_L = \delta_{L/K}(x)\mathcal{O}_L.$$

综上, 我们完成了定理的证明. □

注记 8.3. 这个命题的证明中蕴含着一个很有用的结论. 当$\mathcal{O}_L = \mathcal{O}_K[x]$时, 由*(8.6)*, 对偶模

$$\mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K} = \frac{1}{f'(x)}\mathcal{O}_L = \mathcal{O}_K\frac{1}{f'(x)} + \mathcal{O}_K\frac{x}{f'(x)} + \cdots + \mathcal{O}_K\frac{x^{n-1}}{f'(x)}$$

为自由$\mathcal{O}_K$模, 其中$n = [L:K]$.

回顾第一章的内容, 我们知道一般情况下$\mathcal{O}_L$关于$\mathcal{O}_K$的整基不一定存在, 并且即使$\mathcal{O}_L$关于$\mathcal{O}_K$的整基存在也不能保证幂元整基的存在性, 但是下面的结论说明在完备的离散赋值域中, 幂元整基是存在的.

命题 8.3. 设K为完备的离散赋值域, 其赋值环为$\mathcal{O}_K$, $\mathfrak{p}$为$\mathcal{O}_K$的唯一非零素理想. 设L/K为域的有限可分扩张, $\mathcal{O}_L$为其赋值环, $\mathfrak{P}$为$\mathcal{O}_L$的唯一非零素理想. 如果剩余类域$(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$为有限可分扩张, 则存在 $x \in \mathcal{O}_L$使得

$$\mathcal{O}_L = \mathcal{O}_K[x].$$

证明: 设$\lambda = \mathcal{O}_L/\mathfrak{P}, \kappa = \mathcal{O}_K/\mathfrak{p}$. 因为$\lambda/\kappa$为有限可分扩张, 存在$\beta \in \mathcal{O}_L$使得

$$\lambda = \kappa(\bar{\beta}),$$

其中$\bar{\beta} = \beta \bmod \mathfrak{P} \in \lambda$. 设$\tilde{f}(t)$为$\bar{\beta}$在$\kappa$上的极小多项式, $f(t) \in \mathcal{O}_K[t]$为首一多项式使得

$$f(t) \bmod \mathfrak{p} = \tilde{f}(t).$$

我们断言存在$\beta^* \in \mathcal{O}_L$使得$f(\beta^*)$为$\mathcal{O}_L$上的素元并且$\beta^* \equiv \beta \pmod{\mathfrak{P}}$. 事实上, 因为$\tilde{f}(\bar{\beta}) = 0$, 有$\mathrm{ord}_{\mathfrak{P}}(f(\beta)) \geq 1$. 如果$\mathrm{ord}_{\mathfrak{P}}(f(\beta)) = 1$, 则令$\beta^* = \beta$. 下面考虑$\mathrm{ord}_{\mathfrak{P}}(f(\beta)) \geq 2$的情形. 取$\mathcal{O}_L$上的一个素元$\pi_L$. 则

$$f(\beta + \pi_L) = f(\beta) + f'(\beta)\pi_L + g(\beta)\pi_L^2, \tag{8.7}$$

其中$g(t) \in \mathcal{O}_L[t]$. 因为$\lambda/\kappa$为有限可分扩张, 极小多项式$\tilde{f}(t)$无重根. 因此$\mathrm{ord}_{\mathfrak{P}}(f'(\beta)) = 0$. 由命题7.2, 有$\mathrm{ord}_{\mathfrak{P}}(f(\beta+\pi_L)) = 1$. 此时令$\beta^* = \beta+\pi_L$即可. 由上面的讨论, 断言成立.

