普通高等教育"十一五"国家级规划教材

北京大学数学教学系列丛书

研究生
数学基础课教材

抽象代数 II

徐明曜　赵春来　编著

北京大学出版社
PEKING UNIVERSITY PRESS

北京大学数学教学系列丛书

ISBN 978-7-301-08528-8

9 787301 085288 >

责任编辑：刘　勇
封面设计：林胜利

定价：18.00元

北京大学数学教学系列丛书

抽象代数 II

徐明曜 赵春来 编著

北京大学出版社
PEKING UNIVERSITY PRESS

图书在版编目 (CIP) 数据

抽象代数 II / 徐明曜，赵春来编著. —北京：北京大学出版社，2007.3

(北京大学数学教学系列丛书)

ISBN 978-7-301-08528-8

I. 抽… II. ①徐…②赵… III. 抽象代数－高等学校－教材 IV. O211

中国版本图书馆 CIP 数据核字 (2006) 第 148161 号

书　　名：抽象代数 II
著作责任者：徐明曜　赵春来　编著
责 任 编 辑：刘　勇
标 准 书 号：ISBN 978-7-301-08528-8/O · 0633
出　版　者：北京大学出版社
地　　址：北京市海淀区成府路 205 号　100871
网　　址：http://www.pup.cn
电　　话：邮购部 62752015　发行部 62750672　理科编辑部 62752021
出版部 62754962
电 子 信 箱：zpup@pup.pku.edu.cn
印　刷　者：北京大学印刷厂
发　行　者：北京大学出版社
经　销　者：新华书店
890 mm × 1240 mm　A5　9 印张　270 千字
2007 年 3 月第 1 版　2007 年 3 月第 1 次印刷
印　　数：0001—4000 册
定　　价：18.00 元

内 容 简 介

本书是作者多年来在北京大学为硕士研究生开设抽象代数课程的讲义，书中系统讲述了抽象代数的基本理论和方法. 它反映了新时期硕士研究生抽象代数课程的教学理念，凝聚了作者及同事们所积累的丰富教学经验. 全书共分为六章，内容包括：预备知识，模，群的进一步知识，Galois 理论，结合代数和有限群的表示论，典型群的初步知识等. 每章配备适量习题，书末附有习题的解答或提示，供读者参考.

本书作为研究生教材，既注意内容的基础性又兼顾先进性. 考虑到硕士生来自不同学校，而在本科阶段所学的抽象代数内容不尽相同，为了使读者有一个共同的基础，本书在前三章都加了第 0 节，分别介绍在本科低年级抽象代数 I 中已学过的环论、群论和域论知识. 本书在叙述上由浅入深、循序渐进、语言精练、清晰易懂，并注意各章节之间的内在联系与呼应，便于教学与自学.

本书可作为综合大学、高等师范院校数学系高年级本科生、研究生的教材或教学参考书，也可供数学工作者阅读.

作者简介

徐明曜 1941 年 9 月生, 1965 年毕业于北京大学数学力学系数学专业, 1980 年在北京大学数学系研究生毕业, 获硕士学位, 并留校任教. 1985 年晋升为副教授, 1988 年破格晋升为教授, 博士生导师.

徐明曜长期从事本科生及研究生代数课程的教学以及有限群论的研究工作, 讲授过多门本科生和研究生课程, 著有《有限群导引》(下册与他人合作); 科研方面自 20 世纪 60 年代起进行有限 p 群的研究工作, 80 年代中期又开创了我国"群与图"的研究领域, 至今已发表论文 80 多篇, 多数发表在国外的重要杂志上. 曾获得国家教委优秀科技成果奖 (1985), 国家教委科技进步二等奖 (1995), 周培源基金会数理基金成果奖 (1995).

赵春来 1945 年 2 月生, 1967 年毕业于北京大学数学力学系数学专业, 1984 年在北京大学数学系研究生毕业, 获博士学位. 1987 年晋升为副教授, 1992 年晋升为教授, 博士生导师.

赵春来长期从事本科生及研究生代数课程的教学以及代数数论的研究工作, 讲授过多门本科生和研究生课程, 与他人合著了《代数学》、《线性代数引论》、《模曲线导引》、《代数群引论》等著作. 他的研究工作主要集中于椭圆曲线的算术理论以及信息安全方面, 在国内外重要学术刊物上发表论文十余篇. 曾获教育部科技进步二等奖 (2004), 北京市优秀教学成果一等奖 (2005), 国家级优秀教学成果二等奖 (2005).

序　言

自 1995 年以来，在姜伯驹院士的主持下，北京大学数学科学学院根据国际数学发展的要求和北京大学数学教育的实际，创造性地贯彻教育部“加强基础，淡化专业，因材施教，分流培养”的办学方针，全面发挥我院学科门类齐全和师资力量雄厚的综合优势，在培养模式的转变、教学计划的修订、教学内容与方法的革新，以及教材建设等方面进行了全方位、大力度的改革，取得了显著的成效. 2001 年，北京大学数学科学学院的这项改革成果荣获全国教学成果特等奖，在国内外产生很大反响.

在本科教育改革方面，我们按照加强基础、淡化专业的要求，对教学各主要环节进行了调整，使数学科学学院的全体学生在数学分析、高等代数、几何学、计算机等主干基础课程上，接受学时充分、强度足够的严格训练；在对学生分流培养阶段，我们在课程内容上坚决贯彻“少而精”的原则，大力压缩后续课程中多年逐步形成的过窄、过深和过繁的教学内容，为新的培养方向、实践性教学环节，以及为培养学生的创新能力所进行的基础科研训练争取到了必要的学时和空间. 这样既使学生打下宽广、坚实的基础，又充分照顾到每个人的不同特长、爱好和发展取向. 与上述改革相适应，积极而慎重地进行教学计划的修订，适当压缩常微、复变、偏微、实变、微分几何、抽象代数、泛函分析等后续课程的周学时. 并增加了数学模型和计算机的相关课程，使学生有更大的选课余地.

在研究生教育中，在注重专题课程的同时，我们制定了 30 多门研究生普选基础课程 (其中数学系 18 门)，重点拓宽学生的专业基础和加强学生对数学整体发展及最新进展的了解.

教材建设是教学成果的一个重要体现. 与修订的教学计划相配合，我们进行了有组织的教材建设. 计划自 1999 年起用 8 年的

时间修订、编写和出版 40 余种教材. 这就是将陆续呈现在大家面前的《北京大学数学教学系列丛书》. 这套丛书凝聚了我们近十年在人才培养方面的思考, 记录了我们教学实践的足迹, 体现了我们教学改革的成果, 反映了我们对新世纪人才培养的理念, 代表了我们新时期的数学教学水平.

经过 20 世纪的空前发展, 数学的基本理论更加深入和完善, 而计算机技术的发展使得数学的应用更加直接和广泛, 而且活跃于生产第一线, 促进着技术和经济的发展, 所有这些都正在改变着人们对数学的传统认识. 同时也促使数学研究的方式发生巨大变化. 作为整个科学技术基础的数学, 正突破传统的范围而向人类一切知识领域渗透. 作为一种文化, 数学科学已成为推动人类文明进化、知识创新的重要因素, 将更深刻地改变着客观现实的面貌和人们对世界的认识. 数学素质已成为今天培养高层次创新人才的重要基础. 数学的理论和应用的巨大发展必然引起数学教育的深刻变革. 我们现在的改革还是初步的. 教学改革无禁区, 但要十分稳重和积极; 人才培养无止境, 既要遵循基本规律, 更要不断创新. 我们现在推出这套丛书, 目的是向大家学习. 让我们大家携起手来, 为提高中国数学教育水平和建设世界一流数学强国而共同努力.

张 继 平

2002 年 5 月 18 日

于北京大学蓝旗营

前　言

代数学是数学专业最基本和最重要的基础课程之一. 它对学好数学本身以及数学在现代科学技术很多方面的应用来说都有重要的意义. 因此我们在数学学习的各个阶段都开设了代数课程. 比如在本科低年级开设的高等代数或线性代数，以及抽象代数或近世代数 (简称抽象代数 I) 等. 本课程是为数学硕士生阶段设计的抽象代数 II 课程.

由于现代代数学有很多分支，而每个分支又都有众多抽象的概念，因此在本科开设的抽象代数中只能讲解代数的基本概念以及概念之间的联系，而不能讲解代数各个分支丰富的内容和深刻的结果. 于是给学生造成了这样一种印象，似乎抽象代数就是若干概念的堆积，看不出代数学有什么深刻的结果. 这种印象和代数学的实际发展是大相径庭的. 事实上，即使是在 19 世纪末和 20 世纪初的代数学就已经有着十分丰富而深刻的结果，更不用说今天的代数学了. 基于此，我们想在本课程中讲解代数学的较为深刻而又有着广泛应用的内容. 为了这样的目的，在内容上就有很多可能的选择. 譬如，群表示论、典型群、有限群、复单 Lie 代数的分类、环论、交换代数、模论、 Galois 理论、代数数论、代数几何、格论、同调代数初步，等等. 根据教学实际和师资情况，我们最后选择了模论、群论的进一步知识、 Galois 理论、结合代数和群的表示论、典型群初步等五块内容. 而其他的也是很好的内容就只能割爱了. 另外，在实际的教学过程中，任课教师还可对这五部分内容有所取舍. 因为我们只有 45 课时的课堂教学时间，而目前已经写的部分差不多可供 60 课时使用.

还有几点是需要向读者说明的.

1. 本书是作为教材而编写的，它不仅要介绍代数学的基本知

识同时也要介绍方法，而且还要突出方法. 因此从知识上并不追求完全，相当多的内容是为了介绍方法而写入的.

2. 学习本书之前应该学过本科抽象代数 I 课程. 由于我校的硕士生来自全国各个学校，而各校所学的内容不尽相同，为了使大家有个共同的基础，我们在第一至第三章前都加了第 0 节，分别介绍在本科抽象代数 I 课程中已经学过的环论、群论和域论知识.

3. 由于读者在本科阶段都受过较充分的抽象代数的训练，在本书中定理的证明写得比较简短，常给读者留有思考的余地. 这样读起来可能会感到吃力，但对训练推理能力以及将来阅读文献、学做研究都会有一定的帮助.

