纪精品规划教材系列

近世代数

JINSHIDAISHU

主编◎阮佶

延边大学出版社

21世纪精品规划教材系列

近世代数

阮　佶　主编

延边大学出版社

图书在版编目(CIP)数据

近世代数 / 阮佶主编. —— 延吉 : 延边大学出版社，2017.7

ISBN 978-7-5688-3258-8

Ⅰ. ①近… Ⅱ. ①阮… Ⅲ. ①抽象代数-教材 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2017)第 185632 号

近世代数

主编:阮佶
责任编辑:沈晓娟
封面设计:可可工作室
出版发行:延边大学出版社
社址:吉林省延吉市公园路 977 号　　**邮编**:133002
网址:http://www.ydcbs.com
E-mail:ydcbs@ydcbs.com
电话:0433-2732435　　**传真**:0433-2732434
发行部电话:0433-2732442　　**传真**:0433-2733266
印刷:三河市德辉印务有限公司
开本:787×1092 毫米　1/16
印张:16　　**字数**:366 千字
版次:2017 年 7 月第 1 版
印次:2017 年 7 月第 1 次
ISBN 978-7-5688-3258-8

定价:36.00 元

前 言

近世代数，又称为抽象代数，是大学数学系的重要基础课之一，主要介绍群、环、域（以及模）的基本概念和基本理论. 在这里人们将受到良好的代数训练，并为进一步学习数学得到一个扎实的代数基础.

我们知道，数、多项式和矩阵的出现是为了刻画一些物理量和几何量，诸如长度、面积、速度、物理定律、空间中点的位置、平面的运动和几何变换等. 它们的表现能力很强，使用数、多项式和矩阵足以刻画许多我们遇到的物理量和几何量. 然而当人们企图刻画对称性——无论是物理现象中，还是数学世界中（尤其是在几何图形中）的对称性，都无法用单个的数、多项式或矩阵去刻画. 为了刻画对称这一概念，人们发现了群. 现在我们知道，群是研究对称性的有力工具. 由于物理、几何、数学中对称这一概念的特殊重要性，因而使群成为近代数学极其深刻和重要的概念之一. 类似地，环、域、模也是刻画物理量和几何量的数学工具. 因而研究群、环、域、模的方式可分为两大类：一类是紧密结合其背景去研究，如晶体群，群与量子力学等；另一类是对群、环、域、模作理论上的研究. 当然两者有着相互的联系. 因此，自然地在介绍群、环、域、模的书中也有两种不同的倾向. 本书则是介绍群、环、域的基本概念和基本理论. 本书作者写的另一本书《正交表的构造》则是以群、环、域为基本工具，讲述正交表的构造原理和方法.

本书是作者在《近世代数基础》张禾瑞（修订本）以及《近世代数》杨子胥（第二版）的基础上，再参考相关教材、专著、文献编写而成. 相比前辈所编写的著作，本着“够用为度”的原则，去掉了一些不必要的内容，加入了配图，使得内容更为形象直接，对习题作了部分调整. 本书即可作为高等院校数学系和其他高职院校的教学用书，也可以作为自学参考书.

全书共六章，可大致分为三个部分：

第一部分，包括引言和第一章基本概念，它是全书的基础；

第二部分，包括第二、三两章，介绍含一个代数运算的群的理论. 其中第二章介绍群的最基本的知识；第三章则进一步介绍正规子群和群的同态与同构，以及和它们相关联的群论中最基本最重要的定理，如群的同态和同构定理，共轭、正规化子和中心化子，Sylow 定理和有限交换群基本定理等等；

第三部分，包括第四、五、六三章，介绍含有两个代数运算的环与域的理论. 其中第四章介绍环的基本知识；第五章介绍环论中一个特殊问题——唯一分解整环内的因子分解理论，并由此介绍了两种特殊的环类，即主理想整环和欧氏环；第六章介绍域，一种加强条件的环，并且主要介绍代数扩域，特别是有限次扩域和有限域.

