I.1: Naive Set Theory

I.1.1

Locate a disucssion of Russell's paradox, and understand it.

Solution: Consider the set $X = \{a | a \notin a\}$, where a represents a set. If $X \in X$, by definition, $X \notin X$, a contradiction. If $X \notin X$, by definition, $X \in X$, another contradiction.
This was noticed by Ernst Zermelo and Bertrand Russell, and caused an effort to make set theory more rigorous. This effort resulted in the Zermelo-Fränkel axioms of set theory. The solution to the paradox is that the aforementioned X is not a set in the first place. $\square$

I.1.2

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

Solution: Let $\sim$ be an equivalence relation on S and let $\mathscr{P}_\sim = S/\sim$ be the set of equivalence classes of elements of S with respect to $\sim$. If S is non-empty, then it has at least one element x. Since $\sim$ is an equivalence relation, it is reflexive, so that $x \sim x$. Hence, the equivalence class $[x]_\sim \neq \varnothing$ for any $x \in S$ as $x \in [x]_\sim$. Let $[x]_\sim$ and $[y]_\sim$ be distinct equivalence classes in S. That is, there exists some $z \in [x]_\sim$ such that $z \notin [y]_\sim$, or vice versa (we suppose the former without loss of generality). Next, suppose that $[x]_\sim$ and $[y]_\sim$ are *not* disjoint, that is, there exists $w \in S$ such that $w \in [x]_\sim$ and $w \in [y]_\sim$. By definition, $w \sim x$. From above, we also have $x \sim z$. Thus, since $\sim$ is an equivalence relation and is transitive, $w \sim z$. However, by definition we also have $y \sim w$, and by transitivity we acquire $y \sim z$, hence $z \in [y]_\sim$, contradicting our definition of z, hence no such point is shared by distinct equivalence classes of S, hence distinct equivalence classes are disjoint. Since for every $x \in S$, we have $x \in [x]_\sim$, we have $\bigcup_{x \in S} [x]_\sim = S$. Thus, $\mathscr{P}_\sim$ is a partition of S. $\square$

I.1.3

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

Solution: Let $\mathscr{P}$ be a partition of S. Since the union of all sets in the partition is S, for every $x \in S$, x is in a unique set of the partition $\mathscr{P}$, since the sets of a partition are disjoint. Define $\sim$ in on S such that $x \sim y$ if and only if x and y lie in the same set of the partition.$\square$

I.1.4

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

Solution: There are five such partitions: $\{1, 2, 3\}$; $\{\{1, 2\}, \{3\}\}$; $\{\{1, 3\}, \{2\}\}$;$\{\{2, 3\}, \{1\}\}$; and $\{\{1\}, \{2\}, \{3\}\}$.$\square$

I.1.5

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

Solution: Let the relation R be defined on the set $S = x, y, z$ by simply specifying $R \subset S^2 = \{(x, x), (y, y), (z, z), (x, y), (y, x), (y, z), (z, y)\}$. This relation is reflexive and symmetric, but is not transitive since $x \sim y$ and $y \sim z$ but $x \not\sim z$.$\square$

I.1.6

Define a relation $\sim$ on the set $\mathbb{R}$ of real numbers by setting $a \sim b \iff b - a \in \mathbb{Z}$. Prove that this is an equivalence relation, and find a 'compelling' description for $\mathbb{R}/\sim$. Do the same for the relation $(a_1, a_2) \approx (b_1, b_2) \iff b_1 - a_1 \in \mathbb{Z}$ and $b_2 - a_2 \in \mathbb{Z}$.

Solution: Since $a - a = 0 \in \mathbb{Z}$ for all $a \in \mathbb{R}$, $a \sim a$. Suppose $a \sim b$. By definition $b - a = n$ for some $n \in \mathbb{Z}$. Then $a - b = -n \in \mathbb{Z}$, so that $b \sim a$. Thus, $\sim$ is reflexive and symmetric. Next suppose $a \sim b$ and $b \sim c$. Then $b - a = m \in \mathbb{Z}$ and $c - b = n \in \mathbb{Z}$. We have $c - a = (c - b) + (b - a) = n - m \in \mathbb{Z}$. Thus, $a \sim c$ and $\sim$ is transitive. Since $\sim$ is symmetric, reflexive, and transitive, it is an equivalence relation. The interpretation of $\sim$ is that it is the set of all sets of translated integers on the real line. Consider the relation $\approx$ defined as above. The proof that this is an equivalence relation is so similar to the proof given above that it is omitted. The partition described by this equivalence relation is the set of all vertically and horizontally translated sets of the integer point lattice $\mathbb{Z} \times \mathbb{Z}$ in the plane.$\square$

I.2: Functions Between Sets

I.2.1

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

Solution: Label S so that $S = \{1, ..., n\}$. The first element can be mapped to any of the n elements of S. Given the mapping for the first element, $(n-1)$ elements remain for the second element, so there are $n(n-1)$ ways to map the first two elements. By induction, we conclude that there are $n(n-1)(n-2)...(2)(1) = n!$ ways of forming a bijection from a set of n elements to itself.□

I.2.2

Prove statement (2) in Proposition 2.1. You may assume that given a family of disjoint nonempty subsets of a set, there is a way to choose one element in each member of the family.

Solution: Statement (2) of Proposition 2.1 states *f has a right-inverse if and only if it is surjective.*

$\Longrightarrow$) Suppose that f has a right inverse g. Then, by definition, for every $b \in B$, $f(g(b)) = b$. Then it is clear that $g(b) \in f^{-1}(b)$, so that f is surjective.
$\Longleftarrow$) Suppose that f is surjective. By definition, the fibers of every element of B, $f^{-1}(b)$, are disjoint and non-empty. If we assume that there is a way to choose one element in each member of this disjoint nonempty subsets of B, then let a_b be the element of A chosen from $f^{-1}(b)$. Then, define $g(b) = a_b$. Then we have $f(g(b)) = f(a_b) = b$ by definition, and g is a left inverse of f. □

I.2.3

Prove that the inverse of a bijection is a bijection and that the composition of two bijections is a bijection.
Solution: Suppose f is a bijection. Then f has an inverse, f^{-1}. We have $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$. Then f is the inverse of f^{-1}, hence f^{-1} is a bijection. Suppose next that $f : A \to B$ and $g : B \to C$ are bijections, and consider $g \circ f : A \to C$. Then $(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A$, and $(g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_B$. Hence $g \circ f$ has an inverse and is therefore bijective.□

I.2.4

Prove that 'isomorphism' is an equivalence relation (on any set of sets).
Solution: Let S be a set of sets and let A, B, C represent elements of S. Since $\mathrm{id}_A : A \to A$ is a bijection, we have $A \sim A$ for all sets A. Suppose $A \sim B$, so that there exists a bijection $f : A \to B$. However, we see from above that the inverse $f^{-1} : B \to A$ is also a bijection, hence $B \sim A$. Suppose next $A \sim B$ and $B \sim C$. Then there exist bijections $f : A \to B$ and $g : B \to C$. From above, their composition $g \circ f : A \to C$ is a bijection, hence $A \sim C$. We have proven the properties of reflexivity, symmetry, and transitivity for isomorphisms and have therefore proven that isomorphism is an equivalence relation in sets of sets. □

I.2.5

Formulate a notion of epimorphism, in the style of the notion of monomorphism seen in §2.6, and prove a result analogous to Proposition 2.3, for epimorphisms and surjections.
Solution: Definition of epimorphism: A set is an *epimorphism* if and only if for all sets Z and for all functions $g : Z \to B$, there exists some function $\alpha : Z \to A$ such that $f \circ \alpha = g$.
Theorem: A function is surjective if and only if it is an epimorphism.
Proof: $\Longrightarrow$) Let f be a surjective function and g a function from Z to B. Since f is surjective, the fibers of the elements of B, $f^{-1}(\{b\})$, are non-empty. Then, define $\alpha : Z \to A$ such that $\alpha(z) = a$ for some $a \in f^{-1}(\{g(z)\})$, which is non-empty because f is surjective, assuming we are allowed to choose a member of each fiber. It is clear that $f \circ \alpha = g$.

