Part I

Exercise solutions

Chapter I)

Section 1)

1.1)

In a nutshell, Russell's paradox proves, by contradiction, that certain mathematical collections cannot be sets. It posits the existence of a "set of all sets that don't contain themselves". Such a set can neither contain itself (since in that case, it would be a "set that does contain itself", and should be excluded); nor can it exclude it itself (since in that case, it would be a "set that doesn't contain itself", and should be included).

1.2)

Prove that any equivalence relation over a set S defines a partition of $\mathcal{P}_S$.

a) $\mathcal{P}_S$ has no empty elements: any element in S is part of at least one equivalence class, the class containing at least that element itself. Since there is no equivalence class constructed independently from elements, there are no empty equivalence classes.

b) Elements of $\mathcal{P}_S$ are disjoint: suppose there is an element x that is part of A and B, two distinct equivalence classes. $\forall a \in A, x \sim a$ and $\forall b \in B, x \sim b$. By transivity through x, $\forall a \in A, \forall b \in B, a \sim b$. Therefore, A and B are the same equivalence class: $A = B$. Contradiction. Therefore all elements of $\mathcal{P}_S$ are disjoint subsets of S.

c) The union of all elements of $\mathcal{P}_S$ makes up S: suppose $\exists x \in S$ such that $x \notin \bigcup_{S_i \in \mathcal{P}_S} S_i$. From the argument made in (a), x exists in at least one equivalence class, the class which contains only x itself. This is one of ou S_i sets. Contradiction. Therefore, $\bigcup_{S_i \in \mathcal{P}_S} S_i = S$

1.3)

Given a partition $\mathcal{P}$ on a set S, show how to define a relation $\sim$ on S such that P is the corresponding partition.

The insight here is to build an equivalence relation such that two elements are equivalent if and only if they are part of the same subset of S, which is understood as their common equivalence class.

We define $\sim$ such that $\forall S_i, S_j \in \mathcal{P}, \forall x \in S_i, \forall y \in S_j, x \sim y \Leftrightarrow S_i = S_j$.

Let us prove that $\sim$ is an equivalence relation.

a) Reflexivity:

$$\forall A \in \mathcal{P}, \forall x \in A, A = A \Rightarrow x \sim x$$

b) Symmetry:

$$\forall S_i, S_j \in \mathcal{P}, \forall x \in S_i, \forall y \in S_j, x \sim y \Leftrightarrow S_i = S_j \Leftrightarrow S_j = S_i \Leftrightarrow y \sim x$$

c) Transitivity:

$$\begin{aligned} \forall S_i, S_j, S_k \in \mathcal{P}, \forall x \in S_i, \forall y \in S_j, \forall z \in S_k, \\ (x \sim y) \cap (y \sim z) \\ \Leftrightarrow \\ (S_i = S_j) \cap (S_j = S_k) \\ \Rightarrow \\ S_i = S_k \\ \Leftrightarrow \\ x \sim z \end{aligned}$$

Therefore, $\sim$ is indeed an equivalence relation, and is generated uniquely by the partition.

1.4)

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

If we start with the 1 element set, we have only one possible partition, one possible equivalence class.

With the 2 element set, there are 2 partitions, $\{\{1, 2\}\}$ and $\{\{1\}, \{2\}\}$.

With the 3 element set, there is:

- 1 partition of type 1-1-1: $\{\{1\},\{2\},\{3\}\}$.
- 3 partitions of type 2-1: $\{\{1\},\{2,3\}\}$, $\{\{2\},\{1,3\}\}$, and $\{\{3\},\{1,2\}\}$.
- 1 partition of type 3: $\{\{1,2,3\}\}$.

Hence, there are five equivalence classes on the 3 element set.
See the Bell numbers: https://oeis.org/A000110

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?

Let's imagine a "similarity relation" we can notate with $\simeq$. We can imagine it to work like a looser version of equality (say for example, if an integer is only 1 away, then it counts as similar).

- reflexive: $\forall a \in S, a \simeq a$ (an element is always "similar" to itself)
- symmetric: $\forall a, b \in S, a \simeq b \Rightarrow b \simeq a$ ("similarity" goes both ways)
- not transitive: $\exists a, b, c \in S, (a \simeq b) \wedge (b \simeq c) \wedge \neg(a \simeq c)$ (just because $a \simeq b$ and $b \simeq c$ are similar, that doesn't mean $a \simeq c$ works, because it is possible for the "similarity gap" to be too large to qualify as "similar". E.g.: $(a, b, c) = (1, 2, 3)$.).

If we use this to define a partition P on some set S: $S/\simeq := P_{\simeq}$, there is ambiguity as to which element should go into which equivalence class.

This idea deserves further discussion.

In terms of graph theory, if we express a set with an internal relation as a graph, we can represent elements as nodes and relationships as edges. Reflexivity means that every node has a loop (unary, self-edge). Symmetry means that the graph is not directed (since every relationship goes both ways). Transitivity means that every connected subset of nodes is a maximal clique (synonymously, every connected component is a complete subgraph).

In a relation which is reflexive and symmetric, but not transitive, you would have connected components of this graph which are not cliques. For these, there is ambiguity as to how you would group their nodes. Two obvious choices would be either:

- to remove the minimal number of edges to obtain n distinct cliques (thereby gaining the *transitive restriction* of the relation) from a given non-clique; or

- to complete the connected subgraph into a clique (thereby gaining the *transitive closure* of the relation).

1.6)

Define a relation $\sim$ on the set $\mathbb{R}$ of real numbers, by setting $a \sim b \Leftrightarrow b-a \in \mathbb{Z}$. 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 $(a_1, a_2) \approx (b_1, b_2) \Leftrightarrow b_1 - a_1 \in \mathbb{Z}$ and $b_2 - a_2 \in \mathbb{Z}$.

TODO: forgot to prove that it's an equivalence relation

$b - a \in \mathbb{Z}$ means that 2 real numbers differ by an integral amount. This means that the equivalence relation algebraically describes the idea that "with this relation, 2 real numbers are the same iff they have the same fractional component x (or $1 - x$ for negative numbers)". Eg, $4.76 \sim 1024.76 \sim -5.34$, since $-5.34 + 10 = 4.76$, etc.

To make an algebraic quotient of a set by an equivalence relation, we take the function which maps each element to its corresponding equivalence class, in the set (partition) containing these equivalence class. Intuitively, this is similar to keeping only one representative element per equivalence class. For the example class above, we can keep the representative 0.76. There is such an equivalence class for every fractional part possible, that is, one for every number in $[0, 1[$. The corresponding map is the "real remainder of division modulo 1". This map is well-defined because each real number has only one output for this map, and all real numbers that are equivalent through $\sim$ are mapped to the same value in the output set.

We should also notice that since $0 \sim 1$, this space loops around on itself. Intuitively, if you increase linearly in the input space $\mathbb{R}$, it goes back to 0 after 0.9999999... in the output space. This output space is thus a circle of perimeter 1.

Similarly, $b_1 - a_1 \in \mathbb{Z}$ and $b_2 - a_2 \in \mathbb{Z}$ means that 2 points in the 2D plane are the same iff they differ in each coordinate by an integral amount. This boils down to combining two such loops from the first part of the exercise: one in the x direction and one in the y direction: what this gives is the small

square $[0,1[\times[0,1[$, which loops to $x=0$ (resp. $y=0$) when $x=1$ (resp. $y=1$) is reached. This space functions like a small torus, of area 1.

Section 2)

2.1)

How many different bijections are there between a set S with n elements and itself?

Any bijection is a choice of a pairs from 2 sets of the same size, where each element is used only once, and each pair has one element from each set. At first there are n choices in each set. We go through each possible input element in order (no choice), for each one, we pick one amongst n possibilities for an output.

There are then $(n-1)$ choice of output left, etc.

Ccl°: $\prod_{i=1}^{i=n} i = n!$

2.2)

Prove that a function has a right-inverse (pre-inverse) iff it is surjective (can use AC).

Let $f \in (A \to B)$.

2.2.a) $\Rightarrow$

Suppose that f has a right-inverse (pre-inverse). We have $\exists g \in (B \to A), f \circ g = id_B$

Suppose that f is not a surjection. This means $\exists b \in B, \nexists a \in A, b = f(a)$

$f(g(b)) = id_B(b) = b$ Necessarily, $g(b)$ is such an a, so $\exists a \in A, b = f(a)$. Contradiction.

Ccl°:: f is a surjection.

2.2.b) $\Leftarrow$

Suppose that f is a surjection.

$\forall b \in B, \exists a \in A, b = f(a)$

We will construct a pre-inverse for f.

The insight here is to realize that a surjection divides its input set into a partition, where each 2-by-2 disjoint subset corresponds to $f^{-1}(\{q\})$, for every q in the output set. More formally, each "fiber" (preimage of a singleton) is a disjoint subset of the input set, and the union of fibers is the input set itself. You can see this in the following diagram:

(add diagram) 1234 to ab 1a 2a (fiber from a) 3b 4b (fiber from b) https://tex.stackexchange.com/questions/157450/producing-a-diagram-showing-relations-between-sets https://tex.stackexchange.com/questions/79009/drawing-the-mapping-of-elements-for-sets-in-latex

Using AC, we select a single element from each such fiber. For each $q \in B$, we name $p_q \in f^{-1}(\{q\})$ the chosen element. We define g as $g \in (B \to A), g = (q \mapsto p_q)$. With this, $\forall b \in B, f \circ g(b) = b$, and so $f \circ g = id_A$. Thus, f has a preinverse.

A summary of this idea: all surjection preinverses are simply a choice of a representative for each fiber of the surjection as the output to the respective singleton.

2.3)

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

2.3.a)

Using the fact that a function is a bijection iff it has a two-sided inverse (Corollary 2.2) we can see from this defining fact, $f \in (A \to B)$ bijective $\Leftrightarrow$ $\exists f^{-1} \in (B \to A), (f^{-1} \circ f = id_A$ and $f \circ f^{-1} = id_B)$ that f is naturally f^{-1}'s (unique) two-sided inverse, and so f^{-1} is also a bijection.

2.3.b)

Let be $f \in (A \to B), g \in (B \to C)$, both bijective (hence with inverses in the respective function spaces). Let $h \in (A \to C), h = g \circ f$ and $h^{-1} \in (C \to A), h^{-1} = f^{-1} \circ g^{-1}$. We have:

$$
\begin{aligned}
h^{-1} \circ h &= (f^{-1} \circ g^{-1}) \circ (g \circ f) \\
&= f^{-1} \circ g^{-1} \circ g \circ f \\
&= f^{-1} \circ id_B \circ f \\
&= f^{-1} \circ f \\
&= id_A
\end{aligned}
$$

$$
\begin{aligned}
h \circ h^{-1} &= (g \circ f) \circ (f^{-1} \circ g^{-1}) \\
&= g \circ f \circ f^{-1} \circ g^{-1} \\
&= g \circ id_B \circ g^{-1} \\
&= g \circ g^{-1} \\
&= id_C
\end{aligned}
$$

Therefore h and h^{-1} are two-sided inverses of each other, and thus bijections. From this we conclude that the composition of any two bijections is also a bijection.

2.4)

Prove that 'isomorphism' is an equivalence relation (on any set of sets).

2.4.a) Problem statement

Let $\mathcal{A}$ be a set of sets. We define the relation $\simeq$ between the elements of $\mathcal{A}$ as the following:

$$\forall X, Y \in \mathcal{A},\ X \simeq Y \Leftrightarrow \text{there exists a bijection between } X \text{ and } Y$$

Let us show that $\simeq$ is an equivalence relation.

2.4.b) Reflexivity

For any set $A \in \mathcal{A}$, the identity mapping on A is a bijection. This means that $\forall A \in \mathcal{A}, A \simeq A$, ie, $\simeq$ is reflexive.

2.4.c) Symmetry

$$\begin{aligned}\forall X, Y \in \mathcal{A},\ X \simeq Y &\Rightarrow \exists f \in (X \to Y) \text{ bijective} \\ &\Rightarrow \exists f^{-1} \in (Y \to X) \text{ bijective} \\ &\Rightarrow Y \simeq X\end{aligned}$$

Therefore, $\simeq$ is symmetric.

2.4.d) Transitivity

Let be $X, Y, Z \in \mathcal{A}$. Suppose that $X \simeq Y$ and $Y \simeq Z$. This means $\exists f \in (X \to Y), g \in (Y \to Z)$, both bijections. Let be $h \in (X \to Z), h = g \circ f$. h is also a bijection since the composition of two bijections is also a bijection (exercise 2.3).

The existence of h implies $X \simeq Z$.

Therefore $\simeq$ is transitive.

2.4.e) Conclusion

Isomorphism, $\simeq$, is a relation on an arbitrary set (of sets) which is always reflexive, symmetric and transitive. It is thus an equivalence relation.

2.5)

Formulate a notion of epimorphism and prove that epimorphisms and surjections are equivalent.

See "notes" file: section "Proofs of mono/inj and epi/surj equivalence".

2.6)

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

A section is the preinverse of a surjection. Here, the surjection in question is π_A the projection of $A \times B$ onto A.

Let $f \in (A \to B)$.

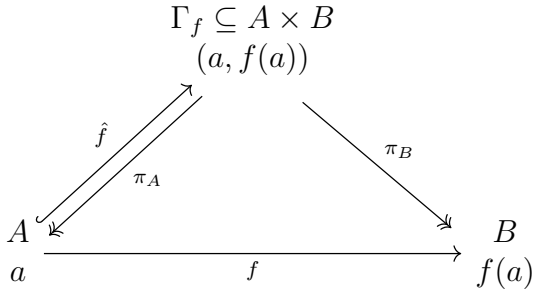
We now consider the function which maps an input $a \in A$ of f to its "geometric representation" (its coordinates in the enclosing space $A \times B$, corresponding to a point of the graph Γ_f).

$$\hat{f} \in (A \to (A \times B)), \hat{f} = (\ a \mapsto (a, f(a))\ )$$

We notice that $\hat{f}(A) = \Gamma_f$.

Naturally, $\pi_A \circ \hat{f} = (a \mapsto a) = id_A$, therefore, $\hat{f}$ is a pre-inverse (section) of π_A.

This set of relationships can be expressed in the following commutative diagram:



PS: see "On sections and fibers" in the "notes" file for a worked example.

2.7)

Let $f \in (A \to B)$ be any function. Prove that the graph Γ_f of f is isomorphic to A.

Using the elements from the previous exercise, we know that $\hat{f}$ is injective from A into $A \times B$. This property is inherited to any restriction of the codomain $Z \subseteq A \times B$, and corresponding implied restriction of the domain to $Y = \hat{f}^{-1}(Z) \subseteq A$. In particular, here, $Y = A$ and $Z = \Gamma_f = \hat{f}(A)$. We now consider $\overline{f} \in (A \to \Gamma_f), \overline{f} = (a \mapsto \hat{f}(a))$. We can see that $\overline{f}$ is injective from being a restriction of an injective function to a smaller codomain. We also know that $\overline{f}$ is surjective, since its domain is its image. Therefore, $\overline{f}$ is a bijection. This means that $A \simeq \Gamma_f$.

2.8)

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

Firstly, elements of $\mathbb{R}$ are equivalent by this map (they have the same output) if they vary by 1 from each other. This is a reference to the equivalence relation $\sim$ in exercise 1.6. Therefore, we will use $\mathbb{R}/\sim \simeq S^1$ in our decomposition. Obviously, the map from $(\mathbb{R} \to \mathbb{R}/\sim)$, which maps each el-

ement of $\mathbb{R}$ to respective their equivalence class is a surjection (since there's no empty equivalence class).

Secondly, as mentioned, we have a bijection $\tilde{f}$ between $\mathbb{R}/\sim$ and S^1, the circle group of unit complex numbers, namely $\tilde{f} = (x \mapsto e^{2\pi i x}$, where each element x of $\mathbb{R}/\sim$ can be understood to correspond to a (class representative) value in the interval $[0, 1[$.

Finally, we do the canonical injection of S^1 into its superset $\mathbb{C}$.

2.9)

Show that if $A \simeq A'$ and $B \simeq B'$, and further $A \cap B = \emptyset$ and $A' \cap B' = \emptyset$, then $A \cup B \simeq A' \cup B'$. Conclude that the operation $A \coprod B$ (as described in §1.4) is well-defined up to isomorphism.

We suppose the aforementioned.

Let f_A be a bijection from $A \to A'$, and f_B be a bijection from $B \to B'$.

We define the following:

$$f \in (A \cup B \to A' \cup B'), \text{ such that } \begin{cases} \forall a \in A,\ f(a) = f_A(a) \\ \forall b \in B,\ f(b) = f_B(b) \end{cases}$$

This function is a well-defined function, since $A \cap B = \emptyset$: every element of the domain has one, and only one, possible image.

Similarly, we define:

$$g \in (A' \cup B' \to A \cup B), \text{ such that } \begin{cases} \forall a \in A',\ g(a) = f_A^{-1}(a) \\ \forall b \in B',\ g(b) = f_B^{-1}(b) \end{cases}$$

Similarly, because $A' \cap B' = \emptyset$, g is well-defined.

Let us study $g \circ f$. We have:

$$\begin{cases} \forall a \in A,\ g(f(a)) = f_A^{-1}(f_A(a)) = a \\ \forall b \in B,\ g(f(b)) = f_B^{-1}(f_B(b)) = b \end{cases}$$

Hence, $g \circ f = id_{A \cup B}$. Similarly, $f \circ g = id_{A' \cup B'}$. Therefore, $g = f^{-1}$, f is a bijection, and $A \cup B \simeq A' \cup B'$.

We'll now do a shift in notation. Let be some arbitrary sets A and B. Let be A_1, A_2, B_1, B_2 such that $A_1 = \{1\} \times A$, $A_2 = \{2\} \times A$, $B_1 = \{1\} \times B$,

and $B_2 = \{2\} \times B$. This means $A \simeq A_1$, $A \simeq A_2$, $B \simeq B_1$, and $B \simeq B_2$. It also means $A_1 \cap A_2 = \emptyset$ and $B_1 \cap B_2 = \emptyset$. From the above, this implies $A_1 \cup B_1 \simeq A_2 \cup B_2$.

This means that the disjoint union of A and B is indeed well-defined, up to isomorphism: so long as 2 respective copies of A and B are made in a way that their intersection is empty, the 2 respective unions of 1 copy each will be isomorphic.

2.10)

Show that if A and B are finite sets, then $|B^A| = |B|^{|A|}$.

The number of $|B^A|$ functions in $B^A = (A \to B)$ can be counted in the following way.

For each element a of A, of which there are $|A|$, we can pick any element of B as the image; a total of $|B|$ choices per choice of a. This means $|B| \times ... \times |B|$, a total of $|A|$ times. Hence, $|B^A| = |B|^{|A|}$.

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 $\mathbb{B} = \{0, 1\}$). Prove that there is a bijection between 2^A and the power set $\mathcal{P}(A)$ of A.

Simply put, every subset A_i of A is built through a series of $|A|$ choices: for each element a in A, do we keep the element a in our subset A_i (output 1) or do we remove it (output 0) ? It is then easy to see that such a series of choices can easily be encoded as a unique function in $A \to \mathbb{B}$. The totality of such series of choices thus corresponds both to the space $A \to \mathbb{B}$, and to the powerset $\mathcal{P}(A)$, and there is a bijection between the two.

Section 3)

3.1)

Let $\mathcal{C}$ be a category. Consider a structure $\mathcal{C}^{op}$ with:

- $Obj(\mathcal{C}^{op}) \coloneqq Obj(\mathcal{C})$;
- for A, B objects of $\mathcal{C}^{op}$ (hence, objects of $\mathcal{C}$), $Hom_{\mathcal{C}^{op}}(A, B) \coloneqq Hom_{\mathcal{C}}(B, A)$

Show how to make this into a category.

3.1.a) Composition

First, to make things clearer and more rigorous, let us distinguish composition in $\mathcal{C}$ as $\circ$ and composition in $\mathcal{C}^{op}$ as $\star$. We define $\star$ as:

$$\begin{aligned}
&\forall f \in Hom_{\mathcal{C}^{op}}(B, A) = Hom_{\mathcal{C}}(A, B),\\
&\forall g \in Hom_{\mathcal{C}^{op}}(C, B) = Hom_{\mathcal{C}}(B, C),\\
&\exists h \in Hom_{\mathcal{C}^{op}}(C, A) = Hom_{\mathcal{C}}(A, C),\\
&f \star g \coloneqq g \circ f = h
\end{aligned}$$

We will now show that $\mathcal{C}^{op}$ with $\star$ verifies the other axioms of a category (namely identity and associativity of composition).

