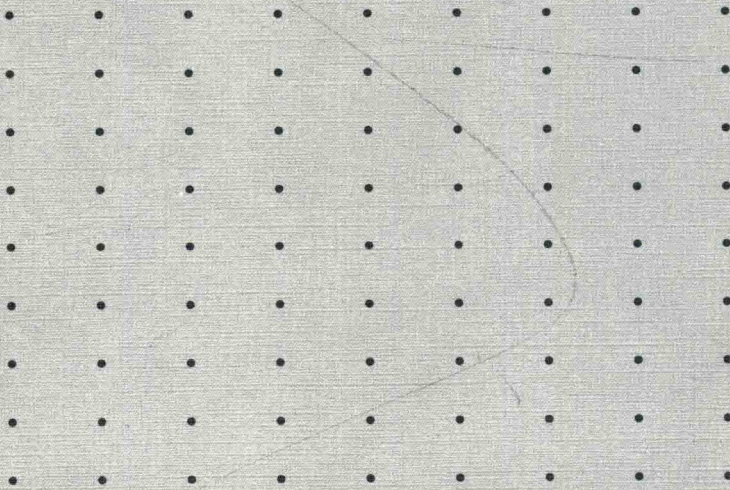


现代数学基础

67.1 代数学方法 (第一卷)

基础架构

■ 李文威



高等教育出版社

现代数学基础

67.1

代数学方法 (第一卷)

基础架构

■ 李文威

高等教育出版社·北京

内容简介

本书主要目的是介绍代数学中的基本结构,着眼于基础数学研究的实际需求。全书既包括关于群、环、模、域等结构的标准内容,也涉及范畴和赋值理论,在恪守体系法度的同时不忘代数学和其他数学领域的交融。

本书可供具有一定基础的数学专业本科生和研究生作为辅助教材、参考书或自学读本之用。

代数学方法 第一卷

Daishuxue Fangfa

图书在版编目(CIP)数据

代数学方法.第一卷,基础架构/李文威著.—北京:高等教育出版社,2019.1

ISBN 978-7-04-050725-6

I. ①代… II. ①李… III. ①代数—高等学校—教材
IV. ①O15

中国版本图书馆CIP数据核字(2018)第232327号

策划编辑 赵天夫 责任编辑 赵天夫
封面设计 赵阳 责任印制 刘思涵

出版发行 高等教育出版社
社址 北京市西城区德外大街4号
邮政编码 100120
购书热线 010-58581118
咨询电话 400-810-0598
网址 <http://www.hep.edu.cn>
<http://www.hep.com.cn>
网上订购 <http://www.hepmall.com.cn>
<http://www.hepmall.com>
<http://www.hepmall.cn>
印刷 天津嘉恒印务有限公司

开本 787mm×1092mm 1/16
印张 28
字数 612千字
版次 2019年1月第1版
印次 2019年1月第1次印刷
定价 99.00元

本书如有缺页、倒页、脱页等质量问题,
请到所购图书销售部门联系调换
版权所有 侵权必究
[物料号 50725-00]

目录

导言	1
第一章 集合论	11
1.1 ZFC 公理一览	12
1.2 序结构与序数	15
1.3 超穷递归及其应用	17
1.4 基数	20
1.5 Grothendieck 宇宙	23
习题	26
第二章 范畴论基础	27
2.1 范畴与态射	28
2.2 函子与自然变换	33
2.3 函子范畴	40
2.4 泛性质	43
2.5 可表函子	46
2.6 伴随函子	49
2.7 极限	56
2.8 完备性	64
习题	69
第三章 么半范畴	71
3.1 基本定义	72

