Contents

Last update: 2024 August 30

1 Introduction

1.1 Categories and Functors

Definition 1.1.1. A *class* is a collection of sets (or sometimes other mathematical objects) that can be unambiguously defined by a property that all its members share.

Definition 1.1.2. A *category* $\mathcal{C}$ consists of three ingredients: a class $\mathrm{obj}(\mathcal{C})$ of *objects*, a set of *morphisms* $\mathrm{Hom}\,(A, B)$ for every ordered pair (A, B) of objects, and *composition* $\mathrm{Hom}\,(A, B) \times \mathrm{Hom}\,(B, C) \to \mathrm{Hom}\,(A, C)$, denoted by

$$(f, g) \mapsto gf,$$

for every ordered tripled A, B, C of objects. These ingredients are subject to the following axioms:

(1) The Hom sets are pairwise disjoint; i.e., each $f \in \mathrm{Hom}\,(A, B)$ has a unique *domain* A and a unique *target* B;

(2) for each object A, there is an *identity morphism* $1_A \in \mathrm{Hom}\,(A, A)$ such that $f1_A = f$ and $1_B f = f$ for all $f : A \to B$;

(3) composition is associative: given morphisms $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, then

$$h(gf) = (hg)f.$$

Example 1.1.1.

(1) **Sets**. The objects in this category are sets, morphisms are functions, and composition is the usual composition of functions. It is an axiom of set theory that if A and B are sets, then the class $\mathrm{Hom}\,(A, B)$ of all functions from A to B is also a set.

(2) **Groups**. Objects are groups, morphisms, are homomorphisms, and composition is the usual composition (as homomorphisms are functions). Part of the verification that **Groups** is a category involves checking that identity functions are homomorphisms and that the composite of two homomorphisms is itself a homomorphism (one needs to know that if $f \in \mathrm{Hom}\,(A, B)$ and $g \in \mathrm{Hom}\,(B, C)$, then $gf \in \mathrm{Hom}\,(A, C)$).

(3) A partially ordered set X can be regarded as the category whose objects are the elements of X, whose Hom sets are either empty or have only one element:

$$\mathrm{Hom}\,(x, y) = \begin{cases} \emptyset & \text{if } x \npreceq y, \\ \{\iota_y^x\} & \text{if } x \preceq y \end{cases}$$

(the symbol ι_y^x is the unique element in the Hom set when $x \preceq y$), and whose composition is given by $\iota_z^y \iota_y^x = \iota_z^x$. Note that $1_x = \iota_x^x$, by reflexivity, while composition makes sense because $\preceq$ is transitive. We insisted in the definition of a category that each $\mathrm{Hom}\,(A, B)$ be a set, but we did not say it was nonempty. This is an example in which this possibility occurs.

(4) **Top**. Objects are topological spaces, morphisms are continous functions, and composition is the usual composition of functions. In checking that **Top** is a category, one must note that identity functions are continuous and that composites of continuous functions are continuous.

(5) The category $\mathbf{Sets}_*$ of all *pointed sets* has as its objects all ordered pairs (X, x_0), where X is a nonempty set and x_0 is a point in X, called the *basepoint*. A morphism $f : (X, x_0) \to (Y, y_0)$ is called a *pointed map*; it is a function $f : X \to Y$ with $f(x_0) = y_0$. Composition is the usual composition of functions. One defines the category $\mathbf{Top}_*$ of all *pointed spaces* in a similar way; $\mathrm{obj}\,(\mathbf{Top}_\star)$ consists of all ordered pairs (X, x_0), where X is a nonempty topological space and $x_0 \in X$, and morphisms $f : (X, x_0) \to (Y, y_0)$ are continuous functions $f : X \to Y$ with $f(x_0) = y_0$.

(6) **Ab**. Objects are abelian groups, morphisms are homomorphisms, and composition is the usual composition.

(7) **Rings**. Objects are rings, morphisms are ring homomorphisms, and composition is the usual composition. We assume that all rings R have a unit element 1, but we do not assume that $1 \neq 0$. We agree, as part of the definition, that $\varphi(1) = 1$ for every ring homomorphism φ. Since the inclusion map $S \to R$ of a subring should be a homomorphism, it follows that the unit element 1 in a subring S must be the same as the unit element 1 in R.

(8) **ComRings**. Objects are commutative rings, morphisms are ring homomorphisms, and composition is theusual composition.

(9) The category ${}_R\mathbf{Mod}$ of all *left R-modules* (where R is a ring) has as its objects all left R-modules, its morphisms as all R-module homomorphisms, and as its composition the usual composition of functions. We denote the sets $\mathrm{Hom}\,(A, B)$ in ${}_R\mathbf{Mod}$ by $\mathrm{Hom}_R\,(A, B)$. If $R = \mathbf{Z}$, then ${}_\mathbf{Z}\mathbf{Mod} = \mathbf{Ab}$, for abelian groups are $\mathbf{Z}$-modules and homomorphisms are $\mathbf{Z}$-maps. There is also a category of right R-modules denoted $\mathbf{Mod}_R$.

