国家精品资源共享课配套教材
普通高等教育“十三五”规划教材
南开大学代数类课程整体规划系列教材

抽象代数

Abstract Algebra

邓少强　朱富海　编著

科学出版社

国家精品资源共享课配套教材

普通高等教育“十三五”规划教材

南开大学代数类课程整体规划系列教材

抽象代数

邓少强　朱富海　编著

科学出版社

北京

内 容 简 介

本书是南开大学代数类课程整体规划系列教材的第二本，主要讲述群、环、模、域等理论中最基础的知识，以大学一年级的高等代数课程为基础. 本书特别注意讲清定理、定义的来源以及其中包含的数学思想. 书中配有大量精心挑选的基本习题和训练与提高题.

本书可用于大学本科数学与应用数学专业两学期的抽象代数课程，特别适合国内985或211学校或类似的本科学校的该课程的教学，也可用于数学爱好者自学或数学工作者参考.

图书在版编目(CIP)数据

抽象代数/邓少强，朱富海编著. —北京：科学出版社，2017.6
国家精品资源共享课配套教材. 普通高等教育“十三五”规划教材. 南开大学代数类课程整体规划系列教材

ISBN 978-7-03-053634-1

Ⅰ. ①抽… Ⅱ. ①邓… ②朱… Ⅲ. ①抽象代数-高等学校-教材 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2017) 第 133247 号

责任编辑：张中兴 / 责任校对：彭 涛
责任印制：吴兆东 / 封面设计：迷底书装

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

北京中石油彩色印刷有限责任公司 印刷
科学出版社发行 各地新华书店经销
*
2017 年 6 月第 一 版 开本：720 × 1000 1/16
2017 年10月第二次印刷 印张：13 3/4
字数：278 000

定价：42.00 元

(如有印装质量问题，我社负责调换)

《南开大学代数类课程整体规划系列教材》
丛书编委会名单

前言

本书是南开大学代数类课程整体规划系列教材的第二本, 适用于我国大学本科数学与应用数学抽象代数课程, 主要讲述群、环、模、域等理论中最基础的知识. 我们假定读者学习过大学一年级高等代数与解析几何课程的最基本内容. 但是除了一些例子中涉及高等代数与解析几何的知识外, 本书的绝大部分内容并不是真的需要高等代数作为基础. 我们的主要目标是让读者通过本课程的学习, 理解和体会代数学的基本思想, 为数学其他课程的学习或将来进行代数学的研究提供必要的代数基础.

全书共四章. 第 1 章讲述群的基本理论, 包括群、子群、商群、群的同态与同构、变换群与置换群、群的扩张、群在集合上的作用及 Sylow 定理; 第 2 章主要讲述环的基础理论包括环、子环与理想、同态、素理想与极大理想、四元数体、主理想整环与欧几里得环, 以及环上的多项式理论; 第 3 章是模论, 除了模的基本定义外, 主要讲述主理想整环上的有限生成模的结构理论. 作为应用, 我们给出了有限生成 Abel 群的分类以及线性变换的标准形理论. 第 4 章讲述 Galois 理论、包括域的扩张理论、Galois 理论的基本定理, 以及方程存在根式解的条件等.

本书的写作中我们特别注意讲清定理、定义的来源以及其中包含的数学思想, 而对于命题和定理的证明都会强调其思路. 为了做到这一点, 我们往往在引入新的定义或结果以前加入一些解释性的说明, 即使有时在职业的数学研究人员看来这可能过于琐碎甚至啰嗦. 我们认为, 现在的数学教育过于强调技巧和逻辑, 而对于数学思想的传授似乎有忽略的倾向. 当然我们的尝试是否合适, 还有待实践的检验. 我们特别期待读者对于本书的有些做法提出建议甚至是批评.

本书可用于大学本科数学与应用数学专业两学期的抽象代数课程, 特别适合国内 985 或 211 学校或类似的本科学校该课程的教学. 值得注意的是, 本书有一定的难度, 因此并不是所有高等学校的抽象代数课程都需要讲授全部内容. 如果是一学期每周四学时, 可以讲授群论的全部内容, 环论除了多项式理论的全部内容, 以及

域论的前四节. 如果是一学期每周三学时, 则可以讲授群论的前六节, 环论的前七节, 以及域论的前四节. 如果是两学期的课程, 则可以讲授全部内容.

