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 $A, B \in \mathcal{P}(S)$, $A \sim B \iff A \subseteq B$. □

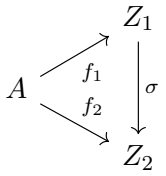
3.6.

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 $gf \in \mathrm{Hom}_{\mathsf{V}}(n, r)$.

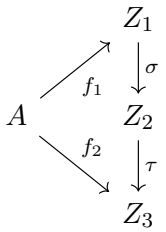
Now, to check that this makes V into a category, we also have to find the identity morphisms. For any $n \in \mathbb{N}$ there is surely the identity matrix with ones on the main diagonal and zeroes elsewhere, we will take this as the identity morphism. This is of course an identity with respect to the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

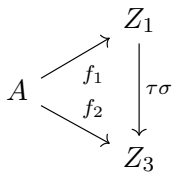
Solution. The category we are considering is similar to the opposite category of C_A, that is everything remains the same but the direction of the arrows change. This category is usually denoted as C^A. The objects of this category are the morphisms $f : A \to Z$ for some $Z \in \mathrm{Obj}(\mathsf{C})$.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

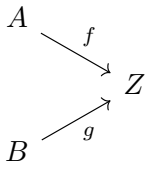
3.10.

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.

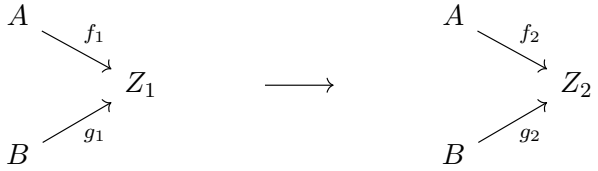
Solution. Lets start by defining the category $\mathsf{C}^{A,B}$:

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

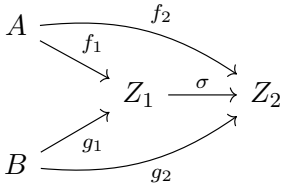


  in C, and

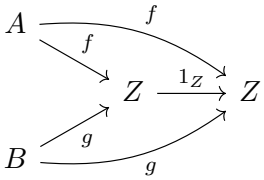
- morphisms



  are commutative diagrams

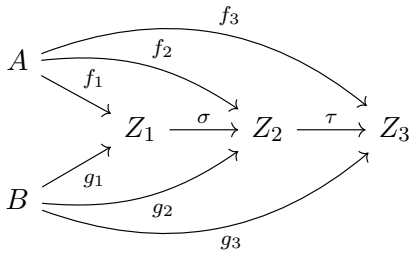


- The identity morphisms will be the diagrams

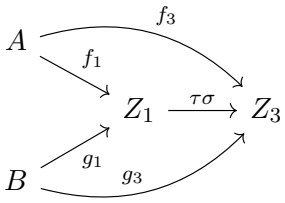


that must commute.

- 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.

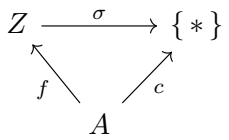
Solution. The final object of the category is, for example (note that any singleton will do), the object

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

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.

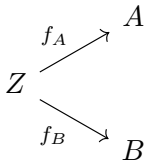
Solution. Suppose A', A'', B', B'' be sets such that $A' \cong A''$, $B' \cong B''$, $A' \cap A'' = \emptyset$ and $B' \cap B'' = \emptyset$. We will first show that $A' \cup B'$ is a coproduct of A' and B' in Set, then the same for $A'' \cup B''$, and finally, using Proposition I.5.4, we will conclude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

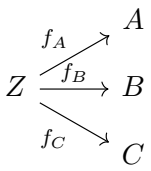
Solution. Let C be a category, and A, B objects of this category. Notice, that the universal property of a product $A \times B$ is based on the accessory category $\mathsf{C}_{A,B}$. Similarly, for $B \times A$, we have a category $\mathsf{C}_{B,A}$. However, these categories are equal - the objects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

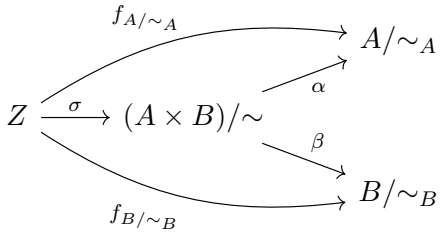
Products and coproducts of indexed sets of objects indeed exist in Set.

□

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

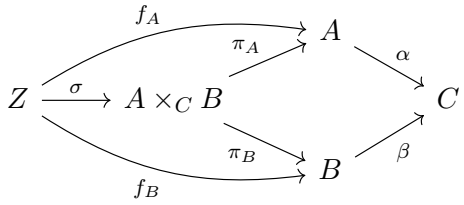
$$[(f_1([a]_{\sim_A}), g_1([b]_{\sim_B}))]_\sim = [(f_2([a]_{\sim_A}), g_2([b]_{\sim_B}))]_\sim.$$

  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

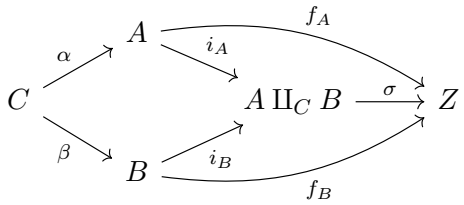


  commute.

  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

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

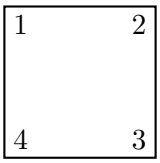
. Clearly, $\sigma^d = e$ and for any $m \leq d$ we have $\sigma^m \neq e$, as $(1)\sigma^m = (d)\sigma^{m-1} = (d-1)\sigma^{m-2} = \cdots = d-(m-1)$. Therefore σ has order d. □

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 relations 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. □

x

3. The category Grp

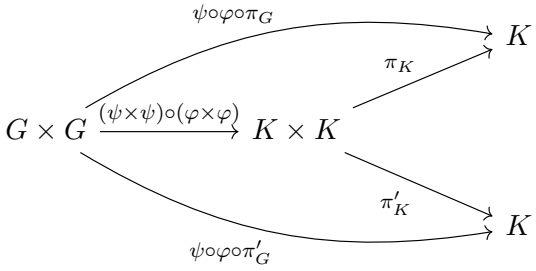
3.1.

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

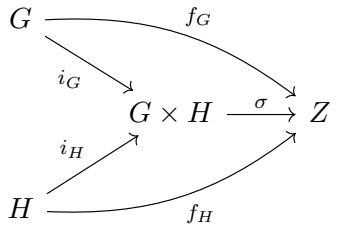
$$\begin{aligned} \pi_K \circ (\psi \times \psi) \circ (\varphi \times \varphi) &= \psi \circ \pi_H \circ (\varphi \times \varphi) \\ &= \psi \circ \varphi \circ \pi_G \end{aligned}$$

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 $G = H \times H \ldots$. 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. □

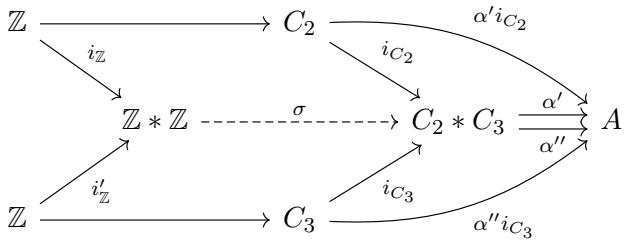
3.6.

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 $0 \leq i_0, i_1, \dots < 2$ and $0 \leq j_0, j_1 \dots < 3$ 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 $(\pi_m^n \pi_n)(z) = \pi_m^n([z]_n) = [z]_m = \pi_m(z)$ 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 $\mathrm{lcm}(m, n) \mid x$. But $\mathrm{lcm}(m, n) = mn$ 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 $\mathrm{Aut}_{\mathsf{Grp}}(C_n)$ 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 $\mathrm{Aut}_{\mathsf{Grp}}(C_n)$ 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.

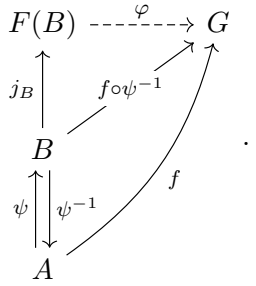
Solution. Let $\varphi : G \to H$ be an isomorphism. Assume G is commutative. Let $g, g' \in G$, $h, h' \in H$ be any elements such that $\varphi(g) = h, \varphi(g') = h'$. Then we have $hh' = \varphi(g)\varphi(g') = \varphi(gg') = \varphi(g'g) = \varphi(g')\varphi(g) = h'h$ and thus H is commutative.

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 $(\varphi + \psi)(a) := \varphi(a) + \psi(a)$.

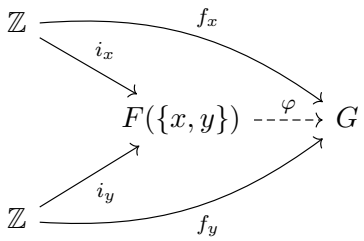
First, we have to check that the operation is well-defined. Let $\varphi, \psi \in H^{\oplus A}$. Then there are only finitely many $a \in A$ such that $\varphi(a) = e_H$ and $\psi(a) = e_H$ (not necessarily for the same elements of A however). Now notice that $(\varphi + \psi)(a) \neq e_H$ only when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

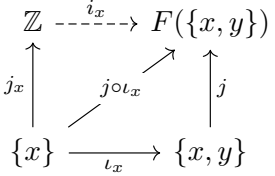
Thus $H^{\oplus A}$ is indeed a group with the operation $+$. □

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



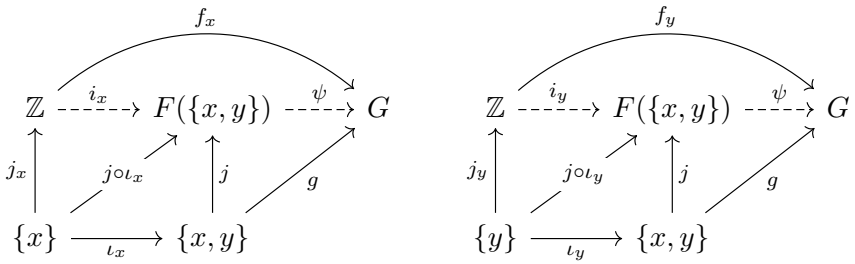
commute. The homomorphism i_x can be obtained by using the universal property of free groups, being the unique homomorphism making the natural diagram



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

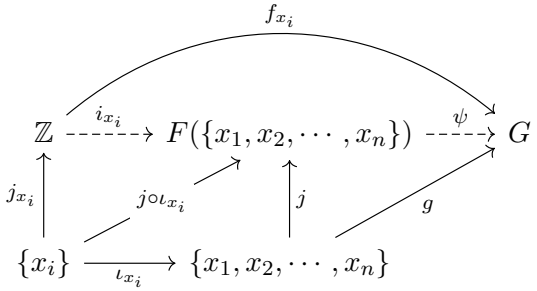


for some choice of a set-function g. The existence of ψ would follow from the universal property. But notice that such a function g is forced on us by the required commutativity of the two diagrams. We must have $g \circ \iota_x = f_x \circ j_x$ so that $g(x) = g \circ \iota_x(x) = f_x \circ j_x(x) = f_x(1)$ 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.

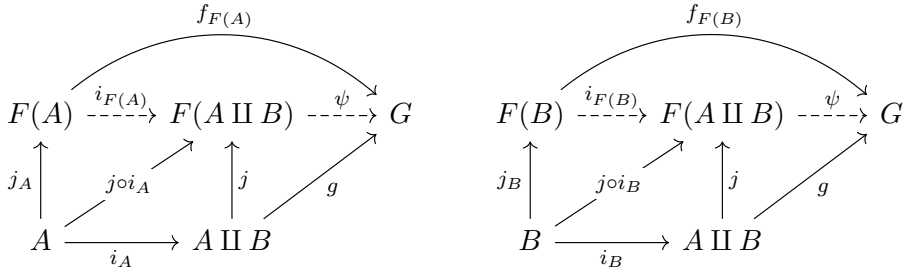
Now note that the situation for free *abelian* groups is entirely analogous. We know $F^{ab}(\{x_i\}) \cong \mathbb{Z}$. Therefore we can continue in the same sake as last time, replacing groups with abelian groups where needed and the coproduct in Grp with coproduct in Ab. Therefore $F^{ab}(\{x_1, x_2,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

5.8.

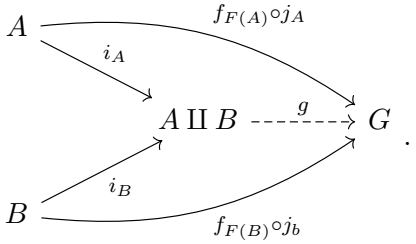
Solution. Generalizing the solutions to Problems II.5.6. and II.5.7. once more, we can consider the free (abelian) groups $F(A \amalg B)$ for some sets A, B.

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 $H_0 \subseteq H_1 \subseteq H_2 \subseteq \ldots$ 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 $\operatorname{Inn}(G)$ as the set of all inner automorphisms of G. Clearly $\operatorname{Inn}(G) \subseteq \operatorname{Aut}(G)$. Let $\gamma_g, \gamma_h \in \operatorname{Inn}(G)$ (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 $\gamma_g \circ \gamma_{h^{-1}} = \gamma_{gh^{-1}} \in \operatorname{Inn}(G)$. Therefore $\operatorname{Inn}(G)$ is a subgroup of $\operatorname{Aut}(G)$.

Now we shall prove that $\operatorname{Inn}(G)$ is cyclic if and only it is trivial if and only if G is abelian. Suppose $\operatorname{Inn}(G)$ 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 $(m_1, m_2, \ldots, m_n) = m_1(1,0,0,\ldots 0) + m_2(0,1,0,\ldots 0) + \cdots + m_n(0,0,0,\ldots,1)$ 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

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

But notice that $gh_i g^{-1}$ 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

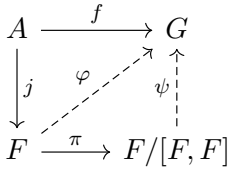
$$\begin{aligned}
\gamma_g(h) &= ghg^{-1} \\
&= gaba^{-1}b^{-1}g^{-1} \\
&= gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} \\
&= \gamma_g(a)\gamma_g(b)\gamma_g(a^{-1})\gamma_g(b^{-1}) \\
&= \gamma_g(a)\gamma_g(b)(\gamma_g(a))^{-1}(\gamma_g(b))^{-1}.
\end{aligned}$$

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 $\mathrm{Aut}(G)$. □

8. Canonical decomposition and Lagrange's theorem

8.1. If a group H may be realized as a subgroup of two groups G_1 and G_2 and if

$$\frac{G_1}{H} \cong \frac{G_2}{H}$$

does it follow that $G_1 \cong G_2$? Give a proof or a counterexample.

Solution. A counterexample is given in the text. Consider $H = C_3$, $G_1 = C_6$, and $G_2 = D_6$. We have $C_6/C_3 \cong C_2$ and $D_6/C_3 \cong C_2$. However, $C_6 \ncong D_6$. This can be seen for example from the respective presentations $(x|x^6)$ and $(x, y|x^2, y^3, xyxy)$. □

8.2. ¬ Extend Example 8.6 as follows. Suppose G is a group and $H \subseteq G$ is a subgroup *of index* 2, that is, such that there are precisely two (say, left-) cosets of H in G. Prove that H is normal in G. [9.11, IV.1.16]

Solution. Consider the set-function $\varphi : G \to C_2$ defined such that $\varphi(g)$ is mapped to the identity of C_2 if $gH = H$ and to the other element, say of C_2 otherwise. Clearly, φ is a group homomorphism as $\varphi(gh)$ is equal to the identity of C_2 if and only if $ghH = H$ which holds only if both $gH = H$ and $hH = H$. $\ker\varphi = H$, as for any $g \notin H$, $gH \neq H$ (as $e_G \in H$, hence $g \in gH$). Thus H is normal in G. □

8.3. Prove that every finite group is finitely presented.

Solution. Let G be a finite group. We can build a presentation of G by taking the set of all the elements of G and $g_i g_j g_k^{-1}$ as the relations, where $g_i g_j = g_k$. Since the underlying set of G is finite, so is its multiplication table. Thus in fact G can be finitely presented. □

8.4. Prove that $(a, b|a^2, b^2, (ab)^n)$ is a presentation of the dihedral group D_{2n}. (Hint: With respect to the generators defined in Exercise 2.5, set $a = x$ and $b = xy$; prove you can get the relations given here from the ones obtained in Exercise 2.5, and conversely.)

Solution. In Exercise 2.5 we have seen that D_{2n} is generated by two elements x and y with the relations $x^2 = e$ and $y^n = e$. Setting $a = x$ and $b = xy$, we can see that $a^2 = e$, $b^2 = xyxy$ which we have shown is the identity, hence $b^2 = e$. Now $(ab)^n = (xxy)^n = y^n = e$. Therefore we have reconstructed the relations $a^2, b^2, (ab)^n$ from the relations x^2 and $y^n = e$.

Conversely, consider the group with the given presentation. Set $x = a$ and $y = ab$. Then $x^2 = e$ and $y^n = (ab)^n = e$ as needed. □

8.5. Let a, b be distinct elements of order 2 in a group G, and assume that ab has finite order $n \geq 3$. Prove that the subgroup generated by a and b in G is isomorphic to the dihedral group D_{2n}. (Use the previous exercise.)

Solution. The subgroup generated by a and b is by definition image of the homomorphism $\varphi : F(a, b) \to G$. Because a and b have order 2, we have $a^2 = b^2 = e$. We also know that ab has order $n \geq 3$ and thus $(ab)^n = e$. In particular, this means that every element of $\operatorname{im} \varphi$ has the form $b^i(ab)^j a^k$ where $0 \leq i, k < 2$ and $0 \leq j < n$. Thus in fact it can be presented as $(a, b|a^2, b^2, (ab)^n)$ and is therefore isomorphic to D_{2n} by Exercise 8.5. □

8.6. ¬ Let G be a group, and let A be a set of generators for G; assume A is finite. The corresponding *Cayley graph* is a directed graph whose set of vertices is in one-to-one correspondence with G, and two vertices g_1, g_2 are connected by an edge if $g_2 = g_1 a$ for some $a \in A$; this edge may be labeled a and oriented from g_1 to g_2. For example, the graph drawn in Example 5.3 for the free group $F(x, y)$ on two generators x, y is the corresponding Cayley graph (with the convention that horizontal edges are are labeled x and point to the right and vertical edges are labeled y and point up).

Prove that if a Cayley graph of a group is a tree, then the group is free. Conversely, prove that free groups admit Cayley graphs that are trees. [§5.3, 9.15]

Solution. Let G be a group with a finite set of generators A. First, suppose that its Cayley graph is a tree, hence acyclic. In particular, every $g \in G$ corresponds to a single vertex of the graph. Since the graph is acyclic, there is a single path from the the vertex corresponding to e_G to g, with labels taken from A. Thus $g = a_1 a_2 \cdots a_n$, $a_i \in A$ for $1 \leq i \leq n$. Every element of G is therefore a product of the generators where no simplification is possible, hence G is a free group.

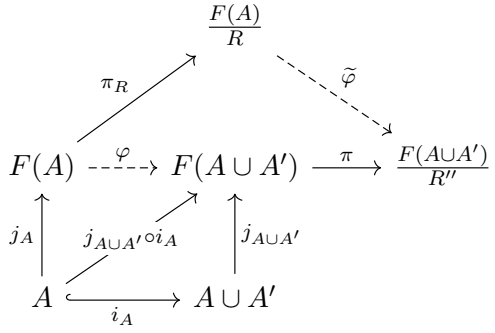
Conversely, assume that G is a free group. Then every $g \in G$ is a product $a_1 a_2 \cdots a_n$, $a_i \in A$ for $1 \leq i \leq n$. Therefore we have a single path from e_G to g in the corresponding Cayley graph labeled with $a_1 a_2 \cdots a_n$. Now if g_1, g_2 are vertices of the graph (and thus elements of G), we have a single path from e to g_1 and from e to g_2 and thus there is only a single path from g_1 to g_2 if we ignore directions in the graph. Thus the graph is a tree. □

8.7. ▷ Let $(A|\mathscr{R})$, resp., $(A'|\mathscr{R}')$, be a presentation for a group G, resp., G' (cf §8.2); we may assume A, A' are disjoint. Prove that the group $G * G'$ presented by

$$(A \cup A' \mid \mathscr{R} \cup \mathscr{R}')$$

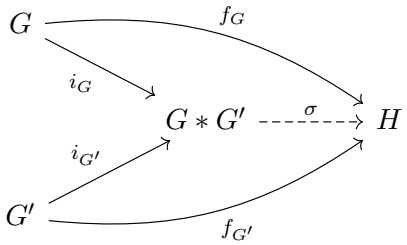
satisfies the universal property for the *coproduct* of G and G' in Grp. (Use the universal properties of both free groups and quotients to construct natural homomorphisms $G \to G * G'$, $G' \to G * G'$.) [§3.4, §8.2, 9.14]

Solution. Let us denote R, R', and R'' as the smallest normal subgroups of $F(A)$, $F(A')$, and $F(A \cup A')$, such that R contains $\mathscr{R}$, R' contains $\mathscr{R}'$, and R'' contains $\mathscr{R} \cup \mathscr{R}'$. Then we have $G = F(A)/R$, $G' = F(A')/R'$, and $G * G' = F(A \cup A')/R''$. Consider the diagram



which we shall show is commutative. φ is the unique homomorphism making the lower diagram commute which exists by the universal property of free groups. Therefore we have a homomorphism $\pi \circ \varphi : F(A) \to F(A \cup A')/R''$. Does $R \subseteq \ker \pi \circ \varphi$? $\ker \pi = R''$ and by definition R'' is the smallest normal subgroup of $F(A \cup A')$ which contains $\mathscr{R} \cup \mathscr{R}'$. In particular, every word $r_\alpha \in \mathscr{R}$ must be mapped to itself by φ and thus if $r \in R$, $\varphi(r) \in R''$. Hence $R \subseteq \ker \pi \circ \varphi$ and therefore $\widetilde{\varphi}$ is the unique homomorphism making the upper diagram commute by the universal property of quotients. Denote this homomorphism as i_G and note it is a homomorphism $G \to G * G'$. The process for producing a natural homomorphism $i_{G'} : G' \to G * G'$ is entirely analogous.

Let H be any group, and $f_G : G \to H$, $f_{G'} : G' \to H$ homomorphisms. We have to show that there is a unique homomorphism $\sigma : G * G' \to H$ making the diagram



commute. Define a homomorphism $\psi : F(A \cup A') \to H$ as $\psi(a) = f_G \circ \pi_R \circ j_A(a)$ for $a \in A$ and $\psi(a) = f_{G'} \circ \pi_{R'} \circ j_{A'}(a)$ for $a \in A'$. ψ is well-defined as A and A' are disjoint by assumption. Suppose that $r \in R''$. We want to show that $\psi(r) = e_H$ and thus $R'' \subseteq \ker \psi$. Again, by definition of R'', we know that r is a product of words from $\mathscr{R} \cup \mathscr{R}'$, say $r = r_1 r_2 \cdots r_n$ where $r_i \in \mathscr{R} \cup \mathscr{R}'$ for $1 \leq i \leq n$. Clearly, each r_i is either a word from $\mathscr{R}$ or $\mathscr{R}'$, and we have $\psi(r_i) = e_H$ as $\pi_R(r_i) = e_G$. Thus $\psi(r) = e_H$. Hence we have a unique induced homomorphism $\sigma : G * G' \to H$ by the universal property of quotients such that $\psi = \sigma \circ \pi$.

It remains to show that σ makes the diagram commute, so that $f_G = \sigma \circ i_G$ and $f_{G'} = \sigma \circ i_{G'}$. We have

$$\begin{aligned}\psi = \sigma \circ \pi &\Longrightarrow \psi \circ \varphi = \sigma \circ \pi \circ \varphi \\ &\Longrightarrow \psi \circ \varphi = \sigma \circ i_G \circ \pi_R \\ &\Longrightarrow \psi \circ \varphi \circ j_A = \sigma \circ i_G \circ \pi_R \circ j_A \\ &\Longrightarrow \psi \circ j_{A \cup A'} \circ i_A = \sigma \circ i_G \circ \pi_R \circ j_A.\end{aligned}$$

For all $a \in A$ we thus have $\psi(a) = \sigma \circ i_G \circ \pi_R(a)$, but $\psi(a) = f_G \circ \pi_R \circ j_A(a) = f_G \circ \pi_R(a)$. π_R is a surjection, hence an epimorphism, and therefore we must have $f_G = \sigma \circ i_G$ as was to be shown. Similarly for $f_{G'} = \sigma \circ i_{G'}$. Thus $G * G'$ indeed satisfies the universal property of the coproduct of G and G' in Grp. □

8.8. ¬ (If you know about matrices (cf. Exercise 6.1).) Prove that $\mathrm{SL}_n(\mathbb{R})$ is a *normal subgroup* of $\mathrm{GL}_n(\mathbb{R})$, and 'compute' $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$ as a well-known group. [VI.3.3]

Solution. Consider a set-function $\varphi : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*$, defined as $\varphi(M) = \det(M)$. Clearly, this function is a homomorphism of the corresponding groups, as if $M_1, M_2 \in \mathrm{GL}_n(\mathbb{R})$, $\varphi(M_1 M_2) = \det(M_1 M_2) = \det(M_1)\det(M_2) = \varphi(M_1)\varphi(M_2)$. It is surjective, as for any $r \in R^*$ we can construct a matrix M with $\det(M) = r$.

$\ker \varphi = \mathrm{SL}_n(\mathbb{R})$ by definition of $\mathrm{SL}_n(\mathbb{R})$. Thus $\mathrm{SL}_n(\mathbb{R})$ is normal in $\mathrm{GL}_n(\mathbb{R})$ and we have $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) = \mathbb{R}^*$. Geometrically, $\mathrm{SL}_n(\mathbb{R})$ are matrices describing linear transformations which do not change the volume. Thus $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$ can be seen as all the various volume scaling factors of linear transformations. □

8.9. ¬ (Ditto.) Prove that $\mathrm{SO}_3(\mathbb{R}) \cong \mathrm{SU}(2)/\{\pm I_2\}$, where I_2 is the identity matrix. (Hint: It so happens that every matrix in $\mathrm{SO}_3(\mathbb{R})$ can be written in the form

$$\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$ and $a^2+b^2+c^2+d^2 = 1$. Proving this fact is not hard, but at this stage you will probably find it computationally demanding. Feel free to assume this, and use Exercise 6.3 to construct a surjective homomorphism $\mathrm{SU}(2) \to \mathrm{SO}_3(\mathbb{R})$; compute the kernel of this homomorphism.)

If you know a little topology, you can now conclude that the fundamental group of $\mathrm{SO}_3(\mathbb{R})$ is C_2. [9.1, VI.1.3]

Solution. Assuming the stated fact about $\mathrm{SO}_3(\mathbb{R})$, we can construct a homomorphism $\varphi : \mathrm{SU}(2) \to \mathrm{SO}_3(\mathbb{R})$ as follows. Let $M \in \mathrm{SU}(2)$. Then we can always rewrite it to the form

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$ and $a^2 + b^2 + c^2 + d^2 = 1$ (by Exercise 6.3). Define $\varphi(M)$ to be a matrix of the form described in the problem, with a, b, c, d taken from the rewritten matrix M. We have to show that φ is in fact a homomorphism. Let $M_1, M_2 \in \mathrm{SU}(2)$. We then have... □

8.10. View $\mathbb{Z} \times \mathbb{Z}$ as a subgroup of $\mathbb{R} \times \mathbb{R}$. Describe the quotient

$$\frac{\mathbb{R} \times \mathbb{R}}{\mathbb{Z} \times \mathbb{Z}}$$

in terms analoguous to those used in Example 8.7. (Can you 'draw a picture' of this group? Cf. Exercise I.1.6.)

Solution. Taking our cue from Example 8.7, consider the group $S^1 \times S^1$. Abstractly, we could invoke the universal property of products to get a homomorphism $\rho : \mathbb{R} \times \mathbb{R} \to S^1 \times S^1$. Concretely, we can define this as $\rho(r_1, r_2) = (2\pi r_1, 2\pi r_2)$. Clearly, $\rho(r_1, r_2) = (0, 0)$ for all integer values of r_1 and r_2, so $\ker \rho = \mathbb{Z} \times \mathbb{Z}$. Therefore by Corollary 8.2 we have

$$\frac{\mathbb{R} \times \mathbb{R}}{\mathbb{Z} \times \mathbb{Z}} \cong S^1 \times S^1.$$

We can identify S^1 as a circle. Similarly we can identify $S^1 \times S^1$ with the torus - one circle going around one axis and the other circle going perpendicularly. □

8.11. (Notation as in Proposition 8.10.) Prove 'by hand' (that is, without invoking universal properties) that N is normal in G if and only if N/H is normal in G/H.

Solution. Let H be a normal subgroup of a group G, and let N be a subgroup of G containing H. Suppose that N is normal in G. Since $H \subseteq N$, H is normal in N. Consider the function $\varphi : G/H \to G/N$ defined as $\varphi(gH) = gN$. Clearly, this is a homomorphism as $\varphi(gHg'H) = \varphi((gg')H) = (gg')N = gNg'N = \varphi(gH)\varphi(g'H)$. What is $\ker \varphi$? $\varphi(gH) = 1_G N$ only if $gN = 1_G N = N$. hence if $g \in N$. We know H is normal in N and thus we have a quotient N/H, which is a subgroup of G/H. The elements of N/H are then the cosets nH for $n \in N$. Thus $\ker \varphi = N/H$ and thus N/H is normal in G/H.

Now let N/H be normal in G/H. We then have two quotient homomorphisms $\pi : G \to G/H$ and $\pi' : G/H \to \frac{G/H}{N/H}$. Consider the homomorphism $\pi' \circ \pi : G \to \frac{G/H}{N/H}$. $\ker \pi' = N/H$. $\pi(g) \in N/H$ if $g \in N$ and thus $\ker \pi' \circ \pi = N$, therefore N is normal in G. □

8.12. (Notation as in Proposition 8.11.) Prove 'by hand' (that is, by using Proposition 6.2) that HK is a subgroup of G if H is normal.

Solution. Let H be a normal subgroup of G. Let $a, b \in HK$, so that $a = h_1k_1$, $b = h_2k_2$ for some $h_1, h_2 \in H$, $k_1, k_2 \in K$. We then have $ab^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1} = h_1kh_2^{-1}$ for some $k \in K$. Now $kh_2^{-1} \in kH = Hk$ (because H is normal in G) and thus there is some $h \in H$ such that $kh_2^{-1} = hk$. This implies $ab^{-1} = h_1(hk) = (h_1h)k \in HK$ and thus HK is a subgroup of G. □

8.13. ¬ Let G be a finite group, and assume $|G|$ is odd. Prove that every element of G is a square. [8.14]

Solution. As a consequence of Lagrange's theorem, the order $|g|$ of any element $g \in G$ divides $|G|$ and hence must be odd. Let $g \in G$, $n = |g|$. As noted, n is odd and hence there is an element $h = g^{\frac{n+1}{2}}$ such that $h^2 = g^{n+1} = g$. Thus every element of G is a square. □

8.14. Generalize the result of Exercise 8.13: if G is a group of order n and k is an integer relatively prime to n, then the function $G \to G$, $g \mapsto g^k$ is surjective.

Solution. Let $\varphi : G \to G$, $\varphi(g) = g^k$. Since $\gcd(k, n) = 1$, there are integers a, b such that $ak + bn = 1$. Let $h \in G$. Then there is an element $g = h^a$, $\varphi(g) = g^k = h^{ak} = h^{1-bn} = hh^{-bn}$. By Lagrange's theorem, we have that $|h|$ divides n, hence in particular $n = x\,|h|$ for some integer x and therefore $h^n = h^{x|h|} = (h^{|h|})^x = e_G^x = e_G$. This implies $h^{-bn} = (h^n)^{-b} = e_G^{-b} = e_G$ and thus $\varphi(g) = h$. Therefore φ is surjective. □

8.15. Let a, n be positive integers, with $a > 1$. Prove that n divides $\phi(a^n - 1)$, where ϕ is Euler's ϕ-function; see Exercise 6.14. (Hint: Example 8.15)

Solution. Let $m = a^n - 1$. Consider the group $G = (\mathbb{Z}/m\mathbb{Z})^*$. By definition, $|G| = \phi(m)$. We have $\gcd(a, m) = \gcd(a, a^n - 1) = 1$, hence $[a]_m \in G$. We want to show that the order of $[a]_m$ in G is n. Notice that $a^n - 1 \equiv 0 \mod m$, hence $a^n \equiv 1 \mod m$, and thus $[a]_m^n = [1]_m$. Let $i < n$ be an integer. Then $a^i < a^n$, which implies $a^i - 1 < a^n - 1$, and thus $a^i \not\equiv 1 \mod m$. Therefore n is the smallest integer such that $[a]_m^n = [1]_m$, hence $|[a]_m| = n$ in G. By Lagrange's theorem it follows that n divides $\phi(a^n - 1)$. □

8.16. Generalize Fermat's little theorem to congruences modulo arbitrary (that is, possibly nonprime) integers. Note that it is *not* true that $a^n \equiv a \mod n$ for all a and n: for example, 2^4 is not congruent to 2 modulo 4. *What* is true? (This generalization is known as Euler's theorem.)

Solution. The proof of Fermat's little theorem is build on the fact that p is prime and therefore we have $[a]_p^{p-1} = [1]_p$. In general, if n is a positive integer, $(\mathbb{Z}/n\mathbb{Z})^*$ does not have to contain the class $[a]_n$, as $\gcd(a, n)$ does not have to equal 1. However, if a and n are coprime, $[a]_n$ is indeed an element of $(\mathbb{Z}/n\mathbb{Z})^*$ and thus in particular the order of $[a]_n$

divides $\phi(n)$ by Lagrange's theorem. Therefore $[a]_n^{\phi(n)} = [1]_n$. Hence $a^{\phi(n)} = 1 \mod n$ whenever a and n are coprime. □

8.17. ▷ Assume G is a finite abelian group, and let p be a prime divisor of $|G|$. Prove that there exists an element in G of order p. (Hint: Let $g \neq e$ be an element of G, and consider the subgroup $\langle g \rangle$; use the fact that this subgroup is cyclic to show that there is an element $h \in \langle g \rangle$ of *prime order* q. If $q = p$, you are done; otherwise, use the quotient $G/\langle h \rangle$ and induction.) [§8.5, 8.18, 8.20, §IV.2.1]

Solution. Let G be a finite abelian group, p a prime divisor of $|G|$. Let $g \in G$, $g \neq e$, and consider the subgroup $\langle g \rangle$. Notice, that we can factor the order of g into its prime divisors. Thus there is at least one element h_0 of $\langle g \rangle$ of prime order q. If $q = p$, we are done. If not, consider the quotient group $H_0 = G/\langle h_0 \rangle$ ($\langle h_0 \rangle$ is normal in G because G is abelian). The order of H_0 is then equal to $\frac{|G|}{|h|}$. We can again take an element g_0 of H_0, consider the subgroup $\langle g_0 \rangle$, find an element h_1 of this group of prime order and compare its order to p. If it is not equal, we can again consider the quotient $H_1 = H_0/\langle h_1 \rangle$.

We can continue this process inductively until we get an element h_i of order p. This works because p divides $|G|$, and therefore some $H_i = H_{i-1}/\langle h_i \rangle$ must have order p (because the order of H_i is equal to $\frac{|G|}{|h_0|\cdots|h_i|}$ by Lagrange's theorem), hence necessarily be cyclic group of order p, and thus contain an element h_{i+1} of order p.

We then have a composition of quotient homomorphisms $\pi = \pi_i \circ \pi_{i-1} \circ \cdots \circ \pi_0 : G \to H_i$, which is surjective. That means that there is some $x \in G$ such that $\pi(x) = h_{i+1}$. Because π is a homomorphism, the order of $\pi(x)$ necessarily divides the order of x. Thus $|x| = ap$ for some integer a. But that means $x^{\frac{|x|}{a}}$ has order p in G. □

8.18. Let G be an abelian group of order $2n$, where n is odd. Prove that G has *exactly one* element of order 2. (It has at least one, for example by Exercise 8.17. Use Lagrange's theorem to establish that it cannot have more than one.) Does the same conclusion hold if G is not necessarily commutative?

