

面向21世纪本科生教材

抽象代数

■ 牛凤文 编著



全国优秀出版社
武汉大学出版社

0153
V412

面向21世纪本科生教材

抽象代数

牛凤文 编著



全国优秀出版社
武汉大学出版社

HAMBURG

图书在版编目(CIP)数据

抽象代数/牛凤文编著. —武汉: 武汉大学出版社, 1992. 4

面向 21 世纪本科生教材

ISBN 7-307-01229-4

I. 抽… II. 牛… III. 高等数学: 抽象代数 IV. O182. 2

责任编辑: 顾素萍 责任校对: 杜 强 版式设计: 支 笛

出版发行: 武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件: wdp4@whu.edu.cn 网址: www.wdp.whu.edu.cn)

印刷: 湖北民政印刷厂

开本: 850×1168 1/32 印张: 15.75 字数: 403 千字

版次: 1992 年 4 月第 1 版 2003 年 10 月第 4 次印刷

ISBN 7-307-01229-4/O·101 定价: 23.00 元

版权所有, 不得翻印; 凡购买我社的图书, 如有缺页、倒页、脱页等质量问题, 请与当地图书销售部门联系调换。

内 容 提 要

本书系统地介绍抽象代数学的基本概念和基础知识，共七章。主要内容有群、群同态与商群；环、环同态与商环；域与域的扩张。

本书叙述深入浅出，文字生动活泼，例题充实新颖有典型性，推理自然详尽，重点突出而难点分散，可供综合性大学或师范院校数学专业作为教材，亦可供从事初等数学教学和研究工作的教师学习参考，也可以作为计算机科学、物理学、生物学和化学有关领域的工作人员的代数学普及读物。

前 言

(一)

古典代数学以研究代数方程的求解为中心,其历史源远流长.

19世纪初,年青数学家伽罗华(Galois)应用群的概念对高次代数方程是否可用根式求解问题进行了透彻研究并给出了明确回答,他成为抽象代数学新思想的启蒙者.

随后,这种把代数学变成集合论的、公理化的科学的改造不断强化,产生了很多新的思想、新的方法、新的观点和新的结果.

到了20世纪20年代,数学的最古老的分支之一的代数学完成了一次根本性的革命.它的标志是范德瓦尔登(Van der Waerden)的《近世代数学》一书的出版.

时至今日,抽象代数学已经成为很多数学分支中最常用的工具,空前普及,以至近年来,人们不再把这门学问冠之以“近世”、“抽象”等高贵头衔,而朴素地称它为《一般代数学》、《基础代数》,甚至《代数学》.

我们把这本书仍然称为《抽象代数学》只是想把它与仅仅讨论以数为对象的那种经典代数学加以区别.

抽象代数学是古典代数学发展的质的飞跃.学好本课程,可以对初等数学中很多容易模糊含混的问题,如算律、逆运算、多项式与根、因式分解等在公理系统中得以明确.

要在高观点之下认识初等代数,学习些抽象代数知识是绝对必要的.

近年来,抽象代数学本身仍在不断地发展.一方面,它在实际应用中找到了用武之地,如群论在晶体对称、运动和生物学中的应用,群论在研究物质结构模型中的应用,布尔代数、泛代数和代数编码在数理逻辑和计算机科学中的应用.另一方面,代数学向数学内部各相邻分支扩展、渗透,使同调代数、李群与李代数、微分代数、范畴论、半群理论与模论等成为学习拓扑学、泛函分析、微分方程论等必不可少的现代准备知识.

人们要在现代数学的学习和研究中有所发展,也需要学习些抽象代数学知识和思想方法.

因此,本书可以作为从事初等数学教学和研究工作的同志的提高书;可以作为要进一步学习代数学、泛函分析、拓扑学和微分方程论的同志的代数入门书;它也可以作为工作在计算机科学、物理学、生物学和化学有关领域的同志的代数学普及读物.

(二)

抽象代数学是数学中最适合于自学的学科之一.笔者就接触过大批自学抽象代数学取得成功的中学数学教师、科技工作者,很多人并没有在课堂上学过抽象代数课程,经过自学钻研,现在却在讲坛上自如地讲授“群论在物理中的应用”、“群论在化学中的应用”、“工程师用的代数学”,等等.

