第3章 函数

3.1 函数的概念

3.1.1 函数的定义

在许多情况下，需要对一个集合里的每个元素指定本集合或另一集合中的一个特定的元素。例如，由选修了程序设计实验课的学生组成的集合为{赵明，钱华，孙丽，李思，周军，吴敏}。一个学期结束，需要为选修了该实验课的每个学生确定一个{优，良，中，及格，不及格}中的元素作为实验课的成绩，如图 3.1 所示。这些学生和成绩之间的关系就是函数的一个例子。

函数是最基本的数学概念之一，也是最重要的数学工具。连续变量函数或实函数在微积分学中的地位是众所周知的，离散对象之间的函数关系在计算机科学研究中有着极其重要的意义。

定义 3.1 设 f 是集合 A 到 B 的关系，如果对每个 $x \in A$，都存在唯一的 $y \in B$ 使得 $<x, y> \in f$，则称关系 f 为集合 A 到 B 的**函数**(function)或**映射**(mapping)，记为 $f: A \to B$ 或 $y = f(x)$。并称 x 为函数 f 的**自变量**(argument)或**源点**，y 为 x 在函数 f 下的**函数值**(value)或**像点**(individual image)。集合 A 称为函数 f 的**定义域**(domain)，记为 $\mathrm{dom}\ f = A$。所有像点组成的集合称为函数 f 的**值域**(range)或函数 f 的**像**(image)，记为 $\mathrm{ran}\ f$ 或 $f(A)$。

函数定义的示意图如图 3.2 所示。

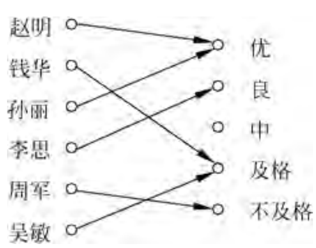

图 3.1　实验课成绩的确定

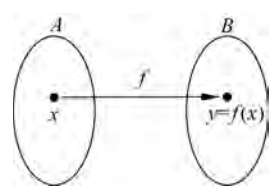

图 3.2　集合 A 到 B 的函数 f

由定义 3.1 可知，函数是一种特殊的关系，它要求 A 中每个元素都与 B 中一个且仅一个元素相关。同时，也可以通过集合 A 上的关系，定义出集合 A 到 A 的函数。

例 3.1 对于图 3.1 所描述的学生与成绩的关系,试写出该函数的定义域和值域。

解 令集合 $A=\{$赵明,钱华,孙丽,李思,周军,吴敏$\}$,集合 $B=\{$优,良,中,及格,不及格$\}$。由图 3.1 可知,f 为 A 到 B 的函数,表示在程序设计实验课上各个学生与成绩的关系,如 f(赵明)=优。可知,f 的定义域是 $\operatorname{dom} f=\{$赵明,钱华,孙丽,李思,周军,吴敏$\}$;f 的值域是 $\operatorname{ran} f=\{$优,良,及格,不及格$\}$,因为除了"中"以外,每个成绩值都被确定给了某个学生。

例 3.2 设集合 $A=\{1,2,3,4\}$ 和 $B=\{a,b,c,d\}$,判断下列 A 到 B 的关系哪些是函数,并写出函数的值域。

① $f_1=\{<1,a>,<2,a>,<3,d>,<4,c>\}$。

② $f_2=\{<1,a>,<2,a>,<2,d>,<4,c>\}$。

③ $f_3=\{<1,a>,<2,b>,<3,d>,<4,c>\}$。

④ $f_4=\{<1,a>,<2,b>,<2,c>,<3,d>,<4,c>\}$。

⑤ $f_5=\{<2,a>,<2,b>,<2,c>,<2,d>,<3,b>,<4,c>\}$。

⑥ $f_6=\{<1,a>,<2,b>,<3,a>,<4,b>\}$。

解 ① f_1 是函数,值域为 $f_1(A)=\{a,c,d\}$。

② f_2 不是函数,因为元素 3 没有像点,且元素 2 在关系 f_2 下的像点为 a 和 d,即不存在唯一的像点。

③ f_3 是函数,值域为 $f_3(A)=\{a,b,c,d\}$。

④ f_4 不是函数,因为元素 2 在关系 f_4 下的像点为 b 和 c,即不存在唯一的像点。

⑤ f_5 不是函数,因为元素 1 没有像点,且元素 2 在关系 f_5 下的像点为 a、b、c 和 d,即不存在唯一的像点。

⑥ f_6 是函数,值域为 $f_6(A)=\{a,b\}$。

例 3.3 设集合 $A=\{$"www.edu.cn","peking university","Guilin","discrete structure","function","range"$\}$,f 是集合 A 到整数集 $\mathbf{Z}$ 的函数,表示对每个字符串返回其长度。写出函数 f 的定义域和值域。

解 由函数 f 的定义可知,该函数的定义域 $\operatorname{dom} f=A$,值域 $\operatorname{ran} f=\{10,17,6,18,8,5\}$。

例 3.4 判断下列关系哪些是函数:

① $f_1=\{<x,y>\mid x\in\mathbf{N},y\in\mathbf{N},x+y<10\}$;

② $f_2=\{<x,y>\mid x\in\mathbf{R},y\in\mathbf{R},|x|=y\}$;

③ $f_3=\{<x,y>\mid x\in\mathbf{R},y\in\mathbf{R},x=|y|\}$;

④ $f_4=\{<x,y>\mid x\in\mathbf{Z},y\in\mathbf{Z},y$ 是 x 的 2 倍$\}$;

⑤ $f_5=\{<x,y>\mid x\in\mathbf{R},y\in\mathbf{R},|x|=|y|\}$;

⑥ $f_6=\{<x,y>\mid x\in\mathbf{R},y\in\mathbf{R},x^2=y\}$。

解 根据函数的定义知,f_2、f_4 和 f_6 是函数。f_1 不是函数,因为 f_1 既不满足定义域为 $\mathbf{N}$,又不满足唯一像点条件;f_3 不是函数,因为 f_3 既不满足定义域为 $\mathbf{R}$,又不满足唯一像点条件;f_5 不是函数,因为 f_5 不满足唯一像点条件。

由上面的几个例子,可以总结出函数的以下几个特点:

① 定义域是集合 A,而不能是集合 A 的任意一个真子集;

② 对于定义域中的任意一个元素都有唯一的值和其对应,也就是说只能是多对一,而

不能是一对多，称之为像点的**单值性**；

③ 集合 A 到 B 的函数 f 的值域 $f(A)$ 是集合 B 的子集，即 $f(A)\subseteq B$；

④ 集合 A 到 B 的函数 f 的基数等于其定义域的基数，即 $|f|=|A|$；

⑤ $f(x)$ 表示一个函数值，而 f 是一个序偶的集合，因此 $f(x)\neq f$。

例 3.5　对于集合 $A=\{1,2,3\}$ 和 $B=\{a,b\}$，试列写出 A 到 B 的所有函数和 B 到 A 的所有函数。

解　设函数 $f: A\to B$，函数 $g: B\to A$。根据函数的定义，$f(1)$ 可以取 a 或者 b 两个值；$f(1)$ 取定一个值时，$f(2)$ 可以取 a 或者 b 两个值；而 $f(2)$ 取定一个值时，$f(3)$ 可以取 a 或者 b 两个值。因此，集合 A 到 B 可以定义出以下 2^3 种不同的函数：

