West Coast
May 2, 2025

Algebra: Chapter 0

By Paolo Aluffi

Contents

Notations

Chapter I. Preliminaries: Set theory and categories

§1. Naive Set Theory

1.1 Locate a discussion of Russel's paradox, and understand it.

Naive set theory assumes the so-called naive or unrestricted comprehension principle: For any formula $\phi(x)$ containing x as a free variable, there will exist the set $\{x : \phi(x)\}$ whose members are exactly those objects that satisfy $\phi(x)$. Let's assume $\phi(x)$ be $x \notin x$ and $R = \{x : x \notin x\}$. Is R a member of itself?. If $R \notin R$, then the condition is satisfied. It implies $R \in R$. This is a contradiction. On the other hand, if $R \in R$, then R must satisfy the condition, i.e. $R \notin R$. This is also a contradiction. ∎

1.2 ▷ Prove that if $\sim$ is an equivalence relation on a set S, then the corresponding family $\mathscr{P}_\sim$ defined in §1.5 is indeed a partition of S; that is, its elements are nonempty, disjoint, and their union is S. [§1.5]

By the reflexivity, $\forall a \in S$, $a \in [a]_\sim$. So

$$\bigcup_{[v]_\sim \in \mathscr{P}_\sim} [v]_\sim = S.$$

Suppose $c \in [a]_\sim \cap [b]_\sim$, then $a \sim c, c \sim b$. By transitivity, $a \sim b$. $\forall x \in [b]_\sim$, $b \sim x$. By transitivity again, $a \sim x$. It implies $[b]_\sim \subset [a]_\sim$. Similarly, $[a]_\sim \subset [b]_\sim$ holds too. Therefore,

$$\text{if } [a]_\sim \cap [b]_\sim \neq \emptyset \Rightarrow [a]_\sim = [b]_\sim.$$

It proves that $\mathscr{P}_\sim$ is a partition of S. ∎

1.3 ▷ Given a partition $\mathscr{P}$ on a set S, show how to define an equivalence relation $\sim$ such that $\mathscr{P} = \mathscr{P}_\sim$. [§1.5]

Define a relation $\sim$ on S as

$$a \sim b \iff \exists A \in \mathscr{P}, \text{ such that } a \in A, b \in A.$$

It is easy to prove this relation is an equivalence on S. ∎

1.4 How many different equivalence relations can be defined on the set $\{1, 2, 3\}$?

The number of equivalence relations is the same as the number of partitions. All possible partitions of $\{1, 2, 3\}$ are:

$$\{\{1\}, \{2\}, \{3\}\},$$
$$\{\{1\}, \{2, 3\}\},$$
$$\{\{1, 2\}, \{3\}\},$$
$$\{\{1, 3\}, \{2\}\},$$
$$\{\{1, 2, 3\}\}.$$

So, there are 5 equivalence relations on $\{1, 2, 3\}$. ∎

1.5 Give an example of a relation that is reflexive and symmetric but not transitive. What happens if you attempt to use this relation to define a partition on the set? (Hint: Thinking about the second question will help you answer the first one.)

A relation R on set $\{1, 2, 3\}$ is a subset of $\{1, 2, 3\} \times \{1, 2, 3\}$. Taking subset

$$\{\{1, 1\}, \{2, 2\}, \{3, 3\}, \{1, 2\}, \{2, 1\}, \{1, 3\}, \{3, 1\}\}$$

It is easy to verify that R is reflexive and symmetric. $1R2, 1R3$, but 2 and 3 are not related by R because neither$\{2, 3\}$ nor $\{3, 2\}$ is in R. Thus, R is not transitive. ∎

1.6 ▷ Define a relation $\sim$ on the set $\mathbb{R}$ of real numbers, by setting $a \sim b \iff b - a \in \mathbb{Z}$. Prove that this is an equivalence relation, and find a 'compelling' description for $\mathbb{R}/\sim$. Do the same for the relation $\approx$ on the plane $\mathbb{R} \times \mathbb{R}$ defined by declaring $(a_1, a_2) \approx (b_1, b_2) \iff b_1 - a_1 \in \mathbb{Z}$ and $b_2 - a_2 \in \mathbb{Z}$. [§II.8.1, II.8.10]

(Reflexivity): $\forall a \in \mathbb{R}, a - a = 0 \in \mathbb{Z}$. It leads to the reflexivity.
(Symmetry): $\forall a, b \in \mathbb{R}$, if $a - b = k \in \mathbb{Z}$, then $b - a = -k \in \mathbb{Z}$. Thus, $\sim$ is symmetric.
(Transitivity): $\forall a, b, c \in \mathbb{R}$, if $a - b = k_1 \in \mathbb{Z}, b - c = k_2 \in \mathbb{Z}$, then $a - c = k_1 + k_2 \in \mathbb{Z}$. Therefore, $\sim$ is transitive.

$$\mathbb{R}/\sim \cong [0, 1).$$

The proof of $\approx$ being an equivalence relation $\mathbb{R} \times \mathbb{R}$ is similar to that of $\sim$. Thus, we omit it.

$$(\mathbb{R} \times \mathbb{R})/\approx \cong [0, 1) \times [0, 1).$$

∎

§2. Functions between sets

2.1 ▷ How many different bijections are there between a set S with n elements and itself? [§II.2.1]

The number of different bijections between S with n elements to itself is $n!$. ∎

2.2 ▷ Prove statement (2) in Proposition 2.1. You may assume that given a family of disjoint subsets of a set, there is a way to choose one element in each member of the family. [§2.5, V3.3]

($\Longrightarrow$): If $f : A \to B$ has right-inverse, then there is a function $g : B \to A$ such that $f \circ g = \mathrm{id}_B$. Thus

$$b = \mathrm{id}_B(b) = f \circ g(b) = f(g(b)), \forall b \in B,$$

that is, f sends $g(b) \in A$ to b, showing f is surjective.
($\Longleftarrow$): Now assume $f : A \to B$ is surjective. In order to construct a function $g : B \to A$, we have to assign a unique $g(b) = a \in A$ for all $b \in B$. Since the fiber $f^{-1}(b)$, $\forall b \in B$ is not empty, we can select one element $a \in f^{-1}(b)$ as the image of b under g. i.e.

$$g(b) = a, \text{ where } a \in f^{-1}(b).$$

For this g, we have $f \circ g(b) = f(a) = b = \mathrm{id}_B$. Thus g is a right-inverse of f. ∎

2.3 Prove that the inverse of a bijection is a bijection and that the composition of two bijections is a bijection.

If $f : A \to B$ is a bijection, then there exists $g : B \to A$ such that

$$f \circ g = \mathrm{id}_B, \qquad g \circ f = \mathrm{id}_A.$$

It implies f is a left-inverse and a right-inverse of g. Therefore g is a bijection.
If $f : A \to B$ and $g : B \to C$ are two bijections, then

$$f \circ f^{-1} = \mathrm{id}_B, \qquad f^{-1} \circ f = \mathrm{id}_A,$$

$$g \circ g^{-1} = \mathrm{id}_C, \qquad g^{-1} \circ g = \mathrm{id}_B.$$

Thus,

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = (g \circ \mathrm{id}_B) \circ g^{-1} = g \circ g^{-1} = \mathrm{id}_C,$$

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (\mathrm{id}_A \circ f) = f^{-1} \circ f = \mathrm{id}_A.$$

this means that $g \circ f$ has both left-inverse($f^{-1} \circ g^{-1}$) and right-inverse($f^{-1} \circ g^{-1}$). Therefore $g \circ f$ is a bijection. ∎

2.4 ▷ Prove that 'isomorphism' is an equivalence relation (on any set of sets). [§4.1]

Suppose S be a set of sets.
(Reflexivity): $\forall A \in S$, $A \cong A$ since $\mathrm{id}_A : A \to A$ is the bijection between A to itself.
(Symmetry): For $A \in S, B \in S$, if $A \cong B$, then there is a bijection $f : A \to B$. The inverse of f, denoted by f^{-1} is a bijection between B and A. This means $B \cong A$.
(Transitivity): For $A, B, C \in S$ satisfying $A \cong B, B \cong C$, there exist bijections $f : A \to B$ and $g : B \to C$. Composition of bijections is bijection, i.e. $g \circ f : A \to C$ is a bijection. It implies $A \cong C$. ∎

2.5 ▷ Formulate a notion of *epimorphism*, in the style of the notion of *monomorphism* seen in §2.6, and prove a result analogous to Proposition 2.3, for epimorphisms and surjections.[§2.6, §4.2]

A function $f : A \to B$ is an *epimorphism* if for all sets Z and all functions $\alpha', \alpha'' : B \to Z$

$$\alpha' \circ f = \alpha'' \circ f \Longrightarrow \alpha' = \alpha''.$$

Now, we prove: $f : A \to B$ is surjective if and only if f is epimorphism.

($\Longrightarrow$): If f is surjective, then it has a right-inverse g such that

$$f \circ g = \mathrm{id}_B.$$

For all functions $\alpha', \alpha'' : B \to Z$,

$$\alpha' \circ f = \alpha'' \circ f \Longrightarrow \alpha' \circ (f \circ g) = \alpha'' \circ (f \circ g) \Longrightarrow \alpha' \circ \mathrm{id}_B = \alpha'' \circ \mathrm{id}_B \Longrightarrow \alpha' = \alpha''.$$

($\Longleftarrow$): Let's take $Z = \{1, 2, 3\}$ and define

$$\alpha' = \begin{cases} 1, & b \in \mathrm{im} f, \\ 2, & b \notin \mathrm{im} f \end{cases}$$

$$\alpha'' = \begin{cases} 1, & b \in \mathrm{im} f, \\ 3, & b \notin \mathrm{im} f \end{cases}$$

It is obvious that $\alpha' \circ f = \alpha'' \circ f = 1$. Thus $\alpha' = \alpha''$. It means α' could not be 2 and α'' could not be 3. i.e. there isn't $b \notin \mathrm{im} f$. It proves that f is a surjection. ∎

2.6 With notation as in Example 2.4, explain how any function $f : A \to B$ determines a section of π_A.

The section of a surjection is a right-inverse of the function. Define a function $g : A \to A \times B$ as $g(a) = (a, f(a))$. It's easy to verify

$$\pi_A \circ g = \mathrm{id}_A.$$

It proves that $g : A \to A \times B$ is a right-inverse of $\pi : A \times B \to A$. ∎

2.7 Let $f : A \to B$ be any function. Prove that the graph Γ_f of f is isomorphic to A.

Denote $\Gamma_f = \{(a, f(a)) : a \in A\}$ and define $\pi_f : \Gamma_f \to A$ as

$$\pi_f((a, f(a))) = a.$$

Let's define another functon $g : A \to \Gamma_f$ as

$$g(a) = (a, f(a)).$$

So

$$(\pi_f \circ g)(a) = \pi_f(g(a)) = \pi_f((a, f(a))) = a \Rightarrow (\pi_f \circ g) = \mathrm{id}_A.$$

and

$$(g \circ \pi_f)((a, f(a))) = g(\pi_f((a, f(a)))) = g(a) = (a, f(a)) \Rightarrow (g \circ \pi_f) = \mathrm{id}_{\Gamma_f}.$$

This means $\pi_f : \Gamma_f \to A$ is a bijection. i.e. $\Gamma_f \cong A$. ∎

2.8 Describe as explicitly as you can all terms in the canonical decomposition (cf. §2.8) of the function $\mathbb{R} \to \mathbb{C}$ defined by $r \mapsto e^{2\pi i r}$. (This exercise matches one previously. Which one?)

