1 Relations

Definition

A **relation** on a set X is a property of an ordered pair of elements of X which can be true or false.

Example: $<$ is a relation on the set of natural numbers: if a and b are natural numbers then $a < b$ is either true or false.

Definition

Properties of relations: Let $\sim$ be a relation on a set X.

- $\sim$ is called **symmetric** if for any $x, y \in X$ if $x \sim y$ then $y \sim x$.
- $\sim$ is called **reflexive** if for any $x \in X$ we have $x \sim x$.
- $\sim$ is called **transitive** if for any $x, y, z \in X$ if $x \sim y$ and $y \sim z$ then $x \sim z$.
- $\sim$ is called an **equivalence relation** if it is reflexive, symmetric and transitive.

Definition

Let $\sim$ be an equivalence relation on a set X, and let $x \in X$. The **equivalence class** of x, written $[x]$ or $[x]_\sim$, is

$$[x] = \{y \in X | y \sim x\}$$

Theorem

Let $\sim$ be an equivalence relation on a set X. Then

- Every $x \in X$ belongs to some equivalence class.
- If two equivalence classes classes are not disjoint, then they are equal.

2 Functions

Definition

Let $f : X \to Y$ be a function. The set X is called the domain of f. The set Y is called the co-domain of f.

Definition

Let $f : X \to Y$ be a function.

- f is called **injective** or **one-to-one** if for all $a, b \in X$, if $f(a) = f(b)$ then $a = b$.
- The **image** of f, written $\operatorname{im} f$, is $\{f(x) : x \in X\}$.
- f is called **surjective** or **onto** if $\operatorname{im} f = Y$.
- f is called a **bijection** if it is injective and surjective.

Definition

Let $f : X \to Y$ and $g : Y \to Z$ be functions. The **composition** of g and f, written $g \circ f$, is the function $g \circ f : X \to Z$ such that $(g \circ f)(x) = g(f(x))$.

NB: Composition only makes sense when the co-domain of f is the same as the domain of g.

Theorem

Function composition is associative.

If $f : X \to Y, g : Y \to Z, h : Z \to W$, then

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

The reason this is true is because both sides send an input $x \in X$ to the output $h(g(f(x)))$.

Definition

The **identity function** id_X does nothing: it is defined by $\mathrm{id}_X(x) = x$ for all $x \in X$.

Definition

Let $f : X \to Y$ and $g : Y \to X$ be functions. Then

- g is a **left inverse** to f, and f is a **right inverse** to g, if $g \circ f = \mathrm{im}_x$.
- f is **invertible** if there is a function $h : Y \to X$ such that $f \circ h = \mathrm{id}_Y$ and $h \circ f = \mathrm{id}_X$.
- If f is invertible, then there is one and only one function which is a left and right inverse to f - its inverse f^{-1}.

Theorem

Let $f : X \to Y$ be a function.

- f has a left inverse if and only if it is injective.
- f has a right inverse if and only if it is surjective.
- f is invertible if and only if it is a bijection.

Theorem

If functions $f_1, f_2, \ldots, f_n$ are invertible and the composition $f_1 \circ f_2 \circ \cdots \circ f_n$ makes sense, then it is invertible with inverse $f_n^{-1} \circ f_{n-1}^{-1} \circ \cdots \circ f_1^{-1}$.

3 Permutations

Definition

A **permutation** of a set X is a bijection from X to X.

For a set $X = \{1, 2, \ldots, n\}$, the set of all permutations on X is called the **symmetric group on n letters**, S_n.

Definition

If σ and τ are permutations, we will often write their **composition** $\sigma \circ \tau$ as $\sigma\tau$, and refer to it as the **product** of σ and τ.

3.1 Two-row notation

Definition

Given a permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

then on swapping the rows gives

$$\sigma^{-1} = \begin{pmatrix} 3 & 4 & 5 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

and rearranging gives the **inverse** permutation

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$

Theorem

$$\mid S_n \mid = n!$$

Proof: Induction on n.

