Chapter 5: Relations and Functions

謝孫源 講座教授
hsiehsy@mail.ncku.edu.tw
國立成功大學 資訊工程系

Outline

- ***Cartesian Products and Relations***
- Functions: Plain and one-to-one
- Onto Functions: Stirling Numbers of the Second Kind
- Special Functions
- The Pigeonhole Principle
- Function Composition and Inverse Function

Cartesian Products (1/4)

- **Definition 5.1:** For sets A, $B \subseteq U$, the *Cartesian product*, of A and B is denoted by $A \times B$ and equals $\{(a, b) | a \in A, b \in B\}$.

- the elements of $A \times B$ are ordered pairs.
- $|A \times B| = |A| \bullet |B|$

  $A \times B = B \times A$?
- If $n \in \mathbf{Z}^+$, $n \geq 3$, and $A_1, A_2, \ldots, A_n \subseteq U$, the n-fold product of $A_1, A_2, \ldots, A_n$, denoted by $A_1 \times A_2 \times \ldots \times A_n$, equals $\{(a_1, a_2, \ldots, a_n) | a_i \in A_i, 1 \leq i \leq n\}$. The elements of $A_1 \times A_2 \times \ldots \times A_n$ are called ordered *n-tuples*.

Cartesian Products (2/4)

- **Definition 5.1 (cont.):**

  If $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in A_1 \times A_2 \times \ldots \times A_n$, then $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ iff $a_i = b_i$ for all $1 \leq i \leq n$.

- **Example 5.1:** Let $U=\{1, 2, 3, \ldots, 7\}$, $A=\{2, 3, 4\}$, $B=\{4, 5\}$. Then

  a) $A \times B=\{(2, 4), (2, 5), (3, 4), (3, 5), (4, 4), (4, 5)\}$.

  b) $B \times A=\{(4, 2), (4, 3), (4, 4), (5, 2), (5, 3), (5, 4)\}$.

  c) $B^2 = B \times B=\{(4, 4), (4, 5), (5, 4), (5, 5)\}$.

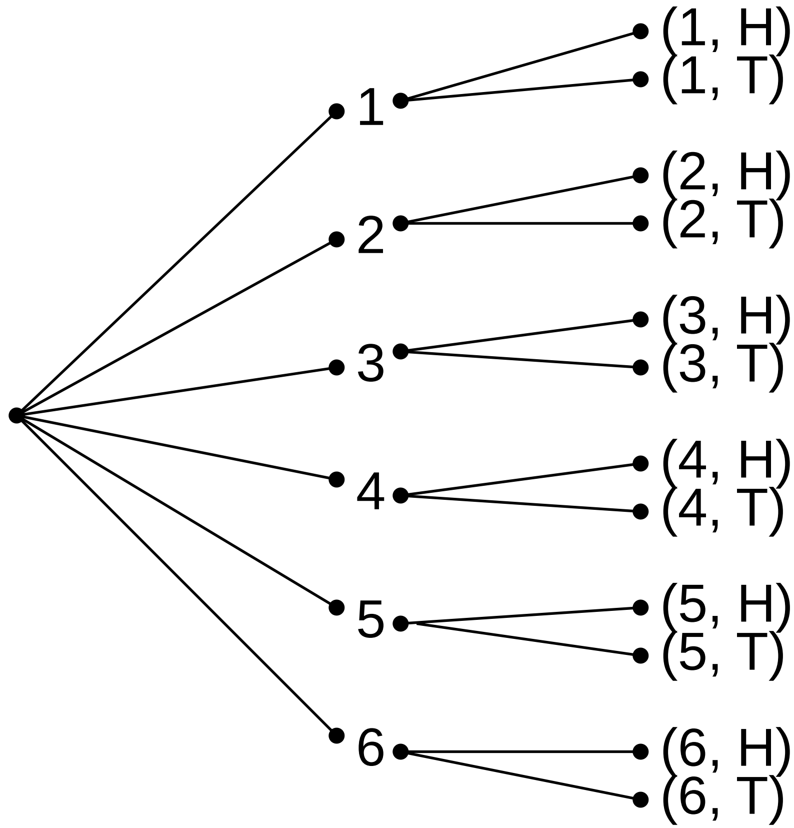
  d) $B^3 = B \times B \times B=\{(a, b, c) | a, b, c \in B\}$; for instance, $(4, 5, 5) \in B^3$.

Cartesian Products (3/4)

- An experiment $\mathcal{E}$ conducted as follows: A single die is rolled and its outcome noted, and then a coin is flipped and its outcome noted. Determine a sample space for I for $\mathcal{E}$.

- Let $\mathcal{E}_1$ denote the first part of experiment $\mathcal{E}$, and let $I_1=\{1, 2, 3, 4, 5, 6\}$ be a sample space for $\mathcal{E}_1$. Likewise let $I_2=\{H, T\}$ be a sample space for $\mathcal{E}_2$, the second part of the experiment. Then $I=I_1\times I_2$ is a sample space for $\mathcal{E}$.

Cartesian Products (4/4)



Relation (1/4)

- **Definition 5.2:** For sets A, $B \subseteq U$, any subset of $A \times B$ is called a *Relation* from A to B. Any subset of $A \times A$ is called a *binary relation* on A.

- **Example 5.5:** $U=\{1, 2, 3, \ldots, 7\}$, $A=\{2, 3, 4\}$, $B=\{4, 5\}$

  With A, B, U as in Example 5.1, the following are Relations from A to B.

  a) $\emptyset$ b) $\{(2, 4)\}$

  c) $\{(2, 4), (2, 5)\}$ d) $\{(2, 4), (3, 4), (4, 4)\}$

  e) $\{(2, 4), (3, 4), (4, 5)\}$ f) $A \times B$

Relation (2/4)

- In general, for finite sets A, B with $|A|=m$ and $|B|=n$, there are 2^{mn} relations from A to B, including the empty relation as well as the relation $A\times B$ itself.

- There are also $2^{nm}(=2^{mn})$ relations from B to A, one of which is also Ø and another of which is $B\times A$. The reason we get the same number of relations from B to A as we have from A to B is that any relation $\mathcal{R}_1$ from B to A can be obtained from a unique relation $\mathcal{R}_2$ from A to B by simply reversing the components of each ordered pair in $\mathcal{R}_2$.