由注记7.8, 元素$f(\beta^*)^i(\beta^*)^j$ $(0 \leq i \leq e(\mathfrak{P}|\mathfrak{p}) - 1, 1 \leq j \leq f(\mathfrak{P}|\mathfrak{p}))$恰好为$\mathcal{O}_L$关于$\mathcal{O}_K$的整基. 因此,

$$\mathcal{O}_K[\beta^*] \subseteq \mathcal{O}_L = \sum_{0\leq i\leq e(\mathfrak{P}|\mathfrak{p})-1} \sum_{1\leq j\leq f(\mathfrak{P}|\mathfrak{p})} f(\beta^*)^i(\beta^*)^j\mathcal{O}_K \subseteq \mathcal{O}_K[\beta^*].$$

这说明

$$\mathcal{O}_L = \mathcal{O}_K[\beta^*].$$

综上, 我们完成了证明. □

注记 8.4. 这个命题的证明中蕴藏着一个有用的结论. 考虑上述证明中构造的β^*. 利用(8.7)容易说明, 对任意的$x \in \mathcal{O}_L$, 如果$\mathrm{ord}_{\mathfrak{P}}(x - \beta^*) \geq 2$, 则

$$\mathcal{O}_L = \mathcal{O}_K[x].$$

下面的定理解释了将$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$称为微分的原因.

定理 8.2. $\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$是由集合

$$\left\{\delta_{L/K}(x) : x \in \mathcal{O}_L\right\}$$

生成的理想.

证明: 首先证明

$$\left\{\delta_{L/K}(x) : x \in \mathcal{O}_L\right\} \subseteq \mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}.$$

对任意的$x \in \mathcal{O}_L$使得$L = K(x)$, 设$f(t) \in \mathcal{O}_K[t]$为$x$在$K$上的极小多项式. 类似于定义4.2, 定义$\mathcal{O}_K[x]$在$\mathcal{O}_L$中的导子为

$$\mathfrak{f}_{\mathcal{O}_K[x]} := \left\{y \in \mathcal{O}_L : y\mathcal{O}_L \subseteq \mathcal{O}_K[x]\right\}.$$

则容易验证(注意因为L/K为可分扩张, $f'(x)\neq 0$)

$$y\in \mathfrak{f}_{\mathcal{O}_K[x]}\Leftrightarrow y\mathcal{O}_L\subseteq \mathcal{O}_K[x]\Leftrightarrow f'(x)^{-1}y\mathcal{O}_L\subseteq f'(x)^{-1}\mathcal{O}_K[x]. \tag{8.8}$$

由注记8.3,

$$\frac{1}{f'(x)},\frac{x}{f'(x)},\cdots,\frac{x^{n-1}}{f'(x)}$$

恰好是$\mathcal{O}_K$模

$$M=\left\{z\in L:\ \mathrm{Tr}_{L/K}(z\mathcal{O}_K[x])\subseteq \mathcal{O}_K\right\}$$

的一组$\mathcal{O}_K$基, 其中$n=[L:K]$. 因此

$$M=\left\{z\in L:\ \mathrm{Tr}_{L/K}(z\mathcal{O}_K[x])\subseteq \mathcal{O}_K\right\}=f'(x)^{-1}\mathcal{O}_K[x]. \tag{8.9}$$

由(8.8)与(8.9), 容易验证

$$\begin{aligned}
y\in \mathfrak{f}_{\mathcal{O}_K[x]}&\Leftrightarrow f'(x)^{-1}y\mathcal{O}_L\subseteq f'(x)^{-1}\mathcal{O}_K[x]=M\\
&\Leftrightarrow f'(x)^{-1}y\in M\ (\text{因为}y\mathcal{O}_L\subseteq \mathcal{O}_K[x])\\
&\Leftrightarrow \mathrm{Tr}_{L/K}\left(f'(x)^{-1}y\mathcal{O}_K[x]\right)\subseteq \mathcal{O}_K\\
&\Leftrightarrow \mathrm{Tr}_{L/K}\left(f'(x)^{-1}y\mathcal{O}_L\right)\subseteq \mathcal{O}_K\\
&\Leftrightarrow f'(x)^{-1}y\in \mathcal{C}_{\mathcal{O}_L/\mathcal{O}_K}=\mathcal{D}^{-1}_{\mathcal{O}_L/\mathcal{O}_K}\\
&\Leftrightarrow y\in f'(x)\mathcal{D}^{-1}_{\mathcal{O}_L/\mathcal{O}_K}.
\end{aligned}$$

