代数数论笔记(1)

Lhzsl

2021 年 1 月 15 日

目录

1 代数整数

1.1 整性

一个**代数数域**K是有理数域Q的有限次扩张，K中的元素叫做**代数数** 。代数数叫做整的，如果它是一个首一整系数多项式$f(x) \in Z[x]$的零点。
由于整性出现在代数的很多方面，下面定义更一般的定义。下面谈到环是总是指带有单位元1的交换环。
定义:$A \subseteq B$是环扩张。$b \in B$叫做在A上整的，如果b是一首一方程

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, n \geq 1$$

的零点，其中$a_i \in A$.如果B的所有元素都在A上是整的，那么称B在A上是整的。
立即有问题产生，那就是：两个在A上是整的元素的和，积是否在A上也是整的？于是有下面的命题。
命题1.1：有限多个元素$b_1, \cdots, b_n \in B$ 在A上都是整的当且仅当环$A[b_1, \cdots, b_n]$看作A模是有限生成的。
命题的证明部分是线性代数的结果：$A = (a_{ij})$ 是任意环上的r阶矩阵，A^*是A的伴随矩阵，则有

$$AA^* = A^*A = det(A)E.$$

E是r阶单位矩阵，对任何向量$x = (x_1, \cdots, x_r)$,

$$Ax = 0 \Rightarrow (detA)x = 0.$$

假设$A - A[b_1, \cdots, b_n]$是有限生成的，$\omega_1, \cdots, \omega_r$是一组生成基，任意$b \in A[b_1, \cdots, b_n]$，有

$$b\omega_i = \sum_{j=1}^{r} a_{ij}\omega_j, i = 1, \cdots, r, a_{ij} \in A.$$

于是有$det(bE - (a_{ij}))\omega_i = 0, i = 1, \cdots, r,$ 由于1能被写成$1 = c_1\omega_1 + \cdots + c_r\omega_r$, 所以有$det(bE - (a_{ij})) = 0$, 这就给出了一个系数在A中的首一多项式，b带入为零。由此易推出
命题1.2:$A \subseteq B \subseteq C$是两个环扩张，如果C在B上是整的，B在A上是整的，那么C在A上是整的。
下面考虑集合

$$\bar{A} = \{b \in B | b \quad integral \quad over \quad A\}$$

由命题1.2知这形成了一个环，把这个环称作A在B中的整闭包。 A在B中叫做整闭的，如果$A = \bar{A}$, 由命题1.2立知$\bar{A}$在B中是整闭的。若A是整环，K是A的分式域，A在K中的闭包叫做A的正规化，此时如果$A = \bar{A}$,A简单的称为整闭的。
一般情况下，A是一个整环，在其分式域中是整闭的， $L|K$是有限次域扩张，B是A在L中的整闭包。则每个元素$\beta \in L$可以写成形式

$$\beta = \frac{b}{a}, b \in B, a \in A,$$

事实上，如果

$$a_n\beta^n+\cdots+a_1\beta+a_0=0,a_i\in A,a_n\neq 0,$$

那么由方程

$$(a_n\beta)^n+\cdots+a_1^{'}(a_n\beta)+a_0^{'}=0,a_i^{'}\in A$$

知 $b=a_n\beta$在A上是整的.
进一步分析，设$\beta\in L$在A上是整的，则其极小多项式$P(x)\in A[x]$. 事实上，设β 是首一多项式$g(x)\in A[x]$的零点，则在$K[x]$中$p(x)$整除$g(x)$，故$p(x)$的所有零点$\beta_1,\cdots,\beta_n$ 都在A上整闭，因此$p(x)$的系数在A上整闭，再由$p(x)\in K[x]$知$p(x)\in A[x]$.由此推出：设A是整闭整环，K是其分式域，$f(x)\in A[x]$为首一多项式，则$f(x)$在$K[x]$中的首一因子都在$A[x]$中。
下面引入迹和范数
定义：$x\in L|K$的迹和范数定义为域K上线性空间L中线性变换

$$T_x:L\to L,\quad T_x(\alpha)=x\alpha,$$

的迹和行列式，即

$$Tr_{L|K}(x)=Tr(T_x),\quad N_{L|K}(x)=det(T_x).$$

设T_x的特征多项式为

$$f_x(t)=det(t*id-T_x)=t^n-a_1t^{n-1}+\cdots+(-1)^na_n\in K[t],n=[L:K].$$

可以看出$a_1=Tr_{L|K}(x)\in K,\quad a_n=N_{L|K}(x)\in K.$ 对任意$x,y\in L,$

$$Tr_{L|K}(x+y)=Tr(T_{x+y})=Tr(T_x+T_y)=Tr(T_x)+Tr(T_y)=Tr_{L|K}(x)+Tr_{L|K}(y)$$

$$N_{L|K}(xy)=det(T_{xy})=det(T_x*T_y)=det(T_x)det(T_y)=N_{L|K}(x)N_{L|K}(y)$$

于是有两个同态

$$Tr_{L|K}:L\to K,\quad N_{L|K}:L^*\to K^*$$

在$L|K$是可分扩张时，有下面命题
命题1.3:若$L|K$是可分扩张，$\sigma:L\to\bar{K}$遍历所有不同的K-嵌入，则有
$(i)\quad f_x(t)=\prod_\sigma(t-\sigma x),$
$(ii)\quad Tr_{L|k}(x)=\sum_\sigma\sigma x,$
$(iii)\quad N_{L|K}(x)=\prod_\sigma\sigma x.$
证明：设x在域K上的极小多项式为

$$p_x(t)=t^m+c_1t^{m-1}+\cdots+c_m,\quad m=[K(x):K],$$

于是$1,x,\cdots,x^{m-1}$是域$K(x)|K$的一组基，若$\alpha_1,\cdots,\alpha_d$是域$L|K(x)$的一组基，则

$$\alpha_1,\alpha_1x,\cdots,\alpha_1x^{m-1};\cdots;\alpha_d,\alpha_dx,\cdots,\alpha_dx^{m-1}$$

是域$L|K$的一组基。容易计算T_x在这组基下的矩阵是分块对角矩阵，每个矩阵块特征多项式是$p_x(t)$，从而$f_x(t) = p_x(t)^d$
所有L的K-嵌入的集合$Hom_K(L, \bar{K})$被等价关系

$$\sigma \sim \tau \Longleftrightarrow \sigma x = \tau x$$

划分到m个等价类，每个等价类有d个元素，若$\sigma_1, \cdots, \sigma_m$是一代表系，则

$$p_x(t) = \prod_{i=1}^{m}(t - \sigma_i x),$$

$f_x(t) = \prod_{i=1}^{m}(t - \sigma_i x)^d = \prod_{i=1}^{m}\prod_{\sigma \sim \sigma_i}(t - \sigma x) = \prod_{\sigma}(t - \sigma x)$.同样的可得到(ii),(iii).
可分扩张$L|K$的一组基$\alpha_1, \cdots, \alpha_n$的**判别式**定义为

$$d(\alpha_1, \cdots, \alpha_n) = det((\sigma_k \alpha_j))^2$$

$\sigma_i, i = 1. \cdots, n$遍历K-嵌入$L \to \bar{K}$.
下面继续讨论域，A是在其分式域中整闭的整环，$L|K$是有限可分域扩张，B是A在K中的闭包，若$x \in B$，则存在首一多项式$f(t) \in A[t]$,使得$f(x) = 0$,任意σ为L到$\bar{K}$的K-嵌入，从而$\sigma f(x) = f(\sigma x) = 0$,即$\sigma x$在A上是整的，由A是整闭的易得到$A = B \bigcap K$,由命题1.3知$Tr_{L|K}(x), N_{L|K}(x) \in K$,又由上分析知$x \in B$时，$\sigma x \in B$，从而

$$Tr_{L|K}(x), N_{L|K}(x) \in A$$

引理1.1 $\alpha_1, \cdots, \alpha_n$是域$L|k$的一组基，且$\alpha_i \in B$(由上面分析这是可以做到的)，$d = d(\alpha_1, \cdots, \alpha_n)$,则有

$$dB \subseteq A\alpha_1 + \cdots + A\alpha_n$$

证明：若$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n \in B, a_j \in k$, 那么$a_j$是线性方程组

$$Tr_{L|K}(\alpha_i \alpha) = \sum_j Tr_{L|K}(\alpha_i \alpha_j) a_j$$

的解。由于$Tr_{L|K}(\alpha_i \alpha) \in A, Tr_{L|K}(\alpha_i \alpha_j) \in A$,因此易知$da_j \in A$,从而

$$d\alpha \in A\alpha_1 + \cdots + A\alpha_n.$$

一组元素$\omega_1, \cdots, \omega_n \in B$叫做B在A上的一组**整基**，如果$\forall b \in B$，b 能唯一写成 $\omega_1, \cdots, \omega_n$的A线性组合(即$b = a_1\omega_1 + \cdots + a_n\omega_n, a_i \in A$)。立知这一组元素是$L|K$的一组基，故元素个数总等于域扩张$[L : K]$的度数，整基的存在说明B是一个自由$A-$模，秩为$n = [L : K]$，一般情况下，整基并不存在，然而，若A是主理想整环，则有下面的命题。
命题1.4:若$L|K$是可分扩张，A是主理想整环，那么每个L的有限生成B子模$M \neq 0$(指M，L作为B的模，$B-$模M是$B-$模L的子模，$M \subseteq L$)是秩为$[L : K]$的自由$A-$模，特别地，B在A上存在整基。
证明：设$M \neq 0$是L的有限生成B子模，$\alpha_1, \cdots, \alpha_n$ 是$L|K$的一组基，乘以A中的某一元素，可使

其全部属于B,故不妨设$\alpha_i \in B$,由引理1.1知$dB \subseteq A\alpha_1 + \cdots + A\alpha_n$.故 $rank(B) \leq [L:K]$,由于$A-$模B的一组生成基也是$K-$模L的一组生成基，于是$rank(B) = [L:K]$，设$\mu_1, \cdots, \mu_r \in M$是$B-$模M的一组生成系，存在$a \in A, a \neq 0$,使得$a\mu_i \in B, i = 1, \cdots, r$,于是 $aM \subseteq B$.并且

$$adM \subseteq dB \subseteq A\alpha_1 + \cdots + \alpha_n = M_0.$$

根据主理想整环上有限生成模的主要定理知M_0是自由$A-$模，从而adM, M 也是自由$A-$模。进而

$$[L:K] = rank(B) \leq rank(M) = rank(adM) \leq rank(M_0) = [L:K],$$

因此，$rank(M) = [L:K]$.

考虑$Z \subseteq Q$在代数数域K中的整闭包$\mathcal{O}_K \subseteq K$，由命题1.4知K的每个有限生成$\mathcal{O}_K-$子模$\mathbf{a}$有$Z-$基$\alpha_1, \cdots$

$$\mathbf{a} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n.$$

基的判别式

$$d(\alpha_1, \cdots, \alpha_n) = det((\sigma_i\alpha_j))^2$$

与$\mathbb{Z}-$基的选取无关：如果$\alpha_1^{'}, \cdots, \alpha_n^{'}$是另一组基，转换矩阵为$T = (a_{ij}), \alpha_i^{'} = \sum_j a_{ij}\alpha_j$, 其系数为整数，逆矩阵的系数也是整数，因此行列式为1或-1，于是

$$d(\alpha_1^{'}, \cdots, \alpha_n^{'}) = det(T)^2 d(\alpha_1, \cdots, \alpha_n) = d(\alpha_1, \cdots, \alpha_n).$$

故记

$$d(\mathbf{a}) = d(\alpha_1, \cdots, \alpha_n)$$

特别地 $\mathcal{O}_K$的整基为$\omega_1, \cdots, \omega_n$，我们得到代数数域K的判别式

$$d_K = d(\mathcal{O}_K) = d(\omega_1, \cdots, \omega_n).$$

1.2 理想

定理2.1： 环$\mathcal{O}_K$是诺特环(即每个理想都是有限生成的)，整闭且其中每个非零素理想都是极大理想。

证明：(1)由命题1.4,$\mathcal{O}_K$的每个非零理想都是有限生成$Z-$模，因此更是有限生成$\mathcal{O}_K-$模。

(2)设P是$\mathcal{O}_K$的非零素理想。取$0 \neq \alpha \in P$,令 $m = N_{K|Q}(\alpha) \in Z - \{0\}$.由上分析知 $m/\alpha \in \mathcal{O}_K$,于是$m = \alpha * m/\alpha \in P$, 即$(m) \in P$.设$\omega_1, \cdots, \omega_n$是$\mathcal{O}_K$的一组整基，即$\mathcal{O}_K = Z\omega_1 \oplus \cdots \oplus Z\omega_n, n = [K:Q]$.则

$$\mathcal{O}_K/m\mathcal{O}_K = (Z\omega_1 \oplus \cdots \oplus Z\omega_n)/Zm\omega_1 \oplus \cdots \oplus Zm\omega_n \cong Z/mZ \oplus \cdots \oplus Z/mZ$$

由环的同构定理知道$\mathcal{O}_K/P \cong (\mathcal{O}_K/m\mathcal{O}_K)/(P/m\mathcal{O}_K)$, 从而$|\mathcal{O}_K/P| \leq |\mathcal{O}_K/m\mathcal{O}_K| = m^n$. 即$\mathcal{O}_K/P$是有限环，由于$P$是素理想，从而$\mathcal{O}_K/P$是有限整环，由熟知的定理(有限整环即是域)知$\mathcal{O}_K/P$是域，从而$P$是极大理想。

(3)由于$\mathcal{O}_K$是Z在域K中的整闭包，因此$\mathcal{O}_K$在K中整闭，更在其分式域中整闭。

定义2.2如果一个整环是诺特的，在其分式域中整闭，且每个素理想都是极大理想，那么称这个环叫做戴德金(Dedekind)整环.
于是下面考虑$\mathcal{O}_K$的一般形式，即戴德金环$\mathcal{O}$,有下主要定理
定理2.3:$\mathcal{O}$的除了$(0),(1)$每一个理想P都存在(不记次序)唯一的素理想分解

$$P = P_1 \cdots P_r$$

为证明此定理需要下面的引理
引理2.4:对$\mathcal{O}$的每个非零理想P,都存在非零素理想$P_1, P_2, \cdots, P_r$,使得

$$P_1 P_2 \cdots P_r \subseteq P$$

证明略(一般代数数论书都会有证明)。
引理2.5:P是$\mathcal{O}$的素理想，定义

$$P^{-1} = \{x \in K | xP \subseteq \mathcal{O}\}.$$

则对于每个非零素理想Q有$QP^{-1} := \{\sum_i a_i x_i | a_i \in Q, x_i \in P^{-1}\} \neq Q$
证明：设$a \in P, a \neq 0$,且$P_1 P_2 \cdots P_r \subseteq (a) \subseteq P$,$r$是使其成立的最小正整数，由于$P$是素理想，易推出必有必有$P_i$不妨设为$P_1 \subseteq P$, 戴德金环中素理想即为极大理想故$P_1 = P$,由于$P_2 \cdots P_n \not\subseteq (a)$,故存在$b \in P_2 \cdots P_n$使得$b \notin a\mathcal{O}$,i.e,$a^{-1}b \notin \mathcal{O}$,另一方面，有$bP \subseteq (a), i.e, a^{-1}bP \subseteq \mathcal{O}$,于是$a^{-1}b \in P^{-1}$, 综上，$P^{-1} \neq \mathcal{O}$
现在设$Q \neq 0$是 $\mathcal{O}$的一个非零理想，$\alpha_1, \cdots, \alpha_n$是其一组是生成系，假设$QP^{-1} = Q$,则对于每个$x \in P^{-1}$,

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

记A为矩阵$(x\delta_{ij} - a_{ij})$,于是$A(\alpha_1, \cdots, \alpha_n)^t = 0$,记$d = det(A)$,则$d\alpha_1 = \cdots = d\alpha_n = 0$,因此$d = 0$,得到$x$在$\mathcal{O}$上是整的，于是$x \in \mathcal{O}$ 由于$\mathcal{O} \subseteq P^{-1}$, 故推出$P^{-1} = \mathcal{O}$,矛盾!
定理2.3的证明:(1)素理想分解的存在性。令$\mathcal{M}$是所有除$(0),(1)$外不存在素理想分解的理想组成的集合。如果$\mathcal{M}$非空，由于$\mathcal{O}$是诺特的，每个理想升链都是有限的，$\mathcal{O}$中的集合包含关系诱导$\mathcal{M}$中的一个序，使其成为偏序集。故$\mathcal{M}$中存在最大的元素，记为Q，它包含在一个极大理想P中，由于$\mathcal{O} \subseteq P^{-1}$

$$Q \subseteq QP^{-1} \subseteq PP^{-1} \subseteq \mathcal{O}.$$

再由引理2.5，有$Q \subsetneq QP^{-1}, P \subsetneq PP^{-1} \subseteq \mathcal{O}$.但$P$是极大理想，从而得到$PP^{1} = \mathcal{O}$,由于$Q$是$\mathcal{M}$中的最大元,并且$Q \neq P, i.e, QP^{-1} \neq \mathcal{O}$.得到$QP^{-1}$有素理想分解$QP^{-1} = P_1 P_2 \cdots P_r$,于是$Q = QP^{-1}P = P_1 P_2 \cdots P_r P$.矛盾!
(2)唯一性的证明略(类似于整数的素因子分解)。
下面引入分式理想，令$\mathcal{O}$是戴德金整环，K为其分式域。
定义2.6：K的一个**分式理想**是$\mathcal{O}-$模K的有限生成非零子模
例如，每一元素$a \in K^*$定义一个分式“主理想”$(a) = a\mathcal{O}$, 显然地，由于$\mathcal{O}$是诺特环，一个$\mathcal{O}-$模K的子模$\mathcal{O}-$模Q是分式理想当且仅当存在$c \in \mathcal{O}, c \neq 0$,使得$cQ \subseteq \mathcal{O}$是环$\mathcal{O}$的一个理想(有些书就用这

