高等学校教材

近世代数导引

数学基础课程系列
简明教材

刘绍学　章　璞

高等教育出版社
HIGHER EDUCATION PRESS

高等学校教材

数学基础课程系列简明教材

近世代数导引

Jinshi Daishu Daoyin

刘绍学　章　璞

高等教育出版社·北京

HIGHER EDUCATION PRESS　BEIJING

内容简介

近世代数（又称为抽象代数）是现代数学的重要基础，在计算机、信息、与通信、物理、化学等领域有广泛的应用，对于提高抽象思维的能力有重要的意义。本书讲述群、环、域这三种基本代数结构中的最基本内容，力图使抽象的概念成为自然出现的研究对象，并强调近世代数中的思想、方法和应用背景。

本书可作为高等学校数学类专业的教材，也可供其他相关专业参考。

图书在版编目 (CIP) 数据

近世代数导引 / 刘绍学，章璞编. —北京：高等教育出版社，2011.1

ISBN 978-7-04-029227-5

I. ①近… II. ①刘… ②章… III. ①抽象代数－高等学校－教材 IV. ① O153

中国版本图书馆 CIP 数据核字（2010）第 190457 号

策划编辑	李 蕊	**责任编辑**	边晓娜	**封面设计**	张申申
版式设计	余 杨	**责任校对**	杨凤玲	**责任印制**	朱学忠

出版发行	高等教育出版社	**购书热线**	010-58581118
社 址	北京市西城区德外大街 4 号	**咨询电话**	400-810-0598
邮政编码	100120	**网 址**	http://www.hep.edu.cn
			http://www.hep.com.cn
经 销	蓝色畅想图书发行有限公司	**网上订购**	http://www.landraco.com
印 刷	北京铭传印刷有限公司		http://www.landraco.com.cn
		畅想教育	http://www.widedu.com
开 本	850 × 1168 1/32	**版 次**	2011 年 1 月第 1 版
印 张	6	**印 次**	2011 年 1 月第 1 次印刷
字 数	150 000	**定 价**	11.90 元

物料号 29227-00

总　　序

2005 年, 高等教育出版社为适应高校数学类专业的教学需求, 经过一段时间的酝酿, 决定在“十一五”期间推出一套“数学基础课程系列简明教材”。这套系列教材包含数学分析、高等代数、解析几何、复变函数、实变函数、概率统计、微分几何等。为做好此事, 在高等教育出版社的主持下成立了编委会, 并邀请了一批有多年教学实践经验的资深教授参加编写工作。这套系列教材中的第一批书目已经被列入普通高等教育“十一五”国家级规划教材。经过几年的努力, 这套教材开始正式与大家见面了。其中多数是新编的, 也有一些是经过教学实践证明优秀的, 深受读者欢迎的教材的修订版。

这套系列教材适用于我国综合性大学、理工科大学以及师范大学中的数学类专业, 作为数学专业基础课的教学用书; 当然, 它们也可以作为理工科中非数学类专业的教学参考书。面向全国各类高校的数学系, 具有较广泛的适用性, 这是我们编写这套系列教材的初衷之一。

在这套系列教材中, 尽管每一本教材的风格各异, 但是在编写的基本理念上大家有着相当多的共识。我们希望这套教材做到以下几点:

首先, 教材内容“少而精”。

众所周知, “少而精”是教学的一个基本原则。它要求在教学中要紧紧地抓住所涉及学科的基础知识与基本训练这个纲, 突出重点, 纲举目张。相反, 内容过多、过杂、过深, 势必使人不得要领, 事倍功半。但是, 有时人们会看不到讲得过多的害处, 会在

某些口号的驱使下使事情脱离了正确的轨道，比如求多求全、追求内容的先进性或现代化等等。我们知道，基础课教材的作用在于它为读者提供后续课以及日后参加工作不可或缺的基础知识、基本方法与基本思想。所讲的内容并非越多越好，越深越好。遗憾的是，目前基础课内容有一种不断扩充的趋势。这虽然出于良好的目的，而其效果却不如愿。实际上，就以我们这些“过来人”为例，认真回想一下自己以前所学到的、真正用得得心应手的内容并不多；而且真正用得到的内容也并不很多。与其求全求多，不如精选最基本的东西，帮助读者真正掌握这些内容的实质、方法和思想。读者有了这样的基础，在他们将来遇到没有学过但确有需要的内容时，也会有能力自学。课程内容“现代化”的要求，应当是针对数学系的整个的教学体系而言的，而不是要求基础课的内容更新换代。这对数学学科而言是无需争议的事实。基础课可以在观念上、记号上为专业课的现代化做些必要的准备，但不应该是把后续课的某些基本概念提到前面来讲述。