Relation (3/4)

- **Example 5.6:** Let $B=\{1, 2\}\subseteq \mathrm{N}$, $U=\mathcal{P}(B)$ and $A=U=\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

  The following is an example of a *binary relation* on A: $\mathcal{R}=\{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}$.

  We can say that the relation $\mathcal{R}$ is the *subset relation* where $(C, D)\in\mathcal{R}$ if and only if $C, D\subseteq B$ and $C\subseteq D$.

- For any set $A\subseteq U$, $A\times\emptyset=\emptyset$ and $\emptyset\times A=\emptyset$.

Relation (4/4)

- **Theorem 5.1:** For any sets A, B, $C \subseteq U$:

  a) $A\times(B\cap C)=(A\times B)\cap(A\times C)$

  b) $A\times(B\cup C)=(A\times B)\cup(A\times C)$

  c) $(A\cap B)\times C=(A\times C)\cap(B\times C)$

  d) $(A\cup B)\times C=(A\times C)\cup(B\times C)$

  Pf: For any a, $b\in U$

  $(a, b)\in A\times(B\cap C) \Leftrightarrow a\in A$ and $b\in B\cap C$

  $\Leftrightarrow a\in A$ and $b\in B$, C

  $\Leftrightarrow a\in A$, $b\in B$ and $a\in A$, $b\in C$

  $\Leftrightarrow (a, b)\in A\times B$ and $(a, b)\in A\times C$

  $\Leftrightarrow (a, b)\in (A\times B)\cap(A\times C)$

Outline

- Cartesian Products and Relations
- ***<u>Functions: Plain and one-to-one</u>***
- Onto Functions: Stirling Numbers of the Second Kind
- Special Functions
- The Pigeonhole Principle
- Function Composition and Inverse Function

Function (1/2)

- **Definition 5.3:** For nonempty sets A, B, a *function*, or *mapping*, f *from* A to B, denoted $f: A \to B$, is a relation from A to B in which every element of A appears exactly once as the first component of an ordered pair in the relation.

- (a, b) is an ordered pair in the function f

  也記作 $f(a)=b$ a: a preimage of b

  b: the image of a under f.

- $(a, b), (a, c) \in f$ implies $b=c$.

Function (2/2)

- **Example 5.9:** For A={1, 2, 3} and B={w, x, y, z}, f ={(1, w), (2, x), (3, x)} is a function, and consequently a relation, from A to B. $\mathcal{R}_1$={(1, w), (2, x)} and $\mathcal{R}_2$= {(1, w), (2, w), (2, x), (3, z)} are relations, but not functions, from A to B. (Why?)

Domain and Range (1/3)

- **Definition 5.4:** For the function $f\colon A \to B$, A is called the *domain* of f and B the *codomain* of f. The subset of B consisting of those elements that appear as second components in the ordered pairs of f is called the *range* of f and is also denoted by $f(A)$ because it is the set of images (of the elements of A) under f.

Domain and Range (2/3)

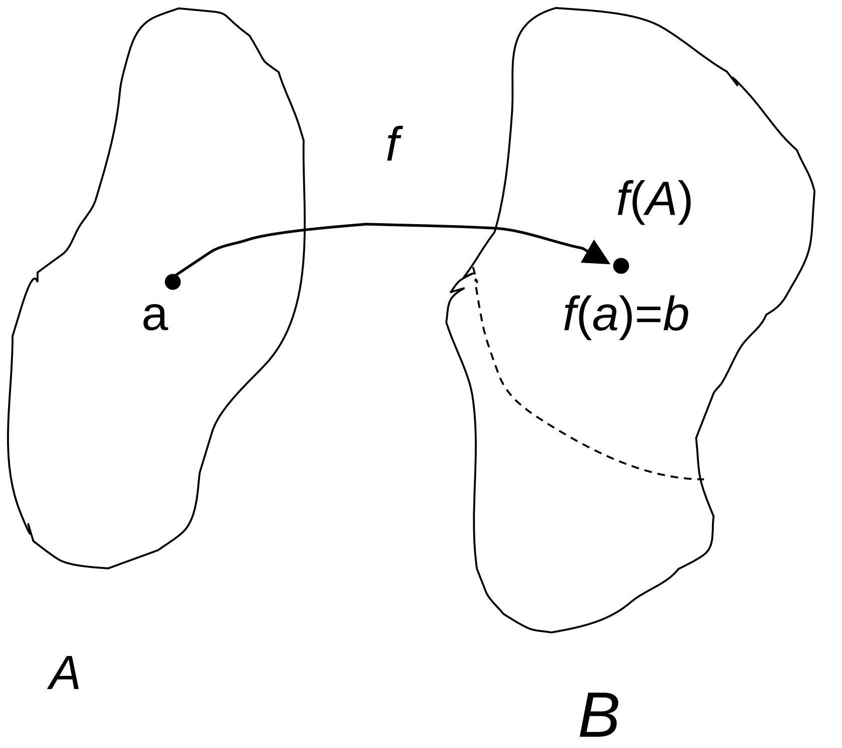


Figure 5.4

Domain and Range (3/3)

- For the general case, let A, B be nonempty sets with $|A|=m$, $|B|=n$. Consequently, if $A=\{a_1, a_2,\ldots, a_m\}$ and $B= \{b_1, b_2,\ldots, b_n\}$, then a typical function $f:A\rightarrow B$ can be described by $\{(a_1, x_1), (a_2,x_2),\ldots,(a_m, x_m)\}$. We can select any of the n elements of B for x_1 and then do the same for x_2. (We can select any element of B for x_2 so that the same element of B maybe selected for both x_1 and x_2.) We continue this selection process until one of the n elements of B is finally selected for x_m. In this way, using the rule of product there are $n^m=|B|^{|A|}$ functions from A to B.

Injective (1/2)

- **Definition 5.5:** A function $f:A\rightarrow B$ is called *one-to-one*, or *injective*, if each element of B appears at most once as the image of an element of A.

- **Example 5.14:** Let A={1, 2, 3} and B={1, 2, 3, 4, 5}. The function f ={(1, 1), (2, 3), (3, 4)} is a one-to-one function from A to B; g={(1, 1), (2, 3), (3, 3)} is a function from A to B, but it fails to be one-to-one because $g(2)=g(3)$ but $2\neq3$.