$\Longleftarrow$) Suppose f is an epimorphism. Let $Z = B$ and $g = \mathrm{id}_B$. Since f is an epimorphism, there exists $\alpha : B \to B$ such that $f \circ \alpha = \mathrm{id}_B$. However, this is precisely what it means to have a left inverse, which implies that f is surjective. $\square$

INTENDED Solution: The solution above was not actually what was intended. The intended definition of epimorphism as given in section 4 (page 29) of the book is: for all sets Z and all functions $\beta', \beta'' : B \to Z$, f is an epimorphism if and only if $\beta' \circ f = \beta'' \circ f \to \beta' = \beta''$.
Theorem: A function is surjective if and only if it is an epimorphism.
Proof: $\Longrightarrow$) Suppose $f : A \to B$ is surjective and $\beta', \beta'' : B \to Z$ are such that $\beta' \circ f = \beta'' \circ f$. Let $b \in B$. Since f is surjective, there exists some $a \in A$ such that $f(a) = b$, hence $\beta'(b) = \beta'(f(a)) = \beta''(f(a)) = \beta''(b)$. Thus, $\beta' = \beta''$.
$\Longleftarrow$) Suppose f is not surjective. We will show by contradiction that f is not an epimorphism. If f is not surjective, there exists some $b_0 \in B$ such that $f(a) \neq b$ for all $a \in A$. Let $Z = \{0, 1\}$ and define $\beta' : B \to Z$ so that $\beta'(b) = 0$ for $b \neq b_0$ and $\beta'(b) = 1$ for $b = b_0$. Define $\beta''(b) = 0$. Thus, it is clear $\beta' \circ f = \beta'' \circ f$ with $\beta' \neq \beta''$, so that f is not an epimorphism. Hence, surjective functions are precisely those functions which are epimorphisms in the Set category. $\square$

I.2.6

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

Solution: A section is a right inverse of a projection function. We need to find $g : A \to A \times B$ such that $\pi_A \circ g = \mathrm{id}_A$. To do this, we can simply choose any function $f : A \to B$ and set $g(a) = (a, f(a))$. It is clear that this is a right inverse (or section) of the projection function. $\square$

I.2.7

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

Solution: Define the function $\phi : \Gamma_f \to A$ by $\phi((a, f(a))) = a$. Since f is a function, it is defined for all $a \in A$, hence the fiber of a is always non-empty and always has $(a, f(a))$ as a member, hence ϕ is surjective. Next, suppose $(a_1, f(a_1) \neq (a_2, f(a_2)$. If $a_1 = a_2$, then we must have $f(a_1) = f(a_2)$ since f is well-defined. However, this contradicts the inequality of the ordered pairs. Thus, $a_1 \neq a_2$, which is to say $\phi((a_1, f(a_1))) \neq \phi((a_2, f(a_2)))$, so that ϕ is injective. Thus, ϕ is a bijection and $\Gamma_F \sim A$. $\square$

I.2.8

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

Solution: This exercise matches Exercise I.1.6. The canonical projection $\mathbb{R} \twoheadrightarrow \mathbb{R}/\sim$ takes $a \in \mathbb{R}$ to the set $\{x \in \mathbb{R} | x = a + n\}$, where $n \in \mathbb{Z}$. The middle bijection of the canonical decomposition, $\mathbb{R}/\sim \tilde{\to} \mathrm{im} f$, is simply $f([a]_\sim = e^{2\pi i a})$. The final injection $\mathbb{C} \hookrightarrow \mathbb{C}$ is just the inclusion of the unit circle into $\mathbb{C}$. $\square$

I.2.9

Show that if $A' \cong A''$, and further $A' \cap B' = \varnothing$ and $A'' \cap B'' = \varnothing$, then $A' \cup B' \cong A'' \cup B''$. Conclude that the operation $A \coprod B$ is well-defined up to isomorphism.

Solution: By definition, there exist bijections $g : A' \tilde{\to} B'$ and $h : A'' \tilde{\to} B''$. Define $f : A' \cup B' \to A'' \cup B''$ by $f(x) = g(x)$ if $x \in A'$ and $f(x) = h(x)$ if $x \in B'$. The function is well defined since A' and B' are disjoint. Suppose next that $x, y \in A' \cup B'$ with $x \neq y$. In the first case, x and y are both in A' or both in B'. Without loss of generality, suppose the former. Since $x, y \in A'$ and g is injective, we have $f(x) = g(x) \neq g(y) = f(y)$. The second case is that x' and y' are not both in A' or B'. Suppose

without loss of generality that $x \in A'$ and $y \in B'$. Then $f(x) = g(x) \in A''$ and $f(y) = h(y) \in B''$. Since $A'' \cap B'' = \varnothing$, $f(x) \neq f(y)$ as in the previous case, hence f is injective. To prove surjectivity suppose $y \in A'' \cup B''$. If $y \in A''$, since g is surjective, there exists $x \in A'$ (hence $A' \cup B'$) such that $g(x) = f(x) = y$. Similarly for $y \in B''$ and h. Hence f is surjective and f is a bijection and the disjoint union is defined to within isomorphism. $\square$.

I.2.10

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

Solution: For $|A| = 1$, there are $|B|$ elements which it can be mapped to, hence $|B|^1$ functions. Suppose that for $|A| = n$, $\left|B^A\right| = |B|^{|A|}$. Then consider the case $|A| = n + 1$. The first n elements can be mapped in $|B|^{|A|}$ ways by our inductive hypothesis, and the $n + 1$-st element can be mapped in $|B|$ ways as well. Hence the number of ways of mapping $n + 1$ elements is $|B|^n|B| = |B|^{n+1} = |B|^{|A|}$. By induction, we have our proof. $\square$

I.2.11

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

Solution: Let $S \subset A$. Define $f_S : A \to \{0, 1\}$ so that for $a \in A$, $f_S(a) = 0$ if $a \notin S$ and $f_S(a) = 1$ if $a \in S$. Next, define $g : \mathscr{P}(A) \to 2^A$, by $g(S) = f_S$ for all $S \in \mathscr{P}(A)$. It is obvious that g is well defined. Suppose S_1, $S_2 \in \mathscr{P}(A)$, with $S_1 \neq S_2$. Then there exists some $s_1 \in S_1$ such that $s_1 \notin S_2$, or vice versa. Without loss of generality, suppose the former. Then, $g(S_1)(s_1) = f_{S_1}(s_1) = 1$ and $g(S_2)(s_1) = f_{S_2}(s_1) = 0$. Hence, $g(S_1) \neq g(S_2)$, and g is injective. Next, suppose $f \in 2^A$, so that $f : A \to \{0, 1\}$. Form the subset $S \subset A$ consisting of all $a \in A$ such that $f(a) = 1$. Then $g(S) = f$, and g is surjective. Since g is injective and surjective, g is a bijection between 2^A and $\mathscr{P}(A)$. $\square$

