抽象代数 I
——代数学基础

孟道骥 陈良云
史毅茜 白瑞蒲 编著

科学出版社
www.sciencep.com

抽象代数 I

——代数学基础

孟道骥　陈良云
史毅茜　白瑞蒲　编著

科学出版社
北京

内 容 简 介

抽象代数(或近世代数)是数学的一个基础学科，也是数学及相关专业的基础课程. 南开大学“抽象代数”课程的改革是陈省身生前倡导的南开大学数学专业教学改革的一部分,《代数学基础》是该课程改革后使用的教材. 本书是由该教材修订、补充而成，内容包括基本概念、环、域、群、模和Galois 理论六部分.

本书力求深入浅出、循序渐进，以利于学生掌握抽象代数课程的精髓. 本书还特别注意与其他课程，如高等代数与解析几何、微分几何、李代数、有限群表示和抽象代数Ⅱ等的联系，加强学生对数学整体的把握.书中基本逐节配有习题，既可帮助读者巩固和拓广教材讲述的内容，又可进行科学研究能力的初步培养.

本书可作为高等院校数学专业本科生及理工科研究生抽象代数课程的教材，也可供有关科技人员及大专院校师生自学参考.

图书在版编目(CIP)数据

抽象代数. I，代数学基础/孟道骥等编著. —北京：科学出版社, 2010

ISBN 978-7-03-026302-5

Ⅰ. 抽… Ⅱ. 孟… Ⅲ. 抽象代数 Ⅳ. O153

中国版本图书馆 CIP 数据核字(2009)第 241756 号

责任编辑：王 静 房 阳 / 责任校对：邹慧卿

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

北京市文林印务有限公司 印刷

科学出版社发行 各地新华书店经销

*

2010 年 1 月第 一 版 开本：B5 (720 × 1000)

2010 年 1 月第一次印刷 印张：15 1/4

印数：1—3 000 字数：305 000

定价：28.00 元

(如有印装质量问题，我社负责调换)

前　言

从 1984 年开始, 我为南开大学数学系本科生讲授抽象代数. 特别根据陈省身先生的倡议, 南开大学于 1986 年创办了数学试点班, 并对该试点班的教学进行了许多改革, 其中一个重要的改革是加强抽象代数的教学. 教学时间由一个学期改为两个学期, 教学内容则要求系统和完整. 1992 年出版的《代数学基础》和之后出版的《南开大学数学教学丛书》都是这个试点班的教材.

《代数学基础》一书除南开大学数学系一直使用外, 还有一些其他学校也在使用, 有的学校还将其作为研究生课程的教材使用. 十多年过去, 情况有了很大的不同. 虽然我在此书出版后不再讲授这门课程, 但书中有一些问题慢慢得到了解答, 这些是需要修改和补充的. 这本书当时印得很少 (复印的不少), 现在已经买不到了, 但是仍不断有读者来询问何处可以买到. 陈良云、史毅茜和白瑞蒲三位老师三四年前就建议、敦促我再版此书, 而且主动为书的再版做了大量工作. 因此, 此书的再版应是他们的功劳. 科学出版社一如既往地积极支持我们, 愿意出版此书. 为了不辜负读者、三位老师和出版社的希望, 我决定再版此书, 当然新版书是我与陈良云、史毅茜、白瑞蒲三位老师共同合作完成的.

由于在学校这门课程的名称是 "抽象代数" 或 "近世代数", 虽然这两个名称未必完全确切, 但习惯成自然, 也不必去计较. 遵从这种习惯, 我们将新书命名为《抽象代数》. 由于扩充了很多内容, 新的《抽象代数》分为两本: 第一本是《抽象代数 I—— 代数学基础》, 基本保持了原书的结构与内容; 第二本是《抽象代数 II—— 结合代数》, 包括结合代数、张量代数、Clifford 代数和有限群表示等四部分内容. 这些内容在代数学中也是基本的, 在其他分支中又经常要用, 但是在抽象代数课程中往往被 "忽略", 实在应该给予它们在抽象代数中相应的地位.

源远流长的代数学, 历来在整个自然科学基础之一的数学中占有极为重要的地位. 今天它仍在蓬勃发展中, 它对数学以及整个自然科学和社会科学的影响与日俱增, 是数学中最有生机与活力的一个分支.

但是, 当我们回顾那漫长曲折的历史时, 却发现代数学在很长一段时期的发展竟是极其缓慢的. 初等代数学是研究数和文字的代数运算 (加法、减法、乘法、除法、乘方、开方) 的理论和方法. 其主要研究对象是多项式方程和多项式方程组的解. 其研究方法是高度计算性的. 16 世纪, 复数的引进是数学史一个重要的转折. 初等代数学相继解决了 2 次、3 次与 4 次方程求解问题. 这些方程的解都可用系数的四则运算与根式运算来给出, 即可用根式解这些方程. 初等代数也因此而达到顶峰. 但是, 当时的数学家们继续探索 5 次与 5 次以上方程的解, 也试图用根式解出这些方程. 经过 200 余年,

并无重要进展. 这里包括许多著名数学家, 如 L.Euler (1707~1783), A. T. Vandermonde (1735~1796), J. L. Lagrange (1736~1813), P. Ruffini (1765~1822) 等. 直到 19 世纪, 代数学的发展才有了转机.

