I. Preliminaries: Set theory and categories

3. Category Theory

3.1.

Solution. To make this into a category, we have to define the composition set-function $\circ_{Cop} : \mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(A,B) \times \mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(B,C) \to \mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(A,C)$, for A, B, C objects of C^{op}. Let $f \in \mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(A,B)$ and $g \in \mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(B,C)$ be morphisms in C^{op}. We will define the morphism $g \circ_{\mathsf{C}^{\mathsf{op}}} f$ as the composition $f \circ_{\mathsf{C}} g$ (in the original category C). Since $f \in \mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(A,B)$, then $f \in \mathrm{Hom}_{\mathsf{C}}(B,A)$ and similarly $g \in \mathrm{Hom}_{\mathsf{C}}(C,B)$ thus $f \circ_{\mathsf{C}} g \in \mathrm{Hom}_{\mathsf{C}}(C,A)$ and therefore $g \circ \mathsf{C}^{\mathsf{op}} f \in \mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(A,C)$.

To confirm this composition makes C^{op} into a category, we have to check all the required properties.

- For any objects $A, B, C, D \in \mathrm{Obj}(\mathsf{C}^{\mathsf{op}})$ the sets of morphisms $\mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(A,B)$ and $\mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(C,D)$ are disjoint unless $A = C$ and $B = D$, as this follows easily from the sets definitions.
- For any $A \in \mathrm{Obj}(\mathsf{C}^{\mathsf{op}})$, we have $\mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(A,A) = \mathrm{Hom}_{\mathsf{C}}(A,A)$, and thus it follows the identity morphisms remain the same.
- The composition is associative, as for any three morphisms f, g, h (from the respective sets), $(h \circ_{\mathsf{C}^{\mathsf{op}}} g) \circ_{\mathsf{C}^{\mathsf{op}}} f = (g \circ_{\mathsf{C}} h) \circ_{\mathsf{C}^{\mathsf{op}}} f = f \circ_{\mathsf{C}} (g \circ_{\mathsf{C}} h) = (f \circ_{\mathsf{C}} g) \circ_{\mathsf{C}} h = h \circ_{\mathsf{C}^{\mathsf{op}}} (f \circ_{\mathsf{C}} g) = h \circ_{\mathsf{C}^{\mathsf{op}}} (g \circ_{\mathsf{C}^{\mathsf{op}}} f)$, as needed.
- We also need to check that the identity morphisms are indeed identities with respect to $\circ_{\mathsf{C}^{\mathsf{op}}}$. Let $f \in \mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(A,B)$. Then $f \circ_{\mathsf{C}^{\mathsf{op}}} 1_A = 1_A \circ_{\mathsf{C}} f = f$. Similarly, $1_B \circ_{\mathsf{C}^{\mathsf{op}}} f = f \circ_{\mathsf{C}} 1_B = f$. □

3.2.

Solution. Suppose A is a finite set. $\mathrm{End}_{\mathsf{Set}}(A) = A^A$, i.e. the set of all the set-functions of the form $f : A \to A$. Since A is a finite set, by Exercise I.2.10 we have $\left|A^A\right| = |A|^{|A|}$. □

3.3.

Solution. Let $f = (a,b)$. We have $1_a = (a,a)$ and $1_b = (b,b)$. By the definition of the composition in this category, we have $f1_a = (a,b) = f$ and $1_b f = (a,b) = f$, which is exactly what we needed. □

3.4.

Solution. We cannot. This is because the relation $<$ is not reflexive. The reflexivity is needed to ensure the existence of identity morphisms in the category. Without it, for any $a \in \mathbb{Z}$, we would have $\mathrm{Hom}(a, a) = \emptyset$, as $a \not< a$. □

3.5.

Solution. We could take the defining relation of the categories considered in Example I.3.3 to be, for any two sets $A, B \in \mathcal{P}(S)$, $A \sim B \iff A \subseteq B$. □

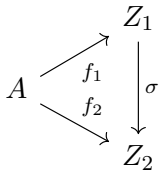
3.6.

Solution. The definition of composition is straightforward. If we have $f \in \mathrm{Hom}_{\mathsf{V}}(n, m)$ and $g \in \mathrm{Hom}_{\mathsf{V}}(m, r)$, f is a $m \times n$ matrix, and g is a $r \times m$ matrix. We can then define the composition gf as the product of the two matrices in that order, the resulting matrix will be $r \times n$, and thus $gf \in \mathrm{Hom}_{\mathsf{V}}(n, r)$.

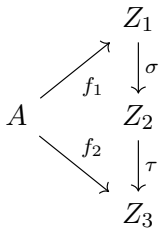
Now, to check that this makes V into a category, we also have to find the identity morphisms. For any $n \in \mathbb{N}$ there is surely the identity matrix with ones on the main diagonal and zeroes elsewhere, we will take this as the identity morphism. This is of course an identity with respect to the composition defined above, as it is an identity with respect to matrix multiplication. The composition is also associative, from the properties of matrix multiplication. □

3.7.

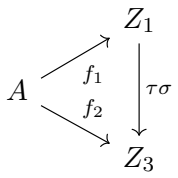
Solution. The category we are considering is similar to the opposite category of C_A, that is everything remains the same but the direction of the arrows change. This category is usually denoted as C^A. The objects of this category are the morphisms $f : A \to Z$ for some $Z \in \mathrm{Obj}(\mathsf{C})$. The morphisms of this category are commutative diagrams:



where σ is a morphism of the ambient category making the given diagram commute. To find the composition of two morphisms in this category, consider the diagram:



Notice that removing the central arrow results in the diagram



which commutes because of the fact that C is a category. □

3.8.

Solution. To construct the category we need to specify its objects and its morphisms:

- $\mathrm{Obj}(\mathsf{InfSet})$:= the class off all infinite sets
- For any two infinite sets $A, B \in \mathrm{Obj}(\mathsf{InfSet})$ we let $\mathrm{Hom}_{\mathsf{InfSet}}(A, B)$:= the set of all set functions between A and B

Now, identities and composition can be inherited from Set. This makes it into a full subcategory of Set though, as for all $A, B \in \mathrm{Obj}(\mathsf{InfSet})$ we have $\mathrm{Hom}_{\mathsf{InfSet}}(A, B) = \mathrm{Hom}_{\mathsf{Set}}(A, B)$. □

3.9.

Solution. We will define the category MSet as follows:

- $\mathrm{Obj}(\mathsf{MSet}) := (S, \sim)$, where S is any set and $\sim \subset S \times S$ is an equivalence relation on S.
- For $(S, \sim_1), (R, \sim_2) \in \mathrm{Obj}(\mathsf{MSet})$ we define $\mathrm{Hom}_{\mathsf{MSet}}((S, \sim_1), (R, \sim_2))$ to be the set of all set-functions $f : S \to R$ such that for $s_1, s_2 \in S$ we have $s_1 \sim_1 s_2 \implies f(s_1) \sim_2 f(s_2)$.
- The identity morphisms for $A = (S, \sim) \in \mathrm{Obj}(\mathsf{MSet})$ in this category will be the set-functions $1_A : S \to S$ such that $1_A(s) = s$. The required condition will obviously hold.
- The composition of two morphisms $f \in \mathrm{Hom}_{\mathsf{MSet}}((S, \sim_1), (R, \sim_2))$, $g \in \mathrm{Hom}_{\mathsf{MSet}}((R, \sim_2), (T, \sim_3))$ will be defined as the standard composition of the underlying set-functions. The required condition will hold, because for $s_1, s_2 \in S$, such that $s_1 \sim_1 s_2$ we have must have $f(s_1) \sim_2 f(s_2)$ and thus $gf(s_1) = g(f(s_1)) \sim_3 g(f(s_2)) = gf(s_2)$. Therefore $gf \in \mathrm{Hom}_{\mathsf{MSet}}((S, \sim_1), (T, \sim_3))$.
- The associativity and identity morphisms being identities with respect to composition all follow from the properties of set-functions.

The category Set is contained in MSet as a full subcategory, as for any $S \in \mathrm{Obj}(\mathsf{Set})$ we have the object $(S, \sim) \in \mathrm{Obj}(\mathsf{MSet})$, where $\sim$ is the "identity" relation where for any

$s, r \in S$ we have $s \sim s$, but $s \not\sim r$. For any $R \in \mathrm{Obj}(\mathsf{Set})$ we then have $\mathrm{Hom}_{\mathsf{Set}}(S, R) = \mathrm{Hom}_{\mathsf{MSet}}(S, R)$

The objects of MSet that correspond to ordinary multisets are those whose underlying set is countable, as by the definition in Example I.2.2, multisets are those sets A for which we have a function $f : A \to \mathbb{N}$. □

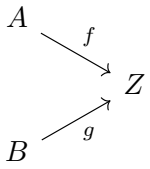
3.10.

Solution. The subobject classifier in Set is the set $\Omega = \{0, 1\}$. For any set S the morphism, a set-function in this case, $f : S \to \Omega$ is then equal to a subset of S, as it defines precisely which elements are part of the subset (those that map to 1, for example), and which are not. □

3.11.

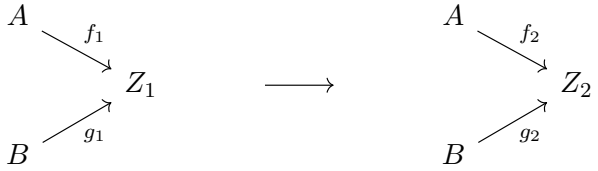
Solution. Lets start by defining the category $\mathsf{C}^{A,B}$:

- $\mathrm{Obj}(\mathsf{C}^{A,B})$ = diagrams

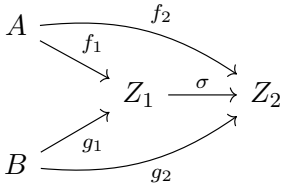


  in C, and

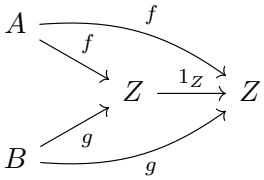
- morphisms



  are commutative diagrams

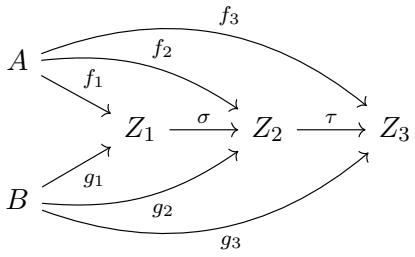


- The identity morphisms will be the diagrams

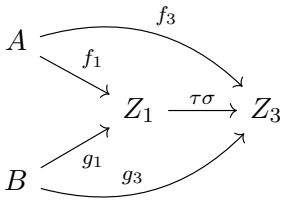


that must commute.

- The composition of two morphisms is again just a product of compositions in C. To see this, notice that the diagram



  is indeed commutative (inherited from C) and thus the diagram



  is commutative as well. Since $\tau\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_3)$, we define this diagram to be the composition of the two given morphisms.

The definition of $\mathsf{C}^{\alpha,\beta}$ is very similar, only adding an object and two arrows into each diagram. □

4. Morphisms

4.1.

Solution. Let C be a category and for any $n \in \mathbb{N}$, f_n a morphism in C such that we can form the composition $((\dots((f_n f_{n-1})f_{n-2})\dots)f_1)$. We will now prove that no matter the way we place the parentheses, the result of the composition remains the same. We will procede by induction on n:

- For $n = 2$, we only have one choice, $(f_2 f_1)$.
- Let $n \in \mathbb{N}$. Suppose that for all $m \leq n$, $m \in \mathbb{N}$, it does not matter how we place the parentheses in the composition $f_m f_{m-1} \dots f_1$. Now, let us have some placement of parentheses on the composition $f_n f_{n-1} \dots f_1$. Then we can split this composition into separate pieces contained in some outer pair of parentheses. Either there is just one pair of those outermost parentheses. Then there is some morphism that is composed with other morphisms in parentheses. Then the rest is shorter than n and we can ignore the parentheses, and then the result follows from the case $n = 2$. Otherwise, those pieces all contain less than n morphisms, and we can reorder the parentheses in them at will. Since the whole composition of those pieces is also shorter than n, we can reorder the parentheses at will.

□

4.2.

Solution. For a category to be a groupoid, all the morphisms have to be isomorphisms. That means every morphism will have a corresponding inverse. By the definition of the categories in Example I.3.3, there is at most one morphism for any two objects A, B, and it exists if and only if $A \sim B$. Therefore, for an inverse to exist, we need there to be a morphism $B \to A$, which only exists if $B \sim A$, and thus $\sim$ must be symmetric. □

4.3.

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

- Suppose f has a right-inverse $g : B \to A$ such that $fg = 1_B$. Let Z_1, Z_2 be any two objects of the category C and $\alpha_1 : B \to Z_1$ and $\alpha_2 : B \to Z_2$ be any morphisms. Then if $\alpha_1 f = \alpha_2 f$, we have $(\alpha_1 f)g = (\alpha_2 f)g$, so $\alpha_1(fg) = \alpha_2(fg)$, thus $\alpha_1 1_B = \alpha_2 1_B$ and therefore $\alpha_1 = \alpha_2$. This proves f is an epimorphism as needed.
- Take for example the category defined in Example I.3.3, $\mathbb{Z}$ endowed with $\leq$. Then take for example the morphism $(4, 5)$. It is an epimorphism, as if we have two morphism $(5, z_1)$ and $(5, z_2)$, $(5, z_1)(4, 5) = (4, z_1)$ and $(5, z_2)(4, 5) = (4, z_2)$. Now if $(4, z_1) = (4, z_2)$, we must have $z_1 = z_2$, but then $(5, z_1) = (5, z_2)$. This epimorphism does not have a right-inverse, because the only choice would be $(5, 4)$, which does not exist as $5 \not\leq 4$.

□

4.4.

Solution. Let C be a category and for A, B, C objects of C, let $f : A \to B$, $g : B \to C$ be monomorphisms. Now, let Z_1, Z_2 be any objects of C and $\alpha_1 : B \to Z_1$, $\alpha_2 : B \to Z_2$. Suppose $\alpha_1(gf) = \alpha_2(gf)$, so $(\alpha_1 g)f = (\alpha_2 g)f$. But we know f is an monomorphism, so $\alpha_1 g = \alpha_2 g$. But g is also an monomorphism, and thus $\alpha_1 = \alpha_2$. Thus, gf is an monomorphism. We can therefore define a category C_{mono}, keeping the same objects as C, but restricting the set of morphisms to monomorphisms only. Since a composition of monomorphisms is itself a monomorphism, the same composition function used in C works in C_{mono}. Identities also remain the same, as they are isomorphisms.

We can do the same for epimorphisms, the proof is essentially the same.

We cannot define a category $\mathsf{C}_{nonmono}$ as the identity morphisms are trivially monomorphisms. □

4.5.

Solution. We cannot simply use the concepts of injective and surjective set-functions, as we are dealing with elements that can be equal to each other. On the other hand, our monomorphisms and epimorphisms will have to be identical to those concepts for the full subcategory of Set.

Let $A = (S, \sim_S), B = (R, \sim_R)$ be objects of MSet, and let $f : A \to B$ be a morphism of this category. For f to be a monomorphism in MSet, it must hold that $[f(a)]_{\sim_R} = [f(b)]_{\sim_R} \implies [a]_{\sim_S} = [b]_{\sim_S}$. For f to be an epimorphism, it must hold that for all classes of equivalence $[b]_{\sim_R} \in R/\sim_R$ there is some $a \in S$ such that $f(a) \in [b]_{\sim_R}$. □

5. Universal properties

5.1.

Solution. Suppose I is an initial object of a category C. This means that for any object A of C, there exists a single morphism $I \to A$. By the construction of C^{op}, $\mathrm{Hom}_{\mathsf{C}^{\mathsf{op}}}(I, A) = \mathrm{Hom}_{\mathsf{C}}(A, I)$, thus it must be a singleton, and therefore I is a final object in C^{op}. □

5.2.

Solution. Suppose $I \neq \emptyset$ is an initial object in Set. By Proposition I.5.4 there is a uniquely defined isomorphism $f : \emptyset \to I$. But there is only one such set-function, defined by the empty graph from $\emptyset$ to I, which is not an isomorphism, because namely, it cannot be surjective. A contradiction. □

5.3.

Solution. Suppose F_1, F_2 are final objects of a category C. Then by the defining property of final objects, there exists unique morphisms $f : F_1 \to F_2$ and $g : F_2 \to F_1$. The only morphism from a final object to itself must be the identity morphism, thus $gf = 1_{F_1}$ and $fg = 1_{F_2}$ and therefore, f is an isomorphism between F_1 and F_2. Moreover, this isomorphism is uniquely determined. □

5.4.

Solution. The initial and final objects of the group Set^* will be the singleton sets with a single distinguished element. To see that they are initial, note that there is a single morphism f from $(\{ s \}, s)$ to any other pointed set (R, r) such that for the underlying set-function we have $f(s) = r$. To see that they are final, we can just send all elements to the single unique element of the final object. □

5.5.

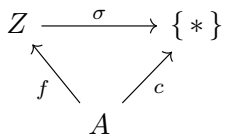
Solution. The final object of the category is, for example (note that any singleton will do), the object

$$A \xrightarrow{c} \{*\}$$

with c being the constant function. This function surely satisfies the constraint posed. To see this is truly a final object of the category, note that for any other object

$$A \xrightarrow{f} Z$$

there is a unique commutative diagram



The uniqueness of this diagram is given by the uniqueness of σ, which can only be the constant function, which surely makes this diagram commute, as for any $a \in A$ $\sigma f(a) = * = c(a)$. □

5.6.

Solution. For $m_1 \times m_2$ to be a product in this category, it must hold that $m_1 \times m_2$ divides both m_1 and m_2, and that any divisor of both of them must divide $m_1 \times m_2$. The only reasonable choice for this product is the greatest common divisor. Similarly for coproducts, both m_1 and m_2 must divide it, and also if they both divide any other positive integer, it is divisible by the coproduct. In this case, it is the least common multiple of the numbers. □

5.7.