I.3: Categories

I.3.1

Let $\mathcal{C}$ be a category. Consider a structure $\mathcal{C}^{op}$ with Obj $(\mathcal{C}^{op})$ = Obj $\mathcal{C}$ and for A, B objects of $\mathcal{C}^{op}$ (hence objects of $\mathcal{C}$), $Hom_{\mathcal{C}^{op}}(A, B) = Hom_{\mathcal{C}}(A, B)$. Show how to make this into a category (that is, define composition of morphisms in $\mathcal{C}^{op}$ and verify the properties listed in §3.1.)
Solution: The identity morphisms are just the identities of the category $\mathcal{C}$. The morphisms are simply denoted in the opposite order as the morphisms of the original category. To prove that this satisfies the properties of morphisms, note that in the original set that if we have morphisms $g \in \mathrm{Hom}_{\mathcal{C}}(C, B)$ and $f \in \mathrm{Hom}_{\mathcal{C}}(B, A)$, there exists a morphism $fg \in \mathrm{Hom}_{\mathcal{C}}(C, A)$. Simply switching out the sets using the definitions, this is identical to saying that for every morphism $f \in \mathrm{Hom}_{\mathcal{C}^{op}}(A, B)$ and $g \in \mathrm{Hom}_{\mathcal{C}^{op}}(B, C)$, there exists a morphism in $\mathrm{Hom}_{\mathcal{C}^{op}}(A, C)$ which we denote by gf. Hence, the law of composition is satisfied under this definition of compositions.

Since the morphisms are simply reversed, we have the associativity of the composition law from:

$$[(hg)f]_{\mathcal{C}^{op}} = [f(gh)]_{\mathcal{C}} = [(fg)h]_{\mathcal{C}} = [h(gf)]_{\mathcal{C}^{op}}$$

That identity morphisms are identities with respect to composition and that sets of morphisms between different object pairs are still disjoint is obvious. □

I.3.2

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

Solution: Since $\mathrm{End}_{\mathrm{Set}}(A) = A^A$, $|\mathrm{End}_{\mathrm{Set}}(A)| = \left|A^A\right| = |A|^{|A|}$. □

I.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.

Solution: In this category, if $f = (a, b)$ and $g = (b, c)$ are morphisms, then $gf = (a, c)$. Hence, $1_a f = (a, a)(a, b) = (a, b)$ by the same definition. □

I.3.4

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

Solution: No. Because $<$ is not reflexive, the required identity morphisms for the relation do not exist. □

I.3.5

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

Solution: It is an instance of the category in Example 3.3 because subset inclusion is reflexive ($A \subset A$ for all sets A) and transitive ($A \subset B$ and $B \subset C$ implies $A \subset C$). □

I.3.6

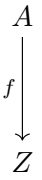
(Assuming some familiarity with linear algebra.) Define a category V by taking Obj$(V) = \mathbb{N}$ and letting $Hom_{\mathscr{V}}(n, m)$ = the set of $m \times n$ matrices with real entries, for all $n, m \in \mathbb{N}$. (Use products of matrices to define composition. Does this category 'feel' familiar?)

Solution: If $f \in \mathrm{Hom_V}(a,b)$ and $g \in \mathrm{Hom_V}(b,c)$, then since $a \times b$ matrices can be multiplied by $b \times c$ matrices to give $a \times c$ matrices, the composition gf defined by matrix multiplication is indeed a member of $\mathrm{Hom_V}(a,c)$. □

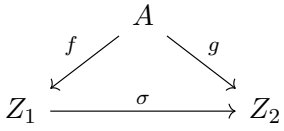
I.3.7

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

Solution: The coslice category is defined with objects as morphisms of a category C from $\mathrm{Hom_C}(A,Z)$ where A is a fixed object of C and Z is any object of C. Diagramatically, they are arrows:



Following the example of slice categories, the morphisms of the coslice category are commutative diagrams corresponding to morphisms in C, namely $\sigma \in \mathrm{Hom_C}(Z_1, Z_2)$ such that if $f \in \mathrm{Hom}_C(A, Z_1)$ and $g \in \mathrm{Hom}_C(A, Z_2)$, then $\sigma f = g$. Diagramatically, the morphisms between f and g are represented by:



□

I.3.8

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

Solution: The above category can be viewed as a full subcategory of Set because it is obvious that $\mathrm{Hom_{C'}}(A,B) = \mathrm{Hom_C}(A,B)$. Furthermore, identity functions and associativity of functions are unaltered when they are between infinite sets. □

I.3.9

An alternative to the notion of multiset introduced in section 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 section 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.)*

Solution: Define the objects of MSet to be sets A equipped with an equivalence relation $\sim$. The morphisms of the set are then defined so that $f \in \mathrm{Hom_{Mset}}(A,B)$ if $f : A/\sim \to B/\sim$ is a function between equivalence relations of A and B. Then it is obvious that MSet is a category. □

I.3.10

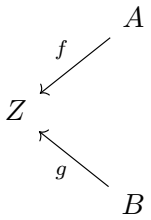
Since the objects of a category C are not (necessarily interpreted as) sets, it is not clear how to make sense of a notion of 'subobject' in general. In some situations it does make sense to talk about subobjects, and the subobjects of any given object A in C are in on-to-one correspondence with the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

Solution: The category Set has a subobject classifier $\Omega = \{0, 1\}$. One can define an isomorphism $\phi : \mathcal{P}(A) \to \{0, 1\}^A$ as follows: If $A_0 \subset A$, then $\phi(A_0) = f_{A_0} : A \to \{0, 1\}$, where $f_X : A \to \{0, 1\}$ is defined such that for $a \in A$, $f(a) = 0$ if $a \notin X$ and $f(a) = 1$ if $a \in X$. In fact, this function/morphism was defined in exercise I.2.11, and it is proven there that this is a bijection. □

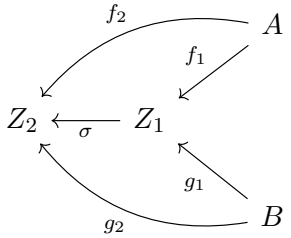
I.3.11

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

Solution: For the category $\mathsf{C}^{A,B}$, the objects consist of two fixed objects of C, A and B, together with morphisms $f \in \mathrm{Hom}_{\mathsf{C}}(A, Z)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(B, Z)$. Diagramatically, the objects of C^A, B can be represented by:

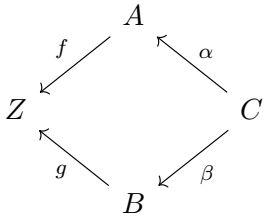


Then a morphism in this category in the set $\mathrm{Hom}_{\mathsf{C}^{A,B}}(Z_1, Z_2)$ is the diagram:

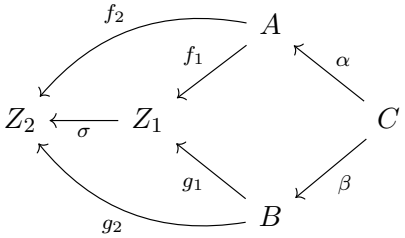


Corresponding to the morphism $\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$.

For the fibered category $C^{\alpha,\beta}$, the objects are the commutative diagrams:



and the morphisms correspond to the commutative diagrams:



Which is essentially $\mathsf{C}_{\alpha,\beta}$ with the arrows reversed. $\square$

I.4: Morphisms

I.4.1

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

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

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

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

so that at every step one is only composing two morphisms. Prove that the result of any such nested composition is independent of the placement f the parentheses.