Let $f : \mathbb{R} \to \mathbb{C}$ be $f(r) = e^{2\pi i r}$.

$$f(r_1) = f(r_2) \iff 1 - e^{2\pi i(r_2 - r_1)} = 0 \iff r_2 - r_1 \in \mathbb{Z}.$$

Denote the unit circle $\{e^{2\pi i r} | r \in \mathbb{R}\}$ on the complex plane as $\mathbb{C}_{|z|=1}$. Define an equivalence relation $\sim$ on $\mathbb{R}$ as $a \sim b \iff a - b \in \mathbb{Z}$ and a function $\tilde{f} : \mathbb{R}/\sim \to \mathbb{C}_{|z|=1}$ as

$$\tilde{f}([r]_\sim) := e^{2\pi i r}.$$

It is easy to verify that $\tilde{f}$ is well-defined and is a bijection and the following diagram holds

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{\quad f \quad} & \mathbb{C} \\ {\scriptstyle \pi}\downarrow & & \uparrow{\scriptstyle i} \\ \mathbb{R}/\sim & \xrightarrow[\quad \tilde{f} \quad]{} & \mathbb{C}_{|z|=1} \end{array}$$

where π is the natural projection, i is the inclusion. Therefore, $f = i \circ \tilde{f} \circ \pi$. ∎

2.9 ▷ Show that if $A' \cong A''$ and $B' \cong B''$, and further $A' \cap B' = \varnothing$ and $A'' \cap B'' = \varnothing$, then $A' \cup B' \cong A'' \cup B''$. Conclude that the operation $A \amalg B$ is well-defined up to *isomorphism* (cf. §2.9) [§2.9, 5.7]

Let $f_1 : A' \to A'', f_2 : B' \to B''$ be the bijections. Define

$$f(x) = \begin{cases} f_1(x), & x \in A', \\ f_2(x), & x \in B' \end{cases}$$

Since $A' \cap B' = \varnothing$, the function f is well-defined. Now, we prove that f is a bijection.

(Injection): For $x_1, x_2 \in A' \cup B'$ and $x_1 \neq x_2$, there are four cases:

1. if $x_1 \in A', x_2 \in A'$, then $f(x_1) = f_1(x_1) \neq f_1(x_2) = f(x_2)$.
2. if $x_1 \in B', x_2 \in B'$, then $f(x_1) = f_2(x_1) \neq f_2(x_2) = f(x_2)$.
3. if $x_1 \in A', x_2 \in B'$, then $f(x_1) = f_1(x_1) \in A''$, $f(x_2) = f_2(x_2) \in B$". Since $A'' \cap B'' = \varnothing$, $f(x_1) \neq f(x_2)$.
4. if $x_1 \in B', x_2 \in A'$, then $f(x_1) = f_2(x_1) \in B''$, $f(x_2) = f_1(x_2) \in A$". Since $A'' \cap B'' = \varnothing$, $f(x_1) \neq f(x_2)$.

It proves that f is an injection.

(Surjection): For $x \in A'' \cup B$", we have either $x \in A''$ or $x \in B$". Therefore there exists $a \in A'$ or $a \in B'$ such that $f(a) = f_1(a) = x$ or $f(a) = f_2(a) = x$.

The existence of a bijection between $A' \cup B'$ and $A'' \cup B''$ implies $A' \cup B' \cong A'' \cup B''$.

Let A', A'' be two 'copies' of A and B', B'' be two 'copies' of B. It is obvious that $A' \cong A''$ and $B' \cong B''$. Meanwhile, by the disjoin union, we know that $A' \cap B' = \varnothing$ and $A'' \cap B'' = \varnothing$. By the result of this problem, we have

$$A' \cup B' \cong A'' \cup B''.$$

It implies $A \coprod B$ is well-defined in term of isomorphism. ∎

2.10 ▷ Show that if A and B are finite sets, then $\left|B^A\right| = |B|^{|A|}$. [§2.1, 2.11, I.4.1]

By definition, $B^A = \{f | f : A \to B\}$. If both A and B are finite, then for each $x \in A$, it can be assigned $|B|$ different values. Therefore, the number of functions from A to B is $|B|^{|A|}$. i.e. $\left|B^A\right| = |B|^{|A|}$ ∎

2.11 ▷ In view of Exercise 2.10, it is not unreasonable to use 2^A to denote the set of functions from an arbitrary set A to a set with 2 elements (say $\{0, 1\}$). Prove that there is a bijection between 2^A and the *power set* of A (cf. §1.2). [§1.2, III.2.3]

Let $\mathcal{P}(A)$ be the power set of A. Define a mapping between $\mathcal{P}(A) \to 2^A$ as following:

$$f(X) = g, \text{ where } g(X) = 1, g(A \backslash X) = 0.$$

Let's prove this map is a bijection.

(Injection): For $X_1, X_2 \in \mathcal{P}(A), X_1 \neq X_2$, we have two functions

$$g_1\big|_{X_1} = 1, g_1\big|_{A\backslash X_1} = 0,$$

$$g_2\big|_{X_2} = 1, g_1\big|_{A\backslash X_2} = 0.$$

If $X_1\backslash X_2 \neq \varnothing$, then $g_1\big|_{X_1\backslash X_2} = 1 \neq 0 = g_2\big|_{X_1\backslash X_2}$. If $X_2\backslash X_1 \neq \varnothing$, then $g_1\big|_{X_2\backslash X_1} = 0 \neq 1 = g_2\big|_{X_2\backslash X_1}$. It proves that $g_1 \neq g_2$.

(Surjection): For a function $g : A \to \{0, 1\}$,

$$f(\{x | x \in A \text{ and } g(x) = 1\}) = g,$$

showing f is surjection. ∎

§3. Categories

3.1 ▷ Let C be a category. Consider a structure C^{op} with:

- $\mathrm{Obj}(\mathsf{C}^{op}) := \mathrm{Obj}(\mathsf{C})$;
- for A, B objects of C^{op} (hence, objects of C), $\mathrm{Hom}_{\mathsf{C}^{op}}(A, B) := \mathrm{Hom}_{\mathsf{C}}(B, A)$

Show how to make this into a category (that is, define composition of morphisms in C^{op} and verify the properties listed in §3.1). Intuitively, the 'opposite' category C^{op} is simply obtained by 'reversing all the arrows' in C. [5.1, §VIII.1.1, §IX.1.2, IX.1.10]

Let's define $*$ as the composition of morphisms between objects in C^{op} and $\circ$ as the composition of morphisms between objects in C.

1. For every object A of $\mathrm{Obj}(\mathsf{C}^{op})$, the identity $1_A \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, A)$ is the one in $\mathrm{Hom}_{\mathsf{C}}(A, A)$.
2. For $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B)$ and $g \in \mathrm{Hom}_{\mathsf{C}^{op}}(B, C)$. $g \circ f \in \mathrm{Hom}_{\mathsf{C}}(C, A)$. By definition, $g \circ f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, C)$. i.e. The composition

   $$(f, g) \mapsto f * g := g \circ f$$

   determines a morphism in $\mathrm{Hom}_{\mathsf{C}^{op}}(A, C)$.
3. For $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B)$, $g \in \mathrm{Hom}_{\mathsf{C}^{op}}(B, C)$ and $g \in \mathrm{Hom}_{\mathsf{C}^{op}}(C, D)$, then

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

   i.e. The composition laws is associative.

4. For $1_A \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, A)$, $1_B \in \mathrm{Hom}_{\mathsf{C}^{op}}(B, B)$ and $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B)$, we have

$$f * 1_A = 1_A \circ f = f, \text{ and } 1_B * f = f \circ 1_B = f.$$

i.e. The identity morphisms are identities with respect to composition.

It proves the structure C^{op} defined in this problem is a category. ∎

3.2 If A is a finite set, how large is $\mathrm{End}_{\mathsf{Set}}(A)$?

The set $\mathrm{End}_{\mathsf{Set}}(A)$ is the set of functions (as morphism) from A to A. Let $|A| = n$, then $|\mathrm{End}_{\mathsf{Set}}(A)| = n^n$. ∎

3.3 ▷ Formulate precisely what it means to say that 1_a is an identity with respect to composition in Example 3.3, and prove this assertion. [§3.2]

$1_a \in \mathrm{Hom}(a, a)$ tells us $a \sim a$, $1_b \in \mathrm{Hom}(b, b)$ tells us $b \sim b$. Let $f \in \mathrm{Hom}(a, b)$. It implies $a \sim b$.

$$a \sim a \text{ and } a \sim b \Longrightarrow a \sim b => f1_a = f,$$

$$a \sim b \text{ and } b \sim b \Longrightarrow a \sim b => 1_b f = f.$$

It proves that identity morphisms are identity with respect to composition. ∎

3.4 Can we define a category in the style of Example 3.3 using the relation $<$ on the set $\mathbb{Z}$?

No. We could not have an identity in $\mathrm{Hom}(n, n)$ since $n \not< n$. ∎

3.5 ▷ Explain in what sense Example 3.4 is an instance of the categories considered in Example 3.3. [§3.2]

The set inclusion $\subseteq$ is a relation defined on members in $\mathscr{P}$.

1. (Reflexivity): For any $A \in \mathscr{P}$, $A \subseteq A$.
2. (Transitivity): For $A, B, C \in \mathscr{P}$, if $A \subseteq B, B \subseteq C$, then $A \subseteq C$.

Thus, the power set $\mathscr{P}$ and set inclusion satisfy the assumption of Example 3.3. Therefore it is a category. ∎

3.6 ▷ (Assuming some familiarity with linear algebra.) Define a category V by taking $\mathrm{Obj}(\mathsf{V}) = \mathbb{N}$ and letting $\mathrm{Hom}_{\mathsf{V}}(m, n) =$ the set of $m \times n$ matrices with real entries, for all $m, n \in \mathbb{N}$. (We will leave the reader the task of making sense of a matrix with 0 rows or columns.) Use product of matrices to define composition. Does this category 'feel' familiar? [§VI.2.1, §VIII.1.3]

Denote the $n \times n$ identity matrix as $I_{n\times n}$.Let's extend definition of $\mathrm{Hom}_{\mathsf{V}}(m,n)$ as following:

- $\mathrm{Hom}_{\mathsf{V}}(0,0) = \{\mathrm{id}_{\varnothing}\}$,
- $\mathrm{Hom}_{\mathsf{V}}(n,0) = \varnothing, \forall n > 0$,
- $\mathrm{Hom}_{\mathsf{V}}(0,m) = \varnothing, \forall m > 0$,
- $\mathrm{Hom}_{\mathsf{V}}(m,n) =$ the set of $m \times n$ matrices with real entries, for all $m > 0, n > 0$.

Let's prove V with structure above be a category.
(Existence of identity):

$$\mathrm{id}_n = \begin{cases} \mathrm{id}_{\varnothing}, & n = 0, \\ I_{n\times n}, & n > 0. \end{cases}$$

(Composition law): For matrix $A \in \mathrm{Hom}_{\mathsf{V}}(m,n)$ and matrix $B \in \mathrm{Hom}_{\mathsf{V}}(n,l)$, the composition is defined as multiplication of matrices AB,i.e.

$$(A,B) \mapsto AB.$$

(Associativity of composition law): Due to associativity of matrices multiplication
(Left and right unit law): Due to the corresponding matrix multiplication property. i.e. $AI = A = IA$.
Let's define a relation $\sim$ on $\mathbb{N}$:

$$\forall n, m \in \mathbb{N}, n \sim m \iff \text{there is an } n \times m \text{ matrix.}$$

This relation is reflexive and transitive. Therefore this category is an instance of Example 3.3. ∎

3.7 ▷ Define carefully the objects and morphisms in Example 3.7, and draw the diagram corresponding to compositon. [§3.2]

Let $\mathbb{C}$ be a category. We define the structure, denoted by C^A as following:

1. $\mathrm{Obj}(\mathsf{C}^A) =$ all morphisms from A to any object of C. i.e. an object of C^A is a morphism $f \in \mathrm{Hom}_{\mathsf{C}}(A,Z)$ for some object Z of C.
2. For $f \in \mathrm{Hom}_{\mathsf{C}}(A,Z)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(A,X)$, define

$$\mathrm{Hom}_{\mathsf{C}^A}(f,g) = \{\sigma \big| \sigma \in \mathrm{Hom}_{\mathsf{C}}(Z,X) \text{ such that } \sigma f = g\}.$$

Equipped the structure defined above, C^A is a category. In fact

1. For object $f \in \mathrm{Hom}_{\mathsf{C}}(A,Z)$ of C^A, the identity 1_f can be chosen as the identity 1_Z in $\mathrm{Hom}_{\mathsf{C}}(Z,Z)$ since $f = 1_Z f$.