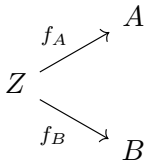
Solution. Suppose A', A'', B', B'' be sets such that $A' \cong A''$, $B' \cong B''$, $A' \cap A'' = \emptyset$ and $B' \cap B'' = \emptyset$. We will first show that $A' \cup B'$ is a coproduct of A' and B' in Set, then the same for $A'' \cup B''$, and finally, using Proposition I.5.4, we will conclude that those two sets are indeed isomorphic.

Let $i_{A'} : A' \to A' \cup B'$ be defined for any $a \in A'$ as $i_{A'}(a) = a$ and similarly for $i_{B'} : B' \to A' \cup B'$ we define for any $b \in B'$ $i_{B'}(b) = b$. Let Z be any set and $f_{A'} : A' \to Z, f_{B'} : B' \to Z$ morphisms. To show that this construction satisfies the universal property for coproducts, we need to find a morphism $\sigma : A' \cup B' \to Z$ which is unique. Indeed to make the relevant diagram commute, the only possible function maps any $c \in A' \cup B'$ to $f_{A'}(c)$ if $c \in A'$ and to $f_{B'}(c)$ otherwise. Note that $A' \cap B' = \emptyset$ and therefore we can either have $c \in A'$ or $c \in B'$ and thus the function is well defined.

Now, since $A' \cong A''$ and $B' \cong B''$, there must be isomorphisms $f : A' \to A''$ and $g : B' \to B''$. Define $i_{A'} = f$ and $i_{B'} = g$. We must now show that $A'' \cup B''$ with those two morphisms forms a coproduct of A' and B' in Set. Let Z be any set and $f_{A'} : A' \to Z, f_{B'} : B' \to Z$ morphisms. Define $\sigma : A'' \cup B'' \to Z$ such that for $c \in A'' \cup B''$ we have $\sigma(c) = f_{A''} f^{-1}$ if $c \in A''$, $\sigma(c) = f_{B''} g^{-1}$ otherwise. Note that $A'' \cap B'' = \emptyset$ and thus either $c \in A''$ or $c \in B''$. Thus $A'' \cup B''$ is also a coproduct in Set. By Proposition I.5.4 it must follow that $A' \cup B' \cong A'' \cup B''$. □

5.8.

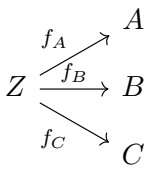
Solution. Let C be a category, and A, B objects of this category. Notice, that the universal property of a product $A \times B$ is based on the accessory category $\mathsf{C}_{A,B}$. Similarly, for $B \times A$, we have a category $\mathsf{C}_{B,A}$. However, these categories are equal - the objects of both are the diagrams



Therefore both $A \times B$ and $B \times A$ in fact satisfy the same universal property (of being final in the category $\mathsf{C}_{A,B}$ with the natural projections π_A, π_B). Therefore, by Proposition I.5.4., it follows that $A \times B \cong B \times A$. □

5.9.

Solution. The reasonable choice for the required universal property is for $A \times B \times C$ to be the final object of the category with objects defined as the diagrams



and morphisms defined similarly as in the category $\mathsf{C}_{A,B}$.

Now, we shall prove that the products $(A \times B) \times C$ and $A \times (B \times C)$ satisfy this universal property. For $(A \times B) \times C$, there must be morphisms $\pi'_{A \times B} : (A \times B) \times C \to A \times B$ and $\pi'_C : (A \times B) \times C$ and because $A \times B$ is in itself a product the morphisms $\pi''_A : A \times B \to A$ and $\pi''_B : A \times B \to B$. We can then define $\pi_A = \pi''_A \pi'_{A \times B}$ and similarly for π_B and π_C Now let Z be any object of C and $f_A : Z \to A, f_B : Z \to B, f_C : Z \to C$ any morphism. The only possible choice for the required morphism σ is the unique morphism

$\sigma' : Z \to (A \times B) \times C$ that must exist because $(A \times B) \times C$ satisfies the ultimate property for product of two objects. This morphism makes the required diagram commute, as $\pi_A \sigma = (\pi''_A \pi'_{A \times B})\sigma' = \pi''_A(\pi'_A \sigma') = \pi''_A f'_A = f_A$ (the last part must hold by the universal property of $A \times B$) and similarly for π_B and π_C. Thus $(A \times B) \times C$ satisfies the required universal property f the product $A \times B \times C$. The case for $A \times (B \times C)$ is entirely analogous.

Therefore by Proposition I.5.4 it follows that $(A \times B) \times C \cong A \times (B \times C)$. The other conclusion we can draw is that if C is a category with products of two objects also has products of three objects. □

5.10.

Solution. Let I be a set of indices, and $X_{i \in I}$ an indexed set of objects of a category C. We will now define the universal properties for products and coproducts of indexed sets.

An object $\prod_{i \in I} X_i$ together with morphisms $\pi_{X_i} : \prod_{i \in I} X_i \to X_i$ for $i \in I$ is a product of $X_{i \in I}$ in C, if for any object Z of C and morphisms $f_{X_i} : Z \to X_i$, there exists a unique morphism σ that makes all the diagrams

$$\begin{array}{ccc} \prod_{i \in I} X_i & \xrightarrow{\pi_{X_i}} & X_i \\ {\scriptstyle\sigma}\uparrow & \nearrow_{f_{X_i}} & \\ Z & & \end{array}$$

commute. Similarly, an object $\coprod_{i \in I} X_i$ together with morphisms $i_{X_i} : X_i \to \coprod_{i \in I} X_i$ is a coproduct of $X_{i \in I}$, if for any object Z of C and morphisms $f_{X_i} : X_i \to Z$, there exists a unique morphism σ that makes all the diagrams

$$\begin{array}{ccc} X_i & \xrightarrow{i_{X_i}} & \coprod_{i \in I} X_i \\ & \searrow^{f_{X_i}} & \downarrow{\scriptstyle\sigma} \\ & & Z \end{array}$$

commute. We say a category has products (coproducts) if for any index set I and objects $X_{i \in I}$ there is an object $\prod_{i \in I} X_i$ ($\coprod_{i \in I} X_i$) satisfying the universal property of products (coproducts) given above.

Now, we have not placed any restraints on the index set I. If the set is finite, it is enough for a product (coproduct) of two objects to exist and we can build the full product (coproduct) similarly as in Problem I.5.9.

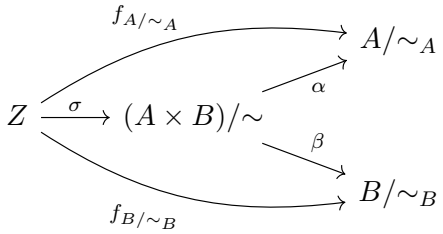
Products and coproducts of indexed sets of objects indeed exist in Set.

□

5.11.

Solution. Let A, B be sets, i.e. objects of the category Set, $A \times B$ their product in Set with the corresponding natural morphisms $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$ and $\sim_A, \sim_B, \sim$ equivalence relations on A, B and $A \times B$ respectively. We assume that both A and B are non-empty, as otherwise the result is vacuous.

- Let b be any element of B (note that we assumed B is non-empty). Then there is a function $a \mapsto [(a, b)]_\sim$, $a \in A$. Then by universal property of quotients there exists a unique function $\alpha : (A \times B)/\sim \to A/\sim_A$, $\alpha([(a, b)]_\sim) = [a]_{\sim_A}$. Similarly, there is a function $\beta : (A \times B)/\sim \to B/\sim_B$.
- Now, let Z be any set and $f_{A/\sim_A} : Z \to A/\sim_A$, $f_{A/\sim_B} : Z \to B/\sim_B$ be set-functions. We want to show that $(A \times B)/\sim$ is a product of $A/\sim_A$ and $B/\sim_B$ in Set. Thus we want to show there is a unique set-function σ making the diagram



  commute. Now, notice that $\pi_{\sim_A} : A \to A/\sim_A$ and $\pi_{\sim_B} : B \to B/\sim_B$ are both surjective set-functions. Therefore there exist right-inverses $g_A : A/\sim_A \to A$ and $g_B : B/\sim_B \to B$. Now we can define $\sigma(z) = [(g_A \circ f_{A/\sim_A}(z), g_B \circ f_{B/\sim_B}(z))]_\sim$. Then clearly we have

$$\begin{aligned} \alpha \circ \sigma(z) &= \alpha([(g_A \circ f_{A/\sim_A}(z), g_B \circ f_{B/\sim_B}(z))]_\sim) \\ &= [g_A \circ f_{A/\sim_A}(z)]_{\sim_A} \\ &= f_{A/\sim_A}(z). \end{aligned}$$

  Similarly for $f_{B/\sim_B}$. However, there is still the issue of uniqueness of this set-function. In general, there are many different right-inverses of $\pi_{\sim_A}$ (and $\pi_{\sim_B}$). To prove σ is unique, suppose $f_1, f_2 : A/\sim_A \to A$, $g_1, g_2 : B/\sim_B \to B$ be two right-inverses of $\pi_{\sim_A}$ and $\pi_{\sim_B}$ respectively. We want to show that

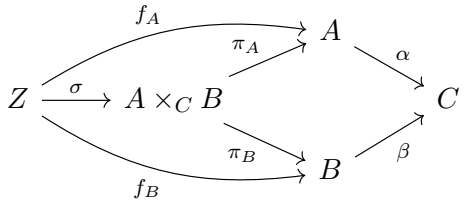
$$[(f_1([a]_{\sim_A}), g_1([b]_{\sim_B}))]_\sim = [(f_2([a]_{\sim_A}), g_2([b]_{\sim_B}))]_\sim.$$

  Suppose $f_1([a]_{\sim_A} = a_1$, $f_2([a]_{\sim_A}) = a_2$, $g_1([b]_{\sim_B}) = b_1$ and $g_2([b]_{\sim_B}) = b_2$. By the definition of equivalence classes, we must have $a_1 \sim_A a_2$ and $b_1 \sim_B b_2$. But then by definition of $\sim$ we have $(a_1, b_1) \sim (a_2, b_2)$, and thus the $[(a_1, b_1)]_\sim = [(a_2, b_2)]_\sim$. Therefore σ is indeed a unique set-function.
- Therefore, we must have have $(A \times B)\backslash\sim \cong (A\backslash\sim_A) \times (B\backslash\sim_B)$ by Proposition I.5.4, which is exactly what we wanted to prove. □

5.12.

Solution. Suppose C is a category.

- Suppose $\alpha : A \to C, \beta : B \to C$ are morphisms in the category C. A fibered product $A \times_C B$ of A and B is an object of C, endowed with morphisms $\pi_A : A \times_C B \to A$ and $\pi_B : A \times_C B \to B$ that is final in $\mathsf{C}_{\alpha,\beta}$: for any object Z of C and morphisms $f_A : Z \to A$, $f_b : Z \to B$, there is a unique morphism σ making the diagram

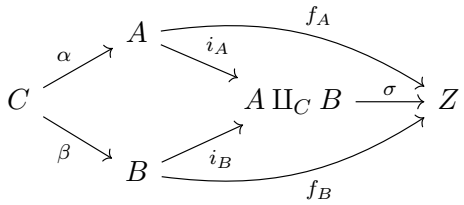


  commute.

  Consider the category Set. Let us define $A \times_C B = \{(a, b) \in A \times B \mid \alpha(a) = \beta(b)\}$ and the morphisms $\pi_A : A \times_C B \to A$ and $\pi_B : A \times_C B \to B$ as the natural projections. To prove that this is a fibered product, suppose Z is any set and $f : Z \to A$ and $g : Z \to B$ morphisms, for which it holds that $\alpha f = \beta g$. Then there is a single possibility for the morphism $\sigma : Z \to A \times_C B$ that makes the following diagram commute:

  The only possibility is $\sigma(z) = (f(z), g(z))$. This makes the diagram commute, because $\alpha(\pi_A \sigma(z)) = \alpha(\pi_A((f(z), g(z)))) = \alpha(f(z)) = \beta(g(z)) = \beta(\pi_B((f(z), g(z)))) = \beta(\pi_B \sigma(z))$. The uniqueness of the definition of σ is enforced by the required commutativity of the diagram. Thus Set is a category with fibered products.

- Suppose $\alpha : C \to A, \beta : C \to B$ are morphisms in the category C. A fibered product $A \amalg_C B$ of A and B is an object of C, endowed with morphisms $i_A : A \to A \amalg_C B$ and $i_B : B \to A \amalg_C B$ that is final in $\mathsf{C}^{\alpha,\beta}$: for any object Z of C and morphisms $f_A : A \to Z$, $f_b : B \to Z$, there is a unique morphism σ making the diagram



  commute.

  Consider the category Set. We shall define $A \amalg_C B = (A \amalg B)/\sim$ where $\sim$ is a relation on $A \amalg B$ where $a \sim b$ if and only if $\alpha i_A(a) = \beta i_B(b)$ (which is an equivalence relation as it is defined based on an equality). □

II. Groups, first encounter

1. Definition of group

1.1.

Solution. Suppose C is a (non-empty) groupoid. Let $*$ be an object of C. Let $G = \mathrm{Aut}(*)$, we will now prove that $(G, \circ)$ (where $\circ$ is the operation of composition of morphisms in C) is a group. $\circ$ is associative because C is a category. Let $e_G = 1_*$ and suppose $g \in G$ be any element of G. Then $g \circ e_G = g \circ 1_* = g = 1_* \circ g = e_G \circ g$ (again by the definition of a category). Also, since $g \in \mathrm{Aut}(*)$, it is an isomorphism and thus it has a (two-sided) inverse g^{-1}. Therefore $(G, \circ)$ is in fact a group.

Now suppose $(G, \bullet)$ is a group. Define C to be a category with a single object, $*$. We shall define for every $g \in G$ a morphism in C, $g : * \to *$. We identify the identity morphism 1_* with e_G. The composition will be equal to the operation $\bullet$, as $\bullet : G \times G \to G$ which is equal by our definition to $\bullet : \mathrm{Hom}_{\mathsf{C}}(*,*) \times \mathrm{Hom}_{\mathsf{C}}(*,*) \to \mathrm{Hom}_{\mathsf{C}}(*,*)$. The required properties of morphisms follow from the properties of a group.

Now, suppose $f \in \mathrm{Hom}_{\mathsf{C}}(*,*)$ is a morphism. Then $f \in G$ and there must exist $f^{-1} \in G$, as G is a group. But then $f^{-1} \in \mathrm{Hom}_{\mathsf{C}}(*,*)$, and by the definition of composition $ff^{-1} \equiv f \bullet f^{-1} = e_G \equiv 1_*$. Thus any morphism of C is necessarily an isomorphism and therefore C is a groupoid.

Thus any group is in fact a group of isomorphisms of a groupoid. Notice however, that there is no need for C to be a groupoid - every group is in fact a group of automorphisms of some object in some category. □

1.2.

Solution. We will consider the standard operations on numbers, $+, \cdot, -, :$. Lets go over the sets one by one:

- Consider the set $\mathbb{N}$. Now, $+$ will not work, as we could not have inverses. The only possible choice for the identity is 0, but there is no $a \in \mathbb{N}$ such that, for example, $1 + a = 0$. $\cdot$ also cannot work, as $0 \cdot 1 = 0 \cdot 2$, but $1 \neq 2$, so cancellation would not work. We cannot use $-$ either, for the same reason as $+$. $:$ also would not work, as we cannot divide by 0. There are no simple modifications we could do to make those operations work, but as we shall see, we can only consider certain subsets of $\mathbb{N}$ that make $+$ and $\cdot$ work.
- Consider $\mathbb{Z}$. $+$ will work, with identity equal to 0. The inverse to any number z will simply be $-z$. $\cdot$ won't work, again by cancellation with 0. If we considered $\mathbb{Z}$ without 0, the problem would be the inverses, as for example 2 does not have an inverse, as for any $a \in \mathbb{Z}$ we have $2 \cdot a \neq 1$ (we either get a greater number, or smaller). $-$ will work similarly to $+$ (being the inverse operation in a sense) and again $:$ won't work.

- Consider $\mathbb{Q}$. $+$ will work similarly as for $\mathbb{Z}$. $\cdot$ will only work if we take out 0 (again because of cancellation). The inverses exist as for $\frac{a}{b}$ we have $\frac{b}{a}$ such that $\frac{a}{b} \cdot \frac{b}{a} = 1$. In this case, both $-$ and $:$ work.
- Consider $\mathbb{R}$. For this set, all operations will work (taking out 0, again, for $\cdot$ and $:$). The situation is the same for $\mathbb{C}$. □

1.3.

Solution. Consider a group G, and $g, h \in G$. Now, $(gh)(h^{-1}g^{-1}) = g((hh^{-1})g^{-1}) = g(e_G g^{-1}) = gg^{-1} = e_G$. But then $h^{-1}g^{-1}$ is in fact an inverse of gh and since the inverse is unique by Proposition II.1.7, it follows that $(gh)^{-1} = h^{-1}g^{-1}$. □

1.4.

Solution. Consider a group G, and $g, h \in G$. Now, since for any $a \in G$, $a^2 = e$, it follows that $g = g^{-1}$ and $h = h^{-1}$ (by Proposition II.1.7). Consider gh. We must have $gh = (gh)^{-1} = h^{-1}g^{-1}$ (by Problem II.1.3), but then $gh = hg$, as $h^{-1} = h$ and $g^{-1} = g$. Therefore G is a commutative group. □

1.5.

Solution. Let $(G, \bullet)$ be a group. Consider its multiplication table. Suppose a row, for example the one for some $a \in G$, contains another $b \in G$ twice. But that would mean that there are $c, d \in G$ with $c \neq d$ such that $a \bullet c = b = a \bullet d$, but then by cancellation $c = d$, a contradiction. Similarly for columns. □

1.6.

Solution. The only group with a single element contains just the identity, and thus necessarily $e \cdot e = e$, therefore there is a single multiplication table.

A group with two elements, a, b, must contain an identity, thus one row and one column of the multiplication table is given. If a is the identity, the only place that is not clear is $b \cdot b$. But because it is a group, it must follow that $b \cdot b = e$, as otherwise b would not have an inverse (as $a \cdot b = b \cdot a = b \neq a$).

