代数学指北

Muke

April 20, 2026

Contents

前言

统一度量衡：

- T_0 为拓扑区分点.
- T_1 为单点集是闭集.
- T_2 为开集分离点.
- T_3 为闭集与点分离+ T_0.
- $T_{3.5}$ 为完全正则+ T_0(也称为 Tychonoff 空间).
- T_4 为闭集分离 + T_1.

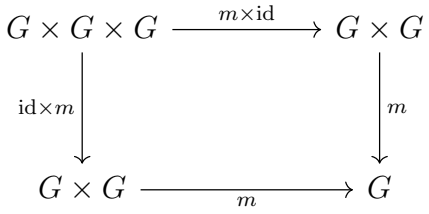
Chapter 1: 初等数学拾遗

1.1 拓扑群

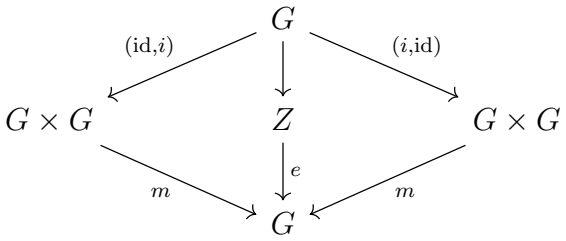
所谓拓扑群即拓扑空间范畴中的群对象，具体来说，在一个有终对象 Z 和有限乘积的范畴 $\mathscr{C}$ 中讨论的群对象包含如下资料，一个 $G \in \mathrm{ob}(\mathscr{C})$ 以及三个态射：

$$m\colon G \times G \to G, \quad i\colon G \to G, \quad e\colon Z \to G$$

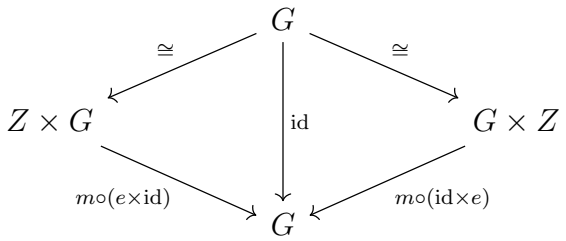
分别编码了群乘法，取逆和单位元，并且满足群公理(结合律，逆元律，幺元律). 我们可以用交换图来刻画这些律，结合律：



逆元律：



幺元律：



很显然拓扑空间范畴中的终对象就是单点空间，拓扑空间范畴中的群对象就是所谓拓扑群. 简单来说，拓扑群就是一个拓扑空间，带有群结构，并且满足群的乘法运算 $m\colon G \to G \to G, (g,h) \mapsto gh$ 与逆元运算 $i\colon G \to G, g \mapsto g^{-1}$ 都是连续的.

定义 1.1.1: 齐性空间

拓扑空间 X，若任意的 $a,b\in X$，存在 $\sigma\in \mathrm{Aut}(X)$，使得 $\sigma(a)=b$，则称 X 是**齐性空间**.

很显然拓扑群都是齐性空间，因为左右平移映射都是同胚. 要达成这个只需要看到

$$G\to G\times G\to G,\quad x\mapsto (x,s)\mapsto xs$$

为群乘法复合含入，从而连续，并且显然可见逆映射也是连续的，故同胚.

命题 1.1.1: 子集乘法相关

G 是拓扑群，A,B 是子集，则若 A 是开集，AB 与 BA 都是开集[a]；若 A 是闭集 B 是有限集，则 AB 和 BA 都是闭集；若 A,B 都是紧集，则 AB 是紧集[b].

[a]注意到 $AB=\bigcup_{b\in B} Ab$ 为开集的并.

[b]只需要看到 $A\times B$ 是紧集，而 AB 为 $A\times B$ 的群乘法连续像，所以紧.

由于拓扑群是齐性的，所以任意一个点处的邻域基本质上都可以有幺元处邻域基得到，所以我们很多时候只需要看幺元处邻域基满足什么性质就可以得到很多东西.

命题 1.1.2: 邻域开根号性质

给定 e 的一个开邻域 V，一定会存在 e 的另外一个开邻域 U 使得[a]

$$U^2:=\{u_1u_2\mid u_1,u_2\in U\}\subset V$$

我们还可以要求上面的“平方根”是对称的[b]，即 $U=U^{-1}$. 由此可以归纳地得到对任意 n，都存在对称的 e 的开邻域 U 使得 $U^n\subset V$.

[a]这一点是来自于群乘法在 $(e,e)\mapsto e$ 处的连续性.

[b]如 $U^2\subset V$，取 $U_0=U\cap U^{-1}$ 即可.

那群里面元素既然都可以取逆，现在给定一个 e 的邻域 U，我们能不能说 U^{-1} 也是 e 的一个邻域呢？这个是可以的，是拓扑群的定义中我们还有一条到现在都没有用过，即取逆的运算 i 是连续的，并且注意到 $i^{-1}=i$，所以 i 还是一个同胚，所以 i 把开集送到开集，于是我们知道

$$U^{-1}=i(U)$$

由左乘映射和右乘映射的同胚性质，我们知道对于 e 的邻域 U，有 $gUg^{-1}=R_{g^{-1}}\circ L_g(U)$ 也是 e 的邻域. 那么拓扑群既然是一个群，它的子群与商群扮演了一种什么样的角色呢？

定义 1.1.2: 开子群与闭子群

我们称一个子群 $H<G$ 是**开子群**，如果 H 作为 G 的一个子集是开集. **闭子群**同理定义.

对拓扑群而言，开子群与闭子群有很好的性质：

命题 1.1.3

所有开子群都是闭子群. 所有有限指数闭子群都是开子群. 含有幺元的任意一个邻域的子群一定是开的.

证明: 假设 $H<G$ 是开子群，要说明 H 是闭的只需要说明 $G\backslash H$ 是开的，考虑 G 对 H 的陪集分解

$$G/H=\bigcup_{i\in I}g_iH$$

其中 g_i 是一个陪集代表元系，并且不妨设 $g_1H=H$，则知

$$G\backslash H=\bigcup_{i\in I,i\neq 1}g_iH$$

由左乘映射是同胚，注意到对于任意的 g_i，都有 g_iH 是开集，所以 $G\backslash H$ 是一族开集的并，于是还是开集，故 H 是闭集，于是开子群同时也是闭子群. 后面命题同理可证. □

对于一般的 G 的子群，不一定是开的或者闭的，但是无论如何，我们都可以赋予子空间拓扑. 给定 $H<G$，我们可以给左陪集空间 G/H 赋予商拓扑 $\rho\colon G\to G/H$，即 $V\subset G/H$ 开当且仅当 $\rho^{-1}V$ 开，G/H 称为相对 H 的左陪集空间.

命题 1.1.4

$H<G$，则商映射 $\rho\colon G\to G/H$ 是开映射，并且 H 是开子群当且仅当 G/H 有离散拓扑.

证明: 只证明开映射，设 S 是 G 的开集，注意到

$$\rho^{-1}(\rho(S))=SH$$

是开集. □

如果给定 G 的一个正规子群 N，我们可以对商群 G/N 赋予商拓扑.

定理 1.1.1

G 是拓扑群，$N\lhd G$，则 G/N 是拓扑群.

命题 1.1.5: 拓扑群同态基本定理

$\varphi\colon G_1\to G_2$ 为拓扑群的开连续同态，则 $G_1/\operatorname{Ker}\varphi\cong\operatorname{Im}\varphi$ 为拓扑群同构.

命题 1.1.6

若 $H \leq L \leq G$，则 $(G/H)/(L/H) \cong G/L$.

一个很好的定理是：

定理 1.1.2: 紧的判定

G 是拓扑群，$H < G$，若 H 与 G/H 都是紧的，则 G 是紧的.

但是我们经常会遇到非紧的拓扑群，所以局部紧可能是更广泛的条件.

定理 1.1.3: 局部紧的刻画

G 是拓扑群，$H < G$，则

(1) G 局部紧 $\iff$ e 存在紧邻域.

(2) G 局部紧，H 闭 $\implies$ H 是局部紧的.

(3) G 局部紧 $\implies$ G/H 是局部紧的.

(4) G/H 与 H 都是局部紧的 $\implies$ G 是局部紧的.

现在我们可以考虑拓扑群的积，这里的积是作为拓扑空间的积.

命题 1.1.7: 拓扑群的积还是拓扑群

$\{G_i\}_{i\in I}$ 是一组拓扑群，则 $G = \prod_{i\in I} G_i$ 是拓扑群.

于是我们由点集拓扑知识立刻得到：

定理 1.1.4

$\{G_i\}_{i\in I}$ 是一组拓扑群，则

(1) $\prod_{i\in I} G_i$ 紧 $\iff$ 每个 G_i 都紧.

(2) $\prod_{i\in I} G_i$ 局部紧 $\iff$ 每个 G_i 都局部紧，并且除有限个以外都紧.

拓扑群的分离性有非常好的性质：

定理 1.1.5: 拓扑群的分离

拓扑群若 T_0 则 $T_{3.5}$. 若 G 的任意左陪集空间 G/H 是 T_0 则 T_3.

Hausdorff 是最基本的性质.

定理 1.1.6: 拓扑群的 Hausdorff 刻画

G 是拓扑群，$\mathscr{F}$ 是 e 的邻域基，*TFAE*:

(1) G 是 *Hausdorff* 空间.

(2) $\delta\colon G \to G\times G, x\mapsto (x,x)$ 是闭映射.

(3) $\{e\}$ 是闭集.

(4) $f\colon H\to G$ 是连续同态，则 $\operatorname{Ker} f$ 是 H 的闭集.

(5) $\bigcap\limits_{U\in\mathscr{F}} U=\{e\}$.

(6) e 的一切开邻域之交是 $\{e\}$.

命题 1.1.8

G，$\{G_i\}$ 都是拓扑群，$H<G$，则

(1) G 是 *Hausdorff* $\Longrightarrow$ H 是 *Hausdorff*.

(2) G/H 是 *Hausdorff* $\Longleftrightarrow$ H 是 G 的闭子群.

(3) H 和 G/H 都 *Hausdorff* $\Longrightarrow$ G 是 *Hausdorff*.

(4) $\prod\limits_{i\in I} G_i$ *Hausdorff* $\Longleftrightarrow$ 每个 G_i 都 *Hausdorff*.

下面我们谈连通性，由于开子群必为闭子群，有限指数闭子群必为开子群，所以：

命题 1.1.9

G 连通则没有真开子群或者有限指数的闭子群.

我们要了解商群与乘积的连通性.

命题 1.1.10: 连通

G, G_i 都是拓扑群，$H < G$，则

(1) G 连通 $\Longrightarrow$ G/H 连通.

(2) H 与 G/H 连通 $\Longrightarrow$ G 连通.

(3) $\prod_{i\in I} G_i$ 连通 $\Longleftrightarrow$ G_i 都连通.

我们记拓扑空间 X 在 x 点处的连通分支为 $\mathrm{Comp}(x)$. 熟知连通分支为非空闭集，并且所有分支构成 X 的分划. 若每个分支都只有一个点则称 X 是完全不连通的.

命题 1.1.11: 完全不连通

G, G_i 都是拓扑群，$H < G$，则

(1) G 完全不连通 $\Longrightarrow$ G/H 完全不连通.

(2) H 与 G/H 完全不连通 $\Longrightarrow$ G 完全不连通.

(3) $\prod_{i\in I} G_i$ 完全不连通 $\Longleftrightarrow$ G_i 都完全不连通.

下面是连通的主定理：

定理 1.1.7

G 是拓扑群，$G^0 = \mathrm{Comp}(e)$，则

(1) $G^0 \lhd G$ 是闭连通正规子群.

(2) G/G^0 是完全不连通的 *Hausdorff* 拓扑群.

(3) G^0 的全体陪集构成 G 的所有分支.

(4) G 的每个开子群都包含 G^0.

最后提一嘴拓扑群的作用.

定义 1.1.3: 拓扑齐性空间

G 作用在拓扑空间 M 上，若对任意的 $x \in M$，在 G 之下的轨道就是 M，则称 M 为相对于 G 的**拓扑齐性空间**.

我们可以很明显看到

$$G_x = \{s \in G \colon sx = x\}$$

为 x 处的稳定子群，若 $y = tx$，则

$$G_y = tG_xt^{-1}$$

这都与一般群作用并无二样.

命题 1.1.12

Hausdorff 空间 M 是拓扑群 G 上的齐性空间，$x \in M$，则 $G/G_x \to M, gG_x \mapsto gx$ 是连续映射.

命题 1.1.13

G 为局部紧群，若存在 G 的开子群 H 使得 G/H 可数，H/G^0 是紧集，则给定齐性的局部紧 *Hausdorff* 空间 M，有 M 与 G/G_x 同胚.

推论 1.1.1

G 为局部紧群，M 为齐性的局部紧 *Hausdorff* 空间，若 G 是紧群或者只有可数连通分支，则 $G/G_x \cong M$.

定义 1.1.4: 完全不连续

离散群 Γ 作用在拓扑空间 M 上，如果 Γ 中任意不同元素构成的序列 $\{\gamma_n\}$，满足对任意的 $x \in M$，$\{\gamma_n x\}$ 没有极限，则称 Γ 在 M 上的作用是**完全不连续**的.

定义 1.1.5: 基本区域

设离散群 Γ 作用在拓扑空间 M 上，T 在 M 上的作用**基本区域**是指 M 的子集 F，满足

(1) $\Gamma(F) = M$.

(2) $\forall \gamma \in \Gamma, \gamma \neq e$，$\gamma F \cap F = \emptyset$.

1.2 Haar测度与群上积分

1.3 群的合成列

1.4 可解群与幂零群

1.5 群的极限与完备化

1.6 环的极限与完备化

1.7 模的张量积

1.8 模的合成列

1.9 半单模

本节中约定 M 为非零的左 R-模，定义环 $A = \mathrm{End}_R(M)^{\mathrm{op}}$，则 M 对下述乘法自然成为右 A-模：

$$(m, a) \mapsto a(m), \quad m \in M, a \in A$$

这是因为

$$((m, a), b) \mapsto (a(m), b) \mapsto b(a(m)) = (b \circ a)(m) = (m, ab)$$

从而 M 构成了 (R, A)-双模，同理对右 R-模可做类似定义，此处不表. 若无特别说明，本节中所考虑的均为左 R-模.

1.10 分次代数

定义 1.10.1: 分次模与分次代数

令 I 为一个交换幺半群，以 $+$ 表二元运算，0 表幺元. 则交换环 R 上的**分次模**是配备直和分解的模 $M=\bigoplus_{i\in I}M_i$. 对两个分次模 M,N 而言，张量积诱导自然的分次结构

$$(M\otimes N)_k=\bigoplus_{i,j\in I,i+j=k}M_i\otimes N_j$$

称 $x\in M_i-\{0\}$ 为 M 中次数为 i 的**齐次元**，也即 $\deg(x)=i$，对 0 不定义次数，**分次子模**即 M 中满足

$$N=\bigoplus_{i\in I}(N\cap M_i)$$

的子模. 交换环 R 上的**分次代数**是配备直和分解的 R-代数 $A=\bigoplus_{i\in I}A_i$，其乘法满足 $A_i\cdot A_j\subset A_{i+j}$ 并且 $1\in A_0$. 因此 A_0 是子代数. 同态 $\varphi\colon A\to B$ 若想为分次代数的同态，需要满足 $\varphi(A_i)\subset B_i$. **分次理想**即 A 中满足 $\mathfrak{a}=\bigoplus_{i\in I}(\mathfrak{a}\cap A_i)$ 的理想，可见当 $\mathfrak{a}\neq A$ 时，$A/\mathfrak{a}=\bigoplus_i A_i/a\cap A_i$ 仍然是分次代数. 当 $(I,+)\subset(\mathbb{Z},+)$ 时称之为分次对象.

容易证明下面的引理：

引理 1.10.1: 分次结构由齐次元决定

I-分次代数(或分次模)中的双边理想(或子模)是分次的，当且仅当它能由齐次元生成.

1.11 张量代数

R 为交换环，本节中记 $\otimes:=\otimes_R$，定义模 M 的 n 重张量积为

$$T^n(M):=\underbrace{M\otimes\cdots\otimes M}_{n},\quad n\geq 1$$

$$T^0(M):=R$$

我们诱导出自然同态

$$\mu_{i,j}\colon T^iM\otimes T^jM\to T^{i+j}M$$

这是一个同构.

定义 1.11.1: 张量代数

定义 R-模 M 的**张量代数**为 $T(M) := \bigoplus_{n=0}^{\infty} T^n(M)$，其乘法和幺元分别由诸 $\mu_{i,j}$ 与 $R = T^0(M) \hookrightarrow T(M)$ 给出. 它带有自然的 R-模单同态 $M = T^1(M) \hookrightarrow T(M)$. 可见 $T(M)$ 为分次代数.

乘法在元素层面展开无非是

$$(x_1 \otimes \cdots \otimes x_n) \cdot (y_1 \otimes \cdots \otimes y_m) = x_1 \otimes \cdots \otimes x_n \otimes y_1 \otimes \cdots \otimes y_m$$

结合律由张量积的性质立刻得到，并且易见此等构造使得 T 与 T^n 均为函子.

定理 1.11.1: 张量代数的泛性质与伴随

张量代数满足如下泛性质：对任意 R-代数 A 与 R-模同态 $f\colon M \to A$，存在唯一的 R-代数同态 $\varphi\colon T(M) \to A$ 使得下图交换

$$\begin{array}{ccc} M & \longrightarrow & T(M) \\ & \searrow^{f} & \downarrow{\scriptstyle \exists!\varphi} \\ & & A \end{array}$$

换言之，函子间有伴随关系

$$T \dashv U$$

其中 U 是从 R-代数到 R-模的遗忘函子.

其证明是近乎显然的，同时近乎显然的是下面的论断：

命题 1.11.1: 张量代数的构造与基变换交换

对环同态 $R \to S$，存在唯一的分次 S-代数同构 $\psi_M\colon T(M \otimes S) \to T(M) \otimes S$，使得图表在 S-模中交换

$$\begin{array}{ccc} & M \otimes S & \\ \swarrow & & \searrow \\ T(M \otimes S) & \longrightarrow & T(M) \otimes S \end{array}$$

可见函子的同构 $T(- \otimes S) \cong T(-) \otimes S$.

由于 T 是左伴随，所以容易看见：

推论 1.11.1

存在分次代数的自然同构 $\varinjlim T(M_i) \cong T\left(\varinjlim M_i\right)$. 特别地，模的商同态 $M \twoheadrightarrow M/N$ 有

$$T(M) \to T(M)/\langle N\rangle \cong T(M/N)$$

其中 $\langle N\rangle$ 是 N 生成的齐次理想.

1.12 对称代数与外代数

定义 1.12.1: 对称代数与外代数

以齐次生成元定义 $T(M)$ 的双边分次理想

$$I_{\mathrm{Sym}}(M) := \langle x\otimes y - y\otimes x \colon x,y\in M\rangle$$

$$I_{\bigwedge}(M) := \langle x\otimes x \colon x\in M\rangle$$

对应的商代数有自然的分次结构:

$$\mathrm{Sym}(M) := T(M)/I_{\mathrm{Sym}(M)}$$

$$\bigwedge(M) := T(M)/I_{\bigwedge}(M)$$

分别称为 M 的**对称代数**与**外代数**.

我们知道有

$$I_{\mathrm{Sym}}(M) = \bigoplus_n I^n_{\mathrm{Sym}}(M)$$

$$I_{\bigwedge}(M) = \bigoplus_n I^n_{\bigwedge}(M)$$

有自然的分次结构，这些理想由二次齐次元生成，所以自然有从 $M\to T(M)$ 诱导的单同态

$$M\hookrightarrow \mathrm{Sym}(M),\quad M\hookrightarrow \bigwedge(M)$$

并且我们易见 Sym 与 $\bigwedge$ 是函子性的，对称代数的群乘法习惯写作

$$(x,y)\mapsto xy$$

当 $x,y\in M$ 时有 $xy=yx$，可见 $\mathrm{Sym}(M)$ 是 $T(M)$ 的交换化. 外代数的乘法习惯写作

$$(x,y)\mapsto x\wedge y$$

注意到对每个 $x,y\in M$，都有

$$x\otimes y + y\otimes x = (x+y)\otimes(x+y) - x\otimes x - y\otimes y \in I_{\mathrm{Sym}}(M)$$

所以可见

$$x \wedge y = -y \wedge x$$

可见 $\bigwedge(M)$ 是 $T(M)$ 的反交换化. 所以可以发现奇数次齐次元可表作 $\omega = \sum_{i=1}^{k} t_i \wedge \eta_i$，其中 $\deg(t_i) = 1$，$\deg(\eta_i) \in 2\mathbb{Z}$，反交换性告诉我们

$$\begin{aligned} \omega \wedge \omega &= \sum_{i,j} t_i \wedge \eta_i \wedge t_j \wedge \eta_j = \sum_{i,j} t_i \wedge t_j \wedge \eta_i \wedge \eta_j \\ &= \sum_{i} (t_i \wedge t_i) \wedge (\eta^i \wedge \eta_i) + \sum_{i<j} (t_i \wedge t_j + t_j \wedge t_i) \wedge (\eta_i \wedge \eta_j) \\ &= 0 + 0 = 0 \end{aligned}$$

Example 1.12.1

若 M 为秩 1 自由模 Rx，则作为分次代数有 $\mathrm{Sym}(M) = R[x]$ 而 $\bigwedge(M) = R \oplus Rx$.

由命题 1.11.1 我们自然可以得到下面的结论：

引理 1.12.1: 对称代数与外代数的构造与基变换交换

对环同态 $R \to S$，有

$$\mathrm{Sym}(- \otimes S) \cong \mathrm{Sym}(-) \otimes S, \quad \bigwedge(- \otimes S) \cong \bigwedge(-) \otimes S$$

并且该同构保持分次结构.

一如多元张量积，M 的 n-次对称幂与外幂也可以由泛性质刻画，令 A 为任意 R-模，令 A 为任意 R-模，令

$$\mathrm{Sym}(M \times n, A) := \{B \in \mathrm{Mul}(M, \cdots, M; A) \colon B(\cdots, x, y, \cdots) = B(\cdots, y, x, \cdots)\}$$

$$\mathrm{Alt}(M \times n, A) := \{B \in \mathrm{Mul}(M, \cdots, M; A) \colon B(\cdots, x, x, \cdots) = 0\}$$

为多重线性函数的子集，容易看出 S_n 会自然作用在其上为

$$(\sigma B)(x_1, \cdots, x_n) = B(x_{\sigma^{-1}(1)}, \cdots, x_{\sigma^{-1}(n)})$$

对 $B \in \mathrm{Sym}(M \times n, A)$，我们有

$$\sigma(B) = B$$

而对 $B \in \mathrm{Alt}(M \times n, A)$，我们有

$$\sigma(B) = \mathrm{sgn}(\sigma) B$$

当 $n = 0$ 的时候，定义 $\mathrm{Sym}(M \times 0, A) = \mathrm{Alt}(M \times 0, A) = A$，注意 $\mathrm{Sym}^0 = \bigwedge^0 = R$，我们会得到下面的命题：

命题 1.12.1

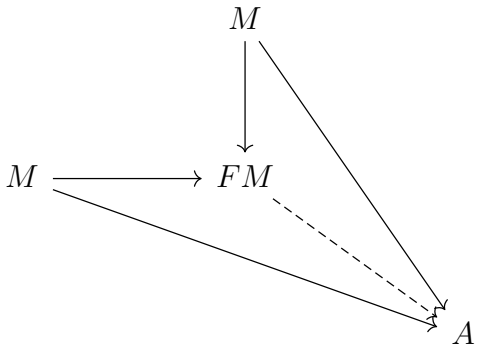
对任意 M 和 $n \geq 1$ 如上，我们有函子的同构

$$\mathrm{Hom}_{\mathbf{Mod}_R}(\mathrm{Sym}^n(M), -) \to \mathrm{Sym}(M \times n, -), \quad \varphi \mapsto ((x_1, \cdots, x_n) \mapsto \varphi(x_1 \cdots x_n))$$

与

$$\mathrm{Hom}_{\mathbf{Mod}_R}(\bigwedge^n(M), -) \to \mathrm{Alt}(M \times n, -), \quad \varphi \mapsto ((x_1, \cdots, x_n) \mapsto \varphi(x_1 \wedge \cdots \wedge x_n))$$

利用张量积的泛性质和各种定义其实立刻得到，上述定理在 $n = 2$ 的情况下本质上就是再说这个图：



其中箭头满足一定条件，F 取对称幂或者外幂.

令 $R - \mathbf{CAlg}_{\mathbb{Z}}$ 表示交换 $\mathbb{Z}$-分次 R-代数构成的范畴，$R - \mathbf{CAlg}^-_{\mathbb{Z}}$ 表示反交换，满足奇数次齐次元素的平方(外积意义下)为 0，的 $\mathbb{Z}$-分次 R-代数所成范畴，我们立刻导出如下结果：

定理 1.12.1: 对称代数与外代数是左伴随

模同态 $M \to \mathrm{Sym}(M)$ 与 $M \to \bigwedge(M)$ 诱导出函子的同构

$$\mathrm{Hom}_{R-\mathbf{CAlg}_{\mathbb{Z}}}(\mathrm{Sym}(-), -) \cong \mathrm{Hom}_{R-\mathbf{Mod}}(-, U(-))$$

$$\mathrm{Hom}_{R-\mathbf{CAlg}^-_{\mathbb{Z}}}(\bigwedge(-), -) \cong \mathrm{Hom}_{R-\mathbf{Mod}}(-, U(-))$$

所以可以看出这两种构造都是左伴随，所以保持余极限. 特别地，保持商结构.

1.13 行列式，迹与判别式

R 为交换环，本节中记 $\otimes := \otimes_R$，设 E 是秩 n 的自由 R-模，$n \in \mathbb{Z}_{\geq 0}$，我们知道

$$\bigwedge^{\max}(E) := \bigwedge^n(E)$$

是秩 1 自由 R-模，故其上的自同态必为纯量乘法 $x \mapsto rx$ 的形式，因而有

$$\mathrm{End}_R(\bigwedge^{\max}(E)) = R$$

此时如果我们考虑 $\varphi \in \mathrm{End}_R(E)$，由外幂的函子性立刻得到一个

$$\bigwedge^{\max}(\varphi)\colon \bigwedge^{\max}(E) \to \bigwedge^{\max}(E)$$

其具体作用为

$$\bigwedge^{\max}(\varphi)(x_1 \wedge \cdots \wedge x_n) = \varphi(x_1) \wedge \cdots \wedge \varphi(x_n)$$

我们就定义 φ 的**行列式**为

$$\det(\varphi) := \bigwedge^{\max}(\varphi) \in \mathrm{End}_R(\bigwedge^{\max}(E)) = R$$

若取定 E 的基 $x_1, \cdots, x_n$，并设

$$\varphi(x_j) = \sum_{i=1}^{n} a_{ij} x_i$$

那么利用反交换多重线性映射的性质可见

$$(\det \varphi)(x_1 \wedge \cdots \wedge x_n) = \left(\sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n} \right) x_1 \wedge \cdots \wedge x_n$$

于是你会发现在这个意义下

$$\det \varphi = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{\sigma(1)1} \cdots a_{\sigma(n)n}$$

而后者实际上就是是 $\det((a_{ij}))$，与我们熟知的矩阵行列式相容.

定理 1.13.1: 伴随矩阵

取定自由 R-模 E 的基 $x_1, \cdots, x_n$，我们可以将 $\mathrm{End}_R(E)$ 中的元素等同于 $M_n(R)$ 的元素，对每个 $A \in M_n(R)$ 定义其**伴随矩阵**为

$$A^\vee := (A_{ji})_{1 \le i,j \le n}, \quad A_{ij} = (-1)^{i+j} M_{ij}$$

M_{ij} 与 A_{ij} 即熟知的余子式与代数余子式，地我们有：

(1) $\varphi, \psi \in \mathrm{End}_R(M)$ 恒有 $\det(\varphi\psi) = \det(\varphi)\det(\psi)$，并且 $\det(\mathrm{id}_E) = 1$.

(2) 矩阵转置 $A \mapsto {}^tA$ 不改变行列式.

(3) 伴随矩阵满足 $AA\vee = \det(A) I_n = A \vee A$.

(4) 自同态 $\varphi \in \mathrm{End}_R(E)$ 可逆当且仅当 $\det \varphi \in R^\times$，此时相应的矩阵 A 满足 $A^{-1} = (\det A)^{-1} A^\vee$.

证明几乎是直白的但繁琐的，相信即可. 对任意的 R-模 M，若令 $E^\vee := \mathrm{Hom}_R(E, R)$，则有良定义的 R 模同态

$$\begin{array}{ccccc} R & \leftarrow & E^\vee \otimes E & \to & \mathrm{End}_R(E) \\ f(x) & \leftarrow\!\shortmid & f \otimes x & \mapsto & [v \mapsto f(v)x] \end{array}$$

设 E 为秩 n 自由模，我们知道 $E^\vee$ 也是秩 n 自由模，并且有

$$E^\vee \otimes E \cong \mathrm{End}_R(E)$$

实际上如果放在线性空间中即

$$\alpha^T \otimes \beta \in M_{n\times n}$$

我们无需选择基就可以对 $\varphi \in \mathrm{End}_R(E)$ 定义行列式，这在之前已经说过，同时我们还可以定义迹，定义为

$$\mathrm{tr}(\varphi) \in R$$

为 φ 在模同态

$$\mathrm{End}_R(E) \to E^\vee \otimes E \to R$$

下的像，最后可以定义特征多项式

$$\mathrm{char}(\varphi, X) := \det(X \cdot \mathrm{id} - \varphi) \in R[X]$$

这里将 φ 等同于 $\mathrm{End}_{R[X]}(E \otimes_R R[X])$ 中相应的元素. 在需要突出 E 或者 R 的地位时，我们就写作

$$\det_R(\varphi|E), \quad \mathrm{tr}_R(\varphi|E), \quad \mathrm{char}_R(\varphi|E)$$

对任意的 $\varphi, \psi \in \mathrm{End}_R(E)$，都有

$$\det(\varphi\psi) = \det(\varphi)\det(\psi), \quad \det(\mathrm{id}_E) = 1, \det(0) = 0$$

$$\det(r\varphi) = r^n \det(\varphi), \quad r \in R$$

$$\mathrm{tr}(r\varphi + s\psi) = r\,\mathrm{tr}(\varphi) + s\,\mathrm{tr}(\psi), \quad r, s \in R$$

$$tr(\mathrm{id}) = n$$

下面考虑 R-代数 A 并且假设 A 是有限秩的自由 R-模.

定义 1.13.1: 范数与迹

对如上的 A 与 $a \in A$，我们可以定义自同态 $m_a \in \mathrm{End}_R(A)$ 为左乘 $x \mapsto ax$，并定义 a 的迹 $\mathrm{tr}_{A/R}(a)$ 与范数 $N_{A/R}(a)$ 还有特征多项式 $\mathrm{char}_{A/R}(a, X)$ 为

$$\mathrm{tr}_{A/R}(a) := \mathrm{tr}(m_a), \quad N_{A/R}(a) := \det(m_a)$$

$$\mathrm{char}_{A/R}(a, X) := \mathrm{char}(m_a, X) = \det_{R[X]}(m_{X-a}|A[X]) = N_{A[X]/R[X]}(X - a)$$

我们很容易看到下面的引理.

引理 1.13.1: 秩的传递性

设 A 为交换 R-代数，E 为自由 A-模，若将 A 视为自由 R-模，则 E 视为自由 R-模也是自由的，若取 E 在 A 上的基 $(e_i)_{i\in I}$ 与 A 在 R 上的基 $(a_j)_{j\in I}$，则 $(e_i a_j)_{i\in I, j\in J}$ 构成 E 在 R 上的基，因此

$$\mathrm{rank}_R(E) = \mathrm{rank}_R(A)\mathrm{rank}_A(E)$$

由此我们有

定理 1.13.2: 行列式与迹的传递性

设 A 为交换 R-代数，同时是有限秩自由 R-模，E 为一个有限秩 A-模，将给定的 $\varphi \in \mathrm{End}_A(E)$ 看做 $\mathrm{End}_R(E)$ 的元素，则

$$\mathrm{tr}_R(\varphi) = \mathrm{tr}_{A/R}(\mathrm{tr}_A(\varphi)), \quad \det_R(\varphi) = N_{A/R}(\det_A(\varphi))$$

$$\mathrm{char}(\varphi, X) = N_{A[X]/R[X]}(\mathrm{char}_A(\varphi, X))$$

如果你可以说服自己相信这件事，我们立刻可以得到：

推论 1.13.1: 范与迹的传递性

设 A-代数 B 同时也是有限秩自由 A-模，则对任意的 $b \in B$ 满足

$$\mathrm{tr}_{B/R}(b) = \mathrm{tr}_{A/R}(\mathrm{tr}_{B/A}(b)), \quad N_{B/R}(b) = N_{A/R}(N_{B/A}(b))$$

$$\mathrm{char}_{B/R}(b, X) = N_{A[X]/R[X]}(\mathrm{char}_{B/A}(b, X))$$

定义 1.13.2: 判别式

设 A 为 R-代数，作为 R-模有基 $x_1, \cdots, x_n$，定义相应的**判别式**为

$$d(x_1, \cdots, x_n) := \det_R(\mathrm{tr}_{A/R}(x_i x_j)) \in R$$

对称 R 双线性型 $(x, y) \mapsto \mathrm{tr}_{A/R}(xy)$ 称为 A 的**迹型式**，不同的基 x_i, y_j 可以通过转移矩阵 T 联系，即 $\vec{y} = T\vec{x}$，可见

$$d(y_1, \cdots, y_n) = \det(T)^2 d(x_1, \cdots, x_n)$$

因此 $d_A := d(x_1, \cdots, x_n) \mod (R^\times)^2$ 为 $R/(R^\times)^2$ 中的元素仅与代数 A 有关，称为 A 的**判别式**. 特别地，d_A 在 R 中生成的主理想是良定义的，称为**判别式理想**.

1.14 无穷 Galois 对应

定义 1.14.1: Krull 拓扑

对于 *Galois* 扩张 E/F，赋予 $\mathrm{Gal}(E/F)$ 拓扑结构，使得它在任意元素 σ 处的一组邻域基为

$$\sigma\,\mathrm{Gal}(E/K), \quad K/F \text{ 为有限 } Galois \text{ 子扩张}$$

称之为 $\mathrm{Gal}(E/F)$ 上的 ***Krull* 拓扑**.

直观地把握，Krull 拓扑的效果相当于说若存在充分大的有限 Galois 子扩张 K/F 使得 $\sigma|_K = \tau|_K$ 时，σ 充分接近 τ. 由于 $\mathrm{Gal}(E/K)$ 是正规子群，定义也可以用 $\mathrm{Gal}(E/K)\sigma$ 改述. 由于邻域基需对有限交封闭，这一点我们可以由

$$\mathrm{Gal}(E/K) \cap \mathrm{Gal}(E/K') = \mathrm{Gal}(E/KK')$$

来得到，注意到 KK'/F 仍然是有限 Galois 扩张. 对任意的有限子扩张 L/F，总可以取 L 在 E 中的正规闭包 $L' \supset L$，可见 L'/F 仍然是有限扩张，并且是正规可分扩张即 Galois 扩张，故可见

$$\mathrm{Gal}(E/L') \subset \mathrm{Gal}(E/L)$$

因此邻域基也可以取作 $\sigma\,\mathrm{Gal}(E/L)$，其中 L 取遍所有有限子扩张. 我们可见在这个拓扑下取逆映射和乘法映射都是连续的，故 $\mathrm{Gal}(E/F)$ 确实是拓扑群.

引理 1.14.1

对任意 *Galois* 扩张 E/F，拓扑群 $\mathrm{Gal}(E/F)$ 是投射有限群，确切地说，存在拓扑群的自然同构

$$\mathrm{Gal}(E/F) \xrightarrow{\sim} \varprojlim_{K/F\text{: 有限 } Galois \text{ 子扩张}} \mathrm{Gal}(K/F)$$

我们相信这件事情，下面的引理刻画了 Galois 群的拓扑性质：

引理 1.14.2

拓扑群 $G := \mathrm{Gal}(E/F)$ 满足一下性质：

(1) G 是 *Hausdorff* 紧空间，并且当 E/F 有限时取离散拓扑.

(2) 对任意有限子扩张 L/F，子群 $\mathrm{Gal}(E/L)$ 为开子群.

(3) 任意开子群 H 都是闭的，并且满足 $|G/H| < \infty$.

(4) 对任意子扩张 L/F，子群 $\mathrm{Gal}(E/L)$ 为闭子群.

(5) 若赋予 E 离散拓扑，则作用映射 $\mathrm{Gal}(E/F) \times E \to E$ 是连续的.

于是我们可以得到本节主定理：

定理 1.14.1: 无穷 Galois 对应

设 E/F 是 *Galois* 扩张，则我们有互逆的双射

$$\begin{aligned} \{\text{中间域 } K\} &\longleftrightarrow \{\text{闭子群 } H \subset \mathrm{Gal}(E/F)\} \\ K/F &\longmapsto \mathrm{Gal}(E/K) \\ E^H/F &\longleftarrow\!\shortmid H \end{aligned}$$

并满足以下性质：

(1) 对应是反包含的.

(2) 双射对于 $\mathrm{Gal}(E/F)$ 在两边的左作用是等变的，并且给出正规闭子群 $H \lhd \mathrm{Gal}(E/F)$ 和 *Galois* 子扩张 K/F 的一一对应.

(3) 对任意中间域 K 皆有双射

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \to \mathrm{Hom}_F(K, E), \quad [\sigma] \mapsto \sigma|_K$$

当 K/F 是 *Galois* 扩张时，上式导出拓扑群的同构

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/K) \cong \mathrm{Gal}(K|F)$$

其中左式赋予商拓扑.

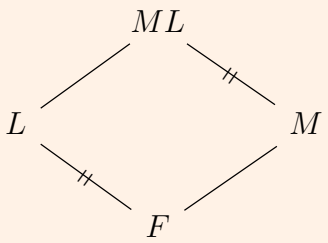
(4) 开子群对应到有限子扩张.

