Algebra: Chapter 0

Book by Paolo Aluffi

:

Contents

1 Preliminaries: Set theories and categories **3**
1.1 Naive Set Theory, Sets . . . 3
1.2 Functions between sets . . . 5
1.3 Categories . . . 8
1.4 Morphisms . . . 11
1.5 Universal properties . . . 12

2 Groups, first encounter **17**
2.1 Definition of group . . . 17
2.2 Examples of Groups . . . 22
2.3 The category Grp . . . 26

Chapter 1

Preliminaries: Set theories and categories

1.1 Naive Set Theory, Sets

Exercise 1.1.1. *Russel's paradox.*

Proof. Assume that $R = \{x \mid x \notin x\}$ is a set. There are two options, either $R \in R$ or $R \notin R$. But if $R \in R$, then R satisfies the condition to be in R which is $R \notin R$. Contradiction. Thus $R \notin R$ must hold. Hence R cannot satisfy the condition to be in R. Thus $R \notin R$ is false. Contradiction. □

Exercise 1.1.2. *If $\sim$ is an equivalence relation on a set S, then the corresponding family $\mathcal{P}_\sim$ is a partition of S: that is, its elements are nonempty, disjoint and their union in S.*

Proof. An arbitrary element of $\mathcal{P}_\sim$ is $[s]_\sim$ with $s \in S$. We have $[s]_\sim = \{t \in S \mid t \sim s\}$. From reflexivity, we get that $s \in [s]_\sim$. Hence each $[s]_\sim$ is non-empty. It clearly also follows then that

$$S = \bigcup_{s \in S} [s]_\sim = \bigcup \mathcal{P}_\sim.$$

Now consider $s, t \in S$, and assume that $[s]_\sim \cap [t]_\sim \neq \emptyset$. Thus there is some $u \in [s]_\sim \cap [t]_\sim$. Hence we have that $u \sim s$ and $u \sim t$. From symmetry, we obtain that $s \sim u$ and $u \sim t$. Hence $s \sim t$ by transitivity. From symmetry we also have $t \sim s$. We now prove that $[s]_\sim = [t]_\sim$. Take $v \in [s]_\sim$, then $v \sim s$. We also have $s \sim t$, hence from transitivity it follows that $v \sim t$ hence $v \in [t]_\sim$. Conversely, if $v \in [t]_\sim$, then $v \sim t$. Since we also have $t \sim s$, it follows from transitivity that $v \sim s$ and thus $v \in [t]_\sim$. Thus we have shown that if $[s]_\sim \cap [t]_\sim \neq \emptyset$, then $[s]_\sim = [t]_\sim$. We obtain by contraposition that if $[s]_\sim$ and $[t]_\sim$ are distinct, then their intersection is empty. □

Exercise 1.1.3. *Given a partition $\mathcal{P}$ on a set S, there is an equivalence relation $\sim$ such that $\mathcal{P}$ is the associated partition.*

Proof. Define $a \sim b$ if and only if there is some $A \in \mathcal{P}$ such that $a, b \in A$.
Let us prove that the relation is an equivalence relation. Take any $a \in S$. Since $\mathcal{P}$ is a partition, there is some $A \in \mathcal{P}$ such that $a \in A$. Hence $a \sim a$ and thus the relation is reflexive.
Assume that $a \sim b$, then there is some $A \in \mathcal{P}$ such that $a, b \in A$. But then clearly $b, a \in A$. Hence $b \sim a$. Hence the relation is symmetric.
Assume that $a \sim b$ and $b \sim c$, then there are $A, B \in \mathcal{P}$ such that $a, b \in A$ and $b, c \in B$. But then $b \in A \cap B$. By the property of a partition, we get that $A = B$. Hence $a, c \in A$. Thus $a \sim c$. And the relation is transitive.
Now take any $a \in S$. There is a unique $A \in \mathcal{P}$ such that $a \in A$. Then

$$[a]_\sim = \{b \in S \mid a \sim b\} = \{b \in S \mid b \in A\} = A.$$

Hence $[a]_\sim \in \mathcal{P}$. Conversely, take $A \in \mathcal{P}$. Since $\mathcal{P}$ is nonempty, we can find some $a \in A$. Hence again we get $A = [a]_\sim$. Thus the partition associated with $\sim$ is $\mathcal{P}$. □

Exercise 1.1.4. *How many different equivalence relations can be defined on the set* $\{1, 2, 3, \}$.

Proof. Let R be some equivalence relation on the set. The relation is certainly reflexive. Thus $(1,1), (2,2), (3,3) \in R$. There are two possibilities:

1. $(1,2) \in R$
   By symmetry, we have $(2,1) \in R$. There are again two possibilities:
   (a) $(2,3) \in R$
   Then by symmetry, we have $(3,2) \in R$. And by transitivity, we have $(1,3), (3,1) \in R$. Hence
   $$R = \{(1,1), (2,2), (3,3), (1,2), (2,1), (1,3), (3,1), (2,3), (3,2)\}$$
   (b) $(2,3) \notin R$
   We cannot have $(3,2) \in R$ by symmetry. And by transitivity, we cannot have either $(1,3)$ or $(3,1) \in R$. Thus
   $$R = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$$
2. $(1,2) \notin R$
   We cannot have $(2,1) \in R$ by transitivity. There are again two possibilities:
   (a) $(2,3) \in R$.
   Now we have $(3,2) \in R$ by symmetry. We cannot have $(1,3)$ or $(3,1)$ in R by transitivity, thus
   $$R = \{(1,1), (2,2), (3,3), (2,3), (3,2)\}$$
   (b) $(2,3) \notin R$.
   We cannot have $(3,2) \in R$ by symmetry. There are two possibilities:
   i. $(1,3) \in R$.
   We must have $(3,1) \in R$ and this is all, thus
   $$R = \{(1,1), (2,2), (3,3), (1,3), (3,1)\}$$
   ii. $(1,3) \notin R$.
   We cannot have $(3,1) \in R$ by symmetry, thus we must have
   $$R = \{(1,1), (2,2), (3,3)\}$$

We obtain 5 equivalence relations on $\{1, 2, 3\}$. □

Exercise 1.1.5. *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'*

Proof. For example, take the set $S = \{1, 2, 3\}$ and take the relation $R = \{(1,1), (2,2), (3,3), (1,2), (2,1), (2,3), (3,2)\}$. This is clearly reflexive and symmetric, but not transitive. If we take any reflexive and symmetric relation $\sim$, we can set
$$[a]_\sim = \{b \in X \mid a \sim b\}$$
We would still have them non-empty and covering X. But they are not anymore disjoint, except if the relation is transitive. □

Exercise 1.1.6. *Define a relation* $\sim$ *on* $\mathbb{R}$ *by setting*
$$a \sim b \;\Leftrightarrow\; a - b \in \mathbb{Z}.$$
Then $\sim$ *is an equivalence relation and* $\mathbb{R}/\sim$ *can be identified with the circle. Analogously, define* $\equiv$ *on* $\mathbb{R} \times \mathbb{R}$ *by setting*
$$(a, b) \equiv (c, d) \;\Leftrightarrow\; a - c \in \mathbb{Z},\; b - d \in \mathbb{Z},$$
and $\mathbb{R} \times \mathbb{R}/\equiv$ *can be identified with a torus.*

Proof. First to prove that $\sim$ is an equivalence relation:

1. $a \sim a$ since $a - a = 0 \in \mathbb{Z}$.

2. If $a \sim b$, then $a - b \in \mathbb{Z}$. Hence $b - a = -(a - b) \in \mathbb{Z}$. Thus $b \sim a$.

3. If $a \sim b$ and $b \sim c$. Then $a - b \in \mathbb{Z}$ and $b - c \in \mathbb{Z}$. Hence $a - c = (a - b) + (b - c) \in \mathbb{Z}$. Hence $a \sim c$.

Now we make a function

$$f : \mathbb{R}/\sim \to S^1 : [x] \to (\cos(2\pi x), \sin(2\pi x)).$$

This is well-defined since if $[x] = [y]$, then $x - y \in \mathbb{Z}$. Hence there is some $n \in \mathbb{Z}$ such that $x = y + n$. Then

$$(\cos(2\pi x), \sin(2\pi x)) = (\cos(2\pi y + 2\pi n), \sin(2\pi y + 2\pi n)) = (\cos(2\pi y), \sin(2\pi y)),$$

hence f is well-defined. To prove that the function is injective, assume that $f([x]) = f([y])$. This means that

$$\cos(2\pi x) = \cos(2\pi y), \;\; \sin(2\pi x) = \sin(2\pi y),$$

then clearly $x - y \in \mathbb{Z}$. Finally it is obvious that f is surjective since every element of S^1 can be expressed as $(\cos(2\pi x), \sin(2\pi x)) = f([x])$.

For the second, we prove that $\equiv$ is an equivalence relation.

