近世代数

高等学校教材

裴定一 郭华光 编著

高等教育出版社

高等学校教材

近世代数

Jinshi Daishu

裴定一　郭华光　编著

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容简介

本教材介绍代数学的一些经典知识,包括群、环、域等代数集合的性质以及域的伽罗瓦理论。书中通过大量实例,较通俗地介绍了近世代数中一些抽象概念。在讲解基础理论的同时,介绍了代数方法在信息科学等学科中的一些应用。了解这些应用,有利于加深对抽象理论的理解,提高学生学习兴趣。本书可作为数学和信息科学相关专业的本科生和研究生的教学和参考用书。

图书在版编目(CIP)数据

近世代数 / 裴定一,郭华光编著. —北京:高等教育出版社,2009.12
ISBN 978-7-04-027958-0

Ⅰ.近… Ⅱ.①裴…②郭… 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 199168 号

策划编辑	杨 波	责任编辑	张耀明	封面设计	张申申
责任绘图	杜晓丹	版式设计	王艳红	责任校对	王 雨
责任印制	毛斯璐				

出版发行	高等教育出版社	购书热线	010-58581118
社 址	北京市西城区德外大街 4 号	咨询电话	400-810-0598
邮政编码	100120	网 址	http://www.hep.edu.cn
总 机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经 销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印 刷	国防工业出版社印刷厂	畅想教育	http://www.widedu.com
开 本	787×960 1/16	版 次	2009 年 12 月第 1 版
印 张	12	印 次	2009 年 12 月第 1 次印刷
字 数	220 000	定 价	15.90 元

本书如有缺页、倒页、脱页等质量问题,请到所购图书销售部门联系调换。

物料号 27958-00

前　言

“近世代数”是大学数学专业的一门基础课。近世代数作为代数学的一个分支，它既包含有深刻的数学理论，又在信息科学，理论物理和分子化学等领域有广泛的应用。

本书讲述了群、环、域等代数集合的基本性质。课程内容的深度定位在一般本科院校的水平上，在内容的叙述上尽量使用浅显的语言，作详尽的解释，使得大多数学生都能读懂大部分内容。同时也考虑学生的不同需要，本教材在内容上也有足够的选择性，例如用专门的一章较深入浅出地介绍了域的伽罗瓦理论。

近世代数课程具有抽象特征，很多学生在学习时会感到困难，产生畏难情绪。本教材坚持从具体到抽象的思维方法，尽可能通过具体的例子讲述一般理论。同时结合教学过程，不断介绍这些抽象理论在相关领域的一些应用，特别用了专门的一章介绍它们在编码和密码中的应用。通过这些应用实例，也有利于帮助学生们更深入理解抽象的理论，并提高他们的学习兴趣。

由于作者水平有限，书中难免有不妥之处，衷心希望读者不吝赐教。

作　者

2008 年 8 月

目 录

第一章　预备知识

本章介绍集合、映射及整数的一些基本知识.

集合和映射是最基础的数学概念, 它们的使用贯穿着本教材的始终.

整数及其运算是本课程里要学习的许多代数对象的典型代表, 它为本课程的抽象内容提供了具体的例子, 有关整数的一些重要概念、重要性质都可以在以后的章节里找到它们的影子.

§1.1　集　合

一些元或研究对象的全体称为集合, 这是数学中最常用的研究对象之一. 通常用大写字母 $A, B, C, \cdots$ 表示. 集合中的元, 常用 $a, b, c, \cdots$ 表示. 元 a 与集合 A 之间的关系是属于和不属于的关系, 记为 $a \in A$ 或者 $a \notin A$. 如果一个集合中没有元, 称这样的集合为空集, 记为 $\varnothing$.

