交换代数基础

冯克勤

高等教育出版社

交换代数基础

冯克勤

高等教育出版社

1985

内 容 提 要

交换代数是研究交换环的一门代数学科，它以代数数论和代数几何为背景，又为这两门学科提供重要的工具。本书讲述了交换代数的基本理论和方法，其内容基本上是经典的，但叙述的方法是现代的，即突出模论和局部化方法。为了阐明交换代数与代数数论、代数几何的关系，本书第六章充分介绍了代数簇和代数整数环的初步知识。

本书文字流畅，条理清晰，论证详细。并附有相当的习题。

本书经高等学校理科数学、力学教材编委会审定，可用作数学系高年级学生选修课教材和研究生基础课教材。本书也可供数学工作者，特别是代数学、代数数论及代数几何工作者参考。

交 换 代 数 基 础

冯 克 勤

*

高等教育出版社出版

新华书店北京发行所发行

二二〇七工厂印装

*

开本850×1168 1/32 印张 8.875 字数 210,000

1986年5月第1版 1986年5月第1次印刷

印数 00,001—7,220

书号 13010·01178 定价 1.80 元

前　言

交换代数是研究交换环的一门代数学科．它的现代形式和作为一门独立的学科虽然只有三十余年的历史，但是它的起源要上溯到一百年前，交换代数以两门古老的数学分支——代数数论和代数几何为背景产生和发展起来，同时也为这两个学科的进一步研究工作提供了不可缺少并且富有成效的代数工具．

大家知道，古典数论(即初等数论)的主要课题是研究整数的性质和方程(组)的整数解．十八世纪末和十九世纪初，Gauss 在研究二次和四次互反律、二平方和和二元二次型等问题时，运用了二次数域和它的代数整数环．到了十九世纪中期，Kummer 研究著名的 Fermat 猜想时，也把 Fermat 方程 $x^n+y^n=z^n$ 放到分圆域的代数整数环上来研究．这就开创了数论研究的一个新的历史时期，将研究对象从有理数域 **Q** 和有理整数环 **Z** 扩展到任意代数数域 K(即 **Q** 的有限次扩域)和它的代数整数环 O_K 上．经过 Dedekind 等人的系统化，建立了理想、模和(现在被称为) Dedekind 整环等概念，从而出现了一门新的学科——代数数论．到 Hilbert 1897 年发表著名的数论报告(Zahlen bericht)，代数数论完成了它的第一阶段．代数数论的这一阶段的历史就是以代数整数环为具体模型研究 Dedekind 整环的历史．

比数论稍晚些时候，几何学也经历了代数化的过程．大家知道，古典几何是研究任意代数方程组的实数解或复数解的性质的一门学科．在 Riemann 和 Weierstrass 所生活的那个时代，解析方法占据统治地位 (Riemann 面上的解析函数和幂级数展开)．Riemann 去世后，M. Noether，Clebsch 等人以及意大利学派发展了纯几何方法．到了十九世纪末，由于 Dedekind 和 Weber 的工作，把代数函数论建立在与代数数论统一的基础之上，1893 年

Hilbert 建立了零点定理，不久 Lasker 建立了代数簇与多项式理想之间的对应关系. 本世纪二十至三十年代，德国女数学家 E. Noether 关于一般交换环上准素分解的工作,以及三十年代 Krull 建立了赋值论、局部环理论和维数理论. 这一切使古典几何建立在坚实的代数基础之上,形成了代数几何这一学科.

正是在代数数论和代数几何的发展和需要的刺激下，交换代数作为它们共同的代数基础逐渐形成一门独立学科. 到了本世纪五十年代,同调代数的出现把对于环的研究又推到一个新的阶段. 在那以后，交换代数具有许多新的特点. 例如：模论起着愈来愈重要的作用，局部化方法和从局部把握整体的原则变成起主导作用的方法和原则. 目前交换代数已经成为从事代数研究工作所不可缺少的一门基础学科.

在这个讲义中，我们讲述交换代数的基本理论和方法. 其内容基本上是经典的,但是叙述方法是现代的,即我们突出模论和局部化方法. 具体说来，我们在第一章简单地介绍交换环的一般性质之后,第二章讲述模论的基本知识,第三章讲述局部化方法. 随后讲述几种类型的交换环(第四章和第五章)，特别是介绍了作为代数几何基础的 Noether 环和作为代数数论基础的 Dedekind 整环. 为了避免读者浮于空泛的概念之上，我们在第六章介绍代数几何和代数数论的基本内容. 主要目的是试图阐明在前五章中所讲述的交换代数知识和方法是如何以代数几何和代数数论为背景并为它们提供有效的代数工具的. 最后一章介绍分次环、维数理论和完备化方法. 本书个别地方需要域论的一些简单知识. 为了方便读者，我们将关于域的扩张的某些事实写成一个附录放在书末,供读者参考.