3.2	严格性与融贯定理	78
3.3	辫结构	80
3.4	充实范畴	85
3.5	2-范畴一瞥	90
	习题	93
第四章	群论	97
4.1	半群, 么半群与群	98
4.2	同态和商群	102
4.3	直积, 半直积与群扩张	107
4.4	群作用和计数原理	111
4.5	Sylow 定理	115
4.6	群的合成列	118
4.7	可解群与幂零群	122
4.8	自由群	127
4.9	对称群	136
4.10	群的极限和完备化	142
4.11	范畴中的群	146
	习题	149
第五章	环论初步	153
5.1	基本概念	154
5.2	几类特殊的环	158
5.3	交换环初探	162
5.4	间奏: Möbius 反演	167
5.5	环的极限与完备化	172
5.6	从么半群环到多项式环	178
5.7	唯一分解性	183
5.8	对称多项式入门	191
	习题	195
第六章	模论	199
6.1	基本概念	200
6.2	模的基本操作	204
6.3	自由模	208
6.4	向量空间	212
6.5	模的张量积	215

6.6	环变换	222
6.7	主理想环上的有限生成模	227
6.8	正合列入门	234
6.9	投射模, 内射模, 平坦模	240
6.10	链条件和模的合成列	244
6.11	半单模	248
6.12	不可分模	251
	习题	255
第七章	代数初步	259
7.1	交换环上的代数	260
7.2	整性, 有限性和 Frobenius 定理	263
7.3	代数的张量积	268
7.4	分次代数	273
7.5	张量代数	278
7.6	对称代数和外代数	281
7.7	牛刀小试: Grassmann 簇	287
7.8	行列式, 迹, 判别式	291
	习题	296
第八章	域扩张	301
8.1	扩张的几种类型	301
8.2	代数闭包	307
8.3	分裂域和正规扩张	311
8.4	可分性	314
8.5	本原元素定理	319
8.6	域扩张中的范数与迹	321
8.7	纯不可分扩张	324
8.8	超越扩张	326
8.9	张量积的应用	329
	习题	333
第九章	Galois 理论	335
9.1	有限 Galois 对应	336
9.2	无穷 Galois 对应	340
9.3	有限域	345
9.4	分圆域	350

9.5	正规基定理	353
9.6	Kummer 理论	356
9.7	根式解判准	363
9.8	尺规作图问题	366
	习题	370
第十章	域的赋值	375
10.1	滤子	376
10.2	Krull 赋值与完备化	380
10.3	域上的赋值	385
10.4	绝对值, 局部域和整体域	387
10.5	个案研究: 单位闭圆盘	394
10.6	一般扩域的赋值	398
10.7	代数扩域的赋值	402
10.8	完备域中求根	407
10.9	Witt 向量	412
	习题	422
	参考文献	425
	符号索引	431
	名词索引暨英译	433

导言

概观

代数一词源自公元 9 世纪波斯学者 al-Khwārizmī 的著作. 李善兰和 A. Wylie 在 1859 年合译 A. De Morgan 的 *Elements of Algebra* 时解释为“补足相消”之术, 亦即解方程式的技艺, 相当于现今的中学数学. 自 20 世纪以降, 代数学的范围扩及更一般的数学对象及其运算, 这一转型始自 E. Noether 等人的一系列工作, 而初定于 B. L. van der Waerden 的巨著《代数学》[42, 43]. 在此意义下, 代数学的初步对象可粗分为群、环、模、域. 若用 Bourbaki 学派的语汇来说, 不妨将数学理解为各种结构的错综变化, 代数结构是带有某种运算的集合, 譬如有理数对四则运算构成有理数域 \mathbb{Q} . 概括地说, 代数学就是关于代数结构的研究.

从集合论的必要回顾出发, 以范畴论视角贯串群、环、模、域和种种衍生概念, 这就组成了本书副标题里的“基础架构”.

按现行教学体系而论, 代数课程上接于数学分析与高等代数或曰线性代数. 举笔者曾执教的中国科学院大学为例, 学生在微积分课程中接触了集合和点集拓扑学的词汇, 线性代数课程则授以向量空间和多项式的基本理论, 同时给予群、环、域的初步实例. 有了这些基础就容易学习更一般的代数结构, 而以有限扩张的 Galois 理论作为总验收. 各院校安排不同, 但代数素养的重要是一切数学工作者的共识. 这不单是为了陶冶美感, 还因为凡是代数结构出现之处, 就有代数学方法施展的空间, 只消列出相关的学科名称, 如代数数论、代数几何、代数拓扑、代数组合乃至代数统计等等, 便可以粗知这门本领的用处. 此外, 代数方法在物理、化学、计算机科学等方面的应用也同样是广为人知的.