1. $(a, b) \equiv (a, b)$ since $a - a = 0 \in \mathbb{Z}$ and $b - b = 0 \in \mathbb{Z}$.

2. Assume that $(a, b) \equiv (c, d)$. Then $a - c \in \mathbb{Z}$ and $b - d \in \mathbb{Z}$. Hence $c - a = -(a - c) \in \mathbb{Z}$ and $d - b = -(b - d) \in \mathbb{Z}$. Thus $(c, d) \equiv (a, b)$.

3. Assume that $(a, b) \equiv (c, d)$ and $(c, d) \equiv (e, f)$. Then $a - c \in \mathbb{Z}$ and $b - d \in \mathbb{Z}$ and $c - e \in \mathbb{Z}$ and $d - f \in \mathbb{Z}$. Hence $a - e = (a - c) + (c - e) \in \mathbb{Z}$ and $b - f = (b - d) + (d - f) \in \mathbb{Z}$. Hence $(a, b) \equiv (e, f)$.

Finally, we make a function

$$g : (\mathbb{R} \times \mathbb{R})/\equiv \to S^1 \times S^1$$

by setting $g([(x, y)]) \to (f([x]), f([y])$. To prove g is well-defined, take $[(x, y)] = [(a, b)]$, then $x - a \in \mathbb{Z}$ and $y - b \in \mathbb{Z}$. Thus $x \sim a$ and $y \sim b$. But this means that $f([x]) = f([a])$ and $f([y]) = f([b])$. To prove that g is injective, assume that $g([(x, y)]) = g([(a, b)])$. Thus $(f([x]), f([y])) = (f([a]), f([b]))$. Thus $f([x]) = f([a])$ and $f([y]) = f([b])$. Since f is injective, we see that $[x] = [a]$ and $[y] = [b]$, meaning that $x - a \in \mathbb{Z}$ and $y - b \in \mathbb{Z}$, hence $[(x, y)] = [(a, b)]$. Finally, it is clear that g is injective since f is. Indeed, take $(a, b) \in S^1 \times S^1$. Then there is some $x, y \in \mathbb{R}$ such that $f([x]) = a$ and $f([y]) = b$. Hence $g([x, y]) = (a, b)$. □

1.2 Functions between sets

Exercise 1.2.1. *How many different bijections are there between a set S and itself.*

Proof. Assume that $S = \{s_1, ..., s_n\}$. In order to construct a bijection $f : S \to S$, we need to choose the image of s_1. There are n choices, namely s_1,..., s_n. Next we choose the image of s_2, there are $n - 1$ choices, namely $\{s_1, ..., s_n\} \setminus \{f(s_1)\}$. We continue this process and see that we have $n(n - 1)(n - 2)....3 \cdot 2 \cdot 1$ options. Hence there are $n!$ bijections between S and itself. □

Exercise 1.2.2. *Assume $A \neq \emptyset$. Let $f : A \to B$ be a function. Then f has a right-inverse if and only if it is surjective.*

Proof. Let g be a right-inverse of f. Take $b \in B$ and let $a = g(b)$. Then

$$f(a) = f(g(b)) = (f \circ g)(b) = b$$

hence f is surjective.
Conversely, let f be surjective. For any $b \in B$, define $g(b)$ by taking an arbitrary element in $f^{-1}(b)$, which exists by surjectivity. Then since $g(b) \in f^{-1}(b)$, we get $f(g(b)) = b$, thus g is a right-inverse. □

Exercise 1.2.3. *The inverse of a bijection is a bijection and the composition of two bijections is a bijection.*

Proof. Let f be a bijection and let g be its inverse. Then $fg = 1$ and $gf = 1$. Hence f is the inverse of g and g is a bijection.
Let f and g be two bijections then

$$fgg^{-1}f^{-1} = f1f^{-1} = ff^{-1} = 1$$

and

$$g^{-1}f^{-1}fg = g^{-1}1g = g^{-1}g = 1.$$

Hence fg is a bijection with inverse $g^{-1}f^{-1}$. □

Exercise 1.2.4. *The notion of being isomorphic is an equivalence relation.*

Proof. Let A be any set, then $\mathrm{id}_A : A \to A$ is a bijection. Thus A is related to A and hence the relation is reflexive.
Let A be related to B, then there is a bijection $f : A \to B$. The inverse $f^{-1} : B \to A$ is also a bijection, hence B is related to A and thus the relation is symmetric.
Let A be related to B and B be related to C, then there are bijections $f : A \to B$ and $g : B \to C$. The composition $g \circ f : A \to C$ is then a bijection. Hence A is related to C and thus the relation is transitive. □

Exercise 1.2.5. *A function $e : A \to B$ is an epimorphism if for all functions $u, v : B \to C$ holds that if $u \circ e = v \circ e$ then $u = v$. Then e is an epimorphism iff it is surjective.*

Proof. Assume first that e is surjective and that $u \circ e = v \circ e$. If $u \neq v$, then there is some $b \in B$ such that $u(b) \neq v(b)$. But since e is surjective, there is some $a \in A$ such that $e(a) = b$. But then $u(e(a)) \neq v(e(a))$ contradicting the fact that $u \circ e = v \circ e$. Thus e is an epimorphism.
Conversely, assume that e is an epimorphism. Define $B' = e(A) \subseteq B$. Define

$$u : B \to \{0, 1\} : b \to 0$$

and define

$$v : B \to \{0, 1\} : b \to \begin{cases} 0 \text{ if } b \in B' \\ 1 \text{ if } b \notin B' \end{cases}$$

Then clearly for any $a \in A$, we have $e(a) \in B'$, thus

$$v(e(a)) = 0 = u(e(a)),$$

hence $v \circ e = u \circ e$. Hence $v = u$ because e is an epimorphism. This implies that there is no $b \in B$ such that $v(b) = 1$, or equivalently, $B' = B$. Thus $e(A) = B$ and e is surjective. □

Exercise 1.2.6. *Any function $f : A \to B$ determines a section of π_A.*

Proof. Indeed, define $F : A \to A \times B : a \to (a, f(a))$. This is a section since

$$(\pi_A \circ F)(a) = \pi_A(a, f(a)) = a.$$

□

Exercise 1.2.7. *Let $f : A \to B$ be any function. Then the graph Γ_f of f is isomorphic to A.*

Proof. We let

$$p_1 : \Gamma_f \to A : (a, b) \to a,$$

and we let

$$i : A \to \Gamma_f : a \to (a, f(a)).$$

This is an inverse pair:

$$p_1(i(a)) = p_1(a, f(a)) = a$$

and if $(a, b) \in \Gamma_f$, then $b = f(a)$, hence

$$i(p_1(a, b)) = i(a) = (a, f(a)) = (a, b).$$

□

Exercise 1.2.8. *Describe as explicitly as you can all terms in the canonical decomposition of the function*

$$f : \mathbb{R} \to \mathbb{C} : x \to e^{2\pi i x}.$$

Proof. Let $\sim$ be the equivalence

$$x \sim y \text{ if and only if } x - y \in \mathbb{Z},$$

as in 1.6. We have that $x \sim y$ if and only if $f(x) = f(y)$. Furthermore, the image of f is the circle $\mathbb{S}^1$. So the canonical decompostion is first the quotient $\mathbb{R} \to \mathbb{R}/\sim$. Then the isomorphism between $\mathbb{R}/\sim$ and the circle, and then the inclusion of the cirle in $\mathbb{C}$. □

Exercise 1.2.9. *If $A' \cong A''$ and if $B' \cong B''$ and if further $A' \cap B' = \emptyset = A'' \cap B''$, then $A' \cup B' \cong A'' \cup B''$. As a consequence, the disjoint union of A and B is well-defined up to isomorphism.*

Proof. Takee a bijection $f : A' \to A''$ and a bijection $g : B' \to B''$. Then define $h : A' \cup B' \to A'' \cup B''$ by setting

$$h(x) = \begin{cases} f(x) & \text{if } x \in A' \\ g(x) & \text{if } x \in B' \end{cases}$$

It is clear that h is a well-defined function since A' and B' are disjoint. It is further clear that h is surjective since f and g are. Injectivity is clear, since if $h(x) = h(y)$, then either $x, y \in A'$ or $x, y \in B'$ in which case $x = y$ by injectivity of f and g, or we have that $x \in A'$ and $y \in B'$ (or the similar case $x \in B'$ and $y \in A'$), in which case we have $f(x) = g(y) \in A'' \cap B''$, which is a contradiction since $A'' \cap B''$ is empty. □

Exercise 1.2.10. *If A and B are finite sets, then $|B^A| = |B|^{|A|}$.*

Proof. Let $A = \{a_1, ..., a_n\}$ and $B = \{b_1, ..., b_m\}$. Any function from A to B is defined by first choosing the image of a_1 (m possibilities), then choosing the image of a_2 (m possibilities), and so on until all elements have an image. In total we makes n choices with each m possibilities. We end up with $m \cdot ... \cdot m$ possibilities, which is m^n. So there are m^n amount of functions. □