本书是作为高等学校数学系代数专业高年级学生选修课和研究生基础课一学期用（每周 3—4 学时）教材而编写的. 假定读者熟悉近世代数中群、环、域基本知识和以同态定理为核心的近世代

数基本方法和技巧. 第七章最后一节需要关于点集拓扑的初步知识. 如果授课时间不够,可以只讲前六章,并且第六章也可酌情删减.

本书是作者于1982年和1983年为中国科学技术大学数学系高年级学生和研究生讲授代数数论和交换代数的基础上写成的. 聂灵沼教授仔细看过原稿,丁石孙教授也提了中肯的建议,刘绍学教授一直关心此书的出版,作者向他们表示谢意. 作者十分希望听到各方面的意见,以便今后将此书作进一步的改进和完善.

主要参考书:

[1] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra* Addison-Wesley Pub. Company, 1969.(有中译本,科学出版社,1982.)

[2] N. Bourbaki, *Commutative Algebra,* Addison-Wesley Pub. Company. (英译本,1972.)

一九八四年春, 于合肥

目　录

第一章　交换环和它的某些性质

我们假定读者在近世代数课程中已经学过环的基本知识，如环的定义，子环，理想，商环，环的同态和同构，环的同态基本定理，环的直和，中国剩余定理，多项式环，主理想环以及唯一因子分解整环等等，在这一章里我们简要地介绍交换环的某些性质，其目的主要是明确我们在本书中采用的一些术语，同时也介绍某些新知识(素理想和极大理想，理想的扩张和限制，环的大根与小根等).

如不声明，本书中的环均指是具有幺元素的交换环.

§ 1.1　理想的运算

设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是环 R 的理想，则

$$\mathfrak{a}+\mathfrak{b}=\{a+b \mid a\in\mathfrak{a}, b\in\mathfrak{b}\}$$

也是环 R 的理想，叫作是理想 $\mathfrak{a}$ 和 $\mathfrak{b}$ 的**和**. 这也是环 R 中同时包含 $\mathfrak{a}$ 和 $\mathfrak{b}$ 的最小理想. 如果 $\mathfrak{a}+\mathfrak{b}=R$，则称理想 $\mathfrak{a}$ 与 $\mathfrak{b}$ **互素**. 类似地，对于环 R 的任意一个理想族 $\mathfrak{a}_i(i\in I)$，其中 I 可以是有限或无限集合，则定义它们的和为

$$\sum_{i\in I}\mathfrak{a}_i=\left\{\sum_{i\in I}a_i \mid a_i\in\mathfrak{a}_i(i\in I)\text{，并且只有有限个 } a_i\neq 0\right\}.$$

这是环 R 中包含所有 $\mathfrak{a}_i(i\in I)$的最小理想.

另一方面，对于环 R 的任意理想族 $\mathfrak{a}_i(i\in I)$，它们的(集合论的)交 $\bigcap_{i\in I}\mathfrak{a}_i$ 是 R 的理想，叫作是诸理想 $\mathfrak{a}_i(i\in I)$的**交**. 它显然是包含在每个理想 $\mathfrak{a}_i(i\in I)$之中的最大理想.

设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是环 R 的两个理想，集合

$$\mathfrak{a}\mathfrak{b}=\left\{\text{有限和}\sum_i a_ib_i \mid a_i\in\mathfrak{a}, b_i\in\mathfrak{b}\right\}$$

也是环 R 的理想，叫作是理想 $\mathfrak{a}$ 与 $\mathfrak{b}$ 的积．由于 R 是交换环，容易推得理想的积运算满足交换律，即 $\mathfrak{ab}=\mathfrak{ba}$．并且，任意有限多个理想 $\mathfrak{a}_1,\mathfrak{a}_2,\cdots,\mathfrak{a}_n$ 的乘积是

$$\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n=\left\{\text{有限和}\sum_i a_{1i}a_{2i}\cdots a_{ni}\,\middle|\,a_{ji}\in\mathfrak{a}_j(1\leqslant j\leqslant n)\right\}.$$

特别地．对于理想 $\mathfrak{a}$ 可以定义它的幂 $\mathfrak{a}^n=\mathfrak{aa}\cdots\mathfrak{a}$（$n$ 个），而规定 $\mathfrak{a}^0=R$．

易知 $\mathfrak{ab}\subseteq\mathfrak{a}\cap\mathfrak{b}$，但是反过来则不一定成立（见习题 5）．

设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是环 R 的两个理想，定义 $\mathfrak{a}$ 对于 $\mathfrak{b}$ 的**商**为

$$(\mathfrak{a}:\mathfrak{b})=\{x\in R\mid x\mathfrak{b}\subseteq\mathfrak{a}\},$$

