Our present *major goal* is to study ways of solving *counting problems*, such as

- How many ways are there to choose a valid password on a computer system?
- What is the probability that two people in this room were born on the same day?
- How many valid Internet addresses are there?

All counting questions reduce to counting the number of elements in some set.

So, we need to agree what we mean by "the number of elements in a set" (some sets, as we know, have infinitely many elements).

We also need to find a way of comparing sizes of sets

We will also need more ways of producing sets out of existing ones.

Cartesian products (named after René Descartes, 1596–1650)

Definition

Let A and B be sets. Then $A \times B$ (the *Cartesian product* of A and B) is the set whose elements are pairs (a, b) with $a \in A$ and $b \in B$.

Example

- Let $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3\}$. Then

$$A \times B = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3), (4,1), (4,2), (4,3)\}$$

- The real plane can be regarded as $\mathbb{R} \times \mathbb{R}$ since every point on the plane is uniquely determined by the ordered pair of its Cartesian coordinates.
- Let $S = \{\spadesuit, \clubsuit, \diamondsuit, \heartsuit\}$ and $V = \{2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A\}$. Then $S \times V$ represents playing cards: for example, $(\spadesuit, Q) \in S \times V$ is the queen of spades and $(\diamondsuit, A) \in S \times V$ is the ace of diamonds.

If $A \neq B$ then $(a, b) \in A \times B$ and $(b, a) \in B \times A$; these are *different* sets. However, if $A = B$ we must remember that an element of $A \times A$ is an *ordered pair*.

For example, if $A = \{0, 1\}$ then $A \times A = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$. Here $(0, 1)$ and $(1, 0)$ are different elements of $A \times A$.

More generally, if we have several sets $A_1, \ldots, A_n$ we can define $A_1 \times \cdots \times A_n$ as the set of all tuples $(a_1, \ldots, a_n)$ where $a_i \in A_i$.

If $A_1 = \cdots = A_n = A$ we often write A^n instead of $A \times \cdots \times A$.

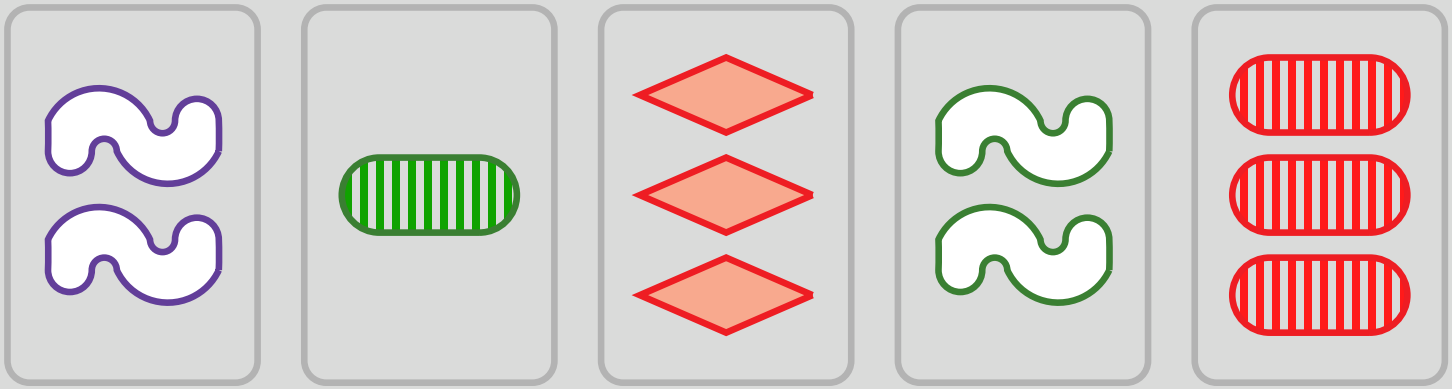
Example

- We can think of a record in a database as an element of the Cartesian product of several sets. For example, the database containing information about students would have a field for student ID, a field for first and last name etc.
- If $A = \{0, 1\}$ then A^N is the set of all bit strings of length N. For example, $A^3 = \{000, 100, 010, 001, 110, 101, 011, 111\}$ (to save space we write abc instead of (a, b, c)).

Example (The game of Set)

Each card has 4 characteristics:

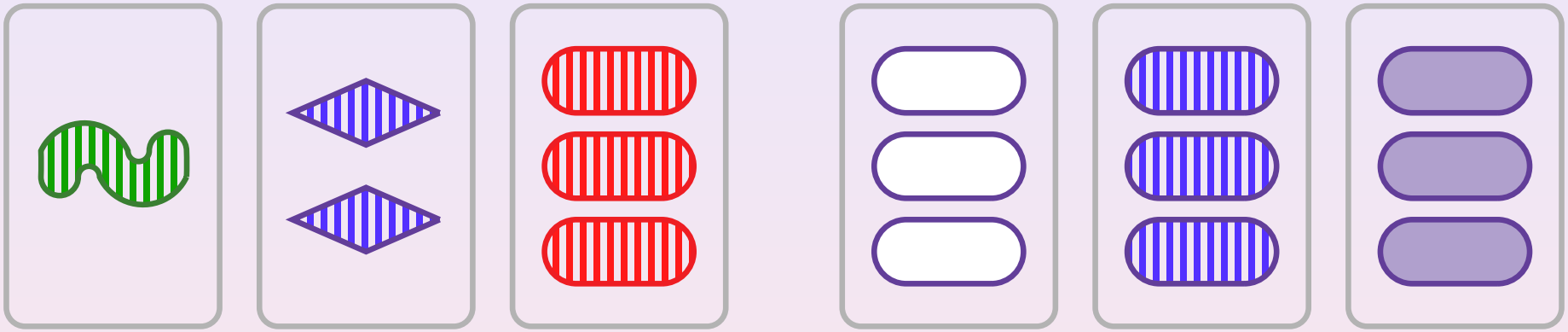
- Number of shapes on the card (1,2,3)
- The color of shapes on the card (red, green, purple)
- Shape (oval, diamond, squiggle)
- Shading (plain, striped, solid)



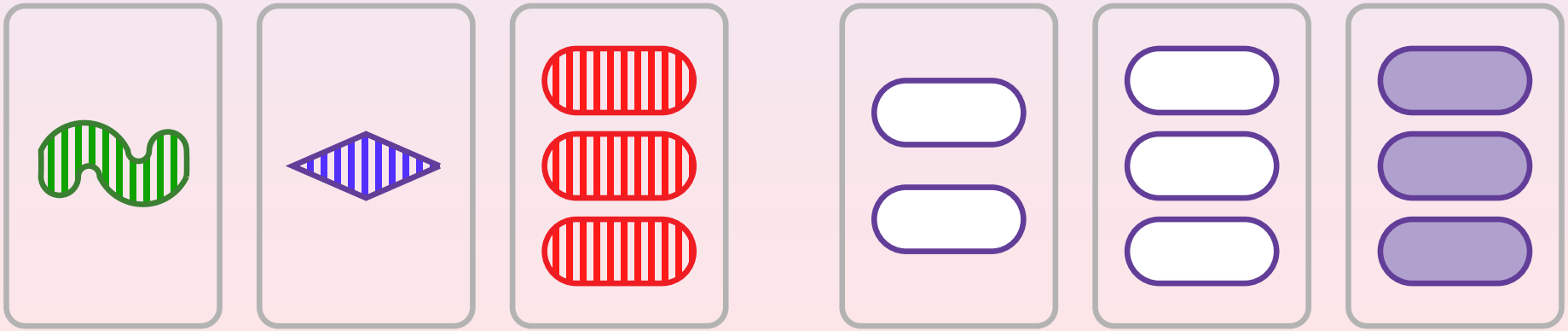
So, if $N = \{1, 2, 3\}$, $C = \{\text{red}, \text{green}, \text{purple}\}$, $S = \{\text{oval}, \text{diamond}, \text{squiggle}\}$ and $F = \{\text{plain}, \text{striped}, \text{solid}\}$ then each card can be represented as an element of $N \times C \times S \times F$.
Alternatively, we can think of each card as an element of $\{0, 1, 2\}^4$ (each characteristic has 3 possible values, encoded by 0, 1 and 2.

A SET is a collection of 3 cards, (a_1, a_2, a_3, a_4), (b_1, b_2, b_3, b_4) and (c_1, c_2, c_3, c_4) such that for each $i \in \{1, 2, 3, 4\}$ either $a_i = b_i = c_i$ or $a_i \neq b_i \neq c_i$.

For example, the following two collections of 3 cards are SETS:



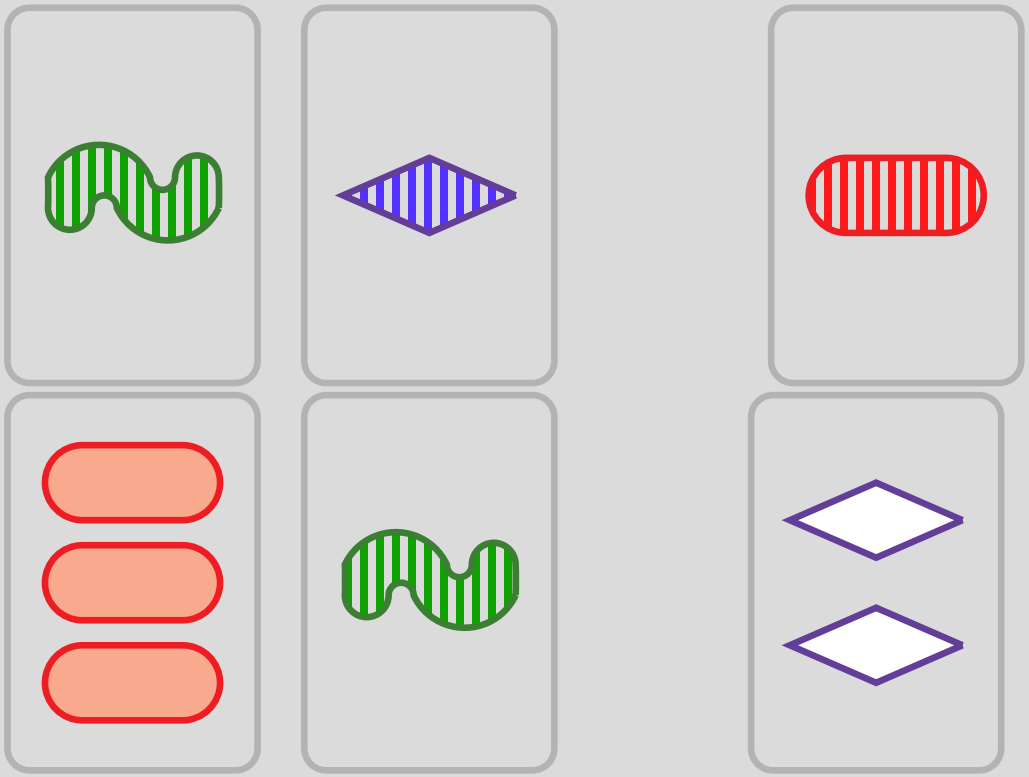
And the following two are not:



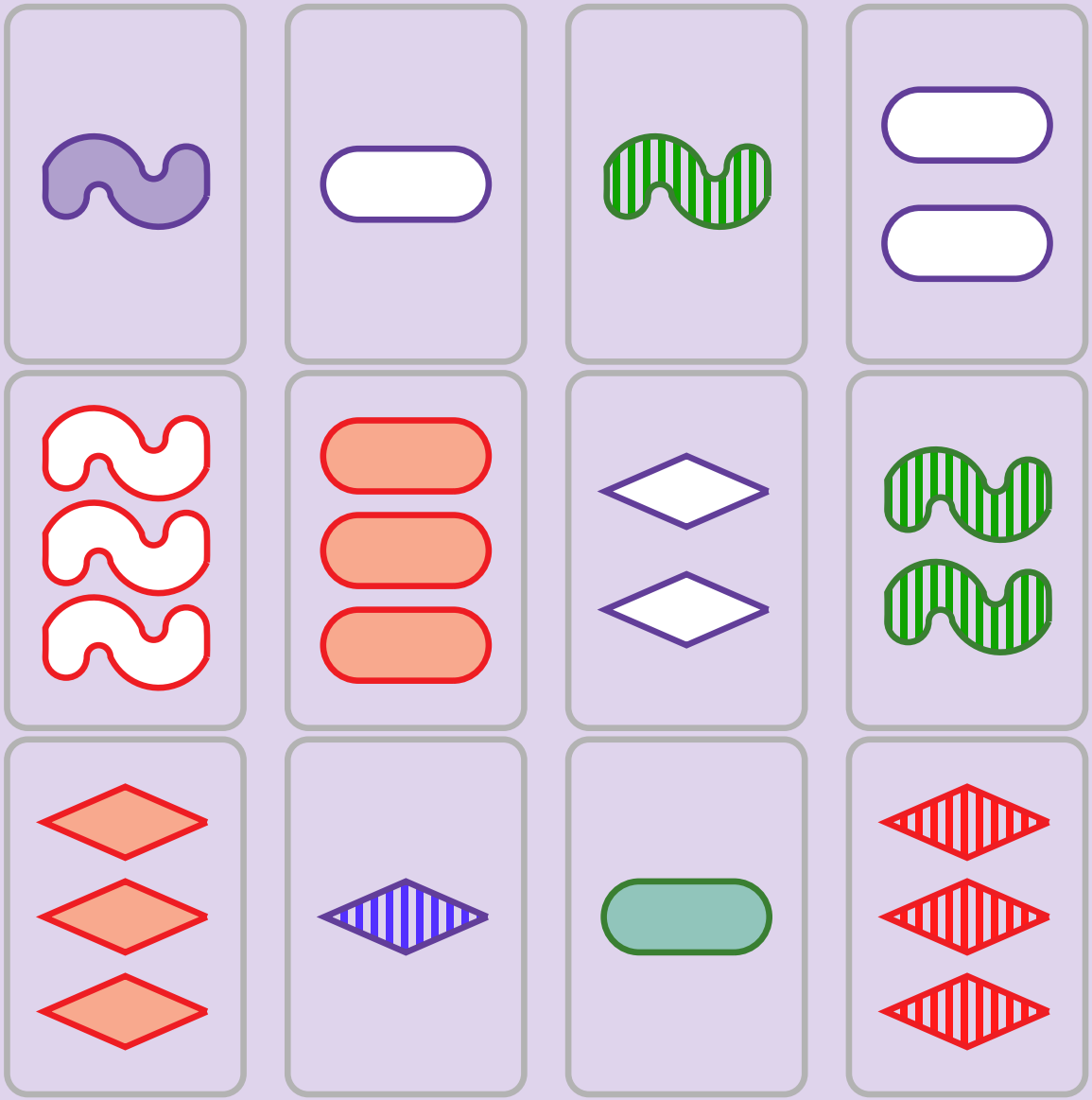
Exercise

Prove that for any pair of cards X, Y there exists a unique card Z such that X, Y and Z form a Set. Use this to design an algorithm for finding all Sets in a given collection of cards.