其次，教材尽可能做到“深入浅出”。

基础课教材是初学者入门的读本，而这些初学者在此之前没有任何学习高等数学的经验。在这种情况下，就要求教材注意循序渐进、由浅入深，尽可能做到通俗易懂，最好还能做到生动有趣，引起读者的兴趣。一个好的数学基础课教材应当既逻辑严谨、体系完整，又深入浅出、平实自然。我们应当学会通过典型的实例和足够详尽的解释，来帮助初学者学会解读数学的抽象形式，透过抽象的数学叙述，正确把握和理解其内容实质。教材的真正水准应当体现在是否能把那些艰深的内容讲得让人感到自然易懂。把本来容易的东西讲得复杂难懂，那是不可取的。为此，我们要注意避免过度形式化的不良倾向。数学工作者由于长期从事数学研究与教学，已经养成了严谨的习惯，追求叙述的一般性与抽象性，但与此同时，也往往形成了某种毛病，那就是忽视描述性语言，忽

视那些抽象形式背后的直观模型，甚至抹杀直观的意义，这是很不妥当的。过度的形式化，不仅造成了初学者的困难，更重要的是歪曲了数学本质，误导了学生。在基础课教材中，为了帮助初学者理解抽象数学形式的意义，除了典型例子之外，用必要的直观描述性语言去解释它的意义，同样是十分重要、不可或缺的。

最后，教材重视基本训练，重视对学生的能力培养。

我们赞同“双基”的提法，即基础课的任务是传授基础知识和掌握基本训练。学好一门数学课程，单单知道有关数学结论是不够的，还要求读者具有一定的分析问题与解决问题的能力。这样，勤于思考，独立思考，并做好相当数量的习题，是完全必要的。这是一切在数学上学而有成的人的共同体会。通过做题可以深入、具体地理解和掌握基本概念、结论和方法；获得计算和推理的能力；理解、掌握应用基本知识和方法解决问题的途径；同时也进一步锻炼刻苦思考和探索的毅力，培养创造性的思维能力和习惯。后面一点不仅对学好数学很重要，而且对读者以后工作能力的提高和事业的成功都是很重要的。在这套教材中，我们精心选配好适合读者的各种例题与习题，它们是教材很重要的组成部分，不可忽视。习题中不仅有基本练习，而且有一些题目，需要读者经过一定的努力，花费一定的时间去探索，才能最终解决。此外，题目富有多样性、趣味性和启发性。当然，我们也不赞成出一些技巧性过强而没有训练价值的偏题与难题。

常言道：“授人以鱼，不如授人以渔”。一本好的基础课教材要努力做到授人以渔，而不只是罗列知识。这就需要帮助读者理解课程内容和方法的实质，理解其中的数学思想。在教材中要尽可能地介绍清楚问题和概念的来龙去脉，包括一些典型的例子；尽可能解释清楚解决问题的思路和方法，其中包括定理证明和计算过程的思路，以提高学生的创新意识与探索精神。

以上是我们对这套教材的希望与要求，也是我们编书的理念。

把它们写在这里，主要是为了自勉，并不表明这些我们已经全部做好了、做到位了。我们希望使用这套教材的师生和其他读者多提宝贵意见，使教材得以不断完善。

"数学基础课程系列简明教材"编委会

2008年1月5日

前　言

我们很高兴为这套“数学基础课程系列简明教材”写一本《近世代数导引》。

作为面向大学生的近世代数 (又称为抽象代数), 这门课研究群、环、域三种最基本的代数结构。这门课的意义不仅在于它的理论和应用, 它是工具和语言, 它的结构之美和力量, 更在于它所能提供的抽象思维方面的训练。每一门数学课程都会提供这种训练, 但在这门课程中抽象的概念更集中, 这使得训练强度更大。具体的背景与抽象的表现之间的矛盾, 对于没有研究经验的本科生来说, 也更突出。而它所包含的思想和提供的训练不仅对整个数学领域是重要的, 而且对其他科技领域乃至社会生活也是基本的和有益的。