其中 $x\mathfrak{b}=\{xb\mid b\in\mathfrak{b}\}$．易知 $(\mathfrak{a}:\mathfrak{b})$ 是 R 的理想，而当 $\mathfrak{a}$ 或 $\mathfrak{b}$ 是主理想时，即 $\mathfrak{a}=(a)=aR$，$\mathfrak{b}=(b)=bR$（$a,b\in R$）时，我们也记成

$$(a:\mathfrak{b})=((a):\mathfrak{b}),\quad(\mathfrak{a}:b)=(\mathfrak{a}:(b)).$$

特别地，

$$(0:\mathfrak{b})=\{x\in R\mid x\mathfrak{b}=(0)\}=\{x\in R\mid bx=0,\text{ 对每个 }b\in\mathfrak{b}\}.$$

我们把 $(0:\mathfrak{b})$ 叫作是 $\mathfrak{b}$ 的**零化理想**，并且表示成 $\mathrm{Ann}(\mathfrak{b})$．而对环 R 中的每个元素 a，a 的零化理想即指为主理想 $(a)=aR$ 的零化理想，记成 $\mathrm{Ann}(a)$．于是

$$\mathrm{Ann}(a)=(0:a)=\{x\in R\mid xa=0\}.$$

如果 $\mathrm{Ann}(a)\neq(0)$，我们称 a 是环 R 中的一个**零因子**．换句话说，a 是环 R 的零因子，当且仅当存在 R 中非零元素 b，使得 $ab=0$．对于每个非零环 R（即 $R\neq(0)$），0 显然是一个零因子，如果环 $R\neq(0)$ 并且没有 0 以外的零因子，我们便称 R 是一个**整环**．

以上我们介绍的理想之间的运算（和，交，积，商）均是同一个环 R 内理想之间的运算．现在谈不同环中理想之间的运算：理想的扩张和限制．设 A 和 B 是两个环，$f:A\to B$ 是环的同态．如果 $\mathfrak{a}$ 为 A 的理想，则集合 $f(\mathfrak{a})$ 一般不必为 B 的理想（试举一例）．我们把 $f(\mathfrak{a})$ 在 B 中所生成的理想

$$f(\mathfrak{a})B=\left\{\text{有限和}\sum_i x_iy_i \,\middle|\, x_i\in f(\mathfrak{a}),y_i\in B\right\}$$

叫作是 A 中理想 $\mathfrak{a}$(通过同态 f)到环 B 中的**扩张**. 或者叫作是 $\mathfrak{a}$ 在 B 中的**扩张理想**,表示成 $\mathfrak{a}^e$. 另一方面,如果 $\mathfrak{b}$ 是环 B 的理想,则

$$f^{-1}(\mathfrak{b})=\{a\in A\,|\,f(a)\in\mathfrak{b}\}$$

必然是环 A 的理想(试证明之),称作是环 B 中理想 $\mathfrak{b}$(通过同态 f)到环 A 中的**限制**,或者叫作是 $\mathfrak{b}$ 在 A 中的**限制理想**,表示成 $\mathfrak{b}^c$. 我们注意,理想的扩张和限制运算不仅与环 A 和 B 有关,而且是依赖于某个环同态 $f:A\to B$ 的. 特别若 A 是 B 的一个子环,而且 $f:A\to B$ 是**包含映射**(即对于每个 $a\in A$,令 $f(a)=a\in B$),则 $\mathfrak{a}^e=\mathfrak{a}B$, $\mathfrak{b}^c=\mathfrak{b}\cap A$.

上面所介绍的理想之间的各种运算具有一些简单的性质. 这些性质几乎均可由运算的定义直接推出,我们将它们全部作为习题列在下面.

习　题

1. 环 R 中理想的和、交、积运算均满足交换律与结合律,并且有如下的分配律:设 $\mathfrak{a},\mathfrak{b},\mathfrak{c}$ 为 R 的理想,则

$$\mathfrak{a}(\mathfrak{b}+\mathfrak{c})=\mathfrak{ab}+\mathfrak{ac}.$$

2. 设 $\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{a}_i,\mathfrak{b}_i$ 均为环 R 的理想,则

$$\mathfrak{a}\subseteq(\mathfrak{a}:\mathfrak{b}),\ (\mathfrak{a}:\mathfrak{b})\mathfrak{b}\subseteq\mathfrak{a}.$$

$$((\mathfrak{a}:\mathfrak{b}):\mathfrak{c})=(\mathfrak{a}:\mathfrak{bc})=((\mathfrak{a}:\mathfrak{c}):\mathfrak{b}).$$

$$(\mathfrak{a}:(\mathfrak{b}+\mathfrak{c}))=(\mathfrak{a}:\mathfrak{b})\cap(\mathfrak{a}:\mathfrak{c}).$$

$$\left(\bigcap_{i\in I}\mathfrak{a}_i:\mathfrak{b}\right)=\bigcap_{i\in I}(\mathfrak{a}_i:\mathfrak{b}),\quad\left(\mathfrak{a}:\sum_{i\in I}\mathfrak{b}_i\right)=\bigcap_{i\in I}(\mathfrak{a}:\mathfrak{b}_i).$$