1799 年, C. F. Gauss (1777~1855) 证明了代数学基本定理, 因此获得博士学位. 他将多项式的根与复平面上的点对应, 从而证明了多项式根的存在. 这里 Gauss 将复数与平面上的点一一对应, 使用 "复数" 这个名词, 对以后数学都有很大影响. 另一个重要的事情是他的方法. 与以前不同的是, Gauss 不是去计算一个根, 而是证明根的存在. 这个方法开创了探讨数学中存在性的新途径. 1801 年, Gauss 在《算术研究》中将等分圆周与二项方程 ($x^p - 1 = 0, p$ 为素数) 联系起来, 并建立了二项方程的理论. 1824 年, N. H. Abel (1802~1829) 解决了用根式求解 5 次方程不可能性问题. Abel 还研究了一类可以用根式解的方程, 后人发现这是具有交换的 Galois 群的方程, 但是用根式解高次方程的问题并未完全解决.

1829 年 5 月, E. Galois (1811~1832) 写出了代数方程可解性的论文, 1830 年 2 月修改后交法国科学院. 由于审稿人去世, 手稿遗失. 1831 年, 他再次修改论文, 交法国科学院, 这次并未得到应有的公正评价. 1832 年, Galois 在决斗前夕写了绝笔信, 整理了他的手稿, 概述了他得到的主要成果. Galois 不幸死于这场决斗. 1846 年, 即 Galois 逝世 14 年后, 他的部分论文才得以发表. 1870 年, C. Jordan (1838~1922) 全面介绍了 Galois 的思想. Galois 在探讨可用根式求解的方程时, 用了根的置换的概念. 实际上, 他已提出了群的概念, 用此理论彻底解决了用根式求解高次方程的问题, 并由此发展了一整套关于群和域的理论 ——Galois 理论.

自从 19 世纪 Galois 建立群论之后, 代数学有了突破性的进展, 主要是群、环、域及 Galois 理论的建立与发展. 无疑这些理论当时处于数学发展的前沿，人们就把它们称为 "近世代数 (modern algebra)". 这些理论与以往的代数，即初等代数相比，抽象性更为突出，如更着重于数学体系结构的研究，因而又被称为 "抽象代数 (abstract algebra)".

由各种代数结构的公理出发研究它们的性质，就是所谓抽象代数. 抽象代数研究的对象是非特定的任意元素集合和定义在这些元素间的、满足若干条件或公理的代数运算, 也就是说, 它以各种代数结构 (或系统) 性质的研究为中心问题. 公理化是抽象代数的主要研究方法. 这一切都与初等代数有天壤之别.

20 世纪, 尤其是 20 世纪 40 年代以后, 代数学与整个数学一样, 以空前的速度突飞猛进地发展. 同时代数学不仅在数学中, 而且在其他科学领域 (如物理学、化学、统计学、计算机科学、信息科学等) 中的影响与应用日益扩大. 抽象代数学的许多观点和方法也越来越 "普及". 随着时光的流逝, 19 世纪, 乃至 20 世纪的前半叶, 离我们越来越远. 这样以往所谓的 "近世代数" 或 "抽象代数" 的内容已经不再处于数学研究的前沿, 它的形象已不再那么虚无缥缈, 但是它的重要性却愈加显示出来了. 这些内容现在已经成了代数学乃至整个数学的基础.

本书分为 6 章.

第 1 章主要讲群、环、域及模的基本概念以及它们的同态基本定理. 大多数教材都是分别讲述群、环、模三种代数体系的同态基本定理的. 但是它们 (还有许多别的代数体系, 如结合代数等) 的同态基本定理是非常相似的. 其实, 它们都基于代数体系中的一种 "同余关系". 1.1节特别讲述了一个代数体系的同余关系, 在此基础上, 群、环、模的同态基本定理就可以统一讲述了,而且以后还可以容易地建立别的代数体系的同态基本定理.

第 2 章主要讲述环的基本理论. 本章是以交换整环的因式分解为中心. 之所以不先讲群再讲环, 是因为整数环、一元多项式环及它们的因式分解定理在初等代数、高等代数中都已出现过, 因而读者是很容易理解的. 即使在一般的交换整环中也不会感到这个理论很 "抽象", 而且在学习时, 读者不仅可以学会这些基本理论, 还可以逐步学会如何进行数学的抽象.

