近世代数

唐高华 主编

清华大学出版社

近世代数

主编　唐高华

编著　唐高华　邓培民　王芳贵
　　任北上　赵巨涛　杨立英

清华大学出版社
北京

内容简介

本书较系统地介绍了群、环、域的基本概念和基本性质. 全书共分 3 章，第 1 章介绍群的基本概念和性质，除了通常的群、子群、正规子群、商群和群的同态基本定理外，还介绍了对称与群、群的直积、有限 Abel 群的结构定理等内容；第 2 章讲述了环、子环、理想与商环、环的同态等基本概念和性质，讨论了整环及整环上的多项式环的性质和应用；第 3 章讨论了域的扩张理论及其在几何作图中的应用. 本书附有相当丰富的习题，有利于读者学习和巩固所学知识.

本书可作为师范院校数学与应用数学专业本科生的教材，也可作为其他院校数学系本科生的教材和参考书，亦可作为其他数学爱好者和工程技术人员的参考书.

图书在版编目(CIP)数据

近世代数/唐高华主编；邓培民等编著. —北京：清华大学出版社，2008. 12
ISBN 978-7-302-18774-5

Ⅰ. 近…　Ⅱ. ①唐… ②邓…　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(2008)第 161815 号

责任编辑：刘　颖
责任校对：赵丽敏
责任印制：孟凡玉
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京四季青印刷厂
装 订 者：三河市李旗庄少明装订厂
经　　销：全国新华书店
开　　本：185×230　**印　张**：10.75　**字　数**：230 千字
版　　次：2008 年 12 月第 1 版　　**印　　次**：2008 年 12 月第1 次印刷
印　　数：1～4000
定　　价：18.00 元

广西师范学院教材建设基金资助出版

FOREWORD 前言

进入21世纪以来，我国基础教育改革在全国各地蓬勃开展，新一轮的课程改革对中学数学教师提出了诸多新的要求.作为师范院校，如何应对新的课程改革，为中学培养合格的优秀教师，是摆在我们面前的紧迫问题.近年来，我们开展了有关高等师范院校数学与应用数学专业课程体系与课程内容改革的研究，这本《近世代数》教材就是该项目研究的成果之一.

近世代数(又名抽象代数)，是以讨论代数系统的性质和结构为中心的一门学科.它是现代科学各个分支的基础，而且随着科学技术的不断进步，特别是计算机的飞速发展，近世代数的思想、理论与方法的应用日臻广泛，现已渗透到科学领域的各个方面与实际应用的各个部门.

近世代数是现代数学的重要基础，近世代数课程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须具备的数学素养之一.我们希望读者通过本课程的学习，能理解和掌握近世代数的基本内容、理论和方法，初步具备用近世代数的思想和理论处理和解决具体问题的能力，为进一步学习后续课程或从事中学数学教学打下坚实的基础.

在编写过程中，笔者吸取了多年的教学实践经验及同类教材的许多优秀成果，同时融入了笔者最新的教改研究成果.初稿完成后，在广西师范学院和广西师范大学试用，并经反复修改、完善.本教材有以下特点：

1. 为了适应高中新课程改革的需要，本教材在内容上除了介绍本课程的传统内容外，还增加了对称与群、多项式的应用、尺规作图等与新的高中课程标准相应模块联系紧密的内容.

2. 结合教材内容，我们介绍了有关的历史回顾和有关数学家的生平，将数学文化与数学美渗透到教材中，以提高读者的学习兴趣，并拓展视野，培养数学素养.

3. 书中尽可能地避免“定义—性质—定理”这一刻板的教材编写模式，尽可能地用一些易于理解的例子来引出一个新的概念和结论，并且用尽可能多的例子来说明新的概念和结

论的意义和应用.

4. 在教材中渗透了现代数学对中学数学教学的指导作用,使读者能意识到学好该门课程对当好中学数学教师的重要意义,对中学数学教学内容有更全面的认识.

5. 在教材中渗透了数学建模的思想和例子,从而使读者感受到抽象数学的力量,提高学习抽象数学的兴趣.

本书是我们这个团队共同策划、分工协作的成果. 在反复研讨的基础上,唐高华、任北上、赵巨涛编写了第 1 章,唐高华、邓培民编写了第 2 章,王芳贵、杨立英编写了第 3 章,最后由唐高华统稿、杨立英审校而成.

本教材的编写得到广西新世纪教改工程项目、广西教育科学“十五”规划项目、广西高校精品课程建设项目和广西师范学院教材出版基金等的资助. 在编写过程中,还得到了编者单位(广西师范学院)院系领导、广大师生和清华大学出版社的大力支持和同行专家的关心,苏华东、韦扬江、高艳艳、林光科、仇翠敏等研究生和本科生帮助进行了录入和校对,谨此致谢.