集合有两种表示方法, 列举法和描述法. 列举法就是把集合中的元一一列举出来. 描述法是利用集合中的元所满足的性质来刻画集合. 如果集合 A 是由具有性质 P 的所有元组成, 则集合 A 可表示为 $A = \{x \mid x \text{ 具有性质 } P\}$. 下面是一些集合的例子:

例 1.1　通常用 $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 分别表示所有自然数、整数、有理数、实数和复数的集合. □

例 1.2　设 m 为一正整数, 对任意的 $0 \leqslant i < m$, 定义

$$[i] = \{km + i \mid k \in \mathbb{Z}\},$$

则 $[0], [1], \cdots, [m-1]$ 都是集合, 在初等数论中, 称为模 m 的同余类或模 m 的剩余类. 以上面的集合为元, 构成另外一个集合, 记为 $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \cdots, [m-1]\}$. □

例 1.3　$\mathbb{Z}[x]$ 表示系数为整数的全体多项式构成的集合; $\mathbb{Q}[x]$、$\mathbb{R}[x]$ 和 $\mathbb{C}[x]$ 有类似的含义. 称集合

$$K = \{\alpha \in \mathbb{C} \mid \text{存在多项式 } f(x) \in \mathbb{Z}[x] \text{ 使得 } f(\alpha) = 0\}$$

中的元称为代数数. 集合

$$R=\{\alpha\in\mathbb{C}\,|\,\text{存在首一多项式 } f(x)\in\mathbb{Z}[x] \text{ 使得 } f(\alpha)=0\}$$

中的元称为代数整数. □

设 A, B 是两个集合, 如果对任意的元 $a\in A$, 都有 $a\in B$, 则称 A 为 B 的子集, 记为 $A\subseteq B$. 如果 $A\subseteq B$, 且存在元 $b\in B$ 使得 $b\notin A$, 则称 A 是 B 的真子集, 记为 $A\subset B$. 如果 $A\subseteq B$ 且 $B\subseteq A$, 则称集合 A 与集合 B 相等, 记为 $A=B$. 约定空集是任何集合的子集.

利用一些已知的集合, 可以构造新的集合, 下面的交集、并集、差集和直积是最基本的几种集合运算:

$$\begin{aligned}&\text{交集: } A\cap B=\{a\,|\,a\in A \text{ 且 } a\in B\};\\&\text{并集: } A\cup B=\{a\,|\,a\in A \text{ 或 } a\in B\};\\&\text{差集: } A\setminus B=\{a\,|\,a\in A \text{ 且 } a\notin B\};\\&\text{直积: } A\times B=\{(a,b)\,|\,a\in A,b\in B\}.\end{aligned}$$

集合的交集和并集的运算可以推广到无穷多个集合的情形, 设 $\{A_i\,|\,i\in I\}$ 为一个子集簇, 其中 I 为某个指标集, 定义该子集簇的交与并分别为

$$\begin{aligned}&\bigcap_{i\in I}A_i=\{x\,|\,\text{对任意的 } i\in I \text{ 有 } x\in A_i\},\\&\bigcup_{i\in I}A_i=\{x\,|\,\text{存在 } i\in I \text{ 使 } x\in A_i\}.\end{aligned}$$

设 A 是一个集合, 用 $|A|$ 表示集合 A 中元的个数, 称为集合 A 的阶, 有时也称为集合 A 的势. 如果集合 A 中元的个数有限, 则称为有限集, 否则称为无限集.

习　题

1. 证明对任意的集合 A, B, 有 $A\cap B$ 是 B 的子集; 而 A 和 B 都是 $A\cup B$ 的子集.

2. 设 $A=\{1,2,3\}$, $B=\{x,y,z\}$, 试求 $A\times B$ 和 $B\times A$.

3. 设 A 为集合, A 的所有子集组成的集合称为 A 的幂集, 记为 $\mathscr{L}(A)$. 设 $A=\{a_1,a_2,\cdots,a_n\}$ 为有限集, 试问 $\mathscr{L}(A)$ 中有多少个元; 并对 $n=4$ 写出所有这些元.

4. 在例 1.3 中, 试问集合 K 与 R 之间的包含关系. 请列举一些分别在集合 K 和 R 中的元, 圆周率 π 在 K 中吗? 在 R 中吗?

5. 对任意集合 A, B, C, 证明:

(1) $A\times(B\cup C)=(A\times B)\cup(A\times C)$;

(2) $(A\cap B)\times C=(A\times C)\cap(A\times C)$.

§1.2 映　射

定义 1.1. 设 A, B 是非空集合. 从 A 到 B 的映射是指一个对应法则, 通过这个法则, 对于集合 A 中的任意一个元 a, 有集合 B 中唯一的一个元 b 与之对应.

