高等学校试用教材

近世代数

吴品三 编

高等教育出版社

高等学校试用教材

近世代数

吴品三 编

高等教育出版社

本书原由人民教育出版社出版。1983年3月9日，上级同意恢复“高等教育出版社”。本书今后改用高等教育出版社名义继续印行。

高等学校试用教材

近世代数

吴品三　编

*

高等教育出版社出版

新华书店北京发行所发行

河北省香河县印刷厂印装

*

开本850×1168 1/32　印张9.25　字数224,000

1979年12月第1版　　1984年2月第5次印刷

印数　60,501—71,700

书号 13010·0403　　定价 0.83 元

前　言

本书是根据1977年底上海教材会议拟定的"近世代数基础"教材编写大纲编写的；全书共分五章，前三章介绍关于群、环、域的基本知识，这部分内容每一个学生都应很好掌握。第四章介绍格的初步知识，第五章对群作进一步讨论，这两章可按照学生具体情况选讲一章或全讲。

根据编者在北京师范大学讲授代数课的经验，学生在学习这一课程时往往对抽象概念不能很好理解，对解题不知如何下手；针对这种情况，本书对每一重要概念都引入较多例子，以增加学生的感性认识，特别对举反例的问题，给与较多注意，这不仅对理解概念有所帮助，而且也是学习数学的一种基本方法。本书在每一重要定理之后都通过较多例题，说明如何应用这个定理，使学生能较好地体会抽象代数的证题方法。在每一章末尾，还附有一些综合运用本章概念的例题。所有这些例子与例题，并不需要都在课堂上讲解，有些可留给学生自己阅读。

为了提高学生的解题能力，本书对习题做了以下安排：按照循序渐进的原则，在每一节后配有一些练习，然后在每一章后配有习题。每节后的练习是比较容易的，凡是真正理解该节内容的学生，做这些练习，应该没有什么困难，可让学生全做。在这个基础上，可按照学生情况，再选留一些章后的习题。

在本书编写过程中，经常得到张禾瑞教授的指导，王世强教授仔细审阅了全部手稿，提出许多改进意见，徐伯勋同志为本书的编辑出版，花了不少功夫，谨此向他们表示感谢。由于编者水平所限，本书定有不妥之处，衷心希望读者指正。

吴品三

1979年4月于北京师范大学

目　　录

第一章　基本概念

§1　集合　子集　集合的运算

在数学中，常常不是讨论处于孤立状态下的各个个体，而是将这些个体联合在一个整体中来进行讨论。例如，我们讨论一个未知量 x 的有理系数多项式 $f(x)$，常常把所有这些多项式看成一个整体，讨论在这个整体中的运算（加、减、乘、除），整除性，既约性，因式分解等等。我们对于“在一定范围内的讨论对象组成的整体”给与一个名称，叫做**集合**。这是数学上的一个最基本的概念，我们通常只用它的各种同义语来解释，而不用比它更简单的概念来定义。

组成一个集合的各个个体，叫做这个集合的元素。

我们用大写拉丁字母 $A, B, C, \cdots$ 来表示集合。特别，用 $\boldsymbol{Z}$ 表示所有整数所组成的集合（简称整数集），$\boldsymbol{Q}$ 表示所有有理数所组成的集合（简称有理数集），$\boldsymbol{R}$ 表示所有实数所组成的集合（简称实数集），$\boldsymbol{C}$ 表示所有复数所组成的集合（简称复数集）。以后，如果没有特别说明，符号 $\boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ 就表示上述集合。

集合的元素常用小写拉丁字母 $a, b, c, \cdots$ 来表示。当 a 是集合 A 的元素时，就说“a 属于 A”，记为“$a\in A$”，也说“A 含有 a”，记为“$A\ni a$”。当 a 不是集合 A 的元素时，用符号“$a\notin A$”表示，读做“a 不属于 A”。

确定一个集合 A，就是要确定：哪些元素属于 A，哪些元素不属于 A。

设有两个集合 A, B，若对于 A 中一切 a，均有 $a\in B$，这时，就说 A 是 B 的子集，（也说 B 是 A 的扩集）用符号“$A\subseteq B$”表示（或

用符号“$B \supseteq A$”表示),读做“A 含于 B”(或读做“B 包含 A”). 若 A 不是 B 的子集,则用符号“$A \not\subseteq B$”表示.