由于这是一本教材，我们在编写过程中曾参阅了国内外大量的有关教材和文献，这里不再一一列出.本书的编写和出版得到了学院领导与有关同志的大力支持和热情帮助，在此谨向所有对本书提出意见和建议的专家、广大教师与读者表示衷心感谢，作者才疏学浅，水平有限，虽然我们作了一定的努力，但书中错误和疏漏之处恐在所难免，恳请读者批评指正.

编　者

2017 年 2 月

目 录

引 言

什么是近世代数？代数学是数学的一个古老分支，有着悠久的历史. 当中可大致分为初等代数学和抽象代数学两部分. 初等代数学是指 19 世纪上半叶以前发展的方程理论，主要研究某一方程组是否可解，如何求出方程所有的根(包括近似根)，以及方程的根有何性质等问题. 法国数学家伽罗瓦(Galois 1811－1832)在 1832 年运用[群]的思想彻底解决了用根式求解代数方程的可能性问题. 他是第一个提出[群]的思想的数学家，人们一般称他为近世代数创始人. 他使代数学由作为解方程的科学转变为研究代数运算结构的科学，即把代数学由初等代数时期推向抽象代数即近世代数时期.

近一百年来，随着数学的发展和应用的需要，代数学的研究对象和研究方法发生了巨大的变化，一系列新的代数领域被建立起来，大大地扩充了代数学的研究范围，形成了所谓的近世代数学. 大家知道，数是我们研究数学的最基本的对象，数的最基本的运算是加、减、乘、除. 但是，数并不是我们研究数学的唯一对象，而且我们所遇到的许多运算也不全是数的普通加、减、乘、除. 例如，向量、力以及多项式、函数、矩阵和线性变换等等，它们虽然都不是数，但却也可以类似于数那样来进行运算. 特别是，尽管这些研究对象千差万别，各有自己的特性，但是从运算的角度看却有着很多共同的性质. 于是，从一般的集合出发，研究各种运算的种种性质，就具有非常重要的意义. 因为它的结论和方法不仅可以渗透到数学的各个部门，而且在其他学科，例如在物理、化学、正交试验设计和编码等理论中都有重要应用.

一个集合，如果有一种或数种代数运算，我们就笼统地称它是一个代数系统. 简言之，近世代数就是研究各种抽象的公理化代数系统的数学学科. 由于代数可处理实数与复数以外的物集，例如向量、矩阵超数、变换等，这些物集的分别是依它们各有的演算定律而定，而数学家将个别的演算经由抽象手法把共有的内容升华出来，并因此而达到更高层次，这就诞生了抽象代数. 抽象代数包含有群论、环论、伽罗瓦理论、格论、线性代数等许多分支，并与数学其它分支相结合产生了代数几何、代数数论、代数拓扑、拓扑群等新的数学学科. 在近世代数中，尽管有时，特别是在举例时，也讲具体的集合和具体的运

算，但其最根本的任务是研究各种抽象的代数系统. 也就是说，不仅集合是抽象的，而且所说的运算也是抽象的. 因此，常把近世代数也叫做抽象代数. 由于代数系统中运算个数以及对运算所要求的附加条件的不同，从而产生了各种各样的不同的代数系统，这就形成了近世代数中各个不同的分支. 其中最基本、最重要的分支是群、环和域，它们所研究的内容极为丰富和广泛. 实践已经证明，这些理论不仅对数学本身产生重要影响并有重要应用，而且对其他学科也有重要影响和应用. 所以，古老的代数学在新的基础上又以全新的面貌和更加旺盛的活力飞速地向前发展着. 因此，抽象代数已经成了当代大部分数学的通用语言.