第 3 章讲域的基本理论, 以域的代数扩张为中心. 只要回顾一下从小学到高中对数的认识是由整数、分数、小数、有理数、无理数直到复数, 实际上就是对数域 (数环) 逐步扩张的认识. 从本质上讲, 这一章对于有高等代数基础的读者是没有什么困难的. 为实现某种目的把一个代数体系在某种条件下扩张, 使之达到某种更趋完美的程度, 现在已经成为数学研究中的一种基本方法. 域的扩张可以说是这种方法应用的一个极好的范例. 3.6 节证明了代数学基本定理. 代数学基本定理无论从内容, 或是证明它的方法在数学史上都是很重要的. 它的证明很多, 但至今没有一个纯代数的证明. 我们采用一个用代数最多, 而用分析最少的证明. 遗憾的是, 由于课时的限制, 我们不可能对超越扩张作深入的讨论, 甚至连 e, π 是超越数都未证明.

第 4 章讲述群的基本理论. 群论的应用日益广泛, 主要归功于变换群的理论, 也就是群在集合上的作用. 在这一章中, 我们用这种方法将一个群以不同方式作用在自身而得到群的许多性质, 如中心、共轭类、Sylow 子群的性质等. 此外, 这一章对有限单群、群扩展、群的直积、可解群与幂零群等也作了介绍. 这些内容在 Galois 理论以及更广泛的领域中都有重要地位. 4.9 节介绍了点群. 群总是某种对称性的表现, 如某些 Lie 群表现了 Riemann 对称空间与 Hermite 对称空间. 点群则是平面正多边形和空间正多面体的对称性的表现. 因此, 除在数学上的意义外, 在物理学和化学上也是很重要的.

第 5 章讲述模论. 模是两个代数体系的结合, 如线性空间是域与交换群的结合, 这是我们早已知道的一种模, 只不过没有使用 "模" 这个词罢了. 模的理论与语言在数学、物理学中运用得越来越普遍, 无疑它已是代数学基础的核心之一. 我们用模论的方法解决了有限生成 Abel 群的分类以及有限维线性空间的线性变换的分类与标准形的问题. 这是模应用的两个极好的例子.

第 6 章讨论 Galois 理论. 由于有限域在信息理论中有广泛的应用, 因此, 系统地介绍有限域是很必要的. 在分圆域之后讲有限域是很方便的, 因此, 将有限域放在这一

章. 本章主要是高次方程的根式解和圆规直尺作图两部分. 这是两个已经圆满解决了的问题, 但它们在历史上长期使许多数学家百思不得其解, 甚至千思却得错解. 只是等到数学家对数学的抽象性有了更进一步的了解, 从而提出诸如群、变换群等比以往更为抽象的概念之后, 这两个问题才迎刃而解. Galois 理论是 "抽象代数" 的开端, 也是它强大生命力最早的光辉例证. 只要寻本溯源, 我们就能深切地感受到这门既近世又古老的学科的无穷魅力, 因而在讨论了代数学的一些基础之后, 回头看看它的源头会更利于我们继续前进.

习题是本书不可忽略的重要组成部分. 华罗庚先生在维诺格拉陀夫的《数论基础》中译本的序中曾说, 如果读该书而不看、不做该书后面的问题, 无异于 "入宝山而空返". 由此可见习题在教材, 尤其是基础课教材中的重要性, 也可见做习题在学习基础课时的重要性. 本书编选的习题目的如下: 有利于掌握基础内容与方法; 适当拓广教材的内容; 初步的科学研究训练等.

这里要衷心感谢帮助过我们的所有老师和同学们, 同时要感谢所在单位对我们工作的大力支持, 没有这些支持, 本书的再版是不可能的.

虽然我们在这门课的教学中以及在编写本书的过程中都尽了很大努力, 但一则由于水平所限, 二则由于数学的教学总是在不断发展之中, 因此, 本书的缺欠和不足肯定存在, 诚恳希望大家不吝指正.

孟道骥

2009 年春于中国科学技术大学

目　录

第1章 基本概念

本书介绍代数学中群、环、域和模的基本概念和理论. 本章介绍群、环、域和模的最基本的概念, 这样在以后的叙述中比较方便.

在本书中, 分别以 **N**、**Z**、**Q**、**R** 和 **C** 表示自然数集、整数集、有理数集、实数集和复数集, **P** 表示一个数域.

"iff" 则如许多数学著作中习惯地表示 "if and only if", 即 "当且仅当" 之意.

1.1 二元运算与同余关系

代数学研究的对象是代数体系, 即具有一种或几种代数运算, 并满足一系列公理的集合. 那什么是代数运算呢? 这只有用集合与映射的语言才能准确地描述. 为此, 先介绍一下集合与映射等有关概念及术语.

如果集合 A 由某个性质 P 决定, 就记 $A=\{x|P(x)\}$.

设 A,B 是两个集合, 则称集合

$$A\times B=\{(x,y)|x\in A,y\in B\}$$

为 A 与 B 的**直乘积**, 或简称为**直积**.

类似地, 可以定义有限个集合的直乘积.

设 A,B 是两个集合, 若规定了法则 $f:\forall x\in A$, 有一 B 中元素 x' 与之对应, 则称 f 是 A 到 B 的一个**映射**. 记 $x'=f(x)$, 称为 x 在 f 下的**像**, 而称 x 为 x' 的一个**原像**.A 到 B 的映射 f 表示为 $f:A\to B$.