Definition 1.1.3. A category $\mathcal{S}$ is a *subcategory* of a category $\mathcal{C}$ if

(1) $\mathrm{obj}\,(\mathcal{S}) \subseteq \mathrm{obj}\,(\mathcal{C})$;

(2) $\mathrm{Hom}_\mathcal{S}\,(A, B) \subseteq \mathrm{Hom}_\mathcal{C}\,(A, B)$ for all $A, B \in \mathrm{obj}\,(\mathcal{S})$, where we denote Hom sets in $\mathcal{S}$ by $\mathrm{Hom}_\mathcal{S}\,(\square, \square)$;

(3) if $f \in \mathrm{Hom}_\mathcal{S}\,(A, B)$ and $g \in \mathrm{Hom}_\mathcal{S}\,(B, C)$, then the composite $gf \in \mathrm{Hom}_\mathcal{S}\,(A, C)$ is equal to the composite $gf \in \mathrm{Hom}_\mathcal{C}\,(A, C)$;

(4) if $A \in \mathrm{obj}\,(\mathcal{S})$, then the identity $1_A \in \mathrm{Hom}_\mathcal{S}\,(A, A)$ is equal to the identity $1_A \in \mathrm{Hom}_\mathcal{C}\,(A, A)$.

A subcategory $\mathcal{S}$ of $\mathcal{C}$ is a *full subcategory* if, for all $A, B \in \mathrm{obj}\,(\mathcal{S})$, we have $\mathrm{Hom}_\mathcal{S}\,(A, B) = \mathrm{Hom}_\mathcal{C}\,(A, B)$.

Example 1.1.2.

1. **Ab** is a full subcategory of **Groups**.

2. A category is *discrete* if its only morphisms are identity morphisms. If $\mathcal{S}$ is the discrete category with $\text{obj}(\mathcal{S}) = \text{obj}(\textbf{Sets})$, then $\mathcal{S}$ is a subcategory of **Sets** that is not a full subcategory.

Definition 1.1.4. Let $\mathcal{C}$ be any category and $\mathcal{S} \subseteq \text{obj}(\mathcal{C})$. The *full subcategory generated by $\mathcal{S}$*, also denoted by $\mathcal{S}$, is the subcategory with $\text{obj}(\mathcal{S}) = \mathcal{S}$ and with $\text{Hom}_{\mathcal{S}}(A, B) = \text{Hom}_{\mathcal{C}}(A, B)$ for all $A, B \in \text{obj}(\mathcal{S})$.

Definition 1.1.5. Let $\mathcal{C}$ and $\mathcal{D}$ be categories.

(1) A *covariant functor* $T : \mathcal{C} \to \mathcal{D}$ is a function satisfying:

(i) if $A \in \text{obj}(\mathcal{C})$, then $T(A) \in \text{obj}(\mathcal{D})$,

(ii) if $f : A \to A'$ in $\mathcal{C}$, then $T(f) : T(A) \to T(A')$ in $\mathcal{D}$,

(iii) if $A \xrightarrow{f} A' \xrightarrow{g} A''$ in $\mathcal{C}$, then $T(A) \xrightarrow{T(f)} T(A') \xrightarrow{T(g)} T(A'')$ in $\mathcal{D}$ and

$$T(gf) = T(g)T(f),$$

(iv) $T(1_A) = 1_{T(A)}$ for every $A \in \text{obj}(\mathcal{C})$.

(2) A *contravariant functor* is a function $T : \mathcal{C} \to \mathcal{D}$ satisfying:

(i) If $B \in \text{obj}(\mathcal{C})$, then $T(B) \in \text{obj}(\mathcal{D})$,

(ii) if $f : B \to B'$ in $\mathcal{C}$, then $T(f) : T(B') \to T(B)$ in $\mathcal{D}$ (Note the reversal of arrows),

(iii) if $B \xrightarrow{f} B' \xrightarrow{g} B''$ in $\mathcal{C}$, then $T(B'') \xrightarrow{T(g)} T(B') \xrightarrow{T(f)} T(B)$ in $\mathcal{D}$ and

$$T(gf) = T(f)T(g),$$

(iv) $T(1_A) = 1_{T(A)}$ for every $A \in \text{obj}(\mathcal{C})$.

Example 1.1.3.

(1) Let $\mathcal{C}$ be a (locally small) category and $A \in \text{obj}(\mathcal{C})$. The Hom *functor* is a function

$$\text{Hom}(A, \Box) : \mathcal{C} \to \textbf{Sets}.$$

If $f : B \to B'$ is in $\mathcal{C}$, then $\text{Hom}(A, f) : \text{Hom}(A, B) \to \text{Hom}(A, B')$ is defined by $h \mapsto hf$ for each $h \in \text{Hom}(A, B)$.