2. Let $f \in \mathrm{Hom}_{\mathsf{C}}(A, Z_1), g \in \mathrm{Hom}_{\mathsf{C}}(A, Z_2), h \in \mathrm{Hom}_{\mathsf{C}}(A, Z_3)$ be objects of C^A.

$$f_{\mathsf{C}^A} \in \mathrm{Hom}_{\mathsf{C}^A}(f, g) \iff f_{\mathsf{C}^A}(f) = g \iff \exists \sigma_1 \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2) \text{ s.t. } \sigma_1 f = g,$$

$$g_{\mathsf{C}^A} \in \mathrm{Hom}_{\mathsf{C}^A}(g, h) \iff g_{\mathsf{C}^A}(g) = h \iff \exists \sigma_2 \in \mathrm{Hom}_{\mathsf{C}}(Z_2, Z_3) \text{ s.t. } \sigma_2 g = h.$$

Define the composition law $*$ as

$$\begin{aligned}(f_{\mathsf{C}^A} * g_{\mathsf{C}^A})(f) &:= g_{\mathsf{C}^A}(f_{\mathsf{C}^A}(f)) \\ &= g_{\mathsf{C}^A}(\sigma_1 f) \\ &= \sigma_2(\sigma_1 f) \\ &= (\sigma_2 \sigma_2) f\end{aligned}$$

Since C is a category, $\sigma_2\sigma_2 \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_3)$. By definition, $\sigma_2\sigma_1$ defines a morphism from f to h.

3. For $f_{\mathsf{C}^A} \in \mathrm{Hom}_{\mathsf{C}^A}(f, g), g_{\mathsf{C}^A} \in \mathrm{Hom}_{\mathsf{C}^A}(g, h), h_{\mathsf{C}^A} \in \mathrm{Hom}_{\mathsf{C}^A}(h, l)$, we have

$$\begin{aligned}((f_{\mathsf{C}^A} * g_{\mathsf{C}^A}) * h_{\mathsf{C}^A})(f) &= h_{\mathsf{C}^A}((f_{\mathsf{C}^A} * g_{\mathsf{C}^A})(f)) \\ &= h_{\mathsf{C}^A}(g_{\mathsf{C}^A}(f_{\mathsf{C}^A}(f))) \\ &= (\sigma_h \sigma_g \sigma_f)(f) \\ &= (g_{\mathsf{C}^A} * h_{\mathsf{C}^A})(f_{\mathsf{C}^A}(f)) \\ &= (f_{\mathsf{C}^A} * (g_{\mathsf{C}^A} * h_{\mathsf{C}^A}))(f)\end{aligned}$$

i.e the composition law is associative.

4. The proof of

$$1_{\mathsf{C}^A} * f_{\mathsf{C}^A} = f_{\mathsf{C}^A}, f_{\mathsf{C}^A} * 1_{\mathsf{C}^A} = f_{\mathsf{C}^A}$$

is straightforward.

This proves that C^A with structure defined in this problem is a category. ∎

3.8 ▷ A *subcategory* C' of a category C consists of a collection of objects of C, with morphisms $\mathrm{Hom}_{\mathsf{C}'}(A, B) \subseteq \mathrm{Hom}_{\mathsf{C}}(A, B)$ for all objects $A, B \in \mathrm{Obj}(\mathsf{C}')$, such that identities and compositions in C make C' into a category. A subcategory C' is *full* if $\mathrm{Hom}_{\mathsf{C}'}(A, B) = \mathrm{Hom}_{\mathsf{C}}(A, B)$ for all $A, B \in \mathrm{Obj}(\mathsf{C}')$. Construct a category of *infinite sets* and explain how it may be viewed as a full subcategory of Set. [4.4,§VI.1.1, §VIII.1.3]

Denote the collection of infinite sets as InfSet and define the following structure on it

1. $\mathrm{Obj}(\mathsf{InfSet})$ = the class of sets with infinitely many elements;
2. for $A, B \in \mathrm{Obj}(\mathsf{InfSet})$, $\mathrm{Hom}_{\mathsf{InfSet}}(A, B) = \{f \,|\, f : A \to B \text{ is a function from } A \text{ to } B\}$.

It is easy to prove that InfSet is a category and it is a full subcategory of Set. ∎

3.9 ▷ An alternative to the notion of *multiset* introduced in §2.2 is obtained by considering sets endowed with equivalence relations; equivalent elements are taken to be multiple instance of elements 'of the same kind'. Define a notion of morphism between such enhanced sets, obtaining a category MSet containing (a 'copy' of) Set as a full subcategory. (There may be more than one reasonable way to do this! This is intentionally an open-ended exercise.) Which objects in MSet determine ordinary multisets as defined in §2.2 and how? Spell out what a morphism of multisets would be from this point of view. (There are several natural motions of morphisms of multisets. Try to define morphisms in MSet so that the notion you obtain for ordinary multisets captures your intuitive understanding of these objects.) [§2.2, §3.2, 4.5]

Let's define the structure on MSet as following:

- Obj(MSet) is the class of tuple $(S, \sim)$, where S is a set and $\sim$ is an equivalence relation on S,
- For objects $(S_1, \sim), (S_2, \approx)$ of MSet,

$$\mathrm{Hom}_{\mathsf{MSet}}((S_1, \sim), (S_2, \approx)) := \{f : S_1 \to S_2 | \forall x, y \in S, x \sim y \Longrightarrow f(x) \approx f(y)\}.$$

Since the identity set function $id_S(x) = x, x \in S_1$ preserves the equivalence relation on S, $id_S \in \mathrm{Hom}_{\mathsf{MSet}}((S_1, \sim), (S_1, \sim))$ is the identity morphism.

The composition law of set-functions will be the composition law of morphisms on MSet. The associativity of composition and left and right unit law hold. Hence MSet with structure defined above is a category.

It is obvious that Set is a full subcategory of MSet.

The *multiset* introduced in §2.2 is defined as $m : S \to \mathbb{N}^*$. So if we define an equivalence relation $\sim_m$ as

$$\forall a, b \in S, a \sim_m b \iff m(a) = m(b),$$

then $(S, \sim_m) \in \mathsf{MSet}$ is a *multiset*. ∎

3.10 Since the objects of a category C are not (necessarily) sets, it is not clear how to make sense of a notion of 'subobject' in general. In some situations it *does* make sense to talk about subobjects, and the subobjects of any given object A in C are in one-to-one correspondence with the morphisms $A \to \Omega$ for a fixed, special object Ω of C, called a *subobject classifier*. Show that Set has a subobject classifier.

For a given set S, its subset $X \subset S$ can be defined by a morphism $f : S \to \Omega = \{0, 1\}$:

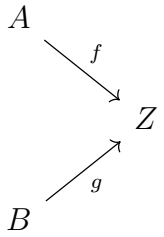
$$f(x) = \begin{cases} 1, & x \in X, \\ 0, & x \in S \setminus X. \end{cases}$$

Conversely, each morphism $f : S \to \Omega$ defines a subset of S. Therefore, the *subobject classifier* of category Set. ∎

3.11 ▷ Draw the relevant diagrams and define composition and identities for the category $\mathsf{C}^{A,B}$ mentioned in Example 3.9. Do the same for the category $\mathsf{C}^{\alpha,\beta}$ mentioned in Example 3.10. [§5.5, 5.12]

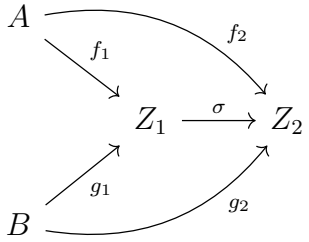
Let C be a category, we define the following structure, denoted as $\mathsf{C}^{A,B}$:

1. $\mathrm{Obj}(\mathsf{C}^{A,B}) = \{(f, g, Z) \big| \forall Z \in \mathsf{C}, f \in \mathrm{Hom}_{\mathsf{C}}(A, Z), g \in \mathrm{Hom}_{\mathsf{C}}(A, Z)\}$



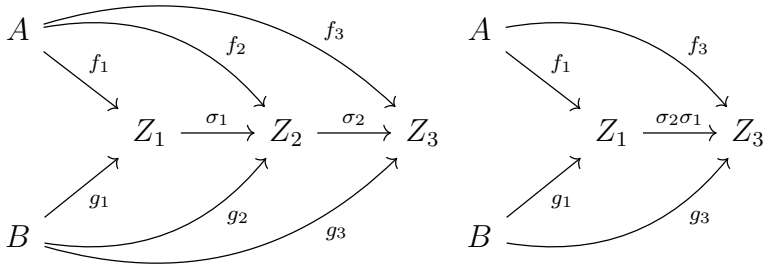
2. A morphism between triple (f_1, g_1, Z_1) and (f_2, g_2, Z_2), denoted by $\sigma_{[(f_1,g_1,Z_1),(f_2,g_2,Z_2)]}$, is defined as

$$\sigma_{[(f_1,g_1,Z_1),(f_2,g_2,Z_2)]}((f_1, g_1, Z_1)) = (f_2, g_2, Z_2) \iff$$
$$\exists \sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2) \text{ s.t. } f_2 = \sigma f_1, g_2 = \sigma g_1.$$



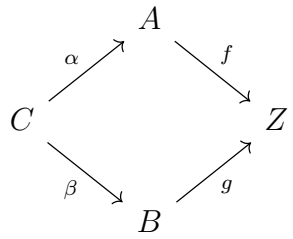
3. The composition law of morphisms, denoted by $*$, is defined as

$$\begin{aligned}
&(\sigma_{[(f_1,g_1,Z_1),(f_2,g_2,Z_2)]} * \sigma_{[(f_2,g_2,Z_2),(f_3,g_3,Z_3)]})((f_1, g_1, Z_1)) \\
=&\sigma_{[(f_2,g_2,Z_2),(f_3,g_3,Z_3)]}(\sigma_{[(f_1,g_1,Z_1),(f_2,g_2,Z_2)]}((f_1, g_1, Z_1))) \\
=&\sigma_{[(f_2,g_2,Z_2),(f_3,g_3,Z_3)]}((\sigma_1 f_1, \sigma_1 g_1, Z_2)) \\
=&(\sigma_2\sigma_1 f_1, \sigma_2\sigma_1 g_1, Z_3)
\end{aligned}$$

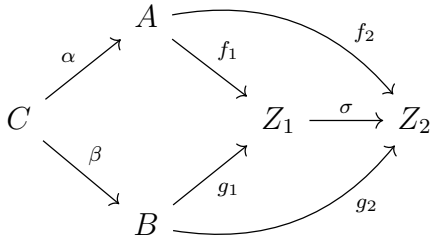


For category $\mathsf{C}^{\alpha,\beta}$

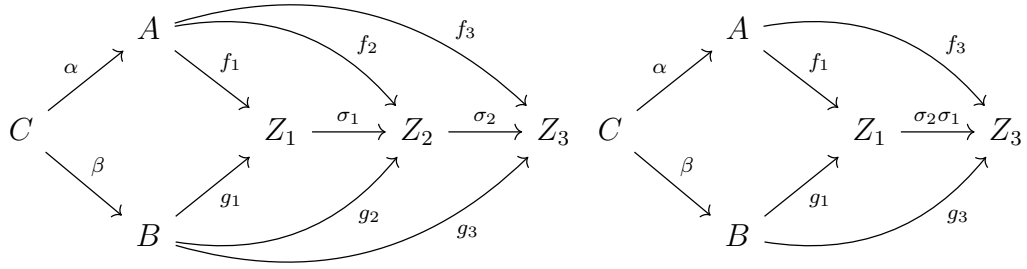
1. Obj($\mathsf{C}^{\alpha,\beta}$) =commutative diagrams