若 $A_0\subseteq A$, A_0 的元素在 f 下的像的集合记为

$$f(A_0)=\{f(x)|x\in A_0\}.$$

若 $B_0\subseteq B$, B_0 中元素所有原像的集合记为

$$f^{-1}(B_0)=\{x\in A|f(x)\in B_0\}.$$

特别地, 当 $B_0=\{y\}$ 为单点集时, $f^{-1}(y)=\{x\in A|f(x)=y\}$ 为 y 的所有原像的集合.

设 A, B, C 为三个集合. 如果有映射

$$f:A\to B,\quad g:B\to C.$$

那么, 可由等式

$$(gf)(x)=g(f(x)),\quad \forall x\in A \tag{1.1.1}$$

定义 A 到 C 的映射 gf. gf 称为映射 g 与 f 的**乘积**. 这时, 称图 1.1.1 为交换图.

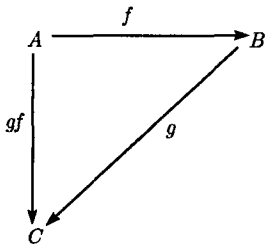

图 1.1.1

当然, 也可定义多个映射的乘积. 关于映射的乘法有下面重要的性质.

性质 1.1.1　映射的乘法满足**结合律**, 即若有 $f: A \to B$, $g: B \to C$, $h: C \to D$, 则有

$$h(gf) = (hg)f. \tag{1.1.2}$$

事实上, 对 $\forall x \in A$ 有

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

由结合律可知在多个映射相乘时, 可以不加括号. 特别地, $h(gf)$ 与 $(hg)f$ 均可简记作 hgf.

下述几种重要映射是以后经常要用到的.

映射 $f: A \to B$ 称为**一一映射**, 如果 B 中每个元素最多只有一个原像, 即对 $\forall y \in B, f^{-1}(y)$ 所含元素个数 $|f^{-1}(y)|$ 为 0 或 1(其中, $|C|$ 表示集合 C 的基数, C 为有限集时, 就是 C 中元素个数). 显然, f 为一一映射的充分必要条件是

$$f(x_1) = f(x_2) \text{ iff } x_1 = x_2,\ \forall x_1, x_2 \in A, \tag{1.1.3}$$

其中, "iff" 是 "if and only if" 的缩写, 是 "当且仅当" 的意思, 以后也这样使用.

映射 $f: A \to B$ 称为**满映射**, 或**A 到 B 上的映射**, 如果 $f(A) = B$, 亦即

$$f^{-1}(y) \neq \varnothing, \quad \forall y \in B. \tag{1.1.4}$$

若映射 $f: A \to B$ 既是一一映射又是满映射, 则称为**一一对应**.

设 f 是一一对应, 即对 $\forall y \in B$, 存在唯一的 $x \in A$, 使 $f(x) = y$. 这样就得到了 B 到 A 上的映射 f^{-1}:

$$f^{-1}(y) = x.$$

不难验证, f^{-1} 是 B 到 A 上的一一对应且

$$\begin{aligned}f(f^{-1}(y)) &= y, \quad \forall y \in B,\\ f^{-1}(f(x)) &= x, \quad \forall x \in A.\end{aligned}$$

由等式 $\mathrm{id}_A(x) = x (\forall x \in A)$ 所定义的映射 $\mathrm{id}_A: A \to A$ 称为 A 的**恒等映射**.

$f: A \to B$ 为一一对应的充要条件是存在 $g: B \to A$, 使

$$gf = \mathrm{id}_A, \quad fg = \mathrm{id}_B. \tag{1.1.5}$$

此时必有 $g = f^{-1}$, 即有二交换图, 如图 1.1.2 所示.

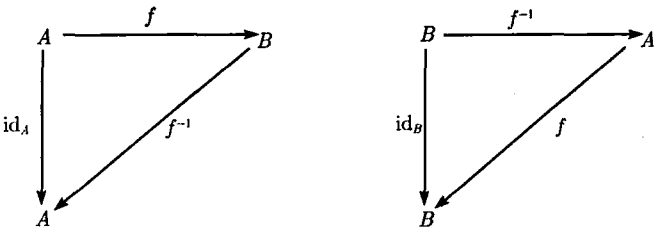

图 1.1.2

综上所述, 对于 A 到 B 上的一一对应 f, 存在唯一的 B 到 A 上的一一对应 f^{-1} 满足式 (1.1.5). 于是可将一一对应 f 称为**可逆映射**, 而将 f^{-1} 称为 f 的**逆映射**. 自然, f 也是 f^{-1} 的逆映射, 即

$$(f^{-1})^{-1} = f. \tag{1.1.6}$$

设 A_0 是集合 A 的子集. 由等式 $i(x) = x(\forall x \in A_0)$ 定义的映射 $i: A_0 \to A$ 称为 A_0 到 A 中的**嵌入映射**. 自然, 嵌入映射是一一的. 又若映射 $f: A_0 \to B$ 与映射 $g: A \to B$ 满足 $gi = f$, 即 $g(x) = f(x)(\forall x \in A_0)$, 则称 g 为 f 的**开拓**, f 为 g 在 A_0 上的**限制**, 记为 $f = g|_{A_0}$, 即图 1.1.3 为交换图.