(2) Let $\mathcal{C}$ be a (locally small) category and $B \in \text{obj}(\mathcal{C})$. The Hom *(contravariant) functor* is a function

$$\text{Hom}(\Box, B) : \mathcal{C} \to \textbf{Sets}.$$

If $f : A \to A'$ is in $\mathcal{C}$, then $\text{Hom}(f, B) : \text{Hom}(A', B) \to \text{Hom}(A, B)$ is defined by $h \mapsto hf$ for each $h \in \text{Hom}(A, B)$.

Example 1.1.4. Recall that a *linear functional* on a vector space V over k is a linear transformation $\varphi : V \to k$ (note that k is a one-dimensional vector space over itself). For example, let $V = C([0,1])$, then integration $f \mapsto \int_0^1 f(t)dt$ is a linear functional on V. If V is a vector space over a field k, then its *dual space* is $V^* = \mathrm{Hom}_k(V,k)$, the set of all linear functionals on V. Note that functions in V^* are closed under pointwise addition —V^* is a vector space over k if we define $af : V \to k$ by $af : v \mapsto a[f(v)]$ for all $f \in V^*$ and $a \in k$. Moreover, if $f : V \to W$ is a linear transformation, then the induced map $f^* : W* \to V*$ is also a linear transformation. The *dual space functor* is $\mathrm{Hom}_k(\square, k) : {}_k\mathbf{Mod} \to {}_k\mathbf{Mod}$.

Definition 1.1.6. If $\mathcal{C}$ is a category, define its *opposite category* $\mathcal{C}^{\mathrm{op}}$ to be the category with $\mathrm{obj}(\mathcal{C}^{\mathrm{op}}) = \mathrm{obj}(\mathcal{C})$, with morphisms $\mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A,B) = \mathrm{Hom}_{\mathcal{C}}(B,A)$ and with composition $g^{\mathrm{op}}f^{\mathrm{op}} = (fg)^{\mathrm{op}}$, where $f^{\mathrm{op}}, g^{\mathrm{op}} \in \mathrm{Hom}_{\mathcal{C}^{\mathrm{op}}}(A,B)$ (note that the composition is the reverse of that in $\mathcal{C}$).

Definition 1.1.7. A morphism $f : A \to B$ in a category $\mathcal{C}$ is an *isomorphism* if there exists a morphism $g : B \to A$ in $\mathcal{C}$ with

$$gf = 1_A \text{ and } fg = 1_B.$$

The morphism g is called the *inverse* of f.

Proposition 1.1.8. *Let $T : \mathcal{C} \to \mathcal{D}$ be a functor of either variance. If f is an isomorphism in $\mathcal{C}$, then $T(f)$ is an isomorphism in $\mathcal{D}$.*

Proof. If g is the inverse of f, apply the functor T to the equations $gf = 1$ and $fg = 1$. □

Definition 1.1.9. Let $S, T : \mathcal{A} \to \mathcal{B}$ be covariant functors. A *natural transformation* $\tau : S \to T$ is a one-parameter family of morphisms in $\mathcal{B}$,

$$\tau = (\tau_A : SA \to TA)_{A \in \mathrm{obj}(\mathcal{A})},$$

making the following diagram commute for all $f : A \to A'$ in $\mathcal{A}$:

$$\begin{tikzcd} SA \arrow[r, "\tau_A"] \arrow[d, "Sf"'] & TA \arrow[d, "Tf"] \\ SA' \arrow[r, "\tau_{A'}"'] & TA'. \end{tikzcd}$$

Definition 1.1.10. Let $X, Y \in \mathrm{obj}(\mathbf{Sets})$ and $f, g \in \mathrm{Hom}(X,Y)$ The *equaliser of f and g* is the set of elements $x \in X$ such that $f(x)$ is equal to $g(x)$ in Y. Symbolically:

$$\mathrm{Eq}(f,g) = \{x \in X \mid f(x) = g(x)\}.$$

Definition 1.1.11. Let $\mathcal{C}$ be a category with a zero morphism. If $f : X \to Y$ is an arbitrary morphism in $\mathcal{C}$, then a *kernel* of f is an equaliser of f and the zero morphism from X to Y; i.e., $\ker f = \mathrm{Eq}(f, 0_{XY}) = \{x \in X \mid f(x) = 0_Y\}$.

1.2 Universal Properties

Definition 1.2.1. Include the categorical definition of universal properties here.

Example 1.2.1.