$f_1=\{\langle 1,a\rangle,\langle 2,a\rangle,\langle 3,a\rangle\}$；　$f_2=\{\langle 1,a\rangle,\langle 2,a\rangle,\langle 3,b\rangle\}$；

$f_3=\{\langle 1,a\rangle,\langle 2,b\rangle,\langle 3,a\rangle\}$；　$f_4=\{\langle 1,a\rangle,\langle 2,b\rangle,\langle 3,b\rangle\}$；

$f_5=\{\langle 1,b\rangle,\langle 2,a\rangle,\langle 3,a\rangle\}$；　$f_6=\{\langle 1,b\rangle,\langle 2,a\rangle,\langle 3,b\rangle\}$；

$f_7=\{\langle 1,b\rangle,\langle 2,b\rangle,\langle 3,a\rangle\}$；　$f_8=\{\langle 1,b\rangle,\langle 2,b\rangle,\langle 3,b\rangle\}$。

同理，集合 B 到 A 可以定义出以下 3^2 种不同的函数：

$g_1=\{\langle a,1\rangle,\langle b,1\rangle\}$；　$g_2=\{\langle a,1\rangle,\langle b,2\rangle\}$；

$g_3=\{\langle a,1\rangle,\langle b,3\rangle\}$；　$g_4=\{\langle a,2\rangle,\langle b,1\rangle\}$；

$g_5=\{\langle a,2\rangle,\langle b,2\rangle\}$；　$g_6=\{\langle a,2\rangle,\langle b,3\rangle\}$；

$g_7=\{\langle a,3\rangle,\langle b,1\rangle\}$；　$g_8=\{\langle a,3\rangle,\langle b,2\rangle\}$；

$g_9=\{\langle a,3\rangle,\langle b,3\rangle\}$。

图 3.3 描述了函数的取值过程。

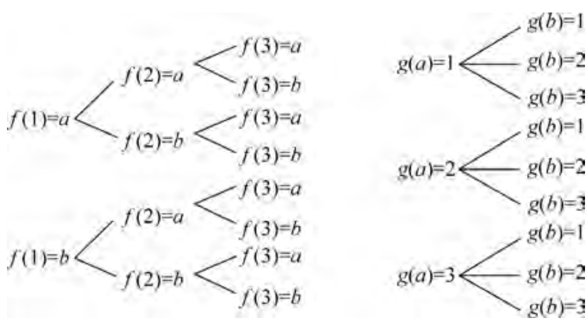

图 3.3　函数的取值过程

从例 3.5 可以看出，对于有限集合 A 和 B，如果 $|A|=m$ 和 $|B|=n$，那么，集合 A 到 B 可以定义出 n^m 种不同的函数。通常，将集合 A 到 B 的所有函数构成的集合记为 B^A，即

$$B^A=\{f \mid f: A\to B\}$$

例 3.6　对于集合 $A=\{1,2,3\}$ 到 $B=\{a,b,c\}$ 的关系 $f=\{\langle 1,a\rangle,\langle 2,b\rangle,\langle 3,c\rangle\}$ 和 $g=\{\langle 1,b\rangle,\langle 2,b\rangle,\langle 3,a\rangle\}$，判断 f、g、$f\cup g$、$f\cap g$、$f-g$、$\sim f$ 和 $f\oplus g$ 是否为 A 到 B 的函数。

解　根据函数的定义，f 和 g 都是集合 A 到 B 的函数。

$f\cup g=\{\langle 1,a\rangle,\langle 1,b\rangle,\langle 2,b\rangle,\langle 3,a\rangle,\langle 3,c\rangle\}$ 不是集合 A 到 B 的函数，因为元素 1 和 3 都不满足唯一像点条件。

$f \cap g=\{<2,b>\}$不是集合 A 到 B 的函数,因为元素 1 和元素 3 都没有像点。

$f-g=\{<1,a>,<3,c>\}$不是集合 A 到 B 的函数,因为元素 2 没有像点。

$\sim f=\{<1,b>,<1,c>,<2,a>,<2,c>,<3,a>,<3,b>\}$不是集合 A 到 B 的函数,因为元素 1、2、3 都不满足唯一像点条件。

$f \oplus g=\{<1,a>,<1,b>,<3,a>,<3,c>\}$不是集合 A 到 B 的函数,因为元素 1 和元素 3 都不满足唯一像点条件,且元素 2 没有像点。

例 3.7 对于集合 $A=\{1,2,3\}$上的关系 $f=\{<1,1>,<2,2>,<3,3>\}$和 $g=\{<1,2>,<2,2>,<3,1>\}$,判断 f、g、$f \cup g$、$f \cap g$、$f-g$、$\sim f$ 和 $f \oplus g$ 是否为 A 到 A 的函数。

解 根据函数的定义,f 和 g 都是集合 A 到 A 的函数。

$f \cup g=\{<1,1>,<1,2>,<2,2>,<3,1>,<3,3>\}$不是集合 A 到 A 的函数,因为元素 1 和元素 3 都不满足唯一像点条件。

$f \cap g=\{<2,2>\}$不是集合 A 到 A 的函数,因为元素 1 和元素 3 都没有像点。

$f-g=\{<1,1>,<3,3>\}$不是集合 A 到 A 的函数,因为元素 2 没有像点。

$\sim f=\{<1,2>,<1,3>,<2,1>,<2,3>,<3,1>,<3,2>\}$不是集合 A 到 A 的函数,因为元素 1、2、3 都不满足唯一像点条件。

$f \oplus g=\{<1,1>,<1,2>,<3,1>,<3,3>\}$不是集合 A 到 A 的函数,因为元素 1 和元素 3 都不满足唯一像点条件,且元素 2 没有像点。

通过例 3.6 和例 3.7 可以看出,函数是一种特殊的关系,可以进行关系的基本运算,但是,函数的并、交、差、补和对称差运算的结果并不一定是函数。

3.1.2 特殊函数

函数描述了集合 A 中元素和集合 B 中元素之间的特殊对应关系。这种对应关系可以是一对一的或多对一的。同时,函数的值域可以是集合 B 的一个真子集,也可以是集合 B 自身。这些不同的情形,形成了下面一些特殊函数。

定义 3.2 设 f 是集合 A 到 B 的函数,对于 A 中任意两个元素 x 和 y,如果 $x \neq y$ 时,都有 $f(x) \neq f(y)$,则称 f 是集合 A 到 B 的**单射函数**(injection)或**一对一的映射**。

例如,集合 $A=\{1,2,3\}$到 $B=\{a,b,c,d\}$的函数 $f=\{<1,a>,<2,b>,<3,c>\}$,对于 A 中任意两个元素 x 和 y,如果 $x \neq y$ 时,都有 $f(x) \neq f(y)$。所以,f 是集合 A 到 B 的单射函数。

定义 3.3 设 f 是集合 A 到 B 的函数,如果函数 f 的值域恰好是集合 B,即 $f(A)=B$,则称 f 是集合 A 到 B 的**满射函数**(surjection)或 ***A* 到 *B* 上的映射**。