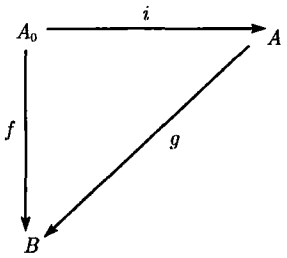

图 1.1.3

下面用集合与映射的语言来描述一个集合中的二元运算.

定义 1.1.1 设 A 是一个集合. $A \times A$ 到 A 的一个映射 φ, 称为 A 的一个**二元运算**.

若记 $\varphi(a,b) = ab$, 则称 ab 为 a 与 b 的**积**. 若记 $\varphi(a,b) = a+b$, 则称 $a+b$ 为 a 与 b 的**和**.

若 A 上的二元运算 $\varphi(a,b) = ab$ 满足结合律

$$(ab)c = a(bc), \quad \forall a,b,c \in A,$$

则此二元运算称为**结合的**.

若 A 上的二元运算 $\varphi(a,b) = ab$ 满足交换律

$$ab = ba, \quad \forall a,b \in A,$$

则此二元运算称为**交换的**. 一般地, 若 $c,d \in A$ 有 $cd = dc$, 则称 c 与 d 是**交换的**.

其实对我们来说二元运算并不陌生. 例如, 数域中的加法与乘法运算都是满足交换律与结合律的二元运算, 而数域中的减法与非零数间的除法运算则是既不满足交换律也不满足结合律的二元运算. 一个数域上的 $n(n \geqslant 2)$ 阶方阵集合中矩阵乘法则是一

个只满足结合律, 而不满足交换律的二元运算. 又如, 实数集 $\mathbf{R}$ 中由 $\mathbf{R}\times\mathbf{R}$ 到 $\mathbf{R}$ 的映射 $(a,b)\to|a-b|$ 定义了一个满足交换律, 但不满足结合律的二元运算.

设集合 A 有二元运算 $(a,b)\to ab$ 且满足结合律, 则对 $\forall n\in\mathbf{N}$($\mathbf{N}$ 表示自然数, 即正整数的集合), 定义

$$a^1=a,\quad a^{n+1}=a^n\cdot a,\quad \forall a\in A,$$

a^n 称为 a 的 n 次**乘幂**, 也简称 n 次幂.

显然, $a^na^m=a^{n+m}$, $(a^m)^n=a^{nm}(\forall a\in A,\ m,n\in\mathbf{N})$. 又若 $a,b\in A$ 且 $ab=ba$, 则 $(ab)^n=a^nb^n(\forall n\in\mathbf{N})$.

此外, 在 A 中也可以定义连乘积

$$\prod_{i=1}^{n}a_i=\left(\prod_{i=1}^{n-1}a_i\right)a_n,\quad a_i\in A,\ i=1,2,\cdots,n.$$

容易证明若有

$$0=n_0<n_1<\cdots<n_r=n,$$

则

$$\prod_{j=1}^{r}\left(\prod_{k=n_{j-1}+1}^{n_j}a_k\right)=\prod_{i=1}^{n}a_i.$$

如果将二元运算记为加法且满足结合律, 于是可定义倍数与连加如下:

$$1\cdot a=a,\quad (n+1)a=na+a,$$

$$\sum_{i=1}^{n}a_i=\left(\sum_{i=1}^{n-1}a_i\right)+a_n.$$

同样有如下与乘法类似的结果:

$$na+ma=(n+m)a,\ n(ma)=(nm)a,\quad \forall a\in A,\ m,n\in\mathbf{N}.$$

若 $a+b=b+a$, 则

$$n(a+b)=na+nb,\quad \forall n\in\mathbf{N},$$

$$\sum_{j=1}^{r}\left(\sum_{k=n_{j-1}+1}^{n_j}a_k\right)=\sum_{i=1}^{n}a_i.$$

为介绍有二元运算的集合 A 的一种重要关系即同余关系, 先讨论一下等价关系.

所谓在集合 A 中定义了二元素间的一个**关系** R, 也就是给出了集合 $A\times A$ 中元素的一个性质 R, 若 $a,b\in A$, (a,b) 有性质 R, 则称 A 与 B 有关系 R, 记为 aRb.

事实上, 集合 A 中关系 R 可由 $A\times A$ 中子集

$$\{(a,b)|a,b\in A,aRb\}$$

来刻画.

反之, 由 $A\times A$ 的一个子集 R, 也可确定 A 一个关系 R : aRb, 若 $(a,b)\in R$.

定义 1.1.2 集合 A 中关系若满足以下条件：

1) **自反性** $aRa, \forall a \in A$;

2) **对称性** 若 aRb, 则 bRa;

3) **传递性** 若 aRb, bRc, 则 aRc,

则称 R 为 A 的一个**等价关系**.

