普通高等教育“十一五”国家级规划教材

国家理科基地教材

数学核心教程系列／柴俊 主编

数学专业50学时课程

近世代数

（第二版）

韩士安 林 磊 编著

科学出版社
www.sciencep.com

普通高等教育“十一五”国家级规划教材

国家理科基地教材
数学核心教程系列/柴俊主编

近世代数

(第二版)

韩士安　林磊　编著

科学出版社

北京

内 容 简 介

本书是普通高等教育“十一五”国家级规划教材. 全书系统介绍了群、环、域的基本概念与初步性质, 共分为三个部分. 第一部分讲述群的基本概念与性质, 除了通常的群、子群、正规子群及群同态的基本定理外, 还介绍了群的应用. 第二部分包括环、子环、理想与商环的基本概念与性质, 特别讨论了整环的性质. 第三部分讨论了域的扩张的理论.

本书可作为高等院校数学专业本科生的教材和参考书.

图书在版编目(CIP)数据

近世代数/韩士安, 林磊编著. —2 版. —北京: 科学出版社, 2009
(国家理科基地教材·数学核心教程系列/柴俊主编: 普通高等教育“十一五”国家级规划教材)

ISBN 978-7-03-025061-2

Ⅰ. 近… Ⅱ. ①韩… ②林… 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 (2009) 第 125129 号

责任编辑: 姚莉丽 房 阳 / 责任校对: 张怡君
责任印制: 张克忠 / 封面设计: 陈 敬

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

丽源印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2004 年 2 月第 一 版 开本: B5 (720×1000)
2009 年 7 月第 二 版 印张: 16
2009 年 7 月第十次印刷 字数: 308 000
印数: 26 501 —31 500

定价: 24.00 元
(如有印装质量问题, 我社负责调换)

序　言

自 20 世纪 90 年代后期, 我国的高等教育改革步伐日益加快. 实行 5 天工作制后, 教学总时数减少, 而新的专业课程却不断出现. 在这样的情况下, 对传统的专业课程应该如何处置, 这样一个不能回避的问题就摆在了我们的面前. 而这时, 教育部师范司启动了面向 21 世纪教学改革计划. 在我们进行 "数学专业培养方案" 项目的研究中, 解决这个问题有两种方案可以选择: 一是简单化的做法, 或者削减必修课的数量, 将一些传统的教学课程从必修课中除去, 变为选修课, 或者少讲内容减少课时; 二是对每门课程的教学内容进行优化、整合, 建立一些理论平台, 减少一些烦琐的论证和计算, 以达到削减课时, 同时又保证基本教学内容的目的. 我们选择了第二种方案.

当我们真正进入实质性操作时, 才感到这样做的困难并不少. 第一个困难是教师对数学的认识需要改变. 理论 "平台" 该不该建? 在人们的印象中, 似乎数学课程中不应该有不加证明而承认的定理, 这样做有悖于数学的 "严密性". 其实这种 "平台" 早已有之, 中学数学中的实数就是例子. 第二个困难是哪些内容属于整合对象, 优化从何处下手. 我们希望每门课的内容要精炼, 尽可能反应这门课程的基本思想和方法, 重视数学能力和数学意识的培养, 让学生体会数学知识产生和发展的过程以及应用价值, 而不去过分地追求逻辑体系的严密性.

教材从 1998 年开始编写, 历时 5 年, 经反复试用, 几易其稿. 在这期间, 我们又经历了一些大事. 1999 年, 高校开始大幅度扩大招生规模, 学生情况的变化, 提示我们教材的编写要适应教育形势的变化, 迎接 "大众教育" 的到来. 2001 年, 针对教育发展的新形势, 教育部高等教育司启动了 21 世纪初高等理工科教育教学改革项目, 在项目 "数学专业分层次教学改革实践" 的研究过程中, 对 "大众教育" 的学生状况有了更具体、更直接的了解. 在经历大规模扩招后, 在校学生的差距不断增大, 应该根据学生的具体情况, 实行分层次、多形式的培养模式, 每个培养模式都应该有各自不同的教学和学习要求. 此外, 教材的内容还应该为教师提供多一些选择, 给学生自我学习的空间, 要反映学科的新进展和新应用, 使所有学生都能学到课程的基本内容和思想方法, 使部分优秀学生有进一步提高的空间. 这个指导思想贯穿了本套教材的最后修改稿.