因此, 如何让这么多抽象概念成为自然出现的研究对象, 是这本教材编写过程中考虑较多的问题。

同时, 作为面向全体同学的课程, 我们严格而仔细地挑选必讲内容: 它们或者是必要的预备, 或者是最基本和重要的。带星号的小节和用楷体打印的部分可作为选讲内容: 这不是说它们不基本, 而是我们有时课时有限, 且同学们能够花在每门课程上的时间有限。

今天的同学更喜欢问所学的这个内容有什么应用? 尽管在这个导引性的教材中, 无法讨论抽象代数在物理和通信等领域中的广泛应用, 也没有涉及伽罗瓦理论, 但在群、环、域每一章中我们都力图展示它的应用成分。例如, 群论中我们强调变换群的几何背景、群在描述对称性方面的意义、 Burnside 引理在计数中的

应用；环论中我们包含了中国剩余定理在秘密共享中的应用；域论中我们用域扩张解决了尺规作图的古代难题。希望在有限的篇幅内让同学们真切地感受到抽象代数的应用空间和潜力。

这门课本身有较多的概念,为了降低学习的难度,本书习题难度适中,没有包含特别难的题目。对初学者感觉较难的内容我们适当作了提示。

北京师范大学数学科学学院和上海交通大学教务处对本书的编写给予了支持；北京师范大学李仲来教授非常关心此书的编写;华东师范大学周青教授讨论了关于代数学教学的内容;何青教授帮助打印前两章并提出宝贵意见；李吉有博士在教学中使用了本书的初稿并提出了宝贵的修改意见。作者表示衷心感谢!

我们与策划编辑李蕊,责任编辑边晓娜的合作是和谐的、愉快的。

作者欢迎读者提出宝贵意见。

刘绍学　于北京师范大学
章　璞　于上海交通大学
2010.5.1

目　　录

第一章 集合与运算

集合的语言是数学的基本语言,每一个数学概念都需要有一个用集合语言叙述的定义,这使得数学概念清楚、明确、不模棱两可. 对已接触过的集合的语言,我们在本章 §1 中作一个简单的回顾,并补充本课程需要的一些有关集合的内容.

数学中论证的形式有两种: 一种是逻辑推理,一种是进行运算. 本课程概括地说,就是研究运算的一门学科. 在本章 §2 中通过回顾已熟悉的具体运算,把一般的二元运算的概念用集合的语言定义清楚,并建立代数结构的思想.

§1 集 合

我们都熟悉下面这些概念: 集合、空集 (记作 $\varnothing$)、元素、子集、集合的包含 (集合 A 包含集合 B 记作 $A \supseteq B$, 或 $B \subseteq A$), 集合的交 (A 和 B 的交记作 $A \cap B$), 集合的并 (A 和 B 的并记作 $A \cup B$), 映射, 单射, 满射, 一一映射 (或称双射), 等等. 这些构成了有关集合的基本语言. 下面为了本课程的需要,强调或新引入有关集合的一些概念.

定义 1.1 集合 A 和集合 B 相等,记作 $A = B$,如果 A 和 B 由完全相同的元素组成.

依定义, $A = B$ 当且仅当 $A \subseteq B$ 且 $B \subseteq A$.

定义 1.2 集合 A 和集合 B 等势,如果存在 A 到 B 的一一映射.

如果我们不在意集合由一些"什么样"的元素组成,而只关心集合的整体"结构"的话,其实等势的集合 (这在有限集的情

况下, 就是有相同个数的元素组成的集合) 也是可以看作“相同”的. 考虑两个对象 (例如两个集合)“绝对”相同和研究两个对象“本质”上相同, 都是我们感兴趣且有意义的课题.