例如,集合 $A=\{1,2,3\}$到 $B=\{a,b\}$的函数 $f=\{<1,a>,<2,b>,<3,a>\}$,函数的值域 $f(A)=\{a,b\}=B$。所以,f 是集合 A 到 B 的满射函数。

定义 3.4 设 f 是集合 A 到 B 的函数,如果函数 f 既是集合 A 到 B 的单射函数又是集合 A 到 B 的满射函数,则称 f 是集合 A 到 B 的**双射函数**(bijection)或**一一对应的映射**。

例如,集合 $A=\{1,2,3\}$到 $B=\{a,b,c\}$的函数 $f=\{<1,a>,<2,b>,<3,c>\}$,对于 A 中任意两个元素 x 和 y,如果 $x \neq y$ 时,都有 $f(x) \neq f(y)$。并且,函数的值域 $f(A)=\{a,b,c\}=B$。所以,f 既是集合 A 到 B 的单射函数又是集合 A 到 B 的满射函数。因此,f 是集合 A 到 B 的双射函数。

例 3.8 判断下列 A 到 B 的关系哪些是函数，并说明是单射函数、满射函数还是双射函数：

① 集合 $A=\{1,2,3\}$ 和 $B=\{a,b,c,d\}$，关系 $f_1=\{<1,a>,<2,b>,<3,d>\}$；

② 集合 $A=\{1,2,3\}$ 和 $B=\{a,b\}$，关系 $f_2=\{<1,a>,<2,a>,<3,b>\}$；

③ 集合 $A=\{1,2,3\}$ 和 $B=\{a,b\}$，关系 $f_3=\{<1,a>,<2,a>,<3,a>\}$；

④ 集合 $A=\{1,2,3\}$ 和 $B=\{a,b,c\}$，关系 $f_4=\{<1,a>,<2,b>,<3,c>\}$；

⑤ 集合 $A=\{1,2,3,4\}$ 和 $B=\{a,b,c\}$，关系 $f_5=\{<1,a>,<2,b>,<3,a>,<4,c>\}$；

⑥ 集合 $A=\{1,2,3\}$ 和 $B=\{a,b\}$，关系 $f_6=\{<1,a>,<2,a>,<2,b>,<3,a>\}$。

解 ① f_1 是函数，且是单射函数。

② f_2 是函数，且是满射函数。

③ f_3 是函数，既不是单射函数，也不是满射函数。

④ f_4 是函数，且是单射函数、满射函数、双射函数。

⑤ f_5 是函数，且是满射函数。

⑥ f_6 不是函数。

例 3.9 判断下列函数是单射函数、满射函数还是双射函数：

① $f:\mathbf{R}\to\mathbf{R}, f(x)=-x^2+2x-1$；

② $f:\mathbf{Z}\to\mathbf{Z}, f(x)=|x|$；

③ $f:\mathbf{Z}\to\mathbf{Z}, f(x)=x-1$；

④ $f:\mathbf{N}\to\mathbf{N}\times\mathbf{N}, f(x)=<x,x+1>$；

⑤ $f:\mathbf{R}^+\to\mathbf{R}^+, f(x)=(x^2+1)/x$，$\mathbf{R}^+$ 为正实数集；

⑥ $f:\mathbf{Z}^+\to\mathbf{R}, f(x)=\ln x$，$\mathbf{Z}^+$ 为正整数集。

解 ① $f(0)=f(2)=-1$，因此不是单射函数；f 在 $x=1$ 处取得最大值 0，因此不是满射函数。

② $f(1)=f(-1)=1$，因此不是单射函数；f 的像点都非负，因此不是满射函数。

③ f 是单射函数、满射函数、双射函数。

④ f 是单射函数；$<0,0>\notin \mathrm{ran}\, f$，因此不是满射函数。

⑤ $f(2)=f(1/2)=5/2$，因此不是单射函数；f 有最小值 2，因此不是满射函数。

⑥ f 是单射函数；f 的像点都非负，因此不是满射函数。

从例 3.8 和例 3.9 可以看出，若 f 是有限集 A 到有限集 B 的函数，则有：

① f 是单射函数的必要条件是 $|A|\leqslant|B|$；

② f 是满射函数的必要条件是 $|B|\leqslant|A|$；

③ f 是双射函数的必要条件是 $|A|=|B|$。

例 3.10 试证明以下论断：若 f 是有限集 A 到有限集 B 的函数，且 $|A|=|B|$，那么，f 是单射函数当且仅当 f 是满射函数。

证明 （必要性）设 f 是单射函数。显然，f 是 A 到 $f(A)$ 的满射函数，故 f 是 A 到 $f(A)$ 的双射函数，因此 $|A|=|f(A)|$。从而，由 $|A|=|B|$ 知 $|f(A)|=|B|$。进而，由 $|f(A)|=|B|$ 且 $f(A)\subseteq B$ 可得 $f(A)=B$。所以，f 是有限集 A 到有限集 B 的满射函数。

（充分性）设 f 是满射函数。对于任意元素 x、$y\in A$，$x\neq y$，假设 $f(x)=f(y)$。由于 f 是 A 到 B 的满射函数，所以 f 也是 $(A-\{x\})$ 到 B 的满射函数，故 $|A-\{x\}|\geqslant|B|$，即

$|A|-1 \geqslant |B|$,这与$|A|=|B|$矛盾。因此,f 是有限集 A 到有限集 B 的单射函数。证毕。

例 3.11 对于有限集 A 和有限集 B,设$|A|=3$、$|B|=4$,计算可定义多少种不同的 A 到 B 的单射函数。

解 A 到 B 的单射函数数目为 4 个元素中取 3 个的排列,即

$$P(4,3)=4!/(4-3)!=24$$

例 3.12 对于有限集 A 和有限集 B,设$|A|=4$、$|B|=3$,计算可定义多少种不同的 A 到 B 的满射函数。

解 如果把 A 中元素的两个元素“合并”成 1 个元素,即把 A 看作由 3 个元素组成的集合,由于从 3 个元素的集合到 3 个元素的集合可定义的双射函数为 $3!=6$ 个,而 4 个元素“合并”成 3 个元素共有 $C(4,2)=6$ 种方案,所以,根据乘法原理,A 到 B 的满射函数数目共有 $6\times6=36$。

例 3.13 对于集合 $A=\{a,b,c,d\}$,计算可定义多少种不同的 A 到 A 的双射函数。

解 为了便于分析问题,先画出双射函数的图形表示,如图 3.4 所示。

由图 3.4 可看出,a、b、c 和 d 的一种排列就确定了 A 到 A 的一个双射函数,所以,A 到 A 可定义的双射函数数目是 4 个元素的全排列,即 $4!=24$。