为了表达简捷,我们将逐渐引用一些通用的记号. 我们用“$\forall x \in A$”表示“对于一切 $x \in A$”,用“$\exists x \in A$”表示“存在一个 $x \in A$”,“$\exists | x \in A$”表示“存在唯一的一个 $x \in A$”. 设 P, Q 是两个命题,“$P \Rightarrow Q$”表示“若 P 成立,则 Q 成立”,“$P \Longleftrightarrow Q$”表示“当且仅当 P 成立时 Q 成立”,“$\vee$”表示“或者”,“$\wedge$”表示“并且”. 这样,“A 含于 B”这个概念可以用符号描述为

$$A \subseteq B \Longleftrightarrow \forall a: (a \in A) \Rightarrow (a \in B)$$

一个集合由其元素唯一确定,故由相同元素组成的两个集合认为是相等的,即

若 A 是 B 的子集,并且 B 也是 A 的子集,就说 $A=B$,即 $A=B \Longleftrightarrow (A \subseteq B) \wedge (B \subseteq A)$

若 A 是 B 的子集,但 $A \neq B$,就说 A 是 B 的真子集,用符号“$A \subset B$”(或 $A \subsetneqq B$)表示,即 $A \subset B \Longleftrightarrow (A \subseteq B) \wedge (\exists a \in B: a \notin A)$.

不含任何元素的集合叫做空集,用符号 ϕ 表示.

一个集合可用列举其元素的方法给定,也可用规定其元素适合的条件来描述,例如

$$A=\{1,2,3\}, B=\{3\}$$

表示 A 这个集合,由 1,2,3 三个数字所组成,而 B 这个集合,由一个数字 3 所组成,易见 $B \subset A$. 当不致引起混淆时,即写出集合的一些元素,就可以看出该集合元素的组成规律时,也用“$\cdots$”表示其余元素,例如

$$\boldsymbol{P}=\{1,2,3,4,\cdots\},$$

$$\boldsymbol{E}=\{2,4,6,8,\cdots\},$$

$$\boldsymbol{Z}=\{0,\pm 1,\pm 2,\pm 3,\pm 4,\cdots\},$$

由 P 的元素的描述,可以看出,P 是全体自然数所组成的集合,E

是全体偶自然数（正偶数）所组成的集合，关于 P, E，我们也可以如下描述：

$$P=\{x \mid x\in \boldsymbol{Z}, x>0\}$$

$$E=\{x \mid x\in \boldsymbol{Z}, x>0 \wedge x=2y, \quad y\in \boldsymbol{Z}\}$$

这就是用“规定元素适合的条件”来描述一个集合的方法，再看一个例子．

$$A=\{x \mid x\in \boldsymbol{R}, x^2=-1\}$$

易见 $A=\phi$，由此可见，空集确实是在讨论问题中可能出现的一个集合．

我们说，对任意集合 S，均有 $\phi\subseteq S$。为此，需证命题“$x\in\phi\Rightarrow x\in S$”成立．但任一命题，只要前提不真，那末，无论结论如何，整个命题被认为成立，故有 $\phi\subseteq S$．

设 A 是给定的一个集合，A 的所有子集所组成的集合叫做 A 的幂集，用符号 2^A 表示．

例如，$A=\{1,2,3\}$，则

$$2^A=\{\phi,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},A\}$$

由此可见，若 A 含有 n 个不同元素，则 2^A 含有 2^n 个不同的元素．这里，需要注意，2^A 的元素是“集合”，它们是当作个体来考虑的．$\{1\}\in 2^A$，不能写 $\{1\}\subset 2^A$，而对 A 来说，$\{1\}\subset A$，不能写成 $\{1\}\in A$．

让我们再强调一下，集合是我们讨论的对象（当然是在一个确定范围内）所组成的整体，每一个对象就是组成这个集合的元素．现在，我们考虑的对象是 A 的子集，而整体是 2^A，故 2^A 的元素是“A 的子集”．对于我们讨论的对象，只是要求能够判别异同，没有其他条件，换句话说，对于两个元素 a, b，只要求能够判别是相同元素，或者是不同元素．给定集合 A，A 的元素可以作为讨论对象，A 的子集当然也可作为讨论对象．