做为分式理想的定义),此后我们把$\mathcal{O}$中的理想叫做K中的整理想

命题2.7：分式理想形成Abel群，记为J_K，单位元是$(1)=\mathcal{O}$,其中元素Q的逆元为

$$Q^{-1}=\{x\in K|xQ\subseteq\mathcal{O}\}$$

证明：元素的结合性，交换性和$Q(1)=Q$都是明显的。对于每个素理想P,$P\subsetneq PP^{-1}\subseteq\mathcal{O}$,在戴德金环中素理想都是极大理想，故$PP^{-1}=\mathcal{O}$。再设$Q=P_1\cdots P_r$是整理想，则 $B=P_1^{-1}\cdots P_r^{-1}$是其逆元：$BQ=\mathcal{O}$暗示$B\subseteq Q^{-1}$.反之，如果$xQ\subseteq\mathcal{O}$,则$xQB\subseteq B$,由于$BQ=\mathcal{O}$ 得到$x\in B$，故$B=Q^{-1}$.最后，若Q是任意的分式理想，存在$c\in\mathcal{O},c\neq 0$,使得$cQ\subseteq\mathcal{O}$,于是$(cQ)^{-1}=c^{-1}Q^{-1}$是cQ的逆元，$QQ^{-1}=\mathcal{O}$

查阅维基百科：分式理想在代数数论和戴德金环论中有不同定义，代数数论中的定义为：

数域K中的非空子集合I叫做K中的分式理想，如果存在$\mu\in\mathcal{O}_K$使得μI 是$\mathcal{O}_K$中的理想。用J_K表示所有K的分式理想组成的集合，可以证明J_K组成群。令P_K是K的分式主理想组成的群，后文将证明它们的商群$CL_K=J_K/P_K$为有限群。

1.3 理想的分解

就像整数理论中要研究整数的素数分解一样，代数数论中要研究理想的素理想分解。设$L|K$是数域的扩张，Q是$\mathcal{O}_K$的一个(整)理想，问题$\mathcal{O}_L$中的理想$Q\mathcal{O}_L$如何分解成$\mathcal{O}_L$中素理想的乘积?由于每个理想Q均是$\mathcal{O}_K$中一些素理想的乘积，因此我们只要对$\mathcal{O}_K$中的每个素理想P弄清楚$P\mathcal{O}_L$在$\mathcal{O}_L$中的素理想分解式就可以。这里事先说明,若L中的素理想$\mathcal{B}$出现在$P\mathcal{O}_L$的素理想分解式中,即$\mathcal{B}|P\mathcal{O}_L$,那么简记为$\mathcal{B}|P$。下面便是一些命题的证明。

引理3.1:设$L|K$是数域的扩张，$\mathcal{B}$为$\mathcal{O}_L$的素理想，则:

(1)$\mathcal{B}\cap\mathcal{O}_K$为$\mathcal{O}_K$的素理想，并且 $\mathcal{B}\cap\mathcal{O}_K=P\Leftrightarrow\mathcal{B}|P$

(2)若$\mathcal{B}\cap\mathcal{O}_K=P$,则$\mathcal{O}_K/P$和$\mathcal{O}_L/\mathcal{B}$均是有限域，并且前者可看成是后者的子域。

证明:(1)易验证$\mathcal{B}\cap\mathcal{O}_K$是$\mathcal{O}_K$的理想，从而只需验证为素理想。$\forall a,b\in\mathcal{O}_K,ab\in\mathcal{B}\cap\mathcal{O}_K$,由于$\mathcal{B}$是$\mathcal{O}_L$中的素理想，从而$a\in\mathcal{B}$或$b\in\mathcal{B}$,即有$a\in\mathcal{B}\cap\mathcal{O}_K$或$b\in\mathcal{B}\cap\mathcal{O}_K$.

若$\mathcal{B}\cap\mathcal{O}_K=P$,则$P\subseteq\mathcal{B}$,从而 $P\mathcal{O}_L\subseteq\mathcal{B}$,于是$\mathcal{B}|P\mathcal{O}_L$,即 $P\mathcal{B}|P$.反之，若P为$\mathcal{O}_K$中的素理想，且$\mathcal{B}|P\mathcal{O}_L$ 于是$P\subseteq P\mathcal{O}_L\subseteq\mathcal{B}$,从而$P=P\cap\mathcal{O}_K\subseteq\mathcal{B}\cap\mathcal{O}_K$,但$\mathcal{O}_K\cap\mathcal{B}$均是$\mathcal{O}_K$中的素理想，从而是极大理想，所以有$\mathcal{B}\cap\mathcal{O}_K=P$

(2)作映射

$$\phi:\mathcal{O}_K\to\mathcal{O}_L/\mathcal{B},\phi(x)=x+\mathcal{B}(x\in\mathcal{O}_K)$$

易知是环同态。$Ker\phi=\mathcal{O}_K\cap\mathcal{B}=P$,从而由同态$\phi$可将环$\mathcal{O}_K/P$看成是$\mathcal{O}_L/\mathcal{B}$ 的子环，由于$\mathcal{O}_K/P$和$\mathcal{O}_L/\mathcal{B}$是有限环(元素个数分别是$N_K(P),N_L(\mathcal{B})$),由于$P$和$\mathcal{B}$分别是$\mathcal{K}$和$\mathcal{L}$的极大理想，从而于$\mathcal{O}_K/P$和$\mathcal{O}_L/\mathcal{B}$是有限域，前者是后者的子域。

1.4 戴德金环的扩张

命题4.1: 若o是戴德金整环，分式域为K, $L|K$是有限域扩张，$\mathcal{O}$是o在L上的整闭包，那么$\mathcal{O}$也是戴德金整环.

证明:(1)由于是o的整闭包，$\mathcal{O}$自然是整闭的。

(2)设$\mathcal{B}$是$\mathcal{O}$的非零素理想，那么$P=\mathcal{O}\cap\mathcal{B}$是o的非零素理想，可以通过构造映射将整环$\mathcal{O}/\mathcal{B}$看作域$o/P$的扩张。因此这一整环也是域，若不然整环将有一非零素理想，其与域o/P的交集是的非零素理想。

(3)若$L|K$是可分扩张，证明是容易的.令$\alpha_1,\cdots,\alpha_n$是$L|K$的包含在$\mathcal{O}$的一组基，判别式为$d=d(\alpha_1,\cdots,$ 么由前面命题知$d\neq 0$, $\mathcal{O}$包含在一有限生成$o-$模$o\alpha_1/d+\cdots+o\alpha_n/d$中。$\mathcal{O}$的每个理想也都包含在这个有限生成$o-$模中，于是$\mathcal{O}$也是有限生成$o-$模，更是有限生成$\mathcal{O}-$模，这就展示了$\mathcal{O}$是诺特的。一般情况后文将给出证明。

o中一个素理想在环$\mathcal{O}$中有唯一的素理想分解

$$P\mathcal{O}=\mathcal{B}_1^{e_1}\cdots\mathcal{B}_r^{e_r}$$

我们经常简记$P\mathcal{O}$为P.若$\mathcal{B}$是$\mathcal{O}$ 的素理想$P=\mathcal{B}\cap o$,由上面可知$\mathcal{B}|P$,我们称$\mathcal{B}$是P的一个素因子，指数e_i叫做分歧指数，域扩张的度数$f_i=[\mathcal{O}/\mathcal{B}:o/P]$叫做$\mathcal{B}$在$P$上的剩余类域次数。

命题4.2：若$L|K$是可分扩张，那么有等式

$$\sum_{i=1}^{r}e_if_i=n$$

证明:由中国剩余定理知,

$$\mathcal{O}/P\mathcal{O}\cong\oplus_{i=1}^{r}\mathcal{O}/\mathcal{B}_i^{e_i}.$$

$\mathcal{O}/P\mathcal{O}$和$\mathcal{O}/\mathcal{B}_i^{e_i}$是域$o/P$上的向量空间(若无特殊说明，下文总是指这两个线性空间在域o/P上的)，若证明

$$dim_{o/P}(\mathcal{O}/P\mathcal{O})=n, dim_{o/P}(\mathcal{O}/\mathcal{B}_i^{e_i})=e_if_i$$

即证明了命题。

设$\bar{\omega}_1,\cdots,\bar{\omega}_m$是$\mathcal{O}/P\mathcal{O}$的一组基，$\omega_1,\cdots,\omega_m\in\mathcal{O}$是其代表元(由命题4.1的证明过程知这一向量空间是有限维的)。只需证明$\omega_1,\cdots,\omega_m$是$L|K$的一组基，假设$\omega_1,\cdots,\omega_m$在域K上线性相关，从而在o上也线性相关。从而存在非零元素$a_1,\cdots,a_m\in o$使得

$$a_1\omega_1+\cdots+a_m\omega_m=0.$$

考虑理想$A=(a_1,\cdots,a_m)$,取$a\in A^{-1}$,使得$a\notin A^{-1}P$,从而aA不包含在P中，于是$aa_1,\cdots,aa_m$属于o，但不全属于P,同余式

$$aa_1\omega_1+\cdots+aa_m\omega_m\equiv 0(modp)$$

说明$\bar{\omega}_1,\cdots,\bar{\omega}_m$在域$o/P$上是线性相关的，矛盾！因此$\omega_1,\cdots,\omega_m$在域K上线性无关。

为证明ω_i是$L|K$的一组基，考虑$o-$模$M=o\omega_1+\cdots+o\omega_m, N+\mathcal{O}/M$.由于$\mathcal{O}=M+P\mathcal{O}$,我们

有$PN=N$.由于$L|K$是可分扩张，由命题4.1证明过程知$\mathcal{O}$是有限生成$o-$模，从而N也是。设$\alpha_1,\cdots,\alpha_s$是一个生成系，那么

$$\alpha_i=\sum_j a_{ij}\alpha_j, a_{ij}\in P.$$

令$A=(a_{ij})-I$,I是单位矩阵，B是A的伴随矩阵。从而$A(\alpha_1,\cdots,\alpha_s)^t=0, BA=dI, d=det(A)$,进而

$$0=BA(\alpha_1,\cdots,\alpha_s)^t=(d\alpha_1,\cdots,d\alpha_s)^t,$$

因此$dN=0$,即$d\mathcal{O}\subseteq M=o\omega_1+\cdots+o\omega_m$. 由于$a_{ij}\in P$,故$d=det((a_{ij})-I)\equiv(-1)^s modp$,即$d\neq 0$,从而$L=dL\subseteq dK\mathcal{O}\subseteq K\omega_1+\cdots+K\omega_m$.综上$\omega_1,\cdots,\omega_m$是$L|K$的一组基。
下面证明第二个等式。考虑o/P上线性空间的递降链

$$\mathcal{O}/\mathcal{B}_i^{e_i}\supseteq\mathcal{B}_i/\mathcal{B}_i^{e_i}\supseteq\cdots\supseteq\mathcal{B}_i^{e_i-1}/\mathcal{B}_i^{e_i}\supseteq(0).$$

下面我们证明$\mathcal{B}_i^{\nu}/\mathcal{B}_i^{\nu+1}$同构于$\mathcal{O}/\mathcal{B}_i$,若$\alpha\in\mathcal{B}_i^{\nu}/\mathcal{B}_i^{\nu+1}$,映射

$$\mathcal{O}\to\mathcal{B}_i^{\nu}/\mathcal{B}_i^{\nu+1}, a\mapsto a\alpha,$$

的核为$\mathcal{B}_i$,由于$\mathcal{B}_i^{\nu}$是$\mathcal{B}_i^{\nu+1}$和$(\alpha)=\alpha\mathcal{O}$的最大公因数,因此$\mathcal{B}_i^{\nu}=\alpha\mathcal{O}+\mathcal{B}_i^{\nu+1}$,从而这是满射，因为$f_i=[\mathcal{O}/\mathcal{B}:o/P]$,我们得到$dim_{o/P}(\mathcal{B}_i^{\nu}/\mathcal{B}_i^{\nu+1})=f_i$,进而

$$dim_{o/P}(\mathcal{O}/\mathcal{B}_i^{e^i})=\sum_{\nu=0}^{e_i-1}dim_{o/P}(\mathcal{B}_i^{\nu}/\mathcal{B}_i^{\nu+1})=e_if_i.$$

设$L|K$是可分扩张，$\theta\in\mathcal{O}$,其极小多项式$p(X)\in o[X]$,且有 $L=K(\theta)$,定义环$o[\theta]$的导子(conductor)为$\mathfrak{F}=\{\alpha\in\mathcal{O}|\alpha\mathcal{O}\subseteq o[\theta]\}$.
命题4.3:P是和$o[\theta]$的导子$\mathfrak{F}$互素,即是$\mathfrak{p}\mathcal{O}+\mathfrak{F}=\mathcal{O}$的o的素理想, 令

$$\bar{p}(X)=\bar{p}_1(X)^{e_1}\cdots\bar{p}_r(X)^{e_r}.$$

是多项式$\bar{p}(X)\equiv p(X)(modP)$在剩余类域$o/P$中的不可约多项式分解，$p_i(X)\in o[X]$是首一的。那么

$$\mathcal{B}_i=P\mathcal{O}+p_i(\theta)\mathcal{O}, i=1,\cdots,r$$

是$\mathcal{O}$的不同的素理想，$\mathcal{B}$的剩余类次数f_i是$\bar{p}_i(X)$的次数，并且

$$P=\mathcal{B}_1^{e_1}\cdots\mathcal{B}_r^{e_r.}$$

证明见Neukirch.Algebraic number theory.p48.
命题4.4：如果$L|K$是可分扩张，那么K中仅有有限个在L上分歧的素理想.
证明：有限可分扩张是单扩张，于是有$\theta\in\mathcal{O}$使得$L=K(\theta)$.设$p(X)\in o[X]$是其在K上的最小多项式。$p(X)$的判别式为

$$d=d(1,\theta,\cdots,\theta^{n-1})=\prod_{i<j}(\theta_i-\theta_j)^2\in o$$

$\prod_{i<j}(\theta_i-\theta_j)^2\in o$是由于$\prod_{i<j}(\theta_i-\theta_j)^2$是关于$\theta_i, i=1,\cdots,n-1$的对称多项式，从而能表示成其初等多项式的关系式，而其初等多项式的值是$p(X)$的系数。下面断言K中每个与d和$o[X]$的导子$\mathfrak{F}$都互素(即$d\notin\mathfrak{p}$且$\mathfrak{p}\mathcal{O}+\mathfrak{F}=\mathcal{O}$)的素理想 $\mathfrak{p}$是不分歧的。事实上，在上述假设下，由上述命题4.3，分歧指数e_i等于1只需在 $o/\mathfrak{p}$中$\bar{p}(X)=p(X)mod\mathfrak{p}$的分解式中$e_i$都是1，即$\bar{p}(X)$无重根，此时由于$\bar{p}(X)$的判别式$\bar{d}=d(mod\mathfrak{p})$非零，于是剩余类域扩张$\mathcal{O}/\mathfrak{P}_i|o/\mathfrak{p}$由元素$\bar{\theta}=\theta(mod\mathfrak{P}_i)$生成，因此是可分的，从而$\mathfrak{p}$不分歧。下面需要证明K中不与d互素(即素理想P满足$d\in P$)或不与$o[X]$的导子$\mathfrak{F}$互素(即素理想$\mathfrak{p}$满足$P\mathcal{O}+\mathfrak{F}\neq\mathcal{O}$)的素理想均为有限个。
由于o是Dedekind整环do有唯一的素理想分解

$$do=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_s^{e_s}.$$

于是只有有限个素理想$\mathfrak{p}_1,\cdots,\mathfrak{p}_s$包含d。
因为$\mathcal{O}$是Dedekind整环,$\mathfrak{F}$有唯一的素理想分解

$$\mathfrak{F}=\mathfrak{P}_1^{a_1}\cdots\mathfrak{P}_t^{a_t}.$$

若$\mathfrak{p}$是o中素理想且$\mathfrak{p}\mathcal{O}+\mathfrak{F}\neq\mathcal{O}$,那么$\mathcal{O}$中存在素理想$\mathfrak{P}$使得$\mathfrak{p}\mathcal{O}+\mathfrak{F}\subseteq\mathfrak{P}$. Dedeking整环中包含等价于整除，于是$\mathfrak{P}|\mathfrak{p}\mathcal{O},\mathfrak{P}|\mathfrak{F}$.j进而$\mathfrak{p}=\mathfrak{P}\cap A$由理想分解的唯一性， $\mathfrak{P}=\mathfrak{P}_i$对某一i成立，综上便有$o$中素理想满足$\mathfrak{p}\mathcal{O}+\mathfrak{F}\neq\mathcal{O}$当且仅当$\mathfrak{p}=\mathfrak{P}_i\cap A$.对于某一i成立，$\mathfrak{P}_i$是导子$\mathfrak{F}$分解式中的素理想。

命题4.5:设$L|K$是数域的扩张，$L=K(\alpha),\alpha\in\mathcal{O}_L,n=[L:K].f(x)=x^n+c_1x^{n-1}+\cdots+c_n\in\mathcal{O}_K[x]$是整数$\alpha$在K上的极小多项式，则
(1)$\mathcal{O}_K[\alpha]$是$\mathcal{O}_L$的子环，并且加法商群$\mathcal{O}_L/\mathcal{O}_K[\alpha]$是有限群；
证明:$\mathcal{O}_K[\alpha]$显然是$\mathcal{O}_L$的子环，由于加法群$\mathcal{O}_L$和$\mathcal{O}_K[\alpha]$均是秩为$[L:K]$的自由Abel群，由Abel群基本定理可以得出加法商群$\mathcal{O}_L/\mathcal{O}_K[\alpha]$是有限群。
(2)设p是素数，P是$\mathcal{O}_K$的素理想，$P|p$,则$\mathcal{O}_K/P$是特征为p的有限域；
证明:由于$P\cap Z=p$,并且$\mathcal{O}_K/P$是p元域Z/pZ的扩域，从而$\mathcal{O}_K/P$是特征为p的有限域.
(3)如果p不整除群$\mathcal{O}_L/\mathcal{O}_K[\alpha]$的阶，令$f(x)$在主理想整环$\mathcal{O}_K/P[x]$中分解为

$$f(x)=p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_g(x)^{e_g}(modp)$$

其中$p_1(x),\cdots,p_g(x)$均为$\mathcal{O}_K[x]$中的首一多项式，并且看作是$\mathcal{O}_K/P[x]$中的多项式时为两两不同的不可约多项式，则P在$\mathcal{O}_L$中的分解式为

$$P\mathcal{O}_L=\mathcal{B}_1^{e_1}\cdots\mathcal{B}_g^{e_g}$$

其中

$$\mathcal{B}_i=(P,p_i(\alpha)),e_i=e(\mathcal{B}_i/P),f(\mathcal{B}_i/P)=degp_i(x)(1\leq i\leq g)$$

