高等学校试用教材

近世代数

杨子胥　编著

高等教育出版社

高等学校试用教材

近世代数

杨子胥　编著

高等教育出版社

内容提要

本书是作者杨子胥教授在长期教学实践基础上，参考国内外大量相关教材、专著、文献并吸纳个人一些科研成果编写而成.

内容包括群，正规子群和有限群，环与域，因子分解，域的扩张等.

本书可作为综合大学理科数学类专业、师范院校数学类专业近世代数教材使用，也可供有关专业的专家参考使用.

图书在版编目（CIP）数据

近世代数/杨子胥编著 .—北京：高等教育出版社，2000

ISBN 7-04-007885-6

Ⅰ.近… Ⅱ.杨… Ⅲ.抽象代数 Ⅳ.0153

中国版本图书馆 CIP 数据核字（2000）第 17629 号

近世代数

杨子胥 编著

出版发行	高等教育出版社		
社　　址	北京市东城区沙滩后街 55 号	邮政编码	100009
电　　话	010-64054588	传　　真	010-64014048
网　　址	http://www.hep.edu.cn		
经　　销	新华书店北京发行所		
印　　刷	高等教育出版社印刷厂		
开　　本	850×1168　1/32	版　　次	2000 年 5 月第 1 版
印　　张	9.25	印　　次	2000 年 5 月第 1 次印刷
字　　数	230 000	定　　价	9.70 元

凡购买高等教育出版社图书，如有缺页、倒页、脱页等质量问题，请在所购图书销售部门联系调换。

序　言

近世代数(或抽象代数)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．它们的表现能力是很强的，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)的对称性时，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极其重要的概念之一．

类似的，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．这样，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．

杨子胥教授从事于高校代数教学与科研工作数十年，经验丰富，成果不断．他编写的这本《近世代数》一书，是他在长期教学

实践的基础上，经过反复修改提炼整理而成的．本书取材广泛，内容丰富且紧扣大纲，前后呼应，非常紧凑．其中一个概念的引入，一种思想的建立或一个定理的证明，都字斟句酌一丝不苟，既保持严格的科学性和系统性，又自然明快易于接受．

近世代数是比较抽象的一门学科，但本书所举正反例子较多，涉及面广，尽量把抽象的概念和问题具体化．而且还特别注意同高等代数的联系，每节所配备的习题的数量和难易程度适当，尤其是文句叙述和表达自然流畅，读来引人入胜，确实不失为一本好的近世代数教材．

杨子胥教授曾在北京师大张禾瑞先生指导下的代数研究班学习和进修，我们在本书中不难看到张禾瑞先生的良好的教学思想和风格的影响．

刘绍学

1998年7月1日于北京师范大学

前　言

本书是在长期教学实践的基础上，参考国内外大量相关教材、专著、文献并吸纳个人一些科研成果，编写而成.

全书共六章，可大致分为三个部分. 第一部分，即第一章基本概念，它是全书的基础，在以后各章都要用到，应予以充分重视. 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有限群，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——因子分解理论，并由此介绍了两种特殊的环类，即主理想环和欧氏环；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.

本书取材广泛，有的高校若教学时间不够，有些内容，例如多项式环、环的直和、非交换环、唯一分解环的多项式扩张、可离扩域或其它内容，可粗讲或不讲. 本书每节都配备有习题，其题量和难度比较适中，个别稍难题目都有提示，各校可根据不同情况择题而作.

本书承蒙我国数学家、中科院院士万哲先研究员和我国数学家、中科院院士王梓坤教授推荐出版，并承蒙我国数学家、北京师范大学博士生导师刘绍学教授撰写序言，作者由衷地对他们表示最诚挚的感谢！

作者才疏学浅，书中错误和疏漏之处恐在所难免，恳请读者批评指正.

作　者

1999年5月

责任编辑　马志鹏
封面设计　张　楠
版式设计　马静如
责任校对　王　巍
责任印制　韩　刚

目　录

引　言

代数学是数学的一个古老分支，有着悠久的历史．但是，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，数的基本运算是加、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，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，它们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、化学中都有重要应用．

一个抽象集合，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代数系统的一门学科．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，一般讲，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、最重要的是群、环和域，它们所研究的内容极为丰富和广泛．这样一来，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.