2. morphisms



3. composition law of morphisms



This proves that $\mathsf{C}^{\alpha,\beta}$ with the structure defined above is a category. ∎

§4. Morphisms

4.1 ▷ Composition is defined for *two* morphisms. If more than two morphisms are given, e.g.,

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{i} E$$

then one may compose them in several ways, for example,

$$(ih)(gf), \quad (i(hg))f, \quad i((hg)f), \quad \text{etc.}$$

so that at every step one is only composing two morphisms. Prove that the result of any such nested composition is independent of the placement of the parentheses.
(Hint: Use induction on n to show that any such choice for $f_n f_{n-1} \cdots f_1$ equals $((\cdots((f_n f_{n-1})f_{n-2})\cdots)f_1)$. Carefully working out the case $n = 5$ is helpful.) [§4.1, §II.1.3]

We prove the statement using induction method.
(Base case): When $n = 3$,

$$(f_3 f_2)f_1 = f_3(f_2 f_1)$$

due to the associativity of morphisms.
(Induction hypothesis): Suppose the statement holds when $n \geq 3$.
(Induction step): Let's prove the statement holds as well for $n+1$. For any given placement of the parentheses, the last calculation is the composition of two morphisms: F_{n+1-i} and G_i, where F_{n+1-i} is the result of $f_{n+1}, f_n, \cdots f_{i+1}$ with the placement of parentheses, G_i is the result of $f_i, f_{i-1}, \cdots, f_1$ with the placement of parentheses and $1 \leq i \leq n$. By the induction hypothesis, we have

$$F_{n+1-i} = ((\cdots(f_{n+1}f_n)\cdots)f_{i+1}), \qquad G_i = (f_i(\cdots(f_2 f_1)\cdots)).$$

Therefore

$$\begin{aligned}
F_{n+1-i}G_i &= F_{n+1-i}(f_i \underbrace{(\cdots(f_2 f_1)\cdots)}_{:=G_{i-1}}) \\
&= \underbrace{(F_{n+1-i}f_i)}_{:=F_{n+1-(i-1)}} G_{i-1} \\
&= \cdots \\
&= F_{n-1}(f_2 f_1) \\
&= (\underbrace{F_{n-1}f_2}_{:=F_n})f_1 \\
&= (F_n f_1)
\end{aligned}$$

This proves, $f_{n+1}f_n \cdots f_1$ with any placement of parenthesis, all result are the same as $((\cdots((f_{n+1}f_n)f_{n-1})\cdots)f_1)$ ∎

4.2 ▷ In Example 3.3 we have seen how to construct a category from a set endowed with a relation, provided this latter is reflexive and transitive. For what types of relations is the corresponding category a groupoid (cf. Example 4.6)? [§4.1]

A category C is a groupoid if and only if the relation is an equivalence relation. ∎

4.3 Let A, B be objects of a category C, and let $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ be a morphism.

- Prove that if f has a right-inverse, then f is an epimorphism.
- Show that the converse does not hold, by giving an explicit example of a category and an epimorphism without a right-inverse.

Let $g \in \mathrm{Hom}_{\mathsf{C}}(B, A)$ be the right-inverse of f, then $fg = 1_B$. For any object Z of C and any $\sigma_1, \sigma_2 \in \mathrm{Hom}_{\mathsf{C}}(B, Z)$. If $\sigma_1 f = \sigma_2 f$, then

$$(\sigma_1 f)g = (\sigma_2 f)g \Longrightarrow \sigma_1(fg) = \sigma_2(fg) \Longrightarrow \sigma_1 = \sigma_2.$$

It proves that f is an epimorphism.

The converse does not hold. For example, let's consider the morphism of the following category Z defined on $\mathbb{Z}$ by the relation $\leq$:

- $\mathrm{Obj}(\mathsf{Z})$ =all integers in $\mathbb{Z}$
- For object a and b of $\mathrm{Obj}(\mathsf{Z})$, the morphism is defined as

$$\mathrm{Hom}_{\mathsf{Z}}(a, b) = \begin{cases} \{(a, b)\}, & \text{if } a \leq b, \\ \varnothing, & \text{otherwise.} \end{cases}$$

It is easy to verify that each morphisms of this category is epimorphism, but only the identities have right-inverse. ∎

4.4 Prove that the composition of two monomorphisms is a monomorphism. Deduce that one can define a subcategory $\mathsf{C}_{\mathsf{mono}}$ of a category C by taking the same objects as in C and defining $\mathrm{Hom}_{\mathsf{C}_{\mathsf{mono}}}(A, B)$ to be the subset of $\mathrm{Hom}_{\mathsf{C}}(A, B)$ consisting of monomorphisms, for all objects A, B. (Cf. Exercise 3.8; of course, in general $\mathsf{C}_{\mathsf{mono}}$ is not full in C.) Do the same for epimorphisms. Can you define a subcategory $\mathsf{C}_{\mathsf{nonmono}}$ of C by restricting to morphisms that are not monomorphisms?

Let $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(B, C)$ be two monomorphisms. For any object Z of C and all morphisms $\sigma_1, \sigma_2 \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$, if $(gf)\sigma_1 = (gf)\sigma_2$, we have

$$(gf)\sigma_1 = (gf)\sigma_2 \Longrightarrow g(f\sigma_1) = g(f\sigma_2) \Longrightarrow f\sigma_1 = f\sigma_2 \Longrightarrow \sigma_1 = \sigma_2.$$

It means the composition of gf is a monomorphism.

Define the structure on $\mathsf{C}_{\mathsf{mono}}$ as the followinig:

- $\mathrm{Obj}(\mathsf{C}_{\mathsf{mono}}) = \mathrm{Obj}(\mathsf{C})$,
- For object A and B of $\mathrm{Obj}(\mathsf{C}_{\mathsf{mono}})$, the morphism is defined as

$$\mathrm{Hom}_{\mathsf{C}_{\mathsf{mono}}}(A, B) = \{f \big| f \in \mathrm{Hom}_{\mathsf{C}}(A, B) \text{ and } f \text{ is a monomorphism}\}.$$

Let's verify $\mathsf{C}_{\mathsf{mono}}$ be a category

- For an object A of $\mathsf{C}_{\mathsf{mono}}$, $1_A \in \mathrm{Hom}_{\mathsf{C}}(A, A)$ is also the identity of $\mathrm{Hom}_{\mathsf{C}_{\mathsf{mono}}}(A, A)$ since identity is a monomorphism.
- Define the composition law of $\mathsf{C}_{\mathsf{mono}}$ as the same as that of C. Since the composition of monomorphisms is monomorphism. This composition law makes sense when it was restricted to $\mathsf{C}_{\mathsf{mono}}$.
- The associativity of composition law and properties of identity hold as well.

Hence $\mathsf{C}_{\mathsf{mono}}$ is a category and it is a subcategory of C.

We can define $\mathsf{C}_{\mathsf{epi}}$ similarly

- $\mathrm{Obj}(\mathsf{C}_{\mathsf{epi}}) = \mathrm{Obj}(\mathsf{C})$,
- For object A and B of $\mathrm{Obj}(\mathsf{C}_{\mathsf{epi}})$, the morphism is defined as

$$\mathrm{Hom}_{\mathsf{C}_{\mathsf{epi}}}(A, B) = \{f \big| f \in \mathrm{Hom}_{\mathsf{C}}(A, B) \text{ and } f \text{ is an epimorphism}\}.$$

But, the structure on $\mathsf{C}_{\mathsf{nonmono}}$ defined as the following

- $\mathrm{Obj}(\mathsf{C}_{\mathsf{nonmono}}) = \mathrm{Obj}(\mathsf{C})$,
- For object A and B of $\mathrm{Obj}(\mathsf{C}_{\mathsf{nonmono}})$, the morphism is defined as

$$\mathrm{Hom}_{\mathsf{C}_{\mathsf{nonmono}}}(A, B) = \{f \big| f \in \mathrm{Hom}_{\mathsf{C}}(A, B) \text{ and } f \text{ isn't an monomorphism}\}.$$

can't make $\mathsf{C}_{\mathsf{nonmono}}$ to be a category. ∎

4.5 Give a concrete description of monomorphisms and epimorphisms in the category MSet you constructed in Exercise I.3.9. (Your answer will depend on the notion of morphism you defined in that exercise!)

A morphism f is monomorphism if and only if f is injective.
A morphism f is epimorphism if and only iif f is surjective. ∎

§5. Universal properties

5.1 Prove that a final object in a category C is initial in the opposite category C_{op} (cf. Exercise I.3.1).

A object $F \in \mathrm{Obj}(\mathsf{C})$ is final if and only if

$$\forall Z \in \mathrm{Obj}(\mathsf{C}), \mathrm{Hom}_{\mathsf{C}}(Z, A) \text{ is a singleton.}$$

Therefore,

$$\forall Z \in \mathrm{Obj}(\mathsf{C}) = \mathsf{C}_{op}, \mathrm{Hom}_{\mathsf{C}_{op}}(A, Z) = \mathrm{Hom}_{\mathsf{C}}(Z, A) \text{ is a singleton.}$$

i.e. F is the initial of the category C_{op}. ∎

5.2 ▷ Prove that $\varnothing$ is the unique initial object in Set. [§5.1].

First of all, the object $\varnothing \in \mathrm{Obj}(\mathsf{Set})$ is initial for category Set since for each $S \in \mathrm{Obj}(\mathsf{Set})$,

$$\mathrm{Hom}_{\mathsf{Set}}(\varnothing, S) = \{\mathrm{id}_{\varnothing}\} \text{ is a singleton.}$$

Suppose $I \in \mathrm{Obj}(\mathsf{Set})$ be another initial of category Set, then there is an isomorphism, therefore bijection, between $\varnothing$ and I. It implies the number of elements in I is 0, i.e. $|I| = 0$. It proves that $I = \varnothing$. ∎

5.3 ▷ Prove that final objects are unique up to isomorphism. [§5.1]

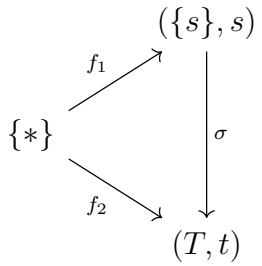
Suppose A, B be two final objects of category C. By definition, there is a unique morphism $f : A \to B$ and unique morphism $g : B \to A$. By composition law, $fg : B \to B$ and $gf : A \to A$ are morphisms. Hence,

$$fg = \mathrm{id}_B, \qquad gf = \mathrm{id}_A.$$

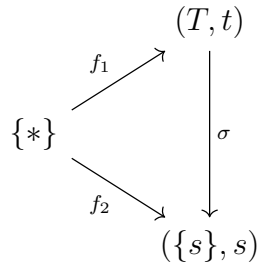
It means $A \cong B$. ∎

5.4 What are initial and final objects in the category of 'pointed sets' (Example 3.8)? Are they unique?

Initial objects: $\{f : \{*\} \to (\{s\}, s)\}$



Since $\{s\}$ is a single point set, $\sigma(s) = t$ is the unique morphism in $\mathrm{Hom}_{\mathsf{Set}^*}(f_1, f_2)$.
Final objects: $\{f : \{*\} \to \{\{s\}, s\}\}$



As shown in the diagram, $\sigma(x) = s, \forall x \in T$ is the unique morphism in $\mathrm{Hom}_{\mathsf{Set}^*}(f_1, f_2)$. ∎

5.5 What are the final objects in the category considered in §5.3? [§5.3]

The category considered in §5.3, denoted by $\mathsf{C}^{A,\sim}$, is

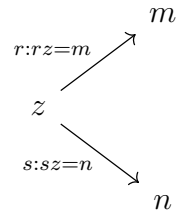
- $\mathrm{Obj}(\mathsf{C}^{A,\sim}) = \{(\phi, Z) \big| \phi : A \to Z \text{ s.t. } \forall a, b \in A, a \sim b \Longrightarrow \phi(a) = \phi(b)\}$,
- $\mathrm{Hom}_{\mathsf{C}^{A,\sim}}((\phi_1, Z_1), (\phi_2, Z_2)) = \{\sigma \big| \sigma : Z_1 \to Z_2 \text{ s.t. } \phi_2 = \sigma\phi_1\}$.