(1) Let G be a group and N a normal subgroup of G. If K is any group and $\varphi : G \to K$ is a homomorphism which annihilates N (that is, $N \subseteq \ker \varphi$), then there is a unique homomorphism $\Phi : G/N \to K$ such that $\Phi \circ \pi = \varphi$, where π is the natural projection map $\pi : G \to G/N$. The following diagram commutes:

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & G/N \arrow[d, "\Phi"] \\ & K \end{tikzcd}$$

(2) Let H be a subgroup of G. If G is any group and $\varphi : K \to G$ is a homomorphism whose image is contained in H (that is, $\operatorname{im} \varphi \subseteq H$), then there is a homomorphism $\Phi : K \to H$ such that $\iota \circ \Phi = \varphi$, where ι is the inclusion map $\iota : H \to G$. The following diagram commutes:

$$\begin{tikzcd} K \arrow[r, "\Phi"] \arrow[dr, "\varphi"'] & H \arrow[d, "\iota"] \\ & G \end{tikzcd}$$

(3) Let $\mathcal{C}$ be a category with a zero morphism. If $f : X \to Y$ is an arbitrary morphism in $\mathcal{C}$ then Definition 1.1.11 gives rise to the following universal property: a kernel of f is an object K together with a morphism $k : K \to X$ such that,

  (1) $f \circ k$ is the zero morphism from K to Y,

  (2) Given any morphism $k' : K' \to X$ such that $f \circ k'$ is the zero morphism, there is a unique morphism $u : K' \to K$ such that $k \circ u = k'$,

which make the following diagrams commute:

(1)
$$\begin{tikzcd} K \arrow[r, "k"] \arrow[dr, "0_{KY}"'] & X \arrow[d, "f"] \\ & Y \end{tikzcd}$$

(2)
$$\begin{tikzcd} & X \arrow[dr, "f"] & \\ & K \arrow[u, "k"] \arrow[r, "0_{KY}"] & Y \\ K' \arrow[uur, "k'"] \arrow[ur, dotted, "u"] \arrow[urr, "0_{K'Y}"'] & & \end{tikzcd}$$

Exercises

Exercise 1.1. Use parts (1) and (2) of Example 1.2.1 to show that if $\varphi : G \to H$ is a group homomorphism, then $G/\ker\varphi \cong \operatorname{im}\varphi$.

Proof. Since $\operatorname{im}\varphi$ is a subgroup of H, the universal property of subgroups gives the correspondence $\varphi = \iota \circ \Phi$, where $\Phi : G \to \operatorname{im}\varphi$ and $\iota : \operatorname{im}\varphi \to H$. Now, since $\ker\Phi$ is a normal subgroup of G, the unversal property of quotient groups gives the correspondence $\Phi = \alpha \circ \pi$, where $\pi : G \to G/\ker\Phi$ and $\alpha : G/\ker\Phi \to \operatorname{im}\varphi$. The following diagram commutes.

$$\begin{tikzcd}
 & G/\ker\Phi \arrow[d, "\alpha"] \\
G \arrow[ur, "\pi"] \arrow[r, "\Phi"] \arrow[dr, "\varphi"'] & \operatorname{im}\varphi \arrow[d, "\iota"] \\
 & H
\end{tikzcd}$$

Claim: $\ker\Phi = \ker\varphi$. If $k \in \ker\Phi$, then $\Phi(k) = 0_{\operatorname{im}\varphi} = 0_H$, hence $k \in \ker\varphi$. Conversely, if $k \in \ker\varphi$, then k must get mapped to something inside the image of φ; i.e., $\varphi(k) = 0_H = 0_{\operatorname{im}\varphi}$ implies $k \in \ker\Phi$.

Claim: α is an isomorphism. Note that Φ is clearly surjective, hence it must be the case that α is surjective. It remains to show that α is injective: this can be done by showing the map $\alpha : \mathrm{G}/\ker\varphi \to \operatorname{im}\varphi$ has a trivial kernel. Let $g \in G$ be any element, note that $\alpha(g\ker\varphi) = \varphi(g)$ by our definition. Hence when $g \in \ker\varphi$, $\alpha(g\ker\varphi) = \alpha(\ker\varphi) = 0_{\operatorname{im}\varphi}$ (the only element of $G/\ker\varphi$ which maps to $0_{\operatorname{im}\varphi}$ is the identity). This establishes the proof that $G/\ker\varphi \cong \operatorname{im}\varphi$[1]. □

Exercise 1.2.

(i) Prove, in every category $\mathcal{C}$, that each object $A \in \mathcal{C}$ has a unique identity morphism.

(ii) If f is an isomorphism in this category, prove that its inverse is unique.

Proof. Let $f : A \to B$. Suppose $1_A, 1'_A \in \operatorname{Hom}(A, A)$ such that $f1_A = f$ and $f1'_A = f$. Take $B = A$ and $f = 1'_A$, then $1'_A 1_A = 1'_A$. Now consider $g : B \to A$. Then $1'_A g = g$. Take $B = A$ and $g = 1_A$, then $1'_A 1_A = 1_A$. Together, this gives $1'_A = 1'_A 1_A = 1_A$. Hence the identity morphism is unique.