Exercise 1.2.11. *There is a bijection between 2^A and the power set of A.*

Proof. Take $f : A \to \{0, 1\}$, then define

$$F : 2^A \to \mathcal{P}(A)$$

as

$$F(f) = \{x \in A \mid f(x) = 1\}.$$

We show this is injective. Take $f, g : A \to \{0, 1\}$ such that $F(f) = F(g)$. Thus if $x \in A$, then $x \in F(f)$ if and only if $x \in F(g)$. Hence $f(x) = 1$ if and only if $g(x) = 1$. This implies that $f = g$.
To show the function is surjective, take $B \subseteq A$. Define the function $f : A \to \{0, 1\}$ by setting $f(x) = 1$ if $x \in A$ and 0 otherwise. Then we clearly have $F(f) = B$. □

1.3 Categories

Exercise 1.3.1. *Let $\mathcal{C}$ be a category. Consider a structure $\mathcal{C}^{op}$ with*

- *$Obj(\mathcal{C}^{op}) := Obj(\mathcal{C})$*
- *For a, B objects of $\mathcal{C}^{op}$ (hence objects of $\mathcal{C}$, $Hom_{\mathcal{C}^{op}}(A, B) := Hom_{\mathcal{C}}(B, A)$.*

Proof. Define for $f \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B)$ and $g \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(B, C)$,

$$g \circ^{\mathrm{op}} f = f \circ g$$

and

$$(1_A)^{\mathrm{op}} = 1_A.$$

We check associativity, if $f \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A, B)$ and $g \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(B, C)$ and $h \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(C, D)$, then

$$\begin{aligned} h \circ^{\mathrm{op}} (g \circ^{\mathrm{op}} f) &= h \circ^{\mathrm{op}} (f \circ g) \\ &= (f \circ g) \circ h \\ &= f \circ (g \circ h) \\ &= f \circ (h \circ^{\mathrm{op}} g) \\ &= (h \circ^{\mathrm{op}} g) \circ^{\mathrm{op}} f \end{aligned}$$

Now we also have that

$$(1_B)^{\mathrm{op}} \circ^{\mathrm{op}} f = f \circ 1_B = f$$

and

$$f \circ^{\mathrm{op}} (1_A)^{\mathrm{op}} = 1_A \circ f = f,$$

hence we have a category. □

Exercise 1.3.2. *If A is a finite set, how large is $End_{SET}(A)$.*

Proof. We know that $\mathrm{End}_{\mathrm{SET}}(A)$ are just all the functions from A to A. WE have proven that the amount of such functions is just $|A|^{|A|}$. □

Exercise 1.3.3. *In example 3.3, 1_a is an identity with respect to composition.*

Proof. Let $f \in \mathrm{Hom}(a, b)$ and $g \in \mathrm{Hom}(b, a)$, then necessarily $f = (a, b)$, $g = (b, a)$ and $1_a = (a, a)$. We have $f1_a = (a, a) = f$ and $1_a g = (a, a) = g$. □

Exercise 1.3.4. *Can we define a category in the style of Example 3.3 using the relation $<$ on the set $\mathbb{Z}$?*

Proof. No, since the relation $<$ is not reflexive. □

Exercise 1.3.5. *Example 3.4 is an instance of the categories considered in Example 3.3.*

Proof. Indeed, this is easy to see by taking for $A, B \in \mathcal{P}(S)$, the relation $A \sim B$ if and only if $A \subseteq B$. □

Exercise 1.3.6. *Define a category V by taking $Obj(V) = \mathbb{N}$ and letting $Hom_V(n, m)$ be the set of $m \times n$-matrices with real entries, for all $n, m \in \mathbb{N}$. Use product of matrices to define composition.*

Proof. Take $A \in \mathrm{Hom}_V(n, m)$, $B \in \mathrm{Hom}_V(m, k)$ and $C \in \mathrm{Hom}_V(k, l)$. Then A is an $m \times n$-matrix, B is an $k \times m$-matrix and C is an $l \times k$-matrix. We have

$$C \circ (B \circ A) = C(BA) = (CB)A = (C \circ B) \circ A$$

Let $A \in \mathrm{Hom}_V(n, m)$, then A is an $m \times n$-matrix. Let I_n be the $n \times n$-identity matrix and let I_m be the $m \times m$-identity matrix. We have

$$A \circ I_n = AI_n = A$$

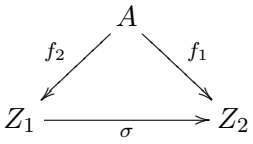
and

$$I_m \circ A = I_m A = A.$$

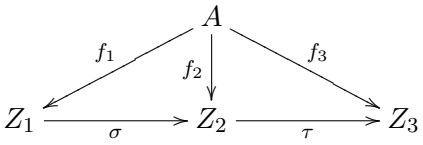
Hence we have a category. □

Exercise 1.3.7. *What are the objects and morphisms in Example 3.7.*

Proof. Objects in this category are arrows $A \to Z$ in $\mathcal{C}$. Let $f_1 : A \to Z_1$ and $f_2 : A \to Z_2$ be arrows in $\mathcal{C}$. Then a morphism is a commutative diagram



Composition then becomes



□

Exercise 1.3.8. *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 composition in $\mathcal{C}$ make $\mathcal{C}'$ into a category. A subcategory 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**.*

Proof. Let the objects of $\mathcal{C}$ be all the infinite sets. Given two infinite sets, let the morphisms between them be all functions between them. This clearly defines a full subcategory of **Set**. □

Exercise 1.3.9. *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 he 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.)*

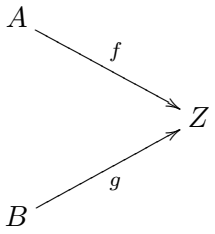
Proof. Given two multisets $(A, \sim)$ and $(B, \sim)$. A morphism is a function $f : A \to B$ such that $a \sim a'$ implies $f(a) \sim f(a')$. It is clear then that **Set** is a full subcategory of the category of multisets, since if A is any set, then the equivalence class of any element is a singleton.
If we take a multiset $m : A \to \mathbb{N}^*$, this correspond to an alternative multiset $(A, \sim)$ such that the equivalence class of any element is finite. A morphism from this point of view would send equal elements to equal elements. □

Exercise 1.3.10. *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 morphims $A \to \Omega$ for a fixed, special object Ω of $\mathcal{C}$, called a subobject classifier. Show that **Set** has a subobject classifier.*

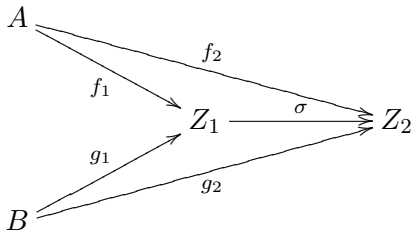
Proof. The subobject classifier is $\Omega = \{0, 1\}$. Indeed, given any morphism $f : A \to \Omega$, this corresponds to the subobject $A' = \{x \in A \mid f(x) = 1\}$. And given any subobject A' of A, we can define the morphism by sending each element of A' to 1 and the rest of the elements to 0. □

Exercise 1.3.11. *Define composition and identities in the category $C^{A,B}$ of Example 3.9, and of the category $C^{\alpha,\beta}$ of Example 3.10.*

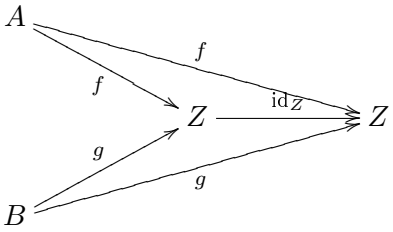
Proof. Objects of $C^{A,B}$ are diagrams



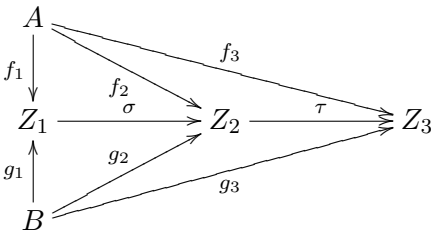
and a morphism is a commutative diagram



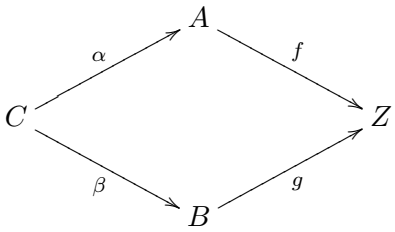
Thus the identity is



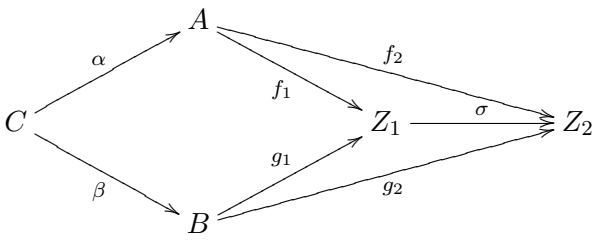
And compositions are



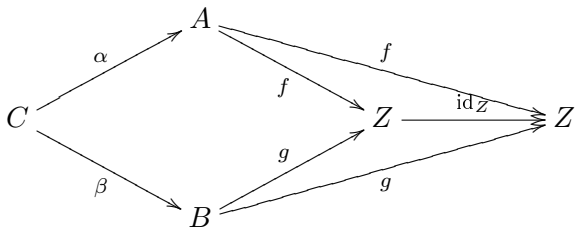
As for $C_{\alpha,\beta}$, objects are diagrams