设 $A=\{1,2,3\}$，$B=\{1,1,2,3\}$。则任取 $a\in A$，均有 $a\in B$，故 $A\subseteq B$。反之，任取 $a\in B$，则也有 $a\in A$，即 $B\subseteq A$，故 $A=B$，这是根据集合相等的定义得出的判断，似乎与我们的常识相违背，其实不然，因为开始我们就约定了集合是"讨论对象"的全体，而对于 A，B，讨论对象只有三个数目，故 $A=B$。

下面我们介绍集合的几种运算。

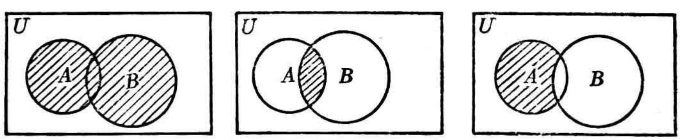
设 A，B 是U的子集，A，B 的交 $A\cap B$ 定义为一切既属于 A 又属于 B 的元素组成的集合，A，B 的并 $A\cup B$ 定义为一切属于 A 或者属于 B 的元素组成的集合，B 在 A 中的余 $A\backslash B$ 定义为一切属于 A 但不属于 B 的元素组成的集合，特别，B 在 U 中的余简称 B 的余集，记为 B'：

$$A\cap B=\{x\mid x\in U,\ (x\in A)\wedge(x\in B)\},$$

$$A\cup B=\{x\mid x\in U,\ (x\in A)\vee(x\in B)\},$$

$$A\backslash B=\{x\mid x\in U,\ (x\in A)\wedge(x\notin B)\}.$$

集合的这三种运算可以用图形表示如下



$A\cup B$　　　　$A\cap B$　　　　$A\backslash B$

设取定集合U，A，B，C 是 U的子集，则集合的上述三种运算 $\cup$，$\cap$，$\backslash$适合以下算律：

(1) $A\cap A=A$，$A\cup A=A$；　(幂等律)

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

(3) $A\cap(B\cap C)=(A\cap B)\cap C$，

$A\cup(B\cup C)=(A\cup B)\cup C$；　(结合律)

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

(5) 若 $A\subseteq C$ 则 $A\cup(B\cap C)=(A\cup B)\cap C$； (模律)

(6) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$， (分配律)

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

(7) $A\cap\phi=\phi$，$A\cup\phi=A$， (泛界)

$A\cap U=A$，$A\cup U=U$；

(8) $A\cap A'=\phi$，$A\cup A'=U$；

(9) $(A')'=A$； (对合律)

(10) $(A\cap B)'=A'\cup B'$，

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

我们证明(4),(5)作为例子，其余留作练习.

设 $x\in A\cap(A\cup B)$，则 $x\in A$，并且 $x\in A$ 或 $x\in B$. 设第一种情形成立，则 $x\in A$；设第二种情形成立，则 $x\in A$ 并且 $x\in B$；总之有 $x\in A$. 即 $A\cap(A\cup B)\subseteq A$.

反之，设 $x\in A$，则 $x\in A\cup B$，从而 $x\in A\cap(A\cup B)$，即 $A\cap(A\cup B)=A$. 同样，可证 $A\cup(A\cap B)=A$，即(4)成立。

设 $x\in A\cup(B\cap C)$，则 $x\in A$ 或者 $x\in B\cap C$，在第一种情形，$x\in A$，从而 $x\in A\cup B$，又题设 $A\subseteq C$，故 $x\in C$，即 $x\in(A\cup B)\cap C$；在第二种情形，$x\in B\cap C$，则 $x\in A\cup B$，且 $x\in C$，即 $x\in(A\cup B)\cap C\Rightarrow A\cup(B\cap C)\subseteq(A\cup B)\cap C$.

反之，设 $x\in(A\cup B)\cap C$，则 $x\in A\cup B$，并且 $x\in C$. 若 $x\in A$，则 $x\in A\cup(B\cap C)$；若 $x\in B$，则 $x\in B\cap C$，从而 $x\in A\cup(B\cap C)\Rightarrow A\cup(B\cap C)\supseteq(A\cup B)\cap C$，即是：在 $A\subseteq C$ 的条件下，有

$$A\cup(B\cap C)=(A\cup B)\cap C,$$

(5) 成立.