证明略去，当 E/F 是有限时，一切回归到有限 Galois 对应.

推论 1.14.1: 基变换

取定扩域 Ω/F，设 L/F 是其中的 *Galois* 扩张而 M/F 是任意子扩张，则 LM/M 也是 *Galois* 扩张，并且有拓扑群的同构

$$\mathrm{Gal}(LM/M) \xrightarrow{\sim} \mathrm{Gal}(L/L\cap M) \subset \mathrm{Gal}(L/F), \quad \sigma \mapsto \sigma|_L$$

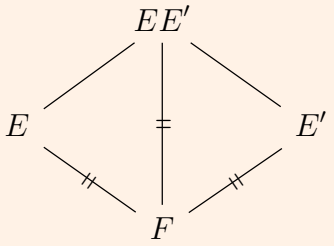


推论 1.14.2

考虑 Ω/F 的 *Galois* 子扩张 E/F 与 E'/F. 此时 EE'/F 也是 *Galois* 扩张，并且有拓扑群之间的单同态

$$\mathrm{Gal}(EE'/F) \to \mathrm{Gal}(E/F) \times \mathrm{Gal}(E'/F), \quad \sigma \mapsto (\sigma|_E, \sigma|_{E'})$$

若 $E \cap E' = F$ 则为同构.



定理 1.14.2: 正规扩张的结构

设 E/F 为正规扩张，则

(1) $E/E^{\mathrm{Aut}_F(E)}$ 是 *Galois* 扩张.

(2) $E^{\mathrm{Aut}_F(E)}$ 等于 F 在 E 中的纯不可分闭包.

(3) $E/E^{\mathrm{Aut}_F(E)}$ 的 *Galois* 群等于 $\mathrm{Aut}_F(E)$.

因此可见正规扩张 E/F 分为两段，第一段是纯不可分扩张 $E^{\mathrm{Aut}_F(E)}/F$，第二段是 Galois 扩张 $E/E^{\mathrm{Aut}_F(E)}$，可以知道 $E = E^\flat E^\sharp$，其中 $E^\flat$ 是可分闭包，$E^\sharp$ 是纯不可分闭包.

命题 1.14.1

设 E/F 是代数扩张，若每个非常数多项式 $P \in F[X]$ 在 E 中皆有根，则 E 是代数闭域.

证明: 我们只需要将 E 嵌入 F 的代数闭包 $\overline{F}$，要证明命题，只需要证明对 $F[X]$ 中每个非常数多项式在 $\overline{F}$ 中的分裂域 K 来证明 $K \subset E$，根据上述讨论，我们知道

$$K = K^\flat K^\sharp$$

所以只需要处理 K/F 可分与纯不可分的情况：

(1) 考虑 K/F 可分的情况，这是有限可分扩张，所以是单扩张，故存在 $u \in K$ 使得 $K = F(u)$，按条件知道极小多项式 P_u 在 E 中有根 v，故存在 $\sigma \in \mathrm{Hom}_F(K, \overline{F})$ 使得 $\sigma(u) = v$，正规性保证了 $K = \sigma(K) = \sigma(F(u)) = F(\sigma(u)) = F(v) \subset E$.

(2) 当 K/F 纯不可分，设 $p = \mathrm{char}(F) > 0$，令 $x \in K$，令极小多项式 P_x 按条件在 E 中有根，而纯不可分性质蕴含 P_x 在 $\overline{F}$ 中恰有一根，知 $x \in E$.

综上知道所有 K 中可分与不可分元都在 E 中，所以 K 在 E 中，得证. □

这个命题告诉我们 Atiyah 上的经典代数闭包存在性的证明只需要进行第一段即可.

Chapter 2: 同调代数速通

2.1 加性范畴与Abel范畴

定义 2.1.1: Pre-additive Category

A category $\mathscr{C}$ is called ***Pre-additive Category*** *if it satisfies the following conditions:*

(1) For any objects $A, B \in \mathrm{ob}(\mathscr{C})$, the morphisms $\mathrm{Hom}(A, B)$ is an abelian group.

(2) The composition of morphisms is bilinear, i.e.

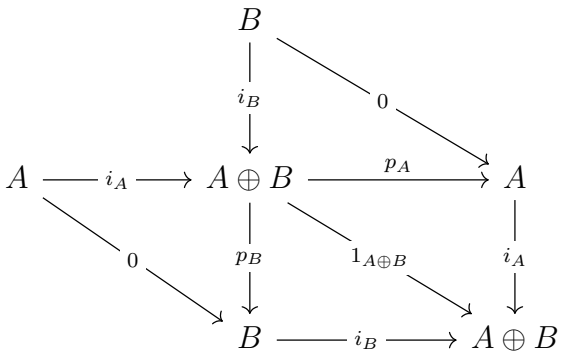
$$f \circ (g + h) = f \circ g + f \circ h, \quad (f + g) \circ h = f \circ h + g \circ h$$

定义 2.1.2: Additive Category

A category $\mathscr{A}$ is called ***Additive Category****, if it is a pre-additive category with zero objects and finite biproducts.*

Remark 2.1.1

Remember that a zero object is both a initial object and a terminal object. And a biproduct is both a product and a coproduct, denoted by $\oplus$. In detail, we have the diagram:



satisfying

$$p_A \circ i_A = 1_A, \quad p_B \circ i_B = 1_B, \quad i_A \circ P_A + i_B \circ p_B = 1_{A \oplus B}$$

In fact, every morphism from $A \oplus B$ to $A \oplus B$ can be expressed as

$$f = \begin{pmatrix} p_A f i_A & p_A f i_B \\ p_B f i_A & p_B f i_B \end{pmatrix}$$

So $i_A p_A + i_B p_B = 1$ is just

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

有限情况下直积等于余积等于双积.

命题 2.1.1: 加性范畴的性质

$\mathscr{C}$ 是加性范畴，$A, B \in \mathscr{C}$，则**零态射** $A \to 0 \to B$ 是 $\mathrm{Hom}_{\mathscr{C}}(A, B)$ 这个 *Abel* 群的零元. 并且加性范畴中的有限积对象也是余积对象.

定义 2.1.3: 加性函子

两个加性范畴 $\mathscr{A}, \mathscr{B}$ 间的函子 F 称为**加性函子**，指对任意的 $A, B, C \in \mathscr{A}$，F 诱导态射群之间的群同态，即 $F\colon \mathrm{Hom}_{\mathscr{A}}(A, B) \to \mathrm{Hom}_{\mathscr{B}}(FA, FB)$ 是群同态.

命题 2.1.2: 加性函子的性质

$F\colon \mathscr{A} \to \mathscr{B}$ 是加性范畴间的加性函子，则

(1) $F(0) \cong 0$，即保持零对象.

(2) $F(0_{AB}) = 0_{F(A)F(B)}$，即保持零态射.

(3) F 保持有限直和.

定义 2.1.4: 核与余核，像与余像

含零对象的范畴 $\mathscr{C}$ 中，映射 $f\colon A \to B$ 有如下的拉回与推出：

$$\begin{array}{ccc} \mathrm{Ker}\, f & \longrightarrow & 0 \\ {\scriptstyle i}\downarrow & \lrcorner & \downarrow \\ A & \xrightarrow[f]{} & B \end{array} \qquad \begin{array}{ccc} 0 & \longrightarrow & \mathrm{Coker}\, f \\ \uparrow & \llcorner & \uparrow{\scriptstyle p} \\ A & \xrightarrow[f]{} & B \end{array}$$

分别称 $(\mathrm{Ker}\, f, i)$ 为 $f\colon A \to B$ 的**核**，$(\mathrm{Coker}\, f, p)$ 为 $f\colon A \to B$ 的**余核**. 而 f 的**像**定义为 f 余核的核，**余像**定义为 f 的核的余核，即

$$\mathrm{Im}\, f = \mathrm{Ker}(\mathrm{Coker}\, f), \quad \mathrm{Coim}\, f = \mathrm{Coker}(\mathrm{Ker}\, f)$$

定义 2.1.5: Abel 范畴

一个 ***Abel 范畴***是指满足如下两个条件的加性范畴：

(1) 所有态射都存在核与余核.

(2) 所有的 *monic* 都是余核的核，*epi* 都是核的余核.

Example 2.1.1
交换群范畴，左右 R-模范畴都是 Abel 范畴的重要例子.

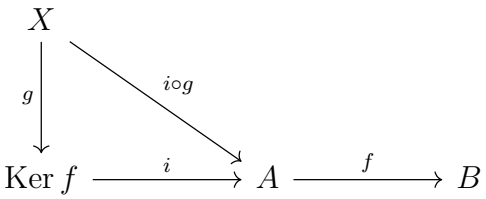
命题 2.1.3

加性范畴的对偶范畴就是加性范畴，*Abel* 范畴的对偶范畴也是 *Abel* 范畴.

引理 2.1.1

在加性范畴中，所有核都是 *monic*，余核都是 *epi*.

证明: 对于核而言



若 $i \circ g = 0$，则使得上图交换的 $X \to \operatorname{Ker} f$ 存在且唯一，注意 0 和 g 都满足，所以 $g = 0$，故 monic. 余核同理. □

定义 2.1.6

Let $f : x \to y$ be a morphism in an abelian category.

(1) *We say f is* ***injective*** *if* $\operatorname{Ker}(f) = 0$.

(2) *We say f is* ***surjective*** *if* $\operatorname{Coker}(f) = 0$.

if $x \to y$ is injective, then we say x is a ***subobject*** *of y and we use the notation $x \subset y$. If $x \to y$ is surjective, the we sat that y is a* ***quotient*** *of x. If $x \subset y$, we denote*

$$y/x = \operatorname{Coker}(x \to y)$$

引理 2.1.2

Let $f: x \to y$ be a morphism in an abelian category $\mathscr{A}$. Then

(1) f is injective if and only if f is a monomorphism.

(2) f is surjective if and only if f is an epimorphism.

(3) f is an isomorphism if and only if f is injective and surjective.

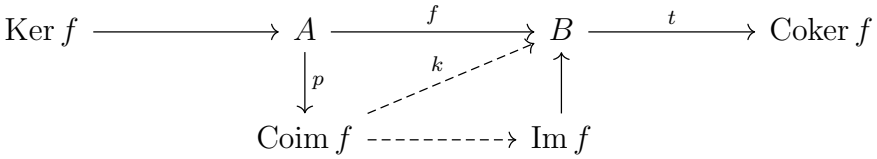
证明: Believe it. □

命题 2.1.4: 余像-像分解

Abel 范畴中的任何态射 $f: A \to B$ 可以有典范的分解

$$A \to \operatorname{Coim} f \to \operatorname{Im} f \to B$$

证明: 看下图



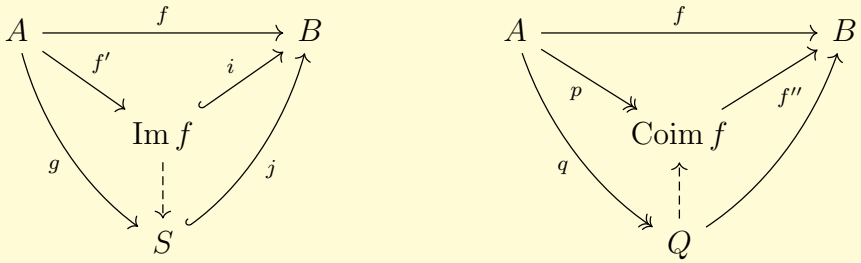
由余像的泛性质可以分解出 k，故有

$$t \circ k \circ p = t \circ f = 0$$

由余核是 epi 知道 $t \circ k = 0$，由核的泛性质诱导 $\operatorname{Coim} f \to \operatorname{Im} f$. □

命题 2.1.5: 像与余像的泛性质

考虑 $f: A \to B$ 的像与余像存在，则有如下泛性质：

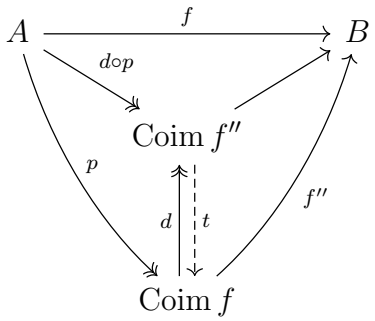


分别刻画了最小子对象和最大商对象的性质.

定理 2.1.1: 同构与满单分解

Abel 范畴中态射 $f\colon A \to B$ 诱导的典范映射 $\operatorname{Coim} f \to \operatorname{Im} f$ 是同构，从而任意态射都可以分解为满态射 $A \to \operatorname{Im} f$ 与单态射 $\operatorname{Im} f \to B$.

证明: 对 $\operatorname{Coim} f \to B$ 作典范的分解，得到



由于满射复合还是满射，所以 $A \to \operatorname{Coim} f''$ 是满射，从而由余像泛性质得到 $\operatorname{Coim} f'' \to \operatorname{Coim} f$，从而由泛性质唯一性得到 $t \circ d = \mathrm{id}$，再注意到 d 是满射，故

$$d \circ t \circ d = d \circ \mathrm{id} = \mathrm{id} \circ d \implies d \circ t = \mathrm{id}$$

从而得到 $\operatorname{Coim} f \cong \operatorname{Coim} f''$，由下面的引理表示 f'' 是单射，从而 $\operatorname{Coim} f \to \operatorname{Im} f$ 是单射，同理可证满射，故同构. 满单分解也立刻得到. □

引理 2.1.3

Abel 范畴中若 $f\colon A \to B$ 满足 $\operatorname{Coim} f \cong A$，这说明 f 是单射. 若 $\operatorname{Im} f \cong B$，这说明 f 是满射.

证明: 只证明 coimgae 情况，由于

$$\operatorname{Ker} f \xrightarrow{i} A \xrightarrow{p} \operatorname{Coim} f$$

复合为零，故

$$p \circ i = 0$$

由于 p 是同构，所以 $i = 0$，所以 $\operatorname{Ker} f = 0$，故 f 单. □

定理 2.1.2: Abel 范畴等价定义

A category $\mathscr{A}$ is called ***Abelian Category*** *if it is an additive category with all kernels and cokernels, and the natural map*

$$\operatorname{Coim} f \to \operatorname{Im} f$$

is an isomorphism for all morphisms f of $\mathscr{A}$.

引理 2.1.4

Let $\mathscr{A}$ be an abelian category. All finite limits and finite colimits exist in $\mathscr{A}$.

证明: Because finite products and equalizers exist. □

定义 2.1.7: Complex and Exact

Let $\mathscr{A}$ be an additive category. Consider a sequence of morphisms

$$\cdots \to x \to y \to z \to \cdots$$

*in $\mathscr{A}$. We say such a sequence is a **complex** if the composition of any two consecutive arrows is zero. If $\mathscr{A}$ is abelian then we say the sequence is **exact** at y if*

$$\mathrm{Im}(x \to y) = \mathrm{Ker}(y \to z)$$

推论 2.1.1: 正合的刻画

考虑 *Abel* 范畴中态射 $A \to B \to C$, *TFAE*:

(1) $\mathrm{Ker}(B \to C) = \mathrm{Im}(A \to B)$.

(2) $\mathrm{Coker}(A \to B) = \mathrm{Coim}(B \to C)$.

(3) $A \to B \to C$ 与 $\mathrm{Ker}(B \to C) = K \to b \to C = \mathrm{Coker}(A \to B)$ 都是零映射.

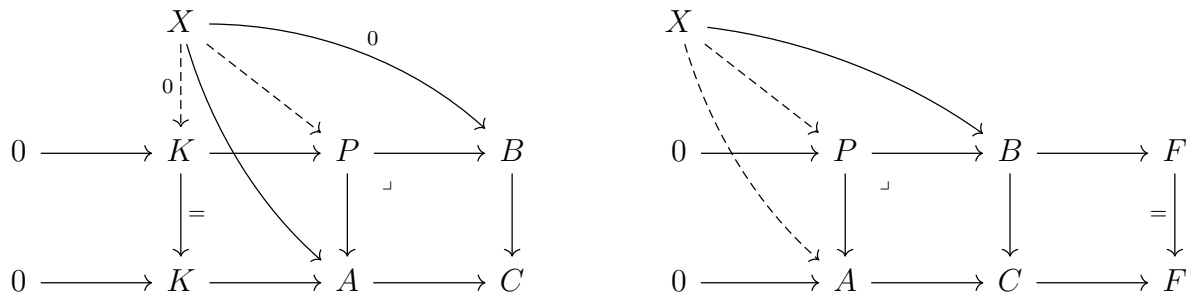
命题 2.1.6

设 $A \to C \leftarrow B$ 的拉回为 P, 则

(1) $0 \to K \to P \to B$ 正合, 则 $0 \to K \to A \to C$ 正合. 特别地, $P \to B$ 单则 $A \to C$ 单.

(2) $0 \to A \to C \to F$ 正合, 则 $0 \to P \to B \to F$ 正合, 特别地 $A \to C$ 单则 $P \to B$ 单.

证明: 只需要分别证明 $K = \mathrm{Ker}(A \to C)$ 与 $P = \mathrm{Ker}(B \to F)$ 即可



交换图道尽一切. □

Remark 2.1.2
此为一般范畴的通用结论.

命题 2.1.7: 拉回与正合

给定 *Abel* 范畴中的一个图表*(*不一定交换*)*:

$$\begin{array}{ccc} P & \xrightarrow{f} & A \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle r} \\ B & \xrightarrow[s]{} & C \end{array}$$

其自然对应了一列映射

$$0 \to P \to A \oplus B \to C \to 0$$

中间两个映射为 (f, g) 与 $(r, -s)^T$，则 $P \to A \oplus B \to C$ 是零映射当且仅当图表交换，左正合当且仅当 P 是拉回，右正合当且仅当 C 是推出，正合当且仅当同时是拉回和推出.

推论 2.1.2: 满射的拉回是满射

图表沿用上面命题，设 $A \to C \leftarrow B$ 的拉回为 P，$A \to C$ 满则有 $P \to B$ 满.

证明: 若 $A \to C$ 满，则很显然

$$(r, -s)^T : A \oplus B \to C$$

是满射，从而

$$0 \to P \to A \oplus B \to C \to 0$$

正合，从而 C 是推出，于是立刻可以由泛性质得到结论. □

Remark 2.1.3
此为 Abel 范畴的特殊结论.

2.2 (AB5) 条件与 Grothendieck 范畴

定义 2.2.1: 内射对象与投射对象

$\mathscr{A}$ 是 *Abel* 范畴，对象 P 若使得 $\mathrm{Hom}_{\mathscr{A}}(P, -) : \mathscr{A} \to \mathbf{Ab}$ 正合，则称 P 是**投射对象**; 若 P 使得 $\mathrm{Hom}_{\mathscr{A}}(-, P)$ 正合，则称为**内射对象**. 一个 *Abel* 范畴**有足够内射对象**指它的任意对象都能单射入一个内射对象; **有足够投射对象**指它的任意对象可以被一个投射对象满射.

定义 2.2.2: 生成元

范畴 $\mathscr{C}$ 的**生成元系**是指指标 $\mathcal{I}$ 为小范畴的 $\mathscr{C}$ 的一簇对象 $\{G_i\}_{i\in\mathcal{I}}$ 使得任意态射 $f\colon X\to Y$ 是同构当且仅当对每个 $i\in\mathcal{I}$ 有 $\mathrm{Hom}_{\mathscr{C}}(G_i,X)\to\mathrm{Hom}_{\mathscr{C}}(G_i,Y)$ 是同构. 如果 $\{G_i\}_{i\in\mathcal{I}}$ 中只有一个元素 G，将其称为**生成元**. 范畴 $\mathscr{C}$ 的一个**余生成元(系)**是 $\mathscr{C}^{op}$ 的一个生成元(系).

Remark 2.2.1

生成元与余生成元分别指使得 $\mathrm{Hom}_{\mathscr{C}}(G,-),\mathrm{Hom}_{\mathscr{C}}(-,G)$ 为忠实函子的对象 G. 投射生成元与内射余生成元分别指使函子为正合忠实函子的对象.

定义 2.2.3: (AB5) 与 Grothendieck 范畴

若 *Abel* 范畴 $\mathscr{A}$ 满足 (AB5): 余完备且滤过余极限正合. 并且存在生成元，则称之为 ***Grothendieck* 范畴**.

Example 2.2.1

环 R 上的模范畴，特别地交换群范畴都是 Grothendieck 范畴，在 $\mathbf{Mod}_R$ 上 R 就是生成元.

定理 2.2.1: Baer 判别法

如 $\mathscr{A}$ 为 *Grothendieck* 范畴，g 为其生成元，则只要 $I\in\mathscr{A}$ 满足对 g 的任意子对象 h，任意 $\varphi\colon h\to I$ 都可以延拓至 $g\to I$，就有 I 内射.

由 Baer 判别法可以知道：

定理 2.2.2

Grothendieck 范畴有足够的内射对象.

推论 2.2.1

Grothendieck 范畴有内射余生成元.

定理 2.2.3: Freyd-Mitchell

$\mathscr{A}$ 是一个 *Abel* 小范畴，则存在环(含幺但未必交换) R 和一个正合全忠实函子 $\iota\colon\mathscr{A}\to\mathbf{Mod}_R$ 使得

$$\mathrm{Hom}_{\mathscr{A}}(M,N)\cong\mathrm{Hom}_R(\iota M,\iota N)$$

这个定理允许我们把图像放到模范畴中使用元素去追图而不是在 Abel 范畴中迷失于繁琐的泛性质追图.

2.3 基本同调符号

We first start in module category.

定义 2.3.1: Chain Complex

*A **chain complex** $C.$ of R-modules is a family $\{C_n\}_{n\in\mathbb{Z}}$ of R-modules, together with R-module maps $d = d_n\colon C_n \to C_{n-1}$ such that each composite $d\circ d\colon C_n \to C_{n-2}$ is zero. The maps d_n are called the **differentials** of $C.$. The kernel of d_n is the module of n-**cycles** of $C.$, denoted $Z_n = Z_n(C.)$. The image of $d_{n+1}\colon C_{n+1}\to C_n$ is the module of n-**boundaries** of $C.$, denoted $B_n = B_n(C.)$. Because $d\circ d = 0$, we have*

$$0 \subseteq B_n \subseteq Z_n \subseteq C_n$$

*for all n. The n^{th} **homology module** of $C.$ is the subquotient $H_n(C.) = Z_n/B_n$ of C_n. Because the dot in $C.$ is annoying, we will often write C for $C.$.*

There is a category $\mathbf{Ch}(\mathbf{Mod}_R)$ of chain complexes of (right) R-modules. The objects are, of course, chain complexes. A **complex morphism** $u\colon C. \to D.$ is a chain complex map, that is, a family of R-module homomorphisms $u_n\colon C_n \to D_n$ commuting with d in the sense that $u_{n-1}d_n = d_n u_n$. That is, such that the following diagram commutes:

$$\begin{array}{ccccc} C_{n+1} & \xrightarrow{d} & C_n & \xrightarrow{d} & C_{n-1} \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle u} \\ D_{n+1} & \xrightarrow[d]{} & D_n & \xrightarrow[d]{} & D_{n-1} \end{array}$$

A morphism $C. \to D.$ of chain complexes is called a **quasi-isomorphism** (Bourbaki uses **homologism**) if the maps $H_n(C.) \to H_n(D.)$ are all isomorphisms. Easy to show that H_n is a functor from $\mathrm{Ch}(\mathbf{Mod}_R) \to \mathbf{Mod}_R$.

The following variant notation is obtained by reindexing with superscripts; $C^n = C_{-n}$. A **cochain complex** $C^{\cdot}$ of R-modules is a family $\{C^n\}$ of R-modules, together with maps $d^n\colon C^n \to C^{n+1}$ such that $d\circ d = 0$. $Z^n(C^{\cdot}) = \mathrm{Ker}(d^n)$ is the module of n-cocycles, $B^n(C^{\cdot}) = \mathrm{im}(d^{n-1}) \subseteq C^n$ is the module of n-coboundaries, and the subquotient $H^n(C^{\cdot}) = Z^n/B^n$ of C^n is the n^{th} **cohomology module** of $C^{\cdot}$. Morphisms and quasi-isomorphisms of cochain complexes are defined exactly as for chain complexes.

A chain complex $C.$ is called **bounded** if almost all the C_n are zero; if $C_n = 0$ unless $a \le n \le b$, we say that the complex has **amplitude** in $[a, b]$. A complex $C.$ is **bounded above** (resp. **bounded below**) if there is a bound b (resp. a) such that $C_n = 0$ for all $n > b$ (resp. $n < a$). The bounded (resp. bounded above, resp. bounded below) chain complexes form full subcategories of $\mathbf{Ch} = \mathbf{Ch}(R\text{-mod})$ that are denoted $\mathbf{Ch}_b$, $\mathbf{Ch}_-$, and $\mathbf{Ch}_+$, respectively.

Similarly, a cochain complex $C^{\cdot}$ is called **bounded above** if the chain complex $C_n = C^{-n}$ is

bounded below, that is, if $C^n = 0$ for all large n; $C^{\cdot}$ is **bounded below** if $C^{\cdot}$ is bounded above, and **bounded** if $C^{\cdot}$ is bounded. The categories of bounded (resp. bounded above, resp. bounded below, resp. non-negative) cochain complexes are denoted $\mathbf{Ch}^b$, $\mathbf{Ch}^-$, $\mathbf{Ch}^+$, and $\mathbf{Ch}^{\geq 0}$, respectively.

Now we put those things into abelian category.

The zero object in $\mathbf{Ch}$ is the complex "0" of zero modules and maps. Given a family $\{A_\alpha\}$ of complexes of R-modules, the product $\prod A_\alpha$ and coproduct (direct sum) $\bigoplus A_\alpha$ exist in $\mathbf{Ch}$ and are defined degreewise: the differentials are the maps

$$\prod_\alpha d_\alpha : \prod_\alpha A_{\alpha,n} \to \prod_\alpha A_{\alpha,n-1} \quad \text{and} \quad \bigoplus_\alpha d_\alpha : \bigoplus_\alpha A_{\alpha,n} \to \bigoplus_\alpha A_{\alpha,n-1},$$

respectively. These suffice to make $\mathbf{Ch}$ into an additive category.

定义 2.3.2: subcomplex and quotient complex

*A chain complex B is called a **subcomplex** of C if each B_n is a submodule of C_n and the differential on B is the restriction of the differential on C, that is, when the inclusions $i_n : B_n \subseteq C_n$ constitute a chain map $B \to C$. In this case we can assemble the quotient modules C_n/B_n into a chain complex*

$$\cdots \to C_{n+1}/B_{n+1} \xrightarrow{d} C_n/B_n \xrightarrow{d} C_{n-1}/B_{n-1} \xrightarrow{d} \cdots$$

*denoted C/B and called the **quotient complex**. If $f : B \to C$ is a chain map, the kernels $\{\mathrm{Ker}(f_n)\}$ assemble to form a subcomplex of B denoted $\mathrm{Ker}(f)$, and the cokernels $\{\mathrm{coker}(f_n)\}$ assemble to form a quotient complex of C denoted $\mathrm{coker}(f)$.*

A subcategory $\mathcal{B}$ of $\mathcal{A}$ is called an **abelian subcategory** if it is abelian, and an exact sequence in $\mathcal{B}$ is also exact in $\mathcal{A}$.

If $\mathcal{A}$ is any abelian category, we can repeat the discussion to define chain complexes and chain maps in $\mathcal{A}$—just replace $\mathbf{Mod}_R$ by $\mathcal{A}$! These form an additive category $\mathbf{Ch}(\mathcal{A})$, and homology becomes a functor from this category to $\mathcal{A}$. In the sequel we will merely write $\mathbf{Ch}$ for $\mathbf{Ch}(\mathcal{A})$ when $\mathcal{A}$ is understood.

Now, you can convince yourself with the following theroem.

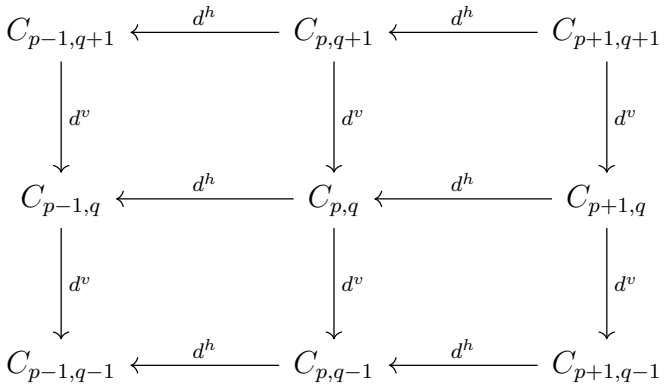
定理 2.3.1

The category $\mathbf{Ch} = \mathbf{Ch}(\mathcal{A})$ of chain complexes is an abelian category.

A **double complex** (or **bicomplex**) in $\mathcal{A}$ is a family $\{C_{p,q}\}$ of objects of $\mathcal{A}$, together with maps

$$d^h : C_{p,q} \to C_{p-1,q} \quad \text{and} \quad d^v : C_{p,q} \to C_{p,q-1}$$

such that $d^h \circ d^h = d^v \circ d^v = d^v \circ d^h + d^h \circ d^v = 0$. It is useful to picture the bicomplex $C_{\cdot}$ as a lattice.



in which the maps d^h go horizontally, the maps d^v go vertically, and each square anticommutes. Each row C_{*q} and each column C_{p*} is a chain complex.

We say that a double complex C is **bounded** if C has only finitely many nonzero terms along each diagonal line $p+q=n$, for example, if C is concentrated in the first quadrant of the plane (a first quadrant double complex).

Remark 2.3.1

Because of the anticommutativity, the maps d^v are not maps in **Ch**, but chain maps f_{*q} from C_{*q} to $C_{*,q-1}$ can be defined by introducing $\pm$ signs:

$$f_{p,q} = (-1)^p d^v_{p,q} : C_{p,q} \to C_{p,q-1}.$$

Using this sign trick, we can identify the category of double complexes with the category $\mathbf{Ch}(\mathbf{Ch})$ of chain complexes in the abelian category **Ch**.

To see why the anticommutative condition $d^v d^h + d^h d^v = 0$ is useful, define the **total complexes** $\mathrm{Tot}(C) = \mathrm{Tot}^{\Pi}(C)$ and $\mathrm{Tot}^{\oplus}(C)$ by

$$\mathrm{Tot}^{\Pi}(C)_n = \prod_{p+q=n} C_{p,q} \quad \text{and} \quad \mathrm{Tot}^{\oplus}(C)_n = \bigoplus_{p+q=n} C_{p,q}.$$

The formula $d = d^h + d^v$ defines maps

$$d : \mathrm{Tot}^{\Pi}(C)_n \to \mathrm{Tot}^{\Pi}(C)_{n-1} \quad \text{and} \quad d : \mathrm{Tot}^{\oplus}(C)_n \to \mathrm{Tot}^{\oplus}(C)_{n-1}$$

such that $d \circ d = 0$, making $\mathrm{Tot}^{\Pi}(C)$ and $\mathrm{Tot}^{\oplus}(C)$ into chain complexes. Note that $\mathrm{Tot}^{\oplus}(C) = \mathrm{Tot}^{\Pi}(C)$ if C is bounded, and especially if C is a first quadrant double complex. The difference between $\mathrm{Tot}^{\Pi}(C)$ and $\mathrm{Tot}^{\oplus}(C)$ will become apparent when we discuss spectral sequences.

Remark 2.3.2

$\mathrm{Tot}^{\Pi}(C)$ and $\mathrm{Tot}^{\oplus}(C)$ do not exist in all abelian categories; they don't exist when $\mathcal{A}$ is the category of all finite abelian groups. We say that an abelian category is **complete** if all infinite direct products exist (and so Tot^{Π} exists) and that it is **cocomplete** if all infinite direct sums exist (and so $\mathrm{Tot}^{\oplus}$ exists). Both these axioms hold in R-mod and in the category of chain complexes of R-modules.

若给定两个 R-模复形 $C_\bullet$ 与 $D_\bullet$，我们可以定义其**张量积** $(C \otimes D)_{\bullet,\bullet}$ 为双复形 $\{C_p \otimes_R D_q\}_{p,q}$，水平与竖直微分分别为 $d \otimes 1$ 与 $(-1)^p \otimes d$.

If C is a chain complex and n is an integer, we let $\tau_{\geq n}C$ denote the subcomplex of C defined by

$$(\tau_{\geq n}C)_i = \begin{cases} 0 & \text{if } i < n \\ Z_n & \text{if } i = n \\ C_i & \text{if } i > n. \end{cases}$$

Clearly $H_i(\tau_{\geq n}C) = 0$ for $i < n$ and $H_i(\tau_{\geq n}C) = H_i(C)$ for $i \geq n$. The complex $\tau_{\geq n}C$ is called the **canonical truncation** of C below n, and the quotient complex $\tau_{<n}C = C/(\tau_{\geq n}C)$ is called the (good) truncation of C above n; $H_i(\tau_{<n}C)$ is $H_i(C)$ for $i < n$ and 0 for $i \geq n$.

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & C_{n+1} & \longrightarrow & C_n & \longrightarrow & C_{n-1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \tau_{\geq n}} & & \downarrow{\scriptstyle \tau_{\geq n}} & & \downarrow{\scriptstyle \tau_{\geq n}} & & \\ \cdots & \longrightarrow & C_{n+1} & \longrightarrow & Z_n & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

Some less useful variants are the **brutal truncations** $\sigma_{<n}C$ and $\sigma_{\geq n}C = C/(\sigma_{<n}C)$. By definition, $(\sigma_{<n}C)_i$ is C_i if $i < n$ and 0 if $i \geq n$. These have the advantage of being easier to describe but the disadvantage of introducing the homology group $H_n(\sigma_{\geq n}C) = C_n/B_n$.

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & C_{n+1} & \longrightarrow & C_n & \longrightarrow & C_{n-1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \sigma_{<n}} & & \downarrow{\scriptstyle \sigma_{<n}} & & \downarrow{\scriptstyle \sigma_{<n}} & & \\ \cdots & \longrightarrow & C_{n+1} & \longrightarrow & C_n & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

Shifting indices, or **translation**, is another useful operation we can perform on chain and cochain complexes. If C is a complex and p an integer, we form a new complex $C[p]$ as follows:

$$C[p]_n = C_{n+p} \quad (\text{resp. } C[p]^n = C^{n-p})$$

with differential $(-1)^p d$. We call $C[p]$ the p -th translate of C . The way to remember the shift is that the degree 0 part of $C[p]$ is C_p. The sign convention is designed to simplify notation later on. Note that translation shifts homology:

$$H_n(C[p]) = H_{n+p}(C) \quad (\text{resp. } H^n(C[p]) = H^{n-p}(C)).$$

We make translation into a functor by shifting indices on chain maps. That is, if $f : C \to D$ is a chain map, then $f[p]$ is the chain map given by the formula

$$f[p]_n = f_{n+p} \quad (\text{resp. } f[p]^n = f^{n-p}).$$

2.4 长正合列

定理 2.4.1: Long Exact Sequence

Let $0 \to A_\cdot \xrightarrow{f} B_\cdot \xrightarrow{g} C_\cdot \to 0$ *be a short exact sequence of chain complexes. Then there are natural maps* $\partial : H_n(C) \to H_{n-1}(A)$*, called* ***connecting homomorphisms****, such that*

$$\dots \xrightarrow{g} H_{n+1}(C) \xrightarrow{\partial} H_n(A) \xrightarrow{f} H_n(B) \xrightarrow{g} H_n(C) \xrightarrow{\partial} H_{n-1}(A) \xrightarrow{f} \dots$$

is an exact sequence.
Similarly, if $0 \to A^\cdot \xrightarrow{f} B^\cdot \xrightarrow{g} C^\cdot \to 0$ *is a short exact sequence of cochain complexes, there are natural maps* $\partial : H^n(C) \to H^{n+1}(A)$ *and a long exact sequence*

$$\dots \xrightarrow{g} H^{n-1}(C) \xrightarrow{\partial} H^n(A) \xrightarrow{f} H^n(B) \xrightarrow{g} H^n(C) \xrightarrow{\partial} H^{n+1}(A) \xrightarrow{f} \cdots .$$

证明: Applying snake lemma to the following diagram

$$\begin{array}{cccccccccc}
(E1) & 0 & \longrightarrow & Z_n(A) & \longrightarrow & Z_n(B) & \longrightarrow & Z_n(C) & & \\
 & & & \downarrow & & \downarrow & & \downarrow & & \\
 & 0 & \longrightarrow & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0 \\
 & & & \downarrow d & & \downarrow d & & \downarrow d & & \\
 & 0 & \longrightarrow & A_{n-1} & \longrightarrow & B_{n-1} & \longrightarrow & C_{n-1} & \longrightarrow & 0 \\
 & & & \downarrow & & \downarrow & & \downarrow & & \\
(E2) & & & \dfrac{A_{n-1}}{dA_n} & \longrightarrow & \dfrac{B_{n-1}}{dB_n} & \longrightarrow & \dfrac{C_{n-1}}{dC_n} & \longrightarrow & 0
\end{array}$$

we can get the row (E1) and (E2) are exace. Notice we can easily induce homomorphism

$$d\colon \frac{A_n}{dA_{n+1}} \to Z_{n-1}A$$

from differential d. Thus we can apply snake lemma again on the diagram

$$\begin{array}{ccccccccc}
 & & H_n(A) & \longrightarrow & H_n(B) & \longrightarrow & H_n(C) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \dfrac{A_n}{dA_{n+1}} & \longrightarrow & \dfrac{B_n}{dB_{n+1}} & \longrightarrow & \dfrac{C_n}{dC_{n+1}} & \longrightarrow & 0 \\
 & & \downarrow d & & \downarrow d & & \downarrow d & & \\
0 & \longrightarrow & Z_{n-1}A & \longrightarrow & Z_{n-1}B & \longrightarrow & Z_{n-1}C & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & H_{n-1}(A) & \longrightarrow & H_{n-1}(B) & \longrightarrow & H_{n-1}(C) & &
\end{array}$$

Thus we get the exact sequence

$$\dots \xrightarrow{g} H_{n+1}(C) \xrightarrow{\partial} H_n(A) \xrightarrow{f} H_n(B) \xrightarrow{g} H_n(C) \xrightarrow{\partial} H_{n-1}(A) \xrightarrow{f} \dots$$

□

We shall now explain what we mean by the naturality of ∂. There is a category $\mathcal{S}$ whose objects are short exact sequences of chain complexes (say, in an abelian category $\mathcal{C}$). Commutative diagrams

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

give the morphisms in $\mathcal{S}$ (from the top row to the bottom row). Similarly, there is a category $\mathcal{L}$ of long exact sequences in $\mathcal{C}$.