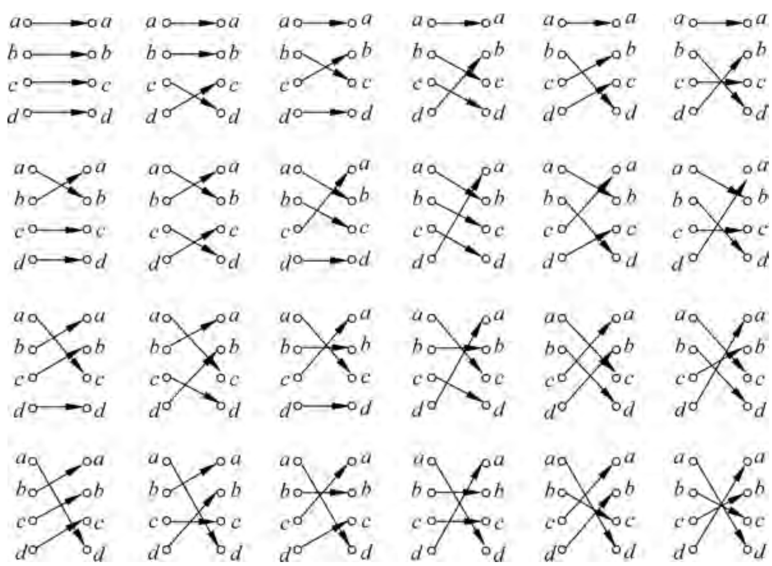

图 3.4 双射函数的图形表示

3.2 函数的运算

3.2.1 复合运算

函数是一种特殊的关系,也应该能够进行关系的复合运算。那么,复合运算的结果是不是像基本运算那样,不一定是函数呢?回答是否定的。函数经复合运算后仍然是函数。

定理 3.1 对于集合 A、B 和 C,f 是 A 到 B 的关系,g 是 B 到 C 的关系,如果 f 和 g

分别是A到B和B到C的函数，那么，复合关系$f\circ g$是A到C的函数。

证明 首先证明$\mathrm{dom}(f\circ g)=A$。

对于任意$x\in A$，由函数$f:A\to B$知，必存在$y\in B$使得$<x,y>\in f$；由函数$g:B\to C$知，对于$y\in B$必存在$z\in C$使得$<y,z>\in g$；因此，$<x,z>\in f\circ g$，即$x\in \mathrm{dom}(f\circ g)$。因此，$A\subseteq \mathrm{dom}(f\circ g)$。

又由复合关系$f\circ g$的定义知，$f\circ g$是A到C的关系，所以$\mathrm{dom}(f\circ g)\subseteq A$。

所以，$\mathrm{dom}(f\circ g)=A$。

再证明$f\circ g$的单值性。设任意$x\in A$，有$z_1\in C$和$z_2\in C$使得$<x,z_1>\in f\circ g$和$<x,z_2>\in f\circ g$，那么，有$y_1\in B$和$y_2\in B$使得$<x,y_1>\in f$、$<y_1,z_1>\in g$、$<x,y_2>\in f$和$<y_2,z_2>\in g$。由f为函数知$y_1=y_2$；又由g为函数知$z_1=z_2$。所以，$f\circ g$为A到C的函数。证毕。

定义 3.5 对于集合A到B的函数f和集合B到C的函数g，复合关系$f\circ g$称为函数f和函数g的**复合函数**(composition function)，记为$f\circ g:A\to C$。并称“$\circ$”为函数的**复合运算**(composition operation)。

注意：$<x,z>\in f\circ g$是指存在y使得$<x,y>\in f$和$<y,z>\in g$，即$y=f(x)$、$z=g(y)=g(f(x))$，因而$f\circ g(x)=g(f(x))$。这说明，当f和g为函数时，它们的复合作用于自变量的次序刚好与复合原始记号的次序相反。

例 3.14 设集合$A=\{a,b,c,d\}$、$B=\{b,c,d\}$和$C=\{a,b,d\}$，集合A到集合B的函数$f=\{<a,b>,<b,b>,<c,d>,<d,d>\}$，集合$B$到集合$C$的函数$g=\{<b,a>,<c,d>,<d,b>\}$，求复合函数$f\circ g$。

解 依据复合函数的定义可以得到

$$f\circ g=\{<a,a>,<b,a>,<c,b>,<d,b>\}$$

例 3.15 对于$\mathbf{R}$到$\mathbf{R}$的函数$f(x)=2x+1$和$g(x)=x^2+1$，求$f\circ g$、$g\circ f$、$f\circ f$和$g\circ g$。

解 依据复合函数的定义可以得到

$$f\circ g(x)=g(f(x))=(2x+1)^2+1=4x^2+4x+2$$
$$g\circ f(x)=f(g(x))=2(x^2+1)+1=2x^2+3$$
$$f\circ f(x)=f(f(x))=2(2x+1)+1=4x+3$$
$$g\circ g(x)=g(g(x))=(x^2+1)^2+1=x^4+2x^2+2$$

例 3.16 对于函数$f:A\to B$和$g:B\to C$，证明以下论断：

① 如果f和g是单(满、双)射函数，则$f\circ g$是单(满、双)射函数；

② 如果$f\circ g$是单射函数，则f是单射函数；

③ 如果$f\circ g$是满射函数，则g是满射函数；

④ 如果$f\circ g$是双射函数，则f是单射函数，g是满射函数。

证明 ① 设f和g是单射函数。对于任意$x_1\in A$和$x_2\in A$，$x_1\neq x_2$，由f是单射函数知，必有$y_1\in B$和$y_2\in B$，$y_1\neq y_2$且$y_1=f(x_1)$、$y_2=f(x_2)$。又由g是单射函数知，$z_1\in C$和$z_2\in C$，$z_1=g(y_1)$，$z_2=g(y_2)$，必有$z_1\neq z_2$。所以，$g(f(x_1))\neq g(f(x_2))$，即$f\circ g(x_1)\neq f\circ g(x_2)$。因此，$f\circ g$是单射函数。

设f和g是满射函数。对于任意$z\in C$，由g是满射函数知，必有$y\in B$使得$g(y)=z$。又由f是满射函数知，必有$x\in A$使得$y=f(x)$。所以，必有$g(f(x))=z$，即$f\circ g(x)=z$。

因此,$f\circ g$ 是满射函数。同理,可证得:如果 f 和 g 是双射函数,则 $f\circ g$ 是双射函数。

② 设 $f\circ g$ 是单射函数,而 f 不是单射函数。那么,有 $x_1\in A$ 和 $x_2\in A$,$x_1\neq x_2$,使得 $f(x_1)=f(x_2)$。从而 $g(f(x_1))=g(f(x_2))$,即 $f\circ g(x_1)=f\circ g(x_2)$。与 $f\circ g$ 是单射函数矛盾。故 f 是单射函数。

③ 设 $f\circ g$ 是满射函数,那么,对于任意 $z\in C$,必有 $x\in A$ 使得 $f\circ g(x)=z$,即 $g(f(x))=z$。因此,必有 $y\in B$,$y=f(x)$ 且 $g(y)=z$。故 g 是满射函数。

④ 设 $f\circ g$ 是双射函数,由②知 f 是单射函数,由③知 g 是满射函数。证毕。

例 3.17 对于集合 $A=\{a_1,a_2,a_3\}$、$B=\{b_1,b_2,b_3,b_4\}$ 和 $C=\{c_1,c_2,c_3,c_4\}$,函数 $f=\{<a_1,b_1>,<a_2,b_2>,<a_3,b_3>\}$ 和函数 $g=\{<b_1,c_1>,<b_2,c_2>,<b_3,c_3>,<b_4,c_3>\}$,可求得 $f\circ g=\{<a_1,c_1>,<a_2,c_2>,<a_3,c_3>\}$。$f\circ g$ 是单射函数,但 g 不是单射函数。