Injective (2/2)

- With $A=\{a_1, a_2, a_3,\ldots, a_m\}$, $B=\{b_1, b_2, b_3,\ldots, b_n\}$, and $m \leq n$, a one-to-one function $f:A \rightarrow B$ has the form $\{(a_1, x_1), (a_2, x_2), (a_3, x_3),\ldots,(a_m, x_m)\}$, where there are n choices for x_1(that is, any element of B), n-1 choices for x_2 (that is, any element of B except the one chosen for x_1), n-2 choices for x_3, and so on, finishing with $n-(m-1)=n-m+1$ choices for x_m. By the rule of product, the number of one-to-one Functions from A to B is $n(n-1)(n-2)\ldots(n-m+1)=\frac{n!}{(n-m)!}=P(n, m)=P(|B|,|A|)$.

Image (1/2)

- **Definition 5.6:** If $f:A\rightarrow B$ and $A_1\subseteq A$, then $f(A_1)=\{b\in B|b=f(a)$, for some $a\in A_1\}$, and $f(A_1)$ is called the *image of* A_1 *under* f.

- **Example 5.15:** For $A=\{1, 2, 3, 4, 5\}$ and $B=\{w, x, y, z\}$, let $f:A\rightarrow B$ be given by $f=\{(1, w), (2, x), (3, x), (4, y), (5, y)\}$. Then for $A_1=\{1\}$, $A_2=\{1, 2\}$, $A_3=\{1, 2, 3\}$, $A_4=\{2, 3\}$, and $A_5=\{2, 3, 4, 5\}$, we find the following corresponding images under f: $f(A_1)=\{f(a)|a\in A_1\}=\{f(a)|a\in\{1\}\}=\{f(a)|a=1\}=\{f(1)\}=\{w\}$;

Image (2/2)

- **Example 5.15 (cont.):**

  $f(A_2)=\{f(a)|a\in A_2\}=\{f\ (a)|a\in\{1, 2\}\}=\{f\ (a)|a=1$ or $2\}=\{f(1), f(2)\}=\{w, x\}$; $f(A_3)=\{f(1), f(2), f(3)\}=\{w, x\}$, and $f(A_3)=f(A_2)$ because $f(2)=x=f(3)$; $f(A_4)=\{x\}$; and, $f(A_5)=\{x, y\}$.

Restriction and Extension (1/4)

- **Theorem 5.2:** Let $f:A\rightarrow B$, with $A_1, A_2 \subseteq A$. Then

  a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

  b) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

  c) $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ when f is injective.

  Pf: For any $b \in B$, $b \in f(A_1 \cap A_2) \Rightarrow b = f(a)$ for some

  $a \in A_1 \cap A_2$

  $\Rightarrow b = f(a)$ for some

  $a \in A_1$, and

  $b = f(a)$ for some

  $a \in A_2$

Restriction and Extension (2/4)

$\Rightarrow b \in f(A_1)$ and $b \in f(A_2)$

$\Rightarrow b \in f(A_1) \cap f(A_2)$

$\therefore\ f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$

- **Definition 5.7:** If f: $A \to B$ and $A_1 \subseteq A$, then $f\,|_{A1}$: $A_1 \to B$ is called the *restriction of f to A_1* if $f|_{A1}(a) = f(a)$ for all $a \in A_1$.

- **Definition 5.8:** Let $A_1 \subseteq A$ and f: $A_1 \to B$. If g: $A \to B$ and $g(a) = f(a)$ for all $a \in A_1$, then we call g an *extension of f* to A.

Restriction and Extension (3/4)

- **Example 5.18:** Let $A=\{w, x, y, z\}$, $B=\{1, 2, 3, 4, 5\}$, and $A_1= \{w, y, z\}$. Let $f: A\to B$, $g: A_1\to B$ be represented by the diagrams in Fig. 5.5. Then $g: f|A_1$ and f is an extension of g from A_1 to A. We note that for the given function $g: A_1\to B$, there are five ways to extend g from A_1 to A.

Restriction and Extension (4/4)

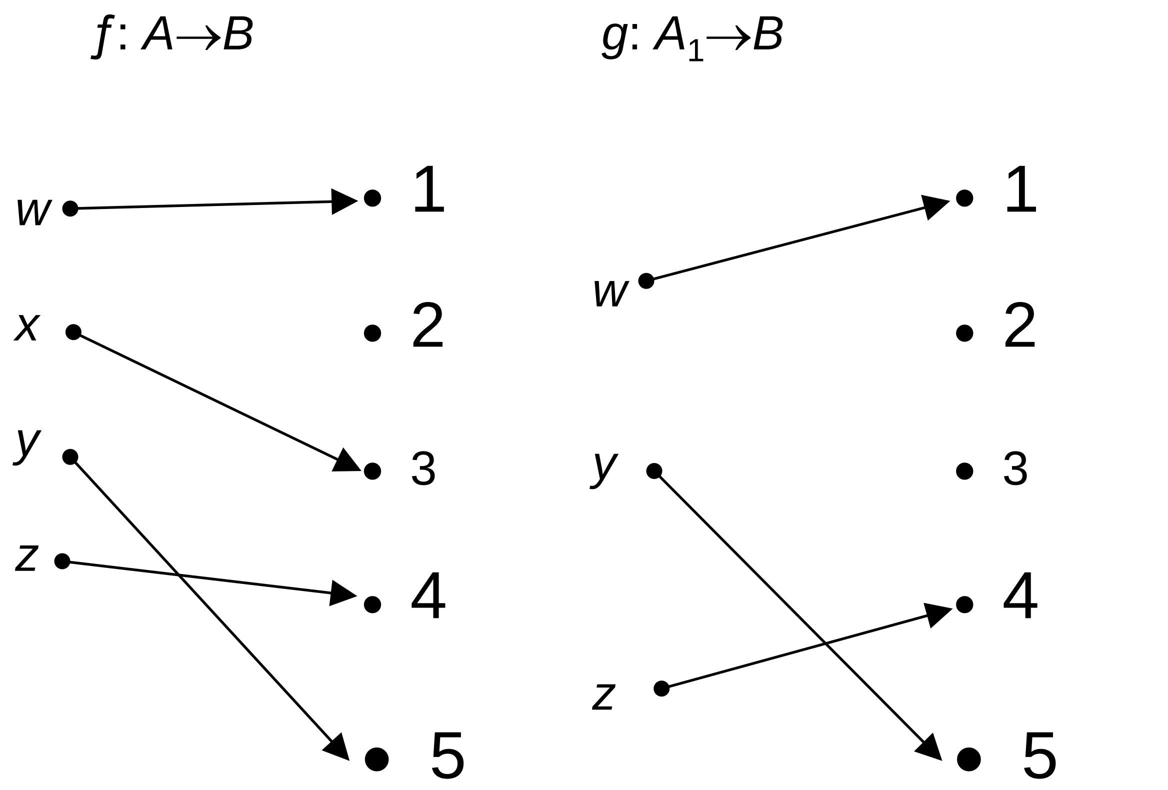


Figure 5.5

Outline

- Cartesian Products and Relations
- Functions: Plain and one-to-one
- ***Onto Functions: Stirling Numbers of the Second Kind***
- Special Functions
- The Pigeonhole Principle
- Function Composition and Inverse Function