4. 本书中的习题是不可不做的，它们是本书重要的组成部分. 这些习题难易程度不等，对于稍难一些的题目都标了星号“*”.

最后，我们要感谢我学院代数组各位同仁，他们参与了本书教学大纲的讨论，并提出了很多有价值的建议.

作　者

2006 年 8 月于北京大学

数学科学学院

目　　录

第 0 章　预备知识

在本章中，我们介绍 Zorn 引理和范畴论的一些最基本的知识.

§0.1　Zorn 引理

Zorn 引理是集合论中一个基本的公理，与之等价的有*选择公理*和*良序定理*等. 我们在这里仅叙述 Zorn 引理. 有关这方面的较详细的论述可以参见 B.L. 范德瓦尔登的《代数学 (I)》(丁石孙、曾肯成、郝鈵新译，科学出版社，1978).

定义 1.1　设 S 是一个集合. 所谓 S 上的一个**偏序** (记为“$\leq$”) 是指满足下述三个条件的二元关系：

(1) 反身性：$a \leq a$ $(\forall\, a \in S)$;

(2) 反对称性：若 $a \leq b$, $b \leq a$, 则 $a = b$ $(\forall\, a, b \in S)$;

(3) 传递性：若 $a \leq b$, $b \leq c$, 则 $a \leq c$ $(\forall\, a, b, c \in S)$.

具有偏序的集合称为**偏序集**. 偏序集的两个元素 a 和 b 称为**可比较的**, 如果 $a \leq b$ 或 $b \leq a$.

定义 1.2　设 S 是偏序集. 如果存在 $m \in S$, 满足

$$m \leq a \text{ 蕴含着 } m = a \quad (\forall\, a \in S),$$

则称 m 为 S 的一个**极大元**. 设 $T \subseteq S$. 如果存在 $s \in S$, 满足

$$t \leq s \quad (\forall\, t \in T),$$

则称 s 为 T 在 S 中的一个**上界**.

定义 1.3　设 S 是偏序集. 称 S 的一个子集 T 为**链** (或**全序链**), 如果 T 的任意两个元素都是可比较的.

Zorn 引理 设 S 是一个偏序集. 如果 S 中的任意一个链在 S 中都有上界, 则 S 有极大元.

§0.2 范畴与函子

定义 2.1 一个**范畴** $\mathfrak{C}$ 由下述三个内容组成:

(1) 一类对象的全体 (记为 Obj $\mathfrak{C}$);

(2) 对于任意两个对象 $A, B \in \mathrm{Obj}\ \mathfrak{C}$, 有一个态射集合 (记为 $\mathrm{Hom}_{\mathfrak{C}}(A, B)$, 或在不致引起混淆时记为 $\mathrm{Hom}(A, B)$);

(3) 对于任意三个对象 A, B, C, 有态射集合的合成映射:

$$\begin{aligned} \mathrm{Hom}_{\mathfrak{C}}(A,B) \times \mathrm{Hom}_{\mathfrak{C}}(B,C) &\to \mathrm{Hom}_{\mathfrak{C}}(A,C), \\ (f,g) &\mapsto f \circ g. \end{aligned}$$

其中的 (2), (3) 两条满足以下三个条件:

(i) $\mathrm{Hom}_{\mathfrak{C}}(A,B) \cap \mathrm{Hom}_{\mathfrak{C}}(C,D) = \varnothing$, 如果 $A \neq C$ 或 $B \neq D$;

(ii) 态射的合成有结合律: 对于任意的 $f \in \mathrm{Hom}_{\mathfrak{C}}(A,B)$, $g \in \mathrm{Hom}_{\mathfrak{C}}(B,C)$ 以及 $h \in \mathrm{Hom}_{\mathfrak{C}}(C,D)$, 有

$$(f \circ g) \circ h = f \circ (g \circ h);$$

(iii) $\mathrm{Hom}_{\mathfrak{C}}(A,A)$ 中存在态射 id_A, 具有如下性质: 对于任意的 $f \in \mathrm{Hom}_{\mathfrak{C}}(A,B)$, $g \in \mathrm{Hom}_{\mathfrak{C}}(B,A)$ (B 为 $\mathfrak{C}$ 的任一对象), 有

$$\mathrm{id}_A \circ f = f, \quad g \circ \mathrm{id}_A = g.$$

定义 2.2 设 $\mathfrak{C}$ 和 $\mathfrak{D}$ 是两个范畴. 如果 Obj $\mathfrak{D}$ 是 Obj $\mathfrak{C}$ 的一部分, 并且对于 Obj $\mathfrak{D}$ 的任意二对象 X 和 Y, 都有

$$\mathrm{Hom}_{\mathfrak{D}}(X,Y) \subseteq \mathrm{Hom}_{\mathfrak{C}}(X,Y), \tag{0.1}$$

则称 $\mathfrak{D}$ 为 $\mathfrak{C}$ 的**子范畴**. 若 (0.1) 式中的 "$\subseteq$" 是 "$=$", 则称 $\mathfrak{D}$ 为 $\mathfrak{C}$ 的**全子范畴**.

定义 2.3 设 X 和 Y 为 $\mathfrak{C}$ 的二对象. 如果存在 $f\in \mathrm{Hom}_{\mathfrak{C}}(X,Y)$ 和 $g\in \mathrm{Hom}_{\mathfrak{C}}(Y,X)$, 使得 $fg=\mathrm{id}_X$, $gf=\mathrm{id}_Y$, 则称对象 X 和 Y **同构**.

例 2.4 设 $\mathfrak{G}$ 的对象 Obj $\mathfrak{G}$ 为所有的群, 对于两个群 G_1 和 G_2, 令 $\mathrm{Hom}_{\mathfrak{G}}(G_1,G_2)$ 为 G_1 到 G_2 的所有群同态组成的集合, 对于三个群 G_1,G_2,G_3, 规定

$$\begin{aligned}\mathrm{Hom}_{\mathfrak{G}}(G_1,G_2)\times \mathrm{Hom}_{\mathfrak{G}}(G_2,G_3) &\rightarrow \mathrm{Hom}_{\mathfrak{G}}(G_1,G_3),\\ (\sigma,\tau) &\mapsto \sigma\tau.\end{aligned}$$

这样就定义了一个范畴 $\mathfrak{G}$, 称为群范畴 (注意: Obj $\mathfrak{G}$ 不是集合). 群范畴 $\mathfrak{G}$ 中二对象的同构就是群同构. 完全平行地可以定义交换群范畴 $\mathbf{Ab}$, 即 Obj $\mathbf{Ab}$ 为所有的交换群; 对于 $A,B\in$ Obj $\mathbf{Ab}$, $\mathrm{Hom}_{\mathbf{Ab}}(A,B)$ 为 A 到 B 的所有群同态组成的集合, $\mathbf{Ab}$ 是 $\mathfrak{G}$ 全子范畴. 环范畴 $\mathfrak{R}$ 的对象 Obj $\mathfrak{R}$ 为所有的环; 对于 $R,S\in$ Obj $\mathfrak{R}$, $\mathrm{Hom}_{\mathfrak{R}}(R,S)$ 为 R 到 S 的所有环同态组成的集合, $\mathfrak{R}$ 是 $\mathbf{Ab}$ 的子范畴, 但不是全子范畴 (例如, 有理数域 $\mathbb{Q}\in\mathfrak{R}$, 易见 $\mathrm{Hom}_{\mathfrak{R}}(\mathbb{Q},\mathbb{Q})$ 只含有零同态和恒同映射, 而 $\mathrm{Hom}_{\mathfrak{G}}(\mathbb{Q},\mathbb{Q})$ 是无穷集合).

类似地, 我们可以定义域范畴、一个域 F 上的线性空间范畴、拓扑空间范畴、集合范畴, 等等.

两个范畴的联系可以用所谓的 "函子" 给出.

定义 2.5 设 $\mathfrak{C}$ 和 $\mathfrak{D}$ 是两个范畴、由 $\mathfrak{C}$ 到 $\mathfrak{D}$ 的一个**共变函子** (或**协变函子**) F 是指:

(1) 对于 $\mathfrak{C}$ 的任一对象 X, F 规定了 $\mathfrak{D}$ 中的相应的对象 $F(X)$;

(2) 设 X 和 Y 为 $\mathfrak{C}$ 的任意二对象. 对于任一 $f\in \mathrm{Hom}_{\mathfrak{C}}(X,Y)$, F 规定了 $\mathrm{Hom}_{\mathfrak{D}}(F(X),F(Y))$ 中的一个元素 (态射) $F(f)$, 满足:

$$F(g\circ f)=F(g)\circ F(f)\quad (\forall\, f\in \mathrm{Hom}_{\mathfrak{C}}(X,Y), g\in \mathrm{Hom}_{\mathfrak{C}}(Y,Z))\tag{0.2}$$

以及

$$F(\mathrm{id}_X)=\mathrm{id}_{F(X)}.$$

如果将 (0.2) 式改为

$$F(g\circ f)=F(f)\circ F(g)\quad (\forall\, f\in \mathrm{Hom}_{\mathfrak{C}}(X,Y),\ g\in \mathrm{Hom}_{\mathfrak{C}}(Y,Z)),$$

则称 F 为由 $\mathfrak{C}$ 到 $\mathfrak{D}$ 的一个**反变函子**. 共变函子和反变函子统称为**函子**.

相应于一个范畴 $\mathfrak{C}$, 有它的**反范畴**(记为 $\mathfrak{C}^0$). $\mathfrak{C}^0$ 的对象与 $\mathfrak{C}$ 的对象相同, 但是对于 $\mathfrak{C}^0$ 中二对象 X, Y 之间的态射集合规定为 $\mathrm{Hom}_{\mathfrak{C}^0}(X,Y)=\mathrm{Hom}_{\mathfrak{C}}(Y,X)$. 于是, 由范畴 $\mathfrak{C}$ 到范畴 $\mathfrak{D}$ 的反变函子可以视为由 $\mathfrak{C}^0$ 到 $\mathfrak{D}$ 的共变函子.

用函子可以定义两个范畴的同构.

