Book of Proof: Part IV, Relations, Functions, and Cardinality

January 22, 2018

Relations

$$5 < 10 \quad 3 < 12 \quad 99 < 999$$

$$5 \not< 5 \quad 12 \not< 3 \quad 10 \not< 0$$

Relations

$$5 < 10 \quad 3 < 12 \quad 99 < 999$$

$$5 \not< 5 \quad 12 \not< 3 \quad 10 \not< 0$$

$$R = \{(5,10), (3,12), (99,999), \ldots\}$$

$$(5,10) \in R \quad (3,12) \in R \quad (99,999) \in R$$

$$(5,5) \notin R \quad (12,3) \notin R \quad (10,0) \notin R$$

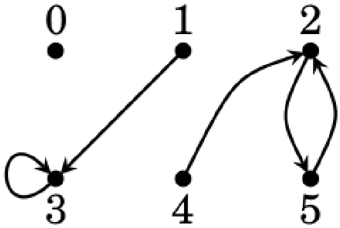
Relations

Definition 11.1 A **relation** on a set A is a subset $R \subseteq A \times A$.
We abbreviate $(x, y) \in R$ as xRy.

Relations in Pictures

Let $B = \{0, 1, 2, 3, 4, 5\}$ and

$$U = \{(1,3), (3,3), (5,2), (2,5), (4,2)\} \subseteq B \times B$$



Properties of Relations

Definition 11.2 Suppose R is a relation on set A.

1. R is **reflexive** if xRy for every $x \in A$.

$$\forall x \in A, xRx$$

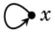
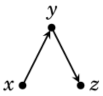
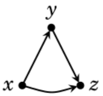
2. R is **symmetric** if xRy implies yRx for all $x, y \in A$.

$$\forall x, y \in A, xRy \Rightarrow yRx$$

3. R is **transitive** if xRy and yRz imply xRz.

$$\forall x, y, z \in A, ((xRy) \wedge (yRz)) \Rightarrow xRz$$

Pictures of Relation Properties

1.	A relation is **reflexive** if for each point x ...		...there is a loop at x:	
2.	A relation is **symmetric** if whenever there is an arrow from x to y ...		...there is also an arrow from y back to x:	
3.	A relation is **transitive** if whenever there are arrows from x to y and y to z ...		...there is also an arrow from x to z:	
	(If $x = z$, this means that if there are arrows from x to y and from y to x ...		...there is also a loop from x back to x.)	

Relations on $\mathbb{Z}$

Relations on $\mathbb{Z}$:	$<$	$\leq$	$=$	$\mid$	$\nmid$	$\neq$
Reflexive	no	yes	yes	yes	no	no
Symmetric	no	no	yes	no	no	yes
Transitive	yes	yes	yes	yes	no	no

Equivalence relations

Definition 11.3 A relation R on a set A is an **equivalence relation** if it is symmetric, reflexive, and transitive.

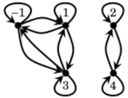
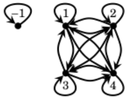
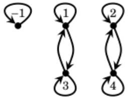
Equivalence relations

Definition 11.3 A relation R on a set A is an **equivalence relation** if it is symmetric, reflexive, and transitive.

Definition 11.4 Suppose R is an equivalence relation on set A. Given any element $a \in A$, the **equivalence class containing** a is the subset $\{x \in A : xRa\}$ of A consisting of all elements of A that relate to a.
This set is denoted $[a]$:

$$[a] = \{x \in A : xRa\}$$

Pictures of equivalence relations

Relation R	Diagram	Equivalence classes (see next page)
"is equal to" $(=)$ $R_1 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4)\}$		$\{-1\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$
"has same parity as" $R_2 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(-1,1),(1,-1),(-1,3),(3,-1),$ $(1,3),(3,1),(2,4),(4,2)\}$		$\{-1,1,3\}$, $\{2,4\}$
"has same sign as" $R_3 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(1,2),(2,1),(1,3),(3,1),(1,4),(4,1),$ $(2,3),(3,2),(2,4),(4,2),(1,3),(3,1)\}$		$\{-1\}$, $\{1,2,3,4\}$
"has same parity and sign as" $R_4 = \{(-1,-1),(1,1),(2,2),(3,3),(4,4),$ $(1,3),(3,1),(2,4),(4,2)\}$		$\{-1\}$, $\{1,3\}$, $\{2,4\}$