Again, for a group with three elements, one must be the identity. Lets mark the elements e, a, b. One row and one column of the multiplication table are again given (the one for e). Now, the only choice for $a \cdot b = e$, as if $a \cdot b = a = a \cdot e$, then by cancellation $a = e$, a contradiction. Then it must also be that $a \cdot a = b$ and $b \cdot b = a$, by Problem II.1.5.

Now, consider a group with four elements. We have to decide three rows and three columns. Now for $a \cdot b$ there are two options, e and c. $a \cdot b \neq a$ nor $a \cdot b \neq b$ as that would lead to a contradiction by the cancellation law of groups. If $a \cdot b = e$, then we also have

$b \cdot a = e$, $a \cdot c = b$ (only b and c are possible but the column contains c already) and thus $a \cdot a = c$. We then have $c \cdot c = e$, thus $b \cdot c = a$, and the other fields follow automatically from Problem II.1.5. automatically (the choice for $a \cdot b$ is in bold):

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	c	$\boldsymbol{e}$	b
b	b	e	c	a
c	c	b	a	e

In case $a \cdot b = c$, we get the following table:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	$\boldsymbol{c}$	b
b	b	c	e	a
c	c	b	a	e

In all cases, the groups are commutative, thus all groups with ≤ 4 elements are necessarily commutative. □

1.7.

Solution. Let G be a group and $g \in G$ an element of finite order, and let $N \in \mathbb{Z}$. Now, suppose $g^N = e$. Then $|g|$ divides N and thus N is a multiple of $|g|$. Now, suppose N is a multiple of $|g|$. Then $N = a\,|g|$ for some $a \in \mathbb{Z}$. But then $g^N = g^{a|g|} = (g^{|g|})^a = e^a = e$ and thus $g^N = e$. □

1.8.

Solution. Suppose G is a finite abelian group, with exactly one element f of order 2. Consider the product $\prod_{g \in G} g$. Now, since for every $g \in G$, $g \neq f, g \neq e$, we have $|g| > 2$, and thus $g \neq g^{-1}$ (otherwise $|g| = 2$ or $g = e$) the product must contain g, g^{-1}. But since G is abelian, we can reorder the product so that the we take the product of g and g^{-1}. But this results in e, so $\prod_{g \in G} g = ef = f$, exactly as we wanted to prove. □

1.9.

Solution. Let G be a group of order n, and let m be the number of elements $g \in G$ of order exactly 2. Therefore there are $n - m$ elements of $g \in G$ of order not 2. One of those elements must be e_G. Notice, that if $|g| > 2$, $g \neq g^{-1}$. Thus for every element g there must also be its inverse g^{-1} and thus $n - m - 1$ must be even. And therefore $n - m$ is odd.

It then follows that if n is even, there must be elements of G with order 2. □

1.10.

Solution. Suppose G is a group and $g \in G$ is an element with odd order. Consider the element g^2. By Proposition II.1.13. we then have $\left|g^2\right| = \frac{|g|}{\gcd(2,|g|)}$. Now since $|g|$ is odd, necessarily we have $\gcd(2, |g|) = 1$. Thus $\left|g^2\right| = |g|$. □

1.11.

Solution. Let G be a group, $a, g \in G$ its elements. Let $|g| = N$. Then $(aga^{-1})^N = ag^N a^{-1} = aea^{-1} = aa^{-1} = e$. Therefore $\left|aga^{-1}\right|$ must divide N. Suppose $\left|aga^{-1}\right| = n \leq N$. Then $(aga^{-1})^n = ag^n a^{-1} = e$, but then $ag^n = a$, so $g^n = e$, a contradiction, as $n \leq N$, but N is the smallest number such that $g^N = e$. Thus $\left|aga^{-1}\right| = |g|$.

Now, suppose $h \in G$. By the fact we just proved, $|gh| = \left|hghh^{-1}\right| = |hge| = |hg|$. □

1.12.

Solution. We have $g^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $g^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $g^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore $|g| = 4$.

Now, we have $h^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$, $h^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore $|h| = 3$.

But $gh = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $(gh)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $(gh)^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$, and so on, so for $n \geq 1$, $(gh)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ and thus never equals the identity matrix, and $|gh| = \infty$. □

1.13.

Solution. An easy example is the group of 4 elements with two elements of order 4 and one of order 2 from Exercise II.1.6., which we know is commutative. From the multiplication table we can see $|a| = |b| = 4$. But $ab = e$, and therefore $|ab| = 1 \neq \text{lcm}(4, 4)$. □

1.14.

Solution. Let G be a group and $g, h \in G$ elements that commute, so that $gh = hg$. Suppose that $\gcd(|g|, |h|) = 1$. Let $|gh| = N$. Note that by Proposition II.1.14 we have that N divides $\operatorname{lcm}(|g|, |h|) = \frac{|g||h|}{\gcd(|g||h|} = |g|\,|h|$.

Now, $(gh)^N = g^N h^N = e_G$ (because g and h commute!). But then $e_G = e_G^{|h|} = (gh)^{N|h|} = g^{N|h|}h^{N|h|} = g^{N|h|}$. But then by Proposition II.1.11 it follows that $|g|$ divides $N\,|h|$. But since $\gcd(|g|, |h|) = 1$, it follows that $|g|$ divides N. Similarly we get that $|h|$ divides N. But again by $\gcd(|g|\,|h|) = 1$, it follows that $|g|\,|h|$ divides N.

But then $N = |gh| = |g|\,|h|$. □

1.15.

Solution. Let G be a commutative group and let $g \in G$ be an element of maximal finite order, that is for any $h \in G$, if h has finite order, then $|h| \leq |g|$. Now, let h be an element of finite order. Suppose that $|h|$ does not divide $|g|$. Then there is a prime number p such that $|g| = p^m r$ and $|h| = p^n s$ for some integers m, n, r, s such that r and s are relatively prime to p and $m < n$ (as if such a prime would not exist, i.e. if $n \leq m$ for all primes in the factorizations of g and h, then h would divide g).

Now, $\left|g^{p^m}\right| = \frac{|g|}{\gcd(|g|, p^m)} = \frac{|g|}{p^m} = r$. $|h^s| = \frac{|h|}{s} = p^n$. Clearly $\gcd(\left|g^{p^m}\right|, |h^s|) = 1$ and thus $\left|g^{p^m}h^s\right| = \left|g^{p^m}\right|\,|h^s| = p^n r$ (by Exercise II.I.14.). But $p^n r > p^m r = |g|$ (as $n > m$), a contradiction to the assumption that g is an element of maximal finite order. □

2. Examples of groups

2.1.

Proof. Let S_n be the group of permutations of the set $\{1, 2, \ldots, n\}$ and let $\sigma, \tau \in S_n$. Associate the $n \times n$ matrices M_σ, M_τ to those permutations as in the text, i.e. for M_σ the entry at $(i, (i)\sigma) = 1$ for all $i \in \{1, 2, \ldots, n\}$ and all other entries will be 0. Consider the matrix $M_\sigma M_\tau$. The entry at (i, j) must be equal to $(i, 1)(1, j) + (i, 2)(2, j) + \cdots + (i, n)(n, j)$ by the definition of matrix multiplication. Now, by the definition of M_σ and M_τ, for the entry to equal 1, there must be a k such that $(i, k) = (k, j) = 1$, but that can only happen, again by the definition, if $k = (i)\sigma$ and $j = (k)\tau = ((i)\sigma)\tau = (i)\sigma\tau$ (because S_n is a group). Therefore, by the definition of $M_{\sigma\tau}$, $M_{\sigma\tau} = M_\sigma M_\tau$. □

2.2.

Proof. Suppose S_n is the group of permutations of the set $\{1, 2, \ldots, n\}$. Let d be a positive integer such that $d \leq n$. Consider the permutation

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

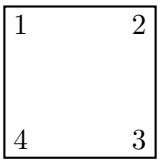
. Clearly, $\sigma^d = e$ and for any $m \leq d$ we have $\sigma^m \neq e$, as $(1)\sigma^m = (d)\sigma^{m-1} = (d-1)\sigma^{m-2} = \cdots = d-(m-1)$. Therefore σ has order d. □

2.3.

Proof. We use the same construction of permutations as we used in Problem II.2.2. □

2.4.

Proof. Label a square as follows:



Now, there are four rotations of this square about its center, resulting in the permutations (falling to the shorter notation) $(1\ 2\ 3\ 4), (2\ 3\ 4\ 1), (3\ 4\ 1\ 2), (4\ 1\ 2\ 3)$. There are two reflections about a line passing through the center and one of the vertices (as if the line passes through one vertex, it also passes by the one directly across the center), those result in the permutations $(1\ 4\ 3\ 2)$ and $(3\ 2\ 1\ 4)$. There are also the two reflections about a line passing through the center and a middle of one of the sides, there we get $(2\ 1\ 4\ 3)$ and $(4\ 3\ 2\ 1)$. But that is all the 8 symmetries of this square, thus we have a homomorphism $D_8 \to S_4$. □

2.5.

Solution. Let D_{2n} be a dihedral group, i.e. the group of symmetries of a regular polygon with n vertices. Let x be a reflection about the center of the polygon and any vertex. Clearly, it must hold that $x^2 = e$, as reflecting about the same line twice returns all the vertices to their original places. Let y be a counterclockwise rotation by $2\pi/n$. Rotating the polygon n times gives us back the original polygon, and thus $y^n = e$. Now, notice that composing those two symmetries like $xyxy$ gives us back the original polygon, thus $(xy)^2 = e$. Manipulating this equation we get $yx = xy^{-1} = xy^{n-1}$ (as $y^{-1} = y^{n-1}$).

Using these relation we can simplify any product in D_{2n}. Suppose $x^{i_1}y^{j_1}x^{i_2}y^{j_2}\ldots$ is such a product and without loss of generality suppose $i_k < 2$ and $j_k < n$ for $k \in \mathbb{N}$ (due to the $x^2 = e$ and $y^n = e$ relations). Now, we can use the relation $yx = xy^{n-1}$ to move all the x in the product to the right. Thus we can in fact simplify any product in D_{2n} to x^iy^j for $0 \leq i < 2, 0 \leq j < n$. □

2.6.

Solution. For the case $n = 1$, we can easily take $g = h$, since $|g| = 2$, we have $gg = e$ and thus $|gh| = 1$ as needed.

Now suppose $n > 1$. Now consider the group D_{2n}. By Problem II.2.5. there are elements $x, y \in D_{2n}$ such that $|x| = 2$, $|y| = n$ and $|xy| = 2$. Let us define $g = xy$ and $h = x$ (so that $|(|\, g) = |(|\, h) = 2$). We have $gh = xyx = y^{-1}$ and thus $|gh| = \left|y^{-1}\right| = |y| = n$. □

2.7.

Solution. By Problem II.2.6. any element of D_{2n} can be written as a product xy^i or y^i, $0 \leq i < n$. Now, consider the elements of the form y^i, $0 < i < n$. For y^i to commute with x, we need to have $xy^i = y^i x$ by definition. But $xy^i = xyy^{i-1} = y^{-i}x$ (as $|xy| = 2$). But that means $y^i = y^{-i} = (y^i)^{-1}$ and thus $\left|y^i\right| = 2$. But by Proposition I.1.13. we know that $\left|y^i\right| = \frac{|y|}{\gcd(i,|y|} = \frac{n}{\gcd(i,n)} = 2$. So in particular $\gcd(i, n) = \frac{n}{2}$. Since $i < n$, it follows that $i = \frac{n}{2}$.

Now consider elements of the form xy^i. If such an element commutes with everything, it has to commute with x in particular. We have $xxy^i = y^i$ and $xy^i x = x^2 y^{-i} = y^{-i}$. Now this can only happen for $i = \frac{n}{2}$. Now, it must also commute with y. We have $yxy^i = xy^{i-1}$ and $xy^i y = xy^{i+1}$. Now, $xy^{i-1} = xy^{i+1}$ would mean $y^{i-1} = y^{i+1}$, which in turn would mean $y^2 = e$. But that only happens if $n = 2$.

Therefore we have found that there are no elements that commute with everything for groups D_{2n} where n is odd. In the case $n = 2$, y and xy commute with everything. In the case $n > 2$, the only such element is $y^{\frac{n}{2}}$, which of course only exists if n is even. □

2.8.

Solution. [not interested] □

2.9.

Solution. Let $n \in \mathbb{N}$ and $\equiv$ be the 'congruence modulo n' relation. Now, let $a, b, c \in \mathbb{Z}$ be numbers. We will prove that $\equiv$ is an equivalence relation:

- We have $a - a = 0$ and trivially $n|0$, thus $a \equiv a$.
- Suppose $a \equiv b$. Then $n|(b - a)$ by definition. But then there is $k \in \mathbb{Z}$ such that $(b - a) = kn$. But then $-(b - a) = (a - b) = -kn$, and that means $n|(a - b)$. Therefore $b \equiv a$.
- Suppose $a \equiv b$ and $b \equiv c$. Then we have $n|(b - a)$ and $n|(c - b)$. But then there are $k, l \in \mathbb{Z}$ such that $(b-a) = kn$ and $(c-b) = ln$. Summing those two equations we obtain $(b - a) + (c - b) = (c - a) = kn + ln = (k + l)n$ and thus $a \equiv c$.

□

2.10.

Solution. Let $\mathbb{Z}/n\mathbb{Z}$ be a cyclic group. The group is the set of equivalence classes of congruence modulo n on $\mathbb{Z}$. Clearly, the n elements $[0]_n, [1]_n, \ldots, [n-1]_n$ are all distinct, as if we had $[i]_n = [j]_n$, $0 \leq i < j < n$ (clearly it does not matter if $i < j$ or $j < i$), then $i \equiv j$ so $n|(j-i)$ and thus $j - i = kn$ for some $k \in \mathbb{Z}$. But that is a contradiction, as $i < j < n$ so $j - i < n$ and $i \neq j$ so $j - i \neq 0$.

Now, let $m \in \mathbb{Z}$ be a number such that $m < 0$ or $n \leq m$. Then we can divide m by n such that we get $n = km + i$ for some $k \in \mathbb{Z}$ and $0 \leq i < n$. But that means $n|(m-i)$ and thus $m \equiv i$ and therefore $[m]_n = [i]_n$.

Thus, there are precisely n elements of $\mathbb{Z}/n\mathbb{Z}$ given above. □

2.11.

Solution. Let $n \in \mathbb{Z}$ be an odd integer. Then we can write $n = 2k + 1$ for some $k \in \mathbb{Z}$ by the definition of an odd integer. Then we have $n^2 = (2k+1)^2 = 4k^2 + 4k + 1$. Now, there are two possibilities, either k is even, or k is odd.

Suppose k is even, then $k = 2l$ for some $l \in \mathbb{Z}$. But then $n^2 = 16l^2 + 8l + 1$, which means $8|n^2 - 1$, so that $n \equiv 1 \mod 8$.

Now suppose k is odd, then $k = 2l+1$ for some $l \in \mathbb{Z}$. Then $n^2 = 16l^2+16l+4+8l+4+1 = 16l^2 + 24l + 9$ so that again $8|n^2 - 1$ and thus $n \equiv 1 \mod 8$. □

2.12.

Solution. If there are some nonzero integers $a, b, c \in \mathbb{Z}$ such that $a^2 + b^2 = 3c^2$, then the equation $[a]_4^2 + [b]_4^2 = 3[c]_4^2$ in $\mathbb{Z}/4\mathbb{Z}$ would also have to hold. Now, notice that for any $n \in \mathbb{Z}$, $[n]_4^2$ can either equal 0 (if n is even) or 1 (n odd). Therefore for the equation to hold in $\mathbb{Z}/4\mathbb{Z}$, a, b, c all have to be even. Let $a = 2k, b = 2l, c = 2m$ for some $k, l, m \in \mathbb{Z}$. Then we have $k^2 + l^2 = 3m^2$. But again, k, l, m have to be even. We can continue this process until we reach 1 for some of the factors, proving that indeed $a^2 + b^2 = 3c^2$ does not have a non trivial solution in $\mathbb{Z}$. □

2.13.

Solution. Suppose that $m, n \in \mathbb{Z}$ are numbers such that $\gcd(m, n) = 1$. Then by Corollary II.2.5. we see that $[m]_n$ is a generator of $\mathbb{Z}/n\mathbb{Z}$. But there is some $a \in \mathbb{Z}$ such that $a[m]_n = [am]_n = [1]_n$. But that means $am \equiv 1 \mod n$, so $n|(am - 1)$, and therefore $(am - 1) = cn$. But that shows exactly what we required, there are $a, b \in \mathbb{Z}$ such that $am - cn = am + bn = 1$.

Conversely, suppose there are integers a, b such that $am + bn = 1$. But then $[am + bn]_n = [am]_n = [1]_n$. But then if $[x]_n \in \mathbb{Z}/n\mathbb{Z}$ is any element of the group, we have $[x]_n = x[1]_n = x[am]_n = xa[m]_n$. But that means $[m]_n$ generates the group, and thus by Corollary II.2.5. $\gcd(m, n) = 1$ must hold. □

2.14.

Solution. Suppose $a \equiv a' \mod n$ and $b \equiv b' \mod n$. Then we have $n|(a'-a)$ and thus $a'-a = kn$, similarly we have $b'-b = ln$, for some $k, l \in \mathbb{Z}$. Now, $a'b'-ab = a'b'-(a'-kn)(b'-ln) = a'b'-(a'b'-a'ln-b'kn+lkn^2) = (-a'l-b'k+lkn)n$. But then $n|(a'b'-ab)$, so $[ab]_n = [a'b']_n$. But that means that multiplication of equivalence classes is well-defined. □

2.15.

Solution. Let $n > 0$ be an odd integer.