限于作者水平,书中难免有错漏和不妥之处,我们恳切希望使用本书的教师和读者予以指正.

作　者

2008 年 7 月

CONTENTS 目录

第1章 群

近世代数研究的主要对象是具有代数运算的集合，即*代数系统*(algebraic system). 群就是具有一个代数运算的代数系统. 具有悠久历史的群理论，现在已发展成为一门范围广泛和内容十分丰富的数学分支，不仅在近代数学中占有重要的地位，而且在数学的其他分支乃至物理学、化学、信息科学等许多领域中都有着广泛的应用.

本章除了介绍群的定义、例子、基本性质和一些特殊群类外，我们还从子群的陪集入手，讨论了正规子群和商群，进而对群论的基本内容——群同态基本定理给予了证明. 为了扩大读者的视野，作为选修内容，本章最后介绍了群的直积和有限 Abel 群的结构定理等.

1.1 预备知识

本节主要对以后各章都要用到的基础知识作简单的介绍. 它们是：集合、映射、代数运算、运算律、代数系统、等价关系与集合的分类等.

1. 集合

具有某种特定性质的元素的全体称为集合(set)，或简称为集.

今后常用$\mathbb{N}$表示自然数集(the set of natural numbers)，$\mathbb{Z}$表示整数集(the set of integers)，$\mathbb{Q}$表示有理数集(the set of rational numbers)，$\mathbb{R}$表示实数集(the set of real numbers)，$\mathbb{C}$表示复数集(the set of complex numbers)，而$\varnothing$表示空集(empty set).

我们用"$x\in A$"表示元素 x 属于集 A，用"$x\notin A$"表示元素 x 不属于集 A.

定义 1.1.1 如果集 A 中的每个元素都属于集 B，则称 A 是 B 的一个子集(subset)并记为 $A\subseteq B$，否则记为 $A\not\subset B$. 如果 $A\subseteq B$，又 B 中至少有一个元素不在 A 中，则称 A 是 B 的一个真子集(proper subset)，记为 $A\subset B$.

空集被认为是任意集合的子集.

一个简单却极为重要的事实是：$A=B\Leftrightarrow A\subseteq B$ 且 $B\subseteq A$. 所以，要说明两个集合 A 与 B 相等，只要证明 A 与 B 相互包含.

定义 1.1.2 集 A 和集 B 的所有公共元素组成的集合，记为 $A\cap B=\{x\mid x\in A$ 且 $x\in B\}$，叫做 A 与 B 的交集，简称 A 与 B 的交(intersection). 由属于集 A 或集 B 的所有元素组成的集合，记为 $A\cup B=\{x\mid x\in A$ 或 $x\in B\}$，叫做 A 与 B 的并集，简称 A 与 B 的并(union).

对于两个以上甚至无穷多个集合，也可以类似地定义集合的交与并.

定义 1.1.3 设 A,B 为两个非空集合，称集合

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

为 A 与 B 的笛卡儿积(Cartesian product).

类似地可以定义有限个非空集的笛卡儿积：

$$A_1\times A_2\times\cdots\times A_m=\{(a_1,a_2,\cdots,a_m)\mid a_i\in A_i,i=1,2,\cdots,m\}.$$

注意：一般地，$A\times B\neq B\times A$.

2. 映射与变换

映射和变换都是函数概念的推广，它们描述了两个集合的元素之间的关系，是数学中最基本的工具之一，以此来研究代数系统是近世代数中最重要的方法之一.

定义 1.1.4 设 A,B 为两个非空集，如果存在一个从 A 到 B 的对应法则 f，使得对 A 中每个元素 a，都有 B 中唯一确定的一个元素 b 与之对应，则称 f 是 A 到 B 的一个映射(mapping). 习惯上称 b 为 a 的像(image)，称 a 为 b 的逆像(inverse image or preimage)，而 A 叫做映射 f 的定义域(domain)，B 叫做 f 的值域(codomain).

注意：通常用记号 $f:A\to B$ 或 $A\xrightarrow{f}B$ 表示 f 是 A 到 B 的映射.

例 1.1.1 对应法则 $f:x\mapsto\dfrac{1}{x-1}$ 即 $f(x)=\dfrac{1}{x-1}(\forall x\in\mathbb{Q})$ 不是 $\mathbb{Q}$ 到 $\mathbb{R}$ 的映射，因为有理数 1 没有像.