3.1.b) Identity

Since $\mathcal{C}$ is a category, since $\mathcal{C}^{op}$ has the same objects, and since, by definition, for all object A, we have $Hom_{\mathcal{C}^{op}}(A, A) = Hom_{\mathcal{C}}(A, A)$, we can take every $id_A \in Hom_{\mathcal{C}}(A, A)$ as the same identity in $\mathcal{C}^{op}$. We can verify that this is compatible with $\star$:

$$\begin{aligned}
\forall A, B \in Obj(\mathcal{C}) &= Obj(\mathcal{C}^{op}),\\
\exists id_A \in Hom_{\mathcal{C}}(A, A) &= Hom_{\mathcal{C}^{op}}(A, A),\\
\exists id_B \in Hom_{\mathcal{C}}(B, B) &= Hom_{\mathcal{C}^{op}}(B, B),\\
\forall f \in Hom_{\mathcal{C}}(A, B) &= Hom_{\mathcal{C}^{op}}(B, A),\\
f = f \circ id_A &= id_A \star f,\\
f = id_B \circ f &= f \star id_B
\end{aligned}$$

3.1.c) Associativity

Using associativity in $\mathcal{C}$, we have:

$$\begin{aligned}
\forall A, B, C, D \in Obj(\mathcal{C}) &= Obj(\mathcal{C}^{op}),\\
\forall f \in Hom_{\mathcal{C}}(A, B) &= Hom_{\mathcal{C}^{op}}(B, A),\\
\forall g \in Hom_{\mathcal{C}}(B, C) &= Hom_{\mathcal{C}^{op}}(C, B),\\
\forall h \in Hom_{\mathcal{C}}(C, D) &= Hom_{\mathcal{C}^{op}}(D, C),
\end{aligned}$$

$$\begin{aligned} h \star (g \star f) = & \quad h \star (f \circ g) \\ = & \quad (f \circ g) \circ h \\ = & \quad f \circ (g \circ h) \\ = & \quad (g \circ h) \star f \\ = & \quad (h \star g) \star f \end{aligned}$$

Therefore, $\star$ is associative.

We conclude that $\mathcal{C}^{op}$ is a category.

3.2)

If A is a finite set, how large is $End_{\text{Set}}(A)$?

We know that, in Set, $End_{\text{Set}}(A) = (A \to A) = A^A$. From a previous exercise, we know that $|B^A| = |B|^{|A|}$, therefore $|End_{\text{Set}}(A)| = |A|^{|A|}$.

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.

Example 3.3 is that of a category over a set S with a (reflexive, transitive) relation $\sim$, where the objects of the category are the elements of S, and the homset between two elements a and b is the singleton (a, b) if $a \sim b$, and $\emptyset$ otherwise. Composition $\circ$ is given by transitivity of $\sim$, where $(b, c) \circ (a, b) = (a, c)$. Reflexivity gives the identities ($id_a = (a, a)$ for any element a).

In this context, to say that "1_a is an identity with respect to composition" means that we can cancel out an element of the form (a, a) from a composition.

Formally, we have:

$$\forall a, b \in S, (b, b) \circ (a, b) = (a, b) = (a, b) \circ (a, a)$$

proving that (b, b) is indeed a post-identity, and (a, a) a pre-identity, in this context.

3.4)

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

(Description of example 3.3 in the exercise 3.3 just above.)

Naively, saying like in example 3.3 "there is a singleton homset $\mathrm{Hom}(a, b)$ each time we have $a < b$", we cannot define such a category, since $<$ is not reflexive, and we would thus lack identity morphisms.

However, in a roundabout way, we can define a category over the *negation* of $<$: "there is a singleton homset $\mathrm{Hom}(a, b)$ each time we DO NOT have $a < b$". Namely this corresponds to the relation $\geq$, which is, itself, reflexive, transitive (and antisymmetric), and is a valid instance of the kind of category presented in example 3.3.

In fact, the pair $(\mathbb{Z}, \geq)$ is an instance of what is called a "totally ordered set", which is a more restrictive kind of "partially ordered set" (also called "poset" for short). Consequently, this kind of category is called a "poset category".

3.5)

Explain in what sense Example 3.4 is an instance of the categories considered in Example 3.3.

(Description of example 3.3 in the exercise 3.3 just above.)

Example 3.4 describes a category $\hat{S}$ where the objects are the subsets of a set S (equivalently: elements of the powerset $\mathcal{P}(S)$ of S), and morphisms between two subsets A and B of S are singleton (or empty) homsets based on whether the inclusion is true (or false).

Inclusion of sets, $\subset$, is also an order relation, this time between the elements of a set of sets (here, $\mathcal{P}(S)$). This means inclusion is reflexive, transitive, and antisymmetric. This makes $\hat{S}$ a poset category, and thus another instance of example 3.3.

3.6)

Define a category V by taking $Obj(V) = \mathbb{N}$, and $Hom_V(n, m) = Mat_{\mathbb{R}}(m, n)$, the set of $m \times n$ matrices with real entries, for all $n, m \in \mathbb{N}$. (I will leave the reader the task to make sense of a matrix with 0 rows or columns.) Use product of matrices to define composition. Does this category 'feel' familiar ?

The formulation of the exercise is strange. It says to use the product of matrices to define composition, and to have homsets be sets of matrices,

but objects of the category are supposed to be integers. I don't know of any matrix with real entries that maps an integer to an integer in this way.

We thus infer that the meaning of the exercise can be one of two things.

Either we suppose the set of objects could rather be understood as "something isomorphic to $\mathbb{N}$", ie, the collection of real vector spaces with finite bases (ie, $\forall n \in \mathbb{N}, \mathbb{R}^n$). In which case, this is just the category of real vector spaces with finite basis (and linear maps as morphisms), which is a subcategory of the category real vector spaces (commonly called $Vect_{\mathbb{R}}$). In this context, any morphism starting from $0 \simeq \mathbb{R}^0 = \{0\}$ is just the injection of the origin into the codomain; and any morphism ending at 0 is the mapping of all elements to the origin.

Otherwise, we understand this as "yes, the objects of the category are integers: this means you should ignore the actual content of the matrices, and instead consider only their effect on the dimensionality of domains and codomains". In this case, this category is a complete directed graph over $\mathbb{N}$ where each edge corresponds to the change in dimension (from domain to codomain) caused by a given linear map.

3.7)

Define carefully objects and morphisms in Example 3.7, and draw the diagram corresponding to composition.

Example 3.7 (on coslice categories) refers to example 3.5 (on slice categories). Let's go over slice categories (since example 3.5 asks the reader to "check all [their various properties]").

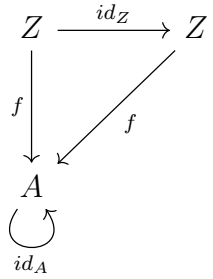
3.7.1) Slice categories

Slice categories are categories made by singling out an object (say A) in some parent (larger) category (say $\mathcal{C}$), and studying all morphisms into that object. These morphisms become the objects of a new category (ie, for any Z of $\mathcal{C}$, $f \in (Z \to A)$ is an object of the slice category, called $\mathcal{C}_A$ in this context). In the slice category, morphisms are defined as those morphism in $\mathcal{C}$ that preserve composition between 2 morphisms into A.

Note that there exist pairs of morphisms $f_1 \in (Z_1 \to A)$ and $f_2 \in (Z_2 \to A)$ between which there is no morphism that exists in the slice category. One such example we can make is in $(Vect_{\mathbb{R}})_{\mathbb{R}^2}$ (see notes "On the morphisms of slice and coslice categories" for more details).

3.7.1.a) Identity

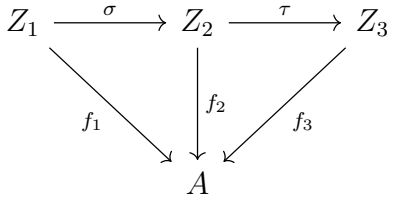
A generic identity morphism is expressed diagrammatically in $\mathcal{C}_A$ as:



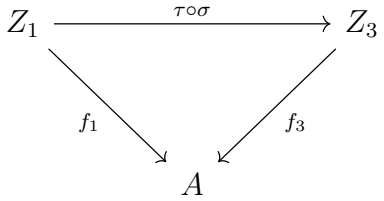
We can see that since $f = f \circ id_Z$ in $\mathcal{C}$, this is compatible with the definition of a (pre-/right-)unit morphism in $\mathcal{C}_A$. Also, since the only maps post-f are maps from $A \to A$, we have id_A as the (post-/left-)unit for every morphism f (ie, $f = id_A \circ f$.

3.7.1.b) Composition

Taking 3 objects of the slice category ($f_1 \in (Z_1 \to A)$, $f_2 \in (Z_2 \to A)$ and $f_3 \in (Z_3 \to A)$), and two morphisms (σ_A mapping f_1 to f_2 via a $\mathcal{C}$-morphism $\sigma \in (Z_1 \to Z_2)$, and τ_A mapping f_2 to f_3 via a $\mathcal{C}$-morphism $\tau \in (Z_2 \to Z_3)$), we have that $f_1 = f_2 \circ \sigma$ and $f_2 = f_3 \circ \tau$. This is expressed as the following commutative diagram.



Composition of morphisms is then defined as $\tau_A \circ_A \sigma_A$ as a mapping from f_1 to f_3, such that $f_1 = f_3 \circ (\tau \circ \sigma)$. This can be understood through the following commutative diagram:



Which commutes, because we have:

$$\begin{aligned} f_1 &= f_2 \circ \sigma \\ &= (f_3 \circ \tau) \circ \sigma \\ &= f_3 \circ (\tau \circ \sigma) \end{aligned}$$

Thus, we have a working composition of morphisms.

3.7.1.c) Associativity

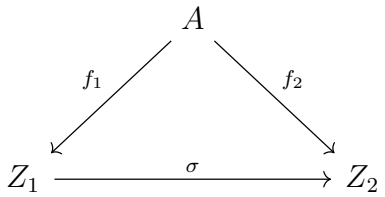
We take 4 objects of the slice category ($f_1 \in (Z_1 \to A)$, $f_2 \in (Z_2 \to A)$, $f_3 \in (Z_3 \to A)$ and $f_4 \in (Z_4 \to A)$), and three morphisms (σ_A mapping f_1 to f_2, τ_A mapping f_2 to f_3, and υ_A mapping f_3 to f_4). Using composition defined as above, we have

$$\begin{aligned} f_1 = \;& f_4 \circ (\upsilon \circ (\tau \circ \sigma)) \\ = \;& f_4 \circ ((\upsilon \circ \tau) \circ \sigma) \\ \Rightarrow & \\ & \upsilon_A \circ (\tau_A \circ \sigma_A) \\ = \;& (\upsilon_A \circ \tau_A) \circ \sigma_A \end{aligned}$$

Through associativity in $\mathcal{C}$.

3.7.2) Coslice categories

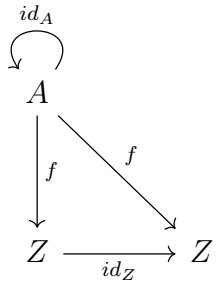
A coslice category $\mathcal{C}^A$ is similar, except it takes the morphisms coming *from* a chosen object A, rather than those going *to* this object A. Below is a commutative diagram in the style of the one of the textbook for slice categories.



We can similarly show that this also defines a category.

3.7.2.a) Identity

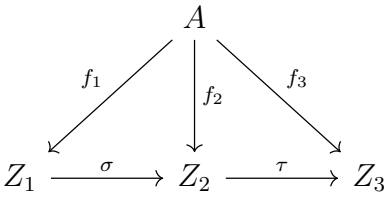
A generic identity morphism is expressed diagrammatically in $\mathcal{C}^A$ as:



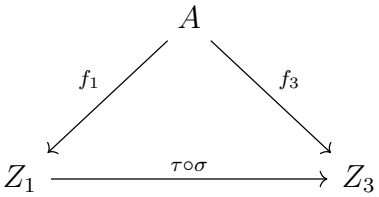
We can see that since $f = id_Z \circ f$ in $\mathcal{C}$, this is compatible with the definition of a (post-/left-)unit morphism in $\mathcal{C}^A$. Also, since the only maps pre-f are maps from $A \to A$, we have id_A as the (pre-/right-)unit for every morphism f (ie, $f = f \circ id_A$.

3.7.2.b) Composition

Taking 3 objects of the slice category ($f_1 \in (A \to Z_1)$, $f_2 \in (A \to Z_2)$ and $f_3 \in (A \to Z_3)$), and two morphisms (σ^A mapping f_1 to f_2 via a $\mathcal{C}$-morphism $\sigma \in (Z_1 \to Z_2)$, and τ^A mapping f_2 to f_3 via a $\mathcal{C}$-morphism $\tau \in (Z_2 \to Z_3)$), we have that $f_1 = \sigma \circ f_2$ and $f_2 = \tau \circ f_3$. This is expressed as the following commutative diagram.



Composition of morphisms is then defined as $\tau^A \circ^A \sigma^A$ as a mapping from f_1 to f_3, such that $f_3 = (\tau \circ \sigma) \circ f_1$. This can be understood through the following commutative diagram:



Which commutes, because we have:

$$\begin{aligned} f_3 &= \tau \circ f_2 \\ &= \tau \circ (\sigma \circ f_1) \\ &= (\tau \circ \sigma) \circ f_1 \end{aligned}$$

Thus, we have a working composition of morphisms.

3.7.2.c) Associativity

We take 4 objects of the slice category ($f_1 \in (A \to Z_1)$, $f_2 \in (A \to Z_2)$, $f_3 \in (A \to Z_3)$ and $f_4 \in (A \to Z_4)$), and three morphisms (σ^A mapping f_1 to f_2, τ^A mapping f_2 to f_3, and υ^A mapping f_3 to f_4). Using composition defined as above, we have

$$
\begin{aligned}
f_4 = &\quad (\upsilon \circ (\tau \circ \sigma)) \circ f_1 \\
= &\quad ((\upsilon \circ \tau) \circ \sigma) \circ f_1 \\
\Rightarrow & \\
&\quad \upsilon^A \circ (\tau^A \circ \sigma^A) \\
= &\quad (\upsilon^A \circ \tau^A) \circ \sigma^A
\end{aligned}
$$

Through associativity in $\mathcal{C}$.

3.8)

A subcategory $\mathcal{C}'$ of a category $\mathcal{C}$ consists of a collection of objects of $\mathcal{C}$, with morphisms $Hom_{\mathcal{C}'}(A, B) \subseteq Hom_{\mathcal{C}}(A, B)$ for all objects A, B in $Obj(\mathcal{C}')$, such that identities and compositions in $\mathcal{C}$ make $\mathcal{C}'$ into a category. A subcategory $\mathcal{C}'$ is *full* if $Hom_{\mathcal{C}'}(A, B) = Hom_{\mathcal{C}}(A, B)$ for all A, B in $Obj(\mathcal{C}')$. Construct a category of *infinite sets* and explain how it may be viewed as a full subcategory of **Set**.

To put it less technically, a "subcategory" $\mathcal{C}'$ is just "picking only certain items of a base category $\mathcal{C}$, and making sure that things stay closed uneder morphism composition". It is "full" if *all* morphisms between the objects that remain are also conserved.

We can construct a category **InfSet** of infinite sets by taking all the objects A of **Set** such that $\nexists n \in \mathbb{N}, |A| = n$, and only homsets between these objects. This is clearly a subcategory of **Set**, since it inherits all identity morphisms, composition works the same, and so does associativity; also, restricting the choice of homsets makes it so that the category is closed (you can't reach a finite set via a homset that went from an infinite to a finite set).

For this category to not be full, there would need to be some homset that loses a morphism, or fully disappears, in the ordeal. However, there is no restriction as to the kind of morphism that is conserved, so any homset that is kept is identical to its original version. Finally, homsets between infinite sets are also infinite sets, so they don't disappear in this operation.

Consequently **InfSet** defined as such 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 instances 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 notions 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 us recall how multisets were defined in §2.2. Since duplicate elements do not exist in sets, multisets were instead defined as functions from a set S to $\mathbb{N}*$, the set of (nonzero) positive integers. This allows each element in S to have a "count", thereby encoding the intuitive notion of multiset. A similar, and equivalent (isomorphic), way of defining it is *via* pairs $(s, n) \in S \times \mathbb{N}*$, which is simpler to think about. We'll call this category **CMSet**, for "count multiset" (TODO: probably has a conventional and better name, but I don't know it). As for morphisms in **CMSet**, we can consider that for any multisets $A = S_A \times \mathbb{N}*$ and $B = S_B \times \mathbb{N}*$, the homset from A to B is simply the set functions from $S_A \times \mathbb{N}*$ to $S_B \times \mathbb{N}*$ as usual.

We first notice that if we restrict **CMSet** to only the objects for which all elements have a count of 1, and where morphisms only ever output to $\{1\}$ in the second coordinate (a subcategory we can call **C1MSet**, for example), we get a "copy" of **Set**: **C1MSet** and **Set** are isomorphic in **Cat**. This is a full subcategory because there are no morphisms that map counts to anything else than $\{1\}$ if we restrict our objects to this form; so all morphisms between the kept objects are also kept.

Now let us do a similar construction, but based on equivalence classes instead. We know that each equivalence class over a set corresponds uniquely to a partition of that set. By considering only these partitions (these "sets of sets") as objects, we can build a category **EMSet** (for "equivalence multiset"). The "count" corresponds simply to the cardinal of a top-level element in the partition. For example, the top-level elements of $M = \{S_1, S_2, S_3\} = \{\{a\}, \{b, c\}, \{d, e, f\}\}$ would be understood to have counts $|S_1| = 1$, $|S_2| = 2$

and $|S_3| = 3$ respectively.

As for morphisms in **EMSet**, they simply map each top-level element of the domain multiset (a distinct subset of the original set) to some other top-level elements in the codomain multiset. This has precisely the same effect as mapping pairs of "value and count" as seen in the previous **CMSet** construction.

In this example, any set itself, when "injected" (by a functor) into **EMSet** would just nest all of its elements into singletons. I.e., $S = \{a, b, c\}$ in **Set** would become $S = \{\{a\}, \{b\}, \{c\}\}$ in **EMSet**. This also shows how restricting **EMSet** to "only objects that are a set of (toplevel) singletons" makes **EMSet** have a "copy" of **Set** as a full subcategory (for similar arguments as above).

Yet another example could be something akin to polynomials with integer coefficients on freeform indeterminates of degree 1 (which would be our set elements); raising the operators one rank, a product of freeform variables with integer powers (multiplicities), etc.

3.10)

Since the objects of a category $\mathcal{C}$ 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 $\mathcal{C}$ are in one-to-one correspondence with the morphisms $A \to \Omega$ for a fixed, special object Ω of $\mathcal{C}$, called a subobject classifier. Show that **Set** has a subobject classifier.

We define the set $\mathbb{B} = \{0, 1\}$, aka the binary alphabet or booleans, as the subobject classifier of **Set**. For any subset A of B, there is a unique map $f : B \to \mathbb{B}$, such that $\forall b \in B, f(b) = 1 \Leftrightarrow b \in A$ (otherwise $f(b) = 0$, of course, as the equivalence and lack of alternatives to 0 as an output imply). The map f always fully describes A from its relationship with B.

3.11)

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

For lack of a better term, we will refer to the categories of the form $\mathcal{C}_{A,B}$ represented by Example 3.9 as "bi-slice categories". The first part of the

exercise is thus asking us to define and explain what "bi-coslice categories" (of the form $\mathcal{C}^{A,B}$) are.

Similarly, we will refer to the categories of the form $\mathcal{C}_{\alpha,\beta}$ represented by Example 3.10 as "fibered bi-slice categories". The second part of the exercise is thus asking us to define and explain what "fibered bi-coslice categories" (of the form $\mathcal{C}^{\alpha,\beta}$) are.

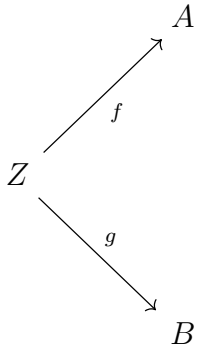
We will, of course, attempt to make more formal and pedagogical all definitions broached in the textbook's examples as well.