Solution. Using Exercise 8.17 we know that G contains an element of order 2, say g. $\langle g \rangle$ is normal in G as G is abelian. Consider $H = G/\langle g \rangle$. By Lagrange's theorem, the order of H is n, hence odd. But, again by Lagrange's theorem, that means that the order of all elements of H is odd. Thus no element other than g can have order 2 in G. (To see this notice that $\pi : G \to H$ is a homomorphism, and the order $\pi(h)$ for any $h \in G$ divides $|h|$.)

No, if G is not commutative this does not hold. The simplest counterexample is the dihedral group D_6 of order $6 = 2 \cdot 3$. There are three distinct reflections about a line of a triangle, each is an element of D_6 of order 2. □

8.19. Let G be a finite group, and let d be a proper divisor of $|G|$. Is it necessarily true that there exists an element of G of order d? Give a proof or a counterexample.

Solution. No, this is not true. Consider the group S_4 of order 24. 12 is a proper divisor of 24 but there is clearly no element of S_4 of this order. □

8.20. ▷ Assume G is a finite abelian group, and let d be a divisor of $|G|$. Prove that there exists a *subgroup* $H \subseteq G$ of order d. (Hint: induction; use Exercise 8.17.) [§IV.2.2]

Solution. We will prove this using strong induction on the order of G. Suppose $|G| = 1$. Then the only divisor is 1 and clearly G itself is the subgroup with order 1.

Now suppose that the statement holds for all groups of $k < n$ for some n and consider a group a G with $|G| = n$. Let $d \neq 1$ (for $d = 1$ we can take the trivial subgroup) be a divisor of n. Let p be a prime number such that $d = kp$ for some integer k. p divides n and therefore by Exercise 8.17 there is an element $x \in G$ of order p and a corresponding subgroup $\langle x \rangle$ of order p.

$\langle x \rangle$ is normal in G because G is abelian, and thus we have a quotient group $G/\langle x \rangle$. The order of this group is smaller than n, therefore it satisfies the induction hypothesis. k divides the order of $G/\langle x \rangle$ and thus there is a subgroup of order k of $G/\langle x \rangle$. By the third isomorphism theorem there is thus a subgroup K of G such that K contains $\langle x \rangle$ and $K/\langle x \rangle$ is the subgroup of $G/\langle x \rangle$ of order k. In particular, we have $|K| = |K/\langle x \rangle| \cdot |\langle x \rangle| = kp = d$. Thus the statement holds for n, completing the proof. □

8.21. ▷ Let H, K be subgroups of a group G. Construct a bijection between the set of cosets hK with $h \in H$ and the set of left-cosets of $H \cap K$ in H. If H and K are finite, prove that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

[§8.5, §iV.4.4]

Solution. Define a function $f : HK/K \to H/(H \cap K)$ as $f(hK) = h(H \cap K)$. We have to prove that it is well-defined. Let $h_1K = h_2K$, we need to show that $f(h_1K) = f(h_2K)$. $h_1K = h_2K$ implies $h_2^{-1}h_1 \in K$, hence $h_2^{-1}h_1 \in H \cap K$, and thus $h_1(H \cap K) = h_2(H \cap K)$. Therefore $f(h_1K) = f(h_2K)$ as desired.

To see that this is an injection, suppose that $f(h_1K) = f(h_2K)$ for some $h_1, h_2 \in H$. Then we have $h_1(H \cap K) = h_2(H \cap K)$, hence $h_2^{-1}h_1 \in H \cap K$, and thus $h_2^{-1}h_1 \in K$. Therefore $h_1K = h_2K$.

To see that it is surjective, assume $h(K \cap H) \in H/(H \cap K)$. Then $f(hK) = h(H \cap K)$ as needed.

Assume H and K are finite. Then the number of cosets of K in HK is $|HK|/K$ (notice that any such coset is equal to $(hk)K = hK$ for some $h \in H, k \in K$). The size of

$H/(H \cap K)$ is $|H| / |H \cap K|$. Since both of those sets are finite and we have shown that they are isomorphic, we have $|HK| / K = |H| / |H \cap K|$ and thus $|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$. □

8.22. ▷ Let $\varphi : G \to G'$ be a group homomorphism, and let N be the smallest normal subgroup containing $\operatorname{im} \varphi$. Prove that G'/N satisfies the universal property of $\operatorname{coker} \varphi$ in Grp.

Solution. Let L be a group and $\alpha : G' \to L$ a homomorphism such that $\alpha \circ \varphi = 0$. $\alpha \circ \varphi = 0$ implies $\operatorname{im} \varphi \subseteq \ker \alpha$. $\ker \alpha$ is a normal subgroup of G', thus we must have $N \subseteq \ker \alpha$ as N is the minimal normal subgroup containing $\operatorname{im} \varphi$. Using the universal property of quotients, we obtain a unique homomorphism $\tilde{\alpha} : G/N \to G'$, proving that G/N (with the quotient homomorphism) satisfies the universal property of cokernels in Grp. □

8.23. ▷ Consider the subgroup

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

of S_3. Show that the cokernel of the inclusion $H \hookrightarrow S_3$ is trivial, although $H \hookrightarrow S_3$ is not surjective. [§8.6]

Solution. By Exercise 8.22, cokernel of the inclusion is the quotient S_3/N where N is the smallest normal subgroup containing H. As we have seen in Exercise 7.1, there is only a single normal subgroup of S_3 not equal to the trivial group or the entire S_3. H is not a subset of this normal group and thus $N = S_3$, therefore the cokernel S_3/S_3 is trivial. However, the inclusion is clearly not surjective. □

8.24. ▷ Show that epimorphisms in Grp do not necessarily have right-inverses. [§I.4.2]

Solution. Consider the homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $\varphi(n) = [n]_2$. Let G be any group and $\beta', \beta'' : \mathbb{Z}/2\mathbb{Z} \to G$ homomorphisms. Suppose $\beta' \circ \varphi = \beta'' \circ \varphi$. Then in particular $\beta'([0]_n) = \beta''([0]_n)$ and $\beta'([1]_n) = \beta''([1]_n)$, hence $\beta' = \beta''$ and thus φ is an epimorphism.

However, notice that there are no non-trivial homomorphisms $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$. To see this, notice that the image of $[1]_n$ would have to divide its order, 2. But all non-identity elements of $\mathbb{Z}$ have infinite order. □

8.25. Let H be a commutative normal subgroup of G. Construct an interesting homomorphism from G/H to $\operatorname{Aut}(H)$. (Cf. Exercise 7.10.)

Solution. By Exercise 7.10 there is a homomorphism $\mathrm{Inn}(G) \to \mathrm{Aut}(H)$ defined as $\gamma_g \mapsto \gamma_g|_H$. Consider the homomorphism $\varphi : G \to \mathrm{Aut}(H)$ defined as the composition of $g \mapsto \gamma_g$ and $\gamma_g \mapsto \gamma_g|_H$.

Let $h \in H$. We have $\varphi(h) = \gamma_h|_H$. Thus for all h' we must have $\varphi(h)(h') = \gamma_h|_H(h')$. $\gamma_h|_H(h') = hh'h^{-1} = hh^{-1}h' = h'$ because H is abelian. Thus $\varphi(h) = id_H$ and therefore $H \subseteq \ker\varphi$.

By the universal property of quotients we then have an induced homomorphism $\tilde{\varphi} : G/H \to \mathrm{Aut}(H)$. □

9. Group actions

9.1. (One more, if you are already familiar with a little linear algebra...) The matrix groups listed in Exercise 6.1 all come with evident actions on a vector space: if M is an $n \times n$ matrix with (say) real entries, multiplication to the right by a column n-vector $\mathbf{v}$ returns a column n-vector $M\mathbf{v}$, and this defines a left-action on $\mathbb{R}^n$ viewed as the space of column n-vectors.

- Prove that, through this action, matrices $M \in \mathrm{O}_n(\mathbb{R})$ preserve lengths and angles in $\mathbb{R}^n$.
- Find an interesting action of $\mathrm{SU}(2)$ on $\mathbb{R}^3$. (Hint: Exercise 8.9.)

Solution.

- Let $M \in \mathrm{O}_n(\mathbb{R})$ and $\mathbf{v}$ be a n-vector. First, we want to show that $||M\mathbf{v}|| = ||\mathbf{v}||$. We have $||M\mathbf{v}|| = M\mathbf{v} \cdot M\mathbf{v} = (M\mathbf{v})^t(M\mathbf{v}) = \mathbf{v}^t M^t M\mathbf{v} = \mathbf{v}^t I_n \mathbf{v} = \mathbf{v}^t\mathbf{v} = \mathbf{v} \cdot \mathbf{v} = ||\mathbf{v}||$ (by viewing $\mathbf{v}$ as a $n \times 1$ matrix).

  Now let $\mathbf{w}$ be n-vector. We know that $\cos\theta = \frac{\mathbf{v}\cdot\mathbf{w}}{||\mathbf{v}||||\mathbf{w}||}$. We have $\frac{M\mathbf{v}\cdot M\mathbf{w}}{||M\mathbf{v}||||M\mathbf{w}||} = \frac{M\mathbf{v}\cdot M\mathbf{w}}{||\mathbf{v}||||\mathbf{w}||}$ because multiplication by M preserves lengths. We also have $M\mathbf{v} \cdot M\mathbf{w} = (M\mathbf{v})^t(M\mathbf{w}) = \mathbf{v}^t M^t M\mathbf{w} = \mathbf{v}^t I_n \mathbf{w} = \mathbf{v}^t\mathbf{w} = \mathbf{v} \cdot \mathbf{w}$. And thus multiplication by M also preserves angles as we wanted to show.
- In Exercise 8.9 we have constructed a surjective homomorphism $\varphi : \mathrm{SU}(2) \to \mathrm{SO}_3(\mathbb{R})$. By definition, an action is in fact a group homomorphism $G \to \mathrm{Aut}_{\mathsf{C}}(A)$ for some object A of a category C. We have a (left-)action of $\mathrm{SO}_3(\mathbb{R})$ on the set $\mathbb{R}^3$, and thus a homomorphism $\sigma : \mathrm{SO}_3(\mathbb{R}) \to \mathrm{Aut}_{\mathsf{Set}}(\mathbb{R}^3)$. Therefore $\sigma \circ \varphi : \mathrm{SU}(2) \to \mathrm{Aut}_{\mathsf{Set}}(\mathbb{R}^n)$ is also a homomorphism representing an action of $\mathrm{SU}(2)$ on $\mathbb{R}^3$. For $M \in \mathrm{SU}(2)$, $\mathbf{v} \in \mathbb{R}^3$ we thus have an action defined as $M\mathbf{v} = \varphi(M)\mathbf{v}$. □

9.2. The effect of the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

on the plane is to respectively flip the plane about the x-axis and to rotate it 90° clockwise about the origin. With this in mind, construct an action of D_8 on $\mathbb{R}^2$.

Solution. First, note that the presentation of D_8 is $(x, y \mid x^2, y^4, xyxy)$. Using this we can identify D_8 with the group generated by the two given matrices, setting x as the matrix flipping the plane (which has order 2) and y as the matrix rotating it by 90° clockwise (with order 4). Clearly $xyxy = I_2$. This provides us with a natural action of D_8 on $\mathbb{R}_2$ by matrix multiplication. □

9.3. ▷ If $G = (G, \cdot)$ is a group, we can define an 'opposite' group $G^\circ = (G, \bullet)$ supported on the same set G, by prescribing

$$(\forall g, h \in G): \quad g \bullet h = h \cdot g.$$

- Verify that G° is indeed a group.
- Show that the 'identity': $G^\circ \to G$, $g \mapsto g$ is an isomorphism if and only if G is commutative.
- Show that $G^\circ \cong G$ (even if G is not commutative!).
- Show that giving a *right*-action of G on a set A is the same as giving a homomorphism $G^\circ \to S_A$, that is, a *left*-action of G° on A.
- Show that the notions of left- and right-actions coincide 'on the nose' for *commutative* groups. (That is, if $(g, a) \mapsto ag$ defines a right-action of a commutative group G on a set A, then setting $ga = ag$ defines a left-action).
- For any group G, explain how to turn a right-action of G into a left-action of G. (Note that the simple 'flip' $ga = ag$ does not work in general if G is not commutative.)

Solution. Going item by item:

- The verification is straightforward. First note that the identity and inverses necessarily remain the same (as $e_G g = g e_G$ for all $g \in G$ and similarly $gg^{-1} = g^{-1}g$). Thus it remains to check that the operation $\bullet$ is associative. Let $g, h, k \in G$. We have $(g \bullet h) \bullet k = k \cdot (g \bullet h) = k \cdot (h \cdot g) = (k \cdot h) \cdot g = (h \bullet k) \cdot g = g \bullet (h \bullet k)$ and thus $\bullet$ is indeed associative. Therefore G° is indeed a group.
- Suppose the given function, call it id, is an isomorphism. Then because it is in fact a homomorphism, we have $h \cdot g = \mathrm{id}(h \cdot g) = \mathrm{id}(g \bullet h) = \mathrm{id}(g) \cdot \mathrm{id}(h) = g \cdot h$ for all $g, h \in G$, showing that G is a commutative group. The same argument can be used to show that id is a homomorphism when G is commutative. It clearly has an inverse $g \mapsto g$ and thus is an isomorphism.
- Define a function $G^\circ \to G$ by $g \mapsto g^{-1}$. This is a homomorphism as $g \bullet h \mapsto (h \cdot g)^{-1} = g^{-1} \cdot h^{-1}$. It is clearly injective, because two different elements of a group cannot have the same inverse. If $g \in G$ is an element, we know that $(g^{-1})^{-1} = g$ and thus $g^{-1} \mapsto g$, therefore it is surjective. Hence we have an isomorphism of G and G°.

- Suppose that we have a right-action of G on a set A, that is a set-function $\rho : A \times G \to A$ such that for all $g, h \in G$, $a \in A$, $\rho(a, e_G) = a$ and $\rho(a, g \cdot h) = \rho(\rho(a, g), h)$. We can define a function $\sigma : G \to \mathrm{Hom}_{\mathsf{Set}}(A, A)$ by setting $\sigma(g)(a) = \rho(a, g)$. Define a function $G^\circ \to \mathrm{Hom}_{\mathsf{Set}}(A, A)$ defined as $g \mapsto \sigma(g)$. Then $g \bullet h \mapsto \sigma(h \cdot g)$ and since $\sigma(h \cdot g)(a) = \rho(a, h \cdot g) = \rho(\rho(a, h), g) = \rho(\sigma(h)(a), g) = \sigma(g)(\sigma(h)(a)) = \sigma(g) \circ \sigma(h)(a)$, this map is a homomorphism. Also we can see that $\sigma(g^{-1})$ acts as the inverse of $\sigma(g)$ and therefore the image of this homomorphism is precisely S_A. Thus we have a homomorphism $G^\circ \to S_A$, and hence a left-action of G° on A (defined by settings $ga = \sigma(g, a) = \rho(a, g)$).
- Suppose G is a commutative group and we have a right-action of G on A, $\rho : A \times G \to A$. Consider a set-function $\rho' : G \times A \to A$ defined as $\rho'(g, a) = \rho(a, g)$ (that is simply reversing the order). We want to show that ρ' defines a left-action of G on A. Clearly $\rho'(e_G, a) = \rho(a, e_G) = a$. Due to commutativity of G we have

$$\begin{aligned} \rho'(g \cdot h, a) &= \rho(a, g \cdot h) \\ &= \rho(a, h \cdot g) \\ &= \rho(\rho(a, h), g) \\ &= \rho(\rho'(h, a), g) \\ &= \rho'(g, \rho'(h, a)) \end{aligned}$$

  and thus ρ' is indeed a left-action of G on A.
- Let G be any group (not necessarily commutative). Suppose we have a right-action of G on a set A. We know that this gives us a left-action of G° on A, that is a homomorphism $\sigma^\circ : G^\circ \to S_A$. We found an isomorphism of G° and G, defined as $g \mapsto g^{-1}$. Composing it with σ° we obtain a homomorphism $G \to S_A$ giving us a left-action of G on A (defined as $\sigma(g) = \sigma^\circ(g^{-1})$). □

9.4. As mentioned in the text, *right*-multiplication defines a right-action of a group on itself. Find *another* natural right-action of a group on itself.

Solution. A natural choice is conjugation on the right, that is we define $\rho : G \times G \to G$ as $\rho(h, g) = g^{-1}hg$. We then have $\rho(h, e_G) = e_G h e_G = h$ and for all $g, h, k \in G$,

$$\rho(k, gh) = (gh)^{-1}k(gh) = h^{-1}(g^{-1}kg)h = h^{-1}\rho(k, g)h = \rho(\rho(k, g), h),$$

showing that ρ is indeed a right-action. □

9.5. Prove that the action by left-multiplication of a group on itself is free.

Solution. Let G be a group. Suppose the action by left-multiplication of G on itself is not free. Then there is an element $g \in G$, $g \neq e_G$, such that $gg = g$. Then by cancellation we have $g = e_G$, a contradiction. □

9.6. Let O be an orbit of an action of a group G on a set. Prove that the induced action of G on O is transitive.

Solution. Let G be a group, A a set, and suppose G acts on A. Consider an orbit of $a \in A$, that is $O = O_G(a) = \{ga \mid g \in G\}$. Let $x, y \in O$. Then by the definition of O, we have $g, h \in G$ such that $x = ga$, $y = ha$. Using the defining property of left-actions we have

$$x = ga = (ge_G)a = (gh^{-1}h)a = (gh^{-1})ha = (gh^{-1})y,$$

proving that the induced action of G on O is indeed transitive. □

9.7. Prove that stabilizers are indeed subgroups.

Solution. Let G be a group, A a set, and suppose G acts on A. Let $a \in A$ and consider the stabilizer $S = \mathrm{Stab}_G(a) = \{g \in G \mid ga = a\}$ of a. Let $g, h \in S$. Then $ga = ha = a$. $ha = a$ implies $h^{-1}a = a$, hence $(gh^{-1})a = g(h^{-1}a) = ga = a$. Thus $gh^{-1} \in S$, showing that S is a subgroup of G. □

9.8. For G a group, verify that G-Set is indeed a category, and verify that the isomorphisms in G-Set are precisely the equivariant bijections.

Solution. Verifying that G-Set is a category 'point by point':

- id_A is clearly an equivariant function and is the identity morphism of (ρ, A).
- As the morphisms are just equivariant functions, composition is clear. We just need to check that the composition of equivariant functions is itself an equivariant function. Let $\varphi_1 : A \to B$, $\varphi_2 : B \to C$ be equivariant functions. By definition, for all $g \in G$, $a \in A$, we have $g\varphi_1(a) = \varphi_1(ga)$, and hence

  $$g(\varphi_2 \circ \varphi_1(a)) = g\varphi_2(\varphi_1(a)) = \varphi_2(g\varphi_1(a)) = \varphi_2(\varphi_1(ga)) = \varphi_2 \circ \varphi_1(ga).$$

  Thus $\varphi_2 \circ \varphi_1$ is an equivariant function.
- Associativity follows from Set.
- Identity morphisms are identities with respect to composition again due to Set.

We shall now verify that equivariant bijections are isomorphisms in this category. By definition, a morphism is an isomorphism if it has a (two-sided) inverse (with respect to composition). Equivariant bijections have a two-sided inverse in Set, so it remains to check that the inverse is also equivariant (and is thus a morphism in G-Set).

Let $\varphi : A \to A'$ be an equivariant bijection. Then there is an inverse set-function $\varphi^{-1} : A' \to A$. Let $g \in G$, $a' \in A'$. We have $\varphi \circ \varphi^{-1}(a') = a'$, which implies

$$\begin{aligned} ga' &= g(\varphi \circ \varphi^{-1}(a')) \\ &= g(\varphi(\varphi^{-1}(a'))) \\ &= \varphi(g\varphi^{-1}(a')) \end{aligned}$$

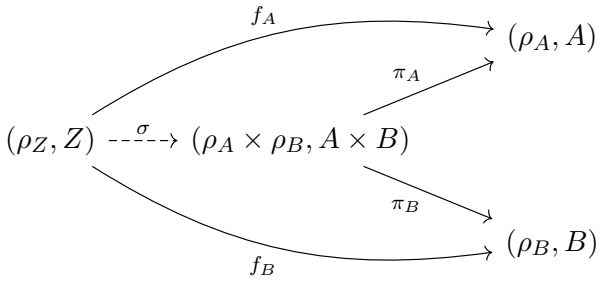
by acting on the left by g and using the fact that φ is equivariant. Applying φ^{-1} to this equation than gives us $\varphi^{-1}(ga') = g\varphi^{-1}(a')$ showing that φ^{-1} is in fact also equivariant. Therefore equivariant bijections are indeed isomorphisms in G-Set. □

9.9. Prove that G-Set has products and coproducts and that every object of G-Set is a coproduct of objects of the type $G/H = \{\text{left-cosets of } H\}$, where H is a subgroup of G and G acts on G/H by left-multiplication.

Solution. Let us first consider products in G-Set. Let (ρ_A, A), (ρ_B, B) be G-sets. Notice, that we can use the fact that G-Set is in fact supported by Set. We thus have a product $A \times B$, and a function $\rho_A \times \rho_B : G \times (A \times B) \to A \times B$ (we can produce this function using the universal property of products, $\rho_A \times \rho_B(g, (a, b)) = (\rho_A(g, a), \rho_B(g, b))$). We shall show that $(\rho_A \times \rho_B, A \times B)$ together with the natural projections $\pi_A : A \times B \to A$, $\pi_B : A \times B \to B$ is in fact a product in G-Set.

We have to ensure that π_A and π_B are morphisms in G-Set, that is, are equivariant. Let $g \in G$, $(a, b) \in A \times B$. We have $\pi_A(\rho_A \times \rho_B(g, (a, b))) = \pi_A((\rho_A(g, a), \rho_B(g, b))) = \rho_A(g, a) = \rho_A(g, \pi_A((a, b)))$ showing that π_A is equivariant. Similarly for π_B.

Let (ρ_Z, Z) be any G-set, and $f_A : Z \to A$, $f_B : Z \to B$ equivariant functions (and thus morphisms in G-Set). We have to prove that there is a unique equivariant function $\sigma : Z \to A \times B$ which makes the diagram



commute. From the universal property of products in Set we have a unique set-function $f_A \times f_B : Z \to A \times B$ which makes the diagram commute in Set. It is enough to show that this function is in fact equivariant. Let $g \in G$, $z \in Z$. We have $f_A \times f_B(\rho_Z(g, z)) = (f_A(\rho_Z(g, z)), f_B(\rho_Z(g, z)))$. f_A and f_B being equivariant functions then implies

$$\begin{aligned}(f_A(\rho_Z(g, z)), f_B(\rho_Z(g, z))) &= (\rho_A(g, f_A(z)), \rho_B(g, f_B(z))) \\ &= \rho_A \times \rho_B(g, (f_A(z), f_B(z))) \\ &= \rho_A \times \rho_B(g, f_A \times f_B(z)),\end{aligned}$$

showing that $f_A \times f_B$ is indeed an equivariant function.

To cut on the formalism, we have shown that if G acts on sets A and B, then G also naturally acts on $A \times B$ with $g(a, b) = (ga, gb)$. Similarly, we could show that G also

acts on $A \amalg B$, with the action being defined as $\rho : G \times (A \amalg B) \to (A \amalg B)$, with

$$\rho(g,a) = \begin{cases} i_A \circ \rho_A(g,a) & \text{if } a \in \operatorname{im} i_A \\ i_B \circ \rho_B(g,a) & \text{otherwise.} \end{cases}$$

ρ is well-defined due to the properties of disjoint unions - $A \amalg B$ contains copies of both A and B (obtained from i_A, i_B), and hence for any $a \in A \amalg B$ we always have either $a \in \operatorname{im} i_A$ or $a \in \operatorname{im} i_B$. To show that this construction is a coproduct in G-Set it is enough to check that the unique set-function σ obtained from the universal property of coproducts in Set is equivariant, which is straightforward.

We know that orbits of an action of a group G on a set A form a partition of A. Any object of G-Set can thus be viewed as the coproduct of the orbits of the respective action together with the induced, transitive, actions on them. By Proposition 9.9 we know such transitive actions are in fact isomorphic to left-multiplication of G on G/H, where H is the stabilizer of any element. Hence every object of G-Set is indeed isomorphic to the coproduct of objects of the type G/H, where H is a subgroup of G, and G acts on G/H by left-multiplication, as claimed. □

9.10. Let H be any subgroup of a group G. Prove that there is a bijection between the set G/H of *left*-cosets of H and the set $H\backslash G$ of *right*-cosets of H in G. (Hint: G acts on the right on the set of right-cosets; Use Exercise 9.3 and Proposition 9.9)

Solution. From Exercise 9.3 we know we can turn a right-action of G on a set A into a left-action of G on A. Let $\rho : H\backslash G \times G \to H\backslash G$ be the action of right-multiplication of G on $H\backslash G$. Then we have a left-action $\rho' : G \times H\backslash G \to H\backslash G$ defined as $\rho'(g, Ha) = \rho(Ha, g^{-1}) = H(ag^{-1})$ for all $g \in G$, $Ha \in H\backslash G$.

Let $Ha, Hb \in H\backslash G$. Notice that $\rho'(b^{-1}a, Ha) = H(a(b^{-1}a)^{-1}) = H(aa^{-1}b) = Hb$ and thus ρ' is transitive. But every transitive (left-)action is in fact isomorphic to the left-multiplication of G on G/S where S is the stabilizer of any $Ha \in H\backslash G$. But if $Ha \in H\backslash G$ is any right-coset, then $\rho'(g, Ha) = H(ag^{-1}) = Ha$ only if $g^{-1} \in H$, and thus only if $g \in H$ (since H is a subgroup). Thus $\operatorname{Stab}_G(Ha) = H$ for all $Ha \in H\backslash G$.

Therefore the transitive action ρ' is isomorphic to the left-multiplication of G on G/H, and thus there is an equivariant bijection $\varphi : H\backslash G \to G/H$, finishing the proof. □

9.11. ¬ Let G be a finite group, and let H be a subgroup of index p, where p is the *smallest prime dividing* $|G|$. Prove that H is normal in G, as follows:

- Interpret the action of G on G/H by left-multiplication as a homomorphism $\sigma : G \to S_p$.
- Then $G/\ker\sigma$ is (isomorphic to) a subgroup of S_p. What does this say about the index of $\ker\sigma$ in G?

- Show that $\ker\sigma \subseteq H$.
- Conclude that $H = \ker\sigma$, by index considerations.

Thus H is a kernel, proving that it is normal. (This exercise generalizes the result of Exercise 8.2) [9.12]

Solution. Let G be a finite group, H a subgroup of index p, where p is the smallest prime dividing $|G|$, so that $[G : H] = p$.

- We can interpret the action of left-multiplication of G on G/H, $\rho(g, aH) = (ga)H$ as a homomorphism $\sigma : G \to \mathrm{Aut}_{\mathsf{Set}}(G/H)$ by setting $\sigma(g)(aH) = \rho(g, aH)$. $[G : H] = p$ implies G/H is a finite set with p elements and thus is isomorphic to the set $\{1, 2, \ldots, p\}$ and hence $\mathrm{Aut}_{\mathsf{Set}}(G/H) \cong S_p$. Thus we can in fact interpret the action as a homomorphism $\sigma : G \to S_p$.
- Using canonical decomposition we can see that $G/\ker\sigma$ is isomorphic to a subgroup $\mathrm{im}\,\sigma$ of S_p. By Lagrange's theorem we know the order of $\mathrm{im}\,\sigma$ must divide the order of S_p, $p!$. Thus $[G : \ker\sigma]$ divides $p!$.
- $\sigma(g) = e$ if for all $aH \in G/H$ we have $\sigma(g)(aH) = aH$. We have $\sigma(g)(aH) = (ga)H$. $(ga)H = aH$ implies $a^{-1}ga \in H$, which holds only when $g \in H$ (we know that $\gamma_{a^{-1}}$ is an automorphism of G by Exercise 4.8, and in particular $\gamma_{a^{-1}}(H) = H$). Thus $\ker\sigma \subseteq H$.
- $\ker\sigma$ is a subgroup of G and thus its order must divide $|G|$. But p is the smallest prime that divides $|G|$, and thus $[G : \ker\sigma] = p$. We have

  $$[G : \ker\sigma] = [G : H] \cdot [H : \ker\sigma],$$

  hence $p = p \cdot [H : \ker\sigma]$, and therefore $[H : \ker\sigma] = 1$. But that implies $H = \ker\sigma$. □

9.12. ¬ Generalize the result of Exercise 9.11, as follows. Let G be a group, and let $H \subseteq G$ be a subgroup of index n. Prove that H contains a subgroup K that is normal in G and such that $[G : K]$ divides the gcd of $|G|$ and $n!$. (In particular, $[G : K] \leq n!$.) [IV.2.23]

Solution. We can generalize the result of Exercise 9.11 by following a similar path of arguments as we took in the proof of that exercise. We have a homomorphism $\sigma : G \to S_n$. $G/\ker\sigma$ is thus isomorphic to a subgroup of S_n, therefore $[G : \ker\sigma]$ divides $n!$. Let $K = \ker\sigma$. Then $K \subseteq H$, and since K is the kernel of σ, it is normal in G. By Lagrange's theorem we have $|G| = [G : K] \cdot |H|$, and thus $[G : K]$ must divide $|G|$. Notice, that since $[G : K]$ divides both $|G|$ and $n!$, it must also divide their gcd. □

9.13. ▷ Prove 'by hand' that for all subgroups H of a group G and $\forall g \in G, G/H$ and $G/(gHg^{-1})$ (endowed with the action of G by left-multiplication) are isomorphic in G-Set. [§9.3]

Solution. Let H be any subgroup of a group G and $g \in G$ any element. We need to find an equivariant bijection

$$\varphi : G/H \to G/(gHg^{-1}).$$

First of all, such a bijection must be well-defined. If $aH = bH$, then $a^{-1}b \in H$, hence $g(a^{-1}b)g^{-1} \in gHg^{-1}$. Reordering the brackets we get $(ga^{-1})(bg^{-1}) = (ag^{-1})^{-1}(bg^{-1}) \in gHg^{-1}$ showing that $(ag^{-1})(gHg^{-1}) = (bg^{-1})(gHg^{-1})$. Thus we define

$$\varphi(aH) = (ag^{-1})(gHg^{-1}).$$

Does this function has an inverse? Using a similar argument we see that if $a(gHg^{-1}) = b(gHg^{-1})$, then $(ag)H = (bg)H$, and $a(gHg^{-1}) \mapsto (ag)H$ is an obvious inverse of φ. Thus φ is a bijection in Set.

Let $x \in G$. Then $x\varphi(aH) = x((ag^{-1})(gHg^{-1})) = (xag^{-1})(gHg^{-1}) = \varphi((xa)H) = \varphi(x(aH))$, showing that φ is equivariant. □

9.14. ¬ Prove that the modular group $\mathrm{PSL}_2(\mathbb{Z})$ is isomorphic to the coproduct $C_2 * C_3$. (Recall that the modular group $\mathrm{PSL}_2(\mathbb{Z})$ is generated by $x = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $y = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, satisfying the relations $x^2 = y^3 = e$ in $\mathrm{PSL}_2(\mathbb{Z})$ (Exercise 7.5). The task is to prove that x and y satisfy *no* other relation: this will show that $\mathrm{PSL}_2(\mathbb{Z})$ is presented by $(x, y \mid x^2, y^3)$, and we agreed that this is a presentation for $C_2 * C_3$ (Exercise 3.8 or 8.7). Reduce this to verifying that no products

$$(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x) \quad \text{or} \quad (y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)y^{\pm 1}$$

with one or more factors can equal the identity. This latter verification is traditionally carried out by cleverly exploiting an action. Let the modular group act on the set of *irrational* real numbers by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(r) = \frac{ar + b}{cr + d}.$$

Check that this does define an action of $\mathrm{PSL}_2(\mathbb{Z})$, and note that

$$y(r) = 1 - \frac{1}{r}, \quad y^{-1}(r) = \frac{1}{1 - r}, \quad yx(r) = 1 + r, \quad y^{-1}x(r) = \frac{r}{1 + r}.$$

Now complete the verification with a case-by-case analysis. For example, a product $(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)y$ cannot equal the identity in $\mathrm{PSL}_2(\mathbb{Z})$ because if it did, it would act as the identity on $\mathbb{R} \smallsetminus \mathbb{Q}$, while if $r < 0$, then $y(r) > 0$, and both yx and $y^{-1}x$ send positive irrationals to positive irrationals.) [3.8]

Solution. As noted, $\mathrm{PSL}_2(\mathbb{Z})$ is generated by x and y such that $x^2 = y^3 = e$. Therefore every element of $\mathrm{PSL}_2(\mathbb{Z})$, is either the identity, x, or a product of the form $(y^{a_1}x)(y^{a_2}x)\cdots(y^{a_n}x)y^b$ for some $n \geq 0$ such that $1 \leq a_i \leq 2$ and $1 \leq b \leq 2$. Since $y^3 = e$, $y^2 = y^{-1}$, and thus indeed it is enough to verify that no element of the form

$$(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x) \quad \text{or} \quad (y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)y^{\pm 1}$$

is equal to the identity.

Consider the prescription for an action given in the problem text. We have $I_2(r) = \frac{r}{1} = r$. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), B = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$, so that $AB = \left(\begin{smallmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{smallmatrix}\right)$. Then

$$\begin{aligned} A(B(r)) &= A(\frac{xr+y}{zr+w}) \\ &= \frac{a\frac{xr+y}{zr+w} + b}{c\frac{xr+y}{zr+w} + d} \\ &= \frac{axr + ay + bzr + bw}{cxr + cy + czr + wd} \\ &= \frac{(ax+bz)r + (ay+bw)}{(cx+cz)r + (cy+dw)} \\ &= (AB)(r), \end{aligned}$$

showing that it is indeed an action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathbb{R} \smallsetminus \mathbb{Q}$.

Suppose we have an element of $\mathrm{PSL}_2(\mathbb{Z})$ of the form $(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)$. If the last factor is yx, for $-1 < r < 0$ we have $(yx)(r) > 0$. But yx and $y^{-1}x$ send positive irrationals to positive irrationals and thus such a product cannot equal the identity. On the other hand, if the last factor is $y^{-1}x$, if $r < -1$, then $(y^{-1}x)(r) > 0$ and by the same consideration such a product cannot equal the identity.

The product of the form $(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)y$ cannot equal the identity as shown in the problem text. So it remains to check $(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)y^{-1}$. And again, if $r < 0$, $y^{-1}(r) > 0$. □

9.15. ¬ Prove that every (finitely generated) group G acts freely on any corresponding Cayley graph. (Cf. Exercise 8.6. Actions on a directed graph are defined as actions on the set of vertices preserving incidence: if the vertices v_1, v_2 are connected by an edge, then so must be gv_1, gv_2 for every $g \in G$.) In particular, conclude that every free group acts freely on a tree. [9.16]

Solution. Let G be a finitely generated group and A a set of generators of G. By the definition of a Cayley graph, we know that the set of vertices of any corresponding Cayley graph is in one-to-one correspondence with the underlying set of G, and thus for brevity we can just take a graph where the set of vertices is exactly G.

Clearly G acts on the set of vertices by left-multiplication. If v_1, v_2 are vertices that are connected by an edge, then by definition $v_2 = v_1 a$ for some $a \in A$, and thus $gv_2 = gv_1 a$, proving that G acts on the Cayley graph by left-multiplication.

Suppose that $g \in G$ acts on a vertex v such that the result is v. Then in particular $gv = v$, and therefore by right-cancellation $g = e_G$, proving that the left-multiplication is in fact free.

In conclusion, any finitely generated group indeed acts freely on any corresponding Cayley graph. Because free groups admit Cayley graphs that are trees (by Exercise 8.6), we also conclude that every free group acts freely on a tree. □

9.16. ▷ The converse of the last statement in Exercise 9.15 is also true: only free groups can act freely on a tree. Assuming this, prove that every subgroup of a free group (on a finite set) is free. [§6.4]

Solution. Let G be a free group on a finite set and H its subgroup. Because G acts freely on a tree, it follows that H acts freely on the same tree - we can restrict the function defining the action $\rho : G \times V \to V$ (where V is the set of the vertices of the tree) to $\rho|_H : H \times V \to V$ and this still defines a free action on the tree.