在建立 "理论" 平台与打好数学基础之间如何进行平衡, 也是本套教材编写中重点考虑的问题. 其实任何基础都是随时代的进步而变化的, 面对科学技术的进步, 对基础的看法也要 "与时俱进", 新的知识充实进来, 一部分老的知识就要被简化、

整合, 甚至抛弃. 并且基础应该以创新为目的, 并不是什么都是越深越好、越厚越好. 在现实条件下, 建立一些 “课程平台” 或 “理论平台” 是解决课时偏少的有效手段, 也可以使数学教学的内容加快走向现代化. 不然的话, 100 年以后, 我们的数学基础大概一辈子也学不完了.

本套教材的主要内容适合每周 3 学时, 总共 50 学时左右的教学要求. 同时, 教材留有适量的选学内容, 可以作为优秀学生的课外或课堂学习材料, 教师可以根据学生情况决定是否讲授.

教材的编写和出版得益于国家理科基地的建设和教育部师范司、高教司教改项目的支持. 我们还要对在本套教材出版过程中提供过帮助的单位和个人表示衷心的感谢. 感谢华东师范大学数学系的广大师生自始至终对教材编写工作的支持, 感谢华东师范大学教务处领导对教材建设的关心. 最后, 感谢张奠宙教授作为教育部两个项目的负责人对本套教材提出的极为珍贵的意见和建议.

尽管我们的教材经过了多次使用, 但其中仍难免有疏漏之处, 恳请广大读者批评指正. 另外, 如对书中内容有不同看法, 欢迎探讨. 真诚希望大家共同努力将我国的高等教育事业推向一个新阶段.

柴　俊

2003 年 7 月于华东师范大学

第二版前言

本教材第一版自 2004 年出版以来, 笔者与我系代数组同仁在使用第一版进行教学的过程中, 发现了一些有待改进之处. 这次修订, 根据这几年的教学经验和反馈的意见, 我们主要做了以下几方面的工作:

(1) 对数学名词的中文译名, 按全国科学技术名词审定委员会审定公布的定名做了核定. 个别没有通用译名的词汇, 则是笔者试译的, 如有不当之处, 欢迎读者斧正.

(2) 为便于教学, 我们对个别章节的次序进行了调整. 将原 3.4 节、3.5 节, 以及原 5.3 节、5.4 节分别进行了对调, 同时, 对相关章节的内容也做了适当调整或修改, 还改写了个别定理的表述与证明, 增加了一些例子.

(3) 第 5 章增加了一节 —— 几何作图. 我们认为, 对于一个有志于中学数学教育的读者, 了解一点有关用直尺和圆规作图的背景是有益的.

(4) 删去了个别特别困难的习题, 补充了一些较为容易的基本习题. 习题编排的次序, 按涉及的概念或理论与各节的内容基本同步. 这样, 读者在学完了一节的部分内容后, 就可以试着去做相应的习题, 不必等到学完整节以后再去做习题. 这样, 更有利于理解和掌握知识.

另外, 应读者要求, 与本教材配套的《近世代数习题解答》一书, 不久也将由科学出版社出版发行.

编 者

2009 年 3 月

第一版前言

"近世代数" 是师范院校和综合性大学数学系本科的一门重要专业基础课. "近世代数" 的基本概念、理论和方法, 是每一位数学工作者所必需具备的基本数学素养之一. 随着我国高等教育改革的深入以及多年来进行教学改革的实践, 我们深切感到, 编写一本合适的《近世代数》教材, 已成当务之急. 我们希望, 学生通过一学期每周 3 至 4 课时的学习, 能理解和掌握 "近世代数" 的基本内容、方法和理论, 初步具备用 "近世代数" 的基本思想和理论处理或解决具体问题的能力, 为他们进一步学习代数的后继课程或从事中学数学教学打下基础. 本教材便是这一要求下的产物. 本教材曾在我系多次试用, 并经反复修改、完善后定稿.