定义 2.6 设 $\mathfrak{C}$ 和 $\mathfrak{D}$ 是两个范畴. 如果存在函子 $F:\mathfrak{C}\to\mathfrak{D}$ 和函子 $G:\mathfrak{D}\to\mathfrak{C}$, 满足:

(1) 对于 $\mathfrak{C}$ 的任一对象 X, $\mathfrak{D}$ 的任一对象 Y, 都有

$$G(F(X))=X,\quad F(G(Y))=Y;$$

(2) 对于 $\mathfrak{C}$ 的任二对象 X 和 X', $\mathfrak{D}$ 的任二对象 Y 和 Y', 都有

$$G(F(f))=f\quad (\forall\, f\in \mathrm{Hom}_{\mathfrak{C}}(X,X')),$$
$$F(G(g))=g\quad (\forall\, g\in \mathrm{Hom}_{\mathfrak{D}}(Y,Y')),$$

则称 F 是由 $\mathfrak{C}$ 到 $\mathfrak{D}$ 的一个**同构**, 同时也称 $\mathfrak{C}$ 与 $\mathfrak{D}$ 是**同构的**或**等价的**.

对于给定的两个范畴, 联系它们之间的函子的概念是"函子态射"(或"自然变换").

定义 2.7 设 $\mathfrak{C}$ 和 $\mathfrak{D}$ 是两个范畴, F 和 G 为由 $\mathfrak{C}$ 到 $\mathfrak{D}$ 的两个函子. 由 F 到 G 的一个**函子态射** Φ 是指: 对于 $\mathfrak{C}$ 的任一对象 X, 给定一个态射 $\Phi_X: F(X)\to G(X)$, 使得下面的图表交换:

$$\begin{tikzcd} F(X) \arrow[r, "\Phi_X"] \arrow[d, "F(f)"'] & G(X) \arrow[d, "G(f)"] \\ F(Y) \arrow[r, "\Phi_Y"] & G(Y) \end{tikzcd}$$

其中 X, Y 为 $\mathfrak{C}$ 的任意两个对象，f 为 X 到 Y 的任一态射. 由 F 到 G 的函子态射的全体记为 $\mathrm{Hom}_{(\mathfrak{C},\mathfrak{D})}(F, G)$. 进一步，如果上述的 Φ_X $(\forall X \in \mathrm{Orb}(\mathfrak{C}))$ 都是同构，则称 Φ 是一个**函子同构**, 并称同构 Φ_X 是**自然的**.

在很多范畴中存在具有特殊重要性的下述对象.

定义 2.8 设 $\mathfrak{C}$ 是一个范畴. $\mathfrak{C}$ 的一个对象 U 称为**始对象**, 如果对于 $\mathfrak{C}$ 的任一对象 X, $\mathrm{Hom}_{\mathfrak{C}}(U, X)$ 都只含有一个元素; 类似地，$\mathfrak{C}$ 的一个对象 Z 称为**终对象**, 如果对于 $\mathfrak{C}$ 的任一对象 X, $\mathrm{Hom}_{\mathfrak{C}}(X, Z)$ 都只含有一个元素.

容易看出，如果一个范畴中存在始对象，则所有的始对象都是同构的. 对于终对象也是如此.

第 1 章　模

在代数学中，除了研究某种代数结构 (如群、环、域、体等) 自身的内部结构之外，考虑代数结构之间的联系也具有重要的意义. 这种联系通常以一种代数结构在另一种代数结构上的“作用”, 即在两个代数结构的元素之间定义某种适当的运算 (请回想“群在集合上的作用”) 的方式实现. 这种考虑使得我们有可能对于各种代数结构的研究更加深入. 本章所讨论的**模**就是具有环作用的交换群. 许多在表面上看来差异很大的代数结构 (如交换群、环、理想、线性空间等) 在模的语言下都统一了起来.

我们首先回顾一下有关环的基本知识.

§1.0　环论知识的复习

本节主要简述在抽象代数 I 课程中读者已经学过的环论知识, 可供读者自己检查是否已经熟知它们. 除了定理 0.25 之外, 教师不一定要讲解.

1.0.1　基本知识

定义 0.1　非空集合 R 称为一个**环**, 如果在 R 中定义了两个二元运算 (叫做加法和乘法), 满足以下六个条件:

(1) 加法结合律:　$(a+b)+c=a+(b+c)$, $\forall\, a,b,c\in R$;

(2) 加法交换律:　$a+b=b+a$, $\forall\, a,b\in R$;

(3) 存在零元素: 存在 $0\in R$, 使对任意的 $a\in R$, 恒有 $0+a=a$;

(4) 存在负元素: 对任意的 $a\in R$, 存在 $-a\in R$, 使得 $a+(-a)=0$;

(5) 乘法结合律:　$(ab)c=a(bc)$, $\forall\, a,b,c\in R$;

(6) 左、右分配律:

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca,\quad \forall\, a,b,c\in R.$$

若环 R 的乘法还满足

(7) 乘法交换律： $ab=ba,\ \forall\ a,b\in R,$

则称 R 为**交换环**.

至少含有两个元素的环 R 若有乘法幺元，即存在 $1\in R$, 使得

$$1a=a1=a,\quad \forall\ a\in R,$$

则称 R 为**有幺元的环**, 或**有 1 的环**, 或**幺环**. 如果有幺元的环 R 的任一非零元素皆有乘法逆元，即对任意的 $a\in R$, $a\neq 0$, 存在 $a^{-1}\in R$, 使得

$$aa^{-1}=a^{-1}a=1,$$

则称 R 为**体**. 乘法满足交换律的体称为**域**.

定义 0.2 设 R 是环，$a\in R$. 如果存在 $b\in R$, $b\neq 0$, 使得 $ab=0$, 则称 a 为 R 的一个**左零因子**.

类似地可定义 R 的**右零因子**.

显然，在交换环中左、右零因子是同一概念 (称为**零因子**).

定义 0.3 设 R 是环，$a\in R$. 若存在正整数 n, 使得 $a^n(=\underbrace{a\cdots a}_{n\text{个}})=0$, 则称 a 为一个**幂零元**.

显然幂零元都是左、右零因子.

定义 0.4 无非零零因子的交换幺环称为**整环**.

下面叙述商域的概念. 设 R 是整环. 令

$$S=\{(a,b)\mid a,b\in R, b\neq 0\}.$$

在 S 上定义一个关系 “$\sim$”:

$$(a,b)\sim(a',b')\ \text{当且仅当}\ ab'=a'b.$$

易验证 $\sim$ 是 S 上的等价关系. 以 $S/\sim$ 记等价类的集合，以 $\overline{(a,b)}$ 记 (a,b) 所在的等价类. 在 $S/\sim$ 上定义加法和乘法如下：

$$\overline{(a,b)}+\overline{(c,d)}:=\overline{(ad+bc,bd)},$$

$$\overline{(a,b)}\ \overline{(c,d)} := \overline{(ac,bd)}.$$

易验证此二运算是良定义的, 并且 $S/\sim$ 在此二运算下构成一个域. 此时 R 与 $S/\sim$ 的子集 $\{\overline{(a,1)}|a\in R\}$ 之间有双射: $a\leftrightarrow\{\overline{(a,1)}\}$. 在此双射下 R 可视为 $S/\sim$ 的 子环(见定义 0.8).

定义 0.5 上面定义的域 $S/\sim$ 称为整环 R 的**商域**.

定义 0.6 设 R 是幺环, $a,b\in R$. 如果 $ab=1$, 则称 a 为 b 的**左逆元**, b 为 a 的**右逆元**. 如果 $ab=ba=1$, 则称 a 为 R 的**可逆元**或**单位**. R 的可逆元的全体构成 (乘法) 群, 称为 R 的**单位群**.

定义 0.7 设 S 和 T 为环 R 的非空子集, S 和 T 的**和**、**差**与**积**分别定义为

$$S+T:=\{a+b\mid a\in S,b\in T\},$$
$$S-T:=\{a-b\mid a\in S,b\in T\},$$
$$ST:=\{ab\mid a\in S,b\in T\}.$$

定义 0.8 若环 R 的非空子集 S 关于 R 的加法、乘法构成环, 则称 S 为 R 的**子环**. 此时亦称 R 是 S 的**扩环**.

易见 S 是 R 的子环当且仅当 $S-S\subseteq S$ 且 $SS\subseteq S$.

定义 0.9 设 S 是交换幺环 R 的扩环, T 是 S 的一个子集. 所谓 R 上**由 T 生成的环** (或由 T **生成的 R-代数**) 是指 S 中包含 T 的最小的 R 的扩环, 记为 $R[T]$. 若 $S=R[T]$, 则称 T 是 S 的 **R-生成元集**, 亦称 S **在 R 上由 T 生成**. 可以由有限集合生成的 R 的扩环称为 R 上**有限生成的环** (或有限生成代数、有限型代数).

定义 0.10 若环 R 的子环 I 还满足 $IR\subseteq I$(或 $RI\subseteq I$), 则称 I 为 R 的**右** (或**左**) **理想**. 若 I 同时是 R 的左、右理想, 则称 I 为 R 的**双边理想**, 简称为**理想**.

定义 0.11 设 R 是环, $T\subseteq R$. 所谓 R 中**由 T 生成的右理想**是指 R 中包含 T 的最小的右理想. 可以由有限集合生成的 R 的右理想称为 R 的**有限生成的右理想**. 对于左理想和双边理想有类似概念. 特别地, 由一个元素 (构成的集合) 生成的理想称为**主理想**.

设 I 为环 R 的一个理想, $a\in R$. 称 $a+I(=\{a\}+I)$ 为 a 所代表的 I 的 (加法)**陪集**. 对于给定的环 R 的理想 I, R 等于 I 的所有陪集的无交并. 在这些陪集组成的集合上定义加法、乘法:

$$(a+I)+(b+I):=(a+b)+I;\quad (a+I)(b+I):=(ab)+I.$$

可以验证这样定义的加法、乘法是良定义的 (即与陪集代表的选取无关). 进而言之, 陪集集合关于此加法、乘法构成环.

定义 0.12 设 R 是环, I 是 R 的理想, 则称上面构造的环为 R 关于 I 的**商环**.

定义 0.13 设 R 和 R' 是环, $\varphi\colon R\to R'$ 是映射. 如果对于所有的 $a,b\in R$ 都有

$$(a+b)^{\varphi}=a^{\varphi}+b^{\varphi},\quad (ab)^{\varphi}=a^{\varphi}b^{\varphi},$$

则称 φ 为 (由 R 到 R' 的) **环同态**. 如果同态 φ 又是单 (满) 射, 则称 φ 为**单 (满) 同态**. 既单又满的同态称为**同构**.