例 3.18 对于集合 $A=\{a_1,a_2,a_3\}$,$B=\{b_1,b_2,b_3\}$ 和 $C=\{c_1,c_2\}$,函数 $f=\{<a_1,b_1>,<a_2,b_2>,<a_3,b_2>\}$ 和函数 $g=\{<b_1,c_1>,<b_2,c_2>,<b_3,c_2>\}$,可求得 $f\circ g=\{<a_1,c_1>,<a_2,c_2>,<a_3,c_2>\}$。$f\circ g$ 是满射函数,但 f 不是满射函数。

例 3.19 对于集合 $A=\{a_1,a_2,a_3\}$、$B=\{b_1,b_2,b_3,b_4\}$ 和 $C=\{c_1,c_2,c_3\}$,函数 $f=\{<a_1,b_2>,<a_2,b_1>,<a_3,b_3>\}$ 和函数 $g=\{<b_1,c_1>,<b_2,c_2>,<b_3,c_3>,<b_4,c_3>\}$,可求得 $f\circ g=\{<a_1,c_2>,<a_2,c_1>,<a_3,c_3>\}$。$f\circ g$ 是双射函数,但 g 不是单射函数,f 不是满射函数。

3.2.2 逆运算

任意关系都可以进行逆运算得到其逆关系。但是对函数而言,就略有不同。由于在函数中一定要求 dom $f=A$ 和 A 中每个元素有唯一的像点。所以,在对一个函数进行逆运算时,为了保证逆运算的结果仍是一个函数,就有相应的特殊要求。

定义 3.6 对于集合 A 到 B 的关系 g,如果关系 g 是 A 到 B 的函数,且其逆关系 g^{-1} 是 B 到 A 的函数,那么称 g^{-1} 是函数 g 的**逆函数**(inverse function)或**反函数**,记为 g^{-1}:$B\rightarrow A$。并称"-1"为函数的**逆运算**(inverse operation)。

例 3.20 判断下列函数哪些存在逆函数,并计算逆函数:

① 集合 $A=\{1,2,3\}$ 到 $B=\{a,b,c\}$ 的函数 $s=\{<1,c>,<2,b>,<3,a>\}$;

② 集合 $A=\{1,2,3\}$ 到 $B=\{a,b,c,d\}$ 的函数 $f=\{<1,a>,<2,b>,<3,d>\}$;

③ $h=\{<x,x+1>\mid x\in\mathbf{Z}\}$;

④ g:$\mathbf{Z}\rightarrow\mathbf{Z}$,$g(x)=x+4$;

⑤ f:$\mathbf{Z}\rightarrow\mathbf{Z}$,$f(x)=2x+1$;

⑥ 集合 $A=\{1,2,3\}$ 到 $B=\{a,b\}$ 的函数 $g=\{<1,a>,<2,a>,<3,b>\}$。

解 ① 集合 $A=\{1,2,3\}$ 到 $B=\{a,b,c\}$ 的逆函数 $s^{-1}=\{<c,1>,<b,2>,<a,3>\}$。

② 关系 $f^{-1}=\{<a,1>,<b,2>,<d,3>\}$ 不是集合 $B=\{a,b,c,d\}$ 到 $A=\{1,2,3\}$ 的函数,所以,函数 f 不存在逆函数。

③ 逆函数 $h^{-1}=\{<x,x-1>\mid x\in\mathbf{Z}\}$。

④ 对于 $<x,x+4>\in g$,应有 $<x+4,x>\in g^{-1}$。令 $x+4=y$,可得 $x=y-4$,即

$<y, y-4> \in g^{-1}$。所以，逆函数 $g^{-1}(x)=x-4$。

⑤ 对于$<x, 2x+1> \in f$，应有$<2x+1, x> \in f^{-1}$。令 $2x+1=y$，可得 $x=(y-1)/2$，即$<y,(y-1)/2> \in f^{-1}$。f^{-1} 不是 **Z** 到 **Z** 的函数。所以，函数 f 不存在逆函数。

⑥ 关系 $g^{-1}=\{<a,1>,<a,2>,<b,3>\}$不是集合 $B=\{a,b\}$到 $A=\{1,2,3\}$的函数，所以，函数 g 不存在逆函数。

定理 3.2 如果 g 是集合 A 到 B 的双射函数，则 g 的逆关系 g^{-1} 是集合 B 到 A 的函数。

证明 由于 g 为双射函数，那么 g 为满射函数，因此对于任意 $y \in B$，必有 $x \in A$ 使得 $g(x)=y$，从而$<y, x> \in g^{-1}$，这表明 $\mathrm{dom}(g^{-1})=B$。

对于任意 $y \in B$，设$<y, x_1> \in g^{-1}$ 和$<y, x_2> \in g^{-1}$，那么 $g(x_1)=g(x_2)=y$。由于 g 是双射函数，那么 g 是单射函数，必有 $x_1=x_2$，从而 g^{-1} 具有单值性。所以，g^{-1} 是集合 B 到 A 的函数。证毕。

例如，例 3.20 中①、③和④列出的都是双射函数，它们的逆关系都是函数；②和⑤中的函数都是单射函数，但都不是满射函数，它们的逆关系都不是函数；⑥中的函数是满射函数，但不是单射函数，它的逆关系不是函数。

例 3.21 双射函数及其逆函数是密码学中的重要工具，可用于密码系统中的加密与解密。假设函数 f 的定义如表 3.1 所示，即 $f(A)=R$，$f(B)=S$，$f(C)=T$ 等。现有一段加密后的密文为“*UZJTIVKVJKILTKLIV*”，试对该密文进行解密，找出其加密前的原文，即明文。

表 3.1 函数 *f*

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$f(x)$	R	S	T	U	V	W	X	Y	Z	A	B	C	D
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$f(x)$	E	F	G	H	I	J	K	L	M	N	O	P	Q

解 由表 3.1 可知，函数 f 是一个双射函数。为了求出给定密文的明文，需求出函数 f 的逆函数 f^{-1}，按照 f^{-1} 的对应关系依次还原对应的字母在函数 f 下的源点，即可得到该密文对应的明文。由表 3.1 可知，函数 f 的逆函数 f^{-1} 如表 3.2 所示。

表 3.2 函数 f^{-1}

x	A	B	C	D	E	F	G	H	I	J	K	L	M
$f^{-1}(x)$	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
$f^{-1}(x)$	W	X	Y	Z	A	B	C	D	E	F	G	H	I

将密文“*UZJTIVKVJKILTKLIV*”中的每个字母在函数 f^{-1} 中找到其对应的像，就可以得到对应的明文，即“*DISCRETESTRUCTURE*”。

例 3.22 设集合 $A=\{0,1,2,3,4,5,6,7,8,9\}$，$f$ 和 g 均为 A 上的函数，且对于任意 $x \in A$，$f(x)=(x+5)(\bmod 10)$，$g(x)=(x+1)(\bmod 10)$。若数字串按$(f^{-1} \circ g) \circ f$ 的方式加密，试求数字串“26198750”加密后的密文，以及密文“19250683”加密前的数字串。

解 由于$(f^{-1} \circ g) \circ f(x)=f(f^{-1} \circ g(x))=f(g(f^{-1}(x)))$，根据函数 f 和 g 的定义，