例 1.1.2 设 g 为 $\mathbb{Q}$ 到 $\mathbb{Q}$ 的对应法则，其中

$$g:\frac{x}{y}\mapsto x+y,\quad \text{即 } g\left(\frac{x}{y}\right)=x+y,\quad \forall\ \frac{x}{y}\in\mathbb{Q},$$

那么 g 不是 $\mathbb{Q}$ 到 $\mathbb{Q}$ 的映射. 因为对于 $\dfrac{2}{4}=\dfrac{4}{8}$，却有 $g\left(\dfrac{2}{4}\right)=6,g\left(\dfrac{4}{8}\right)=12$，即 $\mathbb{Q}$ 中相同的元素的像却不相同.

从上面的例子可知：集 A 到集 B 的对应法则 f 要成为映射，必须满足：

(1) 在 f 之下 A 中的每个元素在 B 中必须有像.

(2) A 中相等元素的像也必须相等，即 A 中每个元素的像必唯一.

例 1.1.3 设 $A=\mathbb{R}^+=\{x\mid x\in\mathbb{R},x>0\},B=\mathbb{R}$，则对应法则

$$f:x\mapsto\sqrt{x},\quad \forall x\in\mathbb{R}^+$$

是 $\mathbb{R}^+$ 到 $\mathbb{R}$ 的一个映射.

例 1.1.4 设 A 为非空集合，则对应法则

$$I_A:x\mapsto x,\quad \forall x\in A$$

是映射. 习惯上称 I_A 为 A 的恒等映射(identity mapping).

定义 1.1.5 设 $f:A\to B$ 是映射.

(1) 若 $S\subseteq A$，则 B 的子集

$$\{f(x)\mid x\in S\}$$

称为 S 在 f 下的像，记作 $f(S)$. 特别地，当 $S=A$ 时，$f(A)$ 称为映射 f 的像，记作 $\mathrm{Im}f$.

(2) 若 $T\subseteq B$，则 A 的子集

$$\{x\in A\mid f(x)\in T\}$$

称为 T 在 f 下的逆像，记作 $f^{-1}(T)$.

注意：$f^{-1}(T)$ 只是一个 A 的子集的符号，这里并不意味着映射 f 可逆.

定义 1.1.6 设 $f:A\to B, g:C\to D$，如果 $A=C, B=D$，且 $\forall x\in A$，都有 $f(x)=g(x)$，则称 f 与 g 相等，记为 $f=g$.

定义 1.1.7 设 $f:A\to B$ 是映射.

(1) 若 $\forall x_1, x_2\in A, x_1\neq x_2$ 均有 $f(x_1)\neq f(x_2)$，则称 f 为单射(injection)；

(2) 若 $\forall y\in B$，均有 $x\in A$ 使 $y=f(x)$，则称 f 为满射(surjection)；

(3) 若 f 既是单射又是满射，则称 f 为双射(bijection).

例 1.1.3 的映射是单射，但不是满射. 例 1.1.4 的映射是双射.

定义 1.1.8 集合 A 到 A 自身的映射叫做 A 的一个变换(transformation).

很明显，当 A 为有限集时，映射 $f:A\to A$ 是单射的充要条件为 f 是满射. 这时 A 上的变换通常用“列表法”表示. 譬如，设 $A=\{1,2,3\}$，定义 A 上的变换

$$f:1\mapsto 3, 2\mapsto 1, 3\mapsto 2,$$

那么 f 可表示为 $f=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$.

一般地，集 $A=\{1,2,\cdots,n\}$ 上的变换 f 均可表为

$$f=\begin{pmatrix}1 & 2 & 3 & \cdots & n\\ f(1) & f(2) & f(3) & \cdots & f(n)\end{pmatrix}.$$

类似于复合函数的概念，我们给出两个映射的合成的概念.

定义 1.1.9 设 A, B 和 C 均为非空集合，而 $f:A\to B, g:B\to C$ 都是映射，那么由 f 和 g 可确定一个从 A 到 C 的映射 $h:A\to C$，其中

$$h(x)=g(f(x)),\quad \forall x\in A,$$

称 h 是 f 与 g 的合成(composition)，记作 $h=gf$.

很显然，如果 $f:A\to B$，那么 $fI_A=f, I_Bf=f$.

类似于反函数，对于双射而言，我们可以引入逆映射的概念.

定义 1.1.10 设 $f:A\to B$ 为双射，那么由 f 可确定另一个映射 $h:B\to A$，其中

$$h:b\to a,\quad \text{如果 } f(a)=b,\quad \forall b\in B,$$

称 h 为 f 的逆映射(inverse mapping)，记为 f^{-1}.

很容易验证下列的结论：如果 $f:A\to B$ 为双射，则

(1) $f^{-1}:B\to A$ 也是双射且 $(f^{-1})^{-1}=f$.

(2) $ff^{-1}=I_B, f^{-1}f=I_A$.