本书所用符号

Z	整数集(环)
Q	有理数集(域)
$\|G\|$	群 G 的阶
$\|a\|$	群中元素 a 的阶
U_n	n 次单位根群
$GL_n(F)$	域 F 上一般线性群
$SL_n(F)$	域 F 上特殊线性群
$\leqslant$	子群或子环
$<$	真子群或真子环
$\lhd$	正规子群或理想
$<M>$	由 M 生成的子群或理想
$<a>$	由元素 a 生成的子群或理想
$\sim$	同态
$\cong$	同构
$T(M)$	M 的全体变换作成的半群
$S(M)$	集合 M 上的对称群
S_n	n 次对称群
A_n	n 次交代群
K_4	*Klein* 四元群
$C(G)$	群 G 的中心
$C(S)$	群中子集 S 的中心化子
$N(S)$	群中子集 S 的正规化子

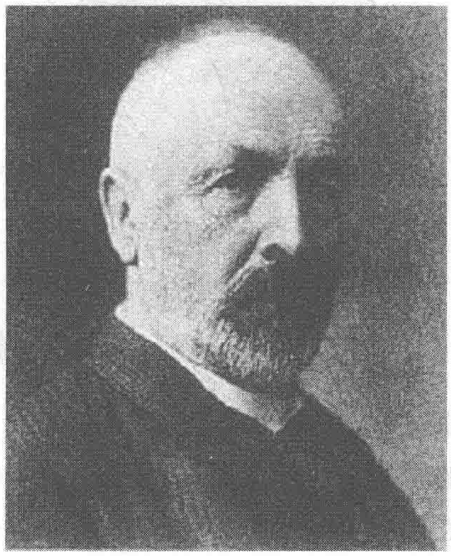
$Ker\varphi$	同态 φ 的核
$Im\varphi$	同态 φ 的象
$AutG$	群 G 的自同构群
$InnG$	群 G 的内自同构群
$T(n)$	n 的正因数个数
$(G:H)$	子群 H 的指数
Z_n	模 n 剩余类环
R_{nxn}	环 R 上的 n 阶全阵环
$EndG$	加群 G 的自同态环
$charR$	环 R 的特征
$U(R),R^*$	环 R 的单位群(乘群)
$P(M)$	M 的幂集环
$r(A)$	矩阵 A 的秩
$GF(p^n)$	伽罗瓦域
$(E:F)$	扩域 E 在子域 F 上的次数

第一章　基本概念

本章所介绍的内容，是在以后各章中都要用到的基本概念. 它们是：集合、映射与变换、代数运算、运算律、同态与同构、等价关系与集合的分类等.

§1　集合

集合论是数学的一个基本的分支学科，由德国数学家康托尔(*Georg Cantor*，1845—1918) 所创立，研究对象是一般集合. 集合论在数学中占有一个独特的地位，是整个现代数学的逻辑基础，它的基本概念已渗透到数学的所有领域，包含了集合、元素和成员关系等最基本的数学概念. 在大多数现代数学的公式化中，集合论提供了要如何描述数学物件的语言，它和逻辑与一阶逻辑共同构成了数学的公理化基础，以未定义的“集合”与“集合成员”等术语来形式化地建构数学物件.



康托尔

我们在讨论问题时，在一定范围内所说的对象，例如，数、向量、多项式、矩阵、点、直线，甚或书架上的书，桌子上的茶杯、钢笔、铅笔等，都笼统地称为元素或元.

若干个(有限个或无限个) 固定元素的全体，叫做一个集合，或简称为集.

集合常用大写拉丁字母 $A,B,C,\cdots\cdots,G,R,F,\cdots\cdots$ 等表示；集合中的元素常用小写拉丁字母 $a,b,c,\cdots\cdots,x,y,\cdots\cdots$ 来表示.

如果 x 是集合 A 中的一个元素，就说 x 属于集合 A 或集合 A 包含 x，记为 $x\in A$ 或 $A\in x$；如果 x 不是集合 A 中的元素，就说 x 不属于集合 A 或集合 A 不包含 x，记为 $x\notin A$ 或 $A\notin x$. 不包含任何元素的集合称为空集合，记为 $\varnothing$.

常用 Z 表示整数集，Z^* 表示非零整数集；用 Q 表示有理数集，Q^* 表示非零有理数集.