Assuming the converse of the last statement in Exercise 9.15 it follows that H must itself be a free group. □

9.17. ▷ Consider G as a G-set, by acting with left-multiplication. Prove that $\mathrm{Aut}_{G\text{-}\mathsf{Set}}(G) \cong G$. [§2.1]

Solution. The automorphisms of G in G-Set are equivariant bijections $\varphi : G \to G$. By the definition of equivariant functions, we have $g\varphi(h) = \varphi(gh)$ for all $g, h \in G$. In particular, for $h = e_G$, we have $\varphi(g) = g\varphi(e_G)$ for all $g \in G$. Therefore every φ is uniquely determined by the image of e_G.

That means we have a function $\gamma : \mathrm{Aut}_{G\text{-}\mathsf{Set}}(G) \to G$ defined as $f(\varphi) = \varphi(e_G)$. γ is well-defined as if $\varphi_1 = \varphi_2$, then in particular we must have $\varphi_1(e_G) = \varphi_2(e_G)$, and hence $\gamma(\varphi_1) = \gamma(\varphi_2)$.

γ is injective, because if $\gamma(\varphi_1) = \gamma(\varphi_2)$, then $\varphi_1(e_G) = \varphi_2(e_G)$ and we have already noted that φ_1 and φ_2 are uniquely determined by the image of e_G. Thus $\varphi_1 = \varphi_2$.

Suppose that $x \in G$. Then there is a function $\varphi : G \to G$ such that $\varphi(g) = gx$ for all $g \in G$ (in particular $\varphi(e_G) = x$). φ is clearly a bijection with the inverse $g \mapsto gx^{-1}$ for all $g \in G$. We have $g\varphi(h) = g(hx) = (gh)x = \varphi(gh)$ showing that φ is in fact equivariant with respect to left-multiplication. Therefore $\gamma(\varphi) = \varphi(e_G) = x$, showing that γ is surjective.

γ is hence a bijection between $\mathrm{Aut}_{G\text{-}\mathsf{Set}}(G)$ and G. Suppose that $\varphi_1, \varphi_2 \in \mathrm{Aut}_{G\text{-}\mathsf{Set}}(G)$. Then $\gamma(\varphi_1 \circ \varphi_2) = \varphi_1 \circ \varphi_2(e_G) = \varphi_1(\varphi_2(e_G)) = \varphi_1(e_G)\varphi_2(e_G)$ (by the considerations in the first paragraph), showing that γ is a homomorphism of groups.

Concluding, γ is an isomorphism of the groups $\mathrm{Aut}_{G\text{-}\mathsf{Set}}(G)$ and G and thus $\mathrm{Aut}_{G\text{-}\mathsf{Set}}(G) \cong G$. □

9.18. Show how to construct a *groupoid* carrying the information of the action of a group G on a set A. (Hint: A will be the set of objects of the groupoid. What will be the morphisms?)

Solution. Define a category C by setting $\mathrm{Obj}(\mathsf{C}) = A$ and for all $a, b \in A$, $\mathrm{Hom}_{\mathsf{C}}(a, b) = \{g \in G \mid ga = b\}$. We have to verify that this indeed defines a category:

- $e_G a = a$, thus $e_G \in \mathrm{Hom}_{\mathsf{C}}(a, a)$, and we have an identity morphism on a.
- If $g \in \mathrm{Hom}_{\mathsf{C}}(a, b)$ and $h \in \mathrm{Hom}_{\mathsf{C}}(b, c)$ for some $a, b, c \in A$, then $ga = b$, $hb = c$, and thus $h(ga) = (hg)a = c$, showing that $hg \in \mathrm{Hom}_{\mathsf{C}}(a, c)$. Therefore we can compose morphisms.
- Associativity follows from associativity of G.
- Identity morphism is clearly an identity with respect to composition, again following from the fact that G is a group.
- $\mathrm{Hom}_{\mathsf{C}}(a, b)$ and $\mathrm{Hom}_{\mathsf{C}}(c, d)$ are obviously disjoint unless $a = c$ and $b = d$.

Let $a, b \in A$, $g \in \mathrm{Hom}_{\mathsf{C}}(a, b)$, so that $ga = b$. Then in particular $g^{-1}(ga) = (g^{-1}g)a = e_G a = g^{-1}b$ and thus $g^{-1} \in \mathrm{Hom}_{\mathsf{C}}(b, a)$, showing that every morphism has an inverse, and thus is an isomorphism. Therefore C is a groupoid. □

10. Group objects in categories

10.1. Define all the unnamed maps appearing in the diagrams in the definition of group object, and prove they are indeed isomorphisms when so indicated. (For the projection $1 \times G \to G$, what is left to prove is that the composition

$$1 \times G \to G \to 1 \times G$$

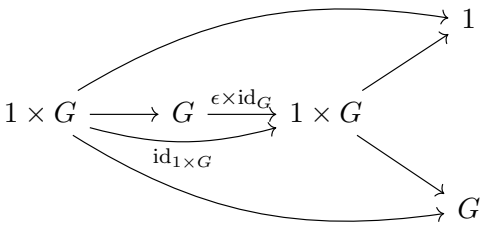
is the identity, as mentioned in the text.)

Solution. Starting with the morphism $(G \times G) \times G \to G \times (G \times G)$, notice, that we have already proved in Exercise I.5.9 that if C is a category with products, then $(G \times G) \times G$ and $G \times (G \times G)$ both satisfy the universal property of the product of three objects $G \times G \times G$ and are therefore isomorphic by Proposition I.5.4.

Next we shall look at $1 \times G \to G$. As noted, 1 is final and therefore there is a unique morphism $\epsilon : G \to 1$. The composition

$$G \xrightarrow{\epsilon \times \mathrm{id}_G} 1 \times G \longrightarrow G$$

is the identity id_G by the universal property of products. Consider the diagram



which commutes - $\mathrm{id}_{1\times G}$ is the unique morphism making the diagram commute, but so is the composition of the projection $1 \times G \to G$ and $\epsilon \times \mathrm{id}_G$. Thus they must be equal. This shows that the second composition,

$$1 \times G \longrightarrow G \xrightarrow{\epsilon\times\mathrm{id}_G} 1 \times G$$

is also the identity, proving that $1 \times G \to G$ (the projection morphism) is in fact an isomorphism.

The situation for the map $G \times 1 \to G$ is entirely analogous. □

10.2. ▷ Show that *groups*, as defined in §1.2, are 'group objects in the category of sets'. [§10.1]

Solution. Let $(G, \cdot)$ be a group. Define the functions $m : G \times G \to G$, $e : \{e\} \to G$ ($\{e\}$ is a final object in Set), and $\iota : G \to G$ as $m(g, h) = g \cdot h$, $e(e) = e_G$, and $\iota(g) = g^{-1}$. The first diagram (defining associativity of multiplication) is clearly commutative for m, as for all $g, h, k \in G$ we have

$$\begin{aligned} m \circ (m \times \mathrm{id}_G)((g, h), k) &= m(g \cdot h, k) = (g \cdot h) \cdot k \\ m \circ (\mathrm{id}_G \times m)(g, (h, k)) &= m(g, h \cdot k) = g \cdot (h \cdot k) \end{aligned}$$

and $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ because G is a group.

The diagrams defining the existence of two-sided identity also commute, as for all $g \in G$ we have

$$\begin{aligned} m \circ (e \times \mathrm{id}_G)(e, g) = m(e_G, g) &= e_G \cdot g = g \\ \pi_{\{e\}}(e, g) &= g \\ m \circ (\mathrm{id}_G \times e)(g, e) = m(g, e_G) &= g \cdot e_G = g \\ \pi_G(g, e) &= g. \end{aligned}$$

And for the last two diagrams, for all $g \in G$,

$$\begin{aligned} m \circ (\mathrm{id}_G \times \iota) \circ \Delta(g) = m \circ (\mathrm{id}_G \times \iota)(g, g) = m(g, g^{-1}) &= g \cdot g^{-1} = e_G \\ e \circ \epsilon(g) = e(e) &= e_G \end{aligned}$$

and similarly for the other diagram.

All the diagrams thus commute because of the related properties of groups as defined in §1.2. Thus the set G together with m, e, ι in fact are a group object in Set. □

10.3. Let $(G, \cdot)$ be a group, and suppose $\circ : G \times G \to G$ is a group homomorphism (w. r. t. $\cdot$) such that $(G, \circ)$ is *also* a group. Prove that $\circ$ and $\cdot$ coincide. (Hint: First prove that the identity with respect to the two operations must be the same)

Solution. Using the 'operational' notation in place of functional, $\circ$ being a homomorphism (w. r. t. $\cdot$) implies $(a \circ b) \cdot (c \circ d) = (a \cdot c) \circ (b \cdot d)$ for all $a, b, c, d \in G$.

$(G, \cdot)$ and $(G, \circ)$ are groups, thus we have elements $e_G \in G$ (the identity with respect to $\cdot$) and $e_\circ \in G$ (the identity with respect to $\circ$). Then

$$e_G = e_G \cdot e_G = (e_\circ \circ e_G) \cdot (e_G \circ e_\circ) = (e_\circ \cdot e_G) \circ (e_G \cdot e_\circ) = e_\circ \circ e_\circ = e_\circ$$

and thus the identity with respect to both operations is the same element.

Let $a, b \in G$. Then

$$a \circ b = (a \cdot e_G) \circ (e_G \cdot b) = (a \circ e_G) \cdot (e_G \circ b) = a \cdot b$$

and thus $\circ$ and $\cdot$ in fact coincide. □

10.4. Prove that every *abelian* group has exactly one structure of group object *in the category* Ab.

Solution. Let $(G, \cdot)$ be an abelian group, and $\circ : G \times G \to G$, $e : 1 \to G$ (where 1 is a final object in Ab), and $\iota : G \to G$ morphisms in Ab (and thus homomorphisms of abelian groups), such that the relevant diagrams for group objects commute. We will show that $(G, \circ)$ is a group and thus $\cdot$ and $\circ$ coincides by Exercise 10.3.

$\circ$ is well-defined by the assumption that it is in fact a group homomorphism. For all $g \in G$, $g \circ e = g = e \circ g$ (where e is taken to be the image of e) by the commutativity of the relevant diagrams, and thus there is an identity element with respect to $\circ$. Inverses exist, because for any $g \in G$, we have an element $\iota(g)$ which is an inverse of g again by the commutativity of the relevant diagrams. Associativity also follows similarly.

Therefore by Exercise 10.3 we see that $\cdot$ and $\circ$ coincide, and therefore there is exactly one structure of a group object for G in Ab. □

10.5. By the previous exercise, a group object in Ab is nothing other than an abelian group. What is a group object in Grp?

Solution. Notice that the morphisms in Grp are in fact group homomorphisms. In particular, every group object must have a homomorphism $\iota : G \to G$ defining the inverse of any element. Since ι is a group homomorphism, in particular, if $(G, \cdot)$ is a group, for any $g, h \in G$ we must have $\iota(g \cdot h) = \iota(g) \cdot \iota(h)$. We must also have $\iota(g) = g^{-1}$ because of the required commutativity of the diagrams relating m and ι. But that means

$$g^{-1} \cdot h^{-1} = \iota(g) \cdot \iota(h) = \iota(g \cdot h) = (g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$$

for all $g, h \in G$. This forces G to be abelian, and therefore group objects in Grp are precisely abelian groups. □

III. Rings and modules

1. Definition of ring

1.1. ▷ Prove that if $0 = 1$ in a ring R, then R is a zero-ring. [§1.2]

Solution. Let R be a ring such that $0 = 1$ in R. Let $r \in R$. Then $0 = 1$ implies $r \cdot 0 = r \cdot 1 = r$, but $r \cdot 0 = 0$ by Lemma 1.2, and thus $r = 0$. Therefore R only has a single element and is a zero-ring. □

1.2. ¬ Let S be a set, and define operations on the power set $\mathscr{P}(S)$ of S by setting $\forall A, B \in \mathscr{P}(S)$

$$A + B := (A \cup B) \smallsetminus (A \cap B), \quad A \cdot B = A \cap B.$$

Prove that $(\mathscr{P}(S), +, \cdot)$ is a commutative ring. [2.3, 3.15]

Solution. First we will show that $(\mathscr{P}(S), +)$ is an abelian group. The operation $+$ is well-defined, because if A and B are subsets of S, then so must be $A \cup B$, $A \cap B$, and $A \smallsetminus B$. The operation is also both associative and commutative, which follows from the properties of $\cup$ and $\cap$. For any $A \in \mathscr{P}(S)$, we have $A + \emptyset = (A \cup \emptyset) \smallsetminus (A \cap \emptyset) = A \smallsetminus \emptyset = A$ and since $\emptyset \in \mathscr{P}(S)$, $\emptyset$ is the identity with respect to $+$ ($+$ is commutative so showing 'one side' is enough). We also have $A + A = (A \cup A) \smallsetminus (A \cap A) = A \smallsetminus A = \emptyset$ showing that each element is its own inverse. Thus $(\mathscr{P}(S), +)$ is indeed an abelian group.

The associativity and commutativity of $\cdot$ is clear (because $\cap$ is both associative and commutative). The identity with respect to $\cdot$ must be the whole S (which is in particular a subset of itself), as for any $A \in \mathscr{P}(S)$ we have $A \cdot S = A \cap S = A$ (since $A \subseteq S$).

The only thing that remains is to check the distributive properties. Let $A, B, C \in \mathscr{P}(S)$. We have

$$\begin{aligned}
(A + B) \cdot C &= ((A \cup B) \smallsetminus (A \cap B)) \cap C \\
&= ((A \cup B) \cap C) \smallsetminus (A \cap B) \\
&= ((A \cap C) \cup (B \cap C)) \smallsetminus (A \cap B) \\
&= ((A \cap C) \cup (B \cap C)) \smallsetminus ((A \cap C) \cap (B \cap C)) \\
&= (A \cdot C \cup B \cdot C) \smallsetminus (A \cdot C \cap B \cdot C) \\
&= A \cdot C + B \cdot C
\end{aligned}$$

and similarly for the other property.

Thus $(\mathscr{P}(S), +, \cdot)$ is a commutative ring. □

1.3. ¬ Let R be a ring, and let S be any set. Explain how to endow the set R^S of set-functions $S \to R$ of two operations $+, \cdot$ so as to make R^S into a ring, such that R^S is just a copy of R if S is a singleton. [2.3]

Solution. If S is a singleton, each set-function $S \to R$ 'selects' a single element of R, and thus it is natural to consider the operations $+, \cdot$ defined by $(f+g)(s) = f(s)+g(s)$ (with $+$ in the right-hand side being the addition operation in R) and $(f \cdot g)(s) = f(s) \cdot g(s)$. In the singleton case, each function $f : S \to R$ is identified with $f(s)$ (where $s \in S$ is the single element) and thus R^S is just R.

Now suppose S is any set, not necessarily a singleton. We have to prove that R^S with the operations defined above is in fact a ring in this case. If f_1, f_2, g_1, g_2 are functions $S \to R$, such that $f_1 = f_2$ and $g_1 = g_2$, we have for all $s \in S$

$$(f_1 + g_1)(s) = f_1(s) + g_1(s) = f_2(s) + g_2(s) = (f_2 + g_2)(s)$$

and

$$(f_1 \cdot g_1)(s) = f_1(s) \cdot g_1(s) = f_2(s) \cdot g_2(s) = (f_2 \cdot g_2)(s)$$

thus both operations are well-defined. All the required properties follow from the fact that R is a ring, for example, for all $f, g, h \in S^R$, $s \in S$, we have

$$\begin{aligned}((f+g)+h)(s) &= (f+g)(s) + h(s)\\ &= (f(s)+g(s)) + h(s)\\ &= f(s) + (g(s)+h(s))\\ &= f(s) + (g+h)(s)\\ &= (f+(g+h))(s)\end{aligned}$$

showing that $+$ is associative operation on R^S. Identity with respect to $+$ is the function $s \mapsto 0$ for all $s \in S$, identity with respect to $\cdot$ is the function $s \mapsto 1$ (again for all $s \in S$). Additive inverse of a function $f : S \to R$ is just the function $-f : S \to R$ such that $-f(s) = -(f(s))$ for all $s \in S$. □

1.4. ▷ The set of $n \times n$ matrices with entries in a ring R is denoted $\mathcal{M}_n(R)$. Prove that componentwise addition and matrix multiplication make $\mathcal{M}_n(R)$ into a ring, for any ring R. The notation $\mathfrak{gl}_n(R)$ is also commonly used, especially for $R = \mathbb{R}$ or $\mathbb{C}$ (although this indicates one is considering them as *Lie algebras*) in parallel with the analogous notation for the corresponding groups of units; cf. Exercise II.6.1. In fact, the parallel continues with the definition of the following sets of matrices:

- $\mathfrak{sl}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) \mid \operatorname{tr}(M) = 0\}$;
- $\mathfrak{sl}_n(\mathbb{C}) = \{M \in \mathfrak{gl}_n(\mathbb{C}) \mid \operatorname{tr}(M) = 0\}$;
- $\mathfrak{so}_n(\mathbb{R}) = \{M \in \mathfrak{sl}_n(\mathbb{R}) \mid M + M^t = 0\}$;
- $\mathfrak{su}(n) = \{M \in \mathfrak{sl}_n(\mathbb{C}) \mid M + M^\dagger = 0\}$.

Here $\operatorname{tr}(M)$ means the *trace* of M, that is, the sum of its diagonal entries. The other notation matches the notation used in Exercise II.6.1. Can we make rings of these sets by endowing them with ordinary addition and multiplication of matrices? (These sets are all Lie algebras; cf. Exercise VI.1.4.) [§1.2, 2.4, 5.9, VI.1.2, VI.1.4]

Solution. Showing that $\mathcal{M}_n(R)$ for an arbitrary n and a ring R is an abelian group with respect to componentwise addition is trivial, as it is reduced to the properties of the addition group of the ring R. We have already seen that the set of invertible $n \times n$ matrices form a group under matrix multiplication, in particular it follows that the operation is necessarily associative (as this property does not depend on the invertibility of matrices) and that there is an identity with respect to matrix multiplication (the matrix I_n). Of course, in general matrices do not have to be invertible, and therefore there is no guarantee of the existence of inverse matrices (under multiplication), but that is not a required property for rings.

Thus it remains to check the distributive properties. Let $A = (a_{i,j}), B = (b_{i,j}), C = (c_{i,j}) \in \mathcal{M}_n(R)$. Then

$$\begin{aligned}(A+B)\cdot C &= (a_{i,j}+b_{i,j})\cdot(c_{i,j})\\ &= (\sum_{r=1}^{n}((a_{i,r}+b_{i,r})c_{r,j}))\\ &= (\sum_{r=1}^{n}(a_{i,r}c_{r,j}+b_{i,r}c_{r,j}))\\ &= (\sum_{r=1}^{n}(a_{i_r}c_{r,j})+\sum_{r=1}^{n}(b_{i,r}c_{r,j}))\\ &= A\cdot C + B\cdot C\end{aligned}$$

and

$$\begin{aligned}A\cdot(B+C) &= (a_{i,j})\cdot(b_{i,j}+c_{i,j})\\ &= (\sum_{r=1}^{n}(a_{i,r}(b_{r,j}+c_{r,j})))\\ &= (\sum_{r=1}^{n}(a_{i,r}b_{r,j}+a_{i,r}c_{r,j}))\\ &= A\cdot B + A\cdot C\end{aligned}$$

(where we are using the properties of the underlying ring R in every step).

$\mathfrak{sl}_n(\mathbb{R})$ and $\mathfrak{sl}_n(\mathbb{C})$ cannot be made into rings, because tr is not well behaved on multiplication. For example, we have

$$A = \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \quad B = \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \quad A\cdot B = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix},$$

but $\operatorname{tr}(A) = \operatorname{tr}(B) = 0$ and $\operatorname{tr}(AB) = 1$. Therefore both sets would not be closed under multiplication.

The other two sets have a similar problem. Take $\mathfrak{so}_n(\mathbb{R})$. We have

$$A = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \in \mathfrak{so}_n(\mathbb{R}),$$

but

$$A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \notin \mathfrak{so}_n(\mathbb{R}).$$

The same counterexample holds for $\mathfrak{su}(n)$. □

1.5. Let R be a ring. If a, b are zero-divisors in R, is $a + b$ necessarily a zero-divisor?

Solution. No, take $R = \mathbb{Z}/6\mathbb{Z}$. Then $[2]_6$ and $[3]_6$ are both zero-divisors, but $[2]_6 + [3]_6 = [5]_6$ is not a zero-divisor (in particular because it is a unit in R, as $[5]_6 \cdot [5]_6 = [1]_6$). □

1.6. ¬ An element a of a ring R is *nilpotent* if $a^n = 0$ for some n.

- Prove that if a and b are nilpotent in R and $ab = ba$, then $a + b$ is also nilpotent.
- Is the hypothesis $ab = ba$ in the previous statement necessary for its conclusion to hold?

[3.12]

Solution. Let R be a ring and $a, b \in R$ be nilpotent in R, such that $ab = ba$. Then there are some n, m such that $a^n = b^m = 0$. Then by the binomial theorem (which requires the hypothesis $ab = ba$), $(a + b)^{m+n} = \sum_{i=0}^{m+n} c_i a^i b^{m+n-i}$ where c_i is the corresponding binomial coefficient. For $i \leq n$ we have $m + n - i > m$ and thus $b^{m+n-i} = 0$. For $i > n$, $a^i = 0$. Thus $(a + b)^{m+n} = 0$.

If $ab \neq ba$, then the conclusion does not have to hold. Take

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

where both $a^2 = b^2 = 0$ and thus a and b are nilpotent. But

$$a + b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

is not nilpotent (in fact, $(a + b)^2 = I_2$). □

1.7. Prove that $[m]$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$ if and only if m is divisible by all prime factors of n.

Solution. Suppose $[m]$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$. Then $[m]^a = [0]$ for some a, hence n must divide m^a. In particular, if p is a prime divisor of n, p must also divide m^a. The prime factorization of m^a is the prime factorization of m 'multiplied by itself' a times. If p divides m^a, it divides some factor of the prime factorization of m^a, and thus it must divide the prime factorization of m, showing that p divides m. Thus every prime factor of n divides m.

On the other hand, suppose m is divisible by all prime factors of n. Let $n = p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n}$ be the prime factorization of n. By our assumption, $m = x p_1 p_2 \cdots p_n$ for some x. Let $i = i_1 i_2 \cdots i_n$. Then $m^i = x^i p_1^i p_2^i \cdots p_n^i$. $p_j^i = (p_j^{i_j})^{i/i_j} = 0$ and thus $m^i = 0$ showing that m is nilpotent in $\mathbb{Z}/n\mathbb{Z}$. □

1.8. Prove that $x = \pm 1$ are the only solutions to the equation $x^2 = 1$ in an integral domain. Find a ring in which the equation $x^2 = 1$ has more than 2 solutions.

Solution. Manipulating the equation we get $x^2 - 1 = 0$, and hence $(x-1)(x+1) = 0$. In an integral domain, there are no non-zero zero-divisors and thus we must have either $x - 1 = 0$ or $x + 1 = 0$, and thus $x = \pm 1$ are the only solutions to the equation.

In the ring $\mathbb{Z}/8\mathbb{Z}$ we have $[3]_8^2 = [1]_8$, showing that $[3]_8$ is a solution of $x^2 = 1$, and thus the equation has more than 2 solutions in $\mathbb{Z}/8\mathbb{Z}$. □

1.9. ▷ Prove Proposition 1.12. [§1.2]

Solution. Let R be a ring. For every $u \in R$, let $\rho_u : R \to R$ denote right-multiplication by u, $\lambda_u : R \to R$ left-multiplication by u.

Suppose $u \in R$ is a left-unit, and let $v \in R$ be such that $uv = 1$. For all $r \in R$

$$\lambda_u \circ \lambda_v(r) = \lambda_u(vr) = u(vr) = (uv)r = 1_R r = r.$$

That is λ_v is a right-inverse of λ_u, and thus λ_u is surjective. Conversely if λ_u is surjective, then there is $v \in R$ such that $\lambda_u(v) = 1_R$ and thus $uv = 1_R$, showing that u is a left-unit.

We also have

$$\rho_v \circ \rho_u(r) = \rho_v(ru) = (ru)v = r(uv) = r1_R = r,$$

showing that ρ_u is a injective, hence showing that u is not a right-zero-divisor.

Assume that $u \in R$ is a (two-sided) unit, $v, v' \in R$ such that $uv = v'u = 1_R$. Then we have $v = 1_R v = (v'u)v = v'(uv) = v'1_r = v'$, showing that necessarily $v = v'$ and thus inverses of two-sided units are unique.

Let G be the set of two-sided units of R. $1_R \in G$ as 1_R is trivially a unit. If $u \in G$, then u^{-1} is also a unit as $uu^{-1} = 1_R$ and thus $u^{-1} \in G$. If $u, v \in G$, then $uv \in G$, because $uvv^{-1}u^{-1} = 1_R$ in R and thus uv is a unit. Therefore G with the operation of multiplication of R is in fact a group (associativity is clear). □

1.10. Let R be a ring. Prove that if $a \in R$ is a right-unit and has two or more left-inverses, then a is *not* a left-zero-divisor and *is* a right-zero-divisor.

Solution. Let R be a ring, $a \in R$ right-unit that has two or more left-inverses. By Proposition 1.12, left-multiplication by a is injective, and thus a is not a left-zero-divisor. Assume $b, b' \in R$ such that $b \neq b'$, $ba = b'a = 1_R$. Then $ba - b'a = 0_R$ (right-cancellation in the additive group of R), hence $(b - b')a = 0_R$ (by distributivity). But $b \neq b'$ implies $b - b' \neq 0$, and thus a is a right-zero-divisor. □

1.11. ▷ Construct a field with 4 elements: as mentioned in the text, the underlying abelian group will have to be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $(0,0)$ will be the zero element, and $(1,1)$ will be the multiplicative identity. The question is what $(0,1) \cdot (0,1)$, $(0,1) \cdot (1,0)$, $(1,0) \cdot (1,0)$ must be, in order to get a *field*. [§1.2, §V.5.1]

Solution. Multiplication must distribute over addition, which implies

$$(1,0) = (1,0) \cdot ((1,0) + (0,1)) = (1,0) \cdot (1,0) + (1,0) \cdot (0,1)$$
$$(0,1) = (0,1) \cdot ((1,0) + (0,1)) = (0,1) \cdot (1,0) + (0,1) \cdot (0,1)$$

In particular, we cannot have $(0,1) \cdot (0,1) = (1,1)$ nor $(1,0) \cdot (1,0) = (1,1)$. Thus the only reasonable choice is to let $(0,1) \cdot (0,1) = (1,0)$, $(1,0) \cdot (1,0) = (0,1)$. This forces $(0,1) \cdot (1,0) = (1,0) \cdot (0,1) = (1,1)$. □

1.12. ▷ Just as complex numbers may be viewed as combinations $a + bi$, where $a, b \in \mathbb{R}$ and i satisfies the relation $i^2 = -1$ (and commutes with $\mathbb{R}$), we may construct a ring $\mathbb{H}$ by considering linear combinations $a+bi+cj+dk$ where $a, b, c, d \in \mathbb{R}$ and i, j, k commute with $\mathbb{R}$ and satisfy the following relations:

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Addition in $\mathbb{H}$ is defined componentwise, while multiplication is defined by imposing distributivity and applying the relations. For example,

$$(i+j+k)\cdot(2+k) = 1\cdot 2+i\cdot 2+j\cdot 2+1\cdot k+i\cdot k+j\cdot k = 2+2i+2j+k-j+i = 2+3i+j+k.$$

(i) Verify that this prescription does indeed define a ring.

(ii) Compute $(a + bi + cj + dk)(a - bi - cj - dk)$, where $a, b, c, d \in \mathbb{R}$.

(iii) Prove that $\mathbb{H}$ is a division ring.

Elements of $\mathbb{H}$ are called *quaternions*. Note that $Q_8 := \{\pm 1, \pm i, \pm j, \pm k\}$ forms a subgroup of the group of unit of $\mathbb{H}$; it is noncommutative group of order 8, called the *quaternionic group*.

(iv) List all subgroups of Q_8, and prove that they are all normal.

(v) Prove that Q_8, D_8 are not isomorphic.

(vi) Prove that Q_8 admits the presentation $(x, y \mid x^2y^{-2}, y^4, xyx^{-1}y)$.

[§II.7.1, 2.4, IV.1.12, IV.5.16, IV.5.17, V.6.19]

Solution. Going item by item:

(i) $(\mathbb{H}, +)$ is clearly an abelian group (precisely because $(\mathbb{R}, +)$ is an abelian group). The required properties of multiplication are a little bit more tricky, but it is fairly obvious that the operation is well-defined and associative because it is based on the properties of multiplication in $\mathbb{R}$. The multiplicative identity is also 1. Associativity is built into the definition of multiplication. Thus $(\mathbb{H}, +, \cdot)$ is indeed a ring.

(ii) $(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$. Notice that $(a - bi - cj - dk)(a + bi + cj + dk)$ also equals $a^2 + b^2 + c^2 + d^2$.

(iii) Let $a+bi+cj+dk$ be an element of $\mathbb{H}$. Notice that by the last point, multiplying it on either side by $\frac{1}{a^2+b^2+c^2+d^2}(a - bi - cj - dk)$ we get 1, thus every quaternion has an inverse and therefore $\mathbb{H}$ is a division ring (but not a field as the multiplication is not commutative in general, as can be seen from the given relations).

(iv) Excluding the trivial group and the whole group as subsets. $\{\pm 1\}$ is a subgroup (and it is trivially normal by the relations). We have a subgroup $\{\pm 1, \pm x\}$ for each $x = i, j, k$ (note that it must contain -1 because $x^2 = -1$, and thus also $-x$). For example, take the subgroup $\{\pm 1, \pm i\}$. $j\{\pm 1, \pm i\}j^{-1} = \{\pm j, \pm ji\}(-j) = \{\pm 1, \pm jij\}$. $jij = -ijj = i$. Similarly for k. Thus each such subgroup is in fact normal. There are no other possible subgroups, as the product of any two of i, j, k is equal to the third.

(v) D_8 has a subgroup of order 2 which is not normal, however, all subgroups of Q_8 are normal. Therefore they cannot be isomorphic.

(vi) Notice that i, j, k all have order 4 in Q_8 and that the product of any two of them is equal to the third one and thus can generate the whole group. Every element of the group given by the presentation is of the form $x^a y^b$ where $0 \leq a \leq 1$ and $0 \leq b \leq 3$ ($xyx^{-1}y = e$ implies $xy = y^{-1}x$ hence $yx = xy^{-1}$). Taking $x = i$, $y = j$, we see that the elements are thus $i^0 j^0 = 1$, $i^0 j^2 = -1$, $i^1 j^0 = i$, $i^1 j^2 = -i$, $i^0 j^1 = j$, $i^0 j^3 = -j$, $i^1 j^1 = k$ and lastly $i^1 j^3 = -k$. Thus Q_8 admits the given presentation. □

1.13. ▷ Verify that the multiplication defined in $R[x]$ is associative. [§1.3]

Solution. Let $f(x), g(x), h(x) \in R[x]$, such that

$$f(x) = \sum_{i \geq 0} a_i x^i, \quad g(x) = \sum_{i \geq 0} b_i x^i, \quad h(x) = \sum_{i \geq 0} c_i x^i$$

Then

$$\begin{aligned}(f(x)\cdot g(x))\cdot h(x) &= \sum_{k\geq 0}\sum_{i+j=k} a_i b_j x^{i+j}\cdot \sum_{i\geq 0} c_i x^i \\ &= \sum_{r\geq 0}\sum_{s+p=r}(\sum_{i+j=s} a_i b_j)c_p x^{s+p} \\ &= \sum_{r\geq 0}\sum_{(i+j)+p=r}(a_i b_j)c_p x^{(i+j)+p} \\ &= \sum_{r\geq 0}\sum_{i+(j+p)=r} a_i(b_j c_p)x^{i+(j+p)} \\ &= \sum_{r\geq 0}\sum_{i+s=r} a_i(\sum_{j+p=s} b_j c_p)x^{i+s} \\ &= \sum_{i\geq 0} a_i x^i \cdot \sum_{k\geq 0}\sum_{i+j=k} b_i c_j x^{i+j} \\ &= f(x)\cdot(g(x)\cdot h(x))\end{aligned}$$

and thus multiplication in $R[x]$ is associative as claimed. □

1.14. ▷ Let R be a ring, and let $f(x), g(x) \in R[x]$ be nonzero polynomials. Prove that

$$\deg(f(x)+g(x)) \leq \max(\deg(f(x)), \deg(g(x))).$$

Assuming that R is an integral domain, prove that

$$\deg(f(x)\cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

[§1.3]

Solution. Suppose that

$$f(x) = \sum_{i\geq 0} a_i x^i, \quad g(x) = \sum_{i\geq 0} b_i x^i.$$

Then by definition

$$f(x)+g(x) = \sum_{i\geq 0}(a_i + b_i)x^i.$$

Suppose that $\deg(f(x)) < \deg(g(x))$. Then in particular, $a_{\deg(f(x))} + b_{\deg(g(x))} = a_{\deg(f(x))}$, because $b_{\deg(f(x))} = 0$, hence $\deg(f(x)+g(x)) = \deg(f(x))$. Similarly if $\deg(g(x)) < \deg(f(x))$. Thus $\deg(f(x)+g(x)) \leq \max(\deg(f(x)), \deg(g(x)))$.

By definition of multiplication in $R[x]$, we see that $d = \deg(f(x)\cdot g(x))$ must be the largest integer such that if $i+j=d$, $a_i b_j \neq 0$. R is an integral domain, hence $a_i b_j = 0$ only if either $a_i = 0$ or $b_j = 0$. $\deg(f(x))$ is the largest i such that $a_i \neq 0$ and similarly $\deg(g(x))$ is the largest integer j such that $b_j \neq 0$, thus in particular we have $a_{\deg(f(x))} b_{\deg(g(x))} \neq 0$, with $d = \deg(f(x)\cdot g(x)) = \deg(f(x)) + \deg(g(x))$. □

1.15. ▷ Prove that $R[x]$ is an integral domain if and only if R is an integral domain. [§1.3]

Solution. Suppose that $R[x]$ is an integral domain. Polynomials of degree 0 are just a copy of R in $R[x]$, in particular, the operations on polynomials are identical to the operations in R for constants. If $r \in R[x]$ is a constant polynomial such that $r \neq 0$, then r is not a zero-divisor (because $R[x]$ is an integral domain), and thus it cannot be a zero-divisor in R.

On the other hand, let R be an integral domain and suppose that $R[x]$ is *not* an integral domain. Let $f(x), g(x)$ be polynomials such that $f(x) \cdot g(x) = 0$ and denote $n = \deg(f(x))$, $m = \deg(g(x))$. Since R is an integral domain, we know that $\deg(f(x) \cdot g(x)) = n+m'$, so let us consider the term $a_n b_m x^{n+m}$. By definition of the degree of a polynomial, we see that $a_n \neq 0$, $b_m \neq 0$. But R is an integral domain, which means $a_n b_m \neq 0$, contradicting our assumption that $f(x) \cdot g(x) = 0$. □

1.16. Let R be a ring, and consider the ring of power series $R[[x]]$ (cf. §1.3).

(i) Prove that a power series $a_0 + a_1 x + a_2 x^2 + \cdots$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R. What is the inverse of $1 - x$ in $R[[x]]$?

(ii) Prove that $R[[x]]$ is an integral domain if and only if R is.

Solution. Suppose that $a_0 + a_1 x + a_2 x^2 + \cdots$ is a unit in $R[[x]]$. Then there must be another power series $b_0 + b_1 x + b_2 x^2 + \cdots$ such that their multiple (on either side) is equal to 1. This implies $a_0 b_0 = b_0 a_0 = 1$ in R, and thus a_0 is a left-unit in R.

On the other hand, let a_0 be a unit in R. If $b_0 + b_1 x + b_2 x^2 + \cdots$ is to be an inverse of $a_0 + a_1 x + a_2 x^2 + \cdots$, then we must have $a_0 b_0 = 1$, and thus $b_0 = a_0^{-1}$ (which exists and is unique because a_0 is a unit in R). Notice that we can calculate the rest of the required coefficient recursively, for example $b_1 = -a_0^{-1}(a_1 b_0)$, or $b_2 = -a^{-1}(a_1 b_1 + a_2 b_0)$. In general, $b_n = -a_0^{-1} \sum_{i=1}^{n} a_i b_{n-1}$ for $n \geq 1$. This power series is thus an inverse of $a_0 + a_1 x + a_2 x^2 + \cdots$ in $R[[x]]$ (it works as both left- and right-inverse) and thus $a_0 + a_1 x + a_2 x^2 + \cdots$ is a unit in $R[[x]]$.