- Let m be an integer and $\gcd(m,n) = 1$. By Exercise II.2.13. there are integers a, b such that $am + bn = 1$. We then have $4am + 4bn = 4am + 2n + 4bn - 2n = 2a(2m+n)+(2b-a)2n = 4$. That means $\gcd(2m+n, 2n)|4$, as the gcd must divide the whole equation. But $2m+n$ is odd, since n is odd. Thus $\gcd(2m+n, 2n) = 1$.
- Now, let r be an integer and suppose $\gcd(r, 2n) = 1$. Then we have, again by Exercise II.2.13., $ar + b2n = 1$ for some integers a, b. But then we have $ar - an + b2n + an = a(r-n) + (2b+a)n = 2a\frac{r-n}{2} = (2b-a)n = 1$. Using the result of Exercise II.2.13. again we get $\gcd(\frac{r-n}{2}, n) = 1$.
- Consider the function $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/2n\mathbb{Z})^*$ defined as $f([m]_n) = [2m+n]_{2n}$. Now, this function is well defined, as if $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^*$ we have $\gcd(m,n) = 1$ so $\gcd(2m+n, 2n) = 1$ and thus $[2m+n]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$. Now, define a function $g : (\mathbb{Z}/2n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ as $g([r]_{2n}) = [\frac{r-n}{2}]_n$. This function is again well defined. Now, $gf([m]_n) = g([2m+n]_{2n}) = [\frac{2m}{2}]_n = [m]_n$ and thus g is a left-inverse of f. $fg([r]_{2n}) = f([\frac{r-n}{2}]_n) = [2\frac{r-n}{2} + n]_{2n} = [r-n+n]_{2n} = [r]_{2n}$ and thus g is also a right-inverse of f. Therefore f is a bijective function. But that means $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$ are isomorphic. □

2.16.

Solution. To find the last digit of $1238237^{18238456}$ we will work in $\mathbb{Z}/10\mathbb{Z}$. We have $[1238237]_{10} = [7]_{10}$. Now $[7^2]_{10} = [9]_{10}$, $[7^3]_{10} = [3]_{10}$, $[7^4]_{10} = [1]_{10}$. But $[18238456]_4 = 0$, and thus the last digit is 1. □

2.17.

Solution. Suppose $m \equiv m' \mod n$. Then $n|(m'-m)$ so $m'-m = kn$ for some integer k. Now, suppose that $\gcd(m,n) = 1$. Then by Exercise II.2.13. there are integers a, b such that $am + bn = 1$. But $m = m' - kn$, so we have $a(m'-kn) + bn = am' - akn + bn = am' + (b-ak)n = 1$, and thus $\gcd(m', n) = 1$.

If $\gcd(m', n) = 1$, then again there are integers a, b such that $am' + bn = 1$. But $m' = kn - m$, so $am' + bn = a(kn-m) + bn = akn - am + bn = (-a)m + (ak+b)n = 1$ and thus $\gcd(m,n) = 1$. □

2.18.

Solution. Define the function as follows. For $[m]_d$ we move every element up to d m places to the right, wrapping around. This way, $[0]_d$ is the identity permutation, $[1]_d$ is the permutation $(d\ 1\ 2\ \dots\ d-2\ d-1\ d+1\ \dots n)$. Composing this morphism gets us the permutation $(d-1\ d\ 1\dots)$ etc. So indeed, those morphisms preserve the structure. □

2.19.

Solution. Multiplication table for $(\mathbb{Z}/5\mathbb{Z})^*$:

$\cdot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

Multiplication table for $(\mathbb{Z}/12\mathbb{Z})^*$:

$\cdot$	[1]	[5]	[7]	[11]
[1]	[1]	[5]	[7]	[11]
[5]	[5]	[1]	[11]	[7]
[7]	[7]	[11]	[1]	[5]
[11]	[11]	[7]	[5]	[1]

Now note that we can clearly see $(\mathbb{Z}/12\mathbb{Z})^*$ has 3 elements of order 2, but $(\mathbb{Z}/5\mathbb{Z})^*$ has two elements of order 4 and a single element of order 2. Therefore we cannot relabel the elements in a way the two groups would correspond. □

3. The category Grp

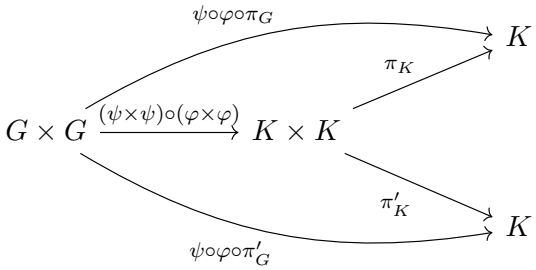
3.1.

Solution. Let C be a category with products and $\varphi : G \to H$ a morphism in C. Now, if we have products $G \times G$ and $H \times H$ with the morphisms $\pi_G, \pi'_G : G \times G \to G$ and $\pi_H, \pi'_H : H \times H \to H$, we can use the universal property of products as follows: Since $H \times H$ with π_H, π'_H satisfies the universal property, for any object X, such that there are morphisms $f_H, f'_H : X \to H$, there is a unique morphism $X \to H \times H$. Now notice that for $G \times G$ we have two morphisms $\varphi \circ \pi_G : G \times G \to H$ and $\varphi \circ \pi'_G : G \times G \to H$. Therefore

due to the unique property of products there is a unique morphism $\varphi\times\varphi : G\times G \to H\times H$ such that $\pi_H \circ (\varphi \times \varphi) = \varphi \circ \pi_G$ and $\pi'_H \circ (\varphi \times \varphi) = \varphi \circ \pi'_G$. □

3.2.

Solution. Let C be a category with products and $\varphi : G \to H$ and $\psi : H \to K$ morphisms in C. By Exercise II.3.1. there are then morphisms $(\varphi \times \varphi) : G \times G \to H \times H$ and $(\psi \times \psi) : H \times H \to K \times K$ and also $(\psi \circ \varphi) \times (\psi \circ \varphi) : G \times G \to K \times K$ (since $\psi \circ \varphi : G \to K$) compatible with the natural projections. Now we will prove the diagram



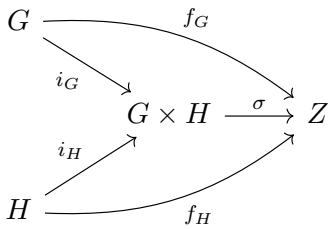
commutes. Note that by Exercise II.3.1. we have $\pi_K \circ (\psi \times \psi) = \psi \circ \pi_H$ and $\pi_H \circ (\varphi \times \varphi) = \varphi \circ \pi_G$. Thus we have

$$\begin{aligned}\pi_K \circ (\psi \times \psi) \circ (\varphi \times \varphi) &= \psi \circ \pi_H \circ (\varphi \times \varphi) \\ &= \psi \circ \varphi \circ \pi_G\end{aligned}$$

and similarly for the other side. But we know $(\psi \circ \varphi) \times (\psi \circ \varphi)$ is the unique morphism making the diagram commute (by Exercise II.3.1.) and therefore $(\psi \circ \varphi) \times (\psi \circ \varphi) = (\psi \times \psi) \circ (\varphi \times \varphi)$. □

3.3.

Solution. Suppose G and H are abelian groups. Consider the product of those groups, $G \times H$, with the two natural homomorphisms $i_G : G \to G \times H$ $(g \mapsto (g, e_H))$ and $i_H : H \to G \times H$ $(h \mapsto (e_G, h))$. For this construction to satisfy the universal property of coproducts in Ab, for any abelian group Z such that there are homomorphisms $f_G : G \to Z$ and $f_H : H \to Z$, there must be a unique homomorphism $\sigma : G \times H \to Z$ making



commute. Now, the only choice for σ is given by the set-function $\sigma((a,b)) = f_G(a)f_H(b)$. We have to check that σ is a group homomorphism. We have

$$\begin{aligned}\sigma((a,b)(c,d)) &= \sigma((ac,bd)) \\ &= f_G(ac)f_H(bd) \\ &= f_G(a)f_G(c)f_H(b)f_H(d) \\ &= f_G(a)f_H(b)f_G(c)f_H(d) \\ &= \sigma((a,b))\sigma((c,d))\end{aligned}$$

precisely because Z is commutative. Therefore, $G \times H$ satisfies the universal propery of coproducts in C. □

3.4.

Solution. H does not necessarily have to be the trivial group. We can consider a countably infinite product $G = H \times H \dots$. Then indeed $G \cong G \times H$. □

3.5.

Solution. Let $\mathbb{Q} = G \times H$. If both G, H are trivial, then $\mathbb{Q}$ would be trivial, and thus, without loss of generality, say that G is non-trivial. Now, consider the canonical projection π_G.

We will show that π_G is in fact an injective homomorphism. First of all, notice that for $m \neq 0$ and any $g \in G$ such that $g^m = e_G$ we have $(g, e_H)^m = (g^m, e_H) = (e_G, e_H)$. But $\mathbb{Q}$ has no non-zero elements of finite order, and thus $g = e_G$.

Now suppose that π_G is not an injective homomorphism and thus there are two rational numbers $\frac{a_1}{b_1}, \frac{a_2}{b_2}$, such that $a_1, a_2, b_1, b_2 \neq 0 \in \mathbb{Z}$ and $\frac{a_1}{b_1} \neq \frac{a_2}{b_2}$, for which $\pi_G(\frac{a_1}{b_1}) = \pi_G(\frac{a_2}{b_2})$. Then we have $\pi_G(\frac{a_1}{b_1})^{b_1 b_2} = \pi_G(a_1)^{b_2} = \pi_G(1)^{a_1 b_2}$ and similarly $\pi_G(\frac{a_2}{b_2}) = \pi_G(1)^{a_2 b_1}$ (because π_G is a group homomorphism). Then we must have $\pi_G(1)^{a_1 b_2} = \pi_G(1)^{a_2 b_1}$ and thus $\pi_G(1)^{a_1 b_2 - a_2 b_1} = e_G$. But that means $\pi_G(1) = e_G$ (by the last paragraph) and thus π_G maps every integer to e_G.

Now suppose $\frac{a}{b}$ is a rational number, $a, b \neq 0 \in \mathbb{Z}$. Now $\pi_G(\frac{a}{b})^b = \pi_G(a) = e_G$. But by the same argument of order we thus have $\pi_G(\frac{a}{b}) = e_G$. That means π_G maps everything to e_G. Since π_G is necessarily a surjective homomorphism, G is trivial, a contradiction. Therefore π_G must be an injective homomorphism. But since $\pi_G((e_G, h)) = e_G$ for all $h \in H$ by definition, H must necessarily be trivial. □

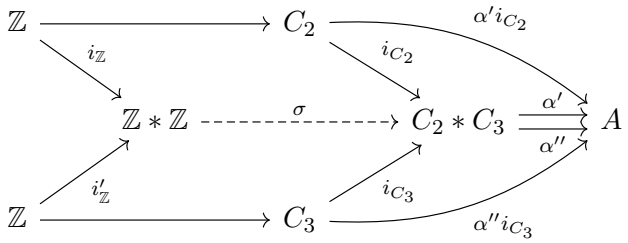
3.6.

Solution. Going point by point:

- Let $f : C_2 \to S_3$ be defined as $f(e) = (1\ 2\ 3)$ and $f(x) = (2\ 1\ 3)$. Then $f(x^n) = e$ if $2|n$ or $f(x^n) = (2\ 1\ 3)$ otherwise. Thus this is an injective homomorphism. Now, let $g : C_3 \to S_3$ be defined as $g(e) = (1\ 2\ 3)$, $g(x) = (2\ 3\ 1)$ and $g(x^2) = (3\ 1\ 2)$. Now, $g(x)g(x) = (3\ 1\ 2) = g(x^2)$, and $g(x)g(x^2) = (1\ 2\ 3)$, so it is indeed an injective homomorphism.
- Suppose $C_2 \times C_3$ is the coproduct of C_2 and C_3 in Grp. By the universal property of coproducts, as there are morphisms $C_2 \to S_3$ and $C_3 \to S_3$, this means there is a unique homomorphism $\sigma : C_2 \times C_3 \to S_3$, such that $\sigma i_{C_2} = f$ and $\sigma i_{C_3} = g$.
- Now, notice that i_{C_2} must necessarily map an element $x \in C_2$ to (x, e_{C_3}), and similarly for i_{C_3}. But then we have $f(x_1)g(x_2) = \sigma((x_1, e_{C_3})(e_{C_2}, x_2)) = \sigma((x_1, x_2)) = \sigma((e_{C_2}, x_2)(x_1, e_{C_3}) = g(x_2)f(x_1)$. But we have, for example, $(2\ 1\ 3)(2\ 3\ 1) = (3\ 2\ 1)$ and $(2\ 3\ 1)(2\ 1\ 3) = (1\ 3\ 2)$. Thus σ cannot exist (precisely because S_3 is not commutative). □

3.7.

Solution. Let $\mathbb{Z} * \mathbb{Z}$, $C_2 * C_3$ be a coproduct in Grp. Let A be a group and $\alpha' : C_2 * C_3 \to$ and $\alpha'' : C_2 * C_3 \to A$ any two homomorphisms. Consider the diagram



Now, by the universal property of coproducts, σ is a unique homomorphism making the diagram commute. Notice, that by the universal property of coproducts we can also see α' is the unique homomorphism making the right half of the diagram commute. But that means $\alpha' = \alpha''$ and thus σ is an epimorphism. But that means it is a surjective set-function and thus a surjective homomorphism. □

3.8.

Solution. Define a group G as the group generated by two elements x, y such that $x^2 = e_G$ and $y^3 = e_G$. Then we can define group homomorphisms $i_{C_2} : C_2 \to G$ and $i_{C_3} : C_3 \to G$ as follows: $i_{C_2}(e_{C_2}) = e_G$, $i_{C_2}(c_2) = x$, $i_{C_3}(e_{C_3}) = e_G$, $i_{C_3}(c_3) = y$, $i_{C_3}(c_3^2) = y^2$.

Suppose Z is any group, and $f : C_2 \to Z$ and $g : C_3 \to Z$ group homomorphisms. To prove that G satisfies the universal property of coproducts in Grp we have to construct a group homomorphism $\sigma : G \to Z$, such that $\sigma i_{C_2} = f$ and $\sigma i_{C_3} = g$. Now notice

that we must have $\sigma i_{C_2}(c_2) = \sigma(x) = f(c_2)$ and $\sigma i_{C_3} = \sigma(y) = g(c_3)$. Since x and y generate every element of G, this is enough for us to construct σ. If $x^{i_0}y^{j_0}x^{i_1}y^{j_1}\dots$ where $0 \leq i_0, i_1, \cdots < 2$ and $0 \leq j_0, j_1 \cdots < 3$ is an element of G, we define $\sigma(x^{i_0}y^{j_0}x^{i_1}y^{j_1}\dots) = f(c_2)^{i_0}g(c_3)^{j_0}\dots$.

It is clear that σ is a homomorphism that makes the relevant diagram commute. □

3.9.

Solution. The definition of the fiber product is pretty straightforward, and follows straight from the definition for Set. We only have to check that the definition indeed results in a group and satisfies the required universal property. Let A, B, C be groups and $\alpha : A \to C$, $\beta : B \to C$ group homomorphisms. Define $A \times_C B = \{\, (a, b) \in A \times B \mid \alpha(a) = \beta(b) \,\}$.

To check that this construction is a group, we will take the operation to be the same as the one on $A \times B$, i.e. $(a, b)(c, d) = (ac, bd)$. This operation is well-defined, as we have $\alpha(a) = \beta(b)$ and $\alpha(c) = \beta(d)$, and since α, β are group homomorphisms, $\alpha ab = \alpha(a)\alpha b = \beta c \beta d = \beta cd$. Now, we have to prove that (e_A, e_B) is an element of the group. But we have $\alpha(e_A) = e_C = \beta(e_B)$, again because they are homomorphisms. Now, suppose $(a, b) \in A \times_C B$. Then $\alpha(a) = \beta(b)$, so $(\alpha(a))^{-1} = (\beta(b))^{-1}$) and again because they are homomorphisms, $\alpha(a^{-1}) = \beta(b^{-1})$. Therefore $(a^{-1}, b^{-1}) \in A \times_C B$, but that is an inverse of (a, b). Thus $A \times_C B$ is a group.

Now, we have to prove that this construction satisfies the universal property of a fiber product. Suppose Z is a group and f, g the respective homomorphisms, such that $\alpha f = \beta g$. To ensure the commutativity of the respective diagram, we have to define $\sigma : Z \to A \times_C B$ as follows: $\sigma(z) = (f(z), g(z))$. It is well defined, as we have $(\alpha f)(z) = (\beta g)(z)$, so $\alpha(f(z)) = \beta(g(z))$. To see that this is a group homomorphism, note that $\sigma(z_1 z_2) = (f(z_1 z_2), g(z_1 z_2)) = (f(z_1)f(z_2), g(z_1)g(z_2)) = (f(z_1), g(z_1))(f(z_2), g(z_2)) = \sigma(z_1)\sigma(z_2)$.

The commutativity of the diagram follows from the definition easily, note that we have $(\pi_A \sigma)(z) = \pi_A(\sigma(z)) = \pi_A((f(z), g(z))) = f(z)$ so $\alpha \pi_A \sigma = \alpha f$ and similarly for the other side of the diagram.

To define the fibered coproduct in Ab we require knowledge of quotients, which have yet to be introduced. □

4. Group homomorphisms

4.1.

Solution. Suppose $m|n$ and $a \equiv a' \mod n$. Then $n|(a' - a)$. But then $m|(a' - a)$, and thus $[a]_m = [a']_m$.

To check it makes the diagram commute, notice that for any $z \in \mathbb{Z}$ we have $(\pi^n_m \pi_n)(z) = \pi^n_m([z]_n) = [z]_m = \pi_m(z)$ by the definition of the function.

To verify it is indeed a group homomorphism, let a, b be elements of $\mathbb{Z}_n$. Then we have $\pi_m^n(a+b) = [a+b]_m = [a]_m + [b]_m = \pi_m^n(a) + \pi_m^n(b)$.

Thus π_m^n is a well-defined group homomorphism that makes the diagram commute. The hypothesis $m|n$ is necessary as the order of all elements of $\mathbb{Z}_n$ divides n and the order of all elements of $\mathbb{Z}_m$ divides m, and it also must hold that $|\pi_m^n(z)| \mid |z| \mid n$. Now if $m \nmid n$, then $\pi_m^n([1]_n) = [1]_m$ but $|\pi_m^n([1]_n)| = m \nmid n$, a contradiction. □

4.2.

Solution. The homomorphism is defined pretty explicitly so we can easily check that the image of the homomorphism is the set $\{ (0,0), (1,1) \}$, which is in fact not isomorphic to the set underlying $C_2 \times C_2$. We can actually show that there is no such isomorphism.