命题 2.4.1: naturality of ∂

The long exact sequence is a functor from $\mathcal{S}$ to $\mathcal{L}$. That is, for every short exact sequence there is a long exact sequence, and for every map of short exact sequences there is a commutative ladder diagram

$$\begin{array}{ccccccccccc} \cdots & \xrightarrow{\partial} & H_n(A) & \longrightarrow & H_n(B) & \longrightarrow & H_n(C) & \xrightarrow{\partial} & H_{n-1}(A) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \xrightarrow{\partial} & H_n(A') & \longrightarrow & H_n(B') & \longrightarrow & H_n(C') & \xrightarrow{\partial} & H_{n-1}(A') & \longrightarrow & \cdots \end{array}$$

证明: Just embed into $\mathbf{Mod}_R$ and push elements to chase. □

The data of the long exact sequence is sometimes organized into the mnemonic shape

$$\begin{array}{ccc} H_*(A) & \longrightarrow & H_*(B) \\ & {\scriptstyle\partial}\nwarrow \quad \swarrow & \\ & H_*(C) & \end{array}$$

This is called an **exact triangle** for obvious reasons. This mnemonic shape is responsible for the term "triangulated category".

2.5 δ-函子

定义 2.5.1: δ-函子

*A (covariant) homological (resp. cohomological) **δ-functor** between $\mathcal{A}$ and $\mathcal{B}$ is a collection of additive functors $T_n\colon \mathcal{A}\to\mathcal{B}$ (resp. $T^n\colon \mathcal{A}\to\mathcal{B}$) for $n\geq 0$, together with morphisms*

$$\delta_n\colon T_n(C)\to T_{n-1}(A)$$

(resp. $\delta^n\colon T^n(C)\to T^{n+1}(A)$) defined for each short exact sequence $0\to A\to B\to C\to 0$ in $\mathcal{A}$. Here we make the convention that $T^n=T_n=0$ for $n<0$. These two conditions are imposed:

1. *For each short exact sequence as above, there is a long exact sequence*

$$\cdots\to T_{n+1}(C)\xrightarrow{\delta} T_n(A)\to T_n(B)\to T_n(C)\xrightarrow{\delta} T_{n-1}(A)\cdots$$

(resp.

$$\cdots\to T^{n-1}(C)\xrightarrow{\delta} T^n(A)\to T^n(B)\to T^n(C)\xrightarrow{\delta} T^{n+1}(A)\cdots).$$

In particular, T_0 is right exact, and T^0 is left exact.

2. *For each morphism of short exact sequences from $0\to A'\to B'\to C'\to 0$ to $0\to A\to B\to C\to 0$, the δ's give a commutative diagram*

$$\begin{array}{ccc} T_n(C') & \xrightarrow{\delta} & T_{n-1}(A') \\ \downarrow & & \downarrow \\ T_n(C) & \xrightarrow{\delta} & T_{n-1}(A) \end{array} \qquad \begin{array}{ccc} T^n(C') & \xrightarrow{\delta} & T^{n-1}(A') \\ \downarrow & & \downarrow \\ T^n(C) & \xrightarrow{\delta} & T^{n-1}(A) \end{array}$$

这个看似复杂的定义来自短正合列推出正合列的普遍观察.

定义 2.5.2: δ-函子之间的态射

对两个上同调 δ-函子 (F^n,δ_F), $(G^n,\delta_G)\colon \mathscr{A}\to\mathscr{B}$，它们间的**态射**指一族自然变换 $t^n\colon F^n\to G^n$ 使得对于任意 $\mathscr{A}$ 中的短正合列 $0\to A\to B\to C\to 0$ 有交换图

$$\begin{array}{ccc} F^n(C) & \xrightarrow{\delta_F} & F^{n+1}(A) \\ {\scriptstyle t^n}\downarrow & & \downarrow{\scriptstyle t^{n+1}} \\ G^n(C) & \xrightarrow[\delta_G]{} & G^{n+1}(A) \end{array}$$

同样也可以定义同调 δ-函子之间的态射，略下不表.

定义 2.5.3: 万有 δ-函子与可拭性

若 δ-函子 $F=(F^n,\delta_F)\colon \mathscr{A}\to\mathscr{B}$ 满足对任意 δ-函子 $G=(G^n,\delta_G)\colon \mathscr{A}\to\mathscr{B}$ 和自然变换 $t\colon F^0\to G^0$，都存在唯一的 δ-函子态射 $\{t^n\}_{n\geq 0}$ 使得 $t^0=t$，则称 F 为一个**万有 δ-函子**. 若 δ-函子 F 满足对每个 $n>0$ 和任意的 $A\in\mathscr{A}$，存在单射 $u=u(A,n)\colon A\hookrightarrow B$ 使得 $F^n u=0$，则称 F 为**可拭的 *(effaceable)***. *We call F **coeffaceable** if for every A there is a surjection $u:P\to A$ such that $F(u)=0$.*

定理 2.5.1: 可拭函子均万有

可拭的 δ-函子都是万有 δ-函子.

证明: 设已有 $G,t\colon F^0\to G^0$，我们归纳地构造 t^n，对 $A\in\mathscr{A}$，取嵌入 $u\colon A\hookrightarrow B$ 使得 $F^{n+1}u=0$，令 $C=\operatorname{Coker} u$，则有正合列 $0\to A\to B\to C\to 0$. 作用 δ 函子得到的长正合列得到

$$F^nB\to F^nC\to F^{n+1}A\to 0$$

由正合得到

$$F^{n+1}A\cong \operatorname{Coker}(F^nB\to F^nC)$$

定义自然变换 t_A^{n+1} 为使得下图交换的唯一态射

$$\begin{array}{ccc}
\operatorname{Coker}(F^nB\to F^nC) & \xrightarrow{t^n} & \operatorname{Coker}(G^nB\to G^nC) \\
\Big\downarrow{\scriptstyle \delta_F\cong} & & \Big\downarrow{\scriptstyle \delta_G} \\
F^{n+1}A & \xrightarrow[t_A^{n+1}]{} & G^{n+1}A
\end{array}$$

即 $t_A^{n+1}=\delta_G\circ t^n\circ\delta_F^{-1}$，可以验证此构造满足万有性. □

推论 2.5.1

取同调函子和取上同调函子都是万有的 δ-函子.

证明: 只需要验证可拭. 给定任意复形 $C.$，定义复形

$$D_i=C_i(i\neq n+1),\quad D_{n+1}=C_{n+1}\oplus\operatorname{Ker} d_n$$

定义 $d'_{n+1}\colon D_{n+1}\to C_{n+1},\quad (c,k)\mapsto d_{n+1}(c)+k$，其他地方的微分 $d'_i=d_i$，则我们考虑

$$C_{n+1}\oplus\operatorname{Ker} d_n\xrightarrow{d'_{n+1}} C_n\xrightarrow{d_n} C_{n-1}$$

有 $\operatorname{Im} d'_{n+1}=\operatorname{Im} d_{n+1}+\operatorname{Ker} d_n=\operatorname{Ker} d_n$，故 $H_n(D.)=0$，所以 $H_n(C.\to D.)=0$. 故可拭，知万有. □

2.6 链同伦

定义 2.6.1: 分裂

*A complex C is called **split** if there are maps $s_n\colon C_n \to C_{n+1}$ such that $d = d \circ s \circ d$. The maps s_n are called the **splitting maps**. If in addition C is acyclic (exact as a sequence), we say that C is **split exact**.*

分裂实际上是在局部提供了一个拟逆，我们考虑 $p = ds\colon C_n \to C_n$，会注意到 $p^2 = d\circ s\circ d\circ s = d \circ s = p$，故 p 是一个幂等算子，若我们在模范畴内考虑，幂等算子自然提供了一个分解，对任意的 $x \in C_n$，有

$$x = p(x) + (x - p(x))$$

其中 $p(x) \in \operatorname{Im} p$，$x - p(x) \in \operatorname{Ker} p$，故

$$C_n = \operatorname{Im} p \oplus \operatorname{Ker} p$$

其中

$$\operatorname{Im} p = \operatorname{Im} ds = \operatorname{Im} d$$

道理在于 $\operatorname{Im} ds \subset \operatorname{Im} d$，而 ds 在 $\operatorname{Im} d$ 上是恒等态射. 所以得到直和分解

$$C_n = \operatorname{Im} d_{n+1} \oplus \operatorname{Ker}(d_{n+1} \circ s_n)$$

我们如果令 $q = s_{n-1}d_n$，也有 $q^2 = q$ 是幂等算子，所以有另外的直和分解

$$C_n = \operatorname{Im} q \oplus \operatorname{Ker} q$$

此外，ds 在 $\operatorname{Im} d$ 上恒等也可以说明 s 在 d 的像上是单射，所以 $\operatorname{Im} q = \operatorname{Im} s_{n-1}d_n \cong \operatorname{Im} d_n$，并且 $\operatorname{Ker} s_{n-1}d_n = \operatorname{Ker} d_n = Z_n$，我们有分解

$$C_n \cong \operatorname{Im} d_n \oplus Z_n = B_{n-1} \oplus Z_n$$

我们再考虑 $r = d_{n+1} \circ s_n$，这仍然是一个幂等算子，注意

$$\operatorname{Im} r = \operatorname{Im} d_{n+1}s_n = \operatorname{Im} d_{n+1} = B_n \subset Z_n$$

于是我们可以把 r 限制在 Z_n 上变成 $r\colon Z_n \to Z_n$，仍然是幂等，所以有分解

$$Z_n = \operatorname{Im} r \oplus (Z_n \cap \operatorname{Ker} r) = B_n \oplus (Z_n \cap \operatorname{Ker} r)$$

由于

$$H_n = Z_n/B_n = B_n \oplus (Z_n \cap \operatorname{Ker} r)/B_n = Z_n \cap \operatorname{Ker} r$$

故

$$Z_n = B_n \oplus H_n$$

从而

$$C_n = B_{n-1} \oplus H_n \oplus B_n$$

这就是分裂给我们的直和分解，如果是正合分解的，那就是 $H_n = 0$，即

$$C_n = B_{n-1} \oplus B_n$$

这就归结到我们熟知的正合列中的分裂诱导直和的情况.

Now suppose that we are given two chain complexes C and D, together with randomly chosen maps $s_n \colon C_n \to D_{n+1}$. Let f_n be the map from C_n to D_n defined by the formula $f_n = d_{n+1}s_n + s_{n-1}d_n$.

$$\begin{array}{ccccc} C_{n+1} & \xrightarrow{d} & C_n & \xrightarrow{d} & C_{n-1} \\ & \swarrow^{s} & \downarrow{\scriptstyle f} & \swarrow^{s} & \\ D_{n+1} & \xrightarrow{d} & D_n & \xrightarrow{d} & D_{n-1} \end{array}$$

Dropping the subscripts for clarity, we compute

$$df = d(ds + sd) = dsd = (ds + sd)d = fd.$$

Thus $f = ds + sd$ is a chain map from C to D.

定义 2.6.2: 零伦与收缩

*We say that a chain map $f \colon C \to D$ is **null homotopic** if there are maps $s_n \colon C_n \to D_{n+1}$ such that $f = ds + sd$. The maps $\{s_n\}$ are called a **chain contraction** of f.*

The chain contraction construction gives us an easy way to proliferate chain maps: if $g \colon C \to D$ is any chain map, so is $g + (sd + ds)$ for any choice of maps s_n. However, $g + (sd + ds)$ is not very different from g, in a sense that we shall now explain.

定义 2.6.3: 链同伦

*We say that two chain maps f and g from C to D are **chain homotopic** if their difference $f - g$ is null homotopic, that is, if*

$$f - g = sd + ds.$$

*The maps $\{s_n\}$ are called a **chain homotopy** from f to g. Finally, we say that $f \colon C \to D$ is a **chain homotopy equivalence** (Bourbaki uses **homotopyism**) if there is a map $g \colon D \to C$ such that gf and fg are chain homotopic to the respective identity maps of C and D.*

定义链同伦的一大好处是我们可以有更多手段处理同调群.

引理 2.6.1: 链同伦诱导相同的同调群映射

If $f \colon C \to D$ is null homotopic, then every map $f_* \colon H_n(C) \to H_n(D)$ is zero. If f and g are chain homotopic, then they induce the same maps $H_n(C) \to H_n(D)$.

证明: It is enough to prove the first assertion, so suppose that $f = ds + sd$. Every element of $H_n(C)$ is represented by an n-cycle x. But then $f(x) = d(sx)$. That is, $f(x)$ is an n-boundary in D. As such, $f(x)$ represents 0 in $H_n(D)$. □

2.7 投射消解和内射消解

定义 2.7.1: 投射消解

*Let M be an object of $\mathcal{A}$. A **left resolution** of M is a complex P with $P_i = 0$ for $i < 0$, together with a map $\varepsilon : P_0 \to M$ so that the augmented complex*

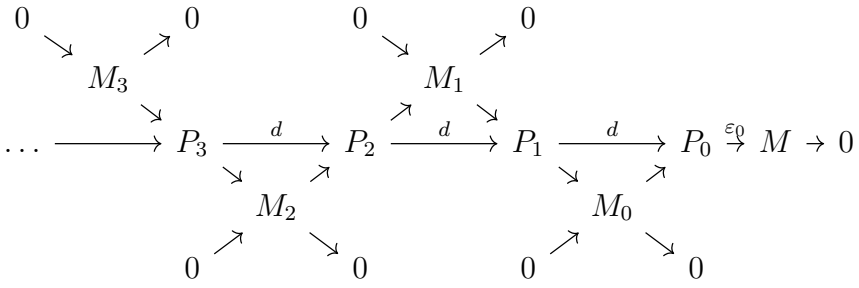
$$\cdots \xrightarrow{d} P_2 \xrightarrow{d} P_1 \xrightarrow{d} P_0 \xrightarrow{\varepsilon} M \to 0$$

*is exact. It is a **projective resolution** if each P_i is projective.*

引理 2.7.1: R-模存在投射消解

Every R-module M has a projective resolution. More generally, if an abelian category $\mathcal{A}$ has enough projectives, then every object M in $\mathcal{A}$ has a projective resolution.

证明: See the diagram.



□

定义 2.7.2: 内射消解

*Let M be an object of $\mathcal{A}$. A **right resolution** of M is a cochain complex $I^\cdot$ with $I^i = 0$ for $i < 0$ and a map $M \to I^0$ such that the augmented complex*

$$0 \to M \to I^0 \xrightarrow{d} I^1 \xrightarrow{d} I^2 \xrightarrow{d} \cdots$$

*is exact. This is the same as a cochain map $M \to I$, where M is considered as a complex concentrated in degree 0. It is called an **injective resolution** if each I^i is injective.*

同理可以证证明：

引理 2.7.2: R-模存在内射消解

If the abelian category $\mathcal{A}$ has enough injectives, then every object in $\mathcal{A}$ has an injective resolution.

前面定义了足够投射和足够内射. 那么这些对象很多的时候我们就能对一个一般的对象作投射和内射消解. 一个好的 Abel 范畴应该是这样的.

定理 2.7.1

有足够投射对象的 *Abel* 范畴的任意对象存在投射消解，有足够内射对象的 *Abel* 范畴的任意对象存在内射消解.

下面是重要的比较定理：

定理 2.7.2: 投射的Comparison

Let $P_\cdot \xrightarrow{\varepsilon} M$ be a projective resolution of M and $f' : M \to N$ a map in $\mathcal{A}$. Then for every resolution $Q_\cdot \xrightarrow{\eta} N$ of N there is a chain map $f : P_\cdot \to Q_\cdot$ lifting f' in the sense that $\eta \circ f_0 = f' \circ \varepsilon$. The chain map f is unique up to chain homotopy equivalence.

定理 2.7.3: 内射的Comparison

Let $N \to I^\cdot$ be an injective resolution of N and $f' : M \to N$ a map in $\mathcal{A}$. Then for every resolution $M \to E$ there is a cochain map $F : E \to I^\cdot$ lifting f'. The map F is unique up to cochain homotopy equivalence.

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & M & \longrightarrow & E^0 & \xrightarrow{d} & E^1 & \xrightarrow{d} & E^2 & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle \exists} & & \downarrow{\scriptstyle \exists} & & \downarrow{\scriptstyle \exists} & & \\ 0 & \longrightarrow & N & \longrightarrow & I^0 & \xrightarrow{d} & I^1 & \xrightarrow{d} & I^2 & \longrightarrow & \cdots \end{array}$$

其证明是归纳构造的，过程略去，相信即可.

引理 2.7.3: Horseshoe Lemma

Suppose given a diagram

$$\begin{array}{ccccccccccc}
 & & & & & & & & 0 & & \\
 & & & & & & & & \downarrow & & \\
\cdots & \longrightarrow & P_2' & \longrightarrow & P_1' & \longrightarrow & P_0' & \xrightarrow{\varepsilon'} & A' & \longrightarrow & 0 \\
 & & & & & & & & \downarrow{\scriptstyle i_A} & & \\
 & & & & & & & & A & & \\
 & & & & & & & & \downarrow{\scriptstyle \pi_A} & & \\
\cdots & \longrightarrow & P_2'' & \longrightarrow & P_1'' & \longrightarrow & P_0'' & \xrightarrow{\varepsilon''} & A'' & \longrightarrow & 0 \\
 & & & & & & & & \downarrow & & \\
 & & & & & & & & 0 & &
\end{array}$$

where the column is exact and the rows are projective resolutions. Set $P_n = P_n' \oplus P_n''$. Then the P_n assemble to form a projective resolution P of A, and the right-hand column lifts to an exact sequence of complexes

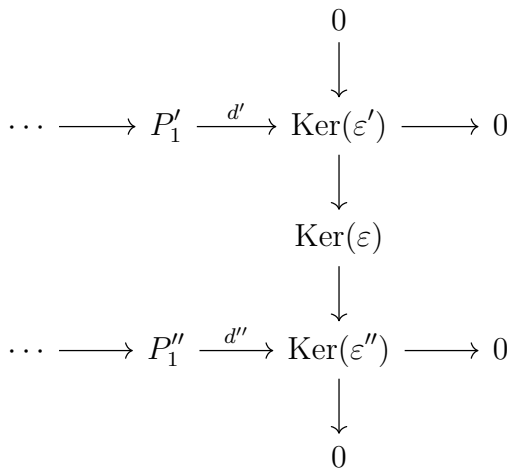
$$0 \to P' \xrightarrow{i} P \xrightarrow{\pi} P'' \to 0,$$

where $i_n : P_n' \to P_n$, $\pi_n : P_n \to P_n''$ are the natural inclusion and projection, respectively.

证明: 由于 $A \to A''$ 是满射，P_0'' 是投射模，这告诉我们存在提升 $f_2 \colon P_0'' \to A$，而原本的 $A' \to A$ 记为 f_1，我们定义 $\varepsilon(p', p'') = f_1(p') + f_2(p'')$，很显然这使得下图交换.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Ker}(\varepsilon') & \longrightarrow & P_0' & \xrightarrow{\varepsilon'} & A' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Ker}(\varepsilon) & \longrightarrow & P_0 & \xrightarrow{\varepsilon} & A & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Ker}(\varepsilon'') & \longrightarrow & P_0'' & \xrightarrow{\varepsilon''} & A'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The right two columns of (*) are short exact sequences. The Snake Lemma 1.3.2 shows that the left column is exact and that $\mathrm{coker}(\varepsilon) = 0$, so that P_0 maps onto A. This finishes the initial step and brings us to the situation



The filling in of the "horseshoe" now proceeds by induction. □

2.8 导出函子

定义 2.8.1: 左导出函子

*Let $F : \mathcal{A} \to \mathcal{B}$ be a right exact functor between two abelian categories. If $\mathcal{A}$ has enough projectives, we can construct the **left derived functors** $L_iF(i \geq 0)$ of F as follows. If A is an object of $\mathcal{A}$, choose (once and for all) a projective resolution $P \to A$ and define*

$$L_iF(A) = H_i(F(P)).$$

定义 2.8.2: 右导出函子

*Let $F\colon \mathcal{A} \to \mathcal{B}$ be a left exact functor between two abelian categories. If $\mathcal{A}$ has enough injectives, we can construct the **right derived functors** $R^iF(i \geq 0)$ of F as follows. If A is an object of $\mathcal{A}$, choose an injective resolution $A \to I^{\cdot}$ and define*

$$R^iF(A) = H^i(F(I^{\cdot})).$$

Note that since $0 \to F(A) \to F(I^0) \to F(I^1)$ is exact, we always have $R^0F(A) \cong F(A)$.

Note that since $F(P_1) \to F(P_0) \to F(A) \to 0$ is exact, we always have $L_0F(A) \cong F(A)$.

如果函子反变，那么右正合函子需要做内射消解，左正合函子需要做投射消解. 比较定理和链同伦保持同调群告诉我们导出函子是良定义的，即不依赖具体的消解的选择.

推论 2.8.1

If A is projective, then $L_iF(A) = 0$ for $i \neq 0$.

证明: Consider projective resolution

$$\cdots \to 0 \to \cdots \to 0 \to 0 \to A \to A \to 0$$

□

引理 2.8.1: 函子性

If $f : A' \to A$ is any map in $\mathcal{A}$, there is a natural map $L_iF(f) : L_iF(A') \to L_iF(A)$ for each i.
对右导出有同样的结果.

证明: Let $P' \to A'$ and $P \to A$ be the chosen projective resolutions. The comparison theorem yields a lift of f to a chain map $\tilde{f}$ from P' to P, hence a map $\tilde{f}_*$ from $H_iF(P')$ to $H_iF(P)$. Any other lift is chain homotopic to $\tilde{f}$, so the map $\tilde{f}_*$ is independent of the choice of $\tilde{f}$. The map $L_iF(f)$ is $\tilde{f}_*$. □

定理 2.8.1: 导出函子是加性函子

Each L_iF is an additive functor from $\mathcal{A}$ to $\mathcal{B}$.

证明: The identity map on P lifts the identity on A, so $L_iF(id_A)$ is the identity map. Given maps $A' \xrightarrow{f} A \xrightarrow{g} A''$ and chain maps $\tilde{f}, \tilde{g}$ lifting f and g, the composite $\tilde{g}\tilde{f}$ lifts gf. Therefore $g_*f_* = (gf)_*$, proving that L_iF is a functor. If $f_1 : A' \to A$ are two maps with lifts $\tilde{f}_1$, the sum $\tilde{f}_1 + \tilde{f}_2$ lifts $f_1 + f_2$. Therefore $(f_1 + f_2)_* = f_{1*} + f_{2*}$, proving that L_iF is additive. □

定理 2.8.2: 导出函子是万有 δ-函子

$F\colon \mathscr{A} \to \mathscr{B}$ 有足够投射*(resp.* 内射*)*对象，导出函子 $L_\bullet F$*(resp.* $R^\bullet F$*)* 总是万有*(resp.* 上*)*同调 δ-函子.

证明: 以左导出为例，首先证明是 δ-函子，给定正合列 $0 \to A' \to A \to A'' \to 0$，取 A' 与 A'' 的投射消解 $P'_\bullet$ 与 $P''_\bullet$，马蹄引理给出 A 的投射消解 $P_\bullet = P'_\bullet \oplus P''_\bullet$ 使得有正合列

$$0 \to P'_\bullet \to P'_\bullet \oplus P''_\bullet \to P''_\bullet \to 0$$

由于 F 是加性函子，所以作用之后仍然保持直和，从而保护正合，从而再取同调得到. 其函子性来自于同调的函子性. 万有性质只需要检查可拭，注意前面已经证明投射对象 P 的导出函子 $L_iFP = 0 (i > 0)$，而任意对象都可以被投射对象打满，从而得证. □

Remark 2.8.1
这个推论告诉我们，协变函子 F, G 的导出函子 R^nF 与 R^nG 同构当且仅当 $R^0F \cong R^0G$. 这个事实在层上同调的研究中有十分广泛的应用.

利用 δ-函子可以得到：

定理 2.8.3: 导出函子基本性质

设 $\mathscr{A}, \mathscr{B}$ 是 *Abel* 范畴，$\mathscr{A}$ 有足够内射对象，$F\colon \mathscr{A} \to \mathscr{B}$ 是协变左正合函子，则

(1) R^nF 是加性函子，并且 $R^0F = F$.

(2) 每个短正合列 $0 \to A \to B \to C \to 0$ 诱导长正合列

$$\cdots \to R^nF(A) \to R^nF(B) \to R^nF(C) \xrightarrow{\delta^n} R^{n+1}F(A) \to \cdots$$

(3) 对到 $0 \to A' \to B' \to C' \to 0$ 的态射，则有交换图

$$\begin{array}{ccc} R^nF(C) & \xrightarrow{\delta^n} & R^{n+1}F(A) \\ \downarrow & & \downarrow \\ R^nF(C') & \xrightarrow[\delta^n]{} & R^{n+1}F(A') \end{array}$$

推论 2.8.2: 导出与有限直和交换

由于导出函子是加性函子，所以与有限直和是交换的.

定理 2.8.4: 维数移动

(1) 若 $0 \to M \to P \to A \to 0$ 正合，满足 $L_iFP = 0 (\forall i \geq 1)$，我们称这样的 P 是 ***F*-零调的**，则 $L_{i+1}FA \cong L_iFM (\forall i \geq 1)$，且 $L_1FA \cong \mathrm{Ker}(FM \to FP)$.

(2) 若更进一步，有正合列 $0 \to M \to P_m \to P_{m-1} \to \cdots \to P_0 \to A \to 0$，其中 P_i 均 F-零调，则有

$$L_{i+m+1}FA \cong L_iFM, \quad \forall i \geq 1$$

并且

$$L_{m+1}FA \cong \mathrm{Ker}(FM \to FP_m)$$

证明: (1) 由于是 δ-函子，所以诱导长正合列

$$L_{i+1}FP \to L_{i+1}FA \to L_iFM \to L_iFP$$

前后都是 0，所以同构.

(2) 分裂成一堆短正合列然后用 (1) 归纳立刻得到. □

定理 2.8.5: FHHF Theorem

Suppose $F\colon \mathcal{A} \to \mathcal{B}$ is a covariant functor of abelian categories, and let $X^\bullet$ be a bounded-below complex in $\mathcal{A}$.

1. *If F is right exact, describe a natural morphism $F(H^n(X^\bullet)) \to H^n(F(X^\bullet))$.*
2. *If F is left exact, describe a natural morphism $H^n(F(X^\bullet)) \to F(H^n(X^\bullet))$.*
3. *If F is exact, show that the morphisms in (1) and (2) are isomorphisms.*

证明: 给定一个复形:

$$X^0 \xrightarrow{d^0} X^1 \xrightarrow{d^1} X^2 \xrightarrow{d^2} \cdots \xrightarrow{d^{n-1}} X^n \xrightarrow{d^n} \cdots$$

通过作用一个协变函子，我们会得到

$$FX^0 \xrightarrow{Fd^0} FX^1 \xrightarrow{Fd^1} FX^2 \xrightarrow{Fd^2} \cdots \xrightarrow{Fd^{n-1}} FX^n \xrightarrow{Fd^n} \cdots$$

如果 F 是右正合的，则可以得到下面的正合:

$$\begin{array}{ccccccc} B^n & \longrightarrow & Z^n & \longrightarrow & H^n(X^\bullet) & \longrightarrow & 0 \\ \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle F} \\ F(B^n) & \longrightarrow & F(Z^n) & \longrightarrow & F(H^n(X^\bullet)) & \longrightarrow & 0 \end{array}$$

我们现在尝试去构造自然变换，注意到上面的正合列告诉我们

$$F(H^n(X^\bullet)) \cong \frac{F(Z^n)}{\operatorname{Im} Fi^n}$$

还有:

$$\begin{array}{ccccccccc} X^{n-1} & \xrightarrow{d^{n-1}} & B^n & \xrightarrow{i^n} & Z^n & \xrightarrow{j^n} & X^n & \xrightarrow{d^n} & X^{n+1} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ FX^{n-1} & \xrightarrow{Fd^{n-1}} & FB^n & \xrightarrow{Fi^n} & FZ^n & \xrightarrow{Fj^n} & FX^n & \xrightarrow{Fd^n} & FX^{n+1} \end{array}$$

我们有

$$H^n(F(X^\bullet)) = \frac{\operatorname{Ker} Fd^n}{\operatorname{Im} Fd^{n-1}}$$

由于

$$F(d^n) \circ F(j^n) = F(d^n \circ j^n) = F(0) = 0 \implies \operatorname{Im} Fj^n \subseteq \operatorname{Ker} Fd^n$$

从而诱导出自然的态射

$$Fj^n\colon F(Z^n) \to \operatorname{Ker} Fd^n$$

并且有

$$Fj^n(\operatorname{Im} Fi^n) = \operatorname{Im} Fj^n \circ Fi^n = \operatorname{Im} F(j^n \circ i^n)$$

设 $k^n = j^n \circ i^n \colon B^n \to X^n$，我们知道

$$\begin{array}{ccccccc} Z^{n-1} & \longrightarrow & X^{n-1} & \xrightarrow{p^{n-1}} & B^n & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ FZ^{n-1} & \longrightarrow & FX^{n-1} & \xrightarrow{Fp^{n-1}} & FB^n & \longrightarrow & 0 \end{array}$$

右正合保持满射，有

$$d^{n-1} = k^n \circ p^{n-1} \implies Fd^{n-1} = F(k^n) \circ F(p^{n-1})$$

由 Fp^{n-1} 满射，我们知道

$$\operatorname{Im} Fd^{n-1} = \operatorname{Im} Fk^n = Fj^n(\operatorname{Im} Fi^n)$$

所以会有自然的映射

$$\widetilde{Fj^n} \colon F(H^n(X^\bullet)) \cong \frac{F(Z^n)}{\operatorname{Im} Fi^n} \to \frac{\operatorname{Ker} Fd^n}{\operatorname{Im} Fd^{n-1}} = H^n(F(X^\bullet))$$

对左正合情况同理. 正合时是同构，机械验证即可. □

定理告诉我们正合函子可以和同调交换，所以立刻得到正合函子还可以和导出函子交换：

定理 2.8.6: 正合函子可以和导出函子交换

$\mathscr{A}, \mathscr{B}, \mathscr{C}$ 是 Abel 范畴，若 $U \colon \mathscr{B} \to \mathscr{C}$ 是正合函子，则

$$U(L_nF) \cong L_n(UF), \quad U(R^nG) \cong R^n(UG)$$

2.9 映射锥与映射柱

定义 2.9.1: 映射锥

Let $f : B. \to C.$ be a map of chain complexes. The ***mapping cone*** *of f is the chain complex $\operatorname{cone}(f)$ whose degree n part is $B_{n-1} \oplus C_n$. In order to match other sign conventions, the differential in $\operatorname{cone}(f)$ is given by the formula*

$$d(b, c) = (-d(b), d(c) - f(b)), \quad (b \in B_{n-1}, c \in C_n).$$

That is, the differential is given by the matrix

$$\begin{bmatrix} -d_B & 0 \\ -f & +d_C \end{bmatrix} : \begin{array}{ccc} B_{n-1} & \xrightarrow{-} & B_{n-2} \\ \oplus & \searrow^{-} & \oplus \\ C_n & \xrightarrow[+]{} & C_{n-1} \end{array}$$

Any map $f_*: H_*(B) \to H_*(C)$ can be fit into a long exact sequence of homology groups by use of the following device. There is a short exact sequence

$$0 \to C \to \mathrm{cone}(f) \xrightarrow{\delta} B[-1] \to 0$$

of chain complexes, where the left map sends c to $(0, c)$, and the right map sends (b, c) to $-b$. Recalling that $H_{n+1}(B[-1]) \cong H_n(B)$, the homology long exact sequence (with connecting homomorphism ∂) becomes

$$\cdots \to H_{n+1}(\mathrm{cone}(f)) \xrightarrow{\delta_*} H_n(B) \xrightarrow{\partial} H_n(C) \to H_n(\mathrm{cone}(f)) \xrightarrow{\delta_*} H_{n-1}(B) \xrightarrow{\partial} \cdots .$$

The following lemma shows that $\partial = f_*$, fitting f_* into a long exact sequence.

引理 2.9.1

The map ∂ in the above sequence is f_*.

证明: If $b \in B_n$ is a cycle, the element $(-b, 0)$ in the cone complex lifts b via δ. Applying the differential we get $(db, fb) = (0, fb)$. This shows that

$$\partial[b] = [fb] = f_*[b].$$

□

推论 2.9.1: 拟同构与映射锥零调

A map $f: B \to C$ is a quasi-isomorphism if and only if the mapping cone complex $\mathrm{cone}(f)$ is exact. This device reduces questions about quasi-isomorphisms to the study of split complexes.

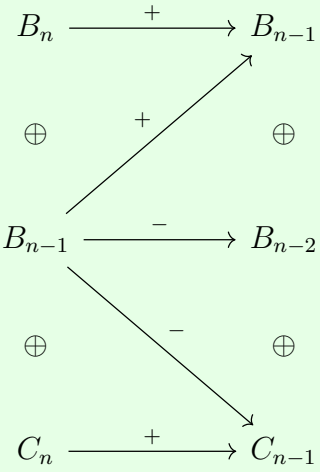
定义 2.9.2: 映射柱

A related construction is that of the ***mapping cylinder*** *cyl*(f) *of a chain complex map* $f : B_* \to C_*$ *. The degree* n *part of cyl*(f) *is* $B_n \oplus B_{n-1} \oplus C_n$ *, and the differential is*

$$d(b, b', c) = (d(b) + b', -d(b'), d(c) - f(b')).$$

That is, the differential is given by the matrix

$$\begin{bmatrix} d_B & id_B & 0 \\ 0 & -d_B & 0 \\ 0 & -f & d_C \end{bmatrix} :$$



The cylinder is a chain complex because

$$d^2 = \begin{bmatrix} d_B^2 & d_B - d_B & 0 \\ 0 & d_B^2 & 0 \\ 0 & fd_B - d_C f & d_C^2 \end{bmatrix} = 0.$$

引理 2.9.2

The subcomplex of elements $(0, 0, c)$ *is isomorphic to* C*, and the corresponding inclusion* $\alpha : C \to cyl(f)$ *is a quasi-isomorphism.*

证明: The quotient $\mathrm{cyl}(f)/\alpha(C)$ is the mapping cone of $-\mathrm{id}_B$, so it is null-homotopic. The lemma now follows from the long exact homology sequence for

$$0 \longrightarrow C \xrightarrow{\alpha} \mathrm{cyl}(f) \longrightarrow \mathrm{cone}(-\mathrm{id}_B) \longrightarrow 0.$$

□

Here is how to use mapping cylinders to fit f_* into a long exact sequence of homology groups. The subcomplex of elements $(b, 0, 0)$ in $\mathrm{cyl}(f)$ is isomorphic to B , and the quotient $\mathrm{cyl}(f)/B$ is the mapping cone of f . The composite $B \to \mathrm{cyl}(f) \xrightarrow{\beta} C$ is the map f , where β is the equivalence of exercise 1.5.4, so on homology $f_* : H(B) \to H(C)$ factors through $H(B) \to H(\mathrm{cyl}(f))$. Therefore we

may construct a commutative diagram of chain complexes with exact rows:

$$\begin{array}{ccccccccc}
 & & & & C & & & & \\
 & & & \overset{f}{\nearrow} & \uparrow{\scriptstyle \beta} & & & & \\
0 & \longrightarrow & B & \longrightarrow & \mathrm{cyl}(f) & \longrightarrow & \mathrm{cone}(f) & \longrightarrow & 0 \\
 & & & & \uparrow{\scriptstyle \alpha} & & \| & & \\
 & & 0 & \longrightarrow & C & \longrightarrow & \mathrm{cone}(f) & \xrightarrow{\delta} & B[-1] \longrightarrow 0.
\end{array}$$

The homology long exact sequences fit into the following diagram:

$$\begin{array}{ccccccccccc}
\cdots & \xrightarrow{-\partial} & H_n(B) & \longrightarrow & H_n(\mathrm{cyl}(f)) & \to & H_n(\mathrm{cone}(f)) & \xrightarrow{-\partial} & H_{n-1}(B) & \longrightarrow & \cdots \\
 & & \|\sim & \overset{f}{\searrow} & \|\sim & & \| & & \|\sim & & \\
\cdots & \longrightarrow & H_{n+1}(B[-1]) & \xrightarrow{\partial} & H_n(C) & \longrightarrow & H_n(\mathrm{cone}(f)) & \xrightarrow{\delta} & H_n(B[-1]) & \xrightarrow[\partial]{} & \cdots
\end{array}$$

引理 2.9.3

This diagram is commutative, with exact rows.