设 A,B 是两个集合，若 $A\cap B=\phi$，则说 A 与 B 不相交.

集合的交与并的概念也可以推广到任意多个集合上去. 设 A_i $(i\in I)$ 是集合 U 的子集，定义集合族 $\{A_i|i\in I\}$ 的交为

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

此处 A_i 的所有下标 i 组成的集合 I 叫做集合族$\{A_i\}$的标集。

集合族$\{A_i \mid i\in I\}$的并为

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

特别，当标集 $I=\phi$ 时，规定

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

对于 U 的任意子集 A，下列两个等式成立：

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

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

我们证明第一个等式，另一个等式作为练习。

$$x\in A\cup\left(\bigcap_{i\in I} A_i\right)\Longleftrightarrow(x\in A)\vee(x\in A_i,\ \forall i\in I)\Longleftrightarrow$$

$$x\in A\cup A_i,\ \forall i\in I\Longleftrightarrow x\in\bigcap_{i\in I}(A\cup A_i)$$

即
$$A\cup\left(\bigcap_{i\in I} A_i\right)=\bigcap_{i\in I}(A\cup A_i)$$

练　　习

1．设 $A=\{x \mid x\in \boldsymbol{R},\ |x|\geqslant 5\}$，

$B=\{x \mid x\in \boldsymbol{R},\ -6\leqslant x<0\}$，

求 $A\cup B, A\cap B, A\backslash B, B\backslash A$，并用图形表示。

2．证明：$(A\subset B)\Longleftrightarrow(A\cup B=B)\Longleftrightarrow(A\cap B=A)$。

3．证明：$(A=B)\Longleftrightarrow(A\cup B=A\cap B)$。

4．设 $A_n=(n,\infty)$，(n,∞)表示实数轴上的开区间，即$(n,\infty)=\{x \mid x\in \boldsymbol{R},$

$n<x<\infty\}, n=0,1,2,\cdots,$

求 $$\bigcup_{n=0}^{\infty} A_i,\quad \bigcap_{i=0}^{\infty} A_i.$$

5. 设 $A=\{x \mid x\in Z,\ x^2-3x+2=0\}$，写出 2^A。

6. 设 A,B 是 U 的子集，规定 $A\dot{+}B=(A\backslash B)\cup(B\backslash A)$，证明

$a)$ $A+B=B+A$，$b)$ $A+\phi=A$，$c)$ $A+A=\phi$。

§2 映射 映射的合成

上一节介绍的集合，是近代数学的一个最基本的概念，数学的每一分支都离不开它；本节将要介绍的映射，也是这样的一个基本概念。

定义 1 设 A、B 是给定的两个集合，如果有一个规则 f，通过它，对于每一个 $x\in A$，唯一确定一个 $y\in B$，那末，就说 f 是 A 到 B 的一个映射，记为

$$f:\ A\to B$$

A 叫做映射 f 的定义域，B 叫做 f 的值域，y 说是 x 在 f 作用下的象，记作 $y=f(x)$，并用符号

$$f:\ x\mapsto y$$

表示，x 说是 y 的一个原象。

由以上定义可知：一个映射必须联系着两个集合与一个对应规则。两个映射 f, g，$f: A\to B$，$g: A_1\to B_1$，当且仅当 $A=A_1$，$B=B_1$，且对一切 $x\in A$，均有 $f(x)=g(x)$ 时，才认为是相等的，用符号表示，即

$$f=g\Longleftrightarrow[A=A_1]\wedge[B=B_1]\wedge[\forall x\in A: f(x)=g(x)]$$

我们看几个例子：

例 1 设 $A=\{a, b, c\}$，$B=\{1,2,3,4\}$

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

是 A 到 B 的一个映射.

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

也是 A 到 B 的一个映射,但

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

不是 A 到 B 的映射,因为 c 在 h 作用下没有象.