Congruence as equivalence relations

Example 11.8 proved that $\equiv \pmod{n}$ is an equivalence relation.

$$xRy = \{(x, y) : x \equiv y \pmod{3}\}$$

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod{3}\} \\
&= \{x \in \mathbb{Z} : 3 \mid (x - 0)\} = \{x \in \mathbb{Z} : 3 \mid x\} \\
&= \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\} = [3] = [6] \\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod{3}\} \\
&= \{x \in \mathbb{Z} : 3 \mid (x - 1)\} \\
&= \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\} = [4] = [7] \\
[2] &= \{x \in \mathbb{Z} : x \equiv 2 \pmod{3}\} \\
&= \{x \in \mathbb{Z} : 3 \mid (x - 2)\} \\
&= \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\} = [5] = [7]
\end{aligned}$$

Partitions

Definition 11.5 A **partition** of a set A is a set of non-empty subsets of A, such that the union of all the subsets equals A, and the intersection of any two different subsets is $\emptyset$.

$\{[0], [1], [2]\}$ under the relation $\equiv \pmod 3$, is a partition of $\mathbb{Z}$:

$$\{[0], [1], [2]\} = \{\{..., 0, 3, 6, ...\}, \{..., 1, 4, 7, ...\}, \{..., 2, 5, 8, ...\}\}$$

Equivalence Relations and Partitions

Theorem 11.2 Suppose R is an equivalence relation on set A. The the set $\{[a] : a \in A\}$ of equivalence classes of R forms a partition of A.

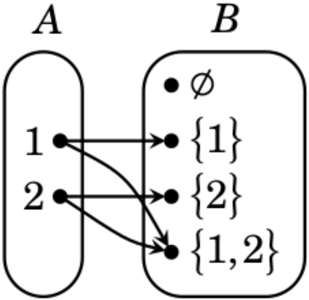
Conversely, any parition of A describes an equivalence relation R where xRy if and only if x and y belong to the same set in the parition.

The Integers Modulo n

$$
\begin{aligned}
[0] &= \{x \in \mathbb{Z} : x \equiv 0 \pmod 5)\} &= \{x \in \mathbb{Z} : 5 \mid (x-0)\} &= \{\ldots, -10, -5, 0, 5, 10, 15, \ldots\}, \\
[1] &= \{x \in \mathbb{Z} : x \equiv 1 \pmod 5)\} &= \{x \in \mathbb{Z} : 5 \mid (x-1)\} &= \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\}, \\
[2] &= \{x \in \mathbb{Z} : x \equiv 2 \pmod 5)\} &= \{x \in \mathbb{Z} : 5 \mid (x-2)\} &= \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}, \\
[3] &= \{x \in \mathbb{Z} : x \equiv 3 \pmod 5)\} &= \{x \in \mathbb{Z} : 5 \mid (x-3)\} &= \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}, \\
[4] &= \{x \in \mathbb{Z} : x \equiv 4 \pmod 5)\} &= \{x \in \mathbb{Z} : 5 \mid (x-4)\} &= \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}.
\end{aligned}
$$

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

Definition 11.7 A **relation** from a set A to a set B is a subset $R \subseteq A \times B$.
We abbreviate the statement $(x, y) \in R$ as xRy.



Functions

Definition 12.1 Suppose A and B are sets. A **function** from A to B (denoted as $f : A \to B$) is a relation $f \subseteq A \times B$, satisfying the property that for each $a \in A$, the relation f contains exactly one ordered pair of the form (a, b). The statement $(a, b) \in f$ is abbreviated $f(a) = b$.

