0.1 Proving simple properties

Simply defining a category is not enough. We must prove that the definitions said category hold.

0.1.1 Example 1: composition of group homomorphisms

Given: $(G, \bullet), (G', \bullet'), (G'', \bullet'')$ and $G \xrightarrow{f} G' \xrightarrow{g} G''$

Prove: $\forall a, b \in G \,.\, (g \circ f)(a \bullet b) \overset{?}{=} (g \circ f)a \bullet (g \circ f)b$

$$\begin{aligned}(g \circ f)(a \bullet b) &= g(f(a \bullet b)) \\ &= g(f(a) \bullet' f(b))) \\ &= g(f(a)) \bullet'' g(f(b)) \\ &= (g \circ f)a \bullet'' (g \circ f)b\end{aligned}$$

0.1.2 Example 2: associativity of matrix multiplication

Given: $m \xrightarrow{A} n \xrightarrow{B} p \xrightarrow{C} l$ and $A \xrightarrow{R} B \xrightarrow{S} C \xrightarrow{T} D$

Prove: $(R; S); T \overset{?}{=} R; (S; T)$

(a note on notation: $(matrix_{row}^{col} \mid {}^{row<m}_{col<n}))$

We know $(a_i^j \mid {}^{i<m}_{j<n})\ (b_j^k \mid {}^{j<n}_{k<p}) = (\sum_{j<n} a_i^j b_j^k \mid {}^{i<m}_{k<p})$

For any row i and column j, the (i, j)th entry of $(R; S); T$ is:

$$\begin{aligned}(R; S); T &= (\sum_{j<n} a_i^j b_j^k)(T) \\ &= \sum_{k<p}(\sum_{j<n} a_i^j b_j^k)(c_k^q) \\ &= \sum_{k<p}\sum_{j<n} a_i^j b_j^k c_k^q \\ &= \ldots \quad \text{(form is symmetrical at this point)}\end{aligned}$$

0.2 The category which is the product of two categories

The category the product of categories $C \times D$ consists of:

- An object (X, Y) such that $X \in C, Y \in D$
- The morphism $(X, Y) \to (W, Z) = (f, g)$ where

$$f : X \to W \in C$$
$$g : Y \to Z \in D$$

- The identity morphism $id_{(X,Y)} = (id_X, id_Y)$
- The composite $(X,Y) \xrightarrow{(f,g)} (W,Z) \xrightarrow{(h,k)} (U,V) = (f;k, g;k)$

0.3 The opposite (dual) category

The dual category of C is C^{op}, and consists of:

- All objects $X \in C$
- Morphisms $X \to Y \in C^{op}$ are morphisms $Y \to X \in C$
- The identity morphism $id_X : X \to X \in C^{op}$ is the morphism $id_X \in C$
- Compositions $X \underset{X,Y,Z}{;} Z \in C^{op}$ are compositions $Z \underset{Z,Y,X}{;} X \in C$

0.4 Isomorphisms

0.4.1 The inverse morphism

The inverse of $f : A \to B$ is $g : B \to A$ such that:

f ; g = id_A and g ; f = id_B

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "id_A"'] & B \arrow[d, "g"] \\
& A
\end{tikzcd}
\qquad
\begin{tikzcd}
B \arrow[r, "g"] \arrow[dr, "id_B"'] & A \arrow[d, "f"] \\
& B
\end{tikzcd}$$

(Theorem) if f has inverses g and g', then $g = g'$

0.4.2 Isomorphisms

An isomorphism is a morphism with an inverse. If f is an isomorphism, then $f : A \cong B$

For example:

- In **Set**, all bijections are isomorphisms
- In **Mat**, all non-singular matrices are isomorphisms

- In the category of towns, all identities id_X are isomorphisms, but no other morphism is an isomorphism. This is because identity routes are single item lists, and composing two routes (concatenating routes) can never be done in a way such that the length of the resulting route decreases. i.e. there are no inverses.

  Given we need a composition that results in a route of length 1, no morphism other than single town routes (identity routes) will do.

0.5 Initial and terminal objects

An object $X \in C$ is **initial** when for all $Y \in C$ there is a unique function $X \to Y$. i.e. $\forall Y \in C \,.\, \exists! f : X \to Y$

An object $X \in C$ is **terminal** when for all $Y \in C$ there is a unique function $Y \to X$. i.e. $\forall Y \in C \,.\, \exists! f : Y \to X$

For example, in **Set**:

- There is exactly one initial object, which is the **empty set**. This is because there is only one function from the empty set to any other set, the **empty function**, $f_A : \varnothing \to A$.
- Every singleton set is a terminal object. This is because there is a unique function $f_1 : A \to 1$ where $1 = ()$ for any set A. We know this because there is only a single item in 1 which elements in any set can map to.

Note that there can be a function with an **empty domain**, but there cannot be a function with **non-empty domain** and **empty co-domain** since there wouldn't be anything to map to from the domain. The standard set-theoretic way to define functions explains this:

1. **Cartesian product** : $A \times B = \{(a, b) \mid a \in A, b \in B\}$

   The product is a set of ordered pairs.
2. **Relation** : $R \subset A \times B$ where R is a relation between sets A and B, often written as $a\,R\,b$
3. **Function** : $f : A \to B$ is a relation such that:
   - **there exist images** : $\forall a \in A \,.\, \exists b \in B \,.\, (a, b) \in f$

     This is different to **surjectivity**, which states that everything in B is an image. This condition requires the existence of images. Surjectivity is vacously true for empty sets.
   - **images are unique** : $\forall a \in A \,.\, (a, b) \in f \wedge (a, b') \in f \Rightarrow b = b'$.