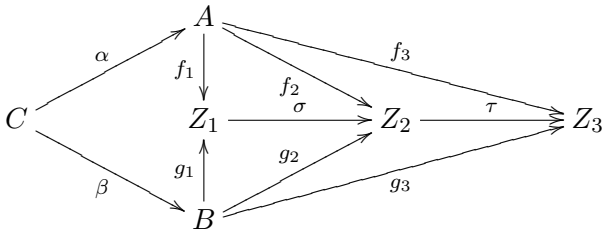
and a morphism is a commutative diagram



Thus the identity is



And compositions are



□

1.4 Morphisms

Exercise 1.4.1. *Composition is defined for two morphisms. If more than two morphisms are given then one may compose them in several ways. Prove that the result of any such nested composition is independent of the placement of parantheses.*

Proof. The result is true for $n = 3$. Now given a nested composition of $f_1, ..., f_n$. We can write this as

$$(f_1 \circ .... \circ f_k) \circ (f_{k+1} \circ ... \circ f_n),$$

where between the brackets we have a well-defined product by the induction hypothesis. Another composition is

$$(f_1 \circ ... \circ f_l) \circ (f_{l+1} \circ ... \circ f_n).$$

Assume WLOG that $l < k$, then we can write using the induction hypothesis and the associative law

$$\begin{aligned}(f_1 \circ .... \circ f_k) \circ (f_{k+1} \circ ... \circ f_n) &= ((f_1 \circ ... \circ f_l) \circ (f_{l+1} \circ ... \circ f_k)) \circ (f_{k+1} \circ ... \circ f_n) \\ &= (f_1 \circ ... \circ f_l) \circ ((f_{l+1} \circ ... \circ ...f_k) \circ (f_{k+1} \circ ... \circ f_n)) \\ &= (f_1 \circ ... \circ f_l) \circ (f_{l+1} \circ ... \circ f_n),\end{aligned}$$

hence the two expressions are equal. □

Exercise 1.4.2. *Let X be a set equipped with a reflexive and transitive relation R. This induces a category $\mathcal{R}$. When is this category a groupoid.*

Proof. We want that every morphism is an isomorphism. So take a morphism $x \; R \; y$. An inverse would be given by $y \; R \; x$. Thus the category is a groupoid if and only if R is symmetric. □

Exercise 1.4.3. *Let A, B be objects of a category $\mathcal{C}$ and let $f \in Hom_{\mathcal{C}}(A, B)$ be a morphism.*

1. *If f has a right-inverse, then f is an epimorphism.*
2. *The converse does not hold.*

Proof. 1. Let $u, v : B \to C$ be two morphisms such that $u \circ f = v \circ f$. Then by applying the right-inverse g of f, we get

$$u = u \circ \mathrm{Id}_B = u \circ f \circ g = v \circ f \circ g = v \circ \mathrm{Id}_B = v.$$

2. As for the converse, take the monoid $\mathbb{N}$ with addition. This defines a category. Note that $n+2 = m+2$ implies $n = m$, thus 2 is an epimorphism. But of course 2 has no right-inverse in $\mathbb{N}$.

□

Exercise 1.4.4. *The composition of monomorphisms is a monomorphism. Hence given a category $\mathcal{C}$ we can define a subcategory $\mathcal{C}_{mono}$ by taking the same objects as $\mathcal{C}$ and by taking as morphisms in $\mathcal{C}_{mono}$ the monomorphisms in $\mathcal{C}$. The same can be done for epimorphisms, but there is not a category of non-monomorphisms.*

Proof. Let $f : A \to B$ and $g : B \to C$ be monomorphisms. Assume $u, v : D \to A$ are such that $(g \circ f) \circ u = (g \circ f) \circ v$. Since g is a monomorphism, we get that $f \circ u = f \circ v$. Since f is a monomorphism we end up with $u = v$.
The identity $\mathrm{Id}_A : A \to A$ is a monomorphism since $\mathrm{Id}_A \circ u = \mathrm{Id}_A \circ v$ obviously implies $u = v$. Hence the monomorphisms define a category.
Now let $f : A \to B$ and $g : B \to C$ be epimorphisms. Assume that $u, v : C \to D$ are such that $u \circ g \circ f = v \circ g \circ f$. Since f is an epimorphism, we get that $u \circ g = v \circ g$. Since g is an epimorphism, we obtain that $u = v$.
The identity $\mathrm{Id}_C : C \to C$ is an epimorphism since $u \circ \mathrm{Id}_C = v \circ \mathrm{Id}_C$ clearly implies $u = v$. Hence the epimorphisms define a category.
The non-monomorphisms do not form a subcategory, since the identities form monomorphisms. □

Exercise 1.4.5. *Give a concrete description of monomorphisms and epimorphisms in the category **MSet**.*

Proof. The monomorphisms are exactly injective maps. Indeed, assume that a map f has this property and that $f \circ u = g \circ v$. Then if $f(u(x)) = g(v(x))$, then clearly $u(x) = v(x)$. Conversely, let f be non-injective and let $x \neq y$ be such that $f(x) \neq f(y)$. Define $u(*) = x$ and $v(*) = y$. Then $f \circ u \neq f \circ v$.
The epimorphisms are exactly the surjective maps. Indeed, if $u(f(x)) = v(f(x))$ for all x. Then given y, there is some x such that $f(x) = y$. But then we see that $u(y) = v(y)$. Conversely, if f is not surjective, let $\{0, 1\}$ be a multiset with $0 \sim 1$. We define $u(x) = 0$ for all x. We define $v(x) = 0$ if $x = f(y)$ for some y, and 1 otherwise, then $u \circ f \neq v \circ f$. □

1.5 Universal properties

Exercise 1.5.1. *The final object in a category $\mathcal{C}$ is the initial object in the category $\mathcal{C}^{op}$.*

Proof. Let F be the final object in $\mathcal{C}$. This implies for any object C in $\mathcal{C}$, that there is a unique morphism $C \to F$ in $\mathcal{C}$. By definition of morphisms in $\mathcal{C}^{\mathrm{op}}$, we see that there is a unique morphism $F \to C$ in $\mathcal{C}^{\mathrm{op}}$, hence the object F is initial in $\mathcal{C}^{\mathrm{op}}$. □

Exercise 1.5.2. *$\emptyset$ is the unique initial object in **SET**.*

Proof. Let I be another initial object, then there is a bijection $f : I \to \emptyset$. If I is nonempty, the it has an element $x \in I$. But then $f(x) \in \emptyset$, which is a contradiction. Hence $I = \emptyset$. □

Exercise 1.5.3. *Final objects are unique up to isomorphism.*

Proof. Let F and F' be final objects. Since F' is final, there is a morphism $f : F \to F'$. Since F is final, there is a morphism $g : F' \to F$. We have that $g \circ f : F \to F$ is a morphism between F and F. But 1_F is also such a morphism. Since F is final, such a morphism is unique, hence $g \circ f = 1_F$. We also have that $f \circ g$ is a morphism between F' and F'. But $1_{F'}$ is also such a morphism. Since F' is final, such a morphism is unique, hence $f \circ g = 1_{F'}$. We obtain that f and g are inverses. Since f is thus an isomorphism, we get that F and F' are isomorphic. □

Exercise 1.5.4. *Find the final and initial objects in the category of pointed sets.*

Proof. The singleton $\{*\}$ with the function $\mathrm{Id} : \{*\} \to \{*\}$ is both final and initial. Indeed, let $(A, f : \{*\} \to A)$ be another pointed set. There is clearly only one function $A \to \{*\}$, namely

$$g : A \to \{*\} : x \to *$$

This satisfies $g(f(*)) = * = \mathrm{Id}(*)$, hence $(\{*\}, \mathrm{Id})$ is final.
Also, the only function $h : \{*\} \to A$ satisfying $h(*) = f(*)$ is clear. Hence $(\{*\}, \mathrm{Id})$ is an initial object too. □

