前　言

交换代数是研究交换环的一门代数学科，它起源于两个经典数学分支：代数几何和代数数论，作为这两门学科的公共代数工具逐步发展成一门独立的学科，成为从事数学研究所不可缺少的基础之一.

中国科学技术大学数学系多年来一直为数学系研究生和高年级本科生开设交换代数课程，作者本人也曾五次讲授该课程. 1995 年以来，该课程列为数学系研究生的公共基础课程之一. 本书是为这一公共基础课程编写的教材. 学过近世代数的读者均可学习本教材.

本书在讲述交换代数经典的 Noether 环和 Dedekind 整环理论的同时，突出模论和局部化方法. 书中关于模论的许多定理及其证明，稍加调整即可适用于非交换环上的模. 本书也介绍了范畴和函子，侧重介绍了 Hom 函子、张量积函子和局部化函子. 这些内容也是学习同调代数所必需的预备知识.

本书是按一学期 80 学时(4 学分)来安排课程内容和习题的. 通常 60 学时可以讲完全部内容，剩余学时可选讲 1～2 个专题，例如 Gröbner 基理论等.

本书是在冯克勤教授的鼓励和支持下完成的，实际上是以冯克勤教授所著《交换代数基础》为蓝本撰写的，作者在此向他表示感谢. 在教学过程中，郭学军博士和讨论班的同学们提出了许多修改意见，在此一并致谢. 作者也期望听到各方面的意见，以利于改进今后的教学工作.

宋光天

2002 年春于合肥

目 录

第 1 章　环、模和范畴的基本知识

1.1　环的理想和根

在近世代数课程中，我们已学过有关环的基本知识，如理想、商环、环同态和同态基本定理等，这些都是学习交换代数的必要基础. 本节将复述其中的一些重要概念，明确所采用的术语和记号，并介绍一些新知识.

若不加声明，本书中所说的**环**均指有单位元 1_R（常简记为 1）的交换环；**环同态** $f:R\to S$ 均保持单位元，即 $f(1_R)=1_S$；环 R 的**子环**均含有 R 的单位元 1_R.

符号 $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 分别表示自然数集、整数环、有理数域、实数域和复数域.

1.1.1　理想的运算

设 I,J 是环 R 的理想. R 的子集

$$I+J=\{a+b\mid a\in I,\ b\in J\},$$
$$I\cap J=\{a\mid a\in I\ 且\ a\in J\},$$
$$IJ=\{\sum_{i=1}^{n}a_ib_i\mid a_i\in I, b_i\in J, n\in\mathbb{N}\},$$
$$(I:J)=\{x\in R\mid xJ\subseteq I\}$$

均是 R 的理想，分别称为理想 I 与 J 的**和**、**交**、**积**、**商**. 零理想 0 与 J 的商 $(0:J)$ 叫做 J 的**零化理想**，记作 $\mathrm{Ann}_R(J)$. 主理想 aR，$a\in R$，的零化理想也称为元素 a 的**零化理想**，记作 $\mathrm{Ann}_R(a)$.

不难验证，环 R 的理想的和、交、积运算均满足交换律和结合律，且有如下的分配律：

$$I(J+K)=IJ+IK,$$

其中 I,J,K 均是R 的理想. 进而可定义理想 I 的**幂** I^n 为 n 个 I 的积，并约定 $I^0=R$.

环 R 的两个理想 I 和 J 称为是**互素**的，如果 $I+J=R$. 若环 R 的理想 $I\neq R$，则称 I 是环 R 的**真理想**.

对于环 R 的任意一个理想族 I_α，$\alpha\in A$，定义它们的**和**为

$$\sum_{\alpha\in A} I_\alpha = \left\{\sum_{\alpha\in A} x_\alpha \,|\, x_\alpha\in I_\alpha,\ \alpha\in A,\text{且只有有限个 } x_\alpha\neq 0\right\}.$$

这是环 R 中包含所有 I_α，$\alpha\in A$，的最小理想.

1.1.2 素理想和极大理想

环 R 的理想 P 称为**素理想**，如果 $P\neq R$，且满足条件：若 a，$b\in R$，且 $ab\in P$，则 $a\in P$ 或 $b\in P$. 环 R 的理想 M 称为**极大理想**，如果 $M\neq R$，且 M 与 R 之间不存在 R 的理想；即若 I 是 R 的理想，且 $M\subseteq I\subseteq R$，则 $I=M$ 或 $I=R$.

我们知道，环 R 的真理想 I 是素(极大)的，当且仅当商环 R/I 是整环(域). 于是，极大理想必是素理想.

非零环是否含有极大理想？答案是肯定的. 证明中要用到集合论中的一个基本结果，叫做 Zorn 引理，今后我们还将多次使用它.

集合 S 上的二元关系 $\leqslant$ 称为 S 上的一个**部分序**(或**偏序**)，如果对于任意 $x,y,z\in S$，均有

(1) $x\leqslant x$；

(2) 若 $x\leqslant y$，$y\leqslant x$，则 $x=y$；

(3) 若 $x\leqslant y$，$y\leqslant z$，则 $x\leqslant z$.

此时称 $(S,\leqslant)$ 为一个**部分序集**. 所谓"部分"是指，在 S 中可能有元素 x 和 y，使得 $x\leqslant y$ 和 $y\leqslant x$ 均不成立，此时称 x 与 y 是不

可比较的．如果 $x\leqslant y$ 和 $y\leqslant x$ 中至少有一个成立，则称 x 与 y 是**可比较**的．设 T 是部分序集 $(S,\leqslant)$ 的子集．如果 T 中任意两个元素可比较，则称 T 是一个**链**．S 中的元素 x 称为子集 T 的一个**上界**，如果对于每个 $t\in T$ 均有 $t\leqslant x$．T 中元素 x 称为 T 的一个**极大(小)元**，如果 T 中每个与 x 可比较的元素 y，均有 $y\leqslant x$ $(x\leqslant y)$；称 $x\in T$ 是 T 的**最大(小)元**，如果对于 T 中的每个元素 y，均有 $y\leqslant x(x\leqslant y)$．一个部分序集 $(S,\leqslant)$ 称为是**良序集**，如果 S 的每个非空子集均有最小元．注意，良序集必是一个链，反之未必．

Zorn 引理　*设 $(S,\leqslant)$ 是一个非空部分序集，若 S 中的每个链在 S 中有上界，则 S 必有极大元．*

Zorn 引理有许多等价形式，例如下面的良序化原理和超穷归纳原理，以及选择公理．

良序化原理　*对于任意集合 S 均存在 S 的一个部分序 $\leqslant$，使得 $(S,\leqslant)$ 是良序集．*

超穷归纳原理　*设 T 是良序集 $(S,\leqslant)$ 的子集，如果对于每个 $x\in S$，$\{y\in S\mid y<x\}\subseteq T$ 蕴含 $x\in T$，则 $T=S$．*

下面用 Zorn 引理证明极大理想的存在性．

定理 1.1.1　*设 I 是环 R 的真理想，则存在 R 的极大理想 M，使得 $M\supseteq I$．*

证明　设 Σ 是 R 中所有不等于 R 且包含 I 的理想构成的集合．Σ 关于理想的包含关系 $\subseteq$ 构成一个非空部分序集(因为 $I\in\Sigma$)．设 T 是 Σ 中的一个链．令 $J=\bigcup\limits_{X\in T}X$，则 J 是 R 的包含 I 的理想；且 $J\neq R$．这是因为，假定 $J=R$，则 $1\in J$，于是存在 $X\in T$ 使得 $1\in X$，从而 $X=R$，这与 $X\in T\subseteq\Sigma$ 矛盾．所以 $J\in\Sigma$．又由于对于任意 $X\in T$ 均有 $X\subseteq J$，故 J 是 T 在 Σ 中的上界．由 Zorn 引理，Σ 必有极大元 M．M 就是 R 的极大理想，且包含 I．　□

环 R 的所有素理想构成的集合称为 R 的**素谱**，记作 $\operatorname{Spec} R$；

R 的所有极大理想构成的集合称为R 的**极大谱**，记作 Max R. 于是，对于每个非零环 R，Spec $R \supseteq$ Max $R \neq \varnothing$.

命题 1.1.2 设 I 是环R 的理想，$P_1,\cdots,P_n$ 是R 的素理想. 若 $I\subseteq \bigcup\limits_{i=1}^{n} P_i$，则存在 $j\in\{1,\cdots,n\}$，使得 $I\subseteq P_j$.

证明 不妨设对于每个 $j\in\{1,\cdots,n\}$，$I\not\subseteq \bigcup\limits_{\substack{i=1\\ i\neq j}}^{n} P_i$，且 $n\geqslant 2$. 假定对于每个 j 均有 $I\not\subseteq P_j$，则对于每个 j，存在 $a_j\in I\backslash(\bigcup\limits_{\substack{i=1\\ i\neq j}}^{n} P_i)$，且 $a_j\in P_j$. 设 $a=a_1+a_2a_3\cdots a_n\in P_j$(某个 j). 若 $j>1$，则 $a_1=a-a_2a_3\cdots a_n\in P_j$，这矛盾. 若 $j=1$，则 $a_2a_3\cdots a_n=a-a_1\in P_1$，从而存在某个 $j>1$，使得 $a_j\in P_1$，这也矛盾. 所以，存在某个 j，使得$I\subseteq P_j$. □

1.1.3 素根和 Jacobson 根

一个环 R 的所有幂零元构成的集合记作 $\mathrm{Nil}(R)$.

定理 1.1.3 (Krull) 对于任意非零环 R，$\mathrm{Nil}(R)$是 R 的所有素理想的交.

证明 记 R 的所有素理想的交为N. 若 $x\in \mathrm{Nil}(R)$，则存在 $n\geqslant 1$，使得 $x^n=0\in N$. 于是对于每个素理想 P 均有 $x^n\in P$，从而$x\in P$. 所以 $\mathrm{Nil}(R)\subseteq N$.

若 $x\notin \mathrm{Nil}(R)$，记 $S=\{x^n\mid n\in\mathbb{N}\}$，则 $S\cap 0=\varnothing$. 令 $\Sigma=\{I$ 是 R 的理想$\mid S\cap I=\varnothing\}$，则 Σ 关于理想的包含关系$\subseteq$构成一个非空部分序集. 设 T 是Σ 中一个链，则 $J=\bigcup\limits_{I\in T} I$ 是R 的理想，且 $S\cap J=\varnothing$，从而 J 是T 在Σ 中的一个上界. 由 Zorn 引理，Σ 有极大元P. 下证 P 是素理想. 若 $a,b\in R\backslash P$，由 P 的极大性，存在 $m,n\in\mathbb{N}$，使得 $x^m\in aR+P$，$x^n\in bR+P$. 于是 $x^{m+n}\in(aR+P)(bR+P)\subseteq abR+P$. 这表明 $ab\notin P$. 所以 P 是素理想. 再由 $x\notin P$ 可知$x\notin N$.

所以，$\mathrm{Nil}(R)=N$. □

注　零环 R 的素谱为空集，此时约定 $\mathrm{Nil}(R)=R$.

由上述定理可知，$\mathrm{Nil}(R)$是环 R 的理想，叫做 R 的**素根**(或 **Nil 根**). 当 $\mathrm{Nil}(R)=0$ 时，称 R 为**半素环**.

环 R 的所有极大理想的交称为 R 的 **Jacobson 根**，记作 $\mathrm{Rad}(R)$. 由于 $\mathrm{Spec}\,R\supseteq\mathrm{Max}\,R$，故 $\mathrm{Rad}(R)\supseteq\mathrm{Nil}(R)$. 因此，也常称 $\mathrm{Rad}(R)$为大根，而称 $\mathrm{Nil}(R)$为小根.

注　对于零环 R，约定 $\mathrm{Rad}(R)=R$.

环 R 的乘法可逆元称为 R 的**单位**，R 的所有单位构成的乘法群称为 R 的**单位群**，记作 $\mathrm{U}(R)$.

下述命题给出 $\mathrm{Rad}(R)$一个元素形式的刻画.

命题 1.1.4　对于任意非零环 R，均有

$$\mathrm{Rad}(R)=\{x\in R\mid 1-xR\subseteq \mathrm{U}(R)\}.$$

证明　记上式右边为 I. 若 $x\notin I$，则存在 $y\in R$ 使得 $1-xy\notin \mathrm{U}(R)$，据定理 1.1.1，$1-xy$ 含于 R 的某个极大理想 M 中. 假定 $x\in\mathrm{Rad}(R)$，则 $x\in M$，从而 $1=xy+(1-xy)\in M$. 这是一个矛盾. 所以 $x\notin\mathrm{Rad}(R)$. 这表明 $I\supseteq\mathrm{Rad}(R)$.

反之，若 $x\notin\mathrm{Rad}(R)$，则存在 R 的极大理想 M 使得 $x\notin M$. 于是 $xR+M=R$，故存在 $y\in R$ 和 $m\in M$，使得 $xy+m=1$. 于是 $1-xy=m\in M$，所以 $1-xy\notin\mathrm{U}(R)$，从而 $x\notin I$. 这表明 $I\subseteq\mathrm{Rad}(R)$. □

1.1.4　理想的根

设 I 是环 R 的理想. 令

$$\sqrt{I}=\{a\in R\mid 存在\ n\geqslant 1，使得\ a^n\in I\}.$$

不难验证，$\sqrt{I}$是 R 的包含 I 的理想，叫做 I 的**根**；且 R 的零理想 0 的根$\sqrt{0}=\mathrm{Nil}(R)$. 这一概念将在第 3 章中出现，它在代数几何中是基本的.

命题 1.1.5 设 $I, I_1, \cdots, I_n$ 是环 R 的理想. 则

(1) $\mathrm{Nil}(R/I)=\sqrt{I}/I$.

(2) $\sqrt{I}$是 R 的所有包含 I 的素理想之交.

(3) $\sqrt{I}=R \Leftrightarrow I=R$.

(4) $\sqrt{\sqrt{I}}=\sqrt{I}$.

(5) $\sqrt{\bigcap_{i=1}^{n} I_i}=\bigcap_{i=1}^{n}\sqrt{I_i}$.

(6) 若 $P\in \mathrm{Spec}\, R$，则对于每个正整数 n，均有$\sqrt{P^n}=P$.

证明 (1) 按定义验证.

(2) 由于 R/I 的素理想一一对应于R 的包含I 的素理想，据定理 1.1.3 和(1)，立得(2).

(3)~(6) 按定义验证. □

1.1.5 局部环和半局部环

仅有一个极大理想的非零环叫做**局部环**，仅有有限多个极大理想的非零环叫做**半局部环**. 于是，每个非零有限环均是半局部环.

若 M 是局部环R 的唯一极大理想，域 R/M 称为R 的**剩余类域**. 下述定理给出局部环的一些性质刻画.

定理 1.1.6 设 M 是环R 的理想，且 $M\neq R$，则下列条件等价：

(1) R 是局部环，且 M 是R 的唯一极大理想；

(2) $R\backslash M=\mathrm{U}(R)$；

(3) M 是R 的极大理想，且 $1+M\subseteq \mathrm{U}(R)$.

证明 (1)⇒(2)：由于 $M\neq R$，从而 $M\cap \mathrm{U}(R)=\varnothing$，于是 $R\backslash M\supseteq \mathrm{U}(R)$. 若 $x\notin \mathrm{U}(R)$，则 $xR\neq R$，于是由(1)，$xR\subseteq M$. 所以 $x\notin R\backslash M$. 这表明 $R\backslash M\subseteq \mathrm{U}(R)$.

(2)⇒(3)：若 R 的理想I 包含但不等于M，由(2)，I 必含R

的单位，从而 $I=R$，所以 M 是 R 的极大理想. 若存在 $m\in M$ 使得 $1+m\notin \mathrm{U}(R)$，由(2)，$1+m\in M$. 于是 $1\in M$，这矛盾. 所以(3)成立.

(3)⇒(1)：假定 R 有极大理想 $L\neq M$，则 $L+M=R$. 于是存在 $l\in L$，$m\in M$，使得 $l+m=1$. 由(3)，$l=1-m\in \mathrm{U}(R)$，从而 $L=R$，这是一个矛盾. □

例　设 p 是素数，则 $\mathbb{Z}/p^n\mathbb{Z}$ 是局部环.

在第 2 章 2.5 节中，将用局部化方法构造出一类局部环.

习　题　1.1

1. 设 I，J，K，$I_\alpha(\alpha\in A)$是环 R 的理想. 证明：

(1) 若 I 与 J 互素，则 $I\cap J=IJ$.

(2) $((I:J):K)=(I:JK)=((I:K):J)$.

(3) $(\bigcap_{\alpha\in A}I_\alpha:J)=\bigcap_{\alpha\in A}(I_\alpha:J)$，$(I:\sum_{\alpha\in A}I_\alpha)=\bigcap_{\alpha\in A}(I:I_\alpha)$.

(4) $\sqrt{I+J}=\sqrt{\sqrt{I}+\sqrt{J}}$，$\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}=\sqrt{IJ}$.

(5) $\sqrt{I}$ 与 $\sqrt{J}$ 互素 ⇔ I 与 J 互素.

2. (**中国剩余定理**)设 $I_1,\cdots,I_n$ 是环 R 的两两互素的理想. 证明：

(1) 对于任意 $a_1,\cdots,a_n\in R$，存在 $a\in R$，使得 $a\equiv a_i \pmod{I_i}$，$i=1,\cdots,n$.

(2) $R/(\bigcap_{i=1}^{n}I_i)\simeq\coprod_{i=1}^{n}(R/I_i)$.

3. 设 P 是环 R 的真理想. 证明：P 是 R 的素理想 ⇔ 对于 R 的任意理想 I 和 J，若 $IJ\subseteq P$，则 $I\subseteq P$ 或 $J\subseteq P$.

4. 设 P 是环 R 的素理想，I 和 J 是 R 的理想，证明：若 $P=I\cap J$，则 $P=I$ 或 $P=J$.

5. 设 R 是环. Spec R 关于包含关系的极小元叫做 R 的**极小素理想**. 试用 Zorn 引理证明：非零环必含极小素理想.

6. 证明：有限环和主理想整环中的素理想均是极大理想.

7. 试求 $\mathbb{Z}$、$\mathbb{Z}/n\mathbb{Z}$ 和域 k 上的多项式环 $k[x]$ 的素谱、极大谱、素根和 Jacobson 根.

8. 设 R 是环，证明：$\mathrm{Nil}(R/\mathrm{Nil}(R))=0$，$\mathrm{Rad}(R/\mathrm{Rad}(R))=0$.

9. 设 R 是环，若 $x\in \mathrm{Nil}(R)$，$y\in \mathrm{U}(R)$，则 $x+y\in \mathrm{U}(R)$.

10. 设 R 是环，$f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$. 证明：

(1) $f(x)\in \mathrm{U}(R[x])\Leftrightarrow a_0\in \mathrm{U}(R)$，且 $a_1,\cdots,a_n\in \mathrm{Nil}(R)$.

(2) $f(x)\in \mathrm{Nil}(R[x])\Leftrightarrow a_0,a_1,\cdots,a_n\in \mathrm{Nil}(R)$.

(3) $f(x)$ 是 $R[x]$ 中的零因子 $\Leftrightarrow$ 存在 $a\in R$，$a\neq 0$，使得 $af(x)=0$.

(4) $\mathrm{Nil}(R[x])=\mathrm{Rad}(R[x])=\mathrm{Nil}(R)[x]$.

11. 设 R 是环，$R[[x]]$ 是 R 上的形式幂级数环. $f(x)=\sum_{i=0}^{\infty}a_ix^i\in R[[x]]$. 证明：

(1) $f(x)\in \mathrm{U}(R[[x]])\Leftrightarrow a_0\in \mathrm{U}(R)$.

(2) $\mathrm{Nil}(R[[x]])\subseteq \mathrm{Nil}(R)[[x]]$. 等号是否一定成立?

(3) 若 R 是域，则 $R[[x]]$ 是局部环.

12. 设 $\mathfrak{m}$ 是环 R 的极大理想，$n\geqslant 1$. 证明：商环 $R/\mathfrak{m}^n$ 只有一个素理想，从而是局部环.

1.2 模及其基本性质

1.2.1 定义和例

非空集合 M 称为环 R 上的一个**左 R-模**，如果 M 是一个加法 Abel 群，且有 R 与 M 的元素间的乘法

$$R\times M\to M;\ (r,m)\mapsto rm,$$

满足以下条件：对于任意 $r,s\in R$；$x,y\in M$，均有

(1) $r(x+y)=rx+ry$;

(2) $(r+s)x=rx+sx$;

(3) $(rs)x=r(sx)$;

(4) $1_R x=x$.

也称 R 为模 M 的**系数环**. 对称地，可给出**右** R-**模**的定义，其系数环 R 作用在模 M 的右边. 每个左 R-模 M 都有一个自然的右 R-模结构，其系数环 R 在加群 M 上的右作用为 $xr=rx$, $r\in R$, $x\in M$. 如不加声明，本书中所说的 R-**模**均指左 R-模，其右 R-模结构均指上述自然的右作用.

若系数环 R 是域，则 R-模就是域上的线性空间.

由 R-模 M 的定义及线性代数中同样的方法，不难推导出 M 具有以下性质：对于任意 $r\in R$, $x\in M$, $n\in\mathbb{Z}$, 均有

(1) $r0_M=0_M$, $0_R x=0_M$;

(2) $(-r)x=-(rx)=r(-x)$;

(3) $n(rx)=(nr)x=r(nx)$.

为简便起见，常将加群 M 的零元 0_M、环 R 的零元 0_R 以及数零均写成 0. 只有一个元素 0 的 R-模叫做**零模**，也表示成 0.

例　(1) 设 A 为任意一个加法 Abel 群. 对于每个 $n\in\mathbb{N}$ 和 $a\in A$, 令 $na=a+a+\cdots+a$ (n 个 a), $(-n)a=-na$, 且 $0a=0$. 不难验证，关于整数环 $\mathbb{Z}$ 在 A 上的这种作用，A 构成一个 $\mathbb{Z}$-模. 所以，每个 Abel 群可自然地看成 $\mathbb{Z}$-模. 反之，由定义可知，每个 $\mathbb{Z}$-模 M 就是加群 M 按上述方式确定的 $\mathbb{Z}$-模.

(2) 环 R 的理想均是 R-模.

(3) 设 $f:R\to S$ 是环同态. 若 M 是 S-模，对于 $r\in R$ 和 $x\in M$, 定义 $rx=f(r)x$. 不难验证，这使 M 成为一个 R-模，这样每个 S-模均可看作 R-模. 特别地，若 R 是 S 的子环，则 S 是 R-模.

若 R-模 M 的非空子集 N 对于 M 的运算构成一个 R-模，则称 N 是 M 的一个**子模**，换句话说，N 是 M 的子模当且仅当 N 是 M 的非空子集，且对于任意 $x,y\in N$ 和 $r\in R$, 均有 $x+y\in N$

和 $rx\in N$. 由子模的定义，不难验证，对于任意 R-模 M，均有

(1) M 的子模的子模仍是 M 的子模；

(2) M 的子模(有限个或无限个)的交仍是 M 的子模；

(3) M 的子模的升链并仍是 M 的子模.

设 X 是 R-模 M 的子集. M 的所有包含 X 的子模(M 就是一个)的交 N 称为 M 的**由 X 生成的子模**，且称 X 是子模 N 的一个**生成元集**. 当 $X=\varnothing$ 时，约定 $N=0$. 当 $X=\{a\}$，$a\in M$ 时，$N=\{ra\mid r\in R\}=Ra$，称为由 a 生成的**循环子模**. 当 X 是有限子集时，称 N 是 M 的**有限生成子模**.

设 M_1,M_2 是 R-模 M 的子模. 易知

$$M_1+M_2=\{x+y\mid x\in M_1,\ y\in M_2\}$$

是 M 的子模，叫做 M_1 与 M_2 的**和**. $M_1\cap M_2$ 也是 M 的子模. 不难验证，子模的和与交运算满足交换律和结合律. 对于 R-模 M 的子模族 M_λ，$\lambda\in\Lambda$，定义它们的**和**为

$$\sum_{\lambda\in\Lambda}M_\lambda=\{\sum_{\lambda\in\Lambda}x_\lambda\mid x_\lambda\in M_\lambda,\ \lambda\in\Lambda,\ \text{且只有有限个 } x_\lambda\neq 0\}.$$

设 N 是 R-模 M 的子模，则 N 是 M 的子加群. 定义 R 在商群 M/N 上的作用为

$$r(m+N)=rm+N,\ m\in M,\ r\in R.$$

这样定义的作用是合理的，即与陪集 $m+N$ 的代表元的选择无关. 事实上，若 $m+N=n+N$；$m,n\in M$，则 $m-n\in N$. 于是对于任意的 $r\in R$，$rm-rn=r(m-n)\in N$，从而 $rm+N=rn+N$. 进而可以验证 M/N 构成一个 R-模，称为 M 关于子模 N 的 R-**商模**.

下述引理是很重要的.

引理 1.2.1 (**Nakayama**) 设 M 是有限生成 R-模，I 是环 R 的理想，且 $I\subseteq\mathrm{Rad}(R)$. 若 $IM=M$，则 $M=0$.

证明 假定 $M\neq 0$. 设 $\{u_1,u_2,\cdots,u_n\}$ 是 M 的一个元素个数最小的生成元集. 由于 $IM=M$，存在 $r_1,\cdots,r_n\in I$，使得 $u_n=$

$r_1u_1+\cdots+r_nu_n$，从而$(1-r_n)u_n=r_1u_1+\cdots+r_{n-1}u_{n-1}$．由于$r_n\in I\subseteq\mathrm{Rad}(R)$，据命题 1.1.4，$1-r_n\in\mathrm{U}(R)$，于是 $u_n=(1-r_n)^{-1}r_1u_1+\cdots+(1-r_n)^{-1}r_{n-1}u_{n-1}$．这表明 M 可由$\{u_1,\cdots,u_{n-1}\}$生成，这与 n 的最小性矛盾．所以 $M=0$．　□

推论 1.2.2　设 N 是有限生成 R-模 M 的子模，I 是 R 的理想且 $I\subseteq\mathrm{Rad}(R)$．若 $M=IM+N$，则 $M=N$．

证明　用上述引理于有限生成 R-商模 M/N．由于 $I(M/N)=(IM+N)/N=M/N$，从而 $M/N=0$，即 $M=N$．　□

设 L 和 N 是 R-模 M 的子模．定义

$$(L:N)=\{a\in R\mid aN\subseteq L\}.$$

这是 R 的理想．当 $L=0$ 为零模时，$(0:N)$称为 N 的**零化理想**，记作 $\mathrm{Ann}_R(N)$．不难验证，$(L:N)$就是商模 M/L 的子模$(N+L)/L$ 的零化理想．R-模 M 称为是**忠实 R-模**，如果 $\mathrm{Ann}_R(M)=0$．

设 M 是 R-模，$x\in M$．记 $\mathrm{Ann}_R(Rx)$为 $\mathrm{Ann}_R(x)$，称为元素 x 的**零化理想**．若 $\mathrm{Ann}_R(x)\neq 0$，则称 x 是 M 的**扭元素**．记 R-模 M 的所有扭元素作成的集合为 $\mathrm{T}(M)$．若 $\mathrm{T}(M)=0$，则称 M 是**无扭 R-模**．显然，无扭 R-模必是忠实 R-模．

命题 1.2.3　设 R 是整环，M 是 R-模，则 $\mathrm{T}(M)$是 M 的子模，称为 M 的**扭子模**，且 $M/\mathrm{T}(M)$是无扭 R-模．

证明　设 $x,y\in\mathrm{T}(M)$，则存在 $r,s\in R\backslash 0$，使得 $rx=sy=0$．由于 R 是整环，故 $rs\neq 0$，且 $rs(x+y)=0$，所以 $x+y\in\mathrm{T}(M)$．对于每个 $t\in R$，$r(tx)=t(rx)=0$，从而 $tx\in\mathrm{T}(M)$．所以 $\mathrm{T}(M)$是 M 的子模．

设 $\bar{x}=x+\mathrm{T}(M)\in\mathrm{T}(M/\mathrm{T}(M))$，$x\in M$．则存在 $r\in R\backslash 0$，使得 $r\bar{x}=0$，即 $rx\in\mathrm{T}(M)$，于是存在 $s\in R\backslash 0$，使得 $s(rx)=0$．由于 $sr\neq 0$，$x\in\mathrm{T}(M)$，从而 $\bar{x}=0$．所以 $\mathrm{T}(M/\mathrm{T}(M))=0$．　□

1.2.2 R-模同态和同态基本定理

设 M 和 N 为 R-模，映射 $f:M\to N$ 称为一个 **R-模同态**（或 **R-同态**），如果对于任意 $x,y\in M$ 和 $r\in R$，均有

(1) $f(x+y)=f(x)+f(y)$;

(2) $f(rx)=rf(x)$.

若 f 还是一个单（满、双）射，则称 f 是 **R-模单同态**（**满同态**、**同构**）. 若存在 R-模 M 到 N 的一个 R-模同构，则称 M 与 N 是 **R-同构的**，记作 $M\simeq N$.

R-模 M 到 N 的所有 R-同态构成的集合记作 $\mathrm{Hom}_R(M,N)$. 对于 $f,g\in\mathrm{Hom}_R(M,N)$，定义

$$f+g:M\to N;\ x\mapsto f(x)+g(x).$$

不难验证，$f+g$ 仍是 R-同态，且 $\mathrm{Hom}_R(M,N)$ 关于这个加法构成一个加法 Abel 群；其零元为 **R-零同态** $0:M\to N;x\mapsto 0_N$; $f\in\mathrm{Hom}_R(M,N)$ 的负元为 $-f:M\to N;x\mapsto -f(x)$. 对于 $r\in R$ 和 $f\in\mathrm{Hom}_R(M,N)$，定义 r 在 f 上的作用为

$$rf:M\to N;\ x\mapsto rf(x).$$

容易验证，rf 也是 R-同态，且使 $\mathrm{Hom}_R(M,N)$ 构成一个 R-模. 这是一类重要的 R-模.

若 $f:M\to N$ 和 $g:N\to P$ 是 R-同态，则 f 与 g 的合成 $gf:M\to P;\ x\mapsto g(f(x))$ 仍是 R-同态. 容易验证，对于任意 $f,f_1,f_2\in\mathrm{Hom}_R(M,N)$; $g,g_1,g_2\in\mathrm{Hom}_R(N,P)$ 和 $r\in R$，均有

(1) $g(f_1+f_2)=gf_1+gf_2$;

(2) $(g_1+g_2)f=g_1f+g_2f$;

(3) $(rg)f=r(gf)=g(rf)$.

设 $f:M\to N$ 是 R-模同态. 记

$$\mathrm{Im}\,f=\{f(x)\in N\mid x\in M\},$$
$$\mathrm{Ker}\,f=\{x\in M\mid f(x)=0\}=f^{-1}(0).$$

容易验证，$\mathrm{Im}\,f$ 是 N 的子模，$\mathrm{Ker}\,f$ 是 M 的子模，分别称为 f 的**像**与**核**.

设 P 是 R-模 M 的子模. 自然映射 $\varphi: M \to M/P$; $x \mapsto \overline{x} = x + P$ 是 R-同态，称 φ 是从 M 到商模 M/P 的**自然 R-同态**.

定理 1.2.4（**R-模同态基本定理**）　设 $f: M \to N$ 是 R-同态，P 是含于 $\mathrm{Ker} f$ 中的子模. 则存在唯一的 R-同态

$$g: M/P \to N;\ x + P \mapsto f(x)$$

使得 $g\varphi = f$，其中 $\varphi: M \to M/P$ 是自然 R-同态.

并且，g 是 R-满同态当且仅当 f 是 R-满同态；g 是 R-单同态当且仅当 $P = \mathrm{Ker}\,f$.

特别地，当 f 是 R-满同态时，有 R-同构

$$M/\mathrm{Ker}\,f \simeq N.$$

证明　由群的同态基本定理可知 g 是加群同态，为证 g 是 R-同态，只需证 $g(r\overline{x}) = rg(\overline{x})$，其中 $x \in M$，$\overline{x} = x + \mathrm{Ker}\,f$，$r \in R$. 这是因为 $g(r\overline{x}) = g(\overline{rx}) = f(rx) = rf(x) = rg(\overline{x})$. □

用上述定理和群论中的相应方法，不难证明下面三个定理.

定理 1.2.5　设 N, P 是 R-模 M 的子模，且 $N \subseteq P \subseteq M$，则有 R-同构

$$(M/N)/(P/N) \simeq M/P.$$

定理 1.2.6　设 N, P 是 R-模 M 的子模，则有 R-同构

$$(N + P)/N \simeq P/(N \cap P).$$

定理 1.2.7　设 N 是 R-模 M 的子模，$\mathscr{S}$ 是 M 的所有包含 N 的子模构成的集合，$\mathscr{T}$ 是 R-商模 M/N 的所有子模构成的集合，则映射

$$\psi: \mathscr{S} \to \mathscr{T};\ P \mapsto P/N$$

是保序双射.

1.2.3　直积与直和

设 M_i，$i \in I$，是一族 R-模. 笛卡尔积 $\prod_{i \in I} M_i$ 的元素表示成

$(x_i)_{i\in I}$，其中 $x_i\in M_i$ 对于每个 $i\in I$ 成立．元素 $(x_i)_{i\in I}=(y_i)_{i\in I}$ 当且仅当对于每个 $i\in I$ 均有 $x_i=y_i$．当下标集 I 是可数集 $\{1,2,\cdots\}$ 时，元素 $(x_i)_{i\in I}$ 可表示成 $(x_1,x_2,\cdots)$．定义运算

$$(x_i)_{i\in I}+(y_i)_{i\in I}=(x_i+y_i)_{i\in I};\ x_i,y_i\in M_i;$$

$$r(x_i)_{i\in I}=(rx_i)_{i\in I},\ x_i\in M_i,\ r\in R.$$

容易验证，$\prod\limits_{i\in I}M_i$ 关于上述运算构成一个 R-模，称为 R-模 M_i，$i\in I$，的**直积**．$\prod\limits_{i\in I}M_i$ 的子集

$$\bigoplus_{i\in I}M_i=\{(x_i)_{i\in I}\mid x_i\in M_i,\ i\in I;\text{且只有有限个 } x_i\neq 0\}$$

是 $\prod\limits_{i\in I}M_i$ 的 R-子模，称为 R-模 M_i，$i\in I$，的**直和**．当下标集 I 是有限集时，直和与直积是一致的．对于每个 $k\in I$，映射

$$\pi_k:\ \prod_{i\in I}M_i\to M_k;\ (x_i)_{i\in I}\mapsto x_k$$

是 R-满同态，叫做**标准投影**；而映射

$$\tau_k:\ M_k\to\prod_{i\in I}M_i;\ x_k\mapsto(y_i)_{i\in I},$$

其中 $y_k=x_k$，而当 $i\neq k$ 时 $y_i=0$，是 R-单同态，叫做**标准嵌入**．

R-模的直积与直和有如下的“泛性”．

定理 1.2.8　设 M_i，$i\in I$，是一族 R-模，N 是任意 R-模．

(1) 若 f_i: $N\to M_i$，$i\in I$，是一族 R-同态，则存在唯一的 R-同态

$$f:\ N\to\prod_{i\in I}M_i;\ x\mapsto(f_i(x))_{i\in I},$$

使得对于每个 $i\in I$ 均有 $\pi_i f=f_i$，即下图交换：

$$\begin{tikzcd}
N \arrow[r, "f"] \arrow[d, "f_i"'] & \prod\limits_{i\in I}M_i \arrow[dl, "\pi_i"] \\
M_i &
\end{tikzcd}$$

(2) 若 g_i: $M_i\to N$，$i\in I$，是一族 R-同态，则存在唯一的 R-同态

$$g: \bigoplus_{i\in I} M_i \to N;\ (x_i)_{i\in I} \mapsto \sum_{i\in I} g_i(x_i),$$

使得对于每个 $i\in I$ 均有 $g\tau_i = g_i$，即下图交换：

$$\begin{tikzcd}
N & \bigoplus_{i\in I} M_i \arrow[l, "g"'] \\
M_i \arrow[u, "g_i"] \arrow[ur, "\tau_i"'] &
\end{tikzcd}$$

证明　(1) 直接验证可知 f 是 R-同态，且满足 $\pi_i f = f_i$，$i\in I$. 又若 R-同态 $f':N\to \coprod_{i\in I} M_i$ 亦满足 $\pi_i f' = f_i$，$i\in I$，则对于任意的 $i\in I$ 和 $x\in N$，由标准投影的定义，有 $\pi_i f(x) = f_i(x) = \pi_i f'(x)$，从而 $f(x) = f'(x)$，$x\in N$. 所以 $f = f'$.

(2) 注意到 $(x_i)_{i\in I} \in \bigoplus_{i\in I} M_i$ 中只有有限个 $x_i \neq 0$，故 $\sum_{i\in I} g_i(x_i)$ 是有限和. 仿(1)可证(2).　□

下面用 R-同态来刻画 R-模的有限直和.

定理 1.2.9　设 $M, M_1, M_2, \cdots, M_n$ 是 R-模. 则 $M \simeq M_1 \oplus M_2 \oplus \cdots \oplus M_n$ 的充要条件是存在 R-同态 $p_i: M\to M_i$ 和 $q_i: M_i \to M$，$i = 1,2,\cdots,n$，使得

(1) $p_i q_i = 1_{M_i}$，$i = 1,2,\cdots,n$；

(2) $p_i q_j = 0$，$1\leqslant i\neq j\leqslant n$；

(3) $q_1 p_1 + q_2 p_2 + \cdots + q_n p_n = 1_M$.

证明　必要性：设 $f: M\to \bigoplus_{i=1}^{n} M_i$ 是 R-同构，π_i 和 τ_i 分别是 $\bigoplus_{i=1}^{n} M_i$ 的标准投影和标准嵌入. 令 $p_i = \pi_i f$，$q_i = f^{-1}\tau_i$，不难验证，p_i 和 q_i 满足条件(1)，(2)，(3).

充分性：令 $\varphi = \sum_{i=1}^{n} q_i \pi_i$，$\psi = \sum_{i=1}^{n} \tau_i p_i$. 直接验证 $\psi\varphi =$

$1_{\oplus M_i}$，且 $\varphi\psi = 1_M$. 从而 φ 即为所需的R-同构. □

习 题 1.2

1. 记 $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$，$n$ 为正整数. 证明：$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}) = 0$，$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_m, \mathbb{Z}_n) \simeq \mathbb{Z}_d$，其中 $d = (m, n)$是 m 和 n 的最大公因数.

2. 试确定 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z})$和 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q})$.

3. 设 M 是R-模. 证明：

(1) $\mathrm{Hom}_R(R, M) \simeq M$.

(2) M 是忠实$R/\mathrm{Ann}_R(M)$-模.

4. 设 M 是循环R-模. 证明：存在 R 的理想I，使得 $M \simeq R/I$.

5. 有限生成 R-模的子模或商模是否是有限生成R-模?

6. 设 R 是环S 的子环，且 S 是有限生成R-模. 证明：若 M 是有限生成S-模，则 M 是有限生成R-模.

7. 设 M 是有限生成R-模，X 是M 的任意一个生成元集. 证明：X 必含一个有限子集X_0，使得 X_0 生成 M.

8. 证明：非零的有限生成 R-模M 必含有一个极大子模(M 的子模N 叫做M 的**极大子模**，如果 $N \neq M$，并且若 M 的子模 $N' \supset N$，则有 $N' = M$).

9. 设 N, P 是R-模M 的子模. 证明：

(1) $\mathrm{Ann}_R(N + P) = \mathrm{Ann}_R(N) \cap \mathrm{Ann}_R(P)$.

(2) $(N : P) = \mathrm{Ann}_R((P + N)/N)$.

10. 设 M 是R-模，$f \in \mathrm{Hom}_R(M, M)$且 $f^2 = f$. 证明：$M = \mathrm{Ker}\, f \oplus \mathrm{Im}\, f$.

11. 设 $f: M \to N$ 和$g: N \to M$ 是R-同态，且 $gf = 1_M$. 证明：$N = \mathrm{Im}\, f \oplus \mathrm{Ker}\, g$.

12. 证明：$(\mathbb{Q}, +)$不是有限生成 $\mathbb{Z}$-模.

1.3　范畴和函子

1.3.1　定义和例

一个**范畴** $\mathscr{C}$ 由下列成份构成：

(1) 一个由**对象**组成的类 $\mathrm{ob}\mathscr{C}$，常以 $A\in\mathrm{ob}\mathscr{C}$ 表示 A 是范畴 $\mathscr{C}$ 中的一个对象；

(2) 对于 $\mathrm{ob}\mathscr{C}$ 中每个有序对象对 (A,B)，有一个由**态射**组成的集合 $\mathrm{Hom}_{\mathscr{C}}(A,B)$，其中的态射常表示成 $f:A\to B$；

(3) 对于 $\mathrm{ob}\mathscr{C}$ 中任意三元有序对象组 (A,B,C)，存在一个映射

$$\mathrm{Hom}_{\mathscr{C}}(B,C)\times\mathrm{Hom}_{\mathscr{C}}(A,B)\to\mathrm{Hom}_{\mathscr{C}}(A,C);\ (g,f)\mapsto gf.$$

称 $gf:A\to C$ 为态射 $g:B\to C$ 与 $f:A\to B$ 的**合成**，且满足以下条件：

(i) 若有序对象对 $(A,B)\neq(C,D)$，则

$$\mathrm{Hom}_{\mathscr{C}}(A,B)\cap\mathrm{Hom}_{\mathscr{C}}(C,D)=\varnothing;$$

(ii) 若 $f:A\to B$，$g:B\to C$，$h:C\to D$ 是 $\mathscr{C}$ 中的态射，则

$$h(gf)=(hg)f;$$

(iii) 对于 $\mathscr{C}$ 中的每个对象 B，存在 $1_B\in\mathrm{Hom}_{\mathscr{C}}(B,B)$，使得对于 $\mathscr{C}$ 中任意态射 $f:A\to B$ 和 $g:B\to C$，均有 $1_Bf=f$ 和 $g1_B=g$.

关于范畴的定义，要注意以下几点：

(1) 范畴 $\mathscr{C}$ 的所有对象构成一个类，未必是集合；而 $\mathrm{Hom}_{\mathscr{C}}(A,B)$ 必须是集合(可以是空集)，称为从 A 到 B 的**态射集**. 如果 $\mathrm{ob}\mathscr{C}$ 是一个集合，则称 $\mathscr{C}$ 是**小范畴**.

(2) 范畴的态射未必是映射. 像集合映射的合成一样，态射的合成是一个部分二元运算.

(3) 对于每个对象 B，态射集 $\mathrm{Hom}_{\mathscr{C}}(B,B)$ 关于态射的合成

构成一个半群，条件(iii)中的 1_B 是其单位元，因而唯一. 也称 1_B 为**单位元态射**.

范畴 $\mathscr{D}$ 称为是范畴 $\mathscr{C}$ 的**子范畴**，如果 $\mathrm{ob}\,\mathscr{D}\subseteq\mathrm{ob}\,\mathscr{C}$，且对于任意 $A,B\in\mathrm{ob}\,\mathscr{D}$，均有 $\mathrm{Hom}_{\mathscr{D}}(A,B)\subseteq\mathrm{Hom}_{\mathscr{C}}(A,B)$ 且 $\mathrm{Hom}_{\mathscr{C}}(A,A)$ 中的 $1_A\in\mathrm{Hom}_{\mathscr{D}}(A,A)$，并且 $\mathscr{D}$ 中态射的合成就是 $\mathscr{C}$ 中态射的合成. 又若对于任意 $A,B\in\mathrm{ob}\,\mathscr{D}$ 均有 $\mathrm{Hom}_{\mathscr{D}}(A,B)=\mathrm{Hom}_{\mathscr{C}}(A,B)$，则称 $\mathscr{D}$ 是 $\mathscr{C}$ 的**全子范畴**.

由范畴 $\mathscr{C}$ 中的态射 f,g,h 作成的下图称为**交换图**，如果 $gf=h$.

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \\
& C
\end{tikzcd}$$

例 (1) 所有的非空集合构成一个范畴，记作 $\mathscr{Set}$，其态射为集合间的映射，而态射的合成就是映射的合成.

(2) 所有的群构成一个范畴，记作 $\mathscr{G}$，其态射为群同态. 所有的 Abel 群也构成一个范畴，记作 $\mathscr{Ab}$. 由定义，$\mathscr{G}$(忘掉群运算)是 $\mathscr{Set}$ 的子范畴，而 $\mathscr{Ab}$ 是 $\mathscr{G}$ 的全子范畴.

(3) 环 R 上的所有 R-模构成一个范畴，记作 $\mathscr{M}_R$，其态射是 R-模同态.

(4) 设 $\mathscr{C}$ 是一个范畴，构作范畴 $\mathscr{C}^\circ$ 如下：

(i) $\mathrm{ob}\,\mathscr{C}^\circ=\mathrm{ob}\,\mathscr{C}$；

(ii) 对于任意 $A,B\in\mathrm{ob}\,\mathscr{C}^\circ$，$\mathrm{Hom}_{\mathscr{C}^\circ}(A,B)=\mathrm{Hom}_{\mathscr{C}}(B,A)$，也就是说，将 $\mathscr{C}$ 中的每个态射 $f:B\to A$ 中的箭头反向就是 $\mathscr{C}^\circ$ 中的态射 $f:A\to B$；反之亦然；

(iii) $\mathscr{C}^\circ$ 中态射 $f:A\to B$ 和 $g:B\to C$ 的合成 $gf:A\to C$ 就是 $\mathscr{C}$ 中态射 $g:C\to B$ 和 $f:B\to A$ 的合成 $fg:C\to A$.

这样，如果在 $\mathscr{C}$ 中有交换图

$$\begin{tikzcd} C \arrow[r, "g"] \arrow[dr, "h = fg"'] & B \arrow[d, "f"] \\ & A \end{tikzcd},$$

则在 $\mathscr{C}^{\circ}$ 中有反向的交换图

$$\begin{tikzcd} C & B \arrow[l, "g"'] \\ & A \arrow[u, "f"'] \arrow[ul, "h = gf"] \end{tikzcd};$$

反之亦然. 易证，$\mathscr{C}^{\circ}$是一个范畴，叫做 $\mathscr{C}$ 的**对偶范畴**.

范畴 $\mathscr{C}$ 中的对象 A 和B 称为是**同构**的，记作 $A \simeq B$，如果存在态射 $f: A \to B$ 和$g: B \to A$，使得 $gf = 1_A$ 且 $fg = 1_B$. 此时也称 f 是从 A 到 B 的**同构(态射)**. 例如，集合间的双射、群同构和 R-模同构分别是范畴 $\mathscr{Set}$，$\mathscr{G}$ 和 $\mathscr{M}_R$ 中的同构态射.

范畴 $\mathscr{C}$ 中的对象 $A(Z)$称为 $\mathscr{C}$ 的一个**始(终)对象**，如果对于 $\mathscr{C}$ 中任意对象 X，$\mathrm{Hom}_{\mathscr{C}}(A, X)(\mathrm{Hom}_{\mathscr{C}}(X, Z))$恰含一个态射. 既是始对象又是终对象的对象称为 $\mathscr{C}$ 的**零对象**. 由定义，$\mathscr{C}$ 的始(终)对象恰是它的对偶范畴 $\mathscr{C}^{\circ}$的终(始)对象. 这表明，始对象与终对象是对偶的概念，统称为 $\mathscr{C}$ 的 **泛对象**. 例如，$\mathscr{Set}$ 无始对象，而一元集均是终对象；平凡群均是 $\mathscr{G}$ 的始(终、零)对象；而零 R-模$\{0\}$是 $\mathscr{M}_R$ 的始(终、零)对象.

命题 1.3.1　一个范畴 $\mathscr{C}$ 的始(终、零)对象(如果存在)在同构意义下唯一.

证明　设 A 和A'是 $\mathscr{C}$ 的始对象. 则存在唯一的态射 $f: A \to A'$和$g: A' \to A$，于是 $gf \in \mathrm{Hom}_{\mathscr{C}}(A, A)$. 又由于 $\mathrm{Hom}_{\mathscr{C}}(A, A) = \{1_A\}$，故 $gf = 1_A$. 同理可证 $fg = 1_{A'}$. 所以 $A \simeq A'$. 对偶地，可

证终对象的唯一性，进而可得零对象的唯一性. □

下面介绍范畴中的三类重要对象：积、余积和自由对象.

设$\{A_\lambda,\ \lambda\in\Lambda\}$是范畴$\mathscr{C}$中对象构成的一个集合. 构作范畴$\mathscr{D}$如下：令

$$\mathrm{ob}\mathscr{D}=\{(B,f_\lambda,\lambda\in\Lambda)\mid B\in\mathrm{ob}\mathscr{C},f_\lambda\in\mathrm{Hom}_{\mathscr{C}}(B,A_\lambda),\lambda\in\Lambda\};$$

从$\mathscr{D}$中对象$(B,f_\lambda,\lambda\in\Lambda)$到$(C,g_\lambda,\lambda\in\Lambda)$的态射是$h\in\mathrm{Hom}_{\mathscr{C}}(B,C)$，使得对于每个$\lambda\in\Lambda$均有$g_\lambda h=f_\lambda$，即有交换图

$$\begin{tikzcd}
B \arrow[r, "h"] \arrow[d, "f_\lambda"'] & C \arrow[dl, "g_\lambda"] \\
A_\lambda &
\end{tikzcd}$$

$\mathscr{D}$中态射的合成就是$\mathscr{C}$中态射的合成. 范畴$\mathscr{D}$的终对象$(P,\pi_\lambda,\lambda\in\Lambda)$叫做$\mathscr{C}$中对象集$\{A_\lambda,\lambda\in\Lambda\}$的**积**，常简称$P$为$\{A_\lambda,\lambda\in\Lambda\}$的积，记作$P=\coprod\limits_{\lambda\in\Lambda}A_\lambda$. 由命题1.3.1，它在同构意义下唯一. 于是$\{A_\lambda,\lambda\in\Lambda\}$的积$P$及态射$\pi_\lambda:P\to A_\lambda(\lambda\in\Lambda)$具有下述泛性：对于$\mathscr{C}$中任意对象$B$和态射$f_\lambda:B\to A_\lambda$，$\lambda\in\Lambda$，存在$\mathscr{C}$中唯一的态射$h:B\to P$，使得对任意$\lambda\in\Lambda$均有$\pi_\lambda h=f_\lambda$，即下图交换：

$$\begin{tikzcd}
B \arrow[r, "h"] \arrow[d, "f_\lambda"'] & P \arrow[dl, "\pi_\lambda"] \\
A_\lambda &
\end{tikzcd}$$

对偶地，$\mathscr{D}$的对偶范畴$\mathscr{D}^\circ$的终对象$(Q,\tau_\lambda,\lambda\in\Lambda)$称为$\mathscr{C}$中对象集$\{A_\lambda,\lambda\in\Lambda\}$的**余积**，常简称$Q$是$\{A_\lambda,\lambda\in\Lambda\}$的余积，记作$Q=\coprod\limits_{\lambda\in\Lambda}A_\lambda$，它也在同构意义下唯一. 于是$\{A_\lambda,\lambda\in\Lambda\}$的余积$Q$及态射$\tau_\lambda:A_\lambda\to Q(\lambda\in\Lambda)$具有下述泛性：对于$\mathscr{C}$中任意对象$B$和态射$g_\lambda:A_\lambda\to B$，$\lambda\in\Lambda$，存在$\mathscr{C}$中唯一的态射$k:Q\to B$，使

得对于任意 $\lambda \in \Lambda$ 均有 $k\tau_\lambda = g_\lambda$，即下图交换：

$$\begin{tikzcd}
B & Q \arrow[l, "k"'] \\
& A_\lambda \arrow[ul, "g_\lambda"] \arrow[u, "\tau_\lambda"']
\end{tikzcd}$$

例如，由定理 1.2.8 可知，R-模族 $\{M_\lambda,\ \lambda \in \Lambda\}$ 的直积(连同标准投影)就是它们在 $\mathscr{M}_R$ 中的积，而直和(连同标准嵌入)就是它们在 $\mathscr{M}_R$ 中的余积.

范畴 $\mathscr{C}$ 称为**具体范畴**，如果 $\mathscr{C}$ 中每个对象 A 对应于一个称为**承载集**的集合 $\sigma(A)$，而 $\mathscr{C}$ 中的态射 $f: A \to B$ 也是 $\sigma(A)$ 到 $\sigma(B)$ 的映射，且态射的合成就是映射的合成. 例如，$\mathscr{Set}$，$\mathscr{G}$ 和 $\mathscr{M}_R$ 都是具体范畴. 通常将具体范畴中的对象 A 与其承载集 $\sigma(A)$ 等同起来.