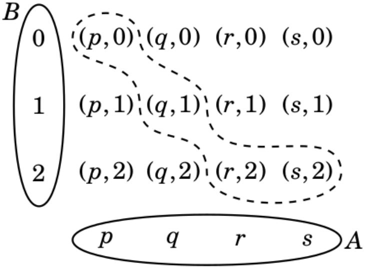
Functions

Definition 12.1 Suppose A and B are sets. A **function** from A to B (denoted as $f : A \to B$) is a relation $f \subseteq A \times B$, satisfying the property that for each $a \in A$, the relation f contains exactly one ordered pair of the form (a, b). The statement $(a, b) \in f$ is abbreviated $f(a) = b$.

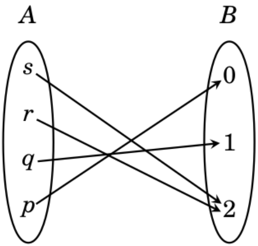
Definition 12.2
For a function $f : A \to B$, the set A is called the **domain** of f.
The set B is called the **codomain** of f.
The **range** of f is the set $\{f(a) : a \in A\} = \{b : (a, b) \in f\}$.

Example function

$$
\begin{aligned}
A &= \{p, q, r, s\} \\
B &= \{0, 1, 2\} \\
f &= \{(p, 0), (q, 1), (r, 2), (s, 2)\}
\end{aligned}
$$



(a)



(b)

Example function

$$\phi : \mathbb{Z}^2 \to \mathbb{Z}$$

$$\phi(m, n) = 6m - 9n$$

$$\phi = \{((m, n), 6m - 9n) : (m, n) \in \mathbb{Z}^2\} \subseteq \mathbb{Z}^2 \times \mathbb{Z}$$

Example function

$$\phi : \mathbb{Z}^2 \to \mathbb{Z}$$

$$\phi(m, n) = 6m - 9n$$

$$\phi = \left\{((m, n), 6m - 9n) : (m, n) \in \mathbb{Z}^2\right\} \subseteq \mathbb{Z}^2 \times \mathbb{Z}$$

- What is the domain?
- What is the codomain?
- What is the range?

Example function

$$\phi : \mathbb{Z}^2 \to \mathbb{Z}$$

$$\phi(m, n) = 6m - 9n$$

$$\phi = \{((m, n), 6m - 9n) : (m, n) \in \mathbb{Z}^2\} \subseteq \mathbb{Z}^2 \times \mathbb{Z}$$

- What is the domain?
- What is the codomain?
- What is the range?

$$\{3k : k \in \mathbb{Z}\}$$

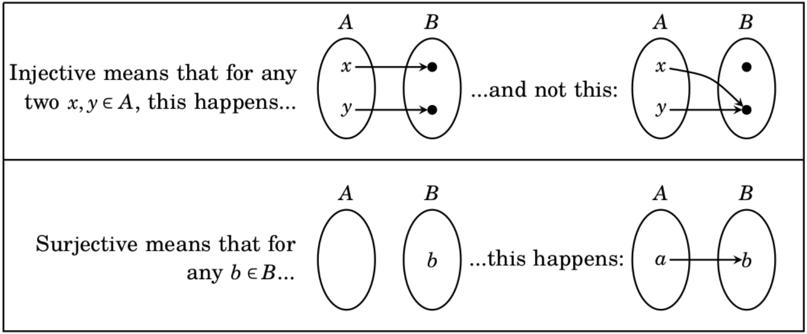
Equality of functions

Definition 12.3 Two functions $f : A \to B$ and $g : C \to D$ are **equal** if $A = C$, $B = D$, and $f(x) = g(x)$ for every $x \in A$.

