北京工业大学研究生创新教育系列著作

基础代数

姚海楼　平艳茹　编著

科学出版社

北京工业大学研究生创新教育系列著作

基础代数

姚海楼　平艳茹　编著

科学出版社
北京

内 容 简 介

本书从基础代数的基本概念开始，通过基本例子，逐步介绍群、环、模、域的基本概念和基本理论．全书共分8章．第1章首先将全书所用到的集合与映射等基本知识进行简明扼要介绍，然后介绍半群与群、子群与陪集、循环群与变换群及群的同构、正规子群与商群、群同态与同态基本定理、群的直积．第2章介绍环的基本知识，主要内容有环的定义与基本性质，子环、理想与商环，环的同态与同态基本定理，素理想与极大理想、分式环，环的特征与素域，以及环的直和．第3章介绍交换环的因子分解理论，主要内容有唯一分解环、主理想环与欧氏环以及多项式环有关唯一分解性质等．第4章介绍群论的进一步理论，主要内容有群在集合上的作用、p-子群与西罗定理、有限交换群、幂零群与可解群．第5章介绍模的基本理论，主要内容有模的定义与基本性质，子模与模同态，模同态的基本定理，本质子模与多余子模，加补与交补，模的根与基座，自由模、投射模与内射模等．第6章介绍了环的进一步理论，主要内容有单环与本原环、环的Jacobson根、半单环、阿廷环与诺特环以及局部环．第7章与第8章介绍域论与伽罗瓦理论，主要内容包括扩域、分裂域、闭包和正规性、尺规作图问题、有限域、超越基、伽罗瓦理论的基本定理、多项式的伽罗瓦群、分离性、循环扩域和分圆扩域、根扩域和一般n次代数方程根的公式求解理论等．

本书是基础代数的入门书籍，可作为数学专业的本科生的近世代数教材与研究生的基础代数教材，也可供相关专业的教师和科研人员参考．

图书在版编目（CIP）数据

基础代数/姚海楼，平艳茹编著．—北京：科学出版社，2016.6

北京工业大学研究生创新教育系列著作

ISBN 978-7-03-048969-2

Ⅰ．①基… Ⅱ．①姚… ②平… Ⅲ．①代数-研究生-教材 Ⅳ．①O15

中国版本图书馆CIP数据核字（2016）第138994号

责任编辑：钱 俊 胡庆家／责任校对：彭 涛

责任印制：张 伟／封面设计：蓝正设计

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

北京京华虎彩印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2016年6月第 一 版 开本：720×1000 B5

2016年6月第一次印刷 印张：23 1/2

字数：452 000

定价：98.00元

（如有印装质量问题，我社负责调换）

前　　言

现代代数学是以研究数字、文字和更一般元素的代数运算的规律，以及与这些运算适合的公理而定义的各种代数结构（群、环、模、域、代数、格等）的性质为中心问题的. 由于代数运算贯穿在任何数学理论和应用数学问题里，且代数结构及其元素的一般性、现代代数学的一般方法和结果渗透到各个不同的数学领域中，现代代数学成为具有新面貌和新内容的充满活力的数学领域.

群、环、模和域是四个基本的代数结构. 抽象代数的理论和思想不仅对数学工作者是必要的，也是值得一般的科学工作者借鉴的. 本书从第 1 章到第 7 章给出这四个代数结构的基本性质和基本理论. 第 8 章较为详细地介绍伽罗瓦理论. 希望读者通过对这些内容的学习，能够掌握群、环、模和域这四个代数结构的基本理论. 同时，也希望读者通过对抽象的数学对象的了解、认识、理解和把握，养成良好的数学抽象的思维习惯.

本书是按照本科数学专业“近世代数”课程与硕士研究生“基础代数”课程的教学需要来编写的. 1.1 节以朴素的集合论知识作为起点，为后面各章节提供必要的集合论的预备知识. 1.2 节到第 4 章给出通常“近世代数”课程的群、环、域的基本理论，内容比较丰富，如果按每周 3～4 学时全部讲授完，显然不可能. 教师可根据教学时间等具体情况进行选择，同时要求学生增大阅读量. 群的学习不仅要掌握一些基本概念，更要掌握群的结构理论. 有限群的西罗定理是研究有限群结构的重要工具，所以，这些内容应该是必读的. 而且这部分内容在第 8 章讨论域的伽罗瓦理论时也是必不可少的工具. 因此，第 4 章围绕有限群的结构展开讨论，较为详细地介绍西罗定理、有限交换群结构定理、有限群的轨道公式、幂零群与可解群等. 模是域上线性空间在一般环上的推广. 由于表示论的兴起，模的作用越来越重要，现在已经成为数学领域特别是代数学领域的重要研究工具. 同时，模论本身也是一个重要研究领域，有许多重要问题有待研究解决. 因此，许多高校的数学专业特别是代数学方向的研究生或是单独开设模论课程，或是在相关课程里加入模论的基本内容. 所以，第 5 章较为详细地介绍模的基本理论. 特别地，为更好地学习模这部分内容，借助向量空间的概念与模的概念作比较，以便让学生有直观的认识；用一定篇幅介绍子模的加补和交补及其性质，以及本质子模和多余子模，并尽可能地在展开内容讨论时应用它们，以便于学生学习掌握. 第 6 章介绍环的现代理论，主要内容包括环的 Jacobson 根和若干特殊环诸如半单环、局部环与诺特环等，并以模为工具对它们进行刻画. 第 7 章介绍域扩张的基本理论，并通过域的代数扩张理论解决