对于任意 $x\in A$，$f(x)$、$g(x)$、$f^{-1}(x)$、$g(f^{-1}(x))$和 $f(g(f^{-1}(x)))$的函数值如表 3.3 所示。

表 3.3 各函数值

x	0	1	2	3	4	5	6	7	8	9
$f(x)$	5	6	7	8	9	0	1	2	3	4
$g(x)$	1	2	3	4	5	6	7	8	9	0
$f^{-1}(x)$	5	6	7	8	9	0	1	2	3	4
$g(f^{-1}(x))$	6	7	8	9	0	1	2	3	4	5
$f(g(f^{-1}(x)))$	1	2	3	4	5	6	7	8	9	0

由表 3.3 可知，数字串"26198750"加密后的密文为"37209861"。

为求解密文"19250683"加密前的数字串，首先求出解密函数。根据数字串的加密方式，可知解密函数为$((f^{-1}\circ g)\circ f)^{-1}=f^{-1}\circ(g^{-1}\circ f)$。

又因 $f^{-1}\circ(g^{-1}\circ f)(x)=(g^{-1}\circ f)(f^{-1}(x))=f(g^{-1}(f^{-1}(x)))$。对于任意 $x\in A$，$f(g^{-1}(f^{-1}(x)))$的函数值如表 3.4 所示。

由表 3.4 可知，密文"19250683"加密前的数字串为"08149572"。

表 3.4 各函数值

x	0	1	2	3	4	5	6	7	8	9
$f(x)$	5	6	7	8	9	0	1	2	3	4
$g(x)$	1	2	3	4	5	6	7	8	9	0
$f^{-1}(x)$	5	6	7	8	9	0	1	2	3	4
$g^{-1}(x)$	9	0	1	2	3	4	5	6	7	8
$g^{-1}(f^{-1}(x))$	4	5	6	7	8	9	0	1	2	3
$f(g^{-1}(f^{-1}(x)))$	9	0	1	2	3	4	5	6	7	8

3.3 函数的应用

哈希函数(Hash function)也称为散列函数或 Hash 函数，是一种将任意长度的输入字符串变换成固定长度的输出字符串的函数。在数据结构中，通常借助哈希函数来加速对数据项的查找过程。根据应用情况的不同，通常也将哈希函数的输出称为哈希值、哈希码、散列值等。

在线性表、树等数据结构中，每个记录所在的相对位置是随机的，与记录的关键字之间不存在确定关系，因此，在这些数据结构中查找记录时需要进行一系列的关键字比较操作，相应的查找效率依赖于查找过程中所进行的比较次数。如果希望不经过任何比较，仅用一次存取就能得到需要的记录，就必须建立一个关于存储位置和关键字的对应关系 f，使得每个关键字与一个唯一的存储位置相对应。在查找时，只要根据这个对应关系 f 就能找到给定值 key 的像 f(key)。而一旦数据结构中存在关键字与 key 相等的记录，则其必定在 f(key)存储位置上，这样不需要进行比较就可以直接取得所查找的记录。这里的对应关系

f 实际上就是一个哈希函数，而按照这种思路建立的表格则称为哈希表(Hash table)。

例如，如果要建立一张学生成绩表，最简单的方法是以学生的学号作为关键字，1 号学生的记录位置在第 1 条，10 号学生的记录位置在第 10 条，以此类推。此时，如果要查看学号为 5 的学生成绩，则只要取出第 5 条记录就可以。这样建立的表实际上就是一张简单的哈希表，其哈希函数为 $f(\text{key})=\text{key}$。然而，很多情况下的哈希函数并不如此简单。为了查看方便，可能会以学生的名字作为关键字。此时，为了能够根据学生的名字直接定位出相应记录所在的位置，需要将这些名字转换为数字，构造出相应的哈希函数。下面给出两个不同的哈希函数。

(1) 考察学生名字的汉语拼音，将其中第一个字母在英语字母表中的序号作为哈希函数值。例如，“蔡军”的汉语拼音第一个字母为字母 C，因此取 03 作为其哈希值。

(2) 考察学生名字的汉语拼音，将其中第一个字母和最后一个字母在英语字母表中的序号之和作为哈希函数值。例如，“蔡军”的汉语拼音第一个字母和最后一个字母分别为 C 和 N，因此取 17 作为其哈希值。

分别应用这两个哈希函数，成绩表中部分学生名字不同的哈希函数值如表 3.5 所示。

表 3.5 学生名字的哈希函数值

key	李丽（LILI）	赵宏英（ZHAOHONGYING）	肖军（XIAOJUN）	吴小艳（WUXIAOYAN）	肖秋梅（XIAOQIUMEI）	陈伟（CHENWEI）
$f_1(\text{key})$	12	26	24	23	24	03
$f_2(\text{key})$	21	33	38	37	33	12

在哈希表的构造过程中，可能会出现不同的关键字映射到同一地址的情况，即 $\text{key}_1 \neq \text{key}_2$，但 $f(\text{key}_1)=f(\text{key}_2)$，也将这种现象称为冲突或碰撞(collision)。实际上，由于哈希函数是把任意长度的字符串映射为固定长度的字符串，冲突是必然存在的。可以说，冲突不可能避免，只能尽可能减少。例如，上面给出的两个哈希函数中，应用第二个函数时出现的碰撞比应用第一个函数出现的碰撞要少得多。

常见的构造哈希函数的方法有以下几种。

(1) 直接定址法。直接定址法取关键字或关键字的某个线性函数值为哈希地址，即 $f(\text{key})=\text{key}$ 或 $f(\text{key})=a\cdot\text{key}+b$，其中 a 和 b 为常数。直接定址法所得到的地址空间与关键字集合的大小相同，对于不同的关键字不会发生冲突，但在实际应用中使用这种哈希函数的情况比较少。

(2) 数字分析法。数字分析法适合于关键字由若干数码组成，同时各数码的分布规律事先知道的情况。具体方法是：分析关键字集合中每个关键字中的每位数码的分布情况，找出数码分布均匀的若干位作为关键字的存储地址。

例如，一个由 80 个结点组成的结构，其关键字为 6 位十进制数。选择哈希表长度为 100，则可取关键字中的两位十进制数作为结点的存储地址。具体采用哪两位数码，需要用数字分析法对关键字中的数码分布情况进行分析。假设结点中有一部分关键字如下：

$\text{key}_1=3\ 0\ 1\ 5\ 1\ 4$　　$\text{key}_2=3\ 0\ 3\ 0\ 2\ 7$

$\text{key}_3=3\ 0\ 1\ 1\ 0\ 3$　　$\text{key}_4=3\ 0\ 8\ 3\ 2\ 9$

$\text{key}_5=3\ 0\ 0\ 2\ 8\ 7$　　$\text{key}_6=3\ 0\ 5\ 9\ 3\ 9$

$\text{key}_7=3\ 0\ 0\ 7\ 9\ 2$　　$\text{key}_8=3\ 0\ 0\ 4\ 6\ 3$

对上述关键字分析可以发现,关键字的第 1 位均为 3,第 2 位均为 0,分布集中,不适合作为存储地址。而第 4 位和第 5 位分布均匀,所以该哈希函数可以构造为取第 4、5 位作为结点的存储地址。上述 8 个结点的散列地址为:

$$f(\mathrm{key}_1)=51 \quad f(\mathrm{key}_2)=02 \quad f(\mathrm{key}_3)=10 \quad f(\mathrm{key}_4)=32$$

$$f(\mathrm{key}_5)=28 \quad f(\mathrm{key}_6)=93 \quad f(\mathrm{key}_7)=79 \quad f(\mathrm{key}_8)=46$$