The inverse of $1 - x$ in $R[[x]]$ is $1 + x + x^2 + \cdots$.

One direction is immediate - if $R[[x]]$ is an integral domain, then in particular if $a_0, b_0 \in R$ then we can view them as two power series (such that $a_i = b_i = 0$ for $i \geq 1$), $a_0 \cdot b_0 = 0$ only if $a_0 = 0$ or $b_0 = 0$ in $R[[x]]$. But $\cdot$ in $R[[x]]]$ coincides with multiplication in R in this case and thus R is an integral domain.

Suppose that R is an integral domain. Let $f = a_0 + a_1 x + a_2 x^2 + \cdots, g = b_0 + b_1 x + b_2 x^2 + \cdots \in R[[x]]$ such that $f, g \neq 0$. Then we can choose a_i, b_j such that $a_i, b_j \neq 0$ $(0 \neq i, j)$ and i, j are the smallest such indices. Notice, that the first term of $f \cdot g$ must be $a_i b_j x^{i+j}$, precisely because i, j are the smallest indices such that a_i, b_j are non-zero. $a_i b_j$ is non-zero because R is an integral domain. Therefore $f \cdot g$ must be non-zero, showing that $R[[x]]$ is an integral domain. □

1.17. ▷ Explain in what sense $R[x]$ agrees with the monoid ring $R[\mathbb{N}]$. [§1.4]

Solution. Elements of $R[x]$ are polynomials - finite linear combinations of nonnegative 'powers' of x with coefficients in R:

$$f(x) = \sum_{i \geq 0} a_i x^i.$$

The definition of $R[\mathbb{N}]$ is very similar, the elements are also finite linear combinations with coefficients in R:

$$\sum_{n \in \mathbb{N}} a_n \cdot n.$$

In particular, we can interpret each power x^i as the nonnegative integer i, which gives us

$$\sum_{i \geq 0} a_i \cdot i,$$

which is clearly an element of $R[\mathbb{N}]$. □

2. The category Ring

2.1. ▷ Prove that if there is a homomorphism from a zero-ring to a ring R, then R is a zero-ring. [§2.1]

Solution. Let R be a ring, and $\varphi : \{*\} \to R$ a homomorphism from the zero-ring to R. φ must map the additive and multiplicative identities in $\{*\}$ to the additive and multiplicative identities in R. But since the zero-ring has only a single element, we must have $0 = \varphi(*) = 1$, which by Exercise 1.1 implies that R is a zero-ring. □

2.2. Let R and S be rings, and let $\varphi : R \to S$ be a function preserving both operations $+, \cdot$.

- Prove that if φ is *surjective*, then necessarily $\varphi(1_R) = 1_S$.
- Prove that if $\varphi \neq 0$ and S is an integral domain, then $\varphi(1_R) = 1_S$.

Solution. Suppose φ is surjective. Then there must be an element $r \in R$ such that $\varphi(r) = 1_S$. φ preserves multiplication, which means

$$\varphi(r) = \varphi(r \cdot 1_R) = \varphi(r) \cdot \varphi(1_R) = 1_S \cdot \varphi(1_R) = \varphi(1_R).$$

But that means $\varphi(1_R) = \varphi(r) = 1_S$.

Suppose that $\varphi \neq 0$ and S is an integral domain. Because $\varphi \neq 0$, there must be some $r \in R$ such that $\varphi(r) = s$ for some non-zero $s \in S$. Then in particular

$$s = \varphi(r) = \varphi(r \cdot 1_R) = \varphi(r) \cdot \varphi(1_R) = s \cdot \varphi(1_R).$$

S is an integral domain, which implies left-cancellation by non-zero elements holds, and thus $\varphi(1_R) = 1_S$. □

2.3. Let S be a set, and consider the power set ring $\mathscr{P}(S)$ (Exercise 1.2) and the ring $(\mathbb{Z}/2\mathbb{Z})^S$ you constructed in Exercise 1.3. Prove that these two rings are isomorphic. (Cf. Exercise I.2.11.)

Solution. The elements of $(\mathbb{Z}/2\mathbb{Z})^S$ are set-functions from S to $\mathbb{Z}/2\mathbb{Z}$. We have already shown in Exercise I.2.11 that there is a bijection between the functions from S to any set with two elements and $\mathscr{P}(S)$. It remains to show that the corresponding bijection is in fact a ring homomorphism.

The bijection φ maps subsets of S to the indicator functions $S \to \mathbb{Z}/2\mathbb{Z}$, such that if $A \subseteq S$, $\varphi(A) = i_A$, where

$$i_A(a) := \begin{cases} [1]_2 & a \in A \\ [0]_2 & a \notin A \end{cases}.$$

Let $A, B \subseteq S$. Then $\varphi(A+B) = i_{A+B}$ where $A+B = (A \cup B) \smallsetminus (A \cap B)$. $i_{A+B}(a) = [1]_2$ only if $a \in (A \cup B) \smallsetminus (A \cap B)$, which implies $a \in A \cup B$ and $a \notin A \cap B$. Thus we must have either $a \in A, a \notin B$ or $a \in B, a \notin A$. This clearly implies $i_{A+B}(a) = i_A + i_B$, because if $a \in A$ *and* $a \in B$, then $i_A(a) + i_B(a) = [1]_2 + [1]_2 = [0]_2$. Therefore $\varphi(A + B) = \varphi(A) + \varphi(B)$ and thus φ preserves addition.

Similarly, $i_{A \cdot B}(a) = [1]_2$ only if $a \in A \cap B$, hence only if $a \in A$, $a \in B$. $i_A \cdot i_B(a) = 1_A(a) \cdot i_B(a)$ which also can equal $[1]_2$ only when $a \in A$ and $a \in B$ (because multiplication by $[0]_2$ equals $[0]_2$). Thus $i_{A \cdot B} = i_A \cdot i_B$ and therefore $\varphi(A \cdot B) = \varphi(A) \cdot \varphi(B)$, showing that φ preserves multiplication.

The multiplicative identity in $\mathscr{P}(S)$ is S, $\varphi(S) = i_S$. As we have seen in Exercise 1.3, i_S is the identity with respect to multiplication in $(\mathbb{Z}/2\mathbb{Z})^S$ and thus φ preserves the multiplicative identity.

Thus φ is indeed a ring homomorphism, and because it is a bijection, $\mathscr{P}(S) \cong (\mathbb{Z}/2\mathbb{Z})^S$. □

2.4. Define functions $\mathbb{H} \to \mathfrak{gl}_4(\mathbb{R})$ and $\mathbb{H} \to \mathfrak{gl}_2(\mathbb{C})$ (cf. Exercises 1.4 and 1.12) by

$$a + bi + cj + dk \mapsto \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix},$$

$$a + bi + cj + dk \mapsto \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

for all $a, b, c, d \in \mathbb{R}$. Prove that both functions are injective ring homomorphisms. Thus, quaternions may be viewed as real or complex matrices.

Solution. It is clear that both functions are well-defined and that they are injective. We must show that they are ring homomorphisms. Both functions preserve addition, because addition is defined componentwise in all three rings $\mathbb{H}$, $\mathfrak{gl}_4(\mathbb{R})$, and $\mathfrak{gl}_2(\mathbb{C})$.

Multiplication requires some calculation work to check, but is not hard in any particular way. For example, if we have two quaternions $a_1 + b_1 i + c_1 j + d_1 k$, $a_2 + b_2 i + c_2 j + d_2 k$, it is immediately checked that the products of the corresponding matrices have $a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2$ and $(a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2)i$ respectively as the element in the first column of the first row. Thus both functions also preserve multiplication.

Multiplicative identity in $\mathbb{H}$ is just 1, and thus we immediately see that both functions preserve multiplicative identities.

Thus both functions are in fact injective ring homomorphisms. □

2.5. ¬ The *norm* of a quaternion $w = a + bi + cj + dk$, with $a, b, c, d \in \mathbb{R}$, is the real number $N(w) = a^2 + b^2 + c^2 + d^2$.

Prove that the function from the multiplication group $\mathbb{H}^*$ of nonzero quaternions to the multiplicative group $\mathbb{R}^+$ of positive real numbers, defined by assigning to each nonzero quaternion its norm, is a homomorphism. Prove that the kernel of this homomorphism is isomorphic to SU(2) (cf. Exercise II.6.3). [4.10, IV.5.17, V.6.19]

Solution. Notice that if $w = a + bi + cj + dk$ is a nonzero quaternion, then $N(w) = (a + bi + cj + dk)(a - bi - cj - dk)$. $a - bi - cj - dk$ is also a nonzero quaternion and is often denoted w^*. If w_1, w_2 are quaternions, then $(w_1 w_2)^* = w_2^* w_1^*$. Thus we have $N(w_1 w_2) = (w_1 w_2)(w_1 w_2)^* = (w_1 w_2)(w_2^* w_1^*) = w_1(w_2 w_2^*) w_1^* = w_1 N(w_2) w_1^* = N(w_1) N(w_2)$, showing that N is a group homomorphism (it preserves multiplication).

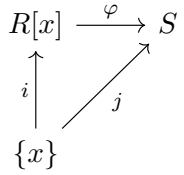
$\ker N$ is the set of quaternions $a + bi + cj + dk$ such that $a^2 + b^2 + c^2 + d^2 = 1$. In Exercise 2.4 we have seen that there is an injective homomorphism from $\mathbb{H}$ to $\mathfrak{gl}_2(\mathbb{C})$. Thus $\ker N$ as a subgroup of $\mathbb{H}$ is isomorphic to a subgroup of $\mathfrak{gl}_2(\mathbb{C})$, such that each quaternion is mapped to the corresponding complex matrix with $a^2 + b^2 + c^2 + d^2 = 1$. But in Exercise II.6.3 we have that such a set of matrices is isomorphic to SU(2). Thus $\ker N \cong \mathrm{SU}(2)$. □

2.6. ▷ Verify the 'extension property' of polynomial rings, stated in Example 2.3. [§2.2]

Solution. The property states that if $\alpha : R \to S$ is a fixed ring homomorphism, and $s \in S$ is an element such that $s\alpha(r) = \alpha(r)s$ for all $r \in R$, then there is a unique ring homomorphism $\overline{\alpha} : R[x] \to S$ extending α and sending x to s.

This is very similar to the universal property of polynomial rings discussed in the text for the case $n = 1$. However, we are not working with polynomial rings over $\mathbb{Z}$ but rather a generic ring R. There is also no requirement for S to be a commutative ring (besides the condition on α).

Taking our cue, we have set-functions $i : \{x\} \to R[x]$ defined by $i(x) = x$ and $j : \{x\} \to S$, $j(x) = s$. For the diagram



to commute we must have $\varphi(x) = s$. Since φ must be a ring homomorphism, necessarily

$$\begin{aligned}\varphi(\sum m_i x^i) &= \sum \varphi(m_i)\varphi(x)^i \\ &= \sum \varphi(m_i)s^i.\end{aligned}$$

The natural choice is to let $\varphi(r) = \alpha(r)$ for all $r \in R$, thus φ would in fact yield our extension $\overline{\alpha}$. Of course, φ does not necessarily have to equal α in general, but as an extension of α it would be unique (if it is indeed a ring homomorphism).

We then have

$$\begin{aligned}\varphi(\sum m_i x^i + \sum n_i x^i) &= \varphi(\sum (m_i + n_i)x^i) \\ &= \sum \alpha(m_i + n_i)s^i \\ &= \sum (\alpha(m_i) + \alpha(n_i))s^i \\ &= \sum \alpha(m_i)s^i + \sum \alpha(n_i)s^i \\ &= \varphi(\sum m_i x^i) + \varphi(\sum n_i x^i),\end{aligned}$$

the identity clearly sends 1 to 1, and multiplication is also preserved due to the commutativity condition on α:

$$\begin{aligned}\varphi(\sum m_i x^i \sum n_i x^i) &= \varphi(\sum\sum m_i n_j x^{i+j}) \\ &= \sum\sum \alpha(m_i n_j)s^{i+j} \\ &= \sum\sum \alpha(m_i)\alpha(n_j)s^i s^j \\ &= \sum\sum \alpha(m_i)s^i\alpha(n_j)s^j \\ &= \sum \alpha(m_i)s^i \cdot \sum \alpha(n_j)s^j \\ &= \varphi(\sum m_i x^i)\varphi(\sum n_i x^i)\end{aligned}$$

(the crucial step depends precisely on the fact that s commutes with $\alpha(r)$ for all $r \in R$). □

2.7. ▷ Let $R = \mathbb{Z}/2\mathbb{Z}$, and let $f(x) = x^2 - x$; note $f(x) \neq 0$. What is the polynomial function $R \to R$ determined by $f(x)$? [§2.2, §V.4.2, §V.5.1]

Solution. $f([0]_2) = f([1]_2) = [0]_2$, so $f(r) = 0$ for $r \in R$, even when $f(x)$ is not a zero polynomial. □

2.8. Prove that every subring of a field is an integral domain.

Solution. Suppose F is a field, $R \subseteq F$ a subring. Let $a, b \in R$, and suppose $ab = 0$ and $a, b \neq 0$. Then in particular a and b are two-sided units in F, and therefore there are inverses $a^{-1}, b^{-1} \in F$. Then (in F) we have $0 = a^{-1}(ab) = (a^{-1}a)b = b$, a contradiction. Similarly $0 = (ab)b^{-1} = a(bb^{-1}) = a$, again, a contradiction. Therefore we must have either $a = 0$ or $b = 0$, showing that R is an integral domain. □

2.9. ¬ The *center* of a ring R consists of the elements a such that $ar = ra$ for all $r \in R$. Prove that the center is a subring of R.

Prove that the center of a division ring is a field. [2.11, IV.2.17, VII.5.14, VII.5.16]

Solution. Let R be a ring, C its center. Clearly, $C \subseteq R$ by definition. Let $a, b \in C$, $r \in R$. We have

$$\begin{aligned}(a - b)r &= ar - br \\ &= ra - rb \\ &= r(a - b)\end{aligned}$$

showing that $(C, +)$ is a subgroup of $(R, +)$. Similarly,

$$\begin{aligned}(ab)r &= a(br) \\ &= a(rb) \\ &= (ar)b \\ &= (ra)b \\ &= r(ab)\end{aligned}$$

showing that C is closed with respect to $\cdot$. Lastly, 1_R commutes with all $r \in R$ and thus $1_R \in C$. Therefore C is in fact a subring of R.

C is a commutative ring, because for any $a, b \in C$ we must have $ab = ba$ by the definition of a center. Thus it is enough to check that a center of a division ring is again a division ring. Assume that R is a division ring, and let $c \in C$. In particular, $c \in R$ and thus c is a two-sided unit in R, meaning we have a unique inverse $c^{-1} \in R$. $cr = rc$ implies $c^{-1}(cr) = c^{-1}(rc)$, hence $r = c^{-1}rc$ and thus $rc^{-1} = c^{-1}r$, showing that $c^{-1} \in C$. But C is a subring of R and thus preserves multiplication, therefore c is in fact a two-sided unit in C, proving that C is a field. □

2.10. ¬ The *centralizer* of an element a of a ring R consists of the elements $r \in R$ such that $ar = ra$. Prove that the centralizer of a is a subring of R, for every $a \in R$.

Prove that the center of R is the intersection of all its centralizers.

Prove that every centralizer in a division ring is a division ring. [2.11, IV.2.17, VII.5.16]

Solution. Suppose R is a ring and let C_a denote the centralizer of a in R. Let $a \in R$ be arbitrary. Clearly $C_a \subseteq R$. Let $x, y \in C_a$. $(x-y)a = xa-ya = ax-ay = a(x-y)$ showing that $x-y \in C_a$ so that $(C_a, +)$ is a subgroup of $(R, +)$. Similarly, $(xy)a = x(ay) = a(xy)$ so that $xy \in C_a$. 1_R commutes with a and thus $1_R \in C_a$. Therefore C_a is a subring of R.

Let C be the center of R, and suppose $c \in R$. Then by definition of a center, $cr = rc$ for all $r \in C$. Let $a \in R$ be arbitrary. Then $ca = ac$ and thus $c \in C_a$. Therefore c is an element of the intersection of all centralizers of R. Similarly, suppose c is an element of the intersection of the centralizers. Let $r \in R$ be arbitrary. Then in particular $c \in C_r$ and thus $cr = rc$, showing that $c \in C$. Thus C is in fact the intersection of all centralizers of R.

Assume R is a division ring, $a \in R$, $r \in C_a$ arbitrary. Then $r \in R$ and thus we have an inverse $r^{-1} \in R$. $ar = ra$ implies $r^{-1}(ar)r^{-1} = r^{-1}(ra)r^{-1}$ and hence $r^{-1}a = ar^{-1}$ showing that $r^{-1} \in C_a$. Thus r is a two-sided unit in C_a, showing that C_a is a division ring. □

2.11. ¬ Let R be a division ring consisting of p^2 elements, where p is a prime. Prove that R is commutative, as follows:

- If R is not commutative, then its center C (Exercise 2.9) is a proper subring of R. Prove that C would then consist of p elements.
- Let $r \in R$, $r \notin C$. Prove that the centralizer of r (Exercise 2.10) contains both r and C.
- Deduce that the centralizer of r is the whole of R.
- Derive a contradiction, and conclude that R had to be commutative (hence, a field).

This is a particular case of Wedderburn's theorem: every finite division ring is a field. [IV.2.17, VII.5.16]

Solution. Suppose that R is not commutative. Then the center C of R must be a proper subring of R. This implies $(C, +)$ is a proper subgroup of $(R, +)$. The order of $(C, +)$ must divide the order of $(R, +)$, which is p^2. There are only two choices, 1 and p. But the order cannot be 1 as $(C, +)$ must contain both 0_R and 1_R (because C is a subring of R), thus C must have exactly p elements.

Let $r \in R$, $r \notin C$. $r \in C_r$ because trivially $rr = rr$. Let $c \in C$. Then in $cr = rc$ because C is the center of R, and thus $c \in C_r$. Thus C_r contains both r and C.

Centralizers are subrings, and thus by the same argument as in the first paragraph we see that C_r must contain p^2 elements, because $C \subsetneq C_r$. Therefore the centralizer of r is in fact the whole of R.

This is however a contradiction. $C_r = R$ implies that r commutes with all $r \in R$ and thus r must be in C, contradicting our assumption that $r \notin C$. But this means C must be the whole of R, and thus R has to be commutative. □

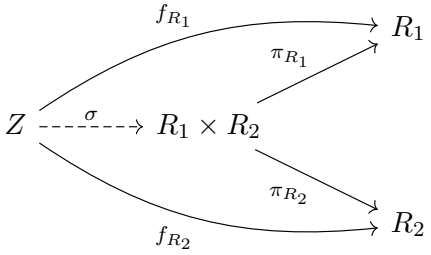
2.12. ▷ Consider the inclusion map $\iota : \mathbb{Z} \to \mathbb{Q}$. Describe the cokernel of ι in Ab and its cokernel in Ring (as defined by the appropriate universal property in the style of the one given in §II.8.6). [§2.3, §5]

Solution. Interpreting $\mathbb{Z}$ and $\mathbb{Q}$ as abelian groups we see that $\operatorname{coker} \iota = \frac{\mathbb{Q}}{\operatorname{im} \iota} = \frac{\mathbb{Q}}{\mathbb{Z}}$, i.e. all fractions $0 < \frac{a}{b} < 1$.

For the Ring case, consider any ring homomorphism $\varphi : \mathbb{Q} \to R$ such that $\varphi \circ \iota = 0_R$. In particular, for all $z \in \mathbb{Z}$ we have $\varphi(\iota(z)) = 0_R$ which implies $\varphi(1) = 0_R$. But φ must be a ring homomorphism and thus must preserve the multiplicative identity. Therefore R must be the zero-ring. In fact, the cokernel of any ring homomorphism is the zero-ring. □

2.13. ▷ Verify that the 'componentwise' product $R_1 \times R_2$ of two rings satisfies the universal property for products in a category, given in §I.5.4. [§2.4]

Solution. This is straightforward, first notice that $\pi_{R_1} : R_1 \times R_2 \to R_1$ and $\pi_{R_2} : R_1 \times R_2 \to R_2$, the natural projections, are in fact ring homomorphisms. Let Z be a ring, $f_{R_1} : Z \to R_1$, $f_{R_2} : Z \to R_2$ ring homomorphisms. We will show that there is a unique ring homomorphism $\sigma : Z \to R_1 \times R_2$ making the diagram



commute. Similarly to the case for Grp, the definition of σ is forced upon us by the required commutativity of the diagram. We must have $\sigma(z) = (f_{R_1}(z), f_{R_2}(z))$ for all $z \in Z$. As we have seen, σ is in particular a group homomorphism of $(Z, +)$ and $(R_1 \times R_2, +)$. $\sigma(1_Z) = (1_{R_1}, 1_{R_2})$ because f_{R_1} and f_{R_2} are ring homomorphisms.

It remains to show that σ preserves multiplication. Let $z_1, z_2 \in Z$. Then

$$\begin{aligned}\sigma(z_1 z_2) &= (f_{R_1}(z_1 z_2), f_{R_2}(z_1 z_2)) \\ &= (f_{R_1}(z_1) f_{R_1}(z_2), f_{R_2}(z_1) f_{R_2}(z_2)) \\ &= (f_{R_1}(z_1), f_{R_2}(z_1))(f_{R_1}(z_2), f_{R_2}(z_2)) \\ &= \sigma(z_1)\sigma(z_2),\end{aligned}$$

showing that σ is indeed a ring homomorphism. Uniqueness was forced upon us by the required commutativity, and thus $R_1 \times R_2$ in fact satisfies the universal property of products in Ring. □

2.14. ▷ Verify that $\mathbb{Z}[x_1, x_2]$ (along with the evident morphisms) satisfies the universal property for the coproduct of two copies of $\mathbb{Z}[x]$ in the category of *commutative* rings. Explain why it does not satisfy it in Ring. [§2.4]

Solution. The evident morphisms are $i_1 : \mathbb{Z}[x] \to \mathbb{Z}[x_1, x_2]$, defined as $i_1(\sum m_i x^i) = \sum m_i x_1^i$, and $i_2 : \mathbb{Z}[x] \to \mathbb{Z}[x_1, x_2]$ defined analogously. Let R be a commutative ring, $f_1, f_2 : \mathbb{Z}[x] \to R$ ring homomorphisms. Then in particular there must be elements $r, s \in R$ such that $f_1(x) = r$, $f_2(x) = s$.

By the universal property of polynomial rings, there is a unique homomorphism $\sigma : \mathbb{Z}[x_1, x_2] \to R$ such that

$$\sigma(\sum m_{i,j} x_1^i x_2^j) = \sum \iota(m_{i,j}) s^i r^j = \sum \iota(m_{i,j}) f_1(x)^i f_2(x)^j,$$

and

$$\begin{aligned}\sigma \circ i_1(\sum m_i x^i) &= \sigma(\sum m_i x_1^i) = \sum \iota(m_i) f_1(x)^i = f_1(\sum m_i x^i) \\ \sigma \circ i_2(\sum m_i x^i) &= \sigma(\sum m_i x_2^i) = \sum \iota(m_i) f_2(x)^i = f_2(\sum m_i x^i),\end{aligned}$$

proving that $\mathbb{Z}[x_1, x_2]$ satisfies the universal property of a coproduct of $\mathbb{Z}[x]$ by itself in the category of commutative rings.

If R is not commutative, there is no guarantee r and s are going to commute. In fact, if r and s do not commute, there is no ring homomorphism $\mathbb{Z}[x_1, x_2] \to R$ such that $x_1 \mapsto r$, $x_2 \mapsto s$, because any such function would not preserve multiplication. □

2.15. ▷ For $m > 1$ the abelian groups $(\mathbb{Z}, +)$ and $(m\mathbb{Z}, +)$ are manifestly isomorphic: the function $\varphi : \mathbb{Z} \to m\mathbb{Z}$, $n \mapsto mn$ is a group isomorphism. Use this isomorphism to transfer the structure of 'ring without identity' $(m\mathbb{Z}, +, \cdot)$ back onto $\mathbb{Z}$: give an explicit formula for the 'multiplication' $\bullet$ this defines on $\mathbb{Z}$ (that is, such that $\varphi(a \bullet b) = \varphi(a) \cdot \varphi(b)$). Explain why structures induced by different positive integers m are nonisomorphic as 'rings without 1'.

(This shows that there are many different ways to give a structure of ring without identity to the *group* $(\mathbb{Z}, +)$. Compare this observation with Exercise 2.16.) [§2.1]

Solution. Define $\bullet$ as $a \bullet b = m(a \cdot b)$. Then $\varphi(a \bullet b) = \varphi(m(a \cdot b)) = m^2(a \cdot b) = (ma) \cdot (mb) = \varphi(a) \cdot \varphi(b)$. This gives us a 'ring without identity' structure on $\mathbb{Z}$, as the operation is clearly associative, and distributivity is easily checked as

$$(a + b) \bullet c = m((a + b) \cdot c) = m(a \cdot c + b \cdot c) = m(a \cdot c) = m(b \cdot c) = a \bullet c + b \bullet c$$

and similarly

$$a \bullet (b + c) = m(a \cdot (b + c)) = m(a \cdot b + a \cdot c) = m(a \cdot b) + m(a \cdot c) = a \bullet b + a \bullet c.$$

Let $(R_1, +, \bullet_1)$ be such a structure for $m_1 > 1$, $(R_2, +, \bullet_2)$ for $m_2 > 1$, with $m_1 \neq m_2$. Suppose that $\varphi : R_1 \to R_2$ is a ring isomorphism (in the ring without identity sense). Let $\varphi(1) = x$. Then $\varphi(n) = \varphi(n1) = n\varphi(1) = nx$ for all $n \in \mathbb{Z}$. In particular, $\varphi(m_1) = m_1 x$. We then have

$$m_1 x = \varphi(m_1) = \varphi(1 \bullet_1 1) = \varphi(1) \bullet_2 \varphi(1) = m_2(\varphi(1) \cdot \varphi(1)) = m_2 x^2,$$

hence $\varphi(m_1) = \varphi(m_2 x)$. φ is an isomorphism, and thus we must have $m_1 = m_2 x$, showing that m_2 divides m_1. Similarly we can show that m_1 divides m_2 using the inverse of φ. But since m_1 and m_2 are positive integers, $m_1 = m_2$, a contradiction. □

2.16. ▷ Prove that there is (up to isomorphism) only one structure of a ring *with identity* on the abelian group $(\mathbb{Z}, +)$. (Hint: Let R be a ring whose underlying group is $\mathbb{Z}$. By Proposition 2.7, there is an injective ring homomorphism $\lambda : R \to \mathrm{End}_{\mathsf{Ab}}(R)$, and the latter is isomorphic to $\mathbb{Z}$ by Proposition 2.6. Prove that λ is surjective.) [§2.1, 2.15]

Solution. Let R be a ring whose underlying group is $(\mathbb{Z}, +)$. By Proposition 2.7, there is an injective ring homomorphism $\lambda : R \to \mathrm{End}_{\mathsf{Ab}}(R)$, $\lambda(r) = \lambda_r$ for all $r \in R$. The underlying group of R is $\mathbb{Z}$, hence we can interpret λ as a function $R \to \mathrm{End}_{\mathsf{Ab}}(\mathbb{Z})$ instead. Let $\varphi \in \mathrm{End}_{\mathsf{Ab}}(\mathbb{Z})$. Then $\varphi : \mathbb{Z} \to \mathbb{Z}$ is a group homomorphism, and we must have $\varphi(z) = z\varphi(1) = \varphi(1)z$ for $z \in \mathbb{Z}$ (because in $(\mathbb{Z}, +)$ $an = na$ for all $n, a \in \mathbb{Z}$), and thus $\varphi = \lambda_{\varphi(1)}$. Therefore λ is surjective. But $\mathrm{End}_{\mathsf{Ab}}(\mathbb{Z})$ is isomorphic to $\mathbb{Z}$ (as a ring) by Proposition 2.6. Therefore $R \cong \mathbb{Z}$. □

2.17. ¬ Let R be a ring, and let $E = \mathrm{End}_{\mathsf{Ab}}(R)$ be the ring of endomorphisms of the underlying abelian group $(R, +)$. Prove that the center of E is isomorphic to a subring of the center of R. (Prove that if $\alpha \in E$ commutes with all right-multiplications by elements of R, then α is left-multiplication by an element of R; then use Proposition 2.7.)

Solution. Denote $C(R)$ and $C(E)$ as the center of R and E respectively. Let $\alpha \in E$ and suppose that α commutes with all right-multiplications by elements of R. In particular, for $r \in R$ we have $\alpha \circ \mu_r = \mu_r \circ \alpha$. Therefore $\alpha(r) = \alpha \circ \mu_r(1_R) = \mu_r \circ \alpha(1_R) = \alpha(1_R)r$, hence α is in fact left-multiplication by $\alpha(1_R)$.

By Proposition 2.7, there is an injective ring homomorphism $\lambda : R \to E$. Notice, that every element $\alpha \in C(E)$ must necessarily commute with all right-multiplications by elements of R, and therefore α is a left-multiplication by an element of R. Because λ is injective, this means there must be a unique element $a \in R$ such that $\lambda(a) = \alpha$ and $a = \alpha(1_R)$.

Let $r \in R$. Then because α commutes with μ_r we have

$$\alpha(1_R)r = \alpha(r) = \alpha \circ \mu_r(1_R) = \mu_r \circ \alpha(1_R) = \mu_r(\alpha(1_R)) = r\alpha(1_R)$$

and thus a commutes with every element of R and is therefore an element of the center of R.

We then have a set-function $\varphi : C(E) \to C(R)$, defined by $\varphi(\alpha) = \alpha(1_R)$. This set-function is well-defined by the preceding considerations. Let $\alpha, \beta \in C(E)$. Then $\varphi(\alpha + \beta) = (\alpha+\beta)(1_R) = \alpha(1_R)+\beta(1_R) = \varphi(\alpha)+\varphi(\beta)$, and thus φ is a group homomorphism. $\varphi(\alpha \circ \beta) = \alpha(\beta(1_R)) = \alpha(1_R)\beta(1_R)$. $\varphi(\mathrm{id}_{C(E)}) = \mathrm{id}_{C(E)}(1_R) = 1_R$. Therefore φ is a ring homomorphism.

Notice, that if $\alpha \neq \beta$, then there is some $r \in R$ such that $\alpha(1_R)r = \alpha(r) \neq \beta(r) = \beta(1_R)r$. But that means $\alpha(1_R) \neq \beta(1_R)$ and thus $\varphi(\alpha) \neq \varphi(\beta)$. Therefore we have an injective ring homomorphism $C(E) \hookrightarrow C(R)$ and thus $C(E)$ is in fact isomorphic to a subring of $C(R)$ (it *is not* a subring as $C(E)$ and $C(R)$ do not share the same underlying set). □

2.18. ▷ Verify the statements made about right-multiplication μ, following Proposition 2.7. [§2.5]

Solution. Let $r, s, a \in R$. We have $\mu_{r+s}(a) = a(r + s) = ar + as = \mu_r(a) + \mu_s(a)$ and $\mu_{rs}(a) = a(rs) = (ar)s = \mu_r(a)s = \mu_s \circ \mu_r(a)$. $\mu_1(a) = a1 = a$ and thus $\mu_1 = \mathrm{id}_R$. □

2.19. Prove that for $n \in \mathbb{Z}$ a positive integer, $\mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ *as a ring.*

Solution. Consider the function $\varphi : \mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$ defined by $\varphi(\alpha) = \alpha([1]_n)$ for all group homomorphisms $\alpha : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. φ is clearly a group homomorphism, as the addition in $\mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ is defined so that for all $z \in \mathbb{Z}/n\mathbb{Z}$

$$(\alpha + \beta)(z) = \alpha(z) + \beta(z)$$

and in particular

$$\varphi(\alpha + \beta) = (\alpha + \beta)([1]_n) = \alpha([1]_n) + \beta([1]_n) = \varphi(\alpha) + \varphi(\beta).$$

Let $\alpha(1) = [a]_n$. Notice, that for any $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ we have

$$\alpha([b]_n) = \alpha(b[1]_n) = b\alpha([1]_n) = b[a]_n = [ba]_n = [ab]_n = a[b]_n$$

and thus in particular

$$\alpha(\beta([1]_n)) = a\beta([1]_n) = \alpha([1]_n)\beta([1]_n).$$

Therefore,

$$\varphi(\alpha \circ \beta) = \alpha \circ \beta([1]_n) = \alpha([1]_n)\beta([1]_n) = \varphi(\alpha)\varphi(\beta)$$

as required. Clearly, $\varphi(\mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}) = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}([1]_n) = [1]_n$. Thus φ is a ring homomorphism.
For $[a]_n \in \mathbb{Z}/n\mathbb{Z}$, let $\psi([a]_n)$ be the homomorphism $\alpha : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by

$$(\forall [b]_n \in \mathbb{Z}/n\mathbb{Z}) : \quad \alpha(n) = a[b]_n.$$

For $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$ we have

$$\begin{aligned}\psi([a]_n + [b]_n)([c]_n) &= \psi([a+b]_n)([c]_n) \\ &= (a+b)[c]_n = a[c]_n + b[c]_n = [ac]_n + [bc]_n \\ &= \psi([a]_n)([c]_n) + \psi([b]_n)([c]_n) \\ &= (\psi([a]_n) + \psi([b]_n))([c]_n)\end{aligned}$$

showing that ψ is a group homomorphism. Similarly,

$$\begin{aligned}\psi([a]_n[b]_n)([c]_n) &= \psi([ab]_n)([c]_n) \\ &= (ab)[c]_n = a(b[c]_n) \\ &= a\psi([b]_n)([c]_n) \\ &= \psi([a]_n) \circ \psi([b]_n)([c]_n).\end{aligned}$$

Lastly, $\psi([1]_n)([a]_n) = 1[a]_n = [a]_n$ and thus $\psi([1]_n) = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$. Thus ψ is a ring homomorphism.
Let $[a]_n \in \mathbb{Z}/n\mathbb{Z}$, $\alpha \in \mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z})$, then

$$\varphi \circ \psi([a]_n) = \psi([a]_n)([1]_n) = a[1]_n = [a]_n$$

and similarly

$$\psi \circ \varphi(\alpha)([a]_n) = \psi(\alpha([1]_n))([a]_n) = \alpha([1]_n)[a]_n = \alpha([a]_n)$$

showing that ψ is an inverse of φ, proving that φ is an isomorphism and thus $\mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. □

3. Ideals and quotient rings

3.1. Prove that the image of a ring homomorphism $\varphi : R \to S$ is a subring of S. What can you say about φ if its image is an ideal of S? What can you say about φ if its kernel is a subring of R?

Solution. Suppose R, S are rings, $\varphi : R \to S$ a ring homomorphism. Then in particular, φ is a group homomorphism of the underlying abelian groups $(R, +)$ and $(S, +)$, thus $\operatorname{im}\varphi$ is a subgroup of $(S, +)$. Let $s, s' \in \operatorname{im}\varphi$. Then we have $r, r' \in R$ such that $\varphi(r) = s$, $\varphi(r') = s'$. Because φ is a ring homomorphism we have $\varphi(rr') = \varphi(r)\varphi(r') = ss'$, $\varphi(rr') \in \operatorname{im}\varphi$, hence $ss' \in \operatorname{im}\varphi$, and thus $\operatorname{im}\varphi$ is closed with respect to multiplication. We also have $\varphi(1_R) = 1_S$ and thus $1_S \in \operatorname{im}\varphi$, showing that $\operatorname{im}\varphi$ is indeed a subring of S.

Suppose that $\operatorname{im}\varphi$ is an ideal of S. Then since $1_S \in \operatorname{im}\varphi$, for arbitrary $s \in S$ we have $s \in \operatorname{im}\varphi$ and thus $\operatorname{im}\varphi = S$. Therefore φ is surjective, and by the first isomorphism theorem $S = R/\ker\varphi$.