Example



Exercise: find all SETS in the following collection of cards



Relations

One of the reasons for introducing Cartesian products is that we can use them to describe *relations*.

For example, we often used the comparison of integers. This establishes a *relation* between two integers, $x < y$ or $y > x$.

Definition

A *relation* R on a set S is a subset of $S \times S$. If $s, s' \in S$ are such that $(s, s') \in R$ we say that s and s' are in relation R (or related by R). Sometimes this is denoted by sRs'.

Example

Let $\mathbb{Z}$ be the set of all integers.

- Let $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \leq y\}$. This is the familiar *order relation* on integers.

Example

- Fix positive integer m and let $R_m = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : m \mid x - y\}$. When x and y are in this relation, we say that x is equal to y modulo m and write $x \equiv y \pmod{m}$.
- Let U be a set and let S be the set of all subsets of U. Let $R = \{(X, Y) \in S \times S : X \subset Y\}$. This is the familiar *inclusion relation* between sets. Note that this relation does not involve all pairs $(X, Y) \in S \times S$.

Properties of relations

Let S be a set and let R be a relation on S.

- *Transitive relations*: R is transitive if for all $x, y, z \in S$, $xRy, yRz \implies xRz$ (that is, if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$).
- *Reflexive relations:* R is reflexive if xRx for all $x \in S$;
- *Symmetric relations:* R is symmetric if for all $x, y \in S$, $xRy \implies yRx$;
- *Antisymmetric relations:* R is antisymmetric if for all $x, y \in S$, $xRy, yRx \implies x = y$.
- *Equivalence relations:* R is an equivalence relation if R is reflexive, symmetric and transitive;
- *Partial orders:* R is a partial order if R is reflexive, antisymmetric and transitive;
- *Total orders:* R is a total order if it is transitive and for every $x \neq y \in S$ either xRy or yRx.

Example

- The relation $x < y$ on $\mathbb{Z}$ is a total order;
- The relation $x \equiv y \pmod{m}$ is an equivalence;
- The relation $X \subset Y$ is a partial order;

Definition

If A and B are set, a subset R of $A \times B$ is called a *relation* between A and B.

If R is an equivalence relation on S then for any $x \in S$ we denote $[x]$ the set $\{y \in S : (x, y) \in R\}$. It is called the *equivalence class of x with respect to the relation R*.

Clearly, $x \in [x]$ so every element of S is in some equivalence class.

Example

For the relation $x \equiv y \pmod 3$, we have three different equivalence classes: $[0] = \{3k : k \in \mathbb{Z}\}$, $[1] = \{3k + 1 : k \in \mathbb{Z}\}$ and $[2] = \{3k + 2 : k \in \mathbb{Z}\}$. Since every integer can be written uniquely as $3k + r$ with $r \in \{0, 1, 2\}$, we conclude that $\mathbb{Z} = [0] \cup [1] \cup [2]$.

Theorem (Fundamental property of equivalence relations)

Let S be a set and R be an equivalence relation on S. Then equivalence classes with respect to R provide a partition of S, that is, S is the union of equivalence classes and two equivalence classes are either equal or have empty intersection.

Remark

The converse is also true: every partition of a set S gives rise to an equivalence relation.

Proof.

Since R is reflexive, $x \in [x]$ and so S is the union of equivalence classes of R.
Suppose that $[x]$, $[y]$ are equivalence classes. If $z \in [x] \cap [y]$ for some $z \in S$ then $z \in [x]$ and $z \in [y]$. But then xRz and zRy which by transitivity of R means that xRy and so $x \in [y]$ and $y \in [x]$.
Now, since $x \in [y]$ we have $[x] \subset [y]$. Indeed, if $t \in [x]$ then tRx; but, since $x \in [y]$, xRy and so by transitivity tRy that is, $t \in [y]$. Likewise, $y \in [x] \implies [y] \subset [x]$. Therefore, if $[x] \cap [y] \neq \emptyset$ then $[x] = [y]$. $\square$

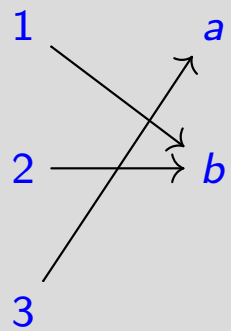
Maps

Definition

Let A and B be non-empty sets. We say that we are given a *map* (or a *function*) f from A to B and write $f : A \to B$ if for each $a \in A$ we are given a *unique* $b = f(a) \in B$.
The set A is called the *domain* of f and B is called the *codomain* of f.
If $f(a) = b$ then b is the *image* of a or the *value* of f at a and a is a *preimage* of b.
The set $\{b \in B : b = f(a) \text{ for some } a \in A\}$ is called the *image* of f or the *range* of f and is denoted by $f(A)$ or $\operatorname{im} f$.
If X is a subset of B, we denote $f^{-1}(X) = \{a \in A : f(a) \in X\}$.
In particular, for any $b \in B$, $f^{-1}(\{b\}) = \{a \in A : f(a) = b\}$.