要指明一个集合是由哪些元素构成的，可以用列举法，例如

$$A=\{1,3,5\},B=\{\text{东},\text{西}\},C=\{1,\frac{1}{2},\frac{1}{3},\frac{1}{4},\cdots\};$$

有时也可以用描述法，例如

$$E=\{\text{全体自然数}\}F=\{x\mid x\text{是实数且}x^2<1\}.$$

定义 1 如果集合 A 的每个元素都属于集合 B，则称 A 是 B 的一个子集，记为 $A\subseteq B$. 如果 A 是 B 的一个子集，B 中又有元素不在 A 中，则称 A 是 B 的一个真子集，记为 $A\subset B$(如图 1.1).

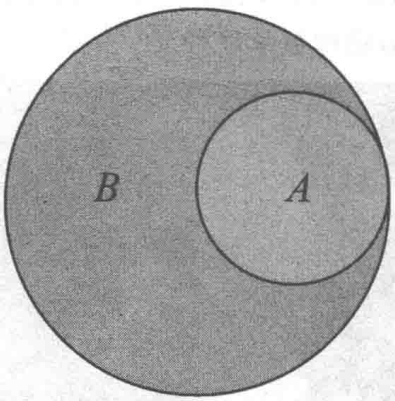


图 1.1

空集合 $\varnothing$ 被认为是任意集合的一个子集.

当集合 A 不是集合 B 的子集或真子集时，分别记为 $A\nsubseteq B$ 或 $A\not\subset B$.

显然，$A\subseteq B$ 意味着 $A\subset B$ 或 $A=B$(即 A 与 B 是由完全相同的元素作成的集合). 一个虽然简单但却非常重要的事实是：

$$A=B\text{当且仅当}A\subseteq B\text{且}B\subseteq A.$$

因此，要证两个集合 A 与 B 相等，常需证明 $A \subseteq B$ 且 $B \subseteq A$，即 A 与 B 互相包含. 这个事实虽然简单，但它却是贯穿到整个近世代数中的一个一般方法.

如果把集合 A 的每一个子集当成一个元素，则 A 的所有子集(包括空集) 也作成一个集合，称为 A 的幂集，记为 $P(A)$.

如果集合 A 包含无限多个元素，则记为 $|A| = \infty$；如果 A 包含 n 个元素，则记为 $|A| = n$. 于是易知，当 $|a| = n$ 时有

$$|P(A) = 2n.$$

定义 2　由集合 A 和集合 B 的所有公共元素构成的集合，记为 $A \cap B$，叫做 A 与 B 的交集，简称 A 与 B 的交(如图 1.2).

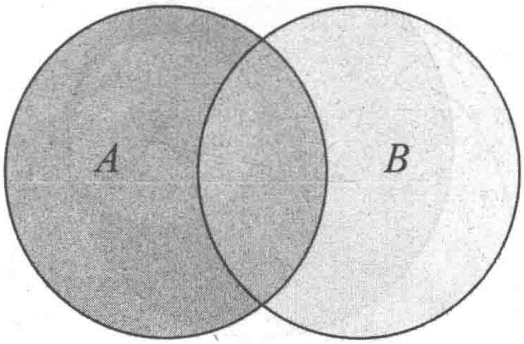


图 1.2

例如，集合 $A = \{0,1,2,3\}$ 与集合 $B = \{0,2,4\}$ 的交为 $A \cap B = \{0,2\}$.

但是，集合 A 与集合 $C = \{4,5,6\}$ 的交为空集合，即 $A \cap C = \varnothing$.

定义 3　由属于集合 A 或集合 B 的所有元素作成的集合，记为 $A \cup B$，叫做 A 与 B 的并集，简称 A 与 B 的并(如图 1.3).