证明: It suffices to show that the right square (with $-\partial$ and δ) commutes. Let (b, c) be an n -cycle in $\mathrm{cone}(f)$, so $d(b) = 0$ and $f(b) = d(c)$. Lift it to $(0, b, c)$ in $\mathrm{cyl}(f)$ and apply the differential:

$$d(0, b, c) = (0 + b, -db, dc - fb) = (b, 0, 0).$$

Therefore ∂ maps the class of (b, c) to the class of $b = -\delta(b, c)$ in $H_{n-1}(B)$. □

The cone and cylinder constructions provide a natural way to fit the homology of every chain map $f : B \to C$ into some long exact sequence (see 1.5.2 and 1.5.7). To show that the long exact sequence is well defined, we need to show that the usual long exact homology sequence attached to any short exact sequence of complexes

$$0 \to B \xrightarrow{f} C \xrightarrow{g} D \to 0$$

agrees both with the long exact sequence attached to f and with the long exact sequence attached to g. We first consider the map f . There is a chain map $\varphi : \mathrm{cone}(f) \to D$ defined by the formula $\varphi(b, c) = g(c)$. It fits into a commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & C & \longrightarrow & \mathrm{cone}(f) & \xrightarrow{\delta} & B[-1] \longrightarrow 0 \\
 & & & & \downarrow{\scriptstyle \alpha} & & \| & & \\
0 & \longrightarrow & B & \longrightarrow & \mathrm{cyl}(f) & \longrightarrow & \mathrm{cone}(f) & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \varphi} & & \\
0 & \longrightarrow & B & \xrightarrow{f} & C & \xrightarrow{g} & D & \longrightarrow & 0
\end{array}$$

Since β is a quasi-isomorphism, it follows from the 5-lemma and 1.3.4 that φ is a quasi-isomorphism as well. The following exercise shows that φ need not be a chain homotopy equivalence.

To continue, the naturality of the connecting homomorphism ∂ provides us with a natural isomorphism of long exact sequences:

$$\begin{array}{ccccccccccc}
\cdots & \xrightarrow{\partial} & H_n(B) & \longrightarrow & H_n(\mathrm{cyl}(f)) & \longrightarrow & H_n(\mathrm{cone}(f)) & \xrightarrow{\partial} & H_{n-1}(B) & \longrightarrow & \cdots \\
 & & \| & & \|\cong & & \|\cong & & \|\sim & & \\
\cdots & \xrightarrow{\partial} & H_n(B) & \xrightarrow{\partial} & H_n(C) & \longrightarrow & H_n(D) & \xrightarrow{\partial} & H_{n-1}(B) & \xrightarrow[\partial]{} & \cdots
\end{array}$$

2.10 Tor 和 Ext 与平衡性

定义 2.10.1: Ext 与 Tor

对 R-模 M，左正合函子 $G = \mathrm{Hom}_R(-, M)$ 的右导出函子记为 $\mathrm{Ext}^\bullet_R(-, M) := R^\bullet G$，右正合函子 $F = - \otimes_R M$ 的左导出函子记为 $\mathrm{Tor}^R_\bullet(-, M) := L_\bullet F$. 不会引起歧义时常省略 R.

但是注意到 Hom 与 $\otimes$ 有两个输入，很自然会提出下面的问题，即对 $\mathrm{Hom}_R(-, N)$ 右导出后输入 M 和对 $\mathrm{Hom}_R(M, -)$ 右导出后输入 N 是否一样？同理对 $- \otimes_R N$ 左导出后代入 M 和对 $M \otimes_R -$ 左导出后代入 N 是否一样？本小节证明它们确实是一样的，这种性质称为平衡性. 首先给定 M 与 N 的投射消解 $P_\bullet \to M$ 与 $Q_\bullet \to N$，考虑下图：

$$\begin{array}{ccccccc}
\vdots & & \vdots & & \vdots & & \\
\downarrow & & \downarrow & & \downarrow & & \\
M \otimes Q_2 & & P_0 \otimes Q_2 & \longleftarrow & P_1 \otimes Q_2 & \longleftarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
M \otimes Q_1 & & P_0 \otimes Q_1 & \longleftarrow & P_1 \otimes Q_1 & \longleftarrow & P_2 \otimes Q_1 \longleftarrow \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
M \otimes Q_0 & & P_0 \otimes Q_0 & \longleftarrow & P_1 \otimes Q_0 & \longleftarrow & P_2 \otimes Q_0 \longleftarrow \cdots \\
 & & & & & & \\
 & & P_0 \otimes N & \longleftarrow & P_1 \otimes N & \longleftarrow & P_2 \otimes N \longleftarrow \cdots
\end{array}$$

为了避免各种复杂的操作，我们提前调用一下谱序列的包，我们对 $P_i \otimes Q_j$ 这个第一象限双复形在两个方向上计算 E^1-页，首先在 $\downarrow$ 方向，由于 P_i 是投射模，从而平坦，故 E^1-页为

$$\begin{array}{ccccccc}
0 & \longleftarrow & 0 & \longleftarrow & 0 & \longleftarrow & \cdots \\
 & & & & & & \\
0 & \longleftarrow & 0 & \longleftarrow & 0 & \longleftarrow & \cdots \\
 & & & & & & \\
P_0 \otimes N & \longleftarrow & P_1 \otimes N & \longleftarrow & P_2 \otimes N & \longleftarrow & \cdots
\end{array}$$

容易看出 E^2-页收敛，故

$$
{}_{\downarrow}E^2_{p,0} = H_p(P_\bullet \otimes N) = \mathrm{Tor}_p(M, N)
$$

现在在 $\leftarrow$ 方向计算 E^1-页得到

$$
\begin{array}{ccc}
\vdots & \vdots & \vdots \\
\downarrow & \downarrow & \downarrow \\
M \otimes Q_2 & 0 & 0 \\
\downarrow & \downarrow & \downarrow \\
M \otimes Q_1 & 0 & 0 \\
\downarrow & \downarrow & \downarrow \\
M \otimes Q_0 & 0 & 0
\end{array}
$$

同样 E^2-页收敛，故

$$
{}_{\leftarrow}E^2_{0,q} = H_q(M \otimes Q_\bullet)
$$

所以可以得到

$$
H_n(P_\bullet \otimes N) \cong {}_{\downarrow}E^2_{p,0} \cong H_n(\mathrm{Tot}(P_\bullet \otimes Q_\bullet)) \cong {}_{\leftarrow}E^2_{0,q} \cong H_n(M \otimes Q_\bullet)
$$

于是我们看出 Tor 确实不依赖对输入变量的选择. 下面我们来说明 Ext 的平衡性，对于 M, N 而言，我们考虑 M 的投射消解 $P_\bullet \to M$ 与 N 的内射消解 $N \to I^\bullet$，考虑下面的双复形：

$$
\begin{array}{ccccccc}
\vdots & \vdots & & \vdots & & & \\
\uparrow & \uparrow & & \uparrow & & & \\
\mathrm{Hom}(M, I^2) & \mathrm{Hom}(P_0, I^2) & \longrightarrow & \mathrm{Hom}(P_1, I^2) & \longrightarrow & \cdots & \\
\uparrow & \uparrow & & \uparrow & & \uparrow & \\
\mathrm{Hom}(M, I^1) & \mathrm{Hom}(P_0, I^1) & \longrightarrow & \mathrm{Hom}(P_1, I^1) & \longrightarrow & \mathrm{Hom}(P_2, I^1) & \longrightarrow \cdots \\
\uparrow & \uparrow & & \uparrow & & \uparrow & \\
\mathrm{Hom}(M, I^0) & \mathrm{Hom}(P_0, I^0) & \longrightarrow & \mathrm{Hom}(P_1, I^0) & \longrightarrow & \mathrm{Hom}(P_2, I^0) & \longrightarrow \cdots \\
 & & & & & & \\
 & \mathrm{Hom}(P_0, N) & \longrightarrow & \mathrm{Hom}(P_1, N) & \longrightarrow & \mathrm{Hom}(P_2, N) & \longrightarrow \cdots
\end{array}
$$

由于 $\mathrm{Hom}(P_i, -)$ 与 $\mathrm{Hom}(-, I_j)$ 都是正合函子，先在 $\uparrow$ 方向上计算 E_1-页得到：

$$
\begin{array}{ccccc}
0 & \longrightarrow & 0 & \longrightarrow & 0 \longrightarrow \cdots \\
0 & \longrightarrow & 0 & \longrightarrow & 0 \longrightarrow \cdots \\
\mathrm{Hom}(P_0, N) & \longrightarrow & \mathrm{Hom}(P_1, N) & \longrightarrow & \mathrm{Hom}(P_2, N) \longrightarrow \cdots
\end{array}
$$

所以可以看出 E_2-页收敛，有

$$
{}_{\uparrow}E_2^{n,0} = H^n(\mathrm{Hom}(P_\bullet, N))
$$

再在 $\to$ 方向计算 E_1-页得到

$$\begin{array}{ccc} \vdots & \vdots & \vdots \\ \uparrow & \uparrow & \uparrow \\ \mathrm{Hom}(M, I^2) & 0 & 0 \\ \uparrow & \uparrow & \uparrow \\ \mathrm{Hom}(M, I^1) & 0 & 0 \\ \uparrow & \uparrow & \uparrow \\ \mathrm{Hom}(M, I^0) & 0 & 0 \end{array}$$

同理 E_2-页收敛，得到

$$ {}_{\to}E_2^{0,n} = H^n(\mathrm{Hom}(M, I^\bullet)) $$

所以可以得到

$$ H^n(\mathrm{Hom}(P_\bullet, N)) = {}_{\uparrow}E_2^{n,0} \cong H^n(\mathrm{Tot}(\mathrm{Hom}(P_\bullet, I^\bullet))) \cong {}_{\to}E_2^{0,n} = H^n(\mathrm{Hom}(M, I^\bullet)) $$

所以得到了 Ext 的平衡性，于是我们可以自由地计算 Tor 与 Ext.

2.11 左导出函子的性质，Tor，挠与平坦

我们要说明一个非常重要的引理，即零调分解引理.

引理 2.11.1: 零调消解引理

设 $F : \mathcal{A} \to \mathcal{B}$ 是 *Abel* 范畴上的右正合函子，$\mathcal{A}$ 有足够的投射对象，如果

$$ \cdots \to X_2 \to X_1 \to X_0 \to M \to 0 $$

是一个 $\mathcal{A}$ 中正合列，且每个 X_n 都是 F-零调的(即 $L_kF(X_n) = 0$ 对所有 $k > 0$)，则

$$ L_nF(M) \cong H_n(F(X_\bullet)) $$

> **Remark 2.11.1**
> 这个引理的强大在于允许我们使用更广泛的正合消解来计算导出函子.

证明: 对于 $n = 0$，由于 F 是右正合函子，作用于正合列后末端保持正合：

$$ F(X_1) \xrightarrow{F(d_1)} F(X_0) \xrightarrow{F(\varepsilon)} F(M) \to 0 $$

因此 $H_0(F(X_\bullet)) = F(X_0)/\mathrm{im}F(d_1) \cong F(M) \cong L_0F(M)$，结论成立. 对于 $n \geq 1$，令 $K_n = \ker(d_n) = \mathrm{im}(d_{n+1})$.我们可以截取出如下正合列：

$$ 0 \to K_n \xrightarrow{i_n} X_{n-1} \xrightarrow{d_{n-1}} X_{n-2} \to \cdots \to X_1 \xrightarrow{d_1} X_0 \xrightarrow{\varepsilon} M \to 0 $$

由于 X_i 均为 F-零调对象，直接利用定理 2.8.4 可直接得出：

$$L_nF(M) = L_{(n-1)+1}F(M) \cong \mathrm{Ker}(F(K_n) \xrightarrow{F(i_n)} F(X_{n-1})) \tag{2.1}$$

接下来计算复形同调群 $H_n(F(X_\bullet)) = \mathrm{Ker}F(d_n)/\mathrm{Im}F(d_{n+1})$.考虑原长正合列在 X_n 处的分解：

$$X_{n+1} \xrightarrow{d_{n+1}} X_n \xrightarrow{\pi_n} K_n \to 0$$

由 F 的右正合性，应用后此序列依然在末端正合：

$$F(X_{n+1}) \xrightarrow{F(d_{n+1})} F(X_n) \xrightarrow{F(\pi_n)} F(K_n) \to 0$$

这说明 $F(\pi_n)$ 必为满射，并且 $\mathrm{Ker}F(\pi_n) = \mathrm{Im}F(d_{n+1})$. 同时，由于 $d_n = i_n \circ \pi_n$，故有 $F(d_n) = F(i_n) \circ F(\pi_n)$. 对于任意 $x \in F(X_n)$，

$$x \in \mathrm{Ker}F(d_n) \iff F(\pi_n)(x) \in \mathrm{Ker}F(i_n)$$

即 $\mathrm{Ker}F(d_n)$ 正好是 $\mathrm{Ker}F(i_n)$ 在映射 $F(\pi_n)$ 下的原像. 所以有交换图：

$$\begin{array}{ccccc} FX_n & \xrightarrow{F\pi_n} & FK_n & \xrightarrow{Fi_n} & FX_{n-1} \\ \uparrow & & \uparrow & & \\ \mathrm{Ker}\, Fd_n & \xrightarrow{F\pi_n} & \mathrm{Ker}\, Fi_n & & \end{array}$$

由同态定理可以得到：

$$H_n(F(X_\bullet)) = \frac{\mathrm{Ker}F(d_n)}{\mathrm{Im}F(d_{n+1})} = \frac{\mathrm{Ker}F(d_n)}{\mathrm{Ker}F(\pi_n)} \cong F(\pi_n)(\mathrm{Ker}F(d_n)) = \mathrm{Ker}F(i_n)$$

结合公式 (2.1)，我们得到 $\forall n \geq 1$：

$$L_nF(M) \cong \mathrm{Ker}F(i_n) \cong H_n(F(X_\bullet))$$

证明完毕. □

引理 2.11.2: 暂时存疑

F 是左伴随，则投射对象的滤过余极限是 F-零调的.

证明: 我们暂时承认它. □

定理 2.11.1: 左导出与滤过余极限交换

设 $\mathscr{A}$ 与 $\mathscr{B}$ 是满足 *(AB5)* 的 *Abel* 范畴，$\mathscr{A}$ 有足够投射对象，$F\colon \mathscr{A} \to \mathscr{B}$ 是左伴随，则 $L_\bullet F$ 与滤过余极限交换，即对滤过图表 I，有

$$L_nF(\operatorname*{colim}_{i\in I} A_i) = \operatorname*{colim}_{i\in I}(L_nF(A_i))$$

证明: 由于 F 是左伴随，所以与任意余极限交换，而 (AB5) 保证了滤过余极限是正合的，现在考虑 A_i 的投射消解 $P_{i,\bullet} \to A_i$，所以我们有正合消解

$$\operatorname*{colim}_{i\in I} P_{i,\bullet} \to \operatorname*{colim}_{i\in I} A_i$$

由于 $\operatorname*{colim}_{i\in I} P_{i,n}$ 是 F-零调的，所以我们知道

$$\begin{aligned} L_nF(\operatorname*{colim}_{i\in I} A_i) &\cong H_n(F(\operatorname*{colim}_{i\in I} A_i)) \\ &\cong H_n(\operatorname*{colim}_{i\in I} F(A_i)) \\ &\cong \operatorname*{colim}_{i\in I} H_n(F(A_i)) \\ &\cong \operatorname*{colim}_{i\in I} LF_n(A_i) \end{aligned}$$

得证. □

推论 2.11.1

由于 *tensor* 是 *hom* 的左伴随，所以 Tor 保持滤过余极限，再结合张量积是典范交换的，故

$$\operatorname{Tor}_n(A, \operatorname*{colim}_{\textit{filtered}} B_i) = \operatorname*{colim}_{\textit{filtered}} \operatorname{Tor}_n(A, B_i), \quad \operatorname{Tor}_n(\operatorname*{colim}_{\textit{filtered}} A_i, B) = \operatorname*{colim}_{\textit{filtered}} \operatorname{Tor}_n(A_i, B)$$

命题 2.11.1

投射对象的任意直和*(若存在)*还是投射对象.

证明: 注意到 P 投射当且仅当对任意的满射 $A \to B$ 都有 $\operatorname{Hom}(P, A) \to \operatorname{Hom}(P, B)$ 满射，注意到

$$\operatorname{Hom}(\bigoplus P_i, A) \cong \prod \operatorname{Hom}(P_i, A) \to \prod \operatorname{Hom}(P_i, B) \cong \operatorname{Hom}(\bigoplus P_i, B)$$

是满射，所以是投射对象. □

命题 2.11.2

在余完备的 *Abel* 范畴 $\mathscr{A}$ 中，若有足够投射对象，且任意直和函子是正合函子，若 F 是一个左伴随，则有

$$L_\bullet F\left(\bigoplus A_i\right) \cong \bigoplus L_\bullet F(A_i)$$

Remark 2.11.2
模范畴与层范畴的任意直和都是正合的.

我们熟知下面的引理：

引理 2.11.3

PID 上自由模的子模都自由，从而 PID 上投射模自由.

命题 2.11.3: Abel 群上的 Torsion

A, B 是 Abel 群，即 $\mathbb{Z}$-模，则

(1) 对 $n \geq 2$，有 $\mathrm{Tor}_n^{\mathbb{Z}}(A, B) = 0$.

(2) $\mathrm{Tor}_n^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, B) = \begin{cases} B/mB, & n = 0 \\ {}_mB = \{b \in B : mb = 0\}, & n = 1 \end{cases}$. 其中 ${}_mB$ 是 B 的 m-挠部分.

证明: 由于 $\mathbb{Z}$ 是 PID，所以其上自由模的子模自由，所以考虑 A 的投射消解

$$0 \to \mathrm{Ker}\,\varepsilon \to P_0 \xrightarrow{\varepsilon} A \to 0$$

其中 $\mathrm{Ker}\,\varepsilon$ 是投射模 P_0 的子模，由于投射 $\mathbb{Z}$-模自由，所以 $\mathrm{Ker}\,\varepsilon$ 是自由模的子模，所以自由，从而投射，所以 A 是有限长度消解，故可以看出来当 $n \geq 2$ 时导出都是 0，现在只需要计算 $n = 0, 1$ 的情况即可，注意

$$\mathrm{Tor}_0^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, B) = \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} B \cong B/mB$$

而

$$\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, B) = \mathrm{Ker}\,(m\mathbb{Z}B \to \mathbb{Z}B) = {}_mB$$

故得证. □

Remark 2.11.3
注意到我们的论证对于 PID 都是对的.

若我们赋予正整数整数意义下的偏序，则构成一个滤过集，我们有

$$\mathbb{Q}/\mathbb{Z} = \operatorname*{colim}_n \mathbb{Z}/n\mathbb{Z}$$

所以 $\mathbb{Q}/\mathbb{Z}$ 是一个滤过余极限，于是

$$\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, B) = \operatorname*{colim}_n \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, B) = \operatorname*{colim}_n {}_nB = \mathrm{Tor}(B)$$

所谓 $\mathrm{Tor}(B)$ 即 B 的挠部分. 这也解释了 Torsion 函子的名字.

定理 2.11.2: 平坦刻画

下列关于 R-模 M 的条件是等价的:

(1) M 平坦.

(2) 对任意的 $n>0$，R-模 N，都有 $\mathrm{Tor}_n(M,N)=0$.

(3) 对任意的 R-模 N，$\mathrm{Tor}_1(M,N)=0$.

(4) 对 R 的所有理想 I，都有 $\mathrm{Tor}_1(M,R/I)=0$.

(5) 对 R 的所有有限生成理想 I，都有 $\mathrm{Tor}_1(M,R/I)=0$.

证明: (1) 推 (2) 推 (3) 推 (4) 推 (5) 是显然的，因为平坦模的张量积是正合函子，所以正次数导出都是 0，现在证 (5) 推 (4)，只需要注意到任意理想都是有限生成理想的滤过余极限，而张量积作为左伴随和余极限交换，所以自然得证. (4) 推 (3) 我们可以归纳地证明对有限生成模是正确的，由于 R/I 是一个元素生成的模，所以 $k=1$ 得证，下面我们假设 $<k$ 时成立，则取 N 是一个 k 个元素生成的模，R/I 为第 k 个生成元生成的循环子模，则

$$0\to K\to N\to R/I\to 0$$

是正合列，其中 K 是前 $k-1$ 个元素生成的模，而

$$I=\mathrm{Ker}(R\to \mathrm{Coker}(K\to N))$$

对其使用长正合列得到

$$\mathrm{Tor}_1(M,K)\to \mathrm{Tor}_1(M,N)\to \mathrm{Tor}_1(M,R/I)$$

由归纳假设 $\mathrm{Tor}_1(M,K)=0$，而条件告诉我 $\mathrm{Tor}_1(M,R/I)=0$，于是可以知道有限生成模都是对的，然后利用滤过余极限得到任意模都是对的. 现在证明 (3) 推 (1)，这只需要注意到对任意的模正合列

$$0\to N'\to N\to N''\to 0$$

考虑其长正合列

$$0=\mathrm{Tor}_1(M,N'')\to M\otimes N'\to M\otimes N\to M\otimes N''\to 0$$

所以平坦. □

推论 2.11.2

我们立刻注意到，在任意整环 R 上，平坦都可以推出无挠.

命题 2.11.4: PID 上平坦等价于无挠

R 是 PID，则

(1) A 是无挠 R-模，则 $\mathrm{Tor}_n(A,B)=0$ 对任意 $n>0$，R-模 B 都成立.

(2) A 是无挠 R-模当且仅当 $\mathrm{Tor}_1(A,B)=0$ 对任意 R-模 B 成立.

(3) A 平坦当且仅当无挠.

证明: 由于无挠模是有限生成无挠子模在包含关系下的滤过余极限，所以只需要对有限生成的情况考虑，而 PID 上有限生成模的结构定理告诉我们有限生成无挠模就是自由模，在 PID 的语境下自由模和投射模没有区别，所以无挠模是投射模的滤过余极限，故

$$\mathrm{Tor}_n(A,B)=\operatorname{colim}\mathrm{Tor}(P_i,B)=0$$

于是 (1) 得证，而 (2)(3) 是同一个命题的不同叙述，无挠我们已经证明 $\mathrm{Tor}_1(A,B)=0$ 对任意 B 成立，而这等价于平坦，所以无挠可以推平坦，下面我们要用平坦推无挠，考虑 $r\in R$，则有

$${}_rA=\mathrm{Tor}_1(A,R/(r))$$

而平坦告诉我后者为 0，于是无挠. □

此外，由于平坦模是 $\otimes$ 函子的零调对象，所以有零调消解定理我们知道 Tor 函子也可以使用平坦消解得到.

定理 2.11.3: 平坦消解计算 Tor

A,B 是 R-模，若 A 存在平坦模的消解

$$\cdots\to M_2\to M_1\to M_0\to A\to 0$$

则有

$$\mathrm{Tor}_n(A,B)=H_n(M_\bullet\otimes B)$$

若 $f\colon R\to T$ 是环同态，并且满足在这个同态下 T 是平坦 R-模，则称 f 是平坦环同态. 很显然若 $f\colon R\to T$ 是平坦环同态，则 $-\otimes_R T$ 是正合函子. 经典例子就是局部化嵌入是平坦环同态：$R\to S^{-1}R$.

引理 2.11.4

$R\to T$ 是平坦环同态，若 P 是投射 R-模，则 $P\otimes_R T$ 是投射 T-模.

证明: 注意到

$$P\oplus Q=\bigoplus R$$

所以

$$P\otimes_R T\oplus Q\otimes_R T\cong(\bigoplus R)\otimes_R T\cong\bigoplus(R\otimes_R T)\cong\bigoplus T$$

所以 $P\otimes_R T$ 仍然是自由 T-模的直和项，所以投射. □

命题 2.11.5: 平坦基变换

设 $R\to T$ 是平坦环同态，则对 R-模 M 和 T-模 N 有

$$\mathrm{Tor}_n^R(M,N)=\mathrm{Tor}_n^T(M\otimes_R T,N)$$

作为推论，由于 $R\to T$ 是平坦环同态，则 $-\otimes_R T$ 正合，则对一切 R-模 M,N 都有

$$T\otimes_R\mathrm{Tor}_n^R(M,N)\cong\mathrm{Tor}_n^T(M\otimes_R T,N\otimes_R T)$$

证明: 取投射消解 $P_\bullet\to M$，则左边是 $P_\bullet\otimes N$ 的同调群，由于 T 是平坦 R-模，于是 $P_\bullet\otimes_R T\to M\otimes_R T$ 是投射消解，右边也是 $(P_\bullet\otimes_R T)\otimes_T N\cong P_\bullet\otimes_R N$ 的同调群，得证. 后面的推论是导出函子与正合函子交换的直接推论. □

推论 2.11.3

由于 $R\to S^{-1}R$ 是平坦环同态，所以

$$S^{-1}\mathrm{Tor}_n^R(M,N)=\mathrm{Tor}_n^{S^{-1}R}(S^{-1}M,S^{-1}N)$$

2.12 右导出函子的性质，Ext 与扩张

同理我们也有对右导出的零调消解引理，即可以用零调对象的消解计算右导出，不再赘述. 对投射情况对偶，我们有

命题 2.12.1

内射对象的任意直积还是内射对象.

环 R 上的模 M 可除是指对任意非零因子 $r\in R\setminus\mathrm{Ann}(M)$，总有 $rM=M$. 放在 $\mathbb{Z}$ 上就是指可以被 n 等分，所以称之为可除.

引理 2.12.1

内射模总是可除的.

证明: 若 M 是内射模，则对 $r \notin \mathrm{Ann}(M)$，$\times r\colon M \to M$ 是单射，所以由内射知道

$$\mathrm{Hom}_R(M,M) \to \mathrm{Hom}_R(M,M)$$

是满射，注意到 $\mathrm{Hom}_R(M,M) \cong M$，所以等价于 $\times r\colon M \to M$ 还是满射，故知道可除. □

定理 2.12.1: 内射模的同调刻画

下列关于 R-模 N 的条件是等价的:

(1) N 是内射模.

(2) 对所有的 $n>0$ 以及任意的 R-模 M，$\mathrm{Ext}^n(M,N)=0$.

(3) 对任意的 R-模 M，$\mathrm{Ext}^1(M,N)=0$.

(4) 对任意的 R 的理想 I，$\mathrm{Ext}^1(R/I,N)=0$.

证明: (1) 一路推到 (4) 是显然的，(4) 推 (1) 即 Baer 准则. □

定理 2.12.2: Dedekind 整环上内射模的刻画

Dedekind 整环上内射等价于可除.

证明: 根据 Baer 准则，为证 M 是内射模，只需证明对 R 的任意非零理想 I 及任意 R-模同态 $f: I \to M$，均可延拓为 $R \to M$ 的同态. 即需在 M 中找到 $\hat{m} \in M$，使得对所有 $x \in I$，均有 $f(x) = x\hat{m}$. 因为 R 是 Dedekind 整环，对给定的非零理想 I，存在另一个非零理想 J 使得它们互素(即 $I+J=R$)，且其乘积 $IJ=(c)$ 为非零主理想. 考虑将 f 限制在 (c) 上. 设 $f(c)=m_0$. 因为 M 是可除模，存在 $m_c \in M$ 使得 $cm_c = m_0$. 对于任意 $y \in (c)$，设 $y=rc$ $(r \in R)$，则有:

$$f(y) = f(rc) = rf(c) = rm_0 = rcm_c = ym_c$$

由 $I+J=R$，存在 $a \in I$ 与 $b \in J$ 使得 $a+b=1$. 在 M 中构造元素 $\hat{m} = f(a) + bm_c$. 对于任意给定的 $x \in I$，计算 $x\hat{m}$:

$$x\hat{m} = x(f(a)+bm_c) = f(xa) + (xb)m_c$$

由于 $x \in I$ 且 $b \in J$，它们的乘积落在交集中，即 $xb \in IJ = (c)$. 由前述对理想 (c) 的性质可知，对于 (c) 中的元素 xb，有 $(xb)m_c = f(xb)$. 将其代入上式可得:

$$x\hat{m} = f(xa) + f(xb) = f(xa+xb) = f(x(a+b)) = f(x\cdot 1) = f(x)$$

综上所述，我们找到了 $\hat{m} \in M$ 满足 $f(x) = x\hat{m}$ 对所有 $x \in I$ 成立，即同态 f 成功延拓至整个 R. 由 Baer 准则知，M 是内射模. □

推论 2.12.1: PID 上模的刻画

注意到 *PID* 是 *Dedekind* 整环，所以 *PID* 上内射等价于可除. 于是我们彻底分类了 *PID* 上的内射模，投射模和平坦模. 即在 *PID* 上内射等价于可除，平坦等价于无挠，投射等价于自由.

定理 2.12.3: 投射模的同调刻画

下面关于 R-模 M 的条件是等价的：

(1) M 是投射模.

(2) 对所有的 $n>0$ 以及任意的 R-模 N，都有 $\mathrm{Ext}^n(M,N)=0$.

(3) 对任意的 R-模 N，$\mathrm{Ext}^1(M,N)=0$.

容易计算得到：

命题 2.12.2: Ext 的性质

A,B 是 $\mathbb{Z}$-模，即 *Abel* 群，则

(1) $\mathrm{Ext}^n_{\mathbb{Z}}(A,B)=0$，$\forall n\geq 2$.

(2) 对任意 *Abel* 群 B，$\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},B)={}_mB$，$\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z},B)=B/mB$.

(3) 对任意 *Abel* 群 B，$\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z},B)=B$，$\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z},B)=0$.

(4) 对任意 R-模 $\{M_i\}$，都有

$$\mathrm{Ext}^n_R\left(\bigoplus_{i\in I}M_I,N\right)\cong\prod_{i\in I}\mathrm{Ext}^n_R(M_i,N)$$

$$\mathrm{Ext}^n_R\left(N,\prod_{i\in I}M_I\right)\cong\prod_{i\in I}\mathrm{Ext}^n_R(N,M_i)$$

(5) 对于有限生成 *Abel* 群 A，总是可以计算 $\mathrm{Ext}^n_{\mathbb{Z}}(A,B)$.

我们称一个 R-模 A 是有限展示的，如果存在有限秩自由模 R^m 与 R^n 使得存在正合列

$$R^m\to R^n\to A\to 0$$

即 A 是有限生成且约束关系有限的模.

命题 2.12.3

若 A 是一个有限展示模，则对于 R 的任意乘性子集，有同构

$$S^{-1}\operatorname{Hom}_R(A,B)\cong\operatorname{Hom}_{S^{-1}R}(S^{-1}A,S^{-1}B)$$

证明: 很显然当 $A=R$ 的时候是同构的，并且由于 Hom 是加性函子，所以当 $A=R^m$ 的时候也是同构的，注意下图：

$$\begin{array}{ccccccc}
R^m & \longrightarrow & R^n & \longrightarrow & A & \longrightarrow & 0 \\
0 & \longrightarrow & \operatorname{Hom}_R(A,B) & \longrightarrow & \operatorname{Hom}_R(R^n,B) & \longrightarrow & \operatorname{Hom}_R(R^m,B) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & S^{-1}\operatorname{Hom}_R(A,B) & \longrightarrow & S^{-1}\operatorname{Hom}_R(R^n,B) & \longrightarrow & S^{-1}\operatorname{Hom}_R(R^m,B) \\
 & & \downarrow & & \downarrow\cong & & \downarrow\cong \\
0 & \longrightarrow & \operatorname{Hom}_{S^{-1}R}(S^{-1}A,S^{-1}B) & \longrightarrow & \operatorname{Hom}_{S^{-1}R}(S^{-1}R^n,S^{-1}B) & \longrightarrow & \operatorname{Hom}_{S^{-1}R}(S^{-1}R^m,S^{-1}B)
\end{array}$$

5-引理告诉我们左边是同构. □

定理 2.12.4: Ext 与局部化交换

R 是一个 *Noether* 环，A 是一个有限生成 R-模. 则对任意的乘性子集 S，任意的 R-模 B，都有

$$S^{-1}\operatorname{Ext}^n_R(A,B)=\operatorname{Ext}^n_{S^{-1}R}(S^{-1}A,S^{-1}B)$$

证明: 取 A 的一个自由消解 $F_\bullet\to A$，其中 F_i 都是有限生成的自由 R-模，则 $S^{-1}F_\bullet\to S^{-1}A$ 也是有限生成自由 $S^{-1}R$-模的消解(注意局部化是正合函子). 所以

$$\begin{aligned}
S^{-1}\operatorname{Ext}^n_R(A,B) &= S^{-1}(H^n(\operatorname{Hom}_R(F_\bullet,B)))\cong H^n(S^{-1}\operatorname{Hom}_R(F_\bullet,B)) \\
&\cong H^n(\operatorname{Hom}_{S^{-1}R}(S^{-1}F,S^{-1}B))=\operatorname{Ext}^n_{S^{-1}R}(S^{-1}A,S^{-1}B)
\end{aligned}$$

故得证. □

下面我们讨论 Ext 与扩张的关系.

定义 2.12.1: Abel 范畴中的扩张

Abel 范畴 $\mathscr{A}$ 中过对象 x,y 的**扩张**指短正合列 $0\to y\to z\to x\to 0$ 的一个等价类，称前者与 $0\to y\to z'\to x\to 0$ 等价当且仅当下图交换

$$\begin{array}{ccccccccc}
0 & \longrightarrow & y & \longrightarrow & z & \longrightarrow & x & \longrightarrow & 0 \\
 & & \downarrow= & & \downarrow & & \downarrow= & & \\
0 & \longrightarrow & y & \longrightarrow & z' & \longrightarrow & x & \longrightarrow & 0
\end{array}$$

实际上由 5-引理知道 $z\to z'$ 是同构.

定理 2.12.5: Baer 和

给定 *Abel* 范畴 $\mathscr{A}$ 中的两个对象 x, y，x 过 y 做的所有扩张构成一个 *Abel* 群，其中单位元为 $0 \to y \to y \oplus x \to x \to 0$. 而对两个不同的扩张 z, z'，构造他们的和如下：考虑 p 为 $z \to x \leftarrow z'$ 的拉回，即

$$p = \{(c, c') \in z \oplus z' : \overline{c} = \overline{c'}\}$$

将 p 商掉 $\{(b, -b) : b \in y\}$ 定义为 z'' 即可. 逆元 $z \to x$ 为 $-(z \to x) : z \to x$.

通过一些繁琐的验证可以得到这个定理，这个定理允许我们将 x 过 y 的所有扩张看成是一个 Abel 群，而下面的定理告诉了我们 Ext 与之的关系.

定理 2.12.6: 模范畴扩张的 Ext 刻画

对两个 R-模 M, N，M 过 N 的扩张在 *Baer* 和意义下构成的 *Abel* 群同构于 $\mathrm{Ext}^1_R(M, N)$. 对应关系为

$$0 \to N \to X \to M \to 0$$

送到其诱导的长正合列

$$\mathrm{Hom}_R(N, N) \to \mathrm{Ext}^1_R(M, N)$$

所诱导的 id_N 的像. 反过来对 $x \in \mathrm{Ext}^1_R(M, N)$，与投射模 P 使得

$$0 \to K \to P \to M \to 0$$

正合，诱导长正合列

$$\mathrm{Hom}(K, N) \to \mathrm{Ext}^1_R(M, N) \to 0\, \mathrm{Ext}^1_R(P, N) = 0$$

从而可以任取 x 的原像 $\beta : K \to N$，考虑 $P \leftarrow K \to N$ 的推出 X，检查这诱导了

$$0 \to N \to X \to M \to 0$$

的正合列.

证明略去不表，定理表明若 $\mathrm{Ext}^1(M, N) = 0$，则其对应的扩张 Abel 群只有幺元，即只有分裂正合列，于是我们得到下面的推论：

推论 2.12.2: 投射，内射与分裂

考虑模的短正合列

$$0 \to I \to M \to P \to 0$$

若 P 是投射模或者 I 是内射模，则此正合列分裂.

证明: 考虑 $\mathrm{Ext}^1(P, I) = 0$ 立刻得到. □

2.13 万有系数定理

定理 2.13.1: 同调万有系数定理(UCT)

设 $P_\bullet$ 是由平坦 R-模构成的链复形，满足 $d(P_n) \subset P_{n-1}$ 也是平坦 R-模，则对 R-模 M 由如下的短正合列

$$0 \to H_n(P_\bullet) \otimes_R M \to H_n(P_\bullet \otimes_R M) \to \operatorname{Tor}_1^R(H_{n-1}(P_\bullet), M) \to 0$$

证明: 观察正合列

$$0 \to K_n \to P_n \to d(P_n) \to 0$$

对任意模 M 由 Tor 导出的长正合列为

$$\operatorname{Tor}_2(d(P_n), M) \to \operatorname{Tor}_1(K_n, M) \to \operatorname{Tor}_1(P_n, M)$$

由于前后都是平坦模的正次数导出，所以自然是 0，所以 $\operatorname{Tor}_1(K_n, M) = 0$ 对任意 M 成立，所以 K_n 是平坦模. 这样我们再考虑长正合列的另外一部分

$$0 = \operatorname{Tor}_1(d(P_n), M) \to K_n \otimes M \to P_n \otimes M \to d(P_n) \otimes M \to 0$$

因此

$$0 \to K_n \otimes M \to P_n \otimes M \to d(P_n) \otimes M \to 0$$

正合，若令 $K_\bullet$ 与 $d(P_\bullet)$ 的微分为 0 映射，则我们立刻得到一个复形短正合列

$$0 \to K_\bullet \otimes M \to P_\bullet \otimes M \to d(P_\bullet) \otimes M \to 0$$

写出其同调长正合列得到

$$\begin{array}{ccccccccc} H_{n+1}(d(P_\bullet) \otimes_R M) & \xrightarrow{\partial} & H_n(K_\bullet \otimes_R M) & \to & H_n(P_\bullet \otimes_R M) & \to & H_n(d(P_\bullet) \otimes_R M) & \xrightarrow{\partial} & H_{n-1}(K_\bullet \otimes_R M) \\ \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle =} & & & & \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle =} \\ d(P_{n+1}) \otimes_R M & & K_n \otimes_R M & & & & d(P_n) \otimes_R M & & K_{n-1} \otimes_R M \end{array}$$

具体计算可以发现所谓的 ∂ 实际上就是 $i \otimes \mathrm{id}_M$，其中 i 为

$$0 \to d(P_{n+1}) \xrightarrow{i} K_n \to H_n(P_\bullet) \to 0$$

由于 k_n 和 $d(P_{n+1})$ 都是平坦模，所以这是 $H_n(P_\bullet)$ 的平坦消解，因此

$$\operatorname{Tor}_1^R(H_n(P_\bullet), M) = \operatorname{Ker}\left(d(P_{n+1} \otimes_R M) \to K_n \otimes_R M\right) = \operatorname{Ker} \partial_n$$

而

$$H_{n+1}(P_\bullet) \otimes_R M = \operatorname{Tor}_0^R(H_{n+1}(P_\bullet), M) = \operatorname{Coker}\left(d(P_{n+1} \otimes_R M) \to K_n \otimes_R M\right) = \operatorname{Coker} \partial_{n+1}$$

而

$$\operatorname{Coker}\partial_{n+1}=\operatorname{Im}\left(H_n(K_\bullet\otimes_R M)\to H_n(P_\bullet\otimes_R M)\right)=\operatorname{Ker}\left(H_n(P_\bullet\otimes_R M)\to H_n(d(P_\bullet)\otimes_R M)\right)$$

于是得到正合列

$$0\to\operatorname{Ker}f\to H_n(P_\bullet\otimes_R M)\to\operatorname{Im}f\to 0$$

其中 $f\colon H_n(P_\bullet\otimes_R M)\to H_n(d(P_\bullet)\otimes_R M)$，故得到

$$0\to H_{n+1}(P_\bullet)\otimes_R M\to H_{n+1}(P_\bullet\otimes_R M)\to\operatorname{Tor}_1^R(H_n(P_\bullet),M)\to 0$$

平移一下下标就得到题目要证的. □

推论 2.13.1

如果 P_n 与 $d(P_n)$ 都是投射模，则所得的正合列(非典范地)分裂，换言之

$$H_n(P_\bullet\otimes_R M)=(H_n(P_\bullet)\otimes_R M)\oplus\operatorname{Tor}_1^R(H_{n-1}(P_\bullet),M)$$

由于自由 *Abel* 子群自由，所以 $\mathbb{Z}$-模的投射消解满足条件.