Final objects: Each object $(\phi, \{s\}) \in \mathrm{Obj}(\mathsf{C}^{A,\sim})$, where $\phi(x) = s, \forall x \in A$, is a final object. ∎

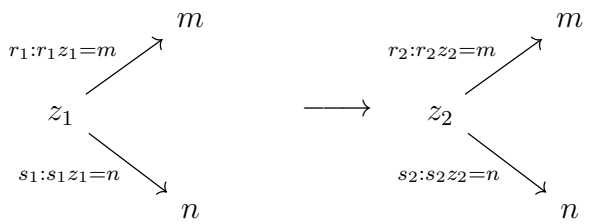
5.6 ▷ Consider the category corresponding to endowing (as in Example 3.3) the set $\mathbf{Z}^+$ of positive integers with the divisibility relation. Thus there is exactly one morphism $d \to m$ in this category if and only if d divides m without remainder; there is no morphism between d and m otherwise. Show that this category has products and coproducts. What are their 'conventional' names? [§VII.5.1]

Let's define the structure on $\mathsf{Div}_{m,n}$ as follow:

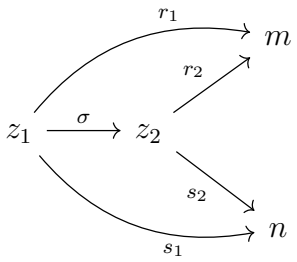
- $\mathrm{Obj}_{\mathsf{Div}_{m,n}} = \{(z, r, s) \big| rz = m, sz = n\}$, i.e.



- $\mathrm{Hom}_{\mathsf{Div}_{m,n}}((z_1, r_1, s_1), (z_2, r_2, s_2)) = \{\sigma \in \mathbb{Z} | z1\sigma = z_2\}$.i.e



are commutative diagrams



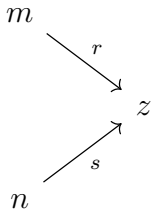
With this structure above, $\mathsf{Div}_{m,n}$ is a category. Let's consider the following object

$$\mathsf{GCD}(m,n) := \left(\gcd(m,n), \frac{m}{\gcd(m,n)}, \frac{n}{\gcd(m,n)} \right)$$

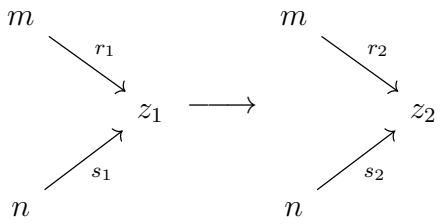
in $\mathsf{Div}_{m,n}$. For any object $(z,r,s) \in \mathsf{Div}_{m,n}$, there is a unique morphism from (z,r,s) to $\mathsf{GCD}(m,n)$ since common divisor of m,n is also the divisor of $\gcd(m,n)$. Therefore, $\mathsf{GCD}(m,n)$ is a final object of $\mathsf{Div}_{m,n}$.

For $\mathsf{Div}^{m,n}$, define structure

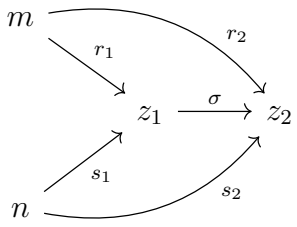
- $\mathrm{Obj}_{\mathsf{Div}^{m,n}} = \{(r,s,z) \big| rm = z, sn = z\}$, i.e.



- $\mathrm{Hom}_{\mathsf{Div}^{m,n}}((r_1,s_1,z_1),(r_2,s_2,z_2)) = \{\sigma \in \mathbb{Z} | z_1\sigma = z_2\}$.i.e



are commutative diagrams



With the structure above, $\mathsf{Div}^{m,n}$ is a category. Consider the object

$$\mathsf{LCM}(m,n) := \left(\frac{\operatorname{lcm}(m,n)}{m}, \frac{\operatorname{lcm}(m,n)}{n}, \operatorname{lcm}(m,n)\right),$$

for any object (r,s,z), there is a unique morphism from $\mathsf{LCM}(m,n)$ to (r,s,z) since the common multiple of m,n is also the multiple of $\operatorname{lcm}(m,n)$. Hence $\mathsf{LCM}(m,n)$ is an initial object. ∎

5.7 Redo Exercise I.2.9, this time using Proposition 5.4.

Define $\mathrm{i}_A : A \to A \cup B, \mathrm{i}_B : B \to A \cup B$ as

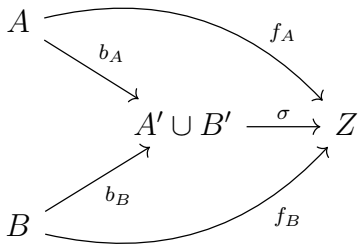
$$\mathrm{i}_A(a) = a, \forall a \in A, \mathrm{i}_B(b) = b, \forall b \in B.$$

For any object $(f_A, f_B, Z) \in \operatorname{Obj}(\mathsf{C}^{A,B})$, there is a unique morphism $\sigma : A \cup B \to Z$

$$\sigma(x) = \begin{cases} f_A(x), & \text{if } x \in A, \\ f_B(x), & \text{if } x \in B. \end{cases}$$

i.e. $(\mathrm{i}_A, \mathrm{i}_B, A \cup B)$ is an initial object of $\mathsf{C}^{A,B}$.

Since $A \cong A'$ and $B \cong B'$, there are bijections $b_A : A \to A'$ and $b_B : B \to B'$. For any object $(f_A, f_B, Z) \in \operatorname{Obj}(\mathsf{C}^{A,B})$, we can define a unique morphism σ such that the diagram

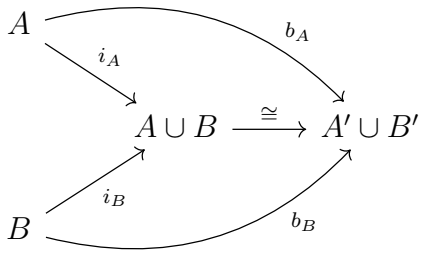


is commutative, where

$$\sigma(x) = \begin{cases} f_A(b_A^{-1}(x)), & \text{if } x \in A', \\ f_B(b_B^{-1}(x)), & \text{if } x \in B'. \end{cases}$$

It implies that $(b_A, b_B, A' \cup B')$ is also an initial object of $\mathsf{C}^{A,B}$.

By Proposition 5.4, the two initial objects are isomorphic, i.e.



is commutative. ∎

5.8 Show that in every category C the products $A \times B$ and $B \times A$ are isomorphic, if they exist. (Hint: Observe that they both satisfy the universal property for the product of A and B; then use Proposition 5.4.)

∎

5.9 Let C be a category with products. Find a reasonable candidate for the universal property that the product $A \times B \times C$ of three objects of C ought to satisfy, and prove that both $(A \times B) \times C$ and $A \times (B \times C)$ satisfy this universal property. Deduce that $(A \times B) \times C$ and $A \times (B \times C)$ are necessarily isomorphic.

5.10 Push the envelope a little further still, and define products and coproducts for families (i.e., indexed sets) of objects of a category.
Do these exist in Set?
It is common to denote the product $\underbrace{A \times \cdots \times A}_{n \text{ times}}$ by A^n.

5.11 Let A, resp. B, be a set, endowed with an equivalence relation $\sim_A$, resp. $\sim_B$. Define a relation $\sim$ on $A \times B$ by setting

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 \sim_A a_2 \text{ and } b_1 \sim_B b_2.$$

(This is immediately seen to be an equivalence relation.)

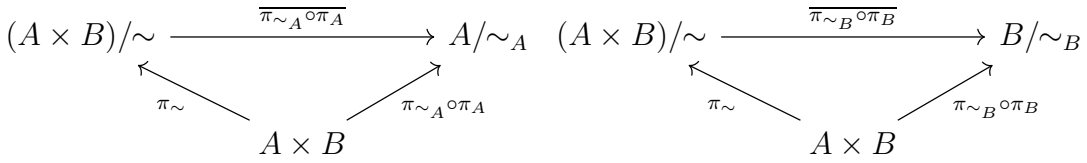
- Use the universal property for quotients (§5.3) to establish that there are functions

$$(A \times B)/\sim \to A/\sim_A, (A \times B)/\sim \to B/\sim_B .$$

- Prove that $(A \times B)/\sim$, with these two functions, satisfies the universal property for the product of $A/\sim_A$ and $B/\sim_B$.
- Conclude (without further work) that $(A \times B)/\sim \cong (A/\sim_A) \times (B/\sim_B)$.

Let denote

$$\begin{aligned}
\pi_\sim &: A \times B \to (A \times B)/\sim, \qquad \pi_\sim((a,b)) = [(a,b)]_\sim, \\
\pi_A &: A \times B \to A, \qquad \pi_A((a,b)) = a, \\
\pi_B &: A \times B \to B, \qquad \pi_A((a,b)) = b, \\
\pi_{\sim_A} &: A \to A_{\sim_A}, \qquad \pi_{\sim_A}(a) = [a]_{\sim_A}, \\
\pi_{\sim_B} &: B \to B_{\sim_B}, \qquad \pi_{\sim_B}(b) = [b]_{\sim_B}.
\end{aligned}$$



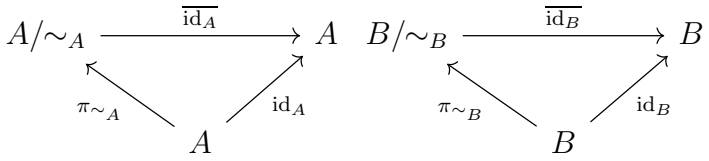
The function $\overline{\pi_{\sim_A} \circ \pi_A} : (A \times B)/\sim \to A/\sim_A$ is

$$\overline{\pi_{\sim_A} \circ \pi_A}([(a,b)]_\sim) = [a]_{\sim_A},$$

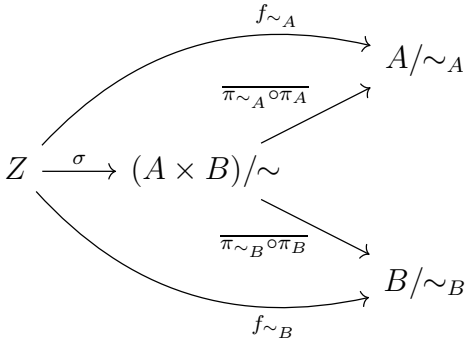
and the function $\overline{\pi_{\sim_B} \circ \pi_B} : (A \times B)/\sim \to B/\sim_B$ is

$$\overline{\pi_{\sim_A} \circ \pi_A}([(a,b)]_\sim) = [b]_{\sim_B}.$$

Applying universal property of quotients on identity function on A and B:



Let's find σ such that the diagram



is commutative. Simple calculation shows the function $\sigma : Z \to (A \times B)/\sim$ is unique and defined as

$$\sigma(z) = \pi_\sim\Big(\big((\overline{\mathrm{id}_A} \circ f_{\sim_A})(z), (\overline{\mathrm{id}_B} \circ f_{\sim_B})(z)\big)\Big), \forall z \in Z.$$

It proves that $(A \times B)/\sim$ satisfies the universal property for the product of $A/\sim_A$ and $B/\sim_B$.