证明:令$f_i=degp_i(x)(1\leq i\leq g)$.我们证明下面事实；
对于每个i，或者$\mathcal{B}_i=\mathcal{O}_L$,或者$\mathcal{O}_L/\mathcal{B}_i$是$|\mathcal{O}_K/p|^{f_i}$元域。这是因为：$p_i(x)$在$\mathcal{O}_K/P[x]$中不可约，从而$F_i=\mathcal{O}_K/P[x]/(p_i(x))$为域，自然同态$\phi:\mathcal{O}_K[x]\rightarrow\mathcal{O}_K/P[x]/(p_i(x))$是满同态，并且$Ker\phi=(P,p_i(x))$,从而有同构

$$\mathcal{O}_K/(P,p_i(x))\simeq\mathcal{O}_K/P[x]/(p_i(x))=F_i$$

从而左边也是域。因此$(P,p_i(x))$是$\mathcal{O}_K[x]$的极大理想，再做映射

$$\pi:\mathcal{O}_K[x]\to\mathcal{O}_L/\mathcal{B}_i,\pi(f(x))=f(\alpha)+\mathcal{B}_i$$

这是环同态，由于$\mathcal{B}_i=(P,p_i(\alpha))$,从而$(P,p_i(x))\subseteq Ker\pi$,但是$(P,p_i(x))$是$\mathcal{O}_K[x]$的极大理想。因此$Ker\pi=(P,p_i(x))$或者$\mathcal{O}_K[x.]$
我们再证π是满同态，这即证明$\mathcal{O}_K[\alpha]+\mathcal{B}_i=\mathcal{O}_L$即可，由于$p\in P\subseteq\mathcal{B}_i$,从而$p\mathcal{O}_L\subseteq\mathcal{B}_i$,于是只要证明$\mathcal{O}_K[\alpha]+p\mathcal{O}_L=\mathcal{O}_L$即可，这是因为$p\nmid|\mathcal{O}_L/\mathcal{O}_K[\alpha]|$,而$|\mathcal{O}_L/P\mathcal{O}_L|=p^{[L:Q]}$,从而$|\mathcal{O}_L/\mathcal{O}_K[\alpha]+p\mathcal{L}|$可除尽$(|\mathcal{O}_L/\mathcal{O}_K[\alpha]|,|\mathcal{O}_L/P\mathcal{O}_L|)=1$,因此$|\mathcal{O}_L/\mathcal{O}_K[\alpha]+p\mathcal{L}|=1$,即$\mathcal{O}_K[\alpha]+p\mathcal{O}_L=\mathcal{O}_L$，从而$\pi$为满同态，于是$\mathcal{O}_L/\mathcal{B}_i$或者同构于$\mathcal{O}_K[x]/(P,p_i(x))\cong F_i$,从而$\mathcal{O}_L/\mathcal{B}_i$是$|\mathcal{O}_K/P|^{f_i}$元域；或者同构于$\mathcal{O}_K[x]/\mathcal{O}_K[x]$,即$\mathcal{B}_i=\mathcal{O}_L$.
当$i\neq j$时,$(\mathcal{B}_i,\mathcal{B}_j)=1$.这是因为$p_i(x),p_j(x)$是$\mathcal{O}_K/P[x]$中的不同的不可约多项式，而$\mathcal{O}_K/P[x]$是主理想整环，从而有

$$h(x),k(x)\in\mathcal{O}_K/P[x]$$

使得$hp_i+kp_j\equiv1(modP)$,带入$x=\alpha$即知

$$p_i(\alpha)h(\alpha)+p_j(\alpha)k(\alpha)\equiv1(modP\mathcal{O}_L)$$

于是$1\in(P,p_i(\alpha),p_j(\alpha))=(\mathcal{B}_i,\mathcal{B}_j)$
$P\mathcal{O}_L|\mathcal{B}_1^{e_1}\cdots\mathcal{B}_g^{e_g}$.这是因为；令$\gamma_i=p_i(\alpha)$, 则$\mathcal{B}_i=(P,\gamma_i)$,由(2)知当$i\neq j$时$(P,\gamma_i,\gamma_j)=1$.令$A=(P,\gamma_1^{e_1}\cdots\gamma_g^{e_g})$,则

$$\mathcal{B}_1\mathcal{B}_2=(P,\gamma_1)(P,\gamma_2)=(P^2,P\gamma_1,P\gamma_1,\gamma_1\gamma_2)=(P(P,\gamma_1,\gamma_2),\gamma_1\gamma_2)=(P,\gamma_1\gamma_2)$$

$$\mathcal{B}_1^2=(P,\gamma_1)^2=(P^2,P\gamma_1,\gamma_1^2)\subseteq(P,\gamma_1^2)$$

由此归纳下去，

$$\mathcal{B}_1^{e_1}\cdots\mathcal{B}_g^{e_g}\subseteq(P,\gamma_1^{e_1}\cdots\gamma_g^{e_g})=A$$

只需再证$A=P\mathcal{O}_L$即可。为此将$x=\alpha$带入$f(x)\equiv p_1(x)^{e_1}\cdots p_g(x)^{e_g}(modP)$,便得到

$$\gamma_1^{e_1}\cdots\gamma_g^{e_g}\equiv f(\alpha)=0(modP\mathcal{O}_L)$$

即$\gamma_1^{e_1}\cdots\gamma_g^{e_g}\in P\mathcal{O}_L$,从而$A=(P,\gamma_1^{e_1}\cdots\gamma_g^{e_g})=P\mathcal{O}_L$.
现在来证明(3):我们不妨假设$\mathcal{B}_1,\cdots,\mathcal{B}_s$均不为$\mathcal{O}_L$,而$\mathcal{B}_{s+1},\cdots,\mathcal{B}_g=\mathcal{O}_L$,则$\mathcal{B}_i(1\leq i\leq s)$均为$\mathcal{O}_L$的素理想，并且$P\subseteq\mathcal{B}_i.f_i(\mathcal{B}_i/P)=[\mathcal{O}_L/\mathcal{B}_i:\mathcal{O}_K/P]=f_i(1\leq i\leq s)$.由上知$\mathcal{B}_i\Phi(1\leq i\leq s)$两两互异，由$P\mathcal{O}_L|\mathcal{B}_1^{e_1}\cdots\mathcal{B}_g^{e_g}$知$P\mathcal{O}_L=\mathcal{B}_1^{d_1}\cdots\mathcal{B}_s^{d_s},d_i\leq e_i(1\leq i\leq s)$.由于$n=d_1f_1+\cdots d_sf_s\leq e_1f_1+\cdots e_gf_g$,且$f(x)\equiv p_1(x)^{e_1}\cdots p_g(x)^{e_g}$ 知$s=g,e_i=d_i(1\leq i\leq g)$,命题证毕。

1.5 Hilbert分歧理论

若数域扩张$L|K$是伽罗瓦扩张，素理想的分解问题将会变得更重要和有趣，下面记号仍与上面相同，即o是戴德金整环，分式域为K, $L|K$是有限域扩张，$\mathcal{O}$是o在L上的整闭包，记伽罗瓦群

为$G=G(L|K)$,任给$a\in\mathcal{O}$,a的共轭元$\sigma a\in\mathcal{O},\forall\sigma\in\mathcal{O}$.若$\mathfrak{P}$是$\mathcal{O}$中的素理想，且$\mathfrak{P}\cap o=\mathfrak{p}$,则对于每个$\sigma\in G,\sigma\mathfrak{P}\cap 0=\sigma(\mathfrak{P}\cap o)=\sigma\mathfrak{p}=\mathfrak{p}$.理想$\sigma\mathfrak{P}$叫做$\mathfrak{P}$的共轭理想。

命题5.1伽罗瓦群在$\mathcal{O}$的所有卧于素理想$\mathfrak{p}$(即：满足$\mathfrak{P}\cap o=\mathfrak{p}$的$\mathfrak{P}$组成的集合)的素理想$\mathfrak{P}$组成的集合上的作用是可迁的.

证明:设$\mathfrak{P}$和$\mathfrak{P}^{'}$是卧于$\mathfrak{p}$上的两个素理想,若对任意$\sigma\in G$,都有$\mathfrak{P}^{'}\neq\sigma\mathfrak{P}$,那么由中国剩余定理知存在$x\in\mathcal{O}$使得

$$x\equiv 0\quad(mod\quad\mathfrak{P}^{'}),x\equiv 1\quad(mod\quad\sigma\mathfrak{P}),\sigma\in G$$

于是范数$N_{L|K}(x)=\prod_{\sigma\in G}\sigma x$属于理想$\mathfrak{P}^{'}\cap o=\mathfrak{p}$.令一方面，对于所有$\sigma\in G$,$x\notin\sigma\mathfrak{P}$,因此$\sigma x\notin\mathfrak{P}$,推出$\prod_{\sigma\in G}\sigma x\notin\mathfrak{P}\cap o=\mathfrak{p}$,矛盾!

定义5.2:如果$\mathfrak{P}$是$\mathcal{O}$的素理想，子群

$$G_{\mathfrak{P}}=\{\sigma\in G|\sigma\mathfrak{P}=\mathfrak{P}\}$$

叫做域K上理想$\mathfrak{P}$的分解群，域

$$Z_{\mathfrak{P}}=\{x\in L|\sigma x=x,\forall\sigma\in G_{\mathfrak{P}}\}$$

叫做K上理想$\mathfrak{P}$的分解域。

由定义$Z_{\mathfrak{P}}$是$G_{\mathfrak{P}}$的不动域，即$Z_{\mathfrak{P}}=Inv(G_{\mathfrak{P}})$,由伽罗瓦理论知$Gal(L|Z_{\mathfrak{P}})=G_{\mathfrak{P}}$

下面再说一下一些定义，o中理想$\mathfrak{p}$在L中叫做**完全分裂**(totally split)的，如果$\mathfrak{p}$的分解式$\mathfrak{p}\mathcal{O}=\mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_r^{e_r}$
$n=[L:K]$于是对于所有$i=1,\cdots,r,e_i=f_i=1$;理想称为分歧的，如果$\exists 1\leq i\leq r,e_i>1$.否则便称不分歧;若$r=1$,即$\mathfrak{p}\mathcal{O}=\mathfrak{P}^n$(有关系式$\sum_{i=1}^{r}e_if_i=n$),则称理想是完全分歧，最后若$\mathfrak{p}\mathcal{O}=\mathfrak{P}(r=1,e(\mathfrak{P}/\mathfrak{p})=1,f(\mathfrak{P}/\mathfrak{p})=n)$称理想是惯性的。

设$\mathfrak{P}$是$\mathfrak{p}\mathcal{O}$在$\mathcal{O}$中素理想分解中的一理想，σ遍历$G/G_{\mathfrak{P}}$中元素的代表元，那么$\sigma(\mathfrak{P})$遍历卧于$\mathfrak{p}$上的所有素理想，且每个出现一次，即有$r=(G:G_{\mathfrak{P}})$.特别地，有

$$G_{\mathfrak{P}}=1\Leftrightarrow Z_{\mathfrak{P}}=L\Leftrightarrow\mathfrak{p}\quad is\quad totally\quad split$$

$$G_{\mathfrak{P}}=G\Leftrightarrow Z_{\mathfrak{P}}=K\Leftrightarrow\mathfrak{p}\quad is\quad nonsplit$$

$L|K$是伽罗瓦扩张时，剩余类域次数f_i，分歧指数e_i与i无关事实上，记$\mathfrak{P}=\mathfrak{P}_1$任意$\mathfrak{P}_i$,存在$\sigma_i\in G$使得$\mathfrak{P}_i=\sigma_i\mathfrak{P}$,(这可由命题5.1推得,)同构$\sigma_i:\mathcal{O}\to\mathcal{O}$诱导同构

$$\mathcal{O}/\mathfrak{P}\to\mathcal{O}/\sigma_i\mathfrak{P},\quad a\quad mod\quad\mathfrak{P}\mapsto\sigma_i a\quad mod\sigma_i\mathfrak{P},$$

故

$$f_i=[\mathcal{O}/\sigma_i(\mathfrak{P}):o/\mathfrak{p}]=[\mathcal{O}/\mathfrak{P}:o/\mathfrak{p}],i=1,\cdots,r.$$

进一步，由于$\sigma_i(\mathfrak{p}\mathcal{O})=\mathfrak{p}\mathcal{O}$,从而由

$$\mathfrak{P}^v|\mathfrak{p}\mathcal{O}\Leftrightarrow\sigma_i(\mathfrak{P}^v)|\sigma_i(\mathfrak{p}\mathcal{O})\Leftrightarrow(\sigma_i\mathfrak{P})^v|\mathfrak{p}\mathcal{O}$$

推出$e_i,i=1,\cdots,r$相等。

于是o中理想$\mathfrak{p}$在$\mathcal{O}$中的素理想分解有形式$\mathfrak{p}=(\prod_{\sigma}\sigma\mathfrak{P})^e$,其中$\sigma$遍历$G/G_{\mathfrak{P}}$的代表系。

令$\mathfrak{P}_Z = \mathfrak{P}\cap Z_{\mathfrak{P}}$，从而首先$\mathfrak{P}_Z \subset \mathfrak{P} \subset \mathcal{O}$,即$\mathfrak{P}_Z$在o上是整的，从而$\mathfrak{P}_Z$包含于o在域$Z_{\mathfrak{P}}$整闭包$\mathcal{O}_{Z_{\mathfrak{P}}}$,且易见是其素理想.
为了进一步应用命题5.1，下面说明一下看法，由伽罗瓦理论知域扩张$L|Z_{\mathfrak{P}}$是伽罗瓦扩张，环$\mathcal{O}_{Z_{\mathfrak{P}}}$是Dedekind整环，且可知$\mathcal{O}_{Z_{\mathfrak{P}}}$在L中闭包恰为$\mathcal{O}$(可证明两者相互包含)。命题5.1中基取在Dedekind整环o上(一般都取成整数环Z),由上分析还可将基取在$\mathcal{O}_{Z_{\mathfrak{P}}}$上，从而可得到下述命题
命题5.3(i)$\mathfrak{P}_Z$在L上不分裂，即$\mathfrak{P}$是L中唯一位于$\mathfrak{P}_Z$上的素理想。
(ii)$\mathfrak{P}$在$Z_{\mathfrak{P}}$上分歧指数为e,剩余类域次数为f.
(iii)$\mathfrak{P}_Z$在域K上分歧指数和剩余类域次数均为1.
证明：(i)由于$G(L|Z_{\mathfrak{P}}) = G_{\mathfrak{P}}$卧于$\mathfrak{P}_Z$上的理想是$\sigma\mathfrak{P},\sigma\in G(L|Z_{\mathfrak{P}})$,都是$\mathfrak{P}$.
(ii)伽罗瓦扩张下，分歧指数，剩余类域次数均为常数，基本公式$n = efr$,这里$n := |G|, r = (G : G_{\mathfrak{P}})$,于是$|G_{\mathfrak{P}}| = [L : Z_{\mathfrak{P}}] = ef$.令$e^{'}, e^{''}$分别是$\mathfrak{P}$在$Z_{\mathfrak{P}}$和$\mathfrak{P}_Z$在K上的分歧指数，那么在$Z_{\mathfrak{P}}$中$\mathfrak{p} = \mathfrak{P}_Z^{e^{''}}\ldots$，在L中$\mathfrak{P}_Z = \mathfrak{P}^{e^{'}}$.于是$\mathfrak{p} = \mathfrak{P}^{e^{''}e^{'}}\ldots$,立即$e = e^{''}e^{'}$.相似的可得到等式$f = f^{'}f^{''}$.有理想$\mathfrak{P}_Z$在L中分解得基本公式得到$[L : Z_{\mathfrak{P}}] = e^{'}f^{'}$,于是$e^{'}f^{'} = ef$,进而$e^{'} = e, f^{'} = f, e^{''} = f^{''} = 1$.
对于每个$\sigma\in G_{\mathfrak{P}}, \sigma\mathcal{O} = \mathcal{O}, \sigma\mathfrak{P} = \mathfrak{P}$,于是$\sigma$诱导出自同构

$$\bar{\sigma} : \mathcal{O}/\mathfrak{P} \longrightarrow \mathcal{O}/\mathfrak{P}, a \quad mod \quad \mathfrak{P} \longmapsto \sigma a \quad mod \quad \mathfrak{P}$$

令$\kappa(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}, \kappa(\mathfrak{p}) = o/\mathfrak{p}$,有下面命题
命题5.4:域扩张$\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$是正规扩张，$G_{\mathfrak{P}} \longrightarrow G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$是满射。
证明:由命题5.3知$[\mathcal{O}_{Z_{\mathfrak{P}}}/\mathfrak{P}_Z : o/\mathfrak{p}] = f^{''} = 1$,于是两者相同，即有$\kappa(\mathfrak{p}) = \mathcal{O}_{Z_{\mathfrak{P}}}/\mathfrak{P}_Z = \kappa(\mathfrak{P}_Z)$.伽罗瓦群 $G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) = G(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_Z))$.于是可以假设$K = Z_{\mathfrak{P}}$,这样做的好处是$G_{\mathfrak{P}}$是域扩张$L|Z_{\mathfrak{P}} = L|K$的伽罗瓦群，这在后面要用到。设$\theta\in\mathcal{O}$是$\bar{\theta}\in\kappa(\mathfrak{P})$的一代表元，$f(X), \bar{g}(X)$分别是$\theta$在域K上，$\bar{\theta}$在域$\kappa(\mathfrak{p})$上的最小多项式，那么$\bar{\theta} = \theta mod\mathfrak{P}$是多项式$\bar{f}(X) = f(X)mod\mathfrak{p}$的零点，于是$\bar{g}(X)$整除$\bar{f}(X)$由于$L|K$是正规扩张，$f(X)$在$\mathcal{O}$分解为一次因式，故$\bar{f}(X)$在$\kappa(\mathfrak{P})$中也分解成一次因式，$\bar{g}(X)$同样是，这说明$\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$是正规扩张。
现在设$\bar{\theta}$是$\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$的极大可分子扩张的本原元素(在代数数域的扩张都是可分扩张.这里的基取为Dedekind整环o,不是整数环Z),

$$\bar{\sigma}\in G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p})) = G(\kappa(\mathfrak{p})(\bar{\theta})|\kappa(\mathfrak{p})).$$

那么$\bar{\sigma}\bar{\theta}$是$\bar{g}(X)$的根，因此也是$\bar{f}(X)$的根，故存在$f(X)$的零点$\theta^{'}$使得 $\theta^{'} \cong \bar{\sigma}\bar{\theta} mod\mathfrak{P}$.$\theta^{'}$与$\theta$是共轭的，即存在$\sigma\in G(L|K)$使得$\theta^{'} = \sigma\theta$.($G_{\mathfrak{P}}$是域扩张$L|Z_{\mathfrak{P}} = L|K$的伽罗瓦群),由于$\sigma\theta\cong\bar{\sigma}\bar{\theta} mod\mathfrak{P}$.故$\sigma$映射到$\bar{\sigma}$.这就证明了满射.
定义5.5:同态$G_{\mathfrak{P}} \longrightarrow G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$的核$I_{\mathfrak{P}} \subseteq G_{\mathfrak{P}}$叫做$\mathfrak{P}$在K上的惯性群，其不动域$T_{\mathfrak{P}} = \{x\in L|\sigma x = x, \forall\sigma\in I_{\mathfrak{P}}\}$叫做$\mathfrak{P}$在K上的惯性域。从而有域“塔” $K \subseteq Z_{\mathfrak{P}} \subseteq T_{\mathfrak{P}} \subseteq L$.同时还看出$I_{\mathfrak{P}}$是$G_{\mathfrak{P}}$的正规子群，从而由伽罗瓦理论知$T_{\mathfrak{P}}|Z_{\mathfrak{P}}$是正规扩张且$G(T_{\mathfrak{P}}|Z_{\mathfrak{P}}) \cong G_{\mathfrak{P}}/I_{\mathfrak{P}}$.实际上由于可分扩张的子扩张是可分扩张，从而$T_{\mathfrak{P}}|Z_{\mathfrak{P}}$是伽罗瓦扩张，再结合命题5.4知 $G(T_{\mathfrak{P}}|Z_{\mathfrak{P}}) \cong G(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}))$.
若剩余类域扩张$\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$是可分扩张，那么$|G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))| = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = f$.从而$[T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = |G(T_{\mathfrak{P}}|Z_{\mathfrak{P}})| = (G_{\mathfrak{P}} : I_{\mathfrak{P}}) = f$.再由$[L : Z_{\mathfrak{P}}] = ef, G(L|T_{\mathfrak{P}}) = I_{\mathfrak{P}}$知$|I_{\mathfrak{P}}| = [L : T_{\mathfrak{P}}] = e$.