Exercise 1.5.5. *What are the final objects in the category of §5.3?*

Proof. The final objects are the singletons $\{*\}$, with the constant morphisms $\varphi : A \to \{*\}$. Given any other set Z and a morphism $\psi : A \to Z$ satisfying $a \sim b$ implies $\psi(a) = \psi(b)$, we define $f : Z \to \{*\}$ the constant map. We have

$$f(\psi(a)) = * = \varphi(a),$$

as desired. □

Exercise 1.5.6. *Consider the category corresponding to endowing the set $\mathbb{Z}^+$ of positive integers with the divisibility relation. Thus there is exactly one morphism $d \to m$ if and only if d divides m without remainder; there is no morphism between d and m otherwise. This category has products and coproducts. What are their convential name.*

Proof. Translating the product requirement, we get that n is the product of a and b if n divides both a and b, and if m divides both a and b, then m divides n. Thus n is the greatest common divisor of a and b.
Translating the coproduct requirement, we get that n is the coproduct of a and b if both a and b divides n, and if a and b divide m, then n divides m. Thus n is the least common multiple. □

Exercise 1.5.7. *If $A' \cong A''$ and $B' \cong B''$, and further $A' \cap B' = \emptyset$ and $A'' \cap B'' = \emptyset$, then $A' \cup B' \cong A'' \cup B''$.*

Proof. We have that both $A' \cup B'$ and $A'' \cup B''$ are coproducts of A' and B' in **Set**. Coproducts are unique up to isomorphism, which concludes the proof. □

Exercise 1.5.8. *In every category, the product $A \times B$ and $B \times A$ are isomorphic.*

Proof. By the universal property, given any two morphisms $f_A : C \to A$ and $f_B : C \to B$, there is a unique morphism $f : C \to A \times B$ such that $p_A \circ f = f_A$ and $p_B \circ f = f_B$. Switching the order of the morphismss, we thus see that $(A \times B, p_A, p_B)$ satisfies the universal property of the product of B and A. Hence $A \times B$ and $B \times A$ are isomorphic. □

Exercise 1.5.9. *Let $\mathcal{C}$ be a category with products. Find a reasonable candidate for the universal property for the product $A \times B \times C$ of three objects. Both $(A \times B) \times C$ as $A \times (B \times C)$ satisfy this universal property and hence are isomorphic.*

Proof. The universal property of $A \times B \times C$ goes as follows: given any three morphisms $f_A : D \to A$, $f_B : D \to B$ and $f_C : D \to C$, there is a unique morphism $f : D \to A \times B \times C$ such that $f_A = p_A \circ f$, $f_B = p_B \circ f$ and $f_C = p_C \circ f$.
We show that $(A \times B) \times C$ satisfy this property. Given the three morphisms, $f_A : D \to A$, $f_B : D \to B$ and $f_C : D \to C$, by the universal property there is a unique morphism $h : D \to A \times B$ such that $p_A \circ h = f_A$ and $p_B \circ h = f_B$. By the universal property again, there is a unique morphism $f : D \to (A \times B) \times C$ such that $p_1 \circ f = h$ and $p_2 \circ f = f_C$. But then $p_A \circ p_1 \circ f = f_A$ and $p_B \circ p_2 \circ f = f_B$.
To show uniqueness, assume that g also satisfies $p_2 \circ g = f_C$, $p_A \circ p_1 \circ g = f_A$ and $p_B \circ p_1 \circ g = f_B$. Then by uniqueness of the universal property, we have that $p_1 \circ g = p_1 \circ f$. Hence by uniqueness again, we get that $g = f$.
We show that $A \times (B \times C)$ satisfy this property. Given the three morphisms, $f_A : D \to A$, $f_B : D \to B$ and $f_C : D \to C$, by the universal property there is a unique morphism $h : D \to B \times C$ such that $p_B \circ h = f_B$ and $p_C \circ h = f_C$. By the universal property again, there is a unique morphism $f : D \to A \times (B \times C)$ such that $p_1 \circ f = f_A$ and $p_2 \circ f = h$. But then $p_B \circ p_2 \circ f = f_B$ and $p_C \circ p_2 \circ f = f_C$.

To show uniqueness, assume that g also satisfies $p_1 \circ g = f_A$, $p_B \circ p_2 \circ g = f_B$ and $p_C \circ p_2 \circ g = f_C$. Then by uniqueness of the universal property, we have that $p_2 \circ g = p_2 \circ f$. Hence by uniqueness again, we get that $g = f$. □

Exercise 1.5.10. *Define products and coproducts for families of objects in a category. Do these exist in* ***Set****?*

Proof. Let $(A_i)_{i\in I}$ be a family of objects. We say that $(P, \pi_i : P \to A_i)$ is the product of this family if for every family of morphisms $f_i : C \to A_i$ there is a unique morphism $f : C \to P$ such that $\pi_i \circ f = f_i$.
In **Set**, we define

$$\prod_{i\in I} A_i = \left\{ x : I \to \bigcup_{i\in I} A_i \mid x(i) \in A_i \ \forall i \in I \right\},$$

with $\pi_i(x) = x(i)$. Let $f_i : C \to A_i$ be functions. We want $f : C \to \prod_{i\in I} A_i$ such that $\pi_i \circ f = f_i$. Thus $f(c)(i) = f_i(c)$. With this definition, we define f and the diagram commutes.
Let $(A_i)_{i\in I}$ be a family of objects. We say that $(I, \iota_i : A_i \to I)$ is the product of this family if for every family of morphisms $f_i : A_i \to C$ there is a unique morphism $f : I \to C$ such that $f \circ \iota_i = f_i$.
In **Set**, we define

$$\coprod_{i\in I} A_i = \bigcup_{i\in I} A_i \times \{i\},$$

with $\iota_i(x) = (x, i)$. Let $f_i : A_i \to C$ be functions. We want $f : \coprod_{i\in I} A_i \to C$ such that $f \circ \iota_i = f_i$. Thus $f(c, i) = f_i(c)$. With this definition, we define f and the diagram commutes. □

Exercise 1.5.11. *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*

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

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

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

3. *$(A \times B)/\sim$ is isomorphic to $(A/\sim_A) \times (B/\sim_B)$.*

Proof. 1. Let $f : A \times B \to A/\sim_A$ given by $f(a, b) = [a]$. If $(a_1, b_1) \sim (a_2, b_2)$. Then $[a_1] = [a_2]$, thus $f(a_1, b_1) = f(a_2, b_2)$. Thus equivalent elements have the same image. By the universal property of quotients, we get a function $F : (A \times B)/\sim \to A/\sim_A$.
Let $g : A \times B \to B/\sim_B$ given by $f(a, b) = [b]$. If $(a_1, b_1) \sim (a_2, b_2)$. Then $[b_1] = [b_2]$, thus $g(a_1, b_1) = g(a_2, b_2)$. Thus equivalent elements have the same image. By the universal property of quotients, we get a function $G : (A \times B)/\sim \to B/\sim_B$.

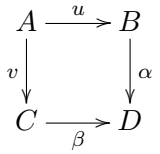
2. Let $H : D \to A/\sim_A$ and $K : D \to B/\sim_B$ be functions. Define $A : D \to (A \times B)/\sim$ by sending $A(d)$ to (a, b), where $[a] = H(d)$ and $[b] = K(d)$. This is well-defined since if $H(d) = [a] = [a']$ and $K(d) = [b] = [b']$, we have $(a, b) \sim (a', b')$.
Now, we have that if $A(d) = [(a, b)]$. Then $F(A(d)) = [a] = H(d)$, and $G(A(d)) = [b] = K(d)$.
Now for uniqueness, assume that if $B(d) = [(a, b)]$. Then $F(B(d)) = [a]$ and $G(B(d)) = [b]$. Thus we must have $[a] = F(B(d)) = H(d)$ and $[b] = G(B(d))$, which is the same as the map A above.

3. Follows by uniqueness of the product up to isomorphism.

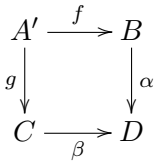
□

Exercise 1.5.12. *Define the notion of fibered products and fibered coproducts as terminal objects of the categories $C_{\alpha,\beta}$ and $C^{\alpha,\beta}$, by stating carefully the corresponding universal properties. Define the fibered products and coproducts in* ***Set*** *concretely.*

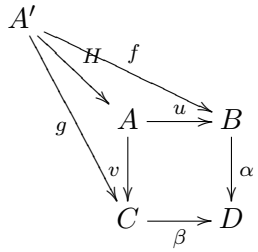
Proof. A fibered product is a commutative diagram



If



is another diagram, then there is a unique arrow H such that

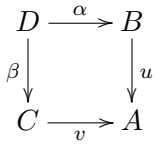


In **Set**, we let

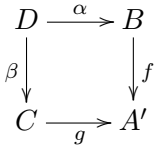
$$A = \{(b, c) \in B \times C \mid \alpha(b) = \beta(c)\}$$

and $u(b, c) = b$ and $v(b, c) = c$. In the case of the other diagram, we want $u(H(a)) = f(a)$ and $v(H(a)) = g(a)$. So it is clear the unique map H making the diagram commute is $H(a) = (f(a), g(a))$. This is well defined since $\alpha(f(a)) = \beta(g(a))$.

