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

本科生
数学基础课教材

抽象代数 I

赵春来 徐明曜 编著

北京大学出版社
PEKING UNIVERSITY PRESS

北京大学数学教学系列丛书

抽象代数 I

赵春来　徐明曜　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 I / 赵春来, 徐明曜编著. — 北京: 北京大学出版社, 2008.10

(北京大学数学教学系列丛书)

ISBN 978-7-301-14168-7

I. 抽 … II. ①赵 … ②徐 … III. 抽象代数 – 高等学校 – 教材 IV. O153

中国版本图书馆 CIP 数据核字 (2008) 第 124478 号

书　　名: **抽象代数 I**

著作责任者: 赵春来　徐明曜　编著

责 任 编 辑: 刘　勇

标 准 书 号: ISBN 978-7-301-14168-7/O · 0759

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　编辑部 62752021

出版部 62754962

电 子 信 箱: zpup@pup.pku.edu.cn

印　刷　者: 北京汇林印务有限公司

发　行　者: 北京大学出版社

经　销　者: 新华书店

890mm×1240mm　A5　7 印张　180 千字

2008 年 10 月第 1 版　2008 年 10 月第 1 次印刷

印　　数: 0001—4000 册

定　　价: 18.00 元

作者简介

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).

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).

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的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. 本课程是为学习过高等代数或线性代数的本科生而编写的. 本书可以作为我们为研究生编写的《抽象代数 II》的预备教材.

现代代数学有很多分支，而每个分支又都有众多的抽象的概念，因此初学者大多会觉得抽象代数似乎就是若干概念的堆积，看不出有什么深刻的结果和用途. 在本书中，我们一方面要讲解必要的基础知识，同时也力图使读者能够对于代数学的主要思想和方法有所体会. 例如，在讲解了群的知识之后，我们用群论的方法考查了正多面体，以诠释群论本质上是研究对称的学科；在讲解了环和域之后，我们介绍了它们在几何与数论方面的应用.

本书总的安排大体上依循了我们多年教学中使用的聂灵沼和丁石孙教授编写的《代数学引论》. 该引论是为一学年的代数学教学而编著的. 为了能够将授课时间限制在一个学期之内 (约 45 学时)，本书不得不在内容上作较大的压缩 (也作了一些补充). 第一章 (群、环、体、域的基本概念) 中把这些代数结构具有共性的部分 (例如子结构、商结构、同态、同构、直和与直积等) 一并作了介绍；第二、三、四章分别讲授群、环、域比较专门的内容；第五章简述了模与格的最基础的一些知识.

前面提到，我们已经出版了《抽象代数 II》作为研究生教材. 由于研究生的生源复杂，其本科和研究生阶段不一定在同一学校学习. 因此，《抽象代数 I》和《抽象代数 II》内容上有一些重叠，其目的是使两部书都尽量做到独立自封，各成一完整的教材.

本书的习题较多，都是经过我们精心挑选的. 其中包含了大量精典的例子，并且给出了比较详细的提示或解答，这有利于读者理解正文的教学内容. 不过我们仍然建议大家尽量独立地给出

解答，而不是直接去看习题提示.

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

2008 年 3 月于北京大学

数学科学学院

目　录

第 1 章　群、环、体、域的基本概念

本章介绍代数学中最基本、最常见的一些概念和结果.

首先我们回顾一下集合论中的一些简单知识. 设 A, B 为两个集合. φ 称为由 S 到 T 的一个**映射**, 如果对于任一 $a \in A$, 都唯一存在 B 中的元素 $\varphi(a)$ 与之对应. 此时 $\varphi(a)$ 称为 a(在 φ 下) 的**像** , a 称为 $\varphi(a)$(在 φ 下) 的**原像** 或**反像**. 一般地, 设 S 为 A 的任一子集, 则 $\{\varphi(a) \mid a \in S\}$ 称为 S(在 φ 下) 的**像**, 常记为 $\varphi(S)$; 设 T 为 B 的任一子集, 则 $\{a \in S \mid \varphi(a) \in T\}$ 称为 T (在 φ 下) 的**反像**, 常记为 $\varphi^{-1}(T)$. 如果 A 中任意两个不同元素在 φ 下的像都不同, 则称 φ 为**单射**. 如果 B 中任一元素在 A 中都有原像, 则称 φ 为**满射**. 既单又满的映射称为**双射**, 或**一一对应**.