3.11.1) Bi-slice categories

3.11.1.a) Objects and morphisms

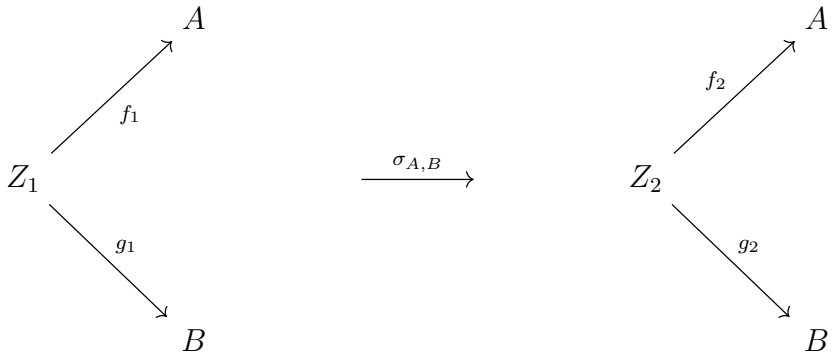
To make a bi-slice category $\mathcal{C}_{A,B}$, we pick 2 objects A and B of a base category $\mathcal{C}$, and consider for all other objects Z of $\mathcal{C}$, all pairs of morphisms $(f, g) \in (Z \to A) \times (Z \to B)$. These pairs of morphisms are the objects of the bi-slice category $\mathcal{C}_{A,B}$. Morphisms $\sigma_{A,B}$ are defined from an object $p_1 = (f_1, g_1) \in (Z_1 \to A) \times (Z_1 \to B)$ to an object $p_2 = (f_2, g_2) \in (Z_2 \to A) \times (Z_2 \to B)$ so that we have both $f_1 = f_2 \circ \sigma$ and $g_1 = g_2 \circ \sigma$, for some $\sigma \in (Z_1 \to Z_2)$.

A generic object in $\mathcal{C}_{A,B}$ is of the form:

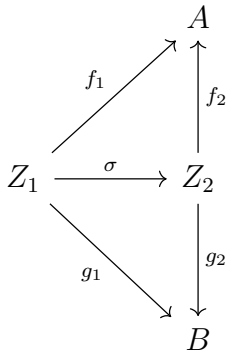


3.11.1.b) Morphisms

Morphisms are defined between objects as



such that the following diagram commutes



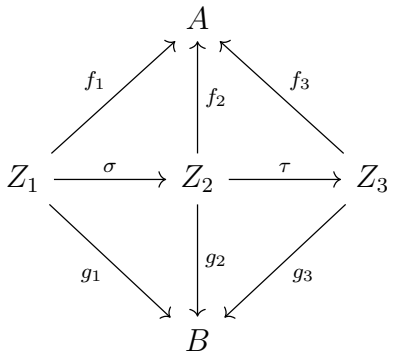
3.11.1.c) Identity

It is clear that identity morphisms exist for all objects, simply by taking $Z = Z_1 = Z_2$, $f_1 = f_2$, $g_1 = g_2$ and $\sigma = id_Z$, in the diagram above.

3.11.1.d) Composition

Let be 3 objects of $\mathcal{C}_{A,B}$, which we will name p_1, p_2 and p_3 (and define with the respective (Z_n, f_n, g_n) triplet for p_n).

Composition $\tau_{A,B} \circ \sigma_{A,B} = p_1 \mapsto p_3$ of two morphisms $\sigma_{A,B} = p_1 \mapsto p_2$ and $\tau_{A,B} = p_2 \mapsto p_3$ is defined so that the following diagram commutes.



3.11.1.e) Associativity

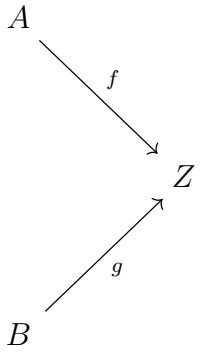
Associativity follows from associativity of morphisms in $\mathcal{C}$, similarly to what was done for slice categories in exercise 3.7 .

3.11.2) Bi-coslice categories

3.11.2.a) Objects and morphisms

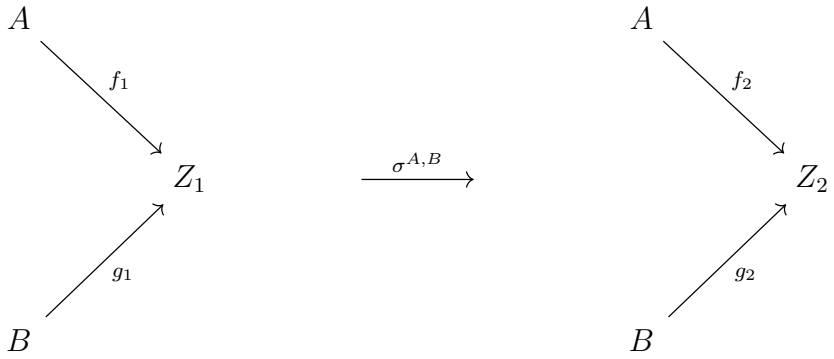
To make a bi-coslice category $\mathcal{C}^{A,B}$, we similarly pick 2 objects A and B of our base category $\mathcal{C}$, but instead consider, for all other objects Z of $\mathcal{C}$, all pairs of morphisms $(f, g) \in (A \to Z) \times (B \to Z)$.

A generic object in $\mathcal{C}^{A,B}$ is of the form:

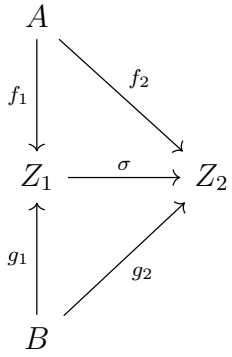


3.11.2.b) Morphisms

Morphisms are defined between objects as



such that the following diagram commutes



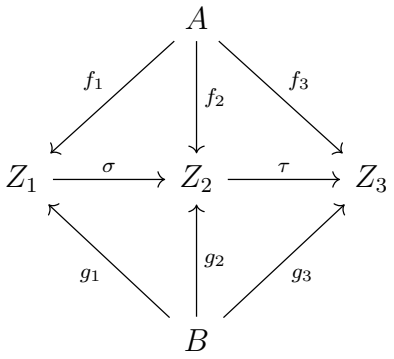
3.11.2.c) Identity

It is clear that identity morphisms exist for all objects, simply by taking $Z = Z_1 = Z_2$, $f_1 = f_2$, $g_1 = g_2$ and $\sigma = id_Z$, in the diagram above.

3.11.2.d) Composition

Let be 3 objects of $\mathcal{C}^{A,B}$, which we will name p_1, p_2 and p_3 (and define with the respective (Z_n, f_n, g_n) triplet for p_n).

Composition $\tau^{A,B} \circ \sigma^{A,B} = p_1 \mapsto p_3$ of two morphisms $\sigma^{A,B} = p_1 \mapsto p_2$ and $\tau^{A,B} = p_2 \mapsto p_3$ is defined so that the following diagram commutes.



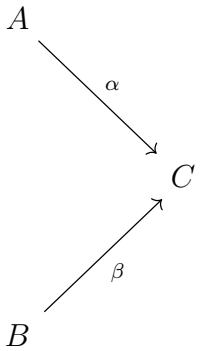
3.11.2.e) Associativity

Associativity follows from associativity of morphisms in $\mathcal{C}$, similarly to what was done for slice categories in exercise 3.7 .

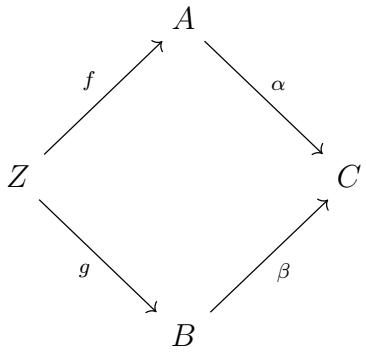
3.11.3) Fibered bi-slice categories

3.11.3.a) Objects

To build a fibered bi-slice category $\mathcal{C}_{\alpha,\beta}$, one takes a base category $\mathcal{C}$, as well as a fixed pair of morphisms $\alpha : A \to C$ and $\beta : B \to C$ in $\mathcal{C}$, that point to a common object C of $\mathcal{C}$. Our basic "fixed construct" from $\mathcal{C}$ looks like so:



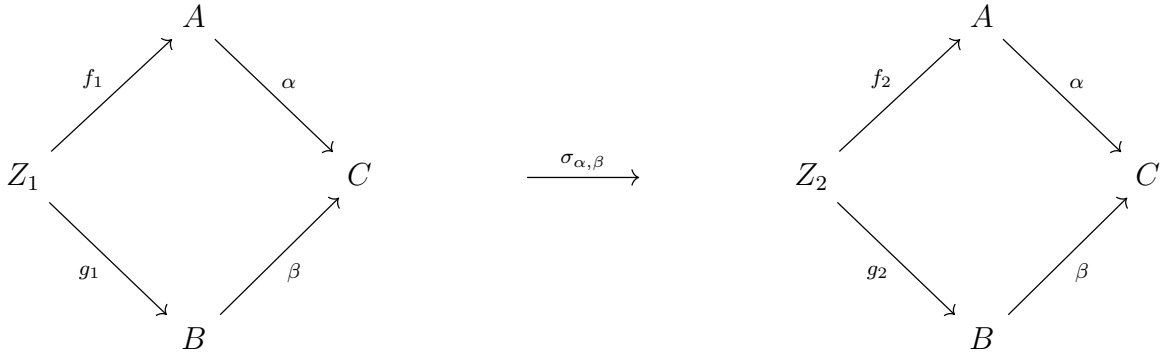
The role of the category $\mathcal{C}_{\alpha,\beta}$ is now to study the morphisms into this construct. A generic object from this new category looks like so:



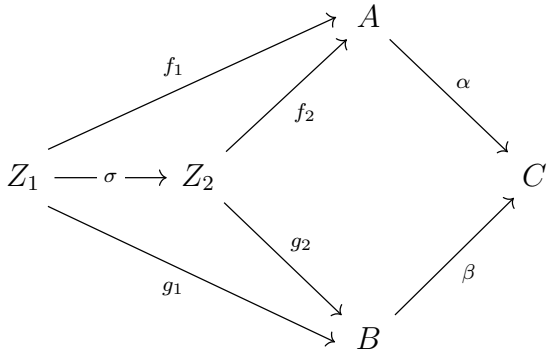
such that the diagram commutes. This means that valid object in $\mathcal{C}_{\alpha,\beta}$ are triplets (Z, f, g), with $f : Z \to A$ and $g : Z \to B$, such that $\alpha \circ f = \beta \circ g$. In a caricatural way, this boils down to studying "the comparison of the different paths one can use to reach C, knowing that the last steps are on one hand, α, and on the other, β".

3.11.3.b) Morphisms

Morphisms are defined between objects as:



such that the following diagram commutes



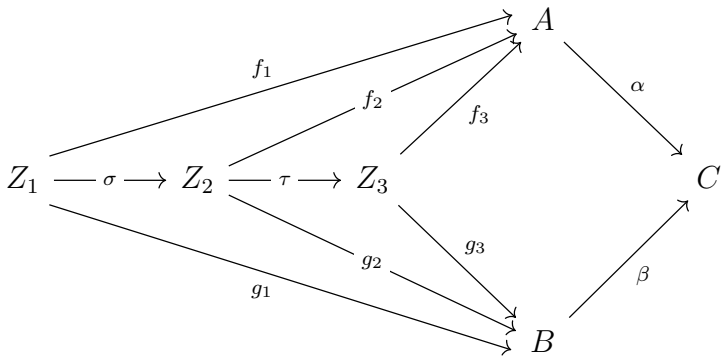
3.11.3.c) Identity

Once again, it is clear that identity morphisms exist for all objects, simply by taking $Z = Z_1 = Z_2$, $f_1 = f_2$, $g_1 = g_2$ and $\sigma = id_Z$, in the diagram above.

3.11.3.d) Composition

Let be 3 objects of $\mathcal{C}_{\alpha,\beta}$, which we will name p_1, p_2 and p_3 (and define with the respective (Z_n, f_n, g_n) triplet for p_n).

Composition $\tau_{\alpha,\beta} \circ \sigma_{\alpha,\beta} = p_1 \mapsto p_3$ of two morphisms $\sigma_{\alpha,\beta} = p_1 \mapsto p_2$ and $\tau_{\alpha,\beta} = p_2 \mapsto p_3$ is defined so that the following diagram commutes.



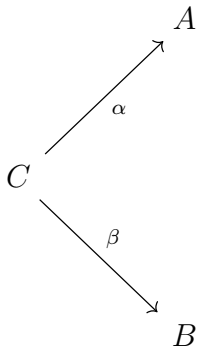
3.11.3.e) Associativity

Associativity follows from associativity of morphisms in $\mathcal{C}$, similarly to what was done for slice categories in exercise 3.7 .

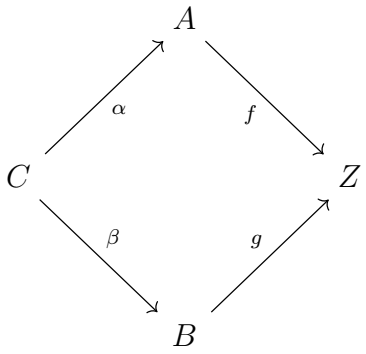
3.11.4) Fibered bi-coslice categories

3.11.4.a) Objects

To build a fibered bi-coslice category $\mathcal{C}^{\alpha,\beta}$, one takes a base category $\mathcal{C}$, as well as a fixed pair of morphisms $\alpha : C \to A$ and $\beta : C \to B$ in $\mathcal{C}$, that originate from a common object C of $\mathcal{C}$. Our basic "fixed construct" from $\mathcal{C}$ looks like so:



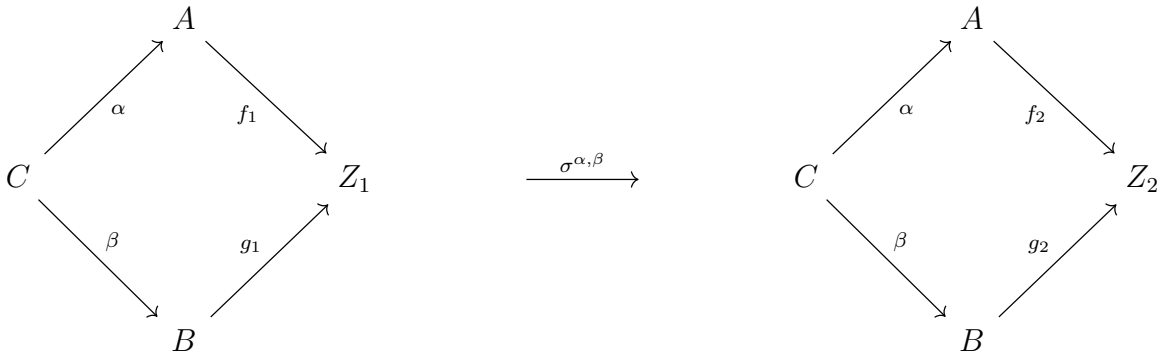
The role of the category $\mathcal{C}^{\alpha,\beta}$ is now to study the morphisms from this construct. A generic object from this new category looks like so:



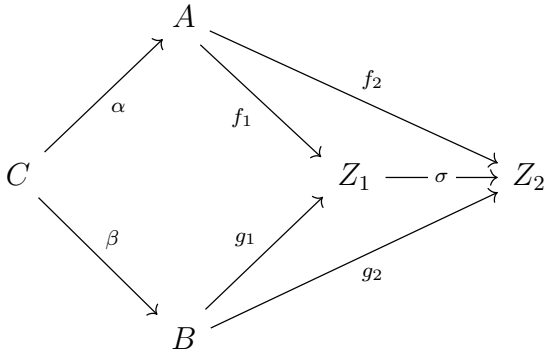
such that the diagram commutes. This means that valid object in $\mathcal{C}^{\alpha,\beta}$ are triplets (Z, f, g), with $f : A \to Z$ and $g : B \to Z$, such that $f \circ \alpha = g \circ \beta$. In a caricatural way, this boils down to studying "the comparison of the different paths one can build by starting from C, knowing that the choice of first step is on one hand, α, and on the other, β".

3.11.4.b) Morphisms

Morphisms are defined between objects as:



such that the following diagram commutes



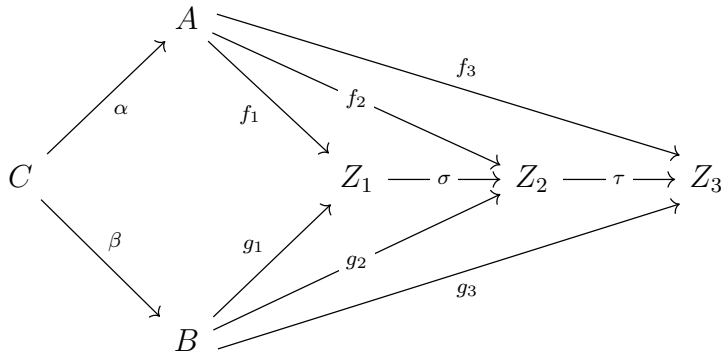
3.11.4.c) Identity

Once again, it is clear that identity morphisms exist for all objects, simply by taking $Z = Z_1 = Z_2$, $f_1 = f_2$, $g_1 = g_2$ and $\sigma = id_Z$, in the diagram above.

3.11.4.d) Composition

Let be 3 objects of $\mathcal{C}^{\alpha,\beta}$, which we will name p_1, p_2 and p_3 (and define with the respective (Z_n, f_n, g_n) triplet for p_n).

Composition $\tau^{\alpha,\beta} \circ \sigma^{\alpha,\beta} = p_1 \mapsto p_3$ of two morphisms $\sigma^{\alpha,\beta} = p_1 \mapsto p_2$ and $\tau^{\alpha,\beta} = p_2 \mapsto p_3$ is defined so that the following diagram commutes.



3.11.4.e) Associativity

Associativity follows from associativity of morphisms in $\mathcal{C}$, similarly to what was done for slice categories in exercise 3.7 .

Section 4)

4.1)

Composition is defined for *two* morphisms. If more than 2 morphisms are given, one may compose them in several ways, so that every step only consists in composing 2 morphisms. Prove that for any such valid sequence of morphisms, the order of parentheses doesn't matter.

This boils down to showing that associativity is a global property, that doesn't just make parentheses meaningless when there are 3 elements and 2 operators between them, but in general n elements with $(n-1)$ operators between them.

Note: A useful way of visualizing this is representing the order of operations as a binary tree, and noticing that applying associativity (forwards or backwards) is just a tree rotation (resp. right or left) at a given node. Then it is easy to show that one can always obtain a "left comb binary tree". Since every choice of parentheses is equal to this left comb choice, and equality is transitive, every choice of parentheses is equal to every other choice.

To be more rigorous, we will proceed by induction.

Hypothesis: $P(n) =$ "for a given n, for $f_n f_{n-1} \cdot f_1$ any valid, composable, ordered sequence of morphisms in our base category $\mathcal{C}$, any choice H of parentheses to compose elements of this sequence 2-by-2, giving a formula

s_H, will lead to the same result, which can be seen by always having $s_H = (\cdot(f_n f_{n-1})\cdot)f_1$".

Initialization: We initialize at $n = 3$; the validity is immediate as it is precisely the definition of associativity.

Heredity: We suppose the hypothesis $P(n)$ true for a given $n \geq 3$; let us show that this implies that the hypothesis is true for $P(n+1)$.

What this means is that, no matter the composable ordered sequence $f_n f_{n-1} \cdot f_1$ of n functions, for a fixed n, the order of parentheses does not matter. Note that though n is chosen and fixed; the statement is true for EVERY (ordered, composable) sequence of functions. We add a new function g to this sequence. By a simple renaming of the functions, we deduce that it doesn't matter where we insert g, so we'll insert it at the very right to simplify our argument, giving us the sequence $f_n f_{n-1} \cdot f_1 g$.

Here, there are 3 cases. Either:

- g is part of the last composition (i.e., it's not in a semantically necessary parenthethical grouping; it can be made external to all parentheses),
- g is part of the first composition (i.e., the first operation is $(f_1 g)$)
- it isn't either (it's inside some non-removable parentheses, and needs to be composed earlier on, but not as the first operation).

If g is part of the last composition, then by applying the hypothesis $P(n)$ to the terms $f_n f_{n-1} \cdot f_1$, we immediately find that our new sequence can be made equal to $((\cdot(f_n f_{n-1})\cdot)f_1)g$, which is precisely what we wanted for $P(n+1)$.