Solution: For $n = 3$, we know from associativity of morphisms that evaluation order for $f_n f_{n-1} \dots f_1$ is immaterial. Suppose that the order is immaterial for some integer n and consider choices for $f_{n+1} f_n f_{n-1} \dots f_1$. Then the final evaluation will be of the form $(f_{n+1} f_n f_{n-1} \dots f_i)(f_{i-1} \dots f_1)$. Since order is immaterial for products of length less than or equal to n, we have $(f_{n+1} f_n f_{n-1} \dots f_i) = f_{n+1}(f_n f_{n-1} \dots f_i)$. Thus, the final evaluation is then $f_{n+1}(f_n f_{n-1} \dots f_i)(f_{i-1} \dots f_1) = f_{n+1}(f_{n+1} f_n f_{n-1} \dots f_1)$ by associativity. Therefore, the order of evaluation for $n+1$ terms is also immaterial, and by induction the order of evaluation of morphisms is always immaterial and general associativity is true. □

I.4.2

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

Solution: In a groupoid, every morphism is an isomorphism. Hence, for all $f \in \mathrm{Hom}_C(A, B)$ there exists some $g \in \mathrm{Hom}_C(B, A)$ with $gf = 1_A$ and $fg = 1_B$. In the category built from a relation $\sim$, this is saying that if $a \sim b$, we have $b \sim a$, hence the relation is also symmetric and therefore must be an equivalence relation. □

I.4.3

Let A, B be objects of a category C and let $f \in Hom_C(A, B)$ be a morphism.

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

Solution: For the first problem, suppose that f has a right inverse and suppose $\beta', \beta'' \in \mathrm{Hom}_{\mathsf{C}}(B, Z)$ such that $\beta' f = \beta'' f$. Since f has a right inverse $g \in \mathrm{Hom}_{\mathsf{C}}(A, B)$, we have $(\beta' f)g = (\beta'' f)g \to \beta'(fg) = \beta'(fg) \to \beta' 1_B = \beta'' 1_B \to \beta' = \beta''$.

Let a category C be formed by taking the objects to be elements of $\mathbb{Z}$ and the morphisms to be such that for $a, b \in \mathbb{Z}$, the element $(a, b) \in \mathrm{Hom}_{\mathsf{C}}(a, b)$ is the only element of $\mathrm{Hom}_{\mathsf{C}}(a, b)$ if and only if $a \leq b$, otherwise $\mathrm{Hom}_{\mathsf{C}}(a, b) = \varnothing$. Then every morphism is an epimorphism, for if $\beta', \beta'' \in \mathrm{Hom}_{\mathsf{C}}(b, z)$, then both morphisms are necessarily equal since $\mathrm{Hom}_{\mathsf{C}}(b, z)$ has only one morphism, namely (b, z). Thus, it is vacuous that for $f \in \mathrm{Hom}_{\mathsf{C}}(a, b)$ (implying $f = (a, b)$ for some $a \leq b \in \mathbb{Z}$) that $\beta' f = \beta'' f \to \beta' = \beta''$. Thus, it is clear that every morphism of the category is an epimorphism. However, suppose $a < b$ is a strict inequality. Then there cannot exist a right inverse simply because there cannot exist any morphism $g \in \mathrm{Hom}_{\mathsf{C}}(b, a)$, as it would imply that $a \geq b$, contradicting our assumption, hence there is an example of a category containing morphisms which are epimorphisms that do not have right inverses. □

I.4.4

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

Solution: To prove that the composition of two monomorphisms is a monomorphism, let f, g be monomorphisms with $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(B, C)$. Let $\alpha', \alpha'' \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$ and suppose that $(gf)\alpha' = (gf)\alpha''$. By the associativity of morphisms, this implies $g(f\alpha') = g(f\alpha'')$. Since g is a monomorphism, this implies $f\alpha' = f\alpha''$. Since f is a monomorphism, $\alpha' = \alpha''$. Hence, it follows that gf is a monomorphism, and compositions of monomorphisms are monomorphisms. One can define $\mathsf{C}_{\mathrm{mono}}$ is closed under morphism and therefore that this is a category.

For epimorphisms, let g and f be as above, except they are epimorphisms. Let $\beta', \beta'' \in \mathrm{Hom}_{\mathsf{C}}(B, Z)$ with $\beta'(gf) = \beta''(gf)$. By associativity, we have $(\beta' g)f = (\beta'' g)f$. Since f is an epimorphism, we have $\beta' g = \beta'' g$, and since g is an epimorphism $\beta' = \beta''$ and so compositions of epimorphisms are epimorphisms and a corresponding category can be defined.

No category of non-monomorphisms can be defined since identities are monomorphisms! □

I.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!)

Solution: Since my category for MSet has morphisms that are just subets of Set, monomorphisms are just injections and epimorphisms are surjections. □

I.5: Universal properties

I.5.1

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

Solution: Suppose A is final in C. Then for any object Z in the category, there exists a unique morphism $f : Z \to A$. From this, we know that there exists a unique morphism $f : A \to Z$, for any object Z of C^{op}. It follows immediately that A is an initial category of C^{op}. □

I.5.2

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

Solution: Suppose A is a set such that $A \neq \varnothing$. Then there exists some a such that $a \in A$. Let $Z = \{0, 1\}$. We can define a function $f_1 : A \to Z$ such that $f_1(a) = 0$. However, we can also define a function $f_2 : A \to Z$ with $f_2(a) = 1$. Hence, there are at least two distinct functions f_1, f_2 from A to Z, and non-empty sets cannot be initial objects of Set. □.

I.5.3

Prove that final objects are unique up to isomorphism.

Solution: For every object A of C there is at least one element in $\mathrm{Hom}_{\mathsf{C}}(A, A)$, which is the identity 1_A. If F is final, there exists a unique morphism $F \to F$, which is the identity 1_F. Suppose F_1 and F_2 are both final in C. Since F_2 is final, there exists a unique morphism $f : F_1 \to F_2$. Similarly, since F_1 is final, there exists a unique morphism $g : F_2 \to F_1$. Since $gf \in \mathrm{Hom}_{\mathsf{C}}(F_1, F_1)$, we must have $gf = 1_{F_1}$, and since $fg \in \mathrm{Hom}_{\mathsf{C}}(F_2, F_2)$, we have $fg = 1_{F_2}$. Hence, $f : F_1 \to F_2$ is an isomorphism. □

I.5.4

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

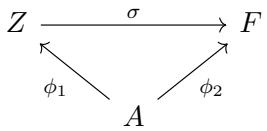
Solution: Singleton pairs $(\{a\}, a)$ are initial objects of the category of pointed sets. Let (Z, z) be an arbitrary set-element pair object of the pointed-set category. Then there exists only one function $\sigma : \{a\} \to Z$ defined by $\sigma(a) = z$. Furthermore, non-singletons are not initial objects, for if $Z = \{0, 1\}$ and B has at least two elements, b_1 and b_2, we can consider, without loss of generality, the object (B, b_1) in the pointed set category and consider morphisms in $\mathrm{Hom}_{\mathsf{C}}((B, b_1), (Z, 0))$. Let $\sigma_1 : B \to Z$ be defined such that $\sigma(b_1) = \sigma(b_2) = 0$, but let $\sigma_2(b_1) = 0$ while $\sigma(b_2) = 1$. Both σ_1 and σ_2 are morphisms in $\mathrm{Hom}_{\mathsf{C}}((B, b_1), (Z, 0))$, but are distinct, hence non-singletons cannot be initial objects of the pointed set category.

Singleton pairs are also the final objects of the pointed set category. Given an arbitrary pair (Z, z) there exists only one possible morphism $\sigma : (Z, a) \to (\{a\}, a)$, namely the function $\sigma(z) = a$ for ALL $z \in Z$. If the pair is not a singleton pair, then there are more morphisms as in the case above, so singleton pairs are the unique final objects of the pointed-set class. □

I.5.5

What are the final objects of the category considered in section 5.3?

