科学版

研究生教学丛书

交换代数导论

南基洙 王 颖 编著

科学出版社

科学版研究生教学丛书

交换代数导论

南基洙　王　颖　编著

科学出版社

北京

内 容 简 介

在假定读者熟悉群、环、域等抽象代数学基本知识的基础之上，本书用尽可能初等的方式，系统地介绍了交换代数学的基本研究对象和研究方法. 本书共 8 章，分别是环与理想、模、局部化、链条件、整扩张、赋值环、完备化和维数.

本书可以作为高等学校数学专业和相关专业本科高年级学生和研究生的教材，也可以作为中学教师、高校教师和工程技术人员的参考书.

图书在版编目(CIP)数据

交换代数导论/南基洙，王颖编著. —北京：科学出版社，2012
(科学版研究生教学丛书)

ISBN 978-7-03-035367-2

Ⅰ. ①交… Ⅱ. ①南… ②王… Ⅲ. ①交换环-研究生-教材
Ⅳ. ①O187.3

中国版本图书馆 CIP 数据核字(2012) 第 192118 号

责任编辑：王 静 / 责任校对：宋玲玲
责任印制：闫 磊 / 封面设计：陈 敬

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京佳艺恒彩印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2012 年 8 月第 一 版 开本：B5(720 × 1000)
2012 年 8 月第一次印刷 印张：12 3/4
字数：262 000

定价：32.00 元

(如有印装质量问题，我社负责调换)

前　言

源于代数几何和代数数论的交换代数, 无疑是我们学习、研究代数几何和代数数论不可或缺的基础. 它也是我们进一步学习和研究交换代数组合学、有限群表示论和有限群的不变式理论等学科的重要保障.

本书以尽可能简洁、直观的形式, 介绍了交换代数的基本研究对象、研究采用的基本方法, 以及所要研究的基本性质与属性等. 全书共 8 章. 第 1 章介绍环, 与环结构密切相关的理想、特殊元素, 以及理想的运算和准素分解等; 第 2 章介绍模的各种运算、有限生成模, 以及模之间的联络正合列和张量积等; 第 3 章介绍现代数学研究中常用的局部化方法和一些局部化性质; 第 4 章介绍链条件方法和 Gröbner 基; 第 5 章介绍整性质、上升和下降定理, 以及 Hilbert 零点定理; 第 6 章介绍赋值环、Dedekind 整环, 以及分式理想等; 第 7 章介绍环与模的分次结构、完备化方法, 以及 p-adic 数等; 第 8 章则以 Hilbert 多项式为切入点, 介绍环的维数、多项式环和形式幂级数环的维数, 以及正则序列和 Cohen-Macaulay 环等. 依据我们的教学实践, 40 学时左右即可讲授完本书的主要内容.

本书的出版得到了大连理工大学教改基金和教育部高等学校博士学科点专项科研基金 (201101647) 的支持和资助. 本书是在我们多年为数学专业低年级研究生讲授 Atiyah M F 和 MacDonald I G 的名著*Introduction to Commutative Algebra*基础上整理而成的. 当然, 期间还参考了其他许多相关文献和书籍. 例如, Matsumura H 的*Commutative Ring Theory*和 Eisenbud D 的*Commutative Algebra with a View toward Algebraic Geometry* 等. 在整理讲义的过程, 我校数学专业研究生赵辉芳、韦扬江、韩祥、曾玲莉等参加听课的学生提出了诸多的编排、整理和补充内容的建议. 在此向他们表示衷心的感谢! 更要向诸多参考文献的作者和出版社致以由衷的感谢!

受作者水平所限, 书中难免有不妥之处, 敬请读者斧正.

南基洙　王　颖
大连理工大学创新园
2012 年 6 月

目　录

引　言

把代数方程和曲线、曲面等几何对象联系在一起的这个创造, 无疑是数学发展中最丰富、最有效的设想之一. 把代数应用于几何, 强调代数的一般性, 可以非常有效地将推理程序机械化、减少解决问题的工作量.