If g is part of the first composition, we isolate it so that it isn't anymore. To do so, we apply "backwards" associativity on the grouping of terms $F_k(f_1 g)$ in order to obtain $(F_k f_1)g$, where F_k is the appropriate choice of $(f_k \cdot f_2)$ such that associativity can be applied (with $2 \leq k \leq n$). This makes it so that our problem is identical to our final case, solved just below.

If g is part of neither the first nor last composition, then we consider the innermost composition $(f_k f_{k-1})$ to be a single element h. We now have a sequence of only n terms. We apply our hypothesis $P(n)$. This makes g the outermost right term, part of the last composition. Unravelling h back into two members, we see that we are back at our initial case, with an arbitrary order of parentheses for the $f_n f_{n-1} \cdot f_1$ terms, and g outermost. We already saw that this implied $P(n+1)$.

Conclusion: since we have initialization and heredity of our hypothesis in all cases, we can conclude by induction that it is true for all $n \geq 3$.

4.2)

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

We remind example 4.6 : a groupoid is a category in which every morphism is an isomorphism. This means that every morphism needs to be 2-way invertible.

In this context, this means that for every morphism $a \sim b$, there should be a corresponding inverse morphism $b \sim a$. This property is precisely the symmetry of a relation.

This means that all sets with an equivalence relation can be reconstructed into a groupoid.

4.3)

Let A, B be objects of a category $\mathcal{C}$, and $f \in Hom_{\mathcal{C}}(A, B)$ a morphism. Prove that if f has a pre-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 pre-inverse.

4.3.a)

f has a pre-inverse $\Rightarrow$ f is an epimorphism

Let $\mathcal{C}$ be a category. Let $f \in Hom_{\mathcal{C}}(A, B)$, having some pre-inverse which we'll call $g \in Hom_{\mathcal{C}}(B, A)$:

Let Z be an arbitrary object of $\mathcal{C}$, and $\beta', \beta" \in Hom_{\mathcal{C}}(B, Z)$:

$$\begin{aligned} \beta' \circ f = \beta'' \circ f \Rightarrow (\beta' \circ f) \circ g &= (\beta'' \circ f) \circ g \\ &= \beta' \circ (f \circ g) = \beta'' \circ (f \circ g) \\ &= \beta' \circ id_B = \beta'' \circ id_B \\ &= \beta' = \beta'' \end{aligned}$$

This means that f is an epimorphism.

4.3.b)

f is an epimorphism $\not\Rightarrow$ f has a pre-inverse

As was mentioned in the text, "order" categories (poset categories) where there's only at most one morphism between any two objects makes it so that every morphism is trivially an epimorphism (i.e., since there is at most one morphism "$\leq$" between any two elements, so you always have $\beta' = \beta$" $=\leq$, and since $\beta' = \beta$" is always true, anything implication with it as a necessary condition is also true, and therefore every morphism is true). However, only identities have any kind of inverse (since they are isomorphisms, they are their own inverse); other combinations of elements go one-way, because of antisymmetry.

See also here and here.

4.4)

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

4.4.a)

Mono

Let be $f \in Hom_{\mathcal{C}}(A, B)$ and $g \in Hom_{\mathcal{C}}(B, C)$ be monomorphisms. Let us show that $g \circ f$ is also a monomorphism.

Let Z be an arbitrary object of $\mathcal{C}$, and α', α" $\in Hom_{\mathcal{A}}(Z, A)$:

$$\begin{aligned}(g \circ f) \circ \alpha' = (g \circ f) \circ \alpha'' = g \circ (f \circ \alpha') = g \circ (f \circ \alpha'') \\ \Rightarrow f \circ \alpha' = f \circ \alpha'' \text{ because } g \text{ is mono} \\ \Rightarrow \alpha' = \alpha'' \text{ because } f \text{ is mono}\end{aligned}$$

This means that the composition of 2 monomorphisms is always an monomorphism. We can thus make a subcategory. Taking all objects, properties, and homsets of $\mathcal{C}$, but restricting the homsets only to the monomorphisms, we

know that this makes a new category $\mathcal{C}_{mono}$ since it is closed under composition, has identities (which are iso, and *a fortiori* mono) and associativity.

4.4.b)

Epi

Let be $f \in Hom_{\mathcal{C}}(A, B)$ and $g \in Hom_{\mathcal{C}}(B, C)$ be epimorphisms. Let us show that $g \circ f$ is also a epimorphism.

Let Z be an arbitrary object of $\mathcal{C}$, and $\beta', \beta" \in Hom_{\mathcal{C}}(C, Z)$:

$$\begin{aligned} \beta' \circ (g \circ f) = \beta'' \circ (g \circ f) = (\beta' \circ g) \circ f = (\beta'' \circ g) \circ f \\ \Rightarrow \beta' \circ g = \beta'' \circ g \text{ because } f \text{ is epi} \\ \Rightarrow \beta' = \beta'' \text{ because } g \text{ is epi} \end{aligned}$$

This means that the composition of 2 epimorphisms is always an epimorphism. We can thus make a subcategory. Taking all objects, properties, and homsets of $\mathcal{C}$, but restricting the homsets only to the epimorphisms, we know that this makes a new category $\mathcal{C}_{epi}$ since it is closed under composition, has identities (which are iso, and *a fortiori* epi) and associativity.

4.4.c)

Nonmono and nonepi

We could consider the fact that (TODO prove lol) we can't obtain a monomorphism from the composition of two non-monomorphisms (you need at least one monomorphism in the mix). However, the real problem is identities. Identities are iso, and thus mono. You can't make a category without identities, so there is no such $\mathcal{C}_{nonmono}$. the same reasoning applies to $\mathcal{C}_{nonepi}$.

4.5)

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

We'll use our **CMSet** construction, where elements of multisets consisted of a pair of the set-element and its count in the multiset.

We recall that in the way we formulated this, morphisms were just simple set functions on "(element, count)" pairs (i.e., returning any other "(element, count)" pair of the codomain). Let be a morphism of multisets $f \in (A \to B)$.

Labelling the elements of the domain A as a_i and of the codomain B as b_j with $i \in I$, $j \in J$, and I, J any two indexing sets such that $card(A) = card(I)$ and $card(B) = card(J)$, we can see that A and B now just look like "normal" sets.

We now simply recycle the notion of injections and surjections. These form our monomorphisms and epimorphisms respectively.

Section 5)

5.1)

Prove that a final object in a category $\mathcal{C}$ is initial in the opposite category $\mathcal{C}^{op}$

Let $\mathcal{C}$ be a category. Let $\mathcal{C}^{op}$ be the dual category on $\mathcal{C}$. Let F be a final object in $\mathcal{C}$. This means that for every object Z in $\mathcal{C}$, there is a single morphism from Z to F. We will call this morphism f_Z (respectively).

We remind how we defined composition in $\mathcal{C}^{op}$ as $\star$, respecting:

$$\begin{aligned}
&\forall f \in Hom_{\mathcal{C}^{op}}(B, A) = Hom_{\mathcal{C}}(A, B),\\
&\forall g \in Hom_{\mathcal{C}^{op}}(C, B) = Hom_{\mathcal{C}}(B, C),\\
&\exists h \in Hom_{\mathcal{C}^{op}}(C, A) = Hom_{\mathcal{C}}(A, C),\\
&f \star g \coloneqq g \circ f = h
\end{aligned}$$

In this case, we see that $\forall Z \in Obj(\mathcal{C}^{op}) = Obj(\mathcal{C}), f_Z \in Hom_{\mathcal{C}^{op}}(F, Z) = Hom_{\mathcal{C}}(Z, F)$. This implies that the homset $Hom_{\mathcal{C}^{op}}(F, Z)$ contains a single morphism, f_Z. This means that F is initial in $\mathcal{C}^{op}$.

5.2)

Prove that $\emptyset$ is the *unique* initial object in **Set**.

First we will prove that it is initial, then that it is unique.

Initiality: we take an arbitrary set Z in **Set**. We wish to study $Hom_{\mathbf{Set}}(\emptyset, Z) = Z^{\emptyset}$. We recall that functions (in category theory) are defined as "applications" / "mappings" are in traditional set theory (i.e., as a relation between sets where every antecedent in the domain has a singleton image in the codomain; the key point being that "no input has no result when passed through the function"). Let I be an initial element in **Set**. We write $|I| = n$

and $|Z| = m$. We know that $|Z^I| = |Z|^{|I|} = m^n$. For I to be initial, this is true if and only if $m^n = 1$ for all m, and so if and only if $n = 0$. We recall that the empty set is the only set with $|\emptyset| = 0$, therefore $I = \emptyset$.

Now this is already enough to prove unicity, but let us spell it out for pedagogy's sake.

Unicity: We recall that two objects of **Set** are isomorphic if, and only if, there exists a bijection between them. This is equivalent to saying that two sets have the same cardinal. We once again recall that the empty set is the only set with $|\emptyset| = 0$; there are no bijections relating to the empty set, other than its identity, the unique morphism in $Hom_{\mathbf{Set}}(\emptyset, \emptyset)$. Using proposition 5.4 (that terminal objects are unique up-to-isomorphism), we finally deduce that $\emptyset$ is the unique initial object in **Set**.

NB: the unique function in $Z^\emptyset$ is always the empty function.

5.3)

Prove that final objects are unique up to isomorphism.

Let us suppose we have a category $\mathcal{C}$ with two final objects, F_1 and F_2.

For every object A of $\mathcal{C}$ there is at least one element in $Hom_{\mathcal{C}}(A, A)$, namely the identity 1_A. If F is final, then there is a unique morphism $F \to F$, which therefore must be the identity 1_F.

We assumed that F_1 and F_2 are both final in $\mathcal{C}$. Since F_1 is final, there is a unique morphism $f : F_2 \to F_1$ in $\mathcal{C}$. Since F_2 is final, there is a unique morphism $g : F_1 \to F_2$ in $\mathcal{C}$. Consider $fg : F_1 \to F_1$; as observed, necessarily the composite $fg = 1_{F_1}$ since F_1 is final. By the same token $gf = 1_{F_2}$. Thus f and g are inverses of each other, proving f is an isomorphism. Since there exists an isomorphism between F_1 and F_2, $F_1 \simeq F_2$.

5.4)

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

We recall that a pointed set is just a regular set with a special, identified point, and that the category of pointed sets **Set*** is built upon the same objects as **Set**, but where each object A in **Set** is multiplied into $|A|$ copies of itself in **Set*** (one for each choice of special point; this implies that the empty set is not a part of **Set***, since it has no point). Morphisms in **Set***

are set functions, but with the restriction of mapping the special point in the domain to the special point in the codomain.

Given this information, we will prove that the initial and final objects in **Set*** are the singleton sets.

Let (O, o) be a singleton set in **Set***. Let o be the single element of O; it is necessarily also the special point, as there is no other choice. For any codomain (Z, z_0) in **Set***, the condition that "special points map to special points" restricts our choice of function to the unique function (o, z_0), thus, O is initial. If O had more than one element, there would exist some Z (non-singletons) for which the other element would allow another degree of freedom (and thus O would not be initial).

Similarly, now studying Z as a domain and O as a codomain, we see that that only function from Z to O is (like in **Set**) the function which maps everything (including Z's special point) to o. Thus, O is final. If O had more than one element, there would similarly be many choices for any Z of cardinal ≥ 2, so long as the special point maps to the special point.

Every singleton pointed set is both initial and final in **Set*** and is thus a zero object. These are also the only such pointed sets.

5.5)

What are the final objects in the category considered in §5.3?

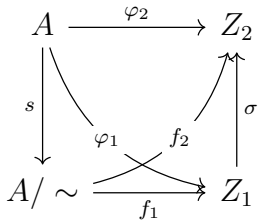
The category considered in paragraph 5.3 is the coslice category over some set A, written $\mathcal{C}_A$. However, what is presented in this paragraph is some extra structure that arises when considering the statement "The quotient $A/\sim$ is universal with respect to the property of mapping A to a set in such a way that equivalent elements have the same image". We thus give some equivalence relation $\sim$ on A and study the quotient set $A/\sim$ in the general coslice category; to do this, we consider the subcategory $\mathcal{Q}$ of $\mathcal{C}_A$ where only φ such that "equivalence is preserved" (i.e., such that $\forall a', a'' \in A, a' \sim a'' \Rightarrow \varphi(a') = \varphi(a'')$).

With:

- s the canonical surjection of A onto its quotient $A/\sim$,
- φ_1 (resp. φ_2) being some arbitrary function from A to some arbitrary Z_1 (resp. Z_2),
- σ any function (if it exists) such that $\sigma\varphi_1 = \varphi_2$

- f_1 (resp. f_2) is the (unique!) function such that $sf_1 = \varphi_1$ (resp. $sf_2 = \varphi_2$)

The following diagram commutes, and summarizes the situation.

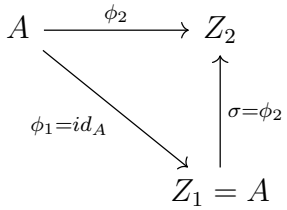


Objects in this category $\mathcal{C}_A$ (and *a fortiori* $\mathcal{Q}$) are denoted as (φ, Z) and are obtained from what used to be *morphisms* (regular functions) in **Set**. Morphisms are mappings $\sigma_{\mathcal{Q}} : (\varphi_1, Z_1) \to (\varphi_2, Z_2)$ such that one exists if and only if $\exists \sigma \in (Z_1 \to Z_2), \sigma\varphi_1 = \varphi_2$, and $\forall a', a'' \in A, a' \sim a'' \Rightarrow \varphi(a') = \varphi(a'')$.

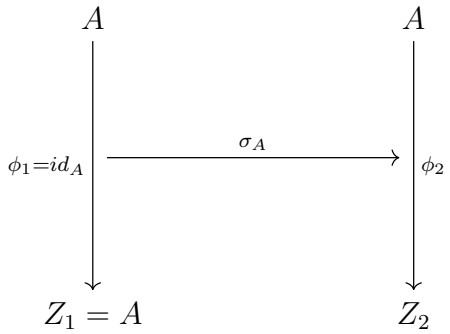
Since the textbook also asks whether such a category has initial objects, we will first also answer this and consider all terminal objects.

The initial object of a general coslice category is (id_A, A). This is easily verified by doing $\varphi_1 = id_A$, necessarily $\sigma\varphi_1 = \sigma id_A = \sigma = \varphi_2$, in $\mathcal{C}$. This implies that, for the domain (id_A, A) in $\mathcal{C}_A$ and any codomain (ϕ_2, Z_2), there always exists a unique morphism $\sigma_A \in Hom_{C_A}((id_A, A), (\phi_2, Z_2))$ in $\mathcal{C}_A$, corresponding to the (existing and unique) $\sigma = \phi_2$ in $\mathcal{C}$. We also see that this object satisfies the "equivalence preservation" condition, hence it exists in $\mathcal{Q}$, and is also the initial object in $\mathcal{Q}$.

The below are this description first in $\mathcal{C}$, followed by the description in $\mathcal{C}_A$.

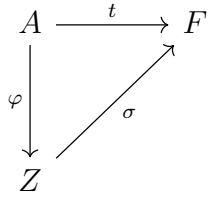


Now in $\mathcal{C}_A$.



A general coslice category has a final object (t, F) (or many final objects (t_i, F_i)) iff $\mathcal{C}$ has a final object F (or many final objects F_i). In that case, any final object (t, F) in $\mathcal{C}_A$ corresponds to the unique morphism from A to F (for any final F) in $\mathcal{C}$. Let us verify this.

Let F be final in $\mathcal{C}$, and t be the unique morphism $t \in Hom_{\mathcal{C}}(A, F)$. Let (φ, Z) be an arbitrary object of $\mathcal{C}_A$. Let be σ such that $\sigma\varphi = t$. We consider the following diagram:



Since F is final in $\mathcal{C}$, σ is unique and always exists. Also, since σ is unique and always exist, the choice of φ is irrelevant: this same σ works for all choices of φ for a given arbitrary Z. This proves that $\sigma_{\mathcal{C}_A}$ exists and is unique for all (φ, Z). Finally, since σ works for all choices of φ, it works for those that satisfy the "equivalence preservation" condition, and so does t: this means that (t, F) is indeed a final object in $\mathcal{Q}$.

5.6)

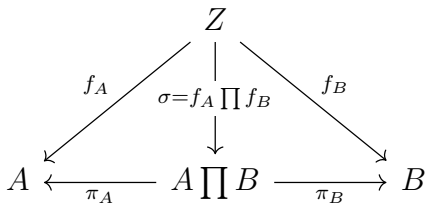
Consider the category corresponding to endowing (as in Example 3.3) the set $\mathbb{Z}^+$ of positive integers with the divisibility relation. Thus there is exactly one morphism $d \to m$ in this category if and only if d divides m without remainder; there is no morphism between d and m otherwise. Show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

Like example 3.3, this is a case of "category made from an order relation over a set", since divisibility is an order relation (reflexive, antisymmetric,

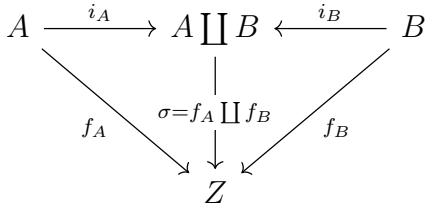
transitive).

Let us remind the definition of categorical products and coproducts. We consider some general category $\mathcal{C}$.

An object $A \prod B$ is the product of two objects A and B iff there is a unique morphism π_A (resp. π_B) from $A \prod B$ to A (resp. B), and for every Z in $\mathcal{C}$, and for every pair of morphisms $f_A : Z \to A$ and $f_B : Z \to B$, there exists a single morphism $\sigma = f_A \prod f_B$ such that $\pi_A \sigma = f_A$ and $\pi_B \sigma = f_B$. This is summarized in the following commutative diagram.

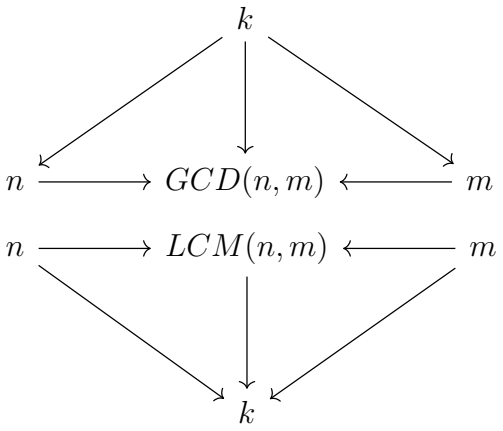


An object $A \coprod B$ is the coproduct of two objects A and B iff there is a unique morphism i_A (resp. i_B) from A (resp. B) into $A \coprod B$, and for every Z in $\mathcal{C}$, and for every pair of morphisms $f_A : A \to Z$ and $f_B : B \to Z$, there exists a single $\sigma = f_A \coprod f_B$) such that $\sigma i_A = f_A$ and $\sigma i_B = f_B$. This is summarized in the following commutative diagram.



We now return to our "divisibility order category". We write its objects as simple integers, and the (if it exists, unique) morphism representing "divisibility of m by n" as $(n|m)$. The conventional name of the product for this category is "greatest common divisor" (or "meet"), and of the coproduct, "least common multiple" (or "join").

The following commutative diagrams represent this fact. Take two arbitrary naturals m and n. Any number k which divides both m and n also divides their GCD. Likewise, if k is a multiple of both n and m, then it is a multiple of their LCM.

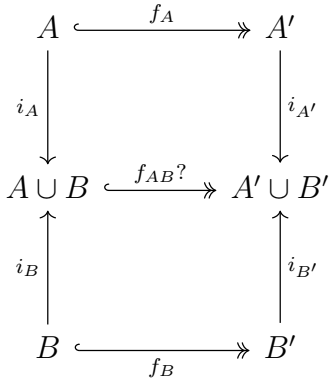


5.7)

Redo Exercise 2.9 ("Show that if $A \simeq A'$ and $B \simeq B'$, and further $A \cap B = \emptyset$ and $A' \cap B' = \emptyset$, then $A \cup B \simeq A' \cup B'$. Conclude that the operation $A \coprod B$ (as described in §1.4) is well-defined up to isomorphism") this time using Proposition 5.4. (the unicity up-to-isomorphism of terminal objects).

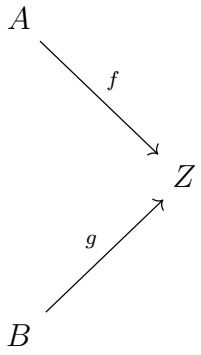
TODO, fix, since $\mathbf{Set}^{A,B}$ and $\mathbf{Set}^{A',B'}$ need to both be treated.