本课程只假定读者学过中学代数并知道一点矩阵运算规则,此外不要求任何高等数学内容做为准备知识.当然,学过解析几何和高等代数的读者理解本课程的概念会快些,但没学过这类课程的同志直接攻读抽象代数学,一般来说,应该没有原则性障碍.

学好本课程的关键在于对“公理化方法”实质和一些重要抽象概念的理解.

初学者往往被代数学中一个接一个新的概念所困扰,难理解又容易忘记.这实际上是理解的深刻程度的问题,只要读者对重要概念多花些工夫、多思考、多琢磨、多分析比较各种实例,最后能达

到用自己的习惯语言描述这些概念,逐渐就能运用自如.

整个课本中,抽象概念很多.但真正重要的、具有开创意义的,不过 3、5 个而已.只要把这几个概念理解透彻,对于其余属平行引进性质的东西就不需每个都花费同样大的气力了.

切忌把抽象代数学单纯作为“知识”来学,平均使用力量,每个定义都能背下来,但没有一个能“悟出真谛”.学习抽象代数学的一个重要目的是提高“抽象思维”能力.

(三)

本书共分七章.第二章和第三章为群论初步,第四章介绍环论,第七章讨论域的扩张理论.其余三章是准备或过渡或处理专门问题的.

第二章和第三章在本书中地位显要.它给出了处理一个代数体系的“全过程”.对于初学者来说,每个想法,每个解决办法都是新的.所说的初等代数到近世代数的“飞跃”,即从研究数的运算到研究抽象代数系统的结构之“飞跃”,就在这里完成.

处理其他代数系统的问题,虽然各有各的特点和侧重面,但群论中的思想方法对所有代数体系的研究都有指导意义.

关于本书中主要概念的重要程度、中心内容的依赖关系、对读者科学地分配学时的建议可分别见附表 1 和目录.

(四)

现将本书编写过程中的一些想法和做法说明一下.

(1) 课程的具体内容分为四级,最重要的结果称为定理,次之者称为命题,为配合理解定义、定理和命题而举的例是经过选择而有代表意义的,读者应弄懂它们所能说明的问题.每节所穿插的例题不要求读者一定记住.通常,例题中所用的解题方法属典型技巧而且思路比较明确,值得借鉴.

(2) 书中使用了不很明确的语言,分别加上了引号,如“拼

凑”、“缩影”等,读者能大致体会出意思就可以了.

(3) 在定理和命题的证明中有时夹杂着一些猜测和分析性的语言,这样易于理解证明的思路,但不太整齐规范.有时在证明之前把分析想法单列出来,证明就显得干净利落些,读者做习题时应采取后面的办法,分析部分可以不写出来.

(4) 在定理和命题的证明中,如果多说几句话就可直接证明的事情,一般就不一定引用前面某章某节某定理,因为许多读者时间分散,学后面内容时对前面很久以前读过的内容可能已有些遗忘,要求不断地翻回去重看,思想上会产生压力.

(5) 对于抽象代数学中最重要的概念和思想方法,采取难点分散、逐渐加深理解的方法,每次遇到都认真对待.如,等价关系、商集、陪集、商群、剩余环这一个系列;又如,子集生成的子群、子环、理想、子域这一个系列,等等.

(6) 凡是没有列入书后索引的术语,读者可按各种汉语词典的解释加以理解,如“组成”、“充分必要条件”、“蕴涵”、“程序”,等等.

(7) 每节所附的习题并不是按难易程度决定其前后顺序.前面的习题没做出来时,可以放一放,经过一段时间学习与复习后再做,对读者仍然有好处.

面向 **21** 世纪本科生教材

高等数学教程（上、下册）

空间解析几何

 抽象代数

复变函数

线性空间引论

常微分方程

泛函分析基础

数学物理方程

计算方法

信息论基础

数值计算方法

离散数学

运筹学及其应用

线性规划

目 录

前言	1
第一章 集合、映射和关系	1
§ 1 集合	1
§ 2 笛卡尔积和关系	10
§ 3 等价关系、分类和商集	15
§ 4 映射	24
§ 5 置换	43
§ 6 运算	50
小结	61
复习题	62
第二章 群与子群	64
§ 1 群的定义	64
§ 2 子群	75
§ 3 对称群与置换群	87
§ 4 循环群	100
§ 5 阶数	109
§ 6* 群的外直积	119
小结	126
复习题	128