本书的习题是我们精心设计的, 分为基本习题和训练与提高题. 基本习题是围绕课程内容设计的, 属于基本要求. 一般说来, 一名普通的学生应该有能力完成其中的大部分. 而训练与提高题是为拓展学生视野和进行基础科学训练而设计的, 不在基本要求之内. 事实上, 即使是优秀的学生, 也不一定有能力全部解决这些问题. 除了习题外, 我们还在正文中设计了很多思考题. 这些思考题有的紧扣教材内容, 是为了加深学生对课程内容的理解, 有的是为了指出某些重要的结果. 一般来说, 学生在学习过程中可以解决大部分的思考题, 不过值得注意的是, 部分思考题难度是很大的, 只有参考的价值.

本书是我们根据多年抽象代数课程的教学实践, 通过深入研究和总结而编写的, 部分内容在南开大学数学 "伯苓班" 试用过多次. 本书的编写过程中也有很多学生和同事提出了大量宝贵的修改意见, 我们也根据这些意见多次进行校对和修改.

虽然如此, 限于作者水平, 书中不足之处在所难免, 敬请读者批评指正.

作 者

2016 年 12 月

目录

引　言

抽象代数是高等代数和解析几何这一课程在抽象层面上的延续. 在高等代数与解析几何中主要研究了多元一次方程组的求解及由此发展而来的矩阵、线性空间和线性变换等理论, 这些理论在抽象代数的理论体系中也占有举足轻重的地位, 不仅提供了大量的具体例子, 而且提供了很多思想方法. 一元高次方程, 即多项式理论的研究正是抽象代数理论发展的起源, 其历史可以追溯到 4000 年前的古巴比伦时期. 楔形文字泥板记录了 4000 年前的古巴比伦人对二次方程求根的探索, 实际上他们已经找到求根公式了. 然而经过了 3000 多年的沉寂, 直到文艺复兴时期, 在一批意大利数学家的努力下, 三、四次方程的求根公式问题才取得了突破. 首先是 Ferro 和 Tartaglia 独立的发现了后来被称为 Cardano 公式的三次方程求根公式. Cardano 的学生 Ferrari 在此基础上找到了四次方程的求根方法. 1770 年, Lagrange 用一种统一的方法来处理低于五次的方程的求根方法, 他的方法体现了根置换的思想. 不过在应用到五次以上方程求解时遇到了实质性的困难, 也提示人们五次以上方程未必有求根公式. 1799 年, Ruffini 证明一般五次以上方程不可解, 不过证明中有漏洞. 直到 1824 年, Abel 给出了后来被称为 Abel-Ruffini 定理的完整证明, 正式宣告一般五次以上方程不可用根式解. 尽管如此, 还是有很多高次方程是明显可解的. 法国数学家 Galois 在前人的研究工作的基础上引入群和域的思想来描述方程的根的对称性. 域论的简单性质就能给出古希腊三大几何作图难题的否定回答. 进一步, Galois 理论可以给出正 n 边形可以尺规作图的充要条件. 最为重要的是, 域论和群论的结合得到了一元高次方程可用根式解的充要条件. 从此, 代数学研究开始了新的篇章.

在很多杰出的数学家的努力下, 群论迅速发展成为一门崭新的数学分支. 出于判断方程是否可用根式解的需要, Galois 证明了 $A_n(n \geqslant 5)$ 是单群. 由此开启了数学家们对群论的核心问题——有限单群分类的研究. 这一史诗般的研究工作持续了百年, 跨越了整个 20 世纪. 从 1963 年 Feit 和 Thompson 发表长达 255 页的论文证

明了 Burnside 关于奇数阶群都是可解群的猜想开始, 有限单群的研究进入了快车道. Gorenstein 引领了有限单群分类的国际合作, 并于 1983 年宣布分类工作完成. 然而, 漏洞很快被发现, 直到 2004 年这一漏洞才被一篇 1221 页的论文填补. 尽管目前公认有限单群的分类工作已经完成, 不过由于篇幅太长, 微小的漏洞仍然会被发现; 并且, 简化分类证明的工作也在不断进行中.