几何概念可以用代数表示, 几何目标可以通过代数达到; 反过来, 给代数语言以几何解释, 可以更直观地把握那些语言的意义, 同时又可以得到直观启发、提出新的问题和发现新的结论. Lagrange 曾对代数和几何之间的关系作过非常深刻的表述 "只要代数同几何分道扬镳, 它们的进展就缓慢, 它们的应用也就狭窄. 但是, 当这两门科学结成伴侣时, 它们就能彼此吸取养分、取得新鲜的活力, 并以快速的步伐走向完善. "

在代数的帮助下, 不但能够迅速地证明关于几何的事实, 而且这种探索问题的方式, 几乎是自动的. 以代数为工具研究几何对象的性质和结构, 具有巨大的优越性和便利性. 例如, 我们可以非常方便地用线性方程组

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2, \\ \cdots \quad \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

来描述 n 维空间中 m 个平面 (超平面) 交点的分布情况. 我们也可以方便地用向量内积的代数语言表述直线间夹角的几何性质等. 即若令 $\alpha = (x_1, x_2, \cdots, x_n)$, $\beta = (y_1, y_2, \cdots, y_n)$, 则

$$\alpha\beta = x_1y_1 + x_2y_2 + \cdots + x_ny_n = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}\sqrt{y_1^2 + y_2^2 + \cdots + y_n^2}\cos(\alpha, \beta).$$

进一步, 我们知道一元多项式方程

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

勾画了平面上的一条曲线, 而多元多项式方程

$$f(x_1, x_2, \cdots, x_n) = 0$$

则表示 n 维空间中的一个曲面. 于是, 多元多项式方程组

$$\begin{cases} f_1(x_1,x_2,\cdots,x_n)=0, \\ f_2(x_1,x_2,\cdots,x_n)=0, \\ \cdots\ \cdots \\ f_m(x_1,x_2,\cdots,x_n)=0 \end{cases}$$

就描述了 n 维空间中 m 个曲面交点 (线、面) 的分布情况. 因此, 如果用

$$V(f_1,f_2,\cdots,f_m)=\{(x_1,x_2,\cdots,x_n)\in F^n\,|\,f_i(x_1,x_2,\cdots,x_n)=0,1\leqslant i\leqslant m\}$$

表示这些曲面交点的集合, 那么就得到了曲面组和点集合之间的一个对应关系:

$$(f_1,f_2,\cdots,f_m)\to V(f_1,f_2,\cdots,f_m).$$

并且有

$$V(f_1,\cdots,f_k,f_{k+1},\cdots,f_m)=V(f_1,\cdots,f_k)\cap V(f_{k+1},\cdots,f_m)$$

和

$$V(fg)=V(f)\cup V(g),\quad f,g\in F[x_1,x_2,\cdots,x_n].$$

又由于我们不妨视曲面组 $I=(f_1,f_2,\cdots,f_m)$ 为多元多项式环 $F[x_1,x_2,\cdots,x_n]$ 的一个理想, 所以对应关系 $((f_1,f_2,\cdots,f_m)\to V(f_1,f_2,\cdots,f_m))$ 实际上是在理想和点集合之间建立了对应, 同时这种对应也蕴涵着对象间关系之间的联系. 例如, 当多元多项式环 $F[x_1,x_2,\cdots,x_n]$ 的理想之间关系是 $I\subseteq J$ 时, 它们对应的点集合之间的关系为 $V(I)\supseteq V(J)$.

反之, 对于给定的点集合 $V=\{a_1,a_2,\cdots,a_m\}(\subseteq F^n)$, 一定存在一个曲面组

$$I(V)=\{f(x_1,x_2,\cdots,x_n)\in F[x_1,x_2,\cdots,x_n]\,|\,f(a_i)=0,1\leqslant i\leqslant m\},$$

即以点 $a_1,a_2,\cdots,a_m$ 为共同交点的曲面组的集合. 于是, 在点集合和曲面组集合之间也存在着一个对应关系:

$$V\to I(V).$$

而且, 当点集合 $V=S\cup T$ 时, 有

$$I(V)=I(S\cup T)=I(S)\cap I(T).$$

对此, 如果采用的是抽象代数的语言, 那么曲面组集合

$$I(V)=\{f(x_1,x_2,\cdots,x_n)\in F[x_1,x_2,\cdots,x_n]\,|\,f(a_i)=0,1\leqslant i\leqslant m\}$$

就恰好构成了多元多项式环 $F[x_1,x_2,\cdots,x_n]$ 的一个理想. 这就是说, 我们可以在几何对象点集合和代数对象理想之间建立一种对应, 而且这种对应也蕴涵了对象间关系之间的联系. 例如, 当点集合之间的关系是 $S\subseteq T$ 时, 它们对应的理想之间的关系为 $I(S)\supseteq I(T)$.