This is what we are give by the prompt:

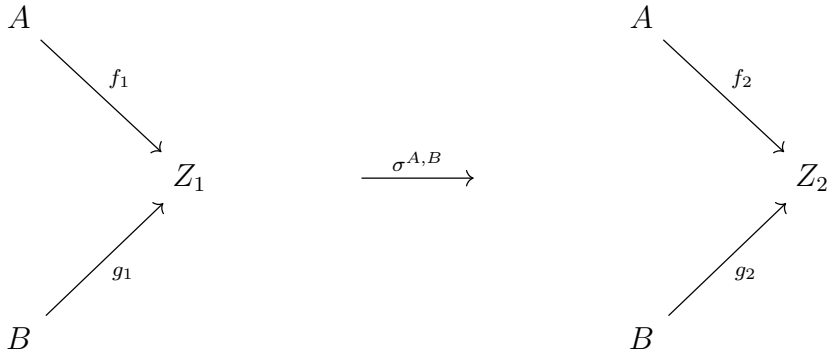


with $A \cup B = A \coprod B$ and $A' \cup B' = A' \coprod B'$ since $A \cap B = \emptyset$ and $A' \cap B' = \emptyset$.

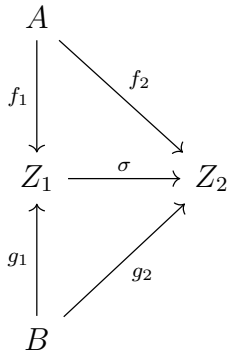
We define $\mathbf{Set}^{A,B}$ as the "bicoslice category of A and B over $\mathbf{Set}$". Objects in this category are pairs of morphisms (f, g) from A and B, respectively, into sets Z. They can be diagrammed as follows.



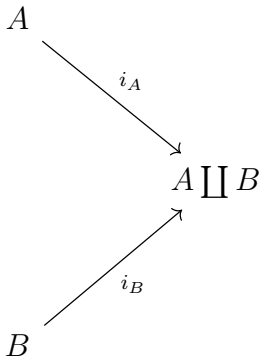
Morphisms are defined between objects as



such that the following diagram commutes in **Set**



Let us call I the following object of $\mathbf{Set}^{A,B}$, where $A \coprod B$ is any choice of valid disjoint union of A and B:



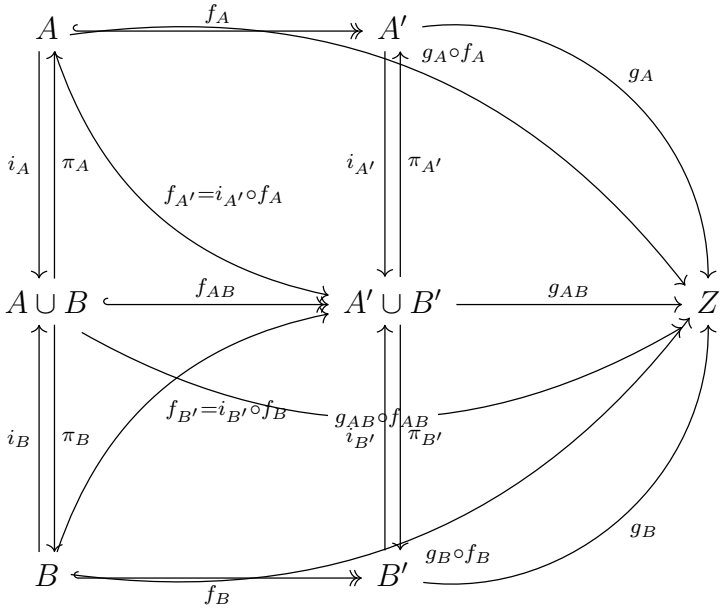
By definition of a coproduct, we know that in such a configuration, a morphism $\sigma^{A,B}$ from this object into any other object of $\mathbf{Set}^{A,B}$ exists and is unique, and so is the σ on which it is based. This means that I is initial in $\mathbf{Set}^{A,B}$.

TODO fix and explain

We observe that i_A, i_B, $i_{A'}$ and $i_{B'}$ are all injections, and thus are post-cancellable, by maps π_A, π_B, $\pi_{A'}$ and $\pi_{B'}$ (which are surjections).

$f_{A'} = i_{A'} \circ f_A$ and $f_{B'} = i_{B'} \circ f_B$ together define a unique map f_{AB} from $A \coprod B$ to $A' \coprod B'$.

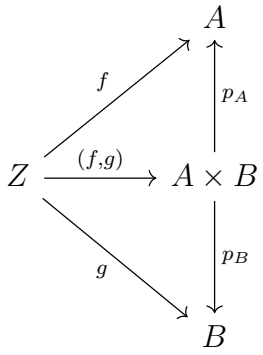
We set arbitrary $g_A : A' \to Z$ and $g_B : B' \to Z$; we have $g_A \circ f_A = g_A \circ i_{A'} \circ f_A$ and $g_B \circ f_B = g_B \circ i_{B'} \circ f_B$. These define a unique map from $A \coprod B$ to Z, which we'll write $g_{AB} \circ f_{AB}$.



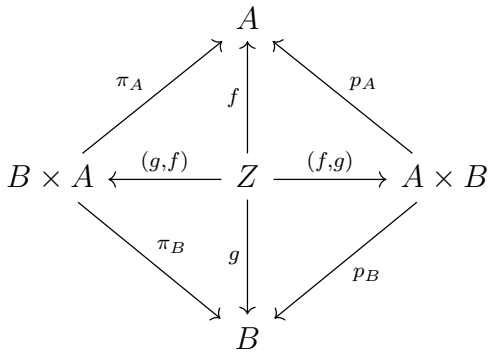
5.8)

Show that in every category $\mathcal{C}$ 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.)

Let us first remind the definition of the product of two sets. It is the set made of all pairs of A and B (ordered sequences of two elements, where the first element in the sequence comes from A and the second comes from B) It is the structure such that the following diagram commutes, and (f, g) is unique.

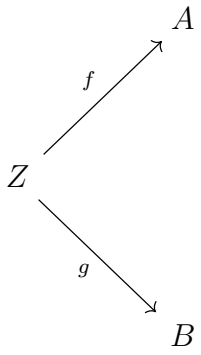


Now to extend the diagram to consider both $A \times B$ and $B \times A$.

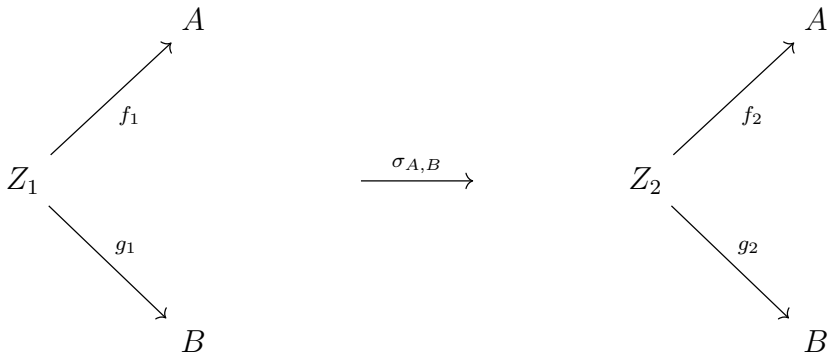


We seek to prove that given such a commutative diagram (with a unique (f, g) and (g, f)), which we will call D, then we have $A \times B \simeq B \times A$.

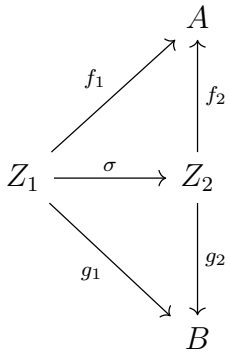
We define $\mathcal{C}_{A,B}$ as the "bislice category of A and B over $\mathcal{C}$". Objects in this category are pairs of morphisms (f, g) from sets Z, into A and B, respectively. They can be diagrammed as follows.



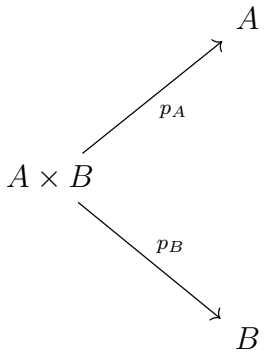
Morphisms are defined between objects as



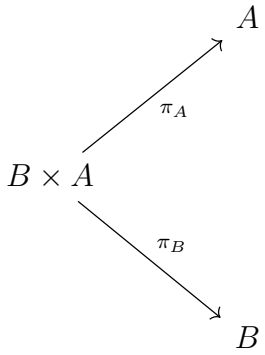
such that the following diagram commutes in $\mathcal{C}$:



We now define the following objects:



and

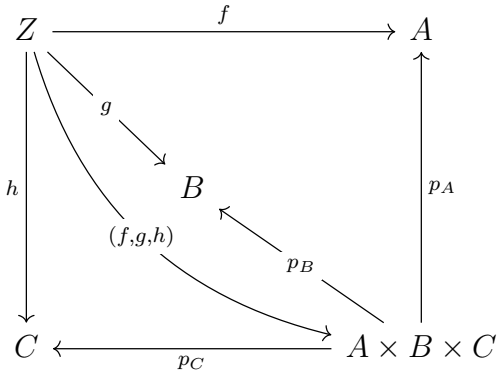


Using the diagram D defined above, and the definition of a product (ie, that the maps from any Z to it in the appropriate configuration are unique). We deduce that both $A \times B$ and $B \times A$ are final objects in $\mathcal{C}_{A,B}$. Finally, using Proposition 5.4, i.e., that final objects in a category are unique up-to-isomorphism, we conclude that $A \times B \simeq B \times A$.

5.9)

Let $\mathcal{C}$ 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 $\mathcal{C}$ 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.

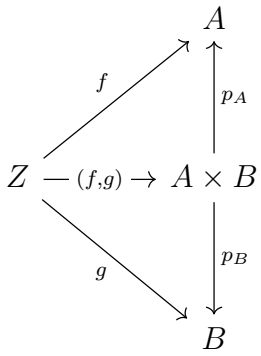
Given 3 objects A, B, C of $\mathcal{C}$. We propose the following universal property that $A \times B \times C$ should respect: for all objects Z of $\mathcal{C}$, and triplet of maps f, g, and h from Z to A, B and C respectively, there exists a unique triplet-map (f, g, h) is unique such that the following diagram commutes.



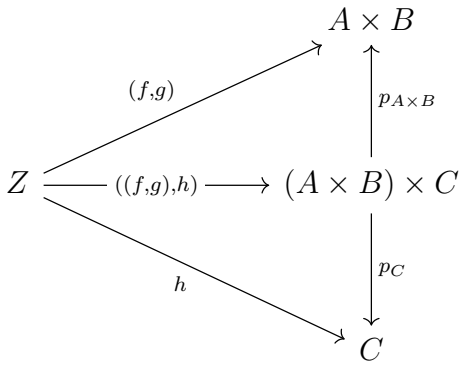
We will now show that both $(A \times B) \times C$ and $A \times (B \times C)$ satisfy this universal property.

5.9.a)

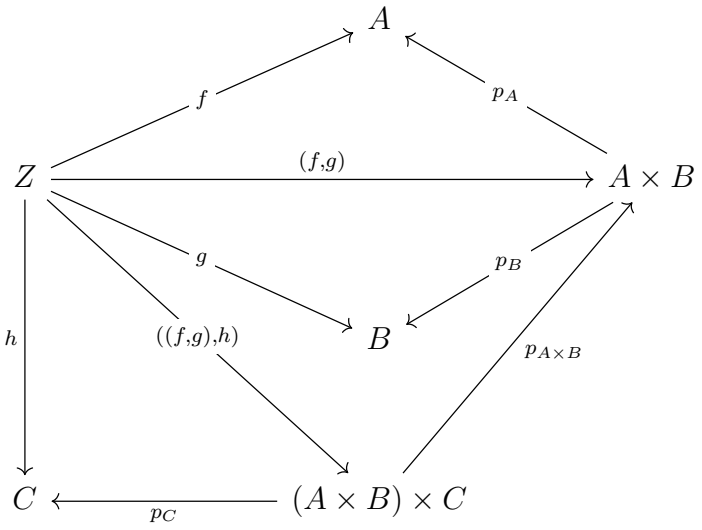
We start with



and

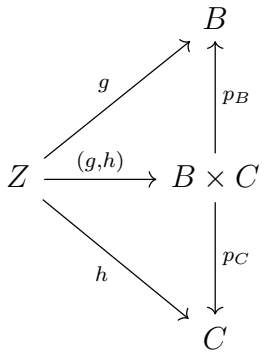


From both of these universal products, we deduce the following commutative diagram.

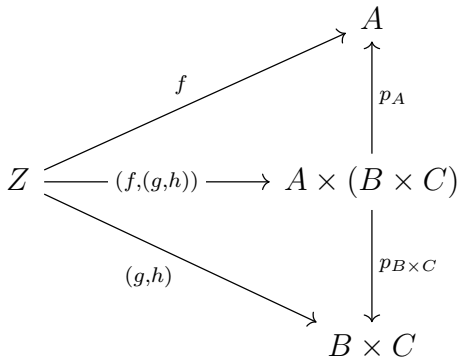


5.9.b)

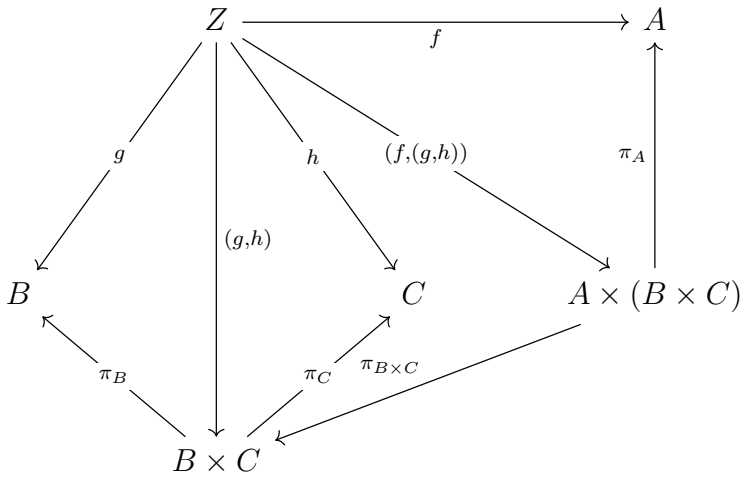
We start with



and

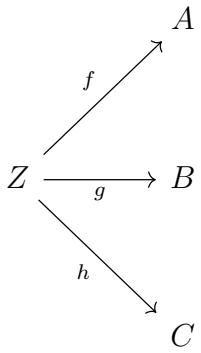


From both of these universal products we deduce the following commutative diagram:

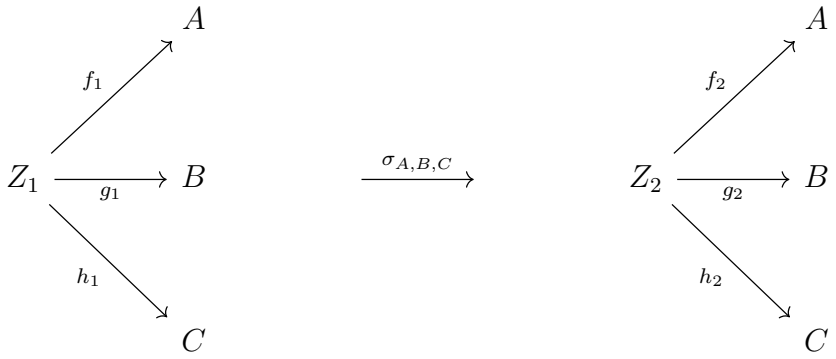


5.9.c)

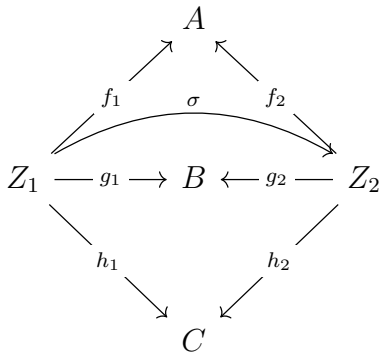
We now consider the $\mathcal{C}_{A,B,C}$ as the "trislice category of A, B and C over $\mathcal{C}$". Objects in this category are of the form:



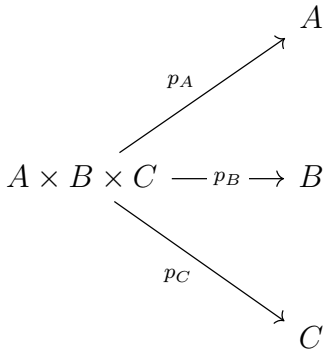
Morphisms are defined between objects as:



such that there exists a σ making the following diagram commute in $\mathcal{C}$:



We now define the following object:

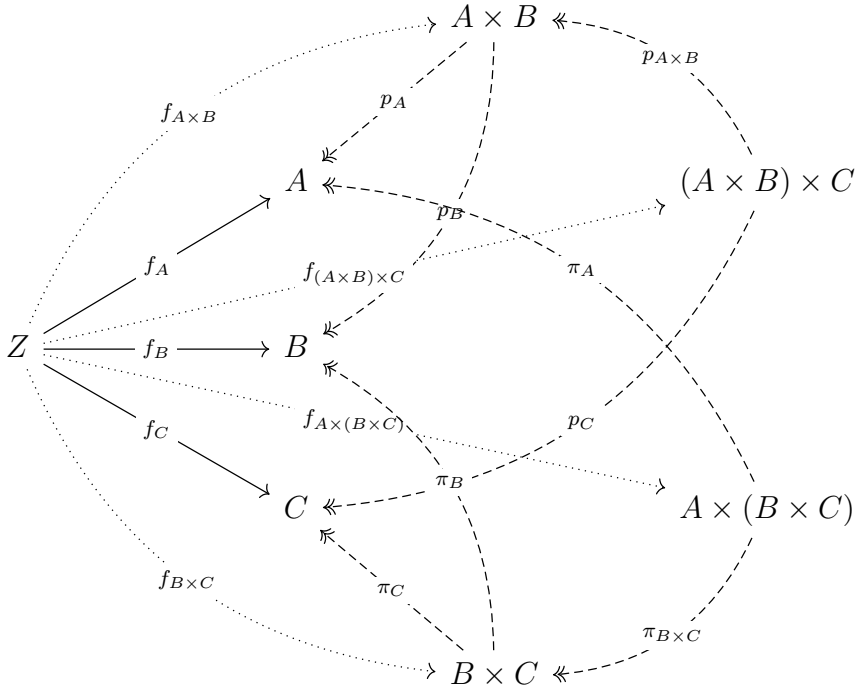


and using the two universal properties we have shown above, we know that necessarily $(A \times B) \times C$ and $A \times (B \times C)$ are terminal objects in $\mathcal{C}_{A,B,C}$. This is because they are final objects in respective bislice categories, given that $((f, g), h)$ and $(f, (g, h))$ are both unique; and we can compose $p_A \circ p_{A \times B}$, etc, to get immediate projections, making them final in the trislice category as well. To be precise:

$$(((A \times B) \times C),\ p_A \circ p_{A\times B},\ p_B \circ p_{A\times B},\ p_C)$$

$$((A \times (B \times C)),\ \pi_A,\ \pi_B \circ \pi_{B\times C},\ \pi_C \circ \pi_{B\times C})$$

are both final objects in $\mathcal{C}_{A,B,C}$, as is shown by the following commutative diagram, which is composed from the diagrams above:



We use Proposition 5.4 to deduce that $(A \times B) \times C$ and $A \times (B \times C)$, as terminal objects in $\mathcal{C}_{A,B,C}$, are necessarily isomorphic. Therefore, given this "associativity up-to-isomorphism" of a triple product, it is legitimate to call $A \times B \times C$ (with no parentheses) "the" (unique, up-to-isomorphism) final object in $\mathcal{C}_{A,B,C}$.

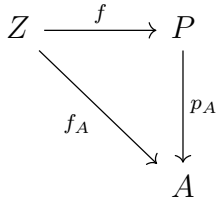
5.10)

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 $A \times \cdots \times A$ (n times) by A^n.

Let $\mathcal{F}$ be an (ordered) family of objects in some category $\mathcal{C}$.