本课程的任务是，介绍近世代数中最基本的代数系统——群、环、域的最基本的概念和性质.

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

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，…，G，R，F，…等表示；集合中的元素常用小写拉丁字母 a，b，c，…，x，y，…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 $A\ni x$；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 $A\not\ni x$．

不包含任何元素的集合称为空集合，记为 $\varnothing$．

今后常用 $\mathbf{Z}$ 表示整数集，$\mathbf{Z}^*$ 表示非零整数集；用 $\mathbf{Q}$ 表示有理数集，$\mathbf{Q}^*$ 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

$$A=\{1,3,5\},\quad B=\{\text{东},\text{西}\},$$

$$C=\left\{1,\frac{1}{2},\frac{1}{3},\frac{1}{4},\cdots\right\};$$

有时也可以用描述法，例如

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

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，又 B 中有元素不在 A 中，则称 A 是 B 的一个真子集，记为 $A\subset B$.

空集合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：

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

因此，两个集合 A 与 B 相等时，常需证明 $A\subseteq B$ 且 $B\subseteq A$，即 A 与 B 互相包含. 这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 $|P(A)|=2^n$.

定义 2 由集合 A 和集合 B 的所有公共元素作成的集合，记为 $A\cap B$，叫做 A 与 B 的交集，简称 A 与 B 的交.

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.

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

$$A\cup B=\{-3,-2,0,1,2,3\}.$$

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

习题　1.1

1. 证明本节的等式(4).

2. 若 $A\cap B=A\cap C$，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：
$$|P(A)|=2^n.$$

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

5. 设 A，B 是两个集合. 称集合
$$A-B=\{a\mid a\in A,a\notin B\}$$
为 B 关于 A 的余集. 当 $Y\subseteq X$ 时，用 Y' 表示 Y 在 X 中的余集. 证明：若 A，$B\subseteq X$，则
$$(A\cup B)'=A'\cap B',\quad (A\cap B)'=A'\cup B'.$$

§2　映射与变换

通过映射来研究代数系统，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. 如果有一个法则 φ，它对于 X 中每个元素 x，在 Y 中都有一个唯一确定的元素 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

$$\varphi:\quad x\longrightarrow y \quad 或 \quad y=\varphi(x),$$

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.

例 1 设 X 为有理数集，Y 为实数集，则法则

$$\varphi:\quad x\longrightarrow\frac{1}{x-1},\quad 即\quad \varphi(x)=\frac{1}{x-1}$$

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 中都有唯一确定的象，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

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

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

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

即 X 中相等的元素在 Y 中的象不唯一. 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

$$\varphi:\quad x\longrightarrow 2x,\quad 即\ \varphi(x)=2x$$

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唯一确定的象，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 中每个元素的象是唯一的；

(3) X中每个元素的象必须属于 Y.

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

$$\varphi:\quad 1\longrightarrow 0,\quad 2\longrightarrow 0,\quad 3\longrightarrow 9,$$

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

例 5 设 $X=\{1,2,3,\cdots\}$，Y 为有理数集. 则法则

$$\varphi:\quad x\longrightarrow x^2,\quad \text{即}\quad \varphi(x)=x^2$$

也是 X 到 Y 的一个映射.

例 6 设 X 为数域 F 上全体 n 维向量作成的集合. 则法则

$$\varphi:\quad (a_1,a_2,\cdots,a_n)\longrightarrow a_1\qquad (a_i\in F)$$

即 $\varphi((a_1,a_2,\cdots,a_n))=a_1$ 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 之下不一定 Y 中每个元素都有逆象.

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 X 到 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，φ 是 X 到 Y 的满射当且仅当 $\varphi(X)=Y$.

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 里的一一映射.

我们不难检查上面所举的例子中，哪些是满射，哪些是单射.

定义 4 集合 X 到 Y 的一个映射，如果既是单射又是满射，则称它为 X 到 Y 的一个双射(或 X 到 Y 上的一一映射).