域论也在 Abel 和 Galois 的工作基础上不断发展. 1871 年, 数域的概念被 Dedekind 首先引入. 1881 年, Kronecker 定义了有理函数域. 1893 年, H. M. Weber 给出了域的抽象定义. 1910 年, E. Steinitz 研究了域的性质, 给出了素域、完备域等概念. 1928 年至 1942 年, E. Artin 系统地研究了群与域的关系, 发展了 Galois 理论. 到目前为止, 对于代数数域的研究始终是数论研究的一个重要方向.

比域论更广泛的是环论. 我们熟知的整数、多项式全体都构成环. 在数论的早期研究包括对 Fermat 大定理的研究中, 代数整数环的重要性不断体现, 其中的因式分解的不唯一性也给包括 Cauchy 在内的数学家们带来了极大的困扰. 1843 年, Hamilton 经过十年努力发现了四元数体, 这是一种不满足乘法交换律的环或代数. 很快, 在 1857 年, Cayley 引入了矩阵乘法, 矩阵代数得到迅速发展, 为包括环论在内的抽象代数的发展奠定了基础. 随后, Clifford, Wedderburn, Artin 等一批数学家为环论的发展做出了极大贡献. 其中最值得一提的是被誉为 "数学史上最重要的女性" 的 Emmy Noether, 她提出的模论使得抽象代数的很多概念和理论得以统一起来, 并被广泛应用到代数拓扑、代数几何等领域中. 实际上, 代数学领域内的各种表示理论都可以看做是模论.

第1章 群

在 18 世纪 Euler 和 Gauss 对于数论的研究中已经有了群的概念的萌芽; Lagrange, Raffini 和 Abel 对于方程根式解的研究中运用了根的置换的思想, 研究了置换群的性质; 群的概念的提出要归功于 Galois, 他利用群彻底解决了方程根式解的充要条件. 在 20 世纪, 群论的一个重大研究成果是在很多群论学家的共同努力之下完成了有限单群的分类. 当然, 群论的研究工作远远没有结束, 群的用途也越来越广泛. 如 18 世纪后半叶, Klein 把群的思想运用到几何分类的研究中, Lie 在对偏微分方程的研究中提出了 Lie 群的概念, 这些都开创了新的研究领域. 在其他学科, 如物理、化学等, 群论也有广泛的应用. 本章我们将介绍群的基本理论, 研究群分类的基本思想和基本工具.

1.1 半群与群

顾名思义, 抽象代数是在抽象的层面上研究代数结构. 简单地说, 一个代数结构其实就是一个定义了一种或多种运算的非空集合, 而我们要研究的正是其中的运算规律. 首先来看一些熟知的例子. 在整数集 $\mathbb{Z}$, 非负整数集或自然数集 $\mathbb{N}=\{a\in\mathbb{Z}|a\geqslant 0\}$, 以及任何一个数域 $\mathbb{P}$ (如有理数域 $\mathbb{Q}$、实数域 $\mathbb{R}$、复数域 $\mathbb{C}$ 等) 上, 多项式集合 $\mathbb{P}[x]$ 等集合上都有加法和乘法两种运算. 矩阵理论中的 $\mathbb{P}^{m\times n}$ 有加法和数乘运算. 特别地, $\mathbb{P}^{n\times n}$ 上还具有乘法运算. 容易验证, 我们熟知的 n 阶可逆矩阵的全体 $\mathrm{GL}(n,\mathbb{P})$、实正交矩阵的全体 $\mathrm{O}(n)$ 在矩阵乘法的运算下是封闭的. 这些运算都是由两个元素对应到一个元素的一种法则, 它们都有自己的特性, 也有一些共性. 本书的群、环、模和域等理论实际上都是从这些共性中抽象出来的.

为了方便叙述, 首先引入一个记号. 设 A,B 为两个非空集合, 用 $A\times B$ 表示 A 与 B 的直积集合, 它是由所有有序对 (a,b) 组成的, 其中 $a\in A,b\in B$, 也就是说

$$A\times B=\{(a,b)|\,a\in A,b\in B\}.$$

这个概念自然可以推广到有限个集合的情形.

现在我们从一些熟知的数学对象中提炼出如下定义.