5.10.a)

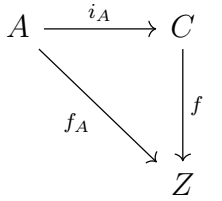
A product of the elements of $\mathcal{F}$ is defined as an object P of $\mathcal{C}$ together with a family of morphisms $\{p_A : P \to A\}_{A\in\mathcal{F}}$ such that for any object Z and family of morphisms $\{f_A : Z \to A\}_{A\in\mathcal{F}}$, there exists a unique morphism $f : Z \to P$ such that the following diagram commutes for all $A \in \mathcal{F}$:



These exist in **Set** for all finite families of sets, however, for infinite families of sets, their existence is conditional on the (famous) axiom of choice (it is actually precisely the point of the axiom of choice).

5.10.b)

A coproduct of the elements of $\mathcal{F}$ is defined as an object C of $\mathcal{C}$ together with a family of morphisms $\{i_A : A \to C\}_{A\in\mathcal{F}}$ such that for any object Z and family of morphisms $\{f_A : A \to Z\}_{A\in\mathcal{F}}$, there exists a unique morphism $f : C \to Z$ such that the following diagram commutes for all $A \in \mathcal{F}$:



These exist in **Set** for all families of sets, however, for infinite families of sets, their existence is conditional on the axiom of choice.

5.11)

Let A, resp. B, be sets, endowed with equivalence relations $\sim_A$, resp. $\sim_B$. Define a relation $\sim$ on $A \times B$ by setting $(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 \sim_A a_2$ and $b_1 \sim_B b_2$. (This is immediately seen to be an equivalence relation.)

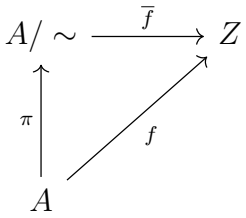
- Use the universal property for quotients (§5.3) to establish that there are functions $(A \times B)/\sim \to A/\sim_A$, and $(A \times B)/\sim \to B/\sim_B$;

- prove that $(A \times B)/\sim$, with these two functions, satisfies the universal property for the product of $A/\sim_A$ and $B/\sim_B$;

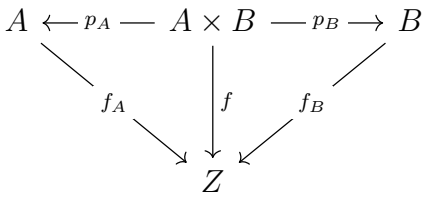
- conclude (without further work) that $(A \times B)/\sim \simeq (A/\sim_A) \times (B/\sim_B)$.

5.11.a)

First, we remind the universal property for quotients. Given an equivalence relation $\sim$ over a set A, there is a single map $\pi : A \to A/\sim$ such that, for any map $f : A \to Z$ verifying $f(a_1) = f(a_2)$ whenever $a_1 \sim a_2$ (i.e., the morphism f is "well-defined" for the equivalence relation $\sim$), there exists a unique map $\overline{f} : A/\sim \to Z$ such that $f = \overline{f} \circ \pi$. This is summarized in the following commutative diagram:



We now apply the universal property of products to obtain the following commutative diagram:

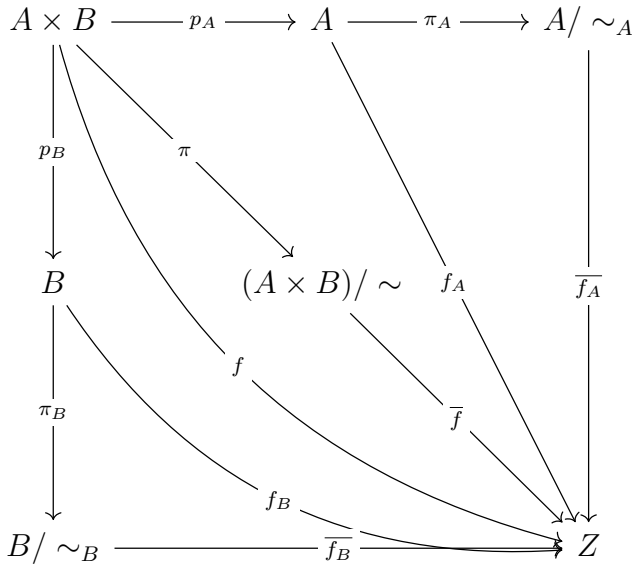


We then consider a well-defined map $f : (A \times B) \to Z$ (i.e., $f(a_1, b_1) = f(a_2, b_2)$ whenever $(a_1, b_1) \sim (a_2, b_2)$). We apply the universal property of quotients to the relation $\sim$ defined over $A \times B$. We define the map $\pi : A \times B \to (A \times B)/\sim$ as $\pi(a, b) = [(a, b)]_\sim$. We define the map $\overline{f} : (A \times B)/\sim \to Z$ as $\overline{f}([(a, b)]_\sim) = f(a, b)$. We remind that such an f is unique, and that $\overline{f} \circ \pi = f$.

We do a similar construction for $A/\sim_A$ with f_A and $B/\sim_B$ with f_B. We can do so since these maps are also well-defined. Indeed, we have:

$$
\begin{cases}
(a_1, b_1) \sim (a_2, b_2) \\
(a_1, b_1) \sim (a_2, b_2) \Rightarrow f(a_1, b_1) = f(a_2, b_2) \\
f = f_A \circ p_A \\
f = f_B \circ p_B
\end{cases}
$$
$$
\Rightarrow
$$
$$
\begin{cases}
a_1 \sim_A a_2 \text{ and } b_1 \sim_B b_2 \\
f_A(p_A(a_1, b_1)) = f_A(p_A(a_2, b_2)) \\
f_B(p_B(a_1, b_1)) = f_B(p_B(a_2, b_2))
\end{cases}
$$
$$
\Rightarrow
$$
$$
\begin{cases}
f_A(a_1) = f_A(a_2) \\
f_B(b_1) = f_B(b_2)
\end{cases}
$$

The combination of all previous steps gives us the following commutative diagram.



Let us recap a little what's in diagram a little, to show that it is a justified construction:

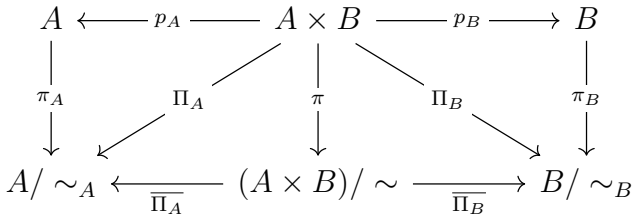
- $A \times B$ is a product, and so we may obtain p_A, p_B, f_A, and f_B;
- f is well-defined for the equivalence relation $\sim$, and so we may obtain $\overline{f}$ and π;
- f_A is well-defined for the equivalence relation $\sim_A$, and so we may obtain $\overline{f_A}$ and π_A;

- f_B is well-defined for the equivalence relation $\sim_B$, and so we may obtain $\overline{f_B}$ and π_B;

Therefore, we have the maps $\Pi_A = \pi_A \circ p_A \in (A \times B) \to A/\sim_A$ and $\Pi_B = \pi_B \circ p_B \in (A \times B) \to B/\sim_B$. Π_A and Π_B are well-defined because they are compositions of well-defined maps. For π_A and π_B, we know that the projector and unique function part (of the universal property of quotients) are necessarily well-defined, otherwise they wouldn't compose to a well-defined map. As for p_A and p_B, they are well-defined because they are projections, and projections are always well-defined.

Since Π_A and Π_B are well-defined, we can "quotient through" (i.e., use the universal property of quotient for) $(A \times B)/\sim$.

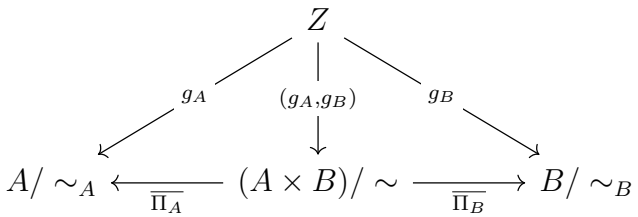
This gives us the following commutative diagram (compatible with the one above, but it's too messy to represent both at the same time):



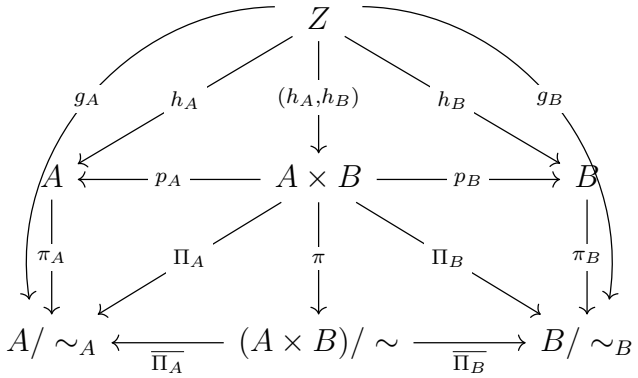
These are precisely our functions $\overline{\Pi_A} \in (A \times B)/\sim \to A/\sim_A$ and $\overline{\Pi_B} \in (A \times B)/\sim \to B/\sim_B$, and they are unique, as per the universal property of quotients.

5.11.b)

What we wish to prove now is that $(A \times B)/\sim$ is the product of $A/\sim_A$ and $B/\sim_B$. Said otherwise, we wish to show that, for all Z, g_A and g_B in the appropriate configuration, the following diagram commutes:



Using the fact that $(A \times B)$ is already a product, and studying maps h_A and h_B from Z into A and B respectively, we can make the following commutative diagram:



The internal parts of the diagram (except h_A and h_B which are arbitrary, all other arrows are unique morphisms) force g_A and g_B to commute with the rest of the diagram: any pairs of maps g_A and g_B that make the diagram commute must necessarily be constrained by the existing morphisms (as the composition of unique morphisms). Any choice of maps g_A and g_B must respect $g_A = \pi_A \circ h_A$ and $g_B = \pi_B \circ h_B$, for corresponding arbitrary (but inferred) h_A and h_B; said otherwise, maps g_A and g_B in this configuration can only exist if they make the diagram commute. Therefore, we have shown that $(A \times B)/\sim$ satisfies the universal property of the product of $A/\sim_A$ and $B/\sim_B$, and we have $(g_A, g_B) = \pi \circ (h_A, h_B)$ (though it's not shown on the above diagram, in order to improve legibility).

5.11.c)

We know that elements that verify a common universal property are terminal objects (of the same kind) in some comma category. Here, both $(A \times B)/\sim$ and $((A/\sim_A) \times (B/\sim_B))$ are final objects in the bislice category $\mathbf{Set}_{A,B}$. Since they are both final objects in the same category, they are isomorphic.

Conclusion: $((A \times B)/\sim) \simeq ((A/\sim_A) \times (B/\sim_B))$

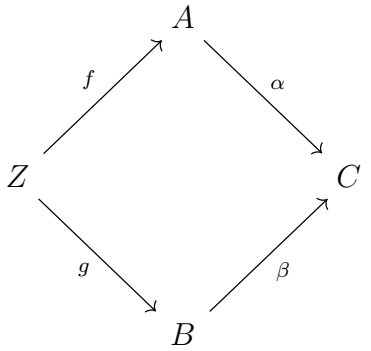
5.12)

Define notions of fibered products and coproducts, as terminal objects of the categories $\mathcal{C}_{\alpha,\beta}$, $C^{\alpha,\beta}$ 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.3.9, III.6.10, III.6.11]

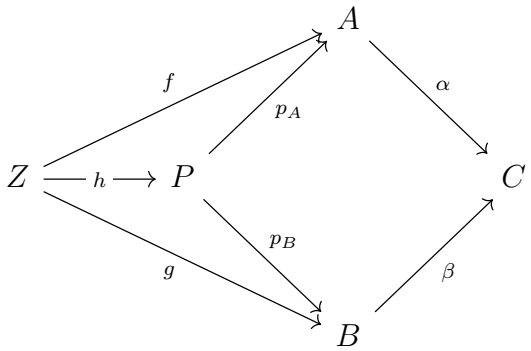
5.12.a)

We first define the fibered product (or "pullback"). We suggest the reader goes to check section 3.11.3 of this exercises solutions document for a refresher on the concept "fibered bislice category" $\mathcal{C}_{\alpha,\beta}$. We will use the same notation, i.e., fixing two morphisms $\alpha : A \to C$ and $\beta : B \to C$ (with common codomain) in a category $\mathcal{C}$.

This means, for any generic object (Z, f, g) of $\mathcal{C}_{\alpha,\beta}$, we have the following diagram:



We first propose a candidate for what it means to be a "fibered product", which we will be able to show is a final object in $\mathcal{C}_{\alpha,\beta}$. A fibered product P of A and B over C in a category $\mathcal{C}$ is an object P together with morphisms $p_A : P \to A$ and $p_B : P \to B$ such that for any object Z in $\mathcal{C}$ and morphisms $f : Z \to A$ and $g : Z \to B$ such that $\alpha \circ f = \beta \circ g$, there exists a unique morphism $h : Z \to P$ such that the following diagram commutes:



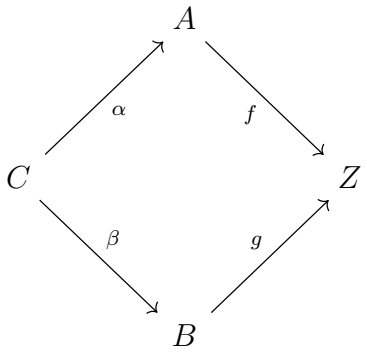
We will now show that this object P induces a terminal object in $\mathcal{C}_{\alpha,\beta}$; this boils down to showing that (P, p_A, p_B) is final in $\mathcal{C}_{\alpha,\beta}$. Let (Z, f, g) be an arbitrary object of $\mathcal{C}_{\alpha,\beta}$. A morphism σ from (Z, f, g) to (P, p_A, p_B) is a "raising" of a morphism $h : Z \to P$ such that $p_A \circ h = f$ and $p_B \circ h = g$. This

raising σ is unique if and only if h is unique. Since P is presupposed to verify the universal property, such an h, if it exists, is indeed unique. Therefore, (P, p_A, p_B) is final (*a fortiori* terminal) in $\mathcal{C}_{\alpha,\beta}$.

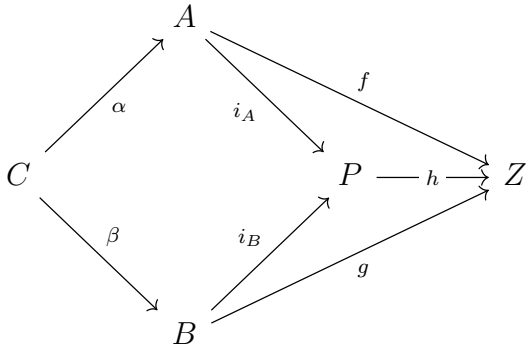
5.12.b)

We now define the fibered coproduct (or "pushout"). We suggest the reader goes to check section 3.11.4 of this exercises solutions document for a refresher on the "fibered bicoslice category" $C^{\alpha,\beta}$. We will use the same notation, i.e., fixing two morphisms $\alpha : C \to A$ and $\beta : C \to B$ (with common domain) in a category $\mathcal{C}$.

This means, for any generic object (f, g, Z) of $C^{\alpha,\beta}$, we have the following diagram:



We first propose a candidate for what it means to be a "fibered coproduct", which we will be able to show is an initial object in $C^{\alpha,\beta}$. A fibered coproduct P of A and B over C in a category $\mathcal{C}$ is an object P together with morphisms $p_A : A \to P$ and $p_B : B \to P$ such that for any object Z in $\mathcal{C}$ and morphisms $f : A \to Z$ and $g : B \to Z$ such that $f \circ \alpha = g \circ \beta$, there exists a unique morphism $h : P \to Z$ such that the following diagram commutes:



We will now show that this object P induces an initial object in $C^{\alpha,\beta}$; this boils down to showing that (i_A, i_B, P) is initial in $C^{\alpha,\beta}$. Let (f, g, Z) be an arbitrary object of $C^{\alpha,\beta}$. A morphism σ from (i_A, i_B, P) to (f, g, Z) is a "raising" of a morphism $h : P \to Z$ such that $h \circ i_A = f$ and $h \circ i_B = g$. This raising σ is unique if and only if h is unique. Since P is presupposed to verify the universal property, such an h, if it exists, is indeed unique. Therefore, (i_A, i_B, P) is initial (*a fortiori* terminal) in $C^{\alpha,\beta}$.

5.12.c)

(I wouldn't have come up with this without Wikipedia as a hint...)

In **Set**, the fibered product (pullback) of (A, α) and (B, β) over C, is a special subset of the cartesian product $A \times B$ that registers some extra information, pertaining to the functions α and β. We write this object as

$$P = A \times_{\alpha,C,\beta} B = A \times_C B = \{(a, b) \in A \times B \mid \alpha(a) = \beta(b)\}$$

.

Concretely, this can also be expressed as

$$P = \bigcup_{c \in \alpha(A) \cap \beta(B)} \alpha^{-1}[\{c\}] \times \beta^{-1}[\{c\}]$$

. This is the set of all pairs (of inputs) (a, b) such that $\alpha(a) = \beta(b)$. Let us show this is the case with a simple example.

Let $A = \{1, 2, 3\}$, $B = \{w, x, y, z\}$, and $C = \{l, m, n, p\}$. We define $\alpha : A \to C$ as $\{(1, m), (2, m), (3, n)\}$, and $\beta : B \to C$ as $\{(w, l), (x, m), (y, n), (z, n)\}$. We have $\alpha(A) = \{m, n\}$ and $\beta(B) = \{l, m, n\}$, therefore $\alpha(A) \cap \beta(B) = \{m, n\}$. The fibered product is then:

$$\begin{aligned} P &= (\alpha^{-1}[\{m\}] \times \beta^{-1}[\{m\}]) \cup (\alpha^{-1}[\{n\}] \times \beta^{-1}[\{n\}]) \\ &= \{\{1, 2\} \times \{x\}\} \cup \{\{3\} \times \{y, z\}\} \\ &= \{(1, x), (2, x)\} \cup \{(3, y), (3, z)\} \\ &= \{(1, x), (2, x), (3, y), (3, z)\} \end{aligned}$$

A simple way to verify this is to verify that for each pair (a, b) in P, $\alpha(a) = \beta(b)$, and that no such other pairs are missing.

5.12.d)

https://math.stackexchange.com/questions/3021738/pushout-in-the-category-of-sets-proof

https://math.stackexchange.com/questions/2240882/understanding-an-example-of-a-pushout-in-mathbfset

In **Set**, the fibered coproduct (pushout) of (α, A) and (β, B) over C is a special quotient of the disjoint union $A \sqcup B$ that registers some extra information, pertaining to the functions α and β. We write this object as

$$P = A \sqcup_{\alpha,C,\beta} B = A \sqcup_C B = (A \sqcup B)/\sim$$

, where $\sim$ is an equivalence relation defined as $\sim := cl_{eq}(R)$, the equivalence closure of the relation

$$R = \{((0, a), (1, b)) \in (A \sqcup B) \times (A \sqcup B) \mid \exists c \in C, a = \alpha(c) \text{ and } b = \beta(c)\}$$

(i.e., two elements are equivalent if they are both the output of some common c, or if there is any chain of such equivalences between them).

(We remind that the equivalence closure, if elements of the set are seen as vertices and the relation pairs as edges of a graph, can be thought of, visually, as "completing the cliques" of each connected component in the graph, including self-loops; hence the idea that if there is any path between two elements, then they are equivalent and should be directly linked. We also remind that this corresponds uniquely to a partition of the set; the elements of which, called cosets, are what allow us to do an algebraic quotient.)

The fibered coproduct is the set P obtained by taking the disjoint union $A \sqcup B$ and identifying $a \in A$ with $b \in B$ if there exists $c \in C$ such that $\alpha(c) = a$ and $\beta(c) = b$ (and all identifications that follow to keep the equality relation an equivalence relation). There is no more concrete of a definition than this; it really boils down to identifying elements with a common preimage element through $\alpha^{-1}(A)$ and $\beta^{-1}(B)$ in C, via an equivalence relation.

Let us show this is the case with a simple example. We will keep the elements of A and B distinct in order to remove the visual clutter that comes with the $(0, ...)$ and $(1, ...)$ of the general disjoint union.