本书主题有时也称为“近世代数”或“抽象代数”. 所谓近世, 总是相对于当时当世而论, 早在 1955 年 van der Waerden 发表《代数学》第四版时便已舍弃此词, 于今更无必要. 至于说抽象, 充其量是初学者的错觉, 作为课名或书名完全不得要领, 而且似乎有恫吓读者之嫌. 本书题为“代数学方法”, 一则是因为当代代数学范围过广, 本书仅择

有趣有用者而述,不求体系大而全.第二也是最关键的一点,则是因为数学的本质存在于交融互摄,只为授课与学科划分方便才打包于一词.所以本书绝不视代数为疆界分明的学科;与分析、拓扑学等脱钩的纯代数即便存在,也仅是千万种研究方向之一.《庄子·应帝王》中有混沌凿七窍的故事,强凿疆界同样令数学趋于停滞消亡.

许多本科代数教材的内容大致以1950—1960年代为分限.绝不是说代数的内涵与方法就此定型;恰恰相反,此后数学经历了空前的发展,包括对经典题材有了更新更透彻的理解.若就本书范围而论,当属范畴论的兴起最为突出.这是拜拓扑学之赐,在数学中建立起的一套关系哲学,其中真正重要的并非一个数学结构“是什么”(比方说,它作为集合有哪些成员),而是结构之间的联系,或者说是结构的功能与角色.笔者所愿强调的正是拓扑学,尤其是同伦论的贡献,代数学至今仍从中领受新鲜的工具和挑战;这些根源不难凭拓扑直觉来把握,倘若因虚构的学科藩篱而轻易放过,对读者可是莫大损失.

当然,真正伟大的理论可以超越时代,光芒恒在.如何以现代形式来撷取精华,去其枝蔓而无损它们本有的辉煌?这是笔者自期的目标.一步到位显然是不切实际的,是以本书对某些主题将以经典或者“半经典”的观点来料理.

这里还必须说明历史的顺序不同于概念的顺序.一般说来,新的概念在数学上能站稳脚跟很少是因为它们简明通透,恰好相反:它们得先在既有的、最为艰深的问题上一试锋芒,尽管新概念终将成为未来大厦的基石,而旧日难题反倒会成为课后习题,如此遂显得理论框架是第一义的,应用却属于外来的、派生的.我们不得不承认这种重构是学习的必由之路,也算是数学进步的一种标志.但是读者也应当明白代数学中各种概念不只是筑起一座座坚实的大厦,就其谱系观之又仿佛一张大网,其中的节点相互支撑.如反映在方法上,这就要求学者具有处处不滞,纵横兼顾的慧眼.

本书的初步准备工作可追溯到2013年左右.在同各地学生的交流中,笔者深感于广大学子的禀赋与热忱,而另一方面,学校师长所能够或愿意给予的又与此极不相称.很遗憾,互联网在这方面无补于资源的不均.即便有明眼人推荐教材,其内容又普遍过时,一涉科研,障碍立现.基于这些考量,本书在编排上设定了几点目标:

- ◇ 兼具自学、参考书与教学资源的多重功能;
- ◇ 参照实际科研需求,尤其是思想与符号的更新换代;
- ◇ 突出开放性,强调代数学与其他问题的交融.

有鉴于此,这不是为某一门课或某所院校量身打造的教本,章节与授课顺序和课时也没有必然的联系.因此无论是教师或自学者都应该自主取舍.

尽管教材的结构总须按直线发展,实际学习时种种主题势必有所交错重复,犹如刀剑淬火,这是吸收新知的自然规律.但不同群体适合于不同的学习节奏,如作为参考书更要另当别论,本书的折中方式是大略以逻辑顺序为锚,必要的跳跃/回顾则倚靠交叉参照来实现.对于已有一定代数基础的读者,若能活用这些参照和书后索引,各章大致是可以独立阅读的.