因此,

$$\delta_{L/K}(x)=f'(x)\in \mathfrak{f}_{\mathcal{O}_K[x]}\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}\subseteq \mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K},$$

即

$$\left\{\delta_{L/K}(x):\ x\in\mathcal{O}_L\right\}\subseteq \mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}.$$

由上面的讨论, 要证明该定理我们还只需说明: 对$\mathcal{O}_L$的任意非零素理想$\mathfrak{P}$, 存在$x\in\mathcal{O}_L$使得 $L=K(x)$且$\mathrm{ord}_{\mathfrak{P}}(\delta_{L/K}(x))=\mathrm{ord}_{\mathfrak{P}}(\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K})$.

设$\mathfrak{p}=\mathfrak{P}\cap\mathcal{O}_K$, $\kappa=\widehat{\mathcal{O}_{\mathfrak{p}}}/\mathfrak{p}\widehat{\mathcal{O}_{\mathfrak{p}}}$, $\lambda=\widehat{\mathcal{O}_{\mathfrak{P}}}/\mathfrak{P}\widehat{\mathcal{O}_{\mathfrak{P}}}$. 为了方便, 设$K_{\mathfrak{p}}$为$K$在$L_{\mathfrak{P}}$中的闭包. 由定理7.12, $\mathfrak{P}$-adic赋值的等价类是由$\mathrm{id}\in\mathrm{Hom}_K(L,K_{\mathfrak{p}}^{\mathrm{alg}})$确定的. 如果$\sigma,\sigma'\in\mathrm{Hom}_K(L,K_{\mathfrak{p}}^{\mathrm{alg}})$所确定的$\mathfrak{p}$-adic赋值的延拓相同, 则称$\sigma$与$\sigma'$是等价的(记作$\sigma\sim\sigma'$). 由定理7.12,

$$\sigma\sim\sigma'\Leftrightarrow \text{存在}\mu\in\mathrm{Hom}_{K_{\mathfrak{p}}}(K_{\mathfrak{p}}^{\mathrm{alg}},K_{\mathfrak{p}}^{\mathrm{alg}})\text{使得}\sigma'=\mu\circ\sigma.$$

设$\mathrm{Hom}_K(L,K_{\mathfrak{p}}^{\mathrm{alg}})$在该等价关系下的一组代表元系为

$$\mathrm{id}=\sigma_1,\sigma_2,\cdots,\sigma_r,$$

设$\mathfrak{P}_i$为$\mathcal{O}_L$的素理想使得$\mathfrak{p}\subseteq\mathfrak{P}_i$并且$|\cdot|_{\mathfrak{P}_i}$的等价类是由$\sigma_i$确定的(显然$\mathfrak{P}_1=\mathfrak{P}$), 设$|\cdot|_{\mathfrak{P}_i}=|\cdot|_{\mathfrak{p}}\circ\sigma_i$, 并且显然$|\cdot|_{\mathfrak{P}}$为$K_{\mathfrak{p}}^{\mathrm{alg}}$上的赋值$|\cdot|_{\mathfrak{p}}$在$L$上的限制.

由命题8.3及其证明, 存在$\beta^*\in\widehat{\mathcal{O}_{\mathfrak{P}}}$使得$\kappa(\overline{\beta^*})=\lambda$, $f(\beta^*)$为$\widehat{\mathcal{O}_{\mathfrak{P}}}$中的素元并且$\widehat{\mathcal{O}_{\mathfrak{P}}}=\widehat{\mathcal{O}_{\mathfrak{p}}}[\beta^*]$, 其中$\overline{\beta^*}=\beta^*\bmod\mathfrak{P}$并且$f(t)\in\widehat{\mathcal{O}_{\mathfrak{p}}}[t]$为$\beta^*$在$K_{\mathfrak{p}}$上的极小多项式. 由中国剩余定理, 存在$\alpha\in\mathcal{O}_L$使得