通常用字母 $f, g, h, \cdots$ 表示映射, 记为 $f: A\longrightarrow B$ 或者 $A\xrightarrow{f}B$. 其中 A 称为映射 f 的定义域, B 称为值域. b 称为 a 在映射 f 下的像, 而 a 称为 b 在映射 f 下的原像, 记为 $b=f(a)$ 或 $f: a\mapsto b$.

一个映射有三个要素: 定义域、值域和对应法则 f. 因此要确定一个映射, 实际上是对定义域 A 中的每一个元 a, 在值域 B 中给 a 找像. 设 f 和 g 是从集合 A 到集合 B 的两个映射, 如果对任意的 $a\in A$ 都有 $f(a)=g(a)$, 则称这两个映射相等, 记为 $f=g$.

如果映射 f 的定义域 A 和值域 B 相同, 即 $A=B$, 则称映射 f 是定义在集合 A 上的映射.

在映射的定义中, 对于任意 $a\in A$, 存在唯一的 $b\in B$ 与之对应. 在定义映射的时候, 如果元 a 有不同的表示形式, 则 $b=f(a)$ 必须与 a 的表示形式没有关系, 这就是像的唯一性, 称之为良性定义.

例 1.4　令 $A=B=\mathbb{Z}/5\mathbb{Z}=\{[0],[1],[2],[3],[4]\}$ (见例 1.2), 定义对应法则 $f: A\longrightarrow B$ 如下:

$$f([x])=\begin{cases}[x/2], & \text{如果 } x \text{ 是偶数},\\ [x], & \text{如果 } x \text{ 是奇数},\end{cases}$$

则 f 不是从 A 到 B 的映射, 因为 $[1]=[6]$, $[1]=f([1])=f([6])=[3]$, 这显然是不可能的. □

定义 1.2. 设 $f: A\longrightarrow B$ 是映射.

(1) 如果对任意的元 $a_1, a_2\in A$, 当 $a_1\neq a_2$ 时, 就有 $f(a_1)\neq f(a_2)$, 则称 f 是单射.

(2) 如果对任意的元 $b\in B$, 总存在元 $a\in A$, 使得 $b=f(a)$, 则称 f 为满射.

(3) 如果 f 既是单射又是满射, 则称 f 为一一映射, 也称为双射.

设 $f: A\longrightarrow B$ 是映射, 集合 C 是 A 的子集. 则 f 诱导一个从 C 到 B 的映射 f_1, 定义如下: 对任意的 $a\in C$, 令 $f_1(a)=f(a)$. 称映射 f_1 为映射 f 在集

合 C 上的限制.

若 f_1 是从集合 C 到 B 的映射, 而 $C \subseteq A$. 设 f 是从 A 到 B 的映射, 如果对任意的 $x \in C$, 都有 $f(x) = f_1(x)$, 则称映射 f 是 f_1 在集合 A 上的扩张. 易知限制是唯一的, 而扩张可能不是唯一的.

设 f 是从集合 A 到集合 B 的映射, g 是从集合 B 到集合 C 的映射, 则由 f 和 g 可诱导出一个从集合 A 到集合 C 的映射 h 如下: 对任意的 $a \in A$, 定义 $h(a) = g(f(a))$. 称 h 为映射 g 与 f 的合成, 记为 $h = g \circ f$, 可用下图表示为

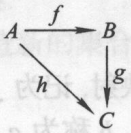

图 1.1 映射的合成

例 1.5 令 $A = \{1, 2, 3, 4\}$, f, g 是定义在 A 上的映射, 定义如下:

$$f(1) = 2, \quad f(2) = 4, \quad f(3) = 1, \quad f(4) = 3,$$

$$g(1) = 4, \quad g(2) = 1, \quad g(3) = 2, \quad g(4) = 3.$$

则 $f \circ g$ 和 $g \circ f$ 分别定义了 A 上的映射, 具体表示如下:

$$\begin{aligned}
&(f \circ g)(1) = f(g(1)) = f(4) = 3,\\
&(f \circ g)(2) = f(g(2)) = f(1) = 2,\\
&(f \circ g)(3) = f(g(3)) = f(2) = 4,\\
&(f \circ g)(4) = f(g(4)) = f(3) = 1,\\
&(g \circ f)(1) = g(f(1)) = g(2) = 1,\\
&(g \circ f)(2) = g(f(2)) = g(4) = 3,\\
&(g \circ f)(3) = g(f(3)) = g(1) = 4,\\
&(g \circ f)(4) = g(f(4)) = g(3) = 2.
\end{aligned}$$

这个例子也表示 $f \circ g$ 和 $g \circ f$ 是 A 上不同的两个映射. □

关于映射的合成, 有如下的命题:

定理 1.1. 设 $f : A \longrightarrow B$, $g : B \longrightarrow C$, $h : C \longrightarrow D$ 为映射, 则有 $(h \circ g) \circ f = h \circ (g \circ f)$.