Let $A = \{1, 2, 3\}$, $B = \{w, x, y, z\}$, and $C = \{l, m, n\}$. We define $\alpha : C \to A$ as $\{(l, 1), (m, 1), (n, 2)\}$, and $\beta : C \to B$ as $\{(l, x), (m, y), (n, z)\}$. We have:

- $\alpha^{-1}(\{1\}) = \{l, m\}$ and $\beta^{-1}(\{x\}) = \{l\}$, so $1 \sim x$;

- $\alpha^{-1}(\{1\}) = \{l, m\}$ and $\beta^{-1}(\{y\}) = \{m\}$, so $1 \sim y$, and by closure, $1 \sim x \sim y$;
- $\alpha^{-1}(\{2\}) = \{n\}$ and $\beta^{-1}(\{z\}) = \{n\}$, so $2 \sim z$;
- $\alpha^{-1}(\{3\}) = \emptyset$ and $\beta^{-1}(\{w\}) = \emptyset$, so you might think that $3 \sim w$, however, since there is no $c \in C$ such that $\alpha(c) = 3$ and $\beta(c) = w$, we have $3 \nsim w$;

This information corresponds to the following partition of $A \sqcup B$: $\{\{1, x, y\}, \{2, z\}, \{3\}, \{w\}\}$. The fibered coproduct is then:

$$\begin{aligned} P &= (A \sqcup B)/\sim \\ &= \{1, 2, 3, w, x, y, z\}/\sim \\ &= \{\{1, x, y\}, \{2, z\}, \{3\}, \{w\}\} \\ &= \{[1], [2], [3], [w]\} \end{aligned}$$

A way to verify this is to verify that each equivalence class is disjoint, and that all pairs of elements within an equivalence class are related by $\sim$ (by applying α or β where appropriate and drawing the graph of the relation).

Chapter II)

Section 1)

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.

Let us first remind the definition of a groupoid: a groupoid is a category in which every morphism is an isomorphism.

(Side-note: by "group of isomorphisms", what Aluffi rather meant is "group of isomorphisms (of the single object) in a groupoid (that has a single object)". Otherwise, with multiple objects, things fail: for example, there are multiple identities, one per object, not universally applicable to each object. This is precisely why the notion of "groupoid" was invented, to extend the notion of group in such a way.)

Let $(G, \cdot)$ be a group, i.e., some form of algebraic structure with a set of elements G and a binary operation $\cdot$ which is associative, unitary, and invertible. We want to show that there exists a groupoid $\mathcal{C}$ such that $(G, \cdot)$ is the group of isomorphisms of $\mathcal{C}$.

Let us define $\mathcal{C}$ as follows:

- There is a single object X in $\mathcal{C}$, and its elements are the elements of G (we could call X "G", of course, but we'll be distinct for pedagogy's sake). Our goal is to prove that $Hom(X, X)$ is isomorphic to G, and thus is itself a group.

- For any element g of X, there is a unique morphism $f_g \in Hom(X, X)$ such that $\forall x \in X, f_g(x) = (x \mapsto g \cdot x)$.

- Composition of morphisms is defined as follows: $f_a \circ f_b = (x \mapsto a \cdot (b \cdot x)) = (x \mapsto (a \cdot b) \cdot x) = f_{a \cdot b}$.
- There is an identity morphism $id_X = (x \to e \cdot x)$, with e the identity element of G, and $\forall f \in Hom(X, X), f \circ id_X = f = id_X \circ f$.
- It is immediate to see that these morphisms are associative since $(G, \cdot)$ is associative. Take f_a, f_b, and f_c in $Hom(X, X)$, for $a, b, c \in X$: $(f_a f_b) f_c = (x \to ((a \cdot b) \cdot c)x) = (x \to (a \cdot (b \cdot c))x) = f_a(f_b f_c)$.
- Every such morphism has an inverse, namely, $f_{g^{-1}} = (x \mapsto g^{-1} \cdot x)$ which by definition of a group necessarily exists. It is easy to verify that $f_g \circ f_{g^{-1}} = f_{g^{-1}} \circ f_g = f_{g \cdot g^{-1}} = f_{g^{-1} \cdot g} = (x \mapsto x = id_X)$.

This is a groupoid, because, it is a category (composition, associativity, identity) where every morphism is an isomorphism (every morphism has an inverse), and the group of isomorphisms of (the single-object category) $\mathcal{C}$, here $Hom(X, X)$, is precisely isomorphic to $(G, \cdot)$.

1.2)

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

I suppose Aluffi is referring to §I.1.1, and not §(II.)1.1. In there he mentions:

- $\mathbb{N}$: the set of natural numbers (that is, nonnegative integers);
- $\mathbb{Z}$: the set of integers;
- $\mathbb{Q}$: the set of rational numbers;
- $\mathbb{R}$: the set of real numbers;
- $\mathbb{C}$: the set of complex numbers.

Let us go through these sets one by one:

- $\mathbb{N}$: $(\mathbb{N}, +)$ is not a group (needs negative numbers, $x + 5 = 0$ has no solution), and neither is $(\mathbb{N}, \cdot)$ (e.g., $5 \cdot x = 1$ has no solution in $\mathbb{N}$).

- $\mathbb{Z}$: $(\mathbb{Z}, +)$ is a group, but $(\mathbb{Z}, \cdot)$ is not because it is not invertible (e.g., $2 \cdot x = 1$ has no solution in $\mathbb{Z}$).

- $\mathbb{Q}$: $(\mathbb{Q}, +)$ is a group, but $(\mathbb{Q}, \cdot)$ is not because it is not fully invertible (e.g., $0 \cdot x = 1$ has no solution in $\mathbb{Q}$). However, remove 0 from $(\mathbb{Q}, \cdot)$ and it becomes a group.

- $\mathbb{R}$: $(\mathbb{R}, +)$ is a group, but $(\mathbb{R}, \cdot)$ is not because it is not fully invertible (e.g., $0 \cdot x = 1$ has no solution in $\mathbb{R}$). However, remove 0 from $(\mathbb{R}, \cdot)$ and it becomes a group.

- $\mathbb{C}$: $(\mathbb{C}, +)$ is a group, but $(\mathbb{C}, \cdot)$ is not because it is not fully invertible (e.g., $0 \cdot x = 1$ has no solution in $\mathbb{C}$). However, remove 0 from $(\mathbb{C}, \cdot)$ and it becomes a group.

We can see that $(\mathbb{N}, +)$ is not a group, but $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all groups. Also, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, and $(\mathbb{C}, \cdot)$ are not groups. However, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, and $(\mathbb{C}^*, \cdot)$ are groups.

1.3)

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

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

$$(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e$$

Therefore, $h^{-1}g^{-1}$ is a 2-sided inverse for gh, and since the inverse of an element in a group is unique, $(gh)^{-1} = (h^{-1}g^{-1})$

1.4)

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

If $forall g \in G, g^2 = e$, then every element is its own inverse, i.e., multiply by g^{-1} on the left (or right), and we have $\forall g \in G, g = g^{-1}$. Let be $a, b \in G$. Then, we have $ba = (ba)^{-1} = a^{-1}b^{-1} = ab$, which is the definition of commutativity. Therefore, G is commutative.

1.5)

The 'multiplication table' of a group is an array compiling the results of all multiplications $g \cdot h$ (with the value on each row being the left operand, and the value on each column being the right operand; of course the table depends on the order in which the elements are listed in the top row and left-most 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!).

Another way to phrase this question is "prove that every element of the group can be reached in a single operation from any other (on the left, or on the right, both work)". Written in function notation, this means:

$$\forall a, b \in G, \exists g_r, g_c \in G, b = g_r \cdot a \text{ and } b = a \cdot g_c$$

For every element a, we can reach the identity with a^{-1} (on either side). Every element b can then be reached from the identity by multiplying it (on either side). We just have to pick the same side both times to find either $g_r = b \cdot a^{-1}$ and $g_c = a^{-1} \cdot b$. Since the group is closed under "multiplication", both these elements are guaranteed to exist.

This implies that every row and every column of the multiplication table of a group contains all elements of the group exactly once, since any element can be reached in a single multiplication (i.e., there as many possible inputs (1 sided operand) as possible outputs (i.e., applying an operand is an injection) and all outputs are reached (it's also a surjection)). This also implies that the multiplication table is a "Latin square", which is a square array of $|G|$ symbols, each occurring exactly once in each row and exactly once in each 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.

These multiplication tables are usually called "Cayley tables".

1.6.a) 1-element group

For the unique table of the trivial group (only 1 element); e is necessarily its own inverse. Some examples of this group are $(\{0\}, +)$ or $(\{1\}, \times)$. This group is trivially commutative.

$\cdot$	e
e	e

1.6.b) 2-element group

For the unique table of the group with 2 elements; both elements are necessarily their own inverse (or else there would be no e which is necessarily a self-inverse). Some examples of this group are $(\{1, -1\}, \times)$, or $(\mathbb{Z}_2, +)$ (two-hour clock with addition). This group is commutative, since, like in the exercise 1.4, every element is its own inverse.

$\cdot$	e	a
e	e	a
a	a	e

1.6.c) 3-element group

For the unique table of the group with 3 elements; the 3 elements cannot all be their own inverses, because if 2 elements are their own inverse, the third one cannot have an inverse. Another way of seeing this is the below: no matter the value given for each ?, this cannot be a Latin square (if we put two e's then we have multiple inverses, so we can deduce that a and b are inverses, and then we $a = b$; if we put two a's, we lose associativity (e.g.: $(aa)b = eb = b \neq a(ab) = aa = e$); etc).

$\cdot$	e	a	b
e	e	a	b
a	a	e	?
b	b	?	e

Instead, the 2 non-identity elements are necessarily inverses of each other. Some examples of this group are $(\{1, j, \overline{j}\}, \times)$ (where $j = e^{\tau/3}$ is a complex number called the third root of unity), or $(\mathbb{Z}_3, +)$ (three-hour clock with addition). This group is commutative because the identity necessarily commutes with everything, and inverses necessarily commute together, so here, all elements commute.

$\cdot$	e	a	a^{-1}
e	e	a	a^{-1}
a	a	a^{-1}	e
a^{-1}	a^{-1}	e	a

1.6.d) 4-element groups

For the case where $|G| = 4$, we have two possibilities.

The first one is a table where every element is a self-inverse. This gives you a group that is isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ (the Klein four-group, a torus made up of 2 two-hour clocks). Note that the permutations of the elements of the group give the same table, so there is only one table for this group up to reordering. It is commutative for the same reason as exercise 1.4.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

The second possibility where one element other than the identity is its own inverse, and the other two are mutual inverses. This gives you a group that is isomorphic to $(\mathbb{Z}_4, +)$ (a four-hour clock with addition, where 1 and -1 are mutual inverses, and 0 and 2 are their own inverse). Note that the permutations of the elements of the group give the same table, so there is only one table for this group up to reordering.

Since the identity and respective inverses commute, all that's left is to check the commutativity of the self-inverse element a with both of the mutual-inverses elements b and c. In this case, it is because there is "only one option left" in the Latin square that we get commutativity: e.g., $a \cdot b$ cannot equal e since they are not inverses, cannot equal a since $b \neq e$, cannot equal b since $a \neq e$, so we must have $a \cdot b = c$. The same reasoning can be applied to $b \cdot a$ to get c (hence $a \cdot b = b \cdot a$). With a relabelling, we apply this reasoning to $a \cdot c$ to get b and to $c \cdot a$ to get b (hence $a \cdot c = c \cdot a$). With this, we have proven commutativity.

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

1.6.e) Conclusion and remark

With that, we've proven that all groups of order ≤ 4 are commutative.

(Note that the commutativity can also be "seen" in all these tables by the fact that they are their own transpose.)

1.7)

Prove Corollary 1.11: Let g be an element of finite order, and let $n \in \mathbb{Z}$. Then $g^n = e \Leftrightarrow \exists k \in \mathbb{Z}, n = k|g|$ (n is a multiple of $|g|$).

By Lemma 1.10, if $g^n = e$, then $|g|$ divides n. Therefore, $\exists k \in \mathbb{Z}, n = k|g|$.

For the converse, we suppose $\exists k \in \mathbb{Z}, n = k|g|$. By definition of the order of a group element, $g^{|g|} = e$, so $g^n = g^{|g|k} = (g^{|g|})^k = e^k = e$. Hence, $g^n = e$.

1.8)

Let G be a finite group, with exactly one element f of order 2. Prove that $\Pi_{g \in G} g = f$.

I had some trouble, so I checked online and found this, meaning that the group probably needs to be not just finite but also abelian:

https://math.stackexchange.com/questions/2550052/let-g-be-a-finite-abelian-group-with-exactly-one-element-of-order-2-denoted

(A couple of notes: since $f^2 = e \Leftrightarrow f = f^{-1}$, it also means that f is the only self-inverse (involution) in G. Also, the order of operation is not given: this gives us a hint that the property $(\Pi_{g \in G}\ g)^2 = e$ does not rely on the order of operations.)

Since f is the only element which is a self-inverse of order 2, e is the only self-inverse of order 1, we have that for all other elements a g in G, g is not its own inverse. This means that the product of all elements of G is a product of pairs of inverses, which cancel out to the identity (given commutativity), except for the self-inverse f which remains. Therefore, $\Pi_{g \in G} g = f$.

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.

(This would be trivial if we could use Lagrange's theorem.)

Let us consider the set of elements of G of order 2, $M = \{g \in G \mid |g| = 2\}$, with $|M| = m$. We know that for all $g \in M$, $g = g^{-1}$. This means that M is the set of self-inverse elements (not counting e). This means that $G - M$ contains only pairs of inverses (with k such pairs), and the self-inverse e, so has its cardinal can be written $|G - M| = |G| - |M| = n - m = 2k + 1$, i.e., it is an odd number.

If $|G| = n$ is even, then it can be written as $2l$ for some $l \in \mathbb{N}$ with $l > k$. Consequently $|M| = |G| - (n - m) = 2l - (2k + 1) = 2(l - k) - 1$, which is odd, and > 0 since $l > k$. Therefore, G necessarily contains at least 1 element of order 2.

1.10)

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

We write $|g| = 2k + 1$ since it is odd.

$g^{|g|} = e \Rightarrow (g^2)^{|g|} = (g^{|g|})^2 = e^2 = e$

By Corollary 1.11, $(g^2)^{|g|} = (g^2)^{2k+1} = e \Leftrightarrow \exists l \in \mathbb{N}, |g| = 2k + 1 = l|g^2|$. Since $|g|$ is odd, both l and $|g^2|$ must be odd.

1.11)

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

Let $a, g \in G$.

$$\begin{aligned}(aga^{-1})^{|g|} &= (aga^{-1})(aga^{-1})...(aga^{-1}) \\ &= ag(a^{-1}a)g(a^{-1}a)g...ga^{-1} \\ &= ag^{|g|}a^{-1} \\ &= aea^{-1} \\ &= (aa^{-1}) \\ &= e\end{aligned}$$

By Lemma 1.10, $|aga^{-1}|$ is a divisor of $|g|$.

By definition, $(aga^{-1})^{|aga^{-1}|} = e$. However, similarly to above, $(aga^{-1})^{|aga^{-1}|} = ag^{|aga^{-1}|}a^{-1}$. So we have $ag^{|aga^{-1}|}a^{-1} = e$; then, multiplying on the left by a^{-1} and right by a, we get $g^{|aga^{-1}|} = e$. By Lemma 1.10, $|g|$ is a divisor of $|aga^{-1}|$.

Since the divisibility relation is an order relation (antisymmetric), the only time two numbers can be mutually divisors of each other is if we're in the reflexive case (i.e., they are equal). Therefore, $|g| = |aga^{-1}|$.

Applying this identity to the elements $g \to gh$ with $a \to h$, we have $|gh| = |(h)(gh)(h^{-1})| = |hg|$

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]

We remind call that the neutral element for 2D square matrix multiplication is the identity matrix I_2.

$$g^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$g^4 = (g^2)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

$$h^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$

$$h^3 = h^2h = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

We will now prove by induction that $\forall n \geq 1, P(n) : (gh)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$.

Initiatialization:

$$gh = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

True for $n = 1$.

Inheritance:

We suppose $P(n)$ true for a specific n, we'll show that $P(n+1)$ holds.

$$(gh)^{n+1} = (gh)^n(gh) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (n+1) \\ 0 & 1 \end{pmatrix}$$

Therefore $P(n+1)$ is true. This prives inheritance.

By induction, $P(n)$ is true for all $n \geq 1$.

Therefore, there exists no $n \geq 1$ such that $(gh)^n = I_2$, hence $|gh| = \infty$.

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]

We take the 6-hour clock Z_6, and $g = h = [3]_6$, the equivalence class of 3 modulo 6. We have $g^2 = h^2 = gh = hg = [3]_6 + [3]_6 = [6]_6 = [0]_6$, so $|g| = |h| = 2$ and $|gh| = 1$. However, $\text{lcm}(|g|, |h|) = 2 \neq |gh| = 1$

1.14)

As a counterpoint to Exercise 1.13, prove that if g and h commute, and $\gcd(|g|, |h|) = 1$ (they are coprime), 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]

First, we remark that for any $x \in G$, $x^N = e \Leftrightarrow e = (x^{-1})^N$, so $|x| = |x^{-1}|$.

We have that $\gcd(|g|, |h|) = 1$, and we know that $|g||h| = \gcd(|g|, |h|)\text{lcm}(|g|, |h|)$ so we have $|g||h| = \text{lcm}(|g|, |h|)$.

Let $N = |gh|$. Then, given that $(gh)^N = e$, that g and h commute, and multiplying by $(h^{-1})^N$ on the right of both side, we have $(gh)^N(h^{-1})^N = g^N h^N (h^{-1})^N = g^N(hh^{-1})^N = g^N = e(h^{-1})^N = (h^{-1})^N$. Therefore, $g^N = (h^{-1})^N = f$.

We now study $f^{|g|}$ and $f^{|h|}$.

We have $f^{|g|} = (g^N)^{|g|} = g^{N|g|} = e$.

Similarly, $e = h^{|h|} = (h^{-1})^{|h|} = ((h^{-1})^{|h|})^N = ((h^{-1})^N)^{|h|} = f^{|h|}$ (by our initial remark).

Therefore, $M = |f| = |g^N| = |(h^{-1})^N| = |h^N|$ divides both $|g|$ and $|h|$. Since $|g|$ and $|h|$ are coprime, $M = 1$. Therefore $f = g^N = e$, so $N = |gh|$ is a multiple of $|g|$ and $f = (h^{-1})^N = e$ so $N = |gh|$ is a multiple of $|h^{-1}| = |h|$. Since $|g|$ and $|h|$ are coprime, we can further say that $|gh|$ is a multiple of

their LCM/product $|g||h|$ (using, for example, the fundamental theorem of arithmetic).

Using Proposition 1.14 (i.e, if $gh = hg$, then $|gh|$ divides $\text{lcm}(|g|, |h|)$), we can also tell that $N = |gh|$ divides $\text{lcm}(|g|, |h|) = |g||h|$.

Putting both results together using the antisymmetry of the divisibility relation, we have $N = |gh| = |g||h|$.

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 (the fact that the order of the product of two elements with coprime order is equal to the product of their orders) to compute the order of $g^{p^m} h^s$.) [§2.1, 4.11, IV.6.15]

We suppose that $|h|$ is finite but does not divide $|g|$. Using the fundamental theorem of arithmetic, if $|h|$ doesn't divide $|g|$, then it has at least one prime factor that $|g|$ does not have. Then, there is a prime integer p such that $|g| = p^m r$, $|h| = p^n s$, with r and s (potentially composite), both independently coprime with p, and $0 \leq m < n$.

We know from exercise 1.14 that if 2 elements a and b commute (which is always the case in a commutative group like here), if the two elements have coprime order, then $|ab| = |a||b|$.

The order $|x^k|$ of x^k, is $\frac{|x|}{\gcd(|x|,k)}$, assuming $|x|$ is finite (Proposition 1.13).

We study $g^{p^m} h^s$.

The order of g^{p^m} is $\frac{|g|}{\gcd(|g|,p^m)} = \frac{p^m r}{p^m} = r$ because p^m divides $|g|$.

Similarly, the order of h^s is $|h|/\gcd(|h|, s) = \frac{p^n s}{s} = p^n$ because s divides $|h|$.

Since G is a commutative group, g^{p^m} and h^s commute. By Exercise 1.14, $|g^{p^m} h^s| = |g^{p^m}||h^s| = p^n r = p^{n-m}(p^m r) = p^{n-m}|g| > |g|$.

This is a contradiction with the fact that $|g|$ has *maximal* finite order. Therefore, our assumption that $|h|$ does not divide $|g|$ must be false.

Conclusion: if G is an abelian group, $g \in G$ has maximal finite order, and $h \in G$ has finite order in G, then $|h|$ divides $|g|$.

Section 2)

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

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

would be

$$M_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \tag{2}$$

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.