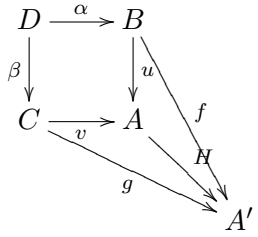
A fibered coproduct is a commutative diagram



If



is another diagram, then there is a unique arrow H such that



In **Set**, we let

$$A = (B \times \{0\}) \cup (C \times \{1\}) / \sim,$$

where $\sim$ is the equivalence relation generated by $\alpha(d) \sim \beta(d)$ for each $d \in D$. We define $u(b) = (b, 0)$ and $v(c) = (c, 1)$. In the case of the other diagram, we want $H(u(a)) = f(a)$ and $H(v(a)) = g(a)$. So it is clear the unique map H making the diagram commute is $H(a, 0) = f(a)$ and $H(b, 1) = g(b)$. This is well defined since $H(\alpha(d), 0) = H(f(\alpha(d))) = H(g(\alpha(d))) = H(\alpha(d), 1)$. $\square$

Chapter 2

Groups, first encounter

2.1 Definition of group

Exercise 2.1.1. *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.*

Proof. Let G be a group. Define a category $\mathcal{C}$ by setting

- $\mathrm{Obj}(\mathcal{C}) = \{*\}$
- $\mathrm{Hom}(*,*) = G$
- $f \circ g = g \cdot f$
- $1_* = 1_G$

It is then clear that the isomorphisms from $*$ to $*$ is exactly G. □

Exercise 2.1.2. *Which sets of numbes of §1.1 can be made into groups by some standard operation.*

Proof.
1. $\mathbb{Z}$ is a group under addition.
2. $\mathbb{Q}$ is a group under addition.
3. $\mathbb{Q}^*$ is a group under multiplication.
4. $\mathbb{R}$ is a group under addition.
5. $\mathbb{R}^*$ is a group under multiplication.
6. $\mathbb{C}$ is a group under addition.
7. $\mathbb{C}^*$ is a group under multiplication.

□

Exercise 2.1.3. *For all elements g and h of a group G, we have $(gh)^{-1} = h^1 g^{-1}$.*

Proof. We have

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

and

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

By uniqueness of the inverse follows that $(gh)^{-1} = h^{-1}g^{-1}$. □

Exercise 2.1.4. *Suppose $g^2 = e$ for all elements g of a group G, then G is commutative.*

Proof. Take any $g, h \in G$. Then

$$e = (gh)^2 = ghgh.$$

Multiply both sides with g on the left, we get

$$g = g^2hgh = hgh.$$

Multiply by h on the left, we get

$$hg = h^2gh = gh,$$

hence h and g commute. □

Exercise 2.1.5. *The multiplication table of a group is an array compiling the results of all multiplications. Every row and every column of the multiplication table of a group contains all elements of the group exactly once.*

Proof. Take the row indexed by $g \in G$. Let $h \in G$ be arbitrary. Then in row g, and column $g^{-1}h$, we find the element h. If we find an element in row g more than one times, that means there are distinct columns h and h' such that $gh = gh'$. Then $g^{-1}gh = g^{-1}gh'$, implying $h = h'$. Contradiction.

Take the column indexed by $h \in G$. Take $g \in G$ arbitrary. Then in row gh^{-1} and column h, we find the element g. If we find an element in column h more than one times, that mean there are distinct rows g and g' such that $gh = g'h$. This implies that $ghh^{-1} = g'hh^{-1}$. Then $g = g'$, a contradiction. □

Exercise 2.1.6. *There is only one possible multiplication table for G if G has exactly 1, 2 or 3 elements. There are two distinct table of 4 elements, up to reordering of the elements of G. All groups of order ≤ 4 are commutative.*

Proof.

1. A group of 1 element, e, must clearly have the following table

	e
e	e

2. A group of order 2 must have an identity element e and another element a. Clearly we must have $ee = e$ and $ea = ae = e$. If $aa = a$, then $a^{-1}aa = a^{-1}a$, hence $a = e$, a contradiction. We obtain the following table

	e	a
e	e	a
a	a	e

3. A group of 3 elements must have an identity element e, and two other elements a and b. We must have the following table

	e	a	b
e	e	a	b
a	a		
b	b		

   By the previous exercise, we must have that either $aa = e$ or $aa = b$. If $aa = e$, then we have

	e	a	b
e	e	a	b
a	a	e	
b	b		

   By the previous exercise, we must have $ba = b$. But then we get $b^{-1}ba = b^{-1}b$, thus $a = e$, a contradiction. We must have $aa = b$ and then the table trivially fills up as

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

4. There must be an identity element e, and three other elements a,b, and c, we get

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

We either have $aa = e$, $aa = b$ or $aa = c$. The latter two options are clearly equivalent by relabeling.

- Assume $aa = b$, we get

	e	a	b	c
e	e	a	b	c
a	a	b		
b	b			
c	c			

From the previous exercise, we get either $ab = e$ or $ab = c$. If $ab = e$, we can fill up the table

	e	a	b	c
e	e	a	b	c
a	a	b	e	c
b	b			
c	c			

But the column c then contains two $c's$, a contradiction. Thus we must have $ab = c$, and thus

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b			
c	c			

We must have the $ca = e$, henc the table fills up as

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	c

- Assume $aa = e$, we get

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c		
c	c	b		

Now we have either $cc = e$ or $cc = a$. We obtain the following tables

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

This is equivalent with the previous table under the reordering $b \leftrightarrow a$. The other possibility is

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

All the obtained tables are easily checked to be commutative.

□

Exercise 2.1.7. *Let g be an element of finite order, and let $N \in \mathbb{Z}$. Then $g^N = e$ if and only if N is a multiple of $|g|$.*

Proof. Assume first that $g^N = e$. If N is positive, then it follows from Lemma 1.10 that N is a multiple of $|g|$. If $N = 0$, then N is clearly a multiple of $|g|$. If $N < 0$, then $g^{-N} = e$, hence $-N$ is a multiple of $|g|$ by hte previous. This implies directly that N is a multiple of $|g|$.
Conversely, if $N = a|g|$ for some $a \in \mathbb{Z}$, then

$$g^N = (g^{|g|})^a = e^a = e,$$

hence the result. □

Exercise 2.1.8. *Let G be an abelian finite group, with exactly one element f of order 2, then $\prod_{g \in G} g = f$.*

Proof. Group the product so that each element is paired with its inverse. This is only impossible if an element equals its inverse and thus has order 1 or 2. The other elements are cancelled, providing the right result. □

Exercise 2.1.9. *Let G be a finite group, of order n, and let m be the number of elements $g \in G$ of order exactly 2. Then $n - m$ is odd. Thus if n is even, then G necessarily contains elements of order 2.*

Proof. Let A be the subset of G consisting of elements which are not of order 2. These can either be the identity, or a nonidentity element. If $g \in A$ is a non-identity element, then $g^{-1} \in A$ is a distinct element from g. Thus A can be subdivided in pairs $\{g, g^{-1}\}$ and a singleton $\{e\}$. Thus A must be odd. This implies that $n - m$ is odd. In the case that n is even, it must be the case that m is odd, thus there is at least one element of order 2. □

Exercise 2.1.10. *Suppose the order of g is odd, what can you say about the order of g^2?*

Proof. By Proposition 1.13,

$$|g^2| = \frac{|g|}{\gcd(2, |g|)} = |g|.$$

□

Exercise 2.1.11. *For all g and h in a group G, we have $|gh| = |hg|$.*

Proof. First we prove $|g| = |aga^{-1}|$. Indeed, we have

$$(aga^{-1})^n = (aga^{-1})(aga^{-1})...(aga^{-1}) = ag^n a^{-1}.$$

Now if $(aga^{-1})^n = 1$, then $ag^n a^{-1} = 1$ and thus $g^n = 1$. Conversely, if $g^n = 1$, then $(aga^{-1})^n = ag^n a^{-1} = aa^{-1} = 1$. Thus $|g| = |aga^{-1}|$.
Now, we have that

$$|gh| = |hghh^{-1}| = |hg|.$$

Completing the proof. □

Exercise 2.1.12. *In the group of invertible 2×2 matrices, consider*

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

We have $|g| = 4$, $|h| = 3$ and $|gh| = \infty$.

Proof.

1. We compute g^2:
$$g^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$
And thus we have
$$g^3 = gg^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$
We obtain
$$g^4 = g^3 g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
Hence $|g| = 4$.

2. We compute h^2:
$$h^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}.$$
Thus
$$h^3 = hh^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$
Hence $|h| = 3$.

3. We compute gh:
$$gh = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$
We claim by induction that
$$(gh)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$
To prove this, it suffices to compute
$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}.$$
Hence the result holds and $|gh| = \infty$.