Let $f : A \to B$ be an isomorphism. Suppose $g, g' : B \to A$ are inverses of f. Then $g = 1_A g = (g'f)g = g'(fg) = g'1_B = g'$. Hence inverses are unique. □

Exercise 1.3. If $T : \mathcal{A} \to \mathcal{B}$ is a functor, define $T^{\mathrm{op}} : \mathcal{A}^{\mathrm{op}} \to \mathcal{B}$ by $T^{\mathrm{op}}(A) = T(A)$ for all $A \in \operatorname{obj}(\mathcal{A})$ and $T^{\mathrm{op}}(f^{\mathrm{op}}) = T(f)$ for all morphisms f in $\mathcal{A}$. Prove that T^{op} is a functor having variance opposite to the variance of T.

[1] We can write $\varphi = \iota \circ \alpha \circ \pi$. In other words, *every* momorphism takes the form of a quotient map, followed by an isomorphism, followed by an inclusion.

Exercise 1.4.

(i) If X is a set, define FX to be the free group having basis X, that is, the elements of FX are reduced words on the alphabet X and multiplication is juxtaposition followed by cancellation. If $\varphi : X \to Y$ is a function, prove that there is a unique homomorphism $F\varphi : FX \to FY$ such that $(F\varphi) \mid X = \varphi$.

(ii) Prove that F : **Sets** $\to$ **Groups** is a functor (F is called the *free functor*).

Exercise 1.5.

(i) Define $\mathcal{C}$ to have objects all ordered pairs (G, H), where G is a group and H is a normal subgroup of G, and to have morphisms $\varphi_* : (G, H) \to (G_1, H_1)$, where $\varphi : G \to G_1$ is a homomorphism with $\varphi(H) \subseteq H_1$. Prove that $\mathcal{C}$ is a category if composition in $\mathcal{C}$ is defined to be ordinary composition.

(ii) Construct a functor $Q : \mathcal{C} \to$ **Groups** with $Q(G, H) = G/H$.

(iii) Prove that there is a functor **Groups** $\to$ **Ab** taking each group G to G/G', where G' is its commutator subgroup.

Exercise 1.6. Let R be a ring. An (additive) abelian group M is an *almost left R-module* if there is a function $R \times M \to M$ which satisfies all of the left R-module axioms except for Axiom (4): we do not assume that $1m = m$ for all $m \in M$. Prove that if M is an almost left R-module then $M = M_1 \oplus M_0$, where $M_1 = \{m \in M : 1m = 1\}$ and $M_0 = \{m \in M : rm = 0 \text{ for all } r \in R\}$ are subgroups of M that are almost left R-modules (in fact, M_1 is a left R-module).

Proof. □

Exercise 1.7. Prove that every right R-module is a left R^{op}-module and vice versa.

Exercise 1.8. Let M be a left R-module.

(i) Prove that $\operatorname{Hom}_R(M, M)$ is a ring with 1 under pointwise addition and composition as multiplication.

(ii) The ring $\operatorname{Hom}_R(M, M)$ is called the *endomorphism ring of M* and is denoted $\operatorname{End}_R(M)$. Elements of $\operatorname{End}_R(M)$ are called *endomorphisms*. Prove that M is a left $\operatorname{End}_R(M)$-module.

(iii) If a ring R is regarded as a left R-module, prove that $\operatorname{End}_R(R) \cong R^{\text{op}}$ as rings.

Proof. The details of $\operatorname{Hom}_R(M, M)$ being an abelian group are left out —associativity and commutativity are shown easily, the identity is the zero map 0_{MM} and inverses follow from this. Let $\varphi, \psi, \gamma \in \operatorname{Hom}_R(M, M)$. Note that function composition is automatically associative. "1" in this case is the identity morphism: $(\varphi \circ \text{id}_M)(m) = \varphi(\text{id}_M(m)) = \varphi(m)$ and $(\text{id}_M \circ \varphi)(m) = \text{id}_M(\varphi(m)) = \varphi(m)$. Function composition distributes over pointwise addition as follows:

$$\begin{aligned}(\varphi \circ (\psi + \gamma))(m) &= \varphi((\psi + \gamma)(m)) \\ &= \varphi(\psi(m) + \gamma(m)) \\ &= \varphi(\psi(m)) + \varphi(\psi(m)) \\ &= (\varphi \circ \psi)(m) + (\varphi \circ \gamma)(m) \\ &= ((\varphi \circ \psi) + (\varphi \circ \gamma))(m).\end{aligned}$$

Distribution from the right follows similary, hence $\mathrm{Hom}_R(M, M)$ is a unital ring.