$$|\alpha-\beta^*|_{\mathfrak{P}}=|\alpha-\beta^*|_{\mathfrak{p}}\text{充分小},$$

并且

$$|\alpha-1|_{\mathfrak{P}_i}\text{充分小}\ (\forall 2\leq i\leq r).$$

因为L/K为有限可分扩张, 存在$\gamma\in\mathcal{O}_L$使得$L=K(\gamma)$. 取$\mathfrak{p}$的素元π_K以及一个充分大的整数N, 用$\alpha+\pi_K^N\gamma$代替上面的α. 则这种操作并不影响上面的逼近性质. 因此, 不妨设$L=K(\alpha)$. 由注记8.4, 有$\widehat{\mathcal{O}_{\mathfrak{P}}}=\widehat{\mathcal{O}_{\mathfrak{p}}}[\alpha]$. 由命题8.2,

$$\mathcal{D}_{\widehat{\mathcal{O}_{\mathfrak{P}}}/\widehat{\mathcal{O}_{\mathfrak{p}}}}=\delta_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha)\widehat{\mathcal{O}_{\mathfrak{P}}}.$$

由上面的讨论, 要证明该定理还只需证明

$$\mathrm{ord}_{\mathfrak{P}}\left(\delta_{L/K}(\alpha)\right)=\mathrm{ord}_{\mathfrak{P}}\left(\delta_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha)\right).$$

类似于定理7.18的证明, 利用定理7.5容易说明

$$\left\{\sigma\in\mathrm{Hom}_K(L,K_{\mathfrak{p}}^{\mathrm{alg}}):\ \sigma\sim\mathrm{id}\right\}$$

中的元素与集合$\mathrm{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}},K_{\mathfrak{p}}^{\mathrm{alg}})$中的元素是一一对应的. 因此,

$$\begin{aligned}\delta_{L/K}(\alpha)&=\prod_{\sigma\in\mathrm{Hom}_K(L,K_{\mathfrak{p}}^{\mathrm{alg}})\setminus\{\mathrm{id}\}}(\alpha-\sigma(\alpha))\\&=\prod_{\substack{\sigma\sim\mathrm{id}\\\sigma\neq\mathrm{id}}}(\alpha-\sigma(\alpha))\cdot\prod_{i=2}^{r}\prod_{j}(\alpha-\mu_{ij}\sigma_i(\alpha))\\&=\prod_{\sigma\in\mathrm{Hom}_{K_{\mathfrak{p}}}(L_{\mathfrak{P}},K_{\mathfrak{p}}^{\mathrm{alg}})\setminus\{\mathrm{id}\}}(\alpha-\sigma(\alpha))\cdot\prod_{i=2}^{r}\prod_{j\in X_i}(\alpha-\mu_{ij}\sigma_i(\alpha))\\&=\delta_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha)\cdot\prod_{i=2}^{r}\prod_{j\in X_i}(\alpha-\mu_{ij}\sigma_i(\alpha)),\end{aligned}\tag{8.10}$$

其中这些$\mu_{ij} \in \mathrm{Hom}_{K_\mathfrak{p}}(K_\mathfrak{p}^{\mathrm{alg}}, K_\mathfrak{p}^{\mathrm{alg}})$使得

$$\left\{\sigma \in \mathrm{Hom}_K(L, K_\mathfrak{p}^{\mathrm{alg}}) : \sigma \sim \sigma_i\right\} = \{\mu_{ij}\sigma_i : j \in X_i\} \ (\forall 2 \leq i \leq r).$$

对任意的$2 \leq i \leq r$, 利用赋值延拓的性质容易验证

$$\begin{aligned} |\alpha - \mu_{ij}\sigma_i(\alpha)|_\mathfrak{P} &= |\alpha - \mu_{ij}\sigma_i(\alpha)|_\mathfrak{p} \\ &= \left|\sigma_i(\alpha) - \mu_{ij}^{-1}(\alpha)\right|_\mathfrak{p} \\ &= \left|\sigma_i(\alpha) - 1 + 1 - \mu_{ij}^{-1}(\alpha)\right|_\mathfrak{p} \end{aligned} \tag{8.11}$$