The two products are isomorphic by Proposition 5.4. i.e. $(A \times B)/\sim \cong A/\sim_A \times B/\sim_B$. ∎

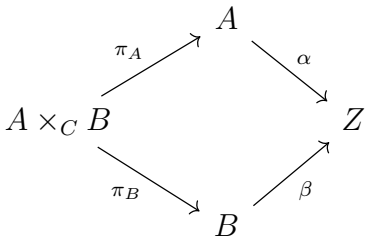
5.12 Define the notions of fibered products and fibered coproducts, as terminal objects of the categories $\mathsf{C}_{\alpha,\beta}, \mathsf{C}^{\alpha,\beta}$ considered in Example 3.10 (cf. also Exercise 3.11), by stating carefully the corresponding universal properties.
As it happens, Set has both fibered products and coproducts. Define these objects 'concretely', in terms of naive set theory. [II.2.9, III.6.10, III.6.11]

Let's consider category $\mathsf{C}_{\alpha,\beta}$, where $\mathsf{C} = \mathsf{Set}$. Define

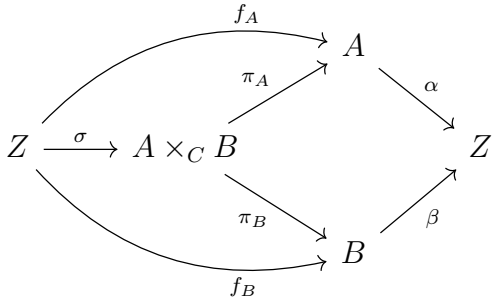
$$A \times_C B = \{(a,b) \big| \alpha(a) = \beta(b)\} \subset A \times B.$$

$$\pi_A : A \times_C B \to A, \qquad \pi_A((a,b)) = a,$$
$$\pi_B : A \times_C B \to B, \qquad \pi_B((a,b)) = b.$$

Therefore the following diagram is commutative



To proof $A \times_C B$ satisfies the universal property for the product of A and B, we need find the σ such that the following diagram is commutative.

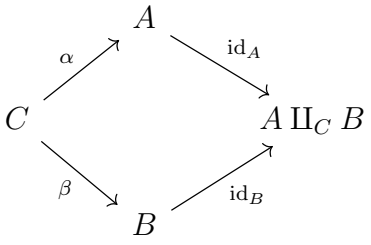


Since $(\alpha \circ f_A)(z) = (\beta \circ f_B)(z), \forall z \in Z$, it implies that $(f_A(z), f_B(z)) \in A \times_C B, \forall z \in Z$.Therefore, we can choose σ as

$$\sigma(z) = (f_A(z), f_B(z)), \forall z \in Z.$$

Hence $A \times_C B$ together with the prjections π_A, π_B is a fibered product.

Let's consider the diagram

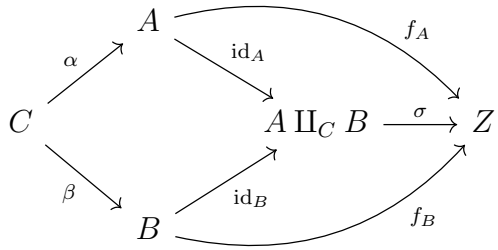


To make this diagram commutative, we need have the following equivalence relation

$$(0,a) \sim (1,b) \iff \exists c \in C \text{ s.t. } a = \alpha(c), b = \beta(c).$$

Therefore $A \amalg_C B = (A \amalg B)/\sim$.

Now, we can consider the following diagram:



To make this diagram commutative, we can define

$$\sigma(t) = \begin{cases} f_A(a), & \text{if } t = (0,a), \\ f_B(b), & \text{if } t = (1,b). \end{cases}$$

It is easy to verify, for all $c \in C$,

$$(\sigma \circ \mathrm{id}_A \circ \alpha)(c) = (\sigma \circ \mathrm{id}_B \circ \beta)(c).$$

Hence, $A \amalg_C B$ together with the inclusions is a fibered coproduct. ∎

Chapter II. Groups, first encounter

§1. Definition of group

1.1 ▷ Write a careful proof that every group is the group of isomorphisms of a groupoid. In particular, every group is the group of automorphisms of some object in some category.[§2.1]

■

1.2 ▷ Consider the 'sets of numbers' listed in §1.1, and decide which are made into groups by conventional operations such as + and ·. Even if the answer is negative (for example, $(R, \cdot)$ is not a group), see if variations on the definition of these sets lead to groups (for example, $(R^*, \cdot)$ is a group; cf. §1.4). [§1.2]

1. $\mathbb{N}$ is not a group under operation + or ·.
2. $\mathbb{Z}$ is a group under operation +, but not under operation ·.
3. $\mathbb{N}^*$ and $\mathbb{Z}^*$ can't be a group under operation ·.
4. $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are groups under operation +, but can't be groups under operation ·.
5. $\mathbb{Q}^*, \mathbb{R}^*$ and $\mathbb{C}^*$ are groups under operation ·.

These statements are easy to be verified. ■

1.3 Prove that $(gh)^{-1} = h^{-1}g^{-1}$ for all elements g, h of a group G.

Since

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = gg^{-1} = e_G$$

and

$$(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}h = e_G,$$

it turns out $(gh)^{-1} = h^{-1}g^{-1}$. ■

1.4 Suppose that $g^2 = e$ for all elements g of a group G; prove that G is commutative.

By assumption, for all elements $g, h \in G$

$$hghg = e = gg$$

it means $hgh = g$ then $hghh = gh$. It implies $hg = gh$.i.e. G is commutative. ■

1.5 The 'multiplication table' of a group is an array compiling the results of all multiplications $g \bullet h$:

$\bullet$	e	$\cdots$	h	$\cdots$
e	e	$\cdots$	h	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g	g	$\cdots$	$g \bullet h$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

(Here e is the identity element. Of course the table depends on the order in which the elements are listed in the top row and leftmost column.) Prove that every row and every column of the multiplication table of a group contains all elements of the group exactly once (like Sudoku diagrams!).

If $f \bullet g = f \bullet h$, then $g = h$. It is a contradiction.Hence there is no equal elements in f-row. If $g \bullet f = h \bullet f$, then $g = h$. It is a contradiction too. Hence there is no equal elements in f-column. ∎

1.6 ¬ Prove that there is only one possible multiplication table for G if G has exactly 1, 2, or 3 elements. Analyze the possible multiplication tables for groups with exactly 4 elements, and show that there are two distinct tables, up to reordering the elements of G. Use these tables to prove that all groups with ≤ 4 elements are commutative.
(You are welcome to analyze groups with 5 elements using the same technique, but you will soon know enough about groups to be able to avoid such brute-force approaches.) [2.19]

If $|G| = 1$, then $G = \{1\}$. It is trivial group.
If $G = \{1, a\}$, then $a^2 = 1$.
If $G = \{1, a, b\}$, then $ab = 1$. It implies $a^2 = b$. Hence G is a cyclic group $\{1, a, a^2\}$.
Now, let consider $G = \{1, a, b, c\}$

If one of a^2, b^2, c^2 is not 1, say, $a^2 \neq 1$, then $a^3 \neq 1$ and $G = \{1, a, a^2, a^3\}$ is a cyclic group. In fact, suppose $a^3 = 1$. The possible values of ab are 1 or c. If $ab = 1$, then $b = a^2$ and $ac = 1$ because $ac = b$ implies $c = a$, this contradicts to our assumption. But if $ac = 1$, $ab = 1$, then $b = c$ also contradicts to our assumption. Therefore, we must have $ab = c, ac = b$. This leads to $a^2 = 1$ and contradicts to our assumption. Hence $a^3 \neq 1$.

If $a^2 = b^2 = c^2 = 1$, then $G = \{1, a, b, ab\}$. ∎

1.7 Prove Corollary 1.11.

($\Longrightarrow$): This is Lemma 1.10.
($\Longleftarrow$): Suppose $N = n\,|g|$, then $g^N = (g^{|g|})^n = e^n = e$. ∎

1.8 ¬ Let G be a finite abelian group with exactly one element f of order 2. Prove that $\prod_{g \in G} g = f$.[4.16]

By assumption, there are only two elements $1, f$ such that $1^{-1} = 1, f^{-1} = f$. Hence

$$\prod_{g\in G} g = (\prod_{g\in G\setminus\{1,f\}} g) \bullet f = (\underbrace{1 \bullet 1 \bullet \cdots \bullet 1}_{\frac{|G|-2}{2}}) \bullet f = f.$$

The statement is proved. ∎

1.9 Let G be a finite group, of order n, and let m be the number of elements $g \in G$ of order exactly 2. Prove that $n - m$ is odd. Deduce that if n is even, then G necessarily contains elements of order 2.

Let's rewrite set G as

$$G = \{1\} \cup \{g \big| g \in G, |g| = 2\} \cup \{g \big| g \in G, |g| > 2\}.$$

If $|g| > 2$, then $|g^{-1}| > 2$ and $g \neq g^{-1}$. Hence $\big|\{g \big| g \in G, |g| > 2\}\big| = 2k, k \in \mathbb{N}$ and $n = 1 + m + 2k$. This is $n - m = 2k + 1$, an odd number.

If n is even number, then $m = n - (2k + 1) > 0$, i.e. G contain elements of order 2. ∎

1.10 Suppose the order of g is odd. What can you say about the order of g^2?

If $|g|$ is odd, then $\gcd(2, |g|) = 1$. Hence $|g^2| = \frac{|g|}{\gcd(2,|g|)} = |g|$ ∎

1.11 Prove that for all g, h in a group G, $|gh| = |hg|$.(Hint: Prove that $|aga^{-1}| = |g|$ for all a, g in G.)

For $h, g \in G$,

$$(hgh^{-1})^{|g|} = hg^{|g|}h^{-1} = 1.$$

Therefore $|hgh^{-1}| \mid |g|$. On the other hand, $g = h^{-1}(hgh^{-1})h$ implies $|g| \mid |hgh^{-1}|$. This proves $|hgh^{-1}| = |g|$. Taking $g = gh$, we have $|hg| = |hghh^{-1}| = |gh|$ ∎

1.12 ▷In the group of invertible 2×2 matrices, consider

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Verify that $|g| = 4$, $|h| = 3$ and $|gh| = \infty$.[§1.6]

$g \neq I, g^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq I, g^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \neq I, g^4 = I$. So $|g| = 4$.

$h \neq I, h^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \neq I, h^3 = I$, So $|h| = 3$

$gh = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, (gh)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ So. $|gh| = \infty$. ∎

1.13 ▷Give an example showing that $|gh|$ is not necessarily equal to $\text{lcm}(|g|, |h|)$, even if g and h commute.[§1.6, 1.14]

Let's consider the group $\mathbb{Z}_{12}$ defined as the following:

1. $\mathbb{Z}_{12} = \{[0], [1], [2], \cdots, [11]\}$
2. For $[a], [b] \in \mathbb{Z}_{12}$, define the group product as $[a][b] = [c]$, where $c = (a + b) \mod 12$.

It is easy to verify that $\mathbb{Z}_{12}$ is a commutative group, and

1. $|[2]| = 6$ and $|[4]| = 3$. Thus $\text{lcm}(|[2]|, |[4]|) = 6$
2. $[2][4] = [6]$ and $|[6]| = 2$.

It shows that $|[2][4]| \neq \text{lcm}(|[2]|, |[4]|)$. ∎

1.14 ▷ As a counterpoint to Exercise 1.13, prove that if g and h commute and $\gcd(|g|, |h|) = 1$, then $|gh| = |g|\,|h|$.(Hint: Let $N = |gh|$; then $g^N = (h^{-1})^N$.What can you say about this element?) [§1.6, 1.15, IV.2.5]

As suggested in hint, we calculate

$$1 = (gh)^N = g^N h^N \Longrightarrow g^N = (h^{-1})^N.$$

Therefore, g^N and $(h^{-1})^N$ has the same order, denoted by t. By Proposition 1.13, we have

$$t = \left|g^N\right| = \frac{|g|}{\gcd(N, |g|)} = \frac{|h|}{\gcd(N, |h|)} = \left|(h^{-1})^N\right|.$$

It is obvious that t is a common divisor of $|g|$ and $|h|$. Since $\gcd(|g|, |h|) = 1$, t must be 1. This means $g^N = 1 = (h^{-1})^N$. Thus

$$|g| \mid N, |h| \mid N \Longrightarrow |g|\,|h| \mid N.$$

On the other hand, since $(gh)^{|g||h|} = 1$, $N \mid |g|\,|h|$.