Solution: They are again singletons. Consider the diagram:

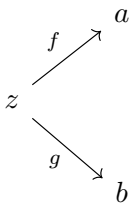


and let $F = \{f\}$ be a singleton. Then the only map $\phi_2 : A \to F$ is $\phi_2(a) = f$ for all $a \in A$. Similarly, the only map $\sigma : Z \to F$ is the map defined by $\sigma(z) = f$ for all $z \in Z$. $\sigma \circ \phi_1 = \phi_2$, so the diagram commutes. Since σ is unique for a given set Z, the pair (F, ϕ_2) is a final object of A and singletons are final objects of this category. $\square$

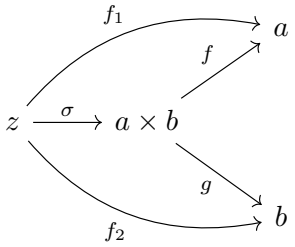
I.5.6

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?

Solution: For products, we insist that for all $a, b \in \mathbb{Z}^+$, that the category $\mathsf{C}_{a,b}$ has final objects. In the category $\mathsf{C}a, b$, the morphisms are diagrams:

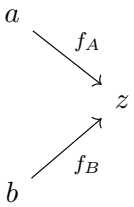


In other words, $z \in \mathbb{Z}^+$ such that $z|a$ and $z|b$. If $\mathsf{C}_{a,b}$ has final objects, then the diagram:

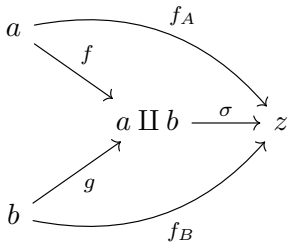


commutes with a unique morphism σ for all $z \in \mathbb{Z}^+$. In particular, this implies that $a \times b \in \mathbb{Z}^+$, that $a \times b$ divides both a and b, and that for every $z \in \mathbb{Z}^+$ such that $z|(a \times b)$, $z|a$ and $z|b$. This means that $a \times b$ precisely meets the definition of the **greatest common denominator of a and b**, or $\gcd(a, b)$.

Similarly, the existence of coproducts in this category is contingent upon the existence of initial objects in the category $\mathsf{C}^{a,b}$ for all $a, b \in \mathbb{Z}^+$. In this category, the objects are the morphism diagrams:



In other words, $z \in \mathbb{Z}^+$ such that $a|z$ and $b|z$. Then a morphism in $\mathsf{C}^{a,b}$ with a final object (the coproduct) is diagramatically represented by:



In other words, for every $z \in \mathbb{Z}^+$ such that $a|z$ and $b|z$, there exists a unique $a \amalg b \in \mathbb{Z}^+$ such that $a|(a \amalg b)$, $b|a \amalg b$, and $(a \amalg b)|z$. This is precisely the **least common denominator of a and b**, or $\text{lcd}(a, b)$.

I.5.7

Redo Exercise 2.9, this time using Proposition 5.4

Solution: Exercise 2.9 asks us to show that the operation $A \amalg B$ is well-defined up to isomorphism. This almost immediately follows from Proposition 5.4, which states that all initial and final objects of categories are isomorphic to one another. Since $A \amalg B$ is an initial object of the category $\mathsf{C}^{A,B}$, it is isomorphic to any other initial object of this category, hence isomorphic to any other coproduct of the category.

I.5.8

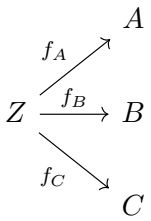
Show that in every category C the products $A \times B$ and $B \times A$ are isomorphic.

Solution: By definition, both products are final objects of $\mathsf{C}_{A,B}$ as $\mathsf{C}_{A,B} = \mathsf{C}_{B,A}$, and hence are isomorphic by Proposition 5.4. $\square$

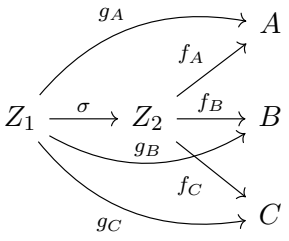
I.5.9

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

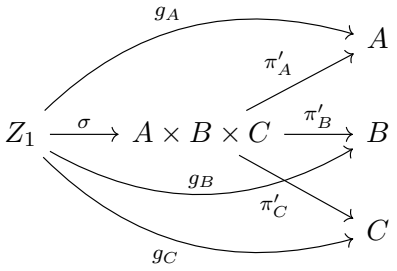
Solution: Let $\mathsf{C}_{A,B,C}$ denote the category whose objects are the three morphisms in C from a single object Z to A, B and C, denoted diagramatically by:



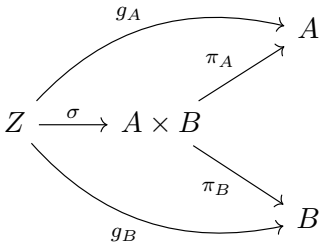
whose morphisms in $\text{Hom}_{\mathsf{C}_{A,B,C}}(Z_1, Z_2)$ correspond to morphisms $\sigma \in \text{Hom}_{\mathsf{C}}(Z_1, Z_2)$, such that the following diagram commutes:



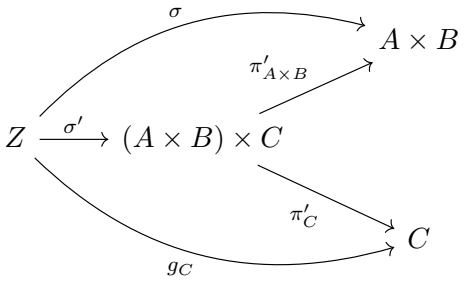
and $A \times B \times C$ is an object in $\mathsf{C}_{A,B,C}$ together with morphisms π'_A, π'_B, π'_C such that for every object Z of $\mathsf{C}_{A,B,C}$, there is a unique $\sigma \in \text{Hom}_{\mathsf{C}_{A,B,C}}(Z, A \times B \times C)$ the following diagram commutes:



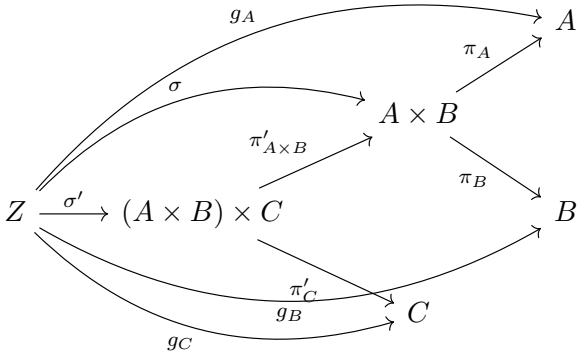
Proof of Theorem: (i) For arbitrary Z there exists a unique morphism σ such that the following diagram commutes:



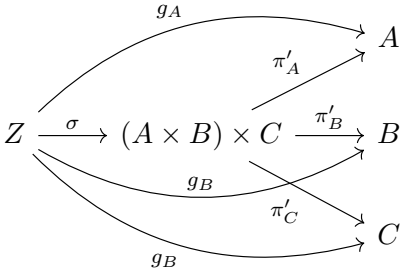
In other words $\pi_A\sigma = g_a$ and $\pi_B\sigma = g_b$. Finally, by the definition of $(A \times B) \times C$ there exists a unique morphism σ' such that the following diagram commutes:



Notice then, that by combining the previous two diagrams, this means σ' is the unique morphism such that the below diagram commutes:



This immediately implies that σ' is the unique morphism for which the following diagram of $\mathsf{C}_{A,B,C}$ commutes:



where $\pi'_A = \pi'_A \circ \pi'_{A\times B}$ and $\pi'_B = \pi'_B \circ \pi'_{A\times B}$. $\square$