□

Exercise 2.1.13. *$|gh|$ is not necessarily equal to $lcm(|g|, |h|)$, even if g and h commute.*

Proof. In $\{1, -1\}$ with the product. Let $g = h = -1$. Then $|g| = |h| = 2$. But $|gh| = |1| = 1$. And $1 \neq \text{lcm}(|g|, |h|)$. □

Exercise 2.1.14. *If g and h commute and $gcd(|g|, |h|) = 1$, then $|gh| = |g||h|$.*

Proof. Let $N = |gh|$, then $(gh)^N = 1$. Since g and h commute, we have $g^N = (h^{-1})^N$. The order of g^N is $\frac{|g|}{\gcd(|g|,N)}$ and the order of $|h^{-1}|^N$ is $\frac{|h|}{\gcd(|h|,N)}$. We obtain that

$$\frac{|g|}{\gcd(|g|, N)} = \frac{|h|}{\gcd(|h|, N)}.$$

It follows that $|g|$ and $|h|$ have a prime divisor in common which would be a contradiction, unless if $\gcd(|g|, N) = |g|$ and $\gcd(|h|, N) = |h|$. This implies that $|g|$ and $|h|$ divide N. Since $\gcd(|g|, |h|) = 1$, we get that $|g||h|$ divide N. Since N also divides $|g||h|$ by Proposition 1.14, we get that $|gh| = |g||h|$. □

Exercise 2.1.15. *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 $|h| \leq |g|$. In fact, if h has finite order in G, then $|h|$ divides $|g|$.*

Proof. Let h be such that $|h|$ is finite but does not divide $|g|$. Then there is a prime p such that we can write $|h| = p^n s$ and $|g| = p^m r$ with r and s relatively prime to p and $m < n$. Then by g^{p^m} has order $|g|/\gcd(p^m, |g|) = r$. Also, h^s has order $|h|/\gcd(s, |h|) = p^n$. By the previous exercise, we get that $g^{p^m} h^s$ has order $p^n r$. This is an order larger than $|g|$, a contradiction. □

2.2 Examples of Groups

Exercise 2.2.1. *One can associate an $n \times n$ matrix M_σ with a permutation $\sigma \in S_n$ by letting the entry $(i, \sigma(i))$ be 1 and letting the other entries be 0. 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.

Proof. We have that

$$\begin{aligned} M_\sigma M_\tau(i,j) &= \sum_{k=1}^{n} M_\sigma(i,k) M_\tau(k,j) \\ &= M_\sigma(i, \sigma(i)) M_\tau(\sigma(i), j) \\ &= M_\tau(\sigma(i), j) \end{aligned}$$

This is 1 if $j = \tau(\sigma(i))$ and 0 otherwise. □

Exercise 2.2.2. *If $d \leq n$, then S_n contains elements of order d.*

Proof. Take (1 2 3 4 ... d). □

Exercise 2.2.3. *For every positive integer n, find an element of order n in $S_{\mathbb{N}}$.*

Proof. Use (1 2 3 4 ... n). □

Exercise 2.2.4. *Define a homomorphism $D_8 \to S_4$ by labelling vertices of a square. List the 8 permutations in the image of this homomorphism.*

Proof.

- 1
- (1 2 3 4)
- (1 3)(2 4)
- (1 4 3 2)
- (1 2)(3 4)
- (1 4)(2 3)
- (1 3)
- (2 4)

□

Exercise 2.2.5. *Describe generators and relations for all dihedral groups D_{2n}.*

Proof. Let x be the reflection about a line through the center of a regular n-gon and a vertex, and let y be the counterclockwise rotation by $2\pi/n$.
It is easy to see geometrically that $x^2 = 1$, $y^n = 1$ and $xy = y^{-1}x$.
These relations generate entire D_{2n} because the third relation shows how to commute y and x. This implies that any element can be written in the form $y^a x^b$, with $0 \leq a < n$ and $b \in \{0, 1\}$. There are $2n$ such elements so we get the entire dihedral group. □

Exercise 2.2.6. *For every positive integer n construct a group containing two elements g and h such that $|g| = 2$, $|h| = 2$, and $|gh| = n$.*

Proof. Let x be the reflection about a line through the center of a regular n-gon and a vertex, and let y be the counterclockwise rotation by $2\pi/n$.
Take $g = x$ and $h = xy$. Then $|g| = 2$, and $|gh| = |y| = n$. We also have that $h^2 = xyxy = xx^{-1}yy = 1$, thus $|h| = 2$. □

Exercise 2.2.7. *Find all elements of D_{2n} that commute with every other element.*

Proof. Let x be the reflection about a line through the center of a regular n-gon and a vertex, and let y be the counterclockwise rotation by $2\pi/n$.
It is easy to see geometrically that $x^2 = 1$, $y^n = 1$ and $xy = y^{-1}x$. Thus every element of D_{2n} has the form $y^a x^b$, where $0 \leq a < n$ and $b \in \{0, 1\}$.
Assume that y^a commutes with every element. Then it commutes with x, thus

$$y^a x = xy^a = y^{-a}x.$$

Thus $y^a = y^{-a}$ and hence $y^{2a} = 1$. This implies that $a = n/2$ or $a = 0$.. Assume on the other hand that $y^a x$ commutes with every element. Then it commutes with y, thus

$$y^{a+1}x = y^a xy = y^{a-1}x.$$

This implies that $y^{a+1} = y^{a-1}$, hence $y^2 = 1$. This is only possible if $n = 2$.
Thus in D_4, the group is abelian. For $n > 2$, we have that if n is odd, then no element commutes with every other element. If $n = 2a$ is even, then y^a and 1 is the only element that commutes with all elements. Indeed, it clearly commutes with any element of the form y^c. If the element is of the form $y^c x$, then

$$y^c xy^a = y^c y^{-a}x = y^c y^a x = y^a y^c x.$$

As desired. □

Exercise 2.2.8. *Find the orders of the groups of symmetries of the five platonic solids.*

Proof.

1. The tetrahedron. Let p be an arbitrary vertex of the tetrahedron. Then we can map this to 4 possible points $f(p)$. Let q be adjacent to p, then $f(q)$ must be adjacent to $f(p)$. Thus there are 3 possibilities for $f(q)$. In total we have 12 possibilities which completely determine the motion. We get a group of order 12.

2. The Cube. Let p be an arbitrary vertex of the cube. Then we can map this to 8 possible points $f(p)$. Let q be adjacent to p, then $f(q)$ must be adjacent to $f(p)$. Thus there are 3 extra possibilities. In total we have 24 possibilities which completely determine the motion. We get a group of order 24.

3. The octahedron. Let p be an arbitrary vertex of the octahedron. We can map this to 6 possible points $f(p)$. Let q be adjacent to p, then $f(q)$ must be adjacent to $f(p)$. Thus there are 4 extra possibilities. In total we have 24 possibilities which completely determine the motion. We get a group of order 24.

4. The dodecahedron. Let p be an arbitrary vertex of the dodecahedron. We can map this to 20 possible points $f(p)$. Let q be adjacent to p, then $f(q)$ must be adjacent to $f(p)$. Thus there are 3 extra possibilities. In total we have 60 possibilities which completely determine the motion. We get a group of order 60.

5. The icosahedron. Let p be an arbitrary vertex of the icosahedron. We can map this to 12 possible points $f(p)$. Let q be adjacent to p, then $f(q)$ must be adjacent to $f(p)$. Thus there are 5 extra possibilities. In total we have 60 possibilities which completely determine the motion. We get a group of order 60.

□

Exercise 2.2.9. *Congruence mod n is a congruence relation.*

Proof.

- Since n divides $a - a = 0$, we have that $a \cong b$.
- Assume that $a \cong b$. Then n divides $a - b$,m eaning that $a - b = kn$. But then $b - a = (-k)n$, so n divides $b - a$ and $b \cong a$ holds.
- Assume that $a \cong b$ and $b \cong c$. Then $kn = a - b$ and $ln = b - c$. Thus $(l + k)n = a - c$, and we get that a$\cong c$.