证明. 容易知道 $h \circ (g \circ f)$ 和 $(h \circ g) \circ f$ 都是从 A 到 D 的映射. 对任意的

$a \in A$ 有

$$\big(h \circ (g \circ f)\big)(x) = h\big((g \circ f)(x)\big) = h\big(g(f(x))\big),$$
$$\big((h \circ g) \circ f\big)(x) = (h \circ g)(f(x)) = h\big(g(f(x))\big).$$

即 $h \circ (g \circ f) = (h \circ g) \circ f$, 证毕. □

设 $f: A \longrightarrow B$ 是映射, 对任意的 $S \subseteq A$, 令

$$f(S) = \{f(a) \,|\, a \in S\}.$$

称 $f(S)$ 为 S 在映射 f 下的像. 对任意的 $T \subseteq B$, 令

$$f^{-1}(T) = \{a \in A \,|\, f(a) \in T\}.$$

称 $f^{-1}(T)$ 为 T 在映射 f 之下的原像.

例 1.6　令 $A = \{1,2,3,4\}$, $B = \{a,b,c\}$, 定义映射 $f: A \longrightarrow B$ 如下:

$$f(1) = a, \quad f(2) = a, \quad f(3) = a, \quad f(4) = c.$$

映射 f 不是满射, 也不是单射. 令 $S = \{1,4\}$, 则 $f(S) = \{a,c\}$. 如果令 $T = \{a,b\} \subseteq B$, 则 $f^{-1}(T) = \{1,2,3\}$. □

利用像和原像的定义, 不难证明如下的命题:

定理 1.2. 设 $f: A \longrightarrow B$ 是映射, 则

(1) 对任意的 $S \subseteq A$, 有 $S \subseteq f^{-1}(f(S))$;

(2) 对任意的 $T \subseteq B$, 有 $f(f^{-1}(T)) \subseteq T$. 当 f 是满射时, 等号成立.

证明. 证明简单, 留给读者. □

设 $f: A \longrightarrow A$ 是映射, 如果对任意的 $x \in A$ 都有 $f(x) = x$, 则称 f 为恒等映射, 通常记为 I_A. 对于任意的映射 $f: A \longrightarrow B$, 利用映射合成的定义不难验证 $f \circ I_A = f$, $I_B \circ f = f$. 因此恒等映射也常称为单位映射.

利用映射的合成, 可以如下判断单射、满射和双射:

定理 1.3. 设 $f: A \longrightarrow B$ 是映射, 则

(1) f 是单射 $\Longleftrightarrow$ 存在映射 $g: B \longrightarrow A$, 使得 $g \circ f = I_A$;

(2) f 是满射 $\Longleftrightarrow$ 存在映射 $g: B \longrightarrow A$, 使得 $f \circ g = I_B$;

(3) f 是双射 $\Longleftrightarrow$ 存在映射 $g: B \longrightarrow A$, 使得 $g \circ f = I_A$, $f \circ g = I_B$, 这样的 g 是唯一的, 记为 f^{-1}.

证明. (1) 的证明. "$\Longrightarrow$": 如果 f 是单射, 即对任意的 x_1, $x_2 \in A$, 如果 $x_1 \neq x_2$, 就有 $f(x_1) \neq f(x_2)$. 因此定义映射 $g: B \longrightarrow A$ 如下:

$$g(b) = \begin{cases} a, & \text{如果存在 } a \in A, \text{使得 } f(a) = b \\ a_0, & \text{如果不存在 } a \in A, \text{使得 } f(a) = b \end{cases}$$

其中 a_0 为 A 中任一固定元. 则有: (i) g 是映射, 即对任一 $b \in B$, 存在唯一的 $a \in A$, 使得 $g(b) = a$. 这一点可由 g 的构造以及 f 是单射的条件来保证. (ii) $g \circ f = I_A$, 对任一 $a \in A$, 令 $b = f(a)$, 则 $g \circ f(a) = g(f(a)) = g(b) = a$, 因此 $g \circ f = I_A$.