若将定义 0.13 中的条件 $(ab)^{\varphi}=a^{\varphi}b^{\varphi}$ 改为 $(ab)^{\varphi}=b^{\varphi}a^{\varphi}$, 则称 φ 为 (由 R 到 R' 的) **环反同态**. 相应地有**单 (满) 反同态**和**反同构**.

定义 0.14 设 $\varphi\colon R\to R'$ 是环同态. φ 的**核**定义为

$$\ker\varphi:=\{a\in R\mid a^{\varphi}=0\};$$

φ 的**像**定义为

$$\operatorname{im}\varphi:=\{a'\in R'\mid 存在\ a\in R,\ 使得\ a^{\varphi}=a'\}.$$

定理 0.15 (同态基本定理) 设 $\varphi\colon R\to R'$ 是环同态, 则

(1) $\ker\varphi$ 是 R 的理想;

(2) $\operatorname{im}\varphi$ 是 R' 的子环;

(3) $\overline{\varphi}\colon R/\ker\varphi\to\operatorname{im}\varphi$, $(a+\ker\varphi)^{\overline{\varphi}}=a^{\varphi}$ $(a\in R)$ 是环同构.

推论 0.16 设 $\varphi\colon R\to R'$ 是环同态, 则

(1) φ 是单同态当且仅当 $\ker\varphi=\{0\}$;

(2) φ 是满同态当且仅当 $\operatorname{im}\varphi=R'$.

定理 0.17 (第一同构定理) 设 φ: $R \to R'$ 是环的满同态，则

(1) R 中包含 $\ker\varphi$ 的子环与 R' 的子环在 φ 下一一对应；

(2) R 中包含 $\ker\varphi$ 的理想与 R' 的理想在 φ 下一一对应；

(3) 设 I 为 R 中包含 $\ker\varphi$ 的理想，在 φ 下对应于 R' 的理想 I'，则

$$\begin{aligned} R/I &\to R'/I', \\ a+I &\mapsto a^{\varphi}+I' \quad (a \in R) \end{aligned}$$

是环同构.

推论 0.18 设 $J \subseteq I$ 都是环 R 的理想，则 I/J 是 R/J 的理想，且有环同构

$$(R/J)/(I/J) \cong R/I.$$

定理 0.19 (第二同构定理) 设 S 是环 R 的子环，I 是 R 的理想，则

(1) I 是子环 $S+I$ 的理想；

(2) $S \cap I$ 是 S 的理想；

(3) 映射

$$\begin{aligned} (S+I)/I &\to S/(S\cap I), \\ (s+i)+I &\mapsto s+(S\cap I) \quad (s \in S,\ i \in I) \end{aligned}$$

是环同构.

定义 0.20 设 $R_1, \cdots, R_n$ 都是环. 令

$$R_1 \oplus \cdots \oplus R_n = \{(a_1, \cdots, a_n) \mid a_i \in R_i (1 \leq i \leq n)\}.$$

在 $R_1 \oplus \cdots \oplus R_n$ 中规定二元素的加法、乘法为按分量进行运算，则 $R_1 \oplus \cdots \oplus R_n$ (构成环) 称为 $R_1, \cdots, R_n$ 的**直和**(或外直和).

命题 0.21 设 $I_1, \cdots, I_n$ 都是环 R 的理想，$R = I_1 + \cdots + I_n$，则下述四条等价：

(1) 映射

$$I_1 \oplus \cdots \oplus I_n \to R,$$

$$(a_1,\cdots,a_n) \mapsto a_1+\cdots+a_n$$

是环同构;

(2) R 中任一元素表示为 $I_1,\cdots,I_n$ 的元素之和的表示法唯一;

(3) 0 表示为 $I_1,\cdots,I_n$ 的元素之和的表示法唯一;

(4) 对于任一 i $(1\le i\le n)$, 有

$$(I_1+\cdots+I_{i-1}+I_{i+1}+\cdots+I_n)\cap I_i=\{0\}.$$

(此时我们称 R 等于 $I_1,\cdots,I_n$ 的**内直和**, 亦记为 $R=I_1\oplus\cdots\oplus I_n$.)

1.0.2 素理想与极大理想

本小节中的环都设定为交换幺环.

定义 0.22 设 P 为交换幺环 R 的理想, $P\neq R$. 如果对于任意的 $a,b\in R$, $ab\in P$ 蕴含 $a\in P$ 或 $b\in P$, 则称 P 为 R 的**素理想**. 如果对于任意理想 I, $I\supsetneqq P$ 蕴含 $I=R$, 则称 P 为 R 的**极大理想**.

定理 0.23 设 R 是交换幺环, 则

(1) P 是素理想当且仅当商环 R/P 是整环;

(2) P 是极大理想当且仅当商环 R/P 是域.

推论 0.24 交换幺环的极大理想必是素理想.

下面我们证明极大理想的存在性.

定理 0.25 交换幺环中必存在极大理想.

证明 以 S 记 R 的不等于 R 的所有理想的集合. 则 $\{0\}\in S$, 故 S 非空. 在 S 上定义偏序 "$\le$":

$$I_1\le I_2 \text{ 当且仅当 } I_1\subseteq I_2.$$

(易验证 "$\le$" 确实是偏序关系). 我们断言 S 中存在极大元. 事实上, 对于 S 中的任一全序链

$$I_1\le I_2\le\cdots, \tag{0.1}$$

令 $I=\bigcup\limits_i I_i$. 易验证 I 是 R 的理想, 且 $I\neq R$(因为 $1\notin I$), 故 $I\in S$. 显然 $I_i\le I(\forall\, I)$, 所以 I 是链 (0.1) 的一个上界. 由 Zorn 引理即知

我们的断言为真. 现在设 M 是 S 的一个极大元. 易见 M 是极大理想. 事实上, 若有 R 的理想 J, $J \supsetneq M$, 则 $J \notin S$(否则矛盾于 M 是 S 的极大元). 这意味着 $J = R$. 这就证明了 M 是 R 的极大理想. □

说明 定理 0.25 的证明适用于一般的幺环 (不一定交换). 但是, 对于没有 1 的环这个定理一般讲来并不成立.

1.0.3 多项式环

本小节中的环仍然都假定为交换幺环.

定义 0.26 设 R 为交换幺环. 令

$$S = \{(a_0, a_1, \cdots, a_n, \cdots) \mid a_i \in R(\forall\, i), \text{有限多个 } a_i \text{ 不为零}\}.$$

在 S 上定义加法、乘法:

$$\begin{aligned}&(a_0, a_1, \cdots, a_n, \cdots) + (b_0, b_1, \cdots, b_n, \cdots)\\ &\qquad\qquad := (a_0 + b_0, a_1 + b_1, \cdots, a_n + b_n, \cdots),\\ &(a_0, a_1, \cdots, a_n, \cdots)\cdot(b_0, b_1, \cdots, b_n, \cdots) := (c_0, c_1, \cdots, c_n, \cdots),\end{aligned}$$

其中

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

则 S 在此加法、乘法下构成环, 称为 R 上的**一元多项式环**.

若将 $(0, 1, 0, \cdots)$ 记为 x, 则 R 上的一元多项式环等同于

$$\{a_0 + a_1 x + \cdots + a_m x^m \mid m\text{为非负整数}, a_i \in R\}$$

(其上的运算与通常多项式的运算相同). 因此我们称此多项式环为 R 上的**变元为 x 的一元多项式环**, 记为 $R[x]$.

归纳地可以定义环 R 上的多元多项式环

$$R[x_1, x_2] := R[x_1][x_2],$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$R[x_1, \cdots, x_t] := R[x_1, \cdots, x_{t-1}][x_t].$$

下面的定理是多项式环的刻画性质.

定理 0.27 *R 上有限生成的环是 R 上的 (多元) 多项式环的同态像.*

若 $f(x)=a_0+a_1x+\cdots+a_nx^n\in R[x]$, $a_n\neq 0$, 则称 n 为 $f(x)$ 的**次数**, 记为 $n=\deg f(x)$.

命题 0.28 设 R 为整环, $f(x),g(x)\in R[x]$, $f(x)g(x)\neq 0$, 则

$$\deg(f(x)g(x))=\deg f(x)+\deg g(x).$$

推论 0.29 *整环上的多项式环仍是整环.*

定理 0.30 (带余除法) 设 K 为域, $f(x),g(x)\in K[x]$, $g(x)\neq 0$, 则存在唯一的 $q(x),r(x)\in K[x]$, 满足

$$f(x)=q(x)g(x)+r(x),\qquad \deg r(x)<\deg g(x) \text{ 或 } r(x)=0.$$

1.0.4 整除性理论

本小节中的环都是指整环.

定义 0.31 设 R 为整环, $a,b\in R$. 如果存在 $c\in R$ 使得 $b=ac$, 则称 a 是 b 的**因子**, b 是 a 的**倍式**, 同时称a **整除** b, 记为 $a|b$. 如果 $a,b\neq 0$, $a|b$ 且 $b|a$, 则称 a 与 b **相伴**, 记为 $a\sim b$.

显然, 如果 $a=bc$, 则 $a\sim b$ 当且仅当 c 为 R 的可逆元.

定义 0.32 设 R 为整环, $a_1,\cdots,a_n,b\in R$. 如果 $b|a_i$ $(\forall 1\leq i\leq n)$, 则称 b 为 $a_1,\cdots,a_n$ 的**公因子**. 如果 d 是 $a_1,\cdots,a_n$ 的公因子, 且 $a_1,\cdots,a_n$ 的任一公因子都整除 d, 则称 d 为 $a_1,\cdots,a_n$ 的**最大公因子**, 记为 $d=\gcd(a_1,\cdots,a_n)$ 或 $d=(a_1,\cdots,a_n)$. 相反地, 如果 $a_i|b$ $(\forall 1\leq i\leq n)$, 则称 b 为 $a_1,\cdots,a_n$ 的**公倍式**. 如果 c 是 $a_1,\cdots,a_n$ 的公倍式, 且 c 整除 $a_1,\cdots,a_n$ 的任一公倍式, 则称 c 为 $a_1,\cdots,a_n$ 的**最小公倍**, 记为 $c=\mathrm{lcm}\ (a_1,\cdots,a_n)$ 或 $c=[a_1,\cdots,a_n]$.