通过这些简单的分析, 我们知道, 可以在几何对象点集合和代数对象理想之间建立对应, 并且这种对应可以把代数对象 (理想) 之间的关系转化为几何对象之间的关系. 反之, 它也可以把几何对象之间的关系转化为代数对象 (理想) 之间的关系.

$$F : G = \{\text{几何对象}\} \rightleftarrows A = \{\text{代数对象}\}$$

$$g \rightleftarrows F(g) \in A$$

$$\text{几何对象之间关系}\,(g, g') \rightleftarrows \text{代数对象之间关系}\,(F(g), F(g'))$$

那么, 基于这样一些认识, 我们就有充分的理由将几何对象之间的关系转化为代数对象之间的关系, 然后利用抽象代数作工具, 来刻画代数几何对象的性质与结构. 就如同我们在线性代数中为刻画点、线、面的关系来锻造矩阵代数一样, 描述曲线、曲面之间关系的需求, 催生和促进了交换代数中环、理想、理想分解、相关性和维数等理论的产生和发展. 交换代数的产生和发展得益于代数几何, 同时它也是进一步学习和研究代数几何的重要基础.

交换代数产生和发展的另一个重要源头是代数数论. 无疑, Fermat 猜想是数论研究中十分引人瞩目的一个猜想 ($x^n + y^n = z^n (n > 2)$, 没有非平凡整数解. 在 1995 年英国数学家 Andrew John Wiles 和 Richard Taylor 证明了该猜想). 为解决 Fermat 猜想, 人们提出了一个巧妙而又自然的想法: 如果令 ζ 是一个 n 次本原单位根, 那么

$$x^n - z^n = \prod_{i=0}^{n-1} \left(x - \zeta^i z\right) = y^n.$$

从而, 若再能有 Gauss 整环 $Z[\zeta]$ 是唯一分解环的话, 那么 Fermat 猜想就解决了. 但是, 非常遗憾, 并不是对于所有的整数 n, 我们都能保证 Gauss 整环 $Z[\zeta]$ 具有唯一分解性. 例如当 $n = 23$ 时, Gauss 整环 $Z[\zeta]$ 就不是一个唯一分解环.

为了解决 Gauss 整环 $Z[\zeta]$ 的唯一分解性及其关联性问题, Dedekind 创造了理想数 (理想)、Lasker 则创立准素分解等诸多新的概念、方法和理论. 在 20 世纪初, Noether 将这些理论作了统一的公理化整理和发展. 这些思想和方法都极大地推进了数论研究, 同时也促成了交换代数的产生和发展.

事实上, 交换代数主要是以代数几何和代数数论为背景产生和发展的. 正是由于交换代数与代数几何和代数数论的渊源, 交换代数中几乎所有的概念、方法和结论等都可以在代数几何或代数数论中觅得踪迹. 但是, 它在为代数几何和代数数论提供新的、统一工具的同时, 交换代数本身也逐步成长壮大、发展成为一门独立的数学分支, 并成为学习和从事现代数学研究必不可少的基础理论之一.

第1章 环与理想

环与理想理论是学习交换代数的首要基础. 在本章之中, 我们将简单回顾和介绍环与理想的一些基本概念和重要结论.

1.1 环与子环

定义 1.1.1 令 R 是有两个运算 "$+,\cdot$"(加法、乘法) 的集合, 如果它满足:

(1) $\{R;+\}$ 是交换群,

(2) 乘法运算 "$\cdot$" 适合结合律, 即 $(a\cdot b)\cdot c=a\cdot(b\cdot c)$, $\forall a,b,c\in R$,

(3) 乘法对加法适合分配律, 即对于 $\forall a,b,c\in R$, 有

$$a\cdot(b+c)=a\cdot b+a\cdot c \text{ 和 } (b+c)\cdot a=b\cdot a+c\cdot a,$$

则称代数体系 $\{R;+,\cdot\}$ 是环, 简称 R 是环.