Suppose that $\ker\varphi$ is a subring of R. Then in particular $1_R \in \ker\varphi$, and since $\ker\varphi$ is an ideal of R, $\ker\varphi$ must in fact be the whole R. Thus $\varphi = 0$. □

3.2. ▷ Let $\varphi : R \to S$ be a ring homomorphism, and let J be an ideal of S. Prove that $I = \varphi^{-1}(J)$ is an ideal of R. [§3.1]

Solution. J is a subgroup of $(S, +)$ and thus I must be a subgroup of $(R, +)$ (by Lemma II.6.4). Let $i \in I$, $r \in R$. Then $\varphi(ir) = \varphi(i)\varphi(r)$ and since $\varphi(i) \in J$, $\varphi(ir) \in J$, and thus $ir \in I$. Similarly for ri. Thus I is in fact an ideal of R. □

3.3. ¬ Let $\varphi : R \to S$ be a ring homomorphism, and let J be an ideal of R.

- Show that $\varphi(J)$ need to be an ideal of S.
- Assume that φ is surjective, then prove that $\varphi(J)$ *is* an ideal of S.
- Assume that φ is surjective, and let $I = \ker\varphi$; thus we may identify S with R/I. Let $\overline{J} = \varphi(J)$, an ideal of R/I by the previous point. Prove that

$$\frac{R/I}{\overline{J}} \cong \frac{R}{I + J}.$$

(Of course this is just a rehash of Proposition 3.11.) [4.11]

Solution. Let $\varphi : R \to S$ be a ring homomorphism, J an ideal of R.

- Consider $\varphi : \mathbb{Z} \to \mathbb{Q}$ defined as $\varphi(z) = z$. $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$, but it is not an ideal of $\mathbb{Q}$, because $\frac{1}{2} \cdot 2 \notin 2\mathbb{Z}$.
- Assume that φ is surjective. Let $j \in J, r \in R$. Then $rj \in J$ and thus $\varphi(rj) = \varphi(r)\varphi(j) \in \varphi(J)$. Let $s \in S$. Then there is $r \in R$ such that $\varphi(r) = s$ because φ is surjective. But then $s\varphi(j) \in \varphi(J)$ by the previous consideration and thus $\varphi(J)$ is a left-ideal of S. Similarly, it must be a right-ideal of S.
- Again, assume that φ is surjective, let $I = \ker\varphi$. Then $S \cong R/I$. Let $\overline{J} = \varphi(J)$, which by the previous point is an ideal of R/I.

Notice, that $I \subseteq I + J$ because any ideal must contain 0 (since it must be in particular a subgroup of the corresponding abelian group). Thus

$$I \subseteq \ker(R \to \frac{R}{I+J})$$

and therefore we have an induced ring homomorphism

$$\sigma : \frac{R}{I} \to \frac{R}{I+J}$$

by Theorem 3.8. Explicitly $\sigma(r+I) = r+(I+J)$ and it is clear σ must be surjective (because $I \subseteq I + J$). We have

$$\begin{aligned}
\ker \sigma &= \{r + I \mid \sigma(r + I) = I + J\} \\
&= \{r + I \mid r + (I + J) = (I + J)\} \\
&= \{r + I \mid r \in I + J\} \\
&= \{r + I \mid r = i + j, i \in I, j \in J\} \\
&= \{s \in S \mid \varphi(i + j) = s, i \in I, j \in J\} \\
&= \{s \in S \mid \varphi(j) = s\} \\
&= \varphi(J) \\
&= \overline{J}
\end{aligned}$$

showing that the required isomorphism holds by Corollary 3.10.

□

3.4. Let R be a ring such that every subgroup of $(R, +)$ is in fact an ideal of R. Prove that $R \cong \mathbb{Z}/n\mathbb{Z}$, where n is the characteristic of R.

Solution. Consider the ring homomorphism $f : \mathbb{Z} \to R$ defined by $a \mapsto a \cdot 1_R$ introduced in the text. The image of the homomorphism is a subring of R, by Exercise 3.1. In particular the subgroup corresponding to $\operatorname{im} f$ is an ideal by our assumption. But since $1_R \in \operatorname{im} f$, $\operatorname{im} f = R$, and thus f is surjective. Hence $R \cong \mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z}$ where n is the characteristic of R, by Corollary 3.10. □

3.5. ¬ Let J be a *two-sided* ideal of the ring $\mathcal{M}_n(R)$ of $n \times n$ matrices over a ring R. Prove that a matrix $A \in \mathcal{M}_n(R)$ belongs to J if and only if the matrices obtained by placing any entry of A in any position, and 0 elsewhere, belong to J. (Hint: Carefully contemplate the operation $\left(\begin{smallmatrix} 0&0&0\\0&0&0\\1&0&0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a&b&c\\d&e&f\\g&h&i \end{smallmatrix}\right)\left(\begin{smallmatrix} 0&0&0\\1&0&0\\0&0&0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0&0&0\\0&0&0\\b&0&0 \end{smallmatrix}\right)$.) [3.6]

Solution. Let J be a two-sided ideal of the ring $\mathcal{M}_n(R)$. Let $A \in \mathcal{M}_n(R)$.

Suppose $A \in J$. Notice, that we can obtain any matrix of the given form (a single entry of A in any position, and 0 elsewhere) by multiplying A by a certain matrix on the left and another matrix on the right. Multiplying A on the left by a matrix which has a single entry 1 in any place and 0 elsewhere 'selects a row' of A and 'moves it to another row', as in

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ a & b & c \end{pmatrix},$$

where the matrix on the left 'selected the first row and moved it to the last row'. Similarly, having such a matrix with a single row, we can use another matrix to multiply it on the right and obtain a matrix with a single entry of the original matrix A and 0 elsewhere, 'selecting a single column and choosing one entry in the row', as in

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ a & b & c \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ b & 0 & 0 \end{pmatrix}.$$

In general, multiplying A with a matrix having a single entry 1 in the (n, m)-th place 'selects' the m-th row of A and 'moves it' to the n-th row in the resulting matrix. Multiplying the result by a matrix having a single entry 1 in the (n, m)-th place then 'selects' the n-th entry in the only non-zero row moves it to the m-th row of the resulting matrix, which has 0 in all other entries.

Since J is a two-sided ideal, all such products must in fact be in J.

On the other hand, if all matrices of the given form are in J, then so must be the matrices with a single entry of A in the 'original' place and 0 elsewhere. Since ideals are in fact subgroups of the underlying abelian group, the sum of all such matrices, which is A, must also be in J. □

3.6. ¬ Let J be a two-sided ideal of the ring $\mathcal{M}_n(R)$ of $n \times n$ matrices over a ring R, and let $I \subseteq R$ be the set of $(1, 1)$ entries of matrices in J. Prove that I is a two-sided ideal of R and J consists precisely of those matrices whose entries all belong to I. (Hint: Exercise 3.5.) [3.9]

Solution. Let $i \in I, r \in R$. Then we have a matrix $A \in J$ such that the $(1, 1)$ entry is i. Consider the matrix $B \in \mathcal{M}_n(R)$ such that A the $(1, 1)$ entry is r and all other entries are 0. Because J is a two-sided ideal, we must then have the matrices $A + B \in J$ and $B + A \in J$ with $i + r$ and $r + i$ respectively as the $(1, 1)$ entry, and thus $i + r, r + i \in I$. Similarly, $AB \in J$ and $BA \in J$ and the $1, 1)$ entries are ir and ri respectively, showing that $ir, ri \in I$. Showing that I is in fact a subgroup of $(R, +)$ is trivial (identity is 0_R, associativity and inverses all follow). Thus I is in fact a two-sided ideal of R.

Let $A \in J$ be arbitrary. Then in particular all matrices having a single entry of A as the $(1,1)$ entry and 0 elsewhere must be in J by Exercise 3.5, and thus all entries of A must in fact belong to I.

On the other hand, if A is a matrix whose all entries belong to I, then in particular there must be a matrix with each such entry i in the $(1,1)$-th place in J (by definition of I). Since we can 'move' an entry from the $(1,1)$-th place to an arbitrary place by multiplication on the left or the right by another matrix, and J is a two-sided ideal (so such products again belong to J), it follows that $A \in J$ by Exercise 3.5. □

3.7. Let R be a ring, and let $a \in R$. Prove that Ra is a left-ideal of R and aR is a right-ideal of R. Prove that a is a left-, resp. right-, unit if and only if $R = aR$, resp. $R = Ra$.

Solution. Let $s \in R, b \in Ra$. Then $b = ra$ for some $r \in R$. We have $sb = s(ra) = (sr)a \in Ra$, showing that Ra is a left-ideal of R. Similarly for aR.

Suppose that a is a left-unit. Then there is an element $r \in R$ such that $ar = 1_R$. Since aR is a right-ideal of R, we must in particular have $1_R = ar \in aR$. But $1_R \in aR$ implies $aR = R$. On the other hand, suppose $aR = R$. Then there must be an element $r \in R$ such that $ar = 1_R$, showing that a is a left-unit.

Similarly for right-units. □

3.8. ▷ Prove that a ring R is a division ring if and only if its only left-ideals and right-ideals are $\{0\}$ and R.

In particular, a commutative ring R is a field if and only if the only ideals of R are $\{0\}$ and R. [3.9, §4.3]

Solution. Let R be a ring. Suppose that R is a division ring, and let $I \subseteq R$ be a left-ideal. Let $i \in I$, $i \neq 0$, then there is an element $r \in R$ such that $ri = 1_R$ (because $i \in R$ and since R is a division ring, i is a unit). But $1_R = ri \in I$ (since I is a left-ideal), hence $I = R$. Therefore the only left-ideals of R are $\{0\}$ and R itself. Similarly for right-ideals.

On the other hand, suppose that the only left-ideals and right-ideals of R are $\{0\}$ and R. Let $a \in R$, $a \neq 0$. Then aR is a right-ideal of R (by Exercise 3.7), we have $aR \neq \{0\}$, and hence $aR = R$. But by Exercise 3.7 this implies a is a left-unit. Similarly Ra is left-ideal such that $Ra = R$, and thus a is a right-unit. Therefore R is a division ring. □

3.9. ¬ Counterpoint to Exercise 3.8: It is *not* true that a ring R is a division ring if and only if its only two-sided ideals are $\{0\}$ and R. A nonzero ring with this property is said to be simple; by Exercise 3.8, fields are the only simple *commutative* rings, and division rings are simple.

Prove that $\mathcal{M}_n(\mathbb{R})$ is simple. (Use Exercise 3.6.) [4.20]

Solution. Let J be a two-sided ideal of $\mathcal{M}_n(\mathbb{R})$. In Exercise 3.6 we have seen that the set $I \subseteq \mathbb{R}$ of the $(1,1)$ entries of matrices in J is a two-sided ideal of $\mathbb{R}$. But $\mathbb{R}$ is a field, and is therefore simple. But that implies either $I = \{0\}$ or $I = \mathbb{R}$. Again, by Exercise 3.6, we know that J consists precisely of those matrices whose entries all belong to I. If $I = \{0\}$, the only such matrix is the zero-matrix, and thus J is a singleton (only containing the zero-matrix). If $I = \mathbb{R}$, then J must be the whole of $\mathcal{M}_n(\mathbb{R})$. Thus $\mathcal{M}_n(\mathbb{R})$ is simple.

Notice however, that $\mathcal{M}_n(\mathbb{R})$ is *not* a division ring, as not all $n \times n$ matrices with entries in $\mathbb{R}$ are invertible. □

3.10. ▷ Let $\varphi : k \to R$ be a ring homomorphism, where k is a field and R is a nonzero ring. Prove that φ is *injective*. [§V.4.2, §V.5.2]

Solution. A ring homomorphism is injective if and only if the kernel is $\{0\}$. Kernels are ideals and ass we have seen in Exercise 3.9, fields are simple, and thus the only ideals of k are $\{0\}$ and k itself. But φ is a ring homomorphism, hence $\varphi(1_k) = 1_R$, thus $\ker \varphi \neq k$ and therefore $\ker \varphi = \{0\}$, showing that φ is in fact injective.

Notice that the same argument works for a homomorphism from any simple ring to a nonzero ring. □

3.11. Let R be a ring containing $\mathbb{C}$ as a subring. Prove that there are no ring homomorphisms $R \to \mathbb{R}$.

Solution. Suppose $\varphi : R \to \mathbb{R}$ is a ring homomorphism. Since $\mathbb{C}$ is a subring of R, $1_R = 1$. We have $\varphi(-1) = -\varphi(1) = -1$. But $-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2$ and there is no $r \in R$ such that $r^2 = -1$, a contradiction. □

3.12. ▷ Let R be a *commutative* ring. Prove that the set of nilpotent elements of R is an ideal of R. (Cf. Exercise 1.6. This ideal is called the *nilradical* of R.)

Find a noncommutative ring in which the set of nilpotent elements is *not* an ideal. [3.13, 4.18, V.3.13, §VII.2.3]

Solution. Let I be the set of nilpotent elements of R. If $i, j \in I$ we know that $i + j \in I$ by Exercise 1.6 (because $ij = ji$ as R is commutative). Clearly I is a subgroup of $(R, +)$ (0 is trivially nilpotent, it is an identity, associativity follows from $(R, +)$ and if a is nilpotent, then so must be $-a$). Let $r \in R, i \in I$. Then $(ri)^n = r^n i^n$ (because R is commutative!) and thus $(ri)^n = 0$ showing that $ri \in I$. Thus I is an ideal of R.

The same counterexample as in Exercise 1.6 works to show that the set of nilpotent elements is not necessarily an ideal for noncommutative rings (for $\mathcal{M}_2(\mathbb{R})$ the set is not even a subgroup of the underlying abelian subgroup). □

3.13. ¬ Let R be a commutative ring, and let N be its nilradical (cf. Exercise 3.12). Prove that R/N contains no nonzero nilpotent elements. (Such a ring is said to be *reduced*.) [4.6, VII.2.8]

Solution. Let $r+N \in R/N$, such that $r \notin N$. We have $(r+N)^k = r^k + N$. $r^k + N = N$ only if $r^k \in N$. Suppose $r^k \in N$, and thus there is some n such that $(r^k)^n = 0$, hence $r^{kn} = 0$. But this is a contradiction with the fact that r is not nilpotent. Thus $(r+N)^k \neq N$ for all k and therefore R/N contains no nonzero nilpotent elements. □

3.14. ¬ Prove that the characteristic of an integral domain is either 0 or a prime integer. Do you know any ring of characteristic 1? [V.4.17]

Solution. Let R be an integral domain. Consider the ring homomorphism $f : \mathbb{Z} \to R$, $a \mapsto a \cdot 1_R$. Suppose $\ker f = n\mathbb{Z}$ for some $n \neq 0$. In particular, $n \in \ker f$, and thus $f(n) = 0_R$. Suppose n is composite. Then we can factor it into two integers such that $n = ab$, $a, b \in \mathbb{Z}$, and $a, b < n$. Then we have $a, b \notin n\mathbb{Z}$, hence $f(a), f(b) \neq 0_R$. But that means $0_R = f(n) = f(ab) = f(a)f(b)$, a contradiction to the fact that R is an integral domain. Thus n must be a prime integer.

The only ring of characteristic 1 is the zero-ring. This is due to the fact that $\ker f = \mathbb{Z}$, thus $1 \mapsto 1 \cdot 1_R = 0_R$. □

3.15. ¬ A ring R is *Boolean* if $a^2 = a$ for all $a \in R$. Prove that $\mathscr{P}(S)$ is Boolean, for every set S (cf. Exercise 1.2). Prove that every nonzero Boolean ring is commutative and has characteristic 2. Prove that if an integral domain R is Boolean, then $R \cong \mathbb{Z}/2\mathbb{Z}$.

Solution. Let S be any set, consider the ring $\mathscr{P}(S)$. Let $A \in \mathscr{P}(S)$. Then $A^2 = A \cap A = A$, and thus $\mathscr{P}(S)$ is Boolean.

Let R be a nonzero Boolean ring. Let $a \in R$. Then $a+a = (a+a)^2 = a^2+a^2+a^2+a^2 = a+a+a+a$ and thus $a + a = 0_R$. Let $a, b \in R$. Then

$$a + b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$$

and thus $ab+ba = 0$, and hence $ab = ba$ by the previous consideration. Consider the ring homomorphism $f : \mathbb{Z} \to R$, $a \mapsto a \cdot 1_R$. Notice that $f(2) = f(1+1) = f(1) + f(1) = 0_R$, and thus $\ker f = 2\mathbb{Z}$ showing that the characteristic of R is 2.

Suppose that R is an integral domain, and suppose that R is Boolean. We have $a^2 = a$ for all $a \in R$, and thus $a^2 - a = 0_R$, hence $a(a-1) = 0_R$. Since R is an integral domain, this implies that either $a = 0_R$, or $a = 1_R$. Thus f is surjective, with $\ker f = 2\mathbb{Z}$, hence $R \cong \mathbb{Z}/2\mathbb{Z}$. □

3.16. ¬ Let S be a set and $T \subseteq S$ a subset. Prove that the subsets of S contained in T form an ideal of the power ring $\mathscr{P}(S)$. Prove that if S is finite, then *every* ideal of $\mathscr{P}(S)$ is of this form. For S infinite, find an ideal of $\mathscr{P}(S)$ that is *not* of this form. [V.1.5]

Solution. Let $X, Y \subseteq T$. We have $X - Y = X + Y = (X \cup Y) \setminus (X \cap Y)$, which is contained in T. Let $Z \in \mathscr{P}(S)$. $Z \cdot X = Z \cap X$ which is contained in T. Thus the subset of S contained in T indeed form an ideal of $\mathscr{P}(S)$.

Suppose S is finite, let I be an ideal of $\mathscr{P}(S)$. Since S is finite, we are able to select the largest subset $T \subseteq S$ in I. Since I is an ideal, then in particular every subset of T must be in I, because for all subsets $X \subseteq S$ we have $X \cdot T = X \cap T \in I$, and $\mathscr{P}(S)$ contains all the subsets of T. Because we assumed T is the largest subset of S in I, this must cover the whole of I. Thus every ideal of $\mathscr{P}(S)$ is of the given form.

Consider an infinite set S. Notice, that finite subsets of S form an ideal of S. But this ideal is not of the above form, because it is not constrained to finite subsets. For example the finite subsets of $\mathbb{N}$. □

3.17. ▷ Let I, J be ideals of a ring R. State and prove a precise result relating the ideals $(I + J)/I$ of R/I and $J/(I \cap J)$ of $R/(I \cap J)$.

Solution. Let I, J be ideals of a ring R. Then $I + J$ and $I \cap J$ are ideals of R, $\frac{I+J}{I}$ is an ideal of R/I, $J/(I \cap J)$ is an ideal of $R/(I \cap J)$, and we have

$$\frac{I + J}{I} \cong \frac{J}{I \cap J}.$$

Where the isomorphism is in particular an isomorphism of groups which respects multiplication (as ideals are not necessarily subrings and thus in general do not contain the identity).

Let $a \in I+J, r \in R$, then $a = i+j$ for some $i \in I, j \in J$, and thus $ra = r(i+j) = ri+rj$ where $ri \in I, rj \in J$, because I and J are ideals of R, and thus $ra \in I + J$. Similarly, $ar \in I + J$, showing that $I + J$ is an ideal of R.

Let $a \in I \cap J, r \in R$. Then either $a \in I$ or $a \in J$. Since both I and J are ideals it follows that $ra, ar \in I$ or $ar, ra \in J$, and thus $ar, ra \in I \cap J$. This shows that $I \cap J$ is an ideal of R.

Since $0_R \in I$, $I \subseteq I + J$, and thus by Proposition 3.11 $(I + J)/I$ is an ideal of R/I.

Similarly, $I \cap J \subseteq J$, and thus $J/(I \cap J)$ is an ideal of $R/(I \cap J)$.

Consider the function $\varphi : J \to (I + J)/I$ defined as $j \mapsto j + I$. This is in fact a group homomorphism, and thus by Corollary II.8.2 we have

$$\frac{I + J}{I} \cong \frac{J}{\ker \varphi}$$

as groups. $\ker \varphi = \{j \in J \mid \varphi(j) = 0_R\} = \{j \in J \mid j + I = I\} = \{j \in J \mid j \in I\} = I \cap J$ and thus we have

$$\frac{I + J}{I} \cong \frac{J}{I \cap J}.$$

With the isomorphism being $\widetilde{\varphi}$ obtained from Theorem II.7.12, which is defined as $\widetilde{\varphi}(r + (I \cap J)) = \varphi(r) = r + I$.

It remains to show that this isomorphism respects multiplication. Let $i + (I \cap J), j + (I \cap J) \in J/(I \cap J)$. Then from the definition of multiplication of cosets we have

$$\begin{aligned}\widetilde{\varphi}((i + (I \cap J))(j + (I \cap J))) &= \widetilde{\varphi}(ij + (I \cap J)) \\ &= ij + I \\ &= (i + I)(j + I) \\ &= \widetilde{\varphi}(i)\widetilde{\varphi}(j)\end{aligned}$$

finishing our proof. □

4. Ideals and quotients: Remarks and examples. Prime and maximal ideals

4.1. ▷ Let R be a ring, and let $\{I_\alpha\}_{\alpha \in A}$ be a family of ideals of R. We let

$$\sum_{\alpha \in A} I_\alpha := \left\{ \sum_{\alpha \in A} r_\alpha \text{ such that } r_\alpha \in I_\alpha \text{ and } r_\alpha = 0 \text{ for all but finitely many } \alpha \right\}.$$

Prove that $\sum_\alpha I_\alpha$ is an ideal of R and that it is the smallest ideal containing all of the ideals I_α. [§4.1]

Solution. First we will show that $S = \sum_\alpha I_\alpha$ is a subgroup of $(R, +)$. Let $s, r \in S$. Then s and r are finite sums of elements of the given ideals. In particular, we have an opposite of r which is also a finite sum, and thus $s - r$ is also a finite sum, so that $s - r \in S$.

Let $s \in S, r \in R$. Then $s = s_1 + s_2 + \cdots s_n$ for some n such that $s_i \in I_{\alpha_i}$ (where each $\alpha_i \in A$ and is unique). We have $rs = r(s_1 + s_2 + \cdots + s_n) = rs_1 + rs_2 + \cdots rs_n$. Since each I_{α_i} is an ideal, $rs_i \in I_{\alpha_i}$, and thus $rs \in S$. Similarly, $sr \in S$. Thus S is in fact an ideal of R.

Let J be an ideal of R such that $I_\alpha \subseteq J$ for all $\alpha \in A$. Since J is an ideal, it is in particular a subgroup of $(R, +)$ and therefore it must contain all finite sums of elements of the ideals I_α. Thus $S \subseteq J$, showing that S is in fact the smallest ideal containing all ideals I_α. □

4.2. ▷ Prove that the homomorphic image of a Noetherian ring is Noetherian. That is, prove that if $\varphi : R \to S$ is a surjective ring homomorphism and R is Noetherian, then S is Noetherian. [§6.4]

Solution. Let $\varphi : R \to S$ be a surjective ring homomorphism, suppose that R is Noetherian. By definition, this means that R is a commutative ring such that every ideal is finitely generated. Because φ is surjective, S must also be commutative - if $s, s' \in S$, then there are $r, r' \in R$ such that $\varphi(r) = s, \varphi(r') = s'$, and we have $ss' = \varphi(r)\varphi(r') = \varphi(rr') = \varphi(r'r) = \varphi(r')\varphi(r) = s's$.

By Corollary 3.10, we have $S \cong R/\ker\varphi$. Since $\ker\varphi$ is an ideal of R, say $\ker\varphi = I$, it must be finitely generated, so that $I = (a_1, \ldots, a_n)$. By Proposition 3.11, we know that the ideals of R/I are in one-to-one correspondence with the ideals of R, and J/I is an ideal of R/I if and only if J is an ideal of R. Thus every ideal of S is of the form J/I such that J is an ideal of R, and thus $J = (b_1, \ldots, b_m)$. In particular, J/I is generated by the classes of $b_1, \ldots, b_m$ in R/I, and thus is finitely generated.

Therefore every ideal of S is in fact finitely generated and S is Noetherian. □

4.3. Prove that the ideal $(2, x)$ of $\mathbb{Z}[x]$ is not principal.

Solution. Suppose that $(2, x)$ is a principal ideal of $\mathbb{Z}[x]$. Then $(2, x) = (f(x))$ for some polynomial $f(x) = \sum_{i\geq 0} a_i x^i \in \mathbb{Z}[x]$. In particular, we must have $2 \in (f(x))$ and $x \in (f(x))$. This means that there must be an integer $z \in \mathbb{Z}$ such that $zf(x) = \sum_{i\geq 0} za_i x^i = 2$. But if $\deg f > 0$, $zf(x)$ can never equal 2, thus $f(x)$ must be constant. On the other hand, that means that there can be no z such that $zf(x) = x$ because $\deg f = 0$, a contradiction. □

4.4. ▷ Prove that if k is a field, then $k[x]$ is a PID. (Hint: Let $I \subseteq k[x]$ be any ideal. If $I = (0)$, then I is principal. If $I \neq (0)$, let $f(x)$ be a monic polynomial in I of minimal degree. Use division with remainder to construct a proof that $I = (f(x))$, arguing as in the proof of Proposition II.6.9.) [§4.1, §4.3, §V.4.1, §VI.7.2, §VII.1.2]

Solution. Let k be a field. Suppose $I \subseteq k[x]$ is any ideal. If $I = (0)$, then I is principal. Suppose that $I \neq (0)$. Then there is a monic (i.e. with a leading coefficient of 1) polynomial $f(x)$ in I of minimal degree. It is clear that $(f(x)) \subseteq I$. We shall show that $I \subseteq (f(x))$ by using polynomial division with remainder (which works precisely because k is a field). Let $g(x) \in I$ be a polynomial, then there are polynomials $q(x), r(x) \in k[x]$ such that either $r(x) = 0$ or $\deg r < \deg f$ and

$$g(x) = f(x)q(x) + r(x).$$

I is an ideal, and therefore since $g(x) \in I$, we must have $r(x) = g(x) - f(x)q(x) \in I$. But we have selected $f(x)$ precisely with the condition that $\deg f$ is minimal, and thus $r(x) = 0$. Thus $g(x) = f(x)q(x)$, and since this holds for any $g(x) \in I$, $I = (f(x))$. □

4.5. ▷ Let I, J be ideals in a commutative ring R, such that $I + J = (1)$. Prove that $IJ = I \cap J$. [§4.1, §V.6.1]

Solution. We know that $IJ \subseteq I \cap J$, so it is enough to show that $I \cap J \subseteq IJ$. $I + J = (1)$ implies that for any $i \in I, j \in J$ there is an element $r \in R$ such that $i + j = r$. On the other hand, there must be elements $a \in I$, $b \in J$, such that $a + b = 1$.

Suppose $i \in I \cap J$. Then $i \in I$ and $i \in J$. Since $a + b = 1$, we have $i = i1 = i(a + b) = ia + ib$. But $a \in I$, $b \in J$, and thus $ia \in JI$, $ib \in IJ$. Since R is commutative, $JI = IJ$,

and thus $ia \in IJ$. Thus $i \in IJ + IJ$. But $IJ + IJ = IJ$, and thus $i \in IJ$, showing that $I \cap J \subseteq IJ$. □

4.6. Let I, J be ideals in a commutative ring R. Assume that $R/(IJ)$ is reduced (that is, it has no nonzero nilpotent elements; cf. Exercise 3.13). Prove that $IJ = I \cap J$.

Solution. Let $i \in I \cap J$, then $i \in I$, $i \in J$, and thus $i^2 = ii \in IJ$. $R/(IJ)$ is reduced, hence if $(r + (IJ))^n = r^n + (IJ) = (IJ)$ then $r + (IJ) = (IJ)$, that is if $r^n \in IJ$, then $r \in IJ$. Thus $i^2 \in IJ$ implies $i \in IJ$. □

4.7. ▷ Let $R = k$ be a field. Prove that every nonzero (principal) ideal in $k[x]$ is a generated by a unique *monic* polynomial. [§4.2, §VI.7.2]

Solution. Let $I = (f(x))$ be an ideal of $k[x]$, $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, with $a_d \neq 0$. Because k is a field, we must necessarily have an element $a_d^{-1} \in k$, and $a_d^{-1} f(x) = x^d + a_{d-1}a_d^{-1}x^{d-1} + \cdots + a_1 a_d^{-1} x + a_0 a_d^{-1} \in I$ because I is an ideal. But $f(x) = a_d(a_d^{-1} f(x))$ and thus I is generated by $a_d^{-1} f(x)$ which is a monic polynomial. □

4.8. ▷ Let R be a ring and $f(x) \in R[x]$ a *monic* polynomial. Prove that $f(x)$ is not a (left- or right-) zero-divisor. [§4.2, 4.9]

Solution. Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in R[x]$ be a monic polynomial, and let $g(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0 \in R[x]$ an arbitrary polynomial of degree k. Then $f(x)g(x)$ (or $g(x)f(x)$) is 0 only if all coefficients of the product polynomial are 0. By the definition of polynomial multiplication, the leading term of $f(x)g(x)$ is equal to $a_d b_k x^{d+k} = b_k x^{d+k}$, but $b_k \neq 0$ because $\deg g = k$, and thus $f(x)g(x)$ is nonzero. Similarly for $g(x)f(x)$. Thus $f(x)$ is a non-zero-divisor in $R[x]$. □

4.9. Generalize the result of Exercise 4.8, as follows. Let R be a commutative ring, and let $f(x)$ be a zero-divisor in $R[x]$. Prove that $\exists b \in R, b \neq 0$, such that $f(x)b = 0$. (Hint: Let $f(x) = a_d x^d + \cdots + a_0$, and let $g(x) = b_e x^e + \cdots + b_0$ be a nonzero polynomial of minimal degree e such that $f(x)g(x) = 0$. Deduce that $a_d g(x) = 0$, and then prove $a_{d-i}g(x) = 0$ for all i. What does this say about b_e?)

Solution. Let $f(x) = a_d x^d + \cdots + a_0$ be a zero-divisor in $R[x]$, and $g(x) = b_e x^e + \cdots b_0$ be a nonzero polynomial of minimal degree e such that $f(x)g(x) = 0$. We have $f(x)g(x) = a_d g(x)x^d + \cdots + a_0 g(x) = 0$. If $a_d g(x) \neq 0$, then $f(x)g(x)$ cannot be 0, because the term $a_d b_e x^{d+e}$ comes from the term $a_d g(x)x^d$ of the sum, as all the other terms are polynomials of degree less than $d + e$. Thus $a_d g(x) = 0$.

We can continue this process inductively, already having proved the base case of $i = 0$. Suppose $a_{d-j}g(x) = 0$ for all $0 \leq j \leq i$. Then

$$f(x)g(x) = a_{d-(i+1)}g(x)x^{d-(i+1)} + \cdots a_0 g(x) = 0.$$

The degree of $a_{d-(i+1)}g(x)x^{d-(i+1)}$ is $e+d-(i+1)$ and all the other polynomials in this sum have smaller degree. But that implies $a_{d-(i+1)}g(x) = 0$ as needed.

Because $a_{d-i}g(x) = 0$ for all i, then in particular we must have $a_{d-i}b_e = 0$ for all i. But that implies $f(x)b_e = a_d b_e x^d + \cdots a_0 b_e = 0$, proving the result. □

4.10. ¬ Let d be an integer that is not the square of an integer, and consider the subset of $\mathbb{C}$ defined by

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

- Prove that $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$.
- Define a function $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ by $N(a + b\sqrt{d}) := a^2 - b^2 d$. Prove that $N(zw) = N(z)N(w)$ and that $N(z) \neq 0$ if $z \in \mathbb{Q}(\sqrt{d})$, $z \neq 0$.

The function N is a 'norm'; it is very useful in the study of $\mathbb{Q}(\sqrt{d})$ and of its subrings. (Cf. also Exercise 2.5.)

- Prove that $\mathbb{Q}(\sqrt{d})$ is a field and in fact the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$. (Use N.)
- Prove that $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$. (Cf. Example 4.8.)

[V.1.17, V.2.18, V.6.13, VII.1.12]

Solution. Let d be an integer that is not a square of an integer.

- Let $z, w \in \mathbb{Q}(\sqrt{d})$, $z = a + b\sqrt{d}$, and $w = k + l\sqrt{d}$. We have

  $$z - w = a + b\sqrt{d} - k - l\sqrt{d} = (a - k) + (b - l)\sqrt{d} \in \mathbb{Q}(\sqrt{d}),$$

  showing that $\mathbb{Q}(\sqrt{d})$ is a subgroup of $\mathbb{C}$. We also have

  $$\begin{aligned} zw &= (a + b\sqrt{d})(k + l\sqrt{d}) \\ &= ak + bld + al\sqrt{d} + bk\sqrt{d} \\ &= (ak + bld) + (al + bk)\sqrt{d} \in \mathbb{Q}(\sqrt{d}), \end{aligned}$$

  so $\mathbb{Q}(\sqrt{d})$ is closed with respect to multiplication in $\mathbb{C}$. Lastly,

  $$1 = 1 + 0\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

  Thus $\mathbb{Q}(\sqrt{d})$ is in fact a subring of $\mathbb{C}$.

- By the previous point, we have

$$\begin{aligned} N(zw) &= (ak+bld)^2 - (al+bk)^2 d \\ &= a^2k^2 + 2abkld + b^2l^2d^2 - a^2l^2d - 2abkld - b^2k^2d \\ &= a^2(k^2 - l^2d) - b^2d(k^2 - l^2d) \\ &= (a^2 - b^2d)(k^2 - l^2d) \\ &= N(z)N(w). \end{aligned}$$

  Now, $N(z) = 0$ implies $a^2 - b^2d = 0$, hence $a^2 = b^2d$. Thus in $\mathbb{Q}(\sqrt{d})$ we would have $a = b\sqrt{d}$, which can only happen if $a = b = 0$. Thus if $z \neq 0$, $N(z) \neq 0$.

- It is clear that $\mathbb{Q}(\sqrt{d})$ is commutative, because $\mathbb{C}$ is commutative. Thus we only have to show that it is a division ring. Let $z \in \mathbb{Q}(\sqrt{d})$, $z = a + b\sqrt{d} \neq 0$. It is easy to see that

$$(a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2d = N(z)$$

  and thus, since $N(z) \neq 0$, we have

$$z\frac{a - b\sqrt{d}}{N(z)} = 1$$

  showing that $\frac{a-b\sqrt{d}}{N(z)}$ is an inverse of z, hence z is a unit. Therefore $\mathbb{Q}(\sqrt{d})$ is a field.

  Any subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$ must also contain all the elements of the form $a + b\sqrt{d}$ because it must be closed w. r. t. $+$ and $\cdot$. Thus $\mathbb{Q}(\sqrt{d})$ is in fact the smallest such subfield.

- Consider the polynomial ring $\mathbb{Q}[t]$. Then

$$\frac{\mathbb{Q}[t]}{(t^2 - d)} \cong \mathbb{Q} \oplus \mathbb{Q}$$

  as groups by Proposition 4.6. This isomorphism induces a ring structure on $\mathbb{Q} \oplus \mathbb{Q}$: Let $(a_0, a_1), (b_0, b_1) \in \mathbb{Q} \oplus \mathbb{Q}$. We then have (notation as in Proposition 4.6)

$$(a_0, a_1) = \varphi(a_0 + a_1 t), \quad (b_0, b_1) = \varphi(b_0 + b_1 t).$$

  Of course,

$$\begin{aligned} (a_0 + a_1t)(b_0 + b_1t) &= a_0b_0 + (a_0b_1 + a_1b_0)t + a_1b_1t^2 \\ &= (t^2 - d)a_1b_1 + ((a_0b_0 + da_1b_1) + (a_0b_1 + a_1b_0)t) \end{aligned}$$

  so that

$$\varphi((a_0 + a_1t)(b_0 + b_1t)) = (a_0b_0 + da_1b_1, a_0b_1 + a_1b_0)$$

  and thus the induced multiplication is defined as

$$(a_0, a_1) \cdot (b_0, b_1) = (a_0b_0 + da_1b_1, a_0b_1 + a_1b_0).$$

  In particular, this matches verbatim the multiplication in $\mathbb{Q}(\sqrt{d})$, and thus in fact $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$. □

4.11. Let R be a commutative ring, $a \in R$, and $f_1(x), \ldots, f_r(x) \in R[x]$.

- Prove the equality of ideals

$$(f_1(x), \ldots, f_r(x), x-a) = (f_1(a), \ldots, f_r(a), x-a).$$

- Prove the useful substitution trick

$$\frac{R[x]}{(f_1(x), \ldots, f_r(x), x-a)} \cong \frac{R}{(f_1(a), \ldots, f_r(a))}.$$

(Hint: Exercise 3.3.)