古希腊三大几何问题. 第 8 章较为详细地介绍伽罗瓦理论. 通过对伽罗瓦理论的学习, 学生了解抽象代数的产生及发展的历史渊源和发展动力, 进而掌握群、环、域之间的联系以及深邃的伽罗瓦思想. 建议可根据实际情况选取第 4 章(或第 5 章)到第 8 章适当章节作为研究生"基础代数"课程的内容.

本书配置一些例题和习题, 相当一部分是对教学重点的理解和补充. 这对学生掌握课程内容和灵活应用是很有帮助的.

本书可作为抽象代数学的本科生与研究生课程教材. 本书的编写参照了一些相关文献, 精选了一些内容, 并结合了自己的多年教学经验, 书中的许多定理和命题的证明尽可能深入浅出, 用尽可能最简单的方法给出. 所以, 本书也可作为自学教材. 本书适合数学专业本科生、研究生及数学爱好者学习使用. 通过本书的学习, 读者能较为系统地打下抽象代数学的理论基础, 为数学的其他分支领域特别是代数学领域的学习提供方便.

本书的主要内容由编著者近十余年来在北京工业大学讲授代数学专业研究生的"基础代数"课程和本科生的"近世代数"课程的讲稿整理而成.

由于编著者知识有限, 书中疏漏及不妥之处在所难免, 敬请读者批评指正.

编著者
2015 年 10 月
北京工业大学

符　号　表

$\mathbb{N}$	自然数集
$\mathbb{Z}$	整数集($\mathbb{Z}^+$ 表示正整数集)
$\mathbb{Q}$	有理数域
$\mathbb{R}$	实数域
$\mathbb{C}$	复数域
$\lvert A\rvert$	集合 A 的元素个数;集合 A 的基数或势
∞	无穷大
$\varnothing$	空集
$\subseteq$	包含于
$\in$	属于
$\notin$	不属于
$\subsetneqq$	包含于且不等于
$\supseteq$	包含
$\cap$	集合交
$\cup$	集合并
$\mathcal{P}(A)$或 2^A	集合 A 的幂集
$U-A$	A 在 U 中的差集
$\aleph_0$	全体自然数集$\mathbb{N}$ 的势(读作阿列夫零)
$\aleph$	全体实数集的势(读作阿列夫)
$A\leqslant G$	A 是群 G 的子群
$[G:A]$	子群 A 在群 G 的指数即 A 在群 G 中的陪集个数
$H\lhd G$	H 是群 G 的正规子群
$I\lhd R$	I 是环 R 的理想
$a\mid b$	a 整除 b
$a\nmid b$	a 不整除 b
$\Leftrightarrow$	当且仅当
$\Leftrightarrow:$	表示“定义为”
$\deg f(x)$	多项式 $f(x)$的次数
$A\leqslant M$ 或 $A\hookrightarrow M$	A 是模 M 的子模
$\vee$	表示“或者”,格的并运算

$\wedge$	表示“并且”，格的交运算
$A \overset{*}{\hookrightarrow} M$	子模 A 是模 M 的本质子模(大子模)
$A \overset{\circ}{\hookrightarrow} M$	子模 A 是模 M 的多余子模(小子模)
$A^{\cdot} \hookrightarrow M$	子模 A 在模 M 内的加补
$A' \hookrightarrow M$	子模 A 在模 M 内的交补
$\Rightarrow$	表示“蕴涵”或者“必要性”
$\Leftarrow$	表示 “充分性”
i. e.	表示 “亦即”
$\exists$	存在
$\forall$	任意一个
$a \equiv b \pmod{n}$	a 与 b 模 n 同余
$o(a)$	元素 a 的周期或阶
$\cong$	同构于

目　录

第1章　群　　论

抽象代数的主要研究对象是各种各样的代数系统，即具有一些代数运算的集合. 其中最简单的是具有一个二元代数运算的代数系统，本章将要介绍的群，就是一个这样的代数系统. 群的理论是近代数学的一个重要分支，它在物理学、化学、信息学等领域都有着广泛的应用.