3. 设 $f:A\to B$ 为环的同态,$\mathfrak{a}$ 和 $\mathfrak{b}$ 分别是环 A 和 B 中的理想,求证:

(1) $\mathfrak{a}\subseteq\mathfrak{a}^{ec},\mathfrak{b}\supseteq\mathfrak{b}^{ce}$，$\mathfrak{b}^{c}=\mathfrak{b}^{cec}$，$\mathfrak{a}^{e}=\mathfrak{a}^{ece}$.

(2) 以 C 表示 A 中全部限制理想，以 E 表示 B 中全部扩张理想，即

$$C=\{\mathfrak{b}^c\mid \mathfrak{b}\text{ 为环 }B\text{ 的理想}\},\quad E=\{\mathfrak{a}^e\mid \mathfrak{a}\text{ 为环 }A\text{ 的理想}\}.$$

则 $f:C\to E$，$\mathfrak{a}\mapsto\mathfrak{a}^e$ 和 $g:E\to C,\mathfrak{b}\mapsto\mathfrak{b}^c$ 是互逆的映射。从而给出集合 C 和集合 E 之间的一一对应。

4．设 $f:A\to B$ 为环的同态，$\mathfrak{a}_1,\mathfrak{a}_2$ 为 A 的理想，$\mathfrak{b}_1,\mathfrak{b}_2$ 为 B 的理想，则

$$(\mathfrak{a}_1+\mathfrak{a}_2)^e=\mathfrak{a}_1^e+\mathfrak{a}_2^e,(\mathfrak{b}_1+\mathfrak{b}_2)^c\supseteq\mathfrak{b}_1^c+\mathfrak{b}_2^c.$$
$$(\mathfrak{a}_1\cap\mathfrak{a}_2)^e\subseteq\mathfrak{a}_1^e\cap\mathfrak{a}_2^e,\quad(\mathfrak{b}_1\cap\mathfrak{b}_2)^c=\mathfrak{b}_1^c\cap\mathfrak{b}_2^c.$$
$$(\mathfrak{a}_1\mathfrak{a}_2)^e=\mathfrak{a}_1^e\mathfrak{a}_2^e,\quad(\mathfrak{b}_1\mathfrak{b}_2)^c\supseteq\mathfrak{b}_1^c\cdot\mathfrak{b}_2^c.$$
$$(\mathfrak{a}_1:\mathfrak{a}_2)^e\subseteq(\mathfrak{a}_1^e:\mathfrak{a}_2^e),\quad(\mathfrak{b}_1:\mathfrak{b}_1)^c\subseteq(\mathfrak{b}_1^c:\mathfrak{b}_2^c).$$

并且举例说明以上诸式中的⊆或⊇一般均不能改成等号。

5．设 $\mathbf{Z}$ 为整数环，$m,n\in\mathbf{Z},m,n\geqslant0,\mathfrak{a}=n\mathbf{Z},\mathfrak{b}=m\mathbf{Z}$。求证

(1) $\mathfrak{a}+\mathfrak{b}=(m,n)\mathbf{Z},\mathfrak{a}\cap\mathfrak{b}=[m,n]\mathbf{Z},\mathfrak{a}\mathfrak{b}=mn\mathbf{Z}$，其中 (m,n) 和 $[m,n]$ 分别表示 m 和 n 的最大公约数和最小公倍数。

(2) $\mathfrak{a}$ 和 $\mathfrak{b}$ 互素 $\Longleftrightarrow(m,n)=1\Longleftrightarrow\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b}$.

(3) $(\mathfrak{a}:\mathfrak{b})=q\mathbf{Z}$，其中 $q=n/(n,\ m)$

6．一般地，设 $\mathfrak{a}$ 和 $\mathfrak{b}$ 是环 R 的两个理想，则：$\mathfrak{a}$ 与 $\mathfrak{b}$ 互素 $\Longleftrightarrow\mathfrak{a}\cap\mathfrak{b}=\mathfrak{a}\mathfrak{b}$.