由α的取法,

$$|\sigma_i(\alpha) - 1|_\mathfrak{p} = |\alpha - 1|_{\mathfrak{P}_i}\text{充分小},$$

并且

$$\left|1 - \mu_{ij}^{-1}(\alpha)\right|_\mathfrak{p} = |\alpha - 1|_\mathfrak{p} = 1,$$

其中最后一个等式成立是因为$\mathrm{ord}_\mathfrak{P}(\alpha) \geq 1$. 因此, 由(8.11)与命题7.2, 有

$$|\alpha - \mu_{ij}\sigma_i(\alpha)|_\mathfrak{P} = 1 \ (\forall 2 \leq i \leq r).$$

这说明

$$\mathrm{ord}_\mathfrak{P}\left(\prod_{i=2}^{r}\prod_{j\in X_i}(\alpha - \mu_{ij}\sigma_i(\alpha))\right) = 0.$$

由此与(8.11), 有

$$\mathrm{ord}_\mathfrak{P}\left(\delta_{L/K}(\alpha)\right) = \mathrm{ord}_\mathfrak{P}\left(\delta_{L_\mathfrak{P}/K_\mathfrak{p}}(\alpha)\right).$$

综上, 我们完成了定理的证明. □

下面的定理说明微分$\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}$与第四章的内容有着密切的联系.

定理 8.3. *在本章的假设下. 对$\mathcal{O}_L$的任意非零素理想$\mathfrak{P}$,*

$$e(\mathfrak{P}|\mathfrak{p}) \geq 2 \Leftrightarrow \mathrm{ord}_\mathfrak{P}\left(\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}\right) \geq 1,$$

其中$\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.

证明: 设$\widehat{\mathfrak{P}} = \mathfrak{P}\widehat{\mathcal{O}_\mathfrak{P}}, \widehat{\mathfrak{p}} = \mathfrak{p}\widehat{\mathcal{O}_\mathfrak{p}}$. 则

$$e(\mathfrak{P}|\mathfrak{p}) = e(\widehat{\mathfrak{P}}|\widehat{\mathfrak{p}}). \tag{8.12}$$

由命题8.3, 存在$\beta^* \in \widehat{\mathcal{O}_{\mathfrak{P}}}$使得$\widehat{\mathcal{O}_{\mathfrak{P}}} = \widehat{\mathcal{O}_{\mathfrak{p}}}[\beta^*]$. 设$f(t) \in \widehat{\mathcal{O}_{\mathfrak{p}}}[t]$为$\beta^*$在$K_{\mathfrak{p}}$上的极小多项式. 则由定理7.9, 多项式$\overline{f(t)} = f(t) \bmod \widehat{\mathfrak{p}}$在剩余类域$\widehat{\mathcal{O}_{\mathfrak{p}}}/\widehat{\mathfrak{p}}$上的分解只能形如

$$\overline{f(t)} = \widetilde{p(t)}^m,$$

其中$\widetilde{p(t)}$为剩余类域$\widehat{\mathcal{O}_{\mathfrak{p}}}/\widehat{\mathfrak{p}}$上的首一不可约多项式, m为正整数. 由定理4.4,

$$m = e(\widehat{\mathfrak{P}}|\widehat{\mathfrak{p}}).$$

因此, 由(8.12), 命题8.2以及定理8.1, 容易验证

$$\begin{aligned} e(\mathfrak{P}|\mathfrak{p}) = 1 &\Leftrightarrow e(\widehat{\mathfrak{P}}|\widehat{\mathfrak{p}}) = 1 \\ &\Leftrightarrow m = 1 \\ &\Leftrightarrow f'(\beta^*) \not\equiv 0 \ (\mathrm{mod}\ \widehat{\mathfrak{P}}) \\ &\Leftrightarrow \mathrm{ord}_{\mathfrak{P}}\left(\delta_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\beta^*)\right) = 0 \\ &\Leftrightarrow \mathrm{ord}_{\mathfrak{P}}(\mathcal{D}_{\widehat{\mathcal{O}_{\mathfrak{P}}}/\widehat{\mathcal{O}_{\mathfrak{p}}}}) = 0 \\ &\Leftrightarrow \mathrm{ord}_{\mathfrak{P}}(\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}) = 0. \end{aligned}$$