This proves that $N = |g|\,|h|$ ∎

1.15 ¬ Let G be a commutative group, and let $g \in G$ be an element of maximal finite order, that is, such that if $h \in G$ has finite order, then $|h| \leq |g|$. Prove that in fact if h has finite order in G, then $|h|$ divides $|g|$. (Hint: Argue by contradiction. If $|h|$ is finite but does not divide $|g|$, then there is a prime integer p such that $|g| = p^m r$, $|h| = p^n s$, with r and s relatively prime to p and $m < n$. Use Exercise 1.14 to compute the order of $g^{p^m} h^s$.) [§2.1, 4.11, IV.6.15]

Applying prime factorization theorem to $|g|$ and $|h|$, we have

$$|g| = p_1^{m_1} p_2^{m_2} \cdots p_l^{m_l}, \qquad |h| = p_1^{n_1} p_2^{n_2} \cdots p_l^{n_l},$$

where $m_i \geq 0, n_i \geq 0, i = 1, 2, \cdots l$.

If $|h| \nmid |g|$, then there is p_j such that $n_j > m_j$. So, denoting p_j, m_j, n_j by p, m, n repsectively, we can rewrite $|g|$ and $|h|$ as

$$|g| = p^m r, |h| = p^n s$$

where $m < n$, $\gcd(r, p) = 1, \gcd(s, p) = 1$.

By applying proposition 1.13, we have

$$\left|g^{p^m}\right| = \frac{|g|}{\gcd(p^m, |g|)} = r, |h^s| = \frac{|h|}{\gcd(s, |h|)} = p^n.$$

Since $\gcd(r, p^n) = 1$, the order of $g^{p^m} h^s$ must be $\left|g^{p^m}\right| |h^s| = p^n r$.i.e.

$$\left|g^{p^m} h^s\right| = p^n r > p^m r = |g|.$$

This contradicts the assumption that g is the maximal order element in G. Hence $|h| \mid |g|$. ∎

§2. Examples of groups

2.1 ¬One can associate an $n \times n$ matrix M_σ with a permutation $\sigma \in S_n$, by letting the entry at $(i, \sigma(i))$ be 1, and letting all other entries be 0. For example, the matrix corresponding to the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$$

would be

$$M_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Prove that, with this notation,

$$M_{\sigma\tau} = M_\sigma M_\tau$$

for all $\sigma, \tau \in S_n$, where the product on the right is the ordinary product of matrices.

$\sigma(i) = j \iff$ the entry at (i, j) position of M_σ is 1, the other entries on i-th row, j-th column are zero.

$\tau(j) = k \iff$ the entry at (j, k) position of M_τ is 1, the other entries on j-th row, k-th column are zero.

The entry (i, k) of $M_\sigma M_\tau$ is 1, the other entries in i-th row and k-th column are zero. This

is the same as $M_{\sigma\tau}$ since $(\sigma\tau)(i) = \tau(\sigma(i)) = k$.

Applying this argument with $i = 1, 2, \cdots, n$, we can conclude that $M_{\sigma\tau} = M_\sigma M_\tau$. ∎

2.2 ▷ Prove that if $d \leq n$, then S_n contains elements of order d.[§2.1]

The element

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & d & (d+1) & \cdots & n \\ d & 1 & 2 & \cdots & (d-1) & (d+1) & \cdots & n \end{pmatrix}$$

has order d. ∎

2.3 For every positive integer n find an element of order n in $S_{\mathbb{N}}$.

The element in $S_{\mathbb{N}}$ is an automorphism of $\mathbb{N}$. Define the automorphism $f : \mathbb{N} \to \mathbb{N}$ as the following:

$$f(n) = \begin{cases} d-1, & n = 0, \\ n-1, & 1 \leq n \leq d-1, \\ n, & n \geq d. \end{cases}$$

It is easy to verify that the order of f is d. ∎

2.4 Define a homomorphism $D_8 \to S_4$ by labelling vertices of a square, as we did for a triangle in §2.2. List the 8 permutation in the image of this homomorphis.

Label the vertices of square clockwise by $1, 2, 3, 4$, then the counterclockwise rotations will be

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}.$$

The reflections along the symmetric lines will be

$$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \sigma_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \sigma_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

These are the images of D_8 in S_4 under the homomorphism. ∎

2.5 ▷ Describe generators and relations for all dihedral groups D_{2n}(Hint: Let x be the reflection about a line through the center of a regular n-gon and a vertex, and let y be the counterclockwise rotation by $2\pi/n$. The group D_{2n} will be generated by x and y, subject to three relations. To see that these relations really determine D_{2n}, use them to show that any product $x^{i_1}y^{i_2}x^{i_3}h^{i_4}\cdots$ equals $x^i y^j$ for some i, j with $0 \leq i \leq 1, 0 \leq j < n$)[8.4, §IV 2.5]

Let x be the reflection about a line through the center of a regular n-gon and a vertex and y be the counterclockwise rotation by $2\pi/n$, then we have the following rotations in D_{2n}:

$$y, y^1, y^2, \cdots y^n.$$

It is obvious that there are no equal pairs, i.e. if $1 \leq i, j \leq n$ and $i \neq j$, then

$$y^i \neq y^j.$$

Otherwise, $y^{|i-j|}$ be the identity, but this is impossible since vertices are rotated by angle $2\,|i-j|\,\pi/n$ which is strictly less than 2π.
Now let's consider another set of elements:

$$xy, xy^2, \cdots xy^n.$$

We claim:

- For $0 \leq i, j \leq n$ and $i \neq j$, then $xy^i \neq xy^j$. If they are equal, then $y^i = y^j$. It is impossible.
- For $0 \leq i, j \leq n$, $xy^i \neq y^j$. If $xy^i = y^j$, then

  $$x = y^k, \text{ where } k = \big(\max\{j-i, j+n-i\}\big) \mod n.$$

  It is impossible since x will map at least one vertex to itself while y^k will change the position of all vertices.

Hence, $D_{2n} = \{y, y^1, \cdots, y^n, xy, xy^2, \cdots, xy^n\}$. ∎

2.6 ▷ For every positive integer n construct a group containing elements g, h such that $|g| = 2$, $|h| = 2$, and $|gh| = n$. (Hint: For $n > 1$, D_{2n} will do.) [§1.6]

Let's label the vertices of n-gon clockwise by $1, 2, \cdots, n$. Let g be the reflection about the line through the center and vertex 1. It is easy to proof that $|g| = 2$. Let p be a point defined as:

$$p = \begin{cases} \text{vertex } \frac{n+1}{2}, & \text{if n is odd,} \\ \text{middle point of edge from vertex } \frac{n}{2} \text{ to } \frac{n}{2}+1, & \text{if n is even.} \end{cases}$$

Let f be the reflection about the line through center and p. It is also easy to verify $|f| = 2$, but

$$gf = \text{the counterclockwise rotation by } \frac{2\pi}{n}.$$

So $|gf| = n$. ∎

2.7 ¬ Find all elements of D_{2n} that commute with every other element. (The parity of n plays a role.) [§IV.1.2]

Using the result of Exercise 2.5, the dihedral group D_{2n} can be written as

$$D_{2n} = \{e, y, y^2, \cdots, y^{n-1}, x, xy, \cdots, xy^{n-1}\}$$

Since xy is a reflection, then $xyxy = e$, i.e. $xyx = y^{-1}$.

Let's discuss the following cases:

Rotation $y^k, 0 \leq k \leq n-1$:

- It is obvious that it commute with other rotations.
- For reflection xy^l, if $xy^{l+k} = y^k xy^l$, then $y^{2k} = e$. So $2k \equiv 0 \mod n$. If n is odd, then $k = 0$ and if n is even then $k = \frac{n}{2}$.

Reflection $xy^k, 0 \leq k \leq n-1$:

- For rotation y^l, if $xyk + l = y^l xy^k$, then $y^{2l} = e$. i.e. The reflection can only commute with some rotations, but not all.
- For reflection xy^l, if $xy^k xy^l = xy^l xy^k$, then $y^{2(k+l)} = e$. So the reflection can only commute with some reflection, but not all.

Hence, the center of D_{2n} is $\{e\}$ if n is odd, otherwise $\{e, y^{\frac{n}{2}}\}$. ∎

2.8 Find the orders of the groups of symmetries of the five 'platonic solids'.

2.9 Verify carefully that 'congruence mod n' is an equivalence relation.

The proof is very straightforward:

Reflexivity: Since $a - a = 0 = 0n$, $a \equiv a \mod n$.

Symmetry: If $a \equiv b \mod n$, then $\exists k \in \mathbb{Z}$ s.t. $a - b = kn$. Thus $b - a = (-k)n$. It implies $b \equiv a \mod n$.

Transitivity: If $a \equiv b \mod n$, $b \equiv c \mod n$, then $\exists k_1, k_2 \in \mathbb{Z}$ s.t. $a - b = k_1 n$, $b - c = k_2 n$. Therefore $a - c = (k_1 + k_2)n$. This proves $a \equiv c \mod n$. ∎

2.10 Prove that $\mathbb{Z}/n\mathbb{Z}$ consists of precisely n elements.

On one hand, let's consider set

$$S := \big\{[i]_n | 0 \leq i \leq n-1\big\}.$$

S contains n distinct elements and $S \subset \mathbb{Z}/n\mathbb{Z}$. Therefore $|\mathbb{Z}/n\mathbb{Z}| \geq n$.

On the other hand, for $m \in \mathbb{Z}$, we can rewrite it as

$$m = \left\lfloor \frac{m}{n} \right\rfloor n + r, \text{ where } \left\lfloor \frac{m}{n} \right\rfloor \leq \frac{m}{n} < \left\lfloor \frac{m}{n} \right\rfloor + 1, 0 \leq r \leq n-1.$$

Therefore $m \equiv r \mod n$. It implies $|\mathbb{Z}/n\mathbb{Z}| \leq n$.

This proves $|\mathbb{Z}/n\mathbb{Z}| = n$. ∎

2.11 ▷ Prove that the square of every odd integer is congruent to 1 modulo 8. [§VII.5.1]

Let $n = 2k + 1$, then

$$[n^2]_8 = [4k(k + 1) + 1]_8 = [1]_8.$$

The last equation holds due to $2|k(k + 1)$. ∎

2.12 Prove that there are no nonzero integers a, b, c such that $a^2 + b^2 = 3c^2$. (Hint: By studying the equation $[a]_4^2 + [b]_4^2 = 3[c]_4^2$ in $\mathbb{Z}/4\mathbb{Z}$, show that a, b, c would all have to be even. Letting $a = 2k$,$b = 2\ell$,$c = 2m$, you would have $k^2 + \ell^2 = 3m^2$. What's wrong with that?)