本书部分内容曾在中国科学院大学的本科生与研究生课程上讲授. 编撰过程中广泛参考了既有的教材, 包括但不限于 Bourbaki [3, 5], Jacobson [21, 22], Lang [28], MacLane [29], van der Waerden [42, 43] 等等, 同时参酌了网络资源如 MathOverflow 和 nLab 等; 中文教材如张禾瑞 [55] 和聂灵沼-丁石孙 [59] 也提供了不少借鉴. 在此遥致敬意. 缘于见识和精力的限制, 各种错误或不足之处在所难免, 祈望方家不吝斧正.

编撰过程中承蒙师友及同学们的理解与襄助, 兹就记忆所及者敬列如次, 用申谢忱: 白宸聿、冯琦、黎景辉、刘欣、毛盛开、明杨、荣石、单宁、陶景麾、王丹、席南华、熊锐、张秉宇、张浩、周胜铉、朱任杰、邹昌寒 (按汉语拼音排序). 此外, 高等教育出版社的赵天夫编辑提供了许多专业意见, 在此一并致谢.

李文威

2018 年 3 月于保福寺桥南

背景知识

本书不求建立一套自足的或者界限分明的体系, 何况按科研的普遍经验, 如一味要求万事俱备才敢开疆拓土, 结果往往是一事无成, 代数相关领域尤其如此. 阅读过程中难免会遇上新的或未夯实的新知识点, “引而伸之, 触类而长之” 兴许是更合适的态度. 即便如此, 在此仍有必要描绘一条模糊的底线. 保守估计, 本书期望读者对大学数学专业低年级课程有充分的掌握. 如果还修习过一学期的本科代数课程, 譬如 [59] 的前半部或 [55], 就应当能顺利理解本书大部分的内容, 但这不是必需的. 至于具体情形自然得具体分析, 既系于读者个人的学思经历, 也和胆识有关.

以下列出几类相关的背景知识, 按分量递降排列.

- ▷ **基本素养** 包括逻辑用语、反证和递归等论法, 关于集合的常识和对符号的熟稔, 对数学结构的初步体会, 对抽象语言的感觉等等, 一言以蔽之曰“火候”. 其粗浅方面涵摄于高中或大学一年级课程的内容, 若论造微, 则是数学工作者一生的功课.
- ▷ **矩阵, 向量空间, 多项式** 这些内容在中国一般包含于大一的高等代数或线性代数课程, 如 [51, 52] 等, 初等部分则兼于高中. 读者应该对矩阵和向量空间有最初步的认知, 并了解矩阵和线性变换的关系; 若知悉置换 (对称群) 的操作则更佳. 虽然这些主题皆可划入代数学, 但无论就多数读者的背景或就论述的便利考虑, 都不必从头细说. 这些知识在本书中主要用于举例和节约论证, 其取舍不影响理论主干.
- ▷ **初等数论** 含整除性、素因子分解、辗转相除法等常识, 以及延伸到多项式的情形. 此外读者应该知悉, 或者至少愿意接受同余式的使用, 尤其是在模素数 p 的情形.

最基本的结果如 Fermat 小定理等会偶尔出现,当然,用代数工具是极容易予以证明的.

- ▷ **分析学相关常识** 实数的构造,点集拓扑学初步概念, Cauchy 列及完备性. 多数不脱大学低年级分析或几何类基础课范围. 这些语汇对于处理某些代数结构是方便的,有时甚至是必需的.

针对超过大一范围的背景,例如较深的几何学知识,文中将另外指出参考书籍. 这类知识主要用于举例,对于高年级本科生应该是合理的. 如涉及本科或研究生低年级的基础知识,则从较具代表性并且容易获取的本土教材择一.

内容提要

以下简介各章的内容.