例 2 $A=\boldsymbol{Z}$, $B=\{x \mid x\in\boldsymbol{Z},\ x>0\}$,

$f: n \mapsto |n|$

不是 A 到 B 的映射,因 0 在 f 作用下的象不在 B 中.

$$g: n \mapsto |n|+1$$

是 A 到 B 的一个映射.

$$h: \begin{cases} n \mapsto 1, \text{当 } 2 \mid n \text{ 时(表示 2 是 } n \text{ 的因子)}, \\ n \mapsto 2, \text{当 } 2 \nmid n \text{ 时(表示 2 不是 } n \text{ 的因子)}. \end{cases}$$

也是 A 到 B 的一个映射.

例 3 $A=(F)_n$ 是数域 F 上一切 n 阶方阵的集合

$$B=\{0,1,2,\cdots,n\}$$

$$f: (\alpha_{ij}) \mapsto \text{秩}(\alpha_{ij})$$

这是 A 到 B 的一个映射.

例 4 $A=B=\boldsymbol{Z}$,

$f: n \mapsto n+1$,

$g: n \mapsto n-1$

都是 A 到 B 的映射.

例 5 $A=B$,

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

是 A 到 A 的一个映射,叫做 A 上的单位映射(或恒等映射).

注意,当 $A \neq B$ 时,I_A 与 I_B 是两个不同的映射.

例 6 设 $A\subseteq B$, $i: a \mapsto a$, $\forall a\in A$, 称 i 为 A 到 B 的一个包含映射.

定义 2 设 f 是 A 到 B 的一个映射，如果 $a \neq b$ 有 $f(a) \neq f(b)$，$\forall a, b \in A$，那末，就说 f 是 A 到 B 的一个单射(injection)。如果对于任意 $b \in B$，均存在 $a \in A$，使 $f(a)=b$，那末，就说 f 是 A 到 B 的一个满射(surjection)，满射 f 用符号 $\twoheadrightarrow$ 表示，即 $f: A \twoheadrightarrow B$。若一个映射 f，既是单射，又是满射，则叫做双射 (bijection)，表为 $f: A \leftrightarrow B$。

A 到 B 的单射也叫 A 到 B 里的一一映射，满射也叫 A 到 B 上的映射，双射也叫 A 到 B 上的一一映射。

例 1 的 f 既不是单射，也不是满射，例 1 的 g 是单射，例 2 的 g 是满射，例 3 的 f 是满射，例 4 的 f, g 是双射。

设 f 是 A 到 B 的映射，任取 $S \subseteq A$，命

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

这是 B 的一个子集，叫做 S 在 f 作用下的象，(当 $S=\phi$ 时，$f(S)=\phi$) 当 $S=A$ 时，$f(A)$ 叫做映射 f 的象，通常记为 $\mathrm{Im} f$，即

$$\mathrm{Im} f=f(A)$$

于是，A 到 B 的映射 f 是 A 到 $\mathrm{Im} f$ 的满射。

任取 $T \subseteq B$，命

$$f^{-1}(T)=\{x \mid x \in A, f(x) \in T\}$$

这是 A 的一个子集，叫做"在 f 作用下 T 的完全原象"(当 $T=\phi$ 时，$f^{-1}(\phi)=\phi$)；特别，当 T 仅含有一个元素时，例如，$T=\{b\}$，$f^{-1}(\{b\})$ 也记成 $f^{-1}(b)$。$f^{-1}(b)$ 有可能是空集，例如在例 1 中，$T=\{4\}$，则 $f^{-1}(T)=\phi$。

下面介绍映射合成的概念。

定义 3 设有三个集合 A, B, C，$f: A \to B$，$g: B \to C$，由 f，g 确定的 A 到 C 的映射 $h: a \mapsto g(f(a))\ \forall a \in A$ 叫做映射 f, g 的合成，记为 $h=g \circ f$，即 $h(a)=g(f(a))$。h 可用下图表示：

$$\begin{tikzcd}
A \arrow[rr, "h=g\circ f"] \arrow[dr, "f"'] & & C \\
& B \arrow[ur, "g"'] &
\end{tikzcd}$$