本教材的主要内容包括群、环、域的基本概念与初步性质. 为了适合不同层次学生的教学要求, 给读者和教师有更多的选择余地, 我们将所有的内容分为 5 章. 前 4 章包含了群、环的基本内容, 第 5 章讨论域的扩张. 我们认为: 除了带 $*$ 的部分, 学完前 4 章这些内容, 已达基本要求. 但对于要求较高的学生, 特别是希望将来报考代数研究生的学生, 则要求他们必须学完所有的 5 章和带 $*$ 的部分. 这估计需要每周 4 学时的课时.

在讲解抽象概念和理论的过程中, 我们注意避免 "定义 — 性质 — 定理" 这样一种过于刻板的模式. 我们总是尽可能地用一个简单的易于理解的例子来引出一个新的概念和结论, 并且也用尽可能多的例子来说明新的概念和结论的具体意义及应用. 结合教学内容, 我们还介绍了有关的历史回顾和有关数学家的生平, 以拓展学生的知识面.

选择好习题也是我们关注的重点. 本教材每小节后都附有适量的习题, 大部分习题是比较基本的, 解决这部分习题所需要的方法与技巧可在相应章节的例题中找到, 学生在理解了教材的有关内容后就可以完成. 小部分习题是对教材内容的补充. 少量习题是为部分程度较好的学生准备的 (大多带 $*$), 解决这部分习题需要较高的技巧和对有关知识的深刻理解, 初学时可以不做.

本教材的编写得到了数学系的支持和帮助. 特别是我系代数教研室同仁为本书的编写倾注了极大的热情. 陈志杰教授对本书的编写提出了许多指导性的意见, 吴允升副教授做了不少前期准备工作, 时俭益教授、胡乃红教授、芮和兵教授和瞿森荣老师在试用本教材的初稿进行教学的过程中, 提出了许多建设性的修改意见. 所有这一切, 都使本书增色不少. 借此机会对他们表示衷心的感谢.

最后, 限于编者水平, 书中定有许多不妥之处, 恳请使用本书的教师和读者指正. 编者的 e-mail 地址为: sahan@math.ecnu.edu.cn(韩士安), llin@math.ecnu.edu.cn(林磊).

编　者

2003 年 7 月于华东师范大学

目　录

第 1 章　群

近世代数的主要研究对象是具有代数运算的集合, 这样的集合称为代数系. 群是具有一个代数运算的代数系. 群的理论是近代代数学的一个重要分支, 它在物理学、化学、信息学等许多领域都有广泛的应用.

本章和第 2 章介绍群的初步理论. 本章的 1.1 节讨论等价关系和集合的分类以及它们之间的联系. 1.1 节的内容虽然不属于群论的范畴, 但等价关系和集合的分类却是近世代数中经常出现的两个基本概念, 所以先作一个介绍. 1.2 节 ~1.4 节介绍群、子群、群同构的概念及有关性质. 这是了解群的第一步. 1.5 节和 1.6 节较为详细地讨论了两类最常见的群 —— 循环群与置换群. 学习这部分内容可以熟悉群的运算和性质, 加深对群的理解. 1.7 节是选学内容, 介绍置换群的某些应用, 初学时可以略去, 并不影响后面的学习.

1.1　等价关系与集合的分类

在数学研究中, 常常要对一个集合的元素加以比较, 希望通过元素之间的联系去了解整个集合. 另一方面, 也常常要把一个集合分成若干个子集, 以便对各个子集进行分类研究, 或对其中某些特殊子集加以讨论, 从而了解整个集合的性质. 例如, 在实数集中, 任意两个实数 a 与 b 之间就有 a 大于 b 或 a 不大于 b 两种情况. 同时, 根据一个实数是否大于零, 可以把整个实数集合分解为正实数集 $\mathbf{R}^+$, 负实数集 $\mathbf{R}^-$ 和单独一个数 0 组成的集合 $\{0\}$ 这三个子集合. 又如, 在数域 F 上的一元多项式环 $F[x]$ 中, 对任意两个多项式 $f(x)$ 与 $g(x)$, 有 $f(x)$ 可被 $g(x)$ 整除或 $f(x)$ 不可被 $g(x)$ 整除两种情况. 根据一个多项式被一个非零多项式 $g(x)$ 所除的余式, 可以把整个多项式环 $F[x]$ 分解为许多个子集, 不同的子集没有公共元素, 同一个子集中的多项式在被 $g(x)$ 除时余式都相同.