习惯上, 直接用 0 表示环 R 中加法群的单位元素, 并用 $-a$ 表示元素 a 关于加法群的逆元素, 即 $a+0=0+a=a, a-a=0$, $a\in R$. 也直接用 ab 表示乘法 $a\cdot b$.

进一步, 如果环 R 还满足: $ab=ba, a,b\in R$, 则称 R 是交换环. 如果环 R 中存在关于乘法运算的单位元素 e, 即 $ea=a$, $\forall a\in R$, 则称 R 是有 1 的环. 习惯上, 直接用 1 表示关于乘法运算的单位元素.

也可以将有 1 的环定义成, 使其存在的单位元素 e 满足 $ae=a$, $\forall a\in R$. 容易验证, 这样的两种定义方式是一样的.

事实上, 若令 e_1 满足 $e_1a=a$, e_2 满足 $ae_2=a$, 则

$$e_1=e_1e_2=e_2.$$

注意, 在环的定义中并没有说 $1\neq 0$. 但是, 如果在环 R 中有 $1=0$, 则

$$r=r1=r0=0,\quad \forall r\in R,$$

即环 R 中只有一个元素 0—— 零环. 所以, 如果没有特别说明的话, 以后我们所说的环都指的是非零环, 即在环 R 中有 $1\neq 0$. 另外, **如果没有特别说明的话, 以后我们所指的环都要求是有 1 的、交换的、非零环.**

实际上, 如果环 R 是没有 1 的环, 那么我们很容易将其嵌入一个有 1 的环之中. 例如, 利用环 R 和整数 Z, 可以先构造一个集合 $R\times Z$, 然后规定其中的运算为

$$(r,n)+(s,m)\overset{\text{定义}}{=\!=}(r+s,n+m),$$
$$(r,n)(s,m)\overset{\text{定义}}{=\!=}(rs+ns+mr,nm),$$

那么, 易见集合 $R\times Z$ 在这样规定的运算之下构成一个环, 并且其中 1 为 $(0,1)$. 当然, 其间的嵌入映射为

$$\lambda: R\to R\times Z$$
$$r\to(r,1).$$

令 R 是一个环, 则易知环的运算满足下面的一些简单性质:

(1) $0a=0,\forall a\in R$,

(2) $(-a)\,b=-(ab)\,,a,b\in R$,

(3) $a(b-c)=ab-ac,a,b,c\in R$.

在此, 我们仅考证结果 (1).

事实上, 因为 $0a=(0+0)\,a=0a+0a$, 所以 $0a=0$.

例 1.1.1 我们熟知的整数 Z 在通常的加法和乘法运算之下就是一个环. 另外, 如有理数集 Q、实数集 R 和复数集 C 等在通常的加法和乘法运算之下也都是环. 再有, 这些环上的多项式 $Z[x]=\{a_nx^n+\cdots+a_1x+a_0\,|a_i\in Z,0\leqslant i\leqslant n,n\geqslant 0\}$, $Q[x]$, $R[x]$ 和 $C[x]$ 等也均是环.

一般地, 若令 R 是一个环, $x\notin R$ 是一未定元, 则可以构作一个集合

$$R[x]=\{a_nx^n+\cdots+a_1x+a_0\,|a_i\in R,0\leqslant i\leqslant n\,,0\leqslant n\in Z\}\,.$$

并规定 $f(x),g(x)\in R[x]$ 相等的充分必要条件是它们对应项的系数全相等, 即若令

$$f(x)=a_nx^n+\cdots+a_1x+a_0,\quad g(x)=b_mx^m+\cdots+b_1x+b_0,$$

则 $f(x)=g(x)\Leftrightarrow n=m,a_i=b_i,0\leqslant i\leqslant n$.