对域扩张$L|T_{\mathfrak{P}}$应用命题5.4，即考虑映射 $G_{\mathfrak{P}} \longrightarrow G(\kappa(\mathfrak{P})|\kappa(\mathfrak{B}_T)), \mathfrak{P}_T = \mathfrak{P} \cap T_{\mathfrak{P}}$.注意这里$G_{\mathfrak{P}}$即为$I_{\mathfrak{P}}$.这一映射的核同样是$I_{\mathfrak{P}}$于是得到$G(\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_T)) = 1$.由上假设知$\kappa(\mathfrak{P})|\kappa(\mathfrak{P}_T)$是可分扩张，在结合命题5.4知是伽罗瓦扩张，进而$\kappa(\mathfrak{P}) = \kappa(\mathfrak{P}_T)$.即$\mathfrak{P}$在$\mathfrak{P}_T$上的剩余类域次数为1.再由基本公式知分歧指数e.还可得到$\mathfrak{P}_T$在$\mathfrak{P}_Z$上的分歧指数为1，剩余类域次数是f.

1.6 Minkowski理论

下面首先给出格的定义，然后证明Minkowski的一个定理

定义3.1：V是n维实线性空间，V中的一个**格**是形如

$$\Gamma = \mathcal{Z}\nu_1 + \cdots + \mathcal{Z}\nu_m$$

的子群。其中$\nu_1, \cdots \nu_m$是V中线性无关的向量。集合

$$\mathbf{\Phi} = \{x_1\nu_1 + \cdots x_m\nu_m | x_i \in R, 0 \leq x_i < 1\}$$

称为格的基本网.格称为**完备**的如果$m = n$.

设$e_1, \cdots, e_n$是V的一组标准正交基，则$\mathbf{\Phi} = \{x_1\nu_1 + \cdots x_n\nu_n | x_i \in R, 0 \leq x_i < 1\}$的体积为$vol(\Phi) = |det(A)|$,其中矩阵$A = (a_{ij})$是从基 $e_1, \cdots, e_n$到基$\nu_1, \cdots, \nu_n$的转换矩阵，$\nu_i = \sum_k a_{ik}e_k$.

Minkowski格点定理: 设Γ是欧式空间V中的完备格,X是V中关于原点对称的凸集，若

$$vol(X) > 2^n vol(\Gamma),$$

则X至少包含Γ的一个格点$\gamma \in \Gamma$。

证明：只需证明存在两格点$\gamma_1, \gamma_2 \in \Gamma$,使得

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

为此，假设所有$\frac{1}{2}X + \gamma, \gamma \in \Gamma$,是互不相交的，则集合$\Phi \cap (\frac{1}{2}X + \gamma), \gamma \in \Gamma$对于所有$\gamma \in \Gamma$也是互不相交的，于是有

$$vol(\Phi) \geq \sum_{\gamma \in \Gamma} vol(\Phi \cap (\frac{1}{2}X + \gamma)).$$

集合$\Phi \cap (\frac{1}{2}X + \gamma)$是集合$(\Phi - \gamma) \cap (\frac{1}{2}X)$通过平移得到的，因此两者有相同的体积，但$\Phi - \gamma, \gamma \in \Gamma$覆盖整个空间$V$,因此得到

$$vol(\Phi) \geq \sum_{\gamma \in \Gamma} vol((\Phi - \gamma) \cap \frac{1}{2}X) = vol(\frac{1}{2}X) = \frac{1}{2^n} vol(X),$$

这一矛盾证明了命题。

下面定义整理想的范数

设A是$\mathcal{O}_K$的非零整理想，$\{\omega_1, \cdots, \omega_n\}$是$\mathcal{O}_K$的一组整基，$\{\alpha_1, \cdots, \alpha_n\}$是A的一组整基，则$\alpha_i \in \mathcal{O}_K$,$\{\omega_1, \cdots, \omega_n\}$的整线性组合，于是

$$(\alpha_1, \cdots, \alpha_n)^t = T(\omega_1, \cdots, \omega_n)^t, T = (t_{ij}), t_{ij} \in Z, detT \neq 0$$

如果$\{\omega_1^{'},\cdots,\omega_n^{'}\}$和$\{\alpha_1^{'},\cdots,\alpha_n^{'}\}$分别是$\mathcal{O}_K$和A的另一组整基，则

$$(\alpha_1^{'},\cdots,\alpha_n^{'})^t=M(\alpha_1,\cdots,\alpha_n)^t,(\omega_1,\cdots,\omega_n)^t=N(\omega_1^{'},\cdots,\omega_n^{'})^t$$

其中M和N均为n阶整方阵，并且$|detM|=1,|detN|=1$而

$$(\alpha_1^{'},\cdots,\alpha_n^{'})^t=MTN(\omega_1^{'},\cdots,\omega_n^{'})^t$$

由于$|det(MTN)|=|detT|$,这就表明正整数$|detT|$与$\mathcal{O}_K$和A的整基选取是无关的，即它是理想本身的不变量，在称它为整理想的范数，表示成$N_K(A)=N_{K/Q}(A)$.
设$\sigma_1,\cdots,\sigma_n$是数域K到C中的n个嵌入，$n=[K:Q]$.由于M是整数矩阵，由上可得

$$(\sigma_i(\alpha_1),\cdots,\sigma_i(\alpha_n))^t=M(\sigma_i(\omega_1),\cdots,\sigma_i(\omega_n))^t$$

从而有矩阵等式:$(\sigma_i(\alpha_j))=M(\sigma_i(\alpha_j))$,于是

$$d_K(\alpha_1,\cdots,\alpha_n)=det(\sigma_i(\alpha_j))^2=(detM)^2(det(\sigma_i(\alpha_j))^2)=N_K(A)^2d_K(\omega_1,\cdots,\omega_n)=N_K(A)^2d(K)$$

关于理想的范数还有下面命题
设A为数域K中非零整理想，$A=P_1^{e_1}\cdots P_r^{e_r}$,其中$P_1,\cdots,P_r$是$O_K$中不同的素理想，$e_i\leq 1$,则$N_K(A)=|O_K/A|,N_K(A)=N_K(P_1)^{e_1}\cdots N_K(P_r)^{e_r}$
(证明请看冯克勤著《代数数论入门》)
为将$Minkowski$格点定理应用到数论中，须构造映射,需要下面结论 (证明请看冯克勤著《代数数论入门》)：
(1)每个数域扩张$L|K$都是单扩张，即存在$\gamma\in L$,使得$L=K(\gamma)$
(2)设K是n次数域，即$[K:Q]=n$，则恰有n个从K到$\mathcal{C}$的$Q-$嵌入，其中设有r_1个实嵌入$\sigma_i:K\to R(1\leq i\leq r_1)$和$r_2$个复嵌入$\sigma_{r_1+j}=\bar{\sigma}_{r_1+r_2+j}:K\to C(1\leq j\leq r_2),r_1+2r_2=n$.由此得到映射

$$\sigma:K\to R^n,\sigma(\alpha)=(\sigma_1(\alpha),\cdots,\sigma_{r_1}(\alpha),Re(\sigma_{r_1+1}(\alpha)),\cdots,Re(\sigma_{r_1+r_2}(\alpha)),Im(\sigma_{r_1+1}(\alpha)),\cdots,Im(\sigma_{r_1+r_2}(\alpha)))$$

其中$Re(\gamma),Im(\gamma)$分别表示复数γ的实部和虚部。从而σ为嵌入，称为K到R^n中的正则嵌入。
引理3.2:设$\mathcal{P}$是n次数域K中的非零整理想，则$\sigma((P))$是R_n中的格，并且$Vol(\sigma(P))=2^{-r_2}N(P)|d(K)|^{1/2}$
证明:存在$\alpha_1,\cdots,\alpha_n\in K$,使得$(P)=Z\alpha_1\oplus\cdots\oplus Z\alpha_n$.取$e_1,\cdots,e_n$为$R_n$的标准基，则$\sigma(\alpha_i)=\sum_{j=1}^n x_{ij}e_j$,其中

$$(x_{i1},\cdots,x_{in})=(\sigma_j(\alpha_i),\cdots,\sigma_{r_1}(\alpha_i),Re(\sigma_{r_1+1}(\alpha_i)),\cdots,Re(\sigma_{r_1+r_2}(\alpha_i)),Im(\sigma_{r_1+r_2+1}(\alpha_i)),\cdots,Im(\sigma_n(\alpha_i)))$$

于是$\sigma(P)=Z\sigma(\alpha_1)+\cdots+Z\sigma(\alpha_n)$,并且

$$Vol(\sigma(P))=|det(x_{ij})|=2^{-r_2}|det(\sigma_j(\alpha_i))|=2^{-r_2}|d_K(\alpha_1,\cdots,\alpha_n)|^{1/2}=2^{-r_2}N(P)|d(K)|^{1/2}$$

由于上式右边不为零，即$det(x_{ij})\neq 0$,这表明$\sigma(\alpha_1),\cdots,\sigma(\alpha_n)$是$R-$线性无关的，从而$\sigma(P)=Z\sigma(\alpha_1)+\cdots+Z\sigma(\alpha_n)$是$R^n$中的格。
引理3.3:设P是数域K中的整理想，$[K:Q]=r_1+2r_2$.则
(1)存在$0\neq x\in P$,使得

$$|N_{K/Q}(x)|\leq(\frac{4}{\pi})^{r_2}\frac{n!}{n^n}|d(K)|^{\frac{1}{2}}N_{K/Q}(A)$$

(2)K的每个理想类C中均有整理想$\mathcal{B}$fi使得

$$N_{K/Q}(B) \le (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}|d(K)|^{\frac{1}{2}}$$

证明:对于$y=(y_1,\cdots,y_n)\in R^n$,定义

$$\lambda(y)=\sum_{i=1}^{r_1}|y_i|+2\sum_{j=1}^{r_2}(y^2_{r_1+j}+y^2_{r_1+r_2+j})^{1/2}$$

对于$t>0$,定义集合$B_t=\{y=(y_1,\cdots,y_n)\in R^n|\lambda(y)\le t\}$,可知这是关于原点对称的紧凸集，令$X(t)=\{y|\lambda(y)\le t,y_1\ge 0,\cdots,y_{r_1}\ge 0\}$,则由对称性可得$vol(B_t)=2^{r_1}vol(X(t))$,用极坐标变换后$n-r_1$个变量,即令

$$y_{r_1+j}=\frac{1}{2}\rho_j cos\theta_j, y_{r_1+r_2+j}=\frac{1}{2}\rho_j sin\theta_j,$$

变换的雅可比行列式绝对值为$\rho_j/4$,由于对称性易得到

$$vol(X(t))=2^{r_1}4^{-r_2}(2\pi)^{r_2}\int_Z \rho_{r_1+1}\cdots\rho_{r_1+r_2}dy_1\cdots dy_{r_1}d\rho_{r_1+1}\cdots d\rho_{r_1+r_2}$$

这里

$$Z=\{(y,\rho)\in R^{r+s}|y_i,\rho_i\ne 0,\sum y_i+\sum\rho_i\le t\}$$

问题便归结为积分$\int_Z \rho_{r_1+1}\cdots\rho_{r_1+r_2}dy_1\cdots dy_{r_1}d\rho_{r_1+1}\cdots d\rho_{r_1+r_2}$的计算，令

$$y_i=tx_i, 1\le r_1, \rho_{r_i+j}=tx_{r_i+j}, 1\le j\le r_2,$$

从而

$$\int_Z \rho_{r_1+1}\cdots\rho_{r_1+r_2}dy_1\cdots dy_{r_1}d\rho_{r_1+1}\cdots d\rho_{r_1+r_2}=t^n\int_{Z'} x_{r_i+1}\cdots x_{r_i+r_2}dx_1\cdots dx_{r_1}dx_{r_1+1}\cdots dx_{r_1+r_2}$$

这里$Z^{'}=\{(x_i)\in R^{r_1+r_2}|\sum x_i\le 1\}$,
更一般地，积分

$$I(a_1.\cdots,a_m,t)=\int_{Z(t)} x_1^{a_1}\cdots x_m^{a_m}dx_1\cdots dx_m$$

这里$Z(t)=\{x\in R^m|x_i\ge 0,\sum x_i\le t\}$,积分可以通过减少积分变量，并不断把t利用变量替换变为1求出。最后结果为

$$I(a_1.\cdots,a_m,t)=t^{\sum a_i+m}\frac{\Gamma(a_1+1)\cdots\Gamma(a_m+1)}{\Gamma(a_1+\cdots+a_m+m+1)}.$$

回到上面可得出$vol(X(t))=2^{r_1}4^{-r_2}(2\pi)^{r_2}t^n/n!$
根据引理3.2，对于K中非零整理想P, $\sigma(P)$为R^n中的格，并且

$$Vol(\sigma(P))=2^{-r_2}N(P)|d(K)|^{1/2}$$

当$t^n=(\frac{4}{\pi})^{r_2}N(P)|d(K)|^{1/2}n!$时，$vol(B_t)=2^n vol(\sigma(P))$,从而由Minkowski定理可知存在非零$x\in P$,使得$\sigma(x)\in B_t$,即

$$\lambda(\sigma(x))\le t$$

于是

$$|N_{K/Q}(x)| = \prod_{i=1}^{n} |\sigma_i(x)| \le (\frac{1}{n}\sum_{i=1}^{n} |\sigma_i(x)|)^n = \frac{1}{n^n}(\lambda(\sigma(x)))^n \le \frac{1}{n^n}t^n = (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}N(P)|d(K)|^{1/2}$$

(2)设$P^{'} \in C$.由于$P^{'}$除以任何整数之后仍为理想类C中的理想，因此不妨可以设$P = P^{'}$是整理想，由(1)知有

$$0 \ne x \in P, N(x) \le (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}N(P)|d(K)|^{1/2}$$

令$\mathcal{B} = xP^{-1} = xP^{'}$,由于$x \in P$可知$\mathcal{B}$为C中的整理想，并且

$$N(\mathcal{B}) = N(x)N(P^{'}) \le (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}N(PP^{'})|d(K)|^{1/2}$$

由于$N(PP^{'}) = N(\mathcal{O}_K) = 1$,证毕。
应用Minkowski格点定理可以证明下述定理。
类数有限定理:理想类群$Cl_K = J_K/P_K$是有限群,它的阶数叫做代数数域K的类数。(这里J_K是K的所有分式理想，P_K是K的分式主理想)
证明:若P是$\mathcal{O}_K$中的素理想，$P \cap Z = pZ$,那么$\mathcal{O}_K/P$是Z/pZ的有限域扩张。次数设为$f \ge 1$,从而$N_{K/Q}(P) = p^f$.给定一个p，这里仅有有限个P使得$P \cap Z = pZ$,这是因为这意味着$P|(p)$.由此可知仅有有限个素理想P使得$N_{K/Q}(P) = p^f$.因为每个整理想有素理想表示$A = P_1^{\mu_1}P_2^{\mu_2}\cdots P_r^{\mu_r}, \mu_i > 0$.并且

$$N_{K/Q}(A) = N_{K/Q}(P_1)^{\mu_1}N_{K/Q}(P_2)^{\mu_2}\cdots N_{K/Q}(P_r)^{\mu_r}$$

可知给定一上界$M > 0$, $\mathcal{O}_K$仅有有限个理想A,使得$N_{K/Q}(A) \le M$.因此我们可以通过选定M证明定理。由引理3.3(2)知若令$M = (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}|d(K)|^{\frac{1}{2}}$,则K的每个理想类中都有整理想满足这一条件，从而证明了K只有有限个理想类。