将上面两个例子中所涉及的概念加以推广, 就得到集合上一般的*关系*的概念和*集合的分类*的概念. 本节的主要目的就是介绍这两个概念以及它们之间的联系.

定义 1.1.1　*设 S 是一个非空集合, $\mathcal{R}$ 是关于 S 的元素的一个条件. 如果对 S 中任意一个有序元素对 (a,b), 我们总能确定 a 与 b 是否满足条件 $\mathcal{R}$, 就称 $\mathcal{R}$ 是 S 的一个关系*(relation). *如果 a 与 b 满足条件 $\mathcal{R}$, 则称 a 与 b 有关系 $\mathcal{R}$, 记作 $a\mathcal{R}b$; 否则称 a 与 b 无关系 $\mathcal{R}$. 关系 $\mathcal{R}$ 也称为二元关系.*

上面提到的实数集中元素之间的大于和 $F[x]$ 中多项式的整除都是关系.

例 1　设 S 是一个非空集合, S 的所有子集组成的集合记为 $\mathcal{P}(S)$. 因为对 S 的任意两个子集 A, B, $A \subseteq B$ 或 $A \nsubseteq B$ 有且仅有一个成立, 所以集合的包含关系 "$\subseteq$" 是 $\mathcal{P}(S)$ 的一个关系. 进一步讨论可以发现, 这个关系还具有下面两条性质:

(1) 反身性, 即对 S 的任一子集 A, 有 $A \subseteq A$;

(2) 传递性, 即对 S 的任意子集 A, B, C, 如果 $A \subseteq B$, $B \subseteq C$, 则有 $A \subseteq C$.

例 2　在整数集 $\mathbf{Z}$ 中, 规定 $a \mathcal{R} b \Longleftrightarrow a \mid b$. 因为 $a \mid b$ 与 $a \nmid b$ 有且仅有一个成立, 所以 "$\mid$" 是 $\mathbf{Z}$ 的一个关系. 这个关系也具有反身性和传递性.

例 3　在整数集 $\mathbf{Z}$ 中, 规定 $a \mathcal{R} b \Longleftrightarrow (a, b)=1$(即 a 与 b 互素). 因为 $(a, b)=1$ 与 $(a, b) \neq 1$ 有且仅有一个成立, 所以是 $\mathbf{Z}$ 的一个关系. 这个关系既不满足反身性也不满足传递性, 但却满足所谓的对称性, 即对任意两个整数 a, b, 由 $(a, b) = 1$ 可推出 $(b, a) = 1$.

同时具有反身性、对称性和传递性三条性质的关系是我们特别感兴趣的.

定义 1.1.2　设 $\mathcal{R}$ 是非空集合 S 的一个关系, 如果 $\mathcal{R}$ 满足

(E1) 反身性, 即对任意的 $a \in S$, 有 $a \mathcal{R} a$;

(E2) 对称性, 即若 $a \mathcal{R} b$, 则 $b \mathcal{R} a$;

(E3) 传递性, 即若 $a \mathcal{R} b$, 且 $b \mathcal{R} c$, 则 $a \mathcal{R} c$,

则称 $\mathcal{R}$ 是 S 的一个**等价关系**(equivalence relation), 并且如果 $a \mathcal{R} b$, 则称 a 等价于 b, 记作 $a \sim b$.

定义 1.1.3　如果 $\sim$ 是集合 S 的一个等价关系, 对 $a \in S$, 令

$$[a] = \{x \in S \mid x \sim a\}.$$

称子集 $[a]$ 为 S 的一个**等价类**(equivalence class). S 的全体等价类的集合称为集合 S 在等价关系下的**商集**(quotient set), 记 $S/\sim$.