Solution. Let R be a commutative ring, $a \in R$, $f_1(x), \ldots, f_r(x) \in R[x]$.
Consider an element $g(x) \in (f_1(x), \ldots, f_r(x), x-a)$. Then in particular

$$g(x) = g_1(x)f_1(x) + \cdots + g_r(x)f_r(x) + h(x)(x-a)$$

for some $g_1(x), \ldots, g_r(x), h(x) \in R[x]$. Notice, that since $(x-a)$ is monic, we can divide each $f_i(x)$ by it to produce a polynomial $(x-a)q_i(x) + f_i(a)$. We thus have

$$g(x) = g_1(x)((x-a)q_1(x) + f_1(a)) + \cdots + g_r(x)((x-a)q_r(x) + f_r(a)) + h(x)(x-a)$$

and rewriting this

$$g(x) = g_1(x)f_1(a) + \cdots + g_r(x)f_r(a) + (g_1(x)q_1(x) + \cdots + g_r(x)q_r(x) + h(x))(x-a).$$

Thus $g(x) \in (f_1(a), \ldots, f_r(a), x-a)$. Similarly, for $g(x) \in (f_1(a), \ldots, f_r(a), x-a)$, we can use the fact that $f_i(a) = f_i(x) - (x-a)q_i(x)$, to show that $g(x) \in (f_1(x), \ldots, f_r(x), x-a)$.
Using the above we have

$$\frac{R[x]}{(f_1(x), \ldots, f_r(x), x-a)} = \frac{R[x]}{(f_1(a), \ldots, f_r(a), x-a)}.$$

Using the principle shown in Example 4.1 we see that

$$\frac{R[x]}{(f_1(a), \ldots, f_r(a), x-a)} \cong \frac{R[x]/(x-a)}{(f_1(a), \ldots, f_r(a))},$$

and using Proposition 4.6

$$\frac{R[x]/(x-a)}{(f_1(a), \ldots, f_r(a))} \cong \frac{R}{(f_1(a), \ldots, f_r(a))}.$$

□

4.12. ▷ Let R be a commutative ring and $a_1, \cdots, a_n$ elements of R. Prove that

$$\frac{R[x_1, \ldots, x_n]}{(x_1 - a_1, \ldots, x_n - a_n)} \cong R.$$

[§VII.2.2]

Solution. We can prove this in a straightforward fashion using induction and the fact that $R[x_1, \ldots, x_n] = R[x_1] \ldots [x_n]$. Let $n = 1$. Then this is just Example 4.7, and $R[x_1]/(x_1 - a_1) \cong R$.

Suppose that

$$\frac{R[x_1, \ldots, x_n]}{(x_1 - a_1, \ldots, x_n - a_n)} \cong R.$$

Then by Proposition 3.11

$$\frac{R[x_1, \ldots, x_{n+1}]}{(x_1 - a_1, \ldots, x_{n+1} - a_{n+1})} \cong \frac{R[x_1, \ldots, x_n][x_{n+1}]/(x_{n+1} - a_{n+1})}{(x_1 - a_1, \ldots, x_n - a_n)}.$$

But

$$R[x_1, \ldots, x_n][x_{n+1}]/(x_{n+1} - a_{n+1}) \cong R[x_1, \ldots, x_n]$$

and thus

$$\frac{R[x_1, \ldots, x_n][x_{n+1}]/(x_{n+1} - a_{n+1})}{(x_1 - a_1, \ldots, x_n - a_n)} \cong \frac{R[x_1, \ldots, x_n]}{(x_1 - a_1, \ldots, x_n - a_n)} \cong R.$$

□

4.13. ▷ Let R be an integral domain. For all $k = 1, \ldots, n$ prove that $(x_1, \ldots, x_k)$ is prime in $R[x_1, \ldots, x_n]$. [§4.3]

Solution. Let R be an integral domain. Notice that by definition of polynomials with more than one intermediate, and since R is commutative, $R[x_1, \ldots, x_n] = R[x_1] \ldots [x_n] \cong R[x_n] \ldots [x_1]$.

Then we can apply the 'calculus of ideals and quotients', Proposition 3.11, and Proposition 4.6 as follows. Let $1 \leq k \leq n$. We have

$$\frac{R[x_n] \ldots [x_1]}{(x_1, \ldots, x_k)} \cong \frac{R[x_n] \ldots [x_2]}{(x_2, \ldots, x_k)} \cong \cdots \cong R[x_n] \ldots [x_{k+1}] \cong R[x_{k+1}, \ldots, x_n]$$

and indeed $R[x_{k+1}, \ldots, x_n]$ is an integral domain because R is an integral domain. And thus $(x_1, \ldots, x_k)$ is prime in $R[x_1, \ldots, x_n]$. □

4.14. ▷ Prove 'by hand' that maximal ideas are prime, *without* using quotient rings. [§4.3]

Solution. Let R be a commutative ring and consider a maximal ideal I of R. Suppose that I is not prime, so that there are elements $a, b \in R$ and $a, b \notin I$ such that $ab \in I$. Consider the ideal $I+(a)$. We have $I \subseteq I+(a)$, but since $a \notin I$, we must have $I+(a) = R$. Thus $1_R \in I + (a)$, so that $1_R = ri + sa$ for some $r, s \in R$, $i \in I$. Then

$$b = b1_R = b(ri + sa) = bri + bsa.$$

We have $bri \in I$, because $i \in I$ and I is an ideal. R is commutative, and thus $bsa = s(ab) \in I$, since $ab \in I$. But that means $b \in I$, a contradiction. Thus I must be prime. □

4.15. Let $\varphi : R \to S$ be a homomorphism of commutative rings, and let $I \subseteq S$ be an ideal. Prove that if I is a prime ideal in S, then $\varphi^{-1}(I)$ is a prime ideal in R. Show that $\varphi^{-1}(I)$ is not necessarily maximal if I is maximal.

Solution. Consider such an homomorphism, and suppose I is a prime ideal in S. Let $J = \varphi^{-1}(I)$. Then J is an ideal of R by Exercise 3.2. Let $ab \in J$. Then $\varphi(ab) \in I$ and thus we have either $\varphi(a) \in I$, or $\varphi(b) \in I$. In either case this implies that either $a \in J$ or $b \in J$, showing that J is prime.

As an counterexample for maximality, let $\varphi : \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. $\mathbb{Q}$ is a field, and thus the maximal ideal of $\mathbb{Q}$ is (0). $\varphi^{-1}((0)) = (0)$, however, (0) is not maximal in $\mathbb{Z}$. □

4.16. Let R be a commutative ring, and let P be a prime ideal of R. Suppose 0 is the only zero-divisor of R contained in P. Prove that R is an integral domain.

Solution. Suppose $a, b \in R$, $a \neq 0, b \neq 0$ and $ab = 0$. Since $0 \in P$, $ab \in P$. P is a prime ideal of R, hence we must have either $a \in P$, or $b \in P$. But 0 is the only zero-divisor of R contained in P, a contradiction. □

4.17. ¬ (If you know a little topology...) Let K be a compact topological space, and let R be the ring of continuous real-valued functions on K, with addition and multiplication defined pointwise.

(i) For $p \in K$, let $M_p = \{f \in R \mid f(p) = 0\}$. Prove that M_p is a maximal ideal in R.

(ii) Prove that if $f_1, \ldots, f_r \in R$ have no common zeros, then $(f_1, \ldots, f_r) = (1)$. (Hint: Consider $f_1^2 + \cdots + f_r^2$.)

(iii) Prove that every maximal ideal M in R is of the form M_p for some $p \in K$. (Hint: You will use the compactness of K and (ii).)

If further K is Hausdorff (and, as Bourbaki would have it, compact spaces are Hausdorff), then Urysohn's lemma shows that for any two points $p \neq q$ in K there exists a function $f \in R$ such that $f(p) = 0$ and $f(q) = 1$. If this is the case, conclude that $p \mapsto M_p$ defines a bijection from K to the set of maximal ideals of R. (The set of maximal ideals of a commutative ring R is called the *maximal spectrum of* R; it is contained in the (prime) spectrum $\operatorname{Spec} R$ defined in §4.3. Relating commutative rings and 'geometric' entities such as topological spaces is the business of *algebraic geometry*.)

The compactness hypothesis is necessary: cf. Exercise V.3.10. [V.3.10]

Solution. Let K be a compact topological space, R the ring of continuous real-valued functions on K. Let $p \in K$. Consider the evaluation function $e_p : R \to \mathbb{R}$, $f \mapsto f(p)$. This is a ring homomorphism following the pointwise definition of addition and multiplication in K, with identity in R being the constant function 1. $\ker e_p = M_p$, and thus by the first isomorphism theorem of rings we have $R/M_p \cong \mathbb{R}$. Since $\mathbb{R}$ is a field, M_p is maximal in R.

Let $f_1, \ldots, f_r \in R$ be continuous functions with no common zeros. Consider the ideal $I = (f_1, \ldots, f_r)$. Then $f_1^2 + \cdots + f_r^2 \in I$. Notice, that each $f_i^2(x) \geq 0$ for all $x \in K$. Now since $f_1, \ldots, f_r$ share no common zeros, we must have $f_1^2 + \cdots + f_r^2(x) > 0$ for all $x \in K$. But that implies that we have an inverse function in R and thus $1 \in I$, which implies $I = R = (1)$.

Let M be a maximal ideal of R. Let Z denote all common zeros of all $f \in M$. Suppose $Z = \emptyset$. Then the complement of Z is an open cover of K, and thus we have a finite subcover of K, because K is compact. We then have $\bigcap_{i=1}^{n} z(f_i) = \emptyset$. But that would imply by the last point that $M = (1)$, a contradiction to the fact that M is maximal. Thus Z is not empty. Therefore we have some $p \in K$ such that for all $f \in R$, $f(p) = 0$. In particular, we must have $M \subseteq M_p$, but M is maximal, and thus $M = M_p$.

Consider the function from K to the set of maximal ideals of R defined by $p \mapsto M_p$. By the last point, this function is surjective. Let $p \neq q$. By Urysohn's lemma, we then have a function $f \in R$ such that $f(p) = 0$, $f(q) = 1$, so that $f \in M_p$ and $f \notin M_q$, and thus $M_p \neq M_q$. But this means that the function is injective, showing it is indeed a bijection. □

4.18. Let R be a commutative ring, and let N be its nilradical (Exercise 3.12). Prove that N is contained in every prime ideal of R. (Later on the reader will check that the nilradical is in fact the intersection of all prime ideals of R: Exercise V.3.13.)

Solution. Let R be a commutative ring, N its nilradical, and P a prime ideal of R. Suppose $r \in N$ is a nilpotent element of R, and $r \notin P$. Let n be the smallest number such that $r^n = 0_R$. P is prime, and thus R/P is an integral domain. Because $r \notin P$, $r + P \in R/P$. By definition of multiplication of cosets, we have $(r + P)^n = r^n + P = 0_R + P = P$, but that means $r + P$ is a zero-divisor in R/P (as $(r + P)(r^{n-1} + P) = P$ and $r + P \neq P$, $r^{n-1} + P \neq P$), a contradiction to the fact that R/P is an integral domain. □

4.19. Let R be a commutative ring, let P be a prime ideal in R, and let I_j be ideals of R.

(i) Assume that $I_1 \cdots I_r \subseteq P$; prove that $I_j \subseteq P$ for some j.

(ii) By (i), if $P \supseteq \bigcap_{j=1}^{r} I_j$, then P contains one of the ideals I_j. Prove or disprove: if $P \supseteq \bigcap_{j=1}^{\infty} I_j$, then P contains one of the ideals I_j.

Solution. Let R be a commutative ring, P its prime ideal, I_j ideals of R. Assume that $I_1 \cdots I_r \subseteq P$. Suppose that no ideal I_j is a subset of P. Then in particular there must be an element $i_j \in I_j$ and $i_j \notin P$ for all j. Consider the element $i_1 \cdots i_r \in I_1 \cdots I_r$. We have $I_1 \cdots I_r \subseteq P$, hence $i_1 \cdots i_r \in P$. P is prime, and thus we must have $i_j \in P$ for some j, a contradiction.

$P \supseteq \bigcap_{j=1}^{r} I_j$ implies that P contains one of the ideals I_j because $I_1 \cdots I_r \subseteq \bigcap_{j=1}^{r} I_j$. However, in the case of an infinite intersection, this does not work. Consider $\mathbb{Z}$, let $P = (0)$, which is prime (trivially). All the ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Notice that the elements of the ideal $n\mathbb{Z} \cap m\mathbb{Z}$ are integers which are multiples of both n and m. In particular, we can look at $\bigcap_{p \text{ prime}} p\mathbb{Z}$. Clearly, the only multiple of *all* the prime numbers is 0, thus $P = (0) = \bigcap_{p \text{ prime}} p\mathbb{Z}$, but $p\mathbb{Z} \not\subseteq P$ for any prime p. □

4.20. Let M be a two-sided ideal in a (not necessarily commutative) ring R. Prove that M is maximal if and only if R/M is a simple ring (cf. Exercise 3.9).

Solution. Let M be a two-sided ideal of a ring R. By the third isomorphism theorem, ideals of R/M are in one-to-one correspondence with ideals of R containing M. Let I be an ideal of R such that $M \subseteq I$.

Suppose M is maximal. Then we have either $I = M$, or $I = R$. In the first case, we get $I/M = M/M = (0)$ as an ideal of R. Similarly, in the second case, we have $I/M = R/M = (1)$ as an ideal of R/M. Thus R/M is simple as the only two-sided ideals are (0) and (1).

On the other hand, suppose R/M is a simple ring. Then by the third isomorphism theorem we know I/M is an ideal of R/M. Since R/M is simple, I/M is either (0) or (1). In the first case, $I/M = (0)$ implies $I = M$. In the second, $I/M = (1)$ implies $I = R$, showing that M is maximal in R. □

4.21. ▷ Let k be an algebraically closed field, and let $I \subseteq k[x]$ be an ideal. Prove that I is maximal if and only if $I = (x - c)$ for some $c \in k$. [§4.3, §V.5.2, §VII.2.1, §VII.2.2]

Solution. Let k be an algebraically closed field, $I \subseteq k[x]$ an ideal. Suppose that $I = (x-c)$ for some $c \in k$. Then $k[x]/(x-c) = k$ and thus I is maximal, because k is a field.

Suppose I is maximal. Since k is a field, $k[x]$ is a PID, and thus $I = (f(x))$ for some $f(x) \in k[x]$. k is algebraically closed, and thus there is some $c \in k$ such that $f(c) = 0$.

In particular, $f(x) = (x-c)g(x)$ for some $g(x) \in k[x]$. But that implies $I = (x-c)$. □

4.22. Prove that (x^2+1) is maximal in $R[x]$.

Solution. $R[x]/(x^2+1) \cong \mathbb{C}$ and $\mathbb{C}$ is a field, thus (x^2+1) is maximal in $R[x]$. □

4.23. A ring R has Krull dimension 0 if every prime ideal in R is maximal. Prove that fields and Boolean rings (Exercise 3.15) have Krull dimension 0.

Solution. Fields have only two ideals - (0) and (1). (0) is a prime ideal, and it is clearly maximal.

Let R be a Boolean ring, so that $a^2 = a$ for all $a \in R$. Then in particular every quotient of R must be a Boolean ring - if I is any ideal of R, $(a+I)^2 = a^2 + I = a + I$ for all $a \in R$. Let I be a prime ideal of R. Then R/I is an integral domain, because I is prime, and it is a Boolean ring by the previous consideration. By Exercise 3.15 we thus have $R/I \cong \mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z}$ is a field. Thus I is maximal in R. □

4.24. Prove that the ring $\mathbb{Z}[x]$ has Krull dimension ≥ 2. (It is in fact exactly 2; thus it corresponds to a *surface* from the point of view of algebraic geometry.)

Solution. We know that (0) and $(2, x)$ are prime ideals of $\mathbb{Z}[x]$. Consider (2). The elements of $\mathbb{Z}/(2)$ are polynomials with coefficients in $\mathbb{Z}/2\mathbb{Z}$, and thus $\mathbb{Z}/(2) \cong \mathbb{Z}/2\mathbb{Z}[x]$. Since $\mathbb{Z}/2\mathbb{Z}$ is an integral domain, $\mathbb{Z}/2\mathbb{Z}[x]$ is an integral domain, and thus (2) is prime in $\mathbb{Z}[x]$. Notice that $(0) \subsetneq (2) \subsetneq (2, x)$, and thus the Krull dimension of $\mathbb{Z}[x]$ is ≥ 2. □

5. Modules over a ring

5.1. ▷ Let R be a ring. The *opposite* ring R° is obtained from R by reversing the multiplication: that is, the product $a \bullet b$ in R° is defined to be $ba \in R$. Prove that the identity map $R \to R^\circ$ is an isomorphism if and only if R is commutative. Prove that $\mathcal{M}_n(\mathbb{R})$ is isomorphic to its opposite (*not* via the identity map!). Explain how to turn right-R-modules into left-R-modules and conversely, if $R \cong R^\circ$. [§5.1, VIII.5.19]

Solution. Let R be a ring, consider the identity map $\mathrm{id} : R \to R^\circ$. Suppose id is an isomorphism. Then we have $ba = \mathrm{id}^{-1}(ba) = \mathrm{id}^{-1}(a \bullet b) = \mathrm{id}^{-1}(a)\mathrm{id}^{-1}(b) = ab$ for all $a, b \in R$, showing that R is commutative. On the other hand, suppose R is commutative. Then id is a ring homomorphism - it is clearly a homomorphism of the underlying abelian groups, $\mathrm{id}(1) = 1$ by definition, and $\mathrm{id}(ab) = ab = ba = a \bullet b = \mathrm{id}(a) \bullet \mathrm{id}(b)$. Since id is by definition a bijection, id is a ring isomorphism.

Consider the ring $R = \mathcal{M}_n(\mathbb{R})$. This ring is not commutative and thus we cannot use the identity map as an isomorphism to its opposite. We can however show that the

function $\varphi : R \to R^\circ$ defined by $\varphi(M) = M^t$ is a ring isomorphism. First of all, notice that it is in fact a bijection - the function $R^\circ \to R$ defined by $M \mapsto M^t$ acts as an inverse because $(M^t)^t = M$. φ is a group homomorphism, because $(A+B)^t = A^t + B^t$. The transpose of I_n is I_n and thus φ also preserves the identity. Now, $\varphi(AB) = (AB)^t = B^tA^t = A^t \bullet B^t = \varphi(A) \bullet \varphi(B)$. Thus, φ is a bijective ring homomorphism and is thus an isomorphism.

Suppose that $R \cong R^\circ$, so that we have an isomorphism $\varphi : R \to R^\circ$. Let M be a right-R-module. The structure of a right-R-module is given by a map $\rho : M \times R \to M$, satisfying the required properties. Define a map $\delta : R^\circ \times M \to M$ as $\delta(r, m) = \rho(m, r)$. Let us now check that δ is indeed a left-action of R° on M. We have

$$\delta(r, m+n) = \rho(m+n, r) = \rho(m, r) + \rho(n, r) = \delta(r, m) + \delta(r, n)$$

and similarly

$$\begin{aligned} \delta(r+s, m) &= \rho(m, r+s) \\ &= \rho(m, r) + \rho(m, s) \\ &= \delta(r, m) + \delta(s, m). \end{aligned}$$

The crucial property is the 'associativity of multiplication':

$$\begin{aligned} \delta(r \bullet s, m) &= \delta(sr, m) \\ &= \rho(m, sr) \\ &= \rho(\rho(m, s), r) \\ &= \delta(r, \rho(m, s) \\ &= \delta(r, \delta(s, m)). \end{aligned}$$

Obviously, $\delta(1, m) = \rho(m, 1) = m$. Thus δ is a left-action of R° on M. This gives us a ring homomorphism $\sigma : R^\circ \to \mathrm{End}_{\mathsf{Ab}}(M)$. But then $\sigma \circ \varphi : R \to \mathrm{End}_{\mathsf{Ab}}(M)$ is also a ring homomorphism, and thus we have obtained a left-R-module structure on M. The other direction is analogous. □

5.2. ▷ Prove Claim 5.1. [§5.1]

Solution. Let R be a ring, M an abelian group. Suppose $\rho : R \times M \to M$ is a function satisfying the given conditions. Define a function $\sigma : R \to \mathrm{End}_{\mathsf{Ab}}(M)$ as $\sigma(r)(m) = \rho(r, m)$. We shall show that σ is a ring homomorphism. First of all, the image of any r under σ is a group homomorphism because

$$\sigma(r)(m+n) = \rho(r, m+n) = \rho(r, m) + \rho(r, n) = \sigma(r)(m) + \sigma(r)(n).$$

For any $r, s \in R$, $m \in M$, we then have

$$\sigma(r+s)(m) = \rho(r+s, m) = \rho(r, m) + \rho(s, m) = \sigma(r)(m) + \sigma(s)(m)$$

and

$$\sigma(rs)(m) = \rho(rs, m) = \rho(r, \rho(s, m)) = \sigma(r)(\rho(s, m)) = \sigma(r)(\sigma(s)(m)).$$

Thus $\sigma(r+m) = \sigma(r)+\sigma(m)$ and $\sigma(rs) = \sigma(r)\circ\sigma(s)$. We also have $\sigma(1)(m) = \rho(1, m) = m$ so that $\sigma(1) = \mathrm{id}_M$. Thus σ is a ring homomorphism as needed.

On the other hand, suppose $\sigma : R \to \mathrm{End}_{\mathsf{Ab}}(M)$ is a ring homomorphism. Define $\rho : R \times M \to M$ by $\rho(r, m) = \sigma(r)(m)$. The preceding argument shows that ρ in fact satisfies the given conditions. □

5.3. ▷ Let M be a module over a ring R. Prove that $0 \cdot m = 0$ and $(-1) \cdot m = -m$, for all $m \in M$. [§5.2]

Solution. Let M be a module over a ring R, $m \in M$. Then we have $0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m$, and thus by cancellation (in M), $0 \cdot m = 0$.

Now, $0 = 0 \cdot m = (1 - 1) \cdot m = 1 \cdot m + (-1) \cdot m = m + (-1) \cdot m$. Adding $-m$ on the left we obtain $-m = -m + m + (-1) \cdot m = (-1) \cdot m$, as needed. □

5.4. ¬ Let R be a ring. A nonzero R-module M is *simple* (or *irreducible*) if its only submodules are $\{0\}$ and M. Let M, N be simple modules, and let $\varphi : M \to N$ be a homomorphism of R-modules. Prove that either $\varphi = 0$ or φ is an isomorphism. (This rather innocent statement is known as Schur's lemma.) [5.10, 6.16, VI.1.16]

Solution. Let R be a ring, M and N simple R-modules, and $\varphi : M \to N$ a homomorphism of R-modules. We know that submodules map onto submodules under R-module homomorphisms. Thus we must have either $\varphi(M) = \{0\}$ or $\varphi(M) = N$. In the first case we have $\varphi = 0$. In the second, φ is clearly surjective. Suppose $a, b \in M$ are such that $\varphi(a) = \varphi(b)$. Then $\varphi(a - b) = 0$, and thus $a - b \in \ker \varphi$. But since kernels are submodules, we must have $\ker = \{0\}$ (as it clearly cannot be equal to M), and thus $a - b = 0$, hence $a = b$, showing that φ is injective. Therefore φ is a bijective homomorphism of R-modules, and is thus an isomorphism. □

5.5. Let R be a commutative ring, viewed as an R-module over itself, and let M be an R-module. Prove that $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, M) \cong M$ as R-modules.

Solution. Let R be a commutative ring, M an R-module. Define a function

$$\varphi : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, M) \to M$$

defined as $\varphi(f) = f(1)$. Let $f, g \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, M)$. Then $\varphi(f + g) = (f + g)(1) = f(1) + g(1) = \varphi(f) + \varphi(g)$, and thus φ is a group homomorphism. Now let $r \in R$. Then $\varphi(rf) = (rf)(1) = r(f(1)) = r\varphi(f)$, and thus φ is in fact a homomorphism of R-modules.

Let $m \in M$. Notice that $f : R \to M$, defined by $f(r) = rm$, is clearly an R-module homomorphism, and $\varphi(f) = f(1) = 1m = m$. Thus φ is surjective. Now suppose that $\varphi(f) = \varphi(g)$ for some $f, g \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, M)$. Then $f(1) = g(1)$. Since both f, g are R-module homomorphisms, we must have $rf(1) = rg(1)$, hence $f(r) = g(r)$ for all $r \in R$, and thus $f = g$. Thus φ is injective, showing that indeed φ is an isomorphism as needed. □

5.6. Let G be an abelian group. Prove that if G has a structure of $\mathbb{Q}$-vector space, then it has only one such structure. (Hint: First prove that every nonidentity element of G has necessarily infinite order. Alternative hint: The unique ring homomorphism $\mathbb{Z} \to \mathbb{Q}$ is an epimorphism.)

Solution. Let G be an abelian group. Then it has a unique structure as a $\mathbb{Z}$-module, i.e. there is a unique ring homomorphism $\varphi : \mathbb{Z} \to \mathrm{End}_{\mathsf{Ab}}(G)$. As we have seen, the inclusion $\iota : \mathbb{Z} \to \mathbb{Q}$ is an epimorphism. Let $\alpha_1, \alpha_2 : \mathbb{Q} \to \mathrm{End}_{\mathsf{Ab}}(G)$ be ring homomorphisms. Then notice that since φ is the unique homomorphism $\mathbb{Z} \to \mathrm{End}_{\mathsf{Ab}}(G)$, we must have $\alpha_1 \circ \iota = \alpha_2 \circ \iota = \varphi$, and thus because ι is an epimorphism, $\alpha_1 = \alpha_2$. Therefore there is a unique structure of a $\mathbb{Q}$-vector space on G. □

5.7. Let K be a field, $k \subseteq K$ be a subfield of K. Show that K is a vector space over k (and in fact a k-algebra) in a natural way. In this situation, we say that K is an *extension* of k.

Solution. Let K be a field, $k \subseteq K$ a subfield. Then in particular the inclusion $\iota : k \to K$ is a ring homomorphism, both k and K are commutative (because they are fields), and thus K is a k-algebra. □

5.8. What is the initial object of the category R-Alg?

Solution. Let R be a commutative ring. The objects of R-Alg are ring homomorphisms $\alpha : R \to S$, satisfying the condition that $\alpha(R)$ is contained in the center of S. Homomorphisms of R-algebras are ring homomorphisms preserving the module structure.

The initial object of R-Alg is the identity homomorphism $\mathrm{id}_R : R \to R$ (it is clear that $\mathrm{id}_R(R) = R$ and since R is commutative, the whole ring is in fact contained in its center). To see this, notice that if we have any R-algebra, say $\alpha : R \to S$, then the unique homomorphism R and S (as R-algebras) is just α - it is a ring homomorphism, and it is compatible with the module structure. □

5.9. ¬ Let R be a commutative ring, and let M be an R-module. Prove that the operation of composition on the R-module $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ makes the latter an R-algebra in a natural way.

Prove that $\mathcal{M}_n(R)$ (cf. Exercise 1.4) is an R-algebra, in a natural way. [VI.1.12, VI.2.3]

Solution. Let R be a commutative ring, M an R-module. Consider the R-module $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$. Notice, that we have $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M) \subseteq \mathrm{End}_{\mathsf{Ab}}(M)$, and we know $\mathrm{End}_{\mathsf{Ab}}(M)$ is in fact a ring, with the operations of addition and composition, as we have seen in §1.1. Clearly, composition preserves $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$, and thus $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ is a ring. Define a function $\alpha : R \to \mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ by $r \mapsto r \cdot \mathrm{id}_M$ (where $r\varphi(m) = \varphi(rm)$. It is not hard to check that α is a ring homomorphism: Let $r, s \in R$, then using the R-module structure of $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ we have

$$\alpha(r+s) = (r+s) \cdot \mathrm{id}_M = r \cdot \mathrm{id}_M + s \cdot \mathrm{id}_M = \alpha(r) + \alpha(s)$$

and

$$\alpha(rs) = (rs) \cdot \mathrm{id}_M = r \cdot (s \cdot \mathrm{id}_M) = r \cdot (\alpha(s)) = \alpha(r) \circ \alpha(s)$$

Clearly we also have $\alpha(1_R) = 1_R \cdot \mathrm{id}_M = \mathrm{id}_M$. The ring $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ is not commutative in general, however, notice that for $r \in R$, $\varphi \in \mathrm{End}R\text{-}\mathsf{Mod}(M)$, $m \in M$, we have

$$(\alpha(r) \circ \varphi)(m) = (r \cdot \mathrm{id}_M \circ \varphi)(m) = \mathrm{id}_M(r \cdot \varphi(m)) = \mathrm{id}_M(\varphi(rm)) = \varphi(rm)$$

and

$$(\varphi \circ \alpha(r))(m) = \varphi(r \cdot \mathrm{id}_M(m)) = \varphi(rm).$$

Therefore $\alpha(R)$ is indeed contained in the center of $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$. Thus $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ with the operation of composition is in fact an R-algebra in a natural way.

Consider the function $\alpha : R \to \mathcal{M}_n(R)$ defined by mapping r to the $n \times n$ matrix with r in all entries on the main diagonal and 0_R elsewhere. Clearly, this is a ring homomorphism. It is not hard to see that $\alpha(R)$ is contained in the center of $\mathcal{M}_n(R)$, because all such matrices commute with each other (because R itself is commutative). Thus $\mathcal{M}_n(R)$ is an R-algebra in a natural way. □

5.10. Let R be a commutative ring, and let M be a simple R-module (cf. Exercise 5.4). Prove that $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ is a division R-algebra.

Solution. Let R be a commutative ring, M a simple R-module. Then $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ is an R-algebra, by Exercise 5.9. Noting the result of Exercise 5.4., we see that every $f \in \mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ such that $f \neq 0$, f is an isomorphism and thus has an inverse in the endomorphism ring of M. This makes the ring a division ring, and hence a division R-algebra. □

5.11. ▷ Let R be a commutative ring, and let M be an R-module. Prove that there is a natural bijection between the set of $R[x]$-module structures on M (extending the given R-module structure) and $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$. [§VI.7.1]

Solution. Let R be a commutative ring, M an R-module. $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ together with the operation of composition is an R-algebra by Exercise 5.9. The R-algebra structure corresponds to a ring homomorphism $\alpha : R \to \mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$. Let $\varphi \in \mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$. Then since $\alpha(R)$ is contained in the center of the ring $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$, we can use the universal property of polynomials to extend α to $\overline{\alpha} : R[x] \to \mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ (mapping x to φ). We can use $\overline{\alpha}$ to define an $R[x]$-module structure on M by defining

$$\rho(f(x), m) = \overline{\alpha}(f(x))(m).$$

Indeed, ρ defines an action of $R[x]$ on M - let $f(x), g(x) \in R[x]$, $m, n \in M$. Then

$$\begin{aligned}\rho(f(x), m+n) &= \overline{\alpha}(f(x))(m+n) = \overline{\alpha}(f(x))(m) + \overline{\alpha}(f(x))(n) \\ &= \rho(f(x), m) + \rho(f(x), n),\end{aligned}$$

because $\overline{\alpha}(f(x))$ is an R-module homomorphism,

$$\begin{aligned}\rho(f(x)+g(x), m) &= \overline{\alpha}(f(x)+g(x))(m) = \overline{\alpha}(f(x))(m) + \overline{\alpha}(g(x))(m) \\ &= \rho(f(x), m) + \rho(g(x), m)\end{aligned}$$

and

$$\begin{aligned}\rho(f(x)g(x), m) &= \overline{\alpha}(f(x)g(x))(m) = \overline{\alpha}(f(x)) \circ \overline{\alpha}(g(x))(m) \\ &= \rho(f(x), \rho(g(x), m))\end{aligned}$$

because $\overline{\alpha}$ is a ring homomorphism. Finally, $\rho(1, m) = \overline{\alpha}(1)(m) = \mathrm{id}_M(m) = m$. Notice, that $\overline{\alpha}$ is uniquely determined by φ, and thus each φ determines a unique $R[x]$-module structure on M.

Conversely, if we have an $R[x]$-module structure on M, then the function $\varphi : M \to M$ defined by $\varphi(m) = xm$ is an R-module homomorphism - for $m, n \in M$ we have $\varphi(m+n) = x(m+n) = xm + xn = \varphi(m) + \varphi(n)$ (because of the $R[x]$-module structure on M) and for $r \in R$ we have $\varphi(rm) = xrm = rxm = r\varphi(m)$ (because R commutes with x in $R[x]$). □

5.12. ▷ Let R be a ring. Let M, N be R-modules, and let $\varphi : M \to N$ be a homomorphism of R-modules. Assume φ is a bijection, so that it has an inverse φ^{-1} as a set-function. Prove that φ^{-1} is a homomorphism of R-modules. Conclude that a bijective R-module homomorphism is an isomorphism of R-modules. [§5.2, §VI.2.1, §IX.1.3]

Solution. Let R be a ring, M, N be R-modules, $\varphi : M \to N$ a homomorphism of R-modules. Assume φ is a bijection. Because M and N are in particular abelian groups, φ^{-1} (as a set-function inverse of φ) is a group homomorphism. It remains to check that φ^{-1} is compatible with the R-module structure. Let $r \in R$, $n \in N$, and $m \in M$ be such that $\varphi(m) = n$. Then $\varphi(rm) = r\varphi(m) = rn$, and thus $\varphi^{-1}(rn) = rm = r\varphi^{-1}(n)$. Thus φ^{-1} is indeed an R-module homomorphism, and thus we can conclude that bijective R-module homomorphisms are in fact isomorphisms of R-modules. □

5.13. Let R be an integral domain, and let I be a nonzero *principal* ideal of R. Prove that I is isomorphic to R as an R-module.

Solution. Let R be an integral domain, and I a nonzero principal ideal of R. Then $I = (a)$ for some $a \in R$, $a \neq 0$. Define a function $\varphi : R \to I$ by $\varphi(r) = ar$. Clearly, for $r, s \in R$, $\varphi(r+s) = a(r+s) = ar + as = \varphi(r) + \varphi(s)$ and $\varphi(sr) = asr = sar = s\varphi(ar)$ (because R is commutative). Thus φ is an R-module homomorphism.

Let $i \in I$. Then $i = ar$ for some $r \in R$, and thus φ is surjective. Suppose $r, s \in R$, and $\varphi(r) = \varphi(s)$. Then $0 = \varphi(r-s) = a(r-s)$. Since R is an integral domain, there are no nonzero zero-divisors, and thus $r - s = 0$, hence $r = s$. Thus φ is a bijective R-module homomorphism, and by Exercise 5.12, I and R are isomorphic as R-modules. □

5.14. ▷ Prove Proposition 5.18. [§5.4]

Solution. Let R be a ring, N, P, submodules of an R-module M. $N + P$ is a subgroup of M and for $r \in R$, $n \in N$, $p \in P$, we have $r(n+p) = rn + rp$ with $rn \in N$, $rp \in P$, and thus $rn + rp \in N + P$. Therefore $N + P$ is a submodule of M.

Similarly $N \cap P$ is a subgroup of P. Let $r \in R$, $m \in N \cap P$. Then $m \in N$ and $m \in P$, hence $rm \in N$ (because N is an R-module), and $rm \in P$ (because P is an R-module). Therefore $rm \in N \cap P$ and thus $N \cap P$ is a submodule of P.

Consider the homomorphism $\varphi : P \to (N+P)/N$ defined by $\varphi(p) = p + N$. φ is clearly surjective, as the elements of $(N+P)/N$ are of the form $n + p + N$ with $n \in N$, $p \in P$, but $n + N = N$, and thus $n + p + N = p + N = \varphi(p)$.