1.7 单位定理

1.8 分圆域

1.9 局部化

定义1：仅有唯一极大理想的环称为**局部环**.
若A是局部环，其极大理想为$\mathcal{M}$,则任意$a \in \mathcal{M}$是A中单位，这是由于主理想(a)不包含在任何极大理想中，从而是整个环，即可逆，进而还有$A^* = A - \mathcal{M}$.
定义2：离散赋值环是一个仅有一个不为零的极大理想的主理想整环(即局部主理想整环。)
离散赋值环中的极大理想形式为$P = (\pi) = \pi\mathcal{O}$,$\pi$为素元，由于每个不属于$P$的元素都是单位(即可逆)，从而在相伴的意义下，$\pi$是$\mathcal{O}$唯一的素元.$\mathcal{O}$中的非零元素因此能被写成形式$\varepsilon\pi^n, \varepsilon \in \mathcal{O}^*, n \ge 0$.更一般地，分式域$K$中非零元素$a \ne 0$能被唯一写成形式

$$a = \varepsilon\pi^n, \varepsilon \in \mathcal{O}^*, n \in Z.$$

这里指数n叫做a的值，记为$\nu(a)$,明显的有$(a)=P^{\nu(a)}$.
赋值是一函数$\nu:K^*\to Z$.令$\nu(0)=\infty$.通过简单的计算，得到$\nu(ab)=\nu(a)+\nu(b),\nu(a+b)\geq min\{\nu(a),\nu(b)\}$
命题：若$\mathcal{O}$是戴德金整环，$S\subseteq\mathcal{O}-\{0\}$是乘性子集，那么$\mathcal{O}S^{-1}$也是戴德金整环。
证明。
命题:$\mathcal{O}$是诺特整环，$\mathcal{O}$是戴德金整环当且仅当对于每个非零素理想$P\neq 0,$,环的局部化$\mathcal{O}_P$是离散赋值环。
证明:
$\mathcal{O}$是戴德金整环，对于每个非零素理想$P\neq 0$,有离散赋值环$\mathcal{O}_P$,和赋值$\nu_P:K\to Z$.赋值在理想的分解的有下述作用：如果$x\in K^*$,并且$(x)=\prod_P P^{\nu_P}$是主理想(x)的素理想的分解，那么对于每个P,有$\nu_P=\nu_P(x)$. 事实上，对于每个$\mathcal{O}$的素理想$Q\neq 0$ 由于$P\neq Q$时,$P\mathcal{O}_Q=\mathcal{O}_Q$,因此

$$x\mathcal{O}_Q=(\prod_P P^{\nu_P})\mathcal{O}_Q=Q^{\nu_Q}\mathcal{O}_Q=\mathcal{M}_Q^{\nu_Q}$$

因此$\nu_Q(x)=\nu_Q$
$\mathcal{O}$是戴德金环，令

$$\mathcal{O}(X)=\{\frac{f}{g}|f,g\in\mathcal{O},g\notin P,P\subseteq X\},$$

这里X是$\mathcal{O}$的一些不为零素理想为其元素组成的集合，$\mathcal{O}(X)$的非零素理想为$P_X=P\mathcal{O}(X)=\{\frac{f}{g}|f\in P,g\notin P,P\subseteq X\},P\subseteq X$,则可验证$\mathcal{O}_P=\mathcal{O}(X)_{PX}$,事实上，

$$\mathcal{O}(X)_{PX}=\{\frac{f}{g_1}/\frac{f_2}{g_2}|f\in\mathcal{O},f_2\in\mathcal{O}-P,g_1,g_2\notin X\},\mathcal{O}_P=\{\frac{f}{g}|f\in\mathcal{O},g\in\mathcal{O}-P\}$$

剩下的只需验证两者相互包含。
命题8.1：

$$1\to\mathcal{O}^*\to\mathcal{O}(X)^*\to\oplus_{P\notin X}K^*/\mathcal{O}_P^*\to CL(\mathcal{O})\to CL(\mathcal{O}(X))\to 1$$

为正合列,并且$K^*/\mathcal{O}_P^*\cong Z$
证明:这里第二个箭头为包含映射，第三个箭头是包含映射$\mathcal{O}(X)^*\to K^*$,和投射$K^*\to K^*/\mathcal{O}_P^*$的合成。若$a\in\mathcal{O}(X)^*$属于该复合映射的核，那么对于$P\notin X,a\in\mathcal{O}_P$,由于$\mathcal{O}_P=\mathcal{O}(X)_{PX}$,故对于$P\in X$,同样有$a\in\mathcal{O}_P$,于是$a\in\cap_P\mathcal{O}_P^*=\mathcal{O}^*$.这就证明了此处的正合性。
箭头

$$\oplus_{P\notin X}K^*/\mathcal{O}_P^*\to CL(\mathcal{O})$$

为映射

$$\oplus_{P\notin X}\alpha_P\quad mod\mathcal{O}_P^*\mapsto\prod_{P\notin X}P^{\nu_P(\alpha_P)}$$

这里$\nu_P:K^*\to Z$是关于$\mathcal{O}_P$的K^*上的赋值。设$\oplus_{P\notin X}\alpha_P\quad mod\mathcal{O}_P^*$是该映射核中元素，即像为一主理想设为$(\alpha)$，$\prod_{P\notin X}P^{\nu_P(\alpha_P)}=(\alpha)=\prod_{P\in X}P^{\nu_P(\alpha)},\alpha\in K^*$ 由于理想分解的唯一性，上述意味着对于$P\in X,\nu_P(\alpha)=0$,对于$P\notin X,\nu_P(\alpha_P)=\nu_P(\alpha)$, 进而可推出$\alpha\in\cap_{P\in X}\mathcal{O}_P^*=\mathcal{O}(X)^*,\alpha\equiv\alpha_P mod(\mathcal{O}_P^*)$.这就证明了此处的正合性。

箭头$CL(\mathcal{O}) \to CL(\mathcal{O}(X))$.是映射$Q \mapsto Q\mathcal{O}(X)$.$X$中的素理想$P$映射到$\mathcal{O}(X)$中的素理想，由于$CL(\mathcal{O}(X))$被这种形式的理想生成的，因此映射是满射。若$P \notin X$,我们有$P\mathcal{O} = (1)$,这因为这该映射的核包含形如$\prod_{P \notin X} P^{\nu_P(\alpha_P)}$的理想，这是前一个映射的像，因此这里也是正合的。最后，域的赋值$\nu_P : K^* \to Z$给出了同构$K^*/\mathcal{O}_P^* \cong Z$.

1.10 order

定义1：$K|Q$是n次代数数域，K的一个**order**是$\mathcal{O}_K$的一个包含长度为n的整基的子环，环$\mathcal{O}_K$叫做K的极大**order**。

命题：K的一个**order**是一维(Krull维数)(每个素理想是极大理想)诺特整环

证明:

在下面，我们设$\mathcal{O}$是一维诺特整环，K是其分式域。环的分式理想不再形成群，当可以考虑可逆理想，即对于分式理想A,存在分式理想B,使得$AB = \mathcal{O}$.分式理想A的逆仍为理想$A^{-1} = \{x \in K | xA \subseteq \mathcal{O}\}$

命题：$\mathcal{O}$的分式理想A是可逆的当且仅当对于每个素理想$P \neq 0$,$A_P = A\mathcal{O}_P$是$\mathcal{O}_P$的主分式理想。

证明:设A是可逆理想,$AB = \mathcal{O}.1 = \sum_{i=1}^{r} a_i b_i, a_i \in A, b_i \in B$,显然存在$a_i b_i \in \mathcal{O}_P$但不属于极大理想$P\mathcal{O}_P$,故不妨假设$a_1 b_1$是$\mathcal{O}_P$的单位，于是$A_P = a_1\mathcal{O}_P$,这是由于若$x \in A_P, xb_1 \in A_P B = \mathcal{O}_P$,因此$x = xb_1(b_1 a_1)^{-1} a_1 \in a_1\mathcal{O}_P$.

反之，设对于每个素理想P,$A_P = A\mathcal{O}_P$是主理想$a_P\mathcal{O}_P, a_P \in K^*$,我们可设$a_P \in A$,则可断定分式理想$A^{-1} = \{x \in K | xA \subseteq \mathcal{O}\}$是$A$的逆，假如不是，那么存在极大理想$P$,使得$AA^{-1} \subseteq P \subseteq \mathcal{O}$.设$a_1, \cdots, a_n$是理想$A$的生成系，由于$a_i \in A_P\mathcal{O}_P$,我们可写$a_i = a_P \frac{b_i}{s_i}, b_i \in \mathcal{O}, s_i \in \mathcal{O} - P$.于是$s_i a_i \in a_P\mathcal{O}$,令$s = s_1 \cdots s_n$,有$sa_i \in a_P\mathcal{O}, i = 1, \cdots, n$于是$sa_P^{-1}A \subseteq \mathcal{O}$,故$sa_P^{-1} \in A^{-1}$,这将导致$s = sa_P^{-1}a_P \in A^{-1}A \subseteq P$,矛盾!

记$\mathcal{O}$的可逆理想组成的群为$J(\mathcal{O})$,它包含分式主理想$a\mathcal{O}, a \in K^*$组成的群$P(\mathcal{O})$.

定义:商群

$$Pic(\mathcal{O}) = J(\mathcal{O})/P(\mathcal{O})$$

叫做环$\mathcal{O}$的Picard群。

当$\mathcal{O}$是戴德金环时，Picard群无非是理想类群CL_K.一般情况下，对于$J(\mathcal{O}), Pic(\mathcal{O})$.我们有下面描述

命题：映射$A \mapsto (A_P) = (A\mathcal{O}_P)$给出同构

$$J(\mathcal{O}) \cong \oplus_P P(\mathcal{O}_P)$$

证明：对于每个$A \in J(\mathcal{O}), A_P = A\mathcal{O}_P$是主理想，由于$A$仅包含在有限多个素理想(极大理想)$P$中,我们有态射

$$J(\mathcal{O}) \to \oplus_P P(\mathcal{O}_P), A \mapsto (A_P) = (A\mathcal{O}_P)$$

单射:若对任意素理想P,有$\mathcal{O}_P = A_P$.那么$A \subseteq \cap_P \mathcal{O}_P = \mathcal{O}$.于是就有$A = \mathcal{O}$,不然存在极大理想$P$，使得$A \subseteq P \subset \mathcal{O}.i.e A_P \subseteq P\mathcal{O}_P \neq \mathcal{O}_P$.

为证明满射，任给$(a_P\mathcal{O}_P) \in \oplus_P P(\mathcal{O}_P)$。$\mathcal{O}-$模$A = \cap_P a_P\mathcal{O}_P$是K的分式理想：事实上，对于几

乎所有P,有$a_P\mathcal{O}_P=\mathcal{O}_P$,于是存在$c\in\mathcal{O}$,使得$ca_P\in\mathcal{O}_P$对于所有$P$成立，即是$cA\subseteq\cap_P\mathcal{O}_P=\mathcal{O}$.下面需要证明的便是

$$A\mathcal{O}_P=a_P\mathcal{O}_P,\forall P$$

由A的定义知$\subseteq$的证明是平凡的。需要证的是$a_P\mathcal{O}_P\subseteq A\mathcal{O}_P$,

环$\mathcal{O}$在K中的正规化(即在K中的闭包)记为$\bar{\mathcal{O}}$ﬁ能够证明是戴德金环，有下引理

引理：$\mathcal{O}$是一维诺特整环，$\bar{\mathcal{O}}$是其正规化，那么对于$\mathcal{O}$的每个非零理想$A\neq 0$,商环$\bar{\mathcal{O}}/A\bar{\mathcal{O}}$是有限生成$\mathcal{O}-$模。

1.11 一维概型

1.12 习题

1.(Stickelberger)代数数域K的判别式$d_K\equiv 0$或$\equiv 1\quad(mod 4)$

2.设d无平方因子整数，p是不能整除$2d$的素数，$\mathcal{O}$是$\mathcal{Q}(\sqrt{d})$的整数环.证明$(p)=p\mathcal{O}$是$\mathcal{O}$的素理想当且仅当同余式$x^2\equiv d(modp)$无解。

3.证明:只有有限个素理想的Dedekind整环是主理想整环。

4.若A是Dedekind整环，$I\subset A$是非零理想，那么A/I的每个理想都是主理想。

5.Dedekind整环的每个理想能被两个元素生成。

6.设D是整环，证明下述条件等价：

(i)D是Dedekind整环;

(ii)D的每个分式理想可逆;

(iii)D的每个非零理想有唯一的素理想分解

7.设K是代数数域，$\mathcal{O}_K$是Z在K中的整闭包，有命题:Dedekind整环是UFD当且仅当是PID，从而研究UFD转换为探究PID。在代数中探究环是否为PID可能更为容易研究于是便定义出理想类群，下面给出另一种理想类群的定义：$\mathcal{O}_K$中理想I等价于J当且仅当存在$\alpha,\beta\in\mathcal{O}_K$使得

$$\alpha I=\beta J.$$

易验证这是等价关系，进一步定义等价类之间的乘法形成群，单位元是所有主理想形成的等价类，下面是两个练习:

(i)验证所有主理想形成一等价类，即若I是使得$\alpha I=(\beta)$成立的理想，那么I是主理想。

(ii)验证上述理想类群的定义与通常定义等价.(第一同构定理)

8.设$\mathfrak{a}$是K的整理想，$\mathfrak{a}^m=(\alpha)$.证明$\mathfrak{a}$在域$L=K(\sqrt[m]{\alpha})$中是主理想，即$\mathfrak{a}\mathcal{O}_L=(\beta),\beta\in\mathcal{O}_L$.

9.证明对于每个数域K,存在有限域扩张L,使得K的每个理想是主理想。

10.若代数数域扩张$L|K$是伽罗瓦扩张，其伽罗瓦群不是循环群，那么K至多有有限个不分裂的素理想。

11.若代数数域$L|K$是伽罗瓦扩张，$\mathfrak{P}$是在K上不分歧的素理想(即$\mathfrak{p}=\mathfrak{P}\cap K$在L上不分歧)，那么有且仅有一个子同构$\phi_{\mathfrak{P}}\in G(L|K)$使得

$$\phi_{\mathfrak{P}}a\equiv a^q\quad mod\quad\mathfrak{P}\quad\forall a\in\mathcal{O}$$

这里$q = |\kappa(\mathfrak{p})|$.这个自同构叫做Frobenius自同构.分解群$G_{\mathfrak{P}}$是循环的，$\phi_{\mathfrak{P}}$是$G_{\mathfrak{P}}$的一生成元。
12.(Dirichlet's prime number theorem)对于每个自然数n存在无限个素数$p \equiv 1 \quad mod \quad n.$
13.对于每个有限Abel群G,存在伽罗瓦扩张$K|Q$使得$G(K|Q) \cong G.$
14.每个二次域$Q(\sqrt{d})$都包含在某个分圆域$Q(\zeta_n)$.ζ_n是n次本原单位根。
15.设$L|K$是代数数域的有限域扩张(不必是伽罗瓦扩张)，$N|K$是$L|K$的正规闭包，证明:K中理想$\mathfrak{p}$在L上完全分裂当且仅当它在N上完全分裂.(对于G的子群U和V,考虑G中的等价关系$\sigma \sim \sigma' \iff \sigma' = u\sigma v, \exists u \in U, v \in V$,对应的等价类$U\sigma V = \{u\sigma v | u \in U, v \in V\}$,叫做G关于U，V的双陪集，所有这些双陪集组成的集合记作$U \setminus G/V$)

解答

3.设R是Dedekind整环，$\mathfrak{p}_1, \cdots, \mathfrak{p}_n$是R的所有素理想，对任意$1 \le i \ne j \le n, \mathfrak{p}_i + \mathfrak{p}_j = R$(这是由于Dedekind整环中，素理想都是极大理想，而$\mathfrak{p}_i + \mathfrak{p}_j$是包含极大理想$\mathfrak{p}_i$的理想，从而是整个环)，同样可知$\mathfrak{p}_1^2, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$两两互素，取$\pi \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$(由Dedekind整环中理想分解的唯一性，$\mathfrak{p}_1 \setminus \mathfrak{p}_1^2$非空)，由中国剩余定理存在$x \in R$使得

$$x \equiv \pi \pmod{\mathfrak{p}_1^2}, \ x \equiv 1 \pmod{\mathfrak{p}_k}, \ k = 2, \ldots, n$$

设主理想$(x) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}, e_i \in N$,若有$e_i \ge 1, i \ge 2$,则$x \in (x) \subset \mathfrak{p}_i$,但是$x \equiv 1(mod \mathfrak{p}_i)$,因此这是不可能的，故$(x) = \mathfrak{p}_1^{e_1}, e^1 \ge 1$,然而$x \notin \mathfrak{p}_1^2$,从而由$x \in (x) = \mathfrak{p}_1^{e_1}$推出$e_1 = 1$,于是$(x) = \mathfrak{p}_1$.同样可知R中每个素理想都是主理想，于是R的每个理想是主理想。
4.设$I = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$.,由中国剩余定理得到$A/I \cong \bigoplus_{i=1}^{n} A/\mathfrak{p}_i^{e_i}$.,从而只需证明$A/\mathfrak{p}_i^{e_i}$的理想是主理想，考虑投射$\pi : A \to A/\mathfrak{p}_i^{e_i}$.$A/\mathfrak{p}_i^{e_i}$的所有理想为$\mathfrak{p}_i^n (1 \le n \le e_i)$在$\pi$下的像，若$\pi(\mathfrak{p}_i) = \pi(\mathfrak{p}_i^2)$,那$\pi(\mathfrak{p}_i) = 0$,此时$A/\mathfrak{p}_i^{e_i}$是域，否则取$\alpha \in \pi(\mathfrak{p}_i) \setminus \pi(\mathfrak{p}_i^2)$.那么$(\alpha)$是真理想，且$(\alpha) \not\subset \pi(\mathfrak{p}_i^n), n \ge 2$,由此推出$(\alpha) = \pi(\mathfrak{p}_i)$,故$\pi(\mathfrak{p}_i^n) = (\alpha^n)$.因此$A/\mathfrak{p}_i^{e_i}$主理想。
5.设R是Dedekind整环,I是R中理想，任取$a \in I \setminus \{0\}$,令$J = Ra$,则$J \subset RI = I$,考虑商环R/J,由上题知R/J中理想I/J是主理想，即有$b \in R$使得$I = Rb + J$,但由于$J = Ra$,故$I =< a, b >$
8.首先$(\mathfrak{a}\mathcal{O}_L)^m = \alpha\mathcal{O}_L = (\sqrt[m]{\alpha}\mathcal{O}_L)^m$,$\mathcal{O}_L$中每个理想都有唯一的素理想分解,于是$\mathfrak{a}\mathcal{O}_L = \prod_{i=1}^{s} \mathfrak{p}_i^{k_i}$,$\mathfrak{p}$是素理想,$k_i \in Z$,从而$(\sqrt[m]{\alpha}\mathcal{O}_L)^m = (\mathfrak{a}\mathcal{O}_L)^m = \prod_{i=1}^{s} \mathfrak{p}_i^{mk_i}$,进而$\sqrt[m]{\alpha}\mathcal{O}_L = \prod_{i=1}^{s} \mathfrak{p}_i^{mk_i/m} = \mathfrak{a}\mathcal{O}_L$,取$\beta = \sqrt[m]{\alpha}$即为所证命题。
9.设$|Cl_K| = n$(类数有限定理),记Cl_K的元素为$[I_1], \cdots, [I_n,]$对于每个$1 \le k \le n$取$J_k \in [I_k]$.存在整数m_k,$\alpha_k \in \mathcal{O}_K$使得$J_k^{m_k} = (\alpha_k)$,由上题知$J_1, \cdots, J_k$在域$L = K(\sqrt[m_1]{\alpha_1}, \ldots, \sqrt[m_n]{\alpha_n})$.的整数环中都是主理想，剩下的只需验证若$I \subset \mathcal{O}_K, I \simeq J_1$,则$I$是$\mathcal{O}_K$中主理想，如果$I \simeq J_1$,那么存在$x, y \in \mathcal{O}_K$使得$xI = yJ_1$,于是

$$x^{m_1} I^{m_1} = y^{m_1} J_1^{m_1} = (y^{m_1} \alpha_1)$$

因此$xI\mathcal{O}_L = y \sqrt[m_1]{\alpha_1}\mathcal{O}_L$,从而存在$z \in I\mathcal{O}_L$使得$xz = y \sqrt[m_1]{\alpha_1}$,断言$I = (z)$,显然$(z) \subseteq I\mathcal{O}_L$,反之，任取$w \in I$.那么$xw = y \sqrt[m_1]{\alpha_1} v = xzv, v \in \mathcal{O}_L$,由于$\mathcal{O}_L$是整环，因此$zv = w$,所以$I \subseteq (z)$,故$I$是$\mathcal{O}_L$中主理想。
10.由于可分扩张$L|K$中只有有限个素理想分歧，故不妨只需证明不分裂且不分歧的素理想只有有

限个，设$\mathfrak{p}$是这样的素理想，于是$\mathfrak{p}\mathcal{O}=\mathfrak{P},\mathfrak{P}\in\mathcal{O}.f[\mathcal{O}/\mathfrak{P}:o/\mathfrak{p}]=[L:K]$. 由$\mathfrak{p}$不分裂知$G_{\mathfrak{P}}=G$.再由$\mathfrak{p}$不分歧知$I_{\mathfrak{P}}=1$.从而$G\cong Gal(\mathcal{O}/\mathfrak{P}|o/\mathfrak{p})$.但有限域扩张$\mathcal{O}/\mathfrak{P}|o/\mathfrak{p}$的伽罗瓦群是循环群，而根据假设G不是循环群，矛盾！于是不存在这样的素理想，即K中不分裂的素理想是分歧的，从而有有限个.