设 $\mathscr{C}$ 是一个具体范畴，X 是一个集合. 构作范畴 $\mathscr{D}$ 如下：令

$$\mathrm{ob}\mathscr{D} = \{\text{映射 } f: X \to A \mid A \in \mathrm{ob}\mathscr{C}\}.$$

从 $\mathscr{D}$ 中的对象 $f: X \to A$ 到对象 $g: X \to B$ 的态射集 $\mathrm{Hom}_{\mathscr{D}}(f, g)$ 是所有使得下图

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "g"'] & A \arrow[d, "h"] \\
& B
\end{tikzcd}$$

交换的态射 $h \in \mathrm{Hom}_{\mathscr{C}}(A, B)$. 而 $\mathscr{D}$ 中态射的合成就是 $\mathscr{C}$ 中态射的合成. 范畴 $\mathscr{D}$ 的始对象 $\tau: X \to F$，$F \in \mathrm{ob}\mathscr{C}$，称为 $\mathscr{C}$ 的在集合 X 上的**自由对象**，也常简称 F 是 $\mathscr{C}$ 中的自由对象. 于是 X 上的自由对象 F 及映射 $\tau: X \to F$ 具有下述泛性：对于任意 $A \in \mathrm{ob}\mathscr{C}$ 和映射 $f: X \to A$，存在 $\mathscr{C}$ 中唯一的态射 $h: F \to A$，使得下图交换：

$$\begin{tikzcd} X \arrow[r, "\tau"] \arrow[dr, "f"'] & F \arrow[d, "h"] \\ & A \end{tikzcd}.$$

例如，自由群是 $\mathscr{G}$ 中的自由对象，自由 Abel 群是 $\mathscr{A}b$ 中的自由对象. R-模范畴 $\mathscr{M}_R$ 中的自由对象将在第 2 章 2.2 节中给出.

1.3.2 函子

范畴 $\mathscr{C}$ 到范畴 $\mathscr{D}$ 的一个(**共变**)**函子** $F:\mathscr{C}\to\mathscr{D}$ 由下列成份构成:

(1) 对于每个 $A\in\mathrm{ob}\mathscr{C}$，有唯一的 $F(A)\in\mathrm{ob}\mathscr{D}$ 与之对应，也可以说，F 是从类 $\mathrm{ob}\mathscr{C}$ 到 $\mathrm{ob}\mathscr{D}$ 的一个"映射"；

(2) 对于任意 $A,B\in\mathrm{ob}\mathscr{C}$，有一个映射，仍记作 F:

$F:\mathrm{Hom}_{\mathscr{C}}(A,B)\to\mathrm{Hom}_{\mathscr{D}}(F(A),F(B))$; $f\mapsto F(f)$,

满足下列条件:

(i) 对于任意 $A\in\mathrm{ob}\mathscr{C}$，$F(1_A)=1_{F(A)}$；

(ii) 对于任意 $f\in\mathrm{Hom}_{\mathscr{C}}(A,B)$和 $g\in\mathrm{Hom}_{\mathscr{C}}(B,C)$，均有

$$F(gf) = F(g)F(f).$$

对偶地，范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的一个**反变函子** $F':\mathscr{C}\to\mathscr{D}$ 是从 $\mathscr{C}$ 到 $\mathscr{D}^{\circ}$的(共变)函子. 于是对于任意 $f\in\mathrm{Hom}_{\mathscr{C}}(A,B)$和 $g\in\mathrm{Hom}_{\mathscr{C}}(B,C)$，均有 $F'(f)\in\mathrm{Hom}_{\mathscr{D}}(F(B),F(A))$，$F'(g)\in\mathrm{Hom}_{\mathscr{D}}(F(C),F(B))$，并且 $F'(gf)=F'(f)F'(g)$.

这样，范畴 $\mathscr{C}$ 中的一个交换图

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

经(共变)函子 $F:\mathscr{C}\to\mathscr{D}$ 作用，得到 $\mathscr{D}$ 中一个同向的交换图

$$\begin{tikzcd} F(A) \arrow[r, "F(f)"] \arrow[dr, "F(h)"'] & F(B) \arrow[d, "F(g)"] \\ & F(C) \end{tikzcd},$$

而经反变函子 $F':\mathscr{C}\to\mathscr{D}$ 作用，得到 $\mathscr{D}$ 中一个反向的交换图

$$\begin{tikzcd} F'(A) & F'(B) \arrow[l, "F'(f)"'] \\ & F'(C) \arrow[ul, "F'(h)"] \arrow[u, "F'(g)"'] \end{tikzcd}.$$

例　(1) **恒等函子** $1_{\mathscr{C}}:\mathscr{C}\to\mathscr{C}$，它将 $\mathscr{C}$ 中的每个对象和态射对应到自身.

(2) 设 $\mathscr{D}$ 是范畴 $\mathscr{C}$ 的子范畴，将恒等函子限制到 $\mathscr{D}$ 上，得到**嵌入函子** $E:\mathscr{D}\to\mathscr{C}$.

(3) 将一个具体范畴 $\mathscr{C}$ 中的每个对象 A 对应于它的承载集 $\sigma(A)$，可得到从 $\mathscr{C}$ 到 $\mathscr{S}et$ 的"遗忘"函子. 又若忘掉环 R 在 R-模 M 上的作用，将 M 对应到它的加群，则可得到从 $\mathscr{M}_R$ 到 $\mathscr{A}b$ 的一个遗忘函子.

设 $F:\mathscr{C}\to\mathscr{D}$ 和 $G:\mathscr{D}\to\mathscr{E}$ 是函子. 可定义从 $\mathscr{C}$ 到 $\mathscr{E}$ 的函子 $GF:\mathscr{C}\to\mathscr{E}$ 如下：对于每个 $A\in\operatorname{ob}\mathscr{C}$，令 $(GF)(A)=G(F(A))$；而对于每个 $f\in\operatorname{Hom}_{\mathscr{C}}(A,B)$，令 $(GF)(f)=G(F(f))$. 容易验证，GF 是从 $\mathscr{C}$ 到 $\mathscr{E}$ 的函子，叫做 F 与 G 的**合成**. 类似地可定义两个反变函子或一个共变函子与一个反变函子的合成. 易知，两个反变函子的合成是一个共变函子，而一个共变函子与一个反变函子的合成是一个反变函子.

下面介绍有重要意义和广泛应用的 Hom 函子.

设 $\mathscr{C}$ 是一个范畴，任意取定 $\mathscr{C}$ 中的一个对象 D，构作函子

$\mathrm{Hom}_{\mathscr{C}}(D,-):\mathscr{C}\to\mathscr{Set}$ 如下：将 $\mathscr{C}$ 中每个对象 A 对应到态射集 $\mathrm{Hom}_{\mathscr{C}}(D,A)$，且将 $\mathscr{C}$ 中态射 $f:A\to B$ 对应到映射

$$f^* = \mathrm{Hom}_{\mathscr{C}}(D,f):\ \mathrm{Hom}_{\mathscr{C}}(D,A)\to\mathrm{Hom}_{\mathscr{C}}(D,B)$$
$$g\mapsto f^*(g)=fg.$$

容易验证，对于 $\mathscr{C}$ 中任意态射 $f:A\to B$ 和 $g:B\to C$，均有 $(gf)^*=g^*f^*$，且对于任意 $A\in\mathrm{ob}\,\mathscr{C}$，均有 $(1_A)^*=1_{\mathrm{Hom}_{\mathscr{C}}(D,A)}$，从而 $\mathrm{Hom}_{\mathscr{C}}(D,-)$ 是从 $\mathscr{C}$ 到 $\mathscr{Set}$ 的一个(共变)函子.

又构作反变函子 $\mathrm{Hom}_{\mathscr{C}}(-,D):\mathscr{C}\to\mathscr{Set}$ 如下：将 $\mathscr{C}$ 中每个对象 A 对应到态射集 $\mathrm{Hom}_{\mathscr{C}}(A,D)$，且将 $\mathscr{C}$ 中态射 $f:A\to B$ 对应到映射

$$f_*:\mathrm{Hom}_{\mathscr{C}}(B,D)\to\mathrm{Hom}_{\mathscr{C}}(A,D);\ g\mapsto f_*(g)=gf.$$

不难验证，对于 $\mathscr{C}$ 中任意态射 $f:A\to B$ 和 $g:B\to C$，均有 $(gf)_*=f_*g_*$，且对于任意 $A\in\mathrm{ob}\,\mathscr{C}$，均有 $(1_A)_*=1_{\mathrm{Hom}_{\mathscr{C}}(A,D)}$，进而 $\mathrm{Hom}_{\mathscr{C}}(-,D)$ 是从 $\mathscr{C}$ 到 $\mathscr{Set}$ 的一个反变函子.

$\mathrm{Hom}_{\mathscr{C}}(D,-)$ 和 $\mathrm{Hom}_{\mathscr{C}}(-,D)$ 统称为关于对象 D 的 **Hom 函子**.

下面讨论 R-模范畴 $\mathscr{M}_R$ 的 Hom 函子，这是一类特别重要的 Hom 函子.

设 R 是环，M 是 R-模. 对于每个 R-模 A，$\mathrm{Hom}_R(M,A)$ 是一个 R-模. 函子 $\mathrm{Hom}_R(M,-)$ 将每个 R-模同态 $f:A\to B$ 对应于 $f^*=\mathrm{Hom}_R(M,f):\mathrm{Hom}_R(M,A)\to\mathrm{Hom}_R(M,B)$. f^* 还是 R-模同态. 事实上，对于任意 $g,h\in\mathrm{Hom}_R(M,A)$，均有 $f^*(g+h)=f(g+h)=fg+fh=f^*(g)+f^*(h)$；且对于任意 $r\in R$ 和 $g\in\mathrm{Hom}_R(M,A)$，均有 $f^*(rg)=r(fg)=(rf^*)(g)$. 这样，$\mathrm{Hom}_R(M,-)$ 是一个从 $\mathscr{M}_R$ 到自身的共变函子. 类似地可证，$\mathrm{Hom}_R(-,M)$ 是一个从 $\mathscr{M}_R$ 到自身的反变函子.

R-模范畴的 Hom 函子 $\mathrm{Hom}_R(M,-)$ 和 $\mathrm{Hom}_R(-,M)$ 还保持 R-模同态的加法和 R-模运算，也就是说，对于任意 R-模 A

和 B；$f,g\in \mathrm{Hom}_R(A,B)$，以及 $r\in R$，均有

$$(f+g)^*=f^*+g^*,\ (rf)^*=rf^*;$$
$$(f+g)_*=f_*+g_*,\ (rf)_*=rf_*.$$

事实上，对于任意 $h\in \mathrm{Hom}_R(M,A)$和 $k\in \mathrm{Hom}_R(B,M)$，均有 $(f+g)^*(h)=(f+g)h=fh+gh=f^*(h)+g^*(h)=(f^*+g^*)(h)$，$(rf)^*(h)=(rf)h=(rf^*)(h)$，$(f+g)_*(k)=k(f+g)=(f_*+g_*)(h)$，和$(rf)_*(k)=k(rf)=(rf_*)(k)$. 所以，Hom 函子 $\mathrm{Hom}_R(M,-)$和 $\mathrm{Hom}_R(-,M)$分别给出了 R-模同态

$$\mathrm{Hom}_R(A,B)\to \mathrm{Hom}_R(\mathrm{Hom}_R(M,A),\mathrm{Hom}_R(M,B));f\mapsto f^*,$$
$$\mathrm{Hom}_R(A,B)\to \mathrm{Hom}_R(\mathrm{Hom}_R(B,M),\mathrm{Hom}_R(A,M));f\mapsto f_*.$$

特别地，当 $M={}_RR$ 时，对于每个 R-模A，记 $A^*=\mathrm{Hom}_R(A,R)$，叫做 A 的**对偶模**，这是线性代数中域上线性空间 V 的对偶空间 V^* 的自然推广，且称 $D=\mathrm{Hom}_R(-,R):\mathscr{M}_R\to\mathscr{M}_R$ 为 $\mathscr{M}_R$ 的**对偶函子**，这是一个反变函子. D 与 D 的合成，记作 D^2，是一个共变函子，叫做 $\mathscr{M}_R$ 的**双对偶函子**. D^2 将每个 R-模 A 对应到 $A^{**}=\mathrm{Hom}_R(A^*,R)$，且将每个 R-模同态 $f:A\to B$ 对应到 R-模同态 $D^2(f):A^{**}\to B^{**}$. 对于每个 R-模A 和$a\in A$，映射

$$\eta_A(a):A^*\to R;\ f\mapsto f(a)$$

是 R-模同态，进而可定义 R-模同态

$$\eta_A:A\to A^{**};\ a\mapsto \eta_A(a).$$

并且，对于任意 R-模同态$f:A\to B$，均有下图交换：

$$\begin{tikzcd}
A \arrow[r, "\eta_A"] \arrow[d, "f"'] & A^{**} \arrow[d, "D^2(f)"] \\
B \arrow[r, "\eta_B"] & B^{**}
\end{tikzcd}.$$

这是因为，对于任意 $a\in A$ 和 $g\in B^*$，均有 $((\eta_B f)(a))(g)=(\eta_B(f(a))(g)=g(f(a))$ 和 $((D^2(f)\eta_A)(a))(g)=(D^2(f)(\eta_A(a)))(g)=((\eta_A(a))f_*)(g)=(\eta_A(a))(f_*(g))=(\eta_A(a))(gf)=(gf)(a)=g(f(a))$. 所以 $\eta_B f=D^2(f)\eta_A$.

上述交换图给出了 $\mathscr{M}_R$ 的恒等函子与双对偶函子 D^2 之间的自然联系，这种联系具有一般性.

1.3.3 自然变换

设 F,G 是从范畴 $\mathscr{C}$ 到 $\mathscr{D}$ 的共变函子，从函子 F 到 G 的一个**自然变换** $\eta:F\to G$ 是：对于每个 $A\in\mathrm{ob}\mathscr{C}$ 有一个 $\eta_A\in\mathrm{Hom}_{\mathscr{D}}(FA,GA)$ 与之对应，并且对于任意 $A,B\in\mathrm{ob}\mathscr{C}$ 和 $f\in\mathrm{Hom}_{\mathscr{C}}(A,B)$，均有下图交换：

$$\begin{tikzcd}
FA \arrow[r, "\eta_A"] \arrow[d, "F(f)"'] & GA \arrow[d, "G(f)"] \\
FB \arrow[r, "\eta_B"] & GB
\end{tikzcd}.$$

又若每个 η_A，$A\in\mathrm{ob}\mathscr{C}$，均是同构态射，则称 $\eta:F\to G$ 是一个**自然同构**，也称函子 F 与 G 自然同构，记作 $F\simeq G$. 类似地，可定义两个反变函子间的自然变换和自然同构.

前面给出 R-模范畴 $\mathscr{M}_R$ 的恒等函子 1 与双对偶函子 D^2 间的联系 $\eta:A\mapsto\eta_A$，$A\in\mathrm{ob}\mathscr{M}_R$，就是一个典型的自然变换 $\eta:1\to D^2$.

设 $\mathscr{C}$ 是域 k 上的所有有限维线性空间构成的范畴，其态射是 k-线性映射. 对于每个 $V\in\mathrm{ob}\mathscr{C}$，$\eta_V:V\to V^{**}$ 是 k-线性空间同构，从而 $\eta:1_{\mathscr{C}}\to D^2$ 是自然同构.

1.3.4　范畴的等价

现在讨论范畴之间的关系. 称范畴 $\mathscr{C}$ 与 $\mathscr{D}$ 是**同构**的, 记作 $\mathscr{C}\simeq\mathscr{D}$, 如果存在函子 $F:\mathscr{C}\to\mathscr{D}$ 和 $G:\mathscr{D}\to\mathscr{C}$, 使得 $GF=1_{\mathscr{C}}$ 且 $FG=1_{\mathscr{D}}$. 例如, Abel 群范畴与 $\mathbb{Z}$-模范畴是同构的.

范畴的同构是相当强的限制条件, 以至于在多数情况下可将两个同构的范畴等同起来. 范畴间的一种适用范围更广的关系是如下定义的重要关系:称范畴 $\mathscr{C}$ 与 $\mathscr{D}$ 是(自然)**等价**的, 记作 $\mathscr{C}\sim\mathscr{D}$, 如果存在函子 $F:\mathscr{C}\to\mathscr{D}$ 和 $G:\mathscr{D}\to\mathscr{C}$, 使得

$$GF\simeq 1_{\mathscr{C}},\quad FG\simeq 1_{\mathscr{D}}.$$

容易验证, 范畴的等价满足反身性、对称性和传递性, 从而是一个等价关系. 同构的范畴是等价的, 反之未必(习题 1.3.6).

范畴等价的典型例子将在第 3 章 3.5 节中介绍.

习　题　1.3

1. 试确定集合范畴 $\mathscr{Set}$ 中对象的积和余积(提示:考虑笛卡尔积和不交并).

2. 试确定交换环范畴 $\mathscr{CR}$ 中集合 X 上的自由对象(提示:考虑 $\mathbb{Z}$ 上以 X 为不定元集的多项式环).

3. 设 G 是群, $G^{ab}=G/G'$, 其中 G'是G 的换位子群. 若 $f:G\to H$ 是群同态, 则 f 诱导出群同态$\bar{f}:G^{ab}\to H^{ab}$. 验证: 由此可定义 Abel 化函子 $ab:\mathscr{G}\to\mathscr{G}$; 并且自然同态 $\nu_G:G\to G^{ab}$ 导出恒等函子 $1_{\mathscr{G}}$ 到 ab 的一个自然变换 $\nu:1_{\mathscr{G}}\to ab$.

4. 设 GL_n, $n\geqslant 1$, 是从交换环范畴 $\mathscr{CR}$ 到群范畴 $\mathscr{G}$ 的函子, 它将每个环 R 对应到 $GL_n(R)$, 是 R 上的 n 阶可逆方阵构成的群(叫做 R 上的 n 阶一般线性群). 证明: 行列式导出一个自然变换 $det:GL_n\to GL_1$.

5. 设 R 是交换环. 证明: R-模范畴 $\mathscr{M}_R$ 的恒等函子与 Hom

函子 $\mathrm{Hom}_R(R, -)$ 自然同构.

6. 设 $\mathscr{C}$ 是一个范畴, $\mathscr{D}$ 是以 ob $\mathscr{C}$ 关于对象的同构关系的一个完全代表元类为对象类的 $\mathscr{C}$ 的全子范畴, 叫做 $\mathscr{C}$ 的**骨架子范畴**. 证明: $\mathscr{D}$ 与 $\mathscr{C}$ 等价; 但是, 一般地 $\mathscr{D}$ 与 $\mathscr{C}$ 不同构.

第2章 模论初步

2.1 正合列和 Hom 函子

2.1.1 正合列和短五引理

R-模同态序列

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \longrightarrow \cdots \longrightarrow M_{n-1} \xrightarrow{f_n} M_n$$

叫做一个**正合列**，如果 $\mathrm{Im}f_i = \mathrm{Ker}f_{i+1}, i = 1, 2, \cdots, n-1$；也称上述序列**在 M_i 处正合**，$i = 1, 2, \cdots, n-1$. 而形如

$$0 \to A \to B \to C \to 0$$

的 R-模正合列叫做**短正合列**.

例 (1) R-模同态 $f: A \to B$ 是满的当且仅当 R-模同态序列 $A \xrightarrow{f} B \longrightarrow 0$ 正合；此时有短正合列

$$0 \longrightarrow \mathrm{Ker}f \xrightarrow{\tau} A \xrightarrow{f} B \longrightarrow 0,$$

其中 τ 是嵌入映射. 而 R-模同态 $g: A \to B$ 是单的当且仅当 R-模同态序列 $0 \longrightarrow A \xrightarrow{g} B$ 正合；此时有短正合列

$$0 \longrightarrow A \xrightarrow{g} B \xrightarrow{v} \mathrm{Coker}g \longrightarrow 0,$$

其中 $\mathrm{Coker}g = B/\mathrm{Im}g$，叫做 R-同态 $g: A \to B$ 的**余核**，而 v 是 B 到 $B/\mathrm{Im}g$ 的自然 R-同态. 对于任意 R-模同态 $f: A \to B$，均有正合列

$$0 \longrightarrow \mathrm{Ker}f \xrightarrow{\tau} A \xrightarrow{f} B \xrightarrow{v} \mathrm{Coker}f \longrightarrow 0.$$

(2) 对于任意 R-模 A_1 和 A_2，均有短正合列

$$0 \longrightarrow A_1 \xrightarrow{\tau_1} A_1 \oplus A_2 \xrightarrow{\pi_2} A_2 \longrightarrow 0,$$

$$0 \longrightarrow A_2 \xrightarrow{\tau_2} A_1 \oplus A_2 \xrightarrow{\pi_1} A_1 \longrightarrow 0,$$

其中 τ_i 是标准嵌入，π_i 是标准投影.

称由 R-模同态作成的图

$$\begin{tikzcd} A \arrow[r, "h"] \arrow[d, "f"'] & B \arrow[d, "g"] \\ C \arrow[r, "k"] & D \end{tikzcd}$$

是**交换图**，如果 $kf = gh$. 一般地，由 R-模同态作成的图称为是**交换**的，如果组成它的每个形如上图的圈都是交换的.

引理 2.1.1 (蛇形引理) 设有 R-模同态的行正合的交换图

$$\begin{tikzcd} & M' \arrow[r, "\varphi"] \arrow[d, "f'"] & M \arrow[r, "\psi"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "\varphi_1"'] & N \arrow[r, "\psi_1"'] & N'' & \end{tikzcd} \tag{1}$$

则有长正合列

$$\operatorname{Ker} f' \xrightarrow{\varphi_0} \operatorname{Ker} f \xrightarrow{\psi_0} \operatorname{Ker} f'' \xrightarrow{\delta} \operatorname{Coker} f' \xrightarrow{\varphi_2} \operatorname{Coker} f \xrightarrow{\psi_2} \operatorname{Coker} f''. \tag{2}$$

证明 首先，将交换图(1)扩大成图(3)：

$$\begin{tikzcd} & \operatorname{Ker} f' \arrow[r, "\varphi_0"] \arrow[d, "\tau'"] & \operatorname{Ker} f \arrow[r, "\psi_0"] \arrow[d, "\tau"] & \operatorname{Ker} f'' \arrow[d, "\tau''"] & \\ & M' \arrow[r, "\varphi"] \arrow[d, "f'"] & M \arrow[r, "\psi"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "\varphi_1"] \arrow[d, "\nu'"] & N \arrow[r, "\psi_1"] \arrow[d, "\nu"] & N'' \arrow[d, "\nu''"] & \\ & \operatorname{Coker} f' \arrow[r, "\varphi_2"] & \operatorname{Coker} f \arrow[r, "\psi_2"] & \operatorname{Coker} f'' & \end{tikzcd} \tag{3}$$

,

其中 τ', τ, τ'' 是嵌入映射; v', v, v'' 是自然 R-同态. 由于 $f\varphi(\mathrm{Ker}f')=\varphi_1 f'(\mathrm{Ker}f')=0$, 故 $\varphi(\mathrm{Ker}f')\subseteq\mathrm{Ker}f$. 令 φ_0 为 φ 在 $\mathrm{Ker}f'$ 上的限制, 同理可令 ψ_0 是 ψ 在 $\mathrm{Ker}f$ 上的限制. 这样图(3)中的上面两个圈是交换的. 又由于 $\varphi_1(\mathrm{Im}f')\subseteq\mathrm{Im}f$, 这诱导出 R-同态 $\varphi_2:\mathrm{Coker}f'\to\mathrm{Coker}f$. 同理由 ψ_1 可诱导出 R-同态 $\psi_2:\mathrm{Coker}f\to\mathrm{Coker}f''$. 这样图(3)中的下面两个圈也是交换的. 所以图(3)是交换的.

图(3)的上行是正合的: 因为 $\psi\varphi=0$, 由限制映射的定义, $\psi_0\varphi_0=0$, 即有 $\mathrm{Im}\varphi_0\subseteq\mathrm{Ker}\psi_0$. 设 $x\in\mathrm{Ker}\psi_0$, 则 $\psi(x)=0$. 由图(1)中上行的正合性, 存在 $x'\in M'$ 使得 $\varphi(x')=x$. 又由于 $\varphi_1 f'(x')=f\varphi(x')=f(x)=0$ 以及 φ_1 是单的, $f'(x')=0$, 故 $x'\in\mathrm{Ker}f'$. 这样, $\varphi_0(x')=\varphi(x')=x$. 所以, $\mathrm{Ker}\psi_0\subseteq\mathrm{Im}\varphi_0$.

图(3)的底行是正合的: 因为 $\psi_1\varphi_1=0$, 由诱导映射的定义, $\psi_2\varphi_2=0$, 即有 $\mathrm{Im}\varphi_2\subseteq\mathrm{Ker}\psi_2$. 设 $\bar{y}=y+\mathrm{Im}f\in\mathrm{Ker}\psi_2$, 其中 $y\in N$, 则 $\psi_2(\bar{y})=\overline{\psi_1(y)}=0$. 于是 $\psi_1(y)\in\mathrm{Im}f''$, 从而存在 $x''\in M''$使得 $f''(x'')=\psi_1(y)$. 又由于 ψ 是满的, 存在 $x\in M$ 使得 $\psi(x)=x''$. 令 $z=f(x)-y\in N$, 则 $v(z)=\bar{z}=\bar{y}=v(y)$, 并且 $\psi_1(z)=\psi_1 f(x)-\psi_1(y)=f''\psi(x)-\psi_1(y)=\psi_1(y)-\psi_1(y)=0$, 于是 $z\in\mathrm{Ker}\psi_1=\mathrm{Im}\varphi_1$, 因而存在 $z'\in N'$使得 $\varphi_1(z')=z$, 且 $\varphi_2 v'(z')=\varphi_2(\bar{z}')=\overline{\varphi_1(z')}=\bar{z}=\bar{y}$, 从而 $\bar{y}\in\mathrm{Im}\varphi_2$. 所以 $\mathrm{Ker}\psi_2\subseteq\mathrm{Im}\varphi_2$.

现在构作序列(2)中从 $\mathrm{Ker}f''$ 到 $\mathrm{Coker}f'$ 的连接同态 δ. 设 $x''\in\mathrm{Ker}f''$, 由于 ψ 是满射, 存在 $x\in M$ 使得 $\psi(x)=x''$. 又由于 $\psi_1 f(x)=f''\psi(x)=f''(x'')=0$, 故 $f(x)\in\mathrm{Ker}\psi_1=\mathrm{Im}\varphi_1$. 因 φ_1 是单射, 存在唯一的 $x'\in N'$ 使得 $\varphi_1(x')=f(x)$. 令 $\delta(x'')=v'(x')=x'+\mathrm{Im}f'$. 下面验证 $\delta(x'')$与上面的 $x\in M$ 的选择无

关：又若 $y\in M$ 使得 $\psi(y)=x''$，令 $y'=\varphi_1^{-1}f(y)$，则 $x-y\in \mathrm{Ker}\psi=\mathrm{Im}\varphi$，进而存在 $z'\in M'$ 使得 $\varphi(z')=x-y$. 于是 $\varphi_1 f'(z')=f\varphi(z')=f(x-y)=f(x)-f(y)$，从而 $x'-y'=\varphi_1^{-1}f(x)-\varphi_1^{-1}f(y)=f'(z')\in \mathrm{Im}f'$，即有 $v'(x')=v'(y')$. 不难验证 δ 是 R-同态.

序列(2)在 $\mathrm{Ker}f''$ 处正合：由 δ 的定义可知 $\delta\psi_0=0$. 又设 $x''\in\mathrm{Ker}\delta$，则存在 $x\in M$ 使得 $\psi(x)=x''$，且有 $\delta(x'')=v'\varphi_1^{-1}f(x)=0$. 于是 $x'=\varphi_1^{-1}f(x)\in\mathrm{Im}f'$，故存在 $y'\in M'$ 使得 $f'(y')=x'$. 令 $y=x-\varphi(y')$，则 $f(y)=f(x)-f\varphi(y')=f(x)-\varphi_1 f'(y')=f(x)-\varphi_1(x')=0$，即 $y\in\mathrm{Ker}f$，且有 $\psi_0(y)=\psi(y)=\psi(x)-\psi\varphi(y')=\psi(x)=x''$，所以 $\mathrm{Ker}\delta\subseteq\mathrm{Im}\psi_0$.

序列(2)在 $\mathrm{Coker}f'$ 处正合：由 δ 的定义可知 $\varphi_2\delta=0$. 设 $\bar{x}'\in\mathrm{Ker}\varphi_2$，其中 $x'\in N'$，则 $\varphi_2(\bar{x}')=\overline{\varphi_1(x')}=0$，从而 $\varphi_1(x')\in\mathrm{Im}f$. 于是存在 $x\in M$ 使得 $f(x)=\varphi_1(x')$. 由于 $f''\psi(x)=\psi_1 f(x)=\psi_1\varphi_1(x')=0$，故存在 $x''=\psi(x)\in\mathrm{Ker}f''$ 使得 $\delta(x'')=\bar{x}'$. 所以 $\mathrm{Ker}\varphi_2\subseteq\mathrm{Im}\delta$.

综上，序列(2)是正合的. □

上述引理的证明方法通常称为**图追踪法**.

引理 2.1.2 (短五引理) 在引理 2.1.1 的条件下

(1) 若 f' 和 f'' 是 R-单同态，则 f 也是 R-单同态.

(2) 若 f' 和 f'' 是 R-满同态，则 f 也是 R-满同态.

(3) 若 f' 和 f'' 是 R-同构，则 f 也是 R-同构.

证明 由引理 2.1.1 的正合列(2)立得(1)和(2)，进而(3)成立. □

定理 2.1.3 设 $0\longrightarrow M_1\xrightarrow{f}M\xrightarrow{g}M_2\longrightarrow 0$ 是 R-模同态的短正合列，则下列条件等价：

(1) 存在 R-同态 $h:M_2\to M$ 使得 $gh=1_{M_2}$;

(2) 存在 R-同态 $k:M\to M_1$ 使得 $kf=1_{M_1}$;

(3) 存在 R-同构 $\varphi:M_1\oplus M_2\to M$,使得下图交换:

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\tau_1"] \arrow[d, "1"] & M_1\oplus M_2 \arrow[r, "\pi_2"] \arrow[d, "\varphi"] & M_2 \arrow[r] \arrow[d, "1"] & 0 \\ 0 \arrow[r] & M_1 \arrow[r, "f"] & M \arrow[r, "g"] & M_2 \arrow[r] & 0 \end{tikzcd},$$

其中 τ_1 是标准嵌入,π_2 是标准投影.

证明 (1)⇒(3):令 $\varphi:M_1\oplus M_2\to M$;$(x_1,x_2)\mapsto f(x_1)+h(x_2)$,则 φ 是R-同态,且使(3)中的图交换,再由短五引理,φ 是R-同构.

(2)⇒(3):令 ψ: $M\to M_1\oplus M_2$;$x\mapsto(k(x),g(x))$,则 ψ 是 R-同态,且使下图交换:

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "f"] \arrow[d, "1"] & M \arrow[r, "g"] \arrow[d, "\psi"] & M_2 \arrow[r] \arrow[d, "1"] & 0 \\ 0 \arrow[r] & M_1 \arrow[r, "\tau_1"] & M_1\oplus M_2 \arrow[r, "\pi_2"] & M_2 \arrow[r] & 0 \end{tikzcd}.$$

由短五引理,ψ 是R-同构. 令 $\varphi=\psi^{-1}$,即为所求.

(3)⇒(1)和(2):令 $h=\varphi\tau_2$ 和 $k=\pi_1\varphi^{-1}$,其中 τ_2 和 π_1 分别是 $M_1\oplus M_2$ 的标准嵌入和标准投影. 不难验证,h 和 k 即为所求. □

R-模同态的短正合列 $0\longrightarrow M_1\xrightarrow{f}M\xrightarrow{g}M_2\longrightarrow 0$ 称为**可裂(分裂)**的,如果它满足定理 2.1.3 中的条件(1),(2)或(3),此时有 $M\simeq M_1\oplus M_2$. 但是仅由 $M\simeq M_1\oplus M_2$ 还推不出上述正合列是可裂的(习题 2.1.4).

2.1.2 Hom 函子的基本性质

R-模范畴的 Hom 函子具有下述定理给出的**左正合性**.

定理 2.1.4 (1) R-模同态序列 ε: $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ 是正合的当且仅当对于每个 R-模 M, R-模序列 $\mathrm{Hom}_R(M,\varepsilon)$:

$$0 \longrightarrow \mathrm{Hom}_R(M,A) \xrightarrow{f^*} \mathrm{Hom}_R(M,B) \xrightarrow{g^*} \mathrm{Hom}_R(M,C)$$

都是正合的.

(2) R-模同态序列 ε': $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ 是正合的当且仅当对于每个 R-模 M, R-模序列 $\mathrm{Hom}_R(\varepsilon',M)$:

$$0 \longrightarrow \mathrm{Hom}_R(C,M) \xrightarrow{g_*} \mathrm{Hom}_R(B,M) \xrightarrow{f_*} \mathrm{Hom}_R(A,M)$$

都是正合的.

证明 (1) 设序列 ε 是正合的, M 是一个 R-模. 对于任意 $h \in \mathrm{Hom}_R(M,A)$, 若 $f^*(h)=fh=0$, 由于 f 是单射, 则有 $h=0$, 所以 f^* 是单射. 又由于 $gf=0$, $g^*f^*=(gf)^*=0$, 从而 $\mathrm{Im}\, f^* \subseteq \mathrm{Ker} g^*$. 又设 $k \in \mathrm{Ker} g^*$, 则 $g^*(k)=gk=0$, 于是 $\mathrm{Im} k \subseteq \mathrm{Ker} g=\mathrm{Im} f$, 由于 f 是单射, $f: A \to \mathrm{Im} f$ 是 R-同构. 令 $h \in \mathrm{Hom}_R(M,A)$ 是下列 R-同态的合成:

$$M \xrightarrow{k} \mathrm{Im}\, k \xrightarrow{\subseteq} \mathrm{Ker}\, g = \mathrm{Im}\, f \xrightarrow{f^{-1}} A,$$

则 $f^*(h)=fh=k$. 所以 $\mathrm{Ker} g^* \subseteq \mathrm{Im} f^*$, 从而序列 $\mathrm{Hom}_R(M,\varepsilon)$ 正合.

反之, 令 $M=\mathrm{Ker} f$, $\tau: M \to A$ 为包含映射. 由序列 $\mathrm{Hom}_R(M,\varepsilon)$ 的正合性, f^* 是单射, 而 $f^*(\tau)=f\tau=0$, 所以 $\tau=0$. 于是 $M=\mathrm{Ker} f=0$, 即 f 是单射. 再取 $M=A$, 由序列 $\mathrm{Hom}_R(M,\varepsilon)$ 的正合性, $0=g^*f^*(1_A)=gf1_A=gf$, 所以 $\mathrm{Im} f \subseteq \mathrm{Ker} g$. 最后取 $M=\mathrm{Ker} g$, $\tau: M \to B$ 为包含映射, 则 $g^*(\tau)=g\tau=0$. 由于 $\mathrm{Ker} g^*=\mathrm{Im} f^*$, 存在 $h \in \mathrm{Hom}_R(M,A)$ 使得 $f^*(h)=fh=\tau$. 于是对于每个 $x \in M=\mathrm{Ker} g$, 均有 $x=\tau(x)=fh(x) \in \mathrm{Im} f$, 从而 $\mathrm{Ker} g \subseteq \mathrm{Im} f$. 所以序列 ε 是正合的.

(2) 可仿(1)对偶地证明. □

一般地, Hom 函子未必有右正合性(习题 2.1.5).

Hom 函子还保持 R-模的有限直和.

定理 2.1.5　设 $M, A_1, A_2, \cdots, A_n$ 是 R-模, 则有 R-模同构

$$\mathrm{Hom}_R(M, \bigoplus_{i=1}^{n} A_i) \simeq \bigoplus_{i=1}^{n} \mathrm{Hom}_R(M, A_i);$$

$$\mathrm{Hom}_R(\bigoplus_{i=1}^{n} A_i, M) \simeq \bigoplus_{i=1}^{n} \mathrm{Hom}_R(A_i, M).$$

证明　分别将 Hom 函子 $\mathrm{Hom}_R(M, -)$ 和 $\mathrm{Hom}_R(-, M)$ 作用于 $\bigoplus_{i=1}^{n} A_i$ 的标准嵌入 τ_i 和标准投影 π_i 上, 再由定理 1.2.9 立得所需同构. □

Hom 函子也保持可裂正合列.

定理 2.1.6　对于任意 R-模同态序列 ε: $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$, 下列条件等价:

(1) 序列 ε: $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ 是可裂正合列;

(2) 对于任意 R-模 M, 序列 $\mathrm{Hom}_R(M, \varepsilon)$:

$$0 \longrightarrow \mathrm{Hom}_R(M, A) \xrightarrow{f^*} \mathrm{Hom}_R(M, B) \xrightarrow{g^*} \mathrm{Hom}_R(M, C) \longrightarrow 0$$

是可裂正合列;

(3) 对于任意 R-模 M, 序列 $\mathrm{Hom}_R(\varepsilon, M)$:

$$0 \longrightarrow \mathrm{Hom}_R(C, M) \xrightarrow{g_*} \mathrm{Hom}_R(B, M) \xrightarrow{f_*} \mathrm{Hom}_R(A, M) \longrightarrow 0$$

是可裂正合列.

证明　(1)⇒(2): 由定义, 存在 $h \in \mathrm{Hom}_R(C, B)$ 使得 $gh = 1_C$, 从而 $g^* h^* = (gh)^* = 1_{\mathrm{Hom}_R(M,C)}$, 故 g^* 是满射. 再由定理 2.1.3 和定理 2.1.4, 序列 $\mathrm{Hom}_R(M, \varepsilon)$是正合的, 且是可裂的.

(2)⇒(1): 取 $M = C$, 则存在 R-同态 φ: $\mathrm{Hom}_R(M, C) \to \mathrm{Hom}_R(M, B)$使得 $g^* \varphi = 1_{\mathrm{Hom}_R(M,C)}$. 令 $h = \varphi(1_C) \in \mathrm{Hom}_R(C, B)$, 则 $gh = g^* \varphi(1_C) = 1_{\mathrm{Hom}_R(C,C)}(1_C) = 1_C$, 从而 g 是满射, 由

定理2.1.3和定理2.1.4，序列 ε 正合且可裂.

对偶地可证(1)$\Leftrightarrow$(3). □

习 题 2.1

1. 设 $0 \longrightarrow A \longrightarrow B \xrightarrow{f} C \longrightarrow 0$ 和 $0 \longrightarrow C \xrightarrow{g} D \longrightarrow E \longrightarrow 0$ 是 R-模短正合列. 证明它们可粘接成正合列: $0 \longrightarrow A \longrightarrow B \xrightarrow{gf} D \longrightarrow E \longrightarrow 0$.

2. (**五引理**) 设有 R-模同态的行正合的交换图

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[d, "h_1"] & A_2 \arrow[r] \arrow[d, "h_2"] & A_3 \arrow[r] \arrow[d, "h_3"] & A_4 \arrow[r] \arrow[d, "h_4"] & A_5 \arrow[d, "h_5"] \\
B_1 \arrow[r] & B_2 \arrow[r] & B_3 \arrow[r] & B_4 \arrow[r] & B_5
\end{tikzcd}.$$

证明: (1) 若 h_1 是满的，且 h_2，h_4 是单的，则 h_3 是单的.

(2) 若 h_5 是单的，且 h_2，h_4 是满的，则 h_3 是满的.

3. 设有 R-模同态的交换图:

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[d, "h_1"] & A_2 \arrow[r] \arrow[d, "h_2"] & \cdots \arrow[r] & A_{n-1} \arrow[r] \arrow[d, "h_{n-1}"] & A_n \arrow[d, "h_n"] \\
B_1 \arrow[r] & B_2 \arrow[r] & \cdots \arrow[r] & B_{n-1} \arrow[r] & B_n
\end{tikzcd},$$

其中 $h_1,\cdots,h_n$ 均是 R-同构. 证明: 在上图的两行序列之中，若一行是正合的，则另一行也是正合的.

4. 证明: R-模短正合列 $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ 是可裂的$\Leftrightarrow \operatorname{Im} f$ 是 B 的直和项. 试给出一个 R-模短正合列 $0 \longrightarrow A \xrightarrow{f} A \oplus B \xrightarrow{g} B \longrightarrow 0$，它不是可裂的.

5. 在 $\mathbb{Z}$-模范畴中，证明:

(1) $\mathbb{Z} \xrightarrow{\nu} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$ 是正合的，但 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \xrightarrow{\nu^*} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \longrightarrow 0$ 不是正合的，其中 ν 是自然满同态.

(2) $0 \longrightarrow \mathbb{Z} \xrightarrow{i} \mathbb{Q}$ 是正合的，但 $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \xrightarrow{i_*} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow 0$ 不是正合的，其中 i 是包含映射.

6. 设 M_i, N 是 R-模, $i\in I$, 证明:

(1) $\mathrm{Hom}_R(\bigoplus_{i\in I}M_i, N)\simeq\prod_{i\in I}\mathrm{Hom}_R(M_i, N)$.

(2) $\mathrm{Hom}_R(N, \prod_{i\in I}M_i)\simeq\prod_{i\in I}\mathrm{Hom}_R(N, M_i)$.

2.2 自由模

我们知道,模是线性空间的一种推广. 线性代数中的许多概念可不同程度地推广到模上去.

设 M 是 R-模, M 的子集 S 称为是 R-**线性相关**的,如果存在 $x_1,\cdots,x_n\in S$ 和不全为零的 $r_1,\cdots,r_n\in R$, 使得 $r_1x_1+\cdots+r_nx_n=0$; 否则, 称 S 是 R-**线性无关**的, 也就是说, 对于 S 中的任意 n 个元素 $x_1,\cdots,x_n$, 以及 $r_1,\cdots,r_n\in R$, 只要 $\sum_{i=1}^{n}r_ix_i=0$, 就有 $r_1=\cdots=r_n=0$. 称 M 的子集 X 是 M 的一个**基**, 如果 X 是 R-线性无关的, 且 X 生成 M; 这等价于说, M 中的每个元素 x 可表示成 X 中有限个元素的 R-线性组合, 且这种表示法是唯一的. 具有基的 R-模叫做**自由** R-**模**. 例如, 环 R 作为自身上的模 ${}_RR$ 是自由 R-模,有基 $\{1_R\}$.

设 F 是具有基 X 的自由 R-模. 由基的定义可知, F 是循环子模 Rx, $x\in X$, 的直和 $F=\bigoplus_{x\in X}Rx$, 并且 $Rx\simeq{}_RR$, 从而 $F\simeq\bigoplus_{x\in X}{}_RR$(外直和). 另一方面, 对于任意非空集合 X, 直和 $\bigoplus_{x\in X}{}_RR$ 是自由 R-模, 具有基 $\{\tau_x(1_R)\mid x\in X\}$, 其中 τ_x 是 ${}_RR$ 到 $\bigoplus_{x\in X}{}_RR$ 的标准嵌入.

自由模具有下述泛性.

定理 2.2.1 设 F 是具有基 X 的自由 R-模, $\tau: X\to F$ 为包含映射, 则对于任意 R-模 M 和映射 $f: X\to M$, 存在唯一的 R-同态 $h: F\to M$ 使得 $h\tau=f$, 即有交换图

$$\begin{tikzcd} X \arrow[r, "\tau"] \arrow[dr, "f"'] & F \arrow[d, "h"] \\ & M \end{tikzcd}.$$

证明 对于任意 $y \in F$，y 可唯一地表示成 $y = \sum_{x \in X} r_x x$，$r_x \in R$，$x \in X$；令 $h(y) = \sum_{x \in X} r_x f(x)$，则 $h: F \to M$ 是 R-同态，且有 $h\tau = f$. 又若 R-同态 $h': F \to M$ 也使得 $h'\tau = f$，则对于每个 $y = \sum_{x \in X} r_x x \in F$，均有 $h'(y) = \sum_{x \in X} r_x h'\tau(x) = \sum_{x \in X} r_x f(x) = \sum_{x \in X} r_x h\tau(x) = h(y)$. 所以 $h' = h$. 这证明了 h 的唯一性. □

这样，每个自由 R-模均是 R-模范畴 $\mathscr{M}_R$ 中的自由对象. 反之，若 τ: $X \to F$ 是 $\mathscr{M}_R$ 中的自由对象，则 F 是以 $\tau(X)$ 为基的自由 R-模. 这是因为，由定理 2.2.1，映射 $\tau': X \to \bigoplus_{x \in X} R; x \mapsto \tau_x(1_R)$ 也是 X 上的自由对象，因而存在唯一的 R-同构 $h: F \to \bigoplus_{x \in X} R$，使得 $h\tau = \tau'$，所以 F 是自由的，具有基 $\tau(X)$. 此时 τ: $X \to F$ 必是单射.

由自由模的泛性立得

命题 2.2.2 *每个 R-模均是一个自由 R-模的 R-同态像.* □

一般地，R-模未必是自由的. 但有

命题 2.2.3 *每个域上的模均是自由的.*

证明 首先，利用 Zorn 引理可证，域 k 上的模 M 含有极大 k-线性无关组 X，进而可证 X 就是 M 的基. □

注 约定零 R-模是自由的，其基为空集.

一个自由 R-模可以有许多不同的基，下面要证它们具有相同的势.

命题 2.2.4 *若 R-模 M 具有无限基 X，则 M 的任意基 Y 的势 $|Y| = |X|$.*

证明 首先证明 $|Y|$ 是无限的. 假定 $|Y|$ 有限，则 Y 可由 X

中的一个有限子集X_0来R-线性表示，而$X\backslash X_0(\neq\varnothing)$中的元素可由$Y$，从而可由$X_0$来$R$-线性表示，这与$X$是$R$-线性无关的条件矛盾. 所以$|Y|$无限.

对于每个$x\in X$，x可唯一地表示成$x=\sum\limits_{i=1}^{n}r_iy_i$，其中$r_i\in R\backslash\{0\}$，$y_i\in Y$，$i=1,\cdots,n$. 令$\varphi:x\mapsto(y_1,y_2,\cdots,y_n)\in Y^n$，其中$Y^n$是$n$个$Y$的笛卡尔积. 从而有映射$\varphi$: $X\to\bigcup\limits_{n\in\mathbb{N}}Y^n$.

对于任意$(y_1,\cdots,y_n)\in Y^n$，$X_1=\varphi^{-1}((y_1,\cdots,y_n))$是有限集. 这是因为，$\{y_1,\cdots,y_n\}$可由$X$中的有限子集$X_0$来$R$-线性表示，而$X_1$可由$\{y_1,\cdots,y_n\}$，从而可由$X_0$来$R$-线性表示. 假如$X_1$是无限的，则$X_1\backslash X_0(\neq\varnothing)$可由$X_0$来$R$-线性表示，这与$X$是基的条件矛盾，所以$X_1$是有限集.

对于每个$y\in\mathrm{Im}\varphi$，将$\varphi^{-1}(y)$中的有限个元素排定一个次序：$\varphi^{-1}(y)=\{x_1,\cdots,x_n\}$. 令$\psi(x_i)=(y,i)\in\bigcup\limits_{i=1}^{\infty}(Y^n\times\mathbb{N})$，这将$\varphi$改造成一个单射$\psi$: $X\to\bigcup\limits_{i=1}^{\infty}(Y^n\times\mathbb{N})$. 由于$|Y|$是无限的，$|X|\leqslant|\bigcup\limits_{i=1}^{\infty}(Y^n\times\mathbb{N})|=|\bigcup\limits_{i=1}^{\infty}Y^n|\cdot|\mathbb{N}|=|Y|\cdot|\mathbb{N}|=|Y|$. 对称地，可证$|Y|\leqslant|X|$. 所以$|X|=|Y|$. □

再考虑具有有限基的R-模，由命题2.2.4，它的任一基都是有限的. 这样，线性代数中的矩阵和行列式方法可用来研究具有有限基的R-模.

设$X=\{x_1,\cdots,x_m\}$和$Y=\{y_1,\cdots,y_n\}$是R-模M的两个有限基. 假如$m\neq n$，不妨设$m<n$. 由于X可由Y来R-线性表示，存在R上的$n\times m$矩阵A，使得$\{x_1,\cdots,x_m\}=\{y_1,\cdots,y_n\}A$. 同理，存在$R$上的$m\times n$矩阵$B$，使得$\{y_1,\cdots,y_n\}=\{x_1,\cdots,x_m\}B$. 于是$\{y_1,\cdots,y_n\}=\{y_1,\cdots,y_n\}AB$，从而有$AB=I_n$，为$n$阶单位方阵. 由于$m<n$，将$A$添上$n-m$列0，$B$添上$n-m$

行 0，均凑成 n 阶方阵，则有 $(A\ 0)\binom{B}{0}=I_n$. 两边取行列式，得 $0\cdot 0=1$，这矛盾. 所以 $|X|=m=n=|Y|$. 综合上述命题，即得

定理 2.2.5 设 X 和 Y 是自由 R-模 M 的基，则 $|X|=|Y|$. □

于是，可定义自由 R-模 M 的**秩**，记作 $\operatorname{rank}_R M$，是 M 的任一基 X 的势 $|X|$. 不难验证，两个自由 R-模 M_1 与 M_2 的直和 $M_1\oplus M_2$ 仍是自由的，且

$$\operatorname{rank}_R(M_1\oplus M_2)=\operatorname{rank}_R M_1+\operatorname{rank}_R M_2.$$

习 题 2.2

1. 设 M 是秩为 n 的自由 R-模，$X=\{x_1,\cdots,x_n\}\subseteq M$.

(1) 证明：若 X 是 M 的生成元集，则 X 是 M 的一个基.

(2) 若 X 是 R-线性无关的，X 是否是 M 的基？

2. 自由 R-模的子模、同态像以及直积是否是自由 R-模？

3. 证明：有理数加群 $(\mathbb{Q},+)$ 不是自由 $\mathbb{Z}$-模.

4. 设 R 是(交换)环，M 是 R-模，则 $\operatorname{Hom}_R(M,M)$ 是一个环(一般不是交换环)，叫做 M 的 **R-自同态环**，记作 $\operatorname{End}_R(M)$. 证明：

(1) 若 M 是秩为 n 的自由 R-模，则 $\operatorname{End}_R(M)\simeq \mathrm{M}_n(R)$，$R$ 上的 n 阶全矩阵环.

(2) 若 $\varphi: R\to S$ 是环同态，则 φ 导出环同态：

$$\bar{\varphi}: \mathrm{M}_n(R)\to \mathrm{M}_n(S);\ (a_{ij})\mapsto(\varphi(a_{ij})).$$

5. 设 $f(x_1,\cdots,x_n)$, $g(x_1,\cdots,x_n)\in\mathbb{Z}[x_1,\cdots,x_n]$. 若对于任意 $t_1,\cdots,t_n\in\mathbb{Z}$，均有 $f(t_1,\cdots,t_n)=g(t_1,\cdots,t_n)$，则称 $f(x_1,\cdots,x_n)=g(x_1,\cdots,x_n)$ 是一个**代数恒等式**. 证明：若 $f(x_1,\cdots,x_n)=g(x_1,\cdots,x_n)$ 是一个代数恒等式，则对于任意交换环 R 和 $a_1,\cdots,a_n\in R$，均有 $f(a_1,\cdots,a_n)=g(a_1,\cdots,a_n)$(提

示:利用习题 1.3.2).

6. 试用习题5(代数恒等式方法)证明: 对于任意交换环 R, 均有

(1) $\det A \cdot \det B = \det(AB)$; $A, B \in \mathrm{M}_n(R)$.

(2) (**Cayley-Hamilton 定理**) 若 $A \in \mathrm{M}_n(R)$, $\varphi(\lambda) = \det(\lambda I_n - A) \in R[\lambda]$, 则 $\varphi(A) = 0$.

7. 设 R 是环. 证明: 若每个 R-模均是自由的, 则 R 是域.

2.3 投射模和内射模

R-模 P 称为**投射 R-模**, 如果对于任意 R-模满同态 $f: M \to N$ 和 R-模同态 $g: P \to N$, 存在 R-模同态 $h: P \to M$, 使得 $fh = g$, 即有交换图

$$\begin{tikzcd} & P \arrow[dl, "h"'] \arrow[d, "g"] & \\ M \arrow[r, "f"] & N \arrow[r] & 0 \end{tikzcd} .$$

定理 2.3.1 设 P 为 R-模, 则下列条件等价:

(1) P 是投射 R-模;

(2) 函子 $\mathrm{Hom}_R(P, -)$是**正合的**, 即对于任意 R-模短正合列

$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$, 序列

$$0 \longrightarrow \mathrm{Hom}_R(P, M') \xrightarrow{f^*} \mathrm{Hom}_R(P, M) \xrightarrow{g^*} \mathrm{Hom}_R(P, M'') \longrightarrow 0$$

是正合的;

(3) 每个 R-模短正合列 $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ 都是可裂的, 从而 $M \oplus P \simeq N$;

(4) 存在 R-模 Q, 使得 $P \oplus Q$ 是自由 R-模.