进一步, 在集合 $R[x]$ 中我们就按熟知的方式, 定义 "加法、乘法", 即

(1) $f(x)+g(x)=\sum\limits_{k=0}^{\max\{n,m\}}(a_k+b_k)x^k$, 当 $k>n$ 或 $k>m$ 时, 规定 $a_k=0$ 或 $b_k=0$,

(2) $f(x)g(x)=\sum\limits_{k=0}^{n+m}c_kx^k$, 其中 $c_k=\sum\limits_{i+j=k}a_ib_j$,

则容易验证,$(R[x];+,\cdot)$ 构成一个环, 我们将其称之为环 R 上的多项式环. 将此方法自然拓展, 可以定义 n 元多项式环 $R[x_1,\cdots,x_n]$.

类似地, 若令 R 是一个环, $x \notin R$ 是一未定元, 则可以定义一个形式幂级数集合

$$R[[x]] = \{a_0 + a_1x + \cdots + a_nx^n + \cdots | a_i \in R, i \geqslant 0\}.$$

并且, 规定 $f(x), g(x) \in R[[x]]$ 相等的充分必要条件是它们对应项的系数全相等, 即若令

$$f(x) = a_0 + a_1x + \cdots + a_nx^n + \cdots, \quad g(x) = b_0 + b_1x + \cdots + b_mx^m + \cdots,$$

则 $f(x) = g(x) \Leftrightarrow a_i = b_i, i \geqslant 0$.

然后, 在 $R[[x]]$ 中按如下方式定义加法和乘法:

(1) $f(x) + g(x) = \sum\limits_{k=0}^{\infty}(a_k + b_k)x^k$,

(2) $f(x)g(x) = \sum\limits_{k=0}^{\infty} c_kx^k$, 其中 $c_k = \sum\limits_{i+j=k} a_ib_j$,

则容易验证,$(R[[x]]; +, \cdot)$ 构成环, 我们称其为环 R 上的形式幂级数环.

例 1.1.2　令 R 是一个环, 则其上的 n 阶矩阵集合

$$M_n(R) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} | a_{ij} \in R,\ 1 \leqslant i, j \leqslant n \right\}$$

在通常的矩阵加法和乘法运算之下构成一个环 ——n 阶矩阵环 (非交换环). 其上的零元素 (加法单位元) 和 1(乘法单位元), 分别为

$$\begin{pmatrix} 0 & & \\ & \ddots & \\ & & 0 \end{pmatrix} \text{ 和 } \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}.$$

例 1.1.3　令 Z_n 是模 n 的剩余类集合, 即 $Z_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$, 其中 $\bar{i} = \{kn + i | k \in Z\}$, $0 \leqslant i \leqslant n-1$. 我们规定

$$\bar{i} + \bar{j} = \overline{i+j}, \quad \bar{i} \cdot \bar{j} = \overline{ij},$$

则容易验证, $\{Z_n; +, \cdot\}$ 是一个环 —— 模 n 的剩余类环.

定义 1.1.2　令 R 是一个环, S 是环 R 的子集合. 如果集合 S 在环 R 的运算之下构成环, 则称 S 是 R 的子环, 并记其为 $S \subseteq R$.

显然, 环 R 存在两个自然的子环 $\{0\}$ 和 R. 我们称这两个子环是平凡的. 以后, 如果没有特别的说明, 我们所说的子环都要求是非平凡的子环.

例 1.1.4 显然 $Z \subseteq Q \subseteq R \subseteq C$. 如果 R 是一个环, 则 $R \subseteq R[x]$.

例 1.1.5 令下三角矩阵集合为

$$L_n(R) = \left\{ \begin{pmatrix} a_{11} & & \\ \vdots & \ddots & \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} | a_{ij} \in R,\ 1 \leqslant i,j \leqslant n \right\},$$

则容易验证, 在矩阵的加法和乘法运算下, $L_n(R) \subseteq M_n(R)$.

类似地, 有上三角矩阵子环

$$U_n(R) = \left\{ \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \ddots & \vdots \\ & & a_{nn} \end{pmatrix} | a_{ij} \in R,\ 1 \leqslant i,j \leqslant n \right\} \subseteq M_n(R)$$

和对角矩阵子环

$$\mathrm{diag}_n(R) = \left\{ \begin{pmatrix} a_{11} & & \\ & \ddots & \\ & & a_{nn} \end{pmatrix} | a_{ii} \in R, 1 \leqslant i \leqslant n \right\} \subseteq M_n(R).$$

定理 1.1.1 令 R 是一个环, S 是环 R 的子集合, 则 S 是子环的充分必要条件是它满足:

(1) $1 \in S$,

(2) 对于 $\forall a,b \in S$, 有 $a+b \in S$,

(3) 对于 $a \in S$, 有 $-a \in S$,

(4) 对于 $\forall a,b \in S$, 有 $ab \in S$.