例 4　易知, 三角形的全等、相似, 数域 K 上 n 阶方阵的等价、相似、相合等都是等价关系, 而例 1、例 2、例 3 及本节开头所述的关系都不是等价关系.

例 5　设 m 是正整数, 在整数集 $\mathbf{Z}$ 中, 规定

$$a \mathcal{R} b \Longleftrightarrow m \mid a-b, \quad \forall a, b \in \mathbf{Z},$$

则

(1) 对任意整数 a, 有 $m \mid a-a$;

(2) 若 $m \mid a-b$, 则 $m \mid b-a$;

(3) 若 $m \mid a-b$, $m \mid b-c$, 则 $m \mid a-c$,

所以 $\mathcal{R}$ 是 $\mathbf{Z}$ 的一个等价关系. 显然 a 与 b 等价当且仅当 a 与 b 被 m 除有相同的余数, 因此称这个关系为**同余关系**(congruence relation), 并记作 $a \equiv b \pmod{m}$(读作 "a 同余于 b, 模 m"). 整数的同余关系及其性质是初等数论的基础 [1].

设 $a \in \mathbf{Z}$, 则

$$\begin{aligned}[a] &= \{x \in \mathbf{Z} \mid x \equiv a \pmod m\} \\ &= \{x \in \mathbf{Z} \mid m | x-a\} \\ &= \{a+mz \mid z \in \mathbf{Z}\},\end{aligned}$$

$[a]$ 称为整数集 $\mathbf{Z}$ 的一个 (与 a 同余的) 模 m 剩余类, 在数论中, $[a]$ 常记作 $\overline{a}$, 而相应的商集称为 $\mathbf{Z}$ 的模 m 剩余类集, 记作 $\mathbf{Z}_m$.

由

$$\overline{a} = \overline{b} \Longleftrightarrow m \mid a-b,$$

易得

$$\begin{aligned}&\overline{0} = \{\cdots, -2m, -m, 0, m, 2m, \cdots\}, \\ &\overline{1} = \{\cdots, -2m+1, -m+1, 1, m+1, 2m+1, \cdots\}, \\ &\cdots\cdots \\ &\overline{m-1} = \{\cdots, -2m-1, -m-1, -1, m-1, 2m-1, \cdots\}\end{aligned}$$

是模 m 的全体不同的剩余类, 所以

$$\mathbf{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}. \qquad \square$$

集合的等价关系常和下面的概念联系在一起.

定义 1.1.4 如果非空集合 S 是它的某些两两不相交的非空子集的并, 则称这些子集为集合 S 的一种**分类**(partition), 其中每个子集称为 S 一个**类**(class). 如果 S 的子集族 $\{S_i \mid i \in I\}$ 构成 S 的一种分类, 则记作 $\mathcal{P} = \{S_i \mid i \in I\}$.

由此定义可知, 集合 S 的子集族 $\{S_i \mid i \in I\}$ 构成 S 的一种分类当且仅当

(P1) $S = \bigcup\limits_{i \in I} S_i$;

(P2) $S_i \cap S_j = \varnothing$, $i \neq j$.

(P1) 说明 $\{S_i\}$ 这些子集无遗漏地包含了 S 的全部元素; (P2) 说明两个不同的子集无公共元素. 从而 S 的元素属于且仅属于一个子集. 这表明, S 的一个分类必须满足不漏不重的原则.

例 6 设 M 为数域 F 上全体 n 阶方阵的集合, 令 M_r 表示所有秩为 r 的 n 阶方阵构成的子集, 则有

(1) $M = \bigcup\limits_{i=0}^{n} M_i$;

(2) $M_i \cap M_j = \varnothing$, $i \neq j$.

所以 $\{M_i \mid i = 0, 1, \cdots, n\}$ 是 M 的一种分类.

例 7　$\mathbf{Z}_m=\{\overline{a}\mid a=0,1,2,\cdots,m-1\}$ 是整数集 $\mathbf{Z}$ 的一种分类.