证明 (1)$\Rightarrow$(2): 由定理 2.1.4, 只需证 g^* 是满的. 由于 g 是满的, 对于任意 $f \in \mathrm{Hom}_R(P, M'')$, 由(1),存在 $h \in \mathrm{Hom}_R(P,$

M)，使得 $gh=g^*(h)=f$. 所以 g^* 是满的.

(2)⇒(3)：由于 $g^*:\mathrm{Hom}_R(P,N)\to\mathrm{Hom}_R(P,P)$ 是满的，故存在 $h\in\mathrm{Hom}_R(P,N)$，使得 $g^*(h)=gh=1_P$. 由定理 2.1.3，(3)成立.

(3)⇒(4)：由命题 2.2.2，P 是一个自由 R-模 F 的同态像，从而有短正合列 $0\longrightarrow\mathrm{Ker}f\longrightarrow F\xrightarrow{f}P\longrightarrow 0$. 由(3)和定理 2.1.3，$P\oplus\mathrm{Ker}f\simeq F$.

(4)⇒(1)：设 P 是具有基 X 的自由 R-模 F 的直和项，$\pi:F\to P$ 和 $\tau:P\to F$ 分别是标准投影和标准嵌入，$i:X\to F$ 是包含映射. 若 $f:M\to N$ 是 R-满同态，$g:P\to N$ 是 R-同态，对于每个 $x\in X$，可取定一个 $m_x\in f^{-1}(g\pi(x))\in M$. 令 $j:X\to M;x\mapsto m_x$. 由 F 的泛性，存在 R-同态 $h':F\to M$ 使得 $h'i=j$. 于是对于任意 $y=\sum\limits_{x\in X}r_xx\in F$，$r_x\in R$，均有 $fh'(y)=\sum\limits_{x\in X}r_xfh'(x)=\sum\limits_{x\in X}r_xfj(x)=\sum\limits_{x\in X}r_xf(m_x)=\sum\limits_{x\in X}r_xg\pi(x)=g\pi(y)$. 所以 $fh'=$

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[dd, "j"'] & F \arrow[d, shift right, "\pi"'] \arrow[ddl, "h'"'] & \\
 & P \arrow[u, shift right, "\tau"'] \arrow[d, "g"] \arrow[dl, "h"'] & \\
M \arrow[r, "f"] & N \arrow[r] & 0
\end{tikzcd}$$

$g\pi$. 令 $h=h'\tau$，则 $fh=fh'\tau=g\pi\tau=g1_P=g$. □

由定理 2.3.1 可知，自由 R-模均是投射 R-模，但反之不然. 例如，环 $\mathbb{Z}/6\mathbb{Z}$ 是主理想$(\bar{2})$和$(\bar{3})$的直和，故作为 $\mathbb{Z}/6\mathbb{Z}$-模，$(\bar{2})$ 是投射的，但不是自由的，这是因为非零自由 $\mathbb{Z}/6\mathbb{Z}$-模的元素个数大于或等于 6，而 $|(\bar{2})|=3$.

命题 2.3.2　R-模直和 $P=\bigoplus\limits_{i\in I}P_i$ 是投射 R-模当且仅当每个直和项 P_i，$i\in I$，是投射 R-模.

证明　若 P 是投射的，则 P 是某个自由 R-模 F 的直和项，

从而每个 P_i，$i\in I$，均是 F 的直和项，从而是投射的. 反之，若每个 P_i，$i\in I$，是投射的，则存在 R-模 Q_i 使得 $P_i\oplus Q_i=F_i$ 是自由的. 从而 $P\oplus(\bigoplus_{i\in I}Q_i)\cong\bigoplus_{i\in I}F_i$ 是自由的，所以 P 是投射的. □

若 R-模的直积 $\prod_{i\in I}P_i$ 是投射的，同上可证，每个 P_i，$i\in I$，是投射的. 但投射 R-模 P_i，$i\in I$，的直积未必是投射的(习题 2.6.6).

由上可知，投射模作为自由模的直和项，部分地继承了自由模的泛性，也可以说，具有某种"弱泛性".

下面讨论投射模在 R-模范畴中的对偶概念——内射模.

设 Q 是 R-模，称 Q 是**内射 R-模**，如果对于任意 R-模单同态 $f:M\to N$ 和 R-模同态 $g:M\to Q$，存在 R-模同态 $h:N\to Q$ 使得 $hf=g$，即下图交换：

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & N \arrow[dl, "h"] \\
& Q &
\end{tikzcd}$$

定理 2.3.3 设 Q 为 R-模，则下列条件等价：

(1) Q 是内射 R-模；

(2) 函子 $\mathrm{Hom}_R(-,Q)$ 是**正合**的，即对于任意 R-模短正合列 $0\longrightarrow M'\xrightarrow{f}M\xrightarrow{g}M''\longrightarrow 0$，序列

$$0\longrightarrow \mathrm{Hom}_R(M'',Q)\xrightarrow{g_*}\mathrm{Hom}_R(M,Q)\xrightarrow{f_*}\mathrm{Hom}_R(M',Q)\longrightarrow 0$$

是正合的；

(3) 每个 R-模短正合列 $0\longrightarrow Q\xrightarrow{f}M\xrightarrow{g}N\longrightarrow 0$ 都是可裂的，从而 $Q\oplus N\cong M$；

(4) (**Baer 准则**) 对于 R 的任意理想 I 以及 R-同态 $f:I\to Q$，存在 R-同态 $h:R\to Q$ 使得 h 是 f 的扩张，即 $h|_I=f$.

证明 (1)⇒(2)⇒(3)的证明对偶于定理 2.3.1 的相应

部分.

(3)⇒(4): 令 $W=\{(f(a),-a)\in Q\oplus R\mid a\in I\}$, 则 W 是 $Q\oplus R$ 的子模. 记 $M=(Q\oplus R)/W$, 则有 R-同态 $g:R\to M;\ r\mapsto(0,r)+W$ 和 $j:Q\to M;x\mapsto(x,0)+W$. 设 $i:I\to R$ 为包含映射. 对于任意 $a\in I$, 均有 $jf(a)=(f(a),0)+W=(0,a)+W=gi(a)$. 所以 $jf=gi$, 即有交换图

$$\begin{tikzcd} I \arrow[r, "i"] \arrow[d, "f"'] & R \arrow[d, "g"] \\ Q \arrow[r, "j"'] & M \end{tikzcd}.$$

又由于 j 是单射, 由(3), 短正合列 $0\longrightarrow Q\xrightarrow{j}M\longrightarrow\mathrm{Coker}j\longrightarrow 0$ 是可裂的. 由定理2.1.3, 存在 R-同态 $k:M\to Q$ 使得 $kj=1_Q$. 令 $h=kg$, 则 $hi=kgi=kjf=1_Qf=f$, 即 $h|_I=f$.

(4)⇒(1): 设 $f:M\to N$ 是R-单同态, $g:M\to Q$ 是R-同态. 令

$$S=\{k\in\mathrm{Hom}_R(A,Q)\mid \mathrm{Im}f\subseteq A\subseteq N,\ 且\ kf=g\},$$

则 $gf^{-1}:\mathrm{Im}f\to Q$ 属于S. 定义 S 中任意两个元素 $k_1:A_1\to Q$ 和 $k_2:A_2\to Q$ 的二元关系≤如下:

$$k_1\leqslant k_2\Leftrightarrow A_1\subseteq A_2\ 且\ k_2|_{A_1}=k_1,$$

则$(S,\leqslant)$是部分序集. 若$\{k_j:A_j\to Q\mid j\in J\}$是 S 中的一个升链, 令 $k:\bigcup\limits_{j\in J}A_j\to Q;x\mapsto k_j(x)$, 如果 $x\in A_j$. 则 k 是$\{k_j\mid j\in J\}$在 S 中的上界. 由 Zorn 引理, S 有极大元 $h:B\to Q$. 若能证明 $B=N$, 则 $hf=g$, 从而(1)成立.

假定 $B\neq N$, 取 $x\in N\setminus B$, 令 $I=\{r\in R\mid rx\in B\}$, 这是 R 的理想, 且有 R-同态 $l':I\to Q;\ r\mapsto h(rx)$. 由(4), l'可扩张为 R-同态 $l:R\to Q$, 使得 $l|_I=l'$. 记 $B_1=B+Rx$, 则 $B_1\supset B$. 令

$$h':B_1\to Q;\ b+rx\mapsto h(b)+l(r),$$

其中 $b\in B$, $r\in R$. h'是映射, 这是因为: 若 $b+rx=b_1+r_1x\in$

B_1; $b, b_1 \in B$; $r, r_1 \in R$, 则 $b - b_1 = (r_1 - r)x \in B \cap Rx$, 从而 $r_1 - r \in I$, 于是 $h(b) - h(b_1) = h(b - b_1) = h((r_1 - r)x) = l'(r_1 - r) = l(r_1 - r) = l(r_1) - l(r)$, 所以 $h(b) + l(r) = h(b_1) + l(r_1)$. 进而容易验证 $h' \in S$, 且 $h < h'$, 这与 h 的极大性矛盾. □

下述命题是命题 2.3.2 的对偶命题, 其证法可对偶地应用于命题 2.3.2, 但反之不然.

命题 2.3.4 R-模直积 $Q = \prod_{i \in I} Q_i$ 是内射 R-模当且仅当每个直积因子 Q_i, $i \in I$, 是内射 R-模.

证明 设 $\tau_i : Q_i \to Q$ 和 $\pi_i : Q \to Q_i$ 分别是标准嵌入和标准投影. 若 Q 是内射的, 对于任意 R-单同态 $f: M \to N$ 和 R-同态 $g: M \to Q_i$, 存在 R-同态 $h: N \to Q$ 使得 $hf = \tau_i g$, 令 $h_i = \pi_i h$, 则 $h_i f = g$. 所以 Q_i, $i \in I$, 是内射的.

$$
\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, "g"'] & N \arrow[dl, "h_i"'] \arrow[ddl, "h"] \\
& Q_i \arrow[d, shift right, "\tau_i"'] & \\
& Q \arrow[u, shift right, "\pi_i"'] &
\end{tikzcd}
$$

反之, 若每个 Q_i, $i \in I$, 是内射的, 对于任意 R-单同态 $f: M \to N$ 和 R-同态 $g: M \to Q$, 存在 R-同态 $h_i : N \to Q_i$ 使得 $h_i f = \pi_i g$, $i \in I$. 再由定理 1.2.8, 存在唯一的 R-同态 $h: N \to Q$ 使得 $\pi_i h = h_i$, 进而容易验证 $hf = g$. □

一个 R-模 D 是**可除**的, 如果对于任意 $x \in D$ 和非零因子 $r \in R$, 存在 $y \in D$ 使得 $ry = x$. 例如, 有理数加群 $(\mathbb{Q}, +)$ 是可除 $\mathbb{Z}$-模, 但 $(\mathbb{Z}, +)$ 不是可除 $\mathbb{Z}$-模. 易证, 可除 R-模的直积、直和以及商模是可除的.

命题 2.3.5 对于任意环 R, 内射 R-模均是可除 R-模.

证明 设 M 是内射R-模，$x\in M$，r 是R 的非零因子. 则有 R-同态$f:Rr\to M;ar\mapsto ax$. 而 f 可扩张为 R-同态 $g:R\to M$. 令 $y=g(1_R)\in M$，则 $ry=rg(1_R)=g(r)=f(r)=x$. 所以 M 是可除的. □

命题 2.3.6 (1) $\mathbb{Z}$-模A 是可除的当且仅当 A 是内射的.

(2) 任意 $\mathbb{Z}$-模A 可以嵌入一个可除 $\mathbb{Z}$-模.

证明 (1) 若 A 是可除的，对于 $\mathbb{Z}$ 的每个理想 $\mathbb{Z}n$，$n\in\mathbb{Z}$，以及任意 $\mathbb{Z}$-同态$f:\mathbb{Z}n\to A$，存在 $x\in A$，使得 $nx=f(n)$；令 $h:\mathbb{Z}\to A;k\mapsto kx$，则 h 是 $\mathbb{Z}$-同态，且是 f 的扩张. 由 Baer 准则，A 是内射的. 另一部分由命题 2.3.5 立得.

(2) 由命题 2.2.2，A 是一个自由 $\mathbb{Z}$-模 $F=\bigoplus_{x\in X}\mathbb{Z}$ 的同态像，即 $A\simeq F/K$. 而 $\bigoplus_{x\in X}\mathbb{Z}$ 是可除 $\mathbb{Z}$-模 $\bigoplus_{x\in X}\mathbb{Q}$ 的子模，进而 $A\simeq F/K$ 可嵌入可除 $\mathbb{Z}$-模$(\bigoplus_{x\in X}\mathbb{Q})/K$. □

命题 2.3.7 设 R 是环，A 是 $\mathbb{Z}$-模. 则

(1) $\mathrm{Hom}_{\mathbb{Z}}(R,A)$是一个 R-模.

(2) 若 A 是可除 $\mathbb{Z}$-模，则 $\mathrm{Hom}_{\mathbb{Z}}(R,A)$是内射 R-模.

证明 (1) 对于任意 $r\in R$ 和$f\in\mathrm{Hom}_{\mathbb{Z}}(R,A)$，定义 $rf:R\to A;x\mapsto f(rx)$. 不难验证，关于这样的模运算，$\mathrm{Hom}_{\mathbb{Z}}(R,A)$ 是 R-模.

(2) 设 A 是可除的，从而是内射 $\mathbb{Z}$-模. 对于 R 的任意理想I 以及任意 R-同态 $f:I\to\mathrm{Hom}_{\mathbb{Z}}(R,A)$，令 $g:I\to A;a\mapsto f(a)(1_R)$，则 g 是 $\mathbb{Z}$-同态，且可扩张为 $\mathbb{Z}$-同态 $\bar{g}:R\to A$. 对于每个 $r\in R$，令 $h(r):R\to A;x\mapsto\bar{g}(rx)$，则 $h(r)\in\mathrm{Hom}_{\mathbb{Z}}(R,A)$. 进而令 $h:R\to\mathrm{Hom}_{\mathbb{Z}}(R,A);r\mapsto h(r)$，不难验证，$h$ 是 R-同态且是 f 的扩张. 由 Baer 准则，$\mathrm{Hom}_{\mathbb{Z}}(R,A)$是内射 R-模. □

定理 2.3.8 设 R 是环，则每个 R-模M 可嵌入一个内射 R-模.

证明 由命题 2.3.6 的(2)，M 作为 $\mathbb{Z}$-模可嵌入一个内射

$\mathbb{Z}$-模 D，设 τ：$M\to D$ 为嵌入 $\mathbb{Z}$-同态. 由定理 2.1.4，τ 导出 $\mathbb{Z}$-模单同态 τ^*：$\mathrm{Hom}_{\mathbb{Z}}(R,M)\to\mathrm{Hom}_{\mathbb{Z}}(R,D)$，且不难验证，$\tau^*$ 还是 R-模同态.

另一方面，映射 $\mathrm{Hom}_R(R,M)\to M$；$f\mapsto f(1_R)$ 是 R-同构（习题 1.2.3），而 $\mathrm{Hom}_R(R,M)$ 是 $\mathrm{Hom}_{\mathbb{Z}}(R,M)$ 的子模，于是 M 可嵌入 $\mathrm{Hom}_{\mathbb{Z}}(R,D)$. 由命题 2.3.7 的(2)，$\mathrm{Hom}_{\mathbb{Z}}(R,D)$ 是内射 R-模. □

与上述定理对偶的命题是：每个 R-模 M 均是一个投射 R-模的同态像（命题 2.2.2）.

习 题 2.3

1. 设 A 是任意 R-模. R-同态 $\eta_A:A\to A^{**}$ 给出了 R-模范畴 $\mathscr{M}_R$ 的从恒等函子 1 到双对偶函子 D^2 的自然变换 η：$1\to D^2$（参看 1.3.3 小节）. 证明：

(1) 若 A 是自由 R-模，则对偶模 A^* 也是自由 R-模，且 η_A：$A\to A^{**}$ 是 R-单同态.

(2) 若 A 是有限生成投射 R-模，则 A^* 也是有限生成 R-模，且 η_A：$A\to A^{**}$ 是 R-同构.

举例说明（取 R 为域），在(2)中，A 是有限生成的条件不可少.

2. 设 R 是环，P 是 R-模. 证明：

(1) P 是有限生成投射 R-模 $\Leftrightarrow$ 存在幂等阵 $A\in\mathrm{M}_n(R)$，$n\geqslant 1$，使得 $P\simeq R^nA=\{\alpha A\mid\alpha=(a_1,\cdots,a_n)\in R^n\}$.

(2) 设 A,B 分别是 R 上的 m,n 阶幂等方阵，则 $R^mA\simeq R^nB$ $\Leftrightarrow$ 存在 $t\geqslant\max\{m,n\}$，使得 $\mathrm{diag}\{A,0\}$ 和 $\mathrm{diag}\{B,0\}$ 在 $\mathrm{M}_t(R)$ 中相似（$A,B\in\mathrm{M}_n(R)$ 是**相似**的，如果存在 $X\in\mathrm{GL}_n(R)$ 使得 $B=X^{-1}AX$）.

(3) $\mathrm{M}_n(R)$ 中的两个幂等方阵是相似的当且仅当它们是相

抵的($A,B\in \mathrm{M}_n(R)$是**相抵**的，如果存在 $X,Y\in \mathrm{GL}_n(R)$使得 $B=XAY$).

这样，有限生成投射 R-模的同构分类问题可转化为 R 上的幂等方阵的相抵(相似)分类问题.

3. 证明：有理数加群($\mathbb{Q},+$)不是投射 $\mathbb{Z}$-模.

4. 设 A 是可除 $\mathbb{Z}$-模. 证明：

(1) A 的扭子模 $\mathrm{T}(A)$是可除的.

(2) $A=B\oplus \mathrm{T}(A)$，其中 B 是可除无扭 $\mathbb{Z}$-模.

5. 证明：每个可除无扭 $\mathbb{Z}$-模均 $\mathbb{Z}$-同构于$\bigoplus_{i\in I}\mathbb{Q}$.

6. 设 p 是素数. 令

$$\mathbb{Z}(p^{\infty})=\{\overline{a/b}\in \mathbb{Q}/\mathbb{Z}\mid a,b\in \mathbb{Z},\ b=p^i,\ i\geqslant 0\}.$$

证明：

(1) $\mathbb{Z}(p^{\infty})$是可除扭 $\mathbb{Z}$-模.

(2) 每个可除扭 $\mathbb{Z}$-模均 $\mathbb{Z}$-同构于$\bigoplus_{j\in J}\mathbb{Z}(p_j^{\infty})$，其中 p_j 是素数，$j\in J$.

4，5，6 三题给出了可除 $\mathbb{Z}$-模，也就是内射 $\mathbb{Z}$-模的结构.

7. 设 M 是任意 R-模. 证明：

(1) 存在投射 R-模 P_i，$i=0,1,2,\cdots$，和 R-同态 $\varepsilon:P_0\to M$，$d_i:P_i\to P_{i-1}$，使得序列

$$\cdots\longrightarrow P_2\xrightarrow{d_2}P_1\xrightarrow{d_1}P_0\xrightarrow{\varepsilon}M\longrightarrow 0$$

是正合的，叫做 M 的一个**投射分解**.

(2) 存在内射 R-模 Q^i，$i=0,1,2,\cdots$，和 R-同态 $\varepsilon':M\to Q^0$，$d^i:Q^i\to Q^{i+1}$，使得序列

$$0\longrightarrow M\xrightarrow{\varepsilon'}Q^0\xrightarrow{d^0}Q^1\xrightarrow{d^1}Q^2\longrightarrow\cdots$$

是正合的，叫做 M 的一个**内射分解**.

8. (**Eilenberg**) 设 P 是投射 R-模. 证明：存在自由 R-模 F，使得 $P\oplus F$ 是自由 R-模.

2.4 张量积和平坦模

2.4.1 模的张量积

设 R 是环，A,B,C 是 R-模. 映射

$$f:A\times B\to C;(a,b)\mapsto f(a,b)$$

称为 R-**双线性映射**，如果对于任意 $a,a_1,a_2\in A$；$b,b_1,b_2\in B$ 和 $r_1,r_2\in R$，均有

(i) $f(r_1a_1+r_2a_2,b)=r_1f(a_1,b)+r_2f(a_2,b)$；

(ii) $f(a,r_1b_1+r_2b_2)=r_1f(a,b_1)+r_2f(a,b_2)$.

这是域上线性空间的双线性函数的自然推广. 从 $A\times B$ 到 C 的所有 R-双线性映射的全体记作 $\mathrm{BL}(A\times B,C)$.

设 T 是 R-模，$f\in\mathrm{BL}(A\times B,T)$. 若 (T,f) 具有如下泛性：对于任意 R-模 C 和 $g\in\mathrm{BL}(A\times B,C)$，存在唯一的 R-同态 $h:T\to C$，使得 $hf=g$，即使下图交换：

$$\begin{tikzcd}
A\times B \arrow[r, "f"] \arrow[dr, "g"'] & T \arrow[d, "h"] \\
 & C
\end{tikzcd}$$

则称 (T,f) 或 T 为 R-模 A 与 B 的**张量积**，记作 $T=A\underset{R}{\otimes}B$，且记 $f(a,b)=a\otimes b$；$a\in A$，$b\in B$.

如果构作范畴 $\mathscr{T}$ 如下：令

$\mathrm{ob}\,\mathscr{T}=\{(C,g)\mid C\in\mathrm{ob}\mathscr{M}_R,\ g\in\mathrm{BL}(A\times B,C)\}$，

$\mathrm{Hom}_{\mathscr{T}}((C,g),(C',g'))=\{h\in\mathrm{Hom}_R(C,C')\mid hg=g'\}$，

而 $\mathscr{T}$ 中态射的合成就是 R-同态的合成，则 R-模 A 与 B 的张量积就是范畴 $\mathscr{T}$ 的始对象，因而在 R-同构意义下唯一.

R-模 A 与 B 的张量积是存在的，可具体地构作如下：令 F

是以集合 $A\times B$ 为基的自由 R-模，H 是由下列形式的元素生成的 F 的子模：

(1) $(a+a',b)-(a,b)-(a',b)$;

(2) $(a,b+b')-(a,b)-(a,b')$;

(3) $(r_1a,r_2b)-r_1r_2(a,b)$,

其中 $a,a'\in A$；$b,b'\in B$；$r_1,r_2\in R$. 记商模 F/H 为 T，令 f: $A\times B\to T$;$(a,b)\mapsto(a,b)+H$，$\tau:A\times B\to F$ 为包含映射，$\nu:F\to T$ 为自然同态，则 $f=\nu\tau$. 对于任意 R-模 C 和 $g\in \mathrm{BL}(A\times B,C)$，由于 F 是自由 R-模，存在唯一的 R-同态 $k:F\to C$，使得 $g=k\tau$. 又由于 g 是 R-双线性的，$\mathrm{Ker}k\supseteq H$. 由同态基本定理，存

$$\begin{tikzcd}
A\times B \arrow[r, "\tau"] \arrow[d, "g"'] & F \arrow[r, "\nu"] \arrow[dl, "k"] & T \arrow[dll, "h"] \\
C & &
\end{tikzcd}$$

在唯一的 R-同态 $h:T\to C$ 使得 $k=h\nu$，从而 $g=h\nu\tau=hf$. 这表明 (T,f) 具有张量积定义中的泛性，从而是 A 与 B 的张量积. 常将 $T=F/H$ 与 $A\underset{R}{\otimes}B$ 等同，$(a,b)+H$ 与 $a\otimes b$ 等同，$a\in A$，$b\in B$. 由于 F 由 $A\times B$ 生成，所以 $A\underset{R}{\otimes}B$ 由 $\{a\otimes b\mid(a,b)\in A\times B\}$ 生成，从而 $A\underset{R}{\otimes}B$ 的元素可表示成 $\sum\limits_i a_i\otimes b_i$ 的形式，但表示法未必唯一. 还需注意的是，$A\underset{R}{\otimes}B$ 的元素未必都能表示成 $a\otimes b$ 的形式. 由 F/H 的构造可知，在 $A\underset{R}{\otimes}B$ 中有

(1) $(a+a')\otimes b=a\otimes b+a'\otimes b$;

(2) $a\otimes(b+b')=a\otimes b+a\otimes b'$;

(3) $r(a\otimes b)=(ra)\otimes b=a\otimes(rb)$,

其中 $a,a'\in A$，$b,b'\in B$，$r\in R$.

利用张量积的泛性，容易证明张量积的许多性质.

命题 2.4.1 设 A_i, A, B, C 为 R-模，$i\in I$，则有下列 R-模同构：

(1) $A\bigotimes_R B\simeq B\bigotimes_R A$;

(2) $R\bigotimes_R A\simeq A$;

(3) $(\bigoplus_{i\in I}A_i)\bigotimes_R B\simeq\bigoplus_{i\in I}(A_i\bigotimes_R B)$;

(4) $(A\bigotimes_R B)\bigotimes_R C\simeq A\bigotimes_R(B\bigotimes_R C)$.

证明 (1) 令 $f: A\times B\to B\bigotimes_R A;(a,b)\mapsto b\otimes a$，则 f 是 R-双线性的. 由 $A\bigotimes_R B$ 的泛性，存在 R-同态 $f':A\bigotimes_R B\to B\bigotimes_R A$ 使得 $f'(a\otimes b)=b\otimes a$. 对称地，存在 R-同态 $g':B\bigotimes_R A\to A\bigotimes_R B$ 使得 $g'(b\otimes a)=a\otimes b$. 显然 $g'f'=1_{A\otimes_R B}$，$f'g'=1_{B\otimes_R A}$，故 f' 是 R-同构.

(2) 令 $f:R\times A\to A;(r,a)\mapsto ra$，则 f 是 R-双线性的，故存在 R-同态 h: $R\bigotimes_R A\to A$ 使得 $h(r\otimes a)=ra$. 又 $k:A\to R\bigotimes_R A$; $a\mapsto 1_R\otimes a$，是 R-同态，且有 $kh=1_{R\otimes_R A}$，$hk=1_A$. 所以 h 是 R-同构.

(3) 记 τ_i 和 π_i 分别是直和 $\bigoplus_{i\in I}A_i$ 的标准嵌入和标准投影. 类似于(1)和(2)，通过定义 R-双线性映射，可导出 R-同态 h: $(\bigoplus_{i\in I}A_i)\bigotimes_R B\to\bigoplus_{i\in I}(A_i\bigotimes_R B)$ 使得 $h(x\otimes b)=(\pi_i(x)\otimes b)_{i\in I}$，和 k: $\bigoplus_{i\in I}(A_i\bigotimes_R B)\to(\bigoplus_{i\in I}A_i)\bigotimes_R B$ 使得 $k((a_i\otimes b)_{i\in I})=(\sum_{i\in I}\tau_i(a_i))\otimes b$，且有 kh 和 hk 均是恒等映射，故 h 是 R-同构.

(4) 可类似于(1)证明. □

两个自由 R-模的张量积具有下述性质.

命题 2.4.2 设 A 和 B 是分别具有基 X 和 Y 的自由 R-模，则 $A\bigotimes_R B$ 是具有基 $\{x\otimes y\mid x\in X, y\in Y\}$ 的自由 R-模.

证明 由 2.2 节和命题 2.4.1，有 R-同构 $A\bigotimes_R B\simeq(\bigoplus_{x\in X}R)\bigotimes_R$

$(\bigoplus\limits_{y\in Y}R)\simeq\bigoplus\limits_{x\in X,\ y\in Y}(R\bigotimes\limits_R R)\simeq\bigoplus\limits_{x\in X,\ y\in Y}R$，从而 $A\bigotimes\limits_R B$ 是自由的，且通过上述 R-同构可知 $\{x\otimes y\mid x\in X,\ y\in Y\}$ 是 $A\bigotimes\limits_R B$ 的基. □

由命题 2.4.2 可知，对于自由 R-模 A 和 B，有

$$\mathrm{rank}_R(A\bigotimes_R B)=\mathrm{rank}_R A\cdot\mathrm{rank}_R B,$$

$$\mathrm{rank}_R(A\oplus B)=\mathrm{rank}_R A+\mathrm{rank}_R B.$$

设 $f:A\to B$ 和 $f':A'\to B'$ 是 R-模同态，则映射 $g:A\times A'\to B\bigotimes\limits_R B'$；$(a,a')\mapsto f(a)\otimes f'(a')$ 是 R-双线性的，g 导出唯一的 R-同态，记作 $f\otimes f':A\bigotimes\limits_R A'\to B\bigotimes\limits_R B'$，使得 $(f\otimes f')(a\otimes a')=f(a)\otimes f'(a')$；$a\in A$，$a'\in A'$. 又若 $g:B\to C$ 和 $g':B'\to C'$ 是 R-模同态，容易验证：

$$(g\otimes g')(f\otimes f')=(gf)\otimes(g'f').$$

这样，若 f 和 g 是 R-同构，则 $f\otimes g$ 也是 R-同构，且 $(f\otimes g)^{-1}=f^{-1}\otimes g^{-1}$.

2.4.2 张量积函子

任意取定一个 R-模 M，可构作函子 $M\bigotimes\limits_R -:\mathscr{M}_R\to\mathscr{M}_R$ 如下：让每个 R-模 A 对应于 $M\bigotimes\limits_R A$，即 $(M\bigotimes\limits_R -)(A)=M\bigotimes\limits_R A$. 对于任意 R-模同态 $f:A\to B$，令 $(M\bigotimes\limits_R -)(f)=1_M\otimes f:M\bigotimes\limits_R A\to M\bigotimes\limits_R B$. 容易验证，$M\bigotimes\limits_R -$ 是一个函子，称为**张量积函子**.

函子 $M\bigotimes\limits_R -$ 保持 R-模同态的加法，也就是说，若 $f,g\in\mathrm{Hom}_R(A,B)$，则 $(M\bigotimes\limits_R -)(f+g)=(M\bigotimes\limits_R -)(f)+(M\bigotimes\limits_R -)(g)$，即有 $1_M\otimes(f+g)=1_M\otimes f+1_M\otimes g$. 这是因为，对于任意 $x\in M$ 和 $a\in A$，$(1_M\otimes(f+g))(x\otimes a)=x\otimes(f(a)+g(a))=x\otimes f(a)+x\otimes g(a)=(1_M\otimes f)(x\otimes a)+(1_M\otimes g)(x\otimes a)=(1_M\otimes f+1_M\otimes g)(x\otimes a)$.

由命题 2.4.1 的(3)可知，函子 $M\bigotimes\limits_R -$ 还保持 R-模的直和.

函子 $M\underset{R}{\otimes}-$ 具有下述定理给出的**右正合性**.

定理 2.4.3 R-模同态序列 ε: $A\xrightarrow{f}B\xrightarrow{g}C\longrightarrow 0$ 是正合的当且仅当对于每个 R-模 M, R-模同态序列 $M\underset{R}{\otimes}\varepsilon$:

$$M\underset{R}{\otimes}A\xrightarrow{1\otimes f}M\underset{R}{\otimes}B\xrightarrow{1\otimes g}M\underset{R}{\otimes}C\longrightarrow 0$$

都是正合的.

证明 若序列 ε 正合, 则 g 是满的, 从而 $1\otimes g$ 是满的. 又由 $gf=0$, 有 $(1\otimes g)(1\otimes f)=1\otimes(gf)=1\otimes 0=0$, 所以 $\mathrm{Im}(1\otimes f)\subseteq\mathrm{Ker}(1\otimes g)$. 这诱导出 R-同态 $h:\mathrm{Coker}(1\otimes f)\to M\underset{R}{\otimes}C$ 使得 $h(x\otimes b+\mathrm{Im}(1\otimes f))=x\otimes g(b)$; $x\in M$, $b\in B$. 下证 h 是 R-同构, 从而有 $\mathrm{Ker}(1\otimes g)=\mathrm{Im}(1\otimes f)$. 令 $\varphi:M\times C\to\mathrm{Coker}(1\otimes f)$; $(x,c)\mapsto x\otimes b+\mathrm{Im}(1\otimes f)$, 其中 $b\in B$ 使得 $g(b)=c$. 这样定义 φ 是合理的, 这因为: 又若 $b'\in B$ 使得 $g(b')=c$, 则 $b-b'\in\mathrm{Ker}g=\mathrm{Im}f$, 从而 $x\otimes b-x\otimes b'\in\mathrm{Im}(1\otimes f)$. 易证, φ 是 R-双线性的, 从而导出 R-同态 $k:M\underset{R}{\otimes}C\to\mathrm{Coker}(1\otimes f)$ 使得 $k(x\otimes c)=x\otimes b+\mathrm{Im}(1\otimes f)$, 其中 $g(b)=c$. 易知 h 与 k 互逆, 故 h 是 R-同构.

反之, 取 $M={}_RR$, 直接验证下图是交换的:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "h_A"] & B \arrow[r, "g"] \arrow[d, "h_B"] & C \arrow[r] \arrow[d, "h_C"] & 0 \\
R\underset{R}{\otimes}A \arrow[r, "1\otimes f"'] & R\underset{R}{\otimes}B \arrow[r, "1\otimes g"'] & R\underset{R}{\otimes}C \arrow[r] & 0
\end{tikzcd},$$

其中 h_A: $A\to R\underset{R}{\otimes}A$; $a\mapsto 1\otimes a$ 是命题 2.4.1 中(2)的证明中给出的 R-同构, h_B 和 h_C 也是这样的 R-同构. 再由下行正合可得上行也正合. □

稍后以及习题中将给出例子说明张量积函子一般不具有左正合性.

下面讨论 Hom 函子与张量积函子间的伴随关系.

设 B 是R-模, C 是 $\mathbb{Z}$-模. 若 $f\in \mathrm{Hom}_{\mathbb{Z}}(B,C)$, $r\in R$, 定义

$$rf: B\to C;\ b\mapsto f(rb),$$

则 $rf\in \mathrm{Hom}_{\mathbb{Z}}(B,C)$, 且不难验证, 这使 $\mathrm{Hom}_{\mathbb{Z}}(B,C)$成为一个$R$-模. 又若 $g:B\to B'$是R-同态, 则 g 作为 $\mathbb{Z}$-模同态在反变函子 $\mathrm{Hom}_{\mathbb{Z}}(-,C)$下的像 $g_*:\mathrm{Hom}_{\mathbb{Z}}(B',C)\to \mathrm{Hom}_{\mathbb{Z}}(B,C)$不仅是 $\mathbb{Z}$-模同态, 还是 R-模同态. 这样, $\mathrm{Hom}_{\mathbb{Z}}(-,C)$是一个从 R-模范畴 $\mathscr{M}_R$ 到自身的反变函子.

定理 2.4.4 (伴随定理) 设 A 和B 是R-模, C 是 $\mathbb{Z}$-模, 则有 R-模同构

$$\eta_A: \mathrm{Hom}_{\mathbb{Z}}(A\otimes_R B,C)\to \mathrm{Hom}_R(A,\mathrm{Hom}_{\mathbb{Z}}(B,C)),$$

并且对于任意 R-模同态$f:A\to A'$, 下图交换:

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathbb{Z}}(A'\otimes_R B,C) & \xrightarrow{\eta_{A'}} & \mathrm{Hom}_R(A',\mathrm{Hom}_{\mathbb{Z}}(B,C)) \\
\Big\downarrow{\scriptstyle (f\otimes 1_B)_*} & & \Big\downarrow{\scriptstyle f_*} \\
\mathrm{Hom}_{\mathbb{Z}}(A\otimes_R B,C) & \xrightarrow{\eta_A} & \mathrm{Hom}_R(A,\mathrm{Hom}_{\mathbb{Z}}(B,C)).
\end{array}$$

证明 先构作映射 $\eta=\eta_A:f\mapsto\eta(f)$如下: 对于任意 $f\in \mathrm{Hom}_{\mathbb{Z}}(A\otimes_R B,C)$和 $a\in A$, 令

$$\eta(f)(a):B\to C;b\mapsto f(a\otimes b),$$

易证这是一个 $\mathbb{Z}$-模同态. 再令

$$\eta(f): A\to \mathrm{Hom}_{\mathbb{Z}}(B,C);\ a\mapsto \eta(f)(a),$$

验证这是一个 R-模同态, 进而验证, $\eta:f\mapsto\eta(f)$是 R-模同态.

再构作映射 $\xi:\mathrm{Hom}_R(A,\mathrm{Hom}_{\mathbb{Z}}(B,C))\to \mathrm{Hom}_{\mathbb{Z}}(A\otimes_R B,\ C)$; $g\mapsto\xi(g)$如下: 对任意 $a\in A$ 和 $b\in B$, 有 $g(a)\in \mathrm{Hom}_{\mathbb{Z}}(B,C)$, 从而$(g(a))(b)\in C$. 令

$$h': A\times B\to C;\ (a,b)\to(g(a))(b),$$

易证 h'是 $\mathbb{Z}$-双线性的, 从而导出唯一的 $\mathbb{Z}$-同态$h:A\otimes_{\mathbb{Z}} B\to C$ 使

得$h(a\otimes b)=(g(a))(b)$. 令 $\xi(g)=h$, 容易验证 ξ 也是 R-同态.

然后, 验证 $\eta=\eta_A$ 与ξ互逆, 从而 η_A 即为所需的R-同构.

最后, 验证图的交换性. $\square$

用范畴的语言来表述, 伴随定理是说, R-模范畴的反变函子 $\mathrm{Hom}_{\mathbf{Z}}(-\otimes_R B, C)$与反变函子 $\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbf{Z}}(B,C))$自然同构.

命题 2.4.5 *设 I,J 是环R 的理想, M 是R-模, 则有 R-模同构*

(1) $(R/I)\otimes_R M\simeq M/(IM)$.

(2) $(R/I)\otimes_R(R/J)\simeq R/(I+J)$.

证明 (1) 由正合列 $I\xrightarrow{\tau}R\longrightarrow R/I\longrightarrow 0$ 和定理2.4.3, 可得正合列 $I\otimes_R M\xrightarrow{\tau\otimes 1}R\otimes_R M\longrightarrow(R/I)\otimes_R M\longrightarrow 0$. 又由命题2.4.1的(2), 存在 R-同构h: $R\otimes_R M\rightarrow M$ 使得$h(r\otimes m)=rm$, 其中 $r\in R$, $m\in M$, 且 $\mathrm{Im}(\tau\otimes 1)$在 h 下的像为IM, 所以$(R/I)\otimes_R M\simeq(R\otimes_R M)/\mathrm{Im}(\tau\otimes 1)\simeq M/(IM)$.

(2) 令 $M=R/J$. 由(1), $(R/I)\otimes_R(R/J)\simeq(R/J)/(I(R/J))=(R/J)/((I+J)/J)\simeq R/(I+J)$. $\square$

设 $\varphi:R\rightarrow S$ 是环同态, N 是S-模. 定义 R 在N 上的作用为

$$rn=\varphi(r)n;\ r\in R,\ n\in N,$$

可以验证, N 还是一个R-模. 特别地, S-模S 也是一个R-模. 这样, 对于任意 R-模M, 张量积 $S\otimes_R M$ 均是R-模. 定义 S 在$S\otimes_R M$ 上的作用为

$$s(t\otimes m)=(st)\otimes m;\ s,t\in S,\ m\in M,$$

则 $S\otimes_R M$ 是一个S-模. 若 $f:M\rightarrow M'$是R-模同态, 则 R-模同态 $1_S\otimes f:S\otimes_R M\rightarrow S\otimes_R M'$还是$S$-模同态. 进而容易验证, $S\otimes_R -$ 是从 R-模范畴到 S-模范畴的一个函子, 叫做由环同态 $\varphi:R\rightarrow S$ 导

出的**换环函子**.

命题 2.4.6 设 $\varphi: R\to S$ 是环同态. 则

(1) 若 F 是以 X 为基的自由 R-模, 则 $S\bigotimes_R F$ 是以 $\{1\otimes x \mid x\in X\}$ 为基的自由 S-模.

(2) 若 P 是投射 R-模, 则 $S\bigotimes_R P$ 是投射 S-模.

证明 (1) 不妨设 $F=\bigoplus_{x\in X} R$, 由命题 2.4.1, 有 R-模同构 $S\bigotimes_R F = S\bigotimes_R(\bigoplus_{x\in X} R)\simeq\bigoplus_{x\in X}(S\bigotimes_R R)\simeq\bigoplus_{x\in X} S$. 容易验证这还是 S-模同构, 所以 $S\bigotimes_R F$ 是自由 S-模, 且通过上述同构, 可知 $\{1\otimes x\mid x\in X\}$ 是 $S\bigotimes_R F$ 的基.

(2) 由(1)和命题 2.4.1 的(3)以及 P 是一个自由 R-模 F 的直和项立得. □

2.4.3 平坦模

设 M 是 R-模, 由定理 2.4.3, 函子 $M\bigotimes_R - : \mathscr{M}_R\to\mathscr{M}_R$ 是右正合的; 但未必是左正合的. 也就是说, 对于 R-单同态 $f: A\to B$, $1_M\otimes f: M\bigotimes_R A\to M\bigotimes_R B$ 未必是单射. 例如, 当 $M=\mathbb{Z}/2\mathbb{Z}$ 是 $\mathbb{Z}$-模时, 对于 $\mathbb{Z}$-单同态 $f:\mathbb{Z}\to\mathbb{Z}; n\mapsto 2n$, $1_M\otimes f: M\bigotimes_{\mathbb{Z}}\mathbb{Z}\to M\bigotimes_{\mathbb{Z}}\mathbb{Z}$ 是零同态, 但 $M\bigotimes_{\mathbb{Z}}\mathbb{Z}\simeq M\neq 0$(命题 2.4.1).

R-模 M 称为**平坦 R-模**, 如果函子 $M\bigotimes_R - : \mathscr{M}_R\to\mathscr{M}_R$ 是**正合**的, 即对于任意 R-模短正合列 $0\longrightarrow A\xrightarrow{f} B\xrightarrow{g} C\longrightarrow 0$, 序列 $0\longrightarrow M\bigotimes_R A\xrightarrow{1_M\otimes f} M\bigotimes_R B\xrightarrow{1_M\otimes g} M\bigotimes_R C\longrightarrow 0$ 是正合的. 由定理 2.4.3, M 是平坦的当且仅当对于任意 R-单同态 $g: B\to C$, R-同态 $1_M\otimes g: M\bigotimes_R B\to M\bigotimes_R C$ 是单射. 由上可知 $\mathbb{Z}/2\mathbb{Z}$ 不是平坦 $\mathbb{Z}$-模.

命题 2.4.7 (1) 环 R 作为 R-模是平坦的.

(2) R-模的直和 $\bigoplus_{i\in I} M_i$ 是平坦的当且仅当每个 M_i, $i\in I$, 是平坦的.

(3) 投射 R-模都是平坦 R-模.

证明 (1) 设 $f:A\to B$ 是 R-单同态，则有交换图

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "h_A"] & B \arrow[d, "h_B"] \\ R\underset{R}{\otimes} A \arrow[r, "1_R\otimes f"'] & R\underset{R}{\otimes} B \end{tikzcd},$$

其中 h_A 和 h_B 是命题 2.4.1 中(2)的证明中给出的 R-同构. 于是 $1_R\otimes f$ 是单射，所以 ${}_RR$ 是平坦的.

(2) 首先，对于 R-模同态 $f_i:A_i\to B_i$，$i\in I$，容易验证，映射 $\oplus f_i:\bigoplus\limits_{i\in I}A_i\to\bigoplus\limits_{i\in I}B_i;(a_i)_{i\in I}\mapsto(f_i(a_i))_{i\in I}$ 是 R-同态，且 $\oplus f_i$ 为单射当且仅当每个 f_i，$i\in I$，是单射.

设 $f:A\to B$ 是 R-单同态，则有交换图

$$\begin{tikzcd} (\bigoplus\limits_{i\in I} M_i)\underset{R}{\otimes} A \arrow[r, "1_{\oplus M_i}\otimes f"] \arrow[d, "h"] & (\bigoplus\limits_{i\in I} M_i)\underset{R}{\otimes} B \arrow[d, "k"] \\ \bigoplus\limits_{i\in I}(M_i\underset{R}{\otimes} A) \arrow[r, "\oplus(1_{M_i}\otimes f)"] & \bigoplus\limits_{i\in I}(M_i\underset{R}{\otimes} B) \end{tikzcd},$$

其中 h 和 k 是命题 2.4.1 中(3)的证明中给出的 R-同构. 于是 $1_{\oplus M_i}\otimes f$ 为单射，当且仅当 $\oplus(1_{M_i}\otimes f)$ 为单射，当且仅当每个 $1_{M_i}\otimes f$，$i\in I$，为单射. 所以(2)成立.

(3) 由(1)和(2)可知，自由 R-模是平坦的，再由(2)，投射 R-模作为某个自由 R-模的直和项亦是平坦的. □

有理数加群 $\mathbb{Q}$ 作为 $\mathbb{Z}$-模是可除的，其商模 $\mathbb{Q}/\mathbb{Z}$ 也是可除的，从而是内射 $\mathbb{Z}$-模(命题 2.3.6). 对于任意 R-模 M，$\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})$ 还是一个 R-模.

定理 2.4.8 设 M 是 R-模，则下列条件等价：

(1) M 是平坦 R-模；

(2) $\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})$ 是内射 R-模；

(3) 对于 R 的每个理想 I 及包含映射 $\tau:I\to R$，映射 $\tau\otimes 1_M$：

$I\underset{R}{\otimes}M\to R\underset{R}{\otimes}M$ 是R-单同态；

(4) 对于 R 的每个理想I，映射

$$u:I\underset{R}{\otimes}M\to IM;\ \sum_i a_i\otimes m_i\mapsto\sum_i a_im_i$$

是 R-单同态.

证明 (1)⇔(2)：由伴随定理，对任意 R-模同态$f:A\to B$，有下图交换：

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{Z}}(B\underset{R}{\otimes}M,\mathbb{Q}/\mathbb{Z}) \arrow[r, "\eta_B"] \arrow[d, "(f\otimes 1_M)_*"] & \mathrm{Hom}_R(B,\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})) \arrow[d, "f_*"] \\
\mathrm{Hom}_{\mathbb{Z}}(A\underset{R}{\otimes}M,\mathbb{Q}/\mathbb{Z}) \arrow[r, "\eta_A"] & \mathrm{Hom}_R(A,\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})).
\end{tikzcd}$$

由于 η_A,η_B 是R-同构，且 $\mathbb{Q}/\mathbb{Z}$ 是内射 $\mathbb{Z}$-模，$f\otimes1_M:A\underset{R}{\otimes}M\to B\underset{R}{\otimes}M$是$R$-单同态⇔$(f\otimes1_M)_*$是 R-满同态⇔f_*是 R-满同态. 由此立得(1)⇔(2).

(1)⇔(3)：只需证(3)⇒(1). 在上面的交换图中，令 $A=I$，$B=R$，$f=\tau:I\to R$ 是包含映射. 则 $\tau\otimes1_M$ 是单射，从而 τ_* 是单射. 于是由 Baer 准则可知，$\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})$是内射 R-模，再由以上证明即得 M 是平坦的.

(3)⇔(4)：容易验证 u 是R-同态，且下图交换：

$$\begin{tikzcd}
I\underset{R}{\otimes}M \arrow[r, "\tau\otimes1_M"] \arrow[d, "u"] & R\underset{R}{\otimes}M \arrow[d, "\varphi"] \\
IM \arrow[r, "i"] & M
\end{tikzcd},$$

其中 $i:IM\to M$ 是包含映射，φ 使得$a\otimes m\mapsto am$ 是 R-同构. 于是 $\tau\otimes1_M$ 是单射当且仅当 u 是单射. □

命题 2.4.9 (1) 设 R 是整环. 若 M 是平坦R-模，则 M 是无扭 R-模.

(2) 设 R 是主理想整环. 则 R-模M是平坦的当且仅当M是无扭的.

证明 (1) 因 R 是整环，对于任意非零元 $r\in R$，$f_r:R\to Rr;a\mapsto ar$ 是 R-同构. 容易验证，下图交换：

$$\begin{array}{ccc} R\otimes_R M & \xrightarrow{f_r\otimes 1_M} & Rr\otimes_R M \\ \varphi\downarrow & & \downarrow u \\ M & \xrightarrow{g_r} & rM \end{array},$$

其中 $g_r:m\mapsto rm$，$\varphi:a\otimes m\mapsto am$，$u:(ar)\otimes m\mapsto arm$. 若 M 平坦，则由定理2.4.8，u 和 $f_r\otimes 1_M$ 是 R-同构. 又因 φ 是 R-同构，所以 g_r 是 R-同构. 从而 M 无扭.

(2) 若 R 是主理想整环，M 是无扭 R-模，对于 R 的每个非零理想 $I=Rr$，$0\neq r\in R$，上图中的 g_r 是 R-同构，从而 u：$Rr\otimes_R M\to rM$ 是 R-同构，由定理2.4.8，M 是平坦的. □

习 题 2.4

1. 设 A 是 $\mathbb{Z}$-模，$\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$. 证明：

(1) $A\otimes_{\mathbb{Z}}\mathbb{Z}_n\simeq A/nA$，$\mathbb{Z}_m\otimes_{\mathbb{Z}}\mathbb{Z}_n\simeq\mathbb{Z}_{(m,n)}$，其中 (m,n) 是 m 和 n 的最大公因数.

(2) 若 A 是扭 $\mathbb{Z}$-模，则 $A\otimes_{\mathbb{Z}}\mathbb{Q}=0$，但是 $\mathbb{Q}\otimes_{\mathbb{Z}}\mathbb{Q}\simeq\mathbb{Q}$.

2. 分别举出满足下列条件的例子：

(1) $A\otimes_R B\neq A\otimes_{\mathbb{Z}} B$.

(2) $u\in A\otimes_R B$，对于任意 $a\in A$，$b\in B$，均有 $u\neq a\otimes b$.

(3) $a\otimes b=a'\otimes b'$，但 $a\neq a'$，$b\neq b'$.

3. (1) 设 i：$\mathbb{Z}\to\mathbb{Q}$ 是包含映射. 证明：$1\otimes i$：$(\mathbb{Z}/2\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Z}\to(\mathbb{Z}/2\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Q}$ 不是 $\mathbb{Z}$-单同态.

(2) 设 α：$\mathbb{Z}_2\to\mathbb{Z}_4$ 是 $\mathbb{Z}$-单同态，其中 $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$. 证明：$1\otimes\alpha$：$\mathbb{Z}_2\otimes_{\mathbb{Z}}\mathbb{Z}_2\to\mathbb{Z}_2\otimes_{\mathbb{Z}}\mathbb{Z}_4$ 是零映射，但 $\mathbb{Z}_2\otimes_{\mathbb{Z}}\mathbb{Z}_2\neq 0$，$\mathbb{Z}_2\otimes_{\mathbb{Z}}\mathbb{Z}_4\neq 0$.

4. 若 M,N 是平坦 R-模. 证明：$M\otimes_R N$ 也是平坦 R-模.

5. 设 $f:R\to S$ 是环同态(从而 S 是 R-模). 证明: 若 M 是平坦 R-模, 则 $S\bigotimes_R M$ 是平坦 S-模.

6. 证明: 多项式环 $R[x]$ 是平坦 R-模.

7. 设 $R=\mathbb{Z}$, $A=\mathbb{Q}$, $B_i=\mathbb{Z}/p^i\mathbb{Z}$, 其中 p 是素数. 证明: $A\bigotimes_R(\prod_{i=1}^{\infty}B_i)\not\simeq\prod_{i=1}^{\infty}(A\bigotimes_R B_i)$.

8. 设 A',B'分别是 R-模 A,B 的子模. 证明: $(A/A')\bigotimes_R(B/B')\simeq(A\bigotimes_R B)/C$, 其中 C 是 $A\bigotimes_R B$ 的由 $\{a'\otimes b, a\otimes b' \mid a\in A, a'\in A', b\in B, b'\in B\}$ 生成的 R-子模.

9. 设 R 是局部环, M 和 N 是有限生成 R-模. 证明: 若 $M\bigotimes_R N=0$, 则 $M=0$ 或 $N=0$ (提示: 用引理 1.2.1).

10. 证明: 若 R-模 A_i, $i\in I$, 的直积 $\prod_{i\in I}A_i$ 是平坦的, 则每个 A_i 均是平坦的; 反之未必成立.