(3) f^{-1} 是唯一的.

3. 代数运算

前已述及，近世代数的主要任务是研究各种抽象的代数系统. 而代数系统与代数运算有着密切的联系，下面介绍代数运算以及一些常用的运算律.

定义 1.1.11 设 A,B,D 都是非空集合，从 $A\times B$ 到 D 的映射就称为 A,B 到 D 的*代数运算*(algebraic operation). 特别地，当 $A=B=D$ 时，A,A 到 A 的代数运算简称为 A 上的代数运算，或称*二元运算*(binary operation)，具有代数运算的集合 A 就称为*代数系统*.

若 A 是一个代数系统，通常也说 A 关于它的代数运算封闭.

一个代数系统 A 上的代数运算可以用"$\circ$"来表示，并将 (a,b) 在 $\circ$ 下的像记作 $a\circ b$，此时 A 可以记为 $(A,\circ)$.

例 1.1.5 设 $\mathbb{Z}^*=\{x\in\mathbb{Z}\mid x\neq 0\}$，一个 $\mathbb{Z}\times\mathbb{Z}^*$ 到 $\mathbb{Q}$ 的映射：

$$\circ:(a,b)\mapsto a\circ b=\frac{a}{b}$$

就是 $\mathbb{Z},\mathbb{Z}^*$ 到 $\mathbb{Q}$ 的代数运算. 这就是普通数的除法.

例 1.1.6 一个 $\mathbb{Z}\times\mathbb{Z}$ 到 $\mathbb{Z}$ 的映射：

$$\circ:(a,b)\mapsto a\circ b=a-b$$

就是整数集 $\mathbb{Z}$ 上的减法.

可以看出，代数运算就是通常的四则运算在最一般的情况下的一种自然推广. 譬如，通常的加法、减法和乘法都是整数集 $\mathbb{Z}$、有理数集 $\mathbb{Q}$、实数集 $\mathbb{R}$ 和复数集 $\mathbb{C}$ 上的代数运算.

例 1.1.7 通常的减法不是自然数集 $\mathbb{N}$ 上的代数运算，因为 $1-3=-2$，而 -2 不是自然数. 类似地，通常除法 $a\circ b=\dfrac{a}{b}$ 也不是有理数集 $\mathbb{Q}$ 上的代数运算，因为 $(a,0)\mapsto a\circ 0=\dfrac{a}{0}$ 无意义.

当 A,B 都为有限集时，A,B 到 D 的代数运算通常可用一个矩形表给出. 譬如，设 $A=\{a_1,a_2,\cdots,a_n\}$，$B=\{b_1,b_2,\cdots,b_m\}$，则 A,B 到 D 的代数运算 $a_i\circ b_j=d_{ij}$ 可以表示为

	b_1	b_2	$\cdots$	b_m
a_1	d_{11}	d_{12}	$\cdots$	d_{1m}
a_2	d_{21}	d_{22}	$\cdots$	d_{2m}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
a_n	d_{n1}	d_{n2}	$\cdots$	d_{nm}

这个表通常称为*运算表*或*凯莱表*(Cayley table). 在运算表中由 d_{11} 到 d_{nm} 形成的线称为主对角线.

代数学研究的是对代数运算加以某些限制的代数系统. 其实，数、多项式、矩阵、函数等的普通运算，一般地都满足通常所熟悉的一些运算规则，诸如结合律、交换律和分配律等. 近世代数在研究各种代数系统时，也不能脱离这些运算律.

定义 1.1.12 设 $\circ$ 为集合 A 上的一个代数运算，若 $\forall\, a_1,a_2,a_3\in A$，都有

$$(a_1 \circ a_2) \circ a_3 = a_1 \circ (a_2 \circ a_3),$$

则称$\circ$适合结合律(associative law).

定理 1.1.1 设集合 A 上的代数运算$\circ$适合结合律,则对于 A 中任意 $n(n\geqslant 3)$ 个元素 $a_1, a_2, \cdots, a_n$,只要不改变元素的排列顺序,任意一种加括号方法计算所得的结果都相等. □

根据这个定理,对于满足结合律的代数运算来说,任意 n 个元素只要不改变元素的前后次序,就可以随意结合而不必再加括号.这一结论在中学数学中,而且在高等代数或其他课程中都运用过,譬如数、多项式、矩阵和线性变换的通常加法及乘法都可以任意结合而不必加括号.这就说明,近世代数所讨论的代数系统具有抽象性,进而决定了它更具有广泛的适用性.

在代数系统$(A,\circ)$中,对于 A 中两个元素 a, b 而言,$a\circ b$ 不一定等于 $b\circ a$,比如例 1.1.5 和例 1.1.6.下面讨论代数运算适合交换律的问题.