第一章: 集合论 读者对集合应有基本的了解. 本书以集合论居首,一则是尊重体系的严整性,二则是完整说明基数和 Zorn 引理的来龙去脉. 最后介绍的 Grothendieck 宇宙是应用范畴论时的必要安全措施. 大基数理论对一些高阶的范畴论构造实属必需,我们希望在日后探讨同调代数时予以阐明.

第二章: 范畴论基础 本章完整介绍范畴论的基础概念,以范畴,函子与自然变换为中心,着重探讨极限与可表性. 为了说明这些观念是自然的,我们将自数学各领域中博引例证.

第三章: 幺半范畴 这是带有某种乘法操作的范畴. 幺半范畴在实践与理论两面占据要津,因为它一方面是向量空间张量积的提纯,同时又能用来定义范畴的“充实”化,例如实用中常见的加性范畴.

前三章主要在观念或体系上占据首位,实际阅读时不必循序. 建议初学者先迅速浏览,并在后续章节中逐渐认识这些内容的必要性,回头加以巩固. 无须在初次阅读时就强求逐字逐句地理解:这不是唯一的方法,也不是最好的方法.

第四章: 群论 对幺半群和群的基本理论予以较完整的说明,包括自由群的构造,也一并介绍群的完备化. 后者自然地引向 pro-有限群的概念,这是一类可以用拓扑语汇来包装的群论结构,它对于 p -进数、赋值和无穷 Galois 理论的研讨是必需的.

第五章: 环论初步 考虑到后续内容的需要,此章也涉及完备化及对称多项式的初步理论. 之所以称为初步,是为了区别于交换环论(又称交换代数)与非交换环的进阶研究,这些将在后续著作予以探讨.

第六章: 模论 此章触及模论的基本内容,包括张量积. 向量空间和交换群则视作模的特例. 我们还会初步探讨复形、正合列与同调群的概念. 系统性的研究则是同调代数的任务. 关于半单模,不可分模与合成列的内容可以算是后续著作的铺垫.

第七章: 代数初步 这里所谓的“代数”是构筑在模上的一种乘法结构,虽然易生混淆,此词的使用早已积重难返,本书只能概括承受. 本章还将针对代数引入整性的一

般定义, 讨论分次代数, 并以张量代数及衍生之外代数和对称代数为根本实例, 这些也是线性代数中较为深入的题材, 有时又叫作多重线性代数. 称为初步同样是为了区别于代数的细部研究, 特别是非交换代数的表示理论, 那是另一个宏大主题.

第八章: 域扩张 扩域的研究构成了域论的一大特色, 这根植于解方程式的需求. 本书不回避无穷代数扩张和超越扩张, 但对于更精细的结构理论如 p -基等则暂予略过.

第九章: Galois 理论 有限扩域的 Galois 理论常被视为本科阶段代数学的终点, 这还是在课时充足的前提下; 如此就容易给人一种似是而非的印象, 仿佛 Galois 理论的要旨不外是解高次方程和尺规作图. 本章包括这些应用, 但置无穷 Galois 理论于核心位置, 因为在数论等应用中, 由可分闭包给出的绝对 Galois 群才是最根本的对象. 为了阐述这点, 使用 pro-有限群的语言便是难免的.

第十章: 域的赋值 此章第一节是关于滤子与完备化的讨论, 不妨暂时略过. 其后介绍 Krull 赋值的一般概念, 取值容许在任意全序交换群上, 然后引入域上的赋值与绝对值. 这些主题既可以看作代数的支脉, 也可以看作非 Archimedes 分析学的入门. 相关思路现已汇入了数论、几何与动力系统的研究. 最后介绍的 Witt 向量则在算术几何的新近发展中承担了吃重的角色.

对于抽象程度较高的部分, 正文将穿插若干和理论主线无关, 然而饶富兴味或者曾发挥重要历史功用的结果, 例子包括 Möbius 反演 (§5.4), Frobenius 定理 7.2.9, Grassmann 簇的 Plücker 嵌入 (§7.7) 和 Ostrowski 定理 10.4.6 等等.

本书不区分基础内容与选学内容, 读者在订定阅读顺序时宜参酌各章开头的介绍和阅读提示.

