

21世纪高等院校教材

01000100010100100100100101100010010111000100010001010
001000100010100100100100101100010010111000100010001
001000100010100100100100101100010010111000100010001
001000100010100100100100101100010010111000100010001

抽象代数基础教程

庄瓦金 编著



高等教育出版社

21 世纪高等院校教材

抽象代数基础教程

庄瓦金 编著

高等教育出版社

73

责任编辑 李杰文

责任校对 吴 惠

装帧设计 严 榕

图书在版编目 (CIP) 数据

抽象代数基础教程/庄瓦金 编著

—北京：高等教育出版社，2005.1

ISBN 7—04—014057—8

I .抽... II .庄... III .数学—抽象代数—教程

IV.O153

中国版本图书馆 CIP 数据核字(2005)第 135584 号

出版发行 高等教育出版社

社 址 北京市西城区德外大街 4 号

邮政编码 100011

经 销 新华书店北京发行所

印 刷 北京光明印刷厂印装

开 本 850×1168 1/32

印 张 7.8125

字 数 210 千字

版 次 2005 年 1 月第 1 版

印 次 2005 年 1 月第 1 次

定 价 21.00 元

书 号 ISBN 7—04—014057—8/G.43

版权所有 侵权必究

内 容 提 要

本书根据《抽象代数教学大纲》要求，在笔者廿多年教学实践基础上编写而成。书中不仅阐述了群、环和扩域的基础内容，而且重视在公理定义上的思考与推导，以培养学生的抽象数学能力。本书精选了大量典型例题，各章之末设置了“解题探索”，既可帮助学生克服学习抽象代数的困难，也可供报考数学各专业硕士研究生的考生参考。书中还注意抽象代数的应用，并将其阐述溶入于基础之中。

本书可作为高等院校本科数学各专业的《抽象代数》（《近世代数》）课程的教材，也可供其他相关专业的师生自学参考。

前言

本教材是在笔者 1980 年《近世代数》讲义基础上,经多年教学实践修改形成的。修改稿曾在漳州师院 2001 级数学与应用数学专业的《抽象代数》课程使用过,效果良好。根据试用情况,出版前又作了一些修改,并在各章之末增加了“解题探索”。

本教材在以下三方面作了努力。

1 教学内容适用,阐述清晰简洁

本教材按原国家教委颁布的高师《抽象代数教学大纲》要求编写,重点阐述群、环和扩域的基础内容,其中将“因子分解”部分整入环的整除理论之中;同时考察了内容的与时俱进和教学学时限制的矛盾,精选了一些材料整入各章,如第一章编入了与有限群基本结构有关的内容,第二章点及了环的模表示,第三章介绍了 Galois 理论基本定理。因此,本教材为报考数学各专业硕士研究生的同学们提供了较充足的近世代数需求。

在内容阐述上,本教材继承了参考文献[22]的风格,仍节下设款,语言简洁,层次分明。因而既方便师生的教与学,又注意在教学中对学生数学能力的培养。

2 抽象能力培养,整体交错推进

抽象数学能力的培养是抽象代数课程教学中能力培养的核心,本教材至始至终都予关注,并在第一章、第二章之首用简短的几句话把做法挑明。虽然教材中精选了大量代表性强、覆盖面广的例子,并配备了丰富的习题,但我们仍提醒同学们区分抽象对象与具体例子的差异;同时,我们还要求同学们学会在公理定义上的思考与推导,并将其结论应用到具体例子的分析上。这是抽象数学能力培养的第一个全过程,进而还须回味,领悟抽象数学的魅力,因而交错地增进学生的抽象数学能力。这就是教材中对抽象数学能力的第二个全过程的安排,也望教学中留意。

3 基础理论应用,酌情重点述之

抽象代数的理论已有广泛应用。鉴于本课程性质及教学学时限制,教材中不可能用较多的篇幅顾及。但是,本教材仍作些考虑,如点及 Burnside 引理的应用,介绍有限域在编码中的应用,阐述扩域理论在解决尺规作图三大问题、代数方程根式解问题中的应用。参考文献中也注意列入有更多应用的参考书,如参考文献[8, 10]。希望这些都有助于打消部分同学学习抽象代数无用的念头。