By the first isomorphism theorem we then have

$$\frac{N+P}{N} \cong \frac{P}{\ker \varphi}.$$

Now, $\ker \varphi = \{p \in P \mid \varphi(p) = 0\} = \{p \in P \mid p + N = N\} = \{p \in P \mid p \in N\} = N \cap P$, finishing our proof. □

5.15. Let R be a commutative ring, and let I, J be ideals of R. Prove that $I \cdot (R/J) \cong (I+J)/J$ as R-modules.

Solution. Let R be a commutative ring, I, J ideals of R. The elements of $I \cdot (R/J)$ are of the form $\sum_k i_k(r_k + J) = i_k r_k + J$ for $i_k \in I$ and $r_k \in R$. Notice, that $i_k r_k \in I$ because I is an ideal, and thus each such element is in particular an element of $(I+J)/J$. Thus $I \cdot (R/J) \subseteq (I+J)/J$ and the inclusion function $\iota : I \cdot (R/J) \to (I+J)/J$ is an R-module homomorphism - both addition and the R-module structure are clearly preserved.

As ι is an inclusion, it is injective. Let $i + j + J \in (I+J)/J$. Then $i + j + J = i + J$, and since R is a ring (with identity), we have an element $i(1_R + J) = i + J \in I \cdot (R/J)$ such that $\iota(i + J) = i + J$.

Thus ι is in fact an isomorphism of R-modules. □

5.16. ¬ Let R be a commutative ring, M an R-module, and let $a \in R$ be a nilpotent element, determining a submodule aM of M. Prove that $M = 0 \iff aM = M$. (This is a particular case of *Nakayama's lemma*, Exercise VI.3.8.) [VI.3.8]

Solution. Let R be a commutative ring, M an R-module, $a \in R$ nilpotent. Suppose $M = 0$. Then $aM = 0 = M$. On the other hand, suppose $aM = M$. Consider a^nM. The elements of a^nM are of the form a^nm for $m \in M$. Rewriting this, we get $a^{n-1}(am)$, but $am \in aM = M$ and thus $am = m'$ for some $m' \in M$. Continuing this process we see that $a^nM = M$ for all n. But since a is a nilpotent element of R, there is a number n such that $a^n = 0$. This implies $0 = 0M = M$, as needed. □

5.17. ▷ Let R be a commutative ring, and let I be an ideal of R. Noting that $I^j \cdot I^k \subseteq I^{j+k}$, define a ring structure on the direct sum

$$\operatorname{Rees}_R(I) := \bigoplus_{j\geq 0} I^j = R \oplus I \oplus I^2 \oplus I^3 \oplus \cdots.$$

The homomorphism sending R identically to the first term in this direct sum makes $\operatorname{Rees}_R(I)$ into an R-algebra, called the *Rees algebra* of I. Prove that if $a \in R$ is a non-zero-divisor, then the Rees algebra of (a) is isomorphic to the polynomial ring $R[x]$ (as an R-algebra). [5.18]

Solution. The natural way to define multiplication on $\operatorname{Rees}_R(I)$ is to let the $(r_0, r_1, \dots) \cdot (s_0, s_1, \dots) = (r_0s_0, r_1s_0 + r_0s_1, \dots)$, i.e. letting the k-th entry equal $\sum_{i+j=k} r_is_j$. This works, because $r_i \in I^i$, $s_j \in I^j$, and thus $r_is_j \in I^i \cdot I^j \subseteq I^{i+j} = I^k$. This multiplication is very similar to the way how the multiplication in $R[x]$ is defined.

Let $a \in R$ be a non-zero-divisor, consider $\operatorname{Rees}_R((a))$. We can define a function $\varphi : R[x] \to \operatorname{Rees}_R((a))$ by setting $\varphi(r) = (r, 0, 0, \dots)$ for $r \in R$, and $\varphi(x) = (0, a, 0, \dots)$. For any $f(x)$ we can then define $\varphi(f(x))$ by enforcing the conditions of an R-algebra homomorphism on φ. Notice, that φ defined in this way is a bijection. □

5.18. With notation as in Exercise 5.17 let $a \in R$ be a non-zero-divisor, let I be any ideal of R, and let J be the ideal aI. Prove that $\operatorname{Rees}_R(J) \cong \operatorname{Rees}_R(I)$.

Solution. □

6. Products, coproducts, etc., in R-Mod

6.1. ▷ Prove Claim 6.3. [§6.3]

Solution. Let R be a ring, A a set. We want to show that $F^R(A) \cong R^{\oplus A}$ as R-modules. Notice, that every element of $R^{\oplus A}$ can be written uniquely as a finite sum

$$\sum_{a\in A} r_a j(a), \quad r_a \neq 0 \text{ for only finitely many } a;$$

indeed, any $\alpha : A \to R \in R^{\oplus A}$ is defined only on finite number of $a \in A$. If $a \in A$ is such that $\alpha(a) \neq 0$, then $\alpha(a) = r$ for some $r \in R$. But then $\alpha(a) = rj_a(a)$. Since $1 = j_a(a) \neq j_b(a) = 0$ for any $b \in A$, $a \neq b$, then the above sum in fact precisely defines the function α.

Using this observation, we will show that $R^{\oplus A}$ satisfies the universal property of free R-modules. Let $f : A \to M$ be a set-function from A to an R-module M. Define $\varphi : R^{\oplus A} \to M$ by

$$\varphi(\sum_{a\in A} r_a j(a)) := \sum_{a\in A} r_a f(a);$$

this definition is forced upon us by the needed commutativity of the respective diagram. This means φ is certainly uniquely determined. We will check that it is in fact an R-module homomorphism:

$$\begin{aligned}
\varphi(\sum_{a\in A} r_a j(a)) + \varphi(\sum_{a\in A} r'_a j(a)) &= \sum_{a\in A} r_a f(a) + \sum_{a\in A} r'_a f(a) \\
&= \sum_{a\in A} (r_a + r'_a) f(a) \\
&= \varphi(\sum_{a\in A} (r_a + r'_a) j(a)) \\
&= \varphi(\sum_{a\in A} r_a j(a) + \sum_{a\in A} r'_a j(a)),
\end{aligned}$$

and

$$\begin{aligned}
\varphi(r \sum_{a\in A} r_a j(a)) &= \varphi(\sum_{a\in A} r r_a j(a)) \\
&= \sum_{a\in A} r r_a f(a) \\
&= r \sum_{a\in A} r_a f(a) \\
&= r\varphi(\sum_{a\in A} r_a j(a)).
\end{aligned}$$

Thus $R^{\oplus A}$ satisfies the universal property of free R-module on the set A. □

6.2. Prove or disprove that if R is ring, and M is a nonzero R-module, then M is not isomorphic to $M \oplus M$.

Solution. Consider the ring $\mathbb{Z}$, and the $\mathbb{Z}$-module $\mathbb{Z}^{\oplus\mathbb{N}}$. In Exercise II.5.9 we have shown that $\mathbb{Z}^{\oplus\mathbb{N}} \oplus \mathbb{Z}^{\oplus\mathbb{N}} \cong \mathbb{Z}^{\oplus\mathbb{N}}$ as abelian groups, and thus in particular they are isomorphic as $\mathbb{Z}$-modules. □

6.3. Let R be a ring, M an R-module, and $p : M \to M$ an R-module homomorphism such that $p^2 = p$. (Such a map is called a projection.) Prove that $M \cong \ker p \oplus \operatorname{im} p$.

Solution. Let R be a ring, M an R-module, $p : M \to M$ an R-module homomorphism such that $p^2 = p$. Let $m \in M$. Then we have $m = m - p(m) + p(m)$. Notice, that $p(m - p(m)) = p(m) - p^2(m) = 0$. Thus $m - p(m) \in \ker p$, $p(m) \in \operatorname{im} p$.

Define a function $\varphi : \ker p \oplus \operatorname{im} p \to M$ by $\varphi((k, i)) = k + i$. Clearly this is an R-module homomorphism due to the fact that M and $\ker p \oplus \operatorname{im} p$ are R-modules. As we have noted above, every $m \in M$ can be written in the form $(m - p(m)) + p(m)$ where $m - p(m) \in \ker p$ and $p(m) \in \operatorname{im} p$, thus φ is surjective. What is the kernel of φ? Suppose $\varphi((k, i)) = 0$. Then $k + i = 0$, and thus $k = -i$. Noting that $\ker p$ is a submodule of M, that implies $i \in \ker p$. Thus $i \in \ker p \cap \operatorname{im} p$. Since $i \in \operatorname{im} p$, there is some $m \in M$ such that $p(m) = i$. But then $i = p(m) = p^2(m) = p(i) = 0$. Thus $\ker \varphi = \{(0, 0)\}$, showing that φ is injective. Thus φ is a bijective R-module homomorphism, showing that in fact $M \cong \ker p \oplus \operatorname{im} p$. □

6.4. ▷ Let R be a ring, and let $n > 1$. View $R^{\oplus(n-1)}$ as a submodule of $R^{\oplus n}$, via the injective homomorphism $R^{\oplus(n-1)} \hookrightarrow R^{\oplus n}$ defined by

$$(r_1, \ldots, r_{n-1}) \mapsto (r_1, \ldots, r_{n-1}, 0).$$

Give a one-line proof that

$$\frac{R^{\oplus n}}{R^{\oplus(n-1)}} \cong R.$$

Solution. $(r_1, \ldots, r_{n-1}, r_n) \mapsto r_n$ defines a surjective homomorphism $R^{\oplus n} \to R$ with the kernel being $R^{\oplus(n-1)}$. □

6.5. ▷ (Notation as in §6.3.) For any ring R and any two sets A_1, A_2, prove that $(R^{\oplus A_1})^{\oplus A_2} \cong R^{\oplus(A_1 \times A_2)}$. [§VIII.2.2]

Solution. Let R be any ring, A_1, A_2 any sets. Let $f \in R^{\oplus(A_1 \times A_2)}$. Notice that we can define a function $\varphi_f : A_2 \to R^{\oplus A_1}$ by setting $\varphi_f(a_2)(a_1) = f(a_1, a_2)$ for $a_1 \in A_1$, $a_2 \in A_2$. By the definition of $R^{\oplus(A_1 \times A_2)}$, $f(a_1, a_2) \neq 0$ for only finitely many (a_1, a_2). In particular, this ensures that φ_f is in fact well-defined. Then we can define a function $\varphi : R^{\oplus(A_1 \times A_2)} \to (R^{\oplus A_1})^{\oplus A_2}$ by setting $\varphi(f) = \varphi_f$.

It is easy to show that φ is in fact a homomorphism of R-modules. Let $r \in R$ and $f, g \in R^{\oplus(A_1 \times A_2)}$. Then for every $a_1 \in A_1$, $a_2 \in A_2$, we have

$$\begin{aligned} \varphi(f + g)(a_2)(a_1) &= \varphi_{f+g}(a_2)(a_1) \\ &= (f + g)(a_1, a_2) = f(a_1, a_2) + g(a_1, a_2) \\ &= \varphi(f)(a_2)(a_1) + \varphi(g)(a_2)(a_1), \end{aligned}$$

and

$$\begin{aligned}\varphi(rf)(a_2)(a_1) &= \varphi_{rf}(a_2)(a_1)\\ &= (rf)(a_1,a_2)\\ &= r(f(a_1,a_2))\\ &= r\varphi(f)(a_2)(a_1).\end{aligned}$$

The 0 of $(R^{\oplus A_1})^{\oplus A_2}$ is the function $A_2 \to R^{\oplus A_1}$ mapping all $a_2 \in A_2$ to the 0 of $R^{\oplus A_1}$ which is in turn the function $A_1 \to R$ mapping all $a_1 \in A_1$ to 0. It is then evident from the definition of φ that f maps to 0 only when $f(a_1, a_2) = 0$ for all $a_1 \in A_1$, $a_2 \in A_2$. Thus $\ker\varphi = \{0\}$, and we see that φ is injective.

Now let $g \in (R^{\oplus A_1})^{\oplus A_2}$. Then for each $a_2 \in A$ such that $g(a_2) \neq 0$, we have a function again defined for a finite number of elements $a_1 \in A_1$ such that $g(a_2)(a_1) = r$ for some $r \in R$. This enables us to reconstruct a function $f \in R^{\oplus(A_1\times A_2)}$, by setting $f(a_1, a_2) = g(a_2)(a_1)$. Clearly this is defined only for a finite number of elements $(a_1, a_2) \in A_1 \times A_2$ and thus $f \in R^{\oplus(A_1\times A_2)}$ as needed, showing that φ is surjective, and therefore in fact a bijection. □

6.6. ¬ Let R be a ring, and let $F = R^{\oplus n}$ be a finitely generated free R-module. Prove that $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(F, R) \cong F$. On the other hand, find an example of a ring R and a nonzero R-module M such that $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, R) = 0$. [6.8]

Solution. Let R be a ring, $F = R^{\oplus n}$ a finitely generated free R-module. Define a function $\varphi : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(F, R) \to F$ by setting $\varphi(f) = (f(j(1)), \ldots, f(j(n)))$. Now, if $f, g \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(F, R)$, we have

$$\begin{aligned}\varphi(f+g) &= ((f+g)(j(1)), \ldots, (f+g)(j(n)))\\ &= (f(j(1)) + g(j(1)), \ldots, f(j(n)) + g(j(n)))\\ &= (f(j(1)), \ldots, f(j(n))) + (g(j(1)), \ldots g(j(n)))\\ &= \varphi(f) + \varphi(g)\end{aligned}$$

and thus φ is a group homomorphism.

The kernel of φ consists of homomorphisms which map all $j(i)$ to 0 for $1 \leq i \leq n$. Only such homomorphism $F \to R$ is the one which maps everything to 0 (because every element of F is in fact a sum over $j(i)$), thus φ is injective. On the other hand, let $(r_1, \ldots, r_n) \in F$. Then we can define a function $F \to R$ by forcing $f(j(i)) = r_i$ for $1 \leq i \leq n$. By enforcing the rules for an R-module homomorphism and the fact that each element of F can be written as a sum $\sum_{1\leq i\leq n} s_i j(i)$ (where $s_i \in R$), this indeed defines a homomorphism in $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(F, M)$ and therefore φ is surjective.

Thus $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(F, M) \cong F$ as abelian groups. Since F is an R-module, we can force an R-module structure on $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(F, M)$ (even in the case R is not commutative) by setting $rf = \varphi^{-1}(r\varphi(f))$ for all $r \in R$, $f \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(F, R)$.

If $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$ (which is a non-zero $\mathbb{Z}$-module), then $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, R) = 0$, because in fact the only homomorphism $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}$ must map everything to 0. □

6.7. ▷ Let A be any set.

- For any family $\{M_a\}_{a\in A}$ of modules over a ring R, define the *product* $\prod_{a\in A} M_a$ and coproduct $\bigoplus_{a\in A} M_a$. If $M_a \cong R$ for all $a \in A$, these are denoted R^A, $R^{\oplus A}$, respectively.
- Prove that $\mathbb{Z}^{\mathbb{N}} \ncong \mathbb{Z}^{\oplus\mathbb{N}}$. (Hint: Cardinality.)

[§6.1, 6.8]

Solution. Let A by any set, consider a family $\{M_a\}_{a\in A}$ of modules of a ring R. If A is finite, the product and coproduct is just the direct sum of the modules. The general case is a little bit more involved.

Let us first define the product $\prod_{a\in A} M_a$ as the set of all set-function $\alpha : A \to \bigcup_{a\in A} M_a$, such that $\alpha(a) \in M_a$ for all $a \in A$. Let $r \in R$, $\alpha, \beta \in \prod_{a\in A} M_a$. Define the function $\alpha + \beta : A \to \bigcup_{a\in A}$ by setting $(\alpha + \beta)(a) = \alpha(a) + \beta(a)$. Then indeed $\alpha + \beta \in \prod_{a\in A} M_a$ since for any $a \in A$, $\alpha(a), \beta(a) \in M_a$ by definition, and thus $\alpha(a) + \beta(a) \in M_a$ since M_a is an R-module. Similarly, define $r\alpha$ by setting $(r\alpha)(a) = r(\alpha(a))$. Again, $r\alpha \in \prod_{a\in A} M_a$. Thus $\prod_{a\in A} M_a$ is an R-module. This module, together with the R-module homomorphisms $\pi_a : \prod_{a\in A} M_a \to M_a$ defined by $\pi_a(\alpha) = \alpha(a)$, satisfies the universal property of products of a family of modules - if P is an R-module and $f_a : P \to M_a$ for $a \in A$ are R-module homomorphisms, then the required commutativity of the related family of diagrams forces upon us a function $\sigma : P \to \prod_{a\in A} M_a$, defined by setting $\sigma(p) = \alpha_p$, where $\alpha_p : A \to \bigcup_{a\in A} M_a$ is defined by setting $\alpha_p(a) = f_a(p)$. It is not hard to see that σ is indeed an R-module homomorphism and thus it follows that $\prod_{a\in A} M_a$ is indeed the product of the family $\{M_a\}_{a\in A}$.

The situation with coproducts is a little bit more involved. First notice, that if C is an R-module which satisfies the respective universal property, we have also have the inclusion homomorphisms $\iota_a : M_a \to C$. This means that C must in fact contain all the finite sums of the form $r_1\iota_{a_1}(m_1) + \cdots + r_k\iota_{a_k}(m_k)$, where $r_1, \ldots, r_k \in R$, $a_1, \ldots, a_k \in A$, $m_i \in M_{a_i}$ for $1 \le i \le k$. Using the fact that ι_a is an R-module homomorphism for each $a \in A$, we can then rewrite this to sum to $\iota_{a_1}(r_1m_1) + \cdots + \iota_{a_k}(r_km_k)$. Since M together with the inclusions must be an initial object of the respective category, indeed it can only contain such sums as elements. Combining our knowledge of the products defined above and the way free R-modules are defined, the definition of $\oplus_{a\in A} M_a$ is then simply to take all the functions in $\prod_{a\in A} M_a$ which are non-zero for a finite number of $a \in A$.

$\mathbb{Z}^{\mathbb{N}} \ncong \mathbb{Z}^{\oplus\mathbb{N}}$ because $\mathbb{Z}^{\mathbb{N}}$ is uncountable, while $\mathbb{Z}^{\oplus\mathbb{N}}$ is countable. Thus they cannot be isomorphic as sets, and thus neither as $\mathbb{Z}$-modules. □

6.8. Let R be a ring. If A is any set, prove that $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R^{\oplus A}, R)$ satisfies the universal property for the *product* of the family $\{R_a\}_{a\in A}$, where $R_a \cong R$ for all a; thus,

$\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R^{\oplus A}, R) \cong R^A$. Conclude that $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R^{\oplus A}, R)$ is *not* isomorphic to $R^{\oplus A}$ in general (cf. Exercise 6.6 and 6.7).

Solution. Let R be a commutative ring, A any set. Consider the set $S = \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R^{\oplus A}, R)$. For each $a \in A$, define a function $\pi_a : S \to R_a$ by setting $\pi_a(f) = f(\iota_a(1_R))$ for $f \in S$ and $\iota_a : R_a \to S$ being the injection homomorphism. Indeed, π_a is an R-module homomorphism, because each $f \in S$ is an R-module homomorphism.

We shall show that S with the homomorphisms π_a, $a \in A$, satisfies the universal property of product of the family of R-modules $\{R_a\}_{a\in A}$. Let P be an R-module, and $f_a : P \to R_a$ being R-module homomorphisms for $a \in A$. The commutativity of the respective commutative diagrams forces upon us a definition of a function $\sigma : P \to S$: set $\sigma(p) = \varphi_p$ for $p \in P$, where φ_p is an R-module homomorphism defined by requiring $\varphi_p(\iota_a(1_R)) = f_a(p)$ for $a \in A$. Indeed, since the elements of $R^{\oplus A}$ are finite sums of the form $\sum_i r_i \iota_{a_i}(1_R)$, $a_i \in A$, φ_p is fully defined by the definition given above.

We have to show that σ is an R-module homomorphism. Let $r \in R$, $p, s \in P$. Then $\sigma(p + s) = \varphi_{p+s}$ and

$$\begin{aligned}\varphi_{p+s}(\sum_i r_i\iota_{a_i}(1_R)) &= \sum_i r_i f_{a_i}(p+s) = \sum_i r_i(f_{a_i}(p) + f_{a_i}(s)) \\ &= \sum_i (r_i f_{a_i}(p) + r f_{a_i}(s)) = \sum_i r_i f_{a_i}(p) + \sum_i r_i f_{a_i}(s) \\ &= \varphi_p(\sum_i r_i\iota_{a_i}(1_R)) + \varphi_s(\sum_i r_i\iota_{a_i}(1_R)).\end{aligned}$$

Thus $\sigma(p + s) = \sigma(p) + \sigma(s)$. Similarly, $\sigma(rp) = \varphi_{rp}$ and

$$\begin{aligned}\varphi_{rp}(\sum_i r_i\iota_{a_i}(1_R)) &= \sum_i r_i f_{a_i}(rp) = \\ &= \sum_i r_i r f_{a_i}(p) = \sum_i r r_i f_{a_i}(p) \\ &= r\sum_i r_i f_{a_i}(p) = r\varphi_p(\sum_i r_i\iota_{a_i}(1_R)).\end{aligned}$$

Thus σ is indeed an R-module homomorphism, and is unique by the required commutativity of the respective diagrams. Therefore $S \cong R^A$.

By Exercise 6.6, $\mathbb{Z}^{\oplus\mathbb{N}} \ncong \mathbb{Z}^{\mathbb{N}}$, showing that $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R^{\oplus A}, R)$ is in fact not isomorphic to $R^{\oplus A}$ in general. □

6.9. ¬ Let R be a ring, F a nonzero free R-module, and let $\varphi : M \to N$ be a homomorphism of R-modules. Prove that φ is onto if and only if for all R-module homomorphisms $\alpha : F \to N$ there exists an R-module homomorphism $\beta : F \to M$ such that $\alpha = \varphi \circ \beta$. (Free modules are *projective*, as we will see in Chapter VIII.) [7.8, VI.5.5]

Solution. Let R be a ring, F a nonzero free R-module, $\varphi : M \to N$ a homomorphism of R-modules. First note that since F is free, there is a set A such that $F = F^R(A)$. Suppose φ is onto. Let $\alpha : F \to N$ be an arbitrary R-module homomorphism. Let $f \in F$, so that $f = \sum_{a\in A} r_a a$. Then we can see that $\alpha(f)$ is uniquely determined by the images $\alpha(a)$ for $a \in A$. Since φ is onto, for each $a \in A$ we have (a not necessarily unique) element $m \in M$ such that $\varphi(m) = \alpha(a)$. This enables us to define a function $\beta : F \to M$ by setting $\beta(a) = m$ such that $\varphi(m) = \alpha(a)$ and forcing it to be an R-module homomorphism. Indeed, this is legal, since again, the image of each element of F is uniquely determined by the images of $a \in A$. We then have

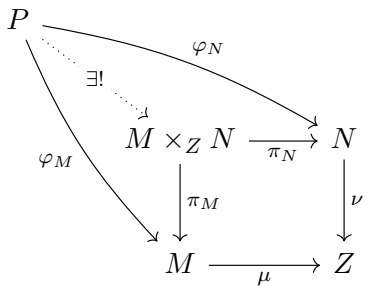
$$\begin{aligned}\varphi \circ \beta(\sum_{a\in A} r_a a) &= \varphi(\sum_{a\in A} r_a \beta(a)) \\ &= \sum_{a\in A} r_a \varphi(\beta(a)) \\ &= \sum_{a\in A} r_a \alpha(a) \\ &= \alpha(\sum_{a\in A} r_a a)\end{aligned}$$

as needed.

On the other hand, suppose that for each R-module homomorphism $\alpha : F \to N$ there is an R-module homomorphism $\beta : F \to M$ such that $\alpha = \varphi \circ \beta$. Let $n \in N$ be arbitrary. Invoking the universal property of free R-modules we get a homomorphism $\alpha : F \to N$ such that $\delta(a) = n$ for some $a \in A$. Then we have a homomorphism $\beta : F \to M$ such that $\alpha = \varphi \circ \beta$ by our assumption. In particular, we have $n = \alpha(a) = \varphi \circ \beta(a)$, hence $\varphi(\beta(a)) = n$. Since this holds for any $n \in N$, φ is onto. □

6.10. ▷ (Cf. Exercise I.5.12.) Let M, N, and Z be R-modules, and let $\mu : M \to Z$, $\nu : N \to Z$ be homomorphisms of R-modules.

Prove that R-Mod has 'fibered products': there exists an R-module $M \times_Z N$ with R-module homomorphisms $\pi_M : M \times_Z N \to M$, $\pi_: M \times_Z N \to N$, such that $\mu \circ \pi_M = \nu \circ \pi_N$, and which is universal with respect to this requirement. That is, for every R-module P and R-module homomorphisms $\varphi_M : P \to M$, $\varphi_N : P \to N$ such that $\mu \circ \varphi_M = \nu \circ \varphi_N$, there exists a unique R-module homomorphism $P \to M \times_Z N$ making the diagram



commute. The module $M \times_Z N$ may be called the *pull-back* of M along ν (or of N along μ, since the construction is symmetric). 'Fiber diagrams'

$$\begin{array}{ccc} M \times_Z N & \longrightarrow & N \\ \downarrow & \square & \downarrow{\scriptstyle \nu} \\ M & \xrightarrow[\mu]{} & Z \end{array}$$

are commutative, but 'even better' than commutative; they are often decorated by a square, as shown here.

Solution. Define a set $M \times_Z N = \{(m, n) \mid m \in M, n \in N, \mu(m) = \nu(n)\}$, and endow it with the component-wise addition and multiplication by $r \in R$ on the left as usual. Indeed, this defines an R-module, as it is clearly a subset of the R-module $M \times N$, and is closed with respect to addition and the left multiplication by r (because μ and ν are R-module homomorphisms!). The definitions of π_M and π_N are immediate.

Let P be an R-module, $\varphi_M : P \to M$, and $\varphi_N : P \to N$ R-module homomorphisms such that $\mu \circ \varphi_M = \nu \circ \varphi_N$. Clearly, the commutativity of the respective diagram forces upon us a definition of a function $\sigma : P \to M \times_Z N$, $\sigma(p) = (\varphi_M(p), \varphi_N(p))$ (this is indeed well-defined because $\mu \circ \varphi_M(p) = \nu \circ \varphi_N(p)$ by definition). It is immediately seen that this is an R-module homomorphism.

Thus $M \times_Z N$ satisfies the universal property of a fibered product as defined above. □

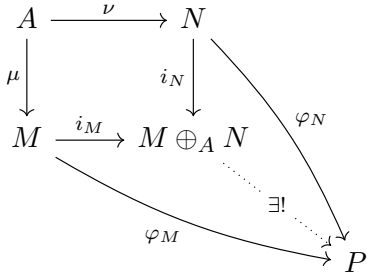
6.11. ▷ Define a notion of *fibered coproduct* of two R-modules M, N, along an R-module A, in the style of Exercise 6.10 (and cf. Exercise I.5.12)

$$\begin{array}{ccc} A & \xrightarrow{\nu} & N \\ {\scriptstyle \mu}\downarrow & & \downarrow \\ M & \longrightarrow & M \oplus_A N \end{array}$$

Prove that fibered coproducts exist in R-Mod. The fibered coproduct $M \oplus_A N$ is called the *push-out* of M along ν (or of N along μ). [§6.1]

Solution. A fibered coproduct of two R-modules is defined as an R-module $M \oplus_A N$ with R-module homomorphisms $i_M : M \to M \oplus_A N$, $i_N : N \to M \oplus_A N$, such that $i_M \circ \mu = i_N \circ \nu$, and which is universal with respect to this requirement. That is, for every R-module P and R-module homomorphisms $\varphi_M : M \to P$, $\varphi_N : N \to P$ such that $\varphi_M \circ \mu = \varphi_N \circ \nu$, there exists a unique R-module homomorphism $M \oplus_A N \to P$

making the diagram



commute.

First notice, that if $A = 0$, then the fibered coproduct coincides with the direct sum $M \oplus N$, that is, there are no restrictions poised by the morphisms μ and ν. In the general case, we want to identify the elements of $M \oplus N$ with the same preimage $a \in A$. In particular, this means we want to consider a quotient by a certain submodule of $M \oplus N$. Consider the set $T = \{(\mu(a), -\nu(a)) \mid a \in A\}$. This is clearly a submodule of $M \oplus N$. Define $M \oplus_A N = (M \oplus_A N)/T$, $i_M(m) = (m, 0) + T$ and $i_N(n) = (0, n) + T$. For $a \in A$ we have $i_M \circ \mu(a) - i_N \circ \nu(a) = ((\mu(a), 0) + T) - ((0, \nu(a)) + T) = (\mu(a), -\nu(a)) + T = T$, hence $i_M \circ \mu(a) = i_N \circ \nu(a)$ as needed (this is why we need to have the $-$ in the definition).

Now consider any R-module P and homomorphisms $\varphi_M : M \to P$ and $\varphi_N : N \to P$ such that $\varphi_M \circ \mu = \varphi_N \circ \nu$. The required commutativity of the above diagram forces upon us a function $\sigma : M \oplus_A N \to P$ defined by $\sigma((m, n) + T) = \varphi_M(m) + \varphi_N(n)$. It is easy to see that this is indeed an R-module homomorphism, proving that $M \oplus_A N$ satisfies the given universal property. □

6.12. Prove Proposition 6.2.

Solution. Let $\varphi : M \to N$ be an R-module homomorphism.

Kernels exist in R-Mod - define $\ker \varphi = \{m \mid \varphi(m) = 0\}$. Indeed, this definition with the inclusion morphism $\ker \varphi \hookrightarrow M$ satisfies the required universal property: Let K be an R-module, $\alpha : K \to M$ a homomorphism such that $\varphi \circ \alpha = 0$. Then $\varphi(\alpha(k)) = 0$ for all $k \in K$, and thus $\alpha(k) \in \ker \varphi$. The required homomorphism $K \to \ker \varphi$ is then just α with restricted target.

Cokernels also exist - define $\operatorname{coker} \varphi = N/\operatorname{im} \varphi$, with $\pi : N \to \operatorname{coker} \varphi$ being the quotient homomorphism. If P is an R-module and $\beta : N \to P$ a homomorphism such that $\beta \circ \varphi = 0$. Then $\operatorname{im} \varphi \subseteq \ker \beta$, and thus by the universal property of quotients we have a unique morphism $\widetilde{\beta} : N/\operatorname{im} \varphi \to P$ making the diagram commute.

Suppose φ is a monomorphism. Consider the diagram

$$\ker \varphi \underset{e}{\overset{i}{\rightrightarrows}} M \xrightarrow{\varphi} N$$

where i is the inclusion, e is the trivial map. Both $\varphi \circ i$ and $\varphi \circ e$ are the trivial map, hence $i = e$ (because φ is a monomorphism). But that implies $\ker \varphi$ is trivial. Now suppose

$\ker\varphi = 0$ and $\varphi(m) = \varphi(n)$ for $m, n \in M$. Then $\varphi(m) - \varphi(n) = \varphi(m-n) = 0$, hence $m - n \in \ker\varphi$ and thus $m - n = 0$. This implies $m = n$, hence φ is injective. Lastly, suppose φ is injective. Then φ is a monomorphism in Set. In particular, the defining property of monomorphism must hold for all R-module homomorphisms, showing that φ is a monomorphism in R-Mod as needed.

Suppose φ is an epimorphism. Consider the diagram

$$M \xrightarrow{\varphi} N \underset{e}{\overset{\pi}{\rightrightarrows}} \operatorname{coker}\varphi$$

where π is the canonical projection and e is the trivial map. Both $\pi \circ \varphi$ (because for $m \in M$, $\varphi(m) \in \operatorname{im}\varphi$ and thus $\varphi(m) + \operatorname{im}\varphi = \operatorname{im}\varphi$) and $e \circ \varphi$ are the trivial map, hence $\pi = e$. That implies $\operatorname{coker}\varphi = 0$. Suppose $\operatorname{coker}\varphi = 0$. Then in particular $N/\operatorname{im}\varphi = 0$ which implies $\operatorname{im}\varphi = N$, hence φ is surjective. Lastly, suppose φ is surjective, then φ is an epimorphism in Set. Thus the defining property of epimorphisms must in fact also hold for all R-module homomorphisms, showing that φ is an epimorphism in R-Mod.

If φ is a monomorphism, then M can be seen as a submodule of N, and thus it is a kernel of the canonical projection $N \to N/M$. On the other hand, if φ is an epimorphism, then by the first isomorphism theorem $N \cong M/\ker\varphi$, which is the cokernel of the inclusion morphism $\ker\varphi \hookrightarrow M$. □

6.13. Prove that every homomorphic image of a finitely generated module is finitely generated.

Solution. Let F be a finitely generated R-module and consider an R-module homomorphism $\varphi : F \to M$. Since F is finitely generated, $F = \langle A \rangle$ for some finite set A, say $\{a_1, \dots, a_n\}$. Thus the elements of F are the finite sums

$$\sum_{1 \le i \le n} r_a a_i$$

(where a_i is identified with the tuple of zeroes with a single 1_R in the i-th place). In particular, the image of every such element is uniquely determined by the image of each a_i. Thus $\operatorname{im}\varphi$ is precisely the set of finite sums

$$\sum_{1 \le i \le n} r_a \varphi(a_i)$$

and is in fact isomorphic to $\langle \varphi(a_1), \dots, \varphi(a_n) \rangle$, and therefore is finitely generated. □

6.14. ▷ Prove that the ideal $(x_1, x_2, \dots)$ of the ring $R = \mathbb{Z}[x_1, x_2, \dots]$ is not finitely generated (as an ideal, i.e., as an R-module). [§6.4]

Solution. Suppose that the ideal $(x_1, x_2, \dots)$ of $R = \mathbb{Z}[x_1, x_2, \dots]$ is finitely generated as an ideal, i.e., $I = (x_1, x_2, \dots) = (g_1, \dots, g_n)$ for $g_i \in R$. Each g_i is a finite polynomial, and thus there must be some intermediate, say x_t, which does not appear in none of the generators and such that if x_j is an intermediate of some g_i, $j < t$. Define an R-module homomorphism $\varphi : R \to R$ by setting $\varphi(x_i) = 0$ for $i < t$, and $\varphi(x_i) = 1$ for $i \geq t$. Clearly, $x_t \in I$. Then because I is finitely generated, x_t is a finite sum $\sum_{1 \leq i \ leqn} r_i g_i$, $r_i \in R$. Then $\varphi(x_t) = \sum_{1 \leq i \leq n} r_i \varphi(g_i) = 0 \neq 1$, a contradiction. □

6.15. ▷ Let R be a commutative ring. Prove that a *commutative* R-algebra S is finitely generated *as an algebra* over R if and only if it is finitely generated *as a commutative algebra* over R. (Cf. §6.5.) [§6.5]

Solution. Let R be a commutative ring, S a commutative R-algebra. Suppose S is finitely generated as an algebra over R. Then there is a surjective R-algebra homomorphism $\varphi : R\langle A \rangle \twoheadrightarrow S$, where A is a finite set. $R\langle A \rangle$ consists of 'noncommutative polynomials' with variables in A, and thus it is easy to see that φ is uniquely determined by the images of $a \in A$. Since S is commutative, we can reorder those images as needed, and thus the elements of S can be seen as finite sums $\sum r\varphi^{i_1}(a_1) \dots \varphi^{i_n}(a_n)$. Then we can easily define an R-algebra homomorphism $\delta : R[x_1, \dots, x_n] \twoheadrightarrow S$ by setting $\delta(x_i) = \varphi(a_i)$.

On the other hand, suppose S is finitely generated as a commutative algebra over R. Then there is a surjective homomorphism of R-algebras $\varphi : R[x_1, \dots, x_n] \twoheadrightarrow S$. Then invoking the universal property of free R-algebras we get a unique homomorphism $\delta : R\langle x_1, \dots, x_n \rangle \to R[x_1, \dots, x_n]$ which is immediately seen to be surjective. Thus $\varphi \circ \delta : R\langle x_1, \dots, x_n \rangle \twoheadrightarrow S$ is a surjective R-algebra homomorphism and therefore S is finitely generated as an R-algebra over R. □

6.16. ▷ Let R be a ring. A (left-)R-module M is *cyclic* if $M = \langle m \rangle$ for some $m \in M$. Prove that simple modules (cf. Exercise 5.4) are cyclic. Prove that an R-module M is cyclic if and only if $M \cong R/I$ for some (left-)ideal I. Prove that every quotient of a cyclic module is cyclic. [6.17, §VI.4.1]

Solution. Let R be a ring. Let M be a simple module and $m \in M$, $m \neq 0$. Then there is a submodule $\langle m \rangle \subset M$. But M is simple, and thus we must have $\langle m \rangle = M$, showing that M is cyclic.