$\square$

2

Module Theory

2.1 Basic Definitions and Examples

Definition 2.1.1. Let R be a ring (not necessarily commutative nor with 1). A *left R-module* or a *left module over R* is a set M together with:

(1) a binary operation $+$ on M under which M is an abelian group, and

(2) an action of R on M (that is, a map $R \times M \to M$) denoted by rm for all $r \in R$ and for all $m \in M$ which satisfies:

   (a) $(r+s)m = rm + rs$, for all $r, s \in R$, $m \in M$

   (b) $(rs)m = r(sm)$, for all $r, s \in R$, $m \in M$

   (c) $r(m+n) = rm + rn$, for all $r \in R$, $m, n \in M$.

   If the ring R has a 1 we impose the additional axiom:

   (d) $1m = m$, for all $m \in M$.

Note 2.1.1. Modules over a field F and vector spaces over F are the same.

Definition 2.1.2. Let R be a ring and let M be an R-module. An *R-submodule of M* is a subgroup N of M which is closed under the action of ring elements; i.e., $rn \in N$ for all $r \in R$, $n \in N$.

Example 2.1.1.

(1) Let R be any ring. Then $M = R$ is a left R-module. The ring action is just normal multiplication in the ring R. When R is a left module over itself, the submodules of R are the left ideals of R. IF R is not commutative its left and right module structure over itself might be different

(2) Let $R = F$ be a field. Note that every vector space over F is an F-module and vice versa. Define

$$F^n = \{(a_1, a_2, ..., a_n) \mid a_i \in F, n \in \mathbf{Z}^+\}$$

as *affine n-space over F*. We can make F^n into a vector space by defining addition and scalar multiplication componentwise. When $F = \mathbf{R}$ we have the familiar Euclidean n-space.

(3) If M is an R-module and S is a subring of R with $1_R = 1_S$, then M is an S-module as well. For example, the field $\mathbf{R}$ is an $\mathbf{R}$-module, a $\mathbf{Q}$-module, and a $\mathbf{Z}$-module.

Example 2.1.2 (Z-Modules)**.** Let $R = \mathbf{Z}$, let A be any abelian group and write the operation of A as $+$. Make A into a $\mathbf{Z}$-module as follows: for any $n \in \mathbf{Z}$ and $a \in A$ define

$$na = \begin{cases} a + a + \ldots + a \quad (n \text{ times}) & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ -a - a - \ldots - a \quad (n \text{ times}) & \text{if } n < 0 \end{cases},$$

where 0 is the identity of the additive abelian group A. This definition of $\mathbf{Z}$ acting on A makes A into a $\mathbf{Z}$-module, and furthermore the module axioms show that this is the only action of $\mathbf{Z}$ on A. Thus every abelian group is a $\mathbf{Z}$-module and vice versa. Furthermore $\mathbf{Z}$-submodules are the same as subgroups.

Proposition 2.1.3 (The Submodule Criterion)**.** *Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if $N \neq \emptyset$ and $x + ry \in N$ for all $r \in R$ and $x, y \in N$.*

Proof. If N is a submodule, then $0 \in N$ so $N \neq \emptyset$. Also N is closed under addition and is sent to itself under the action of elements in R[1].

Conversely, suppose $N \neq \emptyset$ and $x + ry \in N$ for all $r \in R$ and $x, y \in N$. Let $r = -1$, then $x - y \in N$; i.e., N is a subgroup of M. This also gives that $0 \in N$. Let $x = 0$, then $ry \in N$; i.e., N is sent to itself under the action of R. This establishes the proposition. □

Definition 2.1.4. Let R be a commutative ring with identity. An *R-algebra* is a ring A with identity together with a ring homomorphism $f : R \to A$ mapping 1_R to 1_A such that the subring $f(R)$ of A is contained in the center of A. That is, $f(R) \subseteq \mathrm{Z}(A)$.

Definition 2.1.5. If A and B are two R-algebras, an *R-algebra homomorphism* (or isomorphism) is a ring homomorphism (isomorphism, respectively) $\varphi : A \to B$ mapping 1_A to 1_B such that $\varphi(ra) = r\varphi(a)$ for all $r \in R$ and $a \in A$.

Definition 2.1.6. Let R be a ring and M and R-module.

(1) An element m of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \quad \text{for some nonzero } r \in R\}.$$

(2) If N is a submodule of M the *annihilator of N in R* is defined to be

$$\mathrm{Ann}_R(N) = \{r \in R \mid rn = 0 \quad \text{for all } n \in N\}.$$

(3) If I is a right ideal of R, the *annihilator of I in M* is defined to be

$$\mathrm{Ann}_M(I) = \{m \in M \mid am = 0 \quad \text{for all } a \in I\}.$$

[1]This satisfies axioms (1) and (2) from Definition 2.1.1

2.2 Quotient Modules and Module Homomorphisms

Definition 2.2.1. Let R be a ring and let M and N be R-modules.