7．(中国剩余定理) 设 $\mathfrak{a}_1\cdots,\mathfrak{a}_n$ 是环 R 的 n 个理想，并且它们两两互素。求证有环的同构

$$f:R/\mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n\xrightarrow{\sim}R/\mathfrak{a}_1\oplus R/\mathfrak{a}_2\oplus\cdots\oplus R/\mathfrak{a}_n,$$
$$x(\bmod\ \mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n)\mapsto(x(\bmod\ \mathfrak{a}_1),\ x(\bmod\ \mathfrak{a}_2),\cdots,x(\bmod\ \mathfrak{a}_n)),$$

其中⊕表示环的直和，而对每个理想 $\mathfrak{a}$ 和 $x\in R$，我们以 $x(\bmod\ \mathfrak{a})$ 表示 x 在商环 $R/\mathfrak{a}$ 中的标准同态象。

§1.2 素理想和极大理想

设 R 是非零环，R 中的理想 $\mathfrak{p}$ 叫作是**素理想**，是指它满足以下两个条件：

(i) $\mathfrak{p}\neq R$；

(ii) 如果 $a,b\in R$，$ab\in\mathfrak{p}$，则 $a\in\mathfrak{p}$ 或者 $b\in\mathfrak{p}$.

而 R 中理想 $\mathfrak{m}$ 叫作是**极大理想**，是指它满足以下两个条件：

(i′) $\mathfrak{m}\neq R$；

(ii′) $\mathfrak{m}$ 和 R 之间不存在 R 的理想．换句话说，如果 $\mathfrak{a}$ 是 R 中的理想并且 $\mathfrak{m}\subseteq\mathfrak{a}\subseteq R$ 则 $\mathfrak{a}=\mathfrak{m}$ 或者 $\mathfrak{a}=R$.

定理 1 设 $\mathfrak{a}$ 是非零环 R 的理想，则

(1) $\mathfrak{a}$ 为 R 的素理想$\Longleftrightarrow$商环 $R/\mathfrak{a}$ 是整环；

(2) $\mathfrak{a}$ 为 R 的极大理想$\Longleftrightarrow$商环 $R/\mathfrak{a}$ 是域.

证明 (1) 若 $\mathfrak{a}$ 为 R 的素理想，则 $\mathfrak{a}\neq R$，从而 $R/\mathfrak{a}$ 不是零环．进而，设 $\bar{x},\bar{y}\in R/\mathfrak{a}(x,y\in R)$，并且 $\bar{x}\cdot\bar{y}=\bar{0}\in R/\mathfrak{a}$，则 $\overline{xy}=\bar{x}\cdot\bar{y}=\bar{0}$，从而 $xy\in\mathfrak{a}$．由于 $\mathfrak{a}$ 为素理想，从而 $x\in\mathfrak{a}$ 或者 $y\in\mathfrak{a}$，即 $\bar{x}=\bar{0}$ 或者 $\bar{y}=\bar{0}$．这就表明 $R/\mathfrak{a}$ 中没有非零的零因子，即 $R/\mathfrak{a}$ 是整环．反过来，如果 $R/\mathfrak{a}$ 为整环，则 $R/\mathfrak{a}\neq(0)$，即 $\mathfrak{a}\neq R$．进而，如果 $x,y\in R$，$xy\in\mathfrak{a}$，则 $\bar{x}\cdot\bar{y}=\overline{xy}=\bar{0}\in R/\mathfrak{a}$，由于$R/\mathfrak{a}$是整环，从而 $\bar{x}=\bar{0}$ 或者 $\bar{y}=\bar{0}$，即 $x\in\mathfrak{a}$ 或者 $y\in\mathfrak{a}$，这就表明 $\mathfrak{a}$ 是 R 的素理想.

(2) 若 $\mathfrak{a}$ 为 R 的极大理想，则 $R/\mathfrak{a}\neq(0)$，并且对于 $R/\mathfrak{a}$ 中每个非零元素 $\bar{x}$(即 $\bar{x}\neq\bar{0}$，$x\in R$)，则 $x\notin\mathfrak{a}$．于是由 x 和 $\mathfrak{a}$ 所生成的理想 $xR+\mathfrak{a}$ 大于 $\mathfrak{a}$．由 $\mathfrak{a}$ 的极大性即知 $xR+\mathfrak{a}=R$．由于 $1\in R$，从而存在 $r\in R$ 和 $a\in\mathfrak{a}$，使得 $xr+a=1$．因此 $\bar{x}\cdot\bar{r}=\overline{xr}=\overline{1-a}=\bar{1}-\bar{a}=\bar{1}-\bar{0}=\bar{1}\in R/\mathfrak{a}$．这就表明非零商环 $R/\mathfrak{a}$ 中每个非零元素 $\bar{x}$ 均有乘法逆元素．于是 $R/\mathfrak{a}$ 为域．反过来，如果$R/\mathfrak{a}$ 为域，则 $R/\mathfrak{a}\neq(0)$，于是 $\mathfrak{a}\neq R$．进而，假设 $\mathfrak{b}$ 为 R 的理想并且 $\mathfrak{a}\subseteq\mathfrak{b}\subseteq R$．如果 $\mathfrak{a}\neq\mathfrak{b}$，则有 $x\in\mathfrak{b}$，$x\notin\mathfrak{a}$．从而在 $R/\mathfrak{a}$ 中 $\bar{x}\neq\bar{0}$．由于 $R/\mathfrak{a}$ 为域，于是有 $r\in R$，使得 $\bar{x}\,\bar{r}=\bar{1}$，即 $xr-1\in\mathfrak{a}$．于是 $1\in xr+\mathfrak{a}\subseteq xR+\mathfrak{a}\subseteq\mathfrak{b}$．这就表明 $\mathfrak{b}=R$．从而 $\mathfrak{a}$ 是 R 的极大理想．▌