11. 设 $0\to A\to B\to C\to 0$ 是 R-模正合列. 证明: 若 A 和 C 是平坦的, 则 B 也是平坦的.

12. 设 R 是环. 证明: R-模范畴 $\mathscr{M}_R$ 的恒等函子 1 与张量积函子 $R\bigotimes_R -$ 自然同构.

2.5 分式环、分式模和局部化

在“近世代数”课程中我们已学过由整环 R 构造它的分式域 F, 目的在于将整环 R 上的数学问题放到分式域 F 上去考虑, 以利用域的好性质来解决整环 R 上的问题. 现将这一思想推广到一般交换环及其上的模上去.

2.5.1 分式环

设 R 是环, R 的子集 S 称为 R 的一个**乘法集**, 如果 $1_R\in S$, 且 S 关于 R 的乘法构成一个么半群. 例如, 若 P 是 R 的素理想,

则 $S=R\backslash P$ 是 R 的乘法集.

设 S 是环 R 的乘法集. 定义 $R\times S$ 的二元关系～如下：对于 (a,s), $(b,t)\in R\times S$,

$$(a,s)\sim(b,t)\Leftrightarrow \text{存在 } u\in S, \text{ 使得 } uat=ubs.$$

不难验证，这是 $R\times S$ 的一个等价关系. 记 $(a,s)\in R\times S$ 所在的等价类为 a/s，且记商集 $(R\times S)/\sim=\{a/s\mid a\in R,\ s\in S\}$ 为 $S^{-1}R$. 定义 $S^{-1}R$ 的加法和乘法如下：

$$a/s+b/t=(at+bs)/st,\qquad (a/s)(b/t)=ab/st.$$

需证运算与代表元的选择无关. 若 $a/s=a'/s'$, $b/t=b'/t'$，则存在 $u,v\in S$ 使得 $u(as'-a's)=0$, $v(bt'-b't)=0$. 于是 $uv((at+bs)s't'-(a't'+b's')st)=(as'-a's)uvtt'+(bt'-b't)vuss'=0$，从而 $(at+bs)/st=(a't'+b's')/s't'$. 类似地可证，$ab/st=a'b'/s't'$. 进而不难验证，$S^{-1}R$ 关于上述加法和乘法构成环，其单位元为 1/1，零元为 0/1. 环 $S^{-1}R$ 称为 R 关于乘法集 S 的**分式环**. 此时，有环同态 φ: $R\to S^{-1}R$; $a\mapsto a/1$，叫做**正则同态**.

命题 2.5.1　设 S 是环 R 的乘法集. 则

(1) 正则同态 $\varphi:R\to S^{-1}R$ 的核 $\mathrm{Ker}\varphi=\bigcup\limits_{u\in S}\mathrm{Ann}_R(u)$.

(2) φ 是单同态当且仅当 S 不含 R 的零因子.

证明　设 $a\in R$，则 $a\in\mathrm{Ker}\varphi\Leftrightarrow a/1=0/1\Leftrightarrow$ 存在 $u\in S$ 使 $u(a-0)=ua=0$，于是(1)成立，进而(2)成立. □

若 S 是整环 R 的乘法集，则正则同态 $\varphi:R\to S^{-1}R$ 是单同态；特别地，当 $S=R\backslash\{0\}$ 时，$S^{-1}R$ 就是 R 的**分式域**(商域). 这是因为，对每个 $u\in S$, $\varphi(u)=u/1$ 在 $S^{-1}R$ 中有乘法逆元 $1/u$.

分式环 $S^{-1}R$ 具有下述泛性.

命题 2.5.2　设 S 是环 R 的乘法集. 若环同态 $f:R\to R'$ 使得 $f(S)\subseteq\mathrm{U}(R')$, $\mathrm{U}(R')$ 为 R' 的单位群，则存在唯一的环同态 $g:S^{-1}R\to R'$ 使得 $g\varphi=f$，即下图交换：

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "f"'] & S^{-1}R \arrow[dl, "g"] \\ R' & \end{tikzcd}$$

证明 令 $g:S^{-1}R\to R';\ a/s\mapsto f(a)f(s)^{-1}$，这是一个映射：若 $a/s=b/t$，则存在 $u\in S$ 使 $uat=ubs$，于是 $f(u)f(a)f(t)=f(u)f(b)f(s)$. 由于 $f(u),f(s),f(t)\in \mathrm{U}(R')$，故 $f(a)f(s)^{-1}=f(b)f(t)^{-1}$. 不难验证，$g$ 是环同态.

又若环同态 h：$S^{-1}R\to R'$使得 $h\varphi=f$，则对于任意 $a/s\in S^{-1}R$，均有 $h(a/s)=h((a/1)(s/1)^{-1})=f(a)f(s)^{-1}=g(a/s)$，所以 $h=g$. □

下面讨论环 R 与其分式环 $S^{-1}R$ 的理想间的关系.

命题 2.5.3 设 S 是环 R 的乘法集，$\varphi:R\to S^{-1}R$ 是正则同态. 则

(1) 若 I 是 R 的理想，则

$$S^{-1}I=\{a/s\mid a\in I,\ s\in S\}$$

是 $S^{-1}R$ 的理想；并且 $S^{-1}I=S^{-1}R\Leftrightarrow I\cap S\neq\varnothing$. 又若 R 的理想 $I_1\subseteq I_2$，则 $S^{-1}I_1\subseteq S^{-1}I_2$.

(2) 若 J 是 $S^{-1}R$ 的理想，则 $I=\varphi^{-1}(J)$是 R 的理想，并且 $S^{-1}I=J$.

(3) $S^{-1}R$ 的素理想一一保序(关于包含关系)对应于 R 的与 S 不交的素理想.

证明 (1) 直接按定义验证 $S^{-1}I$ 是 $S^{-1}R$ 的理想. 若 $S^{-1}I=S^{-1}R$，则存在 $a\in I$ 和 $s\in S$ 使得 $a/s=1/1$，从而存在 $u\in S$ 使得 $ua=us\in I\cap S$. 反之，若存在 $u\in I\cap S$，则 $u/1\in S^{-1}I$，且 $u/1$ 在 $S^{-1}R$ 中有逆元 $1/u$，所以，$S^{-1}I=S^{-1}R$. 按定义容易验证，若 $I_1\subseteq I_2$，则 $S^{-1}I_1\subseteq S^{-1}I_2$.

(2) 容易验证 $I=\varphi^{-1}(J)$是 R 的理想. 若 $a/s\in S^{-1}I$，$a\in I$，$s\in S$，则 $a/s=(a/1)(1/s)=\varphi(a)(1/s)\in J$. 反之，若 $b/t\in$

J，$b\in R$，$t\in S$，则 $\varphi(b)=b/1=(b/t)(t/1)\in J$，于是 $b\in I$，从而 $b/t\in S^{-1}I$，所以 $S^{-1}I=J$.

(3) 设 P 是 R 的素理想，且 $P\cap S=\varnothing$. 由(1)和(2)，$S^{-1}P$ 是 $S^{-1}R$ 的理想，且 $S^{-1}P\neq S^{-1}R$. 设 $a/s, b/t\in S^{-1}R$；$a,b\in R$；$s,t\in S$. 若 $(a/s)(b/t)=c/u\in S^{-1}P$，$c\in P$，$u\in S$；则存在 $v\in S$ 使得 $vabu=vstc\in P$. 由于 $vu\notin P$，且 P 是素理想，故 $ab\in P$，从而 $a\in P$ 或 $b\in P$，进而 $a/s\in S^{-1}P$ 或 $b/t\in S^{-1}P$，所以 $S^{-1}P$ 是 $S^{-1}R$ 的素理想；且有 $\varphi^{-1}(S^{-1}P)=P$. 这是因为，若 $a\in\varphi^{-1}(S^{-1}P)$，则 $\varphi(a)=a/1=b/t\in S^{-1}P$，其中 $b\in P$，$t\in S$，于是存在 $u\in S$ 使 $uat=ub\in P$. 由于 $ut\notin P$，所以 $a\in P$，从而 $\varphi^{-1}(S^{-1}P)\subseteq P$. 而反包含是显然的.

设 Q 是 $S^{-1}R$ 的素理想，容易验证，$P=\varphi^{-1}(Q)$ 是 R 的素理想，$P\cap S=\varnothing$，且 $S^{-1}P=Q$.

这样，φ^{-1} 和 S^{-1} 就是 $S^{-1}R$ 的素理想和 R 的与 S 不交的素理想间的一对互逆映射. □

2.5.2　分式模、分式化函子

设 S 是环 R 的乘法集，M 是 R-模. 定义 $S\times M$ 的二元关系如下：对于 (s,m)，$(t,n)\in S\times M$，

$$(s,m)\sim(t,n)\Leftrightarrow \text{存在 } u\in S \text{ 使得 } u(tm-sn)=0.$$

这是 $M\times S$ 的一个等价关系，记 $(s,m)\in S\times M$ 所在的等价类为 m/s，且记商集 $(S\times M)/\sim=\{m/s\mid m\in M,\ s\in S\}$ 为 $S^{-1}M$. 定义 $S^{-1}M$ 的加法以及 $S^{-1}R$ 在 $S^{-1}M$ 上的作用如下：

$$m/s+n/t=(tm+sn)/st,\qquad (a/u)(m/s)=am/us,$$

其中 m/s，$n/t\in S^{-1}M$，$a/u\in S^{-1}R$. 容易验证，上述运算与代表元的选择无关，且使 $S^{-1}M$ 成为一个 $S^{-1}R$-模，叫做 M 的关于环 R 的乘法集 S 的**分式模**. 正则同态 $\varphi: R\to S^{-1}R$ 使得 $S^{-1}M$ 也是 R-模. 令

$$\varphi:\ M\to S^{-1}M;\ m\mapsto m/1.$$

这是 R-模同态，叫做**正则 R-同态**. 不难验证，$\mathrm{Ker}\varphi=\{m\in M\mid$ 存在 $s\in S$ 使 $sm=0\}$. 分式模 $S^{-1}M$ 具有如下的可除性：对于任意 $s\in S$ 和 $m/t\in S^{-1}M$，存在 $m/st\in S^{-1}M$ 使得 $m/t=s(m/st)$.

设 $f:M\to N$ 是 R-模同态. 令

$$S^{-1}f:\ S^{-1}M\to S^{-1}N;\ m/s\mapsto f(m)/s.$$

容易验证这是 $S^{-1}R$-模同态. 又若 $g:N\to P$ 也是 R-模同态，则 $S^{-1}(gf)=(S^{-1}g)(S^{-1}f)$；并且 $S^{-1}1_M=1_{S^{-1}M}$. 这样得到一个从 R-模范畴到 $S^{-1}R$-模范畴的共变函子 $S^{-1}:\mathscr{M}_R\to\mathscr{M}_{S^{-1}R}$，叫做**分式化函子**.

命题 2.5.4 设 S 是环 R 的乘法集. 则

(1) 若 $f,g\in\mathrm{Hom}_R(M,N)$，则 $S^{-1}(f+g)=S^{-1}f+S^{-1}g$.

(2) 若 $f:M\to N$ 是 R-单同态，则 $S^{-1}f:S^{-1}M\to S^{-1}N$ 是 $S^{-1}R$-单同态.

证明 (1) 对于任意 $m/s\in S^{-1}M$，$S^{-1}(f+g)(m/s)=(f+g)(m)/s=(f(m)+g(m))/s=(S^{-1}f)(m/s)+(S^{-1}g)(m/s)=(S^{-1}f+S^{-1}g)(m/s)$. 所以(1)成立.

(2) 若 $m/s\in S^{-1}M$ 使得 $(S^{-1}f)(m/s)=0$，则 $f(m)/s=0$，于是存在 $u\in S$ 使得 $uf(m)=f(um)=0$，从而 $um=0$，进而 $m/s=um/us=0$. 所以 $S^{-1}f$ 是单射. □

现在讨论分式化函子 $S^{-1}:\mathscr{M}_R\to\mathscr{M}_{S^{-1}R}$ 与由正则同态 $\varphi:R\to S^{-1}R$ 导出的换环函子 $S^{-1}R\underset{R}{\otimes}-:\mathscr{M}_R\to\mathscr{M}_{S^{-1}R}$ 之间的关系.

命题 2.5.5 设 S 是环 R 的乘法集，M 和 N 是 R-模. 则

(1) $\eta_M:\ S^{-1}M\to S^{-1}R\underset{R}{\otimes}M;\ m/s\mapsto(1/s)\otimes m$ 是 $S^{-1}R$-模同构.

(2) 若 $f:M\to N$ 是 R-同态，则下图交换：

$$\begin{array}{ccc} S^{-1}M & \xrightarrow{\eta_M} & S^{-1}R\underset{R}{\otimes}M \\ \Big\downarrow{\scriptstyle S^{-1}f} & & \Big\downarrow{\scriptstyle 1\otimes f} \\ S^{-1}N & \xrightarrow{\eta_N} & S^{-1}R\underset{R}{\otimes}N \end{array}$$

证明 (1) 首先，η_M 的定义是合理的：若 $m/s=n/t$；$m,n\in M$；$s,t\in S$，则存在 $u\in S$，使 $utm=usn$，于是$(1/s)\otimes m=(ut/ust)\otimes m=(1/ust)\otimes(utm)=(1/ust)\otimes(usn)=(us/ust)\otimes n=(1/t)\otimes n$. 进而不难验证，$\eta_M$ 是 $S^{-1}R$-同态. 另一方面，映射

$$S^{-1}R\times M\to S^{-1}M;\ (a/s,m)\mapsto(am)/s$$

是 $S^{-1}R$-双线性的，这导出唯一的 $S^{-1}R$-同态 ξ_M：$S^{-1}R\underset{R}{\otimes}M\to S^{-1}M$，使得 $\xi_M((a/s)\otimes m)=(am)/s$. 不难验证，$\eta_M$ 与 ξ_M 是互逆的，所以 η_M 是$S^{-1}R$-同构.

(2) 设 $m/s\in S^{-1}M$，则$(1\otimes f)\eta_M(m/s)=(1\otimes f)((1/s)\otimes m)=(1/s)\otimes f(m)$，而 $\eta_N(S^{-1}f)(m/s)=\eta_N(f(m)/s)=(1/s)\otimes f(m)$. 所以$(1\otimes f)\eta_M=\eta_N(S^{-1}f)$. □

由上述命题可知，函子 S^{-1}与 $S^{-1}R\underset{R}{\otimes}-$ 自然同构，因而具有许多相同的性质.

命题 2.5.6 *设 S 是环R 的乘法集，则函子 S^{-1}和 $S^{-1}R\underset{R}{\otimes}-$：$\mathcal{M}_R\to\mathcal{M}_{S^{-1}R}$是正合的.*

证明 设 $0\longrightarrow A\xrightarrow{f}B\xrightarrow{g}C\longrightarrow 0$ 是 R-模同态短正合列. 则下图交换：

$$\begin{array}{ccccccccc} 0 & \longrightarrow & S^{-1}A & \xrightarrow{S^{-1}f} & S^{-1}B & \xrightarrow{S^{-1}g} & S^{-1}C & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle\eta_A} & & \Big\downarrow{\scriptstyle\eta_B} & & \Big\downarrow{\scriptstyle\eta_C} & & \\ 0 & \longrightarrow & S^{-1}R\underset{R}{\otimes}A & \xrightarrow{1\otimes f} & S^{-1}R\underset{R}{\otimes}B & \xrightarrow{1\otimes g} & S^{-1}R\underset{R}{\otimes}C & \longrightarrow & 0 \end{array}$$

其中 η_A,η_B 和 η_C 是命题 2.5.5 中的自然同构. 由命题 2.5.4 的(2)和定理 2.4.3, 立得上图中的上下两行均正合, 从而 S^{-1} 和 $S^{-1}R\otimes_R -$ 是正合的. □

由上述命题立得

推论 2.5.7 设 S 是环 R 的乘法集, 则 $S^{-1}R$ 是平坦 R-模. □

命题 2.5.8 设 S 是环 R 的乘法集, N 和 P 是 R-模 M 的子模. 则

(1) $S^{-1}(N+P)=S^{-1}N+S^{-1}P$;

(2) $S^{-1}(N\cap P)=S^{-1}N\cap S^{-1}P$;

(3) $S^{-1}(M/N)\simeq S^{-1}M/S^{-1}N$ ($S^{-1}R$-模同构).

证明 (1)和(2)可由定义直接验证. 函子 S^{-1} 作用在短正合列 $0\to N\to M\to M/N\to 0$ 上, 由命题 2.5.6, 得短正合列 $0\to S^{-1}N\to S^{-1}M\to S^{-1}(M/N)\to 0$, 从而(3)成立.

命题 2.5.9 设 S 是环 R 的乘法集, M 和 N 是 R-模, 则有 $S^{-1}R$-模同构:

(1) $S^{-1}(M\oplus N)\simeq S^{-1}M\oplus S^{-1}N$;

(2) $S^{-1}(M\otimes_R N)\simeq S^{-1}M\otimes_{S^{-1}R} S^{-1}N$.

证明 (1) 由命题 2.5.8 的(1)和(2)得到, 或由函子 $S^{-1}R\otimes_R -$ 保持直和以及与 S^{-1} 的自然同构得到.

(2) 映射 $(S^{-1}M)\times(S^{-1}N)\to S^{-1}(M\otimes_R N)$; $(m/s,n/t)\mapsto(m\otimes n)/st$ 是 $S^{-1}R$-双线性的, 导出唯一的 $S^{-1}R$-同态 φ: $S^{-1}M\otimes_{S^{-1}R}S^{-1}N\to S^{-1}(M\otimes_R N)$ 使得 $\varphi((m/s)\otimes(n/t))=(m\otimes n)/st$. 而 $\psi: S^{-1}(M\otimes_R N)\to S^{-1}M\otimes_{S^{-1}R}S^{-1}N$; $(m\otimes n)/s\mapsto(m/s)\otimes(n/1)$ 也是 $S^{-1}R$-同态, 且 φ 与 ψ 是互逆的. 所以 φ 即为所需同构. □

命题 2.5.10 设 S 是环 R 的乘法集. 则

(1) 若 M 是自由R-模, 则 $S^{-1}M$ 是自由$S^{-1}R$-模.

(2) 若 M 是投射R-模, 则 $S^{-1}M$ 是投射$S^{-1}R$-模.

(3) 若 M 是有限生成R-模, 则 $S^{-1}M$ 是有限生成$S^{-1}R$-模.

证明 (1) 由命题2.4.6, $S^{-1}R\underset{R}{\otimes}M$ 是自由$S^{-1}R$-模. 再由命题2.5.5的(1), $S^{-1}M$ 是自由$S^{-1}R$-模.

(2) 同(1)可证.

(3) 若 M 是由 n 个元素生成的R-模, 则 M 是一个秩为 n 的自由 R-模F 的同态像, 即有 $F\to M\to 0$ 正合. 由于函子 S^{-1}是正合的, $S^{-1}F\to S^{-1}M\to 0$ 也是正合的. 且由命题2.4.6的(1), $S^{-1}F$ 是秩为 n 的自由 $S^{-1}R$-模, 所以 $S^{-1}M$ 是有限生成的 $S^{-1}R$-模. □

命题 2.5.11 设 S 是环R 的乘法集, M 是有限生成R-模. 则 $S^{-1}(\mathrm{Ann}_R(M))=\mathrm{Ann}_{S^{-1}R}(S^{-1}M)$.

证明 设 M 是由$\{x_1,\cdots,x_n\}$生成的 R-模, 则 $S^{-1}M$ 是由$\{x_1/1,\cdots,x_n/1\}$生成的 $S^{-1}R$-模. 记 $I_i=\mathrm{Ann}_R(x_i)$, 则 $Rx_i\simeq R/I_i$. 由命题2.5.8的(3), $(S^{-1}R)(x_i/1)=S^{-1}(Rx_i)\simeq S^{-1}R/S^{-1}I_i$, 从而 $S^{-1}(\mathrm{Ann}_R(x_i))=\mathrm{Ann}_{S^{-1}R}(x_i/1)$. 所以 $S^{-1}(\mathrm{Ann}_R(M))=S^{-1}(\bigcap\limits_{i=1}^{n}\mathrm{Ann}_R(x_i))=\bigcap\limits_{i=1}^{n}S^{-1}(\mathrm{Ann}_R(x_i))=\bigcap\limits_{i=1}^{n}\mathrm{Ann}_{S^{-1}R}(x_i/1)=\mathrm{Ann}_{S^{-1}R}(S^{-1}M)$. □

2.5.3 局部化、局部整体性质

设 $\mathfrak{p}$ 是环 R 的素理想, 则 $S=R\backslash\mathfrak{p}$ 是 R 的乘法集. 记分式环 $S^{-1}R$ 为$R_{\mathfrak{p}}$, 叫做 R 在素理想 $\mathfrak{p}$ 处的**局部化**. 由命题2.5.3的(3), $R_{\mathfrak{p}}$的素理想与 R 的含于 $\mathfrak{p}$ 中的素理想一一保序对应, 从而 $R_{\mathfrak{p}}$ 有唯一的极大理想 $\mathfrak{p}_{\mathfrak{p}}=S^{-1}\mathfrak{p}=\{a/s\mid a\in\mathfrak{p},\ s\in R\backslash\mathfrak{p}\}$. 所以, $R_{\mathfrak{p}}$是局部环. 另一方面, 商环 $R/\mathfrak{p}$ 的素理想与 R 的包含 $\mathfrak{p}$ 的素理想一一保序对应. 这提供了研究环 R 的素理想的两个重要

途径. 设 $x\in R$. 若 $x\notin\mathfrak{p}$, 则 $x/1$ 在 $R_{\mathfrak{p}}$ 中可逆. 又由定理1.1.3, 只要 $x\notin\mathrm{Nil}(R)$, 则存在 R 的素理想 $\mathfrak{p}$ 使得 $x\notin\mathfrak{p}$, 从而 $x/1$ 在 $R_{\mathfrak{p}}$ 中可逆. 这是局部化的重要好处.

例如, 设 p 是一个素数, 整数环 $\mathbb{Z}$ 在素理想 $\mathfrak{p}=(p)$处的局部化 $\mathbb{Z}_{\mathfrak{p}}=\{a/b\in\mathbb{Q}\mid a,b\in\mathbb{Z},(b,p)=1\}$, 每个与 p 互素的整数 b 均可作为分母. 这表明, $\mathbb{Z}_{\mathfrak{p}}$ 与 $\mathbb{Z}$ 的分式域 $\mathbb{Q}$ 已相当接近.

设 $\mathfrak{p}$ 是环 R 的素理想, $S=R\backslash\mathfrak{p}$, M 是 R-模. 记 $M_{\mathfrak{p}}=S^{-1}M$, 叫做 M 在 $\mathfrak{p}$ 处的**局部化**. 若 $f:M\to N$ 是 R-模同态, 记 $S^{-1}R$-同态 $S^{-1}f:S^{-1}M\to S^{-1}N$ 为 $f_{\mathfrak{p}}:M_{\mathfrak{p}}\to N_{\mathfrak{p}}$. 且称分式化函子 $S^{-1}:\mathscr{M}_R\to\mathscr{M}_{S^{-1}R}$ 为在素理想 $\mathfrak{p}$ 处的**局部化函子**.

在几何和分析中, 人们研究一点及其附近的某种性质, 并希望通过各点的这种局部性质来把握整体性质. 这种通过局部把握整体的思想方法, 在代数数论中也有成功的应用, 且已成为代数学中的一个有效方法.

关于环或模的某个性质 P 称为是**局部整体性质**, 如果对于每个环 R 或 R-模 M, R 或 M 具有性质 P 当且仅当对每个 $\mathfrak{p}\in\mathrm{Spec}\,R$, $R_{\mathfrak{p}}$ 或 $M_{\mathfrak{p}}$ 均有性质 P. 这样, 要检验 R 或 M 是否具有局部整体性质 P, 只需检验每个局部化 $R_{\mathfrak{p}}$ 或 $M_{\mathfrak{p}}$ 是否具有性质 P. 由于 $R_{\mathfrak{p}}$ 或 $M_{\mathfrak{p}}$ 通常有比 R 或 M 简单的结构, 后一检验往往要容易得多. 这是局部化方法的好处. 下面给出关于环和模的一些基本的局部整体性质.

命题 2.5.12 设 M 是 R-模, 则下列条件等价:

(1) $M=0$;

(2) 对于每个 $\mathfrak{p}\in\mathrm{Spec}\,R$, $M_{\mathfrak{p}}=0$;

(3) 对于每个 $\mathfrak{q}\in\mathrm{Max}\,R$, $M_{\mathfrak{q}}=0$.

证明 (1)⇒(2)⇒(3): 显然.

(3)⇒(1): 假定存在 $x\in M\backslash\{0\}$. 则 $1\notin\mathrm{Ann}_R(x)$, 从而 $\mathrm{Ann}_R(x)\neq R$, 故存在 $\mathfrak{q}\in\mathrm{Max}\,R$ 使得 $\mathrm{Ann}_R(x)\subseteq\mathfrak{q}$. 由(3), 在

$M_{\mathfrak{q}}$ 中 $x/1=0$. 故存在 $u\in R\backslash\mathfrak{q}$ 使得 $ux=0$，从而 $u\in \mathrm{Ann}_R(x)\subseteq\mathfrak{q}$. 这与 $u\in R\backslash\mathfrak{q}$ 矛盾. 所以 $M=0$. □

命题 2.5.13　设 $f:M\to N$ 是 R-模同态. 则

(1) f 是单射 $\Leftrightarrow$ 对于每个 $\mathfrak{p}\in \mathrm{Spec}\,R$，$f_{\mathfrak{p}}$ 是单射
$\Leftrightarrow$ 对于每个 $\mathfrak{q}\in \mathrm{Max}\,R$，$f_{\mathfrak{q}}$ 是单射.

(2) f 是满射 $\Leftrightarrow$ 对于每个 $\mathfrak{p}\in \mathrm{Spec}\,R$，$f_{\mathfrak{p}}$ 是满射
$\Leftrightarrow$ 对于每个 $\mathfrak{q}\in \mathrm{Max}\,R$，$f_{\mathfrak{q}}$ 是满射.

(3) f 是双射 $\Leftrightarrow$ 对于每个 $\mathfrak{p}\in \mathrm{Spec}\,R$，$f_{\mathfrak{p}}$ 是双射
$\Leftrightarrow$ 对于每个 $\mathfrak{q}\in \mathrm{Max}\,R$，$f_{\mathfrak{q}}$ 是双射.

证明　(1) 由于局部化函子是正合的，由正合列 $0\to\mathrm{Ker}f\to M\xrightarrow{f}N$ 导出正合列 $0\to(\mathrm{Ker}f)_{\mathfrak{p}}\to M_{\mathfrak{p}}\xrightarrow{f_{\mathfrak{p}}}N_{\mathfrak{p}}$. 对 $\mathrm{Ker}f$ 用命题 2.5.12，即得(1).

(2) 由正合列 $M\xrightarrow{f}N\to\mathrm{Coker}f\to0$ 导出正合列 $M_{\mathfrak{p}}\xrightarrow{f_{\mathfrak{p}}}N_{\mathfrak{p}}\to(\mathrm{Coker}f)_{\mathfrak{p}}\to0$. 对 $\mathrm{Coker}f$ 用命题 2.5.12，即得(2).

(3) 由(1)和(2)即得. □

命题 2.5.14　设 M 是 R-模，则下列条件等价：

(1) M 是平坦 R-模；

(2) 对于每个 $\mathfrak{p}\in \mathrm{Spec}\,R$，$M_{\mathfrak{p}}$ 是平坦 $R_{\mathfrak{p}}$-模；

(3) 对于每个 $\mathfrak{q}\in \mathrm{Max}\,R$，$M_{\mathfrak{q}}$ 是平坦 $R_{\mathfrak{q}}$-模.

证明　(1)⇒(2)：设 $f:A\to B$ 是 $R_{\mathfrak{p}}$-模单同态. 通过正则环同态 $R\to R_{\mathfrak{p}}$；$a\mapsto a/1$，A 和 B 也是 R-模，且 $f:A\to B$ 也是 R-单同态. 若 M 是平坦 R-模，则 $1\otimes f$: $M\underset{R}{\otimes}A\to M\underset{R}{\otimes}B$ 是 R-单同态. 由局部化函子的正合性，$(1\otimes f)_{\mathfrak{p}}:(M\underset{R}{\otimes}A)_{\mathfrak{p}}\to(M\underset{R}{\otimes}B)_{\mathfrak{p}}$ 是 $R_{\mathfrak{p}}$-模单同态. 又由于下图是交换的：

$$\begin{array}{ccc} M_{\mathfrak{p}}\underset{R_{\mathfrak{p}}}{\otimes}A_{\mathfrak{p}} & \xrightarrow{1\otimes f_{\mathfrak{p}}} & M_{\mathfrak{p}}\underset{R_{\mathfrak{p}}}{\otimes}B_{\mathfrak{p}} \\ \downarrow{\eta_A} & & \downarrow{\eta_B} \\ (M\underset{R}{\otimes}A)_{\mathfrak{p}} & \xrightarrow{(1\otimes f)_{\mathfrak{p}}} & (M\underset{R}{\otimes}B)_{\mathfrak{p}} \end{array},$$

其中 η_A 和 η_B 是命题 2.5.9 的(2)中给出的 $R_{\mathfrak{p}}$-同构. 于是由 $(1\otimes f)_{\mathfrak{p}}$是单射立得 $1\otimes f_{\mathfrak{p}}$ 是单射. 由于 A 和 B 均是 $R_{\mathfrak{p}}$-模，故 $A_{\mathfrak{p}}=A$，$B_{\mathfrak{p}}=B$，且 $f_{\mathfrak{p}}=f$，所以，$1\otimes f$: $M_{\mathfrak{p}}\underset{R_{\mathfrak{p}}}{\otimes}A\to M_{\mathfrak{p}}\underset{R_{\mathfrak{p}}}{\otimes}B$ 是单射，从而 $M_{\mathfrak{p}}$ 是平坦 $R_{\mathfrak{p}}$-模.

(2)⇒(3)：显然.

(3)⇒(1)：设 f: $A\to B$ 是 R-模单同态. 对于任意 $\mathfrak{q}\in \operatorname{Max} R$，由命题2.5.4 的(2)，$f_{\mathfrak{q}}$：$A_{\mathfrak{q}}\to B_{\mathfrak{q}}$ 是 $R_{\mathfrak{q}}$-单同态. 由条件(3)，$1\otimes f_{\mathfrak{q}}$：$M_{\mathfrak{q}}\underset{R_{\mathfrak{q}}}{\otimes}A_{\mathfrak{q}}\to M_{\mathfrak{q}}\underset{R_{\mathfrak{q}}}{\otimes}B_{\mathfrak{q}}$ 是 $R_{\mathfrak{q}}$-单同态. 仍由上述交换图可知，$(1\otimes f)_{\mathfrak{q}}:(M\underset{R}{\otimes}A)_{\mathfrak{q}}\to(M\underset{R}{\otimes}B)_{\mathfrak{q}}$ 是 $R_{\mathfrak{q}}$-单同态. 再由命题 2.5.13，$1\otimes f: M\underset{R}{\otimes}A\to M\underset{R}{\otimes}B$ 是 R-单同态. 所以 M 是平坦 R-模. □

定理 2.5.15 设 R 是局部环，则每个有限生成投射 R-模均是自由 R-模.

证明 设 P 是有限生成投射 R-模，则存在秩为 n 的自由 R-模 F 和 R-满同态 $f: F\to P$. 令 n 是满足上述条件的最小正整数. 记 $K=\operatorname{Ker} f$. 由于 P 是投射的，短正合列 $0\to K\to F\xrightarrow{f}P\to 0$ 是可裂的，于是 $F=P'\oplus K$，其中 $P'\simeq P$. 设 R 的唯一的极大理想为 I. 若能证明 $K\subseteq IF$，则由推论 1.2.2 可知，$F=P'\simeq P$ 是自由的.

设$\{x_1,\cdots,x_n\}$是 F 的基，$x=\sum\limits_{i=1}^{n}r_ix_i$，$r_i\in R$. 假定 $x\in K\setminus IF$，则存在某个 r_i，例如 r_1，使得 $r_1\notin I$. 由定理 1.1.6 可

知，$r_1\in \mathrm{U}(R)$，从而 $x_1=r_1^{-1}x-r_1^{-1}\sum_{i=2}^{n}r_ix_i$，进而 $f(x_1)=-\sum_{i=2}^{n}r_1^{-1}r_if(x_i)$. 这表明 P 可由 $f(x_2),\cdots,f(x_n)$ 生成. 令 $F'=\sum_{i=2}^{n}Rx_i$，$f':F'\to P$ 是 f 在 F' 上的限制，则 F' 是自由的且 f' 是满射，这与 n 的最小性矛盾. □

习 题 2.5

1. 设 S 是环 R 的乘法集，I,J 是 R 的理想. 证明：

(1) $S^{-1}R=0\Leftrightarrow 0\in S$；$S^{-1}R=R\Leftrightarrow S\subseteq \mathrm{U}(R)$.

(2) $S^{-1}(IJ)=(S^{-1}I)(S^{-1}J)$.

(3) $\sqrt{S^{-1}I}=S^{-1}\sqrt{I}$；$S^{-1}(\mathrm{Nil}(R))=\mathrm{Nil}(S^{-1}R)$.

2. 设 R 是非零环，$\Sigma=\{R$ 的乘法集$\mid 0\notin S\}$. 证明：Σ 关于包含关系有极大元，且 $S\in\Sigma$ 是 Σ 中的极大元 $\Leftrightarrow R\backslash S$ 是 R 的极小素理想.

3. 设 S 是环 R 的乘法集，$0\notin S$. 证明：若 R 是整环(主理想整环，唯一因子分解整环)，则 $S^{-1}R$ 也是整环(主理想整环，唯一因子分解整环).

4. 设 $R=\mathbb{Z}/6\mathbb{Z}$，$S=\{\bar{1},\ \bar{2},\ \bar{4}\}$. 证明：$S^{-1}R\simeq\mathbb{Z}/3\mathbb{Z}$ 是域(但 R 不是整环).

5. 设 $\mathfrak{p}$ 是环 R 的素理想，$\mathfrak{m}$ 是 $R_{\mathfrak{p}}$ 中的唯一的极大理想. 证明：$R_{\mathfrak{p}}/\mathfrak{m}$ 同构于整环 $R/\mathfrak{p}$ 的分式域.

6. 设 $\mathfrak{p}_1,\cdots,\mathfrak{p}_n$ 是环 R 的素理想. 证明：

(1) $S=\bigcap_{i=1}^{n}(R\backslash\mathfrak{p}_i)=R\backslash(\bigcup_{i=1}^{n}\mathfrak{p}_i)$ 是 R 的乘法集.

(2) $S^{-1}R$ 是半局部环，且

$\mathrm{Max}(S^{-1}R)=\{S^{-1}\mathfrak{q}\mid\mathfrak{q}$ 是 $\{\mathfrak{p}_1,\cdots,\mathfrak{p}_n\}$ 中的极大元$\}$.

(3) $R_{\mathfrak{p}_i}\simeq(S^{-1}R)_{S^{-1}\mathfrak{p}_i}$ (环同构)，$i=1,\cdots,n$.

(4) 若 R 是整环，则 $S^{-1}R=\bigcap_{i=1}^{n}R_{\mathfrak{p}_i}$ (等式两边均在 R 的分式域中).

7. 设 S 是环 R 的乘法集. 证明：若 M 是内射(平坦)R-模，则 $S^{-1}M$ 是内射(平坦)$S^{-1}R$-模.

8. 设 S 是整环 R 的乘法集，K 是 R 的分式域，M 是 R-模，$\mathrm{T}(M)$ 是 M 的扭子模. 证明：

(1) R-模同态 $f: M\to K\otimes_R M;\ m\mapsto 1\otimes m$ 的核 $\mathrm{Ker}f=\mathrm{T}(M)$.

(2) $\mathrm{T}(S^{-1}M)=S^{-1}(\mathrm{T}(M))$.

(3) M 是(无)扭 R-模 $\Leftrightarrow$ 对于每个 $\mathfrak{p}\in\mathrm{Spec}\,R$，$M_{\mathfrak{p}}$ 是(无)扭 $R_{\mathfrak{p}}$-模 $\Leftrightarrow$ 对于每个 $\mathfrak{m}\in\mathrm{Max}\,R$，$M_{\mathfrak{m}}$ 是(无)扭 $R_{\mathfrak{m}}$-模.

(4) 若 $a\in R$，a 不是 0 和单位，则存在 $\mathfrak{p}\in\mathrm{Spec}\,R$，使得 $a^{-1}\notin R_{\mathfrak{p}}$.

(5) $\bigcap_{\mathfrak{p}\in\mathrm{Spec}\,R}R_{\mathfrak{p}}=\bigcap_{\mathfrak{m}\in\mathrm{Max}\,R}R_{\mathfrak{m}}=R$ (注意，$R_{\mathfrak{p}}$ 均是 K 的子环).

(6) 设 $a,b\in R$，$ab\neq 0$. 则在 R 中 $a\mid b\Leftrightarrow$ 对于每个 $\mathfrak{p}\in\mathrm{Spec}\,R$，在 $R_{\mathfrak{p}}$ 中 $a\mid b\Leftrightarrow$ 对于每个 $\mathfrak{m}\in\mathrm{Max}\,R$，在 $R_{\mathfrak{m}}$ 中 $a\mid b$.

(7) 若 M 是有限生成投射 R-模，则对于每个 $\mathfrak{p}\in\mathrm{Spec}\,R$，$R_{\mathfrak{p}}$-模 $M_{\mathfrak{p}}$ 可自然地看成 K 上线性空间 $K\otimes_R M$ 的子集，且有 $\bigcap_{\mathfrak{p}\in\mathrm{Spec}\,R}M_{\mathfrak{p}}=\bigcap_{\mathfrak{m}\in\mathrm{Max}\,R}M_{\mathfrak{m}}=M$.

2.6 主理想整环上的有限生成模

本节给出主理想整环 R 上的有限生成模的结构定理. 特别地，当 $R=\mathbb{Z}$ 是整数环时，可得到有限生成 Abel 群的结构定理；而当 $R=k[x]$是域 k 上的多项式环时，可导出线性代数中矩阵的相似标准型定理. 本节的主要结果及其证法还将用于证明 Dedekind 整环上的有限生成模的结构定理.

首先证明关于主理想整环上的有限秩自由模的子模的一个关键性结果.

定理 2.6.1 设 R 是主理想整环，M 是秩为 n 的自由 R-模 F 的子模.

(1) 存在 F 的基 $X=\{x_1,\cdots,x_n\}$ 和 $r_1,\cdots,r_t\in R\setminus\{0\}$，其中 $r_1\mid r_2\mid\cdots\mid r_t$，$0\leqslant t\leqslant n$，使得 $\{r_1x_1,\cdots,r_tx_t\}$ 是 M 的基.

(2) 又若存在 F 的基 $Z=\{z_1,\cdots,z_n\}$ 和 $s_1,\cdots,s_t\in R\setminus\{0\}$，其中 $s_1\mid s_2\mid\cdots\mid s_t$，使得 $\{s_1z_1,\cdots,s_tz_t\}$ 也是 M 的基，则 s_i 与 r_i 相伴(即 s_i 与 r_i 仅相差一个单位因子)，$i=1,\cdots,t$.

证明 (1) 对秩 n 进行归纳. 当 $n=1$ 时，$F\simeq R$，显然(1)成立. 当 $n\geqslant 2$ 时，不妨设 $M\neq 0$. 对于 F 的任意基 $Y=\{y_1,\cdots,y_n\}$，令

$$p: M\to R;\ a_1y_1+\cdots+a_ny_n\mapsto a_1,$$

这是一个 R-同态. 记 $I_Y=\mathrm{Im}p$，这是 R 的主理想. 令 $\Sigma=\{I_Y\mid Y$ 是 F 的基$\}$，则 Σ 非空. Σ 关于包含关系含有极大元，这可不用 Zorn 引理而用反证法直接证明：假如对于 Σ 中的每个理想 I 都有 $J\in\Sigma$ 使得 $I\subset J$，则可得无限升链 $I_1\subset\cdots\subset I_n\subset\cdots$. $I=\bigcup\limits_{i=1}^{\infty}I_n$ 也是 R 的理想，于是 $I=Ra$. 因 $a\in I$，从而 a 必属于某个 I_n. 于是 $I_n\subset I_{n+1}\subseteq I\subseteq I_n$，这矛盾. 设 $I_Y=Rr_1$ 是 Σ 中的一个极大元，其中 $Y=\{y_1,\cdots,y_n\}$ 是 F 的一个基，$r_1\in R\setminus\{0\}$，且 $Rr_1=\mathrm{Im}p$. 由于 $Rr_1\simeq R$ 是投射的，由定理2.3.1，存在 R-同态 $q: Rr_1\to M$ 使得 $pq=1_{Rr_1}$. 于是 $M=\mathrm{Ker}p\oplus\mathrm{Im}q$. 因 $\mathrm{Ker}p\subseteq Ry_2\oplus\cdots\oplus Ry_n=F'$，由归纳假定，存在 F' 的基 $\{x_2,\cdots,x_n\}$ 和 $r_2,\cdots,r_t\in R\setminus\{0\}$，其中 $r_2\mid\cdots\mid r_t$，$t\leqslant n$，使得 $\{r_2x_2,\cdots,r_tx_t\}$ 是 $\mathrm{Ker}p$ 的基. 设 $q(r_1)=a_1y_1+\cdots+a_ny_n$. 因 $pq=1_{Rr_1}$，故 $a_1=r_1$. 下证 $r_1\mid a_i$，$i=2,\cdots,n$. 假定 $r_1\nmid a_2$. 设 $(r_1,a_2)=d$，$r_1=db_1$，$a_2=db_2$，则 $(b_1,b_2)=1$. 于是存在 $u_1,u_2\in R$ 使得 b_1u_1

$+b_2u_2=1$. 令 $z_1=b_1y_1+b_2y_2$, $z_2=u_2y_1-u_1y_2$. 由于 $\begin{pmatrix} b_1 & u_2 \\ b_2 & -u_1 \end{pmatrix}$是可逆方阵，其逆为$\begin{pmatrix} u_1 & u_2 \\ b_2 & -b_1 \end{pmatrix}$, 故 $Z=\{z_1,z_2,y_3,\cdots,y_n\}$是 F 的基，且 $q(r_1)=dz_1+a_3y_3+\cdots+a_ny_n$. 于是 $Rr_1\subset Rd\subseteq I_Z$，这与 $I_Y=Rr_1$ 的极大性矛盾. 所以 $r_1\mid a_2$. 同理可证 $r_1\mid a_i, i=3,\cdots,n$. 设 $a_i=a_i'r_1$; $a_i'\in R, i=2,3,\cdots,n$. 令 $x_1=y_1+a_2'y_2+\cdots+a_n'y_n\in F$. 则 $\mathrm{Im}\, q=Rr_1x_1$, $X=\{x_1,x_2,\cdots,x_n\}$是 F 的基，且$\{r_1x_1,\cdots,r_tx_t\}$是 M 的基. 再由 $r_1x_1+r_2y_2\in M$ 和 Rr_1 的极大性，用同上方法可证 $r_1\mid r_2$.

(2) 设从 F 的基X 到Z 的过渡矩阵为A, $Z=XA$，而从 M 的基$\{r_1x_1,\cdots,r_tx_t\}$到$\{s_1z_1,\cdots,s_tz_t\}$的过渡矩阵为 B，则

$$\begin{aligned} & Z\mathrm{diag}\{s_1,\cdots,s_t,0,\cdots,0\} \\ = & X\ \mathrm{diag}\{r_1,\cdots,r_t,0,\cdots,0\}\ \mathrm{diag}\{B,I_{n-t}\} \\ = & ZA^{-1}\ \mathrm{diag}\{r_1,\cdots,r_t,0,\cdots,0\}\ \mathrm{diag}\ \{B,I_{n-t}\}. \end{aligned}$$

所以，$\mathrm{diag}\{s_1,\cdots,s_t,0,\cdots,0\}=A^{-1}\mathrm{diag}\{r_1,\cdots,r_t,0,\cdots,0\}\ \mathrm{diag}\{B, I_{n-t}\}$. 比较上式两边的顺序主子式，可得 $r_1\mid s_1$, $r_1r_2\mid s_1s_2$, $\cdots$, $r_1\cdots r_t\mid s_1\cdots s_t$. 对称地可得 $s_1\mid r_1$, $\cdots$, $s_1\cdots s_t\mid r_1\cdots r_t$. 所以 r_i 与s_i 相伴，$i=1,\cdots,t$. □

定理 2.6.2 设 R 是主理想整环，M 是有限生成R-模.

(1) 存在 $n\geqslant 0$ 和 $r_1,\cdots,r_t\in R$，其中 r_i 不是0和单位，$r_1\mid r_2\mid\cdots\mid r_t$, $t\geqslant 0$，使得

$$M\simeq R^n\oplus R/(r_1)\oplus\cdots\oplus R/(r_t)\ (R\text{-模同构});$$

并且 n 和主理想$(r_1),\cdots,(r_t)$由 M 唯一确定.

(2) 存在 $n\geqslant 0$ 和 R 的素元$p_1,\cdots,p_k$(不必不同), $k\geqslant 0$，以及正整数 $e_1,\cdots,e_k$，使得

$$M\simeq R^n\oplus R/(p_1^{e_1})\oplus\cdots\oplus R/(p_k^{e_k})\ (R\text{-模同构});$$

并且 n 和理想$(p_1^{e_1}),\cdots,(p_k^{e_k})$由 M 唯一确定.

证明　(1) 存在性. 设 M 由 m 个元素生成. 则存在秩为 m 的自由 R-模 F 和 R-满同态 $f: F \to M$. 记 $K = \mathrm{Ker}f$, 则 $M \simeq F/K$. 由定理2.6.1, 存在 F 的基$\{x_1, \cdots, x_m\}$和 $a_1, \cdots, a_u \in R \setminus \{0\}$, 其中 $a_1 | \cdots | a_u$, $0 \leqslant u \leqslant m$, 使得$\{a_1 x_1, \cdots, a_u x_u\}$是 K 的基. 于是

$$\begin{aligned} M &\simeq F/K = (Rx_1 \oplus \cdots \oplus Rx_m)/(Ra_1 x_1 \oplus \cdots \oplus Ra_u x_u) \\ &\simeq (Rx_1/Ra_1 x_1) \oplus \cdots \oplus (Rx_u/Ra_u x_u) \oplus Rx_{u+1} \oplus \cdots \oplus Rx_m \\ &\simeq (R/(a_1)) \oplus \cdots \oplus (R/(a_u)) \oplus R^n, \end{aligned}$$

其中 $n = m - u$. 记 $a_1, \cdots, a_u$ 中后面 t 个不是单位的元素为 $r_1, \cdots, r_t$, 则 $M \simeq R^n \oplus R/(r_1) \oplus \cdots \oplus R/(r_t)$.

唯一性. 又若 $M \simeq R^{n'} \oplus R/(s_1) \oplus \cdots \oplus R/(s_{t'}) = M'$, 其中 $n' \geqslant 0$, s_i 不是 0 和单位, $s_1 | \cdots | s_{t'}$, $t' \geqslant 0$. 设 $h: M \to M'$是 R-同构. 令 $g = hf: F \to M'$, 则 $\mathrm{Ker}g = \mathrm{Ker}f = K$. 因 g 是满的, 可取 $y_i \in F$ 使得 $g(y_i) = \overline{1}_i$ 为 $R/(s_i)$的生成元, $i = 1, \cdots, t'$. $\{y_1, \cdots, y_{t'}\}$是 R-线性无关的. 这是因为, 假定存在不全为零的 $b_1, \cdots, b_{t'} \in R$ 使得 $\sum\limits_{i=1}^{t'} b_i y_i = 0$, 不妨设$(b_1, \cdots; b_{t'}) = 1$. 用 g 作用后得 $\sum\limits_{i=1}^{t'} b_i \overline{1}_i = 0$, 于是 $s_1 | b_i$, $i = 1, \cdots, t'$, 这矛盾. 再取$\{y_{t'+1}, \cdots, y_{t'+n'}\} \subseteq F$, 使得它们在 g 下的像组成$R^{n'}$ 的标准基, 容易证明$\{y_{t'+1}, \cdots, y_{t'+n'}\}$是 R- 线性无关的, 并且$\{y_1, \cdots, y_{t'+n'}\}$也是$R$- 线性无关的. 令 $F' = Ry_1 \oplus \cdots \oplus Ry_{t'+n'}$, 则 F' 是F 的自由子模, 且 $F = F' + K$. 令 $g' = g|_{F'}: F' \to M'$, 且记 $K' = \mathrm{Ker}g'$, 则 $K' = Rs_1 y_1 \oplus \cdots \oplus Rs_{t'} y_{t'} = F' \cap K \subseteq K$. 由定理2.6.1, 存在 K 的基 $\{z_1, \cdots, z_u\}$ 和 $b_1, \cdots, b_{t'} \in R$, 使得 $\{b_1 z_{u-t'+1}, \cdots, b_{t'} z_u\}$ 是 K' 的基. 下证 $Z = \{z_1, \cdots, z_{u-t'}, y_1, \cdots, y_{t'+n'}\}$ 是 F 的基. 若 $\sum\limits_{i=1}^{u-t'} c_i z_i + \sum\limits_{i=1}^{t'+n'} d_i y_i = 0$; $c_i, d_i \in R$, 则 $\sum\limits_{i=1}^{u-t'} c_i z_i$

$= -\sum_{i=1}^{t'+n'} d_i y_i \in F' \cap K = K'$. 由此可知每个 $c_i = 0$，进而每个 $d_i = 0$. 所以 Z 是R- 线性无关的. 再由 $F = F' + K$ 可知，每个 $x \in F$ 可由 Z 来R- 线性表示. 所以 Z 是F 的基，于是$(u - t') + (t' + n') = m = u + n$，从而 $n = n'$. 容易验证$\{z_1, \cdots, z_{u-t'}, s_1 y_1, \cdots, s_{t'} y_{t'}\}$ 是 K 的基. 根据定理2.6.1，$t = t'$，且 s_i 与r_i 相伴，$i = 1, \cdots, t$.

(2) 因主理想整环均是唯一因子分解整环，若 $r \in R$，r 不是 0 和单位，则在相伴意义下，r 可唯一地分解成$r = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$，其中 $p_1, \cdots, p_s$ 是R 中的两两互素的素元，$\alpha_i \geqslant 1$，$1 \leqslant i \leqslant s$. 由中国剩余定理可知，有 R-模同构$R/(\alpha) \simeq R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_s^{\alpha_s})$，并且理想$(p_1^{\alpha_1}), \cdots, (p_s^{\alpha_s})$由 $R/(r)$唯一确定. 应用上述分解于(1)即得(2). □

上述定理的(1)中的理想$(r_1), \cdots, (r_t)$叫做 M 的**不变因子**，而(2)中的理想$(p_1^{e_1}), \cdots, (p_k^{e_k})$叫做 M 的**初等因子**. 将不变因子中的每个 r_i 分解成素元幂 $p_j^{e_j}$ 的积，所有这些素元幂生成的理想$(p_j^{e_j})$组成 M 的初等因子. 反之，由 M 的初等因子，按条件 $r_1 | \cdots | r_t$，可确定 M 的不变因子. 上述定理中的 n 叫做M 的**自由秩**，记作 $\mathrm{rank}_R(M)$.

由上述定理可得

推论 2.6.3 设 R 是主理想整环，M 是有限生成R-模.

(1) 若 M 是无扭的，则 M 是自由的.

(2) 存在 M 的自由子模F，使得 $M = F \oplus \mathrm{T}(M)$，其中 $\mathrm{T}(M)$是 M 的扭子模. □

注 上述推论中，M 是有限生成的条件不可少. 例如，有理数加群$(\mathbb{Q}, +)$是无扭 $\mathbb{Z}$-模，但不是自由 $\mathbb{Z}$-模(习题 2.2.3).

应用定理 2.6.2 于 $R = \mathbb{Z}$，可得有限生成 Abel 群的结构定理.

定理 2.6.4 设 A 是有限生成 Abel 群，则

(1) $A\simeq\mathbb{Z}^n\oplus\mathbb{Z}/(r_1)\oplus\cdots\oplus\mathbb{Z}/(r_k)$,

其中 $n\geqslant0$，$k\geqslant0$，$r_1,\cdots,r_k\geqslant2$，且 $r_1\mid r_2\mid\cdots\mid r_k$；并且 n 和 $\{r_1,\cdots,r_k\}$ 由 A 唯一确定，分别称为 A 的**自由秩**和**不变因子**.