(3) 平方取中法。平方取中法是一种比较常用的构造哈希函数的方法,具体是:将关键字求平方后,取其中间的几位数字作为散列地址。由于关键字平方后的中间几位数字和组成关键字的每一位数字都有关,因此产生冲突的可能性较小,最后究竟取几位数字作为散列地址需要由散列表的长度决定。例如,若结构的存储地址范围是 1～999,则取平方值的中间 3 位,如表 3.6 所示。

表 3.6 平均取中法

关键字 key	key^2	哈希地址	压缩地址
11032710	121720689944100	689	344
11054312	122197813793344	813	406
01110345	001232866019025	866	433
01111401	001235212182801	212	106

若所取哈希函数值超出了存储区的地址范围,则可以再乘以一个比例因子,把哈希函数值放大或缩小,使其位于存储区的范围内。如果上述示例中存储地址范围是 1～500,则可以对哈希地址再乘以 0.5 取整。

(4) 折叠法。折叠法适用于关键字位数很多且关键字中每一位上数字分布大致均匀的情况。具体方法是:将关键字分割成位数相同的几部分(最后一部分的位数可以不同),然后取这几部分的叠加和(舍去进位)作为哈希地址。叠加又可分为移位叠加和间界叠加。其中,移位叠加是将分组后的每组数字的最低位对齐,然后相加;间界叠加是将分组后的每组数字从一端向另一端沿分界线进行来回折叠,然后对齐相加。

例如,西文图书的国际标准图书编号是一个 10 位的十进制数,对某图书编号为 0-383-40284-6,则其通过移位叠加和间界叠加所得到的哈希地址分别如图 3.5(a)和图 3.5(b)所示。

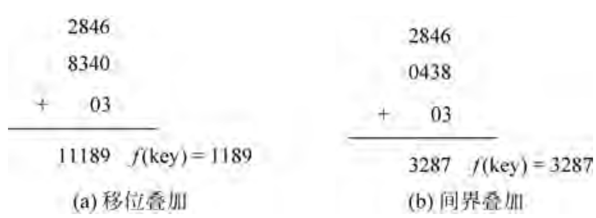

图 3.5 折叠法

(5) 除留余数法。除留余数法取关键字被某个不大于哈希表表长 m 的数 p 除后所得余数为哈希地址,即 $f(\mathrm{key})=\mathrm{key}(\mathrm{mod}\ p)$,其中 $p\leqslant m$。这是一种最简单也最常用的构造哈希函数的方法。它不仅可以对关键字直接取模(mod),也可在折叠、平方取中等运算之后取模。值得注意的是,在使用除留余数法时,对 p 的选择很重要。若 p 选得不好,容易产生

同义词。由经验得知,一般情况下可以选 p 为质数或不包含小于 20 的质因数的合数。

(6) 随机数法。随机数法选择一个随机函数,取关键字的随机函数值为它的哈希地址,即 $f(\text{key})=\text{random}(\text{key})$,其中,random 为随机函数。通常,当关键字长度不等时采用此法构造哈希函数较恰当。

哈希函数中会不可避免地存在冲突,因此在建造哈希表时不仅要设定一个“好”的哈希函数,而且要设定一种处理冲突的方法。假设哈希表的地址集为 $0\sim(n-1)$,冲突是指由关键字得到的哈希地址为 $j(0\leqslant j\leqslant n-1)$的位置上已存有记录,则“处理冲突”就是为该关键字的记录找到另一个“空”的哈希地址。在处理冲突的过程中可能得到一个地址序列 h_i,其中,$h_i\in[0,n-1]$,$i=1,2,\cdots,k$。即在处理哈希地址的冲突时,若得到的另一个哈希地址 h_1 仍然发生冲突,则再求下一个地址 h_2,若 h_2 仍然冲突,再求得 h_3。以此类推,直至 h_k 不发生冲突为止,则 h_k 为记录在表中的地址。通常处理冲突的方法有下列几种。

(1) 开放定址法。开放定址法是当冲突发生时,形成一个检测序列;沿此序列逐个进行地址检测,直至找到一个空位置(开放的地址),将发生冲突的记录放到该地址中,即 $h_i=(f(\text{key})+d_i)(\text{mod } m)$,$i=1,2,\cdots,k(k\leqslant m-1)$,其中,$f(\text{key})$为哈希函数,$m$ 为哈希表表长,d_i 为增量序列。根据对 d_i 的设置又可以有以下 3 种不同的方法:

① $d_i=1,2,3,\cdots,m-1$,称为线性检测再散列;

② $d_i=1^2,-1^2,2^2,-2^2,3^3,\cdots,\pm k^2,(k\leqslant m/2)$,称为二次检测再散列;

③ $d_i=$伪随机数序列,称为伪随机检测再散列。

(2) 再哈希法。再哈希法是当同义词产生地址冲突时计算另一个哈希函数地址,直到冲突不再发生。这种方法不易产生“聚集”,但增加了计算的时间。

(3) 拉链法。拉链法是将所有关键字为同义词的记录存储在同一线性链表中。假设某哈希函数产生的哈希地址在区间$[0\cdots m-1]$上,则首先设立一个指针型向量 ChainHash$[m]$,其每个分量的初始状态都是空指针。接下来,对于哈希地址为 i 的所有记录都插入到以 ChainHash$[i]$为头指针的链表中。

例如,已知一组关键字为(26,36,41,38,44,15,68,12,06,51),表长为 13,选定的散列函数为 $f(\text{key})=\text{key}\ (\text{mod } 13)$,则用拉链法构造的哈希表如图 3.6 所示。