若仍以 R 表示 A 中关系所确定的 $A \times A$ 的子集, 则 R 为等价关系当且仅当下列三个条件同时成立：

1′) $(a,a) \in R, \forall a \in A$;

2′) 若 $(a,b) \in R$, 则 $(b,a) \in R$;

3′) 若 $(a,b) \in R$, $(b,c) \in R$, 则 $(a,c) \in R$.

注意, 在等价关系定义中的三个条件是互相独立的.

例如, 在实数域 $\mathbf{R}$ 中定义关系 R 为

$$aRb \quad \text{iff} \quad ab \neq 0,$$

则 R 满足定义 1.1.2 中条件 2) 与 3), 但不满足条件 1). 此时, $\mathbf{R} \times \mathbf{R}$ 中与 R 对应的子集为 $\{(a,b)|a,b \in \mathbf{R},\ ab \neq 0\}$.

若 R 是集合 A 的一个等价关系且 $a \in A$, 则 A 中所有与 a 有关系 R 的元素集合

$$K_a = \{b \in A | bRa\}$$

称为 a 所在的**等价类** , a 称为这个等价类的**代表元素**.

与等价关系密切相关的概念是集合的**分划**. 集合 A 的一个子集族 $\{A_\alpha\}$ 称为 A 的一个分划, 如果满足

$$A = \bigcup_\alpha A_\alpha, \quad A_\alpha \bigcap A_\beta = \varnothing, \quad \text{若 } \alpha \neq \beta.$$

也称 A 是 $\{A_\alpha\}$ 中所有不相交的集合的并.

定理 1.1.1 设 R 是集合 A 的等价关系, 则由所有不同的等价类构成的子集族 $\{K_a\}$ 是 A 的分划. 反之, 若 $\{A_a\}$ 是 A 的分划, 则可在 A 中定义等价关系, 使得每个 A_a 是一等价类.

证 设 R 是 A 的等价关系. 由 $\forall a \in A$, aRa 知 $a \in K_a$, 于是 $A = \bigcup\limits_a K_a$. 设 $K_a \cap K_b \neq \varnothing$, 即 $\exists c \in K_a \cap K_b$, 对 $\forall x \in K_a$ 有 cRa, xRa, 因而 xRc. 又 cRb, 故 xRb, 即 $x \in K_b$, 从而得 $K_a \subseteq K_b$. 同样可得 $K_b \subseteq K_a$, 故 $K_a = K_b$, 亦即若 $K_a \neq K_b$, 则 $K_a \cap K_b = \varnothing$. 这样就证明了 $\{K_a\}$ 是 A 的分划.

反之, 设 $\{A_\alpha\}$ 是 A 的一个分划. 在 A 中定义关系 R,

$$aRb, \quad \text{若 } \exists A_\alpha, \text{使 } a,b \in A_\alpha.$$

因 $A=\bigcup\limits_{\alpha}A_\alpha$, 故对 $\forall a\in A$, $\exists A_\alpha$, 使 $a\in A_\alpha$, 因此 $a,a\in A_\alpha$, 即 aRa. 其次, 若 aRb, 即 $\exists A_\alpha$, 使 $a,b\in A_\alpha$. 自然 $b,a\in A_\alpha$, 故 bRa. 再次, 若 aRb, bRc, 即有 A_α, A_β, 使 $a,b\in A_\alpha$ 且 $b,c\in A_\beta$, 故 $b\in A_\alpha\cap A_\beta$. 由 $\{A_\alpha\}$ 为 A 的分划知 $A_\alpha=A_\beta$, 因而 aRc. 这样就证明了 R 是等价关系. 由 R 的定义知若 $a\in A_\alpha$, 则 $K_a=A_\alpha$. ∎

定义 1.1.3　设 R 是集合 A 的等价关系. 以关于 R 的等价类为元素的集合 $\{K_a\}$ 称为 A 对 R 的**商集合**. 记为 A/R. 由

$$\pi(a)=K_a,\quad \forall a\in A \tag{1.1.7}$$

定义的 A 到 A/R 上的映射 π 称为 A 到 A/R 上的**自然映射**.

反之, 如果从集合 A 到集合 B 有一个满映射, 则在 A 中也可定义一个等价关系.

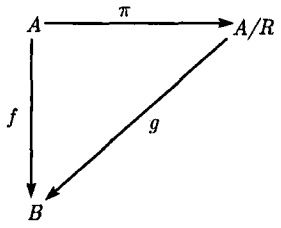

图 1.1.4

定理 1.1.2　设 $f:A\to B$ 是满映射. 在 A 中定义关系 R,

$$aRb,\quad 若\ f(a)=f(b),$$

则 R 是 A 的等价关系. 又设 $\pi:A\to A/R$ 为自然映射, 则有 A/R 到 B 上的一一对应 g 满足

$$g\pi=f, \tag{1.1.8}$$

即图 1.1.4 是交换图.