In fact, there is no isomorphism of the two groups. The generator of C_4 has order 4, but there is no such element in $C_2 \times C_2$ (all non-zero elements have order 2). □

4.3.

Solution. Suppose G is a group of order n isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Let $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ be a group isomorphism. There is an element of order n in $\mathbb{Z}/n\mathbb{Z}$, namely $[1]_n$. By Proposition II.4.8. $|\varphi([1]_n)| = |[1]_n| = n$, thus G contains an element of order n.

Suppose the converse holds, i.e. G is a group of order n which contains an element x of order n. Because x has order n, the elements $x^0, x^1, \ldots, x^{n-1}$ must make up all of G (if some of those elements were equal, it would be a contradiction to the order of x by cancellation). We can define a homomorphism $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ as $\varphi([i]_n) = x^i$.

This is a homomorphism as $\varphi([i]_n + [j]_n) = \varphi([i+j]_n) = x^{i+j} = x^i x^j = \varphi([i]_n)\varphi([j]_n)$.

Now define $\rho : G \to \mathbb{Z}/n\mathbb{Z}$ as $\rho(x^i) = [i]_n$. It is easy to see that this is an inverse of φ and thus φ is an isomorphism of groups. □

4.4.

Solution. We will consider the groups one by one:

Consider $(\mathbb{Z}, +)$. Notice that any element $z \in \mathbb{Z}$ is equal to $z \cdot 1$. Therefore any homomorphism $\varphi : (\mathbb{Z}, +) \to G$ (where G is any group) is uniquely determined by $\varphi(1)$. Let $G = \mathbb{Q}$ (or $\mathbb{R}$) and suppose $\varphi(1) = \frac{a}{b}$ for some $a, b \neq 0 \in \mathbb{Z}$. Then $\varphi(z) = z\varphi(1) = z\frac{a}{b} = \frac{z \cdot a}{b}$. But that clearly means there is no number z such that $\varphi(z) = \frac{a}{b+1}$. Thus φ is not surjective and therefore it cannot be an isomorphism.

- Now consider $(\mathbb{Q}, +)$. Let $x, y \in \mathbb{Q}$, clearly, we can always find non-zero integers a, b such that $ax = by$. However, this is not true in $\mathbb{R}$, if for example $x = \sqrt{2}$ and $y = 1$. Thus the two groups cannot be isomorphic.

- $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are in fact isomorphic. However the construction of the isomorphism is fairly involved. □

4.5.

Solution. Notice that i has order 4 in $(\mathbb{C} \setminus 0, \cdot)$. However, there is no element of $(\mathbb{R} \setminus 0, \cdot)$ of order 4. Since isomorphism preserves order of elements, it follows that the two groups are not isomorphic. □

4.6.

Solution. The two groups are not isomorphic. Suppose there is an isomorphism $\varphi : (\mathbb{Q}, +) \to (\mathbb{Q}^{>0}, \cdot)$. Let y be a number such that $\varphi(y) = 2$ (there must be such a number because φ is an isomorphism). Now we can find a number $x \in \mathbb{Q}$ such that $x + x = y$ in $(\mathbb{Q}, +)$. But then $\varphi(y) = \varphi(x + x) = \varphi(x)\varphi(x) = \varphi^2(x) = 2$. But we know there is no number in $\mathbb{Q}$ with this property. □

4.7.

Solution. Let G be a group and g, h be elements G.

Consider the function $\varphi : G \to G$, $\varphi(g) = g^{-1}$. Suppose φ is a group homomorphism. Then we have $hg = (g^{-1}h^{-1})^{-1} = \varphi(g^{-1}h^{-1}) = \varphi(g^{-1})\varphi(h^{-1}) = gh$. But that means precisely that G is an abelian group. Now suppose G is abelian. Then $\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} = \varphi(h)\varphi(g) = \varphi(g)\varphi(h)$. And thus φ is a group homomorphism.

Consider the function $\psi : G \to G$, $\psi(g) = g^2$. Suppose ψ is a group homomorphism. Then $ghgh = (gh)^2 = \psi(gh) = \psi(g)\psi(h) = g^2h^2 = gghh$. By cancellation we then have $hg = gh$ and thus G is abelian. Now suppose G is abelian. Then $\psi(gh) = (gh)^2 = ghgh = gghh = g^2h^2 = \psi(g)\psi(h)$. And thus ψ is a group homomorphism. □

4.8.

Solution. Let G be a group, and let $g \in G$. Consider the function $\gamma_g : G \to G$, $\gamma_g(a) = gag^{-1}$. Let $a, b \in G$. Then $\gamma_g(ab) = g(ab)g^{-1} = gag^{-1}gbg^{-1} = \gamma_g(a)\gamma_g(b)$. Thus γ_g is a group homomorphism. Now let $\varphi_g : G \to G$ be a function defined as $\varphi_g(a) = g^{-1}ag$. Clearly this is also a group homomorphism. For $a \in G$ we have $(\gamma_g \circ \varphi_g)(a) = \gamma_g(\varphi_g(a)) = \gamma_g(g^{-1}ag) = gg^{-1}agg^{-1} = a$ and $(\varphi_g \circ \gamma_g)(a) = \varphi_g(\gamma_g(a)) = \varphi_g(gag^{-1}) = g^{-1}gag^{-1}g = a$. Thus φ_g is an inverse of γ_g and therefore γ_g is an automorphism of G.

Consider the function $\psi : G \to \mathrm{Aut}(G)$, $\psi(g) = \gamma_g$. Let $g, h \in G$. We have $\psi(gh) = \gamma_{gh}$. Now let a be any element of G. We then have $\gamma_{gh}(a) = (gh)a(gh)^{-1} = ghah^{-1}g^{-1} = g\gamma_h(a)g^{-1} = \gamma_g(\gamma_h(a)) = \gamma_g \circ \gamma_h$. Thus $\psi(gh) = \gamma_{gh} = \gamma_g \circ \gamma_h = \psi(g) \circ \psi(h)$ and therefore ψ is in fact a group homomorphism.

Now suppose ψ is trivial. Then for any $g \in G$ we have $\psi(g) = \gamma_g = id_G$. But that means for every $a \in G$ we must have $gag^{-1} = a$ and thus $ga = ag$ and therefore G must be abelian. Now suppose G is abelian. For any $a, g \in G$ we then have $\gamma_g(a) = gag^{-1} = gg^{-1}a = e_G a = a$, but that means $\gamma_g = id_G$ for every g and thus ψ is a trivial homomorphism. □

4.9.

Solution. Suppose m, n are positive integers and $\gcd(m, n) = 1$. The order of $[1]_m$ in $\mathbb{Z}/m\mathbb{Z}$ is m and the order of $[1]_n$ in $\mathbb{Z}/n\mathbb{Z}$ is n. Consider the element $([1]_m, [1]_n)$ of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Suppose the order of $([1]_m, [1]_n)$ is x, so that $x([1]_m, [1]_n) = ([0]_m, [0]_n)$, which in turn means $x[1]_m = [0]_m$ and $x[1]_n = [0]_n$. Therefore $m \mid x$ and $n \mid x$. Therefore $\operatorname{lcm}(m, n) \mid x$. But $\operatorname{lcm}(m, n) = mn$ as $\gcd(m, n) = 1$. Thus mn must be the order of $([1]_m, [1]_n)$. Now notice that the order of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is mn. Thus by Problem II.4.3. that means $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$. □

4.10.

Solution. Let $p \neq q$ be odd prime integers. By definition, $(\mathbb{Z}/pq\mathbb{Z})^* = \{[n]_{pq} \in \mathbb{Z}/pq\mathbb{Z} \mid \gcd(n, pq) = 1\}$. By Problem II.4.9., we have $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ as $\gcd(p, q) = 1$. But then we can conclude $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \cong (\mathbb{Z}/pq\mathbb{Z})^*$.

Notice, that $[p-1]_p^2 = [p^2 - 2p + 1]_p = [1]_p$ and similarly for $[q-1]_q^2 = [1]_q$. But then we have two different elements $([p-1]_p, [1]_q)$ and $([1]_p, [q-1]_q)$ in $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ of order 2. Therefore there are two elements $x \neq y \in \mathbb{Z}/pq\mathbb{Z}^*$ of order 2.

Now, the order of $(\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*$ is $(p-1)(q-1)$, and therefore even. Suppose $(\mathbb{Z}/pq\mathbb{Z})^*$ is cyclic and let g be a generator of this group. Then $|g| = (p-1)(q-1)$. Suppose g^k has order 2, where $0 < k < (p-1)(q-1)$. Then g^{2k} is the identity. Therefore, since the group is cyclic, $(p-1)(q-1) \mid 2k$, which forces $k = \frac{(p-1)(q-1)}{2}$. But that is a contradiction to the fact that $(\mathbb{Z}/pq\mathbb{Z})^*$ actually contains two different elements of order 2. □

4.11.

Solution. Let p be a prime integer. Assume that the equation $x^d = 1$ can have at most d solutions in $\mathbb{Z}/p\mathbb{Z}$.

Let $G = (\mathbb{Z}/p\mathbb{Z})^*$. G is a commutative group of finite order. Because the order of G is finite, all elements of G also have finite order. Let $g \in G$ be an element of maximal order. Clearly $|g| \leq p - 1$. By Problem II.1.15 we can see that for all $h \in G$, $|h|$ divides $|g|$. But that means $h^{|g|} = 1$ for all $h \in G$.

But that means we produced $p - 1$ solutions of the equation $x^{|g|} = 1$ in $\mathbb{Z}/p\mathbb{Z}$ and thus $p - 1 \leq |g|$ by the fact we have assumed.

Combining the two inequalities we see that $|g| = p-1$ and thus G is cyclic as it contains an element of order $p-1$. □

4.12.

Solution.

- The order of $[9]_{31}$ must divide the order of the group, 30, because it is cyclic. Trying the different divisors we get $[9]_{31}^{15} = [1]_{31}$. Thus $|[9]_{31}| = 15$ in $(\mathbb{Z}/31\mathbb{Z})^*$.
- Consider the equation $x^3 - 9 = 0$ in $\mathbb{Z}/31\mathbb{Z}$. Suppose that c is a solution of this equation, then we have $c^3 = [9]_{31}$ in $(\mathbb{Z}/31\mathbb{Z})^*$. Then we must have $\left|c^3\right| = |[9]_{31}| = 15$. But $\left|c^3\right| = \frac{\text{lcm}(3,|c|)}{3}$ by Proposition II.1.13. and thus we have $\frac{\text{lcm}(3,|c|)}{3} = 15$ so that $\text{lcm}(3,|c|) = 45$. But then $|c| = 45$ which is a contradiction to the fact c as an element of $(\mathbb{Z}/30\mathbb{Z})^*$ must have order dividing 30. Therefore the equation has no solutions. □

4.13.

Solution. Consider the group $\text{Aut}_{\mathsf{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$, the group of isomorphisms of the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. First we will analyze how the isomorphisms look. Let $1, a, b, c$ label the elements of this group. Suppose $\varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is a group isomorphism. Then in particular φ must be a group homomorphism. Therefore we always have $\varphi(1) = 1$. Clearly we have $3 \cdot 2 = 6$ possible bijections which satisfy this constraint. Now we will show that each such bijection is in fact a group homomorphism. Suppose $\varphi(a) = x, \varphi(b) = y, \varphi(a+b) = \varphi(c) = z$. Because φ is a bijection and $a \neq b \neq c$ we have $x \neq y \neq z$ and thus $x + y = z$ and therefore $\varphi(a+b) = \varphi(a) + \varphi(c)$.

But notice that the argument shows that in fact every such φ is a permutation of the three elements a, b, c. And thus $\text{Aut}_{\mathsf{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$ □

4.14.

Solution. Consider the group $\text{Aut}_{\mathsf{Grp}}(C_n)$ for some n. Now, C_n has a generator x of order n. We know that a class $[m]_n$ generates the group $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m,n) = 1$ (by Corollary II.2.5.). But every isomorphism $C_n \to C_n$ must send the generator x to one such element relatively prime to n, as isomorphisms must keep the order of elements. That means that every such isomorphism is determined by the choice of the image of x. Thus the order of $\text{Aut}_{\mathsf{Grp}}(C_n)$ is in fact the number of positive integers $r \leq n$ that are relatively prime to n as required. □

4.15.

Solution. Lets first consider the group of automorphisms of $(\mathbb{Z}, +)$. Clearly we have $z = z \cdot 1$ for every $z \in \mathbb{Z}$ and thus every homomorphism φ of $(\mathbb{Z}, +)$ is determined by $\varphi(1)$. Now for φ to be a bijection, notice that there are only two possible choices: $\varphi(1) = 1$ (the identity morphism) and $\varphi(1) = -1$. Any other choice leads to 1 being absent from the image of φ and thus φ would necessarily not be a bijection. But that means $\mathrm{Aut}_{\mathsf{Grp}}((\mathbb{Z}, +)) \cong C_2$.

Let p be a prime integer. We know C_p has a generator x such that $x^p = 1$. Every isomorphism of C_p is determined by where it maps this generator x, an element x^n such that the order of x^n is also p (so that x^n is also a generator of C_p). But notice that due to this we can look on $\mathrm{Aut}_{\mathsf{Grp}}(C_p)$ as on $(\mathbb{Z}/p\mathbb{Z})^*$. But by Problem II.4.14. we know $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$. □

4.16.

Solution. Let $p > 1$ be an integer. Suppose p is prime. Then by Problem II.4.11. we can see $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group of order $p-1$. Since the group is cyclic, there is exactly one element of order 2, $[-1]_p$. But then by Problem II.1.8. we know $\prod_{g \in (\mathbb{Z}/p\mathbb{Z})^*} g = [-1]_p$. But since p is prime, $\prod_{g \in (\mathbb{Z}/p\mathbb{Z})^*} g = [p-1]_p[p-2]_p \dots [1]_p = [(p-1)!]_p = [-1]_p$. But then $(p-1)! \equiv -1 \mod p$.

Now suppose $(p-1)! \equiv -1 \mod p$ and suppose d is a proper divisor of p. Notice that all the proper divisors of p are contained in the product $(p-1)!$ and thus d divides this number. Then in particular $(p-1)! \equiv 0 \mod d$. But since $d \mid p$, we must have $d \mid p \mid (-1 - (p-1)!)$ and thus $(p-1)! \equiv -1 \mod d$. But that forces $d = 1$ and thus p must be prime. □

4.17.

Solution. For $p = 5$, $[2]_5$ is a generator of $(\mathbb{Z}/5\mathbb{Z})^*$ as its order is 4.

For $p = 7$, $[3]_7$ is a generator of $(\mathbb{Z}/7\mathbb{Z})^*$.

For $p = 11$, $[2]_{11}$ is a generator of $(\mathbb{Z}/11\mathbb{Z})^*$.

For $p = 13$, $[2]_{13}$ is a generator of $(\mathbb{Z}/13\mathbb{Z})^*$. □

4.18.

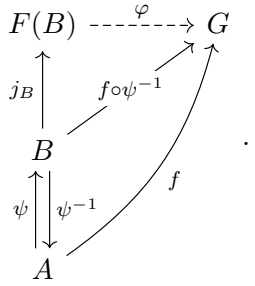
Solution. Let $\varphi : G \to H$ be an isomorphism. Assume G is commutative. Let $g, g' \in G$, $h, h' \in H$ be any elements such that $\varphi(g) = h, \varphi(g') = h'$. Then we have $hh' = \varphi(g)\varphi(g') = \varphi(gg') = \varphi(g'g) = \varphi(g')\varphi(g) = h'h$ and thus H is commutative.

Now assume H is commutative. Now since φ is an isomorphism, there is an inverse φ^{-1}. Let $g, g' \in G$, $h, h' \in H$ be any elements such that $\varphi^{-1}(h) = g, \varphi^{-1}(h') = g'$. We have $gg' = \varphi^{-1}(h)\varphi^{-1}(h') = \varphi^{-1}(hh') = \varphi^{-1}(h'h) = \varphi^{-1}(h')\varphi^{-1}(h) = g'g$ and therefore G is commutative. □

5. Free groups

I found it necessary for my understanding of free groups to prove that if A and B are isomorphic sets, then so must the free groups $F(A)$ ($F^{ab}(A)$) and $F(B)$ ($F^{ab}(B)$) be isomorphic.

Proof. Let A, B be sets such that $A \cong B$. Then there is a bijection $\psi : A \to B$. We will show that $F(B)$ together with the set-function $\psi \circ j_B$ satisfies the same universal property as $F(A)$. Let G be any group and $f : A \to G$ a set-function. Consider the diagram



By the universal property of free product $F(B)$ there is a unique homomorphism φ making the upper part of the diagram commute, so that $\varphi \circ j_B = f \circ \psi^{-1}$. But then $\varphi \circ j_b \circ \psi = f$ and thus $F(B)$ satisfies the universal property of free group on A and therefore $F(A) \cong F(B)$ as needed.

The situation for free abelian groups is entirely analogous. In particular, any finite set A is isomorphic to the set $\{1, 2, \cdots, |A|\}$ and thus $F^{ab}(A) = \mathbb{Z}^{\oplus |A|}$. □

5.1.

Solution. Indeed there is a final object in the category $\mathscr{F}^A$. The only possibility which makes sense is any trivial group $X = \{*\}$ together with the set-function $j : A \to X$ which maps everything to $*$. Let G be any group, $f : A \to G$ any set-function. Since X is in fact final in Grp there exists a unique homomorphism $\varphi : G \to X$. It is clear that this homomorphism makes the relevant diagram commute and thus (j, X) is in fact final in $\mathscr{F}^A$. □

5.2.

Solution. Let T be a trivial group, G any group. Clearly the unique homomorphism $\varphi : T \to G$ sends the only element of T to $e_G \in G$. But if $A \neq \emptyset$, there exists a set-function $f : A \to G$ such that $f(a) \neq e_G$ for some $a \in A$. Now for (e, T) to be initial in $\mathscr{F}^A$, the commutativity of the respective diagram would enforce $f = \varphi \circ e$ and in particular $f(a) = e_G$. □

5.3.