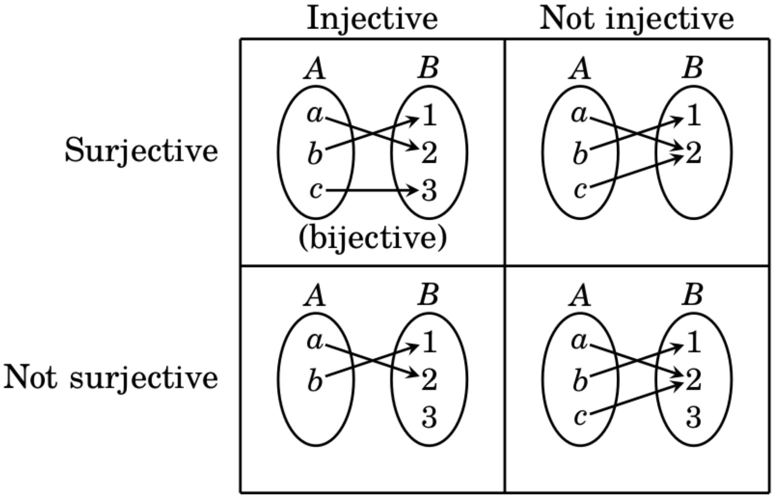
Injections and Surjections

Definition 12.4 A function $f : A \to B$ is

1. **injective** (or one-to-one) if
   for every $x, y \in A$, $x \neq y \Rightarrow f(x) \neq f(y)$;
2. **surjective** (or onto) if
   for every $b \in B$ there is an $a \in A$ with $f(a) = b$;
3. **bijective** if f is both injective and surjective.



Injective and Surjective Examples



Proving a function is an injection

How to show a function $f : A \to B$ is injective:

Direct approach:	**Contrapositive approach:**
Suppose $x, y \in A$, $x \neq y$.	Suppose $x, y \in A$, $f(x) = f(y)$.
$\vdots$	$\vdots$
Therefore $f(x) \neq f(y)$.	Therefore $x = y$.

Contrapositive is usually easier.

How to show a function $f : A \to B$ is not injective:

Find $x, y \in A, x = y$, with $f(x) \neq f(y)$.

Proving a function is a surjection

How to show a function $f : A \to B$ is surjective:

Suppose $b \in B$.

$\vdots$

There exists $a \in A$ with $f(a) = b$.

How to show a function $f : A \to B$ is not surjective:

Find $b \in B$ such that for all $a \in A, f(a) \neq b$.

Example 12.4

Proposition $f : \mathbb{R} - \{0\} \to \mathbb{R}$ defined as $f(x) = \frac{1}{x} + 1$ is injective but not surjective.

Injective.

Example 12.4

Proposition $f : \mathbb{R} - \{0\} \to \mathbb{R}$ defined as $f(x) = \frac{1}{x} + 1$ is injective but not surjective.

Injective. Suppose $x, y \in \mathbb{R} - \{0\}$ and $f(x) = f(y)$.
This implies $\frac{1}{x} + 1 = \frac{1}{y} + 1$.
Algebra shows $x = y$. Therefore f is injective.

Not surjective.

Example 12.4

Proposition $f : \mathbb{R} - \{0\} \to \mathbb{R}$ defined as $f(x) = \frac{1}{x} + 1$ is injective but not surjective.

Injective. Suppose $x, y \in \mathbb{R} - \{0\}$ and $f(x) = f(y)$.
This implies $\frac{1}{x} + 1 = \frac{1}{y} + 1$.
Algebra shows $x = y$. Therefore f is injective.

Not surjective. There exists $b = 1 \in \mathbb{R}$ for which $f(x) = \frac{1}{x} + 1 \neq 1$ for every $x \in \mathbb{R} - \{0\}$.

Example 12.5

Proposition The function $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $g(m, n) = (m + n, m + 2n)$ is both injective and surjective.

Injective.

Example 12.5

Proposition The function $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $g(m,n) = (m+n, m+2n)$ is both injective and surjective.

Injective. Suppose $(m,n), (k,\ell) \in \mathbb{Z} \times \mathbb{Z}$ and $g(m,n) = g(k,\ell)$.
Then $(m+n, m+2n) = (k+\ell, k+2\ell)$.
Then $m+n = k+\ell$ and $m+2n = k+2\ell$.
Algebra shows $m = k$ and $n = \ell$.
Therefore $(m,n) = (k,\ell)$ and g is injective.

Surjective.

Example 12.5

Proposition The function $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ defined by $g(m, n) = (m + n, m + 2n)$ is both injective and surjective.