定义1.1.1 给定非空集合 S, 若有一个法则, 使得对任意 $a,b\in S$, 存在 S 中唯一元素 c 与有序对 (a,b) 对应, 则称 S 上定义了一个**二元运算**. 称 c 为 a,b 的**积**. 换言之, 非空集合 S 上的一个二元运算实际上就是 $S\times S$ 到 S 的一个映射.

这一定义当然可以推广到一般情形, 如果 A,B,D 是三个非空集合, 则一个由直积集合 $A\times B$ 到 D 的映射称为一个 A 与 B 到 D 的**代数运算**. 为了方便, 我们通常会用一些运算符号来表示两个元素 $a\in A,b\in B$ 组成的有序对 (a,b) 在代数运算下的像, 例如, 我们经常将 (a,b) 的像记为 $a*b$, 在不引起混淆的情况下记为 ab. 我们以前用到的运算符号, 如 "+", "×" 等也经常用来表示代数运算.

抽象代数中研究最多的是二元运算. 我们熟知的二元运算大都满足一定的运算规律, 这些运算规律抽象出来就得到如下定义.

定义1.1.2 设非空集合 S 上定义了一个二元运算. 称该运算满足**结合律**, 如果

$$(ab)c=a(bc),\ \ \forall a,b,c\in S.$$

称该运算满足**交换律**, 如果

$$ab=ba,\quad \forall a,b\in S.$$

当运算满足交换律时有时会用 $a+b$ 来表示 ab.

定义1.1.3 设 S 为一个非空集合, 且在 S 上定义了 $*$ 与 $+$ 两种二元运算. 称这两种运算满足 $*$ 对$+$**的左、右分配律**, 如果

$$a*(b+c)=a*b+a*c,\quad (b+c)*a=b*a+c*a,\quad \forall a,b,c\in S.$$

一般将左、右分配律统称为**分配律**.

我们以前涉及的大部分运算都是满足结合律的. 为了方便, 引入如下定义.

定义1.1.4 若非空集合 S 中定义了一个满足结合律的二元运算 $*$, 则称 $\{S;*\}$ 为一个**半群**, 在不至于引起混淆时, 也称 S 是一个**半群**, 将 $a*b$ 简记为 ab.

若半群 S 中存在一个元素 e, 对任意 $a\in S$ 有

$$ea=a\quad (\text{或 } ae=a),$$

则称 e 为 S 的**左 (右) 幺元**. 若 e 既是 S 的左幺元, 又是 S 的右幺元, 则称 e 为 S 的**幺元**. 含幺元的半群称为**幺半群**. 若 S 中的运算还满足交换律, 则称 S 为**交换幺半群**.

思考题1.1.5 试举例说明, 存在半群 S, S 中有左幺元, 但没有右幺元.

思考题1.1.6 若一个半群 S 中既有左幺元, 又有右幺元, S 是否一定为幺半群?

本节开始时提到的所有例子都是半群. 其中, 正整数集 $\mathbb{N}^*$ 对于乘法是幺半群, 对于加法是半群但不是幺半群. 读者可以自行判断其他例子哪些是幺半群, 哪些不是. 要构造一个半群, 需要定义出一个具有结合律的运算. 这一点看似简单, 其实并不容易. 一个很自然的满足结合律的运算是一个非空集合上的变换 (即集合到自身的映射) 的复合.

例1.1.7 记 $M(X)$ 为非空集合 X 上的所有变换的集合, 则 $M(X)$ 在变换的乘法 (即复合) 下构成一个幺半群, 其幺元就是 X 的恒等变换 id_X.

上面的这个例子是由任意的非空集合构造一个幺半群, 而在实际中, 集合往往会带上某些附加的结构, 例如, 线性空间的结构、度量等. 这时我们将保持相应的结构的变换拿出来, 就能构造新的幺半群. 下面我们给出几个这样的例子.

例1.1.8 设 V 是数域 $\mathbb{P}$ 上的线性空间, $\mathrm{End}\,V$ 为 V 上的线性变换的全体, 则 $\mathrm{End}\,V$ 在变换的乘法下构成幺半群, 其幺元就是 V 的恒等变换 id_V.

此外还有一些比较特别的例子.