(2) $A\simeq\mathbb{Z}^n\oplus\mathbb{Z}/(p_1^{e_1})\oplus\cdots\oplus\mathbb{Z}/(p_s^{e_s})$,

其中 $n\geqslant0$，$s\geqslant0$；$p_1,p_2,\cdots,p_s$(不必不同)为素数，$e_1,\cdots,e_s\geqslant1$；并且 n 和 $\{p_1^{e_1},\cdots,p_s^{e_s}\}$ 由 A 唯一确定，后者称为 A 的**初等因子**. □

设 V 是域 F 上的 n 维线性空间，在 V 的给定基 X 下，V 的 F-线性变换 $\mathbf{A}\in\mathrm{Hom}_F(V,V)$ 与 F 上的 n 阶方阵 $A\in F^{n\times n}$ 一一对应，且 $\mathrm{Hom}_F(V,V)$ 与 $F^{n\times n}$ 作为 F 上的线性空间(n^2 维)同构.

取定一个 $\mathbf{A}\in\mathrm{Hom}_F(V,V)$. 设 $R=F[\lambda]$是 F 上的一元多项式环，定义 R 在 V 上的作用如下：

$$f(\lambda)\alpha=f(\mathbf{A})\alpha,\ f(\lambda)\in F[\lambda],\ \alpha\in V,$$

则 V 是有限生成R-模，U 是 V 的 R-子模当且仅当 U 是 V 的 F-子空间且对每个 $\alpha\in U$ 有 $\mathbf{A}\alpha\in U$，即 U 是 V 的 **$\mathbf{A}$-不变子空间**. 循环 R-子模 $R\alpha$，$\alpha\in V$，叫做 α 关于 $\mathbf{A}$ 的**循环子空间**，记作 $C(\alpha)$. 由于$\{\alpha,\mathbf{A}\alpha,\cdots,\mathbf{A}^n\alpha\}$是 F-线性相关的，存在 $f(\lambda)\neq0\in F[\lambda]$使得 $f(\mathbf{A})\alpha=0$. 设 $\mathrm{Ann}_R(\alpha)=(d_\alpha(\lambda))$，$d_\alpha(\lambda)\neq0$ 是 $F[\lambda]$中的首一多项式，则 $d_\alpha(\lambda)$就是 α 关于 $\mathbf{A}$ 的**最小多项式**. 由此可知，V 是有限生成扭 R-模，其自由 R-秩为 0. 设 $\mathrm{Ann}_R(V)=(d_{\mathbf{A}}(\lambda))$，$d_{\mathbf{A}}(\lambda)\neq0$ 是$F[\lambda]$中的首一多项式，则 $d_{\mathbf{A}}(\lambda)$就是线性变换 $\mathbf{A}$ 的**最小多项式**. 应用定理 2.6.2 于有限生成R-模 V，可得

定理 2.6.5 设 $\mathbf{A}$ 是数域 F 上的 n 维线性空间 V 的线性变换.

(1) 存在 $\alpha_i\in V$，α_i 的最小多项式为 $d_i(\lambda)$，$i=1,2,\cdots,k$；

$k\geqslant 0$，使得 $d_t(\lambda)|d_{t-1}(\lambda)|\cdots|d_1(\lambda)=d_{\mathbf{A}}(\lambda)$，且

$$V=C(\alpha_1)\oplus C(\alpha_2)\oplus\cdots\oplus C(\alpha_k);$$

并且$\{d_1(\lambda),\cdots,d_k(\lambda)\}$由 $\mathbf{A}$ 唯一确定，叫做 $\mathbf{A}$ 的**不变因子**.

(2) 存在 $\beta_i\in V$，β_i 的最小多项式为 $p_i(\lambda)^{e_i}$，$i=1,2,\cdots,s$；$s\geqslant 0$；$p_1(\lambda),\cdots,p_s(\lambda)$是 $F[\lambda]$中的首一不可约多项式，$e_1,\cdots,e_s\geqslant 1$，使得

$$V=C(\beta_1)\oplus C(\beta_2)\oplus\cdots\oplus C(\beta_s);$$

并且$\{p_1(\lambda)^{e_1},\cdots,p_s(\lambda)^{e_s}\}$由 $\mathbf{A}$ 唯一确定，叫做 $\mathbf{A}$ 的**初等因子**.

□

将上述定理翻译成矩阵表达的形式，可得域 F 上的 n 阶方阵的 F-相似标准形，以及全系不变量：不变因子和初等因子.

习 题 2.6

1. 设 R 是主理想整环，M 是有限生成 R-模. 证明：

(1) M 的每个子模均是有限生成 R-模.

(2) M 的自由秩等于 M 中 R-线性无关元素的最大个数.

2. 设 R 是主理想整环，$a,b\in R$，a 和 b 均不是 0 和单位. 试求 R-模 $R/(a)\oplus R/(b)$的不变因子.

3. 设 R 是环. 证明：若每个有限生成自由 R-模的任意子模均是自由 R-模，则 R 是主理想整环.

4. 设 A 是主理想整环 R 上的 $m\times n$ 矩阵. 证明：存在 R 上的可逆方阵 P 和 Q 使得 $PAQ=\mathrm{diag}\{\mathrm{diag}\{d_1,\cdots,d_r\},0\}$，其中 $0\neq d_i\in R$，且 $d_1|\cdots|d_r$，并且这样的 $d_1,\cdots,d_r$ 由 A 唯一(在相伴意义下)确定. 试用上述结果证明定理 2.6.1.

5. 试用良序化原理或 Zorn 引理证明：主理想整环 R 上的任意自由 R-模的每个子模均是自由 R-模.

6. 证明：$\coprod\limits_{i=1}^{\infty}\mathbb{Z}$ 是平坦 $\mathbb{Z}$-模，但不是投射 $\mathbb{Z}$-模.

第 3 章　Noether 环和 Artin 环

3.1　理想的准素分解

本节介绍的理想准素分解理论是交换环的经典理想论的支柱，也是代数几何的代数基础之一.

3.1.1　准素理想

环 R 的理想 $\mathfrak{q}$ 称为是**准素**的，如果 $\mathfrak{q}\neq R$，并且，若 $x,y\in R$，$xy\in\mathfrak{q}$，$x\notin\mathfrak{q}$，则存在 $n\geqslant 1$ 使得 $y^n\in\mathfrak{q}$. 由定义可知，R 的素理想均是准素的. 若 R 的理想 $\mathfrak{q}\neq R$，则

$\mathfrak{q}$ 是准素的 $\Leftrightarrow$ 若 $x,y\in R$，$xy\in\mathfrak{q}$，$x\notin\mathfrak{q}$，则 $y\in\sqrt{\mathfrak{q}}$

$\Leftrightarrow$ 若 $x,y\in R$，$xy\in\mathfrak{q}$，$y\notin\sqrt{\mathfrak{q}}$，则 $x\in\mathfrak{q}$

$\Leftrightarrow R/\mathfrak{q}$ 的零因子均是幂零元.

在整数环 $\mathbb{Z}$ 中，理想 (n) 是准素的当且仅当 $(n)=0$，或 (n) 是素理想 (p) 的幂.

命题 3.1.1　*设 $\mathfrak{q}$ 是环 R 的准素理想，则 $\sqrt{\mathfrak{q}}$ 是 R 的包含 $\mathfrak{q}$ 的最小素理想.*

证明　由命题 1.1.5 的(2)，$\sqrt{\mathfrak{q}}$ 是 R 的所有包含 $\mathfrak{q}$ 的素理想之交，故只需证 $\sqrt{\mathfrak{q}}$ 是素理想. 设 $x,y\in R$，$xy\in\sqrt{\mathfrak{q}}$，则存在 $m\geqslant 1$ 使 $(xy)^m=x^my^m\in\mathfrak{q}$. 若 $x^m\in\mathfrak{q}$，则 $x\in\sqrt{\mathfrak{q}}$. 若 $x^m\notin\mathfrak{q}$，则存在 $n\geqslant 1$ 使得 $(y^m)^n\in\mathfrak{q}$，从而 $y\in\sqrt{\mathfrak{q}}$. 所以 $\sqrt{\mathfrak{q}}$ 是素理想. □

设 $\mathfrak{p}$ 是环 R 的素理想，$\mathfrak{q}$ 是 R 的准素理想. 若 $\sqrt{\mathfrak{q}}=\mathfrak{p}$，则称 $\mathfrak{p}$ 是**属于 $\mathfrak{q}$ 的素理想**，而称 $\mathfrak{q}$ 是 $\mathfrak{p}$-**准素理想**.

命题3.1.2 设 $\mathfrak{p}$ 是环 R 的素理想，$\mathfrak{q}_1,\cdots,\mathfrak{q}_n$ 是 R 的 $\mathfrak{p}$-准素理想，则 $\mathfrak{q}=\bigcap_{i=1}^{n}\mathfrak{q}_i$ 也是 $\mathfrak{p}$-准素理想.

证明 显然 $\mathfrak{q}\neq R$. 由命题 1.1.5 的(5)可知，$\sqrt{\mathfrak{q}}=\bigcap_{i=1}^{n}\sqrt{\mathfrak{q}_i}=\bigcap_{i=1}^{n}\mathfrak{p}=\mathfrak{p}$. 又若 $x,y\in R$，$xy\in\mathfrak{q}$，$x\notin\mathfrak{q}$，则存在 i 使得 $xy\in\mathfrak{q}_i$ 且 $x\notin\mathfrak{q}_i$，$1\leqslant i\leqslant n$，从而 $y\in\sqrt{\mathfrak{q}_i}=\mathfrak{p}=\sqrt{\mathfrak{q}}$. 所以 $\mathfrak{q}$ 是 $\mathfrak{p}$-准素理想. □

一般地，准素理想未必是素理想的幂.

例 1 设 R 是域 F 上的多项式环 $F[x,y]$，$\mathfrak{q}=(x,y^2)$是由 x 和 y^2 生成的 R 的理想. 由于 $R/\mathfrak{q}\simeq F[y]/(y^2)\neq 0$，且 $F[y]/(y^2)$中的零因子必是幂零元，所以 $\mathfrak{q}$ 是 R 的准素理想. 并且 $\mathfrak{p}=\sqrt{\mathfrak{q}}=(x,y)$，$\mathfrak{p}^2\subset\mathfrak{q}\subset\mathfrak{p}$. 假定 $\mathfrak{q}=\mathfrak{p}_1^n$，$\mathfrak{p}_1\in\operatorname{Spec}R$，则 $\mathfrak{p}^2\subset\mathfrak{p}_1^n\subset\mathfrak{p}$，分别取根后，由命题 1.1.5 的(6)得 $\mathfrak{p}_1=\mathfrak{p}$. 于是 $\mathfrak{p}^2\subset\mathfrak{p}^n\subset\mathfrak{p}$，这矛盾. 所以 $\mathfrak{q}$ 不是素理想的幂.

另一方面，一般地，素理想的幂也未必是准素的.

例 2 设 F 是域，$R=F[x,y,z]/(xy-z^2)$，$\mathfrak{p}$ 是由 $\bar{x}$ 和 $\bar{z}\in R$ 生成的 R 的理想. 则 $R/\mathfrak{p}\simeq F[y]$是整环，从而 $\mathfrak{p}$ 是 R 的素理想. 但 $\mathfrak{p}^2$ 不是准素的，这是因为，$\bar{x}\,\bar{y}=\bar{z}^2\in\mathfrak{p}^2$，$\bar{x}\notin\mathfrak{p}^2$，且 $\bar{y}\notin\mathfrak{p}=\sqrt{\mathfrak{p}^2}$.

命题 3.1.3 设 I 是环 R 的理想. 若 $\sqrt{I}$ 是 R 的极大理想，则 I 是准素的. 特别地，R 的极大理想 $\mathfrak{m}$ 的幂是 $\mathfrak{m}$-准素的.

证明 设 $\mathfrak{q}=\sqrt{I}$ 是极大理想. 由命题 1.1.5 的(1)可知 $\mathfrak{q}/I=\operatorname{Nil}(R/I)$，且 $\mathfrak{q}/I\in\operatorname{Max}(R/I)$. 又由于 R 的包含 I 的极大理想必包含 $\mathfrak{q}$，所以 $\mathfrak{q}/I$ 是 R/I 的唯一极大理想，故 R/I 是局部环. 于是 R/I 的零因子均属于 $\mathfrak{q}/I$，从而均是幂零元，所以 I 是准素的. 再由命题 1.1.5 的(6)得后一论断. □

命题 3.1.4 设 $\mathfrak{q}$ 是环 R 的 $\mathfrak{p}$-准素理想，$x\in R$.

(1) 若 $x\in\mathfrak{q}$，则$(\mathfrak{q}:x)=R$.

(2) 若 $x\notin\mathfrak{p}$，则 $(\mathfrak{q}:x)=\mathfrak{q}$.

(3) 若 $x\notin\mathfrak{q}$，则 $(\mathfrak{q}:x)$ 是 $\mathfrak{p}$-准素理想.

证明 (1)和(2)由定义直接验证.

(3) 先证 $\sqrt{(\mathfrak{q}:x)}=\mathfrak{p}$. 若 $y\in(\mathfrak{q}:x)$，则 $xy\in\mathfrak{q}$. 由于 $x\notin\mathfrak{q}$，于是 $y\in\mathfrak{p}=\sqrt{\mathfrak{q}}$，从而 $\mathfrak{q}\subseteq(\mathfrak{q}:x)\subseteq\mathfrak{p}$. 取根，得 $\mathfrak{p}\subseteq\sqrt{(\mathfrak{q}:x)}\subseteq\mathfrak{p}$. 所以 $\sqrt{(\mathfrak{q}:x)}=\mathfrak{p}$. 再证 $(\mathfrak{q}:x)$ 是准素的. 若 $y,z\in R$，$yz\in(\mathfrak{q}:x)$，$y\notin\sqrt{(\mathfrak{q}:x)}=\mathfrak{p}$，则 $xyz\in\mathfrak{q}$ 且 $y\notin\mathfrak{p}$，于是 $xz\in\mathfrak{q}$，从而 $z\in(\mathfrak{q}:x)$. 所以 $(\mathfrak{q}:x)$ 是 $\mathfrak{p}$-准素的. □

3.1.2 准素分解

环 R 的理想 I 称为是**可分解**的，如果 I 可表示成有限个准素理想 $\mathfrak{q}_i$ 之交：

$$I=\bigcap_{i=1}^{n}\mathfrak{q}_i.$$

也称上式为 I 的**准素分解**，且称每个 $\mathfrak{q}_i$ 是 I 的**准素分支**. 若上式中某个 $\mathfrak{q}_i$ 包含其余 $n-1$ 个准素分支的交，则在上式中去掉这个 $\mathfrak{q}_i$ 后可得到 I 的一个较简单的准素分解. 又若 I 的一些准素分支有相同的根，例如 $\sqrt{\mathfrak{q}_1}=\cdots=\sqrt{\mathfrak{q}_r}=\mathfrak{p}$，$1<r\leqslant n$，由命题 3.1.2，$\mathfrak{q}=\bigcap\limits_{i=1}^{r}\mathfrak{q}_i$ 仍是 $\mathfrak{p}$-准素的，将 $\bigcap\limits_{i=1}^{r}\mathfrak{q}_i$ 换成 $\mathfrak{q}$，可得到一个更简单的准素分解. 所以，若环 R 的理想 I 是可分解的，则经上述两种“简化”可以得到 I 的准素分解 $I=\bigcap\limits_{i=1}^{k}\mathfrak{q}_i$，使得

(1) $\sqrt{\mathfrak{q}_i}$，$1\leqslant i\leqslant k$，是互不相同的素理想；

(2) $\mathfrak{q}_j\not\supseteq\bigcap\limits_{\substack{i=1\\ i\neq j}}^{k}\mathfrak{q}_i$.

理想 I 的满足上述两个条件的准素分解叫做 I 的**极小准素分解**.

定理 3.1.5（第一唯一性定理） 设 I 是环 R 的理想，$I=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$ 是极小准素分解，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$，$i=1,\cdots,n$. 则 $\{\mathfrak{p}_1,\mathfrak{p}_2,\cdots,\mathfrak{p}_n\}$ 由

I 唯一确定，与极小准素分解的选择无关，均称为**属于 I 的素理想**.

证明 令 $S=\{\mathfrak{p}\in \operatorname{Spec} R \mid$ 存在 $x\in R$ 使得 $\sqrt{(I:x)}=\mathfrak{p}\}$，它由 I 唯一确定. 下证 $S=\{\mathfrak{p}_1,\mathfrak{p}_2,\cdots,\mathfrak{p}_n\}$，从而定理得证.

设 $x\in R$，则 $(I:x)=(\bigcap\limits_{i=1}^{n}\mathfrak{q}_i:x)=\bigcap\limits_{i=1}^{n}(\mathfrak{q}_i:x)$. 由命题 3.1.4 的(1)和(3)得 $\sqrt{(I:x)}=\bigcap\limits_{\substack{j=1\\ x\notin\mathfrak{q}_j}}^{n}\sqrt{(\mathfrak{q}_j:x)}=\bigcap\limits_{\substack{j=1\\ x\notin\mathfrak{q}_j}}^{n}\mathfrak{p}_j$.

若 $\mathfrak{p}\in S$，则 $\mathfrak{p}=\sqrt{(I:x)}=\bigcap\limits_{\substack{j=1\\ x\notin\mathfrak{q}_j}}^{n}\mathfrak{p}_j$，$x\in R$，从而 $\mathfrak{p}$ 等于某个 $\mathfrak{p}_j$(习题 1.1.4). 反之，由准素分解式的极小性可知，对于每个 j 均存在 $x_j\in(\bigcap\limits_{\substack{i=1\\ i\neq j}}^{n}\mathfrak{q}_i)\setminus\mathfrak{q}_j$，进而 $\sqrt{(I:x_j)}=\mathfrak{p}_j\in S$，$1\leqslant j\leqslant n$. 所以 $S=\{\mathfrak{p}_1,\mathfrak{p}_2,\cdots,\mathfrak{p}_n\}$. □

设环 R 的理想 I 有极小准素分解 $I=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$. 在 $\{\mathfrak{p}_1,\mathfrak{p}_2,\cdots,\mathfrak{p}_n\}$ 中关于包含关系的极小元 $\mathfrak{p}_i$ 叫做**属于 I 的极小素理想**或**孤立素理想**，对应的 $\mathfrak{q}_i$ 叫做 I 的**孤立准素分支**；不是孤立素理想的 $\mathfrak{p}_i$ 叫做**属于 I 的嵌入素理想**，对应的 $\mathfrak{q}_i$ 叫做 I 的**嵌入准素分支**.

例 3 设 F 是域，$R=F[x,y]$，理想 $I=(x^2,xy)$ 有两个不同的极小准素分解：

$$I=(x)\cap(x,y)^2=(x)\cap(x^2,y),$$

其中 $(x,y)^2$ 是极大理想 (x,y) 的幂，从而是准素的；而由例 1 可知 (x^2,y) 是准素的；并且，$\sqrt{(x)}=(x)$，$\sqrt{(x,y)^2}=(x,y)=\sqrt{(x^2,y)}$. 所以，这两个准素分解都是极小的，且属于 I 的素理想是 (x) 和 (x,y). 由于 $(x)\subset(x,y)$，所以 (x) 是属于 I 的极小素理想，而 (x,y) 是属于 I 的嵌入素理想.

命题 3.1.6 设 I 是环 R 的可分解理想，则 R 的每个包含 I

的素理想必包含某个属于I的极小素理想. 于是, 属于I的全部极小素理想恰好是集合$\{\mathfrak{p}\in \mathrm{Spec}\ R \mid \mathfrak{p}\supseteq I\}$中关于包含关系的全部极小元.

证明 设$I=\bigcap_{i=1}^{n}\mathfrak{q}_i$是极小准素分解, $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$. 若$R$的素理想$\mathfrak{p}\supseteq I=\bigcap_{i=1}^{n}\mathfrak{q}_i$, 取根后可得$\mathfrak{p}=\bigcap_{i=1}^{n}\mathfrak{p}_i$, 所以$\mathfrak{p}$等于某个$\mathfrak{p}_j$是属于$I$的素理想, 从而包含某个属于$I$的极小素理想, 进而可得后一论断. □

下面讨论准素理想分式化后的性质.

命题3.1.7 设S是环R的乘法集, $\mathfrak{q}$是R的$\mathfrak{p}$-准素理想.

(1) 若$S\cap\mathfrak{p}\neq\varnothing$, 则$S^{-1}\mathfrak{q}=S^{-1}R$.

(2) 若$S\cap\mathfrak{p}=\varnothing$, 则$S^{-1}\mathfrak{q}$是$S^{-1}R$的$S^{-1}\mathfrak{p}$-准素理想.

(3) $S^{-1}R$的准素理想一一保序对应于R的使得$S\cap\sqrt{\mathfrak{q}}=\varnothing$的准素理想$\mathfrak{q}$.

证明 (1) 若$u\in S\cap\mathfrak{p}$, 则存在$n\geqslant 1$使得$u^n\in S\cap\mathfrak{q}$, 由命题2.5.3可知$S^{-1}\mathfrak{q}=S^{-1}R$.

(2) 设$S\cap\mathfrak{p}=\varnothing$, 则$\sqrt{S^{-1}\mathfrak{q}}=S^{-1}\sqrt{\mathfrak{q}}=S^{-1}\mathfrak{p}$(习题2.5.1)是$S^{-1}R$的素理想. 进而容易验证$S^{-1}\mathfrak{q}$是准素的.

(3) 设$\varphi: R\to S^{-1}R$; $a\mapsto a/1$是正则环同态. 若Q是$S^{-1}R$的准素理想, 则$\varphi^{-1}(\sqrt{Q})=\sqrt{\varphi^{-1}(Q)}$是$R$的素理想, 且$S\cap\varphi^{-1}(\sqrt{Q})=\varnothing$. 进而不难验证$\varphi^{-1}(Q)$是$R$的准素理想且$S^{-1}(\varphi^{-1}(Q))=Q$. 再设$\mathfrak{q}$是$R$的$\mathfrak{p}$-准素理想, 且$S\cap\mathfrak{p}=\varnothing$. 由(2), $S^{-1}\mathfrak{q}$是$S^{-1}R$的$S^{-1}\mathfrak{p}$-准素理想. 由命题2.5.3的(3), $\varphi^{-1}(S^{-1}\mathfrak{p})=\mathfrak{p}$. 下证$\varphi^{-1}(S^{-1}\mathfrak{q})=\mathfrak{q}$. 若$a\in\varphi^{-1}(S^{-1}\mathfrak{q})$, 则$a/1\in S^{-1}\mathfrak{q}$, 于是存在$u\in S$使得$ua\in\mathfrak{q}$. 因$S\cap\mathfrak{p}=\varnothing$, 故$u\notin\mathfrak{p}$, 从而$a\in\mathfrak{q}$, 所以$\varphi^{-1}(S^{-1}\mathfrak{q})\subseteq\mathfrak{q}$. 而反包含显然成立. 这样, φ^{-1}和S^{-1}就是所需的保序互逆映射. □

命题3.1.8 设S是环R的乘法集, $I=\bigcap_{i=1}^{n}\mathfrak{q}_i$是$R$的理想$I$

的极小准素分解，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$，且设 $S\cap\mathfrak{p}_i=\varnothing$，$i=1,2,\cdots,m$；$S\cap\mathfrak{p}_j\neq\varnothing$，$j=m+1,\cdots,n$. 则

(1) $S^{-1}I=\bigcap\limits_{i=1}^{m}S^{-1}\mathfrak{q}_i$ 是 $S^{-1}I$ 的极小准素分解.

(2) $\varphi^{-1}(S^{-1}I)=\bigcap\limits_{i=1}^{m}\mathfrak{q}_i$ 是 $\varphi^{-1}(S^{-1}I)$ 的极小准素分解，其中 $\varphi:R\to S^{-1}R$ 是正则环同态.

证明 (1) 由命题 3.1.7 和 2.5.8，$S^{-1}I=\bigcap\limits_{i=1}^{n}S^{-1}\mathfrak{q}_i=\bigcap\limits_{i=1}^{m}S^{-1}\mathfrak{q}_i$，且 $S^{-1}\mathfrak{q}_i$ 是 $S^{-1}\mathfrak{p}_i$-准素的，$i=1,\cdots,m$. 由于 $\mathfrak{p}_1,\cdots,\mathfrak{p}_m$ 两两不同且与 S 不交，由命题 2.5.3 的(3)可知 $S^{-1}\mathfrak{p}_1,\cdots,S^{-1}\mathfrak{p}_m$ 两两不同，所以 $S^{-1}I=\bigcap\limits_{i=1}^{m}S^{-1}\mathfrak{q}_i$ 是极小准素分解.

(2) 由(1)及命题 3.1.7 的(3)立得. □

由上述命题可知，选择适当的乘法集 S，从理想 I 到 $\varphi^{-1}(S^{-1}I)$，可以“杀掉”I 的一部分准素分支. 下面是这一方法的应用.

设环 R 的理想 I 是可分解的，Σ 是属于 I 的所有素理想构成的集合. Σ 的子集 Σ' 称为是一个**孤立集**，如果 $\mathfrak{p}\in\Sigma$，且 $\mathfrak{p}\subseteq\mathfrak{p}'\in\Sigma'$ 蕴含 $\mathfrak{p}\in\Sigma'$. 对于孤立集 Σ'，令 $S=R\setminus(\bigcup\limits_{\mathfrak{p}'\in\Sigma'}\mathfrak{p}')$，则 S 是 R 的乘法集(习题 2.5.6)，且对于每个 $\mathfrak{p}'\in\Sigma'$ 均有 $\mathfrak{p}'\cap S=\varnothing$. 反之，若 $\mathfrak{p}\in\Sigma$ 且 $\mathfrak{p}\cap S=\varnothing$，则 $\mathfrak{p}\subseteq\bigcup\limits_{\mathfrak{p}'\in\Sigma'}\mathfrak{p}'$. 由命题 1.1.2，存在某个 $\mathfrak{p}'\in\Sigma'$ 使得 $\mathfrak{p}\subseteq\mathfrak{p}'$，从而 $\mathfrak{p}\in\Sigma'$. 用这些事实可以证明：

定理 3.1.9(第二唯一性定理) 设 I 是环 R 的理想，$I=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$ 是极小准素分解，$\Sigma=\{\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}\mid i=1,\cdots,n\}$，且设 $\Sigma'=\{\mathfrak{p}_1,\cdots,\mathfrak{p}_m\}$ 是 Σ 的一个孤立集. 则 $\bigcap\limits_{i=1}^{m}\mathfrak{q}_i$ 由 I 和 Σ' 唯一确定，与极小准素分解的选择无关. 特别地，I 的孤立准素分支由 I 唯一确定.

证明 取 R 的乘法集 $S=R\setminus(\bigcup\limits_{i=1}^{m}\mathfrak{p}_i)$，由命题 3.1.8，

$\varphi^{-1}(S^{-1}I)=\bigcap_{i=1}^{m}\mathfrak{q}_i$，而 $\varphi^{-1}(S^{-1}I)$由 I 和Σ'唯一确定. □

一般来说，并不是每个理想都是可分解的. 在 3.3 节中将要证明，在代数几何中特别重要的 Noether 环，它的每个真理想均是可分解的.

习　题　3.1

1. 在 $\mathbb{Z}[x]$中，$\mathfrak{m}=(2,x)$是极大理想. 证明：$\mathfrak{q}=(4,x)$是$\mathfrak{m}$-准素的，但不是素理想的幂.

2. 设 k 是域，$R=k[x,y,z]$. 证明：

(1) $\mathfrak{p}_1=(x,y)$和 $\mathfrak{p}_2=(x,z)$是 R 的素理想，$\mathfrak{m}=(x,y,z)$是 R 的极大理想.

(2) 令 $I=\mathfrak{p}_1\mathfrak{p}_2$，则 $I=\mathfrak{p}_1\cap\mathfrak{p}_2\cap\mathfrak{m}^2$ 是 I 的极小准素分解. 试求属于 I 的极小素理想和嵌入素理想.

3. 证明：对于任意 $i,j\geqslant 1$，(x^i,y^j)均是 $\mathbb{Z}[x,y]$中的(x,y)-准素理想.

4. 试求 $\mathbb{Z}[x,y]$中的理想 $I=(x^2,xy,2)$的一个极小准素分解式，并给出属于 I 的全部素理想. 由此确定$\sqrt{I}$.

5. 设 k 是域，试给出环 $k[x,y]$中的理想(x^2,xy)的三个不同的极小准素分解.

6. 设 $f:R\to S$ 是环的满同态，J 是S 的理想，$I=f^{-1}(J)$. 证明：

(1) I 在R 中是准素的$\Leftrightarrow J$ 在S 中是准素的.

(2) 若 J 在S 中是 $\mathfrak{p}$-准素的，则 I 是$f^{-1}(\mathfrak{p})$-准素的.

7. 设 R 是环，$\{\mathfrak{p}_i \mid i\in I\}$是 Spec R 中的非空链. 证明：$\bigcup_{i\in I}\mathfrak{p}_i$和$\bigcap_{i\in I}\mathfrak{p}_i$ 均是R 的素理想.

8. 设 R 是环，D 是R 中所有零因子构成的集合. 证明：

(1) D 是R 的一些素理想之并.

(2) 若 R 的零理想 0 是可分解的，则 D 是属于 0 的所有素

理想之并.

9. 设 I 是环 R 的理想. 证明:

(1) $I[x]$ 是 $R[x]$ 的理想.

(2) 若 $\mathfrak{p}\in \operatorname{Spec} R$, 则 $\mathfrak{p}[x]\in \operatorname{Spec} R[x]$.

(3) 若 $\mathfrak{q}$ 是 R 中的 $\mathfrak{p}$-准素理想, 则 $\mathfrak{q}[x]$ 是 $R[x]$ 中的 $\mathfrak{p}[x]$-准素理想(提示:利用习题 1.1.10).

(4) 若 $I=\bigcap_{i=1}^{n}\mathfrak{q}_i$ 是 I 在 R 中的极小准素分解, 则 $I[x]=\bigcap_{i=1}^{n}\mathfrak{q}_i[x]$ 是 $I[x]$ 在 $R[x]$ 中的极小准素分解.

(5) 若 $\mathfrak{p}$ 是属于 I 的极小素理想, 则 $\mathfrak{p}[x]$ 是属于 $I[x]$ 的极小素理想.

10. 设 k 是域, $R=k[x_1,\cdots,x_n]$. 证明: 对于每个 $i\in\{1,\cdots,n\}$, $\mathfrak{p}_i=(x_1,\cdots,x_i)$ 均是 R 的素理想, 且 $\mathfrak{p}_i$ 的幂均是 R 的准素理想.

11. 设 I 是环 R 的可分解理想, $\mathfrak{p}$ 是理想的集合 $\{(I:x)\mid x\in R\setminus I\}$ 中的极大元. 证明: $\mathfrak{p}$ 是属于 I 的素理想.

12. 设 S 是环 R 的乘法集. 证明: 若 R 中的每个真理想均可分解, 则 $S^{-1}R$ 中的每个真理想均可分解.

3.2 Noether 模和 Artin 模

3.2.1 链条件

设 M 是一个 R-模, Σ 是 M 的所有 R-子模作成的集合. 称 M 是 **Noether R-模**, 如果 M 满足**升链条件**(ACC): Σ 中的升链都是**稳定**的, 也就是说, 若 $M_1\subseteq M_2\subseteq\cdots\subseteq M_n\subseteq\cdots$ 是 M 的子模的升链, 则存在 $n_0\geqslant 1$, 使得 $M_{n_0}=M_{n_0+1}=\cdots$. 称 R-模 M 满足**极大条件**, 如果 Σ 中的每个非空子集(关于包含关系)均有极大元.

命题 3.2.1　对于 R-模 M，下列条件等价：

(1) M 是 Noether R-模；

(2) M 满足极大条件；

(3) M 的每个子模都是有限生成 R-模.

证明　(1)⇒(2)：设 Σ 是 M 的所有子模作成的集合. 假定 Σ 的非空子集 Σ' 无极大元. 对于 $M_1\in\Sigma'$，存在 $M_2\in\Sigma'$，使得 $M_1\subset M_2$，进而存在 $M_3\in\Sigma'$，使得 $M_2\subset M_3$，如此继续下去，可得 Σ 中的严格升链 $M_1\subset M_2\subset M_3\subset\cdots$，这与 M 满足升链条件矛盾.

(2)⇒(3)：设 N 是 M 的子模. 令 Σ' 是 N 的所有有限生成子模构成的集合，则 $\Sigma'\neq\varnothing$(因 $0\in\Sigma'$). 由(2)，Σ' 中有极大元 P. 假定 $P\neq N$，则存在 $x\in N\backslash P$，令 $P'=P+Rx$，则 P' 也是 N 的有限生成子模，且 $P\subset P'$. 这与 P 的极大性矛盾. 所以 $N=P$ 是有限生成 R-模.

(3)⇒(1)：设 $M_1\subseteq M_2\subseteq\cdots\subseteq M_i\subseteq\cdots$ 是 Σ 中的升链，则 $N=\bigcup\limits_{i=1}^{\infty}M_i$ 是 M 的有限生成子模. 设 $N=Rx_1+\cdots+Rx_n$，$x_i\in N$，则存在 $k_i\geqslant 1$ 使得 $x_i\in M_{k_i}$，$i=1,\cdots,n$. 令 $n_0=\mathrm{Max}\{k_1,\cdots,k_n\}$，则 $N\subseteq M_{n_0}\subseteq M_{n_0+1}\subseteq\cdots\subseteq N$，从而 $M_{n_0}=M_{n_0+1}=\cdots$. □

对偶地，一个 R-模 M 称为 **Artin R-模**，如果 M 满足**降链条件**(DCC)：Σ 中的降链都是**稳定**的，也就是说，若 $M_1\supseteq M_2\supseteq\cdots\supseteq M_n\supseteq\cdots$ 是 M 的子模的降链，则存在 $n_0\geqslant 1$，使得 $M_{n_0}=M_{n_0+1}=\cdots$. 称 R-模 M 满足**极小条件**，如果 Σ 中的每个非空子集(关于包含关系)均有极小元.

命题 3.2.2　对于 R-模 M，下列条件等价：

(1) M 是 Artin R-模；

(2) M 满足极小条件.

证明　(1)⇒(2)：仿命题 3.2.1 中那样反证.

(2)$\Rightarrow$(1)：若 $M_1\supseteq\cdots\supseteq M_n\supseteq\cdots$是 M 的子模的降链，令 $\Sigma'=\{M_n\mid n=1,2,\cdots\}$，则 Σ'中有极小元 M_{n_0}，从而 $M_{n_0}=M_{n_0+1}=\cdots$. □

例 (1) 有限 Abel 群作为 $\mathbb{Z}$-模是 Noether $\mathbb{Z}$-模，也是 Artin $\mathbb{Z}$-模.

(2) 整数环 $\mathbb{Z}$ 作为 $\mathbb{Z}$-模是 Noether $\mathbb{Z}$-模，但不是 Artin$\mathbb{Z}$-模.

(3) 设 p 是一个固定的素数，则 $A=\{\bar{x}\in\mathbb{Q}/\mathbb{Z}\mid x\in\mathbb{Q}$，存在 $n\geqslant1$使得 $p^nx\in\mathbb{Z}\}$是一个加群. 对于每个 $n\geqslant0$，$A_n=(p^{-n}\mathbb{Z})/\mathbb{Z}$是 A 的p^n 阶子群. 且 $A=\bigcup\limits_{i=0}^{\infty}A_n$ 不是有限生成的，从而不是 Noether $\mathbb{Z}$-模. 但 A 的真子群必是有限群，从而 A 是 Artin $\mathbb{Z}$-模.

(4) 设 $R=F[x_1,x_2,\cdots,x_n,\cdots]$是域 F 上的无限多个未定元x_i 的多项式环. 则 R 作为R-模是有限生成的，但 R 既不是 Noether R-模，也不是 Artin R-模.

命题 3.2.3 设 $0\to M'\xrightarrow{f}M\xrightarrow{g}M''\to0$ 是 R-模短正合列，则 M 是 Noether(Artin) R-模当且仅当 M'和 M''是 Noether(Artin) R-模.

证明 设 M 是 Noether R-模. 若 $M_1'\subseteq M_2'\subseteq\cdots\subseteq M_n'\subseteq\cdots$是 M'的子模升链，则 $f(M_1')\subseteq f(M_2')\subseteq\cdots\subseteq f(M_n')\subseteq\cdots$是 M 的子模升链，从而是稳定的. 再由 f 是R-单同态可知前一升链也是稳定的. 所以 M'是 Noether R-模. 又设 $M_1''\subseteq M_2''\subseteq\cdots\subseteq M_n''\subseteq\cdots$ 是 M''的子模升链，则 $g^{-1}(M_1'')\subseteq g^{-1}(M_2'')\subseteq\cdots\subseteq g^{-1}(M_n'')\subseteq\cdots$是 M 的子模升链，从而是稳定的，由此可知前一升链也是稳定的，所以 M''也是 Noether R-模.

设 M'和 M''是 Noether R-模. 为简明起见，不妨设 M'是 M 的子模，f 为包含映射. 且设 $M''=M/M'$，g 为自然满同态. 若 $M_1\subseteq M_2\subseteq\cdots\subseteq M_n\subseteq\cdots$是 M 的子模升链，则 $f^{-1}(M_1)\subseteq$

$f^{-1}(M_2)\subseteq\cdots\subseteq f^{-1}(M_n)\subseteq\cdots$ 和 $g(M_1)\subseteq g(M_2)\subseteq\cdots\subseteq g(M_n)\subseteq\cdots$ 分别是 M' 和 M'' 的子模升链，且 $f^{-1}(M_i)=M'\cap M_i$，$g(M_i)=\overline{M_i}=(M_i+M')/M'$．由于后两个升链是稳定的，存在 $n_0\geqslant 1$ 使得 $M_{n_0}\cap M'=M_{n_0+1}\cap M'=\cdots$，且 $\overline{M}_{n_0}=\overline{M}_{n_0+1}=\cdots$．由定理 1.2.7，$\overline{M}_i=(M_i+M')/M'\simeq M_i/(M_i\cap M')$．于是 $M_{n_0}=M_{n_0+1}=\cdots$．所以 M 是 Noether R-模．

仿上，将升链改为降链，可证另一半．　□

推论 3.2.4　(1) Noether(Artin) R-模的子模和 R-商模仍是 Noether(Artin) R-模．

(2) 若 R-模 M 的子模 N 和商模 M/N 是 Noether(Artin) R-模，则 M 也是 Noether(Artin) R-模．

(3) 设 $M=\bigoplus\limits_{i=1}^{n}M_i$ 是有限个 R-模 M_i 的直和，则 M 是 Noether(Artin) R-模当且仅当每个 M_i 是 Noether(Artin) R-模．

证明　用命题 3.2.3 于正合列 $0\to N\to M\to M/N\to 0$ 和 $0\to M_n\to M\to\bigoplus\limits_{i=1}^{n-1}M_i\to 0$，并对 n 归纳．　□

3.2.2　合成列

设 R-模 $M\neq 0$．若 M 除了 0 和 M 外没有别的子模，则称 M 为**单 R-模**．易证，非零 R-模 M 是单 R-模 $\Leftrightarrow$ 对于每个 $x\in M\setminus\{0\}$，$M=Rx\Leftrightarrow M\simeq R/\mathfrak{q}$，$\mathfrak{q}$ 是 R 的极大理想．例如，素数阶循环群均是单 $\mathbb{Z}$-模，域 F 上的单模就是 F 上的一维线性空间；主理想整环 R 上的单模均同构于 $R/(p)$，p 是 R 的素元．

设 M 是 R-模．M 的子模的有限严格降链 $M=M_0\supset M_1\supset\cdots\supset M_n=0$ 称为 M 的**合成列**，如果 M_i/M_{i+1}，$i=0,\cdots,n-1$，均是单 R-模；而 n 称为该合成列的**长度**．

命题 3.2.5　设 R-模 M 有合成列，则 M 的所有合成列均有相同的长度，且 M 的任意子模的严格降链均可插入一些子模，

使之成为一个合成列.

证明 以 $l(M)$表示模 M 的合成列的长度中的最小者.

(1) 若 N 是M 的子模，且 $N\neq M$，则 N 也有合成列，且 $l(N)<l(M)$. 这是因为：设 $M=M_0\supset M_1\supset\cdots\supset M_{l(M)}=0$ 是 M 的合成列. 令 $N_i=N\cap M_i$，$i=0,1,\cdots,l(M)$. 由于自然 R-同态$N_i\to M_i/M_{i+1}$的核为 $N_i\cap M_{i+1}=N_{i+1}$，所以有 R-单同态 $N_i/N_{i+1}\to M_i/M_{i+1}$. 于是 $N_i/N_{i+1}\simeq M_i/M_{i+1}$是单 R-模，或者 $N_i/N_{i+1}=0$. 于是在子模降链 $N=N_0\supseteq N_1\supseteq\cdots\supseteq 0$ 中去掉重复项即得 N 的一个合成列，且 $l(N)\leqslant l(M)$. 假定 $l(N)=l(M)$. 则 $N_i/N_{i+1}\simeq M_i/M_{i+1}$，$i=0,1,\cdots,l(M)-1$. 由初始条件 $M_{l(M)}=N_{l(M)}=0$ 以及 $N_i\subseteq M_i$，可递归地得到 $M_i=N_i$. 特别地，$M=M_0=N_0=N$，这与所设矛盾. 所以 $l(N)<l(M)$.

(2) M 的子模的严格降链$M=M_0\supset M_1\supset\cdots\supset M_k=0$ 的长度 $k\leqslant l(M)$. 这是因为：由(1)，$l(M)>l(M_1)>\cdots>l(M_k)=0$，所以 $k\leqslant l(M)$.

由(2)可知，M 的任意合成列的长度$k\leqslant l(M)$，再由 $l(M)$ 的最小性可知 $k=l(M)$，所以 M 的所有合成列均有相同的长度. 又若 $M=M_0\supset M_1\supset\cdots\supset M_k=0$ 是 M 的子模的严格降链，而 $k<l(M)$，则有某个 M_i/M_{i+1} 不是单 R-模，从而有子模 M'/M_{i+1}使得 $M_i\supset M'\supset M_{i+1}$. 将 M'插入后其长度增加 1，如此继续下去，直到长度为 $l(M)$. 由(2)可知，这样得到的降链就是 M 的合成列. □

命题 3.2.6 *R-模 M 有合成列当且仅当 M 既是 Noether R-模也是 Artin R-模.*

证明 由命题 3.2.5 可知，若 M 有合成列，则 M 不能有子模的无限严格降链和升链，所以 M 是 Noether R-模，也是 Artin R-模. 反之，若 M 既是 Noether R-模，也是 Artin R-模，不妨设 $M\neq 0$，则 M 的真包含于M 的子模中必有极大元$M_1\subset M$，从而

M/M_1 是单 R-模. 同理, M_1 含有极大子模 M_2 使得 M_1/M_2 是单 R-模. 如此继续下去, 可得严格降链 $M=M_0\supset M_1\supset\cdots\supset M_i\supset M_{i+1}\supset\cdots$, 使得 M_i/M_{i+1} 是单 R-模. 由于 M 是 Artin R-模, 存在 k 使得 $M_k=0$, 从而得到 M 的一个合成列. □

习　题　3.2

1. 设 N_1 和 N_2 是 R-模 M 的子模. 证明: 若 M/N_1 和 M/N_2 均是 Noether(Artin) R-模, 则 $M/(N_1\cap N_2)$ 也是 Noether(Artin) R-模.

2. 设 A 是 $\mathbb{Z}$-模. 证明:

(1) A 是 Noether $\mathbb{Z}$-模 $\Leftrightarrow A$ 是有限生成 $\mathbb{Z}$-模.

(2) A 有合成列 $\Leftrightarrow A$ 是有限 $\mathbb{Z}$-模.

3. 设 S 是环 R 的乘法集, M 是 R-模. 证明: 若 M 是 Noether R-模, 则 $S^{-1}M$ 也是 Noether R-模.

4. 设 M 是有限生成 R-模. 证明:

(1) 若 I 是 R 的理想使得 $IM=M$, 则存在 $a\in I$ 使得 $(1-a)M=0$.

(2) 若 $f: M\to M$ 是 R-满同态, 则 f 是 R-同构.

5. 设 M 是 Artin R-模, $f: M\to M$ 是 R-单同态. 证明: f 是 R-同构(提示: 考虑短正合列 $0\to \mathrm{Im} f^n\to M\to M/\mathrm{Im} f^{n+1}\to 0$, $n=1,2,\cdots$).

6. 设 $M=M_0\supset M_1\supset\cdots\supset M_n=0$ 和 $M=M_0'\supset M_1'\supset\cdots\supset M_n'=0$ 是 R-模 M 的两个合成列. 证明: 存在 $\{1,\cdots,n\}$ 的置换 σ 使得 $M_{i-1}/M_i\simeq M_{\sigma(i)-1}'/M_{\sigma(i)}'$, $i=1,\cdots,n$; 称 $\{M_{i-1}/M_i \mid i=1,\cdots,n\}$ 为 M 的**合成因子**, 在同构意义下由 M 唯一确定(提示: 仿群论中相应定理的证法).

7. 称 R-模 $A(\neq 0)$ 是**不可分解**的, 如果 A 不能分解成两个真子模的直和. 证明: 若 R-模 $M(\neq 0)$ 有合成列, 则存在 M 的不

可分解子模 M_i，使得 $M=M_1\oplus\cdots\oplus M_n$；又若 $M=N_1\oplus\cdots\oplus N_m$，其中 N_i 是M 的不可分解子模，则 $m=n$，且适当交换直和项的次序后有 $N_i\simeq M_i$，$i=1,\cdots,n$.

3.3 Noether 环

环 R 称为 **Noether 环**，如果 R 作为R-模是 Noether R-模. 例如，有限环、域、主理想整环均是 Noether 环. 设 $R=F[x_1,x_2,\cdots,x_n,\cdots]$是域 F 上无限个未定元$x_1,x_2,\cdots,x_n,\cdots$的多项式环，则 R 不是 Noether 环，而 R 的分式域是 Noether 环. 这表明，一般地，Noether 环的子环未必是 Noether 环.

命题 3.3.1 *Noether 环的商环仍是 Noether 环.*

证明 设 R 是 Noether 环，I 是R 的理想. 由推论 3.2.4，R/I 作为R-模是 Noether R-模. 而 R/I 作为 R/I-模的每个子模均是R-模，从而 R/I 是 Noether R/I-模，故 R/I 是 Noether 环. □

命题 3.3.2 *环 R 是 Noether 环当且仅当每个有限生成 R-模均是 Noether R-模.*

证明 设 R 是 Noether 环，M 是有限生成R-模，则 M 是有限秩自由 R-模 R^n 的 R-同态像. 由推论 3.2.4 的(3)，R^n 是 Noether R-模，从而 M 是 Noether R-模.

反之，取 $M={}_RR$ 即得. □

命题 3.3.3 *设 R 是 Noether 环，S 是R 的乘法集，则$S^{-1}R$ 也是 Noether 环.*

证明 由命题 3.3.2 和命题 2.5.10 的(3)立得. □

下面要证 Noether 环 R 的每个真理想均是可分解的.

环 R 的理想I 称为是**可约的**，如果存在 R 的理想I_1 和 I_2 使得 $I=I_1\cap I_2$，且 $I\subset I_1$，$I\subset I_2$；否则，称 I 是**不可约的**，也就

是说，如果 $I=I_1\cap I_2$ 是理想 I_1 和 I_2 的交，则有 $I=I_1$ 或 $I=I_2$. 例如，环 R 的素理想均是不可约的. 特别地，环 R 自身是不可约的.

引理 3.3.4 Noether 环 R 的每个理想均是有限个不可约理想之交.

证明 假定 R 中存在不能表示成有限个不可约理想之交的理想，所有这样的理想构成的非空集合 Σ 中必有极大元 I. 显然 I 是可约的，从而存在理想 I_1 和 I_2 使得 $I=I_1\cap I_2$，且 $I\subset I_1$，$I\subset I_2$. 由 I 的极大性可知 $I_1, I_2\notin\Sigma$，从而 I_1 和 I_2 都可表示成有限个不可约理想之交. 再由 $I=I_1\cap I_2$ 可知 I 可表成有限个不可约理想之交，这与 $I\in\Sigma$ 矛盾. □

引理 3.3.5 Noether 环 R 的不可约真理想均是准素理想.

证明 设 I 是 R 的不可约理想，$I\neq R$. 由 R/I 的理想与 R 的包含 I 的理想一一保序对应可知，0 是 R/I 的不可约理想. 又由于 J 是 R 的包含 I 的准素理想当且仅当 J/I 是 R/I 的准素理想(习题 3.1.6)，只需对 $I=0$ 的情形来证明. 即只需证明:若 0 是 R 的不可约理想，则 0 是准素的. 设 $x,y\in R$，$xy=0$，且 $y\neq 0$. 由于 R 是 Noether 环，理想升链 $\mathrm{Ann}_R(x)\subseteq\mathrm{Ann}_R(x^2)\subseteq\cdots$是稳定的，故存在 $n\geqslant 1$，使得 $\mathrm{Ann}_R(x^n)=\mathrm{Ann}_R(x^{n+1})=\cdots$. 下证 $(x^n)\cap(y)=0$. 若 $a\in(x^n)\cap(y)$，则 $a=bx^n=cy$，$b,c\in R$. 于是 $bx^{n+1}=cxy=0$，从而 $b\in\mathrm{Ann}_R(x^{n+1})=\mathrm{Ann}_R(x^n)$. 这样，$a=bx^n=0$. 所以$(x^n)\cap(y)=0$. 因 0 是不可约理想，且$(y)\neq 0$，所以$(x^n)=0$，从而 $x^n=0$，所以 0 是准素理想. □

由上面两个引理立得

定理 3.3.6 Noether 环的每个真理想均是可分解的. □

称环 R 的理想 I 是**幂零理想**，如果存在 $n\geqslant 1$，使得 $I^n=0$. 环 R 的幂零理想均是幂零元理想，但反之未必.

命题 3.3.7 若 R 是 Noether 环，则 $\mathrm{Nil}(R)$是幂零理想.

证明 可设 $\mathrm{Nil}(R)$是由 $x_1,\cdots,x_k$ 生成的理想，且 $x_i^{n_i}=0$，$n_i\geqslant 1$，$i=1,\cdots,k$. 令 $n=n_1+n_2+\cdots+n_k$，则$(\mathrm{Nil}(R))^n$ 由 $\{x_1^{r_1}x_2^{r_2}\cdots x_k^{r_k}\in \mathrm{Nil}(R)\mid r_i\geqslant 0,\ r_1+r_2+\cdots+r_k=n\}$生成. 而当 $r_1+\cdots+r_k=n$，$r_i\geqslant 0$ 时，至少有某个 $r_i\geqslant n_i$，从而 $x_1^{r_1}\cdots x_k^{r_k}=0$，所以$(\mathrm{Nil}(R))^n=0$. □

推论 3.3.8 *若 R 是 Noether 环，I 是 R 的理想，则存在 $n\geqslant 1$，使得$(\sqrt{I})^n\subseteq I$.*

证明 由命题 3.3.7 和 $\mathrm{Nil}(R/I)=\sqrt{I}/I$（命题 1.1.5 的(1)）立得. □

环 R 的理想 I 称为**根式理想**，如果$\sqrt{I}=I$. 例如，环 R 的素理想均是根式理想.

命题 3.3.9 *Noether 环 R 的真理想 I 是根式理想当且仅当 I 可唯一地表成有限个互不包含的素理想之交.*

证明 设 I 是根式理想，$I\neq R$. 由定理 3.3.6，I 有极小准素分解 $I=\bigcap\limits_{i=1}^{n}\mathfrak{q}_i$，$\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$，取根得 $I=\sqrt{I}=\bigcap\limits_{i=1}^{n}\sqrt{\mathfrak{q}_i}=\bigcap\limits_{i=1}^{n}\mathfrak{p}_i$，去掉其中的嵌入素理想，比如 $\mathfrak{p}_{m+1},\cdots,\mathfrak{p}_n$ 之后，$I=\bigcap\limits_{i=1}^{m}\mathfrak{p}_i$，其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}_m$ 是属于 I 的两两互不包含的极小理想，由命题 3.1.6，$\{\mathfrak{p}_1,\cdots,\mathfrak{p}_m\}$由 I 唯一确定.