(1) A map $\varphi : M \to N$ is an *R-module homomorphism* if it respects the R-module structures of M and N; i.e.,

  (a) $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in M$ and

  (b) $\varphi(rx) = r\varphi(x)$ for all $r \in R$, $x \in M$.

(2) An R-module homomorphism is an *isomorphism* (of R-modules) if it is both injective and surjective. The modules M and N are said to be *isomorphic*, denoted $M \cong N$, if there is some R-module isomorphism $\varphi : M \to N$.

(3) If $\varphi : M \to N$ is an R-module homomorphism, let $\ker\varphi = \{m \in M \mid \varphi(m) = 0\}$ and let $\operatorname{im}\varphi = \{n \in N \mid n = \varphi(m) \quad \text{for some } m \in M\}$.

(4) Let M and N be R-modules and define $\operatorname{Hom}_R(M, N)$ to be the set of all R-module homomorphisms from M into N.

Note 2.2.1. Any R-module homomorphism is also a homomorphism of the additive groups, but not every group homomorphism need be a module homomorphism (condition (b) may not be satisfied).

Example 2.2.1.

(1) If R is a ring and $M = R$ is a module over itself, then R-module homomorphisms need not be ring homomorphisms and vice versa. For example, when $R = \mathbf{Z}$ the $\mathbf{Z}$-module homomorphism $x \mapsto 2x$ is not a ring homomorphism (1 does not get mapped to 1).

(2) When R is a field, R-module homomorphisms are called *linear transformations*.

(3) $\mathbf{Z}$-module homomorphisms are the same as abelian group homomorphisms; i.e., from Definition 2.2.1 condition (b) is implied by condition (a). For example, $\varphi(2x) = \varphi(x+x) = \varphi(x) + \varphi(x) = 2\varphi(x)$.

(4) Let R be a ring, let I be a two sided ideal of R and suppose M and N are R-modules annihilated by I (i.e., $am = 0$ and $an = 0$ for all $a \in I$, $m \in M$, and $n \in N$). Any R-module homomorphism from N to M is then automatically a homomorphism of (R/I)-modules.

Proposition 2.2.2. *Let M, N, and L be R-modules.*

(1) A map $\varphi : M \to N$ is an R-module homomorphism if and only if $\varphi(rx+y) = r\varphi(x) + \varphi(y)$ for all $x, y \in M$ and all $r \in R$.

(2) Let φ, ψ be elements of $\operatorname{Hom}_R(M, N)$ Define $\varphi + \psi$ by

$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \quad \text{for all } m \in M.$$

Then $\varphi + \psi \in \operatorname{Hom}_R(M, N)$ and with this operation $\operatorname{Hom}_R(M, N)$ is an abelian group. If R is a commutative ring then for $r \in R$ define $r\varphi$ by:

$$(r\varphi)(m) = r\varphi(m) \quad \text{for all } m \in M.$$

Then $r\varphi \in \operatorname{Hom}_R(M, N)$ and with this action of the commutative ring R the abelian group $\operatorname{Hom}_R(M, N)$ is an R-module.

(3) If $\varphi \in \operatorname{Hom}_R(L, M)$ and $\psi \in \operatorname{Hom}_R(M, N)$ then $\psi \circ \varphi \in \operatorname{Hom}_R(L, N)$.

(4) With addition as above and multiplication defined as function composition, $\operatorname{Hom}_R(M, M)$ is a ring with 1. When R is commutative $\operatorname{Hom}_R(M, M)$ is an R-algebra.

Proof. (1) Certainly if φ is an R-module homomorphism then $\varphi(rx + y) = r\varphi(x) + \varphi(y)$. Conversely, if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$, take $r = 1$ to see that φ is additive and take $y = 0$ to see that φ commutes with the action of R on M.[2]

(2) It is straightforward to check that all the abelian group and R-module axioms hold with these definitions. For example $r\varphi$ satisfies (b) from Definition 2.1.1 as follows:

$$\begin{aligned}(r_1\varphi)(r_2m) &= r_1\varphi(r_2m)\\ &= r_1r_2\varphi(m)\\ &= r_2r_1\varphi(m)\\ &= r_2(r_1\varphi)(m).\end{aligned}$$

(3) Let φ and ψ be as given and let $r \in R$ and $x, y \in L$. Then:

$$\begin{aligned}(\psi \circ \varphi)(rx + y) &= \psi(\varphi(rx + y))\\ &= \psi(r\varphi(x) + \varphi(y))\\ &= r\psi(\varphi(x)) + \psi(\varphi(y))\\ &= r(\psi \circ \varphi)(x) + (\psi \circ \varphi)(y).\end{aligned}$$

So, by (1) from this proposition, $\psi \circ \varphi$ is an R-module homomorphism.