例1.1.9 记非空集合 X 的所有子集的集合为 $P(X)$, 称为 X 的**幂集**, 则 $\{P(X);\cup\}$ 是幺半群, 幺元是空集 $\varnothing$. 此外, $\{P(X);\cap\}$ 也是幺半群, 幺元是 X. 这里 $\cup,\cap$ 分别表示集合求并与求交的运算. 这是定义在同一个集合上的两个不同的幺半群. 这个例子说明, 在同一集合上可以定义不同的二元运算, 从而得到不同的代数体系. 从这个意义上来说, 在一个代数体系中, 运算比集合更为本质.

在幺半群中, 不同元素的性质有很大的差异, 如在 $\mathbb{P}^{n\times n}$ 中, 有些矩阵是可逆的, 而有些矩阵是奇异 (不可逆) 的. 相对而言, 可逆矩阵具有更好的性质, 也更容易处理. 由此我们引入下面的定义.

定义1.1.10 设 S 是幺半群, e 是幺元, $a\in S$, 若存在 $b\in S$, 使得 $ba=e$ $(ab=e)$, 则称 b 为 a 的**左 (右) 逆元**. 若 b 既是 a 的左逆元, 又是 a 的右逆元, 即有 $ba=ab=e$, 则称 b 为 a 的**逆元**, 这时称 a 为**可逆元**.

思考题1.1.11 试举例说明, 存在幺半群 S 及 $a\in S$, a 存在左逆元, 但不存在右逆元.

思考题1.1.12 如果一个幺半群 S 中元素 a 既存在左逆元, 又存在右逆元, a 是否一定是可逆元?

下面我们讨论一下幺半群和可逆元的简单性质.

命题1.1.13 幺半群中的幺元是唯一的, 而且任何可逆元的逆元也是唯一的.

证 e 与 e' 均是幺元, 则 $e'=e'e=e$, 故幺元唯一. 设 b 和 b' 都是可逆元 a 的逆元, 则 $b=be=b(ab')=(ba)b'=b'$, 故逆元唯一. □

由这个命题, 以后我们将幺半群中可逆元 a 的逆元记为 a^{-1}. 有了上面的这些准备, 本章最重要的概念——群就该出场了. 群是抽象代数中第一个, 也是最重要的一个概念. Galois 在研究代数方程的根式解的问题时, 他用到了根的置换的概念, 这里包含的原理其实就是, 一个代数方程的根的全体具有某种对称性, 而这些对称性将构成一个群. 这是群的概念第一次被用到数学研究中.

定义1.1.14 *如果幺半群 G 中的每个元都是可逆元, 则称 G 为一个群. 若群中运算还满足交换律, 则称 G 为交换群或 Abel 群. 群 G 中所含元素的个数记为 $|G|$, 称为 G 的阶. 若 $|G|$ 无限, 则称 G 为无限群. 若 $|G|$ 有限, 则称 G 为有限群. 特别地, 若 G 只有一个元素, 则称为平凡群.*

群的概念是通过对数学研究对象中出现的对称性进行高度抽象而得到的一类代数体系的总称, 因此具有非常广泛的应用. 群的研究不但是抽象代数中最重要的课题, 也与其他数学分支, 如分析学、几何学、拓扑学等紧密相关.

一般说来, 用上面的定义来直接验证一个代数体系是群比较麻烦, 下面的定理将定义 1.1.14 中的条件作了减弱.

定理1.1.15 *设 G 是一个半群, 则 G 是一个群当且仅当以下条件满足:*

(1) *G 中存在左幺元, 即存在 $e \in G$, 使得对任意 $a \in G$, 有 $ea = a$;*

(2) *G 中任意元素都存在左逆元, 即对任意 $a \in G$, 存在 $b \in G$, 使得 $ba = e$.*

证 必要性显然. 对于充分性, 需要证明左幺元 e 也是右幺元, 且 G 中任何元素的左逆元也是它的右逆元. 对任何 $a \in G$, 设 b 为 a 的左逆元, c 为 b 的左逆元, 则有 $a = (cb)a = c(ba) = ce$. 于是 $ab = (ce)b = cb = e$. 故 b 是 a 的逆元. 进一步,

$$ae = a(ba) = (ab)a = a,$$

故 e 也是右幺元. □

思考题1.1.16 *将定理中的左幺元和左逆元同时改为右幺元和右逆元, 结论是否成立? 若半群 G 中存在左幺元, 且每个元都有右逆元, G 是否一定是群?*

一般说来, 要完全确定一个群的结构, 就是确定这个群中的所有元以及任何两个元的积. 如果 $G = \{a_1, \cdots, a_n\}$ 为有限群, a_1 为幺元, 则 G 的乘法可以用如下的表格形式给出.