When $n = 1$ there is a unique bijection $\{1\} \to \{1\}$, namely the identity map, so $\mid S_1 \mid = 1 = 1!$ as required.

The number of elements of S_n is the number of different ways to order the elements $1, 2, \ldots, n$. An ordering of $1, 2, \ldots, n$ is the same thing as an ordering of $1, 2, \ldots, n-1$ with n inserted into one of n positions, so the number of possible orderings is n times the number of orderings of $1, \ldots, n-1$, which is $(n-1)!$ by the inductive hypothesis.

So $\mid S_n \mid = x \times (n-1)! = n!$.

3.2 Cycles

Definition

Let $a_0, \ldots, a_{m-1}$ be distinct elements of $\{1, 2, \ldots, n\}$. Then $(a_0, \ldots, a_{m-1})$ is the permutation in S_n such that

- $a_i \mapsto a_{i+1}$ for $0 \leq i \leq m-1$, $a_{m-1} \mapsto a_0$,
- and if $x \neq a_1, \ldots, a_m$ then $x \mapsto x$.

Such a permutation is called an m-**cycle**.

Definition

A permutation which is an m-cycle for some m is called a cycle.

Counter-example: Not every permutation is a cycle, e.g. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

Definition

Two cycles $(a_0, \ldots, a_{m-1})$ and $(b_0, \ldots, b_{m-1})$ are **disjoint** if no a_i is equal to any b_j.

Any permutation can be written as a product of disjoint cycles, e.g. the permutation above is equal to $(1, 2)(3, 4)$.

Definition — Theorem

Let $m \in \mathbb{Z}$ and $\sigma \in S_n$. Then

$$\sigma^m = \begin{cases} \sigma \circ \cdots \circ \sigma (m \text{ times}) & m > 0 \\ \text{id} & m = 0 \\ \sigma^{-1} \circ \cdots \circ \sigma^{-1} (-m \text{ times}) & m < 0 \end{cases}$$

and for any $a, b \in \mathbb{Z}$,

$$\sigma^a \sigma^b = \sigma^{a+b}$$

Definition — Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

Definition — Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

4 Groups

A group is a very simple mathematical object consisting of two things: (a) a **set** G and (b) a way of combining two elements of the set to produce another, called the **group operation**.

This group operation has to obey three rules mimicing those obeyed by the symmetries of a physical object called the group axioms.

Definition

A group $(G, *)$ is a set G with a binary operation $*$ which contains an element e such that

- (Identity axiom) For all $g \in G$, $e * g = g * e = g$.
- (Inverses axiom) For all $g \in G$, there exists $h \in G$ such that $h * g = g * h = e$.
- (Associativity axiom) For all $g, h, k \in G$, $(g*h)*k = g*(h*k)$.

A binary operation on G is a function that takes as input a pair of elements of G and outputs a single element of G: that is, a function $G \times G \to G$.

Examples:

- $+$ is a binary operation on the set of integers $\mathbb{Z}$.
- $-$ is a binary operation on the set of complex numbers $\mathbb{C}$.
- $-$ is **not** a binary operation on the set of strictly positive integers $\mathbb{N}$, because it doesn't always output an element of $\mathbb{N}$.
- $a * b = 2 \quad \forall \quad a, b \in \mathbb{R}$ is a binary operation on the real numbers $\mathbb{R}$.

Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

Definition — Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

4.1 The Symmetric Group

Definition — Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

4.2 Subgroups

Definition — Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

4.3 Cosets and Lagrange's Theorem

Definition — Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

4.4 The Dihedral Groups

Definition — Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

4.5 Homomorphisms and Isomorphisms

Definition — Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

5 Categories

Definition — Theorem

Description: Text

$$\mathbf{v} \cdot \mathbf{w} = 0 \iff \alpha = \frac{\pi}{2} \iff \mathbf{v} \perp \mathbf{w}$$

References

[1] Matthew Towers, UCL. *MATH0007: Algebra for Joint Honours Students*. 2020. URL: https://www.ucl.ac.uk/~ucahmto/0007/_book/.