本教材是《抽象代数》创建漳州师院优秀课程的标志性成果,其出版得到了有关领导、同行专家的支持,值此致以诚挚的感谢。

当然,由于编写时间紧、笔者学识簿,教材中定有不少错误或欠妥之处,敬请各位专家及广大读者批评指正。

庄瓦金

2005 年 1 月于漳州芗江新村

目 录*

前言	1
预备章 代数运算 二元关系	1
§ 1 二元代数运算	1
1.1 定义与例子	1
1.2 半群的概念	3
§ 2 等价关系	6
2.1 二元关系	6
2.2 等价关系	8
2.3 满射的分解	10
§ 3 偏序关系	11
3.1 基本概念	11
3.2 Zorn 引理	13
第一章 群	16
§ 1 群的定义	16
1.1 定义与例子	16
1.2 刻画定理	18
§ 2 子群 同态	22
2.1 子群的概念	22
2.2 群的同态	25
§ 3 循环群	31
3.1 元素的阶	31
3.2 循环群的若干结论	32
§ 4 变换群	36
4.1 定义与例子	36
4.2 Cayley 定理	38
4.3 置换群	39
§ 5 子群的陪集	43
5.1 陪集的概念	44

2 * 目录中用楷体排的节、款属选学内容, 可视教学时数与学生实际酌情选用。

5.2 Lagrange 定理	46
§ 6 正规子群	49
6.1 正规子群的概念	49
6.2 商群的概念	52
6.3 有限单群	55
§ 7 同态定理	58
7.1 同态基本定理	59
7.2 子群的对应关系	62
7.3 同构定理	63
§ 8 群在集合上的作用	65
8.1 定义与例子	65
8.2 轨道与稳定子群	67
8.3 Burnside 引理	70
§ 9 Sylow 定理	72
§ 10 有限交换群的结构	76
10.1 群的直积	76
10.2 结构定理	80
§ 11 解题探索	85
11.1 元素的阶 循环群	85
11.2 群子集	86
11.3 正规子群	88
11.4 自同构群	89
11.5 有限群	91
第二章 环	96
§ 1 环的概念	96
1.1 环的定义	96
1.2 环的乘法半群	100
§ 2 无零因子环	102
2.1 无零因子环的概念	103
2.2 除环 域	105

§ 3 理想 商环	109
3.1 子环的概念	110
3.2 理想	111
3.3 商环	115
§ 4 环的同态	117
4.1 同态的概念	117
4.2 同态定理	119
§ 5 挖补定理及其应用	123
5.1 同构嵌入原理	124
5.2 分式域	125
5.3 多项式环	129
§ 6 素理想与极大理想	134
6.1 素理想的概念	134
6.2 极大理想	135
§ 7 唯一分解环	139
7.1 整除的概念	139
7.2 唯一分解环的刻画	142
7.3 最大公因子	145
§ 8 主理想整环与 Euclid 环	148
8.1 主理想整环	148
8.2 Euclid 环	150
§ 9 Gauss 整环上的多项式环	152
9.1 本原多项式	152
9.2 因式分解定理	154
9.3 多项式的根	156
§ 10 环的表示与模	160
10.1 End G 与环的表示	160
10.2 模的概念	164
§ 11 解题探索	168
11.1 交换性 零因子	168

11.2 除环 正则环	171
11.3 同态与同构	173
11.4 理想	177
11.5 整除理论	180
第三章 域的扩张	184
§ 1 单扩域	184
1.1 扩域的概念	184
1.2 单扩域	186
§ 2 代数扩域	189
2.1 有限扩域	189
2.2 代数扩域	191
2.3 应用: 尺规作图问题	194
§ 3 多项式的分裂域	197
3.1 存在、唯一性定理	197
3.2 可分扩域	203
3.3 分裂域的正规性	206
§ 4 有限域	209
4.1 有限域的基本结论	209
4.2 应用: 编码	214
§ 5 Galois 理论基本定理	220
5.1 Galois 扩域	220
5.2 Galois 对应	222
5.3 应用: 用根式解代数方程问题	225
§ 6 解题探索	231
6.1 有限扩域	231
6.2 多项式的分裂域	233
6.3 特征 p 之域	236
参考文献	240