Example

- The assignment $x \mapsto x+1$ defines a map $f : \mathbb{Z} \to \mathbb{Z}$ with $f(x) = x+1$. We have $\operatorname{im} f = \mathbb{Z}$ and each $y \in \mathbb{Z}$ has a unique preimage, namely $y-1$.
- The assignment $x \mapsto x^2$ defines a map $f : \mathbb{Z} \to \mathbb{N}$ with $f(x) = x^2$. The image of f is the set of *perfect squares*. For example, $4, 9 \in \operatorname{im} f$ and $3, 5 \notin \operatorname{im} f$. If $m \in \operatorname{im} f$ and $m \neq 0$ then m has two preimages.
- The same assignment as in the previous example defines a map $f : \mathbb{R} \to \mathbb{R}$. Now $\operatorname{im} f$ is the set of all non-negative real numbers.
- Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$. The following diagram represents a map $f : A \to B$



Here b has two preimages (1 and 2) and a has one preimage (3).

- Given a set S, there is a always a map $\mathrm{id}_S : S \to S$ which sends every element of S to itself. This is called the *identity* map.
- We can also define a map from any set S to the singleton set $\{\emptyset\}$ by $s \mapsto \emptyset$ for all $s \in S$.
- Given a set S and an element $s \in S$ we can define a map $\{\emptyset\} \to S$ by $\emptyset \mapsto s$.
- If X is a non-empty subset of A and $f : A \to B$ is a map then we can *restrict* f to X and thus obtain a map $g : X \to B$ where $g(x) = f(x)$ for all $x \in X$. The standard notation is $g = f|_X$.
- Let $f : A \to B$ be a map. If Y is any set such that $\mathrm{im}\, f \subset Y$ (in particular, Y can be a subset of B or any set containing B) then we can regard f as a map $f : A \to Y$. Note, however, that this is a different map since the target set is different.
- Let $f, g : A \to B$ be maps. We say that $f = g$ if for all $a \in A$, $f(a) = g(a)$.

Injective, surjective and bijective maps

Definition

Let A, B be non-empty sets and $f : A \to B$ be a map.
We say that f is *injective* or *one-to-one* if for all $a, a' \in A$, $f(a) = f(a')$ implies that $a = a'$.
We say that f is *surjective* or *onto* if for all $b \in B$ there is $a \in A$ such that $f(a) = b$. That is, $\operatorname{im} f = B$ or every $b \in B$ has a preimage with respect to f.
A map which is both injective and surjective is called *bijective*, or a *bijection* or a *bijective correspondance*

Example

- The map $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x + 1$ is bijective.
- The map $f : \mathbb{Z} \to \mathbb{N}$, $x \mapsto x^2$ is neither injective nor surjective
- The map $f : \mathbb{R} \to \mathbb{R}^+$, $x \mapsto x^2$ where $\mathbb{R}^+$ is the set of non-negative real numbers is surjective but not injective.
- The map from our last example was surjective but not injective too.
- The map $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto 2n + 1$ is injective but not surjective. Indeed, if $f(n) = f(n')$ then $2n + 1 = 2n' + 1$. This implies that $2n = 2n'$ and so $n = n'$. However, $2 \notin \operatorname{im} f$
- Let A and B be sets. Define $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$ by $\pi_A((a, b)) = a$ and $\pi_B((a, b)) = b$ for all $a \in A$, $b \in B$. These maps are called *standard projections*. They are clearly surjective but contains precisely one element, are not injective. Indeed, if $b \neq b' \in B$ then $\pi_A((a, b)) = \pi_A((a, b')) = a$ for all $a \in A$.