综上, 我们完成了定理的证明. □

8.2 判别式

我们首先给出判别式的定义.

定义 8.4. 记号如上. 将由集合

$$\{d(b_1, b_2, \cdots, b_n) : \ b_1, b_2, \cdots, b_n \in \mathcal{O}_L \text{为} L/K \text{的一组基}\}$$

在$\mathcal{O}_K$上生成的理想称为$\mathcal{O}_L$关于$\mathcal{O}_K$的判别式, 记作$d_{\mathcal{O}_L/\mathcal{O}_K}$.

注记 8.5. 如果$b_1, b_2, \cdots, b_n \in \mathcal{O}_L$为$\mathcal{O}_L$关于$\mathcal{O}_K$的一组整基, 则显然有

$$d_{\mathcal{O}_L/\mathcal{O}_K} = d(b_1, b_2, \cdots, b_n)\mathcal{O}_K.$$

为了揭示判别式与微分之间的联系, 我们给出理想范数的定义.

定义 8.5. 记号如上. 定义

$$\mathrm{N}_{L/K} : \ J(\mathcal{O}_L) \to J(\mathcal{O}_K)$$

为完全积性函数, 其中对$\mathcal{O}_L$的任意非零素理想$\mathfrak{P}$, 设$\mathfrak{p}=\mathfrak{P}\cap\mathcal{O}_K$, 定义

$$\mathrm{N}_{L/K}(\mathfrak{P})=\mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}.$$

理想的范数与元素的范数有着如下联系.

命题 8.4. 记号如上. 对任意的$x\in L^\times$,

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

证明: 要证明该命题仅需证明对$\mathcal{O}_K$的任意非零素理想$\mathfrak{p}$, 都有

$$\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{N}_{L/K}(x)\mathcal{O}_K\right)=\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{N}_{L/K}(x\mathcal{O}_L)\right).$$

设

$$\mathfrak{p}\mathcal{O}_L=\mathfrak{P}_1^{e(\mathfrak{P}_1|\mathfrak{p})}\mathfrak{P}_2^{e(\mathfrak{P}_2|\mathfrak{p})}\cdots\mathfrak{P}_r^{e(\mathfrak{P}_r|\mathfrak{p})},$$

其中这些$\mathfrak{P}_i$为$\mathcal{O}_L$上两两不同的非零素理想并且$\mathfrak{p}\subseteq\mathfrak{P}_i$. 则由推论7.3,

$$\mathrm{N}_{L/K}(x)=\prod_{i=1}^{r}\mathrm{N}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(x). \tag{8.13}$$

对任意的$1\leq i\leq r$, 设$\pi_i\in L_{\mathfrak{P}_i}$为$L_{\mathfrak{P}_i}$上的素元, 即$\mathrm{ord}_{\mathfrak{P}_i}(\pi_i)=1$. 设$x=\pi_i^{\mathrm{ord}_{\mathfrak{P}_i}(x)}\varepsilon_i$, 其中$\varepsilon_i\in\widehat{\mathcal{O}_{\mathfrak{P}_i}}^\times$. 因为

$$\mathrm{N}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\varepsilon_i)\in\widehat{\mathcal{O}_{\mathfrak{p}}}^\times,$$