第三章 群的同态	129
§ 1 群的同构	130
§ 2 群上的可逆变换	143
§ 3 群的同态	160
§ 4 商群	173
§ 5* 群的内直积和外直积	192
小结.....	204
复习题.....	206
第四章 环与理想	208
§ 1 环的定义	208
§ 2 子环和理想	222
§ 3 理想与商环(I)	241
§ 4 环的同态映射	252
§ 5* 环的直和	271
小结.....	278
复习题.....	279
第五章 从环到域	281
§ 1 除环和域	281
§ 2 理想与商环(II)	293
§ 3 嵌入问题	301
§ 4 交换环上的多项式	312
§ 5 素域	334
小结.....	339
复习题.....	341
第六章 因子分解理论	342
§ 1 整除	342

§ 2 主理想整环和欧氏环	356
§ 3 唯一分解整环上的多项式环	367
小结	379
复习题	380
第七章 域的扩张	381
§ 1 单纯扩张域	381
§ 2 有限扩张	395
§ 3 代数扩张	412
§ 4 代数封闭域	418
小结	426
复习题	428
习题解答与提示	429
附录	483
名词索引	486

第一章 集合、映射和关系

本课程要对多种多样的代数体系进行分析、比较、归纳、概括,从理论上加以抽象化、公理化,背景十分广泛.笼统说来,代数体系是一些有代数运算的集合.所以,我们首先要熟悉集合论中的基本概念、符号和思维方法.

这一章是抽象代数学的基础,也差不多是所有现代数学分支的基础.

为使自学者不过多依赖其他参考书,使本书基本上自成体系,这里可以说是从头讲起.

对集合和映射概念比较熟悉的读者可对照例题检查一下自己原有的理解是否正确.初学者则必须认真地弄懂定义中每一个字的含义,搞清楚定理证明和习题中每一步推理的根据.

第三节中,等价关系与分类、商集与自然映射都是本书中经常用到的,而且要不断深化的概念,读者必须很好地掌握.

§1 集 合

在中学阶段,大家已经反复使用诸如集合、元素等概念.每一组对象的全体形成一个集合,集合里的各个对象叫做这个集合的元素.

本书用大写英文字母 A, B, C, \dots 代表集合,用小写英文字母 a, b, c, \dots 表示元素.

例如,这里有某青年小组名单如下

张奋学, 22岁, 男, 拟考抽象代数学;

王忠, 26岁, 男, 拟考英语;

李立, 22岁, 女, 拟考政治经济学;

张自强, 29岁, 男, 拟考英语;

王群, 22岁, 女, 拟考英语.

那么, 本组王姓青年的集合是

$$\{\text{王忠}, \text{王群}\};$$

该组人员年龄组成的集合是

$$\{22\text{岁}, 29\text{岁}, 26\text{岁}\};$$

他们中男青年拟考课程的集合为

$$\{\text{抽象代数学}, \text{英语}\}.$$

用 \mathbf{I} 代表所有整数形成的集合; 用 \mathbf{R} 代表所有实数形成的集合; 用 \mathbf{C} 代表所有复数形成的集合.

$a \in A$ 表示 a 是集合 A 的一个元素, 也说是 a 属于 A , A 含有 a . 如果 a 不是 A 的元素, 则记为 $a \notin A$, 也说是 a 不在 A 里, A 不含 a .

定义 1 集合 A 和 B 是相等的(记为 $A = B$)当且仅当 A 的每个元素都是 B 的元素且 B 的每个元素都是 A 的元素.