11.域扩张$\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$是伽罗瓦扩张，有下述关系

$$I_{\mathfrak{P}}=1\iff T_{\mathfrak{P}}=L\iff \mathfrak{p}\quad is\quad unramified\quad in\quad L$$

进而$G(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))\cong G_{\mathfrak{P}}$.有限域扩张$\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$的伽罗瓦群是循环群，从而$G_{\mathfrak{P}}$是循环群。由有限域的伽罗瓦理论知$Gal(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$的生成元是映射$\sigma:x\mapsto x^q.(x\in\kappa(\mathfrak{p})),q=|\kappa(\mathfrak{p})|$.在同构对应下，记$\sigma$在$G_{\mathfrak{P}}$ 中对应元素为$\phi_{\mathfrak{P}}$.则

$$\phi_{\mathfrak{P}}a\equiv a^q(mod\mathfrak{P}),\forall a\in\mathcal{O}.$$

这是由于如果$\tau\in G_{\mathfrak{P}}$并且对于每个$a\in\mathcal{O}$均有$\tau a\equiv a^q(mod\mathfrak{P})$,则在同构下$\tau\mapsto\bar{\tau}$,对于每个$\bar{a}\in\bar{L}$均有$\bar{\tau}(\bar{a})=\bar{a}^q$.即$\bar{\tau}=\sigma$,从而$\tau=\phi_{\mathfrak{P}}$.

12.设$n\geq 2$.用反证法，若只存在有限个这样的素数,记为$p_1,\cdots,p_m$,令$q=\prod_{1\leq i\leq m}p_i$.考虑

$$\Phi_n(xnq),x\in Z,$$

$\Phi_n(X)$是n次分圆多项式，显然存在$x\in Z$使得$\Phi_n(xnq)>1$.此时存在素数P 使得$p|\Phi_n(xnq)$. 由于$\Phi_n(X)$的常数项为1，且$\Phi_n(X)$为整系数多项式,故$p\nmid xnq$,从而$p\neq p_i$.因为$xnq\in F_p$是n次本原单位根，由拉格朗日定理得$n|p-1$,于是$p\equiv 1(mod\quad n)$.矛盾!从而证明命题。

13.G是有限$Abel$群，根据有限$Abel$群结构定理，存在$n_1,\cdots,n_k$使得

$$G\cong(\mathbb{Z}_{n_1},+)\oplus(\mathbb{Z}_{n_2},+)\oplus(\mathbb{Z}_{n_k},+)$$

对任意$n_i(i=1,\cdots,k)$由$Dirichlet$素数定理,存在素数p_i使得$n_i|p_i-1$,从而有满射$(\mathbb{Z}/p_i\mathbb{Z})^\times\to(\mathbb{Z}_{n_i},+)$. 令$n=p_1\cdots p_k$,由中国剩余定理

$$(\mathbb{Z}/n\mathbb{Z})^\times\cong\prod_{i=1}^k(\mathbb{Z}/p_i\mathbb{Z})^\times,$$

于是有典范态射$\phi:(\mathbb{Z}/n\mathbb{Z})^\times\to G$, ϕ是满射，$(\mathbb{Z}/n\mathbb{Z})^\times/ker(\phi)\cong G$。已知$Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})=(\mathbb{Z}/n\mathbb{Z})^\times$(这里把同构看作相等)，这里$\xi_n$是$n$次本原单位根,由$Galois$理论知存在$\mathbb{Q}(\xi_n)$的包含$\mathbb{Q}$的子域$K$使得$Gal(\mathbb{Q}(\xi_n)/K)=ker(\phi)$,由于$Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$是$Abel$群，$K$是$\mathbb{Q}$的$Galois$扩张，从而

$$Gal(K/\mathbb{Q})\cong Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})/Gal(\mathbb{Q}(\xi_n)/K)\cong G.$$

证毕。

15.设$\mathfrak{p}$是K上的素理想,$P_{\mathfrak{p}}$是L中所有卧$\mathfrak{p}$上素理想组成的集合，设$N|K$是$L|K$的正规闭包，令$G=Gal(N|K),H=Gal(N|L)$.设$\mathfrak{P}$是N中卧于$\mathfrak{p}$上的一个素理想，$G_{\mathfrak{P}}=\{\sigma\in G|\sigma\mathfrak{P}=\mathfrak{P}\}$ 是$\mathfrak{P}$的分解群，则有G的双陪集$H\setminus G/G_{\mathfrak{P}}$到$P_{\mathfrak{p}}$的双射

$$H\sigma G_{\mathfrak{P}}\mapsto\sigma\mathfrak{P}\cap L$$

(后文给出证明)$\mathfrak{p}$是完全分裂的等价于$G_{\mathfrak{P}}$是平凡的，因此只需证明$G_{\mathfrak{P}}$是平凡的当且仅当$\mathfrak{p}$在L上完全分裂.
若$G_{\mathfrak{P}}$是平凡的(即$\mathfrak{p}$在N上完全分裂)，那么双陪集即是G关于H的陪集，于是由由伽罗瓦理论知$[G:H]=[L:K]$,这意味着L中有$[L:K]$个卧于$\mathfrak{p}$上的素理想，因此$\mathfrak{p}$在L上完全分裂.
相反地，如果$\mathfrak{p}$在L上完全分裂，那么双陪集的个数等于$[L:K]=[G:H]$,这于H的陪集的个数相同；由于每一个双陪集分解成H的右陪集无交并，从而对于任意$\sigma\in G, H\sigma G_{\mathfrak{P}}=H\sigma$,于是$G_{\mathfrak{p}}$关于G的共轭便包含在H中，即$G_{\mathfrak{p}}$生成的正规子群包含在H中。
但由于$N|K$是$L|K$的正规闭包，H对应于L，由伽罗瓦理论知G无非平凡正规子群，从而G中包含在H中的正规子群是平凡的,即是$\{1\}$,进而$G_{\mathfrak{P}}=\{1\}$
下面证明$H\sigma G_{\mathfrak{P}}$到$\sigma\mathfrak{P}\cap L$是双射.
首先,映射良定义：若$\tau\in G_{\mathfrak{P}}$,那么$\tau\mathfrak{P}=\mathfrak{P}$,因此$\sigma\mathfrak{P}\cap L=\sigma\tau\mathfrak{P}\cap L$.如果$\rho\in H$,那么$\rho$固定L中元素，于是$\rho\sigma\mathfrak{P}\cap L=\rho(\sigma\mathfrak{P}\cap L)=\sigma\mathfrak{P}\cap L$.因此$\rho\sigma\tau$与$\sigma$对应相同的集合。
满射：任给L中卧于$\mathfrak{p}$上的素理想$\mathfrak{q}$，N中存在素理想$\mathfrak{Q}$卧于$\mathfrak{q}$上，从而存在$\sigma\in G$使得$\sigma\mathfrak{P}=\mathfrak{Q}$.因此$H\sigma G_{\mathfrak{P}}$映射到$\sigma\mathfrak{P}\cap L=\mathfrak{Q}\cap L=\mathfrak{q}$.
单射：若$\sigma\mathfrak{P}\cap L=\phi\mathfrak{P}\cap L=\mathfrak{q}$.那么$\sigma\sigma\mathfrak{P}\cap L=\phi\mathfrak{P}\cap L=\mathfrak{P}$和$\phi_{\mathfrak{P}}$都是卧于$\sigma\mathfrak{P}\cap L=\phi\mathfrak{P}\cap L=\mathfrak{q}$上的素理想，因此存在$\rho\in Gal(N|L)=H$使得$\rho\sigma\mathfrak{P}=\phi\mathfrak{P}$.因此$\phi^{-1}\rho\sigma\mathfrak{P}=\mathfrak{P}$.即$\phi^{-1}\rho\sigma\in G_{\mathfrak{P}}$.因此存在 $\rho\in G_{\mathfrak{P}}$使得$\tau\sigma\rho^{-1}=\phi$.故ϕ属于双陪集$H\sigma G_{\mathfrak{P}}$.从而$H\phi G_{\mathfrak{P}}=H\sigma G_{\mathfrak{P}}$.

2 赋值

2.1 p进数域

设p为素数，有理数a的p进赋值$ord_p(a)$定义如下：在$a\neq 0$的情况下，将其表示为$a=p^m\frac{v}{u}(m\in Z, p\nmid u, p\nmid v)$,$ord_p(a)=m$.令$ord_p(0)=\infty$,则以下公式成立
$(i) ord_p(ab)=ord_p(a)+ord_p(b)$.
$(ii) ord_p(a+b)\geq min(ord_p(a),ord_p(b))$.
(iii)如果$ord_p(a)\neq ord_p(b)$,则$ord_p(a+b)=min(ord_p(a),ord_p(b))$.
定义有理数数列$(x_n)_{n\geq 1}$按p进收敛于有理数a为当$n\to\infty$时，$ord_p(x_n-a)\to\infty$.
以上"p进收敛"可以看成如下那样的“在度量空间中的收敛”：对于$a\neq 0$定义范数为

$$|a|_p=p^{-ord_p(a)},$$

$|0|_p=0$. 由此可以定义度量:令有理数a和b之间的距离为

$$d_p(a,b)=|a-b|_p,$$

可验证d_p满足正定性，对称性，三角不等式，于是(Q,d_p)成为度量空间.
像有理数集Q利用完备化得到实数集R那样，Q在距离d_p下也有完备化，记为Q_p,称之为p进数域，其子集

$$Z_p=\{a\in Q_p : ord_p(a)\geq 0\}.$$

中的元素叫做p进整数。

下面定义逆向极限

定义：当给出集合$X_n(n=1,2,\cdots,)$和映射$f_n:X_{n+1}\to X_n(n=1,2,\cdots,)$的系统

$$\cdots X_4\to X_3\to X_2\to X_1$$

时，称乘积集合$\prod_{n\geq 1}X_n$的子集合

$$\{(a_n)_{n\geq 1}\in\prod_{n\geq 1}X_n|\forall n\geq 1,f(a_{n+1})=a_n\}$$

为该系统的逆向极限(inverse limit)，记为$\lim\limits_{\leftarrow}X_n$.

在定义中，取$X_n=Z/p^nZ$,取f_n为从$Z/p^{n+1}Z$到Z/p^nZ的自然投射，系统

$$\cdots\to Z/p^4Z\to Z/p^3Z\to Z/p^2Z\to Z/pZ$$

的逆向极限为$\lim\limits_{\leftarrow}Z/p^nZ$.

命题1：(i)$Z_{(p)}\subseteq Z_p$,在Q_p中有$Q\cap Z_p=Z_{(p)}$.

(ii)设m是整数，则

$$p^mZ_p=\{a\in Q_p:ord_p(a)\geq m\}.$$

(iii)对于所有整数$m\geq 0$,有

$$Z/p^mZ\cong Z_{(p)}/p^mZ_{(p)}\cong Z_p/p^mZ_p.$$

(iiii)Z_p是Z在Q_p中的闭包。

证明：(i)由定义$Z_{(p)}=\{\frac{a}{b}:a,b\in Z,p\nmid b\}$，故显然有$Z_{(p)}\subseteq Z_p$,后半部分，可以证明等号两边相互包含，从而两者相等。

(ii)这是明显的。

(iii)对于第一个同构，考虑映射

$$\phi:Z_{(p)}\to Z/p^nZ:\frac{a}{b}\mapsto\frac{a\quad mod\quad p^n}{b\quad mod\quad p^n}(a,b\in Z,p\nmid b).$$

这里注意到$b\quad mod\quad p^n$是Z/p^nZ中可逆元，映射是满射:$\forall z\in Z/p^nZ,\phi(\frac{z}{1})=z$.再有

$$\phi(\frac{a}{b})=0\iff\frac{a\quad mod\quad p^n}{b\quad mod\quad p^n}=0\iff a\quad mod\quad p^n=0\iff\frac{a}{b}\in p^nZ_{(p)}$$

于是$ker(\phi)=p^nZ_{(p)}$.于是$Z_{(p)}/p^n\cong Z/p^nZ$.

对于第二个同构，注意到$Z_{(p)}\subset Z_p.Z_{(p)}\cap p^mZ_p=p^mZ_{(p)}$,故由嵌入诱导的映射$Z_{(p)}/p^mZ_{(p)}\to Z_p/p^mZ_p$为单射，另外设$a\in Z_p$,由于$Q$在$Q_p$中稠密，故存在$x\in Q$使得$ord_p(x-a)\geq m$.由于$x-a\in p^mZ_p,m\geq 0,a\in Z_p$,故$x\in Q\cap Z_p=Z_{(p)}$,因此$a=x+(a-x)\in Z_{(p)}+p^mZ_p$.从而上述映射是满射。

(iiii)用定义验证即可，可见Neukirch, Algebraic number theory p112.

命题2：

$$\lim_{\leftarrow}Z/p^nZ\cong Z_p.$$

证明:为此需构造两者的映射，首先给出映射$\lim\limits_{\leftarrow} Z/p^nZ \to Z_p$.对于每个$n \geq 1$,取整数$x_n$使得$x_n$的像为$a_n$,由于当$m,n \geq N$时$x_m \equiv x_n \mod p^N$(即$|x_m - x_n|_p \leq \frac{1}{p^N}$),故$(x_n)_{n\geq 1}$是个p进Cauchy序列，从而在$Q_p$中收敛.因为对所有的n,$ord_p(x_n) \geq 0$,所以这个极限属于$Z_p$.
下面对于每个正整数n考虑映射

$$Z_p \to Z_p/p^nZ_p \to Z_{(p)}/p^nZ_{(p)} \to Z/p^nZ$$

后三项由上命题知是同构的，其间的映射是同构映射。$\forall a \in Z_p$,由于Z在Z_p中稠密，从而存在$x \in Z$使得$ord_p(x-a) \geq n$,即$x - a \in p^nZ_p$.从而从而上述映射中具体元素对应为

$$a \mapsto x + p^nZ_p \mapsto x \mapsto \phi(x) = x \mod p^n, x \in Z$$

那么由于$a \equiv x \mod p^n, \phi(x) \equiv x \mod p^n$得到$a \equiv \phi(x) \mod p^n$.记$\psi_n(a) := \phi(x)$从而由此得到的序列$\{\psi_n(a)\}$收敛到$a$.这就证明了映射的合成 $Z_p \to \lim\limits_{\leftarrow} Z/p^nZ \to Z_p$是$Z_p$上的恒等映射。
设$\{x_n\} \in \lim\limits_{\leftarrow} Z/p^nZ$收敛到$s$,由于当$m \geq n$时$x_m \equiv x_n \mod p^n$，即$|x_m - x_n|_p \leq \frac{1}{p^n}$，固定n，令m趋于正无穷，由范数的连续性得到$|s - x_n|_p \leq \frac{1}{p^n}$,即 $x_n \equiv s \mod p^n$对任意n成立，于是在Z/p^nZ中$x_n = \psi_n(s)$.这说明复合映射$\lim\limits_{\leftarrow} Z/p^nZ \to Z_p \to \lim\limits_{\leftarrow} Z/p^nZ$是恒等映射。
该命题证明也可见Neukirch, Algebraic number theory p114.
上面两命题中，$Z_p/p^nZ_p \cong Z/p^nZ$也可直接证明得到：考虑映射$a \mapsto a \mod p^nZ_p$.其核为p^nZ_p.是满射，事实上，$\forall a \in Z_p$,由于Z在Z_p中稠密，从而存在$x \in Z$使得$ord_p(x-a) \geq n$,即$x-a \in p^nZ_p$.因此$Z_p/p^nZ_p \cong Z/p^nZ$.注意到$x \mapsto a$给出了逆映射。
p进数首先是由Hensel引进的，给出的定义为:
定义:对于每一素数p，p进整数是一个形式无穷级数

$$a_0 + a_1p + a_2p^2 + \cdots,$$

这里$0 \leq a_i < p, i = 0,1,2,\cdots$,所有p进整数组成的集合记为$Z_p$. 后文用到下面命题：
命题3：Z/p^nZ中剩余类$a \mod p^n$能被唯一表示成形式

$$a \equiv a_0 + a_1p + a_2p^2 + \cdots + a_{n-1}p^{n-1} mod \quad p^n$$

这里$0 \leq a_i < p, i = 0,\cdots,n-1$. 证明用数学归纳法。这里略去
对于每个整数，或更一般地，对于任意$f \in Z_{(p)}$.定义剩余类序列

$$\bar{s_n} = f \quad modp^n \in Z/p^nZ, n = 1,2,\cdots,$$

由上命题知$s_n = a_0 + a_1p + a_2p^2 + \cdots + a_{n-1}p^{n-1}, n = 1,2,...$,这定义了p进整数$\sum_{v=0}^{\infty} a_vp^v \in Z_p$.叫做f的p进展开，类似于洛朗级数，扩展p进整数到形式级数

$$\sum_{v=-m}^{\infty} a_vp^v = a_{-m}p^{-m} + \cdots + a_{-1}p^{-1} + a_0 + a_1p + \cdots,$$