证明 利用子环的定义即可. □

不难看出, 如果 A,B 都是环 R 的子环, 则 $A \cap B$ 也是环 R 的子环. 但是 $A \cup B$ 不一定是子环. 例如, $R[x], R[y]$ 都是 $R[x,y]$ 的子环, 但是, 对于 $x,y \in R[x] \cup R[y]$, 却显然有 $x+y \notin R[x] \cup R[y]$, 所以 $R[x] \cup R[y]$ 不是 $R[x,y]$ 的子环.

例 1.1.6 令 $Z[\mathrm{i}] = \{a+b\mathrm{i} \,|\, a,b \in Z\}$, 则 $Z[\mathrm{i}]$ 当然是复数集 C 的子集合. 另外, 容易验证它适合定理 1.1.1, 所以 $Z[\mathrm{i}]$ 是复数集 C 的子环 ——Gauss 型环.

例 1.1.7 令 $S \subseteq R$ 是一个子环,$\alpha \in R$, 则易知

$$S[\alpha] = \left\{ \sum_{i=0}^{n} s_i \alpha^i \,|\, s_i \in S, 0 \leqslant i \leqslant n, n \geqslant 0 \right\}$$

是环 R 的一个子环 (请与例 1.1.1 比较一下). 类似地, 如果 M 是环 R 的子集合, 则 $S[M] \subseteq R$. 我们称 $S[M]$ 是由子环 S 和集合 M 生成的子环. 容易证明

$$S[M \cup N] = (S[M])[N].$$

而且, 我们有

$$S[T]=\bigcap_{i\in I}S_i,$$

其中 $S_i, i\in I$, 是所有包含子环 S 和集合 T 的子环.

事实上, 显然有 $S[T]\subseteq\bigcap\limits_{i\in I}S_i$. 另外一方面, $S[T]$ 本身就是一个子环, 所以当然有 $S[T]\supseteq\bigcap\limits_{i\in I}S_i$. 因此, $S[T]=\bigcap\limits_{i\in I}S_i$.

这就是说, $S[T]$ 是包含子环 S 和集合 T 的最小的环 R 的子环.

1.2　同态与理想

定义 1.2.1　令 R,R' 是环, 如果存在一个映射 $\varphi: R\to R'$, 并且该映射保持环中运算, 即

$$\begin{aligned}\varphi(a+b)&=\varphi(a)+\varphi(b),\\ \varphi(ab)&=\varphi(a)\varphi(b),\\ \varphi(1_R)&=1_{R'},\end{aligned}$$

其中 $a,b\in R$,1_R 是环 R 的 1,$1_{R'}$ 是环 R' 的 1, 则称映射 φ 是环 R,R' 之间的同态. 如果 R,R' 之间存在同态, 则称环 R 与 R' 同态, 记为 $R\sim R'$.

特别地, 若同态映射 φ 是满射、单射和双射, 则称环 R 与 R' 为满同态、单同态和同构. 如果环 R 与 R' 同构, 则将其记为 $R\cong R'$.

例 1.2.1　令 R 是环, 则易知映射

$$\begin{aligned}\varphi: R[x]&\to R\\ f(x)&\to f(0)\end{aligned}$$

是环的满同态.

实际上, 通常的取值映射就是一个环同态

$$\begin{aligned}\varphi: R[x]&\to R\\ f(x)&\to f(r),\end{aligned}$$

其中 $r\in R$.

例 1.2.2　令 R 是环, 则易知映射

$$\lambda: L_n(R)\to M_n(R)$$

$$\begin{pmatrix}a_{11}&&\\ \vdots&\ddots&\\ a_{n1}&\cdots&a_{nn}\end{pmatrix}\to\begin{pmatrix}a_{11}&&\\ \vdots&\ddots&\\ a_{n1}&\cdots&a_{nn}\end{pmatrix}$$

是环的单同态.