由此定义知道, 如果要列举出一个集合的所有元素, 那么列举的顺序是无关紧要的. 例如

$$\{22\text{岁}, 29\text{岁}, 26\text{岁}\} = \{29\text{岁}, 26\text{岁}, 22\text{岁}\},$$

$$\{\text{春}, \text{夏}, \text{秋}, \text{冬}\} = \{\text{秋}, \text{春}, \text{冬}, \text{夏}\}.$$

在一个无穷集中列举其元素的方法更可用很多不同方式, 例如

$$\{2, 4, 6, \dots, 1, 2, 3, \dots\}$$

$$= \{\dots, 6, 4, 2, 1, 3, 5, \dots\}$$

$$= \{1, 2, 3, 4, \dots\}.$$

今后, 我们最常用的确定一个集合的方法是所谓描述方法, 即用数学表达式给出该集合元素的性质. 例如, 整数 72 的所有因数的集合

$\{\pm 72, \pm 36, \pm 18, \pm 24, \pm 12, \pm 6, \pm 4, \pm 3, \pm 2, \pm 1, \pm 8, \pm 9\}$
可记为

$$\{a \in \mathbf{I} \mid a \text{ 整除 } 72\};$$

对于取定坐标系的平面 \mathbf{R}_2 上以原点为中心的单位圆上所有点所形成的集合可记为

$$\{(x, y) \in \mathbf{R}_2 \mid x^2 + y^2 = 1\};$$

而位于该单位圆以外同时又在以原点为中心半径为 2 的圆内的所有点构成的集合是

$$\{(x, y) \in \mathbf{R}_2 \mid x^2 + y^2 > 1 \text{ 且 } x^2 + y^2 < 4\};$$

上述两圆给定后,在小圆内的所有点和在大圆外的所有点一起形成的集合是

$$\{(x, y) \in \mathbf{R}_2 \mid x^2 + y^2 < 1 \text{ 或者 } x^2 + y^2 > 4\}.$$

在人类文明史上,数字 0 的使用是件很了不起的大事,对数学发展有重要作用.同样,为了方便起见,我们把不含任何元素的集合称为空集,它在集合论中也是有重要作用的,记为 \emptyset . 例如

$$\{x \in \mathbf{R} \mid 2x^2 + 1 = 0\} = \emptyset, \quad \{x \in \mathbf{I} \mid 3x = 5\} = \emptyset.$$

又如,前面提到的青年小组中 20 岁以下青年的集合是空集.

定义 2 设 A, B 都是集合.说集合 A 是集合 B 的子集合,当而且仅当 A 的每个元素都是 B 的元素.换句话说, A 是 B 的子集合当而且仅当 $x \in A$ 蕴涵着 $x \in B$.当 A 是 B 的子集合时,记做 $A \subseteq B$,也说是 A 属于 B 或 B 包含 A .符号 $A \not\subseteq B$ 表示 A 不是 B 的子集.

如果 $A \subseteq B$,但 $A \neq B$,即有 B 的元素不属于 A ,则说 A 是 B 的真子集,记为 $A \subset B$.

因为空集 \emptyset 不含任何元素,说“ \emptyset 的每个元素 a 都具有某某性质”这句话,从形式逻辑上看,在数学中不会引起矛盾.于是,我们可以说“ \emptyset 的任意元素都能被 2 整除”,也可以说“ \emptyset 的每个元素都不能被 2 整除”或“ \emptyset 中的每个元素都是要考抽象代数学的青年人”等等.于是,我们可以约定,对任意集合 A ,都有 $\emptyset \subseteq A$.

任意集合 A ,若 $A \neq \emptyset$,则说 A 是非空集合或 A 非空.由于

$\emptyset \subseteq A$ 永远成立,当 A 非空时,就有 $\emptyset \subset A$.

例题 1 给出集合 $\{1, 2, 3\}$ 所有子集所形成的集合.

首先要提醒读者, \emptyset 是这个集合的一个子集,它不含任何元素并不意味着可写可不写.

其次,要知道 A 也是自己的一个子集.

还有,子集 $\{1, 2\}$ 和子集 $\{2, 1\}$ 是一回事,不要重复开列.

最后,要注意此题答案是唯一确定的,但开列元素的顺序可以不同,下面给出一种写法:

$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

这里容易犯的错误是把某个数字看成是子集.我们说, 2 是 $\{1, 2, 3\}$ 的一个元素,而 2 这一个数字所构成的集合 $\{2\}$ 是 $\{1, 2, 3\}$ 的一个子集.

定义 3 集合 A 的所有子集所形成的集合称为 A 的幂集.

定义 4 由任意集合 A, B 决定一个集合

$$\{x \mid x \in A \text{ 或者 } x \in B\},$$

称为 A 和 B 的并集,记为 $A \cup B$.