我们证明：映射的合成适合结合律，以及恒等映射关于映射的合成的特性．

定理 1 设 $f: A\to B$, $g: B\to C$, $h: C\to D$, 则有

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

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

证 1) 按照映射相等的定义，需要证明映射 $h\circ(g\circ f)$ 与 $(h\circ g)\circ f$ 的定义域与值域都相同，这是明显的，定义域为 A 而值域为 D. 其次，需要证明，对于任意 $x\in A$, 有

$$[h\circ(g\circ f)](x)=[(h\circ g)\circ f](x).$$

由映射合成定义，我们有以下等式：

$$\begin{aligned}[h\circ(g\circ f)](x)&=h[(g\circ f)(x)]=h[g(f(x))]=(h\circ g)(f(x))\\&=[(h\circ g)\circ f](x),\ \forall x\in A,\ \text{即 } h\circ(g\circ f)=(h\circ g)\circ f.\end{aligned}$$

证 2) $I_B\circ f$ 与 f 的定义域均为 A, 值域均为 B. 并且对于任意 $x\in A$, 有 $(I_B\circ f)(x)=I_B(f(x))=f(x)$, 即 $I_B\circ f=f$. 同样，可证 $f\circ I_A=f$. $\square$

我们看例 4 的 f, g, 易见 $f\circ g=g\circ f=I_A$ 而对于例 1 的 g, 我们作 $f: B\to A$, 即

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

则 $f\circ g=I_A$, 但 $g\circ f\neq I_B$, 我们引入以下定义

定义 4 设 $f: A\to B$. 若存在 $g: B\to A$, 使 $g\circ f=I_A$, 则说 f 是左可逆映射，g 叫做 f 的左逆映射．同样，若 $f\circ g=I_B$, 则说 f 是右可逆，g 叫做 f 的右逆映射．当 f 是双侧可逆时，说 f 是可逆映射．

上面例子中，g 是左可逆映射，f 是 g 的左逆映射．若命

$$f_1: 1\mapsto a,\ 2\mapsto b,\ 3\mapsto c,\ 4\mapsto b,$$

则 f_1 是不同于 f 的另一个左逆映射，由此可见，左可逆映射的左逆映射不一定是唯一的.

定理 2 $f: A\to B$. f 是左可逆的充要条件为，f 是单射；f 是右可逆的充要条件为，f 是满射.

证 设 f 是左可逆，即存在 $g: B\to A$，使 $g\circ f=I_A$. 希望证明，当 $f(a_1)=f(a_2)$ 时，有 $a_1=a_2$. 因

$$\begin{aligned}a_1&=I_A(a_1)=(g\circ f)(a_1)=g(f(a_1))=g(f(a_2))\\&=(g\circ f)(a_2)=I_A(a_2)=a_2,\end{aligned}$$

即 f 是单射.

反之，设 f 是 A 到 B 的单射，希望证明，存在 $g_1: B\to A$，使 $g_1\circ f=I_A$. 为此，取定一个 $a_1\in A$. 作如下对应 g_1:

$$g_1(b)=\begin{cases}a, 若\ \exists a\in A: f(a)=b,\\ a_1, 若\ b\notin f(A),\end{cases}$$

则 $\forall b\in B$，$g_1(b)$ 唯一确定，并且 $\forall a\in A$，$(g_1\circ f)(a)=g_1(f(a))=g_1(b)=a$，即 $g_1\circ f=I_A$.

设 f 是右可逆，即存在 $h: B\to A$，使 $f\circ h=I_B$，希望证明，对任意 $b\in B$，$\exists a\in A: f(a)=b$. 因 $b\in B$，故有 $b=I_B(b)=(f\circ h)(b)=f(h(b))$，即存在 $h(b)\in A$，使 $f(h(b))=b$，故 f 是满射.

反之，设 f 是满射，则对于每一 $b\in B$，存在一个 $a\in A$，使 $f(a)=b$. 一般情形，这样的 a 不止一个，但是，我们只取定一个，作 $g_2: b\mapsto a$，这是 B 到 A 的一个映射，并且 $\forall b\in B$，$(f\circ g_2)(b)=f(g_2(b))=f(a)=b$，即 $f\circ g_2=I_B$. 故 f 是右可逆. □

推论 $f: A\to B$，则 f 是可逆映射的充要条件为：f 是双射.

设 f 是双射，则 f 既有左逆映射 g，又有右逆映射 h，g 与 h 有何关系呢？下面定理说明二者相等.

定理 3 设 $f: A\to B$，且 $g\circ f=I_A$，$f\circ h=I_B$，则 $g=h$.