一般而言, 整环中的一些元素的最大公因子和最小公倍不一定存在.

定义 0.33 设 R 为整环, $a \in R, a \neq 0$ 且 a 不是可逆元. 如果 $a = bc(b, c \in R)$ 蕴含 b 为可逆元或 c 为可逆元, 则称 a 为 R 的**不可约元**; 如果 $a|bc(b, c \in R)$ 蕴含 $a|b$ 或 $a|c$, 则称 a 为 R 的**素元**.

不难证明素元必是不可约元, 但反之则未必.

定义 0.34 设 R 为整环. 如果 R 的任一非零元素都可以表示为有限多个不可约元的乘积, 并且这种表达式是唯一的, 即: 对于任一 $a \in R, a \neq 0$, 如果

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

(其中 $p_i (1 \leq i \leq n)$, $q_j (1 \leq j \leq m)$ 都是不可约元), 则必有 $n = m$, 且适当调换 q_j 的顺序可以使得 $p_i \sim q_i$ $(\forall\, 1 \leq i \leq n)$, 则称 R 是**唯一分解整环**.

定理 0.35 设 R 是整环, 且 R 的任一非零不可逆元都可以表示为有限多个不可约元的乘积, 则下述六条结论等价:

(1) R 是唯一分解整环;

(2) R 中不可约元都是素元;

(3) R 中任意两个元素都有最大公因子;

(4) R 中任意有限多个元素都有最大公因子;

(5) R 中任意两个元素都有最小公倍;

(6) R 中任意有限多个元素都有最小公倍.

定义 0.36 设 R 为整环. 如果 R 的任一理想都是主理想, 则称 R 是**主理想整环**.

设 R 是交换幺环, $a_1, \cdots, a_n \in R$. 我们以 $(a_1, \cdots, a_n)$ 记 (R 的) 由 $\{a_1, \cdots, a_n\}$ 生成的理想. 对于主理想整环 R 以及 $a, b \in R$, 容易验证

$$(a, b) = (c) \text{ 当且仅当 } c \text{ 是 } a, b \text{ 的最大公因子.}$$

因此有

定理 0.37 主理想整环是唯一分解整环.

定义 0.38 设 R 为整环. 如果存在 $R \setminus \{0\}$ 到自然数集 $\mathbb{N}$ 的映射 d, 满足: 对于任意的 $a, b \in R (b \neq 0)$, 存在 $q, r \in R$, 使得

$$a = qb + r, \qquad r = 0 \text{ 或 } d(r) < d(b),$$

则称 R 为**欧几里得环**.

不难证明

定理 0.39 欧几里得环是主理想整环，因而是唯一分解整环.

关于多项式环，一个重要的结果是

定理 0.40 唯一分解整环上的一元多项式环仍是唯一分解整环.

推论 0.41 唯一分解整环上的多元多项式环仍是唯一分解整环.

定理 0.40 的基础是所谓 "Gauss 引理" 以及域上的一元多项式环是欧几里得环. Gauss 引理是关于 "本原多项式" 的一个结果.

定义 0.42 设 R 是唯一分解整环，$f(x) \in R[x]$. 如果 $f(x)$ 的各项系数的最大公因子为 1, 则称 $f(x)$ 为 $R[x]$ 中的**本原多项式**.

引理 0.43 (Gauss 引理) 设 R 是唯一分解整环，则 $R[x]$ 中二本原多项式的乘积仍为 $R[x]$ 中的本原多项式.

关于多项式的不可约性，有

命题 0.44 (Eisenstein 判别法) 设 R 是唯一分解整环，K 为 R 的商域，$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in R[x]$. 如果存在 R 的素元 p, 满足

$$p \nmid a_0, \quad p | a_i \ (\forall\, 1 \le i \le n), \quad p^2 \nmid a_n,$$

则 $f(x)$ 在 $K[x]$ 中不可约.

§1.1 模的定义及例

定义 1.1 设 R 是有 1 的环，M 是一个交换群. 如果给定一个映射

$$M \times R \to M,$$

$$(x, a) \mapsto xa$$

满足下述条件:

(1) $(x+y)a = xa + ya,\ \forall\, x, y \in M,\ a \in R$;

(2) $x(a+b) = xa + xb,\ \forall\, x \in M,\ a, b \in R$;

(3) $x(ab) = (xa)b,\ \forall\, x \in M,\ a, b \in R$;

(4) $x1 = x$,

则称 M 为环 R 上的一个**右模**, 或**右 R 模**.

右模还有另一种常见的写法: 将交换群 M 中的运算记为乘法, 而将环 R 在 M 上的作用写成方幂的形式, 即: 将定义 1.1 中的 xa 改写为 x^a.

如果将此定义中的条件 (3) 改为

(3′) $x(ab) = (xb)a,\ \forall\, x \in M,\ a, b \in R$,

其余条件不变, 则称 M 为环 R 上的一个**左模**, 或**左 R 模**. 此时, 将环作用中的环元素写在模元素的左边较为方便, 即: 将上述定义中的映射改为

$$\begin{aligned} R \times M &\to M, \\ (a, x) &\mapsto ax. \end{aligned}$$

应当指出, 从理论上讲, 左模和右模没有本质上的区别. 如果 M 为环 R 上的一个右模, 令 R' 为与 R 反同构的环 (具体地说, R' 作为加法群与 R 一样, R' 中的乘法 xy 定义为 R 中的 yx), 则 M 构成 R' 上的左模. 当然, 若 R 是交换环, 则 R 上的左模和右模没有差别.

以下, 除非特别声明, 我们所说的模都是右模.

只含有一个元素 “0” 的模称为**零模**.

例 1.2 交换群与 $\mathbb{Z}$ 模是等同的. 事实上, 设 M 是一个交换群 (其运算记为加法), 则整数环 $\mathbb{Z}$ 在 M 上有自然的作用:

$$\begin{aligned} M \times \mathbb{Z} &\to M, \\ (x, n) &\mapsto nx. \end{aligned}$$

此作用显然满足定义 1.1 中的四个条件, 所以 M 是 $\mathbb{Z}$ 模. 反之, 任一 $\mathbb{Z}$ 模当然是交换群.

例 1.3 设 M 是一个交换群，则 M 是其自同态环 $\mathrm{End}(M)$ 上的模. 结合例 1.2, 可以认为 $\mathbb{Z} \subseteq \mathrm{End}(M)$.

例 1.4 设 R 是一个环. 规定 R 在加法群 $(R,+)$ 上的作用为右(左) 乘，则 $(R,+)$ 是右 (左) R 模.

例 1.5 域 F 上的线性空间与 F 模是同一回事 (F 在线性空间上的作用规定为数乘).

§1.2 子模与商模，模的同态与同构

定义 2.1 设 M 是 R 模， $N \subseteq M$. 如果将 R 在 M 上的作用限制在 N 上使得 N 成为 R 模, 则称 N 为 M 的一个**子模**.

不难看出，为了验证 R 模 M 的子集 N 是一个子模，只需验证 N 是 M 的子群，并且 N 在 R 作用下封闭.

在上节的例 1.2 中模的子模与子群是同一概念；例 1.3 的子模是子群，但是子群不一定是子模；例 1.5 的子模就是线性子空间；而例 1.4 所述的 $(R,+)$ 作为右 (左)R 模的子模就是环 R 的右 (左) 理想.

设 $M_i(i \in I)$(这里 I 是一个指标集) 为 R 模 M 的一族子模. 定义 $M_i(i \in I)$ 的**交** 为通常集合的交，即 $\bigcap\limits_{i\in I} M_i$; 定义 $M_i(i \in I)$ 的**和**为

$$\sum_{i\in I} M_i = \{x_{i_1} + \cdots + x_{i_n} \mid n \in \mathbb{N}, i_1, \ldots, i_n \in I\}.$$

读者可自行验证它们都是 M 的子模.

定义 2.2 设 N 为 R 模 M 的子模. 规定 R 在商群 M/N 上的作用为

$$\begin{aligned} M/N \times R &\to M/N, \\ (x+N, a) &\mapsto xa + N, \end{aligned}$$

则 M/N 成为一个 R 模，称为 M 关于 N 的**商模**.

应当指出，此定义中的 R 在 M/N 上的作用是良定义的. 这是因为 N 是 M 的子模 (不仅仅是子群).

定义 2.3　设 M 和 T 都是 R 模，$\varphi: M \to T$ 是映射. 如果 φ 满足下述两个条件：

(1) $(x+y)^\varphi = x^\varphi + y^\varphi$, $\forall\, x, y \in M$;

(2) $(xa)^\varphi = x^\varphi a$, $\forall\, x \in M$, $a \in R$,

则称 φ 为 M 到 T 的一个 R **模同态**. 如果 φ 又是单 (满) 射，则称 φ 为 R 模的**单 (满) 同态**. 既单又满的模同态称为**模同构**. 由 M 到 T 的所有 R 模同态构成的集合记为 $\mathrm{Hom}_R(M,T)$; 如果 $T = M$, 则记 $\mathrm{Hom}_R(M,T)$ 为 $\mathrm{End}_R(M)$.

说明　在 $\mathrm{Hom}_R(M,T)$ 上定义加法：对于 $\varphi, \psi \in \mathrm{Hom}_R(M,T)$, 令 $x^{\varphi+\psi} = x^\varphi + x^\psi$ $(x \in M)$(易验证 $\varphi + \psi \in \mathrm{Hom}_R(M,T)$), 则 $\mathrm{Hom}_R(M,T)$ 在此加法下构成交换群. 在 $\mathrm{End}_R(M)$ 上进一步定义乘法为映射的复合，即对于 $\varphi, \psi \in \mathrm{End}_R(M)$, 令 $x^{\varphi\psi} = (x^\varphi)^\psi$ $(x \in M)$, 则 $\mathrm{End}_R(M)$ 构成环.