预备章 代数运算 二元关系

本章学习二元代数运算、半群、等价关系、偏序关系等概念，为以后各章的学习作些准备。

§ 1 二元代数运算

1.1 定义与例子

定义 1 设 A 是一个非空集合， A 的 Descartes 积 $A \times A$ 到 A 的映射 σ 叫做 A 的一个二元代数运算(简称代数运算)。

此时，对于 $\forall a, b \in A$ ，在 σ 作用下，有唯一确定的元素 $c \in A$ ，使得 $\sigma(a, b) = c$ 。通常记 $\sigma(a, b) = a \circ b$ 。

具有代数运算“ $\circ$ ”的集合 A 记作 $(A, \circ)$ ，叫做一个群胚。

注 关于集合与映射的概念及记号，本书沿用[22]的阐述，其中常见的数集有：

$\mathbf{N}^*$ 自然数集， $\mathbf{N}$ 非负整数集， $\mathbf{Z}$ 整数集，
 $\mathbf{Q}$ 有理数集， $\mathbf{R}$ 实数集， $\mathbf{C}$ 复数集。

例 1 设 $A = \mathbf{Z}$ ，大家熟悉的整数的加法运算： $+$ ，减法运算： $-$ ，乘法运算： $\times$ 分别是 $\mathbf{Z}$ 的代数运算。又规定

$$\sigma(a, b) = a \circ b = 0, \forall a, b \in \mathbf{Z};$$

$$\tau(a, b) = a \odot b = a + b + ab, \forall a, b \in \mathbf{Z},$$

则 σ, τ 也分别是 $\mathbf{Z}$ 的代数运算。

在例 1 中，若分别用 $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ 代替 $\mathbf{Z}$ ，则结论也成立。但若用 $\mathbf{N}^*$ 代替 $\mathbf{Z}$ ，则结论不全成立，其中 $(\mathbf{N}^*, -)$ ， $(\mathbf{N}^*, \odot)$ 都不是群胚。

例 2 设 F 是一个数域，那么

1) 多项式的加法运算，乘法运算分别是 $F[x]$ 的代数运算；

2) 矩阵的加法运算是 $F^{m \times n}$ 的代数运算，矩阵的乘法运算是 $M_n(F)$ 的代数运算。

例 3 设 $A \neq \emptyset$ ，在集合论意义下的交与并： $\cap, \cup$ 分别是 A 的幂集合 2^A 的代数运算。

设 $A = \{a_1, a_2, \dots, a_n\}$ 是一个有限集合, 则 A 的代数运算 “ $\circ$ ” 可用下面的 Cayley 表给出:

$\circ$	a_1	$\dots$	a_j	$\dots$	a_n
a_1	c_{11}	$\dots$	c_{1j}	$\dots$	c_{1n}
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_i	c_{i1}	$\dots$	c_{ij}	$\dots$	c_{in}
$\vdots$	$\vdots$		$\vdots$		$\vdots$
a_n	c_{n1}	$\dots$	c_{nj}	$\dots$	c_{nn}

这里 $c_{ij} = a_i \circ a_j$, $i, j = 1, 2, \dots, n$.

例 4 设 $A = \{e, a, b, c\}$, A 的代数运算由下表给出:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

例 5 设 $B = \{0, 1, 2\}$, B 的代数运算由下表给出:

$\circ$	0	1	2
0	1	2	2
1	1	1	1
2	0	0	0

注意, 例 5 中的 0, 1, 2 不是通常的整数, 在这里它们表示集 B 中元素的记号.

注 1) 这里说的代数运算是二元代数运算. 一般地, 给定 $n+1$ 个非空集合 $A_1, A_2, \dots, A_n, A$, 则称 $A_1 \times A_2 \times \dots \times A_n$ 到 A 的映射为 $A_1, A_2, \dots, A_n$ 到 A 的代数运算. 当 $A_1 = A_2 = \dots = A_n$ 时, 则称之为 A 的 n 元代数运算. 一元代数运算是 A 到 A 的映射; 零元代数运算是在 A 中固定某一确定元素, 它不依赖于 A 中的任何元素.

设 A 是一个集合, 若在 A 中定义了若干个代数运算, 则称之为一个泛代数.

2) 关于代数运算的记号, 若 A 是具体集合, 常采用习惯用法; 若 A 是抽象集合, 常采用乘法记号 “ $\circ$ ”, 加法记号 “ $+$ ”. 对于采用

乘法记号的情形,在不致引起混淆情况下,常将 $a \circ b$ 简记为 ab .