例 8　对实数集 $\mathbf{R}$, 令子集 $\mathbf{R}_i=[i,i+1]$, $i\in\mathbf{Z}$. 由于 $i\in\mathbf{R}_i$, 且 $i\in\mathbf{R}_{i-1}$, 同一元素在两个子集中重复出现, 所以 $\{[i,i+1]\mid i\in\mathbf{Z}\}$ 不是 $\mathbf{R}$ 的一种分类.

下面的定理揭示了集合的等价关系与集合的分类这两个概念之间的联系.

定理 1.1.1　*集合 S 的任何一个等价关系都确定了 S 的一种分类, 且其中每一个类都是集合 S 的一个等价类. 反之, 集合 S 的任何一种分类也都给出了集合 S 的一个等价关系, 且相应的等价类就是原分类中的那些类.*

证明　首先, 设 $\sim$ 为集合 S 的一个等价关系, 则

(1) 对任意的 $a\in S$, 由反身性知 $a\in[a]$, 所以 $S=\bigcup\limits_{a\in S}[a]$.

(2) 如果 $[a]\cap[b]\neq\varnothing$, 则有 $c\in[a]\cap[b]$. 于是 $c\sim b$, $c\sim a$, 从而由对称性知 $b\sim c$, 再由传递性知 $b\sim a$. 又对任意的 $b'\in[b]$, 则 $b'\sim b$, 同样由传递性得 $b'\sim a$. 于是 $b'\in[a]$, 因此 $[b]\subseteq[a]$. 同理可证 $[a]\subseteq[b]$. 于是 $[a]=[b]$. 所以不同的类没有公共元素.

从而由 (P1), (P2) 知, 全体等价类形成 S 的一种分类, 显然每一个类都是 S 的等价类.

其次, 如果已知集合 S 的一种分类 $\mathcal{P}$, 在 S 中规定关系 "$\sim$":

$$a\sim b\Longleftrightarrow a\text{ 与 }b\text{ 属于同一类},\quad a,b\in S.$$

对任意的 $a\in S$, 由于 a 属于其本身所在的类, 所以 $a\sim a$. 如果 $a\sim b$, 即 a 与 b 属于同一类, 自然 b 与 a 也属于同一类, 所以 $b\sim a$. 最后, 如果 $a\sim b$, $b\sim c$, 即 a 与 b 属于同一类, b 与 c 属于同一类, 因而 a 与 c 同在 b 所在的类中, 所以 $a\sim c$. 因此 "$\sim$" 是 S 的一个等价关系. 显然, 由此等价关系得到的等价类就是原分类中的那些类. □

定理 1.1.1 说明, 一个集合的分类可以通过等价关系来描述. 试比较例 4、例 5 及例 6、例 7, 可以看出, 这样做在很多情况下是方便的. 另一方面, 等价关系也可以用集合的分类来表示. 通过对集合的各种分类的了解, 使我们能够对集合的不同等价关系及其相互联系进行研究. 不过, 本书不准备对此进行深入的讨论. 仅以下面的例子来说明集合的分类对研究集合的等价关系的作用.

例 9　设 $S=\{a,b,c\}$, 试确定集合 S 的全部等价关系.

解　由定理 1.1.1 知, 只要求出 S 的全部分类, 即求出 S 的所有可能的子集分划即可.

(1) 如果 S 仅分划为一个子集, 则有 $\mathcal{P}_1=\{S\}$;

(2) 如果 S 分划为两个子集, 则有

$$\mathcal{P}_2=\{\{a\},\{b,c\}\},\quad \mathcal{P}_3=\{\{b\},\{a,c\}\},\quad \mathcal{P}_4=\{\{c\},\{a,b\}\};$$

(3) 如果 S 分划为三个子集, 则有 $\mathcal{P}_5=\{\{a\},\{b\},\{c\}\}$.