凡例

章节在参照时以符号 § 为前缀. 各章始于简介和阅读提示, 习题则附于结尾, 多有提示. 定理的证明原则上不归入习题, 少数例外是一些自明的, 可以依样画葫芦的, 或者是甚繁而不难的论证.

证明的结尾以 □ 标记.

人名以拉丁字母转写为主, 唯中日韩越人名则尽量使用汉字. 索引一律按字母或汉语拼音排序, 附带中英对照. 数学术语全部中译, 原则上不再标注原文以免扰乱阅读; 必要时读者可以查阅索引. 译文参照 [56], 少数明显不妥的翻译另改.

数学离不开符号, 代数学尤其如此. 本书采取的符号体系折中于三条原则: 科研实践中的惯例、系统性以及自明性. 兹简述一般性的符号如下, 以备查阅.

- ◇ **逻辑:** 本书谈逻辑的机会不多, 借用其符号的场合倒不少. 我们将以 $\forall \dots$ 表达量词“对所有……”, 以 $\exists \dots$ 表达“存在……”并以 $\exists!$ 表达“存在唯一的……”

我们以 $P \wedge Q$ 表示“ P 而且 Q ”, 以 $P \vee Q$ 表示“ P 或者 Q ”. 命题间的蕴涵关系以 \implies 表达, 因此 $P \iff Q$ 意谓 P 等价于 Q .

- ◇ **定义:** 表达式 $A := B$ 意指 A 被定义为 B . 如果一个表达式或一系列操作无歧义地确定了一个数学对象, 与一切辅助资料的选取无关, 则称该对象为“良好定义”或“确切定义”的, 简称良定.
- ◇ **集合:** 我们以 \cap 表交, \cup 表并, \times 表积; 差集记为 $A \setminus B := \{a : a \in A \wedge a \notin B\}$. 集合的包含关系记作 \subset , 真包含记作 \subsetneq . 一族以 $i \in I$ 为下标的集合表作 $\{E_i : i \in I\}$ 或 $\{E_i\}_{i \in I}$ 之形, 其并写作 $\bigcup_{i \in I} E_i$, 交写作 $\bigcap_{i \in I} E_i$, 积则写作 $\prod_{i \in I} E_i$. 集合的无交并以符号 \sqcup 表示. 空集记为 \emptyset . 集合 E 的元素个数或谓基数记为 $|E|$; 基数为 1 的集合称为独点集. 设 \sim 为集合 E 上的等价关系, 则相应的商集记为 E/\sim , 它由所有 E 中的等价类构成; 我们称等价类中的任一元素为该类的一个代表元.
- ◇ **映射:** 以 $f : A \rightarrow B$ 表示从 A 到 B 的映射 f , 以 $a \mapsto b$ 表示元素 a 被映为 b , 或一并写作

$$f : A \longrightarrow B$$

$$a \longmapsto b.$$

我们以 \hookrightarrow 表示该映射是单射, 以 \twoheadrightarrow 表示满射. 在讨论一般的代数结构乃至范畴时, 这些符号也用于表达单同态和满同态等概念, 至关重要的同构则以 \simeq 或带方向的 $\xrightarrow{\sim}$ 表达, 确切意涵可从上下文推寻. 我们也常以 $\xleftrightarrow{1:1}$ 表示集合间的一一对应, 亦即双射. 映射 $f : B \rightarrow C$ 和 $g : A \rightarrow B$ 的合成写作 $f \circ g = fg : x \mapsto f(g(x))$. 必要时以 $f(\cdot)$ 或 $f(-)$ 的写法强调函数之变量.

对于映射 $f : A \rightarrow B$ 和子集 $B_0 \subset B$, 称 $f^{-1}(B_0) := \{a \in A : f(a) \in B_0\}$ 为 B_0 在 f 下的原像或逆像. 对任意 $b \in B$, 记 $f^{-1}(b) := f^{-1}(\{b\})$, 称为 f 在 b 上的纤维. 记 f 的像为 $f(A)$ 或 $\text{im}(f)$. 对于子集 $A_0 \subset A$, 记 f 在 A_0 上的限制为 $f|_{A_0} : A_0 \rightarrow B$.