3)常义下的除法运算“ $\div$ ”不是 $\mathbf{Q}(\mathbf{R}, \mathbf{C})$ 的二元代数运算,却是 $\mathbf{Q}^* = \mathbf{Q} - \{0\}(\mathbf{R}^* = \mathbf{R} - \{0\}, \mathbf{C}^* = \mathbf{C} - \{0\})$ 的代数运算.对此,有时也称“ $\div$ ”是 $\mathbf{Q}(\mathbf{R}, \mathbf{C})$ 的部分代数运算.

对于代数运算,我们感兴趣的是它的算律及其代数系统,其中最基本的是满足结合律的代数系统.因此,我们来阐述

1.2 半群的概念

定义 2 设 $(A, \circ)$ 是一个群胚,且满足结合律:

$$(a \circ b) \circ c = a \circ (b \circ c), \forall a, b, c \in A,$$

则称 $(A, \circ)$ 是一个半群.

例如, $(\mathbf{Z}, +)$, $(\mathbf{Z}, \times)$, $(M_n(F), \circ)$ 分别是半群.我们来证明例 1 中 $(\mathbf{Z}, \odot)$ 是一个半群.因为 $\forall a, b, c \in \mathbf{Z}$, 有

$$(a \odot b) \odot c = (a + b + ab) \odot c = a + b + c + abc + ab + ac + bc,$$

$$a \odot (b \odot c) = a \odot (b + c + bc) = a + b + c + ab + ac + bc + abc.$$

所以 $(\mathbf{Z}, \odot)$ 也是一个半群.

例 5 的 $(B, \circ)$ 不是半群,因为 $0 \circ (1 \circ 2) = 0 \circ 1 = 2$, $(0 \circ 1) \circ 2 = 2 \circ 2 = 0$.

例 4 的 $(A, \circ)$ 是一个半群,因为 $\forall$ 三个元素 $u, v, w \in A$, 当 u, v, w 中有一个为 e 时,则由 $e \circ x = x \circ e = x (\forall x \in A)$ 易见结合律成立;若这三个元素有两个相等,设 $u = v$, 则有 $(u \circ u) \circ w = w = u \circ (u \circ w)$, 或 $w \circ (u \circ u) = w = (w \circ u) \circ u$ 或 $(u \circ w) \circ u = u \circ (u \circ w) = u \circ (w \circ u)$;若三个元素互不相等且都不等于 e , 则 $u \circ (v \circ w) = u \circ u = e = w \circ w = (u \circ v) \circ w$. 所以 $(A, \circ)$ 是一个半群.

注 有限半群结合律的检验,已有专门的检验方法,同学们可参考文[15, 20]的相应阐述.

在半群中,任意三个有序元素 a, b, c 在运算“ $\circ$ ”下,加括号的两种方式

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

的结果彼此相等,因此可不加括号用 $a \circ b \circ c$ 表示.对于四个元素,有以下加括号方式:

$$[(a_1 \circ a_2) \circ a_3] \circ a_4, [a_1 \circ (a_2 \circ a_3)] \circ a_4, a_1 \circ [(a_2 \circ a_3) \circ a_4], \\ a_1 \circ [a_2 \circ (a_3 \circ a_4)], (a_1 \circ a_2) \circ (a_3 \circ a_4),$$

对于 n 个元素, 有 $(2n-2)!/n!(n-1)!$ 种加括号方式(参考[12]p21-22). 它们都彼此相等吗? 下面的定理给出了肯定的回答.

定理 0.1.1 设 $(A, \circ)$ 是一个半群, 则对于 A 的任意 $n(\geq 2)$ 个有序元素 $a_1, a_2, \dots, a_n$ 的运算, 对它们进行各种加括号方式运算所得结果由元素 $a_1, a_2, \dots, a_n$ 唯一确定. 因此可不用加括号, 记作 $a_1 \circ a_2 \circ \dots \circ a_n$.