证　考虑 $y\in B$ 的原像 $f^{-1}(y)$ 构成的子集族. 显然, $A=\bigcup\limits_{y\in B}f^{-1}(y)$. 又若 $y,z\in B$, 而 $f^{-1}(y)\cap f^{-1}(z)\neq\varnothing$, 即 $\exists a\in A$, 使 $f(a)=y$, $f(a)=z$, 即 $y=z$. 故 $f^{-1}(y)=f^{-1}(z)$, 从而 $\{f^{-1}(y)\}$ 是 A 的一个分划. 于是在 A 中可定义等价关系 $R:aRb$, 若 $\exists f^{-1}(y)$, 使 $a,b\in f^{-1}(y)$, 即 $f(a)=f(b)$. 由此知定理的第一部分成立.

A 中元素 a 所在等价类 $K_a=f^{-1}(f(a))$. 由于 $K_a=K_b$ 当且仅当 $f(a)=f(b)$, 因而由

$$g(K_a)=f(a),\quad \forall a\in A$$

定义了 A/R 到 B 的映射 g. 因 $f(A)=B$, 故 g 是一一对应. 由 π 的定义知式 (1.1.8) 成立. ∎

现在介绍本节最后一个重要概念.

定义 1.1.4　设集合中 A 的二元运算, 记作乘法. 若 A 的一个等价关系 $\sim$ 满足

$$若\ a\sim b,\ c\sim d,\ 则\ ac\sim bd,\forall a,b,c,d\in A, \tag{1.1.9}$$

则称 $\sim$ 为 A 的一个**同余关系**. $a\in A$ 的等价类 K_a 此时也称为 a 的**同余类**.

例 1.1.1 设 $m \in \mathbf{Z}$(所有整数的集合), $m \neq 0$. 在 $\mathbf{Z}$ 中定义关系

$$a \sim b, \quad \text{若 } a \equiv b(\mathrm{mod}\, m).$$

易证 $\sim$ 是等价关系且由 $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$ 可得 $a+c \equiv b+d(\mathrm{mod}\, m)$, $ac \equiv bd(\mathrm{mod}\, m)$. 因而 $\sim$ 对于 $\mathbf{Z}$ 中的加法与乘法都是同余关系.

例 1.1.2 设 $\mathbf{P}[x]$ 是数域 $\mathbf{P}$ 上一元多项式的集合. 设 $f(x) \in \mathbf{P}[x]$, $f(x) \neq 0$. 在 $\mathbf{P}[x]$ 中定义关系 $\sim$: $g(x) \sim h(x)$, 若 $f(x) | (g(x)-h(x))$. 与例 1.1.1 类似可证 $\sim$ 对 $\mathbf{P}[x]$ 中的加法与乘法都是同余关系.

例 1.1.3 以 $\mathbf{P}^{n\times n}$ 表示数域 $\mathbf{P}$ 上所有 n 阶方阵的集合. 方阵的加法与乘法都是 $\mathbf{P}^{n\times n}$ 中的二元运算. 对 $\boldsymbol{A} \in \mathbf{P}^{n\times n}$, 用 $\mathrm{ent}_{ij}\boldsymbol{A}$, $\mathrm{row}_i\boldsymbol{A}$, $\mathrm{col}_j\boldsymbol{A}$ 和 $\det \boldsymbol{A}$ 分别表示 $\boldsymbol{A}$ 的第 i 行第 j 列元素、$\boldsymbol{A}$ 的第 i 行、$\boldsymbol{A}$ 的第 j 列和 $\boldsymbol{A}$ 的行列式.

$\mathbf{P}^{n\times n}$ 中由 $\det \boldsymbol{A} = \det \boldsymbol{B}$ 确定的关系, 对乘法是同余关系, 但对加法除 $n=1$ 的情形外不是同余关系.

$\mathbf{P}^{n\times n}$ 中由 $\mathrm{col}_1\boldsymbol{A} = \mathrm{col}_1\boldsymbol{B}$ 确定的关系, 对加法是同余关系, 但对乘法除 $n=1$ 的情形外不是同余关系.

定理 1.1.3 设集合 A 有二元运算乘法, $\sim$ 是 A 的一个同余关系. 又 π: $A \to A/\sim$ 是自然映射, 则在商集合 $A/\sim$ 中可定义二元运算

$$\pi(a)\pi(b) = \pi(ab), \quad \forall a, b \in A. \tag{1.1.10}$$

证 只需证由 $\pi(a) = \pi(a_1)$, $\pi(b) = \pi(b_1)$ 可得 $\pi(ab) = \pi(a_1b_1)$, 其中, $a, b, a_1, b_1 \in A$. 事实上, 由 π 的定义知 $\pi(a) = \pi(a_1)$, 即 $a \sim a_1$, $\pi(b) = \pi(b_1)$, 即 $b \sim b_1$. 因 $\sim$ 是同余关系, 故 $ab \sim a_1b_1$, 所以 $\pi(ab) = \pi(a_1b_1)$. ∎

习 题 1.1

1. 试问下列关系是否为等价关系, 并验证:

1) 在 $\mathbf{R}$ 中, $x\,R\,y$, 若 $x \geqslant y$;

2) 在 $\mathbf{R}$ 中, $x\,R\,y$, 若 $|x| = |y|$;