注记 1．我们知道，域中非零元素 x 均有乘法逆元素，从而 x 不为零因子($xr=0\Rightarrow r=x^{-1}xr=0$)．这表明域必是整环．于是

由定理 1 可知，环 R 的每个极大理想必然是素理想．但是反过来，素理想不一定是极大理想．例如，对于多项式环 $R=\mathbf{Z}[x]$，(x) 为素理想，从而 $\mathbf{Z}[x]/(x)\cong\mathbf{Z}$ 是整环，但是 $\mathbf{Z}$ 不为域，从而 (x) 不是 R 的极大理想．事实上我们有 $(x)\subset(2,x)\subset\mathbf{Z}[x]$，而 $(2,x)$ 为 $\mathbf{Z}[x]$ 的极大理想，因为商环 $\mathbf{Z}[x]/(2,x)\cong\mathbf{Z}/2\mathbf{Z}$ 是二元域．

2．由定理 1 可知：(0) 为环 R 的素理想 $\Longleftrightarrow R$ 为整环；(0) 为 R 的极大理想 $\Longleftrightarrow R$ 为域．

人们自然会提出一个很基本的问题：每个非零环是否至少存在一个极大理想和素理想？答案是肯定的．为了证明这一点，我们需要用集合论中一个重要结果，叫作 Zorn 引理．因为今后我们不断地使用它，所以我们现在介绍什么是 Zorn 引理，关于它的证明和一些等价形式请参看集合论的书．

集合 Σ 上的一个二元关系 $\leqslant$ 叫作是 Σ 上的一个**部分序**，是指关于 $\leqslant$ 满足以下三个条件：对于任意 $x,y,z\in\Sigma$，

(i) $x\leqslant x$；

(ii) 如果 $x\leqslant y$，$y\leqslant x$，则 $x=y$；

(iii) 如果 $x\leqslant y$，$y\leqslant z$，则 $x\leqslant z$．

这时称 $(\Sigma,\leqslant)$ 是一个部分序集合．所谓“部分”的意思是指，在 Σ 中可能有元素 x,y，使得 $x\leqslant y$ 和 $y\leqslant x$ 均不成立．如果是这种情形，则称 x 和 y 是**不可比较的**．否则，即如果 $x\leqslant y$ 或 $y\leqslant x$ 至少有一个成立，则称 x 和 y 是**可比较的**．设 Σ' 是部分序集合 $(\Sigma,\leqslant)$ 的一个子集合．如果 Σ' 中任意两个元素均可比较，则称 Σ' 是一个**链**．Σ 中元素 x 叫作是子集合 Σ' 的**上界**，是指对每个 $s\in\Sigma'$ 均有 $s\leqslant x$．Σ' 中元素 x 叫作是 Σ' 的一个**极大元**，是指对于 Σ' 中每个与 x 可比较的元素 y，必然 $y\leqslant x$．

Zorn 引理 设 $(\Sigma,\leqslant)$ 是非空的部分序集合．如果 Σ 中每个

链在 Σ 中均有上界，则 Σ 必有极大元.

现在我们用 Zorn 引理来证明非零环中极大理想的存在性. 我们甚至可以证明更强的结果.

定理 2 设 $\mathfrak{a}$ 是非零环 R 中的真理想(即 $\mathfrak{a}\neq R$)，则 R 中存在极大理想 $\mathfrak{m}$，使得 $\mathfrak{m}\supseteq\mathfrak{a}$.

证明 考虑集合

$$\Sigma=\{\mathfrak{b}\mid\mathfrak{b}\text{ 为 }R\text{ 的理想，且 }\mathfrak{a}\subseteq\mathfrak{b}\neq R\}.$$

由于 $\mathfrak{a}\in\Sigma$，从而 Σ 是非空集合. 集合论的包含关系 $\subseteq$ 显然是 Σ 中的部分序，从而 $(\Sigma,\subseteq)$ 是非空部分序集合. 设 Σ' 是 Σ 中的一个链. 令 $\mathfrak{c}=\bigcup\limits_{\mathfrak{b}\in\Sigma'}\mathfrak{b}$(集合论的并集). 我们来证明