证 设 $\pi(a_1, a_2, \dots, a_n)$ 表示有序元素 $a_1, a_2, \dots, a_n$ 在运算“ $\circ$ ”下的任一种加括号方式之结果, 顺序加括号情形的结果记作

$$\prod_{i=1}^n a_i = (((\dots((a_1 \circ a_2) \circ a_3) \circ \dots) \circ a_{n-1}) \circ a_n).$$

定理的正确性在于证明

$$\pi(a_1, a_2, \dots, a_n) = \prod_{i=1}^n a_i. \quad (1)$$

下面对 n 用数学归纳法证明(1).

由于 $(A, \circ)$ 是一个半群, 当 $n=2, 3$ 时, (1) 当然成立.

当 $n>3$ 时, 假定对于 $(2 \leq) k < n$ 时(1)成立. 那么对于 n 的情形, 注意到无论哪种加括号方式, 最后总归结为两个元素相乘. 因此有

$$\pi(a_1, a_2, \dots, a_n) = \pi(a_1, \dots, a_i) \circ \pi(a_{i+1}, \dots, a_n).$$

若 $i=n-1$, 则由归纳假设有

$$\pi(a_1, \dots, a_n) = \pi(a_1, \dots, a_{n-1}) \circ a_n = \left(\prod_{i=1}^{n-1} a_i \right) \circ a_n = \prod_{i=1}^n a_i,$$

(1) 成立.

若 $1 \leq i < n-1$, 则由归纳假设、结合律, 有

$$\begin{aligned} \pi(a_1, \dots, a_n) &= \pi(a_1, \dots, a_i) \circ \pi(a_{i+1}, \dots, a_n) \\ &= \pi(a_1, \dots, a_i) \circ [\pi(a_{i+1}, \dots, a_{n-1}) \circ a_n] \\ &= [\pi(a_1, \dots, a_i) \circ \pi(a_{i+1}, \dots, a_{n-1})] \circ a_n \\ &= \left(\prod_{i=1}^{n-1} a_i \right) \circ a_n = \prod_{i=1}^n a_i, \end{aligned}$$

(1) 也成立. 因此, 由数学归纳法知道定理正确. $\square$

由定理 0.1.1, 我们在半群 $(A, \circ)$ 中引进正整数指数幂的概念, 规

定

$$a^n = \overbrace{a \circ a \circ \cdots \circ a}^{n \uparrow a}, \quad \forall a \in A,$$

并且容易证得指数运算法则成立:

$$a^m \circ a^n = a^{m+n}, \quad (a^m)^n = a^{mn}, \quad \forall a \in A, m, n \in \mathbb{N}^*.$$

注 若代数运算记号采用“+”, 则 a^n 表示为 $na = a + \cdots + a$, 上述的指数法则就是下面的倍数法则:

$$ma + na = (m+n)a, \quad n(ma) = (mn)a, \quad \forall a \in A, m, n \in \mathbb{N}^*.$$

请注意, 这里的 a 未必是数, 它是 $(A, +)$ 中的任意元素.

在群胚、半群中, 交换律也是较常考察的算律. 因此引入

定义 3 设 $(A, \circ)$ 是一个群胚. 若 $\forall a, b \in A$, 都有

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

则称 $(A, \circ)$ 满足交换律, 并称 $(A, \circ)$ 是一个交换群胚. 又若 $(A, \circ)$ 是一个半群, 则称之为交换半群.

$(\mathbb{Z}, +)$, $(\mathbb{Z}, \otimes)$, $(F[x], \circ)$ 都是交换半群, 但 $(M_n(F), \circ)$ 不是交换半群.

在交换半群中, 定理 0.1.1 可开拓为

定理 0.1.2 设 $(A, \circ)$ 是一个交换半群, $a_1, a_2, \dots, a_n \in A (n \geq 2)$,

则

$$a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n} = a_1 \circ a_2 \circ \cdots \circ a_n, \quad (2)$$

这里 $i_1, i_2, \dots, i_n$ 是 $1, 2, \dots, n$ 的任一个排列.

证 对 n 用数学归纳法证明. 当 $n=2$ 时, (2) 当然成立.