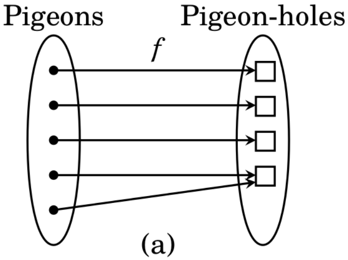
Injective. Suppose $(m, n), (k, \ell) \in \mathbb{Z} \times \mathbb{Z}$ and $g(m, n) = g(k, \ell)$.
Then $(m + n, m + 2n) = (k + \ell, k + 2\ell)$.
Then $m + n = k + \ell$ and $m + 2n = k + 2\ell$.
Algebra shows $m = k$ and $n = \ell$.
Therefore $(m, n) = (k, \ell)$ and g is injective.

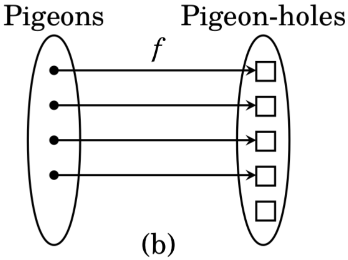
Surjective. Suppose $(b, c) \in \mathbb{Z} \times \mathbb{Z}$.
We need to find $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ for which $g(x, y) = (b, c)$.
We need to find (x, y) such that $x + y = b$ and $x + 2y = c$.
Solving gives $x = 2b - c$ and $y = c - b$.
Therefore $g(2b - c, c - b) = (b, c)$ and so g is surjective.

The Pigeonhole Principle

Suppose A and B are finite sets and $f : A \to B$ is any function.

1. If $|A| > |B|$ then f is not surjective.
2. If $|A| < |B|$ then f is not surjective.





Pigeonhole Principle Example

Proposition If A is any set of 10 integers between 1 and 100, then there exist two different subsets $X, Y \subseteq A$ for which the sum of elelments in X equals the sum of elements in Y.

Examples

$$A = \{5, 11, 16, 23, 44, 47, 50, 61, 67, 81\}$$
$$X = \{5, 11, 16, 23\}$$
$$Y = \{5, 50\}$$

$$A = \{5, 12, 16, 23, 44, 47, 50, 61, 67, 81\}$$
$$X = \{5, 12, 16, 23\}$$
$$Y = \{12, 44\}$$

Pigeonhole Principle Example

Proposition If A is any set of 10 integers between 1 and 100, then there exist two different subsets $X, Y \subseteq A$ for which the sum of elelments in X equals the sum of elements in Y.

Proof. Suppose A is as stated and $X \subseteq A$.
Then X has no more than 10 elements between 1 and 100, so the sum of all elements in X is less than 1000.
How many subsets of A are there?

Pigeonhole Principle Example

Proposition If A is any set of 10 integers between 1 and 100, then there exist two different subsets $X, Y \subseteq A$ for which the sum of elelments in X equals the sum of elements in Y.

Proof. Suppose A is as stated and $X \subseteq A$.
Then X has no more than 10 elements between 1 and 100, so the sum of all elements in X is less than 1000.
How many subsets of A are there?

$$|\mathcal{P}(A)| = 2^{10} = 1024$$

Pigeonhole Principle Example

Proposition If A is any set of 10 integers between 1 and 100, then there exist two different subsets $X, Y \subseteq A$ for which the sum of elelments in X equals the sum of elements in Y.

Proof. Suppose A is as stated and $X \subseteq A$.
Then X has no more than 10 elements between 1 and 100, so the sum of all elements in X is less than 1000.
How many subsets of A are there?

$$|\mathcal{P}(A)| = 2^{10} = 1024$$

By the pigeonhole principle, two of these sets must have the same sum.

Pigeonhole Principle Example

Proposition There are at least two people in Washington State with the same number of hairs on their heads.

Pigeonhole Principle Example

Proposition There are at least two people in Washington State with the same number of hairs on their heads.

Proof.
The population of Washington is more than seven million.
Every human head has fewer than one million hairs.
By the pigeonhole principle, two Washingtonians must have the same number of hairs on their head.