We first notice that we can write down the formal expression of M_σ, as the Krocker delta $\delta_{i\sigma(i)}$. We know that the product of two Kronecker deltas is the Kronecker delta of the product of the indices; namely, $\delta_{ij}\delta_{jk} = \delta_{ik}$. Therefore, we have that the product of two matrices $M_\sigma M_\tau = \delta_{i\sigma(i)}\delta_{\sigma(i)\tau(\sigma(i))} = \delta_{i\tau(\sigma(i))} = M_{\sigma\tau}$, as desired.

2.2)

Prove that if $d \leq n$ then S_n contains elements of order d.

We will use strong induction on n.

Initialization: for S_1, the case is trivial (the identity element has order 1). For S_2, we saw that this group was necessarily isomorphic to $\mathbb{Z}_2$, which has the identity, and one element of order 2.

Heredity: For some $k \in \mathbb{N}$, we suppose that the property is true for all $d \leq k$. We will show that it is true for $k+1$. Keeping the last element fixed, we see that the portion of S_{k+1} that can permute is isomorphic to S_k: by our hypothesis, it thus has elements of order d for all $d \leq k$. We just need to show that we can find an element of order $k+1$ in S_{k+1}.

We take the a cyclic permutation of all elements (which acts like a Caesar cypher of distance parameter 1): each $i > 1$ is mapped to to $i - 1$, and 1 is mapped to $k + 1$. Let us prove that this permutation has order $k + 1$.

We can see that the cycle of this permutation is $1 \to k+1 \to k \to k-1 \to \ldots \to 1$, which has length $k+1$.

We now show that the order of any cyclic permutation is the length of the cycle. Let be S_n a permutation group and C a cycle in it, generated by a permutation σ. We denote elements of the cycle as $c_1, c_2, \ldots, c_m$ with $m \leq n$ such that the cycle can be expressed as $c_1 \to c_2 \to \ldots \to c_m \to c_1$. We have that $\forall j \in [[1, m]], \sigma^0(c_j) = c_j$, trivially. Then, we have $\sigma^1(c_j) = c_{[j]_m+1}$ (meaning j modulo m plus 1), and so on. We see that $\sigma^{n-1}(c_j) = c_{[j]_m+n-1}$, and $\sigma^n(c_j) = c_{[j]_m+n} = c_{[j]_m} = c_j$. Therefore, the order of σ is m, the length of the cycle.

Therefore, we have shown that S_{k+1} has cyclic permutations of length $k+1$, and thus elements of order $k+1$, which completes the proof.

2.3)

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

From the previous exercise, it is clear that any cyclic permutation of length n is such an element.

2.4)

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

We first write the dihedral group D_8 as the group of symmetries of a square. We label the vertices of the square as A, B, C, D, in a clockwise manner. We use 2×2 matrices with these labels to represent the symmetries of the square, and we have that the elements of D_8 are:

$$\begin{bmatrix} A & B \\ D & C \end{bmatrix} \rightarrow \text{Identity}$$

$$\begin{bmatrix} B & C \\ A & D \end{bmatrix} \rightarrow \text{Rotation by } 90^\circ$$

$$\begin{bmatrix} C & D \\ B & A \end{bmatrix} \rightarrow \text{Rotation by } 180^\circ$$

$$\begin{bmatrix} D & A \\ C & B \end{bmatrix} \rightarrow \text{Rotation by } 270^\circ$$

$$\begin{bmatrix} A & D \\ B & C \end{bmatrix} \rightarrow \text{Reflection over the diagonal } AC$$

$$\begin{bmatrix} C & B \\ D & A \end{bmatrix} \rightarrow \text{Reflection over the diagonal } BD$$

$$\begin{bmatrix} D & C \\ A & B \end{bmatrix} \rightarrow \text{Reflection over the horizontal axis}$$

$$\begin{bmatrix} B & A \\ C & D \end{bmatrix} \rightarrow \text{Reflection over the vertical axis}$$

Now, using the $2 \times n$ notation for permutations, we can write the corresponding permutations in S_4 as:

$$\begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix} \to \text{Identity}$$
$$\begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix} \to \text{Rotation by } 90^\circ$$
$$\begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} \to \text{Rotation by } 180^\circ$$
$$\begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix} \to \text{Rotation by } 270^\circ$$
$$\begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} \to \text{Reflection over the diagonal } AC$$
$$\begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix} \to \text{Reflection over the diagonal } BD$$
$$\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} \to \text{Reflection over the horizontal axis}$$
$$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} \to \text{Reflection over the vertical axis}$$

Note that there exist other permutations which are not in the image of this homomorphism, such as the transposition (AB), which is not a symmetry of the square. This homomorphism is thus injective, but not bijective.

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 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 $x^{i_1}y^{i_2}x^{i_3}y^{i_4}\dots$ equals x^iy^j for some i, j with $0 \le i \le 1$, $0 \le j < n$.)

Two of the relations are very easy to see: $x^2 = e$ (for any axial symmetry flip x) and $y^n = e$ (for any n-rotation y). Another hint (given at the bottom of page 52, as done on an imaginary pentagon) tells us to study $yxyx$ (hinting that it is equal to e).

We first note that $x^{-1} = x$ since any axial symmetry is an involution. Geometrically speaking, we can see that the operation $x^{-1}yx$ is a rotation by $2\pi/n$ in the opposite direction to y. We can thus write $x^{-1}yx = y^{-1}$,

and thus $yxyx = e$. This is our 3rd relation, which we can also rewrite as $yx == x^{-1}y^{-1} = xy^{n-1}$.

We can now write any element of D_{2n} as $x^i y^j$ for $0 \leq i \leq 1$, $0 \leq j < n$. Any power of x reduces to e (if the exponent is even) or x (if the exponent is odd), any power k of y reduces to $y^{[k]_n}$, and any yx term sandwiched between an x and a y terms can be changed to xy^{n-1} in order to reduce with the x (or e) on the left, and the $y^{[k]_n}$ on the right. Through this algorithm, we can always get an element of the form $x^i y^j$ for $0 \leq i \leq 1$, $0 \leq j < n$.

2.6)

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

We can take the dihedral group D_{2n}, and take the reflection x and the rotation y (as defined in the previous exercise). Taking $g = x$ and $h = xy$, we have that $|g| = |x| = 2$ (by the first relation), $|h| = |xy| = 2$ (by the third relation) and $|gh| = |xxy| = |y| = n$ (by the second relation).

As for the case with $n = 1$, we take the group $(\mathbb{Z}_2, +)$ and set $g = h = 1$; their sum is the identity 0, which has order 1 (technically, to stay in the D_{2n} picture, this is isomorphic to the group of symmtries of a "2-gon", a line, with either the identity, or a flip across its mediatrix).

2.7)

Find all elements of D_{2n} that commute with every other element. (The parity of n plays a role.)

A pair of elements commute iff $xy = yx$. Let a be our test element. We want a to have the property $\forall x \in D_{2n}, ax = xa$. We can write $a = x^i y^j$ for $0 \leq i \leq 1$, $0 \leq j < n$. We have that $ax = x^i y^j x = x^i y^{j-1}(yx) = x^i y^{j-1} x y^{-1} = x^i y^{j-2} x y^{-2} = \ldots = x^{i+1} y^{-j} = x x^i y^{-j} = xa'$. Therefore, only elements such that $a' = x^i y^{-j} = x^i y^j = a$ commute, this is equivalent (by cancelling the eventual x on both sides and aggregating the y's) to $y^{2j} = e$, which is true iff $j = 0$ or $2j = n$. Therefore, if n is odd, only the identity commutes with all elements, and if n is even, both the identity and the rotation of angle π commute with all elements.

2.8)

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

https://en.wikipedia.org/wiki/Polyhedral_group

The five platonic solids are the tetrahedron, the cube, the octahedron, the dodecahedron, and the icosahedron. We can find the orders of their symmetry groups by finding the number of symmetries of each solid.

TetrahedronL The tetrahedron has 4 vertices, 6 edges, and 4 faces (all equilateral triangles). We can rotate the tetrahedron by $2\pi/3$ about an axis perpendicular through the center of a face. We can also flip the tetrahedron across a plane through an edge and the midpoint of its opposite edge.

(distinct combinations ? proof ?)

... TODO

2.9)

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

We define the relation $\sim$ as $\forall a, b \in \mathbb{Z}, a \sim b \Leftrightarrow \exists k \in \mathbb{Z}, a - b = kn$. We will show that this relation is reflexive, symmetric, and transitive.

Reflexivity:

$$\forall a \in \mathbb{Z}, a - a = 0 = 0 \cdot n \Rightarrow a \sim a$$

Symmetry:

$$\begin{aligned} \forall a, b \in \mathbb{Z}, a \sim b &\Leftrightarrow \exists k \in \mathbb{Z}, a - b = kn \\ &\Leftrightarrow \exists k \in \mathbb{Z}, b - a = -kn \\ &\Leftrightarrow b \sim a \end{aligned}$$

Transitivity:

$$\begin{aligned} \forall a, b, c \in \mathbb{Z}, (a \sim b) \wedge (b \sim c) &\Leftrightarrow \exists k, l \in \mathbb{Z}, (a - b = kn) \wedge (b - c = ln) \\ &\Leftrightarrow a - c = (a - b) + (b - c) = (k + l)n \\ &\Leftrightarrow a \sim c \end{aligned}$$

Therefore, the relation $\sim$ is an equivalence relation.

2.10)

Prove that $\mathbb{Z}/n\mathbb{Z}$ contains precisely n elements.

Each element of $\mathbb{Z}$ can be written uniquely as $m+kn$ with $m \in [[0, n-1]]$ and $k \in \mathbb{Z}$. Therefore, we have n possible values for m. Because congruence modulo n equates two numbers in $\mathbb{Z}$ if their difference is a multiple of n, we have that m and $m + kn$ are equivalent. Therefore, we can consider an equivalence class associated with m to contain all elements of the form $m + kn$. Since we have precisely n such equivalence classes, $\mathbb{Z}/n\mathbb{Z}$ contains precisely n elements.

2.11)

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

We write an odd integer as $2n + 1$ for $n \in \mathbb{Z}$. We have that $(2n + 1)^2 = 4n^2 + 4n + 1 = 4(n^2 + n) + 1$. We can see that $n^2 + n$ is always even, because: if n is even, then n^2 is even, and n is even, so their sum is even; and if n is odd, then n^2 is odd, and n is odd, so their sum is even. Therefore, we can write $n^2 + n = 2m$ for some $m \in \mathbb{Z}$, and thus $(2n + 1)^2 = 8m + 1$, which is congruent to 1 modulo 8.

2.12)

Prove that there are no 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 $a = 2k$, $b = 2l$, $c = 2m$, you would have $k^2 + l^2 = 3m^2$. What's wrong with that?)

We can write $a^2 + b^2 = 3c^2$ as $a^2 + b^2 = 3c^2 + 4k$ with $k = 0$. Any solution to the first equation must thus respect the properties of the second equation. We study these properties by looking at the equation modulo 4.

$$\begin{aligned}[a]_4^2 + [b]_4^2 = [3]_4[c]_4^2 &\Leftrightarrow [a]_4^2 + [b]_4^2 = [-1]_4([c]_4^2) \\ &\Leftrightarrow [a]_4^2 + [b]_4^2 + [c]_4^2 = [0]_4\end{aligned}$$

Since 0 is even, this condition gives us that either two of the numbers have to be odd, or none of them are. However, looking back at the first equation, if c is even, then $[c]_4^2 = 0$, and $[3]_4[c]_4^2 = 0$, which means that a and b must be both even or both odd. If a and b are both odd (i.e., either congruent to

1 or -1), then $[a]_4^2 = 1$ and $[b]_4^2 = 1$ and their sum, supposedly equal to 0, is congruent to 2, which is a contradiction. In this case, both a and b must be even.

Now if c is odd, then $[3]_4[c]_4^2 = [3]_4[1]_4 = [3]_4 = [-1]_4$. Since c is odd, only one of a or b must be odd. Without loss of generality, we choose that to be b, in which case $[b]_4^2 = 1$. Our "the three sum to 0" equation above then tells us that $[a]_4^2 + [2]_4 = [0]_4$, so $[a]_4^2 = [2]_4$, which is a contradiction, because there is no number $[a]_4$ such that $[a]_4^2 = [2]_4$ (the image of the squaring function is $\{[0]_4, [1]_4\}$). Therefore, c cannot be odd.

We've thus shown that the only case not leading to a contradition is the case where all three numbers are even, and this applies to the original equation.

Letting $a = 2k$, $b = 2l$, $c = 2m$, you would have $k^2 + l^2 = 3m^2$, which is just a rewriting of our initial equation. After iteration this process until a maximal instance of 2's has been removed from the prime factorization of each number, we will eventually reach a point where either k, l, or (non-exclusive) m is odd, which is a contradiction. Therefore, there are no integers a, b, c such that $a^2 + b^2 = 3c^2$.

This exercise is interesting because it teaches us that number theoretic equations that rely on odd and evenness can effectively be studied using $\mathbb{Z}/4\mathbb{Z}$.

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 $\gcd(m, n) = 1$.

This is known as Bézout's identity. We remind Corollary 2.5.: The class $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m, n) = 1$. So this exercise can also be reduced to proving that $\exists a, b \in \mathbb{Z}, am + bn = 1$ if and only if $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$.

$\gcd(m, n) = 1 \Rightarrow \exists a, b \in \mathbb{Z}, am + bn = 1$

We suppose that $\gcd(m, n) = 1$, by Corollary 2.5, we have that $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$. This means that for every $[c]_n \in \mathbb{Z}/n\mathbb{Z}$, there exists $a \in \mathbb{Z}$ such that $[am]_n = [c]_n$. If we take $[c]_n = [1]_n$, this means that $am = 1 + kn$ for some $k \in \mathbb{Z}$. We can rewrite this as $am + bn = 1$ for $b = -k$.

$\exists a, b \in \mathbb{Z}, am + bn = 1 \Rightarrow \gcd(m, n) = 1$

We suppose that $\exists a, b \in \mathbb{Z}, am+bn = 1$. We can write this as $am = 1-bn$, which means that m divides $1-bn$. Suppose m and n have a common prime factor p: this prime factor would divide m and n, and thus would divide $1-bn$ (equivalently its opposite $bn-1$) and bn. However, this is a contradiction, because the only number that can divide two numbers that are off by 1 is 1. Therefore, m and n have no common prime factors, and $\gcd(m, n) = 1$.

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.

We remind Lemma 2.2: If $a \equiv a' \mathrm{mod} n$ and$b \equiv b' \mathrm{mod} n$, then $(a+b) \equiv (a'+b') \mathrm{mod} n$.

Our analogue is thus: $a \equiv a' \mathrm{mod} n$ and$b \equiv b' \mathrm{mod} n$, then $(a \times b) \equiv (a' \times b') \mathrm{mod} n$.

We now show that it is well-defined (there exists a commutative square diagram with an epimorphism from $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$ in one direction, and with the respective multiplications in the other). We take $a \equiv a' \mathrm{mod} n$ and$b \equiv b' \mathrm{mod} n$. This means that $a - a' = kn$ and $b - b' = ln$ for some $k, l \in \mathbb{Z}$. We have that $ab - a'b' = ab - ab' + ab' - a'b' = a(b-b') + (a-a')b' = a(ln) + (kn)b' = n(al + kb')$. The first and last terms of this equation give us that $ab \equiv a'b' \mathrm{mod} n$, as needed.

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 $\varphi(n)$ of elements of $(\mathbb{Z}/n\mathbb{Z})^*$ is Euler's φ-function. The reader must proved that if n is odd, then $\Phi(2n) = \Phi(n)$.

2.16)

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

We note that $7^2 = 49$, $7^3 = 343$, and $7^4 = 2401$, so the order of 7 in $(\mathbb{Z}/10\mathbb{Z}, \times)^*$ is 4. Since multiplication is well-defined in $\mathbb{Z}/10\mathbb{Z}$, we have:

$$\begin{aligned}
[1238237^{18238456}]_{10} &= [7]_{10}^{18238456} \\
&= [7]_{10}^{4 \cdot 4559614} \\
&= ([7]_{10}^{4})^{4559614} \\
&= [7^4]_{10}^{4559614} \\
&= [1]_{10}^{4559614} \\
&= [1]_{10}
\end{aligned}$$

2.17)

Show that if $m \equiv m' mod n$, then $\gcd(m, n) = 1$ if and only if $\gcd(m', n) = 1$.

We use the result from exercise 2.13: $\gcd(m, n) = 1 \Leftrightarrow \exists a, b \in \mathbb{Z}, am + bn = 1$; similarly, $\gcd(m', n) = 1 \Leftrightarrow \exists a', b' \in \mathbb{Z}, a'm' + b'n = 1$. We have that $m \equiv m' \mathrm{mod} n$, so $m - m' = kn$ for some $k \in \mathbb{Z}$. We can rewrite this as $m = m' + kn$. We can now substitute m in Bézout's identity: $a(m' + kn) + bn = 1 \Rightarrow am' + akn + bn = 1$. We can now let $a' = a + ak$ and $b' = b$, and we have that $\gcd(m, n) = 1 \Leftrightarrow \gcd(m', n) = 1$.

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 $\mathbb{Z}/n\mathbb{Z}$ corresponds to the product of the corresponding permutations.

We can define the function $f : \mathbb{Z}/d\mathbb{Z} \to S_n$ as $f([a]_d) = \sigma_a$, where σ_a is the permutation that maps i to $i + a$ modulo d (our Caesar cypher mentioned above, over the d first elements, or any choice of d elements really).

This function is injective because the permutation σ_a is uniquely determined by a. This can immediately be seen by studying with which element the first element (which we can label 0) is replaced: it is replaced with a (the a-th element), leading to d distinct outputs for d possible inputs. More formally, if $a, b \in \mathbb{Z}/d\mathbb{Z}, a \neq b$, then σ_a and σ_b are distinct permutations, as they map i to $i + a$ and $i + b$ respectively, and $a \neq b$ implies that $i + a \neq i + b$ for any i.

We can see that the sum of equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ corresponds to the product of the corresponding permutations through the following commutative diagram:

$$\begin{array}{ccc} (\mathbb{Z}/d\mathbb{Z})^2 & \xrightarrow{+_{\mathbb{Z}/d\mathbb{Z}}} & \mathbb{Z}/d\mathbb{Z} \\ ([a]_d, [b]_d) & & [a+b]_d \\ \Big\downarrow{\scriptstyle (f,f)} & & \Big\downarrow{\scriptstyle f} \\ S_n^2 & \xrightarrow[\circ_{S_n}]{} & S_n \\ (\sigma_a, \sigma_b) & & \sigma_{a+b} \end{array}$$

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.

For $\mathbb{Z}/5\mathbb{Z}$, we have the elements $[1]_5, [2]_5, [3]_5, [4]_5$ which are coprime with 5.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

For $\mathbb{Z}/12\mathbb{Z}$, we have the elements $[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}$ which are coprime with 12.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

The two groups are not isomorphic, because the first group has elements of order 4 and the other doesn't. In fact, the former is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, and the latter is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (the Klein 4-group).

Part II

Extra exercises by/for the group

Chapter I) 1) Set notation)

Write the following in set notation (as a list of numbers, and algebraically):

- the set of all odd integers
- the set of all integers that are not multiples of 3
- the set of integers from 10 (included) to 20 (included)
- the set of integers from 10 (included) to 20 (excluded)
- the set of pairs of integers with both elements of the same value
- the set of triplets of real numbers that together sum to 1
- the set of pairs of positive real numbers that together sum to 1
- the set of n-tuplets (for any n) of real number that together sum to 1
- the set of all natural numbers such that there exists at least one triplet of positive even numbers which are all different and which sum to that number.

Now take the sets in their algebraic notation, and represent them both as a list of numbers (as a logical sequence or just a couple of examples), and as a "description" of what they are:

- $\{3n + 2 \mid n \in \mathbb{N}\}$
- $\{3k + 2 \mid k \in \mathbb{Z}\}$
- $\{2^i \mid i \in [[0, 10]]\}$
- $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$
- $\{x \in \mathbb{R} \mid -2 \leq x \leq 2\}$
- $\{(m, n, p) \in \mathbb{N}^3 \mid m + n + p = 10\}$

Chapter I) 3) Slices and coslices)

Provide a concrete example of a slice category and of a coslice category based on the category of real vector spaces $Vect_{\mathbb{R}}$, or its subcategory of finite real vector spaces. How does this relate to the transpose of a matrix, or of a product of matrices ?