定义 1.1.13 设$\circ$为集合 A 上的一个代数运算,若 $\forall a, b\in A$,都有

$$a \circ b = b \circ a,$$

则称$\circ$适合交换律(commutative law).

有限集合 A 上的代数运算$\circ$满足交换律的充要条件是其运算表中关于主对角线对称的元素都相等.

同时满足结合律和交换律的代数运算具有以下重要性质.

定理 1.1.2 若集合 A 上的代数运算$\circ$既满足结合律又满足交换律,则对 A 中任意 n 个元素的运算 $a_1\circ a_2\circ\cdots\circ a_n(a\geqslant 2)$可以随意调换元素的前后次序. □

最后讨论分配律.

定义 1.1.14 设集合 A 有两个代数运算$\circ$及$\oplus$.如果 $\forall a, b, c\in A$,都有

$$a \circ (b \oplus c) = (a \circ b) \oplus (a \circ c),$$

则称运算$\circ$对$\oplus$满足左分配律(left distributive law);如果

$$(b \oplus c) \circ a = (b \circ a) \oplus (c \circ a),$$

则称运算$\circ$对$\oplus$满足右分配律(right distributive law).

定理 1.1.3 设集合 A 有两个代数运算$\circ$及$\oplus$,其中$\oplus$满足结合律.

(1) 如果$\circ$对$\oplus$满足左分配律,则对于 A 中任意 $n+1$ 个元素 $a_1, a_2, \cdots, a_n$ 和 b 都有

$$b \circ (a_1 \oplus a_2 \oplus \cdots \oplus a_n) = (b \circ a_1) \oplus (b \circ a_2) \oplus \cdots \oplus (b \circ a_n).$$

(2) 如果$\circ$对$\oplus$满足右分配律,则对于 A 中任意 $n+1$ 个元素 $a_1, a_2, \cdots, a_n$ 和 b 都有

$$(a_1 \oplus a_2 \oplus \cdots \oplus a_n) \circ b = (a_1 \circ b) \oplus (a_2 \circ b) \oplus \cdots \oplus (a_n \circ b).$$ □

定理 1.1.1 至定理 1.1.3 的证明留给读者作为练习.

4. 等价关系与集合的分类

将集合按一定的规则进行分类是研究集合的一种很有效的方法,而等价关系是集合中一类重要的二元关系,它对于集合的分类起着重要的作用.

(1) 关系

定义 1.1.15 设 A 为非空集合,$A\times A$ 的一个子集 R 称为 A 的一个关系(relation).

$\forall a,b\in A$，若$(a,b)\in R$，则称a与b有关系R，记作aRb. 若$(a,b)\notin R$，则称a与b无关系R，记作$a\not R\ b$.

例 1.1.8 给定实数集$\mathbb{R}$和整数集$\mathbb{Z}$，则

$$R_1=\{(a,b)\mid (a,b)\in \mathbb{R}\times\mathbb{R},a\leqslant b\},$$

$$R_2=\{(a,b)\mid (a,b)\in \mathbb{R}\times\mathbb{R},a=2b\},$$

$$R_3=\{(a,b)\mid (a,b)\in \mathbb{Z}\times\mathbb{Z},a\mid b\},$$

$$R_4=\{(a,b)\mid (a,b)\in \mathbb{Z}\times\mathbb{Z},a\text{与}b\text{的奇偶性相同}\}$$

分别都是实数集$\mathbb{R}$或整数集$\mathbb{Z}$上的关系. 而且$aR_1b\Leftrightarrow a\leqslant b$，故$R_1$就是实数间的“小于或等于”关系；$aR_2b\Leftrightarrow a=2b$，这说明$R_2$为实数间的两倍关系；而$aR_3b\Leftrightarrow a\mid b$，正是整数间的整除关系；对于$R_4$而言，它为整数间的同奇偶性关系.

(2) 等价关系

定义 1.1.16 集合A的关系R若满足：

① 反身性(reflexivity)：$\forall a\in A,aRa$；

② 对称性(symmetry)：$\forall a,b\in A$，若aRb，则bRa；

③ 传递性(transitivity)：$\forall a,b,c\in A$，若aRb且bRc，则aRc.

则称R是A的一个等价关系(equivalence relation)，此时把R习惯上记作$\sim$，aRb也就记为$a\sim b$，并读作a与b等价.