本章主要介绍群的基本理论. 1.1 节介绍集合与映射等基本知识，为后面内容的介绍做准备. 1.2 节介绍半群与群及其基本性质. 1.3 节介绍子群与陪集. 1.4 节介绍循环群与变换群以及群的同构. 循环群与变换群是两类最常见的群. 1.5 节介绍群的正规子群和商群. 1.6 节介绍群的同态基本定理等内容. 1.7 节介绍群的内外直积概念及基本性质.

1.1　集合与映射

1.1.1　集合的概念

集合是数学中最基本的概念之一，没有确切的定义. 一般地，由具有某种特定性质的具体的或抽象的事物全体组成一个集合(set)，简称集，其中的成员称作这个集合的元素(element). 例如，自然数全体就是一个集合，称为自然数集. 每个自然数就称为自然数集的元素.

集合一般用大写英文字母 $A,B,C,\cdots$ 表示，集合中的元素用小写英文字母 $a,b,c,\cdots$ 表示.

对集合 A 来说，某一事物 x 若是集合 A 的元素，就称 x 属于 A，记为 $x\in A$；若 x 不是 A 的元素，即 x 不属于 A，记为 $x\notin A$；二者必居其一.

集合的表示方法通常有两种：一种是直接列出所有的元素，如 $A=\{1,2,3\}$；另一种是规定元素所具有的性质 P 来表示，如 $A=\{x|x\text{ 具有性质 }P\}$.

一个集合 A 的元素个数用 $|A|$ 表示. 当 A 中的元素个数有限时，称 A 为有限集(finite set)；否则，就称 A 为无限集(infinite set). 用 $|A|=\infty$ 表示 A 为无限集，用 $|A|<\infty$ 表示 A 为有限集.

如果集合 A 中的元素都是集合 B 中的元素，则称 A 为 B 的子集(subset)，记为 $A\subseteq B$，读作 A 包含在 B 中，或记作 $B\supseteq A$，读作 B 含有 A. 显然，$A\subseteq A$. 不含有任何元素的集合称为空集(empty set 或 null set)，记为 $\varnothing$. 例如，

$$A=\{x|x\text{ 为实数},x^2+1=0\}$$

是一个空集. 如果 $A\subseteq B$, 且 B 中有一个元素不属于 A, 称 A 是 B 的真子集(proper set).

集合 A 与集合 B 称为相等的, 记为 $A=B$, 如果它们含有相同的元素. 所以, $A=B$ 当且仅当 $A\supseteq B$ 且 $B\supseteq A$.

由集合 A 的所有子集构成的集合称为 A 的幂集(power set), 记作 $\mathcal{P}(A)$ 或 2^A. 例如, 若 $A=\{1,2,3\}$, 则

$$\mathcal{P}(A)=\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},A\}.$$

当 $|A|<\infty$ 时, $\mathcal{P}|(A)|$(即 $\mathcal{P}(A)$ 中元素个数)正好是 $2^{|A|}$. 事实上, 设 $|A|=n$, 则 A 的含有 k 个元素的子集共有 C_n^k 个, 于是, A 的所有子集个数为

$$C_n^0+C_n^1+\cdots+C_n^k+\cdots+C_n^n=2^n=2^{|A|}.$$

1.1.2 集合的运算

设 A 与 B 是两个集合. 由 A 与 B 的一切元素所组成的集合称为 A 与 B 的并集(union set), 记为 $A\cup B$. 所有既属于 A 又属于 B 的元素组成的集合称为 A 与 B 的交集(intersection set), 记为 $A\cap B$.

完全类似地可以定义任意多个集合的并集与交集. 设 $\{A_i \mid i\in I\}$ 是任意一组集合, 其中 i 是集合的指标, 它在某个固定指标集 I 中变化, 由一切 $A_i(i\in I)$ 的所有元素组成的集称为这组集合的并集, 记为 $\bigcup\limits_{i\in I}A_i$; 同时属于每个集合 $A_i(i\in I)$ 的所有元素组成的集合, 称为这组集合的交集, 记为 $\bigcap\limits_{i\in I}A_i$. 注意, 在组成若干个集合的并集时, 同时是两个或两个以上的集合所公有的元素在并集中只算作一个. 当 $A\cap B=\varnothing$ 时, 称 A 与 B 不交(disjoint); 当 $A\cap B\neq\varnothing$ 时, 称 A 与 B 相交. 对于集合 A 与 B, 属于 A 而不属于 B 的元素所构成的集合称为 A 与 B 的差集(difference set), 记为 $A-B$ 或 $A\backslash B$; 称 $A\Delta B=(A-B)\cup(B-A)$ 为 A 与 B 的对称差集(symmetric set). 如果 A 是集合 U 的子集, 则 A 在 U 中的差集称为 A 在 U 中的余集(complementary set), 记为 A', 即 $A'=U-A$.