证明: 由投射，知道短正合列

$$0\to K_n\to P_n\to d(P_n)\to 0$$

分裂，故

$$P_n\cong K_n\oplus d(P_n)$$

作用 $-\otimes_R M$ 得到 $K_n\otimes_R M$ 是 $P_n\otimes_R M$ 的直和分量，而很显然 $\operatorname{Ker}\left(P_n\otimes_R M\to P_{n-1}\otimes_R M\right)$ 是包含 $K_n\otimes_R M$ 的子空间，从而 $K_n\otimes_R M$ 是上述核的直和分量，注意到

$$\frac{\operatorname{Ker}\left(P_n\otimes_R M\to P_{n-1}\otimes_R M\right)}{\operatorname{Im}\left(P_{n+1}\otimes_R M\to P_n\otimes_R M\right)}=H_n(P_\bullet\otimes_R M),\quad \frac{\operatorname{Ker}(P_n\to P_{n-1})\otimes_R M}{\operatorname{Im}\left(P_{n+1}\otimes_R M\to P_n\otimes_R M\right)}=H_n(P_\bullet)\otimes_R M$$

因此知道 $H_n(P_\bullet)\otimes_R M$ 是 $H_n(P_\bullet\otimes_R M)$ 的直和分量，利用前面的正合立刻得到分裂. □

之所以称之为万有系数定理，是因为在代数拓扑中很多同调是 $\mathbb{Z}$-系数的，而万有系数定理允许我们将 $\mathbb{Z}$ 系数的转化为其他 Abel 群系数. 同理我们可以得到上同调的万有系数定理：

定理 2.13.2: 上同调万有系数定理

考虑 R-模 M，对一族由投射模 $P_\bullet$ 组成的复形 $P_\bullet$，且满足 $d(P_n)$ 也是投射的，则对任意 R-模 M 都有如下正合列

$$0\to\operatorname{Ext}_R^1(H_{n-1}(P_\bullet),M)\to H^n(\operatorname{Hom}_R(P_\bullet,M))\to\operatorname{Hom}_R(H_n(P_\bullet),M)\to 0$$

由于本身有投射条件，同理可以得到分裂(非典范)

$$H^n(\operatorname{Hom}_R(P_\bullet,M))\cong\operatorname{Ext}_R^1(H_{n-1}(P_\bullet),M)\oplus\operatorname{Hom}_R(H_n(P_\bullet),M)$$

2.14 Künneth 公式

定理 2.14.1: 复形的 Künneth 公式

$P_\bullet, Q_\bullet$ 为 R-模复形，P_n 与 $d(P_n)$ 平坦，则有短正合列

$$0 \to \bigoplus_{p+q=n} H_p(P_\bullet) \otimes_R H_q(Q_\bullet) \to H_n\left(\mathrm{Tot}^{\oplus}(P_\bullet \otimes Q_\bullet)\right) \to \bigoplus_{p+q=n-1} \mathrm{Tor}_1^R(H_p(P_\bullet), H_q(Q_\bullet)) \to 0$$

若 P_n 与 $d(P_n)$ 投射，则上述正合列(非典范)分裂.

定理 2.14.2: 上复形的 Künneth 公式

$P_\bullet, Q^\bullet$ 为 R-模复形与 R-模上复形，P_n 与 $d(P_n)$ 投射，则有分裂短正合列

$$0 \to \prod_{p+q=n-1} \mathrm{Ext}_R^1(H_p(P_\bullet), H^q(Q^\bullet)) \to H^n\left(\prod \mathrm{Tot}\,(P_\bullet \otimes Q^\bullet)\right) \to \prod_{p+q=n} \mathrm{Hom}_R(H_p(P_\bullet), H^q(Q^\bullet)) \to 0$$

2.15 谱序列 1：滤过

2.16 谱序列 2：双复形

2.17 谱序列 3：正合偶

2.18 同调维数

2.19 群同调与群上同调

群的同调理论主要研究 $\mathbf{Mod}_{\mathbb{Z}[G]}$ 到自身的两个函子 $-^G$ 与 $-_G$.

定义 2.19.1: 群同调和群上同调

对于一个 $\mathbb{Z}[G]$-模 M，我们定义

$$M^G = \{x \in M : gx = x \ \forall g \in G\} = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$$

$$M_G = M/\operatorname{Span}_{\mathbb{Z}[G]}\{gx - x : x \in M, g \in G\} = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M$$

其中 $\mathbb{Z}$ 视为平凡 $\mathbb{Z}[G]$-模. 可见 M^G 为 M 的最大平凡子模，M_G 为 M 的最大平凡商模. 易见这两个函子为伴随关系，因为

$$\mathrm{Hom}_{\mathbb{Z}[G]}(A_G, B) = \mathrm{Hom}_{\mathbb{Z}[G]}(A \otimes_{\mathbb{Z}[G]} \mathbb{Z}, B) = \mathrm{Hom}_{\mathbb{Z}[G]}(A, \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, B)) = \mathrm{Hom}_{\mathbb{Z}[G]}(A, B^G)$$

因此 $-_G$ 是左伴随故右正合，$-^G$ 是右伴随故左正合，并且模范畴有足够的投射对象和内射对象，我们记对应的导出函子为

$$H^n(G; A) = R^n(-^G)(A), \quad H_n(G; A) = L_n(-_G)(A)$$

分别称为**群上同调函子**和**群同调函子**.

或者我们也可以立刻得到

$$H_n(G; A) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A), \quad H^n(G; A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

定义 2.19.2: 增广理想

对群 G，定义同态

$$\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}, \quad \sum_{g \in G} n_g g \mapsto \sum_{g \in G} n_g$$

令 $\mathfrak{I}_G = \ker \varepsilon$，称为 G 的**增广理想**. 对有限群 G，称 $N = \sum_{g \in G} g$ 为 $\mathbb{Z}[G]$ 的**范数元素**，不难检查有 $gN = N = Ng$，并且有 $\mathbb{Z}[G]^G = \mathbb{Z}[G] \cdot N$. 对无限群 G 而言，$\mathbb{Z}[G]^G = 0$.

显然可以看出

$$\mathfrak{I}_G = \bigoplus_{g \in G \setminus \{1\}} \mathbb{Z}(g - 1)$$

因此有正合列

$$0 \to \mathfrak{I}_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

于是我们立刻可以看到

$$M_G = H_0(G, M) = M/\mathfrak{I}_G M, \quad M^G = H^0(G, M) = \{x \in M : \mathfrak{I}_G x = 0\}$$

定理 2.19.1

对群 G 与 G-模 M，有同调情况下的

$$H_1(G,M)=\mathrm{Ker}\left(\mathfrak{I}_G\otimes_{\mathbb{Z}[G]}M\to\mathfrak{I}_GM\right)$$

与上同调情况下的

$$H^1(G,M)=\mathrm{Coker}\left(M\to\mathrm{Hom}_{\mathbb{Z}[G]}(\mathfrak{I}_G,M)\right)$$

证明: 考虑正合列

$$0\to\mathfrak{I}_G\to\mathbb{Z}[G]\to\mathbb{Z}\to0$$

拉出 Tor 的长正合列:

$$\mathrm{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}[G],M)\to\underbrace{\mathrm{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z},M)}_{=H_1(G,M)}\to\mathfrak{I}_G\otimes_{\mathbb{Z}[G]}M\to\underbrace{\mathbb{Z}[G]\otimes_{\mathbb{Z}[G]}M}_{=M}\to\mathbb{Z}\otimes_{\mathbb{Z}[G]}M\to0$$

由于 $\mathbb{Z}[G]$ 是自由 $\mathbb{Z}[G]$-模，所以投射，故 $\mathrm{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}[G],M)=0$，故上面正合列实际为

$$0\to H_1(G,M)\to\mathfrak{I}_G\otimes_{\mathbb{Z}[G]}M\to M\to\mathbb{Z}\otimes_{\mathbb{Z}[G]}M\to0$$

所以得到同调情况，同理拉出 Ext 的长正合列

$$0\to\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},M)\to M\to\mathrm{Hom}_{\mathbb{Z}[G]}(\mathfrak{I}_G,M)\to H^1(G,M)\to0$$

得到上同调情况. □

引理 2.19.1: 交换化

对群 G，我们有同构 $\mathfrak{I}_G/\mathfrak{I}_G^2\cong G/[G,G]$.

证明: 你会发现左边是线性化的操作，右边是交换化的操作，本质上都是在做交换化，右边的交换化自不必说，左边的交换化可以看成如下:

$$\overline{gh-1}=\overline{(g-1)+(h-1)+(g-1)(h-1)}=\overline{g-1}+\overline{h-1}=\overline{hg-1}$$

线性化将乘法变成了加法，从而自然达成了交换化的成就，具体的构造我们只需要注意

$$\varphi\colon\mathfrak{I}_G/\mathfrak{I}_G^2\to G/[G,G],\quad\overline{x-1}\mapsto\overline{x}$$

容易验证这是交换群的同态，并且单射满射都任意验证. □

命题 2.19.1

作为 $\mathbb{Z}[G]$-模有同构 $H_1(G,\mathbb{Z})=\mathbb{Z}\otimes_{\mathbb{Z}[G]}\mathfrak{I}_G\cong G/[G,G]$ 为 G 的交换化.

证明: 仍然是考虑正合列

$$0 \to \mathfrak{I}_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

导出长正合列得到

$$\mathrm{Tor}_1^{\mathbb{Z}[G]}(\mathbb{Z}, \mathbb{Z}[G]) = H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathfrak{I}_G \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z}[G] \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathbb{Z} \to 0$$

由于 $\mathbb{Z}[G]$ 是投射模，所以最左边为 0，故得到正合列

$$0 \to H_1(G, \mathbb{Z}) \to \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathfrak{I}_G \to \mathbb{Z} \to \mathbb{Z} \to 0$$

由于 $\mathbb{Z} \to \mathbb{Z}$ 是同构，所以由正合可以得到

$$H_1(G, \mathbb{Z}) = \mathbb{Z} \otimes_{\mathbb{Z}[G]} \mathfrak{I}_G = \mathfrak{I}_G / \operatorname{Span}_{\mathbb{Z}[G]}\{(g-1)x \colon x \in \mathfrak{I}_G\} = \mathfrak{I}_G / \mathfrak{I}_G^2 = G/[G,G]$$

故得证. □

所以我们可以看到群的交换化自然地作为群同调的一环出现.

推论 2.19.1: 万有系数定理在群同调的应用

若 A 是平凡 $\mathbb{Z}[G]$-模，则 $H_0(G, A) = A$，对 $n \geq 1$ 有非典范的同构:

$$H_n(G, A) \cong (H_n(G, \mathbb{Z}) \otimes_{\mathbb{Z}} A) \oplus \mathrm{Tor}_1^{\mathbb{Z}}(H_{n-1}(G, \mathbb{Z}), A)$$

对上同调而言，$H^0(G, A) \cong A$，对 $n \geq 1$ 有非典范的同构:

$$H^n(G, A) \cong \mathrm{Hom}_{\mathbb{Z}}(H_n(G, \mathbb{Z}), A) \oplus \mathrm{Ext}_{\mathbb{Z}}^1(H_{n-1}(G, \mathbb{Z}), A)$$

证明: 由于平凡 G-模可以看成是 $\mathbb{Z}$-模，于是两个平凡 $\mathbb{Z}[G]$-模的同态和张量本质上就是两个 $\mathbb{Z}$-模的同态和张量，于是可以都看做在 $\mathbb{Z}$-模上. 由于

$$H_n(G, A) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

考虑 $\mathbb{Z}$ 的 $\mathbb{Z}[G]$-模投射消解 $P_\bullet \to \mathbb{Z}$，我们知道

$$H_n(G, A) = H_n(P_\bullet \otimes_{\mathbb{Z}[G]} A)$$

注意到

$$P_\bullet \otimes_{\mathbb{Z}[G]} A \cong \left(P_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z}\right) \otimes_{\mathbb{Z}} A$$

令 $C_\bullet = P_\bullet \otimes_{\mathbb{Z}[G]} \mathbb{Z}$，很明显有

$$H_n(G, \mathbb{Z}) = H_n(C_\bullet)$$

而 $C_\bullet$ 作为 $\mathbb{Z}$-模是自由 $\mathbb{Z}$-模构成的复形，所以满足万有系数定理的条件，故

$$H_n(G, A) = H_n(C_\bullet \otimes_{\mathbb{Z}} A) = (H_n(C_\bullet) \otimes_{\mathbb{Z}} A) \oplus \mathrm{Tor}_1^{\mathbb{Z}}(H_{n-1}(C_\bullet), A)$$

于是得到同调情况，上同调情况同理. □

推论 2.19.2

若 A 是平凡 G-模，则

$$H_1(G,A)\cong G/[G,G]\otimes_{\mathbb{Z}} A,\quad H^1(G,A)\cong \mathrm{Hom}_{\mathbb{Z}}(G/[G,G],A)$$

或者可以写成

$$H_1(G,A)\cong \mathfrak{I}_G\otimes_{\mathbb{Z}[G]} A,\quad H^1(G,A)=\mathrm{Hom}_{\mathbb{Z}[G]}(\mathfrak{I}_G,A)$$

证明: 只需要注意到

$$\mathrm{Tor}_1^{\mathbb{Z}}(H_0(G,\mathbb{Z}),A)=\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Z},A)=0$$
$$\mathrm{Ext}^1_{\mathbb{Z}}(H_0(G,\mathbb{Z}),A)=\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z},A)=0$$

于是立刻得到前两个等式，后两个等式注意命题 2.19.1 即可. □

2.20 Bar 消解

一个紧要的问题就是为 $\mathbb{Z}$ 寻找一个方便计算的 $\mathbb{Z}[G]$-模的消解.

定义 2.20.1: Bar 消解的模

设 G 为一个群，$\mathbb{Z}G$ 为其群环. 第 n 阶自由 $\mathbb{Z}G$-模 F_n 定义为由 G 中元素的 n 元组 $[g_1|g_2|\dots|g_n]$ 生成的自由模. 特别地，F_0 是由空符号 [] 生成的自由模.

定义 2.20.2: [边缘算子]

定义边缘映射 $\partial_n: F_n\to F_{n-1}$ 为如下交错和:

$$\partial_n([g_1|g_2|\dots|g_n])=g_1[g_2|\dots|g_n]+\sum_{i=1}^{n-1}(-1)^i[g_1|\dots|g_ig_{i+1}|\dots|g_n]+(-1)^n[g_1|\dots|g_{n-1}]$$

特别地，对于低阶映射展开如下:

- 增广映射 $\varepsilon(g[])=1$
- $\partial_1([g])=g[]-[]$
- $\partial_2([g_1|g_2])=g_1[g_2]-[g_1g_2]+[g_1]$
- $\partial_3([g_1|g_2|g_3])=g_1[g_2|g_3]-[g_1g_2|g_3]+[g_1|g_2g_3]-[g_1|g_2]$

定理 2.20.1: Bar 消解

由上述 F_n 和 ∂_n 构成的序列：

$$\dots \xrightarrow{\partial_3} F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0$$

是一个链复形，且它是平凡 $\mathbb{Z}G$-模 $\mathbb{Z}$ 的一个显式标准自由消解，称为 *Bar* 消解.

证明: 通过直接代数计算可以验证 $\partial_{n-1} \circ \partial_n = 0$，这保证了序列构成一个链复形. 可以构造同伦如下：

$$s_{-1} \colon \mathbb{Z} \to B_0, \quad 1 \mapsto []$$

与

$$s_n \colon B_n \to B_{n+1}, \quad g_0[g_1|\cdots|g_n] \mapsto [g_0|g_1|\cdots|g_n]$$

可以验证

$$\mathrm{id} = ds + sd$$

所以正合. □

定义 2.20.3: 群上同调与上边缘算子

对 *Bar* 消解应用 $\mathrm{Hom}_{\mathbb{Z}G}(-, M)$ 函子，得到上复形 $C^n(G, M) = \mathrm{Hom}_{\mathbb{Z}G}(F_n, M)$，这等价于所有从 G^n 映射到 M 的函数 $f : G^n \to M$ 的集合. 上边缘算子 $d^n : C^n \to C^{n+1}$ 被诱导为：

$$(d^n f)(g_1, \dots, g_{n+1}) = g_1 \cdot f(g_2, \dots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_{n+1}) + (-1)^{n+1} f(g_1, \dots, g_n)$$

第 n 阶群上同调群定义为：

$$H^n(G, M) = \mathrm{Ker}(d^n) / \mathrm{im}(d^{n-1})$$

定理 2.20.2: 低阶群上同调的代数意义

群上同调 $H^n(G, M)$ 在低阶时具有以下经典代数解释：

(1) $H^1(G, M)$ 中的 *1-cocycle* 等价于交叉同态.

(2) $H^2(G, M)$ 中的 *2-cocycle* 条件给出了群扩张的结合律条件.

证明: 对于 $n = 1$，1-cocycle 要求 $d^1 f = 0$，即：

$$f(g_1 g_2) = g_1 f(g_2) + f(g_1)$$

此等式正是交叉同态的定义.

对于 $n=2$，2-cocycle 要求 $d^2f=0$，展开即为：

$$g_1f(g_2,g_3)-f(g_1g_2,g_3)+f(g_1,g_2g_3)-f(g_1,g_2)=0$$

移项后此等式对应于利用因子集构造群扩张时所必须满足的结合律条件. □

定义 2.20.4: 正则 Bar 消解

在 *Bar* 消解的生成元 $[g_1|\dots|g_n]$ 中，若存在某个 $g_i=1$（单位元），则称该生成元是退化的. 将所有由退化元生成的子复形商去后，剩余的复形称为**正则 *Bar* 消解**(*Normalized Bar Resolution*).

定理 2.20.3

正则 *Bar* 消解依然是 $\mathbb{Z}$ 的自由消解，且使用正则 *Bar* 消解计算出的同调与上同调群与标准 *Bar* 消解的结果完全同构. 在应用层面，这意味着在计算上同调函数 $f(g_1,\dots,g_n)$ 时，只要参数中包含单位元 1，即可规定其函数值为 0.

2.21 自由

引理 2.21.1

任给集合 X，考虑其生成的自由群 $G=F(X)$，则对应的增广理想 $\mathfrak{I}_G$ 为以 $X-1=\{x-1\colon x\in X\}$ 生成的自由 $\mathbb{Z}[G]$-模.

证明: 我们已经知道 $\mathfrak{I}_G$ 由 $\{g-1\colon g\in G\}$ 生成，注意到

$$xy-1=x(y-1)+(x-1),\quad (x^{-1}-1)=-x^{-1}(1-x)$$

于是知道增广理想可以由 $X-1$ 生成. 下面证明是自由模，若有关系

$$0=\sum_{x\in X}b_x(x-1),\quad b_x\in\mathbb{Z}[G]\backslash\{0\}$$

将 b_x 拆分为 $b'_x+b''_xx^{-1}$，其中 b'_x 中的每一项都不以 x^{-1} 结尾，则上式改写为

$$0=\sum_{x\in X}b'_x(x-1)-\sum_{x\in X}b''_x(x^{-1}-1)$$

会发现最后一项是 x 的只能出在在 $b'_x(x-1)$ 的展开中，而最后一项是 x^{-1} 的只能出现在 $b''_x(x^{-1}-1)$ 的展开中，从而 $b'_x=b''_x=0$，即线性无关. □

定理 2.21.1

对于集合 X，自由群 $G=F(X)$，对任意的 $\mathbb{Z}[G]$-模 M，都有

$$H^n(G,M)=H_n(G,M)=0,\quad n\geq 2$$

证明: 考虑正合列

$$0\to\mathfrak{I}_G\to\mathbb{Z}[G]\to\mathbb{Z}\to 0$$

导出长正合列

$$\mathrm{Tor}_n^G(\mathbb{Z}[G],M)\to\mathrm{Tor}_n^G(\mathbb{Z},M)\to\mathrm{Tor}_{n-1}^G(\mathfrak{I}_G,M)$$

由于 $\mathbb{Z}[G]$ 与 $\mathfrak{I}_G$ 都是自由模所以投射，故为 0，中间的即 $H_n(G,M)$，故为 0，同理导出 Ext 的长正合列得到 $H^n(G,M)=0$. □

推论 2.21.1

对集合 X，自由群 $G=F(X)$，则

$$H^n(G,\mathbb{Z})=\begin{cases}\mathbb{Z}, & n=0\\ \mathbb{Z}^{\prod X}, & n=1\\ 0, & n\geq 2\end{cases},\quad H_n(G,\mathbb{Z})=\begin{cases}\mathbb{Z}, & n=0\\ \mathbb{Z}^{\oplus X}, & n=1\\ 0, & n\geq 2\end{cases}$$

证明: $n=0$ 的情况由推论 2.19.1 立刻得到，而推论 2.19.2 告诉我们

$$H_1(G,\mathbb{Z})=\mathfrak{I}_G\otimes_{\mathbb{Z}[G]}\mathbb{Z}=\bigoplus_{x\in X}(x-1)\mathbb{Z}[G]\otimes_{\mathbb{Z}[G]}\mathbb{Z}=\mathbb{Z}^{\oplus X}$$

$$H^1(G,\mathbb{Z})=\mathrm{Hom}_{\mathbb{Z}[G]}(\mathfrak{I}_G,\mathbb{Z})=\mathrm{Hom}\left(\bigoplus_{x\in X}(x-1)\mathbb{Z}[G],\mathbb{Z}\right)=\prod_{x\in X}\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G],x)=\mathbb{Z}^{\prod X}$$

故得证. □

2.22 有限群的上同调

回忆，对有限群 G 而言，我们有范数元素 $N=\sum_{g\in G}g$. 于是对 G-模 M，我们定义了一个同态

$$N\colon M\to M,\quad x\mapsto Nx$$

引理 2.22.1

对有限群 G，$N \in \mathbb{Z}[G]$，则

$$\mathfrak{I}_G = \mathrm{Ker}\left(\mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G]\right)$$

证明: 设 $x = \sum_{g\in G} n_g G$，注意到 $Nx = 0$ 当且仅当

$$\sum_{g\in G} n_g N = 0 \Longrightarrow \sum_{g\in G} n_g = 0$$

得证. □

定义 2.22.1: Tate上同调

对于有限群 G，G-模 A，定义 ***Tate* 上同调**为

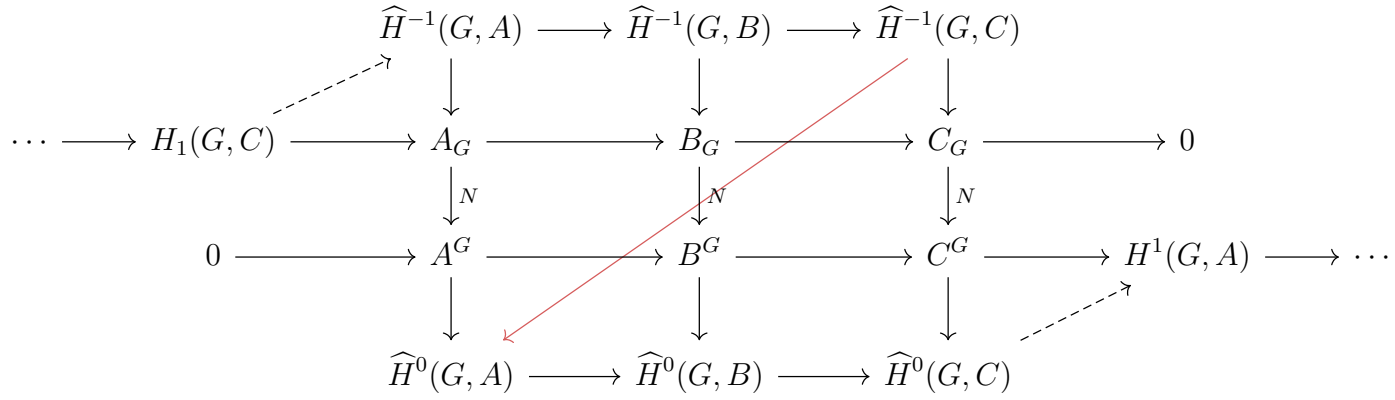
$$\widehat{H}^n(G,A) = \begin{cases} H^n(G,A), & n \geq 1 \\ A^G/NA, & n = 0 \\ \{x \in A\colon Nx = 0\}/\mathfrak{I}_G A, & n = -1 \\ H_{-1-n}(G,A), & n \leq -2 \end{cases}$$

定理 2.22.1: Tate上同调诱导长正合列

对于有限群 G，G-模的短正合列 $0 \to A \to B \to C \to 0$ 诱导长正合序列

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

证明: 将 Tor 和 Ext 的长正合列通过蛇引理连接起来即可:



交换图说明一切. □

Chapter 3: 代数数论入门

3.1 基本内容速览

我们说的数域实指 $\mathbb{Q}$ 的有限扩张 K，K 中的元素被称为代数数，$\mathbb{Z}$ 在 K 中的代数闭包称为 K 的代数整数. 对于域扩张(未必数域，故未必可分) L/K，我们可以定义 $x\in L$ 的范与迹，承接定义 1.13.1 即可，可见在特征多项式

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

中，有

$$a_1=\mathrm{tr}_{L/K}(x),\quad a_n=N_{L/K}(x)$$

我们实际上得到了同态

$$\mathrm{tr}_{L/K}\colon L\to K,\quad N_{L/K}\colon L^\times\to K^\times$$

推论 1.13.1 表明迹与范都是传递的. 若 L/K 还是可分扩张，则我们可以考虑 K 的代数闭包 $\overline{K}$，可见 x 的特征多项式实为

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

故可见

$$\mathrm{tr}_{L/K}(x)=\sum_{\sigma\in\mathrm{Hom}_K(L,\overline{K})}\sigma(x),\quad N_{L/K}(x)=\prod_{\sigma\in\in\mathrm{Hom}_K(L,\overline{K})}\sigma(x)$$

其道理在于对于一般的域扩张 L/K，范数与迹的计算可以拆做两段，对 $x\in L$，我们有

$$N_{L/K}(x)=N_{K(x)/K}(N_{L/K(x)}(x)),\quad \mathrm{tr}_{L/K}(x)=\mathrm{tr}_{K(x)/K}(\mathrm{tr}_{L/K(x)}(x))$$

而 $L/K(x)$ 的计算是显然的，因为此时 x 在 $K(x)$ 上的作用是纯纯的乘法，所以

$$N_{L/K(x)}(x)=x^{[L:K(x)]},\quad \mathrm{tr}_{L/K(x)}=[L:K(x)]x$$

故本质上就是计算

$$N_{K(x)/K}(x),\quad \mathrm{tr}_{K(x)/K}(x)$$

而这个的计算完全由极小多项式刻画，设 $x\in L$ 在 K 上的极小多项式 $P_x=X^n+a_{n-1}X^{n-1}+\cdots+a_0$，则

$$N_{K(x)/K}(x)=(-1)^na_0,\quad \mathrm{tr}_{K(x)/K}(x)=-a_{n-1}$$

这只需要注意到 $1, x, \cdots, x^{n-1}$ 构成了 $K(x)$ 的一组 K-基，而 $\times x$ 在这组基下的矩阵就自然是

$$A := \begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & & & -a_1 \\ & \ddots & & \vdots \\ & & 1 & -a_{n-1} \end{pmatrix}$$

如此就显然. 所以不仅可以见到可分 L/K 的表示，对任意有限扩张我们都可以有统一的表达，

$$\mathrm{tr}_{L/K}(x) = [L:K]_i \sum_{\sigma \in \mathrm{Hom}_K(L, \overline{K})} \sigma(x), \quad N_{L/K}(x) = \prod_{\sigma \in \in \mathrm{Hom}_K(L, \overline{K})} \sigma(x)^{[L:K]_i}$$

其中 $[L:K]_i$ 为 L/K 的不可分次数，即 $[L:K^{\mathrm{sep}}]$. 于是可见 $\mathrm{tr}_{L/K}$ 在 L/K 不可分时恒为 0. 可见有限扩张的迹型式(定义 1.13.2) $\mathrm{tr}_{L/K}$ 作为双线性型非退化当且仅当 L/K 可分，当的部分源于对偶基的存在性，即若有限扩张 E/F 可分则为单扩张 $E = F(x)$，记 x 的极小多项式为 P_x，为 n 次，记

$$\frac{P_x}{X - x} = \sum_{i=0}^{n-1} b_i X^i \in E[X]$$

若 $P_x'(x) \neq 0$，则对 E 的基 $1, x, \cdots, x^{n-1}$，相对于 $\mathrm{tr}_{E/F}$ 的对偶基为

$$\frac{b_0}{P_x'(x)}, \cdots, \frac{b_{n-1}}{P_x'(x)}$$

为了看到这就是对偶基，令 $x_1 = x, \cdots, x_n$ 为 x 的所有共轭，我们首先断言

$$\sum_{i=1}^{n} \frac{P_x}{X - x_i} \frac{x_i^j}{P_x(x_i)} = X^j, \quad 0 \leq j \leq n-1$$

由插值法立刻看到，由 x_i 一定是某个 $\sigma(x)$，我们可以看到

$$\sum_{\sigma \in \mathrm{Hom}_F(E, \overline{F})} \sigma\left(\frac{P_x}{X - x_i} \frac{x^j}{P_x(x_i)} \right) = X^j$$

我们把左边写开即

$$\begin{aligned} X^j &= \sum_{\sigma \in \mathrm{Hom}_F(E, \overline{F})} \sigma\left(\frac{P_x}{X - x_i} \frac{x^j}{P_x(x_i)} \right) \\ &= \sum_{\sigma \in \mathrm{Hom}_F(E, \overline{F})} \left(\frac{x^j}{P_x'(x)} \sum_{i=0}^{n-1} b_i X^i \right) \\ &= \sum_{i=0}^{n-1} \left(\sum_{\sigma \in \mathrm{Hom}_F(E, \overline{F})} \sigma\left(x^j \cdot \frac{b_i}{P_x'(x)} \right) \right) X^i \end{aligned}$$

对比两边系数立刻得到

$$\mathrm{tr}_{E/F}\left(x^j \cdot \frac{b_i}{P_x'(x)} \right) = \sum_{\sigma \in \mathrm{Hom}_F(E, \overline{F})} \sigma\left(x^j \cdot \frac{b_i}{P_x'(x)} \right) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

故知为对偶基，从而可知 L/K 可分当且仅当 $\mathrm{tr}_{L/K}$ 非退化.

我们可以对 $n=[L:K]$ 个元素 $\alpha_1,\cdots,\alpha_n$ 定义判别式为

$$d(\alpha_1,\cdots,\alpha_n)=\det(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))$$

可见若 L/K 不可分则判别式恒为 0，故我们讨论 L/K 可分的情况，此时

$$d(\alpha_1,\cdots,\alpha_n)=\det(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))=\det(\sigma_i(\alpha_j))^2$$

从而对 $L=K(x)$，存在幂基 $1,x,\cdots,x^{n-1}$，我们可以计算其判别式

$$d(1,x,\cdots,x^{n-1})=\prod_{i<j}(x_i-x_j)^2=(-1)^{\frac{n(n-1)}{2}}N_{E/F}(P'_x(x))$$

第一个等号是因为实际上为 Vandermonde 行列式，第二个等号是因为

$$N_{L/K}(P'_x(x))=\prod_{i=1}^{n}P'_x(x_i)=\prod_{i=1}^{n}\prod_{j\neq i}(x_i-x_j)=(-1)^{\frac{n(n-1)}{2}}\prod_{1\leq i<j\leq n}(x_i-x_j)^2$$

判别式还有妙用，即

$$d_{L/K}(\alpha_1,\cdots,\alpha_n)\neq 0\iff \alpha_1,\cdots,\alpha_n\text{ 是 }K\text{-线性无关的}$$

证明是纯粹的线性代数，我们不再赘述.

现在我们考虑数域的情况，L/K 是数域的有限扩张，$\mathcal{O}_K$ 与 $\mathcal{O}_L$ 分别为 K,L 的整数环，任意看见 $\mathcal{O}_L\cap K=\mathcal{O}_K$，这是由于 $\mathcal{O}_K$ 是 $\mathbb{Z}$ 在 K 中的整闭包，从而自然是整闭的. 由于整数的共轭很显然还是整数，所以

$$\mathrm{tr}_{L/K}(x)\in\mathcal{O}_K,\quad N_{L/K}(x)\in\mathcal{O}_K$$

实际上上述结论对整闭整环 A，其分式域 K，有限可分扩张 L 与 A 在 L 中的整闭包 B 都成立，只需要把上面的 $\mathcal{O}_K$ 与 $\mathcal{O}_L$ 替换为 A 与 B 即可. 我们容易看到

$$x\in B^\times\iff N_{L/K}(x)\in A^\times$$

若令 $\alpha_1,\cdots,\alpha_n$ 为 L/K 的一组基，并且 $\alpha_i\in B$，若令 $d=d(\alpha_1,\cdots,\alpha_n)$，则有

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

这是因为若 $\alpha=\sum_{i=1}^{n}a_i\alpha_i\in B$，其中 $a_j\in K$，则 a_j 为线性方程组

$$\mathrm{tr}_{L/K}(\alpha_i\alpha)=\sum_{j=1}^{n}\mathrm{tr}_{L/K}(\alpha_i\alpha_j)a_j$$

并且由于 $\mathrm{tr}_{L/K}(\alpha_i\alpha)\in A$，由 Cramer 法则知道

$$a_j=\frac{*\in A}{\det(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))}=\frac{*}{d}$$

故知道 $da_j \in A$，故 $dB \subset \sum_{i=1}^{n} A\alpha_i$.

B 中的一组元素 $\omega_1, \cdots, \omega_n$ 若使得

$$B = A\omega_1 \oplus \cdots \oplus A\omega_n$$

则称其为 B 在 A 上的一组**整基**，首先我们要说明对任意的 L 中元素 x，都存在某个 $a \in A$ 使得 $ax \in B$，这只需要往 x 的极小多项式

$$x^m + a_1 x^{m-1} + \cdots + a_m = 0$$

上乘一个充分大的数 a^m 使得 $a^m a_i \in A$，把 a_i 的分母通分即可. 所以可见 B 在 K-线性下张成整个 L. 所以这种整基自然是 L 的一组 K 基，从而 $n = [L : K]$，整基的存在使得 B 为一个自由 A-模.

遗憾的是一般来说整基并不存在，但是如果 A 是 PID，那么事情就十分美妙了. 符号同上，L/K 是有限可分扩张，若 A 是 PID，那么 L 的所有有限生成 B-子模 M 都是秩 $n = [L : K]$ 的自由 A-模. 特别地，B 的整基存在. 要看到这个，我们先取 L/K 的一组基 $\alpha_1, \cdots, \alpha_n$，由于乘上一个 A 中的数不影响它们是一组基，所以不妨设这些基元素都落在 B 中，故

$$dB \subset A\alpha_1 \oplus \cdots \oplus A\alpha_n$$

特别地，可见 $\operatorname{rank} B \leq [L : K]$，而 B 是自由 A-模的子模，从而自由，并且 B 的 A-生成元 K-线性生成 L，故 $\operatorname{rank}(B) \geq [L : K]$，故 $\operatorname{rank}(B) = [L : K]$. 现在设 $\mu_1, \cdots, \mu_r$ 是 M 的一组生成元，知存在 $a \in A$ 使得 $aM \subset B$，故 $adM \subset dB$，从而

$$[L : K] = \operatorname{rank}(B) \leq \operatorname{rank}(M) = \operatorname{rank}(adM) \leq \operatorname{rank}(dB) = [L : K]$$

现在我们考虑数域 K，知道 $\mathbb{Z} \subset \mathbb{Q}$ 是 PID，所以所以 K 的有限生成 $\mathcal{O}_K$-子模 $\mathfrak{a}$ 都存在一组 $\mathbb{Z}$-基 $\alpha_1, \cdots, \alpha_n$，其中 $n = [K : \mathbb{Q}]$，对其可以定义判别式为

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

特别地，存在 K 的整基，但可能会存在不同的整基，假设 $\beta_1, \cdots, \beta_n$ 和 $\gamma_1, \cdots, \gamma_n$ 都是 K 的整基，那么由整基的定义我们知道存在元素都在 $\mathbb{Z}$ 中的两个矩阵 M, N 使得

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}, \quad \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} = N \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

于是有 $M = N^{-1}$，容易看出来 $|M| = |N| = \pm 1$. 将 $\operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ 中的元素称为 K 到 $\mathbb{C}$ 的**嵌入**，令 $\sigma_1, \cdots, \sigma_n$ 是 K 到 $\mathbb{C}$ 的全部 n 个嵌入，不难发现

$$(\sigma_i(\beta_j)) = M(\sigma_i(\gamma_j)) \Rightarrow d_{K/\mathbb{Q}}(\beta_1, \cdots, \beta_n) = |M|^2 d_{K/\mathbb{Q}}(\gamma_1, \cdots, \gamma_n) = d_{K/\mathbb{Q}}(\gamma_1, \cdots, \gamma_n)$$

故不同的整基具有相同的判别式，知整基的判别式是数域的一个不变量，我们将其称之为域 K 的**判别式**，记为 d_K 或者 $d(K)$ 或者 $d(\mathcal{O}_K)$. 由于它们线性无关，所以域 K 的判别式不为 0，并且 d_K

是一个整数. 同理可知 $d(\mathfrak{a})$ 也是不变量，它衡量了 $\mathfrak{a}$ 的大小. 也即对两个 K 的有限生成 $\mathcal{O}_K$-子模 $\mathfrak{a}' \subset \mathfrak{a}$，取 $\mathfrak{a}$ 的一组 $\mathbb{Z}$-基 $\alpha_1, \cdots, \alpha_n$，由 PID 上有限生成模的结构定理告诉我们

$$\mathfrak{a}' = A(d_1\alpha_1) \oplus \cdots \oplus A(d_n\alpha_n), \quad d_i \in \mathbb{Z}$$

我们可以良定义其**指数**为

$$(\mathfrak{a} : \mathfrak{a}') := d_1 \cdots d_n$$

是一个有限值，也就是说商模 $\mathfrak{a}/\mathfrak{a}'$ 有限，并且容易看到满足：

$$d(\mathfrak{a}') = (\mathfrak{a} : \mathfrak{a}')^2 d(\mathfrak{a})$$

直观上可以理解出对应的判别式越大，子模在 K 中越稀疏.