Notice $[0]_4^2 = [2]_4^2 = [0]_4, [1]_4^2 = [3]_4^2 = [1]_4$, if $a^2+b^2 = 3c^2$ has solution, then $[a]_4^2+[b]_4^2 = 3[c]_4^2$ has the same solution. So both hand of this equation will be $[0]_4$, i.e. a, b, c are even numbers. Letting $a = 2k$,$b = 2\ell$,$c = 2m$, we have

$$4k^2 + 4\ell^2 = 4(3m^2),$$

thus

$$k^2 + \ell^2 = 3m^2.$$

Now we can assume that k, ℓ, m are odd numbers or zeros otherwise repeat the procedure above to cancel the factor 2. Therefore, $[k]_4^2 + [\ell]_4^2$ could be $[0]_4, [1]_4, [2]_4$ while $3[m]_4^2$ could be $[0]_4, [3]_4$. The equation holds only if they are $[0]_4$. i.e. $k = \ell = m = 0$. This proves only zeros satisfy the equation $a^2 + b^2 = 3c^2$. ∎

2.13 ▷ Prove that if $\gcd(m, n) = 1$, then there exist integers a and b such that

$$am + bn = 1.$$

(Use Corollary 2.5.) Conversely, prove that if $am + bn = 1$ for some integers a and b, then $\gcd(m, n) = 1$. [2.15, §V.2.1, V.2.4]

If $\gcd(m, n) = 1$, then $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$, i.e.

$$\mathbb{Z}/n\mathbb{Z} = \{[m]_n, 2[m]_n, \cdots, (n - 1)[m]_n\}.$$

Thus, $\exists k \in \mathbb{N}$ such that

$$k[m]_n = [1]_n.$$

This is equivalent to $\exists a, b \in \mathbb{Z}$ such that

$$am + bn = 1.$$

Conversely, It is obvious that $1|\gcd(m, n)$. On the other hand, if $am + bn = 1$, then $\gcd(m, n)|1$. It proves that $\gcd(m, n) = 1$. ∎

2.14 ▷ State and prove an analog of Lemma 2.2, showing that the multiplication on $\mathbb{Z}/n\mathbb{Z}$ is a well-defined operation. [§2.3, §III.1.2]

Statement If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then $ab \equiv a'b' \mod n$.
Proof: since $a \equiv a' \mod n$ and $b \equiv b' \mod n$, there exist $k, l \in \mathbb{Z}$ such that

$$a = a' + kn, b = b' + ln.$$

Thus $ab = (a' + kn)(b' + ln) = a'b' + (a'l + kb' + kln)n$. It implies

$$[a]_n[b]_n = [ab]_n = [a'b']_n = [a']_n[b']_n.$$

i.e. the multiplication on $\mathbb{Z}/n\mathbb{Z}$ is well-defined. ∎

2.15 ¬ Let $n > 0$ be an odd integer.

- Prove that if $\gcd(m, n) = 1$, then $\gcd(2m + n, 2n) = 1$. (Use Exercise 2.13.)
- Prove that if $\gcd(r, 2n) = 1$, then $\gcd(\frac{r+n}{2}, n) = 1$. (Ditto.)
- Conclude that the function $[m]_n \to [2m + n]_{2n}$ is a bijection between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$.

The number $\phi(n)$ of elements of $(\mathbb{Z}/n\mathbb{Z})^*$ is Euler's $\phi(n)$-function. The reader has just proved that if n is odd, then $\phi(2n) = \phi(n)$. Much more general formulas will be given later on (cf. Exercise V.6.8). [VII.5.11]

- Suppose $d = \gcd(2m + n, 2n)$. Since $2m + n$ is an odd number and $d \mid (2m + n)$, $d \nmid 2$. Thus $d \mid n$, $d|m$. It implies $d \mid \gcd(m, n)$. Hence $d = 1$.
- If $\gcd(r, 2n) = 1$, then there exist $a, b \in \mathbb{Z}$ such that

$$ar + b(2n) = 1 \Rightarrow 2a\big(\frac{r+n}{2}\big) + (2b - a)n = 1 \Rightarrow \gcd\big(\frac{r+n}{2}, n\big) = 1.$$

- Let's consider $n > 1$ and n is odd. The function $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/2n\mathbb{Z})^*$ defined as

$$f([m]_n) = [2m + n]_{2n}$$

is well-defined. This is because if $[m_1]_n = [m_2]_n$, then

$$2(m_1 - m_2) = 2kn \Rightarrow (2m_1 + n) - (2m_2 + n) = 2kn \Rightarrow [2m_1 + n]_{2n} = [2m_2 + n]_{2n}.$$

By the previous results, f is a bijection.
It proves all results. ∎

2.16 Find the last digit of $1238237^{18238456}$. (Work in $\mathbb{Z}/10\mathbb{Z}$.)

$$[1238237^{18238456}]_{10} = [7^{18238456}]_{10} = [1^{4559614}]_{10} = [1]_{10}.$$

Thus the last digit of $1238237^{18238456}$ is 1. ∎

2.17 ▷ Show that if $m \equiv m' \mod n$, then $\gcd(m, n) = 1$ if and only if $\gcd(m', n) = 1$. [§2.3]

If $m \equiv m' \mod n$,then there is $k \in \mathbb{Z}$ such that $m = m' + kn$. Thus

$$\gcd(m, n) = 1 \iff \exists a, b \in \mathbb{Z} \text{ s.t. } am+bn = 1 \iff am'+(b+k)n = 1 \iff \gcd(m', n) = 1.$$

This proves the statement. ∎

2.18 For $d \leq n$, define an injective function $\mathbb{Z}/d\mathbb{Z} \to S_n$ preserving the operation, that is, such that the sum of equivalence classes in $\mathbb{Z}/d\mathbb{Z} \to S_n$ corresponds to the product of the corresponding permutations.

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & d & (d+1) & \cdots & n \\ d & 1 & 2 & \cdots & (d-1) & (d+1) & \cdots & n \end{pmatrix}$$

Let $f : \mathbb{Z}/d\mathbb{Z} \to S_n$ defined as

$$f([k]_d) = \sigma^d.$$

This map will preserve the operations. ∎

2.19 ▷ Both $(\mathbb{Z}/5\mathbb{Z})^*$ and $(\mathbb{Z}/12\mathbb{Z})^*$ consist of 4 elements. Write their multiplication tables, and prove that no re-ordering of the elements will make them match. (Cf. Exercise 1.6.) [§4.3]

$$(\mathbb{Z}/5\mathbb{Z})^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}.$$

Each non-unit element in $(\mathbb{Z}/5\mathbb{Z})^*$ could generate the entire group.

$$(\mathbb{Z}/12\mathbb{Z})^* = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}.$$

Each non-unit element in $(\mathbb{Z}/5\mathbb{Z})^*$ has order 2. There is no isomorphism between these two groups. ∎

§3. The category Grp

3.1 ▷ Let $\phi : G \to H$ be a morphism in a category C with products. Explain why there is a unique morphism $(\phi \times \phi) : G \times G \to H \times H$ compatible in the evident way with the natural projections. (This morphism is defined explicitly for $\mathsf{C} = \mathsf{Set}$ in §3.1.) [§3.1, 3.2]

■

3.2 Let $\varphi : G \to H, \psi : H \to K$ be morphisms in a category with products, and consider morphisms between the products $G \times G, H \times H, K \times K$ as in Exercise 3.1. Prove that

$$(\psi\varphi) \times (\psi\varphi) = (\psi \times \psi)(\varphi \times \varphi).$$

(This is part of the commutativity of the diagram displayed in §3.2.)

■

3.3 Show that if G, H are abelian groups, then $G \times H$ satisfies the universal property for coproducts in Ab.

Let's define the operation $*$ on $G \times H$ as the following:

$$(g_1, h_1) * (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

It is easy to verify that $(G \times H, *)$ is an abelian group.
Define the inclusion functions

$$\iota_G : G \to G \times H, \iota_G(g) = (g, e_H),$$

$$\iota_H : H \to G \times H, \iota_G(h) = (e_G, h).$$

It is not complicate to verify that both ι_G and ι_H are group homomorphisms.
For homomorphisms $\phi_G : G \to A$ and $\phi_H : H \to A$, we can define a set-function

$$\phi_{GH} : G \times H \to A, \phi_{GH}((g, h)) = \phi_G(g)\phi_H(h).$$

For $g \in G$,

$$(\iota_G \phi_{GH})(g) = \phi_{GH}(\iota_G(g)) = \phi_{GH}((g, e_H)) = \phi_G(g)\phi_H(e_H) = \phi_G(g).$$

For $h \in H$,

$$(\iota_H \phi_{GH})(h) = \phi_{GH}(\iota_H(h)) = \phi_{GH}((e_G, h)) = \phi_G(e_G)\phi_H(h) = \phi_H(h).$$

Now, we prove ϕ_{GH} is a group homomorphism. In fact, $\forall (g_1, h_1), (g_2, h_2) \in G \times H$

$$\begin{aligned}
\phi_{GH}((g_1, h_1) * (g_2, h_2)) &= \phi_{GH}((g_1 g_2, h_1 h_2)) \\
&= \phi_G(g_1 g_2)\phi_H(h_1 h_2) \\
&= (\phi_G(g_1)\phi_H(h_1))(\phi_G(g_2)\phi_H(h_2)) \\
&= \phi_{GH}((g_1, h_1))\phi_{GH}((g_2, h_2))
\end{aligned}$$

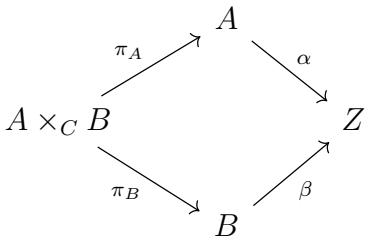
So, we have proved that $G \times H$ is the coproduct in Ab. ■

3.4 Let G, H be groups, and assume that $G \cong H \times G$. Can you conclude that H is trivial? (Hint: No. Can you construct a counterexample?)

■

3.9 Show that fiber products and coproducts exist in Ab. (Cf. Exercise I.5.12. For coproducts, you may have to wait until you know about *quotients*.)

Fiber product: For A, B, C in Ab, let's define the following product structure:



where

$$A \times_C B = \{(a, b) | \alpha(a) = \beta(b)\} \subset A \times B$$

and

$$\pi_A : A \times_C B \to A, \pi_A((a, b)) = a,$$
$$\pi_B : A \times_C B \to B, \pi_B((a, b)) = b.$$

It is not hard to prove:

- For $\forall (a_1, b_1) \in A \times_C B, (a_2, b_2) \in A \times_C B$, define operation $*$ as

$$(a_1, b_1) * (a_2, b_2) = (a_1 a_2, b_1 b_2).$$

  Equipped with $*$, $A \times_C B$ is an abelian group.

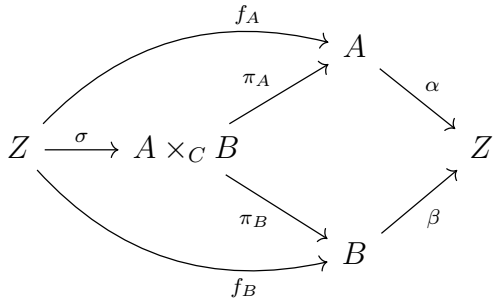
- It is obvious that $\pi_A : A \times_C B \to A$ and $\pi_B : A \times_C B \to B$ are group homomorphisms.

- By definition, $\forall (a, b) \in A \times_C B$,

$$(\alpha\pi_A)((a, b)) = \alpha(a) = \beta(b) = (\beta\pi_B)((a, b)).$$

$\forall Z$ in Ab and the group homomorphisms $f_A : Z \to A$, $\mathrm{f}_B : Z \to B$. If $\alpha f_A = \beta f_B$, then

we can define $\sigma : Z \to A \times_C B$ such that the following diagram commutative:



where $\sigma(z) = (f_A(z), f_B(z))$. It is not hard to prove that σ is a group homomorphism and $f_A = \pi_A\sigma, f_B = \pi_B\sigma$. It proves that $A \times_C B$ with the standard projections is the fibered product of the category Ab.

Fiber coproduct: For C, A, B in Ab and the homomorphisms $\alpha : C \to A, \beta : C \to B$, let's consider the subgroup $\ker(\alpha) \cap \ker(\beta) \subset C$ and the quotient group $C/\big(\ker(\alpha) \cap \ker(\beta)\big)$.

let's define the following structure:

$$A \amalg_C B = \begin{cases} (0, a), & \text{if } a \notin \alpha(C) \subset A \\ (1, b), & \text{if } b \notin \beta(C) \subset B \\ (0, a) \sim (1, b), & \text{if } a = \alpha(c), b = \beta(c). \end{cases}$$

i.e. in $A \amalg_C B$, $(0, a) = (1, b)$, if there is c such that $a = \alpha(c), b = \beta(c)$.

- Define an operation $*$ on $A \amalg_C B$ as the following:

■