类似地, 映射

$$\lambda : R \to M_n(R)$$
$$r \to \begin{pmatrix} r & & \\ & \ddots & \\ & & r \end{pmatrix}$$

也是环的单同态.

例 1.2.3 令映射为

$$\varphi : Z \to Z_n$$
$$m \to \bar{m},$$

则容易验证, 这个映射是整数环 Z 和剩余类环 Z_n 之间的满同态.

例 1.2.4 令 R 是环, 则映射

$$\lambda : Z \to R$$
$$n \to n1_R$$

是环同态. 进一步, 从整数环 Z 至任意环 R 的同态一定具有上面的形式, 即 Z 至环 R 的同态是唯一的.

事实上, 若 $\varphi : Z \to R$ 是环同态, 则 $\varphi(1) = 1_R$, 所以

$$\varphi(n) = \varphi\left(\overbrace{1 + \cdots + 1}^{n}\right) = \overbrace{\varphi(1) + \cdots + \varphi(1)}^{n} = n\varphi(1) = n1_R = \lambda(n),$$

即 $\varphi = \lambda$.

定义 1.2.2 令 I 是环 R 的关于加法运算的子群, 如果对于任意 $r \in R$, 有 $rI \subseteq I (Ir \subseteq I)$, 则称 I 是环 R 的左 (右) 理想. 如果 I 既是左理想, 又是右理想, 则称 I 是环 R 的理想.

显然, 若 R 是交换环, 则其左 (右) 理想都是理想.

例 1.2.5 令 R 是整数环 Z, 则在矩阵环 $M_2(Z)$(非交换) 中,

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} | a, b \in Z \right\}$$

就是一个左理想, 但不是右理想.

显然, 对于环 R 存在两个当然的理想 $0, R$, 我们称这两个理想是平凡的. 一般地, **以后如果没有特别的说明, 我们所说的理想均指的是非平凡的**. 再有, 如果 R 是一个交换环, 并且 $s \in R$, 则容易验证

$$I = \{rs | \forall r \in R\}$$

是环 R 的一个理想 —— 主理想. 更一般地, 若令 S 是交换环 R 的一个子集合, 则对象

$$I=\left\{\sum_{i\in J}r_is_i\,|r_i\in R,s_i\in S,i\in J\right\}$$

是环 R 的一个理想. 我们称这样的理想是由集合 S 生成的, 记为 $I=(S)$(或 $\langle S\rangle$).

定义 1.2.3　令 I 是环 R 的一个理想, 如果存在一个集合 S, 使得 $I=(S)$, 则称 I 是由 S 生成的, 并称 S 是理想 I 的生成集. 特别地, 如果 $|S|<\infty$, 则称 I 是有限生成理想. 如果 $|S|=1$, 则称 I 是主理想.

注意, 对于任意理想 I 来说, 其生成集一定存在. 例如, $I=(I)$. 但是, 一般地, 我们所说的生成集都是指极小生成集, 即 $I=(S)$, 但是 $I\neq(S\backslash\{x\}),x\in S$.

由于任意两个理想的交是理想, 即若 I,J 是环 R 的理想, 则 $I\cap J$ 是环 R 的理想. 所以, 由一个集合 S 生成的理想 (S) 就恰好是环 R 中包含 S 的所有理想的交. 也就是说, 理想 (S) 是包含 S 的极小理想, 即 $(S)=\bigcap\limits_{S\subseteq I\subseteq R}I$.

定理 1.2.1　令 I 是环 R 的一个子集合, 则 I 是 R 的理想的充分必要条件是它满足:

(1) 对于 $\forall a,b\in I$, 有 $a-b\in I$,

(2) 对于 $\forall r\in R$ 和 $\forall a\in I$, 有 $ra\in I$.　□

例 1.2.6　易知 $nZ=\{nk|k\in Z\}(n\neq 1)$ 是整数环 Z 的理想, 但是因为 $1\notin nZ$, 所以 nZ 不是子环 (我们要求的环都是有 1 的!).

例 1.2.7　令 R 是环, 则矩阵环 $M_n(R)$ 中理想 (既左且右) 的形式为

$$M_n(I)=\left\{(a_{ij})_{n\times n}\,|a_{ij}\in I\right\},$$

其中, I 是环 R 的理想.