I.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*?*

Solution: Let $\{A_i\}$ where $i \in \Lambda$ (some indexing set). Expanding on the generalization above, define the category C_Λ whose objects consist of a set in S together with, for all $i \in \Lambda$ a single morphism $S_i \in \mathrm{Hom}_{\mathsf{Set}}(S, A_i)$. The morphisms of C_Λ correspond to the morphisms $\sigma \in \mathrm{Hom}_{\mathsf{Set}}(Z, S)$ such that $Z_i = \sigma S_i$ (corresponding to the commuting of an arbitrary indexed diagram) for all $i \in \Lambda$. $\square$

I.5.11

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

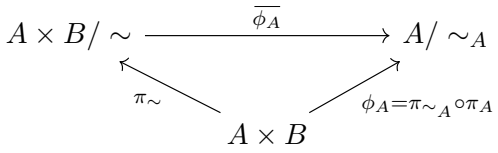
$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 \sim_A a_2 \text{ and } b_1 \sim_B b_2.$$

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

Use the universal property for quotients (section 5.3) to establish that there are functions $(A \times B)/\sim \to A/\sim_A$*,* $(A \times B)/\sim \to B/\sim_B$*.*

Solution: We prove without loss of generality that there exists a function from $A \times B$ to $A/\sim_A$. The case for B is conceptually identical. There exists a function, the natural projection, $\pi_A : A \times B \to A$. There exists a function, the canonical projection, $\pi_{\sim_A} : A \to A/\sim_A$. By taking the composition of these functions, we obtain a map $\phi_A = \pi_{\sim_A} \circ \pi_A : A \times B \to A/\sim_A$. There also exists a map, the canonical projection $\pi_\sim : A \times B \to A \times B/\sim$.

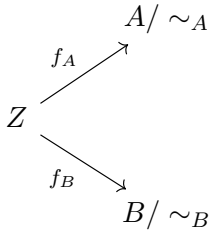
Because $A \times B/\sim$ is an initial object of $\mathsf{Set}_{A,B}$, there exists a unique map $\bar{phi}_a$ such that the following diagram commutes:



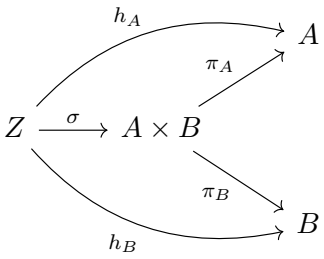
Hence, there exists a function $\overline{\phi_A}$ from $A \times B/\sim$ to $A/\sim_A$. The argument for the existence of a function $\overline{\phi_B} : A \times B/\sim \to B/\sim_B$ is identical. $\square$

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

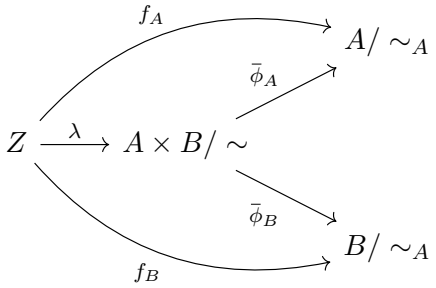
Solution: Let Z with the following diagram be an object in $\mathsf{Set}_{A,B}$:



Define $h_A : Z \to A$ by setting $h_A(z) = a$ for some $a \in f_A(z)$ and $h_B : Z \to A$ by $h_B(z) = b$ for some $b \in f_B(z)$. Then $\pi_{\sim_A} \circ h_A = f_A$, similarly for f_B. Since $A \times B$ is a final object of $\mathsf{Set}_{A,B}$, there exists a unique function σ such that the following diagram commutes:



Let $\lambda = \pi_\sim \circ \sigma$. Let $\overline{\phi_A}$ and $\overline{\phi_B}$ be defined as above. I claim that λ is the unique function for which the following diagram commutes:



(Proof that λ makes the diagram commute) We need to prove:

$$f_A = \overline{\phi_A} \circ \lambda$$
$$f_B = \overline{\phi_B} \circ \lambda$$

Without loss of generality, we prove the case for f_A, and the proof for f_B is identical. Note, that by definition, $\overline{\phi_A} \circ \pi_\sim = \pi_{\sim_A} \circ \pi_A$. Since $\lambda = \pi_\sim \circ \sigma$, we have:

$$\overline{\phi_A} \circ \lambda = \overline{\phi_A} \circ \pi_\sim \circ \sigma = \pi_{\sim_A} \circ \pi_A \circ \sigma = \pi_{\sim_A} \circ h_A = f_A$$

.
The proof for f_B is identical. Hence λ makes the above diagram commute.

(Proof that λ is unique:) Every assertion about A subscripted variables are true for the B subscripted variables. Suppose there exists another function λ_0, for which the above diagram commutes. That is, $\lambda_0 \neq \lambda$ and $\overline{\phi_A} \circ \lambda_0 = \overline{\phi_A}\lambda$. Since $\lambda_0 \neq \lambda$, there exists some $z \in Z$ such that $\lambda_0(z) \neq \lambda(z)$. Note, that since $\bar{\phi_A}\pi_\sim = \pi_{\sim_A} \circ \pi_A$, and since $\pi_\sim$ is a surjective projection function that then necessarily has a right inverse, we have $\bar{\phi_A} = \pi_{\sim_A}\pi_A\pi_\sim^-1$. Let $\lambda_0(z) = [(a_0, b_0)]_\sim$ and $\lambda_0(z) = [(a, b)]_\sim$. We have $\pi_\sim^-1(\lambda_0(z)) = (a_0^*, b_0^*)$ for some $(a_0^*, b_0^*) \in [(a_0, b_0)]_\sim$; and $\pi_\sim^-1(\lambda(z)) = (a^*, b^*)$ for some $(a^*, b^*) \in [(a, b)]_\sim$. Since they are distinct equivalence classes, $[(a_0, b_0)]_\sim \cap [(a, b)]_\sim = \varnothing$. In particular, $(a_0, b_0) \not\sim (a, b)$. By the definition of $\sim$, we have either $a_0 \not\sim_A a$ or $b_0 \not\sim_B b$. Suppose without loss of generality that it is the former. Since $a_0 \neq a$, we then have $a_0 = \pi_A \circ \pi_\sim^-1 \circ \lambda_0(z) \neq \pi_A \circ \pi_\sim^-1 \circ \lambda(z) = a$. Then, since $a_0 \not\sim_A a$, we have $\pi_{\sim_A}(a_0) = \pi_{\sim_A} \circ \pi_A \circ \pi_\sim^-1 \circ \lambda_0(z) = \overline{\phi_A} \circ \lambda_0(z) \neq \overline{\phi_A} \circ \lambda(z) = \pi_A \circ \pi_\sim^-1 \circ \lambda(z) = \pi_{\sim_A}(a)$. In particular, notice $\overline{\phi_A} \circ \lambda_0(z) \neq \overline{\phi_A} \circ \lambda(z)$, directly contradicting our hypothesis about λ_0. Hence, no such λ_0 exists and λ is unique.

Since there exists a unique λ for which the above diagram commutes, this shows that $(A \times B)/\sim$ equipped with functions $\overline{\phi_A}$ and $\overline{\phi_B}$ a final object of the category $\mathsf{Set}A, B$. □

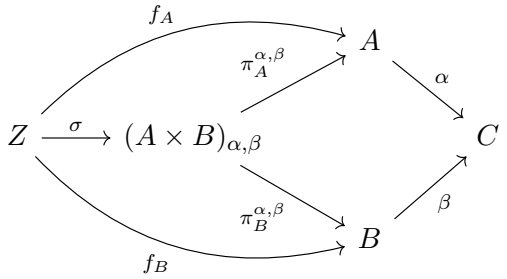
Conclude, without further work that $(A \times B)/\sim \cong (A/\sim_A) \times (B/\sim_B)$.