"$\Longleftarrow$": 对任意的 $x_1, x_2 \in A$, 如果 $f(x_1) = f(x_2)$, 由于 $I_A = g \circ f$, 因此有

$$x_1 = I_A(x_1) = g \circ f(x_1) = g(f(x_1)) = g(f(x_2)) = g \circ f(x_2) = x_2,$$

因此 f 是单射.

(2) 和 (3) 的证明类似, 留作练习. 下面再证明 (3) 中 g 的唯一性. 设 g_1 和 g_2 满足 (3) 中的条件, 则有

$$g_1 = I_A \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ I_B = g_2.$$

定理证毕. □

定理 1.3 (3) 中的 g 称为映射 f 的逆映射. 当两个集合 A 和 B 之间存在一个双射时, 这两个集合含有一样多的元, 即 $|A| = |B|$, 通常称它们是等势的.

设 $X = \{1, 2, 3, \cdots, n\}$ 为 n 元集合, 令 $S_n = \{$ 从 X 到 X 上所有的一一映射 $\}$. 则对任意的 $\sigma \in S_n$, σ 可用如下的方法表示:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix}$$

(其中 $i_1, i_2, \cdots, i_n$ 是元 1, 2, $\cdots$, n 的一个置换.) 这个映射表示 $\sigma(1) = i_1$, $\sigma(2) = i_2, \cdots, \sigma(n) = i_n$.

习　题

1. 试举例说明单射、满射、一一映射、单射但不是满射及满射但不是单射.

2. 证明定理 1.2.

3. 举例说明定理 1.2 中的等号可能不成立.

4. 设 $f: A \longrightarrow B$ 是映射, 则有 $f \circ I_A = f = I_B \circ f$.

5. 试写出 S_3 中的所有元.

6. 设 $\sigma=\begin{pmatrix}1&2&3&4&5\\3&1&5&2&4\end{pmatrix}$, $\tau=\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}\in S_5$. 试计算如下的合成映射 σ^{-1}, $\sigma\tau$, $\tau\sigma$, $\sigma\tau\sigma^{-1}$. $\sigma\tau$ 是否等于 $\tau\sigma$?

7. 设 $f\colon A\longrightarrow B$ 是映射, 设 $S_1,S_2\subseteq A$, 试确定 $f(S_1\cup S_2)$ 与 $f(S_1)\cup f(S_2)$ 的包含关系, $f(S_1\cap S_2)$ 与 $f(S_1)\cap f(S_2)$ 的包含关系?

若 $T_1,T_2\subseteq B$, 试确定 $f^{-1}(T_1\cap T_2)$ 与 $f^{-1}(T_1)\cap f^{-1}(T_2)$ 的包含关系, $f^{-1}(T_1\cup T_2)$ 与 $f^{-1}(T_1)\cup f^{-1}(T_2)$ 的包含关系?

8. 设 $f\colon A\longrightarrow B$ 是映射, 则

(1) 对任意的 $S\subseteq A$, 有 $f(S)=f\circ f^{-1}\circ f(S)$;

(2) 对任意的 $T\subseteq B$, 有 $f^{-1}(T)=f^{-1}\circ f\circ f^{-1}(T)$.

9. 设 $|A|=m$, $|B|=n$, 试问从 A 到 B 中可建立多少个映射?

10. 设 $f\colon A\longrightarrow B$, $g\colon B\longrightarrow C$ 是映射, $h=g\circ f$. 证明:

(1) 若 h 是满射, 则 g 是满射;

(2) 若 h 是单射, 则 f 是单射.

§1.3 等 价 关 系

设 A 是一个集合, R 是积集合 $A\times A=\{(a,b)\,|\,a,b\in A\}$ 的子集, 则称 R 是集合 A 上的一个关系. 对于任意的 $a,b\in A$, 如果 $(a,b)\in R$, 则称 a 与 b 具有关系 R, 记为 aRb. 否则就称 a 与 b 不具有关系 R.

定义 1.3. 设 A 为一集合, R 是 A 上的一个关系, 如果 R 满足下列条件:

- **自反性:** 对任意的 $x\in A$, 有 $(x,x)\in R$;
- **对称性:** 对任意的 $x,y\in A$, 如果 $(x,y)\in R$, 则有 $(y,x)\in R$;
- **传递性:** 对任意的 $x,y,z\in A$, 如果 $(x,y)\in R$, $(y,z)\in R$, 则 $(x,z)\in R$.

则称 R 为集合 A 上的一个等价关系. 通常将等价关系 R 记为 "$\sim$".

例 1.7 设 $X=\{1,2,3,4,5\}$, 令 $R=\{(1,2),(2,3),(3,4),(4,5)\}$, 则 R 定义了集合 A 上的一个关系, 但是它不是等价关系. 因为自反性和对称性都不成立. □

例 1.8 考虑有理数域 $\mathbb{Q}$ 上所有柯西数列所构成的集合 A, 即

$$A=\{\{a_n\}_{n=1}^{\infty}\,|\,a_n\in\mathbb{Q}\text{ 且 }\{a_n\}\text{ 是收敛数列}\}.$$

在集合 A 上定义关系 $\sim$ 如下: 对于任意 $\{a_n\}, \{b_n\} \in A$, 令

$$\lim_{n\to\infty} a_n = a, \quad \lim_{n\to\infty} b_n = b.$$

如果 $a = b$, 则定义 $\{a_n\} \sim \{b_n\}$. 容易验证上面定义的关系 $\sim$ 为 A 上的等价关系. □

例 1.9　设 $A = \mathbb{Z}$, $m > 1$ 是一个正整数, 定义 $R = \{(x, y) \mid x, y \in A$, 且 $x - y$ 能被 m 整除 $\}$. 容易验证, R 是 $\mathbb{Z}$ 上的等价关系. □

设 R 为集合 A 上的等价关系, 对任一 $a \in A$, 称与 a 等价的所有元组成的集合为元 a 所属的等价类, 记为 $[a]$, 即

$$[a] = \{b \in A \mid (a, b) \in R\}.$$

a 称为这个等价类的代表元. 所有等价类构成的集合称为 A 关于 R 的商集, 记为 A/R, 即 $A/R = \{[a] \mid a \in A\}$.

例 1.10　设 $A = \{a, b, c, d, e\}$, 令 $R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, a), (c, d), (d, c), (c, e), (e, c), (d, e), (e, d)\}$. 容易验证 R 为集合 A 上的等价关系, 每个元所属等价类如下:

$$[a] = \{a, b\},$$
$$[b] = \{a, b\},$$
$$[c] = \{c, d, e\},$$
$$[d] = \{c, d, e\},$$
$$[e] = \{c, d, e\}.$$

因此集合 A 关于等价关系 R 只有两个等价类, 故商集 $A/R = \{[a], [c]\}$. □

命题 1.1. *设 R 为集合 A 上的等价关系, 则对任意的 $a, b \in A$, $[a] = [b]$ 当且仅当 $(a, b) \in R$.*

证明. 一方面, 如果 $[a] = [b]$, 则 $b \in [a]$, 由等价类的定义可知 $(a, b) \in R$.

另一方面, 如果 $(a, b) \in R$, 那么对任一 $c \in [b]$, 有 $(b, c) \in R$, 由传递性知 $(a, c) \in R$, 从而 $c \in [a]$, 故 $[b] \subset [a]$. 由对称性可知 $(b, a) \in R$. 对任意的 $c \in [a]$, 有 $(a, c) \in R$, 由传递性可知 $(b, c) \in R$, 从而 $c \in [b]$, 因此 $[a] \subset [b]$. 所以 $[a] = [b]$, 命题得证. □

命题 1.1 表明, 一个等价类可以选择其中的任何一个元为代表元.

定义 1.4. 设 A 是一个集合, $\{U_i \mid i \in I\}$ 是 A 的子集簇, 其中 I 是某个确定的指标集, 如果满足:

(1) 对任意的 $i \neq j, i, j \in I$, 有 $U_i \cap U_j = \varnothing$;

(2) $\bigcup\limits_{i \in I} U_i = A$;

则称 $\{U_i \mid i \in I\}$ 是集合 A 的一个划分.

定理 1.4. 若 R 是集合 A 上的等价关系, 则商集 A/R 是 A 上的一个划分.

证明. (1) 先证明对 A/R 中的任意两个等价类 $[a]$ 和 $[b]$, 如果 $[a] \neq [b]$, 则 $[a] \cap [b] = \varnothing$. 反证法, 如果 $[a] \cap [b] \neq \varnothing$. 任取 $c \in [a] \cap [b]$. 由 $c \in [a]$ 可知 $(a, c) \in R$, 由 $c \in [b]$ 可知 $(b, c) \in R$, 由对称性知 $(c, b) \in R$. 由传递性可知 $(a, b) \in R$, 再由命题 1.1 知 $[a] = [b]$, 与题设矛盾.

(2) 再证明 $A = \bigcup\limits_{[a] \in A/R} [a]$. 一方面, 对任意的 $[a] \in A/R$, 有 $[a] \subseteq A$, 因此 $\bigcup\limits_{[a] \in A/R} [a] \subset A$. 另一方面, 对任意的 $a \in A$, 有 $a \in [a] \subseteq \bigcup\limits_{[a] \in A/R} [a]$, 因此 $A \subseteq \bigcup\limits_{[a] \in A/R} [a]$. □

定理 1.5. 若 $\{U_i \mid i \in I\}$ 是集合 A 的一个划分, 则存在 A 上的一个等价关系 R, 使得 $A/R = \{U_i \mid i \in I\}$.

证明. 定义 A 上的关系 R 如下: $R = \{(a, b) \mid$ 存在 U_i 使得 $a, b \in U_i\}$. 容易验证 R 为 A 上的等价关系. 为了方便, 令 $B = \{U_i \mid i \in I\}$. 对任意的 $[a] \in A/R$, 由于 B 是集合 A 的一个划分, 因此存在某个 $U_i \in B$, 使得 $a \in U_i$. 由 R 的定义可知 $[a] = U_i$, 这说明 $[a] \in B$, 从而 $A/R \subset B$. 另一方面, 对任意的 $U_i \in B$, 选取 $a \in U_i$. 由于 $[a] = U_i$, 因此 $U_i \in A/R$, 即 $B \subset A/R$. □

上面两个定理表明, 集合的划分和等价关系是一回事.

例 1.11 令集合 $A = \{a, b, c\}, U_1 = \{a\}, U_2 = \{b, c\}$. 那么 $\{U_1, U_2\}$ 是集合 A 的一个划分, 利用定理 1.5 的证明方法, 该划分对应的等价关系为: $R = \{(a, a), (b, b), (c, c), (b, c), (c, b)\}$. □

设 $f : A \longrightarrow B$ 是一个映射, 则 f 可诱导出集合 A 上的一个关系 R 如下:

$$R = \{(a, b) \mid f(a) = f(b), a, b \in A\},$$

容易验证 R 是集合 A 上的等价关系, 其商集为 $A/R = \{[a] \mid a \in A\}$. 进一步, 映射 f 还可诱导出一个从集合 A/R 到集合 B 的映射 $\overline{f}$: $\overline{f}([a]) = f(a)$. 于是有如下的定理:

定理 1.6. (1) 上述定义的 $\overline{f}$ 是单射;

(2) $\overline{f}$ 是双射 $\Longleftrightarrow$ f 是满射.

证明. 首先证明 $\overline{f}$ 的定义是良性的. 对任意的 $[a], [b] \in A/R$, 如果 $[a] = [b]$, 由命题 1.1 知 $(a, b) \in R$, 因此 $f(a) = f(b)$, 从而 $\overline{f}([a]) = \overline{f}([b])$.

再证明 $\overline{f}$ 是单射. 对任意的 $[a], [b] \in A/R$, 如果 $\overline{f}([a]) = \overline{f}([b])$, 即 $f(a) = f(b)$, 因此 $(a, b) \in R$, 由命题 1.1 知 $[a] = [b]$.

最后证明 (2). 由 (1) 知 $\overline{f}$ 是单射, 因此 $\overline{f}$ 是双射当且仅当 $\overline{f}$ 是满射. 不难看出 $\overline{f}$ 是满射当且仅当 f 是满射, 证毕. □

上述命题可用下图表示为

图 1.2 映射的分解

其中 $\pi : A \longrightarrow A/R$, $\pi(a) = [a]$, 称之为自然映射或者典范映射.