反之，若 $I=\bigcap\limits_{i=1}^{m}\mathfrak{p}_i$，是两两互不包含的素理想 $\mathfrak{p}_i$ 之交，取根得$\sqrt{I}=\bigcap\limits_{i=1}^{m}\sqrt{\mathfrak{p}_i}=\bigcap\limits_{i=1}^{m}\mathfrak{p}_i=I$，所以 I 是根式理想. □

推论 3.3.10 *Noether 环 R 仅有有限个极小素理想.*

证明 对 $I=\mathrm{Nil}(R)$运用命题 3.3.9 和定理 1.1.3 立得. □

下面证明的 Hilbert 基定理在代数几何中是基本的，且有许多应用，其证明方法值得重视.

定理 3.3.11（Hilbert 基定理） *若 R 是 Noether 环，则多项式环 $R[x_1,x_2,\cdots,x_n]$也是 Noether 环.*

证明　若能证 $n=1$ 时成立，再用归纳法即可得证.

设 I 是 $R[x]$ 的理想，下证 I 是有限生成理想，从而 $R[x]$ 是 Noether 环. 令

$$A=\{a\in R \mid 存在\ f(x)\in I\ 使得\ f(x)\ 的首系数是\ a\},$$

则 A 是 R 的理想，从而是有限生成的. 设 $A=Ra_1+\cdots+Ra_n$，$a_i\in A$，则对于每个 a_i，存在 $f_i(x)\in I$，使得 $f_i(x)$ 的首系数为 a_i. 令 $I'=(f_1(x),\cdots,f_n(x))$，则 $I'\subseteq I$. 又设 r 为 $f_1(x),\cdots,f_n(x)$ 的次数 $r_1,\cdots,r_n$ 中的最大者. 若 $f(x)=ax^m+\cdots+a_0\in I$，则 $a\in A$. 设 $a=\sum\limits_{i=1}^{n}u_ia_i$，$u_i\in R$. 如果 $m\geqslant r$，则 $g(x)=f(x)-\sum\limits_{i=1}^{n}u_if_i(x)x^{m-r_i}\in I$，$\sum\limits_{i=1}^{n}u_if_i(x)x^{m-r_i}\in I'$，且 $g(x)$ 的次数小于 m. 若 $g(x)$ 的次数仍大于 r，继续上述操作. 这样总可找到 $h(x)\in I'$ 和 $l(x)\in I$，使得 $f(x)=h(x)+l(x)$，且 $l(x)$ 的次数小于 r. 令 $M=R\oplus Rx\oplus\cdots\oplus Rx^{r-1}$，则 $l(x)\in I\cap M$. 所以 $I=(I\cap M)+I'$. 因 R 为 Noether 环，M 是有限生成 R-模，由命题 3.3.2，M 是 Noether R-模，再由推论 3.2.4 可知 $I\cap M$ 也是有限生成 R-模. 由于 I' 由 $f_1(x),\cdots,f_n(x)$ 生成，所以 $I=(I\cap M)+I'$ 是有限生成理想. □

习　题　3.3

1. 设 $I_1,\cdots,I_n$ 是环 R 的理想，且 $\bigcap\limits_{i=1}^{n}I_i=0$. 若 $R/I_1,\cdots,R/I_n$ 均是 Noether 环. 证明：R 也是 Noether 环.

2. 设 A 是环 B 的子环，A 是 Noether 环，且 B 是有限生成 A-模. 证明：B 也是 Noether 环.

3. 设 M 是有限生成 R-模. 证明：M 是 Noether R-模 $\Leftrightarrow$ $R/\mathrm{Ann}_R(M)$ 是 Noether 环.

4. 若 $R[x]$ 是 Noether 环，问 R 是否是 Noether 环?

5. 设 R 是 Noether 整环，$\mathfrak{p}$ 是 R 的非零素理想. 证明：$\mathfrak{p}^2 \neq \mathfrak{p}$.

6. 设 k 是域. 证明：$k[x_1, \cdots, x_n]$ 中的每个极大理想均可由 n 个元素生成.

7. 证明：若环 R 的每个素理想均是有限生成的，则 R 是 Noether 环（提示：用反证法. 设 Σ 是 R 中非有限生成的理想的集合. 先证 Σ 必有极大元，且每个极大元均是素理想）.

8. 设环 R 的每个极大理想均可表成 eR，其中 $e^2 = e \in R$. 证明：

(1) R 的准素理想必是极大理想.

(2) R 是 Noether 环（提示：利用习题 3.3.7）.

3.4 Artin 环

环 R 称为 **Artin 环**，如果 R 作为 R-模是 Artin R-模.

命题 3.4.1 设 R 是 Artin 环，则

(1) R 的商环仍是 Artin 环.

(2) 若 M 是有限生成 R-模，则 M 是 Artin R-模.

证明 仿命题 3.3.1 和 3.3.2 的证明. □

例 (1) 有限环和域既是 Noether 环，也是 Artin 环.

(2) 设 F 是域，$R = F[x_1, x_2, \cdots, x_n, \cdots]$，则 R 既不是 Noether 环，也不是 Artin 环，但 R 的分式域是 Artin 环. 这表明，一般地，Artin 环的子环未必是 Artin 环.

(3) 整数环 $\mathbb{Z}$ 是 Noether 环，但不是 Artin 环.

下面将证 Artin 环均是 Noether 环.

命题 3.4.2 Artin 环 R 的素理想均是极大理想.

证明 设 $\mathfrak{p}$ 是 R 的素理想，则 $\overline{R} = R/\mathfrak{p}$ 是 Artin 整环. 若 $x \in \overline{R} \setminus \{0\}$，由降链条件，存在 $n \geqslant 1$，使得 $(x^n) = (x^{n+1})$. 于是 $x^n = x^{n+1}y$，$y \in \overline{R}$. 因 $\overline{R}$ 是整环，故 $1 = xy$，即 x 是 $\overline{R}$ 的单位. 所以 $\overline{R}$ 是域，从而 $\mathfrak{p}$ 是极大的. □

由以上所证立得

推论 3.4.3 (1) 若 R 是 Artin 环，则 $\mathrm{Nil}(R)=\mathrm{Rad}(R)$.

(2) Artin 整环均是域. □

设 R 是非零环. R 中素理想的严格升链 $\mathfrak{p}_0\subset\mathfrak{p}_1\subset\cdots\subset\mathfrak{p}_n$ 的长度定义为 n. 而 R 中素理想严格升链的最大长度叫做 R 的 (Krull)**维数**，记作 $\dim R$；而当最大长度不存在时，令 $\dim R=+\infty$.

例 (1) 域是 0 维环. 由命题 3.4.2，Artin 环均是 0 维环. 一般地，$\dim R=0\Leftrightarrow R$ 的素理想均是极大的.

(2) 整数环 $\mathbb{Z}$ 是 1 维环. 若 R 是整环，则 $\dim R=1\Leftrightarrow R$ 不是域，且 R 的非零素理想均是极大的.

命题 3.4.4 Artin 环 R 仅有有限个极大理想，因而是半局部环.

证明 不妨设 $R\neq 0$. 考虑集合

$$\Sigma=\{\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_r\mid r\geqslant 1,\ \mathfrak{q}_i\in\mathrm{Max}\,R\}.$$

因 R 是 Artin 环且 Σ 非空，Σ 有极小元 $\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_n$，$\mathfrak{m}_i\in\mathrm{Max}\,R$. 若 $\mathfrak{m}\in\mathrm{Max}\,R$，则 $\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_n\cap\mathfrak{m}=\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_n$，从而 $\mathfrak{m}\supseteq\mathfrak{m}_1\cap\cdots\cap\mathfrak{m}_n\supseteq\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n$. 于是，存在某个 $\mathfrak{m}_i$ 使得 $\mathfrak{m}\supseteq\mathfrak{m}_i$，从而 $\mathfrak{m}=\mathfrak{m}_i$. 所以 $\{\mathfrak{m}_1,\cdots,\mathfrak{m}_n\}$ 就是 R 的全部极大理想. □

命题 3.4.5 若 R 是 Artin 环，则 $\mathrm{Nil}(R)$ 是幂零理想.

证明 记 $I=\mathrm{Nil}(R)$. 由降链条件，存在 $n\geqslant 1$，使得 $I^n=I^{n+1}=\cdots$. 记 $J=I^n$，则 $J^2=J$. 假定 $J\neq 0$，则存在 $x\in J$ 使得 $xJ\neq 0$. 令 $\Sigma=\{yJ\mid y\in J$，且 $yJ\neq 0\}$，则 Σ 非空. 由极小条件，Σ 中有极小元 zJ，$z\in J$. 因 $0\neq zJ=zJ^2$，故存在 $u\in J$ 使得 $zuJ\neq 0$. 而 $zuJ\subseteq zJ$，由 zJ 的极小性得 $zuJ=zJ$，从而存在 $v\in J$ 使得 $zu=zuv$. 于是有 $zu=zuv=zuv^2=\cdots=zuv^k=\cdots$，而 $v\in J\subseteq\mathrm{Nil}(R)$ 是幂零元，所以 $zu=0$，这与 $zuJ\neq 0$ 矛盾. 所以 $J=I^n=0$. □

命题 3.4.6 若环 R 的零理想是有限个极大理想的积，则 R

是 Noether 环当且仅当 R 是 Artin 环.

证明 设 $0=\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_n$, $\mathfrak{q}_i\in\operatorname{Max} R$. 令 $M_i=(\mathfrak{q}_1\cdots\mathfrak{q}_{i-1})/(\mathfrak{q}_1\cdots\mathfrak{q}_{i-1}\mathfrak{q}_i)$, $i=2,\cdots,n$. 由于 R-模 M_i 被 $\mathfrak{q}_i$ 零化, 故 M_i 也是 $R/\mathfrak{q}_i$-模, 且与 M_i 作为 R-模的结构一样. 但 $R/\mathfrak{q}_i$ 是域, 从而 M_i 是 $R/\mathfrak{q}_i$ 上的线性空间. 对于域 F 上的线性空间 V, V 是 Artin(或 Noether) F-模 $\Leftrightarrow \dim_F V$ 有限 $\Leftrightarrow F$-模 V 有合成列. 这样, 若 R 是 Artin(或 Noether)环, 则 M_i 作为 R 的商模 $R/\mathfrak{q}_1\cdots\mathfrak{q}_i$ 的子模是 Artin(或 Noether) R-模, 从而 M_i 也是 Artin(或 Noether) $R/\mathfrak{q}_i$-模, 故 M_i 有合成列. 也就是说, 在 $\mathfrak{q}_1\cdots\mathfrak{q}_{i-1}$ 和 $\mathfrak{q}_1\cdots\mathfrak{q}_i$ 之间可插入有限个 R-模, 使得相邻两模之商均是单 R-模, 于是降链 $R\supseteq\mathfrak{q}_1\supseteq\mathfrak{q}_1\mathfrak{q}_2\supseteq\cdots\supseteq\mathfrak{q}_1\cdots\mathfrak{q}_n=0$ 可加细成 R 的一个合成列. 由命题3.2.6, R 是 Artin 环, 且是 Noether 环. □

定理 3.4.7 环 R 是 Artin 环当且仅当 R 是 Noether 环且 $\dim R=0$.

证明 若 R 是 Artin 环, 则由命题 3.4.2 和 3.4.4 可知, $\dim R=0$, 且 R 仅有有限个极大理想, 设为 $\mathfrak{q}_1,\cdots,\mathfrak{q}_n$. 由命题 3.4.2、定理 1.1.3 和命题 3.4.5, $\operatorname{Nil}(R)=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_n$ 是幂零理想. 于是存在 $k\geqslant 1$, 使得 $(\mathfrak{q}_1\cdots\mathfrak{q}_n)^k\subseteq(\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_n)^k=0$, 所以 $0=\mathfrak{q}_1^k\cdots\mathfrak{q}_n^k$. 由命题 3.4.6, R 是 Noether 环.

若 R 是 Noether 环, 且素理想均是极大的, 设 $0=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_n$ 为准素分解, $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$, 则 $\operatorname{Nil}(R)=\sqrt{0}=\bigcap_{i=1}^{n}\mathfrak{p}_i$. 由命题 3.4.5, 存在 $k\geqslant 1$, 使得 $(\mathfrak{p}_1\cdots\mathfrak{p}_n)^k\subseteq(\mathfrak{p}_1\cap\cdots\cap\mathfrak{p}_n)^k=0$, 于是 $0=\mathfrak{p}_1^k\cdots\mathfrak{p}_n^k$. 因 $\mathfrak{p}_i$ 均是极大的, 由命题 3.4.6, R 是 Artin 环. □

定理 3.4.8(Artin 环的结构定理) 每个 Artin 环 R 可表示成有限个 Artin 局部环 R_i 的直和: $R=R_1\oplus\cdots\oplus R_n$. 又若 $R=R_1'\oplus\cdots\oplus R_m'$, 其中 R_i' 均是 Artin 局部环, 则 $n=m$, 且有 $\{1,2,\cdots,n\}$ 的一个置换 σ, 使得 $R_i\simeq R_{\sigma(i)}'$(环同构), $i=1,\cdots,n$.

证明 存在性：据命题 3.4.4，R 有有限个极大理想 $\mathfrak{q}_1,\cdots,\mathfrak{q}_n$. 由定理 3.4.7 的证明，存在 $k\geqslant 1$ 使得 $0=\mathfrak{q}_1^k\cdots\mathfrak{q}_n^k=\mathfrak{q}_1^k\cap\cdots\cap\mathfrak{q}_n^k$（这是因为 $\mathfrak{q}_i^k$ 是两两互素的）. 由中国剩余定理，$R\simeq R/\mathfrak{q}_1^k\oplus\cdots\oplus R/\mathfrak{q}_n^k$，其中 $R/\mathfrak{q}_i^k$ 均是 Artin 局部环，有唯一的极大理想 $\mathfrak{q}_i/\mathfrak{q}_i^k$（习题 1.1.12）.

唯一性：设 $R=R_1\oplus\cdots\oplus R_n$，$R_i$ 均是 Artin 局部环. 令 π_i：$R\to R_i$ 为标准投影，$I_i=\operatorname{Ker}\pi_i$，$i=1,2,\cdots,n$. 则 I_i 两两互素，且 $\bigcap_{i=1}^{n}I_i=0$. 设 $\mathfrak{q}_i$ 是 R_i 的唯一的极大理想，则 $\mathfrak{p}_i=\pi_i^{-1}(\mathfrak{q}_i)$ 是 R 的素理想. 由命题 3.4.2，$\mathfrak{p}_i$ 均是极大理想. 另一方面，因 $\mathfrak{q}_i$ 均是幂零理想，故存在 $k_i\geqslant 1$，使得 $I_i\supseteq\mathfrak{p}_i^{k_i}$，两边取根得 $\sqrt{I_i}\supseteq\mathfrak{p}_i$. 由 $\mathfrak{p}_i$ 的极大性，得 $\sqrt{I_i}=\mathfrak{p}_i$. 由命题 3.1.3 可知 I_i 是 $\mathfrak{p}_i$-准素理想. 所以 $0=\bigcap_{i=1}^{n}I_i$ 是准素分解式. 因 I_i 两两互素，所以 $\mathfrak{p}_i$ 也两两互素，于是 $\mathfrak{p}_i$ 均是属于 0 理想的极小素理想，从而 I_i 均是 0 理想的孤立准素分支. 据定理 3.1.9，I_i，$i=1,\cdots,n$，由 R 唯一确定，从而 $R/I_i\simeq R_i$ 也由 R 唯一确定. □

习 题 3.4

1. 设 M 是 Artin R-模. 证明：$R/\operatorname{Ann}_R(M)$ 是 Artin 环.

2. 设 k 是域，$0\neq f(x)\in k[x]$. 证明：$k[x]/(f(x))$ 是 Artin环，试将它表示成有限个 Artin 局部环的直和.

3. 设 k 是域，$R=k[x^2,x^3]/(x^4)$. 证明 R 是 Artin 局部环.

4. 设 R 是 Artin 局部环，$\mathfrak{m}$ 是 R 的唯一极大理想，$k=R/\mathfrak{m}$. 证明下列条件等价：

(1) R 的每个理想均是主理想；

(2) $\mathfrak{m}$ 是主理想；

(3) $\dim_k(\mathfrak{m}/\mathfrak{m}^2)\leqslant 1$.

5. (**Nagata**)设 $R=F[x_1,x_2,\cdots,x_n,\cdots]$是域 F 上的可数无穷多个未定元的多项式环. 且设 $m_1<m_2<\cdots$是正整数数列, 使得对于每个 $i\geqslant 2$, 均有 $m_{i+1}-m_i>m_i-m_{i-1}$. 令 $\mathfrak{p}_i=(x_{m_i+1},\cdots,x_{m_{i+1}})$, $S=R/\bigcup\limits_{i\geqslant 1}\mathfrak{p}_i$. 证明:

(1) $\mathfrak{p}_i\in\operatorname{Spec}R$, $i\geqslant 1$.

(2) S 是 R 的乘法集.

(3) $S^{-1}R$ 是 Noether 整环.

(4) $\dim S^{-1}R=+\infty$.

3.5 代 数 集

本节介绍交换代数的代数几何背景, 侧重于介绍概念间的联系, 这有助于理解学习和研究交换代数的意义.

3.5.1 代数集与根式理想

设 k 是域, $R=k[x_1,\cdots,x_n]$是 k 上的 n 元多项式环, k^n 是 k 上的 n 维向量空间. 且设 $f=f(x_1,\cdots,x_n)\in R$, $\alpha=(a_1,\cdots,a_n)\in k^n$. 若 $f(\alpha)=f(a_1,\cdots,a_n)=0$, 则称 α 是 f 的**根或零点**, 或称 α 是方程 $f(x_1,\cdots,x_n)=0$ 的**解**. 代数几何研究的基本问题是方程组 $f_i(x_1,\cdots,x_n)=0$, $f_i\in R$, $i=1,2,\cdots,m$, 在 k^n 中的公共解集合的性质. 当 $f_1,\cdots,f_m$ 均是一次多项式时, 这个问题由线性代数中的域上的线性方程组理论完整地解决. 当 f_i 的次数大于 1 时, 这个问题很不简单.

设 $S\subseteq R$. S 中的多项式在 k^n 中的所有公共根的集合记作 $\mathcal{V}(S)$. 设 $A\subseteq k^n$, 称 A 是 k^n 中的一个(仿射)**代数集**, 如果存在 $S\subseteq R$, 使得 $A=\mathcal{V}(S)$; 也称 A 为 S 所对应的 k 上的代数集. 若 I 是由 S 生成的 R 的理想, 易证 $\mathcal{V}(I)=\mathcal{V}(S)$. 由 Hilbert 基定理,

R 的每个理想 I 均是有限生成的，于是讨论有限个 $f_i \in R$ 的公共根集合与讨论 R 的理想 I 所对应的代数集 $\mathscr{V}(I)$ 是一回事．代数几何的基本问题就是研究 k^n 中代数集的性质．

另一方面，任给 k^n 的一个子集 A，令

$$\mathscr{I}(A) = \{f \in R \mid 对于每个\ \alpha \in A,\ f(\alpha) = 0\}.$$

这是 R 的理想，称为 A 所对应的理想．

对应 $S \mapsto \mathscr{V}(S)$ 和 $A \mapsto \mathscr{I}(A)$ 具有以下性质．

命题 3.5.1　设 k 是域，$R = k[x_1, \cdots, x_n]$；S, T, S_λ 均是 R 的子集，$\lambda \in \Lambda$；A, B 是 k^n 的子集．则

(1) $S \subseteq T \Rightarrow \mathscr{V}(S) \supseteq \mathscr{V}(T)$；$A \subseteq B \Rightarrow \mathscr{I}(A) \supseteq \mathscr{I}(B)$．

(2) $S \subseteq \mathscr{I}\mathscr{V}(S)$，$A \subseteq \mathscr{V}\mathscr{I}(A)$．

(3) $\mathscr{V}\mathscr{I}\mathscr{V}(S) = \mathscr{V}(S)$，$\mathscr{I}\mathscr{V}\mathscr{I}(A) = \mathscr{I}(A)$．

(4) $\mathscr{V}(\bigcup\limits_{\lambda \in \Lambda} S_i) = \bigcap\limits_{\lambda \in \Lambda} \mathscr{V}(S_i)$．

(5) $\mathscr{V}(S) \cup \mathscr{V}(T) = \mathscr{V}(ST)$，其中 $ST = \{fg \mid f \in S,\ g \in T\}$；若 S, T 是 R 的理想，则 $\mathscr{V}(S) \cup \mathscr{V}(T) = \mathscr{V}(S \cap T)$．

(6) $\mathscr{V}(R) = \varnothing$，$\mathscr{V}(0) = k^n$．

(7) 若 I 是 R 的理想，则 $\mathscr{V}(I) = \mathscr{V}(\sqrt{I})$．

(8) $\mathscr{I}(A)$ 是 R 的根式理想．

证明　(1),(2),(4),(6)由定义直接推出．

(3) 由(2)有 $S \subseteq \mathscr{I}\mathscr{V}(S)$，再由(1)得 $\mathscr{V}(S) \supseteq \mathscr{V}\mathscr{I}\mathscr{V}(S)$．另一方面，由(2)有 $\mathscr{V}(S) \subseteq \mathscr{V}\mathscr{I}(\mathscr{V}(S)) = \mathscr{V}\mathscr{I}\mathscr{V}(S)$．所以 $\mathscr{V}(S) = \mathscr{V}\mathscr{I}\mathscr{V}(S)$．同样可证 $\mathscr{I}\mathscr{V}\mathscr{I}(A) = \mathscr{I}(A)$．

(5) 易知 $\mathscr{V}(S) \cup \mathscr{V}(T) \subseteq \mathscr{V}(ST)$．若 $\alpha \in \mathscr{V}(ST) \backslash \mathscr{V}(S)$，则存在 $f \in S$ 使得 $f(\alpha) \neq 0$．但对于任意 $g \in T$，均有 $f(\alpha)g(\alpha) = 0$，从而 $g(\alpha) = 0$，所以 $\alpha \in \mathscr{V}(T)$．于是 $\mathscr{V}(ST) = \mathscr{V}(S) \cup \mathscr{V}(T)$．若 S, T 是 R 的理想，则 $ST \subseteq S \cap T$，由(1)得 $\mathscr{V}(S \cap T) \subseteq \mathscr{V}(ST) = \mathscr{V}(S) \cup \mathscr{V}(T)$，而 $\mathscr{V}(S \cap T) \supseteq \mathscr{V}(S) \cup \mathscr{V}(T)$ 是显然的．所以 $\mathscr{V}(S \cap T) = \mathscr{V}(S) \cup \mathscr{V}(T)$．

(7) 因 $I\subseteq\sqrt{I}$，由(1)，$\mathcal{V}(I)\supseteq\mathcal{V}(\sqrt{I})$．若 $\alpha\in\mathcal{V}(I)$，则对于任意的 $f\in\sqrt{I}$，存在 $m\geqslant 1$ 使得 $f^m\in I$，于是 $f^m(\alpha)=0$，从而 $f(\alpha)=0$，所以 $\alpha\in\mathcal{V}(\sqrt{I})$．于是 $\mathcal{V}(I)=\mathcal{V}(\sqrt{I})$．

(8) 若 $f\in\sqrt{\mathcal{I}(A)}$，则存在 $m\geqslant 1$ 使得 $f^m\in\mathcal{I}(A)$．于是对于任意 $\alpha\in A$，$f^m(\alpha)=0$，从而 $f(\alpha)=0$，所以 $f\in\mathcal{I}(A)$．故 $\sqrt{\mathcal{I}(A)}=\mathcal{I}(A)$． □

并非 k^n 的每个子集都是代数集．例如，在 k^1 中，代数集只能是 k^1，$\varnothing$，以及有限集．

设 A 是 k^n 的子集，由命题 3.5.1 的(4)可知，k^n 中包含 A 的代数集(k^n 就是一个这样的代数集)之交仍是代数集，记作 $\overline{A}$，它是 k^n 中包含 A 的最小代数集，称 $\overline{A}$ 为 A 的**闭包**．

由命题 3.5.1 的(8)和(3)可知，对于 k^n 中的每个代数集 A，$\mathcal{I}(A)$是 R 的根式理想，且 $\mathcal{V}\mathcal{I}(A)=A$．假如对于 R 的每个根式理想 I 均有 $\mathcal{I}\mathcal{V}(I)=I$，则 $\mathcal{V}$ 和 $\mathcal{I}$ 是 k^n 中的代数集与 R 中的根式理想之间的一对互逆双射．为此，需限制 k 是代数闭域，并证明下面的 Hilbert 零点定理．这一定理对于代数几何的重要性和基本性相当于一元多项式方程论的代数学基本定理．下面给出的这一定理的证法需要如下引理，其证明将在第 4 章 4.3 节中给出．

引理 4.3.18 设 k 是域，$y_1,\cdots,y_n$ 是 k 的某个扩域中的元素．若 $k[y_1,\cdots,y_n]$是域，则每个 y_i 均是 k 上的代数元．

定理 3.5.2 (Hilbert 零点定理) 设 k 是代数闭域，$R=k[x_1,\cdots,x_n]$，I 是 R 的理想．则

(1) $I\neq R\Rightarrow\mathcal{V}(I)\neq\varnothing$．

(2) $\mathcal{I}\mathcal{V}(I)=\sqrt{I}$．

证明 (1) 由命题 3.5.1 的(1)，不妨设 I 是 R 的极大理想，则 R/I 是域．由于 $I\cap k=0$，可视 k 为 R/I 的子域，于是 $R/I=k[\bar{x}_1,\cdots,\bar{x}_n]$，其中 $\bar{x}_i=x_i+I$．据引理 4.3.18，$\bar{x}_i$ 是 k 上的代数元，而 k 是代数闭域，所以 $\bar{x}_i\in k$．对于任意的 $f(x_1,\cdots,x_n)\in$

I，在 R/I 中，$0=\overline{f(x_1,\cdots,x_n)}=f(\bar{x}_1,\cdots,\bar{x}_n)$，所以$(\bar{x}_1,\cdots,\bar{x}_n)\in\mathscr{V}(I)\neq\varnothing$.

(2) 设 $f\in\sqrt{I}$，则存在 $m\geqslant1$ 使得 $f^m\in I$. 于是，对于任意 $\alpha\in\mathscr{V}(I)$，有 $f^m(\alpha)=0$，从而 $f(\alpha)=0$，所以 $f\in\mathscr{IV}(I)$. 另一方面，设 $0\neq f\in\mathscr{IV}(I)$，要证存在 $m\geqslant1$ 使得 $f^m\in I$，从而 $f\in\sqrt{I}$，进而(2)得证. 令 $R'=k[x_1,\cdots,x_{n+1}]=R[x_{n+1}]$，记 J 为由 I 和 $1-x_{n+1}f$ 生成的 R' 的理想. 假定 $J\neq R'$，由(1)，存在$(a_1,\cdots,a_n,a_{n+1})\in\mathscr{V}(J)$. 于是$(a_1,\cdots,a_n)\in\mathscr{V}(I)$，从而 $1-a_{n+1}f(a_1,\cdots,a_n)=1\neq0$，这是一个矛盾. 所以 $J=R'$. 于是存在 $r_i,r\in R'$，$q_i\in I$，使得 $1=\sum\limits_{i=1}^{t}r_iq_i+r(1-x_{n+1}f)$. 令 $x_{n+1}=1/f$，则 $1=\sum\limits_{i=1}^{t}\bar{r}_iq_i$，其中 $\bar{r}_i\in k[x_1,\cdots,x_n,1/f]$. 取充分大的 $m\geqslant1$，可使 $f^m\bar{r}_i\in R$，$i=1,2,\cdots,t$，从而 $f^m=\sum\limits_{i=1}^{t}(f^m\bar{r}_i)q_i\in I$. □

由定理 3.5.2 的(1)可知，当 k 是代数闭域时，对于任意 $f_1,\cdots,f_m\in R$，只要由它们生成的理想不是 R，则它们在 k^n 中必有公共零点.

定理 3.5.3　设 k 是代数闭域，$R=k[x_1,\cdots,x_n]$. 则 k^n 中的代数集一一反序对应于 R 的根式理想.

证明　设 A 是 k^n 中的代数集，则 $A=\mathscr{V}(I)$，I 是 R 的理想. 由定理 3.5.2，$\mathscr{I}(A)=\mathscr{IV}(I)=\sqrt{I}$ 是 R 的根式理想. 再由命题 3.5.1的(7)，$\mathscr{VI}(A)=\mathscr{V}(\sqrt{I})=\mathscr{V}(I)=A$. 若 I 是 R 的根式理想，则 $\mathscr{V}(I)$是 k^n 中的代数集，且 $\mathscr{IV}(I)=\sqrt{I}=I$. 这样，$\mathscr{V}$ 和 $\mathscr{I}$ 就是所需的一对互逆的双射，其反序性由命题 3.5.1 的(1)可得. □

推论 3.5.4　设 k 是代数闭域，$R=k[x_1,\cdots,x_n]$. 则

$$\operatorname{Max} R=\{(x_1-a_1,\cdots,x_n-a_n)\mid a_1,\cdots,a_n\in k\}.$$

证明　设 $\alpha=(a_1,\cdots,a_n)\in k^n$，则 α 是 $x_1-a_1,\cdots,x_n-a_n$

$\in R$ 的公共根. 故 k^n 中的一点集 $\{\alpha\}$ 均是极小的非空代数集, 且 $\mathscr{I}(\{\alpha\})=(x_1-a_1,\cdots,x_n-a_n)$, 再由定理 3.5.3 即得证. □

3.5.2 不可约代数集与素理想

设 k 是域, k^n 中的代数集 A 称为**不可约**代数集, 如果不存在 k^n 中的代数集 A_1 和 A_2, 使得 $A=A_1\cup A_2$, 且 $A_1\neq A$, $A_2\neq A$.

定理 3.5.5 设 k 是代数闭域, $R=k[x_1,\cdots,x_n]$. 则

(1) k^n 中的非空代数集 A 是不可约的当且仅当 $\mathscr{I}(A)$ 是 R 的素理想.

(2) k^n 中的非空不可约代数集一一反序对应于 R 的素理想.

(3) k^n 中的每个代数集均可唯一地表示成有限个互不包含的不可约代数集之并.

证明 设 A 是 k^n 中的代数集, $A\neq\varnothing$. 则 $I=\mathscr{I}(A)$ 是 R 的根式理想, $I\neq R$, 且 $\mathscr{V}(I)=A$. 因 R 是 Noether 环, 由命题 3.3.9, I 可唯一地表示成 $I=\bigcap\limits_{i=1}^{m}\mathfrak{p}_i$, 其中 $\mathfrak{p}_i$ 是两两互不包含的素理想. 于是 $A=\mathscr{V}(I)=\bigcup\limits_{i=1}^{m}\mathscr{V}(\mathfrak{p}_i)$, 其中 $\mathscr{V}(\mathfrak{p}_i)$ 是 k^n 中的两两互不包含的代数集. 因而若 A 是不可约的, 则 $m=1$, 从而 I 是 R 的素理想. 反之, 若 I 是素理想, $A=A_1\cup A_2$, 其中 A_1 和 A_2 是 k^n 中的代数集. 令 $I_1=\mathscr{I}(A_1)$, $I_2=\mathscr{I}(A_2)$, 则 $I=\mathscr{I}(A)=\mathscr{I}(A_1)\cap\mathscr{I}(A_2)=I_1\cap I_2$. 由于 I 是素理想, 故 $I=I_1$ 或 $I=I_2$, 从而 $A=A_1$ 或 $A=A_2$, 所以 A 是不可约的. 这样(1)和(2)得证. 又由分解 $I=\bigcap\limits_{i=1}^{m}\mathfrak{p}_i$ 的唯一性可得分解 $A=\bigcup\limits_{i=1}^{m}\mathscr{V}(\mathfrak{p}_i)$ 的唯一性. 所以(3)成立. □

设 I 是 $k[x_1,\cdots,x_n]$ 的理想, $I=\bigcap\limits_{i=1}^{m}\mathfrak{q}_i$ 是极小准素分解式, $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$, 则 $\mathscr{V}(\mathfrak{q}_i)=\mathscr{V}(\sqrt{\mathfrak{q}_i})=\mathscr{V}(\mathfrak{p}_i)$, 从而 $\mathscr{V}(I)=\bigcup\limits_{i=1}^{m}\mathscr{V}(\mathfrak{q}_i)=$

$\bigcup_{i=1}^{m}\mathcal{V}(\mathfrak{p}_i)$. 若 $\mathfrak{p}_1\subset\mathfrak{p}_2$，即 $\mathfrak{p}_2$ 是属于 I 的嵌入素理想，则 $\mathcal{V}(\mathfrak{p}_1)\supset\mathcal{V}(\mathfrak{p}_2)$，即代数集 $\mathcal{V}(\mathfrak{p}_2)$ 可嵌入 $\mathcal{V}(\mathfrak{p}_1)$ 之中. 这就是将 $\mathfrak{p}_2$ 称为属于 I 的"嵌入"素理想的几何背景.

3.5.3　坐标环

设 k 是代数闭域，$R=k[x_1,\cdots,x_n]$，V 是 k^n 中的非空代数集，则 $I=\mathcal{I}(V)$ 是 R 中的根式理想，且 $I\neq R$. 对于每个 $f=f(x_1,\cdots,x_n)\in R$，定义映射

$$f:V\to k;\alpha=(a_1,\cdots,a_n)\mapsto f(\alpha)=f(a_1,\cdots,a_n),$$

叫做 V 的一个**多项式函数**. 又若 $g\in R$，则 f 和 g 作为 V 的多项式函数相等 $\Leftrightarrow$ 对于每个 $\alpha\in V$，$f(\alpha)=g(\alpha)\Leftrightarrow f-g\in\mathcal{I}(V)=I$. 也就是说，$V$ 的一个多项式函数相当于商环 R/I 中的一个元素. 商环 R/I 称为代数集 V 的(仿射)**坐标环**，或**多项式函数环**，记作 $k[V]$. 由于 R 是 Noether 环，$k[V]$ 也是 Noether 环.

因 $I\neq R$，故 $I\cap k=0$. 于是可视 k 为 $k[V]$ 的子域，从而 $k[V]$ 还是一个 k-模(k 上的线性空间). 记 $\bar{x}_i=x_i+I$，则 $k[V]=k[\bar{x}_1,\cdots,\bar{x}_n]$. 又因 I 是根式理想，$k[V]$ 不含非零的幂零元，即 $\mathrm{Nil}(k[V])=0$.

这样就将每个代数集 V 与一个代数对象 $k[V]$ 联系起来，由定理 3.5.5 可知，V 是不可约的当且仅当 $k[V]$ 是整环.

3.5.4　k-代数

为了准确地表述坐标环的性质，需要介绍 k-代数的概念.

设 $(A,+,\cdot)$ 是一个(交换)环，k 是一个域. 如果 $(A,+)$ 是一个 k-模，且对于任意 $r\in k$ 和 $a,b\in A$，均有 $(ra)b=a(rb)=r(ab)$，则称 A 是一个(交换)**k-代数**. 若 k-代数间的映射 $f:A\to B$ 是环同态，且是 k-模同态，则称 f 是一个 **k-代数同态**，进而可定义 k-代数同构. 又若 $g:B\to C$ 也是 k-代数同态，则 $gf:A\to C$

也是k-代数同态. 这样, 以 k-代数为对象, k-代数同态为态射, 可构成一个 k-代数范畴, 记作 k-$\mathscr{Al}$. 称一个 k-代数A 是**有限生成**k-代数, 如果存在 $a_1,\cdots,a_n\in A$ 使得$A=k[a_1,\cdots,a_n]$.

由前述可知, 对于代数闭域 k 上的一个代数集 V, 可确定一个 k-代数$A=k[V]$, 满足条件:

(1) A 是有限生成k-代数;

(2) $\mathrm{Nil}(A)=0$, 即 A 是半素环.

反之, 设(交换)k-代数 A 满足上述两个条件. 由(1)可设 $A=k[a_1,\cdots,a_n]$, $a_i\in A$. 则有 k-代数满同态$\varphi:R=k[x_1,\cdots,x_n]\mapsto A$, 使得 $\varphi(x_i)=a_i$, $i=1,\cdots,n$. 记 $\mathrm{Ker}\varphi=I$, 则 $I\neq R$. 由(2), I 是 R 的根式理想, 从而确定一个 k^n 中的代数集 $V=\mathscr{V}(I)$. 这样就建立了 k 上的代数集与满足上述两个条件的 k-代数间的对应关系.

3.5.5 多项式映射

下一步自然要研究代数集之间的联系及分类问题.

设 k 是代数闭域, U 和 V 分别是 k^m 和 k^n 中的代数集. 对于任意的 $f_i=f_i(x_1,\cdots,x_m)\in k[x_1,\cdots,x_m]$, $i=1,\cdots,n$, 可定义映射

$$f=(f_1,\cdots,f_n):k^m\to k^n;\alpha=(a_1,\cdots,a_m)\mapsto(f_1(\alpha),\cdots,f_n(\alpha)).$$

若 $f(U)\subseteq V$, 则称 f 在 U 上的限制, 记作 $f:U\to V$, 是从 U 到 V 的一个**多项式映射**. 又若 $g:V\to W$ 是从代数集 V 到 W 的多项式映射, 则合成 $g\circ f:U\to W$ 也是多项式映射, 这是因为两个多项式的合成仍是多项式, 且$(g\circ f)(U)\subseteq g(V)\subseteq W$. 并且恒等映射 $1_V:V\to V$ 也是多项式映射. 这样, 以 k 上的代数集为对象, 以多项式映射为态射, 构成一个 **k-代数集范畴**, 记作 k-$\mathscr{AS}$. 两个 k 上的代数集 U 和 V 是**同构**的, 如果存在多项式映射 $f:U\to V$ 和$g:V\to U$, 使得 $g\circ f=1_U$, $f\circ g=1_V$.

设 $f:U\to V$ 是代数闭域 k 上的代数集 U 到 V 的多项式映射，对于每个 $h\in k[V]$，均有 $h\circ f\in k[U]$，从而 f 诱导出映射

$$f^*:k[V]\to k[U];\ h\mapsto h\circ f.$$

不难验证，f^* 是环同态. 对于每个 $a\in k\subseteq k[V]$，可视 a 为 V 到 k 的常值为 a 的多项式函数，于是有 $f^*(a)=a$. 所以 f^* 在 k 上的限制是恒等映射. 对于任意 $a\in k$ 和 $h\in k[V]$，均有 $f^*(ah)=f^*(a)f^*(h)=af^*(h)$，故 f^* 还是 k-模同态. 所以 f^* 是 k-代数同态.

又若 $g:V\to W$ 也是 k 上代数集的多项式映射，容易验证，$(g\circ f)^*=f^*\circ g^*:k[W]\to k[U]$，且有$(1_V)^*=1_{k[V]}$. 这样，就可定义一个从 k-代数集范畴到 k-代数范畴的反变函子 $F:k\text{-}\mathscr{AS}\to k\text{-}\mathscr{A}l$，它将 k 上的代数集 V 对应于 $k[V]$，而将 k 上代数集间的多项式映射 $f:U\to V$ 对应于 k-代数同态 $f^*:k[V]\to k[U]$.

反之，设 $\varphi:k[V]\to k[U]$是坐标环的 k-代数同态. 对于每个 $y_i\in k[V]=k[y_1,\cdots,y_n]/\mathscr{I}(V)$，令 $\varphi(y_i)=f_i=f_i(x_1,\cdots,x_m)\in k[U]=k[x_1,\cdots,x_m]/\mathscr{I}(U)$，$i=1,\cdots,n$. 定义映射

$$G(\varphi)=f=(f_1,\cdots,f_n):k^m\to k^n;$$
$$\alpha=(a_1,\cdots,a_m)\mapsto f(\alpha)=(f_1(\alpha),\cdots,f_n(\alpha)).$$

对于任意 $h\in\mathscr{I}(V)$和 $\alpha=(a_1,\cdots,a_m)\in U$，$\varphi(h)=h(f_1,\cdots,f_n)=h\circ f$ 是$k[U]$中的零元，于是 $\varphi(h)(\alpha)=h(f(\alpha))=0$，从而 $f(\alpha)\in V$，所以 $f(U)\subseteq V$. 这样，$f:U\to V$ 是一个多项式映射. 又由于对于任意的 $h\in k[V]$，均有 $\varphi(h)=h(f_1,\cdots,f_n)=h\circ f$，所以 $f^*=\varphi$，即有 $FG(\varphi)=\varphi$. 又若 $\psi:k[W]\to k[V]$也是坐标环的 k-代数同态，容易验证，$G(\psi\circ\varphi)=G(\varphi)\circ G(\psi)$，且有 $G(1_{k[V]})=1_V$. 记 $\mathscr{C}$ 是以 k 上的代数集的坐标环(作为 k-代数)为对象类构成的 $k\text{-}\mathscr{A}l$ 的全子范畴. 由上述证明可知，$G:\mathscr{C}\to k\text{-}\mathscr{AS}$是一个反变函子，它将坐标环 $k[V]$对应于 V，而将坐标环的 k-代数同态 $\varphi:k[V]\to k[U]$对应于多项式映射 $G(\varphi):U\to$

V，并且 $FG=1_{\mathscr{C}}$，$GF=1_{k\text{-}\mathscr{AS}}$，所以有范畴同构 $\mathscr{C}\simeq k\text{-}\mathscr{AS}$. 这样，两个 k 上的代数集同构当且仅当它们的坐标环作为 k-代数同构.

记 $\mathscr{D}$ 是以半素有限生成(交换)k-代数为对象类构成的 $k\text{-}\mathscr{Al}$ 的全子范畴，则上面定义的范畴 $\mathscr{C}$ 是 $\mathscr{D}$ 的子范畴，于是有包含函子 $\tau:\mathscr{C}\to\mathscr{D}$，它将 $\mathscr{C}$ 中的对象及态射对应于自身. 对于每个 $A\in \mathrm{ob}\,\mathscr{D}$，前面已证，总存在一个 k 上的代数集 V 使得 $k[V]\simeq A$. 令 $H(A)=k[V]$，且令 $\eta_A:A\to k[V]=H(A)$ 是一个 k-代数同构. 若 $f:A\to B$ 是 $\mathscr{D}$ 中的态射，令 $H(f)=\eta_B f\eta_A^{-1}:H(A)\to H(B)$. 容易验证，$H:\mathscr{D}\to\mathscr{C}$ 是一个函子，且 $\eta:1_{\mathscr{D}}\to\tau H$ 和 $\eta:1_{\mathscr{C}}\to H\tau$ 均是自然同构. 所以范畴 $\mathscr{D}$ 与 $\mathscr{C}$ 等价，从而 $\mathscr{D}$ 与 $k\text{-}\mathscr{AS}$ 等价. 注意到 $k\text{-}\mathscr{AS}$ 的对象类实际上是一个集合，即 $k\text{-}\mathscr{AS}$ 是一个小范畴，因而 $k\text{-}\mathscr{AS}$ 与 $\mathscr{D}$ 不同构.

这样就建立了 k-代数集范畴与一个“纯代数”的特殊范畴 $\mathscr{D}$ 之间的等价关系.

习 题 3.5

以下的 k 均指代数闭域.

1. 设 $V_1\supseteq V_2\supseteq\cdots\supseteq V_n\supseteq\cdots$ 是 k^n 中的代数集的降链. 证明：存在 $t\geqslant 1$ 使得 $V_t=V_{t+1}=\cdots$.

2. 设 $I=(x^2,xy,yz,zx)$ 是 $k[x,y,z]$ 中的理想，试将 k^3 中的代数集 $\mathscr{V}(I)$ 分解成互不包含的不可约代数集之并.

3. 设 $\alpha_1,\cdots,\alpha_m$ 是 k^n 中的 m 个不同的点. 证明：存在 $f_i\in k[x_1,\cdots,x_n]$ 使得 $f_i(\alpha_j)=0$，如果 $i\neq j$，而且 $f_i(\alpha_i)=1$.

4. 设 F 是无限域. 证明：$\{(a_1,\cdots,a_n)\in F^n \mid a_1\cdots a_n\neq 0\}$ 不是 F 上的代数集.

5. 若域 F 不是代数闭域，试问：

(1) Hilbert 零点定理是否成立?

(2) $F[x_1,\cdots,x_n]$ 中的极大理想是否均有 $\mathfrak{m}=(x_1-a_1,\cdots,$

$x_n - a_n$), $a_i \in F$, 的形式?

6. 设 U 和 V 分别是 k^m 和 k^n 中的代数集. 证明: $U \times V$ 是 k^{m+n} 中的代数集.

7. 设 X 是非空集合, $F[X]$是域 F 上以 X 为不定元集合的(交换)多项式环. 证明: F-代数 $F[X]$是(交换) F-代数范畴中集合 X 上的自由对象.

8. 设 F 是域, A 和 B 是 F-代数, 在 F-模 $A \underset{F}{\otimes} B$ 中定义乘法, 使得 $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$; $a_i \in A$, $b_i \in B$. 证明:

(1) $A \underset{F}{\otimes} B$ 是 F-代数, 叫做 F-代数 A 与 B 的**张量积**.

(2) 若 $f: A \to B$ 和 $g: A' \to B'$ 是 F-代数同态, 则 $f \otimes g: A \underset{F}{\otimes} A' \to B \underset{F}{\otimes} B'$ 是 F-代数同态.

9. 设 U 和 V 是 k 上的代数集. 证明:

$$k[U \times V] \simeq k[U] \underset{k}{\otimes} k[V].$$

10. 设 k 是代数闭域. 证明:

$$\dim k[x_1, \cdots, x_n] = n$$

(提示: 用推论 3.5.4).

第 4 章 Dedekind 整环

本章介绍由 Gauss 和 Kummer 开创，而由 Dedekind 建立起来的 Dedekind 整环理论的基础知识. 代数数论研究的主要对象代数整数环是典型的 Dedekind 整环.

4.1 Dedekind 整环及其理想类群

4.1.1 定义和基本性质

一个整环 R 称为 **Dedekind 整环**，如果对于 R 的任意理想 I 和 J，只要 $I \subseteq J$，就存在 R 的理想 K，使得 $I = JK$. 例如，主理想整环是 Dedekind 整环；特别地，整数环 $\mathbb{Z}$ 是 Dedekind 整环.

命题 4.1.1 设 R 是 Dedekind 整环，则

(1) 对于 R 的每个非零理想 I，存在 R 的理想 J 和 $a \in R\setminus\{0\}$，使得 $IJ = aR$.

(2) R 的两个理想 I 和 J 作为 R-模同构当且仅当存在 $x, y \in R\setminus\{0\}$，使得 $xI = yJ$.

(3) 设 I, X, Y 是 R 的理想，若 $IX = IY$ 且 $I \neq 0$，则 $X = Y$ (消去律).

(4) R 的每个理想 I 均是有限生成 R-模，从而 R 是 Noether 环.

(5) R 的每个非零素理想均是极大理想，即 $\dim R \leqslant 1$.

证明 (1) 取 $a \in I\setminus\{0\}$，则 $aR \subseteq I$，再由定义得证.

(2) 若 $\varphi: I \to J$ 是 R-模同构，不妨设 $I \neq 0$. 取 $y \in I\setminus\{0\}$，令 $x = \varphi(y) \in J$，则对于任意 $a \in I$，$xa = \varphi(y)a = \varphi(ya) = y\varphi(a)$

$\in yJ$，从而 $xI \subseteq yJ$. 同样，由 R-同构 φ^{-1} 可得 $yJ \subseteq xI$，所以 $xI = yJ$. 反之，若 $xI = yJ$，$x, y \in R \backslash \{0\}$，由于 R 是整环，故有 R-模同构 $I \simeq xI = yJ \simeq J$.

(3) 由(1)，存在 R 的理想 J 和 $a \in R \backslash \{0\}$ 使得 $IJ = aR$. 于是 $aX = aRX = JIX = JIY = aRY = aY$，进而有 $X = Y$.

(4) 不妨设 $I \neq 0$. 由(1)，存在 R 的理想 J 和 $a \in R \backslash \{0\}$ 使得 $IJ = aR$. 于是 $a = \sum_{i=1}^{n} a_i b_i$，$a_i \in I$，$b_i \in J$. 令 $\varphi: R^n \to I$；$(x_1, \cdots, x_n) \mapsto a_1 x_1 + \cdots + a_n x_n$，则 φ 是 R-同态. 若 $y \in I$，则 $yb_i \in IJ = aR$，从而存在唯一的 $z_i \in R$ 使得 $yb_i = az_i$，记 $yb_i / a = z_i$. 令 ψ: $I \to R^n$；$y \mapsto (yb_1/a, \cdots, yb_n/a)$，则 φ 亦是 R-同态，且 $\varphi\psi = 1_I$，从而 φ 是 R-满同态. 所以，I 是有限生成 R-模. 再由命题 3.2.1，R 是 Noether 环.

(5) 设 I 是 R 的非零素理想. 假定 I 不是极大的，则存在 R 的理想 J 使得 $I \subset J \subset R$. 因 R 是 Dedekind 整环，存在 R 的理想 K 使得 $I = JK$. 由(3)得 $I = JK \subset RK = K$. 然而由 I 是素理想可得 $K \subseteq I$，这矛盾. 所以 I 是极大的. □

命题 4.1.2 Dedekind 整环 R 的每个非零理想可唯一地(不计因子次序)表示成有限个素理想之积(约定 R 是 0 个素理想之积).

证明 存在性：设 I 是 R 的理想，$I \neq 0$ 和 R，则 I 含于 R 的某个极大理想 $\mathfrak{p}_1$ 中. 因 R 是 Dedekind 整环，存在 R 的理想 I_1，使得 $I = \mathfrak{p}_1 I_1$，且 $I \subset I_1$. 若 I_1 不是极大的，则 I_1 含于 R 的某个极大理想 $\mathfrak{p}_2$ 中，于是存在 R 的理想 I_2 使得 $I_1 = \mathfrak{p}_1 I_2$，并且 $I = \mathfrak{p}_1 \mathfrak{p}_2 I_2 \subset I_1 \subset I_2$. 如此进行下去，经有限步后，必有 $I_r = \mathfrak{p}_r$ 是 R 的极大理想；否则，将导出 R 的理想的严格升链 $I \subset I_1 \subset I_2 \subset \cdots$，这与 R 是 Noether 环矛盾. 所以，$I = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r$ 是有限个素理想之积.

唯一性：若 $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_r=\mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_s$，$\mathfrak{p}_i$ 和 $\mathfrak{q}_j$ 均是 R 的非零素理想. 因 $\mathfrak{p}_1$ 是素理想，且 $\mathfrak{p}_1\supseteq\mathfrak{q}_1\cdots\mathfrak{q}_s$，故 $\mathfrak{p}_1$ 包含 $\mathfrak{q}_1,\cdots,\mathfrak{q}_s$ 中的某一个，不妨设 $\mathfrak{p}_1\supseteq\mathfrak{q}_1$. 由命题4.1.1的(5)，$\mathfrak{p}_1$ 和 $\mathfrak{q}_1$ 是极大的，所以 $\mathfrak{p}_1=\mathfrak{q}_1$. 再由命题4.1.1的(3)得 $\mathfrak{p}_2\cdots\mathfrak{p}_r=\mathfrak{q}_2\cdots\mathfrak{q}_s$. 如此继续下去，可得 $r=s$，且 $\mathfrak{p}_i=\mathfrak{q}_i$(适当变动次序). □

命题 4.1.3 设 R 是 Dedekind 整环，$I=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$ 和 $J=\mathfrak{p}_1^{f_1}\cdots\mathfrak{p}_t^{f_t}$ 是 R 的非零理想，其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}_t$ 是 R 的互不相同的素理想，$e_i,f_i\geqslant 0$. 则

(1) $I\subseteq J$ 当且仅当 $e_i\geqslant f_i$，$i=1,2,\cdots,t$.

(2) $I+J=\prod\limits_{i=1}^{t}\mathfrak{p}_i^{\min\{e_i,f_i\}}$.

(3) $I\cap J=\prod\limits_{i=1}^{t}\mathfrak{p}_i^{\max\{e_i,f_i\}}$.

(4) $IJ=\prod\limits_{i=1}^{t}\mathfrak{p}_i^{e_i+f_i}$.

证明 (1) 若 $I\subseteq J$，则存在 R 的理想 K 使得 $I=JK$. 由命题4.1.2，K 可表示成 R 的素理想 $\mathfrak{q}_1,\cdots,\mathfrak{q}_s$ 之积. 于是有 $\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}=\mathfrak{p}_1^{f_1}\cdots\mathfrak{p}_t^{f_t}\mathfrak{q}_1\cdots\mathfrak{q}_s$. 由素理想分解的唯一性可知 $\{\mathfrak{q}_1,\cdots,\mathfrak{q}_s\}\subseteq\{\mathfrak{p}_1,\cdots,\mathfrak{p}_t\}$，进而有 $e_i\geqslant f_i$，$i=1,\cdots,t$. 反之，若 $e_i\geqslant f_i$，$i=1,\cdots,t$，则显然有 $I\subseteq J$.