(1) $\mathfrak{c}$ 是 R 的一个理想，这是因为：如果 $x_1,x_2\in\mathfrak{c}$，由 $\mathfrak{c}$ 的定义可知有 $\mathfrak{b}_1,\mathfrak{b}_2\in\Sigma'$，使得 $x_1\in\mathfrak{b}_1$，$x_2\in\mathfrak{b}_2$，由于 Σ' 为链，于是 $\mathfrak{b}_1\subseteq\mathfrak{b}_2$ 或者 $\mathfrak{b}_2\subseteq\mathfrak{b}_1$. 从而 x_1 和 x_2 或者均属于 $\mathfrak{b}_1$ 或者均属于 $\mathfrak{b}_2$. 因此 $x_1\neq x_2\in\mathfrak{b}_1\cup\mathfrak{b}_2\subseteq\mathfrak{c}$. 同样地，如果 $r\in R$，$x\in\mathfrak{c}$，则有 $\mathfrak{b}\in\Sigma'$ 使得 $x\in\mathfrak{b}$. 由于 Σ' 中成员 $\mathfrak{b}$ 是理想，从而 $rx\in\mathfrak{b}\subseteq\mathfrak{c}$. 这就表明 $\mathfrak{c}$ 是 R 的理想.

(ii) $\mathfrak{a}\subseteq\mathfrak{c}\neq R$. $\mathfrak{a}\subseteq\mathfrak{c}$ 显然成立. 另一方面，如果 $\mathfrak{c}=R$，则 $1\in\mathfrak{c}$，于是有 $\mathfrak{b}\in\Sigma'$ 使得 $1\in\mathfrak{b}$，即 $\mathfrak{b}=R$. 这与 $\mathfrak{b}\in\Sigma'\subseteq\Sigma$ 以及 Σ 的定义相矛盾. 因此 $\mathfrak{c}\neq R$.

综合(i)和(ii)可知 $\mathfrak{c}\in\Sigma$，并且 $\mathfrak{c}$ 显然是链 Σ' 的上界. 于是 $(\Sigma,\subseteq)$ 满足 Zorn 引理条件. 从而 Σ 必有极大元 $\mathfrak{m}$. 于是 $\mathfrak{m}$ 也就是 R 的极大理想并且 $\mathfrak{m}\supseteq\mathfrak{a}$. ▌

注记 1. 由于每个极大理想均是素理想，从而由定理 2 可知，非零环的每个真理想均包含在某个素理想之中.

2. 在定理 2 中取 $\mathfrak{a}=(0)$，即知每个非零环都至少存在一个极大理想，从而也必然存在素理想.

今后我们以 Spec R 表示环 R 的全部素理想组成的集合，把它叫作是环 R 的**素谱**．而 R 的全部极大理想组成的集合叫作是环 R 的**极大谱**，表示成 Max R．于是，对于每个非零环 R，我们有 $\varnothing\neq$ Max $R\subseteq$ Spec R．

定义 只有一个极大理想的非零环叫作是**局部环**．只有有限个极大理想的非零环叫作是**半局部环**．

如果 R 为局部环，$\mathfrak{m}$ 是它的唯一极大理想，则这个局部环也表成为 $(R,\mathfrak{m})$．域 $R/\mathfrak{m}$ 叫作是局部环的**剩余类域**．下面定理给出局部环的另一些很有益的刻画方式(注意：环 R 中乘法可逆元叫作是环 R 的**单位**．环 R 中全部单位形成乘法群，叫作是环 R 的**单位群**，表示成 $U(R)$)．

定理 3 设 R 为环而 $\mathfrak{m}$ 是 R 的真理想．则下列三条件是彼此等价的：

(1) R 为局部环并且 $\mathfrak{m}$ 是它的唯一极大理想；

(2) $R-\mathfrak{m}=U(R)$；

(3) $\mathfrak{m}$ 是 R 的极大理想并且 $1+\mathfrak{m}\subseteq U(R)$．

证明 (1)$\Rightarrow$(2)：由于 $\mathfrak{m}$ 是真理想，从而 $\mathfrak{m}$ 不能包含单位(注意：$u\in U(R)\Longleftrightarrow(u)=R$)．于是 $R-\mathfrak{m}\supseteq U(R)$．另一方面，对于每个元素 $u\in R-U(R)$，则 (u) 为 R 的真理想，从而 (u) 包含在 R 的某个极大理想之中(定理 2)．但是 R 只有一个极大理想 $\mathfrak{m}$，于是 $(u)\subseteq\mathfrak{m}$，特别地 $u\in\mathfrak{m}$．从而 $R-U(R)\subseteq\mathfrak{m}$．这相当于 $R-\mathfrak{m}\subseteq U(R)$．从而 $R-\mathfrak{m}=U(R)$．

(2)$\Rightarrow$(3)：由 $R-\mathfrak{m}=U(R)$ 可知 $1\notin\mathfrak{m}$，从而 $\mathfrak{m}$ 是真理想．由于比 $\mathfrak{m}$ 大的理想必然包含单位，即必然是 R，从而 $\mathfrak{m}$ 是 R 的极大理想．再用反证法证明 $1+\mathfrak{m}\subseteq U(R)$．如果存在 $m\in\mathfrak{m}$，使得 $1+m\notin U(R)$，则由 $R-\mathfrak{m}=U(R)$ 可知 $1+m\in\mathfrak{m}$．于是 $1\in\mathfrak{m}$，

这不可能. 从而 $1+\mathfrak{m}\subseteq U(R)$.