Surjective (1/8)

- **Definition 5.9:** A function $f: A \to B$ is called *onto*, or *surjective*, if $f(A)=B$—that is, if for all $b \in B$ there is at least one $a \in A$ with $f(a)=b$.

- **Example 5.21:** If $A=\{1, 2, 3, 4\}$ and $B=\{x, y, z\}$, then $f_1=\{(1, z), (2, y), (3, x), (4, y)\}$ and $f_2=\{(1, x), (2, x), (3, y), (4, z)\}$ are both functions from A onto B. However, the function $g=\{(1, x), (2, x), (3, y), (4, y)\}$ is not onto, Because $g(A)=\{x, y\} \subset B$.

Surjective (2/8)

- For finite sets *A*, *B* with |*A*|=*m* and |*B*|=*n*, there are

$$\binom{n}{n}n^m - \binom{n}{n-1}(n-1)^m + \binom{n}{n-2}(n-2)^m - \ldots + (-1)^{n-2}\binom{n}{2}2^m +$$

$$(-1)^{n-1}\binom{n}{1}1^m = \sum_{k=0}^{n-1}(-1)^k\binom{n}{n-k}(n-k)^m = \sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m$$

onto functions from *A* to *B*.

Surjective (3/8)

- **Example 5.26:** If $A=\{a, b, c, d\}$ and $B=\{1, 2, 3\}$, then there are 36 onto functions from A to B or, equivalently, 36 ways to distribute four distinct objects into three distinguishable containers, with no container empty (and no regard for the location of objects in a given container). Among these 36 distributions we find the following collection of six (one of six such possible collections of six):

Surjective (4/8)

- **Example 5.26 (cont.):**

1) $\{a, b\}_1$ $\{c\}_2$ $\{d\}_3$
2) $\{a, b\}_1$ $\{d\}_2$ $\{c\}_3$
3) $\{c\}_1$ $\{a, b\}_2$ $\{d\}_3$
4) $\{c\}_1$ $\{d\}_2$ $\{a, b\}_3$
5) $\{d\}_1$ $\{a, b\}_2$ $\{c\}_3$
6) $\{d\}_1$ $\{c\}_2$ $\{a, b\}_3$,

- where, for example, the notation $\{c\}_2$ means that c is in the second container. Now if we no longer distinguish the containers, these 6=3! Distributions become identical, so there are 36/(3!)=6

Surjective (5/8)

- **Example 5.26 (cont.):**

  ways to distribute the distinct objects *a*, *b*, *c*, *d* among three Identical containers, leaving no container empty. So the number of ways in which it is possible to distribute the *m* distinct objects into *n* identical containers, with no container left empty, is

$$\frac{1}{n!}\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m$$

Surjective (6/8)

- This will be denoted by $S(m, n)$ and is called a *Stirling number of the second kind*. We note that for $|A|=m\geq n=|B|$, there are $n!\cdot S(m, n)$ onto functions from A to B.

- **Example 5.27:** For $m\geq n$, $\sum_{i=1}^{n} S(m,i)$ is the number of possible ways to distribute m distinct objects into n identical containers with empty containers allowed.

Surjective (7/8)

- **Example 5.27 (cont.):**

					$S(m, n)$			
m \ n	1	2	3	4	5	6	7	8
1	1							
2	1	1						
3	1	3	1					
4	1	7	6	1				
5	1	15	25	10	1			
6	1	31	90	65	15	1		
7	1	63	301	350	140	21	1	
8	1	127	966	1701	1050	266	28	1

Surjective (8/8)

- **Example 5.27 (cont.):**
- From the fourth row of Table 5.1 we see that there are 1+7+6=14 ways to distribute the objects *a*, *b*, *c*, *d* among three identical containers, with some container(s) possibly empty.

- **Theorem 5.3:** Let *m*, *n* be positive integers with $1 \le n \le m$. Then

$$S(m+1, n) = S(m, n-1) + nS(m, n).$$

Homework Assignment #1

- **EXERCISES 5.1**

  2, 4
- **EXERCISES 5.2**

  2, 3, 16, 18
- **EXERCISES 5.3**

  2, 4

Outline

- Cartesian Products and Relations
- Functions: Plain and one-to-one
- Onto Functions: Stirling Numbers of the Second Kind
- ***Special Functions***
- The Pigeonhole Principle
- Function Composition and Inverse Function

Binary / Unary operation (1/7)

- **Definition 5.10:** For any nonempty sets A, B, any function $f: A \times A \rightarrow B$ is called a *binary operation* on A. If $B \subseteq A$, then the binary operation is said to be *closed* (*on* A). [When $B \subseteq A$ we may also say that A *is closed under* f.]

- **Definition 5.11:** A function $g: A \rightarrow A$ is called a *unary*, or *monary*, operation on A.

Binary / Unary operation (2/7)

- **Example 5.29:**

a) The function $f : \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}$, defined by $f(a, b) = a - b$, is a closed binary operation on $\mathbf{Z}$.

b) If $g : \mathbf{Z}^+ \times \mathbf{Z}^+ \rightarrow \mathbf{Z}$ is the function where $g(a, b) = a - b$, then g is a binary operation on $\mathbf{Z}^+$, but is *not* closed. For example, we find that $3, 7 \in \mathbf{Z}^+$, but $g(3, 7) = 3 - 7 = -4 \notin \mathbf{Z}^+$.

c) The function $h: \mathbf{R}^+ \rightarrow \mathbf{R}^+$ defined by $h(a) = 1/a$ is a unary operation on $\mathbf{R}^+$.

Binary / Unary operation (3/7)

- **Example 5.30:** Let U be a universe, and let A, $B \subseteq U$.