(2) 因 $I+J$ 是 R 的包含 I 和 J 的最小理想，由(1)立得(2).

(3) 因 $I\cap J$ 是 R 的包含于 I 和 J 之中的最大理想，由(1)立得(3).

(4) 显然. □

命题 4.1.4 设 I 是 Dedekind 整环 R 的非零理想，则 R/I 只有有限个理想，且均是主理想.

证明 由命题4.1.3的(1)可知，R/I 只有有限个理想. 设 $I=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$，其中 $\mathfrak{p}_i$ 是互不相同的素理想，$e_i\geqslant 1$. 若 J 是 R 的理想，且 $J\supseteq I$，则 $J=\mathfrak{p}_1^{f_1}\cdots\mathfrak{p}_t^{f_t}$，其中 $0\leqslant f_i\leqslant e_i$，$i=1,\cdots,t$. 要证

J/I 是 R/I 的主理想. 只需证每个 $\mathfrak{p}_i/I$ 是 R/I 的主理想.

取 $x\in\mathfrak{p}_1\backslash\mathfrak{p}_1^2$. 由于 $\mathfrak{p}_1^2,\mathfrak{p}_2,\cdots,\mathfrak{p}_t$ 两两互素, 据中国剩余定理, 存在 $y\in R$ 使得

$$y\equiv x(\bmod\ \mathfrak{p}_1^2),\ 且\ y\equiv 1(\bmod\ \mathfrak{p}_i),\ i=2,\cdots,t.$$

于是 $y\in\mathfrak{p}_1\backslash\mathfrak{p}_1^2$, 但 $y\notin\mathfrak{p}_i$, $i=2,\cdots,t$. 设 $\mathfrak{m}$ 是 R 的包含 $yR+I$ 的极大理想. 由 $I=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}\subseteq\mathfrak{m}$ 可知, 存在某个 $\mathfrak{p}_j\subseteq\mathfrak{m}$. 由于 $\mathfrak{p}_j$ 是极大理想, 故 $\mathfrak{m}=\mathfrak{p}_j$. 但当 $j\neq 1$ 时, $y\notin\mathfrak{p}_j$, 所以 $\mathfrak{m}=\mathfrak{p}_1$. 这表明 $\mathfrak{p}_1$ 是 R 的包含 $yR+I$ 的唯一极大理想. 由命题 4.1.3, 可设 $yR+I=\mathfrak{p}_1^r$, $r\geqslant 1$. 因 $y\notin\mathfrak{p}_1^2$, 故 $yR+I=\mathfrak{p}_1$, 从而 $\mathfrak{p}_1/I$ 是 R/I 的主理想. □

推论 4.1.5 *设 I 是 Dedekind 整环 R 的非零理想, 则对于任意 $a\in I\backslash\{0\}$, 存在 $b\in I$, 使得 $I=aR+bR$.*

证明 由命题 4.1.4, R/aR 是主理想环, 从而存在 $b\in I$, 使得 $I/aR=(aR+bR)/aR$. 所以 $I=aR+bR$. □

4.1.2 理想类群

设 R 是 Dedekind 整环, 用 R-模同构关系对 R 的非零理想分类, 非零理想 I 所在的 R-模同构类记作 $[I]$, 叫做 I 所在的**理想类**. 且记

$$\mathrm{Cl}(R)=\{[I]\mid I\ 是\ R\ 的非零理想\}.$$

由命题 4.1.1 的(1)和(2)可知, $\mathrm{Cl}(R)$关于乘法

$$[I][J]=[IJ];\ [I],[J]\in\mathrm{Cl}(R)$$

构成一个乘法 Abel 群, 称为 R 的**理想类群**. $\mathrm{Cl}(R)$的单位元为 $[R]$, 是 R 的所有非零主理想构成的理想类. 这样, 一个 Dedekind 整环 R 是主理想整环当且仅当其理想类群 $\mathrm{Cl}(R)$是平凡群.

4.1.3 Dedekind 整环上的有限生成模

首先讨论 Dedekind 整环上有限生成无扭模的结构.

命题 4.1.6 设 R 是 Dedekind 整环，I 和 J 是 R 的非零理想. 则

(1) 存在 R 的理想 $J'\simeq J$ 且 $J'+I=R$.

(2) $I\oplus J\simeq R\oplus IJ$ (R-模同构).

证明 (1) 由命题 4.1.1 的(1)，存在 R 的理想 K 和 $x\in R\backslash\{0\}$，使得 $JK=xR$. 据命题 4.1.4，K/KI 是 R/KI 的主理想，从而存在 $y\in R\backslash\{0\}$ 使得 $K=yR+KI$. 于是 $xR=JK=yJ+JKI=yJ+xI$. 因 $yJ\subseteq xR$，存在 R 的理想 J' 使得 $yJ=xRJ'=xJ'$. 据命题 4.1.1 的(2)，$J\simeq J'$. 并且 $xR=xI+xJ'=x(I+J')$，从而 $R=I+J'$.

(2) 当 I 与 J 互素，即 $I+J=R$ 时，映射 $f:I\oplus J\to R$; $(a,b)\mapsto a+b$ 是 R-模满同态，且 $\mathrm{Ker}\,f=\{(a,-a)\mid a\in I\cap J\}\simeq I\cap J$. 由定理 2.3.1，$I\oplus J\simeq R\oplus(I\cap J)$. 因 $I+J=R$，$I\cap J=IJ$ (习题 1.1.1 的(1)). 所以 $I\oplus J\simeq R\oplus IJ$.

对于一般情形，由(1)，存在 R 的理想 $J'\simeq J$，使得 $I+J'=R$，于是 $I\oplus J\simeq I\oplus J'\simeq R\oplus IJ'\simeq R\oplus IJ$ (命题 4.1.1 的(2)). □

推论 4.1.7 Dedekind 整环 R 的理想均是有限生成投射 R-模.

证明 设 I 是 R 的理想，不妨设 $I\neq 0$. 由命题 4.1.1 的(1)，存在 R 的理想 J 使得 $IJ=aR$，$a\in R\backslash\{0\}$. 由命题 4.1.6，$I\oplus J\simeq R\oplus aR\simeq R\oplus R$. 所以 I 是投射的. 再由推论 4.1.5，I 是有限生成的. □

命题 4.1.8 设 R 是整环，M 是有限生成无扭 R-模. 则 M 同构于某个有限秩的自由 R-模的子模.

证明 设 M 由 $X=\{x_1,\cdots,x_n\}$ 生成，不妨设 $\{x_1,\cdots,x_r\}$ 是 X 中的一个极大 R-线性无关组. 则对于每个 $j\geqslant r+1$，$\{x_1,\cdots,x_r,x_j\}$ 是 R-线性相关的，故存在不全为零的 $a_{1j},\cdots,a_{rj},d_j\in R$，使得 $a_{1j}x_1+\cdots+a_{rj}x_r+d_jx_j=0$. 因 $\{x_1,\cdots,x_r\}$ 是 R-线性无关

的，故 $d_j \neq 0$. 令 $d = d_{r+1} \cdots d_n$，则 $M \simeq dM \subseteq Rx_1 \oplus \cdots \oplus Rx_r \simeq R^r$. □

命题 4.1.9 设 R 是 Dedekind 整环，M 是有限生成 R-模. 则下列条件等价：

(1) M 是无扭 R-模；

(2) M 同构于某个有限秩的自由 R-模的子模；

(3) M 同构于 R 中有限个理想的直和；

(4) M 是投射 R-模.

证明 (1)⇒(2)：由命题 4.1.8 立得.

(2)⇒(3)：设 M 是秩为 r 的自由 R-模 F 的子模. 对秩 r 进行归纳. 当 $r=0$ 时，显然(3)成立. 当 $r \geqslant 1$ 时，设 $\{x_1, \cdots, x_r\}$ 是 F 的基. 令

$$p: M \to R;\ a_1x_1 + \cdots + a_rx_r \mapsto a_r.$$

这是一个 R-同态，$I = \operatorname{Im} p$ 是 R 的理想. 据推论 4.1.7，I 是投射的. 再由定理 2.3.1，$M \simeq I \oplus \operatorname{Ker} p$. 由于 $\operatorname{Ker} p \subseteq Rx_1 \oplus \cdots \oplus Rx_{r-1}$，对 $\operatorname{Ker} p$ 用归纳假定即得(3).

(3)⇒(4)：由推论 4.1.7 和命题 2.3.2 立得.

(4)⇒(1)：由 R 是整环即得. □

由上述命题可知，Dedekind 整环 R 上的有限生成无扭模均同构于一个有限秩的自由 R-模 R^m 与 R 的一个理想 I 的直和.

命题 4.1.10 设 R 是 Dedekind 整环，I 和 J 是 R 的非零理想. 若 $R^m \oplus I \simeq R^n \oplus J$，则 $m = n$，且 $I \simeq J$.

证明 设 $S = R \backslash \{0\}$. 因 $I, J \neq 0$，$S^{-1}I = S^{-1}J = S^{-1}R$ 就是 R 的分式域 F. 若 $R^m \oplus I \simeq R^n \oplus J$，据命题 2.5.9，$F^{m+1} \simeq S^{-1}(R^m \oplus I) \simeq S^{-1}(R^n \oplus J) \simeq F^{n+1}$. 所以 $m = n$. 设 $f: R^n \oplus I \to R^n \oplus J$ 是 R-同构，则 $S^{-1}f$: $F^{n+1} = S^{-1}(R^n \oplus I) \to F^{n+1} = S^{-1}(R^n \oplus J)$是 F 上的线性空间的线性映射，它在 F^{n+1}的标准基下所对应的矩阵 A 是一个 F 上的可逆方阵，并且 $S^{-1}f$ 在 $R^n \oplus I$

上的限制就是 f. 于是, 对于每个 $a\in I$, 均有

$$\begin{pmatrix}1&&&\\&\ddots&&\\&&1&\\&&&a\end{pmatrix}A=\begin{pmatrix}s_{11}&\cdots&s_{1n}&b_1\\\vdots&&\vdots&\vdots\\s_{n+1\,1}&\cdots&s_{n+1\,n}&b_{n+1}\end{pmatrix},$$

其中 $s_{ij}\in R$, $b_i\in J$. 上式两边取行列式, 得 $a\cdot\det A\in J$, 从而 $(\det A)I\subseteq J$. 同样地, 由 R-同构f^{-1}可得$(\det A^{-1})J\subseteq I$, 于是, $J=(\det A)(\det A^{-1})J\subseteq(\det A)I\subseteq J$, 所以 $J=(\det A)I$. 而 $\det A\neq 0$, 所以 $I\simeq J$. □

这样, Dedekind 整环 R 上的有限生成无扭模的同构分类问题就归于R 的理想的同构分类, 因而与 R 的理想类群 $\mathrm{Cl}(R)$直接相关.

命题 4.1.11 设 R 是 Dedekind 整环, M 是有限生成R-模, $\mathrm{T}(M)$是 M 的扭子模, 则存在 M 的无扭子模N, 使得 $M=N\oplus\mathrm{T}(M)$.

证明 据命题 1.2.3, $M/\mathrm{T}(M)$是有限生成无扭 R-模, 再由命题 4.1.9 可知 $M/\mathrm{T}(M)$是投射的. 于是正合列 $0\to\mathrm{T}(M)\to M\to M/\mathrm{T}(M)\to 0$ 是可裂的, 所以存在 M 的子模$N\simeq M/\mathrm{T}(M)$是无扭的, 使得 $M=N\oplus\mathrm{T}(M)$. □

命题 4.1.12 设 S 是 Dedekind 整环 R 的乘法集, 则 $S^{-1}R$ 也是 Dedekind 整环.

证明 设J_1,J_2 是 $S^{-1}R$ 的理想, 且 $J_1\subseteq J_2$. 则 $I_i=J_i\cap R$, $i=1,2$, 是 R 的理想, 并且 $I_1\subseteq I_2$. 于是存在 R 的理想K, 使得 $I_1=I_2K$. 据命题 2.5.3, $J_1=S^{-1}I_1=S^{-1}(I_2K)=(S^{-1}I_2)(S^{-1}K)=J_2(S^{-1}K)$(习题 2.5.1 的(2)), 其中 $S^{-1}K$ 是$S^{-1}R$ 的理想. 所以 $S^{-1}R$ 是 Dedekind 整环. □

最后讨论 Dedekind 整环上的有限生成扭模的结构. 先证一个重要引理.

引理 4.1.13 只有有限个素理想的 Dedekind 整环 R 必是主

理想整环.

证明 设 $\mathfrak{p}_1,\cdots,\mathfrak{p}_n$ 是 R 的所有非零素理想, I 是 R 的任一非零理想. 则 I 可表示成 $I=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_n^{e_n}$, $e_i\geqslant 0$. 取 $a_i\in I\mathfrak{p}_1\cdots\mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\cdots\mathfrak{p}_n\backslash I\mathfrak{p}_1\cdots\mathfrak{p}_n$, $i=1,\cdots,n$. 令 $a=a_1+\cdots+a_n$, 则 $a\in\mathfrak{p}_i^{e_i}\backslash\mathfrak{p}_i^{e_i+1}$, $i=1,\cdots,n$. 由于 $aR\subseteq I$, 可设 $aR=\mathfrak{p}_1^{f_1}\cdots\mathfrak{p}_n^{f_n}$, 其中 $f_i\geqslant e_i\geqslant 0$. 又因 $aR\not\subseteq\mathfrak{p}_i^{e_i+1}$, 所以 $f_i=e_i$, $i=1,\cdots,n$, 故 $I=aR$. □

定理 4.1.14 设 R 是 Dedekind 整环, M 是有限生成扭 R-模, $M\neq 0$. 则存在 R 的 m 个理想 $I_1,\cdots,I_m$, $R\neq I_1\supseteq I_2\supseteq\cdots\supseteq I_m\neq 0$, 使得

$$M\simeq R/I_1\oplus\cdots\oplus R/I_m,$$

并且 m 和 $I_1,\cdots,I_m$ 由 M 唯一确定.

证明 设 M 由非零元 $u_1,\cdots,u_n$ 生成, $n\geqslant 1$. 则 $\mathrm{Ann}_R(u_i)$ 不是 0 和 R. 记 $A=\mathrm{Ann}_R(M)$, 则 $A=\bigcap\limits_{i=1}^{n}\mathrm{Ann}_R(u_i)$不是 0 和 R.

设 $\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ 是 A 的所有两两互素的素理想因子, 则 $r\geqslant 1$. 令 $S=R\backslash(\bigcup\limits_{i=1}^{r}\mathfrak{p}_i)=\bigcap\limits_{i=1}^{r}(R\backslash\mathfrak{p}_i)$, 则 S 是R 的乘法集(习题2.5.6), 且 $S\cap\mathfrak{p}_i=\varnothing$. 但对于 R 中其他的非零素理想 $\mathfrak{p}$, 均有 $\mathfrak{p}\cap S\neq\varnothing$. 这是因为, 由于 $\mathfrak{p},\mathfrak{p}_1,\cdots,\mathfrak{p}_r$ 两两互素, 据中国剩余定理, 存在 $x\in R$, 使得 $x\equiv 0(\mathrm{mod}\,\mathfrak{p})$且 $x\equiv 1(\mathrm{mod}\,\mathfrak{p}_i)$, $i=1,\cdots,r$. 于是 $x\in\mathfrak{p}\cap S$.

记 $R_S=S^{-1}R$. 据命题 2.5.3, R_S 只有有限个素理想 $\mathfrak{p}_1R_S$, $\cdots,\mathfrak{p}_rR_S$. 又由命题 4.1.12, R_S 也是 Dedekind 整环. 再由引理 4.1.13 可知, R_S 是主理想整环. 记 $M_S=S^{-1}M$, 则 M_S 是有限生成扭 R_S-模. 据定理 2.6.2, 存在 R_S 的 m 个理想 $J_1,\cdots,J_m$, $R_S\neq J_1\supseteq J_2\supseteq\cdots\supseteq J_m\neq 0$, 使得 $M_S\simeq R_S/J_1\oplus\cdots\oplus R_S/J_m$. 记 $A_S=S^{-1}A$, 由命题 2.5.11 可知, $A_S=\mathrm{Ann}_{R_S}(M_S)=J_m$.

令 $I_i=J_i\cap R$, 这是 R 的理想. 据命题 2.5.3, $R\neq I_1\supseteq\cdots$

$\supseteq I_m \neq 0$，并且 $S^{-1}I_i = J_i$，$i=1,\cdots,m$. 特别地，$I_m = J_m \cap R = A_S \cap R = A$. 对于每个 $a \in S$，aR 与 A 互素，从而 $\bar{a} = a + A$ 是 R/A 的单位，因此有 R-模同构 $(R/A)_S = S^{-1}(R/A) \simeq R/A$. 于是，由命题 2.4.5，有 R-模同构

$$\begin{aligned}R/I_i &\simeq (R/I_i)/(A(R/I_i)) \simeq (R/I_i) \bigotimes_R (R/A)\\ &\simeq (R/I_i) \bigotimes_R (R/A)_S \simeq (R/I_i) \bigotimes_R (R_S \bigotimes_R (R/A))\\ &\simeq ((R/I_i) \bigotimes_R R_S) \bigotimes_R (R/A) \simeq (R/I_i)_S \bigotimes_R (R/A)\\ &\simeq (R_S/S^{-1}I_i) \bigotimes_R (R/A) \simeq (R_S/J_i) \bigotimes_R (R/A),\\ &i = 1,\cdots,m.\end{aligned}$$

从而有 R-模同构

$$\begin{aligned}M &\simeq M/AM \simeq M \bigotimes_R (R/A) \simeq M \bigotimes_R (R/A)_S\\ &\simeq M \bigotimes_R (R_S \bigotimes_R (R/A)) \simeq (M \bigotimes_R R_S) \bigotimes_R (R/A)\\ &\simeq M_S \bigotimes_R (R/A) \simeq (\bigoplus_{i=1}^{m} R_S/J_i) \bigotimes_R (R/A)\\ &\simeq \bigoplus_{i=1}^{m} ((R_S/J_i) \bigotimes_R (R/A)) \simeq \bigoplus_{i=1}^{m} (R/I_i).\end{aligned}$$

据定理 2.6.2，m 和 $J_1,\cdots,J_m$ 由 M_S 唯一确定，从而由 M 和 $A = \mathrm{Ann}_R(M)$ 唯一确定. 于是 m 和 $I_i = J_i \cap R$ 也由 M 唯一确定. □

习　题　4.1

1. 证明：$\mathbb{Z}[\sqrt{-1}]$ 是主理想整环；$\mathbb{Z}[\sqrt{-5}]$ 是 Dedekind 整环，但不是主理想整环.

2. 证明：Dedekind 整环的准素理想均是素理想的幂.

3. 证明：若 Dedekind 整环 R 是单一因子分解整环，则 R 是主理想整环.

4. 证明：Dedekind 整环 R 上的自由模的子模均同构于 R 的理想的直和(提示：用良序化原理)，从而 Dedekind 整环上的投射

模的子模仍是投射的.

5. 证明：一个整环 R 是 Dedekind 整环 $\Leftrightarrow$ 每个可除 R-模是内射的.

4.2 分式理想

设 R 是整环，F 是 R 的分式域. F 中的非零 R-子模 M 称为 R 的**分式理想**，如果存在 $a\in R\backslash\{0\}$，使得 $aM\subseteq R$. R 的非零理想均是分式理想，为区别起见，R 的非零理想称为**整理想**. F 中的形如 xR，$x\in F\backslash\{0\}$，的分式理想称为 R 的**主分式理想**.

引理 4.2.1 设 F 是整环 R 的分式域，M 是 F 的非零 R-子模，则下列条件等价：

(1) M 是 R 的分式理想；

(2) 存在 $b\in F\backslash\{0\}$，使得 $M\subseteq bR$；

(3) 存在 $c\in F\backslash\{0\}$ 和 R 的整理想 I，使得 $M=cI$.

证明 (1)$\Rightarrow$(2)：若 $aM\subseteq R$，$a\in R\backslash\{0\}$，令 $b=a^{-1}$，则 $M\subseteq bR$.

(2)$\Rightarrow$(3)：令 $I=b^{-1}M\subseteq R$，则 I 是 R 的整理想. 取 $c=b$，则 $cI=M$.

(3)$\Rightarrow$(1)：设 $c=b/a$；$a,b\in R\backslash\{0\}$. 则 $aM=bI\subseteq R$，所以 M 是 R 的分式理想. □

设 M,N 是整环 R 的分式域 F 的 R-子模. 定义 M 与 N 的乘积为

$$MN=\{\sum_{i=1}^{k}m_in_i\in F\mid m_i\in M,\ n_i\in N,\ k\geqslant 1\},$$

这仍是 F 的 R-子模. 并且，当 M 和 N 是 R 的分式理想时，由引理 4.2.1，MN 仍是 R 的分式理想. F 的 R-子模 M 称为是**可逆**的，如果存在 F 的 R-子模 N 使得 $MN=R$，且称 N(是唯一的)为 M 的**逆**，记作 M^{-1}.

命题 4.2.2 设 F 是整环 R 的分式域，M 是 F 中的非零 R-子模. 则 M 是可逆的当且仅当 M 是有限生成投射 R-模；此时，M 是 R 的分式理想.

证明 设 F 的 R-子模 N 使得 $MN=R$. 则 1 可表成 $1=\sum_{i=1}^{t} m_in_i$；$m_i\in M$，$n_i\in N$. 令

$$\varphi:R^t\to M;\ (x_1,\cdots,x_t)\mapsto x_1m_1+\cdots+x_tm_t,$$

$$\psi:M\to R^t;\ m\mapsto(mn_1,\cdots,mn_t).$$

不难验证：φ 和 ψ 是 R-同态，且 $\varphi\psi=1_M$. 据定理 2.1.3 和定理 2.3.1，M 是有限生成投射 R-模.

若 M 是由有限子集 X 生成的投射 R-模，取 X 中元素的公分母 $a\in R\setminus\{0\}$，则 $aM\subseteq R$，所以 M 是 R 的分式理想. 据定理 2.3.1，存在 R-同态 $\varphi:R^t\to M$ 和 $\psi:M\to R^t$，使得 $\varphi\psi=1_M$. 记 $e_1=(1,0,\cdots,0)$，$\cdots$，$e_t=(0,\cdots,0,1)\in R^t$；$\varphi(e_i)=m_i$. 且设 $\pi_i:R^t\to R$ 是对第 i 分量的标准投影，则 $\psi_i=\pi_i\psi$ 是 M 到 R 的 R-同态. 若 $m=s/t$，$m'=s'/t$，其中 $s,s',t\in R$，则

$$m\psi_i(m')=\frac{s}{t}\psi_i\left(\frac{s'}{t}\right)=\frac{1}{t}\psi_i\left(\frac{ss'}{t}\right)$$

$$=\frac{s'}{t}\psi_i\left(\frac{s}{t}\right)=m'\psi_i(m).$$

取定一个 $m_0\in M\setminus\{0\}$. 令 N 是由 $n_i=m_0^{-1}\psi_i(m_0)$，$i=1,\cdots,t$，生成的 F 的 R-子模. 则对于任意 $m\in M$，均有 $mn_i=mm_0^{-1}\psi_i(m_0)=m_0^{-1}m_0\psi_i(m)=\psi_i(m)\in R$，$i=1,\cdots,t$. 所以 $MN\subseteq R$. 又由于 $1=m_0^{-1}m_0=m_0^{-1}\varphi\psi(m_0)=\sum_{i=1}^{t}m_0^{-1}\psi_i(m_0)m_i=\sum_{i=1}^{t}m_in_i\in MN$，所以 $MN=R$，即 M 是可逆的. □

定理 4.2.3 设 R 是整环，则下列条件等价：

(1) R 是 Dedekind 整环；

(2) R 的每个分式理想均是可逆的；

(3) R 的每个整理想均是可逆的；

(4) R 的每个分式理想均是有限生成投射 R-模；

(5) R 的每个整理想均是有限生成投射 R-模；

(6) R 的每个整理想可表示成有限个素理想之积.

证明 (1)⇒(2)：设 M 是 R 的分式理想，据引理 4.2.1，$M = bI$，其中 $b \in F\backslash\{0\}$，F 是 R 的分式域，I 是 R 的整理想. 又由命题 4.1.1 的(1)，存在 R 的整理想 J，使得 $IJ = aR$，$a \in R\backslash\{0\}$. 令 $N = a^{-1}b^{-1}J$，则 $MN = R$，所以 M 是可逆的.

(2)⇒(1)：不妨设 I 和 J 是 R 的整理想，且 $I \subseteq J$. 则 $J^{-1}I \subseteq R$，从而 $J^{-1}I$ 是 R 的整理想. 于是，$I = J(J^{-1}I)$，所以 R 是 Dedekind 整环.

(2)⇔(4)：由命题 4.2.2 立得.

(2)⇔(3)和(4)⇔(5)：由引理 4.2.1 可得.

(1)⇒(6)：由命题 4.1.2 可得.

(6)⇒(3)：只需证 R 的每个非零素理想 $\mathfrak{p}$ 均是可逆的. 取 $c \in \mathfrak{p}\backslash\{0\}$，且设 $cR = \mathfrak{p}_1\cdots\mathfrak{p}_t$，$\mathfrak{p}_i$ 均是 R 的素理想. 由于 cR 是可逆的(有逆 $c^{-1}R$)，从而 $\mathfrak{p}_i$ 均是可逆的. 又由 $cR = \mathfrak{p}_1\cdots\mathfrak{p}_t \subseteq \mathfrak{p}$ 可知，存在某个 $\mathfrak{p}_j \subseteq \mathfrak{p}$. 下面要证 R 的每个可逆素理想均是极大的，于是 $\mathfrak{p} = \mathfrak{p}_j$ 是可逆的.

假定 R 的可逆素理想 $\mathfrak{p}$ 不是极大的，则 $\mathfrak{p}$ 真包含于 R 的某个极大理想 M 之中. 取 $a \in M\backslash\mathfrak{p}$，由条件(6)，$\mathfrak{p} + aR$ 和 $\mathfrak{p} + a^2R$ 均可表示成 R 的素理想之积：

$$(*) \qquad \mathfrak{p} + aR = \mathfrak{p}_1\cdots\mathfrak{p}_m, \quad \mathfrak{p} + a^2R = \mathfrak{q}_1\cdots\mathfrak{q}_n,$$

其中素理想 $\mathfrak{p}_i$ 和 $\mathfrak{q}_j$ 均真包含 $\mathfrak{p}$. 于是，在整环 $\overline{R} = R/\mathfrak{p}$ 中，$\overline{a}\overline{R} = \overline{\mathfrak{p}}_1\cdots\overline{\mathfrak{p}}_m$，$\overline{a}^2\overline{R} = \overline{\mathfrak{q}}_1\cdots\overline{\mathfrak{q}}_n$，其中 $\overline{\mathfrak{p}}_i = \mathfrak{p}_i/\mathfrak{p}$，$\overline{\mathfrak{q}}_j = \mathfrak{q}_j/\mathfrak{p}$ 均是 $\overline{R}$ 的素理想，且 $\overline{a} = a + \mathfrak{p} \in \overline{R}$. 由于 $\overline{a}\overline{R}$ 和 $\overline{a}^2\overline{R}$ 是 $\overline{R}$ 的可逆理想，故 $\overline{\mathfrak{p}}_i$ 和

$\bar{\mathfrak{q}}_j$ 均是$\bar{R}$ 的可逆整理想. 并且, 由$(\bar{a}\bar{R})^2=\bar{a}^2\bar{R}$ 可得

$$(**)\qquad \bar{\mathfrak{p}}_1^2\cdots\bar{\mathfrak{p}}_m^2=\bar{\mathfrak{q}}_1\cdots\bar{\mathfrak{q}}_n.$$

取$\{\bar{\mathfrak{p}}_1,\cdots,\bar{\mathfrak{p}}_m\}$中关于包含关系的极小元, 不妨设是$\bar{\mathfrak{p}}_1$. 由于$\bar{\mathfrak{p}}_1\supseteq\bar{\mathfrak{q}}_1\cdots\bar{\mathfrak{q}}_n$, 故$\bar{\mathfrak{p}}_1$ 包含某个$\bar{\mathfrak{q}}_j$, 不妨设$\bar{\mathfrak{p}}_1\supseteq\bar{\mathfrak{q}}_1$. 又因为$\bar{\mathfrak{q}}_1\supseteq\bar{\mathfrak{p}}_1^2\cdots\bar{\mathfrak{p}}_m^2$, 从而$\bar{\mathfrak{q}}_1$ 包含某个$\bar{\mathfrak{p}}_j$, 于是$\bar{\mathfrak{p}}_1\supseteq\bar{\mathfrak{q}}_1\supseteq\bar{\mathfrak{p}}_j$. 由$\bar{\mathfrak{p}}_1$ 的极小性得$\bar{\mathfrak{p}}_1=\bar{\mathfrak{p}}_j$, 所以$\bar{\mathfrak{p}}_1=\bar{\mathfrak{q}}_1$. 由于$\bar{\mathfrak{p}}_1$ 是可逆的, 从(**)式的两边消去$\bar{\mathfrak{p}}_1$, 然后如此进行下去, 可得$2m=n$, 且适当变换$\bar{\mathfrak{q}}_j$ 的下标后有$\bar{\mathfrak{p}}_i=\bar{\mathfrak{q}}_{2i-1}=\bar{\mathfrak{q}}_{2i}$, $i=1,\cdots,m$. 回到R 中去, 有$\mathfrak{p}_i=\mathfrak{q}_{2i-1}=\mathfrak{q}_{2i}$, $i=1,\cdots,m$. 再由(*)式得$(\mathfrak{p}+aR)^2=\mathfrak{p}+a^2R$, 从而$\mathfrak{p}\subseteq(\mathfrak{p}+aR)^2\subseteq\mathfrak{p}^2+aR$. 若$b\in\mathfrak{p}$, 则$b=s+at$, $s\in\mathfrak{p}^2$, $t\in R$, 于是$at=b-s\in\mathfrak{p}$. 由于$a\in M\backslash\mathfrak{p}$, 故$t\in\mathfrak{p}$, 从而$b\in\mathfrak{p}^2+a\mathfrak{p}$. 因此$\mathfrak{p}\subseteq\mathfrak{p}^2+a\mathfrak{p}$. 而反包含是显然的, 所以$\mathfrak{p}=\mathfrak{p}^2+a\mathfrak{p}$. 由于$\mathfrak{p}$ 是可逆的, $R=\mathfrak{p}\mathfrak{p}^{-1}=\mathfrak{p}^2\mathfrak{p}^{-1}+a\mathfrak{p}\mathfrak{p}^{-1}=\mathfrak{p}+aR\subseteq M$, 这与$M$ 是极大理想矛盾. 所以$\mathfrak{p}$ 是极大的. □

命题 4.2.4 设R 是 Dedekind 整环, M 是R 的分式理想. 则

(1) M 可唯一地表示成$M=IJ^{-1}$, 其中I 和J 是R 的互素的整理想.

(2) M 可唯一地表示成$M=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$, 其中$\mathfrak{p}_1,\cdots,\mathfrak{p}_t$ 是R 的互不相同的素理想, $e_i\in\mathbb{Z}\backslash\{0\}$, $i=1,\cdots,t$.

证明 (1) 由引理 4.2.1, 存在$a\in R\backslash\{0\}$, 使得$aM=L$ 是R 的整理想, 记$L+aR=K$. 可设$L=KI$, $aR=KJ$, 其中I 和J 是R 的整理想. 则$KI+KJ=K$, 从而$I+J=R$, 并且$KJM=aM=L=KI$, 所以$M=IJ^{-1}$. 又若$M=I_1J_1^{-1}$, 其中I_1 和J_1 是R 的互素的整理想, 则$IJ_1=I_1J$. 于是$I=I(I_1+J_1)=II_1+IJ_1=II_1+I_1J=I_1(I+J)=I_1$, 进而有$J=J_1$.

(2) 由(1)和命题 4.1.2 立得. □

设R 是 Dedekind 整环, 由于R 的每个分式理想均可逆, R

的所有分式理想构成一个乘法群，记作 $\mathscr{F}(R)$. 由命题 4.2.4 和定理 4.2.3 可知，$\mathscr{F}(R)$是以 R 的所有非零素理想为基的自由 Abel 群. 记 R 的所有主分式理想构成的 $\mathscr{F}(R)$的子群为 $\mathscr{P}(R)$，由于 R 的每个分式理想均R-同构于R 的一个整理想，且 R 的两个分式理想 R-同构当且仅当它们相差一个主分式理想因子，所以有群同构 $\mathscr{F}(R)/\mathscr{P}(R)\simeq \mathrm{Cl}(R)$，即有 Abel 群正合列

$$0\to\mathscr{P}(R)\to\mathscr{F}(R)\to\mathrm{Cl}(R)\to 0.$$

设 K 是R 的分式域，K^*是 K 的非零元构成的乘法群，则有群的满同态 $\varphi:K^*\to\mathscr{P}(R)$; $a\mapsto aR$, 其核 $\mathrm{Ker}\varphi=\mathrm{U}(R)$是 R 的单位群，于是有 Abel 群正合列

$$0\to\mathrm{U}(R)\to K^*\to\mathscr{P}(R)\to 0.$$

下面介绍域的离散赋值及其离散赋值环，并用以刻画 Dedekind 整环.

设 F 是域. 记 F^*是 F 的非零元作成的乘法群. F 的一个**离散赋值** v 是从F^*到整数加群 $\mathbb{Z}$ 的一个满同态 v: $F^*\to\mathbb{Z}$，且满足条件

$$v(x+y)\geqslant\min\{v(x),v(y)\};\ x,y\in F^*.$$

例 设 p 是素数. 若 $x\in\mathbb{Q}^*$，则 x 可唯一地表成$x=p^na/b$，其中 $a,b,n\in\mathbb{Z}$，且 $p\nmid ab$. 令 $v_p(x)=n$. 容易验证，映射

$$v_p:\ \mathbb{Q}^*\to\mathbb{Z};\ x\mapsto v_p(x)$$

是 $\mathbb{Q}$ 的一个离散赋值，叫做 $\mathbb{Q}$ 的 **p-adic 赋值**.

命题 4.2.5 *设 v 是域F 的离散赋值. 令*

$$R=\{x\in F^*\mid v(x)\geqslant 0\}\cup\{0\}.$$

则

(1) R 是F 的子环，有唯一的极大理想

$$P=\{x\in F^*\mid v(x)>0\}\cup\{0\},$$

从而是局部环.

(2) R 是主理想整环.

证明 (1) 设 $x,y\in R$. 当 $xy=0$ 时，显然有 $x+y$, $xy\in R$.

当 $xy\neq0$ 时，由于 $v(x+y)\geqslant\min\{v(x),v(y)\}\geqslant0$，$v(xy)=v(x)+v(y)\geqslant0$，所以 $x+y$，$xy\in R$. 又由 v 是同态可知 $v(1)=0$，从而 $1\in R$. 所以 R 是 F 的子环. 类似地可证，P 是 R 的理想.

若 x 是 R 的单位，则 $x^{-1}\in R$，从而 $v(x)$，$v(x^{-1})\geqslant0$. 又因 $v(x)+v(x^{-1})=v(xx^{-1})=v(1)=0$，所以 $v(x)=0$. 另一方面，若 $x\in R$ 且 $v(x)=0$，则 $v(x^{-1})=-v(x)=0$，从而 $x^{-1}\in R$. 这证明了

$$\mathrm{U}(R)=\{x\in F^*\mid v(x)=0\}.$$

又由于 $R\backslash P=\mathrm{U}(R)$，据定理 1.1.6，$R$ 是局部环，且 P 是 R 的唯一极大理想.

(2) 设 I 是 R 的非零理想. 令 $m=\min\{v(x)\mid x\in I\backslash\{0\}\}$，且设 $a\in I$ 使得 $v(a)=m$. 若 $x\in I$，则 $v(x/a)=v(x)-v(a)\geqslant0$. 于是 $x/a\in R$，从而 $x\in Ra\subseteq I$. 所以 $I=Ra$. □

整环 R 称为**离散赋值环**，如果存在 R 的分式域 F 的离散赋值 $v:F^*\to\mathbb{Z}$，使得 $R=\{x\in F^*\mid v(x)\geqslant0\}\cup\{0\}$. 容易验证，命题 4.2.5 中的域 F 是子环 R 的分式域，从而 R 就是一个离散赋值环，也称为离散赋值 v 的离散赋值环.

设 R 是 Dedekind 整环，F 是 R 的分式域，$\mathfrak{p}$ 是 R 的非零素理想. 且设 $x,y\in F^*$. 由命题 4.2.4，R 的主分式理想 Rx 和 Ry 可表示成

$$Rx=\mathfrak{p}^e\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t},\quad Ry=\mathfrak{p}^f\mathfrak{p}_1^{f_1}\cdots\mathfrak{p}_t^{f_t},$$

其中 $\mathfrak{p},\mathfrak{p}_1,\cdots,\mathfrak{p}_t$ 是 R 的互不相同的非零素理想；$e,e_i,f,f_i\in\mathbb{Z}$；并且 e 和 f 分别由 Rx 和 Ry 唯一确定. 定义 $v_{\mathfrak{p}}(x)=e$，$v_{\mathfrak{p}}(y)=f$. 于是 $Rxy=\mathfrak{p}^{e+f}\prod_{i=1}^{t}\mathfrak{p}_i^{e_i+f_i}$，且 $R(x+y)\subseteq Rx+Ry=\mathfrak{p}^{\min\{e,f\}}\prod_{i=1}^{t}\mathfrak{p}^{\min\{e_i,f_i\}}$（习题 4.2.1）. 所以 $v_{\mathfrak{p}}(xy)=v_{\mathfrak{p}}(x)+v_{\mathfrak{p}}(y)$，且 $v_{\mathfrak{p}}(x+y)\geqslant\min\{v_{\mathfrak{p}}(x),v_{\mathfrak{p}}(y)\}$. 这样，映射

$$v_{\mathfrak{p}}: F^{*} \to \mathbb{Z};\ x \mapsto v_{\mathfrak{p}}(x)$$

是 F 的一个离散赋值，叫做 F(或 R)的 $\mathfrak{p}$-**adic 赋值**.

命题 4.2.6　设 R 是 Dedekind 整环，F 是 R 的分式域，$\mathfrak{p}$ 是 R 的非零素理想. 则 F 关于 $\mathfrak{p}$-adic 赋值 $v_{\mathfrak{p}}$ 的离散赋值环就是 R 在 $\mathfrak{p}$ 处的局部化 $R_{\mathfrak{p}}$(这里视 $R_{\mathfrak{p}}$ 为 F 的子环).

证明　记 F 关于 $v_{\mathfrak{p}}$ 的离散赋值环为 T. 设 $x \in T \backslash R$, $Rx = IJ^{-1}$，其中 I 和 J 是 R 的互素的整理想(命题 4.2.4)，则 $Jx = I$. 取 $b \in J \backslash \{0\}$. 由 $v_{\mathfrak{p}}(x) \geqslant 0$ 可知 J 与 $\mathfrak{p}$ 互素，从而 $b \notin \mathfrak{p}$. 设 $bx = a \in I$，则 $x = a/b \in R_{\mathfrak{p}}$，所以 $T \subseteq R_{\mathfrak{p}}$. 另一方面，设 $y = a/b \in R_{\mathfrak{p}}$，其中 $a, b \in R$ 且 $b \notin \mathfrak{p}$；则 $v_{\mathfrak{p}}(a) \geqslant 0$，$v_{\mathfrak{p}}(b) = 0$，从而 $v(y) = v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b) \geqslant 0$，所以 $y \in T$. 于是 $R_{\mathfrak{p}} \subseteq T$. 所以 $T = R_{\mathfrak{p}}$. □

定理 4.2.7　设 R 是整环. 则下列条件等价：

(1) R 是 Dedekind 整环；

(2) R 是 Noether 环，且 R 在每个极大理想 $\mathfrak{p}$ 处的局部化 $R_{\mathfrak{p}}$ 是离散赋值环.

证明　(1)⇒(2)：由命题 4.2.6 可得.

(2)⇒(1)：设 I 是 R 的分式理想，F 是 R 的分式域. 则存在 $b \in R \backslash \{0\}$ 使得 $bI \subseteq R$. 因 R 是 Noether 环，$I \simeq bI$ 是有限生成 R-模. 设 $I = \sum_{i=1}^{n} Ra_i$，$a_i \in F \backslash \{0\}$. 记

$$J = \{x \in F \mid xI \subseteq R\}.$$

则 J 是 R-模且 $IJ \subseteq R$. 下面要证 $IJ = R$，从而 I 是可逆的，再由定理 4.2.3 可知，R 是 Dedekind 整环.

设 $\tau: IJ \to R$ 是包含映射，$\mathfrak{p} \in \mathrm{Max}R$. 首先，不难验证 $J = \bigcap_{i=1}^{n} Ra_i^{-1}$. 再由命题 2.5.8 可得 $I_{\mathfrak{p}} = \sum_{i=1}^{n} (Ra_i)_{\mathfrak{p}} = \sum_{i=1}^{n} R_{\mathfrak{p}} a_i$，$J_{\mathfrak{p}} = \bigcap_{i=1}^{n} (Ra_i^{-1})_{\mathfrak{p}} = \bigcap_{i=1}^{n} R_{\mathfrak{p}} a_i^{-1} = \{x \in F \mid xI_{\mathfrak{p}} \subseteq R_{\mathfrak{p}}\}$. 于是 $I_{\mathfrak{p}} J_{\mathfrak{p}} =$

$(IJ)_{\mathfrak{p}}\subseteq R_{\mathfrak{p}}$. 因 $R_{\mathfrak{p}}$ 是离散赋值环，由命题 4.2.5 可知 $R_{\mathfrak{p}}$ 是 Dedekind 整环，故 $I_{\mathfrak{p}}$ 是可逆的，且$(I_{\mathfrak{p}})^{-1}=J_{\mathfrak{p}}$. 于是对于每个 $\mathfrak{p}\in\mathrm{Max}\,R$，$\tau_{\mathfrak{p}}:(IJ)_{\mathfrak{p}}=I_{\mathfrak{p}}J_{\mathfrak{p}}\to R_{\mathfrak{p}}$ 均是满射. 据命题2.5.13，$\tau:IJ\to R$ 也是满射. 所以 $IJ=R$，从而 I 是可逆的. □

习 题 4.2

1. 设 R 是 Dedekind 整环，$I=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$ 和 $J=\mathfrak{p}_1^{f_1}\cdots\mathfrak{p}_t^{f_t}$ 是 R 的分式理想，其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}_t$ 是 R 的互不相同的素理想，$e_i,f_i\in\mathbb{Z}$. 证明：

(1) $I\subseteq J$ 当且仅当 $e_i\geqslant f_i$，$i=1,\cdots,t$.

(2) $I+J=\prod\limits_{i=1}^{t}\mathfrak{p}_i^{\min\{e_i,f_i\}}$.

(3) $I\cap J=\prod\limits_{i=1}^{t}\mathfrak{p}_i^{\max\{e_i,f_i\}}$.

(4) $IJ=\prod\limits_{i=1}^{t}\mathfrak{p}_i^{e_i+f_i}$.

2. 设 I，J 是 Dedekind 整环 R 的分式理想. 证明：

$$(I+J)(I\cap J)=IJ.$$

3. 设 R 是 1 维 Noether 整环. 证明：R 是 Dedekind 整环$\Leftrightarrow$ R 的准素理想均是素理想的幂.

4. 设 R 是整环. 证明：R 是 Dedekind 整环$\Leftrightarrow$对于 R 的每个整理想 I 和 $a\in I\backslash\{0\}$，存在 $b\in I$ 使得 $I=aR+bR$.（提示：用局部整体性质考察局部整环，利用引理 1.2.1 和定理 4.2.7).

5. 设 v 是域 F 的离散赋值，$a,b\in F^*$. 证明：若 $v(a)>v(b)$，则 $v(a+b)=v(b)$.

4.3 整 性

整性是通常的整数概念向一般交换环的成功推广.

设 $A\subseteq B$ 是环的**扩张**，也就是说，A 是环B 的子环，或 B 是

A 的扩环. 设 $b\in B$, 称 b 是 A 上的**整元**, 或 b 在 A 上**整**, 如果 b 是 $A[x]$中某个首一多项式的根. 由定义可知, A 中的元素 a 均在 A 上整, 这因为 a 是首一多项式 $x-a\in A[x]$的根. 设 $A\subseteq B\subseteq C$ 是环的扩张, $c\in C$. 若 c 在 A 上整, 则 c 在 B 上整. 特别地, 有理数 $a\in\mathbb{Q}$ 在 $\mathbb{Z}$ 上整当且仅当 $a\in\mathbb{Z}$, 这是因为 $\mathbb{Z}[x]$中首一多项式的有理数根必是整数.

接下来的问题是, 整元的和、差与积是否仍是整元? 例如, $\sqrt{2}$和$\sqrt[3]{3}$在 $\mathbb{Z}$ 上整, $\sqrt{2}\pm\sqrt[3]{3}$是否在 $\mathbb{Z}$ 上整? 历史上, 为解决这一问题, Dedekind 创造了模这一概念, 用以刻画整元的代数性质.

引理 4.3.1 设 $A\subseteq B$ 是环的扩张, $b\in B$, 则下列条件等价:

(1) b 在 A 上整;

(2) $A[b]$是有限生成 A-模;

(3) 存在 B 的子环D, 使得 $A[b]\subseteq D$, 且 D 是有限生成 A-模;

(4) 存在忠实 $A[b]$-模M, 使得 M 是有限生成A-模.

证明 (1)$\Rightarrow$(2): 若 b 是 $x^n+a_1x^{n-1}+\cdots+a_n\in A[x]$的根, 则对于每个 $r\geqslant 0$, $b^{n+r}=-(a_1b^{n+r-1}+\cdots+a_nb^r)$. 用归纳法可证, 对于每个 $m\geqslant 0$, b^m 可由 $1,b,\cdots,b^{n-1}$来 A-线性表示. 从而, $A[b]$作为 A-模由$\{1,b,\cdots,b^{n-1}\}$生成.

(2)$\Rightarrow$(3): 取 $D=A[b]$即可.

(3)$\Rightarrow$(4): 取 $M=D$. 由于 D 有单位元, 从而 D 是一个忠实$A[b]$-模.

(4)$\Rightarrow$(1): 设 $M=Au_1+\cdots+Au_n$, $n\geqslant 1$. 由于 $bu_i\in M$, $bu_i=\sum\limits_{j=1}^{n}a_{ij}u_j$, $a_{ij}\in A$. 写成矩阵形式就是

$$(bI_n-(a_{ij}))\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix},$$

其中 I_n 表示 n 阶单位方阵. 两边乘以 $bI_n-(a_{ij})$ 的伴随矩阵, 得 $\det(bI_n-(a_{ij}))u_k=0$, $k=1,\cdots,n$. 于是 $\det(bI_n-(a_{ij}))\in \mathrm{Ann}_{A[b]}M$. 由于 M 是忠实的, 故 $\det(bI_n-(a_{ij}))=0$. 这样, b 是 $A[x]$ 中首一多项式 $\det(xI_n-(a_{ij}))$ 的根. 所以 b 在 A 上整.

□

命题 4.3.2 设 $A\subseteq B$ 是环的扩张.

(1) 若 $b_1,\cdots,b_n\in B$ 均在 A 上整, 则 $A[b_1,\cdots,b_n]$ 是有限生成 A-模.

(2) $D=\{b\in B\mid b$ 在 A 上整$\}$ 是 B 的子环.

证明 (1) 对 n 归纳. 当 $n=1$ 时, 由引理 4.3.1 可得. 假定 $A_{n-1}=A[b_1,\cdots,b_{n-1}]$ 是有限生成 A-模. 因 b_n 在 A 上整, 从而 b_n 在 A_{n-1} 上整. 由引理 4.3.1, $A_n=A_{n-1}[b_n]$ 是有限生成 A_{n-1}-模, 从而 A_n 是有限生成 A-模(习题 1.2.6).

(2) 设 $b_1,b_2\in D$. 由(1), $A[b_1,b_2]$ 是有限生成 A-模, 且 $b_1\pm b_2$, $b_1b_2\in A[b_1,b_2]$. 由引理 4.3.1, $b_1\pm b_2$ 和 b_1b_2 在 A 上整, 从而 $b_1\pm b_2,b_1b_2\in D$. 所以 D 是 B 的子环. □

由命题 4.3.2 可知, A 上两个整元的和、差与积仍是 A 上的整元. 命题 4.3.2 中的子环 D 称为 A 在 B 中的**整闭包**. 于是有环扩张 $A\subseteq D\subseteq B$. 若 $D=A$, 则称 A 在 B 中**整闭**. 若 $D=B$, 则称 B 在 A 上整, 也称 $A\subseteq B$ 是环的**整性扩张**.

推论 4.3.3 (整性的传递性) 设 $A\subseteq B\subseteq C$ 是环的扩张. 若 C 在 B 上整, 且 B 在 A 上整, 则 C 在 A 上整.

证明 设 $c\in C$, 则 c 在 B 上整. 设 c 是 B 上首一多项式 $x^n+b_1x^{n-1}+\cdots+b_n$ 的根. 记 $B'=A[b_1,\cdots,b_n]$. 因 $b_1,\cdots,b_n\in B$ 均在 A 上整, 由命题 4.3.2 的(1), B' 是有限生成 A-模, 且 c 在 B' 上整. 于是 $B'[c]$ 是有限生成 B'-模, 进而是有限生成 A-模, 故 c 在 A 上整. 所以 C 在 A 上整. □

推论 4.3.4 设 $A\subseteq B$ 是环的扩张, D 是 A 在 B 中的整闭

包，则 D 在 B 中整闭.

证明 设 $b\in B$. 若 b 在 D 上整，由推论 4.3.3 的证明可知，b 在 A 上整，从而 $b\in D$. 所以 D 在 B 中整闭. □

以下命题表明商环和分式化均保持整性.

命题 4.3.5 设 $A\subseteq B$ 是环的整性扩张.

(1) 若 J 是 B 的理想，$I=J\cap A$，则 $A/I\subseteq B/J$ 是环的整性扩张，这里视单同态 $A/I\to B/J$ 为包含映射.

(2) 若 S 是 A 的乘法集，则 $S^{-1}A\subseteq S^{-1}B$ 是环的整性扩张.

证明 设 $b\in B$，b 是 $x^n+a_1x^{n-1}+\cdots+a_n\in A[x]$ 的根.

(1) 在 B/J 中，$\bar{b}^n+\bar{a}_1\bar{b}^{n-1}+\cdots+\bar{a}_n=0$，其中 $\bar{a}_i=a_i+I\in A/I$，$\bar{b}=b+J\in B/J$，所以 $\bar{b}$ 在 A/I 上整.

(2) 对于任意 $s\in S$，在 $S^{-1}B$ 中，$(b/s)^n+(a_1/s)(b/s)^{n-1}+\cdots+a_n/s^n=0$，所以 b/s 在 $S^{-1}A$ 上整. □

整环 A 称为是**整闭**的，如果 A 在它的分式域中整闭. 例如，整数环 $\mathbb{Z}$ 是整闭的，域 F 上一元多项式环 $F[x]$ 是整闭的(习题 4.3.3).

引理 4.3.6 Dedekind 整环 R 是整闭的.

证明 设 F 是 R 的分式域，$u\in F$. 若 u 在 R 上整，由引理 4.3.1，$M=R[u]$ 是 F 中的有限生成 R-模，从而是 R 的分式理想. 由定理 4.2.3，M 是可逆的. 由于 $uM\subseteq M$，两边乘以 M^{-1}，得 $uR\subseteq R$，从而 $u\in R$. 所以 R 在 F 中整闭. □

引理 4.3.7 设 R 是 Noether 整闭整环，R 的分式域为 F，I 是 R 的分式理想. 则

$$\{x\in F\mid xI\subseteq I\}=R.$$

证明 因 I 是 R 的分式理想，存在 $a\in R\setminus\{0\}$，使得 $aI\subseteq R$. 又因 R 是 Noether 整环，aI 是有限生成 R-模，且 $I\simeq aI$，从而 I 也是有限生成 R-模. 若 $x\in F$ 且 $xI\subseteq I$，则 I 是一个忠实 $R[x]$-模，由引理 4.3.1，x 在 R 上整. 而 R 是整闭的，所以 x

$\in R$. 这样, $\{x\in F \mid xI\subseteq I\}\subseteq R$, 而反包含是显然的. □

引理 4.3.8 设 R 是 Noether 整环, 则 R 的非零理想必含有 R 的非零素理想之积.