因此, 集合 S 共有五个不同的等价关系, 它们是

$$\sim_1=\{a\sim a,b\sim b,c\sim c,a\sim b,b\sim a,a\sim c,c\sim a,b\sim c,c\sim b\};$$

$$\sim_2=\{a\sim a,\ b\sim b,\ c\sim c,\ b\sim c,\ c\sim b\};$$

$$\sim_3=\{a\sim a,\ b\sim b,\ c\sim c,\ a\sim c,\ c\sim a\};$$

$$\sim_4=\{a\sim a,\ b\sim b,\ c\sim c,\ a\sim b,\ b\sim a\};$$

$$\sim_5=\{a\sim a,\ b\sim b,\ c\sim c\}.$$

注 如果用 $B(n)$ 表示一个具有 n 个元素的集合上的不同等价关系的个数, 则有下列的递推公式:

$$B(n+1)=\sum_{k=0}^{n}\mathrm{C}_n^kB(k),\quad n\geqslant 1, \tag{1.1.1}$$

其中 C_n^k 为二项式系数, 并规定 $B(0)=1$, $B(1)=1$. 这个公式的证明以及对数 $B(n)$ 的性质的讨论, 已超出本书的范围. 有兴趣的读者可参考组合数学方面的书籍 (如文献 [2]).

习 题 1-1

1. 试分别举出满足下列条件的关系:

(1) 有对称性, 传递性, 但无反身性;

(2) 有反身性, 传递性, 但无对称性;

(3) 有反身性, 对称性, 但无传递性.

2. 找出下列证明中的错误:

有人断言, 若 S 的关系 $\mathcal{R}$ 有对称性和传递性, 则必有反身性. 这是因为, 对任意的 $a\in S$, 由对称性, 如果 $a\mathcal{R}b$, 则 $b\mathcal{R}a$. 再由传递性, 得 $a\mathcal{R}a$, 所以 $\mathcal{R}$ 有反身性.

3. 证明: 在数域 F 上全体 n 阶方阵的集合 M 中, 矩阵的等价、相合和相似都是等价关系.

4. 设 ϕ 是集合 A 到 B 的映射, $a,b\in A$, 规定关系 "$\sim$":

$$a\sim b\iff\phi(a)=\phi(b).$$

证明: $\sim$ 是 A 的一个等价关系, 并求其等价类.

5. 设 $A=\{1,2,3,4\}$, 在 $\mathcal{P}(A)$ 中规定关系 "$\sim$":

$$S_1\sim S_2\iff S_1\text{ 与 }S_2\text{ 含有相同个数的元素}.$$

证明: $\sim$ 是 $\mathcal{P}(A)$ 的一个等价关系, 并求商集 $\mathcal{P}(A)/\sim$.

6. 在有理数集 $\mathbf{Q}$ 中, 规定关系 "$\sim$":

$$a\sim b\iff a-b\in\mathbf{Z}.$$

证明：$\sim$ 是 $\mathbf{Q}$ 的一个等价关系, 并求出所有的等价类.

7. 在复数集 $\mathbf{C}$ 中, 规定关系 "$\sim$":

$$a \sim b \Longleftrightarrow |a| = |b|.$$

证明：$\sim$ 是 $\mathbf{C}$ 的一个等价关系, 试确定相应的商集 $\mathbf{C}/\sim$, 并给出每个等价类的一个代表元素.

8. 设集合

$$S = \{(a, b) \mid a, b \in \mathbf{Z}, b \neq 0\},$$

在集合 S 中, 规定关系 "$\sim$":

$$(a, b) \sim (c, d) \iff ad = bc.$$

证明：$\sim$ 是 S 的一个等价关系.

*9. 设 $A = \{a, b, c, d\}$, 试写出集合 A 的所有不同的等价关系.

*10. 不用公式 (1.1.1), 直接算出集合 $A = \{1, 2, 3, 4, 5\}$ 的不同的分类数.

参考文献及阅读材料

[1] 闵嗣鹤, 严士健. 初等数论. 第 2 版. 北京: 高等教育出版社, 1990.

本书第 1 章有关于整数整除性的详细讨论, 第 3 章则介绍了同余的概念及其性质.

[2] Aigner M. Combinatorial Theory. Berlin, Heidelberg, New York: Springer-Verlag, 1979.