这个定义中“或者”二字是关键词,它是说只要 x 属于 A, B 之一,它就算 $A \cup B$ 的元素,即 $x \in A$ 蕴涵 $x \in A \cup B$,而 $x \in B$ 亦蕴涵 $x \in A \cup B$, x 同时属于 A 和 B 时,也蕴含 $x \in A \cup B$.

例如,

$$\{1, 2, 3\} \cup \{2, 3, 4, 5\} = \{1, 2, 3, 4, 5\},$$

$$\{x \in \mathbb{I} \mid x \text{ 整除 } 8\} \cup \{x \in \mathbb{I} \mid x \text{ 整除 } 12\}$$

$$= \{-12, -8, -6, -4, -2, -1, 1, 2, 3, -3, 4,$$

$$6, 8, 12\},$$

$$\{(x, y) \in \mathbb{R}_2 \mid x^2 + y^2 < 1\} \cup \{(x, y) \in \mathbb{R}_2 \mid x^2 + y^2 > 4\}$$

$$= \{(x, y) \in \mathbb{R}_2 \mid x^2 + y^2 < 1 \text{ 或者 } x^2 + y^2 > 4\}.$$

定义 5 由任意集合 A, B 可决定一集合

$$\{x \mid x \in A \text{ 同时 } x \in B\},$$

称为 A 和 B 的交集,记为 $A \cap B$.

这个定义中的关键词是“同时”二字,它表示 x 既属于 A 又属于 B ,两件事同时成立,人们也用“并且”,“而且”等表示这种情形.

例如,

$$\{1,2,3\} \cap \{2,3,4,5\} = \{2,3\}.$$

$$\{x \in \mathbf{I} \mid x \text{ 整除 } 8\} \cap \{x \in \mathbf{I} \mid x \text{ 整除 } 12\}$$

$$= \{-4, -2, -1, 1, 2, 4\}.$$

$$\{(x, y) \in \mathbf{R}_2 \mid x^2 + y^2 \geq 1\} \cap \{(x, y) \in \mathbf{R}_2 \mid x^2 + y^2 \leq 4\}$$

$$= \{(x, y) \in \mathbf{R}_2 \mid 1 \leq x^2 + y^2 \leq 4\}.$$

例题 2 如果 A, B 和 C 都是某集合的子集合.证明:

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

分析 我们要证明上式左端集合的每个元素都是右端那个集合的元素,同时右端集合的每一个元素都是左端那个集合的元素.

还有,当已知 x 有某些性质,要证 $x \in X \cup Y$ 时,如果 $x \in Y$,当然 $x \in X \cup Y$; 如果 $x \notin Y$,我们就要证明必有 $x \in X$. 因为“如果 $x \in Y$, 当然 $x \in X \cup Y$ ”一句话恒对,从而不必每次都提起叙述一遍,而直接从“如果 $x \notin Y, \dots$ ”入手验证.

证明 对每个 $x \in (A \cap B) \cup C$, 由并集的定义知 $x \in A \cap B$ 或者 $x \in C$.

当 $x \in C$ 时, x 当然属于 $A \cup C$, 同时,也当然属于 $B \cup C$, 即 $x \in A \cup C$ 且 $x \in B \cup C$.

按交集的定义, $x \in (A \cup C) \cap (B \cup C)$.

当 $x \in A \cap B$ 时, 即 $x \in A$ 并且 $x \in B$. 所以, $x \in A \cup C$ 并且 $x \in B \cup C$. 由交集定义, 知 $x \in (A \cup C) \cap (B \cup C)$.

总之, $x \in (A \cap B) \cup C$ 则必有 $x \in (A \cup C) \cap (B \cup C)$.

反之, 对任意 $x \in (A \cup C) \cap (B \cup C)$, 如果 $x \notin C$, 由于 $x \in A \cup C$ 且 $x \in B \cup C$ 可推出 $x \in A$ 且 $x \in B$, 也就是 $x \in A \cap B$.

这就证明了 $x \in (A \cup B) \cap (B \cup C)$, 则 $x \in (A \cap B) \cup C$. \square

例题 3 问对于集合的交集和并集是否有如下的规律: 对任意集合 A, B 和 C 都有 $(A \cap B) \cup C = A \cap (B \cup C)$.