§1.0　预备知识

作为特殊情形, 集合到自身的映射称为**变换**.

集合 A 与 B 的**笛卡儿积** (亦称为**直积**) 是指 A 的元素与 B 的元素构成的有序对的集合, 即 $\{(a,b) \mid a \in A,\ b \in B\}$, 通常记为 $A \times B$ (类似地可以定义多个乃至无穷多个集合的笛卡儿积). 集合 A 上的一个**二元运算** 即是由 $A \times A$ 到 A 的一个映射. A 上的一个**二元关系** R 定义为 $A \times A$ 的一个子集. 如果 $(a_1, a_2) \in R$, 就称 a_1 与 a_2 有关系 R, 记为 $a_1 R a_2$. 设 R 是 A 上的一个二元关系, 如果满足:

(1) 反身性, 即 aRa $(\forall a \in A)$;

(2) 对称性, 即 $a_1 R a_2$ 蕴含 $a_2 R a_1$ $(\forall a_1, a_2 \in A)$;

(3) 传递性, 即 $a_1 R a_2$ 且 $a_2 R a_3$ 蕴含 $a_1 R a_3$ $(\forall a_1, a_2, a_3 \in A)$,

则称 R 为 A 上的一个**等价关系**. 此时 A 中互相等价的元素组成的子集称为一个**等价类**. 任意两个不同等价类的交为空集，整个集合 A 等于所有等价类的无交并. 等价关系通常用“ $\sim$ ”表示，A 中所有等价类组成的集合记为 $A/\sim$.

如果将等价关系的定义性质 (2) 替换为

(2') 反对称性，即 a_1Ra_2 且 a_2Ra_1 蕴含 $a_1=a_2$,

则称 R 为 A 上的一个**偏序关系**, 或**序关系**. 具有偏序关系的集合称为**偏序集**. 如果一个偏序集中的任意两个元素之间都有偏序关系，则称此偏序集为一个**全序集**. 偏序关系通常用“ $\leq$ ”表示.

习　题

1. 设 X 和 Y 是两个集合，$f\colon X\to Y$ 和 $g\colon Y\to X$ 是两个映射. 如果 $g\circ f=\mathrm{id}_X$, 则称 g 为 f 的一个**左逆**; 如果 $f\circ g=\mathrm{id}_Y$, 则称 g 为 f 的一个**右逆**. 如果 g 既是 f 的左逆又是 f 的右逆，则称 g 为 f 的一个**逆**. 证明

(1) f 有左逆当且仅当 f 是单射;

(2) f 有右逆当且仅当 f 是满射;

(3) f 有逆当且仅当 f 是双射;

(4) 如果 f 有左逆 g, 同时又有右逆 h, 则 $g=h$;

(5) 如果 f 有逆，则 f 的逆唯一，f 的逆记为 f^{-1};

(6) 如果 f 有逆，则 $(f^{-1})^{-1}=f$.

2. 举例说明等价关系的定义中的三个条件是相互独立的 (即任意两条不蕴含剩下的一条).

§1.1　群的基本概念

在这一节中我们将介绍群的一些基本概念. 这些概念的大多数 (例如子结构、商结构、同态、同构、直和等) 在其他的代数结构 (如环、模) 中都有类似的构造.