容易证明, 集合的并与交运算有下面一些性质:

(1) $A\cup A=A$, $A\cap A=A$; (并与交的幂等律)

(2) $A\cup\varnothing=A$; (空集是加法的零元)

(3) $A\cup B=B\cup A$, $A\cap B=B\cap A$; (交换律)

(4) $A\cup(B\cup C)=(A\cup B)\cup C$,
$A\cap(B\cap C)=(A\cap B)\cap C$; (结合律)

(5) $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$,
$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$; (分配律)

(6) $A\cap(A\cup B)=A$, $A\cup(A\cap B)=A$; (吸收律)

(7) 若 $A\subseteq C$, 则 $A\cup(B\cap C)=(A\cup B)\cap C$; (模律)

(8) $(A\cup B)'=A'\cap B'$，$(A\cap B)'=A'\cup B'$； （德·摩根律）

(9) $(A')'=A$；

(10) $(A-B)\cap C=(A\cap C)-(B\cap C)$. （减法分配律）

设 S 是任意一个集，$\{A_i \mid i\in I\}$ 是 S 中的一组子集，则有

(11) $S-\bigcup\limits_{i\in I}A_i=\bigcap\limits_{i\in I}(S-A_i)$；

(12) $S-\bigcap\limits_{i\in I}A_i=\bigcup\limits_{i\in I}(S-A_i)$.

证明 记 $S-\bigcup\limits_{i\in I}A_i$ 为 P，$\bigcap\limits_{i\in I}(S-A_i)$ 为 Q. 下面证明 $P=Q$.

设 $x\in P$，按定义有 $x\in S$ 而且 $x\notin\bigcup\limits_{i\in I}A_i$. 因此，对每个 $i\in I$，$x\notin A_i$，有 $x\in S-A_i(i\in I)$，即 $x\in Q$. 这就是说，凡 P 中的元素都属于 Q，所以 $P\subseteq Q$.

反过来，设 $x\in Q$，则对任何 $i\in I$，有 $x\in S-A_i$，即 $x\in S$，而且 $x\notin A_i(i\in I)$. 因此，$x\notin\bigcup\limits_{i\in I}A_i$，所以 $x\in S-\bigcup\limits_{i\in I}A_i=P$. 这就是说，凡 Q 中的元素必属于 P，所以 $Q\subseteq P$. 综合起来就得到 $P=Q$.

性质(12)的证明是类似的.

1.1.3 映射

映射是函数概念的推广，描述了两个集合的元素之间的关系.

定义 1.1.1 设 A 与 B 是两个集合，A 到 B 的一个映射(map)是指一个法则，它使 A 中每一个元素 a 都有 B 中一个确定的元素 b 与之对应. 如果映射 f 使 B 中元素 b 与 A 中元素 a 对应，就记为 $f(a)=b$. 元素 b 称为 a 在 f 下的像(image). 集合 A 称为 f 的定义域(domain)，集合 B 称为 f 的上域(codomain). 当 $A=B$ 时，也称 A 到 A 的映射为 A 到自身的变换(transformation). 通常用记号 $f:A\to B$ 或 $A\xrightarrow{f}B$ 表示 f 是 A 到 B 的一个映射. 记号 $f:x\mapsto f(x)$ 表示映射 f 所规定的元素之间的具体对应关系. 对于集合 A 到集合 B 的两个映射 f 与 g，如果对 A 中每一个元素 a 都有 $f(a)=g(a)$，则称它们是相等的，记为 $f=g$.

例 1.1.1 设 A 是全体整数的集合，B 为全体奇数的集合，定义

$$f(n)=2n+1 \quad (n\in A),$$

则 f 是 A 到 B 的一个映射.

例 1.1.2 设 $A=B=\mathbb{R}$（实数集合），对应法则 g 定义为 $x\mapsto x^5$，它是熟知的初等函数，这是从 $\mathbb{R}$ 到 $\mathbb{R}$ 的一个映射.

例 1.1.3 设 A 是数域 $\mathbb{F}$ 上的 n 阶矩阵的集合，定义 $h:M\mapsto \det M$（M 的行列式），$M\in A$，这是 A 到数域 $\mathbb{F}$ 的一个映射.

例 1.1.4 设 A 是数域 $\mathbb{F}$ 上的 n 阶矩阵的集合，定义 $S(a)=aE$，$a\in\mathbb{F}$，E 是单位矩阵，这是 $\mathbb{F}$ 到 A 的一个映射.

例 1.1.5 设 A 与 B 是两个非空集合，b_0 是 B 中的一个固定元素，定义 f: