21世纪高等院校选用教材
师范类

近世代数

南京师范大学
朱平天　李伯蕻　邹　园　编

科学出版社

21世纪高等院校选用教材(师范类)

近 世 代 数

南京师范大学

朱平天 李伯蕻 邹园 编

科学出版社

2001

内 容 简 介

本书是根据师范院校教学大纲的要求编写的.全书分为四章:第一章讲基本概念,它是后面各章的基础;第二章介绍群的基本理论;第三章介绍环的基本理论;第四章专门讲整环里的因子分解.

本书可作为师范院校数学教育专业(包括全日制、函授、夜大等)本科学生学习近世代数的教材,也可供从事代数、数论、几何、函数、计算机等的专业人员或教师作为参考书.

图书在版编目(CIP)数据

近世代数/朱平天,李伯棠,邹园编. —北京:科学出版社,2001.8
(21世纪高等院校选用教材(师范类))
ISBN 7-03-009459-X

Ⅰ.近… Ⅱ.①朱…②李…③邹… Ⅲ.抽象代数
Ⅳ.O153

中国版本图书馆CIP数据核字(2001)第045994号

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
新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2001年8月第 一 版 开本:720×1000 1/16
2001年8月第一次印刷 印张:12
印数:1—5 000 字数:213 000
定价: 18.00元
(如有印装质量问题,我社负责调换〈新欣〉)

前　言

近世代数是以讨论代数体系的性质与构造为中心的一门学科.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,特别是计算机的发展与推广,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.目前,在高等学校相关系科都开设了近世代数这门课程,作为师范类高等学校数学系本科生,近世代数是必修课程.

近世代数内容丰富,在师范类高校不可能全部讲授,本书根据师范类教学大纲、教学时数和高等师范学校学生的实际需要,选取了近世代数的基本概念和基本理论的内容编写而成.全书以群、环理论为重点,将域的扩张理论适当压缩并入环论中,既丰富了内容,又精简了章节,可以在规定的80学时左右讲授完.

在全书编写过程中,我们努力作到突出重点,精选典型例题.叙述简明扼要,运用新的符号,内容编排由浅入深符合认识规律,加强基本训练.为了培养学生掌握和运用知识的能力,每节后都配有习题,每章后有复习题,书末还附有部分习题解答或提示,便于自学者参考.

本教材是从1996年开始编写的,1997年完成初稿,经我校以及有关兄弟院校试用4年,其间,校内外代数专家们提出了许多宝贵意见,数易其稿.这其中包含了南京师范大学数学系代数组几代人的科研成果与教学经验,是集体创作的结晶.随着我们认识的不断提高和教育改革的不断深入,我们也将不断修订使之更臻完善,敬请各位专家和广大读者在使用中提出宝贵的意见.

本教材在编写过程中,得到系领导和出版社大力支持,以及同行专家关心,谨此致谢.

编　者

2001年7月

目　录

第一章　基本概念

本章中介绍的一些基本概念是数学各个分支的基础，也是学习本书后面各个代数体系的必备知识.

§1.1　集　　合

集合是近代数学上最基本的概念之一，它指由一些事物所组成的一个整体.

集合通常用大写拉丁字母 $A,B,C,\cdots$ 表示. 特别，粗体 **C** 表示复数集，粗体 **R** 表示实数集，粗体 **Q** 表示有理数集，粗体 **Z** 表示整数集，粗体 **N** 表示自然数集，又 $\mathbf{C}^*$ 表示非零复数集，$\mathbf{R}^+$ 表示正实数集，$\mathbf{R}^-$ 表示负实数集，$2\mathbf{Z}$ 表示偶数集，其余类同.

组成一个集合的各个事物称为这个集合的元素，通常用小写拉丁字母 a，$b,c,\cdots$ 表示. 当 a 是集合 A 的元素时，称为 a 属于 A，记作“$a\in A$”；当 a 不是集合 A 的元素时，称为 a 不属于 A，记作“$a\notin A$”或“$a\overline{\in}A$”.

不含任何元素的集合称为空集，记作“$\varnothing$”. 由全部元素所组成的集合称为全集，记作“U”.

包含有限个元素的集合称为有限集，否则称为无限集. 有限集 A 所包含的元素个数是一个非负整数，记作 $|A|$. 特别，$|\varnothing|=0$.

表示一个集合的方法通常有两种. 一种是列举法，即列出它的所有元素，并且用一对花括号括起来. 例如包含两个整数 $-1,3$ 的集合 S 记作

$$S=\{-1,3\}.$$

另一种是描述法，即用它的元素所具有的特性来刻画，例如

$$T=\{x\mid x^2-2x-3=0\}.$$

表示 T 是由方程 $x^2-2x-3=0$ 的根所组成的集合. 又如

$$\left\{\frac{a}{b}\,\middle|\,a,b\in\mathbf{Z},b\neq 0\right\}$$

表示有理数集 **Q**，而

$$\{a+bi\mid a,b\in\mathbf{R}\}$$

表示复数集 $\mathbf{C}$.

在本书中,有一些语句经常出现,为了简便,现引用一些逻辑符号予以表达."对于任意 $a\in A$"表示为"$\forall a\in A$","存在一个 $a\in A$"表示为"$\exists a\in A$","存在惟一的 $a\in A$"表示为"$\exists!\ a\in A$". 设 P,Q 是两个命题,"若 P 成立,则 Q 成立"表示为"$P\Rightarrow Q$","P 成立当且仅当 Q 成立"表示为"$P\Leftrightarrow Q$".

定义 1.1 设 A,B 是两个集合.

(1) 若

$$\forall a\in A\Rightarrow a\in B,$$

则称 A 是 B 的子集,B 是 A 的扩集,或 A 包含于 B,B 包含 A,记作"$A\subseteq B$"或"$B\supseteq A$". 当 A 不是 B 的子集时,记作"$A\nsubseteq B$".

(2) 若 $A\subseteq B$,且 $\exists b\in B$,而 $b\notin A$,则称 A 是 B 的真子集,记作"$A\subset B$"或"$B\supset A$". 例如,对于任何集合 A,都有 $A\subseteq A$. 又如,$\{1,2\}\subset\{1,2,3\}$.

空集$\varnothing$是任何集合 A 的子集.

集合的包含关系具有下列性质:

(1) 自反性:对于任意的集合 A,有 $A\subseteq A$;

(2) 传递性:若 $A\subseteq B,B\subseteq C$,则 $A\subseteq C$.

定义 1.2 设 A,B 是两个集合,若 $A\subseteq B$,且 $B\subseteq A$,则称 A 与 B 相等,记作"$A=B$".

两个相等的集合包含相同的元素. 例如上面列出的两个集合 S 与 T 相等.

设 A 是一个给定的集合,由 A 的全体子集所组成的集合称为 A 的幂集,记作 2^A. 例如,设 $A=\{1,2,3\}$,则

$$2^A=\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},A\}.$$

下面讨论集合的运算.

定义 1.3 设 A,B 是全集 U 的两个子集.

(1) 由 A 或 B 中所有元素所组成的集合称为 A 与 B 的并,记作"$A\cup B$",即

$$A\cup B=\{x\mid x\in A\text{ 或 }x\in B\}.$$

(2) 由 A 与 B 的所有公共元素所组成的集合称为 A 与 B 的交,记作"$A\cap B$",即

$$A\cap B=\{x\mid x\in A\text{ 且 }x\in B\}.$$

(3) 在全集 U 中取出 A 的全部元素,余下的所有元素所组成的集合称为

A 的余，记作“A'”，即

$$A' = \{x \mid x \in U, x \notin A\}.$$

特别

$$U' = \varnothing,\ \varnothing' = U.$$

例 1　设

$$U = \{x \mid 2 \leqslant x \leqslant 10, x \in \mathbf{Z}\},$$

$$A = \{2,4,6,8\},$$

$$B = \{2,3,5,7\}.$$

则

$$A \cup B = \{2,3,4,5,6,7,8\},$$

$$A \cap B = \{2\},$$

$$A' = \{3,5,7,9,10\},$$

$$B' = \{4,6,8,9,10\}.$$

集合的上述三种运算具有下列性质.

定理 1.1　设 A,B,C 是集合 U 的三个子集，则有

(1) 交换律：$A \cup B = B \cup A$，$A \cap B = B \cap A$；

(2) 结合律：$(A \cup B) \cup C = A \cup (B \cup C)$，
$(A \cap B) \cap C = A \cap (B \cap C)$；

(3) 分配律：$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$，
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$；

(4) 模　律：若 $A \subseteq C$，则 $A \cup (B \cap C) = (A \cup B) \cap C$；

(5) 幂等律：$A \cup A = A$，$A \cap A = A$；

(6) 吸收律：$A \cup (A \cap B) = A \cap (A \cup B) = A$；

(7) 两极律：$A \cup U = U$，$A \cap U = A$，
$A \cup \varnothing = A$，$A \cap \varnothing = \varnothing$；

(8) 补余律：$A \cup A' = U$，$A \cap A' = \varnothing$；

(9) 对合律：$(A')' = A$；

(10) 对偶律：$(A \cup B)' = A' \cap B'$，　$(A \cap B)' = A' \cup B'$.

证　我们证明(4)作为例子，其余留给读者练习.

$\forall x \in A \cup (B \cap C)$，有 $x \in A$ 或 $x \in B \cap C$. 当 $x \in A$ 时，有 $x \in A \cup B$，又因为 $A \subseteq C$，所以 $x \in C$，从而 $x \in (A \cup B) \cap C$；当 $x \in B \cap C$ 时，有 $x \in B$

且$x\in C$,于是 $x\in A\cup B$ 且$x\in C$,从而 $x\in(A\cup B)\cap C$. 由此推出,$A\cup(B\cap C)\subseteq(A\cup B)\cap C$.

反之,$\forall x\in(A\cup B)\cap C$,有 $x\in A\cup B$ 且$x\in C$,于是"$x\in A$ 或$x\in B$",且 $x\in C$,所以 $x\in A$,或"$x\in B$ 且$x\in C$",从而 $x\in A\cup(B\cap C)$. 由此推出,$(A\cup B)\cap C\subseteq A\cup(B\cap C)$.

因此,$A\cup(B\cap C)=(A\cup B)\cap C$.

两个集合的并、交的概念可以推广到任意多个集合的情形. 设 I 是一个下标集,$A_i(i\in I)$是集合 U 的子集,定义集合族$\{A_i\mid i\in I\}$的并为

$$\bigcup_{i\in I}A_i=\{x\mid \exists\, i\in I,\ x\in A_i\},$$

集合族$\{A_i\mid i\in I\}$的交为

$$\bigcap_{i\in I}A_i=\{x\mid \forall\, i\in I, x\in A_i\}.$$

特别,当下标集 $I=\varnothing$时,规定:

$$\bigcup_{i\in I}A_i=\varnothing,\ \bigcap_{i\in I}A_i=U.$$

对于 U 的任意子集B,下列两个等式成立:

$$B\cup\left(\bigcap_{i\in I}A_i\right)=\bigcap_{i\in I}(B\cup A_i),$$

$$B\cap\left(\bigcup_{i\in I}A_i\right)=\bigcup_{i\in I}(B\cap A_i).$$

例 2 设 A,B 是全集U 的两个子集,证明:若 $A\cup B=U$,$A\cap B=\varnothing$,则 $B=A'$.

证 因为

$$A'=A'\cap U=A'\cap(A\cup B)=(A'\cap A)\cup(A'\cap B)$$

$$=\varnothing\cup(A'\cap B)=A'\cap B,$$

所以

$$A'\subseteq B.$$

又因为

$$A'=A'\cup\varnothing=A'\cup(A\cap B)=(A'\cup A)\cap(A'\cup B)$$

$$=U\cap(A'\cup B)=A'\cup B,$$

所以

$$B \subseteq A'.$$

因此 $A' = B$.

定义 1.4 设 A, B 是全集 U 的两个子集,由属于 A 而不属于 B 的所有元素所组成的集合称为 B 在 A 中的余,记作"$A \setminus B$",即

$$A \setminus B = \{x \mid x \in A \text{ 且 } x \notin B\}$$

$$= \{x \mid x \in A \text{ 且 } x \in B'\} = A \cap B'.$$

特别,

$$U \setminus A = A'.$$

例如,对于例 1 中的集合 A, B,有

$$A \setminus B = \{4,6,8\},$$

$$B \setminus A = \{3,5,7\}.$$

例 3 证明:

(1) $A \setminus B = \varnothing \Leftrightarrow A \subseteq B$;

(2) $A \setminus B = A \Leftrightarrow A \cap B = \varnothing$.

证 (1) 若 $A \setminus B = \varnothing$,则

$$A = A \cap U = A \cap (B \cup B') = (A \cap B) \cup (A \cap B')$$

$$= (A \cap B) \cup (A \setminus B) = (A \cap B) \cup \varnothing = A \cap B \subseteq B.$$

反之,若 $A \subseteq B$,则

$$A \setminus B = A \cap B' = (A \cap B) \cap B'$$

$$= A \cap (B \cap B') = A \cap \varnothing = \varnothing.$$

因此 $A \setminus B = \varnothing \Leftrightarrow A \subseteq B$.

(2) 若 $A \setminus B = A$,则

$$A \cap B = (A \setminus B) \cap B = (A \cap B') \cap B$$

$$= A \cap (B' \cap B) = A \cap \varnothing = \varnothing.$$

反之,若 $A\cap B=\varnothing$,则

$$\begin{aligned}A &= A\cap U = A\cap (B\cup B')\\ &=(A\cap B)\cup(A\cap B')\\ &=\varnothing\cup(A\cap B')=A\cap B'=A\setminus B.\end{aligned}$$

因此 $A\setminus B=A\Leftrightarrow A\cap B=\varnothing$.

习 题

1. 指出下列各命题的真假.

(1) $1\in\{1\}$; (2) $1\subseteq\{1\}$; (3) $1=\{1\}$;

(4) $\{1\}\in\{1\}$; (5) $\{1\}\subseteq\{1\}$; (6) $\{1\}\in\{1,\{1\}\}$;

(7) $\varnothing\in\{1\}$; (8) $\varnothing\subseteq\{1\}$; (9) $\varnothing\subset\{1\}$;

(10) $\varnothing\in\varnothing$; (11) $\varnothing\subseteq\varnothing$; (12) $\varnothing\subset\varnothing$.

2. 设 $U=\{a,b,c,d,e,f,g,h\}$, $M=\{a,c,e,h\}$, $N=\{a,d,e,f,g\}$,求 $M\cup N$, $M\cap N$, $M\setminus N$, $N\setminus M$, M', N', $M'\cup N'$, $M'\cap N'$.

3. 设 A,B 是两个集合,若 $A\cap B=A\cup B$,证明:$A=B$.

4. 设 A,B,C 是三个集合,若 $A\cap B=A\cap C$, $A\cup B=A\cup C$,证明:$B=C$.

5. 证明下列三个命题等价:

(1) $A\subseteq B$;

(2) $A\cap B=A$;

(3) $A\cup B=B$.

6. 设 A,B,C 是三个集合,证明:

(1) $A\setminus B=A\setminus(A\cap B)$;

(2) $A\setminus(A\setminus B)=A\cap B$;

(3) $A\setminus(B\cup C)=(A\setminus B)\cap(A\setminus C)$;

(4) $A\setminus(B\cap C)=(A\setminus B)\cup(A\setminus C)$;

(5) $A\cap(B\setminus C)=(A\cap B)\setminus(A\cap C)$;

(6) $(A\setminus B)\cup(B\setminus A)=(A\cup B)\setminus(A\cap B)$.

7. 设 $A=\{x\mid x^2-2x-3=0\}$,写出 A 的幂集 2^A.

8. 设 A 是包含 n 个元素的有限集,求 A 的幂集 2^A 所包含元素个数.

§1.2 映 射

映射是在两个集合之间建立的一种联系,它也是近代数学上最基本的概念之一.我们借助通俗的词"法则"来说明映射的含义.

定义 1.5 设 A,B 是两个给定的非空集合,若有一个对应法则 f,使

$\forall a\in A$,通过 f,$\exists!\ b\in B$ 与其对应,则称 f 是 A 到 B 的一个映射,记作

$$f:A\to B \text{ 或 } A\xrightarrow{f}B.$$

A 称为 f 的定义域,B 称为 f 的值域. b 称为 a 在 f 下的像,a 称为 b 在 f 下的原像,记作 $b=f(a)$ 或 $f:a\mapsto b$.

例 1　设 $A=\{a,b,c\}$,$B=\{1,2,3,4\}$,则

$$f:a\mapsto 1,b\mapsto 2,c\mapsto 3$$

是 A 到 B 的一个映射.

$$g:a\mapsto 2,b\mapsto 2,c\mapsto 2$$

也是 A 到 B 的一个映射. 但是,

$$h:a\mapsto 1,b\mapsto 2$$

不是 A 到 B 的映射,因为 $c\in A$ 在 h 下没有像.

例 2　设 $A=\mathbf{Z}$,$B=\mathbf{N}$,则

$$f:n\mapsto |n|+1,\forall n\in\mathbf{Z}$$

是 $\mathbf{Z}$ 到 $\mathbf{N}$ 的一个映射. 但是,

$$h:n\mapsto |n|,\forall n\in\mathbf{Z}$$

不是 $\mathbf{Z}$ 到 $\mathbf{N}$ 的映射,因为 $0\in\mathbf{Z}$ 在 h 下的像 0 不在 $\mathbf{N}$ 中.

例 3　设 $A=\mathbf{R}^+=\{x\mid x\in\mathbf{R},x>0\}$,$B=\mathbf{R}$,则

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

是 R^+ 到 $\mathbf{R}$ 的一个映射. 但是,

$$h:x\mapsto\pm\sqrt{x},\forall x\in\mathbf{R}^+$$

不是 $\mathbf{R}^+$ 到 $\mathbf{R}$ 的映射,因为在 h 下,$x\in\mathbf{R}^+$ 在 $\mathbf{R}$ 中的像不惟一.

例 4　设 $A=B=\mathbf{Z}$,则

$$f:n\mapsto n+1,\forall n\in\mathbf{Z}$$

是 $\mathbf{Z}$ 到 $\mathbf{Z}$ 的一个映射.

例 5　设 A 是一个非空集合,则

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

是 A 到 A 自身的一个映射,称为 A 的恒等映射(或单位映射).

例 6 设 $A\subseteq B$,则

$$i_A: x \mapsto x, \forall x \in A$$

是 A 到 B 的一个映射,称为 A 到 B 的包含映射.

定义 1.6 设 f 是 A 到 B 的映射,

(1) 若 $S\subseteq A$,则称 B 的子集:

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

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

(2) 若 $T\subseteq B$,则称 A 的子集:

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

为 T 在 f 下的完全原像,记作 $f^{-1}(T)$.特别,当 T 是单元集时,$f^{-1}(\{b\})$也可记作 $f^{-1}(b)$.

例如,对于例 1 中 A 到 B 的映射 f,g,设 $S=\{a,b\}$是 A 的一个子集,$T=\{2,3,4\}$是 B 的一个子集,则

$$f(S)=\{1,2\}, f^{-1}(T)=\{b,c\},$$

$$g(S)=\{2\}, g^{-1}(T)=\{a,b,c\}=A.$$

而

$$\mathrm{Im}f=f(A)=\{1,2,3\}, f^{-1}(2)=\{b\}, f^{-1}(4)=\varnothing,$$

$$\mathrm{Im}g=g(A)=\{2\}, g^{-1}(2)=\{a,b,c\}=A, g^{-1}(4)=\varnothing.$$

定义 1.7 设 f 是 A_1 到 B_1 的映射,g 是 A_2 到 B_2 的映射,若 $A_1=A_2$,$B_1=B_2$,且 $\forall x\in A_1$,都有 $f(x)=g(x)$,则称 f 与 g 相等,记作 $f=g$.

例如,设 $A=\{1,2,3\}$,$B=\{1,2,\cdots,16\}$是两个集合,$f: n \mapsto 2^n$, $g: n \mapsto n^2-n+2$ 是两个 A 到 B 的映射.因为 $f(1)=2=g(1)$,$f(2)=4=g(2)$,$f(3)=8=g(3)$,所以 $f=g$.但是,如果将 A 改作 $D=\{1,2,3,4\}$,并把 f,g 看作 D 到 B 的映射,因为 $f(4)=16$, $g(4)=14$,所以 $f\neq g$.

定义 1.8 设 A,B,C 是三个集合,f 是 A 到 B 的映射,g 是 B 到 C 的映射,规定

$$h: x \mapsto g(f(x)), \forall x \in A,$$

则 h 是 A 到 C 的映射,称为 f 与 g 的合成(或乘积),记作 $h=g\circ f$,即

$$(g \circ f)(x) = g(f(x)),\ \forall x \in A.$$

例 7　设 $A=B=C=\mathbf{R}$,

$$f: x \mapsto x^2,\ \forall x \in \mathbf{R},$$

$$g: x \mapsto 2x,\ \forall x \in \mathbf{R}.$$

是 **R** 到 **R** 的两个映射,则它们的合成分别为

$$g \circ f: x \mapsto 2x^2,\ \forall x \in A,$$

$$f \circ g: x \mapsto (2x)^2,\ \forall x \in A.$$

由例 7 可见,映射的合成不满足交换律.但是我们有

定理 1.2　设 $f: A \mapsto B, g: B \mapsto C, h: C \mapsto D$,则

(1) $h \circ (g \circ f) = (h \circ g) \circ f$(结合律成立);

(2) $I_B \circ f = f,\ f \circ I_A = f$.

证　(1) 显然,$h \circ (g \circ f)$与$(h \circ g) \circ f$有相同的定义域A,相同的值域 D.又$\forall x \in A$,有

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

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

因此,$h \circ (g \circ f) = (h \circ g) \circ f$.

(2) 显然,$I_B \circ f$ 与 f 有相同的定义域A,相同的值域 B.又$\forall x \in A$,有

$$(I_B \circ f)(x) = I_B(f(x)) = f(x),$$

因此,$I_B \circ f = f$.另一式同理可证.

定义 1.9　设 f 是A 到B 的一个映射.

(1) 若$\forall a_1, a_2 \in A$,当 $a_1 \neq a_2$ 时,有 $f(a_1) \neq f(a_2)$,则称 f 是A 到B 的一个单射;

(2) 若$\forall b \in B, \exists a \in A$,使 $f(a)=b$,则称 f 是A 到B 的一个满射;

(3) 若 f 既是满射,又是单射,则称 f 是一个双射.

例如,例 1 中的映射 f 是单射但不是满射;g 既不是单射,也不是满射;例 2 中的映射 f 是满射但不是单射;例 3 中的映射 f 是单射但不是满射;例 4 中的映射 f 与例 5 中的映射 I_A 都是双射.

定义 1.10　设 f 是A 到B 的一个映射.

(1) 若存在 B 到 A 的映射 g_l，使 $g_l \circ f = I_A$，则称 f 是左可逆映射，称 g_l 是 f 的左逆映射；

(2) 若存在 B 到 A 的映射 g_r，使 $f \circ g_r = I_B$，则称 f 是右可逆映射，称 g_r 是 f 的右逆映射；

(3) 若存在 B 到 A 的映射 g，使 $g \circ f = I_A$，$f \circ g = I_B$，则称 f 是可逆映射，称 g 是 f 的逆映射.

由定义可见，可逆映射一定既是左可逆映射，又是右可逆映射，而且可逆映射 f 的逆映射 g 既是 f 的左逆映射，又是 f 的右逆映射.

例如，例 1 中的映射 f 是左可逆的，它有左逆映射：

$$g_l: 1 \mapsto a, 2 \mapsto b, 3 \mapsto c, 4 \mapsto b.$$

例 2 中的映射 f 是右可逆的，它有右逆映射：

$$g_r: n \mapsto n-1, \ \forall n \in \mathbf{N}.$$

例 4 中的映射 f 是可逆的，它有逆映射：

$$f: n \mapsto n-1, \ \forall n \in \mathbf{Z}.$$

定理 1.3 设 A, B 是两个非空集合，f 是 A 到 B 的一个映射，则下列四个命题等价：

(1) f 是单射；

(2) $\forall a_1, a_2 \in A$，当 $f(a_1) = f(a_2)$ 时，有 $a_1 = a_2$；

(3) f 左可逆；

(4) f 左可消，即 $f \circ h = f \circ k \Rightarrow h = k$.