在研究数量关系和空间形式时出现的集合, 都不是一盘散沙的, 而是在其元素之间存在一些联系. 这些集合常具有这样或那样的结构. 例如, 平面上所有点组成的集合中任意两点间有一个距离的概念, 也就是说这个集合有一种几何结构; 全体整数组成的集合 $\mathbb{Z}$ 有加法运算 (以及乘法运算), 也就是说, $\mathbb{Z}$ 有一种代数结构; 又如, 全体实数 $\mathbb{R}$ 组成的集合中元素之间有一个大小关系, 也就是说, $\mathbb{R}$ 有一种序结构. 当然, 有的集合同时具有多种结构, 例如 $\mathbb{R}$, $\mathbb{Z}$ 都是.

下面讨论集合上的关系. 我们知道许多具体集合上的具体关系, 如整数集 $\mathbb{Z}$ 上的大小关系; 平面上所有三角形组成的集合上的相似关系; 实数域 $\mathbb{R}$ 上所有 n 阶矩阵组成的集合 $M_n(\mathbb{R})$ 上的相似关系 (矩阵 $\boldsymbol{A}$ 和 $\boldsymbol{B}$ 相似, 如果 $\exists\ \boldsymbol{T} \in M_n(\mathbb{R}), \boldsymbol{T}$ 非退化, 使得 $\boldsymbol{A} = \boldsymbol{T}\boldsymbol{B}\boldsymbol{T}^{-1}$), 合同关系 (矩阵 $\boldsymbol{A}$ 合同于矩阵 $\boldsymbol{B}$, 如果 $\exists \boldsymbol{T} \in M_n(\mathbb{R}), \boldsymbol{T}$ 非退化, 使得 $\boldsymbol{A} = \boldsymbol{T}\boldsymbol{B}\boldsymbol{T}^T$, 这里 $\boldsymbol{T}^T$ 表示 $\boldsymbol{T}$ 的转置), 等等. 分析一下这些具体的关系, 不难看出, 欲在一集合 M 上引进一个关系, 只需在由 M 的元素组成的所有有序对 (a, b), $a \in M$, $b \in M$, 中选定一些, 而规定被选定的有序对 (x, y) 中元素 x 和元素 y 有该关系. 如 $M_n(\mathbb{R})$ 上的相似关系就是由选定所有矩阵对 $(\boldsymbol{A}, \boldsymbol{B})$, 其中 $\boldsymbol{A} = \boldsymbol{T}\boldsymbol{B}\boldsymbol{T}^{-1}$, $\boldsymbol{T}$ 为某一 n 阶可逆矩阵, 所确定的关系. 上面对“关系”这个概念的描述是清楚的, 然而我们仍想给一个用集合语言的定义, 为此引入如下定义.

定义 1.3 设 M 和 N 是两个集合. 令 $M \times N = \{(m, n) \mid m \in M,\ n \in N\}$. 规定 $M \times N$ 中的两个元 (m, n) 和 (m', n') 相等, 当且仅当 $m = m'$, $n = n'$. 称 $M \times N$ 为集合 M 和 N 的卡氏积.

定义 1.4 设 M 是一个集合. 称 $M \times M$ 的一个子集 $\sim$ 为集

M 上的一个二元关系 (binary relation), 简称关系. 若 $(x,y) \in \sim$, 则规定 x 和 y 有关系 $\sim$, 记作 $x \sim y$; 否则, 规定 x, y 没有关系 $\sim$.

本课程中我们对一种特殊的关系特别感兴趣, 这就是下面的定义中所述的关系.

定义 1.5 设 $\sim$ 为集 M 的一个关系. 若 $\sim$ 满足下列条件:

(i) 自反律: 对任意 $x \in M$, 有 $x \sim x$;

(ii) 对称律: 对任意 $x, y \in M$, 若 $x \sim y$, 则 $y \sim x$;

(iii) 传递律: 对任意 $x, y, z \in M$, 若 $x \sim y$, $y \sim z$, 则 $x \sim z$,

就称 $\sim$ 为 M 上的一个等价关系 (equivalence relation).

不难看出, 上面提到的"矩阵的相似"是 n 阶矩阵集上的一个等价关系. 设 n 是正整数. 称整数 a 模 n 同余于整数 b, 如果 $a-b$ 能被 n 整除. 不难验证, 在整数集 $\mathbb{Z}$ 中"模 n 同余"是 $\mathbb{Z}$ 上的一个等价关系.