由上面结论我们知道 $\mathcal{O}_K$ 是有限生成 $\mathbb{Z}$-代数，即取整基 $\alpha_1, \cdots, \alpha_n$，有

$$\mathcal{O}_K = \mathbb{Z}[\alpha_1, \cdots, \alpha_n]$$

而 $\mathbb{Z}$ 是 Noether 的，所以由 Hilbert 基定理立刻看到 $\mathcal{O}_K$ 是 Noether 环，此外可见 $K = \mathrm{Frac}(\mathcal{O}_K)$，故 $\mathcal{O}_K$ 是整闭的，最后对于 $\mathcal{O}_K$ 的任何理想 $\mathfrak{a}$，$\mathcal{O}_K/\mathfrak{a}$ 都是有限的，所以对于任意素理想 $\mathfrak{p}$，都有 $\mathcal{O}_K/\mathfrak{p}$ 是有限的整环，所以是域. 这表明素理想都极大，所以是一维的，综上我们明白数域的代数整数环是一维整闭诺特整环，即 Dedekind 整环. 交换代数告诉我们 Dedekind 整环中的理想有唯一的素理想分解，即对 $\mathcal{O}_K$ 的任意理想 $\mathfrak{a}$，都存在唯一的素理想分解

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

因为都在域 K 中，所以取逆的操作都是合法的，若允许 $a_i < 0$，则导出了所谓**分式理想**的概念，我们定义 $\mathcal{O}_K$ 的分式理想就是一个有限生成 $\mathcal{O}_K$-模 $M \subset K$. 一个等价定义是说分式理想是一个 $\mathcal{O}_K$-模 $M \subset K$，使得存在 $d \in \mathcal{O}_K - \{0\}$ 有 $dM \subset \mathcal{O}_K$. 直观理解就是分式理想就是把一般意义上的理想统一加上一个分母，分母存在性由诺特性保证.

一个 $\mathcal{O}_K$-模 $M \subset K$ 称为**可逆理想**，如果存在 $\mathcal{O}_K$-模 $N \subset K$，使得 $MN = \mathcal{O}_K$. 事实上这样的 N 是唯一的并且等于 $(\mathcal{O}_K : M) := \{x \in K : xM \subset \mathcal{O}_K\}$. 唯一且等于 $(\mathcal{O}_K : M)$ 的原因是

$$N \subset (\mathcal{O}_K : M) = (\mathcal{O}_K : M)MN = ((\mathcal{O}_K : M)M)N \subset \mathcal{O}_K N = N$$

于是我们可以看到所有的分式理想都是可逆理想，反之亦然，从而分式理想和可逆理想是同一种概念. 可见分式理想在乘法意义下构成一个 Abel 群，我们把这个群记为 I_K. 特别地，我们平时所称的理想，现在称之为**整理想**是 $x = 1$ 的分式理想，任何元素 $u \in K$ 都可以生成一个分式理想，记为 (u) 或者 $u\mathcal{O}_K$，称之为主理想. 所有的主理想构成 I_K 的一个子群，记为 P_K. 我们可以看见 $\mathcal{O}_K$ 的分式理想都存在素理想的唯一分解，即

$$M = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}}, \quad a_\mathfrak{p} \in \mathbb{Z}$$

从而 I_K 实际上是一个自由 Abel 群，其基为 $\mathrm{Spec}\,\mathcal{O}_K - \{0\}$.

令 $\mathrm{Cl}_K = I_K/P_K$ 为 K 的**理想类群**，容易看到有如下正合列成立：

$$1 \to \mathcal{O}_K^\times \to K^\times \to I_K \to \mathrm{Cl}(K) \to 1$$

我们就自然要去研究一头一尾的两个对象，一个是类群，一个是单位.

3.2 理想类群类数有限

定义 3.2.1: Lattice

令 V 为一个 n-为 $\mathbb{R}$-线性空间，V 的一个**格**为形如

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

的子群，其中 $v_1, \cdots, v_m$ 线性无关，m-元组 $(v_1, \cdots, v_m)$ 称为**基**，集合

$$\Phi = \left\{ \sum_{i=1}^{m} x_i v_i \colon x_i \in [0,1) \right\}$$

称为格的一个**基本网格**，格被称为是**完备**的，如果 $m = n$.

我们可见格是 V 的一个离散子群，即格中的每一点都存在一个开邻域不包含其他的点. 可以证明：

命题 3.2.1

子群 $\Gamma \subset V$ 是格当且仅当它是离散的.

容易看到一个格是完备的当且仅当存在一个有界集 M 在格的平移作用下覆盖整个空间 V.

若 V 配备了一个内积，则我们可以对其定义体积的概念，或者说是 Haar 测度. 取定一组正交基 $e_1, \cdots, e_n$，定义其体积为 1，对任意 n 个线性无关的元素 $v_1, \cdots, v_n$，其张成的基本网格

$$\Phi = \left\{ \sum_{i=1}^{n} x_i v_i \colon x_i \in [0,1) \right\}$$

的体积定义为

$$\mathrm{vol}(\Phi) = |\det A|$$

其中 A 是从 e_i 到 v_i 的转移矩阵，由于

$$(\langle v_i, v_j \rangle) = AA^t$$

所以我们可以看到体积满足

$$\mathrm{vol}(\Phi) = |\det(\langle v_i, v_j \rangle)|^{1/2}$$

令 Γ 为 $v_1, \cdots, v_n$ 生成的格，Φ 为其基本网格，我们认为定义 Γ 的体积就是

$$\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi)$$

不难看到这是良定义的. 同样可见格越稀疏，其体积越大.

我们称 S 是凸集合，如果

$$\forall x, y \in S \Rightarrow \frac{1}{2}(x+y) \in S$$

我们称 S 是关于原点对称的，如果

$$\forall x \in S \Rightarrow -x \in S$$

好啦，现在我们可以看到我们需要的很重要的定理了.

定理 3.2.1: Minkowski

设 X 是 $\mathbb{R}^n$ 中关于原点对称的凸集，$\Lambda \subset \mathbb{R}^n$ 是一个完备格，如果有

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

那么 $X \cap (\Lambda \backslash \{0\}) \neq \emptyset$，即 X 至少含有一个非零格点 $\gamma \in \Gamma$. 若 X 还额外是一个紧集，条件可以减弱为

$$\mathrm{vol}(X) \geq 2^n \,\mathrm{vol}(\Lambda)$$

回忆，对数域 K，若 $[K : \mathbb{Q}] = n$，则其复嵌入 $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ 共有 n 个，于是自然会有对角嵌入

$$j \colon K \to K_{\mathbb{C}} := \prod_{\tau} \mathbb{C}, \quad a \mapsto (\tau(a))_{\tau}$$

而复线性空间 $K_{\mathbb{C}}$ 自然是有 Hermite 内积

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

而 Galois 群 $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ 由复共轭生成

$$F \colon z \mapsto \overline{z}$$

同时 F 也可以作用在 $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ 上，作用为

$$F(\tau) = \overline{\tau}, \quad \overline{\tau}(a) = \overline{\tau(a)}$$

我们可以看到 F 自然地作用在 $\prod_{\tau} \mathbb{C}$ 上，对 $z \in \prod_{\tau} \mathbb{C}$，定义其作用为

$$(F(z))_{\tau} = \overline{z}_{\overline{\tau}}$$

可见 F 的作用在内积上是等变的，即

$$\langle Fx, Fy \rangle = F\langle x, y \rangle$$

我们同样可以定义 $K_{\mathbb{C}}$ 上的迹，定义为

$$\mathrm{tr} \colon K_{\mathbb{C}} \to \mathbb{C}, \quad z \mapsto \sum_{\tau} z_{\tau}$$

这同样是 F 等变的，即

$$F(\mathrm{tr}(z)) = \mathrm{tr}(F(z))$$

若我们考虑复合

$$\mathrm{tr}\circ j\colon K\hookrightarrow K_{\mathbb{C}}\to\mathbb{C}$$

就注意到

$$\mathrm{tr}_{K/\mathbb{Q}}(a)=\sum_{\tau}\tau(a)=\mathrm{tr}(j(a))$$

我们真正感兴趣的是

$$K_{\mathbb{R}}=K_{\mathbb{C}}^{F}$$

为 $K_{\mathbb{C}}$ 中的 F-不动点，即 $z_{\overline{\tau}}=\overline{z_{\tau}}$. 我们可以看到 $F(j(a))=j(a)$，故 K 仍然可以嵌入 $K_{\mathbb{R}}$ 中，将 $K_{\mathbb{C}}$ 的 Hermite 内积限制在 $K_{\mathbb{R}}$ 上就得到一个实内积，这是因为

$$F(\langle x,y\rangle)=\langle F(x),F(y)\rangle=\langle x,y\rangle$$

所以发现 $\langle x,y\rangle$ 是实数，故实内积，我们将 $K_{\mathbb{R}}$ 称为**Minkowski 空间**，由于 $F\circ\mathrm{tr}=\mathrm{tr}\circ F$，可见 tr 在 $K_{\mathbb{R}}$ 上取实值，我们要说明实际上有

$$\boxed{K_{\mathbb{R}}=K\otimes_{\mathbb{Q}}\mathbb{R},\quad K_{\mathbb{C}}=K\otimes_{\mathbb{Q}}\mathbb{C}}$$

要看到这个不妨设 $K=Q(x)$，x 的极小多项式为 $p(X)$，则

$$K\otimes_{\mathbb{Q}}\mathbb{C}=K[X]/p(X)\otimes_{\mathbb{Q}}\mathbb{C}=\mathbb{C}[X]/p(X)$$

这对应了 $p(X)$ 有多少实根，有多少复根，分别设为 r_1 个与 r_2 对，则有

$$K\otimes_{\mathbb{Q}}\mathbb{C}=\mathbb{C}^{r_1}\times\mathbb{C}^{2r_2}=\mathbb{C}^{r_1+2r_2}=\mathbb{C}^{n}$$

$K\otimes_{\mathbb{Q}}\mathbb{C}\to K_{\mathbb{C}}$ 的映射可以构造为 $a\otimes z\mapsto j(a)z$，而 F 在其上的作用为

$$F(a\otimes z)=a\otimes\overline{z}$$

可见

$$(K\otimes_{\mathbb{Q}}\mathbb{C})^{F}=K\otimes_{\mathbb{Q}}\mathbb{R}$$

而实根与复根就对应了 $K\to\mathbb{C}$ 的那些实嵌入与复嵌入，分别记为 $\sigma_1,\cdots,\sigma_{r_1}$ 与 $\tau_1,\cdots,\tau_{r_2}$ 及其共轭，则

$$K\otimes_{\mathbb{Q}}\mathbb{R}=\mathbb{R}[X]/p(X)=\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}\cong\mathbb{R}^{r_1}\times\mathbb{R}^{2r_2}=\mathbb{R}^{r_1+2r_2}=\mathbb{R}^{n}$$

我们现在来说明数域的理想类群是有限的，方法是将 $\mathcal{O}_K$ 的每个分式理想嵌入 $\mathbb{R}^n$ 中成为一个格. 回忆一下我们有 r_1 个实嵌入与 r_2 对复嵌入，记为

$$\sigma_1,\cdots,\sigma_{r_1},\quad \sigma_{r_1+1},\cdots,\sigma_{r_1+r_2},\overline{\sigma_{r_1+1}},\cdots,\overline{\sigma_{r_1+r_2}}$$

我们有映射

$$j\colon K\to K_{\mathbb{R}}\cong\mathbb{R}^{n}$$

$$\alpha\mapsto(\sigma_1(\alpha),\cdots,\alpha_{r_1}(\alpha),\mathrm{Re}(\sigma_{r_1+1}(\alpha)),\cdots,\mathrm{Re}(\sigma_{r_1+r_2}(\alpha)),\mathrm{Im}(\sigma_{r_1+1}(\alpha)),\cdots,\mathrm{Im}(\sigma_{r_1+r_2}(\alpha)))$$

任取 $\mathcal{O}_K$ 的整理想，在前面我们早已说明 $\mathfrak{a}$ 是秩为 n 的自由 Abel 群，即

$$\mathfrak{a} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$$

取 $e_1, \cdots, e_n$ 为 $K_{\mathbb{R}} \cong \mathbb{R}^n$ 的标准基，则我们知道

$$j(\alpha_i) = \sum_{j=1}^{n} x_{ij} e_j$$

其中

$$x_{ij} = \begin{cases} \sigma_j(\alpha_i), & 1 \le j \le r_1 \\ \mathrm{Re}(\sigma_j(\alpha_i)), & r_1 + 1 \le j \le r_1 + r_2 \\ \mathrm{Im}(\sigma_j(\alpha_i)), & r_1 + r_2 + 1 \le j \le n \end{cases}$$

于是我们知道

$$j(\mathfrak{a}) = \mathbb{Z}j(\alpha_1) + \cdots + \mathbb{Z}j(\alpha_n)$$

我们下面要说明 $j(\mathfrak{a})$ 构成一个完备格，我们已经知道 $j(\mathfrak{a})$ 的秩小于等于 n，下面只需要说明 $j(\mathfrak{a})$ 的体积大于 0，则自然成为一个完备格.

$$\mathrm{vol}(j(\mathfrak{a})) = |\det(x_{ij})|$$

$$= \left\| \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_1)) & \cdots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_1)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_2)) & \cdots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_2)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_2)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_2)) \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \mathrm{Re}(\sigma_{r_1+1}(\alpha_n)) & \cdots & \mathrm{Re}(\sigma_{r_1+r_2}(\alpha_n)) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{vmatrix} \right\|$$

$$= \left\| \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \sigma_{r_1+1}(\alpha_1) & \cdots & \sigma_{r_1+r_2}(\alpha_1) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \sigma_{r_1+1}(\alpha_2) & \cdots & \sigma_{r_1+r_2}(\alpha_2) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_2)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_2)) \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \sigma_{r_1+1}(\alpha_n) & \cdots & \sigma_{r_1+r_2}(\alpha_n) & \mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) & \cdots & \mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{vmatrix} \right\|$$

$$= 2^{-r_2} \left\| \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \sigma_{r_1+1}(\alpha_1) & \cdots & \sigma_{r_1+r_2}(\alpha_1) & -2i\,\mathrm{Im}(\sigma_{r_1+1}(\alpha_1)) & \cdots & -2i\,\mathrm{Im}(\sigma_{r_1+r_2}(\alpha_1)) \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \sigma_{r_1+1}(\alpha_2) & \cdots & \sigma_{r_1+r_2}(\alpha_2) & -2i\,\mathrm{Im}(\sigma_{r_1+1}(\alpha_2)) & \cdots & -2i\,\mathrm{Im}(\sigma_{r_1+r_2}(\alpha_2)) \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \sigma_{r_1+1}(\alpha_n) & \cdots & \sigma_{r_1+r_2}(\alpha_n) & -2i\,\mathrm{Im}(\sigma_{r_1+1}(\alpha_n)) & \cdots & -2i\,\mathrm{Im}(\sigma_{r_1+r_2}(\alpha_n)) \end{vmatrix} \right\|$$

$$= 2^{-r_2} \left\| \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \sigma_{r_1+1}(\alpha_1) & \cdots & \sigma_{r_1+r_2}(\alpha_1) & \overline{\sigma_{r_1+1}(\alpha_1)} & \cdots & \overline{\sigma_{r_1+r_2}(\alpha_1)} \\ \sigma_1(\alpha_2) & \cdots & \sigma_{r_1}(\alpha_2) & \sigma_{r_1+1}(\alpha_2) & \cdots & \sigma_{r_1+r_2}(\alpha_2) & \overline{\sigma_{r_1+1}(\alpha_2)} & \cdots & \overline{\sigma_{r_1+r_2}(\alpha_2)} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \sigma_{r_1+1}(\alpha_n) & \cdots & \sigma_{r_1+r_2}(\alpha_n) & \overline{\sigma_{r_1+1}(\alpha_n)} & \cdots & \overline{\sigma_{r_1+r_2}(\alpha_n)} \end{vmatrix} \right\|$$

所以我们知道

$$V(j(\mathfrak{a})) = 2^{-r_2} |\det(\sigma_j(\alpha_i))|$$

设 $\beta_1,\cdots,\beta_n$ 是 $\mathcal{O}_K$ 的一组整基，使得 $\mathfrak{a}=\mathbb{Z}(d_1\beta_1)\oplus\cdots\oplus\mathbb{Z}(d_n\beta_n)$，由于都是 $\mathfrak{a}$ 的基，我们知道

$$|\det(\sigma_j(\alpha_i))|=|\det(\sigma_j(d_i\beta_i))|$$

注意到若定义 $N\mathfrak{a}=[\mathcal{O}_K:\mathfrak{a}]$ 为 $\mathfrak{a}$ 的**范数**，则

$$N\mathfrak{a}=[\mathcal{O}_K:\mathfrak{a}]=|d_1d_2\cdots d_n|=\frac{|\det(\sigma_j(d_i\beta_i))|}{|\det(\sigma_j(\beta_i))|}=\frac{|\det(\sigma_j(\alpha_i))|}{\sqrt{|d_K|}}$$

所以我们最终得到

$$\mathrm{vol}(j(\mathfrak{a}))=2^{-r_2}N\mathfrak{a}\sqrt{|d_K|}$$

右边显然不为零，所以体积大于零，于是是满秩的，所以 $\mathfrak{a}$ 构成一个格.

Remark 3.2.1

理想的 norm 之所以称为 norm 的一部分原因是因为它和元素的 norm 是相容的，指

$$N(x)=Nx\mathcal{O}_K=|N_{K/\mathbb{Q}}(x)|$$

理想的范数是积性的，即对于理想 $\mathfrak{a},\mathfrak{b}$，有

$$N\mathfrak{a}\mathfrak{b}=N\mathfrak{a}N\mathfrak{b}$$

要看到这一点，我们只需要看到若理想

$$\mathfrak{a}=\mathfrak{p}_1^{\nu_1}\cdots\mathfrak{p}_r^{\nu_r}$$

则中国剩余定理告诉我们

$$\mathcal{O}_K/\mathfrak{a}=\prod\mathcal{O}_K/\mathfrak{p}_i^{\nu_i}$$

再由于

$$N\mathfrak{p}^\nu=[\mathcal{O}_K:\mathfrak{p}^\nu]=[\mathcal{O}_K:\mathfrak{p}][\mathfrak{p}:\mathfrak{p}^2]\cdots[\mathfrak{p}^{\nu-1}:\mathfrak{p}^\nu]=(N\mathfrak{p})^\nu$$

于是发现

$$N(\mathfrak{a})=\prod N(\mathfrak{p}^\nu)$$

此外可见

$$N\mathfrak{a}=\frac{d(\mathfrak{a})}{d(\mathcal{O}_K)}$$

为判别式除掉域判别式，也就是相对整数环有多稀疏.

引理 3.2.1

存在只跟域 K 相关的常数 M，使得对于任何分式理想 $\mathfrak{a}$，都存在 $x\in\mathfrak{a}^{-1}-\{0\}$，使得

$$N(x\mathfrak{a})\le M$$

证明: 设 $\mathfrak{a}$ 是分式理想，考虑 $\mathfrak{a}^{-1}$ 在映射

$$K\to K_{\mathbb{R}}=\mathbb{R}^{r_1}\times\mathbb{C}^{r_2},\quad x\mapsto(\sigma_1(x),\cdots,\sigma_{r_1}(x),\sigma_{r_1+1}(x),\cdots,\sigma_{r_1+r_2}(x))$$

下的像，构成 $K_{\mathbb{R}}$ 中的格，任取 $K_{\mathbb{R}}$ 中一个关于原点对称的紧凸集 S，设 M_0 是 $K_{\mathbb{R}}$ 上函数

$$|x_1 \cdots x_{r_1} x_{r_1+1}^2 \cdots x_{r_1+r_2}^2|$$

在 S 上的最大值，取

$$\lambda = 2\left(\frac{\mathrm{vol}(j(\mathfrak{a}^{-1}))}{m(S)}\right)^{\frac{1}{n}}$$

所以我们有

$$m(\lambda S) = 2^n \,\mathrm{vol}(j(\mathfrak{a}^{-1}))$$

于是由 Minkowski 定理我们知道存在 $j(x) \in \lambda S \cap j(\mathfrak{a}^{-1})$，于是我们知道

$$\begin{aligned} N(x\mathfrak{a}) &= |N_{K/\mathbb{Q}}(x)| N\mathfrak{a} = \left|\prod_{i=1}^{n} \sigma_i(x)\right| N\mathfrak{a} \\ &\leq \max_{x\in\lambda S} |x_1 \cdots x_{r_1} x_{r_1+1}^2 \cdots x_{r_1+r_2}^2| N\mathfrak{a} \\ &= \lambda^n M_0 N\mathfrak{a} = 2^n \frac{\mathrm{vol}(j(\mathfrak{a}^{-1}))}{m(S)} M_0 N\mathfrak{a} \\ &= 2^n \frac{2^{-r_2} N\mathfrak{a}^{-1}\sqrt{|d_K|}}{m(S)} M_0 N\mathfrak{a} \\ &= 2^{r_1+r_2} M_0 \sqrt{|d_K|} m(S)^{-1} \end{aligned}$$

等式最右边只与 K 相关，命题成立. □

事实上，我们还可以取出一些很好的 S 让这个界更好，我们可以取

$$S = \{(x_1, \cdots, x_{r_1+r_2}) \in K_{\mathbb{R}} \mid |x_1| + \cdots |x_{r_1}| + 2(|x_{r_1+1}| + \cdots + |x_{r_1+r_2}|) \leq 1\}$$

在这个条件下，上面证明过程中取的 M_0 为 n^{-n}，用一步均值就可以看出来. 此时我们知道上界 M 可以取为

$$\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|d_K|}$$

此即我们常说的 **Minkowski bound**. 是计算理想类群的常用手段.

引理 3.2.2: 关键引理

给定 $M > 0$，只有有限多个理想 $\mathfrak{a}$ 满足 $N\mathfrak{a} \leq M$.

证明: 只需要证明只有有限多个素理想满足即可，而我们注意到对于素理想 $\mathfrak{p}$，考虑 $\mathfrak{p} \cap \mathbb{Z} = (p)$，我们知道 $\mathcal{O}_K/\mathfrak{p}$ 是 $\mathbb{Z}/p\mathbb{Z}$ 的有限维线性空间，于是

$$N\mathfrak{p} = [\mathcal{O}_K : \mathfrak{p}] = p^n$$

并且满足 $\mathfrak{q} \cap \mathbb{Z} = (p)$ 的素理想 $\mathfrak{q}$ 只有有限个，这是因为

$$\mathfrak{q} \supset p\mathcal{O}_K$$

也就是说 $\mathfrak{q} \mid p\mathcal{O}_K$，而 $p\mathcal{O}_K$ 存在唯一素理想分解，所以只有有限个 $\mathfrak{q}$ 的范数是 p 的幂，再结合素数的递增和整数的离散性，我们知道最多有有限个素理想的范数小于等于 M. □

令 $h_K = |\mathrm{Cl}(K)| = |I_K/P_K|$ 为 K 的理想类群的类数.

定理 3.2.2: 理想类群类数有限

K 是数域，则 $h_k < +\infty$.

证明: 有了前面的讨论，证明无非是文字游戏：设 Minkowski bound 为 M，由于满足 norm 小于等于 M 的整理想是有限的，并且任何一个分式理想 $\mathfrak{a}$ 都可以乘上一个元素 $x \in \mathfrak{a}^{-1} - \{0\}$ 使得 $N(x\mathfrak{a}) \leq M$，注意 $x\mathfrak{a}$ 是整理想，所以每一个理想类都会对应某一个满足范数小于 M 的整理想，并且不同的理想类不可能对应同一个整理想，由后者的有限性我们知道理想类是有限的. □

3.3 Dirichlet 单位定理

Minkowski 空间也有对应的乘法理论，设 τ 跑遍所有嵌入 $\tau : K \to \mathbb{C}$. 定义

$$K_{\mathbb{C}}^{\times} := \prod_{\tau} \mathbb{C}^{\times}.$$

由所有嵌入组成的映射

$$j : K^{\times} \to K_{\mathbb{C}}^{\times} = \prod_{\tau} \mathbb{C}^{\times}, \qquad a \mapsto (\tau(a))_{\tau}$$

是一个群同态. 事实上，对任意 $a, b \in K^{\times}$，

$$j(ab) = (\tau(ab))_{\tau} = (\tau(a)\tau(b))_{\tau} = j(a)j(b).$$

这就是加法映射

$$j : K \to \prod_{\tau} \mathbb{C}$$

的乘法版本. 在乘法群 $K_{\mathbb{C}}^{\times}$ 上定义同态

$$N : K_{\mathbb{C}}^{\times} \to \mathbb{C}^{\times}, \qquad (z_{\tau})_{\tau} \mapsto \prod_{\tau} z_{\tau}.$$

这是一个群同态，因为

$$N((z_{\tau})_{\tau}(w_{\tau})_{\tau}) = \prod_{\tau}(z_{\tau}w_{\tau}) = \left(\prod_{\tau} z_{\tau}\right)\left(\prod_{\tau} w_{\tau}\right)$$

复合映射

$$K^{\times} \xrightarrow{j} K_{\mathbb{C}}^{\times} \xrightarrow{N} \mathbb{C}^{\times}$$

恰好给出通常的域范数

$$N_{K|\mathbb{Q}} : K^\times \to \mathbb{Q}^\times$$

也就是说，对任意 $a \in K^\times$，

$$N_{K|\mathbb{Q}}(a) = N(j(a)) = \prod_\tau \tau(a)$$

因此，域范数可以理解为所有嵌入值的乘积，这与加法版本中的迹公式完全平行：

$$\mathrm{Tr}_{K|\mathbb{Q}}(a) = \sum_\tau \tau(a)$$

为了得到格论结构，需要从乘法群过渡到加法群. 定义

$$\ell : \mathbb{C}^\times \to \mathbb{R}, \qquad z \mapsto \log|z|$$

这是一个群同态，其中 $\mathbb{C}^\times$ 取乘法结构，$\mathbb{R}$ 取加法结构. 因为

$$\ell(z_1 z_2) = \log|z_1 z_2| = \log|z_1| + \log|z_2| = \ell(z_1) + \ell(z_2)$$

由此得到逐坐标定义的同态

$$\ell : K_{\mathbb{C}}^\times \to \prod_\tau \mathbb{R}, \qquad (z_\tau)_\tau \mapsto (\log|z_\tau|)_\tau$$

这也是一个群同态，因为每个坐标上都是群同态，于是得到复合映射

$$K^\times \xrightarrow{j} K_{\mathbb{C}}^\times \xrightarrow{\ell} \prod_\tau \mathbb{R}$$

即

$$a \mapsto (\log|\tau(a)|)_\tau$$

对任意 $(z_\tau)_\tau \in K_{\mathbb{C}}^\times$，有

$$\mathrm{Tr}(\ell((z_\tau)_\tau)) = \sum_\tau \log|z_\tau| = \log\left|\prod_\tau z_\tau\right| = \ell(N((z_\tau)_\tau))$$

因此

$$\mathrm{Tr} \circ \ell = \ell \circ N$$

作用到 $a \in K^\times$ 上便得到

$$\sum_\tau \log|\tau(a)| = \log|N_{K|\mathbb{Q}}(a)|$$

这是最重要的公式之一. 上述关系可以用交换图表表示为

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{C}}^\times & \xrightarrow{\ell} & \prod_\tau \mathbb{R} \\ \downarrow{\scriptstyle N_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{C}^\times & \xrightarrow{\ell} & \mathbb{R} \end{array}$$

其中下方 $\mathbb{Q}^\times \hookrightarrow \mathbb{C}^\times$ 是自然包含. 回忆 F 为复共轭，作用在整个图表的各个对象上：

- 在 $K^\times$ 上作用平凡；
- 在 $K_{\mathbb{C}}^\times = \prod_\tau \mathbb{C}^\times$ 上，定义同前：
$$(Fz)_\tau = \overline{z_{\overline{\tau}}}$$
- 在 $\prod_\tau \mathbb{R}$ 上，因实数取共轭不变，所以只作用在指标上：
$$(Fx)_\tau = x_{\overline{\tau}}$$

这些映射都与 F 相容，即有

$$F \circ j = j, \qquad F \circ \ell = \ell \circ F, \qquad N \circ F = F \circ N, \qquad \mathrm{Tr} \circ F = \mathrm{Tr}$$

因此整个图表是 $G(\mathbb{C}|\mathbb{R})$-等变的. 对上述图表处处取 F-不动点，得到新的图表. 记

$$K_{\mathbb{R}}^\times := (K_{\mathbb{C}}^\times)^F$$

上标 F 表示不动点，同时记

$$\left[\prod_\tau \mathbb{R}\right]^+$$

为 $\prod_\tau \mathbb{R}$ 在指标交换作用下的不动点部分. 于是得到交换图表

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_{\mathbb{R}}^\times & \xrightarrow{\ell} & \left[\prod_\tau \mathbb{R}\right]^+ \\ \downarrow{\scriptstyle N_{K|\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{R}^\times & \xrightarrow{\ell} & \mathbb{R} \end{array}$$

设 K 的 signature 为 (r, s)，即有 r 个实嵌入

$$\rho_1, \dots, \rho_r : K \to \mathbb{R}$$

有 s 对复共轭嵌入

$$\sigma_1, \overline{\sigma_1}, \dots, \sigma_s, \overline{\sigma_s} : K \to \mathbb{C}$$

因此

$$[K : \mathbb{Q}] = r + 2s$$

考虑按实嵌入与复嵌入对分组，可写为

$$\prod_\tau \mathbb{R} = \prod_\rho \mathbb{R} \times \prod_\sigma (\mathbb{R} \times \mathbb{R})$$

其中每个 σ 表示一对共轭嵌入 $(\sigma, \overline{\sigma})$. 复共轭作用 F 在每个 $\mathbb{R} \times \mathbb{R}$ 因子上交换两个坐标：

$$F(x, y) = (y, x)$$

因此不动点条件就是

$$(x, y) = (y, x)$$

即

$$x = y$$

所以

$$\left[\prod_{\tau} \mathbb{R}\right]^{+} = \prod_{\rho} \mathbb{R} \times \prod_{\sigma} \{(x, x) : x \in \mathbb{R}\}$$

每个复嵌入对只贡献一个实参数，因此这个空间的维数是 $r+s$. 将每个因子 $\{(x,x) : x \in \mathbb{R}\}$ 用映射

$$(x, x) \mapsto 2x$$

识别为 $\mathbb{R}$，便得到一个同构

$$\left[\prod_{\tau} \mathbb{R}\right]^{+} \cong \mathbb{R}^{r+s}$$

乘 2 是为了保持 tr 映射在这个同构下的值不会改变.

$$\mathrm{Tr}(x_1, \ldots, x_{r+s}) = x_1 + \cdots + x_{r+s}.$$

在上述同构

$$\left[\prod_{\tau} \mathbb{R}\right]^{+} \cong \mathbb{R}^{r+s}$$

下，对数映射

$$\ell : K_{\mathbb{R}}^{\times} \to \mathbb{R}^{r+s}$$

可具体写为

$$\ell(x) = \left(\log|x_{\rho_1}|, \ldots, \log|x_{\rho_r}|, \log|x_{\sigma_1}|^2, \ldots, \log|x_{\sigma_s}|^2\right)$$

其中

$$x = (x_\tau) \in K_{\mathbb{R}}^{\times} \subseteq \prod_{\tau} \mathbb{C}^{\times}$$

若 $a \in K^{\times}$，则

$$j(a) = (\tau(a))_\tau \in K_{\mathbb{R}}^{\times}$$

于是对数嵌入可写成

$$a \longmapsto \left(\log|\rho_1(a)|, \ldots, \log|\rho_r(a)|, \log|\sigma_1(a)|^2, \ldots, \log|\sigma_s(a)|^2\right)$$

故对任意 $a \in K^{\times}$，有

$$\mathrm{Tr}(\ell(j(a))) = \log|N_{K|\mathbb{Q}}(a)|.$$

现在若 $u \in \mathcal{O}_K^{\times}$ 是代数整数环的单位，则

$$u \in \mathcal{O}_K^{\times} \iff N_{K|\mathbb{Q}}(u) \in \{\pm 1\}$$

因此等价于

$$\log|N_{K|\mathbb{Q}}(u)|=0$$

于是单位的对数像满足

$$\sum_{i=1}^{r}\log|\rho_i(u)|+\sum_{j=1}^{s}\log|\sigma_j(u)|^2=0$$

也就是说，单位群的像落在超平面

$$H=\left\{(x_1,\dots,x_{r+s})\in\mathbb{R}^{r+s}\;\middle|\;x_1+\cdots+x_{r+s}=0\right\}$$

这个超平面的维数是 $r+s-1$. 我们记 $\mu(K)$ 为 K 中的单位根群，它是 $\mathcal{O}_K^\times$ 的一个有限子群，我们通过一些努力可以知道：

定理 3.3.1: Dirichlet 单位定理

K 是数域，r 是实嵌入个数，s 为复嵌入对数，则

$$\mathcal{O}_K^\times=\mu(K)\times\mathbb{Z}^{r+s-1}$$

其道理在于我们可以通过上述的方式将 $\mathcal{O}_K^\times$ 嵌入 H，我们记这个嵌入为 λ，于是只需要证明 $\Gamma=\lambda(\mathcal{O}_K^\times)$ 是 H 的一个完备格，我们先断言

$$1\to\mu(K)\to\mathcal{O}_K^\times\xrightarrow{\lambda}\Gamma\to 0$$

是正合的. 其道理在于 $j(\operatorname{Ker}\lambda)$ 在 $K_{\mathbb{R}}$ 中是有界的，而 $j(\mathcal{O}_K)$ 是格，可见 $j(\operatorname{Ker}\lambda)$ 是有限子群，而 $K^\times$ 的有限子群只能是单位根群的子群，从而容易得到.

Remark 3.3.1

由上面过程立刻得到如果元素 $u\in\mathcal{O}_K$ 对所有嵌入 σ 都有 $|\sigma(u)|=1$，则 $u\in\mu(K)$.

我们在证明过程中还需要用到引理：

引理 3.3.1: 定范数元素有限

固定一个整数 $a\in\mathbb{Z}$，则在 $\mathcal{O}_K$ 中满足 $|N_{K/\mathbb{Q}}(\alpha)|=a$ 的元素，在模去单位元的相伴关系之后只有有限多个.

证明: 考虑理想 $a\mathcal{O}_K$，商环 $\mathcal{O}_K/a\mathcal{O}_K$ 是有限集，所以只有有限多个陪集，而在每个陪集中，至多只能有一个元素(在相伴意义下)能具有范数 $\pm a$，反之若存在 α,β 在同一个陪集中都满足 $|N(\alpha)|=|N(\beta)|=a$，则

$$\beta=\alpha+a\gamma,\quad\gamma\in\mathcal{O}_K$$

注意到 α,β 整除 a(考虑 $a=N(\alpha)=\prod_\sigma\sigma(\alpha)$)

$$\frac{\alpha}{\beta}=1-\frac{a}{\beta}\gamma\in\mathcal{O}_K$$

同理 $\beta/\alpha \in \mathcal{O}_K$，故 $\alpha/\beta \in \mathcal{O}_K^\times$，所以相伴. □

后面的步骤大概是先把单位群通过对数嵌入 $\lambda : \mathcal{O}_K^\times \to H$ 送到迹为零的超平面 H 中，把乘法问题转化为加法问题；其核正好是单位根群 $\mu(K)$，所以单位群除去扭部分后就等同于像 $\Gamma = \lambda(\mathcal{O}_K^\times)$. 接着证明 Γ 在 H 中既离散又铺满整个空间，也就是一个完全格：离散性来自整数环在 Minkowski 空间中本身是格，而铺满性则借助 Minkowski 定理和“给定范数模单位只有有限多个元素”这一有限性结论，构造出一个有界基本区域，其单位平移覆盖整个范数一曲面，从而对数化后得到 Γ 的平移覆盖整个 H. 因此 $\Gamma \cong \mathbb{Z}^{r+s-1}$，最终推出狄利克雷单位定理

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^{r+s-1}$$

我们可以考虑其**基本单位** $\varepsilon_1, \cdots, \varepsilon_{r+s-1}$，使得它们生成 $\mathcal{O}_K^\times$ 的自由部分，记 $t = r + s - 1$. 在对数嵌入之下，单位群的像落在超平面

$$H = \{(x_1, \ldots, x_{r+s}) \in \mathbb{R}^{r+s} : x_1 + \cdots + x_{r+s} = 0\}$$

向量

$$\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t) \in H$$

张成该格的一个基本网格，其 t 维体积可用来度量这个单位格的大小. 为了计算这个体积，引入向量

$$\lambda_0 = \frac{1}{\sqrt{r+s}}(1, \ldots, 1) \in \mathbb{R}^{r+s}$$

由于 λ_0 与 H 正交且范数为 1，所以由 $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$ 在 H 中张成的 t 维体积，恰好等于由

$$\lambda_0, \lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$$

在 $\mathbb{R}^{r+s}$ 中张成的 $(t+1)$ 维平行多面体体积. 因此这个体积可以写成相应行列式的绝对值. 将这些向量按列排成矩阵之后，对矩阵作初等行变换：把所有行加到某一个固定行上. 由于每一列 $\lambda(\varepsilon_j)$ 的分量和都等于零，这样变换以后，在该固定行中，除第一列对应的 λ_0 之外，其余各项都变为零，而第一列的该项变为

$$\sqrt{r+s}$$

于是整个行列式按该行展开，得到单位格基本平行多面体的体积等于 $\sqrt{r+s}$ 乘上由矩阵

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

的任意一个秩为 t 的子式所给出的行列式绝对值. 记这个绝对值为 R，则有

$$\mathrm{vol}\big(\lambda(\mathcal{O}_K^\times)\big) = \sqrt{r+s} \cdot R$$

这里的 R 称为数域 K 的**regulator**. 之所以可以取上述矩阵的任意一个秩为 t 的子式，是因为所有列向量都落在超平面 H 中，从而各行之间满足一个线性关系，即所有行的和为零，所以删去任意一行所得到的 $t \times t$ 子矩阵，其行列式仅差一个符号，因而绝对值相同. 于是 R 的定义与所删去的那一行无关. 这个结果说明，Dirichlet 单位定理不仅给出单位群的结构，还赋予了其中自由部分一个自然的欧几里得几何不变量.