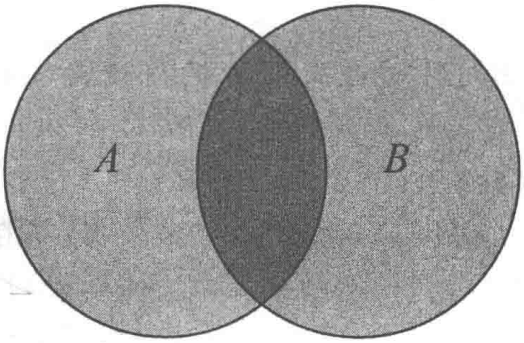


图 1.3

例如，集合 $A = \{0,1,2,3\}$ 与集合 $B = \{0,1,-1,-2,-3\}$ 的并为 $A \cup B = \{-3,-2,-1,0,1,2,3\}$.

对于两个以上甚至无穷多个集合，也可以类似地定义其交与并.

容易推出，集合的交与并有以下性质：

1)$A \cap B = A, A \cup A = A$；(幂等性)

2)$A \cap B = B \cap A = A \cup B = B \cup A$；(交换性)

3)$(A \cap B) \cap C = A \cap (B \cap C), (A \cup B) \cup C = A \cup (B \cup C)$；(结合性)

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

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

定义 4 设 A，B 是两个集合，称集合 $A - B = \{a \mid a \in A, a \mid B\}$ 为 A 与 B 的差集. 特别，当 $B \subseteq B$ 时，用 B' 表示 $A - B$，并称为 B 在 A 中的余集(如图 1.4).

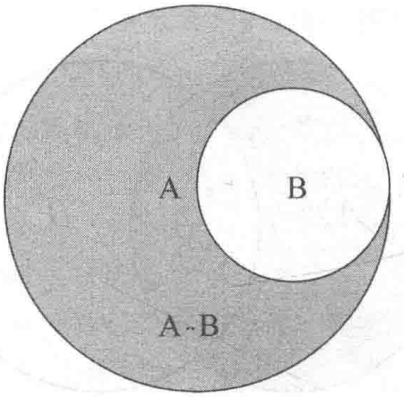


图 1.4

习题 1.1

1. 证明本节的等式 4).

2. 若 $A \cap B = A \cap B$，问：是否 $B = C$? 把 $\cap$ 改成 $\cup$ 时又如何?

3. 设 A 是有限集合，且 $|A| = n$. 证明：$|P(A)| = 2n$.

4. 设 A，B 是两个有限集合. 证明：$|A \cup B| + |A \cup B| = |A| + |B|$.

5. 证明德·摩根(A. *De Morgan*，1806 ~ 1871)律：若存在集合 $A, B \subseteq X$，则

$$(A \cup B)' = A' \cap B', (A \cup B)' = A' \cup B'$$

§2 映射与变换

在数学里，映射是个术语，指两个元素的集之间元素相互“对应”的关系通过映射与变换来研究代数系统，这是近世代数中最重要的方法之一.

定义 1 设 X 与 Y 是两个集合(如图 1.5). 如果有一个法则 φ，它对于 X 中每个元素 x，在 Y 中都有一个惟一确定的元素 y 与它对应，则称 φ 为集合 X 到集合 Y 的一个映射. 这种关系常表示成 $\varphi: x \to y$ 或 $y = \varphi(x)$，并且把 y 叫做 x 在映射 φ 之下的象，而把 x 叫做 y 在映射 φ 之下的原象或逆象.

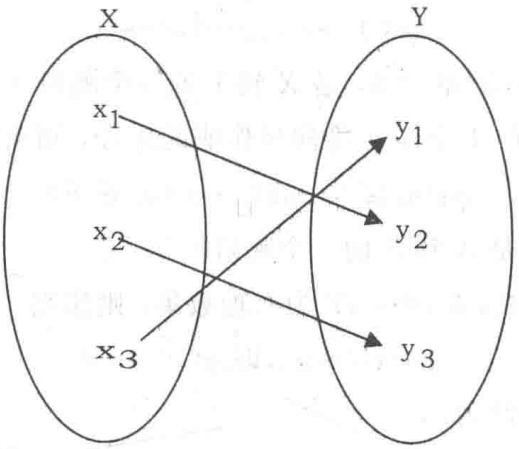


图 1.5

例 1 设 X 为有理数集，Y 为实数集，则法则

$$\varphi: x \to \frac{1}{x-1}, \text{ 即 } \varphi(x) = \frac{1}{x-1}$$

不是 X 到 Y 的映射. 因为，虽然 φ 对于任何不等于 1 的有理数 x 在 Y 中都有惟一确定的象，但是有理数 1 没有确定的象.