类似于群的情形，对于模同态 $\varphi: M \to T$, 定义 φ 的**核**和**像**分别为

$$\ker\varphi = \{x \in M \mid x^\varphi = 0\},$$

$$\mathrm{im}\varphi = \{y \in T \mid \text{存在 } x \in M, \text{ 使得 } x^\varphi = y\}.$$

又定义 φ 的**余核**为

$$\mathrm{coker}\,\varphi = T/\mathrm{im}\,\varphi.$$

容易验证 $\ker\varphi$ 和 $\mathrm{im}\varphi$ 分别是 M 和 T 的子模，并且 φ 是单同态当且仅当 $\ker\varphi = \{0\}$; φ 是满同态当且仅当 $\mathrm{coker}\varphi = \{0\}$.

关于模同态和模同构，有以下的结果.

定理 2.4 (同态基本定理)　设 $\varphi: M \to T$ 是模同态，则

$$\begin{aligned} M/\ker\varphi &\to \mathrm{im}\varphi, \\ \bar{x} &\mapsto \varphi(x) \end{aligned}$$

是模同构，其中 $\bar{x} = x + \ker\varphi$, 是 x 所代表的陪集.

定理 2.5 (第一同构定理)　设 $\varphi: M \to M'$ 是模的满同态，则

(1) M 中包含 $\ker\varphi$ 的子模与 M' 的子模在 φ 下一一对应;

(2) 设 T 为 M 中包含 $\ker\varphi$ 的子模，在 φ 下对应于 M' 的子模 T', 则

$$M/T \to M'/T',$$
$$x+T \mapsto x^{\varphi}+T'$$

是模同构.

推论 2.6 设 N 为 M 的子模， $\pi: M \to M/N, \pi(x) = x+N$ 是典范同态，则在 π 下 M 的包含 N 的子模与 M/N 的子模一一对应；对于 M 的包含 N 的子模 H,

$$M/H \to (M/N)/(H/N),$$
$$x+H \mapsto x^{\pi}+(H/N)$$

是模同构.

定理 2.7 (第二同构定理) 设 H 和 N 为 M 的子模，则有同构

$$(H+N)/N \to H/(H\cap N),$$
$$(h+n)+N \mapsto h+(H\cap N) \quad (\forall\, h\in H, n\in N).$$

这些定理的证明和群论中相应定理的证明类似，在此略去.

在本节最后我们给出模的生成元集的概念.

定义 2.8 设 M 是一个 R 模， $S\subset M$. 所谓**由 S 生成的子模** (记为 $S\cdot R$ 或 SR) 是指 M 的包含 S 的所有子模的交，同时称 S 为 $S\cdot R$ 的一个**生成元集**. 特别地，若 $S\cdot R=M$, 则称 M 由 S**生成**. 如果 M 可以由其有限子集生成，则称 M 是**有限生成的**, 否则称 M 是**无限生成的**. 可以由一个元素 (构成的子集) 生成的模称为**循环模**.

不难看出： $S\cdot R$ 是 M 的包含 S 的最小的子模，同时也有

$$S\cdot R=\left\{\sum_{\text{有限}} s_i a_i \,\middle|\, s_i\in S, a_i\in R\right\}.$$

§1.3 模的直和与直积

定义 3.1 设 I 为一个指标集， $M_i (i\in I)$ 都是 R 模. 令

$$M' = \{(\cdots, x_i, \cdots) \mid x_i \in M_i\}$$

为 M_i $(i \in I)$ 中元素的 "序列" 组成的集合. 定义 M' 中的加法为对应的分量相加, R 在 M' 上的作用为作用到各分量上, 即: 对于 $(\cdots, x_i, \cdots), (\cdots, y_i, \cdots) \in M'$ 和 $a \in R$,

$$(\cdots, x_i, \cdots) + (\cdots, y_i, \cdots) := (\cdots, x_i + y_i, \cdots),$$
$$(\cdots, x_i, \cdots)a := (\cdots, x_i a, \cdots),$$

则 M' (是 R 模) 称为 $M_i (i \in I)$ 的**直积**, 记为 $\prod\limits_{i \in I} M_i$. 又令

$$M = \{(\cdots, x_i, \cdots) \mid x_i \in M_i, \text{ 只有有限多个 } x_i \neq 0\},$$

M 中的加法和 R 在 M 上的作用同上, 则称 M(也是 R 模) 为 $M_i (i \in I)$ 的**直和**, 记为 $\bigoplus\limits_{i \in I} M_i$.

说明 (1) 当 I 是有限集时, 直和与直积是同样的概念; 当 I 是无限集时, 直和是直积的子模.

(2) 当 I 不是可列集时, 此定义中 "序列" 一词及符号 $(\cdots, x_i, \cdots)$ 有含糊之处. 直和与直积的确切的定义可以用范畴论的语言给出. 在那里, 直和与直积是互为对偶的概念, 即分别是两个 "对偶的" 范畴的始对象和终对象. 详言之, 对于给定的一组 R 模 $M_i (i \in I)$, 定义一个范畴 $\mathfrak{C}$, 其对象为 R 模 N 连同一组 R 模同态 $\phi_i: M_i \to N (\forall\, i \in I)$, 记为 (N, ϕ). 由一个对象 (N, ϕ) 到另一对象 (T, ψ) 的态射的集合定义为满足 $\phi_i \eta = \psi_i$ $(\forall\, i \in I)$ 的 R 模同态 $\eta: N \to T$, 也就是使得下面图表交换的同态 η:

$$\begin{tikzcd} & N \arrow[dd, "\eta"] \\ M_i \arrow[ur, "\phi_i"] \arrow[dr, "\psi_i"'] & \\ & T \end{tikzcd}$$

则 $\bigoplus\limits_{i\in I} M_i$ 是此范畴的始对象. $\mathfrak{C}$ 的对偶范畴 $\hat{\mathfrak{C}}$ 的对象为 R 模 N 连同一组 R 模同态 $\hat{\phi}_i: N \to M_i(\forall\, i \in I)$, 记为 $(N, \hat{\phi})$. 由一个对象 $(T, \hat{\psi})$ 到另一对象 $(N, \hat{\phi})$ 的态射的集合定义为满足 $\hat{\eta}\hat{\phi}_i = \hat{\psi}_i(\forall\, i \in I)$ 的 R 模同态 $\hat{\eta}: T \to N$, 也就是使得下面图表交换的的同态 $\hat{\eta}$:

$$\begin{tikzcd} & N \arrow[dl, "\hat{\phi}_i"'] \\ M_i & \\ & T \arrow[ul, "\hat{\psi}_i"] \arrow[uu, "\hat{\eta}"'] \end{tikzcd}$$

则 $\prod\limits_{i\in I}$ 是范畴 $\hat{\mathfrak{C}}$ 的终对象. 注意: 定义 3.1 中对于直和所加的条件"只有有限多个 $x_i \neq 0$" 在范畴语言的叙述中反映为: $\mathfrak{C}$ 的对象中的任一 R 模 N 中的运算只能是有限次加法及 R 作用的复合. 因此, 如果对象 (N, ϕ) 中有无穷多个 $i \in I$ 使得 $\phi_i: M_i \to N$ 不是零同态, 则由对象 (N, ϕ) 到任一对象 (T, ψ) 的态射的集合为空集, 故这样的对象不可能是 $\mathfrak{C}$ 的始对象.

如同线性空间的直和分解一样, 我们希望将一个模分解为它的一些子模的直和. 在这里我们只考虑有限的直和分解.

定理 3.2 设 $M_1, \cdots, M_n$ 是 M 的子模, $M = \sum\limits_{i=1}^{n} M_i$, 则下述四条等价:

(1) 映射

$$\begin{aligned} \varphi:\ M_1 \oplus \cdots \oplus M_n &\to M, \\ (x_1, \cdots, x_n) &\mapsto x_1 + \cdots + x_n \end{aligned}$$

是同构;

(2) M 中任一元素能唯一地表示为 $M_i(1 \leq i \leq n)$ 的元素之和;

(3) M 中零元素能唯一地表示为 $M_i(1 \leq i \leq n)$ 的元素之和;

(4) 对于所有的 $i = 1, \cdots, n$, 都有

$$M_i \cap (M_1 + \cdots + \hat{M}_i + \cdots + M_n) = \{0\}$$

(这里的 $\hat{M}_i$ 的含义是将 M_i 除掉).

证明　(1) $\Rightarrow$ (2). 假若存在 $x \in M$, 使得

$$x = x_1 + \cdots + x_n = y_1 + \cdots + y_n \quad (x_i, y_i \in M_i),$$

其中某个 $x_j \neq y_j$ $(1 \leq j \leq n)$, 则

$$x = (x_1, \cdots, x_n)^{\varphi} = (y_1, \cdots, y_n)^{\varphi}.$$

故 φ 不是单射，矛盾于 φ 是同构.

(2) $\Rightarrow$ (3). 显然.

(3) $\Rightarrow$ (4). 假若存在某个 i $(1 \leq i \leq n)$, 使得

$$M_i \cap (M_1 + \cdots + \hat{M}_i + \cdots + M_n) \neq \{0\}.$$

取 $0 \neq x_i \in M_i \cap (M_1 + \cdots + \hat{M}_i + \cdots + M_n)$, 则

$$x_i = x_1 + \cdots + \hat{x}_i + \cdots + x_n \quad (x_i \in M_i),$$

即有

$$0 = x_1 + \cdots - x_i + \cdots + x_n = 0 + \cdots + 0 + \cdots + 0,$$

矛盾于 0 的表示法唯一.

(4) $\Rightarrow$ (1). 易见 (1) 中的 φ 是 R 模同态. 由 $M = \sum\limits_{i=1}^{n} M_i$ 知 φ 是满射. 故只要说明 φ 是单射，即说明 $\ker\varphi = \{0\}$. 事实上，设 $(x_1, \cdots, x_n) \in \ker\varphi$, 则 $x_1 + \cdots + x_n = 0$. 故对于任一 $i (1 \leq i \leq n)$, 有

$$-x_i = x_1 + \cdots + \hat{x}_i + \cdots + x_n \in M_i \cap (M_1 + \cdots + \hat{M}_i + \cdots + M_n) = \{0\}.$$

所以 $x_i = 0$ $(\forall\, i = 1, \cdots, n)$, 即有 $\ker\varphi = \{0\}$. □

如果模 M 的子模 M_i $(1 \leq i \leq n)$ 满足定理 3.2 的条件，则称 M 为 M_i $(1 \leq i \leq n)$ 的**内直和**, 仍记做 $M = M_1 \oplus \cdots \oplus M_n$. 此时，每一个 M_i 都称为 M 的**直和因子**.