Example

- Let S be the set of students in some course, let $G = \{A+, A, A-, B+, B, B-, C+, C, D, F\}$. Then we can define a map $f : S \to G$ which assigns to each student his or her grade. This map is most likely not to be injective (since more than one student can obtain the same grade) and does not have to be surjective either
- Let A be the set of all bit strings of length 4 (that is, $\{0,1\}^4$), $B = \mathbb{N}$. Then we can define a map $f : A \to B$ which turns a bit string into an integer:

$$(a_3, a_2, a_1, a_0) \mapsto a_0 + a_1 \cdot 2 + a_2 \cdot 4 + a_3 \cdot 8$$

For example, $0110 \mapsto 6$, $1001 \mapsto 9$ etc. This map is easily seen to be injective. Its image is the set of all integers between 0 and 15 (inclusive).
If $B = \{0, 1, 2, \ldots, 15\}$ we can define a map $g : B \to A$ which maps n to its binary representation. Then g is bijective

Example

- Let A be as in the previous example and let $S = \{1, 2, 3, 4\}$. Let B be the *set of all subsets of* S. Then we define a map $f : B \to A$ by $f(X) = (a_1, a_2, a_3, a_4)$ where $a_i = 1$ if $i \in X$ and $a_i = 0$ otherwise. For example, if $X = \{1, 3\}$ then $f(X) = (1, 0, 1, 0)$ and if $X = \{2, 3, 4\}$ then $f(X) = (0, 1, 1, 1)$.
  We can also define $g : A \to B$ as the map which sents (a_1, a_2, a_3, a_4) to $\{i \in \{1, 2, 3, 4\} : a_i = 1\}$. For example, $g((1, 0, 1, 1)) = \{1, 3, 4\}$ and $g((0, 1, 1, 0)) = \{2, 3\}$.

How to check that f is injective/surjective?

- To check that $f : A \to B$ is injective we either show that $f(a) = f(a')$ implies that $a = a'$, or that $a \neq a'$ implies that $f(a) \neq f(a')$ (which is the contrapositive of the previous statement)
- To show that $f : A \to B$ is not injective it is enough to find a pair $a \neq a'$ such that $f(a) = f(a')$.
- To show that $f : A \to B$ is surjective for each $b \in B$ we need to find $a \in A$ such that $f(a) = b$
- To show that $f : A \to B$ is not surjective it is enough to find $b \in B$ such that $b \notin \operatorname{im} f$.

Example

Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $f(m, n) = m + n + 1$.

Question

Is f injective?

No. Indeed, $f(0, 1) = f(1, 0) = 2$ and $(0, 1) \neq (1, 0)$ in $\mathbb{Z} \times \mathbb{Z}$ as a matter of fact, $f(t, m - t) = f(t', m - t')$ for all $m, t, t' \in \mathbb{Z}$.

Question

Is f surjective?

Yes. If $x \in \mathbb{Z}$ then $x = f(x, -1)$ which means that $x \in \operatorname{im} f$ for all $x \in \mathbb{Z}$.

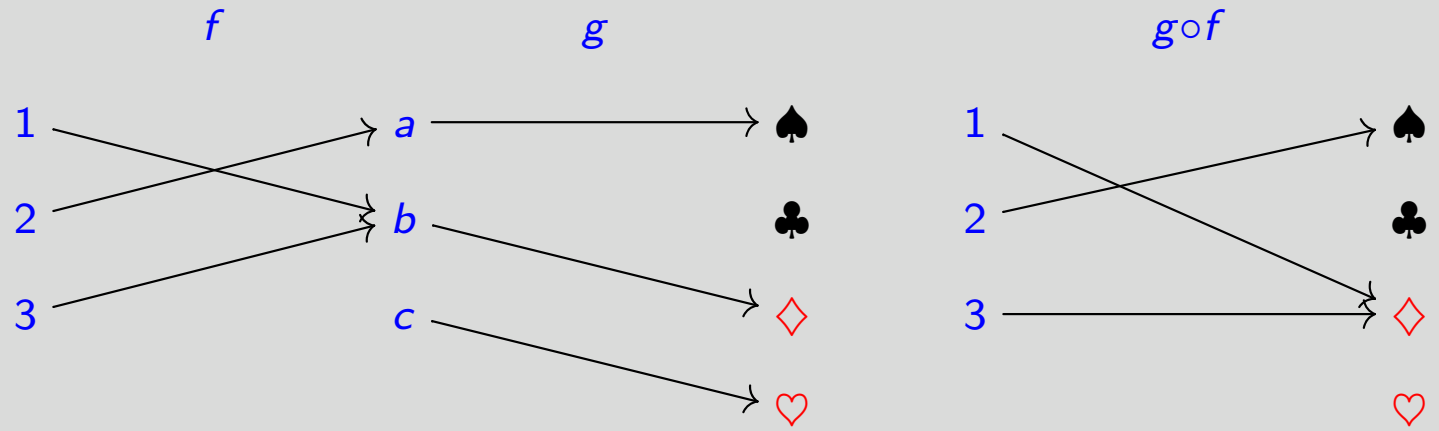
Composition of maps

Definition

Let $f : A \to B$ and let $g : B \to C$. The *composition* $g \circ f$ of f and g is the map $A \to C$ defined by $(g \circ f)(a) = g(f(a))$.

Example

- Let $f : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x + 1$, $g : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x^2$. Then $g \circ f : \mathbb{Z} \to \mathbb{Z}$ is defined by $x \mapsto (x + 1)^2$.
  We can also consider $f \circ g : \mathbb{Z} \to \mathbb{Z}$ which is defined by $x \mapsto x^2 + 1$.
- Let $A = \{1, 2, 3\}$, $B = \{a, b, c\}$, $C = \{\spadesuit, \clubsuit, \diamondsuit, \heartsuit\}$.