From Proposition 5.4, since $(A \times B)/\sim$ and $(A/\sim_A) \times (B/\sim_B)$ are both final objects of the category $\mathsf{Set}_{A,B}$, they are isomorphic in $\mathsf{Set}_{A,B}$, which means they are also isomorphic in Set. □

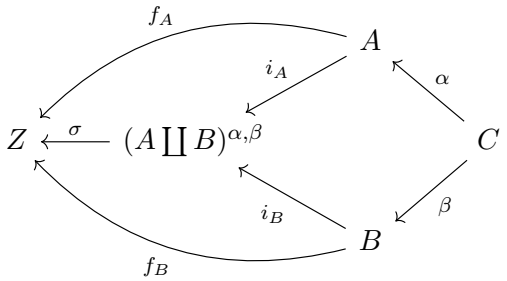
I.5.12

Define the notions of fibered products and fibered coproducts as terminal objects of the categories $\mathsf{C}_{\alpha,\beta}$, $\mathsf{C}^{\alpha,\beta}$ considered in Example 3.10 (cf. also Exercise 3.11), by stating carefully the corresponding universal properties.

Solution: An object $(A \times B)_{\alpha,\beta}$ of a category C is a *fibered product* of A and B with respect to morphisms $\alpha \in \mathrm{Hom}_{\mathsf{C}}(A, C)$ and $\beta \in \mathrm{Hom}_{\mathsf{C}}(B, C)$ if it is a final object in the fibered category $\mathsf{C}_{\alpha,\beta}$. In other words, there exists a unique morphism σ such that for any object $(Z, f_A, f_B) \in \mathrm{Obj}(\mathsf{C}_{\alpha,\beta})$, the following diagram commutes:



Similarly, an object $(A \coprod B)^{\alpha,\beta}$ of a category C with morphisms $i_A \in \mathrm{Hom}_{\mathsf{C}}(A, (A \coprod B)^{\alpha,\beta})$ and $i_B \in \mathrm{Hom}_{\mathsf{C}}(B, (A \coprod B)^{\alpha,\beta})$ is a *fibered coproduct* of A and B with respect to morphisms $\alpha \in \mathrm{Hom}_{\mathsf{C}}(A, C)$ and $\beta \in \mathrm{Hom}_{\mathsf{C}}(B, C)$ if it is an f object in the fibered category $\mathsf{C}^{\alpha,\beta}$. In other words there exists a unique morphism σ such that the following diagram commutes:



(Proof that Set has fibered products) We first need the following lemma: if $\mathsf{C}_{\alpha,\beta}$ has objects, then there is at least one $(a_0, b_0) \in A \times B$ such that $\alpha(a_0) = \beta(b_0)$. If $(Z_0, f_A, f_B) \in \mathsf{C}_{\alpha,\beta}$, then for all $z \in Z_0$ we have $\alpha(f_A(z)) = \beta(f_B(z))$. With $a_0 = f_A(z)$ and $b_0 = f_B(z)$, the lemma is obvious.

Consider the maps $\pi_A^{\alpha,\beta} : A \times B \to A$ and $\pi_B^{\alpha,\beta} : A \times B \to B$ defined by:

$$\pi_A^{\alpha,\beta}((a,b)) = \begin{cases} a_0, & \alpha(a) \neq \beta(b) \\ a, & \alpha(a) = \beta(b) \end{cases}$$

$$\pi_B^{\alpha,\beta}((a,b)) = \begin{cases} b_0, & \alpha(a) \neq \beta(b) \\ b, & \alpha(a) = \beta(b) \end{cases}$$

Then $\alpha \circ \pi_A^{\alpha,\beta} = \beta \circ \pi_B^{\alpha,\beta}$ Let $\sigma : Z \to A \times B$ be defined by $\sigma(z) = (f_A(z), f_B(z))$. Note that $\pi_A^{\alpha,\beta}(\sigma(z)) = \pi_A^{\alpha,\beta}(f_A(z)) = f_A(z)$, since $\alpha \circ f_A = \beta \circ f_B$. Then these functions make the above diagram for $\mathsf{C}_{\alpha,\beta}$ commute. If another σ_0 made this diagram commute, then $A \times B$ with π_A and π_B would not be a final object of $\mathsf{Set}_{A,B}$, contradicting Proposition 5.6. Hence, *Set* has fibered products □

(Proof that Set has fibered coproducts) This proof is pretty much identical to the proof that Set has fibered products. □

II.1: Definition of group

II.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.

Solution: Let $(G, \bullet)$ be a group. Define a category C such that $\bullet$ is the only object and the morphisms are defined as all $f \in G$. Define composition, then by $f \circ g = f \bullet g$. By definition, associativity and the existence of an inverse (simply the inverse of the group) such that composition of the inverse is an identity are satisfied. All objects are in $\mathrm{Aut}(\bullet, \bullet)$. $\square$

II.1.2

Consider the 'sets of numbers' listed in § 1.1 and decide which are made into groups by conventional oeprations 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).

Solution: $(\mathbb{Z}^+, +)$ is a group. The operation $+$ is associative, the identity is 0. And the inverse of $n \in \mathbb{Z}$ is $-n \in \mathbb{Z}$. It is quite obvious, along the same lines of reasoning, that all of the additive groups $(\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$. Both $\mathbb{Q}/\{0\}$ and $\mathbb{R}/\{0\}$ are groups, since every element but 0 in $\mathbb{Q}$ and $\mathbb{R}$ have inverses. Similarly with $\mathbb{C}$. $\square$

II.1.3

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

Solution: We simply note that $(gh)h^{-1}g^{-1} = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e$. $\square$

II.1.4

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

Solution: Let $a, b \in G$, Then $abba = a(bb)a = aa = e = (ab)(ab)$, and from cancellation we immediately acquire $ab = ba$. $\square$

II.1.5

The 'multiplication table' of a group is an array compiling the results of all multiplications $g \bullet f$.

$\bullet$	e	...	h	...
e	e	...	h	...
...	...	...	...	...
g	g	...	$g \bullet h$	...
...	...	...	...	...

Prove that every row and every column of the multiplication table of a group contains all elements of the group exactly once.

Solution: Stating that every row of the multiplication table contains all elements of the group exactly once is equivalent to saying that for all $g \in G$, for all $f \in G$, there exists some $x \in G$ such that $gx = f$. Furthermore, if $gx_1 = f$ and $gx_2 = f$, then $x_1 = x_2$. For columns, for all $g \in G$, for all $f \in G$, there exists some $y \in G$ such that $yg = f$. Furthermore, if $y_1 g = f$ and $y_2 g = f$, then $y_1 = y_2$.

To prove both of the above, not existence is proven by taking $x = g^{-1}f$ and $y = fg^{-1}$ above. Uniqueness is proven by Proposition 1.8 (the cancellation property of groups). $\square$

II.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.

Solution: It is obvious that there is only one possible multiplication table for one elements. For two elements, one is the identity e, call the other a. We then automatically have $ae = ea = a$ and from the exercise II.1.5 we acquire $aa = ee = e$. For three elements, we have the identity $e$and two other elements, a and b. Multiplication by identity is obvious, so we need only work out the a and b multiplication table. If $a^2 = a$, we would have a contradiction since then $a = e$, but they are distinct. If $a^2 = e$, then by II.1.5, we must have $ab = b$, another contradiction since it too implies $a = e$. Hence $a^2 = b$ and by similar reasoning $b^2 = a$, with $ab = ba = e$.