这里$m \in Z, 0 \leq a_i < p$.这样的级数叫做p进数，所有这样数组成的集合记为Q_p. 有理数的p进展开给出了映射$Q \mapsto Q_p$,将Z映到Z_p内，若将Q与其像等同，则可写$Q \subseteq Q_p, Z \subseteq Z_p$.于是对于$f \in Q$，

有等式$f=\sum_{v=-m}^{\infty}a_vp^v$.
令$s_n=\sum_{v=0}^{n-1}a_vp^v\in Z$,其在$Z/p^nZ$中的剩余类记为$\bar{s_n}=s_n mod \quad p^n$.
命题4： $f=\sum_{v=0}^{\infty}a_vp^v\mapsto(\bar{s_n}=\sum_{v=0}^{n-1}a_vp^v mod \quad p^n)_{n\in N}$是$Z_p$到$\varprojlim Z/p^nZ$的双射。
证明由上命题立知。
由于$\varprojlim Z/p^nZ$是$\prod_{n=1}^{\infty}$的子环，从而通过同构可赋予Z_p环结构，使其成为环。因为任意$f\in Q_p$，f可表示成$f=p^{-m}g,g\in Z_p$,从而将加法乘法扩展到Q_p上，Q_p便成为Z_p的分式域。

2.2 赋值

下面讨论更一般域上的赋值，
定义：域K的一个**赋值**是一个函数

$$|\cdot|:K\to R$$

满足下面性质
(i)$|x|\geq 0$,若$|x|=0\iff x=0$,
(ii)$|xy|=|x||y|$,
(iii)$|x+y|\leq|x|+|y|$.
定义K中两点间的距离是

$$d(x,y)=|x-y|$$

这是K成为度量空间，因此也成为一拓扑空间。
定义：如果K的两个赋值诱导相同的拓扑空间，那么称它们是等价地。
命题：K的两个赋值$|\cdot|_1,|\cdot|_2$等价当且仅当存在实数$s>0$使得对任意$x\in K$有$|x|_1=|x|_2^s$.
证明略。
逼近定理：设$|\cdot|_1,\cdots,|\cdot|_n$是K的两两互不等价地赋值，任给$a_1,\cdots,a_n\in K$,那么对任意$\epsilon>0$,存在$x\in K$使得

$$|x-a_i|_i<\epsilon,\forall i=1,\cdots,n,$$

证明略。
定义：若对所有$n\in N$,赋值$|n|$有界，则称赋值是非阿基米德的，否则，称为阿基米德的。
命题：赋值是非阿基米德的当且仅当赋值满足强三角不等式

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

注记：由$|-x||-x|=|x^2|=|x||x|$得到$|-x|=|x|$.对于任意$|x|\neq|y|$,不妨设$|x|\leq|y|$.首先$|x+y|\leq max\{|x|,|y|\}=|y|$,其次 $|y|=|x+y-x|\leq max\{|x+y|,|-x|\}=max\{|x+y|,|x|\}$,由此推出$|x+y|=|y|=max\{|x|,|y|\}$.
命题:Q的每个赋值等价于赋值$|\cdot|_p$或$|\cdot|$,后者是通常的绝对值赋值。
证明略。
设$|\cdot|$是域K的非阿基米德赋值，令$v(x)=-log|x|(x\neq 0),v(0)=\infty$.我们得到函数$V:K\to R\cup\{\infty\}$,它满足下面性质
(i)$v(x)=\infty\iff x=0$.

(ii)v(xy)=v(x)+v(y),
(iii)$v(x+y) \geq min\{v(x), v(y)\}$,
这里我们约定对于$a \in R$,若$a<\infty, a+\infty = \infty, \infty+\infty = \infty$.
定义在K上且满足上面三个条件的函数叫做K的一个指数赋值。我们不考虑函数$v(x) = 0(x \neq 0), v(0) = \infty$.
K的两个指数赋值v_1, v_2叫做等价的:若$v_1 = sv_2, 0 < s \in R$. 对于每个指数赋值v，我们可以通过令$|x| = q^{-v(x)}$得到一个赋值，这里q是大于1的实数。为了与v区分，我们称$|\cdot|$叫做相应的乘法赋值，或者绝对值赋值。由上注记知，$v(x) \neq v(y) \Longrightarrow v(x+y) = min\{v(x), v(y)\}$
命题: (i)$o = \{x \in K|v(x) \geq 0\} = \{x \in K||x| \leq 1\}$是K的子环;(ii)其全体可逆元为$o^* = \{x \in K|v(x) = 0\} = \{x \in K||x| = 1\}$,(iii)唯一的极大理想是$\mathfrak{p} = \{x \in K|v(x)>0\} = \{x \in K||x|<1\}$.
证明：(1)是显然的（(ii)注意对任意$0 \neq x \in K, v(x^{-1}) = -v(x)$(iii)这是因为$o - \mathfrak{p} = o^*$.而$o^*$中元素是可逆元。
上面的o是整环，K是其分式域，且有对任意$x \in K$,有$x \in o$或者$x^{-1} \in o$.这样的环叫做赋值环。它唯一的极大理想是$\mathfrak{p} = \{x \in o|x^{-1} \notin o\}$.域$o/\mathfrak{p}$叫做o的剩余类域。赋值环是整闭的：若$x \in K$在o上是整的，则有方程式

$$x^n + a_1x^{n-1} + \cdots + a_n = 0, a_i \in o$$

假设$x \notin o$,那么$x^{-1} \in o$,从而$x = -a_1 - a_2x^{-1} - \cdots - a_n(x^{-1})^{n-1} \in o$,矛盾，这说明$x \in o$.
指数赋值v称为离散的,如果存在正实数s,使得$v(K^*) = sZ$.如$s = 1$,则称为正则的，通过除以s,我们总可以由离散赋值得到正则离散赋值，这不改变$o, o^*, \mathfrak{p}$.假设已经这样做了,o中元素$\pi \in o, v(\pi) = 1$叫做素元，任意元素$x \in K^*$有唯一的分解

$$x = u\pi^*, m \in Z, u \in o^*$$

这是因为若$v(x) = m$,那么$v(x\pi^{-m}) = 0$,因此$u = x\pi^{-m} \in o^*$.
命题:如果v是K的一个离散指数赋值，那么

$$o = \{x \in K|v(x) \geq 0\}$$

是主理想整环，因此是离散赋值环(其定义是:有唯一极大理想的主理想整环)
假设v是正则的，那么o的非零理想由

$$\mathfrak{p}^n = \pi^n o = \{x \in K|v(x) \geq n\}, n \geq 0$$

给出，这里π是素元，即$v(\pi) = 1$.有

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong o/\mathfrak{p}.$$

证明:设$\mathfrak{a} \neq 0$是o的一个理想，$x \neq$是o中具有最小赋值的元素，设$v(x) = n$.那么$x = u\pi^n, u \in o^*$,于是$\pi^n o \subseteq \mathfrak{a}$.如果$y = \epsilon\pi^m \in \mathfrak{a}, \epsilon \in o^*$是$\mathfrak{a}$中任意元素，那么$m = v(y) \geq n$,因此$y = (\epsilon\pi^{m-n})\pi^n \in \pi^n o$,因此$\mathfrak{a} = \pi^n o$.同构

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong o/\mathfrak{p}$$

来自于映射$a\pi^n \mapsto a \quad mod \quad \mathfrak{p}$.
在离散赋值域K中，链

$$o \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \cdots .$$

组成了零元素的邻域基。事实上，如果v是正则离散赋值，$|\cdot| = q^{-v}(q > 1)$是相应的乘法赋值，那么

$$\mathfrak{p}^n = \{x \in K||x|<\frac{1}{q^{n-1}}\}.$$

相似的1在K^*有链

$$o^* \supseteq U^{(0)} \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \cdots .$$

组成邻域基。这里

$$U^{(n)} = 1 + \mathfrak{p}^n = \{x \in K^*||1-x|<\frac{1}{q^{n-1}}\}, n > 0$$

注意到$1+\mathfrak{p}^n$在乘法运算下是闭的:如果$x \in U^{(n)}$,那么$|1-x^{-1}| = |x|^{-1}|x-1| = |1-x|<\frac{1}{q^{n-1}}$，于是$x^{-1} \in U^{(n)}$. **命题:**对于$n \geq 1$,$o^*/U^{(n)} \cong (o/\mathfrak{p}^n)^*$.($(o/\mathfrak{p}^n)^*$表示$o/\mathfrak{p}^n$的乘法群.) $U^{(n)}/U^{(n+1)} \cong o/\mathfrak{p}$.
证明:第一个同构由

$$o^* \to (o/\mathfrak{p}^n)^*, u \mapsto u \quad mod \quad \mathfrak{p}^n,$$

诱导，易见映射是满射，若$u \in o^*$，且$u \equiv 1 \quad \mathfrak{p}^n$,则$u \in 1+\mathfrak{p}^n = U^{(n)}$.从而该映射核为$U^{(n)}$.
对于第二个同构，一旦选定素元π，映射

$$U^{(n)} = 1 + \pi^n o \to o/\mathfrak{p}, 1 + \pi^n a \mapsto a \quad mod \quad \mathfrak{p},$$

的核为$U^{(n+1)}$,且为满同态。

2.3 完备化

开头先写下上节中的一些记号，下面将用到

$$o = \{x \in K|v(x) \geq 0\} = \{x \in K||x| \leq 1\},$$

$$o^* = \{x \in K|v(x) = 0\} = \{x \in K||x| = 1\},$$

$$\mathfrak{p} = \{x \in K|v(x)>0\} = \{x \in K||x|<1\}.$$

定义：赋值域$(K, |\cdot|)$称为完备的，若K中每个Cauchy列$\{a_n\}_{n\in\mathbb{N}}$收敛到K中元素a,即$\lim_{n\to\infty} |a_n - a| = 0$.
对于任何赋值域$(K, |\cdot|)$，我们可以通过完备化得到完备域$(\widehat{K}, |\cdot|)$.若$(\widehat{K'}, |\cdot|')$是一个以K为稠密子集的完备域，则存在K-同构

$$\sigma : \widehat{K} \to \widehat{K'}$$

$$|\cdot| - \lim_{n\to\infty} a_n \mapsto |\cdot|' - \lim_{n\to\infty} a_n$$

其中$|\cdot|-\lim\limits_{n\to\infty} a_n$表示$\{a_n\}$在$\widehat{K}$中的极限，$|\cdot|'-\lim\limits_{n\to\infty} a_n$表示$\{a_n\}$在$\widehat{K'}$中的极限。这样$|a|=|\sigma a|'$.这里注意完备域中的范数是由原范数的扩张。

定理(Ostrowski)设K是具有阿基米德赋值$|\cdot|$的完全域，那么存在从K到$\mathbb{R}$或$\mathbb{C}$的的同构σ满足

$$|a|=|\sigma a|^s,\forall a\in K$$

这里常数$s\in(0,1]$.

可以说上述定理已经说明了具有阿基米德赋值的完备域的结构，下面我们将聚焦于域的非阿基米德赋值，为了方便考虑指数赋值，设v是域K的指数赋值，$\widehat{K}$是K的完备化，$\forall a\in\widehat{K}$,令$\widehat{v}(a)=\lim\limits_{n\to\infty} va_n$,这里$a=\lim\limits_{n\to\infty} a_n\in\widehat{K},a_n\in K$.于是获得$\widehat{K}$的一个指数赋值。这里注意到，存在$n_0$,使得当$n>n_0$时，$\widehat{v}(a-a_n)>\widehat{v}(a)(\lim\limits_{n\to\infty} a_n=a,v(0)=\infty)$.由上节的注记知$v(a_n)=\widehat{v}(a_n-a+a)=min\{\widehat{v}(a_n-a),\widehat{v}(a)\}=\widehat{v}(a)$.因此$v(K^*)=\widehat{v}(\widehat{K^*})$.进而有若$v$是正则离散的，$\widehat{v}$也是正则离散的.

与$(\mathbb{Q},v_p)$类似，有下面命题.

命题$o\subseteq K,\widehat{o}\subseteq\widehat{K}$分别是关于$v,\widehat{v}$的赋值环，$\mathfrak{p},\widehat{\mathfrak{p}}$是极大理想，那么有

$$\widehat{o}/\widehat{\mathfrak{p}}\cong o/\mathfrak{p}$$

并且若v是离散的，进一步有

$$\widehat{o}/\widehat{\mathfrak{p}}^n\cong o/\mathfrak{p}^n,n\geq 1.$$

证明：考虑映射$o\to\widehat{o}/\widehat{\mathfrak{p}},x\mapsto x\mod\widehat{\mathfrak{p}}$,该映射核为$\mathfrak{p}$,且为满射，事实上，任意$x\in\widehat{o}$,存在$a\in o$使得$\widehat{v}(x-a)>0$,即$x-a\in\widehat{\mathfrak{p}}$,从而$x\equiv a\mod\widehat{\mathfrak{p}}$,此即证明满射。

若v是离散的，即$v(K^*)=sZ$,不妨设$s=1$,若不然，则考虑赋值v/s,总可化为正则离散赋值，此时，由上节命题知，$\mathfrak{p}^n=\pi^n o=\{x\in K|v(x)\geq n\},n\geq 0$,这里$\pi$是o中素元，即$v(\pi)=1$.注意到$\pi$同样也是$\widehat{K}$中素元，$\widehat{v}(\pi)=1$,同样$\widehat{\mathfrak{p}}^n=\pi^n\widehat{o}=\{x\in\widehat{K}|\widehat{v}(x)\geq n\}$.像上一部分那样可证明映射

$$o\to\widehat{o}/\widehat{\mathfrak{p}}^n$$

$$x\mapsto x\mod\widehat{\mathfrak{p}}^n$$

是满射，且核为$\mathfrak{p}^n$.

若v是K的离散赋值，我们有下命题。

命题：设$R\subseteq o$是陪集$\kappa=o/\mathfrak{p}$的所有代表元组成的集合，且$0\in R$,$\pi\in o$是素元，那么对于任意$0\neq x\in\widehat{K}$,存在唯一的收敛级数表示

$$x=\pi^m(a_0+a_1\pi+a_2\pi^2+\cdots),a_i\in R,a_0\neq 0,m\in\mathbb{Z}.$$

证明：设$x=\pi^m u,u\in\widehat{o}^*$,由于上面命题知$\widehat{o}=o+\widehat{\mathfrak{p}}$,因此存在$a\in o,b\in\widehat{o}$使得$x=a+\pi b$,取$a_0\in R$使得$a=a_0+\pi b',b'\in o$则$x=a_0+\pi(b'+b)$, 令$b_1=b'+b$,则$x=a_0+\pi b_1,a_0\in R,b_1\in\widehat{o}$, 注意到由于$u\in\widehat{o}^*$,则$a_0\neq 0$,否则$u=\pi b_1\in\widehat{\mathfrak{p}}$，矛盾！再注意到$R\cap\widehat{\mathfrak{p}}=\{0\}$(注意两者中元素的指数赋值)，从而上述表法唯一。

下面假设$a_0,\cdots,a_{n-1}\in R$已经确定，使得

$$u=a_0+a_1\pi+\cdots+a_{n-1}\pi^{n-1}+\pi^n b_n,b_n\in\widehat{o}$$

且a_i是唯一的，和上面一样，b_n能被唯一的写成$b_n = a_n + \pi b_{n+1}, b_{n+1} \in \hat{o}$. 因此

$$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + \pi^n a_n + \pi^{n+1} b_{n+1}$$

继续下去，我们可得到唯一的级数$\sum_{v=0}^{\infty} a_v \pi^v$,且收敛到$u$(注意到余项$\pi^{n+1}b_{n+1}$收敛到0).
对于每个n，有自然同态$o \longrightarrow o/\mathfrak{p}^n$并且有同态链

$$o/\mathfrak{p} \longleftarrow o/\mathfrak{p}^n \longleftarrow o/\mathfrak{p}^3 \longleftarrow \cdots,$$

逆极限是$\lim\limits_{\leftarrow n} o/\mathfrak{p}^n = \{(x_n) \in \prod_{n=1}^{\infty} o/\mathfrak{p}^n | \lambda_n(x_{n+1}) = x_n\}$. 这里$\lambda_n$是自然同态。我们有下面命题
命题：同态$o \longrightarrow \lim\limits_{\leftarrow n} o/\mathfrak{p}^n, o^* \longrightarrow \lim\limits_{\leftarrow n} o^*/U^{(n)}$是同构。
证明：映射是单射是由于$\cap_{n=1}^{\infty}\mathfrak{p}^n = \{0\}$,下面证明满射，由上一命题证明过程知，元素$a \mod \mathfrak{p}^n$能被唯一表示成形式

$$a \equiv a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \mod \mathfrak{p}^n, a_i \in R$$

每个$s \in \lim\limits_{\leftarrow n} o/\mathfrak{p}^n$因此由求和式组成的序列

$$s_n = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}, n = 1, 2, \cdots,$$

组成，这里$a_i \in R$是固定的，因此s是$x = \lim_{n\to\infty} s_n = \sum_{v=0}^{\infty} a_v\pi^v \in o$的像。第二个同构是

$$o^* \cong (\lim_{\leftarrow n} o/\mathfrak{p}^n)^* \cong \lim_{\leftarrow n}(o/\mathfrak{p}^n)^* \cong \lim_{\leftarrow n} o^*/U^{(n)}.$$

我们的目标是研究完备赋值域K的有限扩张$L|K$,为此必需考虑代数方程的分解因式问题，下面设K是非阿基米德完备赋值域，o是赋值环，$\mathfrak{p}$是极大理想，即剩余类域为$\kappa = o/\mathfrak{p}$.定义多项式$f(x) = a_0 + a_1x + \cdots + a_nx^n \in o[x]$的范数为$|f| = max\{|a_0|, \cdots, |a_n|\}$，我们说$f(x)$是本原的，如果$f(x) \equiv 0 \mod \mathfrak{p}$,即$\exists a_i \notin \mathfrak{p}$也即是$|f| = max\{|a_0|, \cdots, |a_n|\} = 1$.
Hensel 引理:如果本原多项式$f(x) \in o[x]$有模$\mathfrak{p}$分解