§1.4　自 由 模

定义 4.1　设 R 是幺环，M 是 R 模. M 的一个子集 S 称为 R-**线性无关的**, 如果对于 S 的任意有限子集 $\{x_1, \cdots, x_n\}$, R-线性关系

$$x_1a_1 + \cdots + x_na_n = 0$$

蕴含着 $a_1 = \cdots = a_n = 0$. R-线性无关的生成元集称为**基**, 亦称为 R-基. 有基的模称为**自由模**.

回想 §1.3 子模的内直和的定义, 我们知道: $x_1, \cdots, x_r$ 为 M 的一组 R-基与

$$M = x_1R \oplus \cdots \oplus x_nR$$

是一回事, 所以 "M 是以 $x_1, \cdots, x_r$ 为基的自由 R 模" 也可以等价地叙述为 "M 中任一元素可唯一地表示为 $x_1, \cdots, x_r$ 的 R-线性组合".

环 R 上的自由模的最直接的例子是 $R \oplus \cdots \oplus R$ (r 个 R 的直和), 其中的 R 皆视为 R 模. 如果用 e_i 记 $R \oplus \cdots \oplus R$ 中第 i 个分量为 1 而其余分量为 0 的元素, 则 $e_1, \cdots, e_r$ 构成一组基.

在线性代数中, 我们知道对于给定的线性空间, 它的任意一组基中所含的向量的个数都相等. 这个事实对于一般环上的自由模并不成立. 但是我们有下面的结果:

定理 4.2 *设 R 是交换幺环, M 为有限生成的自由 R 模, 则 M 的任意基所含的元素个数都相等.*

证明 由于 M 是有限生成的自由 R 模, 易见 M 的任意一组基中只有有限多个元素. 事实上, 假若 $x_i (i \in I)$ 为 M 的一组基 (I 为无限集), $y_1, \cdots, y_n$ 为 M 的生成元. 将 $y_1, \cdots, y_n$ 表成基元素的 R-线性组合, 则所有的组合式中只出现有限多个 x_i. 取这些 x_i 之外的一个基元素 x_j, 将 x_j 表为生成元 $y_1, \cdots, y_n$ 的 R-线性组合, 再以 $y_1, \cdots, y_n$ 的基元素的 R-线性组合表达式代入, 整理后即得到 x_j 的只含有上述有限多个 x_i 的 R-线性表达式. 这矛盾于 $x_i (i \in I)$ 是基.

设 $\{x_1, \cdots, x_r\}$ 为 M 的一组基. 由于 R 是交换幺环, 故存在极大理想. 设 $\mathfrak{m}$ 为一个极大理想. 令

$$N = x_1\mathfrak{m} + \cdots + x_r\mathfrak{m}.$$

易验证 N 是 M 的子模, 且 $N = M\mathfrak{m}$. 故商模 M/N 可以视为商环 $F = R/\mathfrak{m}$ 上的模. 而 $\mathfrak{m}$ 是极大理想, 所以 F 是域, 于是 M/N

是 F-线性空间. 我们断言 x_i $(1 \leq i \leq r)$ 在商模 M/N 中的像 $\bar{x}_i$ $(1 \leq i \leq r)$ 是 M/N 的一组 F-基. 事实上, 设有 F-线性关系

$$\bar{x}_1\bar{a}_1 + \cdots + \bar{x}_r\bar{a}_r = \bar{0},$$

则

$$\overline{x_1a_1 + \cdots + x_ra_r} = \bar{0},$$

即

$$x_1a_1 + \cdots + x_ra_r \in N = x_1\mathfrak{M} + \cdots + x_r\mathfrak{M}.$$

由于 $\{x_1, \cdots, x_r\}$ 为 M 的一组基, 故必有 $a_i \in \mathfrak{M}(\forall\ 1 \leq i \leq r)$, 即 $\bar{a}_i = \bar{0} \in F(\forall\ 1 \leq i \leq r)$. 这说明 $\bar{x}_i(1 \leq i \leq r)$ 是 F-线性无关的. 又易见 $\bar{x}_i(1 \leq i \leq r)$ 在 F 上生成 M/N, 故我们的断言为真. 由此即知: $r = \dim_F M/N = \dim_F M/M\mathfrak{M}$, 与基的选取无关. □

定义 4.3 交换幺环 R 上的有限生成自由模 M 的基的势称为 M 的**秩**, 记为 $\mathrm{rank}_R(M)$ 或 $\mathrm{r}_R(M)$ 或 $\mathrm{r}(M)$. 特别地, 零模的秩定义为 0.

§1.5 主理想整环上的有限生成模

对于给定的环 R, 一个自然的问题就是: 所有 R 模有哪些可能? 对于一般的环, 这个问题过于复杂. 总的来说, 环的性质越多, 其上的模的结构就越简单 (反之, 如果一个环上的所有的模 (或一部分模) 具有较简单的结构, 则此环就应当有较多的性质). 例如, 性质最多的环是域, 而域上的模就是线性空间, 其结构完全由它的维数所决定. 稍微复杂些的交换环是主理想整环, 即任一理想都是主理想的无非零零因子的交换幺环. 本节将确定这种环上的有限生成模的结构. 作为推论, 给出有限生成交换群的结构定理.

1.5.1 主理想整环上的有限生成自由模

定理 5.1 主理想整环上的有限生成自由模的子模仍为自由模,

且子模的秩不超过原来模的秩.

证明 设 R 是主理想整环, M 是有限生成自由 R 模. 我们对于 M 的秩 $\mathrm{r}(M)$ 作归纳法.

若 $\mathrm{r}(M)=0$, 即 $M=\{0\}$, 则定理的结论显然成立.

设定理的结论对于秩小于 n 的自由模成立. 设 M 是秩为 n 的自由 R 模, $x_1,\cdots,x_n$ 为 M 的一组基, N 为 M 的一个子模. 令

$$\mathfrak{a}=\{a_1\in R\mid x_1a_1+\cdots+x_na_n\in N,\ a_i\in R\ \ (2\leq i\leq n)\}.$$

易见 $\mathfrak{a}$ 是 R 的一个理想 (读者自证之). 由于 R 是主理想整环, 故存在 $f\in R$, 使得

$$\mathfrak{a}=(f).$$

若 $f=0$, 则 N 含于秩为 $n-1$ 的自由模

$$M'=x_2R+\cdots+x_nR$$

中. 由归纳假设, 结论成立. 若 $f\neq 0$, 则存在 $y\in N$, 使得

$$y=x_1f+x_2b_2+\cdots+x_nb_n,$$

其中 $b_i\in R\ (2\leq i\leq n)$. 对于 N 中任一元素

$$x=x_1a_1+\cdots+x_na_n,$$

有 $a_1\in\mathfrak{a}=(f)$, 故存在 $c\in R$ 使得 $a_1=fc$. 于是 $x-yc=x_10+\cdots$, 即 $x-yc\in M'$. 又有 $x-yc\in N$, 故 $x-yc\in M'\cap N$. 这说明 $N\subseteq yR+N'$, 其中 $N'=N\cap M'$. 又显然有 $N\supseteq yR+N'$, 所以

$$N=yR+N'.$$

我们断言

$$yR\cap N'=\{0\}.$$

事实上, 设 $z\in yR\cap N'$, 则存在 $r\in R$ 使得

$$z=yr=x_1fr+x_2b_2r+\cdots+x_nb_nr.$$

因为 $z \in N' \subseteq M'$, 所以 $fr = 0$. 而 $f \neq 0$, 且 R 是整环, 故 $r = 0$. 于是 $z = 0$. 这就证明了我们的断言. 由以上的讨论即知

$$N = yR \oplus N'.$$

现在注意 N' 是秩为 $n-1$ 的自由模 M' 的子模. 由归纳假设, N' 为秩不超过 $n-1$ 的自由模. 设 $y_2, \cdots, y_m$ 为 N' 的 R-基, 其中 $m \leq n-1$. 则

$$N = yR \oplus y_2R \oplus \cdots \oplus y_mR.$$

故 N 是秩为 $m(\leq n)$ 的自由模. □

下面我们给出主理想整环上的有限生成自由模的一个等价说法.

定义 5.2 设 R 为整环, M 为 R 模, $x \in M$. 如果存在 R 中的非零元素 a 使得 $xa = 0$, 则称 x 为**扭元素**, 否则称为**自由元素**. 如果 M 的所有元素都是扭元素, 则称 M 为**扭模**. 如果 M 的所有非零元素都是自由的, 则称 M 为**无扭模**.

定理 5.3 设 M 是主理想整环 R 上的有限生成模, 则 M 是自由的当且仅当 M 是无扭的.

证明 若 $M = \{0\}$, 则 M 是无扭模, 同时是秩为零的自由模, 故定理的结论成立. 以下设 M 不是零模.

首先设 M 是自由模. 设 $x_1, \cdots, x_n$ 为 M 的一组 R-基. 如果 M 不是无扭的, 则存在 $x \in M$, $x \neq 0$ 以及 $a \in R$, $a \neq 0$, 使得 $xa = 0$. 设

$$x = x_1a_1 + \cdots + x_na_n \quad (a_i \in R),$$

则

$$0 = xa = x_1a_1a + \cdots + x_na_na.$$

由于 $x_1, \cdots, x_n$ 是基, 所以 $a_ia = 0$ ($\forall\ 1 \leq i \leq n$). 由于 $x \neq 0$, 故 $a_i(1 \leq i \leq n)$ 不全为零. 这与 $a \neq 0$ 且 R 为整环矛盾. 这就证明了自由模是无扭模.