	a_1	$\cdots$	a_n
a_1	a_1a_1	$\cdots$	a_1a_n
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	a_na_1	$\cdots$	a_na_n

此表称为 G 的 "**群表**". 群表的表示方法显然也适用于有限半群. 更一般地, 如果一个有限集合上定义了二元运算, 我们就可以通过列表的形式来刻画该运算.

下面我们给出群的若干简单而且重要的性质. 我们将会看到, 高等代数中处理可逆矩阵的很多技巧, 在这里也可以应用.

引理1.1.17 *群 G 的运算满足左 (右) 消去律, 即对任意 $a,b,c\in G$, 由 $ab=ac$ $(ba=ca)$ 可以推出 $b=c$.*

证 设 $ab=ac$, 则 $a^{-1}(ab)=a^{-1}(ac)$. 再由结合律得 $(a^{-1}a)b=(a^{-1}a)c$, 即 $b=c$. 故左消去律成立. 同样可证右消去律也成立. □

命题1.1.18 *设 G 是一个半群, 则 G 是群当且仅当对任意 $a,b\in G$, 方程 $ax=b$ 及 $xa=b$ 的解均存在.*

证 若 G 是群, 直接验证知 $a^{-1}b$ 与 ba^{-1} 分别是 $ax=b$ 与 $xa=b$ 的一个解.

反之, 利用定理 1.1.15, 只需证明 G 中有左幺元及每个元有左逆元. 设 $a\in G$, $e\in G$ 是 $xa=a$ 的解. 对任意 $b\in G$, $ax=b$ 有解 $c\in G$, 于是 $eb=e(ac)=(ea)c=ac=b$. 所以 e 是 G 的左幺元. 又对于任意 $a\in G$, $xa=e$ 有解 b, 则 b 为 a 的左逆元. 因此 G 是群. □

命题1.1.19 *有限半群 G 若满足左、右消去律, 则 G 是群.*

证 设 $G=\{a_1,\cdots,a_n\}$. 因半群对运算封闭, 故对任意 $a_i\in G$, 有 $a_ia_1,\cdots,a_ia_n\in G$. 利用左消去律可知 $a_ia_1,\cdots,a_ia_n$ 必两两不等, 从而是 $a_1,\cdots,a_n$ 的一个排列. 因此对任意 $a_i,a_j\in G$, 存在 $a_k\in G$ 使得 $a_ia_k=a_j$, 也就是说, 方程 $a_ix=a_j$ 有解. 同理可证方程 $xa_i=a_j$ 也有解. 于是由命题 1.1.18, G 是一个群. □

注记1.1.20 *这个证明的思想很有用. 群的运算是二元的, 如果固定其中一个元素, 让另一个元素变, 则定义了群上的一个变换, 并且是单射. 事实上, 这个变换也是满射 (请读者自己证明), 这一点在后面研究群在集合上的作用时很重要. 此外, 需要注意的是, 命题 1.1.19 的结论对于无限半群并不成立, 试举例说明.*

从群的定义可以看出, 以前我们接触过的很多集合在相应的二元运算下都是群, 例如, 整数的集合 $\mathbb{Z}$ 在加法下是 Abel 群; 数域 $\mathbb{P}$ 上的任何线性空间对于其上的加法构成 Abel 群; $\mathbb{P}^{n\times m}$ 对于矩阵加法也是一个 Abel 群. 而数域 $\mathbb{P}$ 上 n 阶可逆矩阵的集合 $\mathrm{GL}(n,\mathbb{P})$, 以及实数域 $\mathbb{R}$ 上所有正交矩阵的集合 $\mathrm{O}(n)$, 对于矩阵的乘法也都构成群. 更一般地, 我们从任何幺半群出发都可以构造群.