Let M be an R-module. Suppose M is cyclic. Then $M = \langle m \rangle$ for some $m \in M$. Consider the function $\varphi : R \to M$ defined by $\varphi(r) = rm$. Clearly, this is a surjective R-module homomorphism, because every element of M is of the form rm for some $r \in R$. Then $M \cong R/\ker\varphi$ by the first isomorphism theorem, and $\ker\varphi$ is a submodule of R, and thus an ideal of R. On the other hand, suppose $M \cong R/I$ for some ideal I. Notice, that R/I is an R-module. If $1_R \in I$, then $I = R$ and thus $R/R = 0 = \langle 0 \rangle$. If $1_R \notin I$, then each element of R/I is of the form $r1_R + I$. There must be some $m \in M$ such that the isomorphic image is $1_R + I$, and it is easy to see that this m generates M.

Let M be a cyclic module and consider the quotient M/N by some submodule N of M. Then by the last part, $M \cong R/I$ for some ideal I of R. Since N can then be seen as an a submodule of R/I, there must be a submodule J of R such that $I \subseteq J$ and $N \cong I/J$, and by the third isomorphism theorem we have

$$\frac{M}{N} \cong \frac{R/I}{J/I} \cong \frac{R}{J}.$$

Since $M/N \cong R/J$ as R-modules, and J can then be seen as an ideal of the ring R, M/N is cyclic by the last part. □

6.17. ¬ Let M by a cyclic R-module, so that $M \cong R/I$ for a (left-)ideal I (Exercise 6.16), and let N be another R-module.

- Prove that $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, N) \cong \{n \in N \mid (\forall a \in I), an = 0\}$.
- For $a, b \in \mathbb{Z}$, prove that $\mathrm{Hom}_{\mathsf{Ab}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}) \cong \mathbb{Z}/\gcd(a, b)\mathbb{Z}$.

[7.7]

Solution. Let M be a cyclic R-module so that $M \cong R/I$ for an ideal I, N another R-module.

Consider the R-module homomorphism $\varphi : M \to N$. Denote $P = \{n \in N \mid (\forall a \in I), an = 0\}$. Notice, that since $M \cong R/I$, φ is uniquely determined by the image of m, or rather $1_R + I$ - for all $r \in R$ we have $\varphi(r + I) = \varphi(r1_R + I) = r\varphi(1_R + I)$. In particular, for $a \in I$, we must have $\varphi(a + I) = \varphi(I) = 0 = a\varphi(1_R + I)$. Then clearly we have a well-defined function $\sigma : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, N) \to P$ defined by $\sigma(\varphi) = \varphi(m)$. It is immediately seen that this function is a bijection - it is clearly injective, and it is surjective by the above consideration. P is a subgroup of N (seen as the underlying abelian group), because if $p, s \in P$, then $ap = 0$ and $as = 0$ for all $a \in I$, and thus $a(p - s) = ap - as = 0$ for all $a \in I$. Thus $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, N) \cong P$ as abelian groups.

Let $a, b \in \mathbb{Z}$. $\mathbb{Z}/a\mathbb{Z}$ and $\mathbb{Z}/b\mathbb{Z}$ are cyclic $\mathbb{Z}$-modules. Then by the above

$$\mathrm{Hom}_{\mathsf{Ab}}(\mathbb{Z}/a\mathbb{Z}, \mathbb{Z}/b\mathbb{Z}) \cong \{[z]_b \in \mathbb{Z}/b\mathbb{Z} \mid (\forall x \in a\mathbb{Z}), x[z]_b = [0]_b\}.$$

The group on the right hand side is in fact the subgroup of $\mathbb{Z}/b\mathbb{Z}$ which contains elements whose order must divide both b and a (since $a[z]_b = [0]_b$, thus order of $[z]_b$ must divide a). Indeed, since the order of such elements must divide both a and b, the order must in particular divide $\gcd(a, b)$. Thus we can identify the right hand side with the cyclic group $\mathbb{Z}/\gcd(a, b)\mathbb{Z}$ as required. □

6.18. ▷ Let M be an R-module, and let N be a submodule of M. Prove that if N and M/N are both finitely generated, then M is finitely generated.

Solution. Let M be an R-module, N a submodule of M and suppose N and M/N are finitely generated. Then $N = \langle n_1, \ldots, n_k \rangle$ and $M/N = \langle m_1 + N, \ldots, m_l + N \rangle$. Notice, that any $m \in M$ must belong to a single coset of N, say $(r_1 m_1 + \cdots + r_l m_l) + N$, $r_i \in R$. Thus $m = r_1 m_1 + \cdots + r_l m_l + n$ for some $n \in N$. But $n = s_1 n_1 + \cdots + s_k n_k$, $s_i \in R$. Thus

$$m = r_1 m_1 + \cdots + r_l m_l + s_1 n_1 + \cdots + s_k n_k.$$

But since any $m \in M$ can be written in this form, $M = \langle m_1, \ldots, m_l, n_1, \ldots, n_k \rangle$. □

7. Complexes and homology

7.1. ▷ Assume that the complex

$$\cdots \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow \cdots$$

is exact. Prove that $M \cong 0$. [§7.3]

Solution. The image of $0 \to M$ is 0, kernel of $M \to 0$ is M, and they must be equal by exactness at M, thus $M \cong 0$. □

7.2. Assume that the complex

$$\cdots \longrightarrow 0 \longrightarrow M \longrightarrow M' \longrightarrow 0 \longrightarrow \cdots$$

is exact. Prove that $M \cong M'$.

Solution. Let $\varphi : M \to M'$ be the homomorphism in the middle of the complex. By exactness at M, $\ker \varphi = 0$, by the exactness at M', $\operatorname{im} \varphi = M'$. Thus φ is an isomorphism, and $M \cong M'$. □

7.3. Assume that the complex

$$\cdots \longrightarrow 0 \longrightarrow L \longrightarrow M \xrightarrow{\varphi} M' \longrightarrow N \longrightarrow 0 \longrightarrow \cdots$$

is exact. Show that, up to natural identifications, $L = \ker \varphi$ and $N = \operatorname{coker} \varphi$.

Solution. By exactness, the homomorphism $L \to M$ is a monomorphism, and its image is $\ker \varphi$. Since it is a monomorphism, we can identify L with its image, a submodule of M, and thus $L = \ker \varphi$.

Similarly, $\operatorname{im} \varphi$ is equal to the kernel of the homomorphism $M' \to N$, and $M' \to N$ is an epimorphism, so that $N \cong M'/\operatorname{im} \varphi = \operatorname{coker} \varphi$. □

7.4. Construct short exact sequences of $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z} \longrightarrow 0$$

and

$$0 \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow 0.$$

(Hint: David Hilbert's Grand Hotel.)

Solution. For the first one, define $\alpha : \mathbb{Z}^{\oplus\mathbb{N}} \to \mathbb{Z}^{\oplus\mathbb{N}}$ by sending a function $f \in \mathbb{Z}^{\oplus\mathbb{N}}$ to a function $g : \mathbb{N} \to \mathbb{Z}$, $g(0) = 0$, $g(n) = f(n-1)$ for $n \geq 1$ (this is easily seen to be a $\mathbb{Z}$-module homomorphism). Define $\beta : \mathbb{Z}^{\oplus\mathbb{N}} \to \mathbb{Z}$ by sending a function $f \in \mathbb{Z}^{\oplus\mathbb{N}}$ to $f(0)$ (this is also trivially a homomorphism). Clearly, α is a monomorphism, and β is an epimorphism, with $\operatorname{im}\alpha = \ker\beta$.

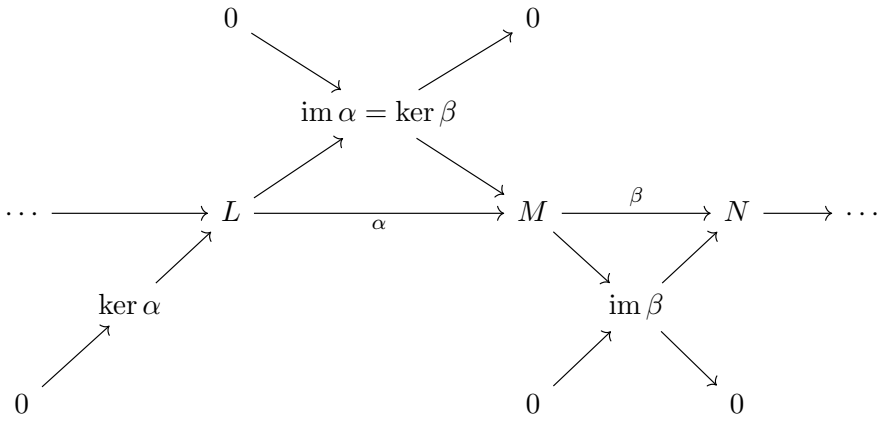
For the second one, define the homomorphism α by sending each function $f : \mathbb{N} \to \mathbb{Z}$ to a function $g : \mathbb{N} \to \mathbb{Z}$ such that $g(n) = 0$ for n odd, and $g(n) = f(\frac{n}{2})$ for n even. This is clearly an injective function, and thus a monomorphism. For the second homomorphism, β, send each $f : \mathbb{N} \to \mathbb{Z}$ to a function $g : \mathbb{N} \to \mathbb{Z}$ such that $g(n) = f(2n+1)$. This is an epimorphism, because if we have a function $g : \mathbb{N} \to \mathbb{Z}$ (defined for a finite number of natural numbers), we can easily define another function $f : \mathbb{N} \to \mathbb{Z}$ by setting $f(2n+1) = g(n)$ for each n. It is easy to see that $\beta(f) = 0$ for functions which are 0 at all odd 'indices', which is precisely the image of α. □

7.5. ▷ Assume that the complex

$$\cdots \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow \cdots$$

is exact and that L and N are Noetherian. Prove that M is Noetherian. [§7.1]

Solution. Using the 'trick' we have seen in §7.1, we can break up the exact complex into a number of short exact sequences:



Using this commutative diagram, we easily see that $\operatorname{im}\alpha = L/\ker\alpha$, and since L is Noetherian $\operatorname{im}\alpha$ must be Noetherian by Proposition 6.7. Thus $\operatorname{im}\alpha = \ker\beta$ is a Noetherian submodule of M. On the other hand, $\operatorname{im}\beta = M/\ker\beta$, and we can view $\operatorname{im}\beta$ as a submodule of N. N is Noetherian, thus $\operatorname{im}\beta$ must be Noetherian, and hence M is Noetherian (both results follow from Proposition 6.7). □

7.6. ▷ Prove the 'split epimorphism' part of Proposition 7.5. [§7.2]

Solution. Suppose the sequence

$$0 \longrightarrow \ker\varphi \longrightarrow M \xrightarrow{\varphi} N \longrightarrow 0$$

splits. Then φ may be identified with the projection $N' \oplus N \to N$, and the embedding function $N \to N' \to N$ then gives a right-inverse of φ. Conversely, assume that φ has a right-inverse ψ, such that $\varphi \circ \psi = \mathrm{id}_N$. Consider the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker\varphi & \xrightarrow{i} & M & \xrightarrow{\varphi} & N & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_{\ker\varphi}} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \mathrm{id}_N} & & \\
0 & \longrightarrow & \ker\varphi & \xrightarrow[i_{\ker\varphi}]{} & \ker\varphi \oplus N & \xrightarrow[\pi_N]{} & N & \longrightarrow & 0
\end{array}$$

where $\alpha : M \to \ker\varphi \oplus N$ is defined by $\alpha(m) = (m - \psi\circ\varphi(m), \varphi(m))$. α is well-defined, because $\varphi(m - \psi\circ\varphi(m)) = \varphi(m) - \varphi\circ\psi\circ\varphi(m) = \varphi(m) - \varphi(m) = 0$. The diagram commutes, because for $k \in \ker\varphi$, we have $\alpha(k) = (k, 0) = i_{\ker\varphi}(k)$, and for $m \in M$ we have $\pi_N \circ \alpha(m) = \varphi(m)$.

Define $\beta : \ker\oplus N \to M$ by $\beta(k, n) = k + \psi(n)$. We then have

$$\begin{aligned}
\alpha\circ\beta(k,n) &= \alpha(k + \psi(n)) \\
&= (k + \psi(n) - \psi\circ\varphi(k + \psi(n)), \varphi(k + \psi(n))) \\
&= (k + \psi(n) - \psi\circ\varphi(k) - \psi\circ\varphi\circ\psi(n), \varphi(k) + \varphi\circ\psi(n)) \\
&= (k + \psi(n) - \psi(0) - \psi(n), n) \\
&= (k, n)
\end{aligned}$$

and similarly

$$\begin{aligned}
\beta\circ\alpha(m) &= \beta(m - \psi\circ\varphi(m), \varphi(m)) \\
&= m - \psi\circ\varphi(m) + \psi\circ\varphi(m) \\
&= m.
\end{aligned}$$

Thus β is an inverse of α, therefore α is an isomorphism, and thus the sequence splits. □

7.7. ▷ Let

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

be a short exact sequence of R-modules, and let L be an R-module.

(i) Prove that there is an exact sequence

$$0 \longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(P, L) \longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(N, L) \longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, L).$$

(ii) Redo Exercise 6.17. (Use the exact sequence $0 \to I \to R \to R/I \to 0$.)

(iii) Construct an example showing that the rightmost homomorphism in (i) need not be onto.

(iv) Show that if the original sequence splits, then the rightmost homomorphism in (i) *is* onto.

[7.9, VIII.3.14, §VIII.5.1]

Solution. Since the given sequence is exact, we can identify M with a submodule of N and P with the quotient N/M.

For (i), define the homomorphism $\alpha : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(P, L) \to \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(N, L)$ by sending a homomorphism $f : P \to L$ to a homomorphism $g : N \to L$ defined by $g(n) = f(\pi(n))$ (where $\pi : N \to P$ is the quotient morphism). Notice that since π is surjective, $\ker \alpha = 0$ and thus the sequence is exact at $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(P, L)$. Define the second homomorphism $\beta : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(N, L) \to \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, L)$ by sending a homomorphism $f : N \to L$ to $f|_M$ (viewing M as a submodule of N and thus $M \subseteq N$). Let $g \in \operatorname{im} \alpha$, then there is $f \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(P, L)$ such that $g(n) = f(\pi(n))$ for all n, and thus for $m \in M$, $g(m) = f(\pi(m)) = 0$, hence $g \in \ker \beta$. Now let $g \in \ker \beta$. Then $\beta(g)(m) = g|_M(m) = 0$ for all $m \in M$. That means we can define a homomorphism $f : P \to L$ by $f(n + M) = g(n)$ (this is well-defined precisely because for $m \in M$, $f(m + M) = f(M) = g(m) = 0$ as needed). $\alpha(f)(n) = f(\pi(n)) = g(n)$ and thus $g \in \operatorname{im} \alpha$, showing that the sequence is exact at $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(N, L)$.

Now, consider the exact sequence $0 \to I \to R \to R/I \to 0$ and let N be an R-module. By (i) we then have an exact sequence

$$0 \longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R/I, N) \xrightarrow{\alpha} \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, N) \xrightarrow{\beta} \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(I, N).$$

Because the sequence is exact, we must have $\operatorname{im} \alpha = \ker \beta$. Since α is a monomorphism, $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R/I, N)$ is isomorphic to a subgroup (or a submodule if R is commutative) of $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, N)$, and thus $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R/I, N) \cong \ker \beta$. $\ker \beta$ are all homomorphisms $f \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, N)$ such that $f(i) = 0$ for all $i \in I$. Each homomorphism $R \to N$ is precisely defined by $n \in N$ such that $f(1_R) = n$. Combining these two facts we see that each morphism in $\ker \beta$ corresponds to $n \in N$ such that $f(i) = f(i1_R) = if(1_R) = in = 0$ for all $i \in I$. Thus $\ker \beta = \{n \in N \mid (\forall i \in I), in = 0\}$ as needed.

For (iii), we can construct an example showing β does not have to be onto by considering the above situation. Consider $R = \mathbb{Z}[x]$, $I = (2, x)$, $N = \mathbb{Z}[x]$. Clearly, every $\mathbb{Z}[x]$-module

homomorphism $\mathbb{Z}[x] \to \mathbb{Z}[x]$ is determined by the image of 1. The homomorphisms $(2, x) \to \mathbb{Z}[x]$ are determined by the images of the generators, 2 and x, which do not have to be equal. The homomorphism $\varphi : (2, x) \to \mathbb{Z}[x]$, $\varphi(2) = 2$, $\varphi(x) = x^2$, does not have a preimage under β - for every homomorphism $\sigma : \mathbb{Z}[x] \to \mathbb{Z}[x]$ we have $\sigma(2) = 2\sigma(1)$ and $\sigma(x) = x\sigma(1)$, and thus $\sigma|_{(2,x)}$ cannot be equal to φ for any σ.

Lastly, suppose the original sequence splits. Then $M \cong X$, $N \cong X \oplus Y$, and $P \cong Y$ for some R-modules X and Y. Then in particular, we can identify β with a homomorphism $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(X \oplus Y, L) \to \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(X, L)$. Given a homomorphism $\varphi : X \to L$, we can easily define a homomorphism $\sigma : X \oplus Y \to L$ with $\sigma(x, y) = \varphi(x)$, such that $\beta(\sigma) = \varphi$, thus β is surjective (formally, this gets quite messy with the various isomorphisms). □

7.8. ▷ Prove that every exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow F \longrightarrow 0$$

of R modules, with F *free*, splits. (Hint: Exercise 6.9.) [§VIII.5.4]

Solution. Label the homomorphism $N \to F$ by φ. We shall show that φ has a right-inverse. φ is onto, and thus for all homomorphisms $\alpha : F \to F$, there is an R-module homomorphism $\beta : F \to M$ such that $\alpha = \varphi \circ \beta$, by Exercise 6.9. In particular, consider $\alpha = \mathrm{id}_F$. Then we have a right-inverse of φ, and thus the sequence splits by Proposition 7.5. □

7.9. Let

$$0 \longrightarrow M \longrightarrow N \longrightarrow F \longrightarrow 0$$

be a short exact sequence of R-modules, with F free, and let L be an R-module. Prove that there is an exact sequence

$$0 \longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(F, L) \longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(N, L) \longrightarrow \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, L) \longrightarrow 0 \ .$$

(Cf. Exercise 7.7.)

Solution. The sequence splits by Exercise 7.8, and thus the existence of the given sequence follows from parts (i) and (iv) of Exercise 7.7. □

7.10. ▷ In the situation of the snake lemma, assume that λ and ν are isomorphisms. Use the snake lemma and prove that μ is an isomorphism. This is called the 'short five-lemma', as it follows immediately from the five-lemma (cf. Exercise 7.14), as well as from the snake lemma. [VIII.6.21, IX.2.4]

Solution. Suppose that λ and ν are isomorphisms. Then $\ker\lambda = \operatorname{coker}\lambda = 0$ and $\ker\nu = \operatorname{coker}\nu = 0$, and thus by the snake lemma we have an exact sequence

$$0 \longrightarrow \ker\mu \longrightarrow 0 \longrightarrow \operatorname{coker}\mu \longrightarrow 0 \ .$$

By Exercise 7.1 it follows that $\ker\mu = \operatorname{coker}\mu = 0$, and thus μ is an isomorphism. □

7.11. ▷ Let

$$(*) \qquad 0 \longrightarrow M_1 \longrightarrow N \longrightarrow M_2 \longrightarrow 0$$

be an exact sequence of R-modules. (This may be called an 'extension' of M_2 by M_1.) Suppose there is *any* R-module homomorphism $N \to M_1 \oplus M_2$ making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & N & \longrightarrow & M_2 & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_1 \oplus M_2 & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

commute, where the bottom sequence is the standard sequence of a direct sum. Prove that (*) splits. [§7.2]

Solution. It is enough to show that the homomorphism $N \to M_1 \oplus M_2$ is an isomorphism. But this follows from Exercise 7.10 - we have two exact sequences connected by isomorphisms $\lambda = \mathrm{id}_{M_1}$, $\nu = \mathrm{id}_{M_2}$ and a homomorphism $\mu : N \to M_1 \oplus M_2$. □

7.12. ¬ Practice your diagram chasing skills by proving the 'four-lemma': if

$$\begin{array}{ccccccc} A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & D_1 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\delta} \\ A_0 & \longrightarrow & B_0 & \longrightarrow & C_0 & \longrightarrow & D_0 \end{array}$$

is a commutative diagram of R-modules with exact rows, α is an epimorphism, and β, δ are monomorphisms, then γ is a monomorphism. [7.13, IX.2.3]

Solution. Let $c \in \ker\gamma$. Then $\gamma(c) = 0$, so that $\gamma(c) \mapsto 0 \in D_0$. By commutativity of the right square we see that $c \mapsto d \in D_1 \mapsto 0 \in D_0$, but δ is a monomorphism, and thus $d = 0$. Since the diagram is exact at C_1, there is some $b \in B_1$ such that $b \mapsto c$. By commutativity of the middle diagram, $\beta(b) \mapsto 0$, thus by exactness at B_0 there is some $a_0 \in A_0$ such that $a_0 \mapsto \beta(b)$. α is an epimorphism, hence there is some $a_1 \in A_1$ such that $\alpha(a_1) = a_0$. By commutativity of the left square, $a_1 \mapsto b' \mapsto \beta(b') = \beta(b)$. β is a monomorphism, and thus $b = b'$. Notice that b' is in the image of the left top homomorphism, thus $b' \mapsto 0 \in C_1$. But $b \mapsto c$, therefore $c = 0$, showing that $\ker\gamma = 0$ as required. □

7.13. Prove another version of the 'four-lemma' of Exercise 7.12: if

$$\begin{array}{ccccccc} B_1 & \longrightarrow & C_1 & \longrightarrow & D_1 & \longrightarrow & E_1 \\ \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\delta} & & \downarrow{\scriptstyle\epsilon} \\ B_0 & \longrightarrow & C_0 & \longrightarrow & D_0 & \longrightarrow & E_0 \end{array}$$

is a commutative diagram of R-modules with exact rows, β and δ are epimorphisms, and ϵ is a monomorphism, then γ is an epimorphism.

Solution. Let $c_0 \in C_0$. Then $c_0 \mapsto d_0 \in D_0 \mapsto 0 \in E_0$. δ is an epimorphism, and thus we have $d_1 \in D_1$ such that $\delta(d_1) = d_0$. $d_1 \mapsto e_1 \in E_1$, by commutativity we must have $\epsilon(e_1) = 0$. But ϵ is a monomorphism, thus $e_1 = 0$. Hence there must be some c_1 which maps to d_1 by exactness at D_1. By commutativity of the middle square we see that $c_0, \gamma(c_1) \mapsto 0$, hence $c_0 - \gamma(c_1)$ is in the kernel of the respective morphism, and we have some $b_0 \in B_0$ such that $b_0 \mapsto c_0 - \gamma(c_1)$ by exactness at C_0. β is an epimorphism, hence there is some b_1 such that $\beta(b_1) = b_0$. $b_1 \mapsto c_1' \in C_1$ and $\gamma(c_1') = c_0 - \gamma(c_1)$ by commutativity. But then $\gamma(c_1 + c_1') = c_0$ and thus γ is an epimorphism. □

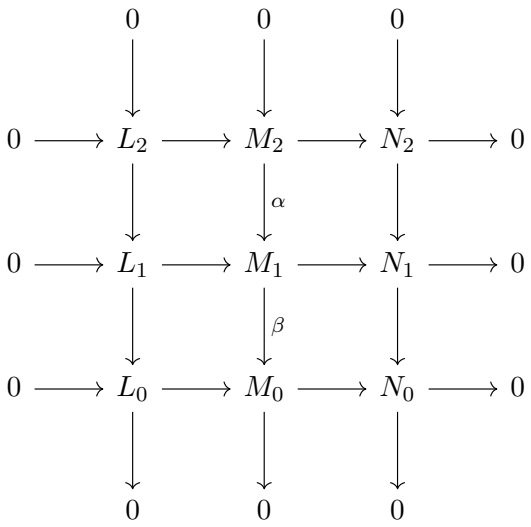
7.14. ¬ Prove the 'five-lemma': if

$$\begin{array}{ccccccccc} A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & D_1 & \longrightarrow & E_1 \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\gamma} & & \downarrow{\scriptstyle\delta} & & \downarrow{\scriptstyle\epsilon} \\ A_0 & \longrightarrow & B_0 & \longrightarrow & C_0 & \longrightarrow & D_0 & \longrightarrow & E_0 \end{array}$$

is a commutative diagram of R-modules with exact rows, β and δ are isomorphisms, α is an epimorphism, and ϵ is a monomorphism, then γ is an isomorphism. (You can avoid the needed diagram chase by pasting together results from the previous exercises.) [7.10]

Solution. First notice, that since β and δ are isomorphisms, they are in fact both monomorphisms and epimorphisms. Then by 7.12, wee see that γ is a monomorphism, and, by 7.13, that γ is an epimorphism. Because R-module monomorphisms are injective, and epimorphisms are surjective, γ is bijective and therefore an isomorphism. □

7.15. ¬ Consider the following commutative diagram of R-modules:



Assume that the three rows are exact and the two rightmost columns are exact. Prove that the left column is exact. Second version: assume that the three rows are exact and the two leftmost columns are exact; prove that the right column is exact. This is the 'nine-lemma'. (You can avoid a diagram chase by applying the snake lemma; for this, you will have to turn the diagram by 90°.) [7.16]

Solution. Assume that the two rightmost columns are exact. Label the homomorphisms between the columns as $\gamma : M_2 \to N_2$, $\mu : M_1 \to N_1$, and $\nu : M_0 \to N_0$. Since the rows are exact, we see that all three are epimorphisms. Applying the snake lemma on those two columns we thus get an exact sequence

$$0 \to \ker \lambda \to \ker \mu \to \ker \nu \to 0.$$

Notice that by exactness of the rows we have $\ker \lambda = L_2$, $\ker \mu = L_1$ and $\ker \nu = L_0$, showing that the leftmost column is in fact exact.

The second version is completely analogous. □

7.16. In the same situation as in Exercise 7.15, assume that the three rows are exact and that the leftmost and rightmost columns are exact.

- Prove that α is a monomorphism and β is an epimorphism.
- Is the central column necessarily exact?

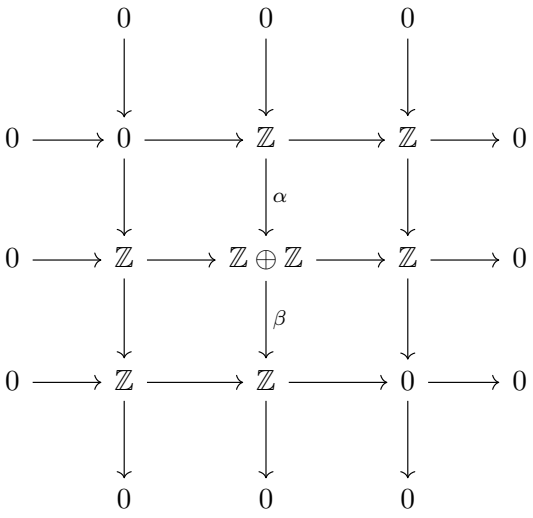
(Hint: No. Place $\mathbb{Z} \oplus \mathbb{Z}$ in the middle, and surround it artfully with six copies of $\mathbb{Z}$ and two 0's.)

- Assume further that the central column is a complex (that is, $\beta \circ \alpha = 0$); prove that it is then necessarily exact.

Solution. For the first point, start with $m_2 \in \ker \alpha$, i.e. $\alpha(m_2) = 0$. Then $\alpha(m_2) \mapsto 0 \in N_1$. We also have $m_2 \mapsto n_2 \in N_2$ and thus by commutativity of the upper right square $n_2 \mapsto 0 \in N_1$. By exactness of the rightmost column, the morphism $N_2 \to N_1$ is a monomorphism, and thus $n_2 = 0$. Then m_2 is in the kernel of the morphism $M_2 \to N_2$, and thus there is some $l_2 \in L_2$ such that $l_2 \mapsto m_2$ (by exactness of the row at M_2). We have $l_2 \mapsto l_1 \in L_1 \mapsto 0 \in M_1$ by commutativity of the upper left square, but the morphism $L_1 \to M_1$ is a monomorphism because the row is exact, and thus $l_1 = 0$. Since $L_2 \to L_1$ is also a monomorphism, this implies $l_2 = 0$. But then $0 \mapsto m_2$ which implies $m_2 = 0$. Thus $\ker \alpha = 0$ and hence α is a monomorphism.

Let $m_0 \in M_0$. $m_0 \mapsto n_0 \in N_0$. $N_1 \to N_0$ is an epimorphism, hence there is $n_1 \in N_1$ such that $n_1 \mapsto n_0$. $M_1 \to N_1$ is also an epimorphism, thus there is $m_1 \in M_1$ such that $m_1 \mapsto n_1$. By commutativity of the lower right square, $\beta(m_1) \mapsto n_0$. But then $m_0 - \beta(m_1) \mapsto 0 \in N_0$, thus there is some $l_0 \in L_0$ such that $l_0 \mapsto m_0 - \beta(m_1)$. $L_1 \to L_0$ is an epimorphism, hence we have some $l_1 \in L_1$ such that $l_1 \mapsto l_0$. $l_1 \mapsto m_1' \in M_1$, and by commutativity of the lower left square $\beta(m_1') = m_0 - \beta(m_1)$. But then $\beta(m_1 + m_1') = m_0$ and thus β is an epimorphism.

The central column is not necessarily exact. Consider the diagram

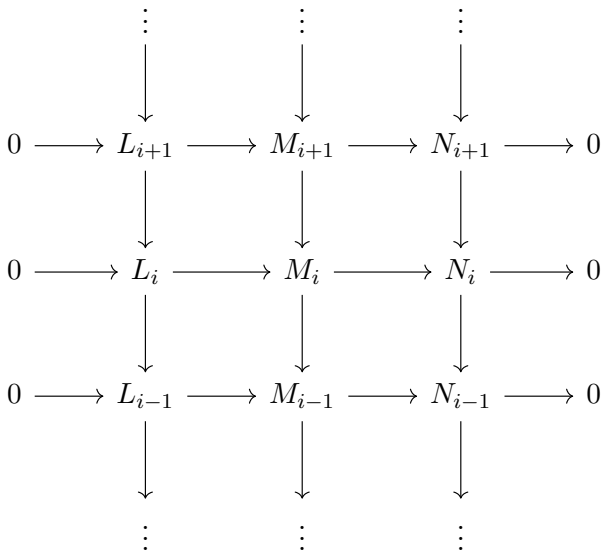


and assume that the rows, the leftmost, and the rightmost columns are exact. Let $a \in \operatorname{im} \alpha$, and suppose $a \in \ker \beta$. Then $\beta(a) = 0$. The two lower left morphisms $\mathbb{Z} \to \mathbb{Z}$ are isomorphisms by exactness, and thus a must necessarily be equal to 0. Then in fact α must map everything to 0, but that is a contradiction with the fact it is a monomorphism from $\mathbb{Z}$.

Lastly, assume that the middle column is a complex. Let $m_1 \in \ker \beta$. $m_1 \mapsto n_1 \in N_1$ and by commutativity $n_1 \mapsto 0 \in N_0$. But then there is some $n_2 \in N_2$ such that $n_2 \mapsto n_1$. $M_2 \to N_2$ is an epimorphism, hence there is some $m_2 \in M_2$ such that $m_2 \mapsto n_2$. Consider $\alpha(m_2)$. By commutativity $\alpha(m_2) \mapsto n_1$, hence $m_1 - \alpha(m_2) \mapsto 0 \in N_1$, thus there is some $l_1 \in L_1$ such that $l_1 \mapsto m_1 - \alpha(m_2)$. $l_1 \mapsto l_0 \in L_0$ and by commutativity $l_0 \mapsto 0 \in M_0$.

Since $L_0 \to M_0$ is a monomorphism, $l_0 = 0$, hence there is some $l_2 \in L_2$ such that $l_2 \mapsto l_1$. $l_2 \mapsto m_2' \in M_2$ and by commutativity $\alpha(m_2') = m_1 - \alpha(m_2)$, hence $\alpha(m_2 + m_2') = m_1$, thus $m_1 \in \operatorname{im}\alpha$, and therefore the middle column is exact. □

7.17. ¬ Generalize the previous two exercises as follows. Consider a (possibly infinite) commutative diagram of R-modules:



in which the central column is a complex and every row is exact. Prove that the left and right columns are also complexes. Prove that if any two of the columns are exact, so is the third. (The first part is straightforward. The second part will take you a couple of minutes now due to the needed diagram chases, and a couple of seconds later, once you learn about the long exact (co)homology sequence in §IX.3.3.) [IX.3.12]

Solution. Suppose $l_i \in \operatorname{im} L_{i+1} \to L_i$. Then there is $l_{i+1} \in L_{i+1}$ such that $l_{i+1} \mapsto l_i$. We also have some $m_i \in M_i$ such that $l_i \mapsto m_i$. $l_{i+1} \mapsto m_{i+1} \in M_{i+1}$, and by commutativity $m_{i+1} \mapsto m_i$. $m_i \in \operatorname{im} M_{i+1} \to M_i$, thus $m_i \mapsto 0 \in M_{i-1}$. We also have $l_i \mapsto l_{i-1} \in L_{i-1}$, and by commutativity $l_{i-1} \mapsto 0$, but $L_{i-1} \to M_{i-1}$ is a monomorphism, and thus $l_{i-1} = 0$, hence $l_i \in \ker L_i \to L_{i-1}$. Thus the leftmost column is a complex.

Similarly, suppose $n_i \in \operatorname{im} N_{i+1} \to N_i$. Then we have some $n_{i+1} \in N_{i+1}$, $n_{i+1} \mapsto n_i$. Since $M_{i+1} \to N_{i+1}$ is an epimorphism, there is some $m_{i+1} \in M_{i+1}$ such that $m_{i+1} \mapsto n_{i+1}$. $m_{i+1} \mapsto m_i \in M_i \mapsto 0 \in M_{i-1} \mapsto 0 \in N_{i-1}$ (because the middle column is a complex). By commutativity of the upper right square, $m_i \mapsto n_i$, and by the commutativity of the lower right square, $n_i \mapsto 0 \in N_{i-1}$, thus $n_i \in \ker N_i \to N_{i-1}$. Therefore the rightmost column is a complex.

For the second part, lets suppose the two left columns are exact. Let $n_i \in \ker N_i \to N_{i-1}$. Then $n_i \mapsto 0 \in N_{i-1}$. $M_i \to N_i$ is an epimorphism, thus there is some $m_i \in M_i$ such that

$m_i \mapsto n_i$. $m_i \mapsto m_{i-1}$ and by commutativity $m_{i-1} \mapsto 0 \in N_{i-1}$. Because the bottom row is exact, there is some $l_{i-1} \in L_{i-1}$ such that $l_{i-1} \mapsto m_{i-1}$. Now, $l_{i-1} \mapsto l_{i-2} \in L_{i-2}$, and $l_{i-2} \mapsto m_{i-2} \in M_{i-2}$. We have $m_{i-1} \mapsto 0 \in M_{i-2}$ (because m_{i-1} is an image of m_i), and thus by commutativity $m_{i-2} = 0$. Since $L_{i-2} \to M_{i-2}$ is a monomorphism, it follows that $l_{i-2} = 0$, hence $l_{i-1} \in \ker L_{i-1} \to L_{i-2}$ and thus there is some $l_i \in L_i$ such that $l_i \mapsto l_{i-1}$. Now, $l_i \mapsto m'_i \in M_i$ and by commutativity $m'_i \mapsto m_{i-1}$. Hence $m_i - m'_i \mapsto 0$, thus $m_i - m'_i \in \ker M_i \to M_{i-1}$, and there is some $m_{i+1} \in M_{i+1}$ such that $m_{i+1} \mapsto m_i - m'_i$. $m_{i+1} \mapsto n_{i+1} \in N_{i+1}$. By commutativity, n_{i+1} maps to the same element of N_i as $m_i - m'_i$. But notice that m'_i maps to 0, because it is an image of l_i and the row is exact, thus $n_{i+1} \mapsto n_i$. Hence $n_i \in \operatorname{im} N_{i+1} \to N_i$. Thus the column is exact.

The other variations are all very similar. □