集合 E 到自身的恒等映射记为 id_E , 不致混淆时也记为 id .

- ◇ **数系:** 记

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

整数 有理数 实数 复数

正整数集和非负整数集分别以自明的符号表为 $\mathbb{Z}_{>1}$ 和 $\mathbb{Z}_{\geq 0}$, 类推可定义 $\mathbb{R}_{>0}$ 等等. 我们偶尔也会提到 Hamilton 的四元数, 它们构成集合 \mathbb{H} , 其定义会适时说明. 谈及角度时一律采取弧度制.

对于实数, 我们以 \gg 表示“充分大于”, 譬如 $x \gg 0$ 表示正数 x 充分大, 而 $0 < x \ll 1$ 表示正数 x 充分接近 0.

◇ **范畴**: 本书一般以无衬线字体如 **Set, Grp, R -Mod** 等标识范畴; 我们将在 §2 解释范畴的定义.

◇ **整数论**: 设 $a, b, n \in \mathbb{Z}$. 符号 $a \mid b$ 意谓 a 整除 b , 而 $a \equiv b \pmod{n}$ 相当于说 $n \mid a - b$, 或者说 a 和 b 对 $\text{mod } n$ 同余 (又读作“模 n 同余”). 给定 n , 同余给出整数集上的一个等价关系, 有时也以 $a \text{ mod } n$ 表示 a 的同余类; 整数的加减乘法可以良定到 $\text{mod } n$ 的同余类上. 二项式系数记作

$$\binom{x}{k} := \frac{x(x-1)\cdots(x-k+1)}{k!}, \quad \binom{x}{0} := 1.$$

◇ **矩阵**: 循国内多数教材的惯例, 本书取横行竖列, 将 $n \times m$ 矩阵写作

$$A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} = \begin{pmatrix} & \vdots & \\ \cdots & a_{ij} & \cdots \\ & \vdots & \end{pmatrix} \begin{matrix} \text{第 } i \text{ 行} \\ \\ \text{第 } j \text{ 列} \end{matrix}$$

的形式, 其行列式记为 $\det A$. 矩阵乘法 $AB = C$ 按 $\sum_j a_{ij}b_{jk} = c_{ik}$ 确定. 矩阵 A 的转置记为 tA . 记 $n \times n$ 单位矩阵为 $1_{n \times n}$ 或 1 .

常用代数结构

由于本书侧重于概念间的交互联系, 在不影响理论主干的前提下, 小范围的交叉参照或谓“偷跑”势不可免, 尤其是在前几章. 读者能获益多少取决于已有的知识. 以下表列若干基础代数结构, 既便于查阅, 也有助于快速地领略或回忆代数学的初步概念.

以下以 $\text{GL}_n(\mathbb{R})$ 表 $n \times n$ -可逆实矩阵集, 以 $M_n(\mathbb{R})$ 表 $n \times n$ -实矩阵集, 以 $\mathbb{Z}/p\mathbb{Z}$ 表示模素数 p 的剩余系.

结构	运算	性质	同态 ϕ 的性质	初步例子
集合 X	无	无	映射 $X \xrightarrow{\phi} Y$	$\{1, 2, 3, \dots\}$
么半群 M	乘法 $(x, y) \mapsto xy$ 么元 $1 \in M$	结合律 $x(yz) = (xy)z$ 么元性质 $1x = x = x1$	映射 $M_1 \xrightarrow{\phi} M_2$ $\phi(xy) = \phi(x)\phi(y)$ $\phi(1) = 1$	$(\mathbb{Z}_{\geq 0}, +)$
群 G	同上	承上, 且 $\forall x$ 有逆元: $xx^{-1} = 1 = x^{-1}x$	同上	$(\mathbb{Z}, +)$ $(\text{GL}_n(\mathbb{R}), \cdot)$
环 R	对加法成交换群 加法么元 $= 0$ 对乘法成么半群 乘法么元 $= 1$	分配律: $r(s + s') = rs + rs'$ $(s + s')r = sr + s'r$	对加, 乘皆为同态	$(\mathbb{Z}, +, \cdot)$ 实多项式环 $(M_n(\mathbb{R}), +, \cdot)$