  (a) If $f: P(U) \times P(U) \rightarrow P(U)$ is defined by $f(A, B) = A \cup B$, then f is a closed binary operation on $P(U)$.

  (b) The function $g: P(U) \rightarrow P(U)$ defined by $g(A) = \overline{A}$ is a unary operation on $P(U)$.

Binary / Unary operation (4/7)

- **Definition 5.12:** Let $f : A\times A\rightarrow B$; that is, f is a binary operation on A.

  a) f is said to be *commutative* if $f\,(a, b)=f\,(b, a)$ for all $(a, b)\in A\times A$.

  b) When $B\subseteq A$ (that is, when f is closed), f is said to be *associative* if for a, b, $c\in A$, $f\,(f(a, b),c)=f(a, f(b, c))$.

Binary / Unary operation (5/7)

- **Example 5.32:**

  (a) Define the closed binary operation $f:\mathbf{Z}\times\mathbf{Z}\rightarrow\mathbf{Z}$ by $f(a, b)=a+b-3ab$. Since both the addition and the multiplication of integers are commutative binary operations, it follows that $f(a, b)=a+b-3ab=b+a-3ba=f(b, a)$, so f is commutative. To determine whether f is associative, consider a, b, $c\in\mathbf{Z}$. Then $f(a, b)=a+b-3ab$ and $f(f(a, b), c)=f(a, b)+c-3f(a, b)c=(a+b-3ab)+c-3(a+b-3ab)c$ $=a+b+c-3ab-3ac-3bc+9abc$, whereas

Binary / Unary operation (6/7)

- **Example 5.32 (cont.):**

  $f(b, c)=b+c-3bc$ and $f(a,f(b, c))$

  $=a+f(b, c)-3af(b, c)$

  $=a+(b+c-3bc)-3a(b+c-3bc)$

  $=a+b+c-3ab-3ac-3bc+9abc$

  Since $f(f(a, b), c)=f(a,f(b, c))$ for all $a, b, c\in\mathbf{Z}$, the closed binary operation f is associative as well as commutative.

Binary / Unary operation (7/7)

- **Example 5.32 (cont.):**

  (b) Consider the closed binary operation h:$\mathbf{Z}\times\mathbf{Z}\rightarrow\mathbf{Z}$, where $h(a, b)=a|b|$. Then $h(3, -2)=3|-2|=3(2)=6$, but $h(-2, 3)=-2|3|=-6$. Consequently, h is *not* commutative. However, with regard to the associative property, if $a, b, c\in\mathbf{Z}$, we find that $h(h(a, b), c)=h(a, b)|c|=a|b||c|$ and $h(a,h(b,c))=a|h(b, c)|=a|b|c||=a|b||c|$, so the closed binary operation h is associative.

Identity (1/8)

- **Definition 5.13:** Let $f : A \times A \to B$ be a binary operation on A. An element $x \in A$ is called an *identity* (or *identity element*) for f if $f(a, x) = f(x, a) = a$, for all $a \in A$.

- **Example 5.34:**

  a) Consider the (closed) binary operation $f : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, where $f(a, b) = a + b$. Here the integer 0 is an identity since $f(a, 0) = a + 0 = 0 + a = f(0, a) = a$, for any integer a.

Identity (2/8)

- **Example 5.34 (cont.):**

  b) We find that there is no identity for the function in part (a) of Example 5.29. For if f had an identity x, then for any $a \in \mathbf{Z}$, $f(a,x) = a \Rightarrow a - x = a \Rightarrow x = 0$. But then $f(x,a) = f(0,a) = 0 – a \neq a$, unless $a = 0$.

  c) Let $A = \{1, 2, 3, 4, 5, 6, 7)$, and let $g: A \times A \to A$ be the (closed) binary operation defined by $g(a, b) = \min\{a,b\}$ that is, the minimum (or smaller) of a, b. This binary operation is commutative and

Identity (3/8)

- **Example 5.34 (cont.):**
  associative, and for any $a \in A$ we have g(a, 7) = min{a, 7} = a = min{7, a} = g(7, a). So 7 is an identity element for g.

- **Theorem 5.4:** Let $f : A \times A \to B$ be a binary operation. If f has a identity, then that identity is unique.

Identity (4/8)

- **Theorem 5.4 (cont.):**

  Proof: If f has more than one identity, let $x_1 x_2 \in A$ with $f(a, x_1)=a=f(x_1, a)$, for all $a \in A$, and $f(a, x_2)=a=f(x_2, a)$, for all $a \in A$. Consider x_1 as an element of A and x_2 as an identity. Then $f(x_1, x_2)=x_1$. Now reverse the roles of x_1 and x_2—that is, consider x_2 as an element of A and x_1 as an identity. We find that $f(x_1, x_2)=x_2$. Consequently, $x_1= x_2$, and f has at most one identity.

Identity (5/8)

- **Example 5.35:** If $A=\{x, a, b, c, d\}$, how many closed binary operations on A have x as the identity?

Let $f : A\times A\rightarrow A$ with $f(x, y)=y=f(y, x)$ for all $y\in A$. Then we may represent f by a tables as in Table 5.2. Here the nine values, where x is the first component—as in (x, c), or the second component—as in (d, x), are determined by the fact that x is the identity element.

Identity (6/8)

- **Example 5.35 (cont.):**

  Each of the 16 remaining (vacant) entries in Table 5.2 can be filled with any one of the five elements in *A*.

  Table 5.2

f	x	a	b	c	d
x	x	a	b	c	d
a	a	_	_	_	_
b	b	_	_	_	_
c	c	_	_	_	_
d	d	_	_	_	_

Identity (7/8)

- **Example 5.35 (cont.):**

  Hence there are 5^{16} closed binary operations on *A* where *x* is the identity.

  Of these $5^{10} = 5^4 \cdot 5^{(4^2-4)/2}$ are commutative.

  We also realize that there are 5^{16} closed binary operations on *A* where *b* is the identity.

  So there are

$$5^{17} = \binom{5}{1} 5^{16} = \binom{5}{1} 5^{5^2 - [2(5)-1]} = \binom{5}{1} 5^{(5-1)^2}$$

Identity (8/8)

- **Example 5.35 (cont.):**

  close binary operations on *A* that have an identity, and of these

  $$5^{11} = \binom{5}{1} 5^{10} = \binom{5}{1} 5^{4} \bullet 5^{(4^2-4)/2}$$

  are commutative.