3.4 Dedekind 整环的扩张

考虑数域 K，我们想要研究 $\mathcal{O}_K$ 的素理想，注意到对任意素理想 $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$，我们取一个非零元素 a 出来，知道

$$0 \neq N_{K/\mathbb{Q}}(a) = \prod_{\sigma} \sigma(a) \in \mathcal{O}_K \cap \mathbb{Z}$$

所以知道 $\mathcal{O}_K \cap \mathbb{Z}$ 是一个素理想 (p)，所以我们想问一个素数 p 在 $\mathcal{O}_K$ 中将如何表示为不同素理想的乘积？我们将从更一般的情况来讨论，从任意 Dedekind 整环 $\mathcal{O}$ 开始，考虑在其分式域的有限扩张的整闭包 $\mathfrak{O}$.

命题 3.4.1

令 $\mathcal{O}$ 为 Dedekind 整环，其分式域为 K，L/K 是有限扩张，$\mathfrak{O}$ 为 $\mathcal{O}$ 在 L 中的整闭包，则 $\mathfrak{O}$ 仍然是 Dedekind 整环.

虽然对不可分的情况也是成立的，但是该命题在可分扩张的时候比较容易证明，因为此时迹非退化，从而可以使用判别式来证明 Noether 性，而我们所关心的问题一般也是可分的.

我们可以说明对于 $\mathfrak{p} \in \mathcal{O}$，总是有

$$\mathfrak{p}\mathfrak{O} \neq \mathfrak{O}$$

这是因为可选择 $\pi \in \mathfrak{p} - \mathfrak{p}^2$，从而可见

$$\pi\mathcal{O} = \mathfrak{p}\mathfrak{a}$$

其中 $\mathfrak{p} \nmid \mathfrak{a}$，从而 $\mathfrak{p} + \mathfrak{a} = \mathcal{O}$. 令 $1 = b + s$，其中 $b \in \mathfrak{p}, s \in \mathfrak{a}$，我们知道 $s \notin \mathfrak{p}$，否则 $\mathfrak{p} = \mathcal{O}$，而

$$s\mathfrak{p} \subset \mathfrak{p}\mathfrak{a} = \pi\mathcal{O}$$

从而若 $\mathfrak{p}\mathfrak{O} = \mathfrak{O}$，则

$$s\mathfrak{O} = s\mathfrak{p}\mathfrak{P} \subset \pi\mathfrak{P}$$

于是 $s = \pi x$，其中 $x \in \mathfrak{O}$，而可见 $x = s/\pi \in K$，故 $x \in \mathfrak{O} \cap K = \mathcal{O}$，从而 $s \in \mathfrak{p}$ 矛盾. 从而我们知道 $\mathfrak{p}$ 在 $\mathfrak{O}$ 中会分裂成素理想的乘积

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

我们称那些 $\mathfrak{P}_i \mid \mathfrak{p}$ 的素理想 lie over $\mathfrak{p}$，而素理想 lie over $\mathfrak{p}$ 当且仅当

$$\mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$$

简单记为 $\mathfrak{P} \mid \mathfrak{p}$，称其指数

$$e_i =: e(\mathfrak{P}_i|\mathfrak{p})$$

为分歧指数，称其剩余域的扩张次数

$$f_i = [\mathfrak{O}/\mathfrak{P}_i : \mathcal{O}/\mathfrak{p}] =: f(\mathfrak{P}_i|\mathfrak{p})$$

为**惯性次数(inertia degree)**，我们要声明分歧指数和惯性次数具有塔性质，即如果 $L/T/K$ 是域的扩张，$\mathfrak{P}|\mathfrak{p}|p$ 是素理想的整除，则我们有

$$e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p}) \cdot e(\mathfrak{p}|p), \quad f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p}) \cdot f(\mathfrak{p}|p)$$

命题 3.4.2: 基本恒等式

令 $L|K$ 为可分扩张，则我们有

$$\sum_{i=1}^{r} e_i f_i = n$$

现在如果给定一个可分扩张 $L|K$，则存在本原元 $\theta \in \mathfrak{O}$ 使得其极小多项式 $p(X) \in \mathcal{O}[X]$，此时我们有 $L = K(\theta)$. 利用这个我们可以计算素理想是如何分裂的. 我们称被 $\mathcal{O}[\theta]$ 包含的 $\mathfrak{O}$ 的最大理想 $\mathfrak{f}$ 为**导子(conductor)**，换言之

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

再换言之

$$\mathfrak{f} = \mathrm{Ann}_{\mathcal{O}[\theta]}(\mathfrak{O}/\mathcal{O}[\theta])$$

定理 3.4.1: 素理想的分解

令 $\mathfrak{p}$ 为 $\mathcal{O}$ 的素理想，并且 $\mathfrak{p}$ 与 $\mathfrak{f}$ 互素，则在 $(\mathcal{O}/\mathfrak{p})[X]$ 中我们有首一不可约分解

$$p(X) = p_1(X)^{e_1} \cdots p_r(X)^{e_r} \mod \mathfrak{p}$$

则令

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

有 $\mathfrak{P}_i$ 均为素理想并且

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

并且满足 $f(\mathfrak{P}_i|\mathfrak{p}) = \deg p_i(X)$.

这里要求与导子互素本质上是为了

$$\mathfrak{O}/\mathfrak{p}\mathfrak{O} = \mathcal{O}[\theta]/\mathfrak{p}\mathcal{O}[\theta]$$

与导子互素一般不太容易检查，我们可以考虑 $m = \#\mathfrak{O}/\mathcal{O}[\theta]$，会注意到 $m\mathfrak{O} \subset \mathcal{O}[\theta]$，故 $m \in \mathfrak{f}$，所以只需要 $\mathfrak{p}$ 与 $m\mathfrak{O}$ 互素就可以得到和导子互素，所以在实践中我们往往首先检查 $\mathfrak{p}$ 是否与 $\#\mathfrak{O}/\mathcal{O}[\theta]$ 互素. 我们称 $\mathfrak{p}$ 在 L 中**完全分裂**，若

$$\mathfrak{p} = \mathfrak{P}_1 \cdot \mathfrak{P}_n$$

即所有 $e(\mathfrak{P}_i|\mathfrak{p}) = f(\mathfrak{P}_i|\mathfrak{p}) = 1$，而 $r = [L : K] = n$. 称分解中

$$\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$$

的某个满足 $e_i = 1$，并且 $\mathfrak{O}/\mathfrak{P}_i|\mathcal{O}/\mathfrak{p}$ 是可分扩张的素理想 $\mathfrak{P}_i$ 为**非分歧**，反之称为**分歧**，若额外还有 $f_i = 1$，则称为**完全分歧**. r 也有时称为**分裂次数**.

实际上，分歧的素理想是比较少的，我们叙述下面的简单情况：

定理 3.4.2: Dedekind判别式定理

$L|K$ 是数域的扩张，$d(K)$ 为 $L|K$ 的判别式，则 $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ 在 L 中分歧当且仅当 $\mathfrak{p} \mid d(K)$.

从而可见只有有限多个素理想是分歧的，绝大部分的素理想都是非分歧的情况.

3.5 Hilbert 分歧理论

本章中考虑 L/K 是 Galois 扩张的情况，我们会发现 $G = \operatorname{Gal}(L/K)$ 中的元素 σ 会作用在 $\mathcal{O}_L$ 上，特别地，对于 $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$，$\mathfrak{P}$ 是 $\mathfrak{p}$ 上的素理想，注意到

$$\sigma\mathfrak{P} \cap \mathcal{O}_K = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \mathfrak{p}$$

所以 $\sigma\mathfrak{P}$ 也是 $\mathfrak{p}$ 上的素理想，称为 $\mathfrak{P}$ 的共轭. 可以证明 G 在 $\{\mathfrak{P} \in \operatorname{Spec} \mathcal{O}_L \colon \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}\}$ 上的作用是传递的.

命题 3.5.1

$G = \operatorname{Gal}(L/K)$ 在 $\{\mathfrak{P} \in \operatorname{Spec} \mathcal{O}_L \colon \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}\}$ 上的作用是传递的.

于是我们可以给出定义：

定义 3.5.1: 分解群与分解域

若 $\mathfrak{P}$ 是 $\mathcal{O}_L$ 的素理想，则子群

$$G_{\mathfrak{P}} := \{\sigma \in G \colon \sigma\mathfrak{P} = \mathfrak{P}\}$$

*称为 $\mathfrak{P}$ 在 K 上的**分解群**，其不变子域*

$$Z_{\mathfrak{P}} := L^{G_{\mathfrak{P}}}$$

*称为 $\mathfrak{P}$ 在 K 上的**分解域**.*

不难注意到 $G_{\sigma\mathfrak{P}} = \sigma G_{\mathfrak{P}} \sigma^{-1}$. 这与 Galois 理论是一样的，毕竟我们会注意到

$$G_{\mathfrak{P}} = \operatorname{Gal}(L/Z_{\mathfrak{P}})$$

在 Galois 扩张的情况下，设 $f_1, \cdots, f_r$ 与 $e_1, \cdots, e_r$ 分别为素理想分解

$$\mathfrak{p} = \mathfrak{P}_r^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

的惯性度与分歧指数，我们可以说明 $f_1 = \cdots = f_r$，$e_1 = \cdots = e_r$，这是因为

$$\mathfrak{p} = \sigma(\mathfrak{p}) = \prod_{i=1}^{r} (\sigma\mathfrak{P}_i)^{e_i}$$

注意到作用可递与素理想的唯一分解，立刻得到分歧指数的相等，再注意到

$$\mathcal{O}_L/\mathfrak{P} \cong \mathcal{O}_L/\sigma\mathfrak{P}, \quad [a] \mapsto [\sigma a]$$

所以 $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}] = [\mathcal{O}_L/\sigma\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$，故惯性度也是都相等的. 所以这是对于 $\mathfrak{p}$ 在域扩张 L/K 上的一个不变量.

现在我们可以令 $\mathfrak{P}_Z = \mathfrak{P} \cap Z_{\mathfrak{P}}$，于是我们有素理想的整除链 $\mathfrak{P} \mid \mathfrak{P}_Z \mid \mathfrak{p}$，利用域扩张的塔性质我们可以证明：

命题 3.5.2

L/K 为 Galois 扩张，$\mathfrak{p}$ 在其上的分歧指数为 e，惯性次数为 f，我们有

(1) $\mathfrak{P}_Z$ 在 L 中惰性，即 $\mathfrak{P}$ 是唯一 over $\mathfrak{P}_Z$ 的素理想.

(2) $\mathfrak{P}$ 在 $Z_{\mathfrak{P}}$ 上的分歧指数为 e，惯性次数为 f.

(3) $\mathfrak{P}_Z$ 在 K 上的分歧指数和惯性度都是 1.

从证明中可见 $\#G_{\mathfrak{P}} = [L : Z_{\mathfrak{P}}] = ef$. 由于对 $\sigma \in G_{\mathfrak{P}}$，有 $\sigma\mathcal{O}_L = \mathcal{O}_L$ 并且 $\sigma\mathfrak{P} = \mathfrak{P}$，于是诱导了自同构

$$\overline{\sigma} \colon \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}, \quad [a] \mapsto [\sigma a]$$

我们将素理想 $\mathfrak{P}$ 的**剩余域**记为 $\kappa(\mathfrak{P})$，同理 $\kappa(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$. 记号同上，我们可以证明 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 是正规扩张，并且可以得到一个满射

$$G_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$$

从而可以得到如下定义：

定义 3.5.2: 惯性群

*定义 $\mathfrak{P}$ 在 K 上的**惯性群**为*

$$I_{\mathfrak{P}} := \mathrm{Ker}\left(G_{\mathfrak{P}} \to \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))\right)$$

定义其不变子域

$$T_{\mathfrak{P}} := L^{I_{\mathfrak{P}}}$$

*为 $\mathfrak{P}$ 在 K 上的**惯性域**.*

显然可见 $\mathrm{Gal}(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}}$，我们自然有正合列

$$1 \longrightarrow I_{\mathfrak{P}} \longrightarrow G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \longrightarrow 1$$

所以 $I_{\mathfrak{P}}$ 是 $G_{\mathfrak{P}}$ 的正规子群，Galois 理论告诉我们 $T_{\mathfrak{P}}/Z_{\mathfrak{P}}$ 是正规扩张(由 $L/Z_{\mathfrak{P}}$ 可分还知道是 Galois 扩张)，于是我们有

$$\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) = \frac{G_{\mathfrak{P}}}{I_{\mathfrak{P}}} = \frac{\mathrm{Gal}(L/Z_{\mathfrak{P}})}{\mathrm{Gal}(L/T_{\mathfrak{P}})} = \mathrm{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}})$$

若额外 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 是可分扩张，结合前面已经说过是正规扩张，则自然是 Galois 扩张，所以我们有

$$(G_{\mathfrak{P}} : I_{\mathfrak{P}}) = [T_{\mathfrak{P}} : Z_{\mathfrak{P}}] = |\,\mathrm{Gal}(T_{\mathfrak{P}}/Z_{\mathfrak{P}})| = |\,\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))| = [\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = f$$

所以可见

$$[L : T_{\mathfrak{P}}] = \#\,\mathrm{Gal}(L/T_{\mathfrak{P}}) = \#I_{\mathfrak{P}} = \#\frac{|G_{\mathfrak{P}}|}{f} = e$$

我们也可以考虑 $\mathfrak{P}_T = \mathfrak{P} \cap T_{\mathfrak{P}}$，有如下结论：

命题 3.5.3

记号承上，若 $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ 是可分扩张，则

(1) $\mathfrak{P}$ 在 $\mathfrak{P}_T$ 上的分歧指数为 e，惯性度为 1.

(2) $\mathfrak{P}_T$ 在 $\mathfrak{P}_Z$ 上的分歧指数为 1，惯性度为 f.

道理在于考虑 Galois 扩张 $L/T_{\mathfrak{P}}$，对于这个扩张而言，$\mathfrak{P}$ 的分解群 $G_{\mathfrak{P}}^{L/T_{\mathfrak{P}}}$ 为那些保持 $\mathfrak{P}$ 不动的 $\mathrm{Gal}(L/T_{\mathfrak{P}}) = I_{\mathfrak{P}} \subset G_{\mathfrak{P}}$ 中的元素，那由于全部都落在 $G_{\mathfrak{P}}$ 中，所以

$$G_{\mathfrak{P}}^{L/T_{\mathfrak{P}}} = I_{\mathfrak{P}}$$

而 $\mathfrak{P}$ 的惯性群 $I_{\mathfrak{P}}^{L/T_{\mathfrak{P}}}$ 为那些使得

$$a \equiv \sigma(a) \mod \mathfrak{P}$$

的 $\sigma \in G_{\mathfrak{P}}^{L/T_{\mathfrak{P}}} = I_{\mathfrak{P}}$，而这由 $I_{\mathfrak{P}}$ 的定义也是自然全部满足的，故

$$I_{\mathfrak{P}}^{L/T_{\mathfrak{P}}} = I_{\mathfrak{P}}$$

所以会存在正合列

$$1 \longrightarrow I_{\mathfrak{P}}^{L/T_{\mathfrak{P}}} \longrightarrow G_{\mathfrak{P}}^{L/T_{\mathfrak{P}}} \longrightarrow \mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_T)) \longrightarrow 1$$

告诉我们

$$\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_T)) = \frac{G_{\mathfrak{P}}^{L/T_{\mathfrak{P}}}}{I_{\mathfrak{P}}^{L/T_{\mathfrak{P}}}} = \frac{I_{\mathfrak{P}}}{I_{\mathfrak{P}}} = 1$$

所以 $\kappa(\mathfrak{P}) = \kappa(\mathfrak{P}_T)$，于是可见

$$f(\mathfrak{P}|\mathfrak{P}_T) = 1$$

而由于 $\mathfrak{P}$ 是 $\mathfrak{P}_Z$ 上唯一的素理想，同理也是 $\mathfrak{P}_T$ 上唯一的素理想，所以基本等式告诉我们

$$e = [L : T_{\mathfrak{P}}] = e(\mathfrak{P}|\mathfrak{P}_T) f(\mathfrak{P}|\mathfrak{P}_T)$$

故

$$e(\mathfrak{P}|\mathfrak{P}_T) = e$$

再利用扩张的塔性质，立刻有

$$e = e(\mathfrak{P}|\mathfrak{P}_Z) = e(\mathfrak{P}|\mathfrak{P}_T)e(\mathfrak{P}_T|\mathfrak{P}_Z), \quad f = f(\mathfrak{P}|\mathfrak{P}_Z) = f(\mathfrak{P}|\mathfrak{P}_T)e(\mathfrak{P}_T|\mathfrak{P}_Z)$$

立刻得到

$$e(\mathfrak{P}_T|\mathfrak{P}_Z) = 1, \quad f(\mathfrak{P}_T|\mathfrak{P}_Z) = f$$

于是我们可见整个分歧过程被完美的刻画.

$$\begin{array}{ccccc}
L & \mathfrak{P} & \mathfrak{P}_T = \mathfrak{P}^e & & \{1\} \\
\uparrow{\scriptstyle e}\,|\,{\scriptstyle 1} & \text{ramify}\,| & & & \downarrow{\scriptstyle e} \\
T_{\mathfrak{P}} & \mathfrak{P}_T & [\kappa(\mathfrak{P}_T) : \kappa(\mathfrak{P}_Z)] = f & & I_{\mathfrak{P}} \\
\uparrow{\scriptstyle 1}\,|\,{\scriptstyle f} & \text{inertia}\,| & & & \downarrow{\scriptstyle f} \\
Z_{\mathfrak{P}} & \mathfrak{P}_Z & \mathfrak{p} = \prod_{i=1}^{r} (\mathfrak{P}_i)_Z & & G_{\mathfrak{P}} \\
\uparrow{\scriptstyle 1}\,|\,{\scriptstyle 1} & \text{split}\,| & & & \downarrow{\scriptstyle r} \\
K & \mathfrak{p} & & & \mathrm{Gal}(L/K)
\end{array}$$

其中 $K \to Z_{\mathfrak{P}}$ 只蕴含了分裂出的不同素理想的信息，没有蕴含分歧与惯性指数的信息，而 $Z_{\mathfrak{P}} \to T_{\mathfrak{P}}$ 蕴含了惯性指数的信息，$T_{\mathfrak{P}} \to L$ 蕴含了分歧指数的信息，通过这些分解我们将 $\mathfrak{P} \mid \mathfrak{p}$ 的过程完全分成了 $\mathfrak{P} \mid \mathfrak{P}_T \mid \mathfrak{P}_Z \mid \mathfrak{p}$，分别蕴含了分歧，惯性，分裂的信息.

对于非分歧的素数 $\mathfrak{P}$ over $\mathfrak{p}$，在 Galois 扩张中我们知道 $e = 1$，从而可见 $I_{\mathfrak{P}} = \{1\}$. 此时有群同构

$$G_{\mathfrak{P}} \cong \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$$

而后者为有限域的 Galois 群，从而是循环群，由 Frobenius 元生成，记 $N = N_{K/\mathbb{Q}}(\mathfrak{p})$，生成元表示为

$$\left(\frac{L|K}{\mathfrak{P}}\right) : \kappa(\mathfrak{P}) \to \kappa(\mathfrak{P}), \quad a \mapsto a^N \mod \mathfrak{P}$$

这是一个 $f = f(\mathfrak{P}|\mathfrak{p})$ 阶元，故这种情况下 $G_{\mathfrak{P}}$ 是一个 f 阶循环群. 关于这个记号，有如下引理：

引理 3.5.1: Frobenius 自同构的性质

设 L/K 为数域的 *Galois* 扩张，$\mathfrak{P} \mid \mathfrak{p}$，并且 $e(\mathfrak{P}|\mathfrak{p}) = 1$，则

(1) $\forall \sigma \in \mathrm{Gal}(L|K)$，都有 $\left(\dfrac{L|K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\dfrac{L|K}{\mathfrak{P}}\right)\alpha^{-1}$.

(2) 若 E 是 $L|K$ 的中间域，令 $\mathfrak{P} \cap E = \mathfrak{P}_E$，则 $e(\mathfrak{P}|\mathfrak{P}_E) = 1$，并且

$$\left(\frac{L|E}{\mathfrak{P}}\right) = \left(\frac{L|K}{\mathfrak{P}}\right)^{f(\mathfrak{P}_E|\mathfrak{p})}$$

(3) 如果 $E|K$ 也是 *Galois* 扩张，则 $e(\mathfrak{P}_E|\mathfrak{p}) = 1$，并且

$$\left(\frac{E|K}{\mathfrak{P}_E}\right) = \left(\frac{L|K}{\mathfrak{P}}\right)\Big|_E$$

证明都是直白的，作为应用，我们可以得到：

命题 3.5.4: 完全分裂与非分歧被合成保持

E_1/K 与 E_2/K 都是 *Galois* 扩张，令 $L = E_1E_2$，则

(1) L/K 也是 *Galois* 扩张，并且 $\mathrm{Gal}(L|K)$ 同构于 $\mathrm{Gal}(E_1|K) \times \mathrm{Gal}(E_2|K)$ 的一个子群.

(2) K 中素理想 $\mathfrak{p}$ 在 L 中不分歧 $\iff$ $\mathfrak{p}$ 在 E_1 与 E_2 中均不分歧.

(3) $\mathfrak{p}$ 在 L 中完全分裂 $\iff$ $\mathfrak{p}$ 在 E_1 与 E_2 中均完全分裂.

证明: (1) 是显然的，我们记嵌入映射为

$$\varphi\colon \mathrm{Gal}(L|K) \to \mathrm{Gal}(E_1|K) \times \mathrm{Gal}(E_2|K)$$

我们看 (2)，设 $\mathfrak{P} \mid \mathfrak{p}$ 为 L 的素理想，令 $\mathfrak{P}_i = \mathfrak{P} \cap \mathcal{O}_{E_i}$，若 $\sigma \in D_{\mathfrak{P}}$，则

$$\sigma(\mathfrak{P}_i) = \sigma(\mathfrak{P} \cap \mathcal{O}_{E_i}) = \mathfrak{P} \cap \mathcal{O}_{E_i} = \mathfrak{P}_i$$

这说明 $\sigma|_{E_i} \in D_{\mathfrak{P}_i}$，于是可见 $\varphi(D_{\mathfrak{P}}) \subseteq D_{\mathfrak{P}_1} \times D_{\mathfrak{P}_2}$. 从而对 $\sigma \in I_{\mathfrak{P}}$，我们知道对任意的 $x \in \mathcal{O}_L$，都有

$$\sigma(x) - x \in \mathfrak{P}$$

从而对任意的 $x \in \mathcal{O}_{E_i}$，有

$$\sigma|_{E_i}(x) - x \in \mathfrak{P} \cap \mathcal{O}_{E_i} = \mathfrak{P}_i$$

可见 $\varphi(I_{\mathfrak{P}}) \subset I_{\mathfrak{P}_1} \times I_{\mathfrak{P}_2}$. 从而我们能看到 $\mathfrak{p}$ 在 E_i 中非分歧 $\iff$ $I_{\mathfrak{P}_1} = I_{\mathfrak{P}_2} = \{1\}$ $\implies$ $I_{\mathfrak{P}} = \{1\}$ $\implies$ $\mathfrak{p}$ 在 L 中非分歧. 反之如果 $\mathfrak{p}$ 在 L 中非分歧，显然可见在子域里非分歧.

(3) 从上面的引理我们知道

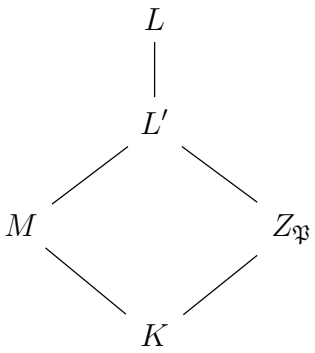
$$\varphi\left(\left(\frac{L|K}{\mathfrak{P}}\right)\right) = \left(\left(\frac{L|K}{\mathfrak{P}}\right)\Big|_{E_1}, \left(\frac{L|K}{\mathfrak{P}}\right)\Big|_{E_2}\right) = \left(\left(\frac{E_1|K}{\mathfrak{P}_1}\right), \left(\frac{E_2|K}{\mathfrak{P}_2}\right)\right)$$

从而 $\mathfrak{p}$ 在 L 中完全分裂 $\iff e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1 \iff \left(\frac{L|K}{\mathfrak{P}}\right) = 1 \iff \left(\frac{E_1|K}{\mathfrak{P}_1}\right) = 1, \left(\frac{E_2|K}{\mathfrak{P}_2}\right) = 1 \iff \mathfrak{p}$ 在 E_1 与 E_2 中完全分裂. 因为生成元为 1 意味着群平凡，从而剩余域也是平凡扩张. □

定理 3.5.1: 分解域与惯性域的最大性质

设 L/K 是数域的 *Abel* 扩张，$\mathfrak{p}$ 是 $\mathcal{O}_K$ 的素理想，$\mathfrak{P} \mid \mathfrak{p}$ 为 L 中的素理想，$Z_\mathfrak{P}$ 与 $T_\mathfrak{P}$ 为分解域与惯性域，则 $Z_\mathfrak{P}$ 为使得 $\mathfrak{p}$ 完全分裂的最大中间域，$T_\mathfrak{P}$ 为使得 $\mathfrak{p}$ 非分歧的最大中间域.*(在 Abel 扩张的情况下不同 $\mathfrak{P}$ 对应的分解群和惯性群是一样的，因为群是交换群.)*

证明: 由于 L/K 是 Abel 扩张，从而可见 $T_\mathfrak{P}$ 与 $Z_\mathfrak{P}$ 为 K 的 Galois 扩张. 考虑子域 M 使得 $\mathfrak{p}$ 在其上完全分裂，令 $L' = MZ_\mathfrak{P}$



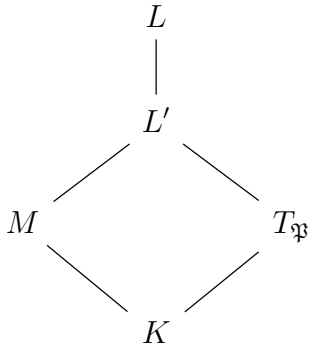
我们知道

$$\begin{aligned}[Z_\mathfrak{P} : K] &= \mathfrak{p} \text{ 在 } Z_\mathfrak{P} \text{ 上的分裂次数} \\ &= \mathfrak{p} \text{ 在 } L \text{ 上的分裂次数} \\ &\geq \mathfrak{p} \text{ 在 } L' \text{ 上的分裂次数}\end{aligned}$$

由前面的命题我们知道完全分裂是可以合成的，从而 $\mathfrak{p}$ 在 L' 中也完全分裂，从而我们知道

$$\mathfrak{p} \text{ 在 } L' \text{ 上的分裂次数} = [L' : K] \geq [Z_\mathfrak{P} : K]$$

可见 $L' = Z_\mathfrak{P}$ 即 $M \subset Z_\mathfrak{P}$. 故分解域是最大的使得 $\mathfrak{p}$ 完全分裂的中间域. 同理若 M 使得 $\mathfrak{p}$ 非分歧，则考虑 $L' = MT_\mathfrak{P}$



我们有所有分歧指数都是 1，从而

$$[L' : K] = f(\mathfrak{P} \cap \mathcal{O}_{L'}|\mathfrak{p})r(\mathfrak{P} \cap \mathcal{O}_{L'}|\mathfrak{p}) \leq f(\mathfrak{P}|\mathfrak{p})r(\mathfrak{P}|\mathfrak{p}) = [T_\mathfrak{P} : K]$$

其中 $r(-)$ 表示分裂次数，故而同理得证. □

最后，对于非 Abel 扩张也有类似的理论，我们浅尝辄止：令 L/K 为任意的可分扩张，可以嵌入进一个 K 的 Galois 扩张 $N/L/K$，令 $G=\mathrm{Gal}(N/K)$，$H=\mathrm{Gal}(N/L)$，令 $\mathfrak{p}$ 为 K 的素理想，$P_{\mathfrak{p}}$ 为 L 中 over $\mathfrak{p}$ 的素理想的集合，若 $\mathfrak{P}$ 为 N 中 over $\mathfrak{p}$ 的素理想，则

$$H\backslash G/G_{\mathfrak{P}}\to P_{\mathfrak{p}},\quad H\sigma G_{\mathfrak{P}}\mapsto \sigma\mathfrak{P}\cap L$$

给出了一个良定义的双射.

3.6 初见 p-adic

p-进数滥觞于 Hensel 从函数论的角度对数论的研究，旨在对整数模拟函数的 Taylor 乃至 Laurent 展开，首先我们可见任意的整数都可以展开成 p-进制的情况，如取 $p=3$，我们有

$$17=2\times 3^0+2\times 3^1+1\times 3^2$$

对这种情况进行模拟与推广，我们自然会有所谓 p-进整数的定义，即形式地定义

$$\mathbb{Z}_p:=\{a_0+a_1p+a_2p^2+\cdots\mid 0\le a_i<p,i\in\mathbb{N}\}$$

若模拟 Laurent 级数允许有限的负指标，则自然得到了 p-进数

$$\mathbb{Q}_p:=\{a_{-m}p^{-m}+\cdots+a_{-1}p^{-1}+a_0+a_1p+\cdots\mid m\in\mathbb{N}^*,0\le a_i<p\}$$

不难看出有自然的结构

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

p-进数的理论在解决丢番图方程时起到了重要的作用，比如随意考虑一个方程

$$F(X_1,\cdots,X_n)=0$$

其中 $F\in\mathbb{Z}[X_1,\cdots,X_n]$，直接解这个方程的整数解想必是不容易的，但是我们可以先考虑 $\mod p$ 情况下方程是否有解，如果在 $\mod p$ 的情况下都无解那整数情况更是无解. 若 $\mod p$ 有解，我们会进一步考虑 $\mod p^2$ 乃至更高次幂的情况下是否有解，我们会期盼是否像小数逼近一样可以得到真正意义上的整数解.

命题 3.6.1

$F(X_1,\cdots,X_n)$ 为整系数多项式，对固定的整数 p，则 $F(X_1,\cdots,X_n)=0$ 有 p-进整数解当且仅当对任意的 $\nu\ge 1$，同余方程

$$F(X_1,\cdots,X_n)\equiv 0\mod p^\nu$$

都有解.

目前 $\mathbb{Z}_p$ 与 $\mathbb{Q}_p$ 还只是形式地定义出来，实际上我们可以给其赋予拓扑，拓扑是由其上绝对值生成的，在 $\mathbb{Q}$ 上我们有通常的绝对值 $|\cdot|$，将其记为 $|\cdot|_\infty$，此外还有很多 p-进绝对值，即考虑

$$|x|_p := p^{-\nu_p(x)}$$

容易验证这是一个绝对值，且满足强三角不等式

$$|a+b|_p \leq \max\{|a|_p, |b|_p\}$$

如用 Cauchy 列的方式定义收敛，我们可以发现 $\mathbb{Q}_p$ 正是 $\mathbb{Q}$ 在 $|\cdot|_p$ 下的完备化，而在这个意义下，p-进整数

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \colon |x|_p \leq 1\}$$

为 $\mathbb{Q}_p$ 中的单位圆盘，其单位

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \colon |x|_p = 1\}$$

为单位圆周上的元素，从而我们可见

$$\mathbb{Q}_p^\times = \mathbb{Z} \times \mathbb{Z}_p^\times$$

并且 $\mathbb{Z}_p$ 的非零理想都是主理想，形如 $p^n\mathbb{Z}_p$，并且有同构

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$$

我们还有一个典范同构

$$\mathbb{Z}_p \cong \mathbb{Z}[[X]]/(X-p)$$

3.7 赋值与完备化

本节对上面的 p-进某某进行一般化，但是脑中需时刻保有 $\mathbb{Q}_p$ 的例子，事实上一切命题都可以从 $\mathbb{Q}_p$ 情况理解，故证明反而是多余的. 本节中多技术性命题，以 $\mathbb{Q}_p$ 的情况理解即可，无需花费时间证明.

定义 3.7.1: 赋值

域 K 上的一个**赋值**为函数

$$|\cdot| \colon K \to \mathbb{R}$$

满足 *(1)* 正定性：$|x| \geq 0$，并且取等当且仅当 $x=0$，*(2)* 乘性：$|xy| = |x||y|$，*(3)* 三角不等式：存在 $a>0$ 使得 $|x+y|^a \leq |x|^a + |y|^a$.

绝对值给出 K 上的度量从而可以诱导拓扑，我们乘两个赋值是等价的，如果他们诱导的拓扑是相同的.

命题 3.7.1

K 上的两个赋值 $|\cdot|_1$ 与 $|\cdot|_2$ 等价当且仅当存在实数 $s>0$ 使得

$$|\cdot|_1 = |\cdot|_2^s$$

于是我们可见如果你想说明两个赋值不是等价的，只需要找到一个 x 使得

$$|x|_1 < 1 \quad \text{and} \quad |x|_2 \geq 1$$

事实上我们可以看到在不同等价类里面的赋值具有某种独立性，逼近定理阐述了这一点

定理 3.7.1: 逼近定理

令 $|\cdot|_1, \cdots, |\cdot|_n$ 为互不等价的赋值，则任给 $a_1, \cdots, a_n \in K$，对任意的 $\varepsilon > 0$，存在 $x \in K$ 使得

$$|x - a_i|_i \leq \varepsilon, \forall i = 1, 2, \cdots, n$$

我们称赋值 $|\cdot|$ 是非阿基米德赋值，如果 $\{|n| : n \in \mathbb{N}\}$ 是有界的，反之则称为阿基米德赋值. 之前所见的 $\mathbb{Q}$ 上的 p-进赋值就是非阿基米德赋值，我们知道 p-进赋值是满足强三角不等式的，而事实上强三角不等式也刻画了非阿基米德赋值：

命题 3.7.2: 非阿赋值

赋值 $|\cdot|$ 非阿当且仅当满足强三角不等式 $|x+y| \leq \max\{|x|, |y|\}$.

强三角不等式下我们可以看到如果 $|x| > |y|$，则有

$$|x| = |x + y - y| \leq \max\{|x + y|, |y|\} \leq |x|$$

从而可以看出

$$|x + y| = |x|$$

于是在非阿赋值的情况下我们可以对 $f(t) \in K[t]$ 定义绝对值，若

$$f = a_0 + a_1 t + \cdots + a_n t^n$$

定义

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

可见

$$|f + g| \leq \max\{|f|, |g|\}, \quad |fg| = |f||g|$$

我们可以如此将绝对值延拓到 $K(t)$ 上为

$$\left|\frac{f}{g}\right| := \frac{|f|}{|g|}$$

现在我们可以对 $\mathbb{Q}$ 上的赋值进行一个刻画:

命题 3.7.3: $\mathbb{Q}$ 上赋值

设 $|\cdot|$ 是 $\mathbb{Q}$ 上赋值，则要么等价于某个素数 p 的 p-进赋值 $|\cdot|_p$，要么等价于无穷赋值 $|\cdot|_\infty$.

令 $|\cdot|$ 为 K 上的一个赋值，我们可以定义

$$v(x) = -\log|x|, \forall x \neq 0$$

并规定 $v(0) = \infty$，于是我们得到一个函数

$$v\colon K \to \mathbb{R} \cup \{\infty\}$$

满足 (1) 正定性：$v(x) = \infty \iff x = 0$，(2) 加性：$v(xy) = v(x) + v(y)$，(3) 强三角不等式：$v(x+y) \geq| \{v(x), v(y)\}$.

我们将 K 上满足如上性质的函数称为**指数赋值**，由赋值的情况可见两个指数赋值等价当且仅当 $v_1 = sv_2$. 为了与指数赋值区分，我们将之前所定义的赋值称为**乘法赋值**或者**绝对值**. 于是在指数赋值下我们可以考虑其赋值环.