由定义 1.1.16 可知，实数域$\mathbb{R}$上n阶矩阵所构成的集合$M_n(\mathbb{R})$中矩阵的合同关系($\boldsymbol{A}=\boldsymbol{C}^{\mathrm{T}}\boldsymbol{BC},\boldsymbol{C}$可逆). 相似关系($\boldsymbol{A}=\boldsymbol{P}^{-1}\boldsymbol{BP},\boldsymbol{P}$可逆)以及等价关系($\boldsymbol{A}=\boldsymbol{PBQ},\boldsymbol{P}$和$\boldsymbol{Q}$都可逆)都是等价关系. 而例 1.1.8 中，$R_1$和$R_3$虽然都适合反身性和传递性，但却不满足对称性；$R_2$对于反身性、对称性和传递性都不满足；$R_4$是等价关系.

在以后的学习中会常碰到的一种重要的等价关系见例 1.1.9.

例 1.1.9 在整数集$\mathbb{Z}$中取定一个正整数m，规定

$$aRb\Leftrightarrow m\mid (a-b),\quad \forall a,b\in\mathbb{Z},$$

则很容易验证得

① $\forall a\in\mathbb{Z}$，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R为$\mathbb{Z}$上的一个等价关系. 称R为$\mathbb{Z}$的关于模m的同余关系(congruence relation). 而aRb通常记作$a\equiv b(\mathrm{mod}\ m)$，或$a\equiv b(m)$，读做$a$与$b$同余模$m$.

定义 1.1.17 若$\sim$是集合A上的一个等价关系，$a\in A$，令

$$[a]=\{x\mid x\in A,a\sim x\},$$

称$[a]$为以a为代表元的A的一个等价类(equivalence class). 由A的全体等价类构成的集合称为集A在等价类关系$\sim$下的商集(quotient set)，记作$A/\sim$.

在例 1.1.8 中，R_4为等价关系. 以 0 和 1 为代表元的等价类分别是

$$[0]=\{x \mid x\in\mathbb{Z},0R_4x\}=\{x \mid x\in\mathbb{Z},x=2m,m\in\mathbb{Z}\};$$

$$[1]=\{x \mid x\in\mathbb{Z},1R_4x\}=\{x \mid x\in\mathbb{Z},x=2m+1,m\in\mathbb{Z}\}.$$

$\mathbb{Z}$ 在 R_4 下的商集为 $\mathbb{Z}/R_4=\{[0],[1]\}$. 其中[0]是全体偶数集,[1]是全体奇数集.

在例 1.1.9 中,习惯上将等价类称为剩余类,$[a]$记作$\overline{a}$,而相应的商集称为$\mathbb{Z}$ 的模 m 剩余类集并记为$\mathbb{Z}_m$. 这样每个剩余类为

$$\overline{0}=\{\cdots,-3m,-2m,-m,0,m,2m,3m,\cdots\};$$

$$\overline{1}=\{\cdots,-3m+1,-2m+1,-m+1,1,m+1,2m+1,3m+1,\cdots\};$$

$$\vdots$$

$$\overline{m-1}=\{\cdots,-2m-1,-m-1,-1,m-1,2m-1,3m-1,4m-1,\cdots\};$$

而$\mathbb{Z}_m=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{m-1}\}$. 譬如,当 $m=3$ 时,$\mathbb{Z}_3=\{\overline{0},\overline{1},\overline{2}\}$,其中

$$\overline{0}=\{\cdots,-9,-6,-3,0,3,6,9,\cdots\};$$

$$\overline{1}=\{\cdots,-8,-5,-2,1,4,7,10,\cdots\};$$

$$\overline{2}=\{\cdots,-7,-4,-1,2,5,8,11,\cdots\}.$$

(3) 集合的分类

若一个非空集 A 能表示成它的一些不相交非空子集的并,那么这些子集构成的集合在以后的学习中会常遇到.

定义 1.1.18 设 $P=\{A_i \mid i\in I,A_i\subseteq A\}$($I$ 为指标集)为非空集合 A 的一个子集族,如果 P 满足:

① $A_i\neq\varnothing$, $\forall i\in I$;

② $A=\bigcup\limits_{i\in I}A_i$;

③ $\forall A_i,A_j\in P$,当 $i\neq j$ 时,有 $A_i\cap A_j=\varnothing$,

则称 P 为 A 的一个分类(partition),其中每个子集 $A_i(i\in I)$称为 A 的一个类.

在例 1.1.8 中,$\mathbb{Z}$ 在 R_4 下的商集$\mathbb{Z}/R_4=\{[0],[1]\}$就是$\mathbb{Z}$ 的一个分类;在例 1.1.9 中,在同余关系 R 下的模 m 剩余类集$\mathbb{Z}_m$ 构成了$\mathbb{Z}$ 的一个分类. 此外,我们再给出例子.

例 1.1.10 设 $A=\{1,2,3,4,5,6,7,8\}$,指出下列哪些是 A 的分类,为什么?