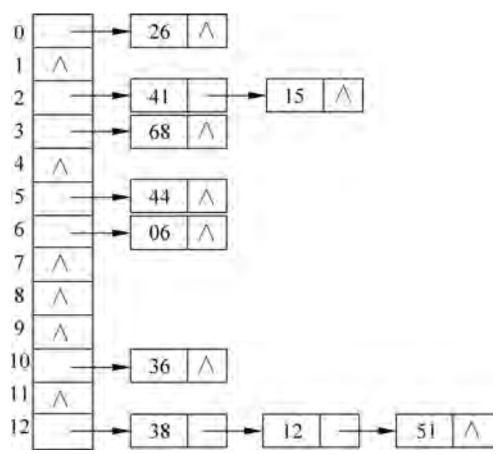

图 3.6 拉链法构造的哈希表

习题

3.1　对于集合 $A=\{x,y,z\}$ 和 $B=\{1,2,3\}$，判断下列 A 到 B 的关系哪些构成函数：

① $\{<x,1>,<x,2>,<y,1>,<y,3>\}$；

② $\{<x,1>,<y,3>,<z,3>\}$；

③ $\{<x,1>,<y,1>,<z,1>\}$；

④ $\{<x,2>,<y,3>\}$；

⑤ $\{<x,1>,<y,2>,<z,3>\}$；

⑥ $\{<x,1>,<x,2>,<y,1>,<y,3>,<z,2>,<z,3>\}$。

3.2　判断下列关系哪些是函数：

① $\{<x,|x|> \mid x\in \mathbf{R}\}$；

② $\{<|x|,x> \mid x\in \mathbf{R}\}$；

③ $\{<x,y> \mid x\in \mathbf{R}, y\in \mathbf{R}, |x|=|y|\}$；

④ $\{<x,y> \mid x\in \mathbf{Z}, y\in \mathbf{Z}, y$ 整除 $x\}$；

⑤ $\{<x,y> \mid x\in \mathbf{Z}, y\in \mathbf{Z}, x=y+1\}$；

⑥ $\{<x,y> \mid x\in \mathbf{N}, y\in \mathbf{N}, x=y+1\}$。

3.3　对于集合 $A=\{a,b,c\}$，问：

① A 到 A 可以定义多少个不同的函数？

② $A\times A$ 到 A 可以定义多少个不同的函数？

③ A 到 $A\times A$ 可以定义多少个不同的函数？

3.4　对于集合 $A=\{a,b,c,d\}$ 和 $B=\{1,2,3\}$，A 到 B 可以定义多少个不同的函数？写出 A 到 B 的 3 个不同函数。

3.5　对于函数 $f:A\to B$ 和 $g:A\to B$，求证：

① $f\cup g$ 为 A 到 B 的函数当且仅当 $f=g$；

② $f\cap g$ 为 A 到 B 的函数当且仅当 $f=g$。

3.6　下列函数哪些是单射函数、满射函数或双射函数：

① $f:\mathbf{Z}^+\to\mathbf{Z}^+$（$\mathbf{Z}^+$ 是正整数集合），$f(x)=3x$；

② $f:\mathbf{Z}\to\mathbf{Z}, f(x)=|x|$；

③ 集合 $A=\{0,1,2\}$ 到 $B=\{0,1,2,3,4\}$ 的函数 f，$f(x)=x^2$；

④ $f:\mathbf{R}\to\mathbf{R}, f(x)=x+1$；

⑤ $f:\mathbf{N}\to\mathbf{N}\times\mathbf{N}, f(x)=<x,x+1>$；

⑥ $f:\mathbf{Z}\to\mathbf{N}, f(x)=|2x|+1$。

3.7　对于集合 A 和 B，且 $|A|=m$，$|B|=n$，问：

① A 到 B 可以定义多少个不同的函数？

② A 到 B 可以定义多少个不同的单射函数？

③ A 到 B 可以定义多少个不同的满射函数？

④ A 到 B 可以定义多少个不同的双射函数？

3.8 对于下列集合对 A 和 B，构造一个 A 到 B 的双射函数：

① $A=\mathbf{N}, B=\mathbf{N}-\{0\}$；

② $A=P(\{1,2,3\}), B=\{0,1\}^3$；

③ $A=[0,1], B=[1/4,1/2]$。

3.9 对于函数 $f: A\to B$ 和 $g: B\to C$，试证明以下结论：

① 如果 f 和 g 是单射函数，则 $f\circ g$ 是单射函数；

② 如果 f 和 g 是满射函数，则 $f\circ g$ 是满射函数；

③ 如果 f 和 g 是双射函数，则 $f\circ g$ 是双射函数。

3.10 对于函数 $f: A\to B$ 和 $g: B\to C$，举例说明以下论断是成立的。

① 如果 f 和 g 是单(满、双)射函数，则 $f\circ g$ 是单(满、双)射函数；

② 如果 $f\circ g$ 是单射函数，则 f 是单射函数；

③ 如果 $f\circ g$ 是满射函数，则 g 是满射函数；

④ 如果 $f\circ g$ 是双射函数，则 f 是单射函数，g 是满射函数。

3.11 对于函数 $f: A\to B$ 和 $g: B\to C$，举例说明以下论断是不成立的：

① 如果 $f\circ g$ 是双射函数，则 g 是单射函数，f 是满射函数；

② 如果 $f\circ g$ 是单射函数，则 g 是单射函数；

③ 如果 $f\circ g$ 是满射函数，则 f 是满射函数。

3.12 对于集合 $A=\{a,b,c,d\}$、$B=\{1,2,3\}$ 和 $C=\{a,b,d\}$，计算以下函数 $f: A\to B$ 和 $g: B\to C$ 的复合函数 $f\circ g$：

① $f=\{<a,1>,<b,2>,<c,1>,<d,3>\}, g=\{<1,a>,<2,b>,<3,d>\}$；

② $f=\{<a,2>,<b,3>,<c,1>,<d,3>\}, g=\{<1,a>,<2,a>,<3,a>\}$；

③ $f=\{<a,3>,<b,1>,<c,2>,<d,3>\}, g=\{<1,b>,<2,b>,<3,b>\}$；

④ $f=\{<a,2>,<b,1>,<c,3>,<d,3>\}, g=\{<1,d>,<2,b>,<3,a>\}$。

3.13 对于下列实数集合上的函数 $f(x)=2x^2+1, g(x)=-x+7, h(x)=2^x$ 和 $k(x)=x+3$，求 $f\circ g$、$g\circ f$、$f\circ f$、$g\circ g$、$f\circ h$、$f\circ k$、$k\circ h$、$h\circ k$。

3.14 对于集合 $A=\{a,b,c,d\}$ 和 $B=\{1,2,3,4\}$，判断以下函数 $f: A\to B$ 的逆关系是否为函数：

① $f=\{<a,1>,<b,2>,<c,3>,<d,4>\}$；

② $f=\{<a,2>,<b,3>,<c,1>,<d,3>\}$；

③ $f=\{<a,3>,<b,1>,<c,2>,<d,4>\}$；

④ $f=\{<a,4>,<b,3>,<c,2>,<d,1>\}$。

3.15 设满射函数 $f: A\to A$ 满足 $f\circ f=f$，证明 $f=I_A$。

3.16 对于函数 $f: \mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}\times\mathbf{Z}, f(<x,y>)=<x+y,x-y>$，证明 f 是单射函数，并举例说明其不是满射函数。

3.17 对于函数 $f: \mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}\times\mathbf{Z}, f(<x,y>)=<x+2,x-y>$，求逆函数 f^{-1}。

3.18 对于函数 $f: \mathbf{Z}\times\mathbf{Z}\to\mathbf{Z}\times\mathbf{Z}, f(<x,y>)=<x-y,x-3>$，求复合函数 $f^{-1}\circ f$

和 $f\circ f$。

3.19 (凯撒密码)设26个英文小写字母构成的集合 $A=\{a,b,\cdots,z\}$,由0～25这26个整数构成的集合 $B=\{0,1,2,\cdots,25\}$。函数 $f:A\to B$ 表示小写英文字母与其字典排序位置的对应关系,且 $f(a)=0,f(b)=1,\cdots,f(z)=25$,$B$ 上的函数 g 定义为 $g(x)=(x+3)\pmod{26}$。若明文按 $(f\circ g)\circ f^{-1}$ 的方式加密,试求:

① 明文"computer"对应的密文;

② 密文的解密函数,并给出密文"khoor"对应的明文。