3) 在 $\mathbf{R}$ 中, $x\,R\,y$, 若 $|x-y| \leqslant 3$;

4) 在 $\mathbf{Z}$ 中, $x\,R\,y$, 若 $x-y$ 为奇数;

5) 在 $\mathbf{C}^{n\times n}$(复数域 $\mathbf{C}$ 上 n 阶方阵的集合) 中, $\boldsymbol{A}\,R\,\boldsymbol{B}$, 若有可逆矩阵 $\boldsymbol{P}, \boldsymbol{Q}$, 使 $\boldsymbol{A} = \boldsymbol{PBQ}$;

6) 在 $\mathbf{C}^{n\times n}$ 中, $\boldsymbol{A}\,R\,\boldsymbol{B}$, 若有矩阵 $\boldsymbol{P}, \boldsymbol{Q}$, 使 $\boldsymbol{A} = \boldsymbol{PBQ}$;

7) 在 $\mathbf{C}^{n\times n}$ 中, $\boldsymbol{A}\,R\,\boldsymbol{B}$, 若有可逆矩阵 $\boldsymbol{P}$, 使 $\boldsymbol{A} = \boldsymbol{P}^{-1}\boldsymbol{BP}$.

2. 假设 R 是非空集合 A 中的一个关系, 并且有对称性和传递性. 有人断定 R 是一个等价关系, 其推理如下:

"对 $a, b \in A$, 从 $a\,R\,b$ 得 $b\,R\,a$, 又从传递性得 $a\,R\,a$, 因而 R 有自反性, 故为等价关系."

他的推理对吗?

3. 设 R 是非空集合 A 中任一关系, 再定义 A 中关系 R_1, R_2 分别为

$$x R_1 y, \text{ 当 } x = y, \ x\,R\,y \text{ 与 } y\,R\,x \text{ 三者之一成立;}$$

$x\,R_2\,y$, 若有 $x_0, x_1, \cdots, x_n$, 使 $x_0 = x$, $x_n = y$ 且

$$x_0\,R_1\,x_1,\ x_1\,R_1\,x_2,\ \cdots,\ x_{n-1}\,R_1\,x_n.$$

1) 证明 R_2 是一个等价关系;

2) 证明若 R 是等价关系, 则 $R_2 = R$, 即 $x\,R_2\,y$ iff $x\,R\,y$;

3) 令 $A = \mathbf{Z}$, n 为一固定整数, R 定义为 $x\,R\,y$, 当 $x - y = n$. 求关系 R_1 与 R_2.

4. 试问下面的二元运算 $*$ 哪些满足交换律, 哪些满足结合律:

1) 在 $\mathbf{Z}$ 中, $a * b = a - b$;

2) 在 $\mathbf{Q}$(有理数的集合) 中, $a * b = ab + 1$;

3) 在 $\mathbf{Q}$ 中, $a * b = ab/2$;

4) 在 $\mathbf{N}$ 中, $a * b = 2^{ab}$;

5) 在 $\mathbf{N}$ 中, $a * b = a^b$.

5. 设 $m \in \mathbf{Z}$, $m \neq 0$. 在 $\mathbf{Z}$ 中定义关系 $\sim$,

$$a \sim b, \quad 若\ a \equiv b (\mathrm{mod}\, m).$$

将对此关系的商集合记为 $\mathbf{Z}_m$(或 $\mathbf{Z}/m\mathbf{Z}$). 试求:

1) $\mathbf{Z}_m$ 中元素个数;

2) 由 $\mathbf{Z}$ 导出的 $\mathbf{Z}_3$ 的加法和乘法;

3) 由 $\mathbf{Z}$ 导出的 $\mathbf{Z}_6$ 的加法和乘法.

1.2　幺半群　群

无论是人类对数学认识的历史, 或个人学习数学的历史, 首先是从自然数集 $\mathbf{N}$ 及其加法运算开始的, 也就是从有一种二元运算的代数体系开始的. 其实, 我们所了解的有一种二元运算的代数体系俯拾皆是. 例如, 线性空间的可逆线性变换集合对于线性变换的乘法; Euclid 空间的正交变换集对于乘法; 一般地, 一个集合的变换 (即此集合对自身的映射) 的集合对变换的乘法等. 因而给这种代数体系以较系统的描述很有必要. 为此, 引进群的概念. 顺便也给出半群与幺半群的概念.

定义 1.2.1　设 S 是非空集合. 在 S 中定义了二元运算称为乘法, 满足结合律, 即

$$(ab)c = a(bc), \quad \forall a, b, c \in S, \tag{1.2.1}$$

则称 S 为**半群**.

如果在半群 M 中存在元素 1, 使得

$$1\,a = a\,1 = a, \quad \forall a \in M, \tag{1.2.2}$$

则称 M 为**幺半群**, 1 称为**幺元素或幺元**.

如果一个幺半群 M(或半群 S) 的乘法还满足交换律, 即

$$ab = ba, \quad \forall a, b \in M\ (\text{或}\ S), \tag{1.2.3}$$