设 $\sim$ 为集 M 上的一个等价关系. 设 $x \in M$, 而令子集

$$[x] = \{y \in M \mid y \sim x\},$$

称之为 x 所在的等价类. 则由自反律知 $x \in [x]$, 由对称律、传递律及自反律知子集 $[x]$ 和子集 $[y]$ 或相等 (当 $x \sim y$ 时) 或 $[x] \cap [y]$ 是空集 (当 x, y 无关系 $\sim$ 时). 如果我们从 M 的所有子集 $[x]$, $x \in M$ 中, 相同者只取其一, 则得到 M 的一些子集 M_i, $i \in I$, 它们具有性质 $M = \bigcup\limits_{i \in I} M_i$, 且这些子集 $M_i (i \in I)$ 中任意两个不相交. 这是一个有用的概念, 特写成下面的定义.

定义 1.6 设 M 是集合, M_i, $i \in I$, 是 M 的一些子集. 如果它们具有如下性质:

(i) $M = \bigcup\limits_{i \in I} M_i$;

(ii) $M_i (i \in I)$ 两两无交, 即对任意 $i, j \in I, i \neq j, M_i \cap M_j = \varnothing$;

则称这些子集 $M_i (i \in I)$ 为集 M 的一个划分 (partition).

用 $|M|$ 表示集 M 所含元素的个数. 如果有限集 M 有一个划分 M_i, $i \in I$, 则 $|M| = \sum\limits_{i\in I} |M_i|$. 这是以后我们用来计数的基本方法.

定义 1.7 设 $M_i(i \in I)$ 为集 M 的一个划分. 把 M_i 看成一个元素, 把由元素 M_i 组成的集合 $\{M_i \mid i \in I\}$ 称作 M 的一个商集 (quotient set).

值得注意的是: 把 M_i 看成 M 的子集, 则 $M_i(i \in I)$ 是 M 的一个划分; 而把 M_i 看成元素, 则 $\{M_i|i \in I\}$ 是 M 的一个商集.

这样, 由集 M 上的一个等价关系 $\sim$ 出发, 把有关系的元素放在一起, 便得到 M 的一个划分 M_i, $i \in I$; 由集 M 的一个划分 $M_i(i \in I)$ 出发, 规定属于此划分中同一子集 M_i 的元素有关系 $\sim$, 便得到一个等价关系; 由集 M 的一个划分 $M_i(i \in I)$ 出发, 而把 M_i 看成一个元素, 则得 M 的一个商集 $\{M_i \mid i \in I\}$; 由 M 的一个商集 $\{M_i \mid i \in I\}$ 出发, 把元素 M_i 还原为 M 的子集 M_i, 则得 M 的一个划分. 因而集 M 的等价关系、划分、商集是同一现象的三种表述方式.

设 n 是正整数. 对于整数集 $\mathbb{Z}$ 上的等价关系"模 n 同余", 详细写出上述三种表述方式.

等价关系: 整数 l 与整数 m 有此关系当且仅当 $l-m$ 能被 n 整除, 记作 $l \equiv m \pmod n$. 特用 $\bar{i}$ 表示整数 i 所在的等价类, 称为模 n 的剩余类 (residue class). 则

$$\bar{i} = \{\cdots, -2n+i, -n+i, i, n+i, 2n+i, \cdots\} = \{kn+i \mid k \in \mathbb{Z}\};$$

$$\bar{i} = \bar{j} \text{ 当且仅当 } i \equiv j \pmod n.$$

划分: $\mathbb{Z}$ 可表示为两两无交的子集之并: $\mathbb{Z} = \bar{0} \bigcup \bar{1} \bigcup \cdots \bigcup \overline{n-1}$.

商集: n 个元素组成的集合 $\{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$, 记为 $\mathbb{Z}_n$.