命题1.1.21 *设 S 是幺半群, 记 $U(S)$ 为 S 中可逆元的全体, 则 $U(S)$ 是群.*

证 显然 $e\in U(S)$, 故 $U(S)$ 非空. 若 $a,b\in U(S)$, 则 $(ab)b^{-1}a^{-1}=a(bb^{-1})a^{-1}=aa^{-1}=e$, $b^{-1}a^{-1}(ab)=e$, 故 $ab\in U(S)$, 且其逆元是 $b^{-1}a^{-1}$. 于是, $U(S)$ 是一个幺半群且每个元都可逆, 因此 $U(S)$ 是一个群. □

由这个定理我们可以得到更多群的例子. 例如, 整数全体对于乘法构成幺半群, 因此其可逆元的全体 $\{1,-1\}$ 对于数的乘法构成群. 下面是一些更一般也更自然的例子.

例1.1.22 (1) *在例 1.1.7 中我们已经知道, 对于非空集合 X, $M(X)$ 为幺半*

群, 则其中的所有可逆变换 (也称为置换) 的全体 S_X 是群, 称为 X 的**对称群**. 特别地, 如果 X 为有限集, 不妨设 $X=\{1,2,\cdots,n\}$, 则 S_X 通常记为 S_n, 称为 n **元对称群**.

(2) 数域 $\mathbb{P}$ 上线性空间 V 上的可逆线性变换的全体 $\mathrm{GL}(V)$, 也就是幺半群 $\mathrm{End}(V)$ 中所有可逆元素构成的集合, 构成一个群, 称为**一般线性群**.

(3) 设 $\mathbb{P}$ 是任意数域, 则 $\mathbb{P}$ 在其加法下构成群, 而对于乘法只构成一个幺半群. 在乘法幺半群中, 一个元素可逆当且仅当其不为零, 因此 $\mathbb{P}^*=\mathbb{P}\setminus\{0\}$ 对于乘法构成群.

习 题 1.1

1. 下列集合 G 中所给的 $*$ 是否是二元运算? 若是, 判断 $(G,*)$ 是否满足交换律? 是否是半群、幺半群或群?

(1) $G=\mathbb{Z}$, $a*b=a-b$;

(2) $G=\mathbb{Z}$, $a*b=a+b-ab$;

(3) $G=\mathbb{Q}-\{0,1\}$, $a*b=ab$;

(4) G 为 $\mathbb{Z}[x]$ 中本原多项式的全体, $f(x)*g(x)=f(x)g(x)$;

(5) $G=\mathbb{N}^*$, $a*b=2^{ab}$;

(6) $G=\mathbb{N}^*$, $a*b=a^b$.

2. 在 $\mathbb{Z}\times\mathbb{Z}$ 中定义乘法为

$$(x_1,x_2)(y_1,y_2)=(x_1y_1+2x_2y_2,x_1y_2+x_2y_1).$$

证明: $\mathbb{Z}\times\mathbb{Z}$ 对此乘法为交换幺半群.

3. 记 $M(\mathbb{N})$ 为 $\mathbb{N}$ 的所有变换组成的幺半群, 其中元素 f 定义为

$$f(n)=n+1,\quad \forall n\in\mathbb{N}.$$

证明: f 有无穷多个左逆元, 但无右逆元.

4. 设集合 X 上有两个二元运算 "$\cdot$" 和 "$*$", 两个运算都有幺元且对任意 $a,b,c,d\in X$ 满足

$$(a*b)\cdot(c*d)=(a\cdot c)*(b\cdot d).$$

证明: 两个运算是一样的并且满足交换律和结合律.

5. 设集合 G 中只有两个元素, 试列举出 G 中所有半群结构, 并找出其中哪些是幺半群? 哪些是群?

6. 证明: 一个有限半群, 如果右消去律成立, 且至少有一个左单位元, 则此半群为群.

7. 试举出一个右消去律成立但不是群的有限半群的例子.

8. 试举出一个无限交换半群的例子, 它有单位元且满足消去律, 但不是群.