□

Exercise 2.2.10. *$\mathbb{Z}/n\mathbb{Z}$ consists of precisely n elements.*

Proof. We show first that the elements $[0], [1], ..., [n-1]$ are all distinct. Indeed, take $0 \leq k, l \leq n-1$, such that $k \cong l$. Then $nx = k-l$ for some x. But since $-(n-1) \leq k-l \leq n-1$, we must have $n|x| = |k-l| < n$, which implies $x = 0$. Thus $k = l$.
Now given any $x \in \mathbb{Z}$, we can write $x = nq + r$, with $0 \leq r < n$. But then $x \cong r$ and $[r]$ is among the classes $[0], [1], ..., [n-1]$. □

Exercise 2.2.11. *The square of every odd integer is congruent to 1 modulo 8.*

Proof. An odd integer is congruent to 1,3,5,7 modulo 8. Thus the squares are

$$1^2 = 1,$$

$$3^2 = 9 = 1,$$

$$5^2 = 25 = 1,$$

$$7^2 = 49 = 1,$$

all in modulo 8. □

Exercise 2.2.12. *There are no integers a, b and c such that $a^2 + b^2 = 3c^2$.*

Proof. We look at the equation in $\mathbb{Z}/4\mathbb{Z}$. We have for $c = 0, 1, 2, 3$ that $3c^2 = 0, 3, 0, 3$. We have the following table for $a^2 + b^2$, with a vertically and b horizontally:

	0	1	2	3
0	0	1	0	1
1	1	2	1	2
2	0	1	0	1
3	1	2	1	2

The only possible solutions are if a, b and hence c are all even. Write $a = 2^m x$, $b = 2^n y$ and $c = 2^k z$, where x, y and z are all odd. We would have

$$2^{2m}x^2 + 2^{2n}y^2 = 2^{2k}z^2.$$

Erasing the factors of 2, we would have a solution that has one term odd, a contradiction. □

Exercise 2.2.13. *If $gcd(m, n) = 1$, then there exists integers a and b such that $am + bn = 1$. Conversely, if $am + bn = 1$ for some integers a and b, then $gcd(m, n) = 1$.*

Proof. By Corollary 2.5, we know that $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$. In particular, there is some integer a such that $[am]_n = [1]_n$, or equivalently n divides $am - 1$. Thus there is some b such that $bn = am - 1$, hence $1 = am - bn$.
Conversely, let $am + bn = 1$ and let d divide m and n. Then clearly d divides 1. Thus $d = \pm 1$. The result follows. □

Exercise 2.2.14. *The multiplication operator on $\mathbb{Z}/n\mathbb{Z}$ is well-defined.*

Proof. Let $[a]_n = [a']_n$ and $[b]_n = [b']_n$. This means that n divides both $a - a'$ as $b - b'$. Now we have that

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'.$$

So we see that n divides $ab - a'b'$. □

Exercise 2.2.15. *Let $n > 0$ be an odd integer.*

- *If $gcd(m, n) = 1$, then $gcd(2m + n, 2n) = 1$.*
- *If $gcd(r, 2n) = 1$, then $gcd\left(\frac{r+n}{2}, n\right) = 1$.*
- *The function*
$$\varphi : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/2n\mathbb{Z})^* : [m]_n \to [2m + n]_{2n}$$
is a bijection.

Proof.

- Take a positive prime number p dividing both $2m + n$ and $2n$. If $p = 2$, then we get from this that p divides n, a contradiction. If $p > 2$, then p divides n. We get that p divides $2m$ and thus m, a contradiction.
- Assume that p is a positive prime number dividing n and $\frac{r+n}{2}$. Since p divides n, we get that p is odd. We also get that $2p$ divides $r + n$. Thus p divides both $r + n$ and n. We get that p divides r and $2n$. Contradiction.
- We check well-defined, assume that $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, that means that $\gcd(m, n) = 1$. By the first point, we get that $\gcd(2m + n, 2n) = 1$, hence $[2m + n]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$. Now define
$$\psi : (\mathbb{Z}/2n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^* : [r]_{2n} \to [(r + n)/2]_n.$$
We check well-defined, assume that $[r]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$. Then $\gcd(r, 2n) = 1$, and thus by the second point $\gcd\left(\frac{r+n}{2}, n\right) = 1$. This means that $[(r+n)/2]_n \in (\mathbb{Z}/n\mathbb{Z})^*$. We check that φ and ψ are inverses. Indeed,
$$\begin{aligned} \psi(\varphi([m]_n)) &= \psi([2m + n]_{2n}) \\ &= [((2m + n) + n)/2]_n \\ &= [m + n]_n \\ &= [m]_n \end{aligned}$$
and
$$\begin{aligned} \varphi(\psi([r]_{2n})) &= \varphi([(r + n)/2]_n) \\ &= [2(r + n)/2 + n]_{2n} \\ &= [r + 2n]_{2n} \\ &= [r]_{2n} \end{aligned}$$

□

Exercise 2.2.16. *Find the last digit of* $1238237^{18238456}$.

Proof. In (mod 10), we have $1238237 \equiv 7$. Thus it suffices to find the last digit of $7^{18238456}$.
We have

$$7^1 \equiv 7,\ 7^2 \equiv 9,\ 7^3 \equiv 3, 7^4 \equiv 1.$$

Since $18238456 = 4 * 4559614$. We get that the last digit is 1. □

Exercise 2.2.17. *If* $m \equiv m'$ *mod* n, *then* $gcd(m, n) = 1$ *if and only if* $gcd(m', n) = 1$.

Proof. We know that $nx = m - m'$. Thus if a divides m and n, it is easily seen to divide m'. If a divides m' and n, it is easily seen to divide m. Thus the result follows. □

Exercise 2.2.18. *If* $d \leq n$, *define an injective function* $\mathbb{Z}/d\mathbb{Z} \to S_n$ *preserving the operation.*

Proof. We define $\theta : \mathbb{Z}/d\mathbb{Z} \to S_n$ by setting $\theta(k) = (1\ 2\ ...\ d)^k$. □

Exercise 2.2.19. *Both* $(\mathbb{Z}/5\mathbb{Z})^*$ *and* $(\mathbb{Z}/12\mathbb{Z})^*$ *consists of* 4 *elements. Write their multiplication tables, and prove no re-ordering of the elements will make them match.*

Proof. We have $(\mathbb{Z}/5\mathbb{Z}^*) = \{1, 2, 3, 4\}$ and $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$. We get as multiplication table for $(\mathbb{Z}/5\mathbb{Z})^*$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

We have only two elements x with $x^2 = 1$. We get as multiplication table for $(\mathbb{Z}/12\mathbb{Z})^*$

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

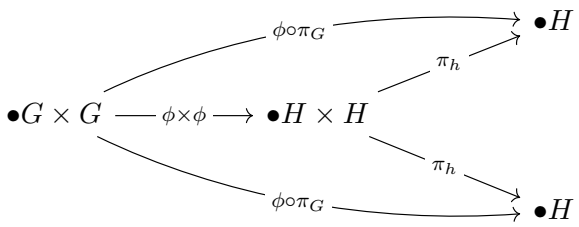
All elements x here satisfy $x^2 = 1$. Thus the two multiplication tables cannot match. □

2.3 The category Grp

Exercise 2.3.1. *Let* $\phi : G \to H$ *be a morphism in a category* C *with products. Explain why there is a unique morphism*

$$(\phi \times \phi) : G \times G \to H \times H.$$

Proof. Since $\phi \circ \pi_G$ is morphism $G \times G \to H$, by universal property of product we know that there exists a unique morphism, called $\phi \times \phi : G \times G \to H \times H$ such that



commutes. □

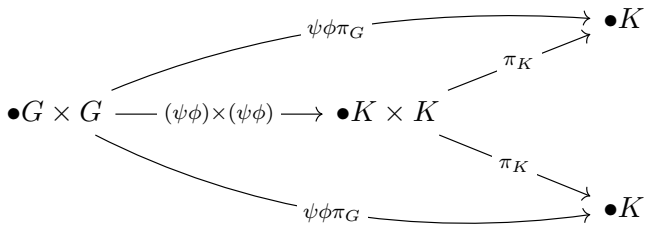
Remarks. Notice that technically the problem is incorrect since there does not exists a unique morphism $G \times G \to H \times H$, however, by univeral property of products, we do know that there is a unique morphism from $G \times G \to H \times H$ which makes the above diagram commute.

Exercise 2.3.2. *Let $\phi : G \to H, \psi : H \to K$ be morphism in a category with prodcuts, and conside morphism between the products, $G \times G$, $H \times H$, $K \times K$ as in exercise 2.3.1. Prove that*

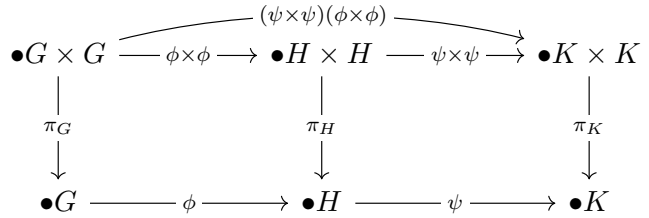
$$(\psi\phi) \times (\psi\phi) = (\psi \times \psi)(\phi \times \phi).$$

(This is part of the commtuativity of the diagram displayed in the section 2.3.2)

Proof. Since $\phi : G \to H$ and $\psi : H \to K$, by the universal property of products, there is unique morphism $(\psi\phi) \times (\psi\phi)$ such that



commutes. Again by universal property of products, we know that there exists unique morphisms $\phi \times \phi : G \times G \to H \times H$ and $\psi \times \psi : H \times H \to K \times K$ such that



commutes. However, since such a morphism $G \times G \to K \times K$ making the baove diagram commutes is unique, it must be the case that $(\psi\phi) \times (\psi\phi) = (\psi \times \psi)(\phi \times \phi)$. □