Theorem

Let A, B be sets and let $f : A \to B$ be a map. Then $\mathrm{id}_B \circ f = f$ and $f \circ \mathrm{id}_A = f$.

Theorem

Composition of maps is associative. That is, if A, B, C, D are sets and $f : A \to B$, $g : B \to C$ and $h : C \to D$ are maps then $(h \circ g) \circ f = h \circ (g \circ f)$ as maps $A \to D$.

Composition of maps *IS NOT* commutative. In fact, if $A \neq C$ then for $f : A \to B$ and $g : B \to C$ $g \circ f$ is defined but $f \circ g$ is not defined. Even if both are defined (in one of our examples we had $A = B = C$), the resulting maps can be different.

Composition and injectivity/surjectivity

Theorem

Let A, B and C be non-empty sets and let $f : A \to B$, $g : B \to C$ be maps.

(a) *If $g \circ f$ is injective then f is injective*

(b) *If $g \circ f$ is surjective then g is surjective.*

(c) *If $g \circ f$ is bijective then f is injective and g is surjective.*

(d) *If f and g are injective then so is $g \circ f$*

(e) *If f and g are surjective then so is $g \circ f$*

(f) *If f and g are bijective then so is $g \circ f$.*

Proof.

To prove (a), suppose that $f(a) = f(a')$, $a, a' \in A$. Then $g(f(a)) = g(f(a'))$ and so $(g \circ f)(a) = (g \circ f)(a')$. Since $g \circ f$ is injective this forces $a = a'$.

To prove (b), let $c \in C$. Since $g \circ f$ is surjective, there exists $a \in A$ such that $(g \circ f)(a) = c$. But this means that $c = g(f(a)) = g(b)$ where $b = f(a) \in B$. Thus, $c \in \operatorname{im} g$.

Part (c) follows from parts (a) and (b)

To prove (d), let $a, a' \in A$ be such that $(g \circ f)(a) = (g \circ f)(a')$. This means that $g(f(a)) = g(f(a'))$. Since g is injective, this forces $f(a) = f(a')$. Since f is injective, this implies that $a = a'$. Thus, we proved that $(g \circ f)(a) = (g \circ f)(a') \implies a = a'$, that is, $g \circ f$ is injective.

To prove (e), let $c \in C$. Since g is surjective, $c = g(b)$ for some $b \in B$. Since f is surjective, $b = f(a)$ for some $a \in A$. Then $c = g(f(a)) = (g \circ f)(a)$. We proved that $c \in \operatorname{im}(g \circ f)$. Since c was arbitrary, this shows that $C = \operatorname{im}(g \circ f)$, that is $g \circ f$ is surjective.

Last statement follows from (d) and (e). □

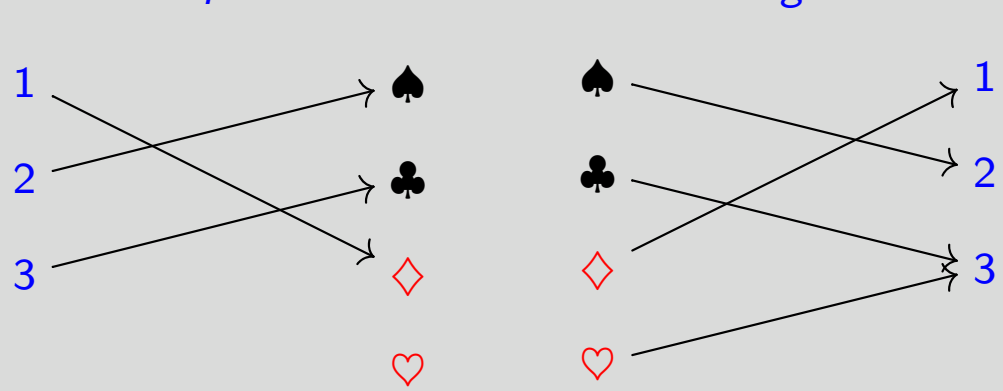
Inverse maps

Definition

Let A, B be non-empty sets and $f : A \to B$, $g : B \to A$ be maps. Note that in this case both $g \circ f$ and $f \circ g$ are defined.
We say that g is a *left inverse* of f if $g \circ f = \mathrm{id}_A$.
We say that g is a *right inverse* of f if $f \circ g = \mathrm{id}_B$.
We say that g is an *inverse* of f if g is a left and a right inverse of f.

Example

Let $A = \{1, 2, 3\}$, $B = \{\spadesuit, \clubsuit, \diamondsuit, \heartsuit\}$.



$g \circ f = \mathrm{id}_A$;
but $f \circ g \neq \mathrm{id}_B$,
since $(f \circ g)(\heartsuit) = \clubsuit$.