当 $n>2$ 时, 假设对于 $n-1$ 情形, (2) 成立. 那么对于 n 情形, 若 $a_{i_n} = a_n$,

则

$$a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n} = (a_{i_1} \circ \cdots \circ a_{i_{n-1}}) \circ a_n = a_1 \circ \cdots \circ a_{n-1} \circ a_n;$$

若 $a_{i_n} \neq a_n$, 则

$$\begin{aligned} a_{i_1} \circ a_{i_2} \circ \cdots \circ a_{i_n} &= (a_{i_1} \circ \cdots \circ a_{i_{k-1}}) \circ a_n \circ (a_{i_{k+1}} \circ \cdots \circ a_{i_n}) \\ &= (a_{i_1} \circ \cdots \circ a_{i_{k-1}} \circ a_{i_{k+1}} \circ \cdots \circ a_{i_n}) \circ a_n = a_1 \circ \cdots \circ a_{n-1} \circ a_n, \end{aligned}$$

(2) 成立. 所以由数学归纳法知道 (2) 成立. □

在交换半群 $(A, \circ)$ 中, 易见以下指数法则成立:

$$(a \circ b)^n = a^n \circ b^n, \quad \forall a, b \in A, n \in \mathbb{N}^*.$$

若 $(A, +)$ 是交换半群, 则称之为加法半群, 并且成立以下的倍数法则:

$$n(a+b) = na + nb, \quad \forall a, b \in A, n \in \mathbb{N}^*.$$

习 题

1 在 $\mathbb{Z}$ 中, $\forall m, n \in \mathbb{Z}$, 规定:

$$1) m \circ n = mn + 1;$$

$$2) m \circ n = m(n+1);$$

$$3) m \circ n = m;$$

$$4) m \circ n = mn^2;$$

$$5) m \circ n = m^2 + n^2;$$

$$6) m \circ n = 3.$$

问哪些情形满足结合律? 哪些情形满足交换律?

2 设 $A = \{a, b\}$, 找出 A 的所有代数运算.

3 设 S 是某个平面上的所有点的集合. $\forall a, b \in S$, 规定 $a \circ b$ 是连接 a, b 的线段的中点. 问“ $\circ$ ”是不是 S 的代数运算? $(S, \circ)$ 是一个半群吗?

4 设 $(S_i, \circ)$ 皆为半群, $i=1, 2$. 在 $S_1 \times S_2$ 中规定

$$(a_1, b_1) \circ (a_2, b_2) = (a_1 \circ a_2, b_1 \circ b_2),$$

则 $(S_1 \times S_2, \circ)$ 也是一个半群, 叫做 S_1 与 S_2 的直积.

§2 等价关系

在抽象代数(近世代数)学习中, 代数系统的等价关系及由此等价关系决定的所在集合的分类既基本又重要. 因此, 本节先来学习它的基本概念, 并介绍与之相关的满射分解.

2.1 二元关系

定义 1 设 A, B 是两个集合, $A \times B$ 的一个子集 R 叫做 A, B 间的一个二元关系. 当 $(a, b) \in R$ 时, 就说 a 与 b 具有关系 R , 记作 aRb ; 当 $(a, b) \notin R$ 时, 就是说 a 与 b 不具有关系 R , 记作 $aR^c b$. A, A 间的二元关系 R 通常叫做 A 上的二元关系.

例 1 1) 设 $A = \mathbb{Z}$, 令

$$R_1 = \{(a, b) | a, b \in \mathbb{Z}, \text{ 且 } a|b\},$$

则 R_1 是 $\mathbb{Z}$ 上的一个二元关系. $\forall a \in \mathbb{Z}$, 都有 $aR_1 ma, m \in \mathbb{Z}$, 但 $2R_1^c 1$.

2) 设 $A = \mathbb{C}$, 令

$$R_2 = \{(a, b) | a, b \in C, \text{ 且 } |a| = |b|\},$$

则 R_2 是 C 上的一个二元关系.

3) 设 F 是一个数域, 令

$$R_3 = \{(A, B) | A, B \in M_n(F), \text{ 且 } B = T^{-1}AT, |T| \neq 0\},$$

则 R_3 是 $M_n(F)$ 上的一个二元关系.

例 2 设 $A = \mathbf{R}$, 令

$$R_1 = \{(a, b) | a, b \in \mathbf{R}, \text{ 且 } a = b\},$$

$$R_2 = \{(a, b) | a, b \in \mathbf{R}, \text{ 且 } a \leq b\},$$

$$R_3 = \{(a, b) | a, b \in \mathbf{R}, \text{ 且 } a = 2b + 1\},$$

$$R_4 = \{(a, b) | a, b \in \mathbf{R}, \text{ 且 } a^2 - b^2 = 1\},$$

则它们分别是 $\mathbf{R}$ 上的二元关系.