Outline

- Cartesian Products and Relations
- Functions: Plain and one-to-one
- Onto Functions: Stirling Numbers of the Second Kind
- Special Functions
- ***The Pigeonhole Principle***
- Function Composition and Inverse Function

Pigeonhole Principle (1/15)

- **Definition :** If m pigeons occupy n pigeonholes and $m>n$, then at least one pigeonhole has two or more pigeons roosting in it.

- **Example 5.39:** An office employs 13 file clerks, so at least two of them must have birthdays during the same month. Here we have 13 pigeons (the file clerks) and 12 pigeonholes (the months of the year).

Pigeonhole Principle (2/15)

- **Example 5.40:** Larry returns from the laundromat with 12 pairs of socks (each pair a different color) in a laundry bag. Drawing the socks from the bag randomly, he’ll have to draw at most 13 of them to get a matched pair.

- **Example 5.41:** Wilma operates a computer with a magnetic tape drive. One day she is given a tape that contains 500,000 “words” of four or fewer lowercase letters. (Consecutive words on the tape are separated by a blank character.) Can it be that the 500,000 words are all distinct?

Pigeonhole Principle (3/15)

- **Example 5.41(cont.) :**

  From the rules of sum and product, the total number of different possible words, using four or fewer letters, is $26^4 + 26^3 + 26^2 + 26 = 475{,}254$

  With these 475,254 words as the pigeonholes, and the 500,000 words on the tape as the pigeons, it follows that at least one word is repeated on the tape.

Pigeonhole Principle (4/15)

- **Example 5.42:** Let $S \subset \mathbf{Z}^{+}$, where $|S|=37$. Then S contains two elements that have the same remainder upon division by 36.

Here the pigeons are the 37 positive integers in S. We know from the division algorithm (of Theorem 4.5) that when any positive integer n is divided by 36, there exists a unique quotient q and unique remainder r, where

$$n = 36q + r, \qquad 0 \leq r < 36.$$

Pigeonhole Principle (5/15)

- **Example 5.42 (cont.) :**
  The 36 possible values of r constitute the pigeonholes, and the result is now established by the pigeonhole principle.

- **Example 5.43:** Prove that if 101 integers are selected from the set $\boldsymbol{S} = \{1,2,3,\ldots,200\}$, then there are two integers such that one divides the other. For each $x \in \boldsymbol{S}$, we may write $x = 2^k y$, with $k \geq 0$, and $\gcd(2,y)=1$. (This result follows from the Fundamental Theorem of Arithmetic.)

Pigeonhole Principle (6/15)

- **Example 5.43 (cont.):**

  Then $y \in T = \{1,3,5,\ldots,199\}$, where $|T|=100$. Since 101 integers are selected from S, by the pigeonhole principle there are two distinct integers of the form $a=2^m y$, $b=2^n y$ for some (the same) $y \in T$. If $m<n$, then $a|b$; otherwise, we have $m>n$ and then $b|a$.

Pigeonhole Principle (7/15)

- **Example 5.44:** Any subset of size six from the set S={1, 2, 3,…, 9} must contain two elements whose sum is 10.

Here the numbers 1, 2, 3,…, 9 are the pigeons, and the pigeonholes are the subsets {1, 9}, {2, 8}, {3, 7}, {4, 6}, {5}. When six pigeons go to their respective pigeonholes, they must fill at least one of two-element subsets whose members sum to 10.

Pigeonhole Principle (8/15)

- **Example 5.46:** Let S be a set of six positive integers whose maximum is at most 14. Show that the sums of the elements in all the nonempty subsets of S cannot all be distinct.

- For each nonempty subset A of S, the sum of the elements in A, denoted s_A, satisfies $1 \leq s_A \leq 9+10+\ldots+14=69$, and there are $2^6-1=63$ nonempty subsets of S.

Pigeonhole Principle (9/15)

- **Example 5.46 (cont.):**

  We should like to draw the conclusion from the pigeonhole principle by letting the possible sums, from 1 to 69, be the pigeonholes, with the 63 nonempty subsets of S as the pigeons, but then we have too few pigeons.

  So instead of considering all nonempty subsets of S, we cut back to those nonempty subsets A of S where $|A| \leq 5$.

Pigeonhole Principle (10/15)

- **Example 5.46 (cont.):**

  Then for each such subset A it follows that $1 \leq s_A \leq 10+11+\ldots+14=60$. There are 62 nonempty subsets A of S with $|A| \leq 5$—namely, all the subsets of S except for and the set S itself. With 62 pigeons (the nonempty subsets A of S where $|A| \leq 5$) and 60 pigeonholes (the possible sums s_A), it follows by the pigeonhole principle that the elements of at least two of theses 62 subsets must yield the same sum.

Pigeonhole Principle (11/15)

- **Example 5.49:** Let us start by considering two particular examples:

1) Note how the sequences 6,5,8,3,7 (of length 5) contains the decreasing subsequence 6,5,3 (of length 3).

2) Now note how the sequence 11,8,7,1,9,6,5,10,3,12 (of length 10) contains the increasing subsequence 8,9,10,12 (of length 4).

Pigeonhole Principle (12/15)

- **Example 5.49 (cont.):**

  These two instances demonstrate the general result: For each $n \in \mathbf{Z}^+$, a sequence of n^2+1 distinct real numbers contains a decreasing or increasing subsequence of length $n+1$.

  To verify this claim let $a_1, a_2, \ldots, a_{n^2+1}$ be a sequence of n^2+1 distinct real numbers. For $1 \le k \le n^2+1$, let x_k = the maximum length of a decreasing subsequence that ends with a_k,

Pigeonhole Principle (13/15)

- **Example 5.49 (cont.):**

  and y_k = the maximum length of an increasing subsequence that ends with a_k.

  For instance, our second particular example would provide

k	1	2	3	4	5	6	7	8	9	10
a_k	11	8	7	1	9	6	5	10	3	12
x_k	1	2	3	4	2	4	5	2	6	1
y_k	1	1	1	1	2	2	2	3	2	4

Pigeonhole Principle (14/15)

- **Example 5.49 (cont.):**

  If, in general, there is no decreasing or increasing subsequence of length $n+1$, the $1 \leq x_k \leq n$ and $1 \leq y_k \leq n$ for all $1 \leq k \leq n^2+1$. Consequently, there are at most n^2 distinct ordered pairs (x_k, y_k). But we have n^2+1 ordered pairs (x_k, y_k), since $1 \leq k \leq n^2+1$. So the pigeonhole principle implies that there are two identical ordered pairs (x_i, y_i), (x_j, y_j), where $i \neq j$—say $i < j$.