Example

- Let A, B be sets. Recall the map $\pi_A : A \times B \to A$, $(a, b) \mapsto a$. Fix $b \in B$ and define $\iota_b : A \to A \times B$ by $\iota_b(a) = (a, b)$. Then we have $\pi_A \circ \iota_b = \mathrm{id}_A$. Thus, π_A is a left inverse of ι_b and ι_b is a right inverse of π_A. This example shows that a left or a right inverse does not have to be unique
- Many examples of inverse maps are studied in calculus. For instance, if A is the set of non-negative real numbers, the inverse map of $f : A \to A$, $x \mapsto x^2$ is called the square root map.

Lemma

Let $f : A \to B$ be a map. If $g : B \to A$ is a left inverse of f and $h : B \to A$ is a right inverse of f then $g = h$.

Proof.

We have $(g \circ f) \circ h = g \circ (f \circ h)$ as maps $B \to A$ since the composition of maps is associative.
Since h is a right inverse of f, $f \circ h = \mathrm{id}_A$ and so $g \circ (f \circ h) = g \circ \mathrm{id}_A = g$.
Since g is a left inverse of f, $g \circ f = \mathrm{id}_B$ and so $(g \circ f) \circ h = \mathrm{id}_B \circ h = h$.
Thus,

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

We proved that $h = g$. □

Corollary

(a) *$f : A \to B$ has an inverse if and only if f has both a left and a right inverse.*

(b) *If f has an inverse then it is unique*

Proof.

If f has an inverse g then g is both a left and a right inverse of f by definition, so there is nothing to do there.
Suppose that $g : B \to A$ is a left inverse of f and $h : B \to A$ is a right inverse of f. Then, by the Lemma, $g = h$ and so f has an inverse.
To prove (b), suppose that f has inverses $g, h : B \to A$. In particular, g is a left inverse of f and h is its right inverse. Then $g = h$ by the Lemma. □

Theorem

Let A, B be non-empty sets and let $f : A \to B$ be a map.

(a) *f has a left inverse if and only if f is injective*

(b) *f has a right inverse if and only if f is surjective*

(c) *f has the inverse if and only if f is bijective*

Thanks to the Corollary on slide 31, we say "the inverse" now, since we know that if f has an inverse at all then it has precisely one.

Proof: (a)

($\Longrightarrow$) If f is a left inverse g, then $g \circ f = \mathrm{id}_A$ is an injective map and so f is injective by part (a) of Theorem on slide 26.
($\Longleftarrow$) Conversely, if f is injective, for every $b \in \operatorname{im} f$ there exists a unique $a_b \in A$ such that $f(a_b) = b$. Fix $a_0 \in A$ and define $g : B \to A$ by

$$g(b) = \begin{cases} a_b, & b \in \operatorname{im} f \\ a_0, & b \notin \operatorname{im} f. \end{cases}$$

Since $a_b = a$ if $b = f(a)$ we have $(g \circ f)(a) = g(f(a)) = a$ for all $a \in A$. Thus, g is a left inverse of f.

This argument shows why a left inverse does not have to be unique: if $\operatorname{im} f \neq B$ we obtain a different left inverse by choosing a different a_0.

Proof: (b) and (c)

($\Longrightarrow$) If f has a right inverse g then $f \circ g = \mathrm{id}_B$ is a surjective map and so f is surjective by part (b) of Theorem on slide 26.

($\Longleftarrow$) Since f is surjective, $\mathrm{im}\, f = B$. Thus, for each $b \in B$ we can choose $a_b \in A$ such that $f(a_b) = b$. Note that this choice is not unique. Define $g : B \to A$ by $g(b) = a_b$. Then $(f \circ g)(b) = f(a_b) = b$ for all $b \in B$. Thus, g is a right inverse of f.

To prove (c), note that f is bijective if and only if it is both injective and surjective. By parts (a) and (b) this happens if and only if f has a left inverse and a right inverse. But by Corollary on slide 31, f has both left and right inverse if and only if it has the inverse.

Example

Let B be the set of all subsets of $S = \{1, 2, 3, 4\}$ and let $A = \{0, 1\}^4$.
Define $f : B \to A$ by $X \mapsto (a_1, a_2, a_3, a_4)$, where $a_i = 1$ if $i \in X$ and $a_i = 0$ if $i \notin X$.
For example, if $X = \{1, 3\}$ then $f(X) = (1, 0, 1, 0)$ and if $X = \{1, 2, 4\}$ then $f(X) = (1, 0, 1, 1)$.
Define $g : A \to B$ by $(a_1, a_2, a_3, a_4) \mapsto \{1 \leq i \leq 4 \ : \ a_i = 1\}$.
For example, $g(1, 1, 0, 1) = \{1, 2, 4\}$; $g(0, 0, 0, 0) = \emptyset$ and $g(1, 1, 1, 1) = \{1, 2, 3, 4\}$
Then $f \circ g = \mathrm{id}_A$ and $g \circ f = \mathrm{id}_B$. This shows that both f and g are bijective.