由定理7.11与命题7.11容易验证

$$\begin{aligned}
\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{N}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(x)\right)&=\mathrm{ord}_{\mathfrak{P}_i}(x)\cdot\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{N}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\pi_i)\right)\\
&=\mathrm{ord}_{\mathfrak{P}_i}(x)\cdot[L_{\mathfrak{P}_i}:K_{\mathfrak{p}}]\cdot\frac{1}{[L_{\mathfrak{P}_i}:K_{\mathfrak{p}}]}\cdot\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{N}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\pi_i)\right)\\
&=\mathrm{ord}_{\mathfrak{P}_i}(x)\cdot[L_{\mathfrak{P}_i}:K_{\mathfrak{p}}]\cdot\mathrm{ord}_{\mathfrak{p}}(\pi_i)\\
&=\mathrm{ord}_{\mathfrak{P}_i}(x)\cdot\frac{[L_{\mathfrak{P}_i}:K_{\mathfrak{p}}]}{e(\mathfrak{P}_i|\mathfrak{p})}\cdot\mathrm{ord}_{\mathfrak{P}_i}(\pi_i)\\
&=\mathrm{ord}_{\mathfrak{P}_i}(x)\cdot f(\mathfrak{P}_i|\mathfrak{p}).
\end{aligned}$$

由此与(8.13),

$$\begin{aligned}
\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{N}_{L/K}(x)\mathcal{O}_K\right)&=\sum_{i=1}^{r}\mathrm{ord}_{\mathfrak{P}_i}(x)\cdot f(\mathfrak{P}_i|\mathfrak{p})\\
&=\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{N}_{L/K}(x\mathcal{O}_L)\right).
\end{aligned}$$

综上, 我们完成了证明. □

下面的定理揭示了微分与判别式之间的联系.

定理 8.4. 记号如上. 则

$$d_{\mathcal{O}_L/\mathcal{O}_K} = \mathrm{N}_{L/K}\left(\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}\right).$$

证明: 要证明该定理仅需说明对$\mathcal{O}_K$的任意非零素理想$\mathfrak{p}$, 都有

$$d_{\mathcal{O}_L/\mathcal{O}_K}(\mathcal{O}_K)_{\mathfrak{p}} = \mathrm{N}_{L/K}\left(\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}\right)(\mathcal{O}_K)_{\mathfrak{p}}.$$

设$S = \mathcal{O}_K \setminus \{\mathfrak{p}\}, (\mathcal{O}_L)_{\mathfrak{p}} = S^{-1}\mathcal{O}_L$. 则容易验证

$$d_{\mathcal{O}_L/\mathcal{O}_K}(\mathcal{O}_K)_{\mathfrak{p}} = d_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}},$$

并且

$$\mathrm{N}_{L/K}\left(\mathcal{D}_{\mathcal{O}_L/\mathcal{O}_K}\right)(\mathcal{O}_K)_{\mathfrak{p}} = \mathrm{N}_{L/K}\left(\mathcal{D}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}}\right).$$

下面来证明

$$d_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}} = \mathrm{N}_{L/K}\left(\mathcal{D}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}}\right).$$

由定理2.6, $(\mathcal{O}_K)_{\mathfrak{p}}$为主理想整环. 由定理1.2, 主理想整环$(\mathcal{O}_K)_{\mathfrak{p}}$在$L$中的整闭包$(\mathcal{O}_L)_p$关于$(\mathcal{O}_K)_{\mathfrak{p}}$的整基$b_1, b_2, \cdots, b_n$是存在的. 再设元素$b_1', b_2', \cdots, b_n' \in L$为$b_1, b_2, \cdots, b_n$在非退化对称双线性型$\mathrm{Tr}_{L/K}(\cdot)$下的对偶基, 即

$$\mathrm{Tr}_{L/K}(b_i b_j') = \begin{cases} 1 & \text{如果 } i = j, \\ 0 & \text{如果 } i \neq j. \end{cases}$$

则

$$\mathcal{C}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}} = (\mathcal{O}_K)_{\mathfrak{p}} b_1' + (\mathcal{O}_K)_{\mathfrak{p}} b_2' + \cdots + (\mathcal{O}_K)_{\mathfrak{p}} b_n'.$$