例 2 设 X 与 Y 都是有理数集，法则

$$\varphi: \frac{b}{a} \to a+b, \text{ 即 } \varphi\left(\frac{a}{b}\right) = a+b$$

不是 X 到 Y 的映射. 因为，例如对于 $\frac{1}{2} = \frac{2}{4}$，却有

$$\varphi\left(\frac{1}{2}\right) = 1+2 = 3, \varphi\left(\frac{2}{4}\right) = 2+4 = 6$$

即 X 中相等的元素在 Y 中的象不惟一. 但映射必须要求 X 中相等的元素在 Y 中

的象也相等.

例 3 设 $X=\{1,2,3\}, Y=\{2,4,8,16\}$，则法则

$\varphi: x \to 2x$，即 $\varphi(x)=2x$

也不是 X 到 Y 的映射. 因为，虽然 φ 对 X 中每个元素都有一个惟一确定的象，但 3 的象 6 却不属于 Y.

这就是说，集合 X 到集合 Y 的一个法则 φ，在满足以下三个条件时才是一个映射：

1) φ 对于 X 中每个元素都必须有确定的象；

2) X 中相等元素的象也必须相等，亦即 X 中每个元素的象是惟一的；

3) X 中每个元素的象都必须属于 Y.

例 4 设 $X=\{1,2,3\}, Y=\{0,4,9,10\}$，则法则

$$\varphi: 1 \to 0, 2 \to 0, 3 \to 9,$$

即 $\varphi(1)=\varphi(2)=0, \varphi(3)=9$，是 X 到 Y 的一个映射.

例 5 设 X 为数域 F 上全体 n 维向量作成的集合，则法则

$$\varphi:(a_1,a_2,\cdots a_n) \to a_1 (a_i \in F)$$

即 $\varphi((a_1,a_2,\cdots a_n))$ 是 X 到 F 的一个映射.

例 6 设 $X=\{1,2,3,\cdots\}, Y$ 为有理数集，则法则

$$\varphi: x_1 \to x^2, \text{即 } \varphi(x)=x^2$$

也是 X 到 Y 的一个映射.

映射是通常函数概念的一种推广，集合 X 相当于定义域. 不过应注意，集合 Y 包含值域，但不一定是值域. 就是说，在映射 φ 之下 Y 中每个元素不一定都有逆象. 例 6 就属于这种情形.

定义 2 设 φ 是集合 X 到集合 Y 的一个映射. 如果在 φ 之下 Y 中每个元素在 X 中都有逆象，则称 φ 为 X 到 Y 的一个满射，或 X 到 Y 上的一个映射.

设 φ 是集合 X 到集合 Y 的一个映射，又 $X_1 \subseteq X, Y_1 \subseteq Y$.

则用 $\varphi(X_1)$ 表示 X_1 中所有元素在 φ 之下全体象作成的集合，称为 X_1 在 φ 之下的象，它是 Y 的一个子集；类似地，用 $\varphi^{-1}(Y_1)$ 表示 Y_1 中所有元素在 φ 之下全体逆象作成的集合，称为 Y_1 在 φ 之下的逆象，它是 X 的一个子集.

显然，X 到 Y 的映射 φ 是满射当且仅当 $\varphi(X)=Y$.

定义 3 设 φ 是集合 X 到 Y 的一个映射. 如果在 φ 之下，X 中不相等的元素在 Y 中的象也不相等，则称 φ 为 X 到 Y 的一个单射，或 X 到 Y 里的一个映射.

我们不难检查在上面所举的例子中，哪些是满射，哪些是单射.