9. 设 $P(X)$ 为非空集合 X 的幂集 (即 X 的所有子集的集合). 对任意 $A, B \in P(X)$, 定义 A 与 B 的对称差 Δ 为

$$A\Delta B = (A \setminus B) \cup (B \setminus A).$$

这里, $A \setminus B = \{x \in A | x \notin B\}$. 试证 $(P(X), \Delta)$ 为一个群. 当 X 只含有两个元素时, 试给出该群的群表, 此时称该群为 **Klein 群**.

10. 证明: $\left\{ \mathrm{e}^{\frac{2k\sqrt{-1}\pi}{n}} = \cos\dfrac{2k\pi}{n} + \sqrt{-1}\sin\dfrac{2k\pi}{n} \middle| k = 0, \cdots, n-1 \right\}$ 是 n 个元的乘法群.

11. 设 $n \in \mathbb{N}, \mathbb{Z}_n$ 表示集合 $\{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$, 在 $\mathbb{Z}_n$ 中定义运算如下

$$\bar{a} \cdot \bar{b} = \bar{c}, \quad \text{其中 } c \text{ 是 } ab \text{ 模 } n \text{ 的余数};$$
$$\bar{a} + \bar{b} = \bar{d}, \quad \text{其中 } d \text{ 是 } a+b \text{ 模 } n \text{ 的余数}.$$

(1) 证明: $\{\mathbb{Z}_n; \cdot\}$ 是交换幺半群, $\{\mathbb{Z}_n; +\}$ 是交换群;

(2) 构造 $\{\mathbb{Z}_4; \cdot\}$ 的半群表;

(3) 设 $\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n | (a, n) = 1\}$, 证明: $\{\mathbb{Z}_n^*; \cdot\}$ 是群;

(4) 设 p 是素数, 利用群的思想证明 **Wilson 定理**: $(p-1)! \equiv -1 \pmod{p}$.

12. 设 $\varphi(n)$ 表示小于 n 的非负整数中与 n 互素的数的个数. 证明 **Euler 定理**:

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \quad a \in \mathbb{N}, \quad (a, n) = 1.$$

特别地, 当 $n = p$ 是素数时, $a^{p-1} \equiv 1 \pmod{n}$ (**Fermat 小定理**).

13. 设 $\mathrm{SL}(2, \mathbb{Z}_n) = \left\{ A = \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \middle| \bar{a}, \bar{b}, \bar{c}, \bar{d} \in \mathbb{Z}_n, \bar{a} \cdot \bar{d} - \bar{b} \cdot \bar{c} = \bar{1} \right\}$. 证明 $\mathrm{SL}(2, \mathbb{Z}_n)$ 在矩阵乘法下是群, 并求 $A \in \mathrm{SL}(2, \mathbb{Z}_n)$ 的逆. 试对任意 $m \in \mathbb{N}$ 定义 $\mathrm{SL}(m, \mathbb{Z}_n)$.

14. 如果半群 G 中的变换 $a \mapsto a'$ 满足:

$$a'(ab) = b = (ba)a', \quad \forall a, b \in G,$$

证明: G 是群.

15. 设 $G = \{(a, b) | a, b \in \mathbb{R}, a \neq 0\}$, 定义 G 中乘法为 $(a, b)(c, d) = (ac, ad + b)$. 证明 G 是群.

16. 设 $A \in \mathbb{R}^{n \times n}$, $\beta \in \mathbb{R}^n$, 定义 $\mathbb{R}^n$ 上变换 $T_{(A,\beta)}$ 为

$$T_{(A,\beta)}(\alpha) = A\alpha + \beta, \quad \forall \alpha \in \mathbb{R}^n.$$

(1) 证明: 当 $|A| \neq 0$ 时 $T_{(A,\beta)}$ 是双射;

(2) 证明: $\mathrm{Aff}(n, \mathbb{R}) = \{T_{(A,\beta)} | |A| \neq 0\}$ 关于映射的乘法构成群, 称为 $\mathbb{R}^n$ 的**仿射变换群**.

17. 举例说明存在数域 $\mathbb{P}$ 上非可逆 n 阶方阵构成的集合使得其在矩阵乘法下构成群, 并证明: 对任意这样的群 G, 存在非负整数 $k \leqslant n$ 和可逆矩阵 $T \in \mathbb{P}^{n \times n}$ 使得对任意 $A \in G$,