(3)⇒(1): 只需证明 R 只有一个极大理想 $\mathfrak{m}$. 设 $\mathfrak{m}'$ 是 R 的任意一个极大理想. 如果 $\mathfrak{m}'\neq\mathfrak{m}$, 由于 $\mathfrak{m}'$ 和 $\mathfrak{m}$ 均是极大理想, 并且 $\mathfrak{m}'+\mathfrak{m}\supset\mathfrak{m}$. 从而 $\mathfrak{m}'+\mathfrak{m}=R$. 于是有 $m\in\mathfrak{m}$, $m'\in\mathfrak{m}'$, 使得 $m+m'=1$. 于是 $m'=1-m\in 1+\mathfrak{m}\subseteq U(R)$, 从而 $\mathfrak{m}'=R$, 这就导致矛盾. 于是 $\mathfrak{m}=\mathfrak{m}'$, 即 $\mathfrak{m}$ 是 R 的唯一极大理想. ▌

例 1 整数环 $\mathbf{Z}$ 为主理想整环, 每个理想均有形式 $n\mathbf{Z}$ ($n\in\mathbf{Z}, n\geqslant 0$). 不难验证: $\mathbf{Z}/n\mathbf{Z}$ 为整环 $\Longleftrightarrow n=0$ 或者素数; $\mathbf{Z}/n\mathbf{Z}$ 为域 $\Longleftrightarrow n$ 为素数. 于是 $\operatorname{Max}\mathbf{Z}=\{p\mathbf{Z}\mid p$ 为素数$\}$, 而 $\operatorname{Spec}\mathbf{Z}=\operatorname{Max}\mathbf{Z}\cup\{(0)\}$.

例 2 设 m 为正整数, 考虑环 $\mathbf{Z}/m\mathbf{Z}$. 设 $m=p_1^{a_1}\cdots p_s^{a_s}$ 是 m 的素因子分解式, 其中 $p_1,\cdots,p_s$ 是两两不同的素数, 而 $a_i\geqslant 1$ ($1\leqslant i\leqslant s$). 由环的同态定理可知 $\mathbf{Z}/m\mathbf{Z}$ 的每个理想均有形式 $n\mathbf{Z}/m\mathbf{Z}$, 其中 $n\mid m$. 并且 $(\mathbf{Z}/m\mathbf{Z})/(n\mathbf{Z}/m\mathbf{Z})\cong\mathbf{Z}/n\mathbf{Z}$. 从而 $n\mathbf{Z}/m\mathbf{Z}$ 为 $\mathbf{Z}/m\mathbf{Z}$ 的素理想 $\Longleftrightarrow\mathbf{Z}/n\mathbf{Z}$ 为整环 $\Longleftrightarrow n$ 为素数 $\Longleftrightarrow\mathbf{Z}/n\mathbf{Z}$ 为域 $\Longleftrightarrow n\mathbf{Z}/m\mathbf{Z}$ 为 $\mathbf{Z}/m\mathbf{Z}$ 的极大理想. 从而 $\operatorname{Max}(\mathbf{Z}/m\mathbf{Z})=\operatorname{Spec}(\mathbf{Z}/m\mathbf{Z})=\{p_i\mathbf{Z}/m\mathbf{Z}\mid 1\leqslant i\leqslant s\}$. 并且 $\mathbf{Z}/m\mathbf{Z}$ 为局部环 $\Longleftrightarrow m$ 为某个素数的幂(即 $s=1$).

例 3 上面例 2 的 $\mathbf{Z}/m\mathbf{Z}$ ($m\geqslant 1$) 为半局部环. 更一般地, 每个有限环均是半局部环, 因为它的子集只有有限多个. 从而极大理想也只有有限多个.

进一步的例子请见习题.

习　题

1. 设 $\mathfrak{p}$ 是环 R 的理想. 求证: $\mathfrak{p}$ 为 R 的素理想 $\Longleftrightarrow$ 对于 R 的任意两个理想 $\mathfrak{a}$ 和 $\mathfrak{b}$, 如果 $\mathfrak{a}\mathfrak{b}\subseteq\mathfrak{p}$, 则 $\mathfrak{a}\subseteq\mathfrak{p}$ 或者 $\mathfrak{b}\subseteq\mathfrak{p}$