证明 若不然, 由于 R 是 Noether 环, 在 R 的所有不包含非零素理想之积的非零理想的集合中必有一个极大者 I, 则 I 不是素理想. 于是存在 R 的理想 I_1 和 I_2, 使得 $I_1\supset I$, $I_2\supset I$, 且 $I_1I_2\subseteq I$. 由 I 的极大性可知, I_1 和 I_2 均含有非零素理想之积, 从而 I_1I_2 亦然; 但 $I_1I_2\subseteq I$, 这与 I 的选择矛盾. □

引理 4.3.9 设 R 是 Noether 整环, 且 $\dim R=1$, F 为 R 的分式域, I 是 R 的非零理想且 $I\neq R$. 则存在 $c\in F\backslash R$, 使得 $cI\subseteq R$.

证明 取 $a\in I\backslash\{0\}$. 由引理 4.3.8, aR 含有非零素理想之积 $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m$, 且设其中的 m 为最小者. 又设 $\mathfrak{p}$ 是包含 I 的极大理想. 则 $\mathfrak{p}_1\cdots\mathfrak{p}_m\subseteq\mathfrak{p}$, 从而 $\mathfrak{p}$ 包含某个 $\mathfrak{p}_j$, 不妨设 $\mathfrak{p}\supseteq\mathfrak{p}_1$. 因 R 是 1 维的, $\mathfrak{p}=\mathfrak{p}_1$. 若 $m=1$, 则 $I=aR=\mathfrak{p}$ 是极大的, 故 $a^{-1}\notin R$, 但 $a^{-1}I\subseteq R$. 若 $m\geqslant 2$, 由 m 的最小性, $\mathfrak{p}_2\cdots\mathfrak{p}_m\nsubseteq aR$. 取 $b\in\mathfrak{p}_2\cdots\mathfrak{p}_m\backslash aR$, 令 $c=b/a$. 则 $c\notin R$, 但 $cI\subseteq c\mathfrak{p}_1\subseteq a^{-1}b\mathfrak{p}_1\subseteq a^{-1}\mathfrak{p}_1\cdots\mathfrak{p}_m\subseteq a^{-1}aR\subseteq R$. □

定理 4.3.10 环 R 是 Dedekind 整环 $\Leftrightarrow R$ 是 Noether 整闭整环, 且 $\dim R\leqslant 1$.

证明 $\Rightarrow$: 由命题 4.1.1 的(4)、(5)以及引理 4.3.6 可得.

$\Leftarrow$: 不妨设 $\dim R=1$. 若 I 是 R 的分式理想, 令 $J=\{a\in F \mid aI\subseteq R\}$, 其中 F 是 R 的分式域, 则 IJ 是 R 的整理想. 再令 $K=\{x\in F \mid xIJ\subseteq R\}$, 则 $K\supseteq R$, 且 $K(IJ)=(KJ)I\subseteq R$, 从而 $KJ\subseteq J$. 由引理 4.3.7, $K\subseteq R$, 所以 $K=R$. 假定 $IJ\neq R$, 由引理 4.3.9, 则 $K\neq R$, 这矛盾. 所以 $IJ=R$, 从而 I 是可逆的. 再由定理 4.2.3, R 是 Dedekind 整环. □

下面讨论环的整性扩张的性质.

命题 4.3.11　设 $A\subseteq B$ 是环的整性扩张.

(1) 若 B 是整环, 则 B 是域$\Leftrightarrow A$ 是域.

(2) 若 $\mathfrak{q}\in \operatorname{Spec} B$, $\mathfrak{p}=\mathfrak{q}\cap A(\in \operatorname{Spec} A)$, 则 $\mathfrak{q}\in \operatorname{Max} B\Leftrightarrow \mathfrak{p}\in \operatorname{Max} A$.

(3) 若 A 是局部环, $\mathfrak{m}$ 是 A 的唯一极大理想, $\mathfrak{q}\in \operatorname{Spec} B$, 则 $\mathfrak{q}\in \operatorname{Max} B\Leftrightarrow \mathfrak{q}\cap A=\mathfrak{m}$.

证明　(1) 若 $b\in B\backslash\{0\}$, 则 b 在 A 上整. 于是存在 $a_i\in A$ 和 $n\geqslant 1$, 使得 $b^n+a_1b^{n-1}+\cdots+a_n=0$. 因 B 是整环, 不妨设 $a_n\neq 0$. 若 A 是域, 则 $a_n^{-1}\in A$, 从而 $b^{-1}=-a_n^{-1}(b^{n-1}+a_1b^{n-2}+\cdots+a_{n-1})\in B$. 所以 B 也是域. 反之, 若 B 为域, 设 $a\in A\backslash\{0\}$, 则 $a^{-1}\in B$ 在 A 上整. 于是存在 $b_i\in A$ 和 $m\geqslant 1$, 使得 $a^{-m}+b_1a^{-(m-1)}+\cdots+b_m=0$, 从而 $a^{-1}=-(b_1+\cdots+b_ma^{m-1})\in A$. 所以 A 也是域.

(2) 由命题 4.3.5 的(1), $A/\mathfrak{p}\subseteq B/\mathfrak{q}$ 是整环的整性扩张. 由(1), $A/\mathfrak{p}$ 是域$\Leftrightarrow B/\mathfrak{q}$ 是域. 所以 $\mathfrak{p}\in \operatorname{Max} A\Leftrightarrow \mathfrak{q}\in \operatorname{Max} B$.

(3) 由(2)及 $\mathfrak{m}$ 的唯一性立得. □

命题 4.3.12　设 $A\subseteq B$ 是环的整性扩张.

(1) (**Lying over**)对于每个 $\mathfrak{p}\in \operatorname{Spec} A$, 均在 $\mathfrak{q}\in \operatorname{Spec} B$, 使得 $\mathfrak{q}\cap A=\mathfrak{p}$.

(2) 若 $\mathfrak{q}_1$, $\mathfrak{q}_2\in \operatorname{Spec} B$, $\mathfrak{q}_1\subseteq \mathfrak{q}_2$, 且 $\mathfrak{q}_1\cap A=\mathfrak{q}_2\cap A=\mathfrak{p}(\in \operatorname{Spec} A)$, 则 $\mathfrak{q}_1=\mathfrak{q}_2$.

证明　设 $\mathfrak{p}\in \operatorname{Spec} A$, $S=A\backslash \mathfrak{p}$ 是 A 的乘法集, 由命题 4.3.5 的(2), $S^{-1}A\subseteq S^{-1}B$ 是环的整性扩张; 且 $S^{-1}A$ 是局部环, 有唯一的极大理想 $S^{-1}\mathfrak{p}$.

(1) 取 $Q\in \operatorname{Max}(S^{-1}B)$, 由命题 2.5.3 的(3), 存在 $\mathfrak{q}\in \operatorname{Spec} B$, 使得 $\mathfrak{q}\cap S=\varnothing$ 且 $S^{-1}\mathfrak{q}=Q$. 由命题 4.3.11 的(3), $S^{-1}\mathfrak{p}=S^{-1}\mathfrak{q}\cap S^{-1}A=S^{-1}(\mathfrak{q}\cap A)$, 但$(\mathfrak{q}\cap A)\cap S=\varnothing$, 所以 $\mathfrak{q}\cap A=\mathfrak{p}$.

(2) 因 $\mathfrak{q}_i \cap A = \mathfrak{p}$，故 $\mathfrak{q}_i \cap S = \varnothing$. 于是，由命题 2.5.3 的(3)，$S^{-1}\mathfrak{q}_i \in \mathrm{Spec}(S^{-1}B)$；且 $S^{-1}\mathfrak{q}_i \cap S^{-1}A = S^{-1}(\mathfrak{q}_i \cap A) = S^{-1}\mathfrak{p}$，由命题 4.3.11 的(3)，$S^{-1}\mathfrak{q}_i$ 是 $S^{-1}A$ 的极大理想，$i=1, 2$. 又因 $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$，所以 $S^{-1}\mathfrak{q}_1 = S^{-1}\mathfrak{q}_2$. 又由于 $\mathfrak{q}_i \cap S = \varnothing$，所以 $\mathfrak{q}_1 = \mathfrak{q}_2$. □

定理 4.3.13 (上行定理) 设 $A \subseteq B$ 是环的整性扩张，$\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{Spec}\ A$，$\mathfrak{p}_1 \subseteq \mathfrak{p}_2$，$\mathfrak{q}_1 \in \mathrm{Spec}\ B$，$\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. 则存在 $\mathfrak{q}_2 \in \mathrm{Spec}\ B$，使得 $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$，且 $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$.

证明 由命题 4.3.5 的(1)，$A/\mathfrak{p}_1 \subseteq B/\mathfrak{q}_1$ 是环的整性扩张. 由命题 4.3.12 的(1)，存在 $Q \in \mathrm{Spec}(B/\mathfrak{q}_1)$，使得 $Q \cap (A/\mathfrak{p}_1) = \mathfrak{p}_2/\mathfrak{p}_1 \in \mathrm{Spec}(A/\mathfrak{p}_1)$. 而 Q 可表示成 $\mathfrak{q}_2/\mathfrak{q}_1$，其中 $\mathfrak{q}_2 \in \mathrm{Spec}\ B$ 且 $\mathfrak{q}_2 \supseteq \mathfrak{q}_1$，并且 $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. □

附加一些条件，可证明与上行定理对应的下行定理. 先做一些准备工作.

设 $A \subseteq B$ 是环的扩张，I 是 A 的理想，$b \in B$. 称 b **在 I 上整**，如果存在首一多项式 $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$，$a_i \in I$，$n \geqslant 1$，使得 $f(b)=0$. 记 $D = \{b \in B \mid b \text{ 在 } I \text{ 上整}\}$，叫做 I 在 B 中的**整闭包**. 又记 C 是 A 在 B 中的整闭包，显然 $I \subseteq D \subseteq C$.

引理 4.3.14 所设同上，则 $D = \sqrt{IC}$，是 C 的一个理想.

证明 若 $b \in D$，则存在 $a_i \in I$，$n \geqslant 1$，使得 $b^n + a_1b^{n-1} + \cdots + a_n = 0$，于是 $b^n \in IC$，从而 $b \in \sqrt{IC}$. 反之，若 $b \in \sqrt{IC}$，则存在 $n \geqslant 1$，使得 $b^n \in IC$. 设 $b^n = \sum_{i=1}^{m} a_ic_i$，其中 $a_i \in I$，$c_i \in C$. 由于 c_i 在 A 上整，故 $M = A[c_1, \cdots, c_m]$ 是有限生成 A-模，且 $b^nM \subseteq IM$. 用引理 4.3.1 中(4)⇒(1)的证法可得 b^n 在 I 上整，从而 b 在 I 上整. 所以 $b \in D$. □

引理 4.3.15 设 $A \subseteq B$ 是整环的扩张，A 是整闭的，I 是 A

的理想，K 是 A 的分式域. 若 $b\in B$ 在 I 上整，b 在 K 上的极小多项式为 $g(x)=x^r+d_1x^{r-1}+\cdots+d_r$，$d_i\in K$，则 $d_i\in\sqrt{I}$，$i=1,\cdots,r$.

证明　因 b 在 I 上整，存在多项式 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$，$a_i\in I$，使得 $f(b)=0$. 于是 $g(x)\mid f(x)$. 设 $f(x)$在 K 上的分裂域为 L，则 $g(x)$在 L 中的根均是$f(x)$的根，从而均在 I 上整. 由根与系数的关系和引理 4.3.14 可知，d_i 均在 I(从而在 A)上整. 因 A 是整闭的，$d_i\in A$，从而 $d_i\in\sqrt{IA}=\sqrt{I}$. □

定理 4.3.16（下行定理）　设 $A\subseteq B$ 是整环的整性扩张，且 A 是整闭的. 若 $\mathfrak{p}_1$，$\mathfrak{p}_2\in\operatorname{Spec}A$，$\mathfrak{p}_1\subseteq\mathfrak{p}_2$，$\mathfrak{q}_2\in\operatorname{Spec}B$，$\mathfrak{q}_2\cap A=\mathfrak{p}_2$，则存在 $\mathfrak{q}_1\in\operatorname{Spec}B$，使得 $\mathfrak{q}_1\cap A=\mathfrak{p}_1$，且 $\mathfrak{q}_1\subseteq\mathfrak{q}_2$.

证明　设 $S=\{u\nu\mid u\in A\backslash\mathfrak{p}_1,\ \nu\in B\backslash\mathfrak{q}_2\}$，则 S 是 B 的乘法集. 令 Σ 是B 中包含 $\mathfrak{p}_1B$ 且与S 不交的理想的全体. 若能证 $\mathfrak{p}_1B\cap S=\varnothing$，则 Σ 非空. 用 Zorn 引理易证，Σ 有极大元 $\mathfrak{q}_1$. $\mathfrak{q}_1$ 必是素理想，这是因为：假定 $a,b\in B$，$ab\in\mathfrak{q}_1$，但 $a,b\notin\mathfrak{q}_1$. 由 $\mathfrak{q}_1$ 的极大性可知，$(\mathfrak{q}_1+aB)\cap S\neq\varnothing$，即存在 $x\in(\mathfrak{q}_1+aB)\cap S$；同理,存在 $y\in(\mathfrak{q}_1+bB)\cap S$. 于是 $xy\in\mathfrak{q}_1\cap S$，这矛盾. 再由 $\mathfrak{q}_1\cap S=\varnothing$可知 $\mathfrak{q}_1\subseteq\mathfrak{q}_2$，且 $\mathfrak{q}_1\cap A=\mathfrak{p}_1$. 这样，$\mathfrak{q}_1$ 即为所需的素理想.

下面用反证法证明 $\mathfrak{p}_1B\cap S=\varnothing$. 假定 $t\in\mathfrak{p}_1B\cap S$，则 $t\in\mathfrak{p}_1B$，由引理 4.3.14，t 在 $\mathfrak{p}_1$ 上整. 再由引理 4.3.15，t 在A 的分式域K 上的极小多项式$g(x)=x^r+d_1x^{r-1}+\cdots+d_r$ 中的 $d_i\in\sqrt{\mathfrak{p}_1}=\mathfrak{p}_1$. 因 $t\in S$，可设 $t=uv$，$u\in A\backslash\mathfrak{p}_1$，$v\in B\backslash\mathfrak{q}_2$，则 v 在 K 上的极小多项式为$h(x)=x^r+\dfrac{d_1}{u}x^{r-1}+\cdots+\dfrac{d_r}{u^r}$. 仍由引理 4.3.14(取 $I=A$)可知，$h[x]\in A[x]$. 于是$\dfrac{d_i}{u^i}=c_i\in A$. 因 $d_i=u^ic_i\in\mathfrak{p}_1$ 且 $u\notin\mathfrak{p}_1$，所以 $c_i\in\mathfrak{p}_1$. 于是 $v^r=-(c_1v^{r-1}+\cdots+c_r)\in$

$\mathfrak{p}_1 B\subseteq \mathfrak{q}_2$，从而 $v\in\mathfrak{q}_2$，这矛盾. □

下面要证明重要的 Noether 正规化引理，并导出证明 Hilbert 零点定理时用到的那个引理.

定理 4.3.17（Noether 正规化引理） 设 A 是域 k 上的有限生成 k-代数. 则存在 A 的子环 B，B 等于 k 或同构于 k 上的多项式环，且 A 在 B 上整.

证明 设 $A=k[u_1,\cdots,u_n]$，$u_i\in A$. 对 n 用归纳法. 当 $n=0$ 时，$A=k$，取 $B=A$ 即可. 下设 $n\geqslant 1$，且 $u_i\notin k$. 设 $R=k[x_1,\cdots,x_n]$是 k 上的多项式环. 若对于任意 $f\in R\backslash\{0\}$ 均有 $f(u_1,\cdots,u_n)\neq 0$，则 $A\simeq R$. 此时取 $B=A$ 即可. 否则，存在 $f\in R\backslash\{0\}$，使得 $f(u_1,\cdots,u_n)=0$. 不妨设 f 中 x_n 的次数不为 0，且设 $d=\deg(f)+1$. 对于 f 中的每个单项式 $\alpha=ax_1^{d_1}\cdots x_n^{d_n}$，其中 $a\in k\backslash\{0\}$，$d_i\geqslant 0$；令 $l(\alpha)=d_n+\sum\limits_{i=1}^{n-1}d^i d_i$. 容易证明，对于 f 中的不同单项式 α 和 β，均有 $l(\alpha)\neq l(\beta)$. 令 $v_i=u_i-u_n^{d^i}\in A$，$i=1,\cdots,n-1$. 将 $u_i=v_i+u_n^{d^i}$，$i=1,\cdots,n-1$，和 u_n 代入 f 和 f 中的一个单项式 $\alpha=ax_1^{d_1}\cdots x_n^{d_n}$（$a\neq 0$），再展开成关于 $v_1,\cdots,v_{n-1},u_n$ 的多项式 $f'=f'(v_1,\cdots,v_{n-1},u_n)$和 $\alpha'=\alpha'(v_1,\cdots,v_{n-1},u_n)$，则 α'的单项式中含有 $au_n^{l(\alpha)}$，这样的单项式在 f'中不会相消. 将 f'按 u_n 的幂合并，则 u_n 的最高次幂的系数在 $k\backslash\{0\}$ 中，所以 u_n 在 $A'=k[v_1,\cdots,v_{n-1}]$上整. 由归纳假定，A'有子环 B 等于 k 或同构于 k 上的多项式环，且 A'在 B 上整. 由整性的传递性，$A=A'[u_n]$在 B 上整. □

引理 4.3.18 设 k 是域，$y_1,\cdots,y_n$ 是 k 的某个扩域中的元素. 若 $k[y_1,\cdots,y_n]$是域，则每个 y_i 均是 k 上的代数元.

证明 由定理 4.3.17，$A=k[y_1,\cdots,y_n]$含有子环 $B=k$ 或同构于 k 上的多项式环，且 A 在 B 上整. 于是只需证 $B=k$. 假

定 $B\simeq k[x_1,\cdots,x_r]$，不妨视同构为相等，则 $x_1^{-1}\in A$ 在 B 上整. 于是存在 $b_0,\cdots,b_{m-1}\in B$，$b_0\neq 0$，$m\geqslant 1$，使得 $x_1^{-m}+b_{m-1}x_1^{-(m-1)}+\cdots+b_0=0$，从而 $x_1^{-1}=-(b_0x_1^{m-1}+\cdots+b_{m-1})\in B$，这矛盾. □

习　题　4.3

1. 设 $A\subseteq B$ 是环的扩张，C 是 A 在 B 中的整闭包，S 是 A 的乘法集. 证明：

(1) $S^{-1}C$ 是 $S^{-1}A$ 在 $S^{-1}B$ 中的整闭包.

(2) 若 A 是整闭整环，则 $S^{-1}A$ 也是整闭整环.

2. 设 $A\subseteq B$ 是环的整性扩张. 证明：

(1) $A\cap \mathrm{U}(B)=\mathrm{U}(A)$.

(2) $A\cap \mathrm{Rad}(B)=\mathrm{Rad}(A)$.

3. 证明：唯一因子分解整环必是整闭整环.

4. 设 k 是域，$A=k[x^2-1]$，$B=k[x]$，$\mathfrak{q}=(x-1)\in \mathrm{Max}\,B$，$\mathfrak{p}=\mathfrak{q}\cap A\in \mathrm{Max}\,A$. 证明：$A\subseteq B$ 是环的整性扩张，但 $A_{\mathfrak{p}}\subseteq B_{\mathfrak{q}}$ 不是环的整性扩张.

5. 设 K 是整环 A 的分式域，$0\neq a\in A$. 证明：

(1) 若 a 和 $a^{-1}\in K$ 均在 A 上整，则 $a\in \mathrm{U}(A)$.

(2) 若 K 在 A 上整，则 A 是域.

6. 设 $A\subseteq B$ 是整环的扩张，C 是 A 在 B 中的整闭包. 证明：

(1) 若 $f(x)$ 和 $g(x)$ 是 $B[x]$ 中的首一多项式，且 $f(x)g(x)\in C[x]$，则 $f(x),g(x)\in C[x]$.

(2) 去掉 A 和 B 是整环的限制，(1)仍成立(提示：先证明存在 B 的扩环 B'，使得 $f(x)g(x)=(x-a_1)\cdots(x-a_n)$，$a_i\in B'$).

7. 设 $A\subseteq B$ 是环的扩张，C 是 A 在 B 中的整闭包. 证明：$C[x]$是 $A[x]$在 $B[x]$中的整闭包. 进而证明，若 A 是整闭整

环，则 $A[x]$也是整闭整环.

8. 设 R 是整环，证明下列三个条件等价：

(1) R 是整闭整环；

(2) 对于每个 $\mathfrak{p}\in \operatorname{Spec} R$，$R_{\mathfrak{p}}$ 是整闭整环；

(3) 对于每个 $\mathfrak{m}\in \operatorname{Max} R$，$R_{\mathfrak{m}}$ 是整闭整环.

9. 设 S_i，T_i，$i\in I$，是环 R 的子环，$S_i\subseteq T_i$，且 S_i 在 T_i 中整闭，$i\in I$. 证明：$\bigcap\limits_{i\in I}S_i$ 在 $\bigcap\limits_{i\in I}T_i$ 中整闭.

10. 设 $A\subseteq B$ 是环的整性扩张. 证明：$\dim A=\dim B$.

11. 证明：$\mathbb{Z}[x]/(x^2+4)$是整环，但不是整闭整环.

12. 证明：(1) $\mathbb{Z}[\sqrt{5}]$是 1 维 Noether 整环，但不是整闭整环.

(2) $k[x_1,x_2]$(k 是域)是 Noether 整闭整环，但维数大于或等于 2.

(3) $\bigcup\limits_{n\geqslant 1}k[x^{\frac{1}{n}}]$($k$ 是域)是 1 维整闭整环，但不是 Noether 环.

13. 设 k 是域，$A=k[x^2-x,x^3-x^2,y]$，$B=k[x,y]$. 证明：对于环的扩张 $A\subseteq B$，上行定理成立，但下行定理不成立.

4.4 代数整数环

本节介绍一类典型的 Dedekind 整环——代数整数环，它是代数数论的基本研究对象.

有理数域 $\mathbb{Q}$ 的有限(次)扩域叫做**代数数域**. 由于复数域 $\mathbb{C}$ 是 $\mathbb{Q}$ 的代数封闭扩域，代数数域总可视为 $\mathbb{C}$ 的子域.

整数环 $\mathbb{Z}$ 在代数数域 F 中的整闭包，也就是 F 中所有 $\mathbb{Z}$ 上的整元构成的子环，叫做 F 的**代数整数环**，记作 O_F.

以下总设 F 是 $\mathbb{Q}$ 的 n 次扩域，O_F 是F 的代数整数环.

4.4.1 迹与范

设 $u\in F$，映射 $f_u:F\to F$；$x\mapsto ux$ 是一个 $\mathbb{Q}$-线性变换. 任

取 F 的一个 $\mathbb{Q}$-基，f_u 唯一对应于一个 $\mathbb{Q}$ 上的 n 阶方阵 A，定义 u 在 $\mathbb{Q}$ 上的最小多项式 $d_u(x)$、特征多项式 $\varphi_u(x)$、**迹** $\mathrm{T}(u)$**和范** $\mathrm{N}(u)$分别是 A 的最小多项式、特征多项式、迹 $\mathrm{tr}\,A$ 和行列式 $\det A$，它们均与 F 的 $\mathbb{Q}$-基的选取无关. 由矩阵的迹与行列式的性质立得

命题 4.4.1 对任意 $u,v\in F$ 和 $a\in\mathbb{Q}$，均有

(1) $\mathrm{T}(u+v)=\mathrm{T}(u)+\mathrm{T}(v)$，$\mathrm{T}(au)=a\mathrm{T}(u)$.

(2) $\mathrm{N}(uv)=\mathrm{N}(u)\mathrm{N}(v)$，$\mathrm{N}(au)=a^n\mathrm{N}(u)$. □

据 Cayley-Hamilton 定理，u 是 $\varphi_u(x)$的一个根，设 $u_1=u$，$u_2,\cdots,u_n$ 是 $\varphi_u(x)$的 n 个复根，则

$$\mathrm{T}(u)=u_1+\cdots+u_n,$$
$$\mathrm{N}(u)=u_1u_2\cdots u_n.$$

设 $u\in F$ 在 $\mathbb{Q}$ 上的最小多项式 $d_u(x)=x^r+b_1x^{r-1}+\cdots+b_r$，则 $d_u(x)$是 $\mathbb{Q}$ 上的不可约多项式，且$\{1,u,\cdots,u^{r-1}\}$是 F 的子域 $\mathbb{Q}[u]$的 $\mathbb{Q}$-基. 设 u 作为 $\mathbb{Q}[u]$上的 $\mathbb{Q}$-线性变换在基$\{1,u,\cdots,u^{r-1}\}$下的矩阵为 B，则

$$B=\begin{bmatrix} 0 & & & -b_r \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -b_2 \\ & & 1 & -b_1 \end{bmatrix}.$$

设$[F:\mathbb{Q}[u]]=m$，则 $mr=n$. 取 F 的 $\mathbb{Q}[u]$-基$\{v_1,\cdots,v_m\}$，则$\{v_1,v_1u,\cdots,v_1u^{r-1},\cdots,v_m,v_mu,\cdots,v_mu^{r-1}\}$是 F 的 $\mathbb{Q}$-基，且 u 在它下的矩阵$A=\mathrm{diag}\{B,\cdots,B\}\in\mathbb{Q}^{n\times n}$. 于是有

命题 4.4.2 所设同上. 则

(1) $\varphi_u(x)=d_u(x)^m$.

(2) $\mathrm{T}(u)=m\ (\mathrm{tr}\,B)=-mb_1$.

(3) $\mathrm{N}(u)=(\det B)^m=(-1)^n b_r{}^m$. □

特别地，当 $\alpha\in O_F$ 时，存在首一多项式 $f(x)\in\mathbb{Z}[x]$使得

$f(\alpha)=0$, 故 $d_\alpha(x)\mid f(x)$. 由于 $\mathbb{Z}[x]$中的不可约多项式在 $\mathbb{Q}[x]$中也不可约, $d_\alpha(x)$相伴于一个 $\mathbb{Z}[x]$中的不可约多项式, 所以 $d_\alpha(x)\in\mathbb{Z}[x]$(习题 4.4.5), 从而 $\varphi_\alpha(x)\in\mathbb{Z}[x]$. 于是 $\mathrm{T}(\alpha)$, $\mathrm{N}(\alpha)\in\mathbb{Z}$. 这证明了

命题 4.4.3 若 $\alpha\in O_F$, 则

(1) $d_\alpha(x)$, $\varphi_\alpha(x)\in\mathbb{Z}[x]$.

(2) $\mathrm{T}(\alpha)$, $\mathrm{N}(\alpha)\in\mathbb{Z}$. □

4.4.2 整基与判别式

引理 4.4.4 *F 中的每个元素均可表示成 r/b 的形式, 其中 $r\in O_F$, $b\in\mathbb{Z}$. 从而 F 是 O_F 的分式域, 且 O_F 是整闭整环.*

证明 设 $u\in F$. 则存在 $f(x)=x^m+a_1x^{m-1}+\cdots+a_m\in\mathbb{Q}[x]\setminus\{0\}$, 使得 $f(u)=0$. 将 a_i 表示成 $a_i=c_i/b$, 其中 $c_i, b\in\mathbb{Z}$, $i=1,\cdots,m$, 且令 $g(x)=b^mf(b^{-1}x)$, 则 $g(x)\in\mathbb{Z}[x]\setminus\{0\}$, $g(x)$是首一的, 且 $g(bu)=0$. 于是 $r=bu$ 在 $\mathbb{Z}$ 上整, 即 $r\in O_F$. 这样 $u=r/b$. 所以 F 是 O_F 的分式域. 由推论 4.3.4, O_F 在 F 中整闭, 所以 O_F 是整闭整环. □

映射

$$F\times F\to\mathbb{Q};\ (u,\nu)\mapsto\mathrm{T}(u\nu)$$

是 $\mathbb{Q}$ 上的线性空间 F 的一个对称双线性函数, 且是非退化的. 这是因为, 对于 F 的任意非零元素 u, 均有 $\mathrm{T}(uu^{-1})=\mathrm{T}(1)=n\neq 0$. 于是, 若$\{\alpha_1,\cdots,\alpha_n\}$是 F 的 $\mathbb{Q}$-基, $u\in F$, 则 $T(u\alpha_i)=0$, $i=1,\cdots,n$, 当且仅当 $u=0$.

引理 4.4.5 *O_F 的每个非零理想 I 均是秩为 n 的自由 $\mathbb{Z}$-模, 且 O_F/I 是有限环, 从而 O_F 是 Noether 环.*

证明 任取 F 的 $\mathbb{Q}$-基$\{\alpha_1,\cdots,\alpha_n\}$, 由引理 4.4.4, 存在 $b\in\mathbb{Z}\setminus\{0\}$使得 $b\alpha_1,\cdots,b\alpha_n\in O_F$. 因此, 不妨一开始就设 $\alpha_1,\cdots,\alpha_n\in O_F$. 令

$$\psi: I \to \mathbb{Z}^n;\ u \mapsto (\mathrm{T}(u\alpha_1), \cdots, \mathrm{T}(u\alpha_n)),$$

则 ψ 是 $\mathbb{Z}$-模单同态. 据定理 2.6.1, $I \simeq \mathrm{Im}\,\psi$ 是秩小于或等于 n 的自由 $\mathbb{Z}$-模. 任取 $u \in I \backslash \{0\}$, 则 $\{u\alpha_1, \cdots, u\alpha_n\}$ 是 I 中的 $\mathbb{Z}$-线性无关子集. 所以, I 是秩为 n 的自由 $\mathbb{Z}$-模, 从而 I 作为 O_F-模是有限生成的. 进而可知 O_F 是 Noether 环. 由于 I 是 O_F 的 $\mathbb{Z}$-子模, 且秩为 n, 据定理 2.6.1, 存在 O_F 的 $\mathbb{Z}$-基 $\{w_1, \cdots, w_n\}$ 和 $a_1, \cdots, a_n \in \mathbb{Z} \backslash \{0\}$, 使得 $\{a_1 w_1, \cdots, a_n w_n\}$ 是 I 的 $\mathbb{Z}$-基, 于是 $|O_F/I| = |\mathbb{Z}/\mathbb{Z}a_1 \oplus \cdots \oplus \mathbb{Z}/\mathbb{Z}a_n| = |a_1 \cdots a_n|$ 是有限的. □

O_F 的 $\mathbb{Z}$-基 $\{w_1, \cdots, w_n\}$ 叫做 O_F 的**整基**, 它也是 F 的 $\mathbb{Q}$-基.

O_F 的两个整基间的过渡矩阵是 $\mathbb{Z}$ 上的 n 阶可逆方阵, 其行列式的值为 ± 1.

对称 $\mathbb{Z}$-双线性函数

$$\mathrm{T}: O_F \times O_F \to \mathbb{Z};\ (\alpha, \beta) \mapsto \mathrm{T}(\alpha\beta)$$

在 O_F 的整基 $\{w_1, \cdots, w_n\}$ 下的矩阵 $(\mathrm{T}(w_i w_j))$ 是一个 $\mathbb{Z}$ 上的 n 阶方阵, 记

$$\mathrm{d}(F) = \det\ (\mathrm{T}(w_i w_j)) \in \mathbb{Z}.$$

由于 T 在 O_F 的不同整基下的矩阵在 $\mathbb{Z}$ 上相合, 所以 $\mathrm{d}(F)$ 与 O_F 的整基的选择无关, 称 $\mathrm{d}(F)$ 为 O_F 或 F 的**判别式**, 它对于寻求 O_F 的整基是有益的(习题 4.4.10).

引理 4.4.6 *O_F 的非零素理想 $\mathfrak{p}$ 均是极大的.*

证明 据引理 4.4.5, $O_F/\mathfrak{p}$ 是有限整环, 从而是有限域, 所以 $\mathfrak{p}$ 是极大的. □

对于 O_F 的非零素理想 $\mathfrak{p}$, 有限域 $O_F/\mathfrak{p}$ 称为关于 $\mathfrak{p}$ 的**剩余类域**.

由上述三个引理和定理 4.3.10 立得

定理 4.4.7 *O_F 是 Dedekind 整环.* □

4.4.3 理想的范与理想类群的有限性

设 I 是 O_F 的非零理想，定义 I 的**范** $\mathrm{N}(I)=|O_F/I|$. 据引理 4.4.5，$\mathrm{N}(I)$是正整数.

命题 4.4.8 (1) 设 I,J 是 O_F 的非零理想，则

$$\mathrm{N}(IJ)=\mathrm{N}(I)\mathrm{N}(J).$$

(2) 设 $u\in O_F\setminus\{0\}$，则 $\mathrm{N}(uO_F)=|\mathrm{N}(u)|$.

证明 (1) 由于 $\mathrm{N}(IJ)=|O_F/IJ|=|O_F/I|\cdot|I/IJ|$，只需证 $\mathrm{N}(J)=|O_F/J|=|I/IJ|$. 据命题 4.1.4，$I/IJ$ 是 O_F/IJ 的主理想，故存在 $a\in I$ 使得 $aO_F+IJ=I$. 据引理 4.1.1 的(1)，存在 O_F 的理想 K 使得 $aO_F=IK$. 于是 $I(K+J)=I$，从而有 $K+J=O_F$. 令

$$f:\ O_F\rightarrow I/IJ;\ x\mapsto ax\ (\mathrm{mod}\ IJ),$$

则 f 是 O_F-模满同态，且 $x\in\mathrm{Ker}\,f\Leftrightarrow ax\in IJ\Leftrightarrow axO_F=xIK\subseteq IJ\Leftrightarrow xK\subseteq J\Leftrightarrow xO_F=x(K+J)\subseteq J\Leftrightarrow x\in J$. 所以 $\mathrm{Ker}\,f=J$，从而 $O_F/J\simeq I/IJ$，于是 $|O_F/J|=|I/IJ|$.

(2) 据引理 4.4.5，uO_F 是 O_F 的秩为 n 的自由 $\mathbb{Z}$-子模. 由定理 2.6.1，存在 O_F 的 $\mathbb{Z}$-基 $\{w_1,\cdots,w_n\}$ 和 $a_1,\cdots,a_n\in\mathbb{Z}$，使得 $\{a_1w_1,\cdots,a_nw_n\}$ 是 uO_F 的 $\mathbb{Z}$-基，于是 $\mathrm{N}(uO_F)=|O_F/uO_F|=|a_1\cdots a_n|$. 另一方面，$\{uw_1,\cdots,uw_n\}$ 也是 uO_F 的 $\mathbb{Z}$-基，故存在 $\mathbb{Z}$ 上的可逆方阵 S，使得 $\{uw_1,\cdots,uw_n\}=\{a_1w_1,\cdots,a_nw_n\}S=\{w_1,\cdots,w_n\}\mathrm{diag}\{a_1,\cdots,a_n\}S$. 于是 $|\mathrm{N}(u)|=|\det(\mathrm{diag}\{a_1,\cdots,a_n\}S)|=|a_1\cdots a_n|=\mathrm{N}(uO_F)$. □

定理 4.4.9 O_F 的理想类群 $\mathrm{Cl}(O_F)$是有限群.

证明 先证对于每个正数 c，O_F 只有有限个非零理想 I 使得 $\mathrm{N}(I)\leqslant c$. 设 $\mathfrak{p}$ 是 O_F 的非零素理想，其剩余类域 $O_F/\mathfrak{p}$ 是 p^r 元有限域，其中素数 $p\in\mathfrak{p}\cap\mathbb{Z}$. 不难验证 $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$ 是 $\mathbb{Z}$ 的素理

想. 另一方面, 对每个素数 $p\leqslant c$, 由 pO_F 的素理想分解式的唯一性可知, O_F 只有有限个素理想 $\mathfrak{p}$ 使得 $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$, 从而 O_F 只有有限个素理想 $\mathfrak{p}$ 使得 $\mathrm{N}(\mathfrak{p})\leqslant c$. 由于 O_F 的每个非零理想均可唯一地表示成有限个素理想之积, 所以 O_F 只有有限个非零理想 I 使得 $\mathrm{N}(I)\leqslant c$.

再证存在正数 c, 使得 O_F 的每个理想类中含有一个整理想 I 满足 $\mathrm{N}(I)\leqslant c$. 而由上所证, 这样的 I 只有有限个, 所以 O_F 的理想类的个数是有限的, 即 $\mathrm{Cl}(O_F)$是有限群.

因 F 是 $\mathbb{Q}$ 上的 n 次扩域, 且是 $\mathbb{Q}$ 上的可分(分离)扩域, 所以 F 是 $\mathbb{Q}$ 上的单代数扩域. 设 $F=\mathbb{Q}[u]$, $u\in F$, 且设 $u_1=u$, $u_2,\cdots,u_n$ 是 u 的特征多项式的 n 个复根. 任取 O_F 的一个整基 $\{w_1,\cdots,w_n\}$, 可设 $w_i=f_i(u)$, 其中 $f_i(x)\in\mathbb{Q}[x]$. 则 $w_{ij}=f_i(u_j)$, $j=1,2,\cdots,n$, 是 w_i 的特征多项式的 n 个根. 令 $c=\prod\limits_{j=1}^{n}(|w_{1j}|+\cdots+|w_{nj}|)$, 下证 c 即为所需的正数.

设 K 是 O_F 的任一非零理想, 则存在 O_F 的非零理想 J 使得 $KJ=aO_F$, $a\in O_F\backslash\{0\}$. 设正整数 k 使得 $k^n\leqslant\mathrm{N}(J)<(k+1)^n$. 考虑集合 $S=\{k_1w_1+\cdots+k_nw_n\mid k_i\in\mathbb{Z}, 且\ 0\leqslant k_i\leqslant k\}$. 因 $|S|=(k+1)^n>\mathrm{N}(J)=|O_F/J|$, S 中必有两个元素模 J 同余, 从而存在 $\xi=k_1w_1+\cdots+k_nw_n\in J\backslash\{0\}$ 使得 $0\leqslant|k_i|\leqslant k$. 于是存在 O_F 的整理想 I 使得 $\xi O_F=IJ$, 并且 $I=a^{-1}KJI=a^{-1}\xi K\simeq K$. 另一方面

$$\begin{aligned}\mathrm{N}(I)\mathrm{N}(J)=\mathrm{N}(IJ)=\mathrm{N}(\xi O_F)&=|\mathrm{N}(\xi)|\\&\leqslant\prod_{j=1}^{n}|k_1w_{1j}+\cdots+k_nw_{nj}|\\&\leqslant\prod_{j=1}^{n}||k_1||w_{1j}|+\cdots+|k_n||w_{nj}||\\&\leqslant k^nc\leqslant\mathrm{N}(J)c.\end{aligned}$$

所以 $\mathrm{N}(I)\leqslant c$. □

在上述定理的证明中事实上给出了计算 O_F 的理想类群的一个方法.

首先确定一个尽可能小的正数 c，使得 O_F 的每个理想类中均含有一个整理想 I 满足 $\mathrm{N}(I)\leqslant c$. 由代数数论可知，一般地，可取 c 为 Minkovski 常数 M_F，它较上述定理证明中给出的 c 要小得多.

满足 $\mathrm{N}(I)\leqslant c$ 的整理想 I 只有有限个，它们均可唯一地表成有限个素理想之积，而这些素理想均是形如 pO_F 的理想的素理想因子，其中 p 是素数且 $p\leqslant c$(习题 4.4.3). 于是

$$A=\{[\mathfrak{p}]\mid \mathfrak{p}\text{ 是 } pO_F \text{ 的素理想因子，素数 } p\leqslant c\}$$

就是理想类群 $\mathrm{Cl}(O_F)$的生成元集.

当 A 不太大时，考查 A 中元素的乘法关系，就可以确定 $\mathrm{Cl}(O_F)$的阶数和结构.

下面讨论形如 pO_F，p 是素数，的理想的素理想分解问题.

设 p 是素数，将 pO_F 分解成非零素理想之积

$$(*)\qquad pO_F=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g},$$

其中 $\mathfrak{p}_1,\cdots,\mathfrak{p}_g$ 是 O_F 的互不相同的非零素理想，$g\geqslant 1$，$e_i\geqslant 1$，$i=1,\cdots,g$，称 g 为 p 的**分裂次数**，e_i 为 $\mathfrak{p}_i$(关于 p)的**分歧指数**. 因 $p\in\mathfrak{p}_i$，故 $\mathfrak{p}_i\cap\mathbb{Z}=p\mathbb{Z}$. 又由环的单同态 $\mathbb{Z}/p\mathbb{Z}\to O_F/\mathfrak{p}_i$，可视 $O_F/\mathfrak{p}_i$ 为 $\mathbb{Z}/p\mathbb{Z}$ 的有限扩域. 于是 $\mathrm{N}(\mathfrak{p}_i)=|O_F/\mathfrak{p}_i|=p^{f_i}$，$i=1,\cdots,g$. 称 f_i 为 $\mathfrak{p}_i$(关于 p)的**剩余次数**. 将分解式($*$)的两边取范可得 $p^n=\mathrm{N}(\mathfrak{p}_1)^{e_1}\cdots\mathrm{N}(\mathfrak{p}_g)^{e_g}=p^{e_1f_1+\cdots+e_gf_g}$，其中 $n=[F:\mathbb{Q}]$. 这证明了

命题 4.4.10 $e_1f_1+e_2f_2+\cdots+e_gf_g=n$. □

下述定理给出了求 pO_F 的素理想分解式的一个颇为有效的方法.

定理 4.4.11 设 $\alpha\in O_F$ 使得 $F=\mathbb{Q}[\alpha]$，$d(x)\in\mathbb{Z}[x]$是 α

的最小多项式. 则

(1) $\mathbb{Z}[\alpha]$是 O_F 的子环, 且加法商群 $O_F/\mathbb{Z}[\alpha]$是有限群.

(2) 设 p 是素数, $p\nmid|O_F/\mathbb{Z}[\alpha]|$, 且设 $d(x)$在有限域 $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$ 上的多项式环 $\mathbb{Z}_p[x]$中分解成

$$d(x)=d_1(x)^{e_1}\cdots d_g(x)^{e_g}\,(\mathrm{mod}\ p),$$

其中 $d_i(x)$是 $\mathbb{Z}[x]$中的首一多项式, 且看作 $\mathbb{Z}_p[x]$中的元素时是互不相同的不可约多项式. 则

1) $\mathfrak{p}_i=(p,d_i(\alpha))$, $i=1,\cdots,g$, 是 O_F 的g 个互不相同的素理想.

2) pO_F 在 O_F 中的素理想分解式为

$$pO_F=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}.$$

3) $\mathfrak{p}_i$ 关于 p 的剩余次数 $f_i=\deg\,(d_i(x))$, $i=1,\cdots,g$.

证明　(1) 显然 $\mathbb{Z}[\alpha]$是 O_F 的子环, 且是以$\{1,\alpha,\cdots,\alpha^{n-1}\}$为基的自由 $\mathbb{Z}$-模. 由定理 2.6.1, 存在 O_F 的 $\mathbb{Z}$-基$\{w_1,\cdots,w_n\}$和 $a_1,\cdots,a_n\in\mathbb{Z}$, 使得$\{a_1w_1,\cdots,a_nw_n\}$是 $\mathbb{Z}[\alpha]$的 $\mathbb{Z}$-基, 从而$|O_F/\mathbb{Z}[\alpha]|=|a_1\cdots a_n|$是有限的.

(2) 设 $f_i=\deg(d_i(x))$, $i=1,\cdots,g$.

1°　对于每个 i, $(p,d_i(x))$是 $\mathbb{Z}[x]$的极大理想. 这是因为: $d_i(x)$在 $\mathbb{Z}_p[x]$中不可约, 从而 $F_i=\mathbb{Z}_p[x]/(d_i(x))$是 p^{f_i}元有限域. 作环的自然满同态

$$\varphi:\ \mathbb{Z}[x]\to F_i;\ g(x)\mapsto g(x)\ (\mathrm{mod}\ p,d_i(x)).$$

则 $\mathrm{Ker}\,\varphi=(p,d_i(x))$是 $\mathbb{Z}[x]$的极大理想.

2°　对于每个 i, $O_F/\mathfrak{p}_i$ 是 p^{f_i}元有限域, 或者 $\mathfrak{p}_i=O_F$. 这是因为: 作环同态

$$\psi:\ \mathbb{Z}[x]\to O_F/\mathfrak{p}_i;\ f(x)\mapsto f(\alpha)\ (\mathrm{mod}\ \mathfrak{p}_i).$$

由于 $\mathfrak{p}_i=(p,d_i(\alpha))$, 故$(p,d_i(x))\subseteq\mathrm{Ker}\,\psi$. 由 1°, $\mathrm{Ker}\,\psi=(p,d_i(x))$, 或者 $\mathrm{Ker}\,\psi=\mathbb{Z}[x]$. 若能证明 ψ 是满同态, 则 2°得证. 要

证 ψ 是满同态，只需证 $\mathfrak{p}_i+\mathbb{Z}[\alpha]=O_F$，即要证 $pO_F+\mathbb{Z}[\alpha]=O_F$. 由于 $R=O_F/(pO_F+\mathbb{Z}[\alpha])$是 $O_F/\mathbb{Z}[\alpha]$的加法商群，故 $|R|$ 整除 $|O_F/\mathbb{Z}[\alpha]|$；同理，$|R|$ 也整除 $|O_F/pO_F|=p^n$. 由条件 $p\nmid|O_F/\mathbb{Z}[\alpha]|$，所以 $|R|=1$，即 $pO_F+\mathbb{Z}[\alpha]=O_F$，所以 ψ 是满同态.

3° $(\mathfrak{p}_i,\mathfrak{p}_j)=O_F$，$1\leqslant i\neq j\leqslant g$. 这是因为：$d_i(x)$和 $d_j(x)$ 在 $\mathbb{Z}_p[x]$中是不同的不可约多项式，从而存在 $u(x)$，$v(x)\in\mathbb{Z}[x]$使得 $d_i(x)u(x)+d_j(x)v(x)=1(\mathrm{mod}\ p)$，用 α 代入后得 $d_i(\alpha)u(\alpha)+d_j(\alpha)v(\alpha)=1(\mathrm{mod}\ pO_F)$. 于是 $O_F=(p,d_i(\alpha),d_j(\alpha))=\mathfrak{p}_i+\mathfrak{p}_j=(\mathfrak{p}_i,\mathfrak{p}_j)$.

4° 记 $r_i=d_i(\alpha)$，$i=1,\cdots,g$，且记 $I=(p,r_1^{e_1}\cdots r_g^{e_g})$. 则 $pO_F=I\supseteq\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$. 这是因为：由 3°，当 $i\neq j$ 时，$(p,r_i,r_j)=O_F$，从而 $\mathfrak{p}_i\mathfrak{p}_j=(p,r_i)(p,r_j)=(p^2,pr_i,pr_j,r_ir_j)=(p(p,r_i,r_j),r_ir_j)=(p,r_ir_j)$；且有 $\mathfrak{p}_i^2=(p,r_i)^2=(p^2,pr_i,r_i^2)\subseteq(p,r_i^2)$. 进而用归纳法可证，$\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}\subseteq I$. 另一方面，将 α 代入 $d(x)=d_1(x)^{e_1}\cdots d_g(x)^{e_g}(\mathrm{mod}\ p)$，可得 $0=d(\alpha)=r_1^{e_1}\cdots r_g^{e_g}(\mathrm{mod}\ pO_F)$. 从而 $r_1^{e_1}\cdots r_g^{e_g}\in pO_F$，所以 $I\subseteq pO_F$，而反包含是显然的，所以 $pO_F=I$.

5° 由 2°，不妨设 $\mathfrak{p}_1,\cdots,\mathfrak{p}_t$ 是 O_F 的素理想，$O_F/\mathfrak{p}_i$ 是 p^{f_i} 元有限域，而 $\mathfrak{p}_{t+1}=\cdots=\mathfrak{p}_g=O_F$. 由 3°可知 $\mathfrak{p}_1,\cdots,\mathfrak{p}_t$ 是 O_F 的互不相同的素理想. 由 4°可设 $pO_F=\mathfrak{p}_1^{e_1'}\cdots\mathfrak{p}_t^{e_t'}$，$e_i'\leqslant e_i$，$i=1,\cdots,t$. 据命题 4.4.10，得

$$n=e_1'f_1+\cdots+e_t'f_t\leqslant e_1f_1+\cdots+e_tf_t\leqslant e_1f_1+\cdots+e_gf_g.$$

但由分解式 $d(x)=d_1(x)^{e_1}\cdots d_g(x)^{e_g}$ 可知，$n=\deg(d(x))=e_1f_1+\cdots+e_gf_g$，所以 $t=g$ 且 $e_i'=e_i$，$i=1,\cdots,g$. 所以 $pO_F=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_g^{e_g}$. □

设 $\alpha\in O_F$. 若$\{1,\alpha,\cdots,\alpha^{n-1}\}$是 O_F 的 $\mathbb{Z}$-基，叫做 O_F 的**幂元整基**，则 $O_F=\mathbb{Z}[\alpha]$，从而 $|O_F/\mathbb{Z}[\alpha]|=1$. 此时，任意素数 p

均适合上述定理的条件. 这样, pO_F 的素理想分解问题归于 α 的最小多项式在 $\mathbb{Z}_p[x]$ 中的不可约因式分解.

习　题　4.4

以下总设 F 是代数数域, O_F 是 F 的代数整数环.

1. 复数 a 叫做**单位根**, 如果存在 $n\geqslant 1$ 使得 $a^n=1$. 证明: F 中的所有单位根作成一个乘法群, 且是有限循环群.

2. 设 I 是 O_F 的整理想, $\mathrm{N}(I)=g$. 证明: $g\in I$.

3. 设 $\mathfrak{p}\in\operatorname{Spec}O_F$, $\mathfrak{p}\neq 0$. 证明: $\mathfrak{p}$ 是形如 pO_F 的理想的素理想因子, 其中 p 是素数.

4. 设 I 是 O_F 的分式理想. 证明: $I^{-1}=\{a\in F\mid aI\subseteq O_F\}$.

5. 设 $f(x)\in\mathbb{Z}[x]$是首一多项式, 而 $g(x)\in\mathbb{Q}[x]$是 $f(x)$ 的首一多项式因式. 证明: $g(x)\in\mathbb{Z}[x]$.

6. (1)证明: 每个二次代数数域均可表示成 $\mathbb{Q}(\sqrt{d})$, 其中 d 是无平方因数的整数;

(2) 如果 d 和 d' 均是无平方因数的整数, 且 $d\neq d'$, 则 $\mathbb{Q}(\sqrt{d})\neq\mathbb{Q}(\sqrt{d'})$.

7. 设 $F=\mathbb{Q}(\sqrt{d})$是二次代数数域, $d\in\mathbb{Z}$, d 无平方因数. 令

$$w=\begin{cases}\dfrac{1}{2}(1+\sqrt{d}), & \text{当 } d\equiv 1(\operatorname{mod}4)\text{ 时},\\ \sqrt{d}, & \text{当 } d\equiv 2,3(\operatorname{mod}4)\text{ 时}.\end{cases}$$

证明: $\{1,w\}$是 O_F 的一个整基, 从而 $O_F=\mathbb{Z}[w]$.

8. 设 $F=\mathbb{Q}(\sqrt{-5})$. 对于素数 $p=2,3,5,7,11,13$; 试求 pO_F 在 O_F 中的素理想分解式. 再对 $F=\mathbb{Q}(\sqrt{10})$做同样的事情.

9. 试求 $F=\mathbb{Q}(\sqrt{-5})$和 $F=\mathbb{Q}(\sqrt{10})$的理想类群.

10. 设 $\alpha_1,\cdots,\alpha_n\in F$. 记

$$\Delta(\alpha_1,\cdots,\alpha_n)=\det(\mathrm{T}(\alpha_i\alpha_j))\in\mathbb{Q},$$

叫做$\{\alpha_1,\cdots,\alpha_n\}$的**判别式**. 证明:

(1) $\Delta(\alpha_1,\cdots,\alpha_n)\neq 0\Leftrightarrow\{\alpha_1,\cdots,\alpha_n\}$是 $\mathbb{Q}$-线性无关的.

(2) 若 $\alpha_1,\cdots,\alpha_n\in O_F$, 且 $\Delta(\alpha_1,\cdots,\alpha_n)=\mathrm{d}(F)$, 则$\{\alpha_1,\cdots,\alpha_n\}$是 O_F 的整基.

(3) 若 $\alpha_1,\cdots,\alpha_n\in O_F$, 且 $\Delta(\alpha_1,\cdots,\alpha_n)$无平方因数, 则$\{\alpha_1,\cdots,\alpha_n\}$是 O_F 的整基.

［Ｇｅｎｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ］
书名＝交换代数导引
作者＝宋光天
页数＝１４６
ＳＳ号＝１１１０９８６９
出版日期＝２００２年

前言
目录