For four elements, there is only one way to multiply by e (a, b, c being the other three elements). For the reasons given above, we cannot have $g^2 = g$ for any $g \in G$ except for e. For a we can have either $a^2 = b$ or $a^2 = c$. If $a^2 = b$, we cannot have $ab = e$, since from the previous exercise we would then have $ac = c$, implying $a = e$ (a contradiction), hence $ab = c$, so that $ac = e$. Next, suppose $ba = e$. Then $b^2 = a$ or $bc = a$. If $bc = a$, since $ac = c$ and $bc = a$, we would have $c^2 = c$, impossible, so it would be the case that $b^2 = a$, but then $bc = b$, a contradiction, hence we must have $ba = c$. Since $ac = e$, we must have $bc = a$, hence $b^2 = e$. For c, this leaves only $ca = e$, $cb = a$, and $c^2 =$ b. Taking $a^2 = c$ gives the second valid multiplication table. □

II.1.7

Prove Corollary 1.11 For reference, the statement of Corollary 1.11 is the following: Let g be an element of finite order, and let $N \in \mathbb{Z}$. Then:

$$g^N = e \iff N \text{ is a multiple of } |g|.$$

Solution: $\implies$) The forward assertion immediately follows from Lemma 1.10.
$\impliedby$) Suppose N is a multiple of $|g|$, so that $N = k|g|$ for some $k \in \mathbb{Z}$. Then, $g^N = g^{k|g|} = (g^{|g|})^k = e^k = e$. □

II.1.8

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

Solution: Let G be such a finite abelia group, consisting of e, f, and the set $\{g_1, g_2, ..., g_k\}$ of all elements of G not equal to the identity e or f. For $1 \leq i \leq k$, g_i^{-1} must be g_j for $j \neq i$. g_i^{-1} cannot be e because it is not the identity and it cannot be g_i since it is not f, the only element of order 2 in the group. Note that $\Pi_{g \in G} g = e g_1 g_2 ... g_k f = g_1 g_2 ... g_k f$. Since G is abelian, we can rearrange the initial product of the g_i's to acquire $\Pi_{g \in G} g = (g_1 g_1^{-1}) ... (g_k g_k^{-1}) f = ef = f$. □

II.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.

Solution: Let $F \subset G$ be all of the elements of G which are of order 2. Let $A = G/(F \cup \{e\})$ Then $|A| = n - m - 1$. If $g \in A$ then g^{-1} cannot be in F, since elements in F are their own inverses and then g would have order two and so not be in A by definition, and $g^{-1} \neq e$ since otherwise $g = e$, also prohibited by the definition of A. $g \neq g^{-1}$ for any g in A since otherwise $|g| = 2$. Thus, for each

$g \in A$ there exists a unique $g^{-1} \neq g \in A$ which is it's inverse. It follows that A has an even number of elements, so that $n - m - 1$ is even, hence $n - m$ is odd. If n is even, then $m = 0$ would imply that $n - m = n$ is even, a contradiction to our previously established statement that $n - m$ is odd . $\square$

II.1.10

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

Solution: By Proposition 1.13, we have $\left|g^2\right| = \frac{|g|}{\gcd(2,|g|)} = |g|$ since $\gcd(2, m) = 1$ for any odd m. $\square$

II.1.11

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

Solution: By a simple inductive argument, it is easy to prove that $(aga^{-1})^n = ag^n a^{-1}$. Hence, $(aga^{-1})^{|g|} = ag^{|g|}a^{-1} = aa^{-1} = e$. If $(aga^{-1})^n = ag^n a^{-1} = e$ for some $n < |g|$, we would acquire $g^n = e$, a contradiction. Hence $\left|aga^{-1}\right| = |g|$. Hence, it follows that $|gh| = \left|h(gh)h^{-1}\right| = |hg|$. $\square$

II.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 $|gh| = \infty$.

Solution: Computing the exponents of g:

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, g^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, g^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, g^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

we see that $|g| = 4$. Computing the exponents of h gives:

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

from which we can see that $|h| = 3$. Next, observe:

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

and we observe the pattern:

$$(gh)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} (gh)^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$$

We postulate that:

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

and it is quite easy to prove this using an inductive argument. It follows that no integer power of $gh$is the identity element and hence $|gh| = \infty$. $\square$

II.1.13

Give an example showing that $|gh|$ is not necessarily equal to $lcm(|g|, |h|)$.

Solution: The solution to II.1.13 demonstrates this. In this problem, $|gh| = \infty$ while $\text{lcm}(|g|, |h|) = 12$. $\square$

II.1.14

As a counterpoint to Exercise 1.13, prove that if g and h commute and $gcd(|g|, |h|) = 1$, then $|gh| = |g||h|$.

Solution: There are two cases. Either one or the other of g or h is the identiy e or they are both not the identity. Assume that one or the other is the identity, assuming without loss of generality that $g = e$. Then we acquire $|g||h| = 1|h| = |eh| = |gh|$.
Next, assume that both are not the identity. Since g and h commute, $(gh)^{|g||h|} = g^{|g||h|}h^{|h||g|} = ee = e$. From this, we conclude $|g||h|$ is a multiple of $|gh|$.
We have $e = (gh)^{|gh||h|} = g^{|gh||h|}h^{|h||gh|} = g^{|gh||h|}$. Hence, $|gh||h|$ is a multiple of $|g|$. Similarly, $|gh||g|$ is a multiple of $|h|$. Recall the following Lemma from basic number theory: If a, b, c are integers with $\gcd(a, c) = 1$ and $c|ab$ then $c|b$. From this we know that $|g|$ divides $|gh|$ and $|h|$ divides $|gh|$. The universal property of the least common multiple states that if $a|m$ and $b|m$, then $\text{lcm}(a, b)|m$. Since $\text{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$, we have $\text{lcm}(|g|, |h|) = |g||h|$, and from the above result $|g||h|$ divides $|gh|$. Since $|g||h|$ and $|gh|$ are multiples of one another, they must be equal. $\square$

II.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, h divides g. (Hint: Argue by contradiction. If $|h|$ is finite but does not divide $|g|$, then there is a prime integer p such that $|g| = p^m r$, $|h| = p^n s$, with r and s relatively prime to p and $m < n$. Use Exercise 1.14 to compute the order of $g^{p^m} h^s$.)

Solution: Since $|h|$ does not divide $|g|$, there must exist some prime p in the prime decomposition of $|h|$ for which the multiplicity n of p in the prime decomposition of $|h|$ is greater than the multiplicity m of p in the prime decomposition of $|g|$. Thus, we can write $|g| = p^m r$ and $|h| = p^n s$. Since m and n are the multiplicities of p, we have $\gcd(p, r) = 1$ and $\gcd(p, s) = 1$.
We have $\left|g^{p^m}\right| = \frac{\text{lcm}(p^m,|g|)}{p^m} = \frac{\text{lcm}(p^m,p^m r)}{p^m} = r$ and $|h^s| = \frac{\text{lcm}(s,|h|)}{s} = \frac{\text{lcm}(s,sp^n)}{s} = p^n$. From above, we see that $\gcd(\left|g^{p^m}\right|, |h^s|) = \gcd(r, p^n) = 1$. Since G is commutative, from problem II.1.14 we see that $\left|g^{p^m} h^s\right| = \left|g^{p^m}\right||h^s| = rp^n > rp^m = |g|$, which contradicts the hypothesis that $|g|$ is the maximal finite order of G. Hence, we must have $|h|$ divides $|g|$. $\square$