反之，设 M 是无扭的. 设 $x_1,\cdots,x_m$ 是 M 的一组生成元. 无妨设 $x_1,\cdots,x_r$ 为其极大线性无关组，即 $x_1,\cdots,x_r$ 是 R- 线性无关的，而 $x_1,\cdots,x_r$, x_j $(r+1\le j\le m)$ 都不是 R- 线性无关的. 令 $N=x_1R+\cdots+x_rR$, 则 N 是自由模. 若 $r=m$, 则 $M=N$ 为自由模. 若 $r<m$, 则有线性关系

$$x_1a_{j1}+\cdots+x_ra_{jr}+x_jb_j=0 \quad (j=r+1,\cdots,m),$$

其中 $a_{ji},b_j\in R$, $b_j\neq 0(\forall\ 1\le i\le r,\ r+1\le j\le m)$. 令

$$b=b_{r+1}\cdots b_m.$$

由于 R 是整环，故 $b\neq 0$. 对于 $j=r+1,\cdots,m$, 由上面的线性关系知

$$x_jb=(-x_1a_{j1}-\cdots-x_ra_{jr})b_{r+1}\cdots\hat{b}_j\cdots b_m\in N.$$

所以 $Mb\subseteq N$. 而 N 为自由模，由定理 5.1 即知 Mb 为自由模. 最后，易见映射

$$\begin{aligned}\varphi: M &\to Mb,\\ x &\mapsto xb\end{aligned}$$

是 R 模同构 (φ 显然是满同态；又：设 $x\in\ker\varphi$, 则 $xb=0$. 而 $b\neq 0$ 且 M 是无扭模，所以 $x=0$. 于是 $\ker\varphi=\{0\}$, 即 φ 是单射), 故 M 是自由模. □

1.5.2 有限生成模分解为自由模和扭模的直和

首先我们给出关于主理想整环上的有限生成模一个简单的事实.

命题 5.4 主理想整环上的有限生成模的子模仍有限生成.

证明 此命题是定理 5.1 的直接推论. 事实上，设 M 是主理想整环 R 上的有限生成模， N 为 M 的子模. 设 $x_1,\cdots,x_m$ 为 M 的一组生成元. 以 R^m 记 m 个 R (作为 R 自身上的模) 的直和，以

$e_i(1\le i\le m)$ 记 R^m 中第 i 个分量为 1 其余分量皆为 0 的元素. 则 R^m 是以 $e_i(1\le i\le m)$ 为基的自由 R 模. 考虑映射

$$\begin{aligned}\varphi: R^m &\to M,\\ \sum_{i=1}^m e_ia_i &\mapsto \sum_{i=1}^m x_ia_i \quad (a_1,\cdots,a_m\in R).\end{aligned}$$

易见 φ 是 R 模的满同态. 令 S 为 N 在 φ 下的完全反像, 则 φ 在 S 上的限制

$$\varphi|_S:\ S\to N$$

是 R 模的满同态. 由于 S 是自由模的子模, 故 S 是自由模. 设 $f_1,\cdots,f_t$ 是 S 的一组 R-基, 则 f_j^{φ} $(1\le j\le t)$ 是 N 的一组生成元. □

下面我们考虑主理想整环上的有限生成模的分解. 首先, 关于扭元素的集合有以下事实:

命题 5.5 整环上的模的扭元素的集合构成一个子模.

证明 设 R 是整环, M 是 R 模. 首先, 0 是扭元素, 故扭元素的集合非空. 现设 x,y 为 M 的扭元素, 则存在 R 的非零元素 a,b 使得

$$xa=0,\quad yb=0.$$

于是 $(x-y)ab=(xa)b-(yb)a=0-0=0$. 由于 R 是整环, 所以 $ab\ne 0$. 故 $x-y$ 为扭元素. 又, 对于任一 $r\in R$, $(xr)a=(xa)r=0$, 故 xr 亦为扭元素. 这说明 M 的扭元素的集合对于 M 中的减法和 R 的作用封闭, 所以构成 M 的子模. □

此命题中的子模称为 M 的**扭子模**, 记为 $M_{\rm tor}$.

命题 5.6 主理想整环上的有限生成模关于其扭子模的商模是自由模.

证明 设 M 是主理想整环 R 上的有限生成模. 根据定理 5.3, 我们只要证明 $M/M_{\rm tor}$ 是无扭模. 设 $\bar{x}\in M/M_{\rm tor}$, $\bar{x}\ne\bar{0}$, 其中 $\bar{x}$ 为 M 的元素 x 在 $M/M_{\rm tor}$ 中所代表的陪集. 假若 $\bar{x}$ 是 $M/M_{\rm tor}$ 的扭元素, 则存在 R 的非零元素 a 使得 $\bar{x}a=\bar{0}$, 即 $\overline{xa}=\bar{0}$, 亦即 $xa\in M_{\rm tor}$. 于是存在 $b\in R$, $b\ne 0$, 使得 $(xa)b=0$, 即

$$x(ab) = 0.$$

而 R 是整环, 所以 $ab \neq 0$. 这说明 $x \in M_{\text{tor}}$, 即 $\bar{x} = \bar{0}$. 矛盾. □

现在我们可以证明本小节的主要结果了.

定理 5.7 主理想整环上的有限生成模等于其扭子模和一个自由子模的直和.

证明 设 M 是主理想整环 R 上的有限生成模. 由命题 5.6 知 M/M_{tor} 是自由 R 模. 设 $\bar{x}_1, \cdots, \bar{x}_r$ 为 M/M_{tor} 的一组基, $x_i \in M(1 \leq i \leq r)$ 为 $\bar{x}_i$ 的代表元. 令

$$N = x_1R + \cdots + x_rR.$$

易见 N 是自由 R 模. 事实上, 如果

$$x_1a_1 + \cdots + x_ra_r = 0 \quad (a_1, \cdots, a_r \in R),$$

则在 M/M_{tor} 中有

$$\bar{x}_1a_1 + \cdots + \bar{x}_ra_r = \bar{0}.$$

而 $\bar{x}_1, \cdots, \bar{x}_r$ 为 M/M_{tor} 的基, 故 $a_i = 0(\forall\, 1 \leq i \leq r)$. 这就证明了 N 是以 $x_1, \cdots, x_r$ 为基的自由模.

我们来证明 $M = N \oplus M_{\text{tor}}$. 首先易见 $M = N + M_{\text{tor}}$. 事实上, 对于任一 $x \in M$, 以 $\bar{x}$ 记 x 在 M/M_{tor} 中的典范像 (即代表的陪集), 则存在 $b_i \in R(1 \leq i \leq r)$, 使得 $\bar{x} = \bar{x}_1b_1 + \cdots + \bar{x}_rb_r$. 令

$$y = x - (x_1b_1 + \cdots + x_rb_r),$$

则 $\bar{y} = \bar{0}$, 即 $y \in M_{\text{tor}}$. 于是

$$x = (x_1b_1 + \cdots + x_rb_r) + y \in N + M_{\text{tor}}.$$

这说明 $M \subseteq N + M_{\text{tor}}$. 又显然有 $M \supseteq N + M_{\text{tor}}$, 故 $M = N + M_{\text{tor}}$.

只需要再证明 $N \cap M_{\text{tor}} = \{0\}$. 设 $x \in N \cap M_{\text{tor}}$, 则存在 $a_1, \cdots, a_r \in R$ 以及 $a \in R$, $a \neq 0$, 使得

$$x = x_1a_1 + \cdots + x_ra_r, \quad xa = 0.$$

于是

$$x_1a_1a+\cdots+x_ra_ra=0.$$

而 $x_1,\cdots,x_r$ 是 N 的基，所以 $aa_i=0\ (\forall\ 1\le i\le r)$. 由 $a\ne 0$ 以及 R 是整环即知 $a_i=0\ (\forall\ 1\le i\le r)$, 故 $x=x_1a_1+\cdots+x_ra_r=0$. □

应当指出，对于主理想整环 R 上的有限生成模 M, 商模 $M/M_{\rm tor}$ 作为 R 模的秩当然是 M 的不变量 (称为 M 的 R **秩**, 或简单地称为**秩**, 记为 $\mathrm{r}_R(M)$, 或简单地记为 $\mathrm{r}(M)$), 但是 M 的秩为 $\mathrm{r}_R(M)$ 的自由子模并不一定是唯一的. 例如，若 $x_1R+\cdots+x_rR$ 是 M 的自由子模， $y\in M_{\rm tor}, y\ne 0$, 则 $(x_1+y)R+\cdots+x_rR$ 也是 M 的自由子模. 显然这两个自由子模不同 (否则，自由子模 $x_1R+\cdots+x_rR$ 中含有非零扭元素 $y=(x_1+y)-x_1$, 矛盾于定理 5.3).

1.5.3　有限生成扭模分解为不可分解循环模的直和

我们的目的是决定主理想整环 R 上的有限生成模 M 的结构. 根据定理 5.7, 问题归结为决定 $M_{\rm tor}$ 的结构. 本小节将给出有限生成扭模的最精细的直和分解.

我们先给出两个术语的定义.

定义 5.8　设 M 是交换幺环 R 上的模， $S\subseteq M$. 令

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

称 $\mathrm{Ann}(S)$ 为 S 的**零化子**. 特别地，若 $S=\{x\}$, 称 $\mathrm{Ann}(S)$ 为 x 的**零化子**, 简记为 $\mathrm{Ann}(x)$.

容易验证 $\mathrm{Ann}(S)$ 是 R 的一个理想且 $\mathrm{Ann}(x)=\mathrm{Ann}(xR)$. $\mathrm{Ann}(x)$ 亦称为 x 的**阶理想** (请对照交换群 (作为 $\mathbb{Z}$ 模) 中一个元素的阶的概念).

零化子是由模的子集决定的 (环的) 理想. 反过来环的理想也决定一个子模.

定义 5.9　设 R 与 M 同上， $\mathfrak{a}$ 是 R 的一个理想. 令

$$\mathrm{M}(\mathfrak{a})=\{m\in M\mid ma=0,\forall\ a\in\mathfrak{a}\}$$

有关此电子图书的说明

本人由于一些便利条件，可以帮您提供各种中文电子图书资料，且质量均为清晰的PDF图片格式，质量要高于网上大量传播的一些超星 PDG 的图书。方便阅读和携带。只要图书不是太新，文学、法律、计算机、人文、经济、医学、工业、学术等方面的图书，我都可以帮您找到电子版本。所以，当你想要看什么图书时，可以联系我。我的 QQ是：85013855，大家可以在 QQ上联系我。

此 PDF 文件为本人亲自制作，请各位爱书之人尊重个人劳动，敬请您不要修改此 PDF文件。因为这些图书都是有版权的，请各位怜惜电子图书资源，不要随意传播，否则，这些资源更难以得到。