① $P_1=\{A_1,A_2,A_3,A_4\}$,其中 $A_1=\{1,2\},A_2=\{3,4,5\},A_3=\{6,7,8\},A_4=\varnothing$;

② $P_2=\{A_1,A_2,A_3,A_4\}$,其中 $A_1=\{1,2,3\},A_2=\{4,5\},A_3=\{6\},A_4=\{8\}$;

③ $P_3=\{A_1,A_2,A_3,A_4\}$,其中 $A_1=\{1,3,4\},A_2=\{2,3,5\},A_3=\{6,7\},A_4=\{8\}$;

④ $P_4=\{A_1,A_2,A_3,A_4\}$,其中 $A_1=\{2,3\},A_2=\{1,4,5\},A_3=\{6,7\},A_4=\{8\}$.

解 ① 因为 $A_4=\varnothing$,故 P_1 不是 A 的分类;

② 因为 $A\neq\bigcup\limits_{i=1}^{4}A_i$ 由于 $7\notin\bigcup\limits_{i=1}^{4}A_i$,所以 P_2 不是 A 的分类;

③ 因为 $A_1\cap A_2\neq\varnothing$,所以 P_3 不是 A 的分类;

④ P_4 为 A 的分类.

下面我们将看到,集合所谓的分类就是利用集合的某种等价关系,将该集合分解成一些称为类的子集. 比如例 1.1.9 中,可以利用"模的同余关系"给出$\mathbb{Z}$ 的一个分类.

集合 A 的分类与集合 A 上的等价关系之间存在着相互制约的联系.

定理 1.1.4 集合 A 的任一个等价关系$\sim$都确定了 A 的一个分类 P,并且每个等价类恰是这个分类 P 中的一个类. 反之,集合 A 的每一个分类 P 也确定 A 的一个等价关系$\sim$,而且 P 中的每个类恰为$\sim$的一个等价类.

证明 设 R 为 A 的一个等价关系,$\forall a\in A$,令

$$[a]=\{x\mid x\in A, x\sim a\}$$

为以 a 为代表元的等价类,那么在等价关系 R 下的商集 $A/\sim=\{[a]\mid a\in A\}$必为 A 的一个分类 P. 这是因为

① $\forall [a]\in A/\sim$,由 $a\sim a$,可知 $a\in[a]$,故$[a]\neq\varnothing$;

② $\forall a\in A$,则 $a\in[a]$,所以 $a\in\bigcup\limits_{[a]\in A/\sim}[a]$,进而 $A\subseteq\bigcup\limits_{[a]\in A/\sim}[a]$,因此 $A=\bigcup\limits_{[a]\in A/\sim}[a]$;

③ 设$[a],[b]\in A/\sim$,且$[a]\cap[b]\neq\varnothing$,则有 $x\in[a]\cap[b]$,故 $x\in[a]$且 $x\in[b]$,所以 $x\sim a$ 且 $x\sim b$,进而知 $a\sim b$. 因此 $a\in[b]$,即$[a]\subseteq[b]$. 同理可证$[b]\subseteq[a]$,故$[a]=[b]$. 也就是说:若$[a]\neq[b]$,则$[a]\cap[b]=\varnothing$. 所以 $A/\sim$为 A 的一个分类,即 $A/\sim=P$.

反之,若 $P'=\{A_i\mid\varnothing\neq A_i\subseteq A, i\in I\}$为集 A 的一个分类. 在 A 中可定义关系$\sim'$. $\sim'=\{(a,b)\mid a,b\in A$,存在 $i\in I$ 使 $a,b\in A_i\}$,显然$\sim'$为 A 上的一个关系.

① $\forall a\in A$,由 $A=\bigcup\limits_{i\in I}A_i$ 知必存在 $j\in I$ 使 $a\in A_j$,所以 $a\sim' a$. 反身性成立;

② $\forall a,b\in A$,若 $a\sim' b$,这意味着存在某个 $A_i\in P$ 使 $a,b\in A_i$,显然 $b,a\in A_i$,所以 $b\sim' a$. 对称性成立;

③ $\forall a,b,c\in A$,若 $a\sim' b$ 且 $b\sim' c$,即存在 A_i 和 A_j 使 $a,b\in A_i$,$b,c\in A_j$,那么 $b\in A_i\cap A_j$,即 $A_i\cap A_j\neq\varnothing$,由分类的定义知,必有 $A_i=A_j$,所以 $a,b,c\in A_i$,故有 $a\sim' c$ 传递性成立.