Solution. Let A be a set , $j : A \to F(A)$ the free group map and $a \neq b$ any two elements of A. Consider the group C_2 and function $f : A \to C_2$, such that $f(a) = 1$, $f(b) = x$ and $f(c) = 1$ for all $c \in A$ such that $c \neq a \neq b$. Now there exists a unique homomorphism $\varphi : F(A) \to C_2$ such that $\varphi \circ j = f$. But that implies $j(a) \neq j(b)$ as otherwise we would have $1 = f(a) = \varphi(j(a)) = \varphi(j(b)) = f(b) = x$. □

5.4.

Solution. We want to show that performing reductions on a word in any order produces the same result - i.e. for every word there exists a unique reduced form of this word.

To prove this, suppose $w \in W(A)$. If there is no pair of letters aa^{-1} or $a^{-1}a$ in w for any $a \in A$, then clearly we have nothing to reduce and the word itself is its unique reduced form.

If there is a single such pair, there is obviously a single way to reduce the word.

There are two interesting cases to check. Suppose $w = w_1aa^{-1}w_2bb^{-1}w_3$ where $a, b \in A$ and $w_1, w_2, w_3 \in W(A)$. Now there are two possibly ways to reduce this word. We can either reduce the first pair producing $w' = w_1w_2bb^{-1}w_3$, or the second producing $w'' = w_1aa^{-1}w_2w_3$. But reducing those two words w', w'' produces the same result $w_1w_2w_3$. Thus the order does not matter in this case.

The second interesting case is of $w = w_1aa^{-1}aw_2$. Both ways to reduce this word produce w_1aw_2 and thus order also does not matter.

But that means that every word has a unique reduced form.

Now the associativity of the operation of $F(A)$ follows: Let $v, w, u \in F(A)$. Then $(v \cdot w) \cdot u = R(vw) \cdot u = R(R(vw), u) = R(v, R(wu)) = v \cdot R(wu) = v \cdot (w \cdot u)$. □

5.5.

Solution. Let $H^{\oplus A}$ be as defined in the text and let $\varphi + \psi$ be defined in the same way as for H^A, so that for every $a \in A$ we have $(\varphi + \psi)(a) := \varphi(a) + \psi(a)$.

First, we have to check that the operation is well-defined. Let $\varphi, \psi \in H^{\oplus A}$. Then there are only finitely many $a \in A$ such that $\varphi(a) = e_H$ and $\psi(a) = e_H$ (not necessarily for the same elements of A however). Now notice that $(\varphi + \psi)(a) \neq e_H$ only when $\varphi(a) \neq e_H$ or $\psi(a) \neq e_H$ (or both). But we know that there are only finitely many such elements of A for both φ and ψ and thus it follows that there are also only finitely many $a \in A$ such that $(\varphi + \psi)(a) \neq e_H$.

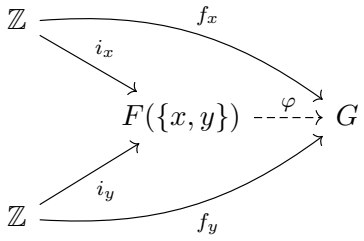
Now, the operation $+$ is associative because it is associative in the group H^A. The identity is the function which sends every element of A to e_H (notice that this is an element of $H^{\oplus A}$ by its definition). An inverse of φ is again defined the same way as in

H^A so that $(-\varphi)(a) = -\varphi(a)$ for all $a \in A$ (again, this is easily seen to be an element of $H^{\oplus A}$).

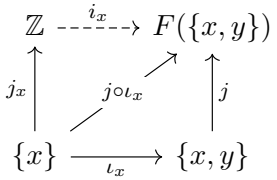
Thus $H^{\oplus A}$ is indeed a group with the operation $+$. □

5.6.

Solution. We want to show that $F(\{x, y\})$ satisfies the universal property for coproduct of $\mathbb{Z}$ by itself in Grp. In other words, for any group G and two homomorphisms $f_x, f_y : \mathbb{Z} \to G$, there is a unique homomorphism $\varphi : F(\{x, y\}) \to G$ making the diagram

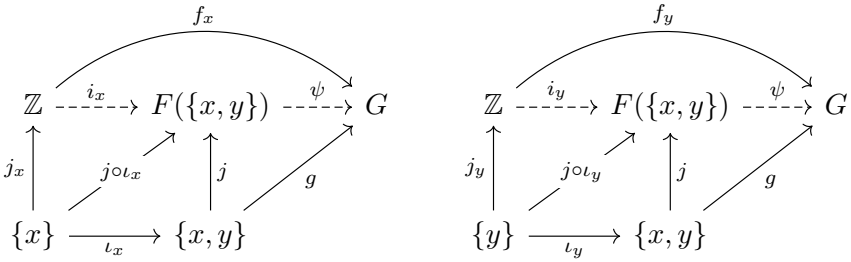


commute. The homomorphism i_x can be obtained by using the universal property of free groups, being the unique homomorphism making the natural diagram



commute, with $j : \{x, y\} \to F(\{x, y\})$ and $j_x : \{x\} \to \mathbb{Z}$ being the set functions defining the free groups. Similarly for i_y.

Let us now consider the universal property of the free group $F(\{x, y\})$. Notice, that it would be only natural to demand for the two diagrams

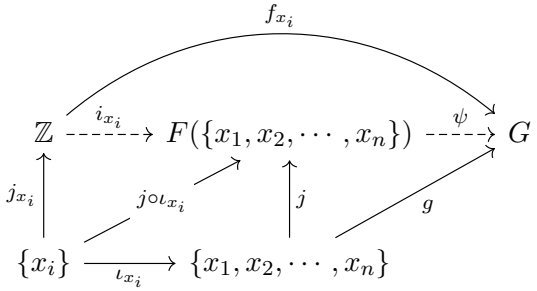


for some choice of a set-function g. The existence of ψ would follow from the universal property. But notice that such a function g is forced on us by the required commutativity of the two diagrams. We must have $g \circ \iota_x = f_x \circ j_x$ so that $g(x) = g \circ \iota_x(x) = f_x \circ j_x(x) = f_x(1)$ and similarly $g(y) = f_y(1)$. Then we have a unique homomorphism $\psi : F(\{x, y\}) \to G$ such that, in particular, we have $\psi \circ i_x = f_x$ and $\psi \circ i_y = f_y$.

Therefore, $F(\{x, y\})$ indeed satisfies the universal property of coproduct of $\mathbb{Z}$ by itself in Grp and thus $F(\{x, y\}) \cong \mathbb{Z} * \mathbb{Z}$. □

5.7.

Solution. Notice that we can extend the solution of Problem II.5.6. to any finite set $\{x_1, x_2, \cdots, x_n\}$. If G is any group and $f_{x_1}, f_{x_2}, \ldots, f_{x_n} : \mathbb{Z} \to G$ group homomorphisms, we can demand all the diagrams of the form



for $1 \leq i \leq n$ to commute for a suitable set-function $g : \{x_1, x_2, \cdots, x_n\} \to G$. Again, g is forced on us by the required commutativity of all the diagrams and it follows that $F(\{x_1, x_2, \cdots, x_n\})$ is the coproduct of $\mathbb{Z}$ by itself n times.

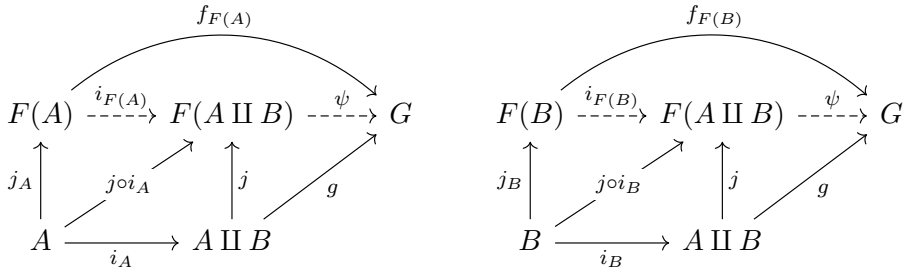
Now note that the situation for free *abelian* groups is entirely analogous. We know $F^{ab}(\{x_i\}) \cong \mathbb{Z}$. Therefore we can continue in the same sake as last time, replacing groups with abelian groups where needed and the coproduct in Grp with coproduct in Ab. Therefore $F^{ab}(\{x_1, x_2, \cdots, x_n\}) \cong \mathbb{Z}^{\oplus n}$. □

5.8.

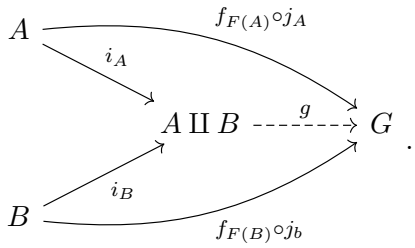
Solution. Generalizing the solutions to Problems II.5.6. and II.5.7. once more, we can consider the free (abelian) groups $F(A \amalg B)$ for some sets A, B.

For the non-abelian case (the result for abelian free groups will follow), let G be any group and $f_{F(A)} : F(A) \to G$, $f_{F(B)} : F(B) \to G$ group homomorphisms.

We can follow a similar procedure as in the proof of Problem II.5.6. Let G be any group and $f_A : F(A) \to G$, $f_B : F(B) \to G$ any homomorphisms. We will again demand the two diagrams



to commute for a suitable set-function $g : A \amalg B \to G$. The definition of this function is not as clearly forced upon us as in Problem II.5.6., however, we can use the universal property of $A \amalg B$ to produce such a function for us:



It follows that $F(A \amalg B)$ indeed satisfies the universal property of the coproduct of $F(A)$ and $F(B)$ in Grp.

As in Problem II.5.7., the abelian case is entirely analogous, only replacing groups with abelian groups where necessary. □

5.9.

Solution. First we will consider the set $\mathbb{N} \amalg \mathbb{N}$. Let $\varphi : \mathbb{N} \amalg \mathbb{N} \to \mathbb{N}$, defined as

$$\varphi(x) = \begin{cases} 2n & \text{if } x = (n, 0) \\ 2n + 1 & \text{if } x = (n, 1) \end{cases}$$

which is clearly a bijective function. Therefore $\mathbb{N} \amalg \mathbb{N} \cong \mathbb{N}$.

By Problem II.5.8. that means $F^{ab}(\mathbb{N}) \cong F^{ab}(\mathbb{N} \amalg \mathbb{N}) \cong F^{ab}(\mathbb{N}) \oplus F^{ab}(\mathbb{N})$.

Now $G = \mathbb{Z}^{\oplus \mathbb{N}} = F^{ab}(\mathbb{N})$. Since $\oplus$ is defined in the same way as direct products of abelian groups, we have in fact showed that $G = F^{ab}(\mathbb{N}) \cong F^{ab}(\mathbb{N}) \oplus F^{ab}(\mathbb{N}) = G \times G$. □

5.10.

Solution. Let $F = F^{ab}(A)$ for some set A.

- Define an equivalence relation $\sim$ on F by setting $f' \sim f$ if and only if $f - f' = 2g$ for some $g \in F$. Consider the set $F/\sim$. Suppose A is infinite. Let $[f]_\sim \in F/\sim$ be an equivalence class. Now f can be understood as the finite sum

$$\sum_{a \in A} m_a j_a,\ m_a \neq 0 \text{ for only finitely many } a.$$

  Notice that for any such f we can construct a new f' such that $f - f' \neq 2g$ for any $g \in F$ by taking any $b \in A$ such that $m_b = 0$, and considering the finite sum $f + j_b$.

Notice that this also satisfies the constraint of there being only finitely many non zero coefficients (the old finite number and one more). But clearly $f - f' = j_b \neq 2g$ for any $g \in F$. Thus $F/\sim$ is infinite.

Now suppose A is finite. Now the elements of F can be understood easily as tuples $(x_1, \ldots, x_{|A|})$. Notice that the equivalence classes of such tuples depend on the parity at each index - two tuples belong in the same equivalence class if $x_i \equiv y_i \mod 2$ for $1 \leq i \leq |A|$. Thus the set $F/\sim$ has $2^{|A|}$ elements and therefore is finite.

- Assume $F^{ab}(B) \cong F^{ab}(A)$. Suppose that A is finite. Then by the first part we know $\left|F^{ab}(A)/\sim\right| = 2^{|A|}$. But since $F^{ab}(B)$ is isomorphic to $F^{ab}(A)$, $F^{ab}(B)/\sim$ must also be isomorphic to $F^{ab}(A)/\sim$ and therefore B must also be finite and $2^{|A|} = 2^{|B|}$. That necessarily means $|A| = |B|$ and because finite sets of the same size are isomorphic we have $A \cong B$. □

6. Subgroups

6.1.

Solution. We will go point by point, for each set trying to determine the possible inclusions to other sets in the list.

- $\mathrm{SL}_n(\mathbb{R}) \subseteq \mathrm{GL}_n(\mathbb{R})$ is obvious. Now let $A, B \in \mathrm{SL}_n(\mathbb{R})$. Now $\det(AB^{-1}) = \det(A)\det(B^{-1}) = 1$ and thus $AB^{-1} \in \mathrm{SL}_n(\mathbb{R})$ and therefore $\mathrm{SL}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

  We also have $\mathrm{SL}_n(\mathbb{R}) \subseteq \mathrm{SL}_n(\mathbb{C})$ as real numbers are in particular complex. Again let $A, B \in \mathrm{SL}_n(\mathbb{R})$. $\det(B^{-1}) = \frac{1}{\det(B)} = 1$ and thus $B^{-1} \in \mathrm{SL}_n(\mathbb{C})$. We have already shown that $AB^{-1} \in \mathrm{SL}_n(\mathbb{R})$.
- $\mathrm{SL}_n(\mathbb{C}) \subseteq \mathrm{GL}_n(\mathbb{C})$. The proof that it is indeed a subgroup is the same as in the last item.
- $\mathrm{O}_n(\mathbb{R}) \subseteq \mathrm{GL}_n(\mathbb{R})$. Let $A, B \in \mathrm{O}_n(\mathbb{R})$. Consider AB^{-1}. We have $(AB^{-1})(AB^{-1})^t = (AB^{-1})((B^{-1})^t A^t) = AA^t = I_n$ and similarly for the other direction and thus $AB^{-1} \in \mathrm{O}_n(\mathbb{R})$.

  $\mathrm{O}_n(\mathbb{R}) \subseteq \mathrm{U}(n)$, because conjugate transpose is identical to a normal transpose on matrices with real entries.
- $\mathrm{SO}_n(\mathbb{R}) \subseteq \mathrm{O}_n(\mathbb{R})$. The proof is again similar to the first item.
- $\mathrm{U}(n) \subseteq \mathrm{GL}_n(\mathbb{C})$. The proof is similar to the proof for $\mathrm{O}_n(\mathbb{R})$.
- $\mathrm{SU}(n) \subseteq \mathrm{U}(n)$. □

6.2.

Solution. Let

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, B = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}.$$

Then

$$B^{-1} = \begin{pmatrix} \frac{1}{x} & \frac{-y}{xz} \\ 0 & \frac{1}{z} \end{pmatrix}.$$

The product is then

$$AB^{-1} = \begin{pmatrix} \frac{a}{x} & \frac{b}{z} - \frac{ay}{xz} \\ 0 & \frac{c}{z} \end{pmatrix}.$$

So the upper triangular matrices form a subgroup of the invertible 2×2 matrices. □

6.3.

Solution. Todo. □

6.4.

Solution. Let G be a group, $g \in G$, $\epsilon_g : \mathbb{Z} \to G$ the exponential map. We know that $\operatorname{im} \epsilon_g$ is a subgroup of G. Now because a subgroup of G must be closed under the operation of G. In particular, if g is an element of a subgroup of G, then its order in the subgroup is the same as its order in G.

There are two possibilities for the order of g. First suppose that g does not have finite order in G. Then the subgroup $\operatorname{im} \epsilon_g$ is clearly isomorphic to $\mathbb{Z}$ - it is enough to consider a similar exponential map $\mathbb{Z} \to \operatorname{im} \epsilon_g$ and notice that it is in fact an isomorphism - surjectivity is immediate, for injectivity notice that $i \neq j$ we have $g^i \neq g^j$ because g does not have finite order.

Now suppose g has a finite order in G, so that $|g| = n$. $\operatorname{im} \epsilon_g$ must then consist of exactly the n elements of the form g^i, $0 \leq i \leq n-1$. Thus $\operatorname{im} \epsilon_g$ is a group of order n and contains an element g of order n, therefore it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. □

6.5.

Solution. Let G be a commutative group, $n > 0$ an integer. Let $x, y \in \{g^n \mid g \in G\}$. Then by definition there are $g, h \in G$ such that $x = g^n, y = h^n$. Then we have $xy^{-1} = g^n(h^n)^{-1} = g^n(h^{-1})^n$. Now notice that G is a commutative group, therefore we can reorder the product $g^n(h^{-1})^n$ to $(gh^{-1})^n$. But that is in fact an element of the set and thus we have proved that it is a subgroup of G.

Now suppose G is not commutative. Then the given set is not necessarily a subgroup. For a counterexample, we can take the group S_3 which we know is not commutative, and $n = 3$. Then we have $H = \{g^3 \mid g \in S_3\} = \{(1,2,3), (1,3,2), (3,2,1), (2,1,3)\}$. But $(1,3,2)(3,2,1) = (3,1,2) \notin H$. And thus H is not closed under the operation of S_3 and therefore is not a subgroup. □

6.6.

Solution. Let H, H' be subgroups of a group G.

Suppose that $H \not\subseteq H'$ and $H' \not\subseteq H$. Then there must be some $h \in H, h' \in H'$ such that $h \notin H'$ and $h' \notin H$. We have $h, h' \in H \cup H'$. For $H \cup H'$ to be a subgroup of G, the element hh' must be in $H \cup H'$. But that means either $hh' \in H$ or $hh' \in H'$. Suppose $hh' \in H$. Then because H is a subgroup of G, and thus it is closed on its operation and $h^{-1} \in H$, we must also have $h^{-1}hh' = e_G h' = h' \in H$, a contradiction. Similarly if $hh' \in H'$. Thus $H \cup H'$ is not a subgroup of G.