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

其中$\bar{g}, \bar{h} \in \kappa[x]$是互素多项式，那么$f(x)$有因式分解$f(x) = h(x)g(x), g, h \in o[x]$且

$$deg(g) = deg(\bar{g}), g(x) \equiv \bar{g}(x) \quad \mathfrak{p}, h(x) \equiv \bar{h}(x) \mod \mathfrak{p}.$$

证明:设$d = deg(f), m = deg(\bar{g})$,那么$d - m \geq deg(\bar{h})$.设$g_0, h_0 \in o[x]$,且$g_0 \equiv \bar{g} \mod \mathfrak{p}, h_0 \equiv \bar{h} \mod \mathfrak{p}, deg(g_0) = m, deg(h_0) \leq d - m$.因为$(\bar{g}, \bar{h}) = 1$,存在多项式$a(x), b(x) \in o[x]$满足$ag_0 + bh_0 \equiv 1 \mod \mathfrak{p}$.从而两个多项式$f - g_0h_0, ag_0 + bh_0 - 1$均属于$\mathfrak{p}[x]$,令$\epsilon = max\{|f - g_0h_0|, |ag_0 + bh_0 - 1|\}$,若$\epsilon = 0$,那么$f = g_0h_0$,证毕，从而考虑$\epsilon \neq 0$,此时有两个多项式中的某个系数设为$\pi$,使得$|\pi| = \epsilon$.从而$\pi^{-1}(f - g_0h_0) \in o[x], \pi^{-1}(ag_0 + bh_0 - 1) \in o[x]$ (这里注意到若f_i是多项式$f - g_0h_0$的系数，那么$|\pi^{-1}f_i| = |\pi^{-1}||f_i| \leq |\pi^{-1}||\pi| = 1$,从而$\pi^{-1}f_i \in o$)
下面说明证明的想法，注意到若g和h若有以下形式

$$g = g_0 + p_1\pi + p_2\pi^2 + \cdots,$$

$$h = h_0 + q_1\pi + q_2\pi^2 + \cdots ,$$

这里$p_i, q_i \in o[x]$且$deg(p_i) < m, deg(q_i) \leq d - m$.我们下面逐步决定多项式$g_{n-1} = g_0 + p_1\pi + \cdots + p_{n-1}\pi^{n-1}, h_{n-1} = h_0 + q_1\pi + \cdots + q_{n-1}\pi^{n-1}$,那么$f \equiv g_{n-1}h_{n-1} \mod \pi^n$(意思是存在多项式$k(x) \in o[x]$使得$f - g_nh_n = \pi^n k(x)$.)令n趋于无穷大，则$f = gh$.
下面我们便开始构造上述形式，对于n=1,由上分析已经存在(即$f - g_0h_0 = (\pi^{-1}(f - g_0h_0))\pi$)。
设我们已经对于n证明了上式$f \equiv g_{n-1}h_{n-1} \mod \pi^n$.下面我们用待定系数确定$p_n, q_n$. 设$g_n = g_{n-1} + p_n\pi^n, h_n = h_{n-1} + q_n\pi^n$,那么$f_n - g_nh_n \equiv (g_{n-1}q_n + h_{n-1}q_n\pi^n) \mod \pi^{n+1}$.两边整除$\pi^n$,得到

$$g_{n-1}q_n + h_{n-1}p_n \equiv g_0q_n + h_0p_n \equiv f_n \mod \pi$$

这里$f_n = \pi^{-n}(f - g_{n-1}h_{n-1}) \in o[x]$.因为$g_0a + h_0b \equiv 1 \mod \pi$.因此有

$$g_0af_n + h_0bf_n \equiv f_n \mod \pi.$$

由于$g_0 \equiv g \mod \mathfrak{p}$且$deg(g_0) = deg(\bar{g})$得到$g_o$的最高项系数是o中可逆元，从而类似于域中带余除法存在$q(x) \in o[x], p_n \in o[x]$使得$b(x)f_n(x) = q(x)g_0(x) + p_n(x), deg(p_n) < deg(g_0) = m$(这里只需回忆带余除法的证明过程即知)，于是

$$g_0(af_n + h_0q) + h_0p_n \equiv f_n \mod \pi$$

省略$af_n + h_0q$中能被π的整除的系数得到多项式q_n.那么$g_0q_n + h_0p_n \equiv f_n \mod \pi$,这里由于$deg(f_n) \leq d, deg(h_0p_n) < (d - m) + m = d, deg(g_0) = m$得到$deg(q_n) \leq d - m$.证毕。
例：多项式$x^{p-1} - 1 \in \mathbb{Z}_p[x]$在剩余类域$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$分解成不同的线性因此，因此由Hensel引理,它在$\mathbb{Z}_p$中也分解成不同的线性因子，从而$\mathbb{Q}_p$包含(p-1)次单位根。
推论：设域K是非阿基米德赋值$|\cdot|$完备域,对于每个不可约多项式$f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x], a_0a_n \neq 0$,那么$|f| = max\{|a_0|, |a_n|\}$.特别地，$a_n = 1, a_0 \in o$暗示$f \in o[x]$.
证明:乘以K中合适的元素，我们就可以假设$f \in o[x], |f| = 1$.设a_r是$a_0, \cdots, a_n$中第一个使得$|a_r| = 1$的系数，那么我们有

$$f(x) \equiv x^r(a_r + a_{r+1}x + \cdots + a_nx^{n-r}) \quad mod \mathfrak{p}.$$

如果$max\{|a_0|, |a_n|\} < 1$,那么$0 < r < n$,这与Hensel引理矛盾。
从这个推论中我们能导出下面赋值扩张的定理

3 抽象类域论

3.1 无限Galois扩张

设$K|k$是无限Galois扩张，一般我们就取K是k的代数闭包。记$G = Gal(K|k)$,对于中间域$k \subset E \subset K$记$H_E = Gal(K|E)$.定义集合 $\mathcal{I} = \{E : E$是$K|k$的中间域，且$E|k$是有限Galois扩张$\}$. $\mathcal{N} = \{H : H = Gal(K|E), E \in \mathcal{I}\}$.

命题1：(1) $\cap_{H\in\mathcal{N}} H=\{e\}$.(2) $\cap_{H\in\mathcal{N}}\sigma H=\{\sigma\}(\forall\sigma\in G)$.
证明：(1)任取$\sigma\in\cap_{H\in\mathcal{N}}H$,对任意$\alpha\in K$，设$E$是$k(\alpha)|k$在$K|k$中的正规闭包，则$E\in\mathcal{I},H_E=Gal(K|E)\in\mathcal{N}$,特别地$\sigma\in H_E$,对$\alpha\in E,\sigma(\alpha)=\alpha$,即$\sigma$在$K$是恒等映射.
(2)$\cap_{H\in\mathcal{N}}\sigma H=\sigma\cap_{H\in\mathcal{N}} H=\sigma$.
命题2：设$H_1,H_2\in\mathcal{N}$,则$H_1\cap H_2\in\mathcal{N}$.
证明：由$\mathcal{N}$的定义，存在$E_1,E_2\in\mathcal{I}$使得$H_1=Gal(K|E_1),H_2=Gal(K|E_2)$.由于$E_1E_2|k$是有限Galois扩张$E_1E_2\in\mathcal{I}$.由Galois理论知$H_1\cap H_2=Gal(K|E_1E_2)$于是$H_1\cap H_2\in\mathcal{N}$.
定义G上的$Krull$拓扑：规定$\{\sigma H:\sigma\in G,H\in\mathcal{N}\}$为$G$上的一个拓扑基。即$G$中子集$H'$为开集当且仅当$H'$为上述拓扑基元素之并。
定理:G在上述拓扑基下为Hausdorff,紧致且完全不连通的拓扑群。
证明:(i)完全不连通。
设$X\subset G$,且$|X|\geq 2$,取$\sigma,\tau\in X$,且$\sigma\neq\tau$. 由$\cap_{H\in\mathcal{N}}\sigma H=\{\sigma\}$知$\tau\notin\cap_{H\in\mathcal{N}}\sigma H$,从而$\exists H_0\in\mathcal{N}$使得$\tau\notin\sigma H_0$,即 $\tau\in G-\sigma H_0$ 注意到

$$X=X\cap G=X\cap(\sigma H_0\cup(G-\sigma H_0))=(X\cap\sigma H_0)\cup(X\cap(G-\sigma H_0))$$

G关于子群H有陪集分解$G=\cup_{i\in I}\sigma_i H$,由此知若$H$是开集，由于$G$是拓扑群，对任意$\sigma\in G$,$\sigma H$为开集，从而$H$为其所有非平凡陪集的补集，为闭集。注意到$\sigma\in X\cap\sigma H_0,\tau\in X\cap(G-\sigma H_0)$,且$\sigma H_0,G-\sigma H_0$均为开集，这就得到$X$是完全不连通的。特别地，$G$是完全不连通的，此处还可以看出，$G$是hausdo
间。

另证:若$\sigma,\tau\in G$且$\sigma\neq\tau$,则存在有限Galois子扩张$E|k$使得$\sigma|_E\neq\tau|_E$(注意到任取$x\in K$,必存在包含x的$K|k$的有限Galois子扩张$E|k$,例如E取$k(x)|k$在$K|k$中的代数闭包。若对任意有限Galois子扩张$E|k$有$\sigma|_E=\tau|_E$,则对任意$x\in K,\sigma(x)=\tau(x)$.矛盾！)因此$\sigma Gal(K|E)\neq\tau Gal(K|E)$,因此$\sigma Gal(K|E)\cap\tau Gal(K|E)=\emptyset$.
对于G的紧性,较快的证明需用逆向极限，这里先不证明。

注:设G关于闭子群H有陪集分解$G=\cup_{i\in I}\sigma_i H$，则由$G$的紧致性,$H$是$G$的开子集当且仅当$(G:H)$有限。
定理：设$H\leq G$,记$H'=Gal(K|K^H)$,则$H'=\bar{H}$(H在G中的闭包.)
证明:显然，$H\leq H'$.下证H'为G中的闭集,只需证$G-H'$为开集.

任取$\sigma\in G-H'$,必有$\alpha\in K^H$使得$\sigma(\alpha)\neq\alpha$.对于$\alpha\in K$,有$E\in\mathcal{I}$使得$\alpha\in E$,于是取$H_0=Gal(K|E)\in\mathcal{N}$.对于$\forall\tau\in H_0$,有$\tau\alpha=\alpha$,于是$\sigma(\tau\alpha)=\sigma\alpha\neq\alpha$,即

$$\sigma\tau(\alpha)\neq\alpha\Rightarrow\sigma\tau\in G-H'\Rightarrow\sigma H_0\in G-H'\Rightarrow G-H\quad is\quad open\Rightarrow H'is\quad closed.$$

下证$\bar{H}=H'$.需证$\forall\sigma\in H',N\in\mathcal{N}$.都有$\sigma N\cap H\neq\emptyset$.
由定义，取$E\in\mathcal{I}$使得$N=Gal(K|E)$,令$H_0=\{\rho|_E:\rho\in H\}$,于是$K^{H_0}=K^H\cap E$,由有限Galois基本定理到$H_0=Gal(E|K^H\cap E)$,由$\sigma\in H',\sigma|_{K^H}=id$,因此$\sigma|_E\in H_0$.存在$\rho\in H$使得$\rho|_E=\sigma|_E$.于

是$\sigma^{-1}\rho \in Gal(K|E) = N$，即$\rho \in \sigma N \cap H.\sigma N \cap H \neq \emptyset$.

命题：设$K|k$是无限Galois扩张，任取$K|k$的一个中间域，则$H_E = Gal(K|E)$是G的一个闭子群。

证：$H_E \leq G$,则$K^{Gal(K|E)} = E \Rightarrow H_E = Gal(K|E) = Gal(K|K^{H_E}) = \bar{H_E}$.

无限Galois扩张基本定理:设$K|k$是无限Galois扩张，令$G = Gal(K|k)$,

3.2 Hilbert定理90和群的上同调

设K是一个域，G为群，交叉态射$f : G \to K^*$是指一个函数f满足对任意的$\sigma, \tau \in G, f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau))$.

定义：设G是一个群,K是域，一个特征是一个从G到K^*的群同态。

若令上面定义中$G = K^*$,我们能看出任何一个域K关于其子域F的$F-$自同态都是一个特征。

Dedekind引理:设$\tau_1, \cdots, \tau_n$是G到K^*的n个不同的特征。则τ_i在K上是线性独立的；即若$\sum_i c_i\tau_i(g) = 0 (c_i \in K)$对任意$g \in G$成立，则$c_i = 0$.

证明略。可查阅相关代数书。

命题:设$K|F$是Galois扩张，令$G = Gal(K|F)$,设$f : G \to K^*$是交叉态射，则存在$a \in K$使得对任意$\sigma \in G$有$f(\tau) = \tau(a)/a$.

证明:因$f(\sigma) \neq 0$对任意$\sigma \in G$成立,故由Dedekind无关性引理存在$c \in K$,使得$\sum_{\sigma \in G} f(\sigma)\sigma(c) \neq 0$.令 $b = \sum_{\sigma \in G} f(\sigma)\sigma(c)$. 则$\tau(b) = \sum_{\sigma \in G} \tau(f(\sigma))(\tau\sigma)(c)$,于是

$$f(\tau)\tau(b) = \sum_{\sigma \in G} f(\tau)\tau(f(\sigma))(\tau\sigma)(c) = \sum_{\sigma \in G} f(\tau\sigma)(\tau\sigma)(c) = b.$$

此即$f(\tau) = b/\tau(b)$.令$a = b^{-1}$即得到结论。

Hilbert定理90:设$K|F$是循环Galois扩张，σ是$Gal(K|F)$的生成元。若$u \in K$,则$N_{K|F}(u) = 1$当且仅当存在$a \in K$使得$u = \sigma(a)/a$成立.

证明:有一侧是显然的。若$u = \sigma(a)/a$,则$N_{K|F}(\sigma(a)) = N_{K|F}(a)$,因此$N(u) = 1$. 反过来，如果$N_{K|F}(u) = 1$,定义映射$f : G \to K^*$, 令$f(id) = 1, f(\sigma) = u, f(\sigma^i) = u\sigma(u) \cdots \sigma^{i-1}(u) (i < n)$. 若说明$f$是交叉映射，则由上述命题，存在$a \in K$使得 $f(\sigma^i) = \sigma^i(a)/a$对所有$i$成立，从而$u = f(\sigma) = \sigma(a)/a$.

4 附录

4.1 Gauss互反律

设p是奇素数,a为不能被p除尽的整数;二次剩余记号$(\frac{a}{p}) \in \{1, -1\}$定义为当在$F_p$中存在a的平方根时(即$x^2 \equiv a \mod p$的整数x存在时)令$(\frac{a}{p}) = 1$,当其不存在时，$(\frac{a}{p}) = -1$.该记号称为Legendre记

号。满足的性质有
(i)$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} mod \quad p.$
(ii)$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}).$
(iii)(Gauss互反律.)对于两个不同的奇素数p, q,$(\frac{q}{p})(\frac{p}{q}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$
下面引入Hilbert记号。
首先做些准备.对于素数p,定义Q的子环$Z_{(p)}$为

$$Z_{(p)} = \{\frac{a}{b} : a, b \in Z, p \nmid b\}.$$

$Z_{(p)}$中的可逆元全体$(Z_{(p)})^{\times}$等于$\{\frac{a}{b} : p \nmid a, p \nmid b\}$.非零有理数可以唯一表示成$p^m u(m \in Z, u \in (Z_{(p)})^{\times})$. 对于素数p与$a, b \in Q^{\times}$,我们来定义Hilbert记号$(a, b)_p$.记

中国剩余定理：$A_1, \cdots, A_n$是环$\mathcal{O}$的理想，且有$A_i + A_j = \mathcal{O}, i \neq j$.令$A = \cap_{i=1}^n A_i$.则有

$$\mathcal{O}/A \cong \oplus_{i=1}^n \mathcal{O}/A_i$$

证明即是考虑映射$\mathcal{O} \to \oplus_{i=1}^n \mathcal{O}/A_i, a \mapsto \oplus_{i=1}^n a \quad mod \quad a_i$.映射的核为$A = \cap_{i=1}^n A_i$,剩下只须证明是满射。
下面是一个类似的命题
命题：如果$A \neq 0$是$\mathcal{O}$的理想，那么

$$\mathcal{O}/A \cong \oplus_P \mathcal{O}_P/A\mathcal{O}_P = \oplus_{P \supseteq A} \mathcal{O}_P/A\mathcal{O}_P$$

证明：令$\bar{A_P} = \mathcal{O} \cap A\mathcal{O}_P$.除有限个素理想外，都有$P \not\supseteq A$,因此$A\mathcal{O}_P = \mathcal{O}_P$(两者相互包含),从而$\bar{A_P} = \mathcal{O}$,进一步分析可知$A = \cap_P \bar{A}_P = \cap_{P \supseteq A} \bar{A}_P$.事实上：任意$a \in \cap_P \bar{A}_P$,理想$B = \{x \in \mathcal{O} | xa \in A\}$不包含在任意极大理想中(事实上：对任意素理想P,$a \in \bar{A}_{P=} \mathcal{O} \cap A\mathcal{O}_P$,从而a可表示为$a = \frac{a'}{s_P}, a' \in A, s_P \notin P$,且有$s_P a = a' \in A$),上述将导致$B = \mathcal{O}, i.e, a = 1 \cdot a \in A.$
如果$P \supseteq A$,那么P是唯一一个包含$\bar{A}_P$的素理想(事实上:由于$P = \mathcal{O} \cap P\mathcal{O}_P$($\subseteq$是平凡的，反方向是由于若$\frac{q}{s} = a \in \mathcal{O} \cap P\mathcal{O}_P$,那么$q = sa \in P$,由于$s \notin P$,得到$a \in P$)$\bar{A}_P = \mathcal{O} \cap A\mathcal{O}_P \subseteq \mathcal{O} \cap P\mathcal{O}_P = P$)，从而任给两个不同的素理想$P, Q$,理想$\bar{A}_P + \bar{A}_Q$不包含在任何极大理想中，因此$\bar{A}_P + \bar{A}_Q = \mathcal{O}$.从而由中国剩余定理得到同构$\mathcal{O}/A \cong \oplus_{P \supseteq A} \mathcal{O}/\bar{A}_P$.再由于$\mathcal{O}/\bar{A}_P = \mathcal{O}_P/A\mathcal{O}_P$,即得到命题。