证 由单射的定义，(1)与(2)是互为逆否命题，从而(1)⇔(2)当然成立. 下面用循环论证方法证明其他结果.

(2)⇒(3) 由(2)，$\forall b \in \mathrm{Im}f$ 在 f 下的原像是惟一的，设为 $a \in A$. 其次再取定一个 $a_0 \in A$，令

$$g(b) = \begin{cases} a, & \text{当 } b \in \mathrm{Im}f, \text{且 } f(a) = b \text{ 时}, \\ a_0, & \text{当 } b \in B \setminus \mathrm{Im}f \text{ 时}, \end{cases}$$

则 g 是 B 到 A 的一个映射，而且 $\forall a \in A$，

$$(g \circ f)(a) = g(f(a)) = g(b) = a,$$

所以 $g \circ f = I_A$，即 f 是左可逆的.

(3)⇒(4) 若 $f \circ h = f \circ k$. 由(3)，存在 f 的左逆映射：$g: B \to A$，使 $g \circ f =$

I_A. 于是 $g\circ(f\circ h)=g\circ(f\circ k)$. 由结合律, $(g\circ f)\circ h=(g\circ f)\circ k$. 从而, $I_A\circ h=I_A\circ k$, 所以 $h=k$.

(4)⇒(1) 反设 f 不是单射, 则 $\exists a_1,a_2\in A$, 使 $a_1\neq a_2$, 而 $f(a_1)=f(a_2)$. 令 C 是任意非空集合, 作 C 到 A 的两个映射 h,k, 使 $\forall c\in C$,

$$h(c)=a_1,\qquad k(c)=a_2.$$

于是 $h\neq k$, 但是 $\forall c\in C$,

$$(f\circ h)(c)=f(h(c))=f(a_1)=f(a_2)=f(k(c))=(f\circ k)(c),$$

所以 $f\circ h=f\circ k$. 这与命题(4)矛盾. 因此 f 是单射.

定理 1.4　设 A,B 是两个非空集合, f 是 A 到 B 的一个映射, 则下列四个命题等价:

(1) f 是满射;

(2) $\mathrm{Im}f=B$;

(3) f 右可逆;

(4) f 右可消, 即 $h\circ f=k\circ f\Rightarrow h=k$.

证　由满射与 $\mathrm{Im}f$ 的定义, (1)与(2)显然等价. 下面用循环论证方法证明其他结果.

(1)⇒(3) 由(1), $\forall b\in B$, 存在原像 $a\in A$, 即 $f(a)=b$. 令

$$g(b)=a,$$

则 g 是 B 到 A 的映射, 而且 $\forall b\in B$,

$$(f\circ g)(b)=f(g(b))=f(a)=b,$$

所以 $f\circ g=I_B$, 即 f 是右可逆的.

(3)⇒(4) 若 $h\circ f=k\circ f$. 由(3), 存在右逆映射: $g:B\mapsto A$, 使 $f\circ g=I_B$. 于是 $(h\circ f)\circ g=(k\circ f)\circ g$. 由结合律, $h\circ(f\circ g)=k\circ(f\circ g)$. 从而, $h\circ I_B=k\circ I_B$, 所以 $h=k$.

(4)⇒(1) 反设 f 不是满射, 则 $\exists b_0\in B\setminus\mathrm{Im}f$. 令 C 是任意一个包含两个不同元素 c_1,c_2 的集合, 作 B 到 C 的两个映射 h,k, 使 $\forall b\in B$,

$$h(b)=c_1;\qquad k(b)=\begin{cases}c_1, & \text{当 } b\neq b_0 \text{ 时},\\ c_2, & \text{当 } b=b_0 \text{ 时}.\end{cases}$$

于是 $h\neq k$, 但是 $\forall a\in A$, $f(a)\in\mathrm{Im}f$, 于是

$$(h\circ f)(a)=h(f(a))=c_1=k(f(a))=(k\circ f)(a).$$