Pigeonhole Principle (15/15)

- **Example 5.49 (cont.):**

  Now the real numbers a_1, $a_2,\ldots,a_{n^2+1}$ are distinct, so if $a_i<a_j$ then $y_i<y_j$, while if $a_j<a_i$ then $x_j>x_i$. In either case we no longer have $(x_i,y_i)=(x_j,y_j)$. This contradiction tells us that $x_k=n+1$ or $y_k=n+1$ for some $n+1\leq k\leq n^2+1$; the result then follows.

Outline

- Cartesian Products and Relations
- Functions: Plain and one-to-one
- Onto Functions: Stirling Numbers of the Second Kind
- Special Functions
- The Pigeonhole Principle
- ***Function Composition and Inverse Function***

Bijective

- **Definition 5.15:** If $f : A \to B$, then f is said to be *bijective*, or to be a *one-to-one correspondence*, if f is both one-to-one and onto.

- **Example 5.50:** If $A=\{1, 2, 3, 4\}$ and $B=\{w, x, y, z\}$, then $f=\{(1, w), (2, x), (3, y), (4, z)\}$ is a one-to-one correspondence from A (on) to B, and $g=\{(w, 1), (x, 2), (y, 3), (z, 4)\}$ is a one-to-one correspondence from B (on) to A.

Identity Function

- **Definition 5.16:** The function $1_A\colon A \to A$, defined by $1_A(a) = a$ for all $a \in A$, is called the *identity function* for A.

- **Definition 5.17:** If $f, g\colon A \to B$, we say that f and g are equal and write $f = g$ if $f(a) = g(a)$ for all $a \in A$.

Composite Function (1/4)

- **Definition 5.18:** If $f: A \to B$ and $g: B \to C$, we define the *composite function*, which is denoted $g \circ f : A \to C$, by $(g \circ f)(a) = g(f(a))$, for each $a \in A$.

- **Example 5.53:** Let $A=\{1, 2, 3, 4\}$, $B=\{a, b, c\}$, $C=\{w, x, y, z\}$ with $f: A \to B$ and $g: B \to C$ given by $f = \{(1, a), (2, a), (3, b), (4, c)\}$ and $g = \{(a, x), (b, y), (c, z)\}$. For each element of A we find:

$$(g \circ f)(1) = g(f(1)) = g(a) = x$$

$$(g \circ f)(2) = g(f(2)) = g(a) = x$$

Composite Function (2/4)

- **Example 5.53 (cont.):**

$$(g \circ f)(3) = g(f(3)) = g(b) = y$$

$$(g \circ f)(4) = g(f(4)) = g(c) = z$$

so

$$g \circ f = \{(1, x), (2, x), (3, y), (4, z)\}.$$

Composite Function (3/4)

- **Theorem 5.6:** If $f:A\rightarrow B$, $g:B\rightarrow C$ and $h:C\rightarrow D$, then $(h\circ g)\circ f=h\circ(g\circ f)$.

Proof: Since the two functions have the same domain, A, and codomain, D, the result will follow by showing that for every $x\in A$,
$((h\circ g)\circ f)(x)=(h\circ(g\circ f))(x)$.
(See the diagram shown in Fig.5.8.)

Using the definition of the composite function, we find that $((h\circ g)\circ f)(x)=(h\circ g)(f(x))=h(g(f(x)))$.

Composite Function (4/4)

- **Theorem 5.6 (cont.):**

  Consequently, the composition of functions is an associate operation.

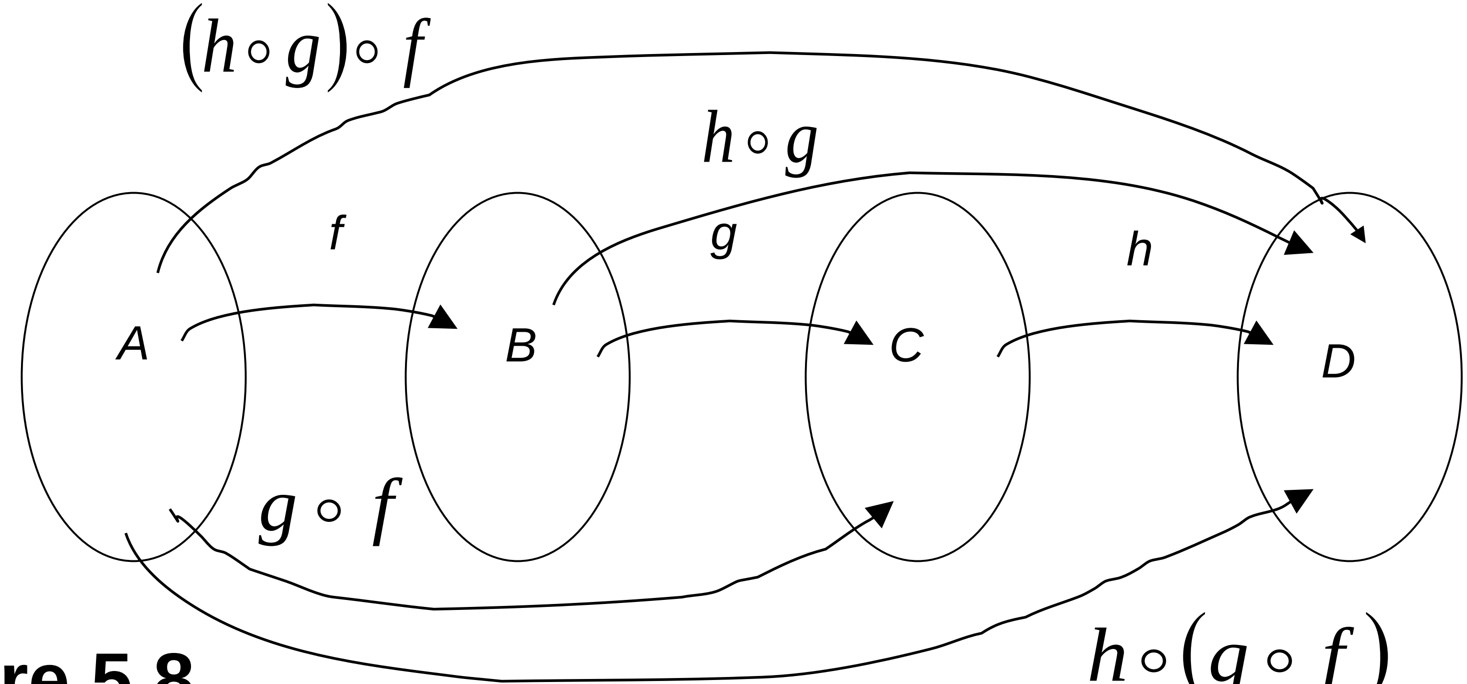


Figure 5.8

Invertible (1/5)

- **Definition 5.21:** If $f:A\to B$, then f is said to be *invertible* if there is a function $g:B\to A$ such that $g\circ f=1_A$ and $f\circ g=1_B$.