结构	运算	性质	同态 ϕ 的性质	初步例子
域 F	同上	承上且 $\forall x \neq 0$ 有乘法逆元: $xx^{-1} = 1 = x^{-1}x$ 乘法交换 $xy = yx$	同上	$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ $\mathbb{Z}/p\mathbb{Z}$
左 R -模 M	对加法成交换群 纯量乘 $R \times M \rightarrow M$	$r(m + m') = rm + rm'$ $(r + r')m = rm + r'm$ $r(r'm) = (rr')m$ 幺元性质 $1m = m$	对加法为同态 $\phi(rm) = r\phi(m)$	域上向量空间

有些文献未要求环的乘法幺元存在. 对于上表的每一种结构, 标为同态的映射都具有以下性质

- ◇ 恒等映射 id_X 是从 X 到自身的同态 (称为自同态),
- ◇ 同态的合成仍为同态,
- ◇ 同态的合成满足结合律 $f \circ (g \circ h) = (f \circ g) \circ h$.

如果结构之间的一对同态 $X \xrightleftharpoons[g]{f} Y$ 满足 $f \circ g = \text{id}_Y$, $g \circ f = \text{id}_X$, 就称它们互逆, 此时 f 和 g 是相互唯一确定的, 记为 $g = f^{-1}$, $f = g^{-1}$. 可逆的同态称为同构. 铭记代数学的一条基本原则: 同构联系了本质上相同的代数结构.

暂时不管集合论的细节, 则上述性质表明: 对于表列的每种结构, 其全体成员 (“对象”) 及其间的同态 (“态射”) 构成范畴的初步实例. 群, 交换群和左 R -模的范畴一般记为 Grp , Ab 和 $R\text{-Mod}$, 依此类推; 对于这些范畴中的对象 X, Y , 其间的全体同态构成了集合 $\text{Hom}_{\text{Grp}}(X, Y)$, $\text{Hom}_{\text{Ab}}(X, Y)$ 等等, 时常简记为 $\text{Hom}(X, Y)$. 从 X 映到自身的同态称为自同态, 它们对态射合成构成一个幺半群, 记为 $\text{End}(X)$; 可逆的自同态称为自同构, 所成的群记为 $\text{Aut}(X)$.

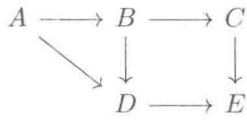
表列诸结构的运算都搭建在集合上, 对之可以证明同构恰好是兼为双射的同态; 但要留意到:

- ◇ 范畴未必由搭建在集合上的结构组成;
- ◇ 对于其他建基在集合上的范畴, 双射同态也未必可逆: 标准的反例是范畴 Top (对象 = Hausdorff 拓扑空间, 态射 = 连续映射), 其中的同构是拓扑空间的同胚, 然而连续的双射未必是同胚.

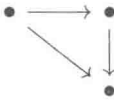
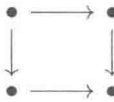
在研究结构之间的同态时, 我们经常会运用交换图表的语言: 这意谓以箭头描述同态, 而交换性意谓图表中箭头的合成是殊途同归的, 基本例子:

$$\begin{array}{ccc}
 A & \xrightarrow{f} & B \\
 \downarrow h & \swarrow g & \\
 C & &
 \end{array}
 \quad \text{交换} \iff g \circ f = h.$$

当然我们还会考虑更复杂的图表, 譬如



等等, 交换性的意蕴可以类推. 图表的交换性能够分块验证; 譬如上图的交换性便可

化约到子图表  和  上检验. 这套工序对于更复杂的图表 (例如

“三维”情形) 是很有用的.

由于交换图表只涉及箭头的合成, 在一般的范畴中也同样适用.