1.1.1 群的定义和简单性质

定义 1.1 如果一个非空集合 G 上定义了一个二元运算 $\circ$, 满足:

(1) **结合律**: $(a\circ b)\circ c=a\circ(b\circ c)$ $(\forall\, a,b,c\in G)$;

(2) 存在**幺元**: 存在 $e\in G$, 使得

$$e\circ a=a\circ e=a \quad (\forall\, a\in G)$$

(e 称为 G 的幺元);

(3) 存在**逆元**: 对任意的 $a\in G$, 存在 $b\in G$, 使得

$$a\circ b=b\circ a=e$$

(b 称为 a 的逆元),

则称 G 关于运算 $\circ$ 构成一个**群**, 记为 $(G,\circ)$, 或简记为 G.

群 G 中若还成立以下的

(4) **交换律**: $a\circ b=b\circ a$ $(\forall\, a,b\in G)$,

则称 G 为**交换群** 或**Abel 群**.

在不致引起混淆的情况下, 运算符号 "$\circ$" 经常略去不写.

由结合律 (1) 可以推出下面的广义结合律:

(1′) **广义结合律**: 对于任意有限多个元素 $a_1, a_2, \cdots, a_n\in G$, 乘积 $a_1a_2\cdots a_n$ 的任何一种 "有意义的加括号方式" (即给定的乘积的顺序) 都得出相同的值, 因而上述乘积是有意义的.

顺便介绍一下半群和幺半群的概念. 如果一个非空集合 S 上有二元运算, 此运算满足结合律, 则称此集合关于这个二元运算构成一个**半群**. 具有幺元的半群称为**幺半群**.

下面我们介绍群中的一些最基本概念和事实.

命题 1.2 (1) *群的幺元唯一;*

(2) *群中任一元素的逆元唯一;*

(3) *群中有消去律, 即 $ax=ay$ 蕴含 $x=y$ (左消去律), $xa=ya$ 蕴含 $x=y$ (右消去律).*

证明　(1) 设 e 和 e' 都是群 G 的幺元，则有 $e = ee' = e'$.

(2) 设 b 和 b' 都是群 a 的逆元，则有

$$b = be = b(ab') = (ba)b' = eb' = b'.$$

(3) 设 $ax = ay$. 两端左乘 a 的逆元 b, 得 $bax = bay$. 而 $ba = e$, 故有 $x = y$. 同样可证右消去律. □

以后我们将 a 的唯一的逆元记为 a^{-1}. 由广义结合律 (1′), 任意有限多个元素的乘积 $a_1a_2\cdots a_n$ 是有意义的. 特别地，我们可以规定群 G 中元素 a 的整数次方幂如下：设 n 为正整数，则像通常一样，令

$$a^n = \underbrace{aa\cdots a}_{n个}, \quad a^0 = e, \quad a^{-n} = (a^{-1})^n.$$

在这种记号下，对于所有整数 m, n, 显然有

$$a^m a^n = a^{m+n}.$$

如果 G 是交换群，则易见 $(ab)^n = a^n b^n$.

群所含的元素个数称为群的**阶**. 群 G 的阶记为 $|G|$. 如果 $|G| < \infty$, 则称 G 为**有限群**, 否则称为**无限群**.

现在我们列举一些常见的群的例子.

例 1.3　整数集合 $\mathbb{Z}$、有理数集合 $\mathbb{Q}$、实数集合 $\mathbb{R}$、复数集合 $\mathbb{C}$ 关于加法都构成群. 非零有理数集合 $\mathbb{Q}^\times$、非零实数集合 $\mathbb{R}^\times$、非零复数集合 $\mathbb{C}^\times$、正实数集合 $\mathbb{R}^+$ 关于乘法都构成群.

例 1.4　设 n 是一个正整数，则 n 次单位根的全体关于乘法构成群，称为 n **次单位根群**, 记为 μ_n, 它包含 n 个元素.

例 1.5　设 n 是一个正整数. 整数集合 $\mathbb{Z}$ 模 n 的剩余类关于加法构成群，它包含 n 个元素. 与 n 互素的剩余类关于乘法构成群，它包含 $\varphi(n)$ 个元素，φ 为 Euler φ 函数.