- **Example 5.58:** Let f, g:**R**→**R** be defined by $f(x)=2x+5$, g(x)=(1/2)(x-5). Then

$$(g\circ f)(x)=g(f(x))=g(2x+5)=(1/2)[(2x+5)-5]=x,$$

and $(f\circ g)(x)=f(g(x))=f((1/2)(x-5))=2[(1/2)(x-5)]$ $+5=x$, so $f\circ g=1_R$ and $g\circ f=1_R$.

Consequently, f and g are both invertible functions.

Invertible (2/5)

- **Theorem 5.7:** If a function $f:A\rightarrow B$ is invertible and a function $g:B\rightarrow A$ satisfies $g\circ f=1_A$ and $f\circ g=1_B$, then this function g is unique.

  Proof: If g is not unique, then there is another function $h:B\rightarrow A$ with $g\circ f=1_A$ and $f\circ g=1_B$

  Consequently,

  $h=h\circ 1_B=h\circ\left(f\circ g\right)=\left(h\circ f\right)\circ g=1_A\circ g=g.$

  We call g the inverse of f and use the notation $g=f^{-1}$.

Invertible (3/5)

- **Theorem 5.8:** A function $f : A \to B$ is invertible if and only if it is one-to-one and onto.

- **Example 5.59:** From Theorem 5.8 it follows that the function $f1:\mathbf{R}\to\mathbf{R}$ defined by $f1(x)=x^2$ is not invertible (it is neither one-to-one nor onto), but $f_2 : [0,+\infty) \to [0,+\infty)$ defined by $f_2(x) = x^2$ is invertible with $f_2^{-1}(x) = \sqrt{x}$.

Invertible (4/5)

- **Example 5.60:** For m, $b \in \mathbf{R}$, $m \neq 0$, the function f :$\mathbf{R} \rightarrow \mathbf{R}$ defined by $f = \{(x, y) | y = mx + b\}$ is an invertible function, because it is one-to-one and onto. To get f^{-1} we note that

$$f^{-1} = \{(x, y) | y = mx + b\}^c = \{(y, x) | y = mx + b\}$$

$$= \underbrace{\{(x, y) | x = my + b\}}_{\text{This is where we wish to change the components of the ordered pairs of } f.} = \{(x, y) | y = (1/m)(x - b)\}.$$

- So f :$\mathbf{R} \rightarrow \mathbf{R}$ is defined by $f(x) = mx + b$, and f^{-1}:$\mathbf{R} \rightarrow \mathbf{R}$ is defined by $f^{-1}(x) = (1/m)(x - b)$.

Invertible (5/5)

- **Example 5.61:** Let f :$\mathbf{R} \rightarrow \mathbf{R}^+$ be defined by $f(x)=e^x$, where e = 2.7183, the base for the natural logarithm. From the graph in Fig. 5.9 we see that f is one-to-one and onto, so f^{-1} :$\mathbf{R}^+ \rightarrow \mathbf{R}$ does exist and $f^{-1} = \{(x,y)|y = e^x\}^c = \{(x,y)|x = e^y\} = \{(x,y)|y = \ln x\}$, so $f^{-1}(x) = \ln x$.

Preimage (1/3)

- **Definition 5.22:** If $f : A \to B$ and $B_1 \subseteq B$, then $f^{-1}(B_1) = \{x \in A \mid f(x) \in B_1\}$. The set $f^{-1}(B_1)$ is called the *preimage of B_1 under f* .

- **Example 5.62:** Let A, $B \subseteq \mathbf{Z}^+$ where $A=\{1, 2, 3, 4, 5, 6\}$ and $B=\{6, 7, 8, 9, 10\}$. If $f : A \to B$ with $f = \{(1, 7), (2, 7), (3, 8), (4, 6), (5, 9), (6, 9)\}$, then the following results are obtained.

Preimage (2/3)

- **Example 5.62 (cont.):**

  a) For $B_1=\{6, 8\}\subseteq B$, we have $f^{-1}(B_1)=\{3, 4\}$, since $f(3)=8$ and $f(4)=6$, and for any $a \in A$, $f \notin B_1$ unless $a=3$ or $a=4$.

  Here we also note that $|f^{-1}(B_1)|=2=|B_1|$.

  b) In the case of $B_2=\{7, 8\}\subseteq B$, since $f(1)=f(2)=7$ and $f(3)=8$, we find that the preimage of B_2 under f is $\{1, 2, 3\}$. And here $|f^{-1}(B_2)|=3>2=|B_2|$.

Preimage (3/3)

- **Example 5.62 (cont.):**

  c) Now consider the subset B_3={8, 9} of B. For this case it follows that $f^{-1}(B_3)$={3, 5, 6} because $f(3)=8$ and $f(5)=f(6)=9$. Also we find that $|f^{-1}(B_3)|=3>2=|B_3|$.

  d) Finally, if $B_4=\{8, 9, 10\}\subseteq B$, then with $f(3)=8$ and $f(5)=f(6)=9$, we have $f^{-1}(B_4)=\{3, 5, 6\}$. So $f^{-1}(B_4)=f^{-1}(B_3)$ even though $B_4\supset B_3$. This result follows because there is no element a in the domain A where $f(a)=10$—that is, $f^{-1}(\{10\})=\emptyset$.

Homework Assignment #2

- **EXERCISES 5.4**

  6, 8
- **EXERCISES 5.5**

  2, 4
- **EXERCISES 5.6**

  2, 22