Now consider an indexed family of subgroups $H_0 \subseteq H_1 \subseteq H_2 \subseteq \dots$ of G. We will show that $\bigcup_{i\geq 0} H_i$ is in fact a subgroup of G. Let $h, h' \in \bigcup_{i\geq 0} H_i$. But that means there must be a minimal index j such that $h, h' \in H_j$ (by the definition of set union and the assumption of set inclusions). Since H_j is a subgroup, we have $hh'^{-1} \in H_j$ and thus $hh'^{-1} \in \bigcup_{i\geq 0} H_i$. Therefore $\bigcup_{i\geq 0} H_i$ is in fact a subgroup of G. □

6.7.

Solution. Let G be a group. Define $\mathrm{Inn}(G)$ as the set of all inner automorphisms of G. Clearly $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G)$. Let $\gamma_g, \gamma_h \in \mathrm{Inn}(G)$ (where $g, h \in G$). Now $\gamma_g \circ \gamma_h^{-1} = \gamma_g \circ \gamma_{h^{-1}}$. Then for any $a \in G$ we have $\gamma_g \circ \gamma_{h^{-1}}(a) = \gamma_g(h^{-1}ah) = (gh^{-1})a(hg^{-1}) = (gh^{-1})a(gh^{-1})^{-1} = \gamma_{gh^{-1}}(a)$. Therefore $\gamma_g \circ \gamma_{h^{-1}} = \gamma_{gh^{-1}} \in \mathrm{Inn}(G)$. Therefore $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

Now we shall prove that $\mathrm{Inn}(G)$ is cyclic if and only it is trivial if and only if G is abelian. Suppose $\mathrm{Inn}(G)$ is cyclic. Then in particular there must exist an element $a \in G$ such that $\forall g \in G\ \exists n \in \mathbb{Z}\ \gamma_g = \gamma_a^n$. In particular we have $gag^{-1} = a^n a a^{-n} = a$. Thus a commutes with every $g \in G$. Therefore $\forall g \in G\ \gamma_g = id_G$ and $\mathrm{Inn}(G)$ is trivial. Now by Problem II.4.8. we know that the homomorphism $g \mapsto \gamma_g$ is trivial if and only if G is abelian. If $\mathrm{Inn}(G)$ is trivial, it is obviously cyclic, which finishes our argument.

Notice that if $\mathrm{Aut}(G)$ is cyclic, its subgroups must also be cyclic (by Propositions II.6.9 and II.6.11.). In particular, $\mathrm{Inn}(G)$ must be cyclic, but as we have proved, that means G must be abelian. □

6.8.

Solution. Let G be an abelian group. Suppose G is finitely generated. By definition there exists a finite subset $A \subseteq G$ such that $G = \langle A \rangle$. $\langle A \rangle$ is an image of the unique homomorphism $F^{ab}(A) \to G$. Because G is the image of this homomorphism, it is necessarily surjective. Let $n = |A|$. Then $F^{ab}(A) = \mathbb{Z}^{\oplus n}$ (this can be seen, for example, from Problem II.5.7). Thus we have a surjective homomorphism $\mathbb{Z}^{\oplus n} \twoheadrightarrow G$.

Now suppose there is a surjective homomorphism $\mathbb{Z}^{\oplus n} \twoheadrightarrow G$ for some n. Now, every element of $\mathbb{Z}^{\oplus n}$ is equal to a tuple $(m_1, m_2, \dots, m_n) = m_1(1,0,0,\dots 0) + m_2(0,1,0,\dots 0) + \dots + m_n(0,0,0,\dots,1)$ and thus the homomorphism is defined by the images of the tuples

with 0 everywhere but a single element which is 1. Let the images of those tuples be $g_1, g_2, \ldots, g_n$. The homomorphism is surjective, therefore we can write every element $g = g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}$ for some $m_1, m_2, \ldots, m_n \in \mathbb{Z}$. Of course, the elements $g_1, g_2, \ldots, g_n$ may not be all distinct, in which case we can simplify the product. Consider the set $A = \{h_1, h_2, \ldots, h_k\}$ defined as all the distinct elements from $g_1, g_2, \ldots, g_n$. In particular, this set is finite and $|A| = k \leq n$. We shall show that $G = \langle A \rangle$. By the universal of free abelian groups we have a homomorphism $\varphi : F^{ab}(A) \to G$ extending the inclusion $A \to G$.

Consider an element $g \in G$. Then we know g is a product of the elements of A such that $h_1^{m_1} h_2^{m_2} \cdots h_k^{m_k}$ for some $m_1, \ldots, m_k$. From the universal property of free abelian groups it also follows that $\varphi(j_{h_i}) = h_i$ for all $1 \leq i \leq k$. In particular it follows that $\varphi(m_1 j_{h_1} + m_2 j_{h_2} + \cdots + m_k j_{h_k}) = h_1^{m_1} h_2^{m_2} \cdots h_k^{m_k} = g$ because φ is a group homomorphism. Thus φ is surjective and therefore $\operatorname{im} \varphi = G$. Then it follows that $G = \langle A \rangle$ and is therefore finitely generated. □

6.9.

Solution. Let G be a finitely generated subgroup of $\mathbb{Q}$. Then $G = \langle A \rangle$ for a finite set $A \subseteq \mathbb{Q}$ so that $A = \{\frac{p_1}{q_1}, \frac{p_2}{q_2}, \cdots, \frac{p_n}{q_n}\}$ for some $n \in \mathbb{N}$, $p_i \in \mathbb{Z}$, $q_i \in \mathbb{Z}$ and $q_i > 0$ for all $1 \leq i \leq n$. It is not hard to see that the elements of G are precisely the elements $m_1 \frac{p_1}{q_1} + m_2 \frac{p_2}{q_2} + \cdots + m_n \frac{p_n}{q_n}$, $m_i \in \mathbb{Z}$ for $1 \leq i \leq n$. Every such element can be rewritten as

$$\frac{m_1 p_1 q_2 \cdots q_n + m_2 q_1 p_2 q_3 \cdots q_n + \cdots + m_n q_1 \cdots q_{n-1} p_n}{q_1 \cdots q_n}.$$

But notice that means $\langle A \rangle \subseteq \langle \frac{1}{q_1 \cdots q_n} \rangle$, which is cyclic. It is not hard to see that it is also a subgroup of this group, and thus G is cyclic.

Suppose that $\mathbb{Q}$ is finitely generated. Similarly to the first part, there must then be a finite set $A \subseteq \mathbb{Q}$ such that $Q = \langle A \rangle$. As we have noted already, the elements of $\langle A \rangle$ look like the fractions above. Consider $\frac{1}{q_1 \cdots q_n + 1}$. Clearly there is no way to generate this element, a contradiction. □

6.10.

Solution. Let $\mathrm{SL}_2(\mathbb{Z})$ denote the group of 2×2 matrices with integer entries and determinant 1. Then $s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are elements of this group.

Let H be the subgroup generated by s and t, so that $H = \langle s, t \rangle$, and let $q \in \mathbb{Z}$. Notice, that s has order 4, and in particular $s^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Now, there are two interesting elements which we can obtain from s and t:

$$x = sts^3 = (sts)s^2 = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

$$y = ststs^3 = (ststs)s^2 = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

It is not hard to see that we have

$$x^q = \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} \quad \text{and} \quad y^q = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}.$$

Let $m \in \mathrm{SL}_2(\mathbb{Z})$, $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $mx^q = \begin{pmatrix} a - qb & b \\ c - qd & d \end{pmatrix}$ and $my^q = \begin{pmatrix} a & b - qa \\ c & d - qc \end{pmatrix}$.

Suppose that both c and d are both nonzero. We can show that one of the multiplications noted above (by x^q or y^q) will necessarily decrease the absolute value of one of them. If $c = d$, it is clear that we can produce a matrix with either c or d equal to 0 by using $q = 1$. Suppose $c \neq d$, then clearly one of the numbers will have larger absolute value than the other. Suppose c has the larger absolute value, then we can produce numbers $k, l \in \mathbb{Z}$ such that $c = kd + l$, with $|l| < |c|$. Setting $q = k$, we can produce a new matrix $\begin{pmatrix} a - kb & b \\ l & d \end{pmatrix}$ such that $|l| < |c|$. Similarly we can decrease d if $|d| > |c|$.

But we can repeat this operation several times, each time either decreasing $|c|$ or $|d|$. Because absolute values are always non-negative, this procedure must stop when either $c = 0$ or $d = 0$, in a finite number of steps.

Therefore it is enough to consider matrices with $c = 0$ or $d = 0$. Suppose $c = 0$, by the condition on determinant being equal to 1, we must have $ad = 1$ and thus $a = d = 1$. We have already shown that $m \in H$ however, as $m = y^q$ for a suitable q. Now suppose $d = 0$. Then we have a condition $bc = -1$. Therefore we have either $m = \begin{pmatrix} a & 1 \\ -1 & 0 \end{pmatrix}$ or $m = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$ for some a. Notice that $sx^q = \begin{pmatrix} q & -1 \\ 1 & 0 \end{pmatrix}$ and $sx^q s^2 = \begin{pmatrix} -q & 1 \\ -1 & 0 \end{pmatrix}$. And thus in either case $m \in H$. □

6.11.

Solution. Suppose S_3 is a coproduct of cyclic groups, then in particular it satisfies the universal property of a coproduct of (cyclic) groups $G_i, i \in I$, where I is a set of indices, with homomorphisms $\iota_i : G_i \to S_3$. Then for any $i \in I$ we can take trivial homomorphisms $f_j : G_j \to G_i$ for $j \in I, j \neq i$ and a homomorphism $id_{G_i} = f_i : G_i \to G_i$ and produce a unique homomorphism $\sigma_i : S_3 \to G_i$ such that $\sigma_i \circ \iota_i = f_i = id_{G_i}$. But that means the order of each G_i must be at most the order of S_3, as otherwise the homomorphisms σ_i could not exist.

Therefore we are looking at a coproduct of cyclic groups of order up to 6. Each ι_i is a group homomorphism, and therefore the order of $\iota_i(x)$ must divide the order of x for all $x \in G_i$. But S_3 has elements of orders 1, 2, and 3. Since a cyclic group C_n has order n and contains an element of order n, the only possible choices we have for our coproduct are C_1, C_2, C_3, C_4, C_6. C_1 is clearly not interesting as we can always add it to

a coproduct without changing the result, because it is the trivial group. Now suppose $G_i = C_4$ for some $i \in I$. Then again by order considerations we would require $\sigma_i(\iota_i(x))$ to divide $\iota(x)$ for all $x \in G_i$. In particular, the generator x of order C_4 has order 4, then $\iota(x)$ must have order 2, and therefore there is no way $\sigma_i(\iota_i(x)) = x$. Similarly for C_6.

Now this means every G_i is either C_1, C_2, or C_3. Suppose C_3 is a part of the coproduct. By the universal property of coproducts there must be a unique homomorphism $\varphi : S_3 \to S_3$ such that all the diagrams

$$\begin{array}{ccc} G_i & \xrightarrow{\iota_i} & S_3 \\ & \searrow^{\iota_i} & \downarrow \varphi \\ & & S_3 \end{array}$$

commute. However, for all $i \in I$, ι_i can never map to an element of order 3 in S_3 (again by order considerations). Therefore no of the diagrams above constrain the elements of order 3 in S_3 in any way, and thus φ cannot be unique as we can either map those elements to themselves (obtaining the homomorphism id_{S_3}) or to e_{S_3}.

We came to the conclusion that there must be an $i \in I$ such that $G_i = C_3$. Now, by the initial consideration that means there must be a unique homomorphism $\sigma_i : S_3 \to C_3$ such that $\sigma_i \circ \iota_i = id_{C_3}$. Let g be the element which generates C_3. We know there are elements $x, y \in S_3$ such that $x^2 = e$, $y^3 = e$ and $yx = xy^2$. Now $\iota_i(g)$ must equal either y or y^2 (the only two elements of S_3 of order 3). Suppose $\iota_i(g) = y$. Then we must have $\sigma_i(y) = g$ and $\sigma_i(x) = e$ (due to order). But $g = ge = \sigma_i(yx) = \sigma_i(xy^2) = eg^2 = g^2$ which is not possible. If $\iota_i(g) = y^2$, then similarly we need $\sigma_i(y^2) = g$ and thus $\sigma_i(y) = g^2$ which again is not possible as we would have $g^2 = \sigma(yx) = \sigma(xy^2) = g$.

Thus S_3 cannot be a coproduct of cyclic groups. □

6.12.

Solution. Let m, n be positive integers and consider the subgroup $\langle m, n\rangle$ of $\mathbb{Z}$. By Proposition II.6.9., we must have $\langle m, n\rangle = d\mathbb{Z}$ for some positive integer d. In particular, d must be the smallest positive integer such that $d = am + bn$ for $a, b \in \mathbb{Z}$. But this means d must be $\gcd(m, n)$. □

6.13.

Solution. Todo. □

6.14.

Solution. Let m be a positive integer. $\phi(m)$ is defined as the number of positive integers $r \leq m$ that are relatively prime to m. By Corollary II.2.5. we know that an element $[n]_m$ generates $\mathbb{Z}/m\mathbb{Z}$ if and only if $\gcd(m,n) = 1$. But that means $\phi(m)$ is in fact the number of generators of C_m.

Consider a cyclic group C_n for some n. Then every element of C_n generates a subgroup of C_n, which must be isomorphic to C_m for some $m \mid n$ by Proposition II.6.11.

It then follows that

$$\sum_{m>0, m|n} \phi(m) = n.$$

□

6.15.

Solution. Let $\varphi : G \to G'$ be a group homomorphism such that it has a left-inverse, that is, a group homomorphism $\psi : G' \to G$ such that $\psi \circ \varphi = \mathrm{id}_G$. Suppose H is a group and $\alpha, \alpha' : H \to G$ two group homomorphisms such that $\varphi \circ \alpha = \varphi \circ \alpha'$. Then we have $\psi \circ \varphi\alpha = \psi \circ \varphi \circ \alpha'$ and thus $\alpha = \alpha'$. But that means φ is a monomorphism. □

6.16.

Solution. Consider the homomorphism $\varphi : \mathbb{Z}/3\mathbb{Z} \to S_3$ given by

$$\varphi([0]) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e, \quad \varphi([1]) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = x, \quad \varphi([2]) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = y$$

which is a monomorphism. Suppose $\psi : S_3 \to \mathbb{Z}/3\mathbb{Z}$ is a homomorphism such that $\psi \circ \varphi = id_{\mathbb{Z}/3\mathbb{Z}}$. Then in particular, we must have $\psi(x) = [1]$ and $\psi(y) = [2]$). S_3 has elements of order 2, which must be mapped to [0] as [1] and [2] have order 3 in $\mathbb{Z}/3\mathbb{Z}$. Notice that we have

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

but

$$\psi(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}) = [0] + [0] = [0] \neq [1] = \psi(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix})$$

because ψ is a homomorphism. Thus there cannot exist any such ψ. □

7. Quotient groups

7.1.

Solution. The trivial group and S_3 are both subgroups of S_3. Now consider the subgroups generated by each element of S_3 which is not the identity:

- $\langle(1\ 3\ 2)\rangle = \{e, (1\ 3\ 2)\}$,
- $\langle(2\ 1\ 3)\rangle = \{e, (2\ 1\ 3)\}$,
- $\langle(3\ 2\ 1)\rangle = \{e, (3\ 2\ 1)\}$,
- $\langle(2\ 3\ 1)\rangle = \langle(3\ 1\ 2)\rangle = \{e, (2\ 3\ 1), (3\ 1\ 2)\}$.

Checking that these are in fact all the possible subgroups of S_3 amounts to trying subgroups generated by two elements which in fact always generate S_3.

Now, the trivial group and S_3 are both normal subgroups of S_3. It is not hard to check that neither subgroup generated by an element of order 2 is normal - for example we have

$$(2\ 3\ 1)(1\ 3\ 2)(3\ 1\ 2) = (3\ 2\ 1)(3\ 1\ 2) = (2\ 1\ 3)$$

so that $\langle(1\ 3\ 2)\rangle$ is not normal. Now it remains to check if $\{e, (2\ 3\ 1), (3\ 1\ 2)\}$ is normal. It is enough to check the left- and right-cosets for $(1\ 3\ 2), (2\ 1\ 3), (3\ 2\ 1)$. We have

$$(1\ 3\ 2)\{e, (2\ 3\ 1), (3\ 1\ 2)\} = \{(1\ 3\ 2), (2\ 1\ 3), (3\ 2\ 1)\}$$
$$\{e, (2\ 3\ 1), (3\ 1\ 2)\}(1\ 3\ 2) = \{(1\ 3\ 2), (3\ 2\ 1), (2\ 1\ 3)\}$$

and similarly for the rest and thus this subgroup is normal. □

7.2.

Solution. Clearly that is not the case. Remember that by the universal property of free groups we have a group homomorphism $\varphi : F((1\ 3\ 2)) \to S_3$ such that $\operatorname{im}\varphi = \langle(1\ 3\ 2)\rangle$ which is not a normal subgroup of S_3. □

7.3.

Solution. By Definition II.7.1., a subgroup N of a group G is normal if $\forall g \in G, \forall n \in N, gng^{-1} \in N$.

We want to show that the following conditions are all equivalent, $\forall g \in G$,

$$N \text{ is normal} \iff gNg^{-1} \subseteq N \iff gNg^{-1} = N \iff gN \subseteq Ng \iff gN = Ng.$$

First suppose that N is a normal subgroup of G and let $g \in G$ be any element. Consider $x \in gNg^{-1}$. Then $x = gng^{-1}$ for some $n \in N$. But because N is normal, $x \in N$ and thus $gNg^{-1} \subseteq N$.

Now let $n \in N$. Since $gNg^{-1} \subseteq N$ for any g, it must also hold for g^{-1} so that $g^{-1}Ng \subseteq N$. Then $n = g(g^{-1}ng)g^{-1} \in gNg^{-1}$ and thus $N \subseteq gNg^{-1}$ and therefore $gNg^{-1} = N$ as required.

Now suppose $x \in gN$. Then $x = gn$ for some $n \in N$. Since $g^{-1}Ng = N$ we have $x = g(g^{-1}n'g) = n'g$ for some $n' \in N$ and thus $x \in Ng$ and therefore $gN \subseteq Ng$.