所以$\sim'$为 A 的一个等价关系,且 $A/\sim'=P$. □

从定理 1.1.4 可看到$\sim=\sim'\Leftrightarrow P=P'$. 即集合 A 的等价关系与 A 的分类是相互确定,一一对应的. 一个集合的分类通过等价关系进行描述,为我们的讨论带来许多方便.

(4) 同余关系

在例 1.1.9 若将整数集$\mathbb{Z}$ 看成一个代数系统$(\mathbb{Z},+)$,其中$+$为整数间通常的加法,那么很容易验证该例中的等价关系具有性质:若 aRb, cRd,则$(a+c)R(b+d)$. 将这一概念进行推广,我们得到了代数系统的同余关系,即:代数系统上的同余关系是一种特殊的等价关系,它能保证具有等价关系的二对元素分别运算后,仍然保持这种关系.

定义 1.1.19 设$(A,\circ)$为一个代数系统,$\sim$是 A 上的一个等价关系,如果 $\forall a,b,c,d\in A$,由$a\sim b, c\sim d\Rightarrow a\circ c\sim b\circ d$,则称$\sim$为对于 A 的运算$\circ$是一个同余关系(congruence relation). 当 $a\in A$,则以 a 为代表元的等价类$[a]$习惯上称为 a 的同余类. 当 $a\sim b$ 时,称 a

与 b 同余且记为 $a\equiv b$.

例 1.1.11 固定正整数 $m\in\mathbb{Z}$ 在代数系统$(\mathbb{Z},\circ)$中(其中$\circ$为通常的乘法),那么$\mathbb{Z}$上的关系 R: $aRb\Leftrightarrow m\mid(a-b)$是$\mathbb{Z}$上对于$\circ$的一个同余关系.

首先,例 1.1.9 已证明了 R 为$\mathbb{Z}$上的等价关系.

其次,若 aRb,cRd,则有

$$m\mid(a-b),\quad 且\quad m\mid(c-d),$$

于是由 $ac-bd=a(c-d)+(a-b)d$,知

$$m\mid(ac-bd),$$

进而得$(ac)R(bd)$.

所以 R 对于$\mathbb{Z}$的通常乘法是一个同余关系.

定理 1.1.5 设$(A,\circ)$为一个代数系统,$\sim$是 A 上的关于$\circ$的一个同余关系,则在商集 $A/\sim$中可定义代数运算

$$\otimes:[a]\otimes[b]=[a\circ b],\quad \forall[a],[b]\in A/\sim.$$

证明 欲证$\otimes$: $A/\sim\times A/\sim\to A/\sim$,$([a],[b])\mapsto[a\otimes b]$是映射,显然只需证明像$[a\circ b]$与$[a],[b]$的代表元选择无关.

事实上,若$[a]=[a']$,$[b]=[b']$,则 $a\sim a'$,$b\sim b'$. 由$\sim$的同余性质,我们得 $a\circ b\sim a'\circ b'$,所以$[a\circ b]=[a'\circ b']$,即$[a]\otimes[b]=[a']\otimes[b']$. 这说明$\otimes$确实是 $A/\sim$的一个代数运算,即$(A/\sim,\otimes)$是一个代数系统. □

习惯上,我们将代数系统$(A/\sim,\otimes)$中的代数运算$\otimes$称为由$(A,\circ)$的代数运算$\circ$诱导出的代数运算.

习题 1.1

1. 假如 $a\equiv b(n)$,$c\equiv d(n)$,那么

$$a+c\equiv b+d(n),\quad a-c\equiv b-d(n),$$

$$ma\equiv mb(n),\quad ac\equiv bd(n).$$

2. 试就 $n=-5$ 时,把整数集$\mathbb{Z}$进行同余分类.

3. 对于下面给出的$\mathbb{Z}$到$\mathbb{Z}$的映射 f,g,h

$$f:x\mapsto 3x;\quad g:x\mapsto 3x+1;\quad h:x\mapsto 3x+2.$$

计算 $f\circ g,g\circ f,g\circ h,h\circ g,f\circ g\circ h$.

4. 在复数集$\mathbb{C}$中,规定二元关系$\sim$: $a\sim b\Leftrightarrow a$ 的辐角$=b$ 的辐角. 证明: $\sim$是$\mathbb{C}$的一个等价关系,决定相应的等价类.

5. 设 $A=\{1,2,3,4\}$,在 2^A 中规定二元关系$\sim$: $S\sim T\Leftrightarrow S,T$ 含有元素个数相同,证明这是一个等价关系. 这里 2^A 表示 A 的幂集合,即由 A 的全部子集为元素构成的集合.

6. R_1,R_2 是 A 的两个等价关系,$R_1\cap R_2$ 是不是 A 的二元关系? 是不是等价关系? 为什么? $R_1\cup R_2$ 是不是 A 的二元关系?