命题 3.7.4: 赋值环

K 的子集

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\} = \{x \in K\colon |x| \leq 1\}$$

为一个局部整闭整环，其单位为

$$\mathcal{O}^\times = \{x \in K \mid v(x) = 0\} = \{x \in K\colon |x| = 1\}$$

其唯一的极大理想为

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

赋值环的理论不再赘述，我们将 $\mathcal{O}/\mathfrak{p}$ 称为其**剩余域**，如果指数赋值 v 的值域是离散的，即

$$v(K^\times) = s\mathbb{Z}, \exists s \in \mathbb{R}^+$$

则称其为**离散赋值**，称其为**规范**的，如果 $s = 1$，任何一个离散赋值都可以等价地规范化. 我们称满足 $v(\pi) = 1$ 的 $\mathcal{O}$ 中的元素为**素元(prime element)**或者是 **uniformizer**，从而对任意的 $x \in K^\times$，都存在某个 $u \in \mathcal{O}^\times$ 与整数 m 使得

$$x = u\pi^m$$

我们将离散赋值(不妨设为规范的)的赋值环，即那些指数赋值非负的元素构成的环 $\mathcal{O}$，称为**离散赋值环**，简称为 DVR，我们熟知 DVR 是 PID，并且是局部环，$\mathcal{O}$ 的所有理想被刻画为

$$\mathfrak{p} \supset \mathfrak{p}^2 \supset \cdots \supset \mathfrak{p}^n \supset \cdots$$

这构成了 0 处的一组邻域基，并且容易看见

$$\mathfrak{p}^n = \pi^n \mathcal{O}, \quad \mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathcal{O}/\mathfrak{p} = \kappa(\mathfrak{p})$$

而对于乘法拓扑群 $K^\times$ 在幺元 1 处的一组邻域基可以如下刻画

$$\mathcal{O}^\times = U^{(0)} \supset U^{(1)} \supset U^{(2)} \supset \cdots$$

其中若素元 π 使得 $|\pi^n| = q^{-n}$，则

$$U^{(n)} = 1 + \mathfrak{p}^n = \left\{ x \in K^\times : |1 - x| \leq \frac{1}{q^{n-1}} \right\}$$

$n \geq 2$ 时称为高阶单位群，而 $n = 1$ 时称为主单位. 类似于加法情况，我们有

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

将其想象成 $\mathbb{Q}_p$ 的情况就非常容易记忆，因为我们很容易看出

$$(\mathbb{Z}_p)^\times/(1 + p^n\mathbb{Z}_p) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times, \quad p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \cong \mathbb{Z}_p/p\mathbb{Z}_p$$

那既然赋值就有度量，那有度量就可以完备化，设 (K, v) 是一个赋值域，将其完备化记为 $\widehat{K}$，我们可以自然地将其 v 延拓到 $\widehat{K}$ 上，即

$$|a| := \lim_{n\to\infty} |a_n|, \quad \hat{v}(a) = -\log|a|$$

若 v 还是非阿的，则我们可以说

$$\hat{v}(a) := \lim_{n\to\infty} v(a_n)$$

这是最终常值的，原因在于若

$$|a - a_n| \to 0 \iff \hat{v}(a - a_n) \to \infty$$

则当 n 充分大的时候，$\hat{v}(a - a_n) > v(a_n)$，由强三角不等式可知

$$v(a_n) = \hat{v}(a_n - a + a) = \min\{a_n \hat{-} a, \hat{v}(a)\} = \hat{v}(a)$$

于是可见延拓之后的指数赋值的值域与之前相同，即 $\hat{v}(\widehat{K}^\times) = v(K^\times)$，可见离散赋值的延拓还是离散赋值，从而 DVR 的结构得以保持.

阿基米德的赋值情况较为简单，我们有如下定理：

定理 3.7.2: Ostrowski

K 是一个阿基米德完备域，赋值为 $|\cdot|$，则存在一个从 K 到 $\mathbb{R}$ 或者 $\mathbb{C}$ 的同构 σ 使得存在 $s \in (0, 1]$ 满足

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

后者是欧式空间的通常绝对值. 换言之，阿基米德完备域在同构意义下只有 $\mathbb{R}$ 和 $\mathbb{C}$.

既然阿基米德的情况已经了然于胸了，我们下面就专注于非阿的情况.

命题 3.7.5

$\mathcal{O} \subset K$ 与 $\widehat{\mathcal{O}} \subset \widehat{K}$ 为非阿赋值域及其完备化的赋值环，$\mathfrak{p}$ 与 $\widehat{\mathfrak{p}}$ 为对应的极大理想，则我们有

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$$

若赋值还是离散的，则

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n, \quad \forall n \geq 1$$

本质上和

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$$

一个道理.

命题 3.7.6

现在我们如果令 $R \subset \mathcal{O}$ 为 $\kappa = \mathcal{O}/\mathfrak{p}$ 的一个代表元系，使得 $0 \in R$，$\pi \in \mathcal{O}$ 为一个素元，可以证明对任意的非零元素 $x \in \widehat{K}^\times$ 存在一个唯一的分解

$$x = \pi^m(a_0 + a_1\pi + a_2\pi^2 + \cdots)$$

其中 $a_i \in R$，$a_0 \neq 0$，$m \in \mathbb{Z}$.

在 $\mathbb{Q}_p$ 中对应的情况即

$$x = p^m(a_0 + a_1 p + \cdots +)$$

因为这种情况下剩余域的代表元系即 $\{0, 1, \cdots, p-1\}$.

别忘记我们一直有拓扑结构，所以实际上我们有：

命题 3.7.7

$\mathcal{O}$ 是完备离散赋值域 K 的赋值环，则典范映射

$$\mathcal{O} \to \varprojlim_n \mathcal{O}/\mathfrak{p}^n$$

是代数同构拓扑同胚，典范映射

$$\mathcal{O}^\times \to \varprojlim_n \mathcal{O}^\times/U^{(n)}$$

也是代数同构拓扑同胚.

现在令 K 是一个完备的非阿赋值域，令 $\mathcal{O}$ 为其赋值环，极大理想为 $\mathfrak{p}$，剩余域为 $\kappa = \mathcal{O}/\mathfrak{p}$. 我们称一个多项式 $f(x) \in \mathcal{O}[x]$ 是本原的，如果 $f(x) \neq 0 \mod \mathfrak{p}$，即

$$|f| = \max\{|a_0|, \cdots, |a_n|\} = 1$$

在解方程这一块，Hensel 引理扮演了一个极其重要的角色.

定理 3.7.3: Hensel's Lemma

$f(x) \in \mathcal{O}[x]$ 为本原多项式，若

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

其中 $\overline{g(x)}, \overline{h(x)} \in \kappa[x]$ 是互素的，则 $f(x)$ 可以被分解为

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

其中 $g, h \in \mathcal{O}[x]$ 使得 $\deg(g) = \deg(\overline{g})$ 并且

$$g(x) \equiv \overline{g}(x) \mod \mathfrak{p}, \quad h(x) \equiv \overline{h}(x) \mod \mathfrak{p}$$

Remark 3.7.1

注意并没有 $\deg(h) = \deg(\overline{h})$，因为模 p 约化可能会使得 f 的次数降低，我们只能保证一个因子的次数.

Hensel 引理允许我们把 $\mathbb{Z}/p\mathbb{Z}$ 中的解提升为 $\mathbb{Z}_p$ 解，我们给出初等数论里面学过的 Hensel 引理版本:

推论 3.7.1: 根的提升版本Hensel引理

令 $f(x) \in \mathbb{Z}[x] \subset \mathbb{Z}_p[x]$，若存在 a_0 使得

$$f(a_0) \equiv 0 \mid p, \quad f'(a_0) \not\equiv 0 \mod p$$

则 a_0 可以提升为 p-进整数根，或者说可以逐步提升到模 p^n 的根，对任意的 n 成立.

证明: 只需要看到

$$f(x) \equiv (x - a_0)h(x) \mod p$$

而由于 $f'(a_0) \neq 0$，所以 $h(a_0) \neq 0$，故 $x - a_0$ 和 $h(x)$ 在 $(\mathbb{Z}/p\mathbb{Z})[x]$ 中互素，从而由 Hensel 引理知道可以提升到 $\mathbb{Z}_p$ 中. □

我们可以看到 $x^{p-1} - 1$ 在 $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ 中分裂，从而重复使用 Hensel 引理可以知道他在 $\mathbb{Z}_p$ 上也分裂，所以我们知道 $\mathbb{Q}_p$ 中有所有的 $p-1$ 次单位根.

推论 3.7.2

令 K 为非阿完备赋值域，则不可约多项式 $f(x)=a_0+a_1x+\cdots+a_nx^n\in K[x]$ 使得 $a_na_0\neq 0$，则有

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

特别地，$a_n=1$ 且 $a_0\in\mathcal{O}$ 能推出 $f\in\mathcal{O}[x]$.

这个推论告诉我们不可约多项式的绝对值由首项系数和常数项所决定，这大大简化了之前需要每一项系数的公式.

证明: 我们对 f 乘上一个合适的 K 中元素，可以不妨设 $f\in\mathcal{O}[x]$ 并且 $|f|=1$，令 a_r 为第一个使得 $|a_r|=1$ 的系数，则我们有

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

若 $\max\{|a_0|,|a_n|\}<1$，则 $0<r<n$，这告诉我们 $f(x)$ 在 $(\mathcal{O}/\mathfrak{p})[x]$ 中可约，由 Hensel 引理知道 f 可约，矛盾. □

由这个推论我们可以得到：

定理 3.7.4

令 K 为一个完备域，有赋值 $|\cdot|$，则对于一个代数扩张 $L|K$，赋值可以唯一地延拓到 L 上. 当 $[L:K]=n$ 为有限扩张时，延拓由下式给出

$$|\alpha|=\sqrt[n]{|N_{L/K}(\alpha)|},\quad\forall\alpha\in L$$

实际上 K 上的指数赋值也可以直接得到了，$[L:K]=n$ 时，延拓 w 由下式给出

$$w(\alpha)=\frac{v(N_{L|K}(\alpha))}{n}$$

下面的命题告诉我们有限维赋范 K-线性空间在拓扑意义上就是 K^n.

命题 3.7.8

K 为完备赋值域，$|\cdot|$ 为赋值，V 是一个 n 维的赋范 K-线性空间，则对任意的基 $v_1,\cdots,v_n$，定义其极大范数

$$||x_1v_1+\cdots+x_nv_n||=\max\{|x_1|,\cdots,|x_n|\}$$

与 V 上原本的范数等价，特别地，V 是完备的，并且同构

$$K^n\to V,\quad(x_1,\cdots,x_n)\mapsto x_1v_1+\cdots+x_nv_n$$

是一个同胚.

3.8 局部域

当我们说一个域是**整体域**，那我们大概是指 $\mathbb{Q}$ 或者 $\mathbb{F}_p(t)$ 的有限扩张，他们的非阿赋值是离散的并且有有限的剩余域. 当我们说**局部域**时，我们指一个带有离散赋值的完备域 K，并且其剩余域是有限域. 对于局部域，若其上的规范指数赋值记为 $v_{\mathfrak{p}}$，令 $|\cdot|_{\mathfrak{p}}$ 表示其上的绝对值，则有

$$|x|_{\mathfrak{p}} = q^{-v_{\mathfrak{p}}(x)}$$

其中 $q = \#\kappa$，为剩余域的大小. 有时我们也把阿基米德局部域 $\mathbb{R}$ 与 $\mathbb{C}$ 称为局部域.

事实上，我们可以说明局部域来自于整体域的离散赋值完备化.

定理 3.8.1: 局部域的刻画

非阿基米德局部域就是 $\mathbb{Q}_p$ 和 $\mathbb{F}_p((t))$ 的有限扩张，阿基米德局部域只有 $\mathbb{R}$ 与 $\mathbb{C}$.

下面提到**局部域若不强调则默认非阿**，局部域有很好的拓扑性质，允许在其上做一些分析：

命题 3.8.1

局部域是局部紧的，局部域的赋值环是紧的.

证明: 只需要考虑

$$\mathcal{O} = \varprojlim \mathcal{O}/\mathfrak{p}^n$$

后者是紧集(有限自然紧)直积的闭子集，从而是紧的，而 $a + \mathcal{O}$ 是任意点 $a \in K$ 的一个紧邻域. □

我们可以说明一个域 K，如果是局部紧的，并且非离散拓扑，那就同构于

$$\mathbb{R}, \mathbb{C}, K/\mathbb{Q}_p, L/\mathbb{F}_p((t))$$

中的一个，其中 $K/\mathbb{Q}_p$ 与 $L/\mathbb{F}_p((t))$ 都是有限扩张，即非离散局部紧拓扑域一定同构于某一个局部域(阿基米德或者非阿基米德). 大概理解为局部紧给我紧和有限性，非离散保证不是平凡拓扑，域结构迫使拓扑来自绝对值，非阿局部紧进一步迫使赋值离散，剩余域有限.

可见特征 p 的局部域形如 $\mathbb{F}_q((t))$，其中 $q = p^f$. 特征 0 的局部域就是 $\mathbb{Q}_p$ 的有限扩张，称为 $\mathfrak{p}$-进数域.

命题 3.8.2

局部域 K 的乘法群有分解

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

其中 π 是一个素元，$q = \#\kappa$ 为剩余域的大小，$U^{(1)} = 1 + \mathfrak{p}$ 为主单位群.

在心中持有例子

$$\mathbb{Q}_p^\times = (p) \times \{1, 2, \cdots, p-1\} \times (1 + p\mathbb{Z}_p)$$

立即可见此命题. 我们还可以在 $K^\times$ 上定义全局对数如下：

命题 3.8.3: 对数

对 $\mathfrak{p}$-进数域 K，存在唯一的连续群同态

$$\log\colon K^\times \to K$$

使得 $\log p = 0$，并且在主单位 $1+x \in U^{(1)}$ 上由下式给出

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdot$$

虽然对数是全局存在的，但是逆不一定，不过小范围内总是有的.

命题 3.8.4: 指数

令 $K|\mathbb{Q}_p$ 为一个 $\mathfrak{p}$-进数域，赋值环为 $\mathcal{O}$，极大理想为 $\mathfrak{p}$，令 $p\mathcal{O} = \mathfrak{p}^e$，则幂级数

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots, \quad \log(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots$$

在 $n > e/(p-1)$ 时给出了代数同构与拓扑同胚

$$\mathfrak{p}^n \underset{\log}{\overset{\exp}{\rightleftarrows}} U^{(n)}$$

下面我们要说明对局部域 K 而言，$U^{(1)}$ 可以自然地看成一个 $\mathbb{Z}_p$-模，其中 $p = \mathrm{char}(\kappa)$. 对 $1+x \in U^{(1)}$ 与任意的 $z \in \mathbb{Z}_p$，我们注意到 $U^{(1)}/U^{(n+1)}$ 的阶为 q^n，其中 $q = \#\mathcal{O}/\mathfrak{p} = p^f$，从而自然成为一个 $\mathbb{Z}/q^n\mathbb{Z}$ 模.

$$U^{(1)} = \varprojlim U^{(1)}/U^{(n+1)}, \quad \mathbb{Z}_p = \varprojlim \mathbb{Z}/q^n\mathbb{Z}$$

于是我们可以通过逆像极限来把 $\mathbb{Z}$-模延拓到 $\mathbb{Z}_p$-模，对任意的 $[m] \in \mathbb{Z}/q^n\mathbb{Z}$，可见任意的 $a \in U^{(1)}/U^{(n+1)}$ 有

$$[m] \cdot a := a^m$$

会发现这不依赖代表元的选取，因为 $a^{q^n} = 1$. 于是由于 $U^{(1)}/U^{(n+1)}$ 是 $\mathbb{Z}/q^n\mathbb{Z}$ 模，所以逆向极限之下有 $U^{(1)}$ 是 $\mathbb{Z}_p$ 模，可以考虑为

$$u^z = (u \mod U^{(n+1)})_n^{z \mod q^n} \in \varprojlim U^{(1)}/U^{(n+1)} \subset \prod U^{(1)}/U^{(n+1)}$$

而在这个意义下，函数

$$f(z) = (1+x)^z$$

是连续的，这是因为若 z 与 z' 足够近，则对充分大的 n 有 $z \equiv z' \mod q^n\mathbb{Z}_p$，则 $(1+x)^z \equiv (1+x)^{z'} \mod U^{(n+1)}$，于是可见连续，所以若 $\mathbb{Z} \ni z_n \equiv z \mod q^n\mathbb{Z}_p$，则有

$$(1+x)^z = \lim_{n\to\infty} (1+x)^{z_n}$$

由于局部域是局部紧的，其乘法群是的 0 的开子群，所以乘法群也是局部紧的拓扑群. 根据以上讨论，我们可以刻画局部域的局部紧乘法子群 $K^\times$.

命题 3.8.5

令 K 为一个局部域，$q = p^f$ 为剩余域的元素个数，则

(1) 若 K 特征 0，则有代数同构拓扑同胚：

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

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

(2) 若 K 特征 p，则有代数同构拓扑同胚：

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

回忆我们在前面(命题 3.8.2)就已经说明

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

所以问题归结到讨论 $U^{(1)}$ 的结构. 对于特征 0 的情况而言，当 n 充分大的时候有

$$\log\colon U^{(n)} \to \mathfrak{p}^n = \pi^n\mathcal{O} \cong \mathcal{O}$$

为代数同构拓扑同胚，而 $\mathcal{O}$ 是秩 $d = [K : \mathbb{Q}_p]$ 的自由 $\mathbb{Z}_p$ 模，所以

$$U^{(n)} \cong \mathbb{Z}_p^d$$

而 $(U^{(1)} : U^{(n)}) = p^a$ 是有限的，从而由 PID 上有限生成模的结构定理知道

$$U^{(1)} \cong \frac{\mathbb{Z}}{p^a\mathbb{Z}} \oplus \mathbb{Z}_p^d$$

其中 $\mathbb{Z}/p^a\mathbb{Z}$ 的部分表示 K 中的 p-幂次单位根群. 特征 p 的情况略去不表. 命题本质上在表明主单位群的结构，对于特征 0 时，有如上结构，告诉我们是有限秩自由群，而对于特征 p 的情况，有

$$U^{(1)} \cong \mathbb{Z}_p^{\mathbb{Z}}$$

为可数秩自由群.

推论 3.8.1

若自然数 n 在 K 上可逆，则有

$$(K^\times : (K^\times)^n) = n(U : U^n) = \frac{n}{|n|_{\mathfrak{p}}} \#\mu_n(K)$$

其中 U 是单位群.

证明: 注意到 $K^\times = (\pi) \times U$，由上面命题看到

$$U \cong \mu(K) \times \mathbb{Z}_p^d \quad \text{resp.} \quad U \cong \mu(K) \times \mathbb{Z}_p^{\mathbb{N}}$$

有正合列

$$1 \to \mu_n(K) \to \mu(K) \xrightarrow{n} \mu(K) \to \mu(K)/\mu(K)^n \to 1$$

可见

$$\#\mu_n(K) = \#\frac{\mu(K)}{\mu(K)^n}$$

当 K 特征 0，可见

$$(U : U^n) = \#\mu_n(K)\#\left(\frac{\mathbb{Z}_p}{n\mathbb{Z}_p}\right)^d = \#\mu_n(K)p^{dv_p(n)} = \frac{\#\mu_n(K)}{|n|_{\mathfrak{p}}}$$

而特征 p 时，有

$$(U : U^{(n)}) = \#\mu_n(K) = \#\mu_n(K)/|n|_{\mathfrak{p}}$$

因为 $(n, p) = 1$，所以 $|n|_{\mathfrak{p}} = 1$. □

3.9 Henselian 域

很多关于完备非阿基米德赋值域的代数性质，其实并不真正依赖完备性，而只依赖于 Hensel 引理. 我们将要在本节说明 Hensel 性等价于赋值对任意代数扩张唯一延拓.

设 (K, v) 是一个非阿赋值域，$\widehat{K}$ 是其完备化，$\hat{v}$ 是到 $\widehat{K}$ 的延拓，$\mathcal{O}$ 与 $\widehat{\mathcal{O}}$ 分别为其赋值环，取 K 在 $\widehat{K}$ 中的可分闭包 K_v，记其赋值环为 $\mathcal{O}_v$，极大理想为 $\mathfrak{p}_v$，有包含关系

$$K \subset K_v \subset \widehat{K}, \quad \mathcal{O} \subset \mathcal{O}_v \subset \widehat{\mathcal{O}}$$

虽然 K_v 一般不完备，但是可以说明 Hensel 引理在其上成立，当 K 特征 0 的时候尤其容易说明，大致原因在于

$$\mathcal{O}/\mathfrak{p} = \mathcal{O}_v/\mathfrak{p}_v = \widehat{\mathcal{O}}/\widehat{\mathfrak{p}}$$

若 $f \in \mathcal{O}_v[x] \subset \widehat{\mathcal{O}}[x]$ 在剩余域(由于全部相等，故无需特指)上分裂为两个互素的因子乘积

$$\overline{f}(x) = \overline{g}(x)\overline{h}(x)$$

由 Hensel 引理我们知道可以提升为 $\widehat{\mathcal{O}}$ 上的分解

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

其中 $g \equiv \overline{g} \mod \widehat{\mathfrak{p}}, h \equiv \overline{h} \mod \widehat{\mathfrak{p}}$，并且 $\deg(g) = \deg(\overline{g})$. 一旦把 g 的最高次数选在 $\mathcal{O}_v^\times$ 中，结合 f 的系数都在 $\mathcal{O}_v$ 中，立刻可以推出 g, h 的所有系数都在 K 上代数，而 K 特征 0，可分闭包就是代数闭包，从而所有系数都在 K_v 中，而系数都在 $\widehat{\mathcal{O}}$ 中，结合

$$K_v \cap \widehat{\mathcal{O}} = \mathcal{O}_v$$

立刻可见 Hensel 引理在 $\mathcal{O}_v$ 上成立. 于是我们可以说服自己非特征 0 的时候也成立.

我们称如上得到的赋值环 K_v 为域 K 相对赋值 v 的 **henselization**. 他保留了完备化重要的代数性质，并且是 K 的代数扩张，不依赖拓扑意义上的完备化，这比完备化更适合处理赋值与代数扩张的问题.

定义 3.9.1: Henselian Field

一个 ***Henselian* 域**是一个域附带其上的非阿基米德赋值，使得其赋值环满足 *Hensel* 引理. 我们有时也称其赋值环 *henselian*.

定理 3.9.1: Henselian 域允许赋值对代数扩张唯一延拓

设 K 是一个 *henselian* 域，带有赋值 $|\cdot|$，则对代数扩张 L/K，存在唯一的到 L 上的赋值延拓. 若 $[L:K]=n$ 为有限扩张，则延拓由

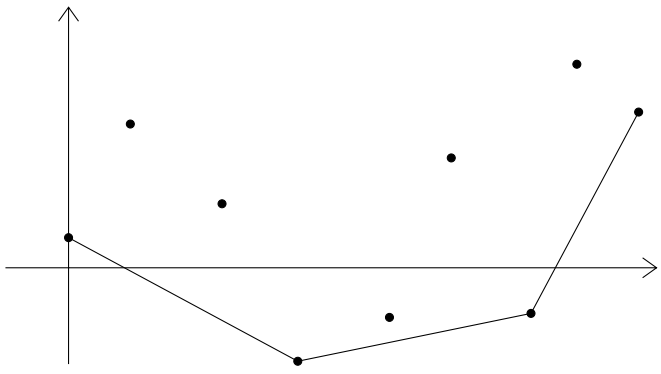
$$|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$$

给出. 对任意的代数扩张，延拓赋值的赋值环都是 K 的赋值环在 L 中的整闭包.

这表明 Hensel 性质已经足以替代完备性来控制代数扩张中的赋值结构，定理的逆命题也是正确的，为了看到这一点，我们需要引牛顿折线法. 令 v 为 K 上的指数赋值，令

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$$

满足 $a_0 a_n \neq 0$. 对第 i 项考虑点 $(i, v(a_i)) \in \mathbb{R}^2$，然后取这 $n+1$ 个点的下凸包，会得到一条折线，称其为**牛顿折线**.



这样的折线由一系列线段组成，我们按顺序将其记为 $S_1, S_2, \cdots$，这些线段的斜率很显然是递增的，我们有如下的结论：

命题 3.9.1: 牛顿折线决定根的赋值结构

令 $f(x)=a_0+a_1x+\cdots+a_nx^n\in K[x]$ 满足 $a_0a_n\neq 0$，v 为 K 上的赋值，w 为 f 的分裂域 L 上的延拓赋值，若 $(r,v(a_r))$ 到 $(s,v(a_s))$ 为某段牛顿折线，将其斜率记为 $-m$，则 f 恰有 $s-r$ 个根 $\alpha_1,\cdots,\alpha_{s-r}$ 使得

$$w(\alpha_1)=\cdots=w(\alpha_{s-r})=m$$

证明是纯粹的初等数学，把根的赋值按赋值大小排列分组就可以立刻得到. 牛顿折线可以把多项式分解成若干同赋值块，设牛顿的折线斜率为

$$-m_r<\cdots<-m_1$$

则

$$f(x)=a_n\prod_{j=1}^{r}f_j(x),\quad f_j(x)=\prod_{w(\alpha_i)=m_j}(x-\alpha_i)$$

因子 f_j 对应着斜率为 $-m_j$ 的那一段牛顿折线.

命题 3.9.2

L 是 f 的分裂域，若赋值 v 允许唯一的赋值 w 延拓在 L 上，则分解

$$f(x)=a_n\prod_{j=1}^{r}f_j(x)$$

是 $K[x]$ 中的分解，即 $f_j(x)\in K[x]$.

道理很简单，本质上依赖延拓的唯一性，考虑 $\sigma\in\mathrm{Gal}(L|K)$，若 w 是延拓，则 $w\circ\sigma$ 也是延拓，所以可见对任意 x，都有

$$w(x)=w(\sigma(x))$$

于是如果 f 不可约，则牛顿折线只有一段，对不可约情况的次数归纳即可.

推论 3.9.1

令 $f(x)=a_0+a_1x+\cdots+a_nx^n\in K[x]$ 不可约，满足 $a_n\neq 0$，若赋值在分裂域中唯一延拓，则有

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

证明: 由于下凸包只有一条线，所以所有系数的赋值都必然大于

$$|\{v(a_0),v(a_n)\}$$

得证. □

我们之前利用 Hensel 引理得到过类似的结论(推论 3.7.2)，并籍此证明了赋值的唯一延拓，现在我们利用赋值唯一延拓的性质也得到了这个结论，从而可以说明赋值唯一延拓足以推出 Hensel 引理，从而可以说明为 Henselian 域.

定理 3.9.2: Henselian 域与赋值的唯一延拓

非阿基米德赋值域 $(K,|\cdot|)$ 是 *henselian* 域当且仅当赋值可以唯一延拓到任意代数扩张上.

我们还可以把情况归结到首一多项式的情况.

命题 3.9.3

一个非阿基米德赋值域 (K,v) 是 *henselian* 域，如果任意的首一多项式 $f(x)\in\mathcal{O}[x]$ 在其剩余域 $\kappa=\mathcal{O}/\mathfrak{p}$ 中分裂为互素的因子

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

则 $f(x)$ 可以被分解为

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

其中 $g,h\in\mathcal{O}[x]$ 为首一多项式使得

$$g(x)\equiv\overline{g}(x)\mod\mathfrak{p},\quad h(x)\equiv\overline{h}(x)\mod\mathfrak{p}$$

现在假设 K 是 henselian 域，有指数赋值 v，L/K 为 n 次代数扩张，则 v 可以唯一延拓到 L 上，由

$$w(\alpha)=\frac{v(N_{L/K}(\alpha))}{n}$$

给出，令 λ 为 L 的剩余域 $\mathcal{O}_L/\mathfrak{P}$，则我们有

$$v(K^\times)\subset w(L^\times),\quad \kappa\subset\lambda$$

其分歧指数为：

$$e=e(w|v):=\big(w(L^\times):v(K^\times)\big)$$

其惯性次数为：

$$f=f(w|v):=[\lambda:\kappa]$$

若 v 是离散赋值，则 w 自然也是，$\mathcal{O},\mathfrak{p},\pi$ 与 $\mathcal{O}_L,\mathfrak{P},\Pi$ 分别为 K 和 L 的赋值环，极大理想与素元，则我们有

$$e=(w(\Pi)\mathbb{Z}:v(\pi)\mathbb{Z})$$

因此可见 $v(\pi)=ew(\Pi)$，于是可见

$$\pi=\varepsilon\Pi^e,\exists\varepsilon\in\mathcal{O}_L^\times$$

因此可见这与我们之前所定义的分歧指数是相容的，因为

$$\mathfrak{p}\mathcal{O}_L=\mathfrak{P}^e$$

命题 3.9.4: 赋值域的基本等式

定义符号乘上，则有 $[L:K] \geq ef$，并且当 v 是离散赋值且 $L|K$ 是可分扩张时，有

$$[L:K] = ef$$

事实上，若 K 的离散赋值是完备的，则即便 L/K 不是可分扩张，也仍然有 $[L:K] = ef$.

3.10 非分歧扩张与驯分歧扩张

本节中我们令 K 是一个 henselian 域，带有非阿基米德赋值 v，对应的乘法赋值为 $|\cdot|$，记其赋值环，极大理想与剩余域为 $\mathcal{O}_K, \mathfrak{p}, \kappa$. L/K 是一个代数扩张，则对应的为 $\mathcal{O}_L, \mathfrak{P}, \lambda$.

定义 3.10.1: 非分歧

有限扩张 $L|K$ 称为**非分歧**的，如果扩张 λ/κ 是可分扩张并且 $[L:K] = [\lambda:\kappa]$. 代数扩张 $L|K$ 称为**非分歧**，如果为有限非分歧子扩张的并.

命题 3.10.1: 非分歧对基变换与子扩张稳定

令 $L|K$ 与 $K'|K$ 为在同一个代数闭包 $\overline{K}$ 中的扩张，令 $L' = LK'$，则有

$$L|K \ \ unramified \implies L'|K' \ \ unramified$$

每个非分歧扩张的子扩张都是非分歧的.

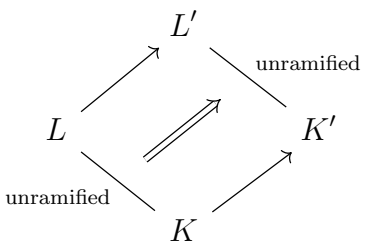
证明: 道理在于可以假设为有限扩张，此时 λ/κ 可分，从而存在本原元使得 $\lambda = \kappa(\overline{\alpha})$，将其提升到 $\alpha \in \mathcal{O}_L$，观察在 K 上的极小多项式 $f(x)$，将其模 $\mathfrak{p}$ 约化为 $\overline{f}(x)$. 通过比较次数我们观察到

$$[\lambda:\kappa] \leq \deg(\overline{f}) \leq \deg f = [K(\alpha):K] \leq [L:K]$$

由于 L/K 非分歧，所以上面全部取等，故可以得到 $L = K(\alpha)$，并且 $\overline{f}$ 正是 $\overline{\alpha}$ 在 κ 上的极小多项式，从而得到 $L' = K'(\alpha)$，令 $g(x) \in \mathcal{O}_{K'}[x]$ 为 α 在 K' 上的极小多项式，很显然 $\overline{g}(x) = g(x) \bmod \mathfrak{p}'$ 为 $\overline{f}(x)$ 在 $\kappa'[x]$ 中的一个因子，从而是可分的，并且不可约，否则由 Hensel 引理知道 g 可约. 于是我们有

$$[\lambda':\kappa'] \leq [L':K'] = \deg(g) = \deg(\overline{g}) = [\kappa'(\overline{\alpha}), \kappa'] \leq [\lambda':\kappa']$$

从而 $[L':K'] = [\lambda':\kappa']$，故非分歧.



若 $L|K$ 为非分歧扩张 $L'|K$ 的子扩张，上面结论告诉我们 $L'|L$ 为非分歧扩张，考虑

$$[\lambda' : \kappa] = [\lambda : \lambda'][\lambda' : \kappa]$$

立刻得到 $L|K$ 非分歧. □

推论 3.10.1: 非分歧扩张的合成还是非分歧的

若 $L|K$ 与 $L'|K$ 是非分歧的，则 $LL'|K$ 是非分歧的.

定义 3.10.2: 极大非分歧子扩张

令 $L|K$ 为代数扩张，则所有非分歧子扩张的合成 $T|K$ 被称为 $L|K$ 的**极大非分歧子扩张**.

命题 3.10.2

T 的剩余域为 κ 在 λ 中的可分闭包 λ_s，T 的赋值群与 K 的相同，即 $w(T^\times) = v(K^\times)$.

可见非分歧扩张的本质是在剩余域上做可分扩张，而不碰赋值群. 现在设 $\overline{K}$ 是 K 的代数闭包，K 在 $\overline{K}$ 中的极大非分歧扩张记为 K_{nr}. 其剩余域为 κ 的可分闭包 $\overline{\kappa}_s$，并且赋值群与 K 相同. 此外若 m 与 κ 的特征互素，则多项式 $x^m - 1$ 在 $\overline{\kappa}_s$ 上完全分裂并且可分，从而有 Hensel 引理知道在 K_{nr} 上分裂. 特别地，如果 κ 是有限域，那么 $\overline{\kappa}_s$ 由这些与特征互素的单位根生成，所以 K_{nr} 也由这些单位根生成.

从这里开始设 $p = \mathrm{char}(\kappa) > 0$，则我们可以定义：

定义 3.10.3: 驯分歧

代数扩张 $L|K$ 被称为**驯分歧 *(tamely ramified)***，如果剩余域的扩张 $\lambda|\kappa$ 是可分扩张，并且 $([L : T], p) = 1$. 若为无穷扩张，在互素条件变为任意 $L|T$ 的子扩张的次数与 p 互素.

驯分歧允许分歧，但是只允许与特征 p 无关的分歧. 若基本等式成立：

$$[L : K] = ef$$

并且 λ/κ 可分，那么 L/K 非分歧当且仅当 $e = 1$，而 L/K 驯分歧当且仅当 $(e, p) = 1$.

命题 3.10.3: 有限驯分歧的结构定理

有限扩张 $L|K$ 是驯分歧的当且仅当扩张 $L|T$ 由根式生成：

$$L = T(\sqrt[m_1]{a_1}, \cdots, \sqrt[m_r]{a_r})$$

使得 $(m_i, p) = 1$. 在这种情况下基本等式总是成立

$$[L : K] = ef$$

命题告诉我们有限驯分歧扩张本质上就是在极大非分歧部分上再添加若干个次数与剩余域特征互素的根式.

推论 3.10.2: 驯分歧对基变换与子扩张稳定

令 $L|K$ 与 $K'|K$ 为 $\overline{K}|K$ 的两个子扩张，$L' = LK'$，则有

$$L|K \ \ tamely\ ramified \implies L'|K' \ \ tamely\ ramified$$

每个驯分歧的子扩张也是驯分歧的.

推论 3.10.3: 驯分歧对合成稳定

驯分歧扩张的合成也是驯分歧的.

定义 3.10.4: 极大驯分歧子扩张

令 $L|K$ 为代数扩张，则所有驯分歧子扩张的合成 $V|K$ 被称为 $L|K$ 的**极大驯分歧子扩张**.

定义 $w(L^\times)^{(p)}$ 为满足下列条件的 $\omega \in w(L^\times)$ 组成的子群：存在一个整数 m，使得 $(m, p) = 1$ 且

$$m\omega \in v(K^\times)$$

换句话说，ω 在商群 $w(L^\times)/v(K^\times)$ 中的阶是与 p 互素的，因此：

$$w(L^\times)^{(p)}/v(K^\times)$$

正好是商群 $w(L^\times)/v(K^\times)$ 中所有阶与 p 互素的元素组成的部分.

命题 3.10.4: 极大驯分歧子扩张的结构定理

$L|K$ 的极大驯分歧子扩张 $V|K$ 满足其赋值群为

$$w(V^\times) = w(L^\times)^{(p)}$$

其剩余域与 κ 在 λ 中的可分闭包 λ_s 相同.

可见极大驯分歧子扩张就是在极大非分歧子扩张的基础上满足赋值群的与 p 无关条件.

$$K \hookrightarrow T \hookrightarrow V \hookrightarrow L$$

$$\kappa \hookrightarrow \lambda_s \xrightarrow{=} \lambda_s \hookrightarrow \lambda$$

$$v(K^\times) \xrightarrow{=} w(T^\times) \hookrightarrow w(L^\times)^{(p)} \hookrightarrow w(L^\times)$$

若 $L|K$ 是有限扩张，$e = e'p^a$，其中 $(e', p) = 1$，则 $[V : T] = e'$. 扩张 $L|K$ 为**完全分歧**，若 $T = K$，即 K 就是自己的极大非分歧子扩张；称 $L|K$ 为**野分歧**，如果不是驯分歧的，即 $V \neq L$.

命题 3.10.5

K 为完备的离散赋值域，其剩余域 $\kappa = \mathbb{F}_q$ 为有限域，令 $L = K(\zeta)$，ζ 为 n 次本原单位根，令 $\mathcal{O}_L|\mathcal{O}_K$ 与 $\lambda|\kappa$ 为赋值环与剩余域的扩张，设 $(n, p) = 1$，则有

(1) $L|K$ 是 f 次非分歧扩张，其中 f 为 q 模 n 的阶，$q = \#\kappa$.

(2) $\mathrm{Gal}(L|K)$ 典范同构于 $\mathrm{Gal}(\lambda|\kappa)$，其生成元为 $\xi \mapsto \xi^q$.

(3) $\mathcal{O}_L = \mathcal{O}_K[\xi]$.

命题 3.10.6

令 ζ 为 p^m-次本原单位根，则有

(1) $\mathbb{Q}_p(\zeta)|\mathbb{Q}_p$ 完全分歧，次数为 $\varphi(p^m) = p^{m-1}(p-1)$.

(2) $\mathrm{Gal}(\mathbb{Q}_p(\zeta)|\mathbb{Q}_p) \cong (\mathbb{Z}/p^m\mathbb{Z})^\times$.

(3) $\mathbb{Z}_p[\zeta]$ 为 $\mathbb{Q}_p(\zeta)$ 的赋值环.

(4) $1 - \zeta$ 为 $\mathbb{Z}_p[\zeta]$ 的素元，其范数为 p.

3.11 赋值的扩张

3.12 赋值的 Galois 理论