并且如果设

$$\mathrm{Hom}_K(L, K^{\mathrm{alg}}) = \{\sigma_i : 1 \leq i \leq n\},$$

则容易验证

$$\begin{pmatrix} \sigma_1(b_1) & \sigma_2(b_1) & \cdots & \sigma_n(b_1) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{pmatrix} \begin{pmatrix} \sigma_1(b_1') & \sigma_1(b_2') & \cdots & \sigma_1(b_n') \\ \sigma_2(b_1') & \sigma_2(b_2') & \cdots & \sigma_2(b_n') \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(b_1') & \sigma_n(b_2') & \cdots & \sigma_n(b_n') \end{pmatrix} = I_n.$$

因此,

$$d(b_1, b_2, \cdots, b_n) \cdot d(b_1', b_2', \cdots, b_n') = 1. \tag{8.14}$$

再利用定理2.6, $(\mathcal{O}_L)_{\mathfrak{p}}$也是主理想整环. 因此, 存在$\beta \in L$使得

$$\begin{aligned}\mathcal{C}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}} &= (\mathcal{O}_K)_{\mathfrak{p}} b_1' + (\mathcal{O}_K)_{\mathfrak{p}} b_2' + \cdots + (\mathcal{O}_K)_{\mathfrak{p}} b_n' \\ &= \beta(\mathcal{O}_L)_{\mathfrak{p}} \\ &= (\mathcal{O}_K)_{\mathfrak{p}}\beta b_1 + (\mathcal{O}_K)_{\mathfrak{p}}\beta b_2 + \cdots + (\mathcal{O}_K)_{\mathfrak{p}}\beta b_n.\end{aligned}$$

由此与(8.14), 容易验证

$$\begin{aligned}d(\beta b_1, \beta b_2, \cdots, \beta b_n)(\mathcal{O}_K)_{\mathfrak{p}} &= \mathrm{N}_{L/K}(\beta)^2 \cdot d(b_1, b_2, \cdots, b_n)(\mathcal{O}_K)_{\mathfrak{p}} \\ &= d(b_1', b_2', \cdots, b_n')(\mathcal{O}_K)_{\mathfrak{p}} \\ &= d(b_1, b_2, \cdots, b_n)^{-1}(\mathcal{O}_K)_{\mathfrak{p}}.\end{aligned}$$

这说明

$$d(b_1, b_2, \cdots, b_n)^2(\mathcal{O}_K)_{\mathfrak{p}} = \mathrm{N}_{L/K}(\beta^{-1})^2(\mathcal{O}_K)_{\mathfrak{p}}.$$

因此, 由命题8.4

$$\begin{aligned}d^2_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}} &= d(b_1, b_2, \cdots, b_n)^2(\mathcal{O}_K)_{\mathfrak{p}} \\ &= \mathrm{N}_{L/K}(\beta^{-1})^2(\mathcal{O}_K)_{\mathfrak{p}} \\ &= \mathrm{N}_{L/K}(\beta^{-1}(\mathcal{O}_L)_{\mathfrak{p}})^2 \\ &= \mathrm{N}_{L/K}\left(\mathcal{D}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}}\right)^2.\end{aligned}$$

这说明

$$d_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}} = \mathrm{N}_{L/K}\left(\mathcal{D}_{(\mathcal{O}_L)_{\mathfrak{p}}/(\mathcal{O}_K)_{\mathfrak{p}}}\right).$$

综上, 我们完成了证明. □

利用该定理与定理8.3, 可以直接得到经典的判别式定理.

定理 8.5. *记号如上. 设$\mathfrak{p}$为$\mathcal{O}_K$的任意非零素理想. 则*

$$\text{存在}\mathcal{O}_L\text{的非零素理想}\mathfrak{P}\text{使得}e(\mathfrak{P}|\mathfrak{p}) \geq 2 \Leftrightarrow \mathrm{ord}_{\mathfrak{p}}\left(d_{\mathcal{O}_L/\mathcal{O}_K}\right) \geq 1.$$