Since the only subset of $\varnothing$ is $\varnothing$, the only relation between A and B (where one of them is $\varnothing$) is $\varnothing$. Thus, the question is whether the empty relation ($\varnothing$) is a function from A to B:

- $A \neq \varnothing$: no, since there exists an $a \in A$ but no $b \in B$ such that $(a, b) \in \varnothing$, the image existence condition is not matched.

- $A = \varnothing$: yes, both existence and uniqueness conditions are vacuously true. i.e. there is no $a \in A$ to disprove the universals.

Note that the conditions state that functions must define a unique output (image) for every input (preimage). This is vacuously true on the input, since there is no input.

Also note that in many languages (such as Java, C, OCaml) there might not be function definition for the signature $\varnothing \to T$. A program without input is a function from the unit set ($1 = \{()\}$). Therefore, function $f : \varnothing \to T$ cannot be defined, but is still a function.

0.6 Exercises

0.6.1 Theorem : every inverse morphism is unique

If $g, g' : D \to C$ are two inverses for $f : C \to D$, then $g = g'$

i.e. $\quad (g \circ f = id_C \wedge f \circ g = id_D) \wedge (g' \circ f = id_C \wedge f \circ g' = id_D) \Rightarrow g = g'$

Proof:

$$\begin{aligned} g &= id_C \circ g \\ &= (g' \circ f) \circ g \\ &= g' \circ (f \circ g) \\ &= g' \circ id_D \\ &= g' \end{aligned}$$

Alternatively:

$$\begin{aligned} g &= g; id_C \\ &= g; (f; g') \\ &= (g; f); g' \\ &= id_D; g' \\ &= g' \end{aligned}$$

0.6.2 Theorem: initial objects have unique isomorphisms between them

If $X, X' \in C$ are initial, there is a unique isomorphism $X \cong X'$

Proof: Given $f : X \to X'$ and $g : X' \to X$

$X \xrightarrow{f} X'$ is a unique morphism because X is initial

$X' \xrightarrow{g} X$ is a unique morphism because X' is initial

$X \xrightarrow{g \circ f} X$ is unique because X is initial, so any morphism from X is unique

$f;g = id_X$ because identity on X must exist, and $f;g$ is unique

$g;f = id_{X'}$ because identity on X' must exist, and $g;f$ is unique

$\therefore g$ and f are inverses

$\therefore X \cong X'$ is a unique isomorphism since f and g are unique

$\therefore X$ and X' are **unique up to isomorphism**.

i.e.

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[dr, "id_X"'] & X' \arrow[d, "g"] \arrow[dr, "id_{X'}"] & \\
& X \arrow[r, "f"] & X'
\end{tikzcd}$$

each morphism is unique, meaning $f;g = id_X$

If objects are **unique up to isomorphism**, they are the same object with different names for things. More formally, all the objects satisfying a given definition are isomorphic.

0.6.3 Theorem: terminal objects have unique isomorphisms between them

If $X, X' \in C$ are terminal, there is a unique isomorphism $X \cong X'$

The proof would have the same structure as the equivalent theorem for initial objects. Only difference would be that the unique morphisms defined are the other way round.

0.6.4 Initial and terminal objects in the category of groups, Grp

(Initial object)

The trivial group $(1, *) = \{e\}$ (group consisting of only the identity element) is an initial object of **Grp**.

First prove $\forall G \in \mathbf{Grp} \; . \; \exists! \; 1 \to G$:

Given group $(G, \bullet)$ with identity e_G, we can define a function f

$f(e) = e_G$ because all group homomorphisms preserve identity

$\forall G \in \mathbf{Grp} \; . \; \exists! \; 1 \to G$ because the morphism defined by f that maps e to e_G is unique

Then prove $\forall G \in \mathbf{Grp} \; . \; 1 \to G$ is a valid morphism:

Show that $f(a) \bullet f(b) = f(a * b)$

$$\begin{aligned} f(e) \bullet f(e) &= e_G \bullet e_G && \text{by definition of } f \\ &= e_G && \text{by definition of the identity element} \\ &= f(e) \\ &= f(e * e) \end{aligned}$$

(Terminal object)

The trivial group $(1, *)$ is also a terminal object in **Grp**.

First, by same argument that makes 1 initial, we show that $\forall G \in \mathbf{Grp} \,.\, \exists!\ G \to 1$. The mapping is defined by

$$\forall g \in G \,.\, f(g) = e$$

Then, we verify that $G \to 1$ is a valid group homomorphism:

Show that $\forall a, b \in G \,.\, f(a) * f(b) = f(a \bullet b)$:

Given $a \bullet b = c$

$$\begin{aligned} f(a) * f(b) &= e * e && \text{by definition of } f \\ &= e && \text{by definition of the identity element and } * \\ &= f(c) && \text{by definition of } f\text{, we know } f(c) = e \\ &= f(a \bullet b) && \text{because } a \bullet b = c \end{aligned}$$