最后重温一下映射的乘法. 设 $f: M \longrightarrow N$ 是集 M 到集 N 的一个映射, $g: N \longrightarrow P$ 是集 N 到集 P 的一个映射, $m \in M$ 在

f 下的像记作 $f(m)$. 如下:

$$M \xrightarrow{f} N, \qquad N \xrightarrow{g} P$$
$$m \mapsto f(m), \qquad n \mapsto g(n)$$
$$m \longmapsto g(f(m))$$

即 M 中元素 m 先经映射 f 映到 $f(m)$, 再经映射 g 映到 $g(f(m))$, 我们把如下映射

$$\begin{aligned} M &\longrightarrow P \\ m &\mapsto g(f(m)) \end{aligned}$$

定义为 f 和 g 的乘积 gf, 即规定 $(gf)(m) = g(f(m)),\ \forall\ m \in M$. 如果再有映射 $h : P \longrightarrow Q$, 即有

$$M \xrightarrow{f} N, \quad N \xrightarrow{g} P, \quad P \xrightarrow{h} Q,$$

则 $(hg)f$ 和 $h(gf)$ 都是 M 到 Q 的映射. 对任意 $m \in M$, 根据映射乘法的定义有

$$\begin{aligned} ((hg)f)(m) &= (hg)(f(m)) = h(g(f(m))), \\ (h(gf))(m) &= h((gf)(m)) = h(g(f(m))), \end{aligned}$$

故 $(hg)f = h(gf)$, 即映射的乘法满足结合律.

我们特别感兴趣的是集 M 到自身的映射, 将之称为集 M 的变换 (transformation). 易见, 集 M 的两个变换的乘积仍是 M 的变换. 这样 M 的所有变换作成的集合 $T(M)$ 就有一个自然的乘法运算, 并且它满足结合律. 下章还将涉及它.

§2 运 算

在本节中我们先回顾一下大家熟悉的数的运算、多项式的运算和矩阵的运算. 这里只讨论加法和乘法, 这是因为, 减法和除法

分别可看成是加法和乘法的副产品. 然后把一般的二元运算用集合的语言定义清楚, 并建立代数结构的思想.

2.1 具体的运算

例 2.1 数的运算 根据整数的加法 (乘法) 运算法则, $\mathbb{Z}$ 中任意两个数的和 (积) 仍在 $\mathbb{Z}$ 中, 所以在整数集 $\mathbb{Z}$ 上有加法 "$+$" 和乘法 "$\cdot$" 运算. 根据这些运算法则还可证明这些运算具有下列性质: 对于任意 a, b, $c \in \mathbb{Z}$ 有

AA. $(a+b)+c=a+(b+c)$ (加法结合律);

AC. $a+b=b+a$ (加法交换律);

MA. $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ (乘法结合律);

MC. $a\cdot b=b\cdot a$ (乘法交换律);

D. $a\cdot(b+c)=a\cdot b+a\cdot c$ (乘法对加法的分配律).

除此之外, 数 0 在加法中占有一个特殊的地位:

对任意 $a\in\mathbb{Z}$, 都有 $a+0=a$; 并且都有 $-a\in\mathbb{Z}$, 使得 $a+(-a)=0$.

数 1 在乘法中占有一个特殊的地位:

对任意 $a\in\mathbb{Z}$, 都有 $a\cdot 1=a$.

当把 $\mathbb{Z}$ 连同 $\mathbb{Z}$ 上的加法、乘法一起考察时, 把它特记成 $(\mathbb{Z},+,\cdot)$, 并称之为**整数环**. 有时我们会讨论只带一个运算, 例如只带加法的 $\mathbb{Z}$, 此时用 $(\mathbb{Z},+)$ 来表示.

类似地, 设 $\mathbb{Q}=\{$所有有理数$\}$. 由于有理数的和与积仍是有理数, 所以 $\mathbb{Q}$ 有加法 "$+$" 和乘法 "$\cdot$". 同样根据有理数的运算法则, 我们知道 $\mathbb{Q}$ 的 "$+$" 和 "$\cdot$" 具有上述整数环中所有性质. 特别地, 还有如下性质:

对任意有理数 $a\neq 0$, 都有 $a^{-1}\in\mathbb{Q}$, 使得 $a\cdot a^{-1}=1$.

我们称 $(\mathbb{Q},+,\cdot)$ 为**有理数域**.

类似地, 设 $\mathbb{R}=\{$所有实数$\}$, $\mathbb{C}=\{$所有复数$\}$. 我们称 $(\mathbb{R},+,\cdot)$ 为**实数域**, 其中 "$+$" 是实数的加法, "$\cdot$" 是实数的乘