例 3 设 $A = \{a, b, c\}$, 令

$$R_1 = \{(a, b), (b, a), (a, a), (b, b)\},$$

$$R_2 = \{(a, a), (b, b), (c, c), (a, b), (b, a), (b, c), (c, b)\},$$

$$R_3 = \{(a, a), (b, b), (c, c), (a, b), (b, c), (a, c)\},$$

则它们分别是 A 上的二元关系.

例 4 设 $A = \mathbf{Q}$, 令

$$R = \{(a, b) | a, b \in \mathbf{Q}, \text{ 且 } a = a + 1\},$$

则 R 是 A 上的一个二元关系, 但 $\forall a, b \in \mathbf{Q}$, 都有 $aR^c b$.

注 1) 设 R 是 A, B 间的一个二元关系, $\forall a \in A, b \in B$, 则 aRb 或 $aR^c b$, 且两者只有一个成立.

2) 设 $R \subseteq A \times B$, 记 $R^c = A \times B - R$, 则 R^c 也是 A, B 间的一个二元关系.

3) 在例 4 中, $R = \emptyset$. 具有这样性质的二元关系叫做空关系.

4) 设 $R \subseteq A \times B$, $D = \{\text{对}, \text{错}\}$, 记

$$aRb = \text{对}, aR^c b = \text{错},$$

则二元关系是一种法则, 可用下面的映射描述:

$$R: A \times B \rightarrow D$$

$$(a, b) \mapsto R(a, b) \in D.$$

最重要的二元关系是

2.2 等价关系

定义 2 设 $\sim$ 是集合 A 上的一个二元关系, 并且满足

- 1) 反身性 $\forall a \in A$, 都有 $a \sim a$;
- 2) 对称性 $\forall a, b \in A$, 若 $a \sim b$, 则 $b \sim a$;
- 3) 传递性 $\forall a, b, c \in A$, 若 $a \sim b, b \sim c$, 则 $a \sim c$,

那么称 $\sim$ 为 A 上的一个等价关系.

上面例 1 中的 R_2, R_3 分别是 $C, M_n(F)$ 上的等价关系. 在例 3 中, R_1 满足对称性和传递性, 但不满足反身性; R_2 满足反身性和对称性, 但不具有传递性; R_3 具有反身性和传递性, 但不具有对称性. 因此, 这三个二元关系都不是等价关系.

例 5 设 $A = \mathbb{Z}$, 取定 $n \in \mathbb{N}^*$, 令

$$\sim = \{(a, b) | a, b \in \mathbb{Z}, \text{ 且 } n | (a - b)\},$$

则 $\sim$ 是 $\mathbb{Z}$ 上的一个等价关系.

证 1) $\forall a \in \mathbb{Z}$, 则 $n | (a - a)$, 所以 $a \sim a$.

2) $\forall a, b \in \mathbb{Z}$, 若 $a \sim b$, 则 $n | (a - b)$. 所以 $n | (b - a)$, 故 $b \sim a$.

3) $\forall a, b, c \in \mathbb{Z}$, 若 $a \sim b, b \sim c$, 则 $n | (a - b), n | (b - c)$. 所以 $n | (a - b) + (b - c)$, 即 $n | (a - c)$. 故 $a \sim c$.

这个等价关系叫做模 n 的同余关系, 常记作

$$a \equiv b \pmod{n},$$

并读作 a 与 b 模 n 同余.

集合 A 上的等价关系与 A 的分类有着密切关系, 为了揭示它们之间的联系, 下面引入

定义 3 设 A 是一个非空集合, $P = \{A_i | \emptyset \neq A_i \subseteq A, i \in I\} \neq \emptyset$, 且满足

$$1) A = \bigcup_{i \in I} A_i;$$

$$2) A_i \cap A_j = \emptyset, i \neq j, i, j \in I,$$

则称 P 是 A 的一个分类, A_i 为 P 的一个类.

引理 0.2.1 设 $\sim$ 是集合 A 上的一个等价关系, $\forall a \in A$, 令