证明　首先, 如果 I 是环 R 的理想, 则 $M_n(I)$ 显然是矩阵环 $M_n(R)$ 的理想.

其次, 如果 J 是矩阵环 $M_n(R)$ 的理想, 则考察集合

$$I=\left\{x\in R\,\middle|\,x=a_{11},(a_{ij})_{n\times n}\in J\subseteq M_n(R)\right\}.$$

那么由于

$$\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\vdots\\ a_{n1}&\cdots&a_{nn}\end{pmatrix}-\begin{pmatrix}b_{11}&\cdots&b_{1n}\\ \vdots&&\vdots\\ b_{n1}&\cdots&b_{nn}\end{pmatrix}=\begin{pmatrix}a_{11}-b_{11}&\cdots&a_{1n}-b_{1n}\\ \vdots&&\vdots\\ a_{n1}-b_{n1}&\cdots&a_{nn}-b_{nn}\end{pmatrix},$$

$$\begin{pmatrix}r&&\\ &\ddots&\\ &&r\end{pmatrix}\begin{pmatrix}a_{11}&\cdots&a_{1n}\\ \vdots&&\vdots\\ a_{n1}&\cdots&a_{nn}\end{pmatrix}=\begin{pmatrix}ra_{11}&\cdots&ra_{1n}\\ \vdots&&\vdots\\ ra_{n1}&\cdots&ra_{nn}\end{pmatrix},$$

所以, 由定理 1.2.1 知道 I 是环 R 的理想.

最后, 我们指出: $J=M_n(I)$. 事实上, 只要指出: 当 $(a_{ij})_{n\times n}\in J$ 时, 有 $a_{ij}\in I$ 即可. 而这点可以由下面的矩阵变换确定:

$$\begin{pmatrix} 0 & & 1 & \\ & E & & \\ 1 & & 0 & \\ & & & E \end{pmatrix}\begin{pmatrix} * & \cdots & * \\ \vdots & a_{ij} & \vdots \\ * & \cdots & * \end{pmatrix}\begin{pmatrix} 0 & & 1 & \\ & E & & \\ 1 & & 0 & \\ & & & E \end{pmatrix}=\begin{pmatrix} a_{ij} & \cdots & * \\ \vdots & & \vdots \\ * & \cdots & * \end{pmatrix}.$$

例 1.2.8 令 R,R' 是环, 如果 $\varphi:R\to R'$ 是环同态, 则

$$\ker\varphi=\{r\in R\,|\varphi(r)=0\}\ (\text{称为核})$$

是环 R 的理想. 也就是说, 若有环同态, 则一定存在一个理想.

事实上, 令 $a,b\in\ker\varphi, r\in R$, 则

$$\varphi(a-b)=\varphi(a)-\varphi(b)=0-0=0,\quad \varphi(ra)=\varphi(r)\varphi(a)=\varphi(r)0=0,$$

即 $a-b, ra\in\ker\varphi$. 所以, 由定理 1.2.1 知道 $\ker\varphi$ 是环 R 的理想.

另外, 如果令 I 是环 R 的理想, 则一定存在一个环的自然同态

$$\begin{aligned}\pi: R&\to R/I\\ r&\to r+I,\end{aligned}$$

其中, $R/I=\{r+I\,|r\in R\}$, 并且 $\ker\pi=I$.

事实上, R/I 是一个环 —— 称为商环. 规定其中的运算为

$$(a+I)+(b+I)\overset{\text{定义}}{=\!=}(a+b)+I,$$

$$(a+I)(b+I)\overset{\text{定义}}{=\!=}ab+I,$$

而且, 其中的零元素是 $0+I=I$, 单位元素 1 为 $1+I$.

定理 1.2.2 (第一同构定理) 令 R,R' 是环, 如果 $\varphi:R\to R'$ 是环同态, 则

$$R/\ker\varphi\cong\operatorname{Im}\varphi\subseteq R',$$

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & \operatorname{Im}\varphi\subseteq R' \\ {\scriptstyle\pi}\downarrow & \nearrow & \\ R/\ker\varphi & & \end{array}$$

其中, 自然同态为 $\pi:R\to R/\ker\varphi, r\to r+\ker\varphi$.