例 1.12 设 $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, 从 A 到 B 的一个映射 f 定义如下: $f(1) = f(2) = f(3) = a$, $f(4) = b$. 则由 f 诱导出的等价关系为

$$R = \{(1,1), (2,2), (3,3), (1,2), (2,1), (1,3), (3,1), (2,3), (3,2), (4,4)\}.$$

它的商集为 $A/R = \{[1], [4]\}$, 其中 $[1] = \{1, 2, 3\} = [2] = [3]$, $[4] = \{4\}$.

映射 f 诱导的从集合 $A/R = \{[1], [4]\}$ 到 B 的映射 $\overline{f}$ 如下: $\overline{f}([1]) = f(1) = a$, $\overline{f}([4]) = c$. 易知 $\overline{f}$ 的定义与 A/R 中元的代表元的选择无关, 即 $\overline{f}$ 是良性定义, 而且 $\overline{f}$ 是单射. 由于 f 不是满射, 因此 $\overline{f}$ 也不是双射. □

习 题

1. 设 $A = \{1, 2, 3, 4, 5, 6\}$, R 是 A 上的小于关系, 试写出 R 的全体元.

2. 设 $A = \mathbb{R}$ 为全体实数的集合, R 是 A 上的小于等于关系, 问 R 满足等价关系定义中的几条?

3. 设 $A = \mathbb{C}$ 为全体复数的集合, $R = \{(x, y) \mid x, y \in \mathbb{C}, |x| = |y|\}$ (这里 $|x|$ 表示复数 x 的模). 问: R 是否是等价关系? 若是, 证明之, 由它所确定的 A 的划分是什么 (用几何语言描述).

4. 设 $A = \{1, 2, 3, 4, 5, 6\}$, $U_1 = \{1, 2, 3\}$, $U_2 = \{4\}$, $U_3 = \{5, 6\}$, 试决定 A 上的等价关系 R, 使得 $A/R = \{U_1, U_2, U_3\}$.

5. 设 $|A|=m$, 试问在 A 上可定义多少个关系? 有多少个等价关系?

6. 设 $A=\{1,2,3,4,5,6\}$, $U_1=\{1,2,3\}$, $U_2=\{4\}$, $U_3=\{5,6\}$.

(1) 试构造映射 $f: A\longrightarrow B$, 使之决定的等价关系 R 满足 $A/R=\{U_1, U_2, U_3\}$;

(2) 试求映射 $\overline{f}: A/R\longrightarrow B$.

§1.4 整除 · 欧氏除法

任意两个整数的和、差、积仍为整数, 但是两个整数的商 (分母不为零)却不一定是整数, 因此引入整除的概念.

定义 1.5. 设 $a, b\in\mathbb{Z}$, 若存在一整数 q, 使得等式

$$a=bq \tag{1.1}$$

成立, 则称 b 整除 a, 或 a 可以被 b 整除, 记成 $b|a$. 此时也称 b 是 a 的因数, a 是 b 的倍数; 若这样的整数 q 不存在, 则称 b 不能整除 a 或 a 不能被 b 整除, 并记为 $b\nmid a$.

对于整除, 有下面简单的性质:

定理 1.7. (1) 如果 $b|a$, $c|b$, 则 $c|a$;

(2) 如果 $m|a$, $m|b$, 则 $m|(a\pm b)$;

(3) 如果 $m|a_1, m|a_2, \cdots, m|a_n$, 则对任意的整数 $q_1, q_2, \cdots, q_n$, 都有 $m|(q_1a_1+q_2a_2+\cdots+q_na_n)$.

证明. 只证明 (3), (1) 和 (2) 可类似地证明.

因为 $m|a_i$, 所以存在 $r_i\in\mathbb{Z}$, 使得 $a_i=r_im$, $i=1, 2, \cdots, n$. 因此

$$q_1a_1+q_2a_2+\cdots+q_na_n=(q_1r_1+q_2r_2+\cdots+q_nr_n)m,$$

而 $q_1r_1+q_2r_2+\cdots+q_nr_n\in\mathbb{Z}$, 因此 $m|(q_1a_1+q_2a_2+\cdots+q_na_n)$. □

定理 1.8 (带余除法). 若 $a, b\in\mathbb{Z}$, $b>0$, 则存在唯一的整数 q 与 r, 使得

$$a=bq+r,\quad 0\leqslant r<b \tag{1.2}$$

成立.

证明. 考虑下面的一个整数序列:

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots.$$