1.2　群的概念

代数最初主要研究的是数, 以及由数所衍生出来的对象. 例如, 代数方程的求根. 初等代数主要研究的就是数以及数的运算. 中学数学虽然有所谓代数式的概念, 但这些概念本质上代表的仍然是数. 高等代数虽引入了行列式、矩阵等概念, 但还是离不开数. 数的一个基本特征是可以进行加法、乘法等运算. 这些运算的共同特点是对任意两个数, 通过某个法则 (如加法法则或乘法法则等), 可唯一求得第三个数. 数学家们发现, 许多抽象的对象也都具有类似于数的这一特征, 于是对它们的结构和性质进行了研究, 并且应用它们解决了许多重大的数学问题和实际问题. 这就导致了近世代数的产生和发展. 近世代数拓展了代数的研究领域, 它所研究的已不再仅仅是数, 而是具有某种运算的代数系统, 这其中最基本的就是群、环和域.

本节的主要目的就是介绍群的基本概念和简单性质. 为此, 首先要对运算这一概念给出明确的定义.

定义 1.2.1　设 A 是一个非空集合, 若对 A 中任意两个元素 a, b, 通过某个法则 "$\cdot$", 有 A 中唯一确定的元素 c 与之对应, 则称法则 "$\cdot$" 为集合 A 上的一个**代数运算**(algebraic operation). 元素 c 是 a, b 通过运算 "$\cdot$" 作用的结果, 将此结果记为 $a \cdot b = c$.

例 1 有理数的加法、减法和乘法都是有理数集 $\mathbf{Q}$ 上的代数运算, 但除法不是 $\mathbf{Q}$ 上的代数运算. 如果只考虑所有非零有理数的集合 $\mathbf{Q}^*$, 则除法是 $\mathbf{Q}^*$ 上的代数运算.

例 2 设 m 为大于 1 的正整数, $\mathbf{Z}_m$ 为 $\mathbf{Z}$ 的模 m 剩余类集. 对 $\overline{a}, \overline{b} \in \mathbf{Z}_m$, 规定

$$\overline{a} + \overline{b} = \overline{a+b},$$
$$\overline{a} \cdot \overline{b} = \overline{ab},$$

则 $+$ 与 $\cdot$ 都是 $\mathbf{Z}_m$ 上的代数运算.

证明 只要证明上面规定的运算与剩余类的代表元的选取无关即可. 设

$$\overline{a} = \overline{a'}, \quad \overline{b} = \overline{b'},$$

则

$$m \mid a - a', \quad m \mid b - b',$$

于是

$$m \mid (a-a') + (b-b') = (a+b) - (a'+b'),$$
$$m \mid (a-a')b + (b-b')a' = (ab) - (a'b'),$$

从而

$$\overline{a+b} = \overline{a'+b'}, \quad \overline{ab} = \overline{a'b'},$$

所以 "+" 与 "·" 都是 $\mathbf{Z}_m$ 上的代数运算. □

分析上面几个例子中的代数运算发现, 这些代数运算不仅仅给出运算的结果, 而且还具有一些相似的运算性质. 比如说, 结合律、交换律等. 在比较理想的情况下 (就像在 $\mathbf{Q}^*$ 中), 还有单位元、可逆元和逆元. 将这些加以综合与推广, 就得到群的概念.

定义 1.2.2 *设 G 是一个非空集合, "$\cdot$" 是 G 上的一个代数运算, 即对所有的 $a, b \in G$, 有 $a \cdot b \in G$. 如果 G 的运算还满足*

(G1) *结合律, 即对所有的 $a, b, c \in G$, 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;*

(G2) *G 中有元素 e, 使对每个 $a \in G$, 有 $e \cdot a = a \cdot e = a$;*

(G3) *对 G 中每个元素 a, 存在元素 $b \in G$, 使 $a \cdot b = b \cdot a = e$,*

则称 G 关于运算 "$\cdot$" 构成一个群(group), *记作 $(G, \cdot)$. 在不致引起混淆的情况下, 也称 G 为群.*

注 (1) (G2) 中的元素 e 称为群 G 的**单位元**(unit element) **或恒等元**(identity); (G3) 中的元素 b 称为 a 的**逆元**(inverse). 我们将证明, 群 G 的单位元 e 和每个元素的逆元都是唯一的. G 中元素 a 的唯一的逆元通常记作 a^{-1}.