Let $x \in Ng$, so that $x = ng$ for some $n \in N$. Then $x = ng = (gg^{-1})ng = g(g^{-1}n)g$. Since $gN \subseteq Ng$ for all $g \in G$, in particular we have $g^{-1}N \subseteq Ng^{-1}$, and thus $g^{-1}n = n'g^{-1}$ for some $n' \in N$ and thus $x = g(n'g^{-1})g = gn'$ and therefore $x \in gN$ so that $Ng \subseteq gN$ and thus $gN = Ng$.

Let $n \in N$. Since $gN = Ng$, there is $n' \in N$ such that $gn = n'g$. But that means $gng^{-1} = n'gg^{-1} = n' \in N$ and thus N is a normal subgroup of G. □

7.4.

Solution. Let A be a set, and $F = F^{ab}(A)$. Consider the equivalence relation $\sim$ defined by setting $f' \sim f$ if and only if $f - f' = 2g$ for some $g \in F$.

Let $a, b \in F$ and suppose $a \sim b$. Let $f \in F$ be any element. Since $a \sim b$, $b - a = 2g$ for some $g \in F$. We then have $(b + f) - (a + f) = b - a = 2g$ and therefore $a + f \sim b + f$. Similarly, $(f+b)-(f+a) = b-a = 2g$ and therefore $f+a \sim f+b$. Thus $\sim$ is compatible with group structure.

It is not hard to understand the quotient $F/\sim$ when A is a finite set. In the general case we have to be more careful. The normal subgroup G of F which corresponds to $\sim$ contains the identity element of G, that is a set-function $\alpha : A \to \mathbb{Z}$, such that $\alpha(a) = 0$ for all $a \in A$. It must then also contain all the set-functions $\beta : A \to \mathbb{Z}$ such that $\beta(a)$ is equal to a multiple of 2 for finitely many elements $a \in A$. Notice that this situation is very similar to the group $\mathbb{Z}$ and its subgroup $2\mathbb{Z}$. Indeed, the only possible cosets of G are the equivalence classes of set-function $\gamma : A \to Z$ such that $\gamma(a) = 1$ for finitely many $a \in A$. Therefore we can identify the quotient $F/\sim$ to $(\mathbb{Z}/2\mathbb{Z})^{\oplus A}$. □

7.5.

Solution. Consider the group $\mathrm{SL}_2(\mathbb{Z})$ defined in Exercise II.6.10. Define an equivalence relation $\sim$ on $\mathrm{SL}_2(\mathbb{Z})$ by setting $A \sim A' \iff A' = \pm A$. Now let $A, B \in \mathrm{SL}_2(\mathbb{Z})$ be matrices such that $A \sim B$. Let $X \in \mathrm{SL}_2(\mathbb{Z})$ be any matrix. Since $A \sim B$ we have $B = \pm A$. There are two cases to consider. If $B = A$, we have $BX = AX$ and $XB = XA$ by simple multiplication by X on the right and left. Similarly, if $B = -A$, we have $B = -I_2A$, thus $BX = (-I_2A)X = -I_2(AX) = -(AX)$ and $XB = X(-I_2A) = (X - I_2)A = (-I_2X)A = -I_2(XA) = -(XA)$ (because $-I_2$ commutes with every element). That means $BX = \pm AX$ and $XB = \pm XA$, and thus $AX \sim BX$ and $XA \sim XB$. Therefore $\sim$ is compatible with group structure.

In Exercise II.6.10. we have shown $\mathrm{SL}_2(\mathbb{Z})$ is generated by the two matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Notice that we have

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

Let $R = TS$. Thus every element of $\mathrm{SL}_2\mathbb{Z}$ is a product of S's and R's. We have $S^2 = -I_2$ and $R^3 = -I_2$ and therefore every product of S's and R's can be simplified to the form

$$(-I_2)^a R^{i_0} S R^{i_1} S \cdots R^{i_{n-1}} S R^{i_n},$$

where a is either 0 or 1 and i_j is not divisible by 3 for $0 < j < n$ (therefore we allow R^{i_0} and R^{i_n} to be $\pm I_2$).

Consider the group $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\sim$. Since $I_2 \sim -I_2$, the cosets corresponding to S and R have order 2 and 3 respectively. Label them as x and y. But by the above we see that every element of $\mathrm{PSL}_2(\mathbb{Z})$ can be written in the form $y^{i_0} x i^{i_1} x \cdots y^{i_{n-1}} x y^{i_n}$ where $i_j \in \mathbb{Z}/3\mathbb{Z}$ and $i_j \neq 0$ for $0 < j < n$. Thus x and y generate $\mathrm{PSL}_2(\mathbb{Z})$. □

7.6.

Solution. Let G be a group, n a positive integer. Consider the relation

$$a \sim b \iff (\exists g \in G) ab^{-1} = g^n.$$

- In general, $\sim$ is not an equivalence relation. As a counterexample we can take the noncommutative group S_3 and $n = 3$. In that case, we clearly have $(1\ 3\ 2) \sim (1\ 2\ 3)$ and $(1\ 2\ 3) \sim (3\ 2\ 1)$, but $(1\ 3\ 2) \not\sim (3\ 2\ 1)$ as $(1\ 3\ 2)(3\ 2\ 1)^{-1} = (1\ 3\ 2)(3\ 2\ 1) = (3\ 1\ 2)$ which is not equal to g^3 for any $g \in G$.
- In the commutative case, $\sim$ is an equivalence relation. Reflexivity and symmetry are immediate, for transitivity assume that $a, b, c \in G$ and suppose $a \sim b, b \sim c$. Then there are $g, h \in G$ such that $ab^{-1} = g^n, bc^{-1} = h^n$. Then $h^n c = (bc^{-1})c = b(c^{-1}c) = be_G = b$ and thus we have $g^n = a(h^n c)^{-1} = a(c^{-1}h^{-n}) = (ac^{-1})h^{-n}$ and thus $ac^{-1} = g^n h^n = (gh)^n$ (because G is commutative). Therefore $a \sim c$ as needed.

  The subgroup of G corresponding to $\sim$ is the equivalence class of e_G. Now if $a \sim e_G$ for some $a \in G$, that means $a = g^n$ for some $g \in G$. Thus the subgroup is the set $\{g^n \mid g \in G\}$. Notice that this generalizes the way we have defined cyclic groups using $\mathbb{Z}$ and the subgroup $\mathbb{Z}/n\mathbb{Z}$.

□

7.7. Let G be a group, n a positive integer, and let $H \subseteq G$ be the subgroup generated by all elements of order n in G. Prove that H is normal.

Solution. We want to show that for any $h \in H$ and $g \in G$, $ghg^{-1} \in H$. First, notice that for any generator h of H (thus an element of G with order n) and any $g \in G$ we have $(ghg^{-1})^n = gh^n g^{-1} = gg^{-1} = e_G$. It is not hard to see that n is in fact the order of ghg^{-1}, as if $k < n$ is a positive integer, $(ghg^{-1})^k = gh^k g^{-1} \neq e_G$ as h has order n.

Let h be an arbitrary element of H. Thus h has the form $\prod_{i\in I} h_i^{k_i}$ for some finite index set I where each h_i is a generator of H and thus has order n in G. If g is an arbitrary element of G, we have

$$\begin{aligned} ghg^{-1} &= g(\prod_{i\in I} h_i^{k_i})g^{-1} \\ &= \prod_{i\in I}(gh_i^{k_i}g^{-1}) \\ &= \prod_{i\in I}(gh_ig^{-1})^{k_i}. \end{aligned}$$

But notice that gh_ig^{-1} has order n, and thus ghg^{-1} is in fact a product of elements of order n and thus $ghg^{-1} \in H$, showing that H is a normal subgroup of G as needed. □

7.8. ▷ Prove Proposition 7.6. [§7.3]

Solution. Let H be any subgroup of a group G and define relation $\sim_L$ by

$$(\forall a, b \in G): \quad a \sim_L b \iff a^{-1}b \in H.$$

We will show that this is an equivalence relation. If a is any element of G, $a^{-1}a = e_G \in H$ because H is a subgroup of G and thus $a \sim_L a$.

Let $a, b \in G$ and suppose $a \sim_L b$. Then $a^{-1}b = h \in H$. Therefore $b^{-1}a = h^{-1} \in H$ and thus $b \sim_L a$.

Let $a, b, c \in G$ and suppose $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}b = h, b^{-1}c = h'$ for some $h, h' \in H$. From $b^{-1}c = h'$ we get $b^{-1} = h'c^{-1}$ and thus $b = ch'^{-1}$. Substituting in $a^{-1}b = h$ we get $a^{-1}ch'^{-1} = h$ and thus $a^{-1}c = hh'$. But $hh' \in H$ and therefore $a \sim_L c$. Thus $\sim_L$ is indeed an equivalence relation.

Now we want to show that $\sim_L$ satisfies (†). Let $a, b \in G$ such that $a \sim_L b$ and let $g \in G$ be arbitrary. We have $a^{-1}b \in H$ and thus $a^{-1}(g^{-1}g)b \in H$. But then $(a^{-1}g^{-1})(gb) = (ga)^{-1}(gb) \in H$ and thus $ga \sim_L gb$ as required. □

7.9. State and prove the 'mirror' statements of Propositions 7.4 and 7.6, leading to the description of relations satisfying (††).

Solution. We will begin with the 'mirror' statement of Proposition 7.4:

Proposition. *Let $\sim$ be an equivalence relation on a group G, satisfying (††). Then*

- *the equivalence class of e_G is a subgroup H of G; and*
- *$a \sim b \iff ab^{-1} \in H \iff Ha = Hb$.*

Now we shall prove this statement. First let $H \subseteq G$ be the equivalence class of e_G, $H \neq \emptyset$ as $e_G \in H$. Let $a, b \in H$. $e_G \sim b$ and thus $b^{-1} \sim e_G$ by using (††)). We also have $ab^{-1} \sim b^{-1} \sim e_G$ by again using (††) (multiplying $a \sim e_G$ on the right by b^{-1}). Thus $ab^{-1} \in H$, showing that H is a subgroup of G.

Next, assume $a, b \in G$ and $a \sim b$. Multiplying on the right by b^{-1}, by (††) we have $ab^{-1} \sim e_G$ and thus $ab^{-1} \in H$. H is closed under the operation of G and thus $Hab^{-1} \subseteq H$, and therefore $Ha \subseteq Hb$. But $\sim$ is symmetric (because it is an equivalence relation) and thus we also have $Hb \subseteq Ha$ and therefore $Ha = Hb$.

Finally, assume $Ha = Hb$. We have $a = e_G a \in Hb$ and hence $ab^{-1} \in H$. By definition of H we have $e_G \sim ab^{-1}$, multiplying on the right by b, (††) implies $a \sim b$ as required.

The 'mirror' statement of Proposition 7.6:

Proposition. *Let H be any subgroup of a group G and define relation $\sim_R$ by*

$$(\forall a, b \in G): \quad a \sim_R b \iff ab^{-1} \in H$$

is an equivalence relation satisfying (††).

We will show that this is an equivalence relation. Let $a \in G$, then $aa^{-1} = e_G \in H$ and thus $a \sim_R a$. Assume $a, b \in G$ and $a \sim_R b$. Then $ab^{-1} = h \in H$, and thus $ba^{-1} = (ab^{-1})^{-1} = h^{-1} \in H$ and therefore $b \sim_R a$.

Lastly assume that $a, b, c \in G$ and $a \sim_R b$, $b \sim_R c$. Then we have $ab^{-1} = h$ and $bc^{-1} = h'$ for some $h, h' \in H$. Then $b = h'c$, hence $ab^{-1} = a(h'c)^{-1} = ac^{-1}h'^{-1} = h$ and thus $ac^{-1} = hh' \in H$, so that $a \sim_R c$. Therefore $\sim_R$ is an equivalence relation.

To show that $\sim_R$ satisfies (††), let $a, b \in G$ such that $a \sim_R b$ and $g \in G$ be arbitrary. From $a \sim_R b$ we know that $ab^{-1} \in H$. Then $a(gg^{-1})b^{-1} = (ag)(g^{-1}b^{-1}) = (ag)(bg)^{-1} \in H$ and thus $ag \sim_R bg$. □

7.10. ¬ Let G be a group, and $H \subseteq G$ a subgroup. With notation as in Exercise 6.7, show that H is normal in G if and only if $\forall \gamma \in \mathrm{Inn}(G), \gamma(H) \subseteq H$.

Conclude that if H is normal in G, then there is an interesting homomorphism $\mathrm{Inn}(G) \to \mathrm{Aut}(H)$. [8.25]

Solution. Suppose H is normal in G. Let $\gamma \in \mathrm{Inn}(G)$ be arbitrary. Then $\gamma = \gamma_g$ for some $g \in G$ and for all $a \in G$ we have $\gamma(a) = \gamma_g(a) = gag^{-1}$. Now since H is normal, for any $h \in H$ we have $\gamma(h) = ghg^{-1} \in H$ and thus $\gamma(H) \subseteq H$.

Now suppose that $\forall \gamma \in \mathrm{Inn}(G)$ we have $\gamma(H) \subset H$. Let $g \in G$ and $h \in H$ be arbitrary. There is an inner automorphism $\gamma_g \in \mathrm{Inn}(G)$ and we have $\gamma_g(h) = ghg^{-1} \in H$. But since that holds for every $g \in G$ and $h \in H$, H is normal in G.

If H is normal in G, we can see that for any $g \in G$ we have $\gamma_g(H) = gHg^{-1} = H$. Therefore $\gamma_g|_H$ is an automorphism of H. Thus we have a homomorphism $\mathrm{Inn}(G) \to \mathrm{Aut}(H)$ defined as $\gamma_g \mapsto \gamma_g|_H$. □

7.11. ▷ Let G be a group, and let $[G,G]$ be the subgroup of G generated by all elements of the form $aba^{-1}b^{-1}$. (This is the *commutator* subgroup of G; we will return to it in §IV.3.3.) Prove that $[G,G]$ is normal in G. (Hint: With notation as in Exercise 4.8, $g \cdot aba^{-1}b^{-1} \cdot g^{-1} = \gamma_g(aba^{-1}b^{-1})$.) Prove that $G/[G,G]$ is commutative.

Solution. Let h be any generator of $[G,G]$, so that $h = aba^{-1}b^{-1}$ for some $a, b \in G$. Assume $g \in G$ is arbitrary, notice that

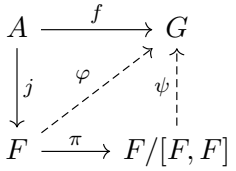
$$\begin{aligned}\gamma_g(h) &= ghg^{-1} \\ &= gaba^{-1}b^{-1}g^{-1} \\ &= gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} \\ &= \gamma_g(a)\gamma_g(b)\gamma_g(a^{-1})\gamma_g(b^{-1}) \\ &= \gamma_g(a)\gamma_g(b)(\gamma_g(a))^{-1}(\gamma_g(b))^{-1}.\end{aligned}$$

But that means $\gamma_g(h)$ maps to another generator of H and thus $\gamma_g(h) \in H$ for arbitrary $h \in H$. Exercise 7.10 implies H is normal in G.

Now consider the quotient group $G/[G,G]$. Let $a, b \in G$. We have $aba^{-1}b^{-1} \in [G,G]$ and thus $aba^{-1}b^{-1}[G,G] = [G,G]$, but then $ab[G,G] = ba[G,G]$ and therefore $G/[G,G]$ is commutative. □

7.12. ▷ Let $F = F(A)$ be a free group, and let $f : A \to G$ be a set-function from the set A to a *commutative* group G. Prove that f induces a unique homomorphism $F/[F,F] \to G$, where $[F,F]$ is the commutator subgroup of F defined in Exercise 7.11. (Use Theorem 7.12.) Conclude that $F/[F,F] \cong F^{ab}(A)$. (Use Proposition I.5.4.) [§6.4, 7.13, VI.1.20]

Solution. Consider the following commutative diagram:



By the universal property of free groups, the homomorphism $\varphi : F \to G$ indeed exists and is unique. Notice, that $[F,F] \subseteq \ker\varphi$, because G is commutative. Using Theorem 7.12 we see that ψ also exists and is unique. Thus f indeed induces a unique homomorphism $F/[F,F] \to G$.

But then $F/[F,F]$ (together with the set-function $\pi \circ j : A \to F/[F,F]$) satisfies the universal property of free abelian group on the set A and thus by Proposition I.5.4 we have $F/[F,F] \cong F^{ab}(A)$. □

7.13. ¬ Let A, B be sets and $F(A), F(B)$ the corresponding free groups. Assume $F(A) \cong F(B)$. If A is finite, prove that B is also and $A \cong B$. (Use Exercise 7.12 to upgrade Exercise 5.10) [5.10, VI.1.20]

Solution. By Exercise 7.12 we see that

$$F(A)/[F(A), F(A)] \cong F^{ab}(A)$$
$$F(B)/[F(B), F(B)] \cong F^{ab}(B).$$

Since $F(A) \cong F(B)$, we must also have $F(A)/[F(A), F(A)] \cong F(B)/[F(B), F(B)]$ (this follows from the basic properties of isomorphisms). Therefore we have $F^{ab}(A) \cong F^{ab}(B)$ and hence B must also be finite, and $A \cong B$. □

7.14. Let G be a group. Prove that $\mathrm{Inn}(G)$ is a *normal* subgroup of $\mathrm{Aut}(G)$.

Solution. Let $\gamma \in \mathrm{Inn}(G)$ and $\varphi \in \mathrm{Aut}(G)$. Since $\gamma \in \mathrm{Inn}(G)$ we know there is some $g \in G$ such that $\gamma = \gamma_g$. Let $a \in G$ be arbitrary. We have $\varphi \circ \gamma \circ \varphi^{-1}(a) = \varphi(g\varphi^{-1}(a)g^{-1}) = \varphi(g)a\varphi(g^{-1}) = \varphi(g)a(\varphi(g))^{-1}$. But that means that $\varphi \circ \gamma \circ \varphi^{-1} = \gamma_{\varphi(g)} \in \mathrm{Inn}(G)$ and thus $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$. □