(4) Note that since the domain and codomain of the elements of $\operatorname{Hom}_R(M, M)$ are the same, function composition is defined. By (3) from this proposition, it is a binary operation on $\operatorname{Hom}_R(M, M)$. As usual function composition is associative. The remaining ring axioms are straight foward to check. The identity function, I, ($I(x) = x$ for all $x \in M$) is seen to be the multiplicative identity of $\operatorname{Hom}_R(M, M)$. If R is commutative, then (2) from this proposition shows that the ring $\operatorname{Hom}_R(M, M)$ is a left R-module and defining $\varphi r = r\varphi$ for all $\varphi \in \operatorname{Hom}_R(M, M)$ and $r \in R$ makes $\operatorname{Hom}_R(M, M)$ into an R-algebra. □

Definition 2.2.3. The ring $\operatorname{Hom}_R(M, M)$ is called the *endomorphism ring of M* and is denoted $\operatorname{End}_R(M)$. Elements of $\operatorname{End}_R(M)$ are called *endomorphisms*.

Note 2.2.2. Let H be a subgroup of G. If G is abelian then H is normal. This is relevant for the following proposition.

Proposition 2.2.4. *Let R be a ring, let M be an R-module and let N be a submodule of M. The (additive, abelian) quotient group M/N can be made into an R-module by defining an action of elements of R by*

$$r(x + N) = rx + N \quad \textit{for all } r \in R,\ x + N \in M/N.$$

The natural projection map $\pi : M \to M/N$ defined by $\pi(x) = x + N$ is an R-module homomorphism with kernel N.

[2] We say φ is *homogeneous* in this case.

Proof. Since M is an abelian group under $+$ the quotient group M/N is defined and is an abelian group. We must show that the action of the ring element r on the coset $x+N$ is well defined. Suppose $x+N=y+N$; i.e., $x-y\in N$. Since N is a (left) R-module, $r(x-y)\in N$. Thus $rx-ry\in N$; i.e., $rx+N=ry+N$.

Since the operations in M/N are "compatible" with those of M, the axioms for an R-module are easily checked. Likewise, the natural projection map π described as above is, in particular, the natural projection of the abelian group M onto the abelian group M/N hence is a group homomorphism with kernel N. The kernel of any module homomorphism is the same as its kernel when viewed as a homomorphism of the abelian group structures. It remains to show that π is a module homomorphism —which it is: $\pi(rm)=rm+N=r(m+N)=r\pi(m)$. □

Definition 2.2.5. Let A,B be submodules of the R-module M. The _sum_ of A and B is the set $A+B=\{a+b \mid a\in A, b\in B\}$.

Definition 2.2.6 (Isomorphism Theorems)**.**

(1)

(2)

(3)

(4)

2.3 Generation of Modules, Direct Sums, and Free Modules

Definition 2.3.1. Let M be an R-module and let $N_1,...,N_n$ be submodules of M.

(1) The _sum_ of $N_1,...,N_n$ is the set of all finite sums of elements from the sets N_i: $\{a_1+a_2+...+a_n \mid a_i\in N_i$ for all $i\}$. Denote this sum by $N_1+N_2+...+N_n$.

(2) For any subset A of M let

$$RA=\{r_1a_1+r_2a_2+...+r_ma_m \mid r_1,...,r_m\in R,\ a_1,...,a_m\in A,\ m\in \mathbf{Z}^+\}$$

(where by convention $RA=\{0\}$ if $A=\emptyset$). If A is the finite set $\{a_1,a_2,...,a_n\}$ we shall write $Ra_1+Ra_2+...+Ra_n$ for RA. Call RA the _submodule of M generated by A_. If N is a submodule of M (possibly $N=M$) and $N=RA$ for some subset A of M, we call A a _set of generators_ or _generating set_ for N, and we say N is _generated_ by A.

(3) A submodule N of M (possibly $N=M$) is _finitely generated_ if there is some finite subset A of M such that $N=RA$, that is, if N is generated by some finite subset.

(4) A submodule N of M (possibly $N=M$) is _cyclic_ if there exists an element $a\in M$ such that $N=Ra$, that is, if N is generated by one element:

$$N=RA=\{ra \mid r\in R\}.$$

Definition 2.3.2. Let $M_1,...,M_k$ be a collection of R-modules. The collection of k-tuples $(m_1,...,m_k)$ where $m_i\in M_i$ with addition and action of R defined componentwise is called the _direct product_ of $M_1,...,M_k$, denoted $M_1\times...\times M_k$. The direct product of $M_1,...,M_k$ is also referred to as the (external) _direct sum_ of $M_1,...,M_k$ and is denoted $M_1\oplus...\oplus M_k$.

Proposition 2.3.3. *Let $N_1, N_2, ..., N_k$ be submodules of the R-module M. Then the following are equivalent:*

(1) The map $\pi : N_1 \times N_2 \times ... \times N_k \to N_1 + N_2 + ... + N_k$ defined by

$$\pi((a_1, a_2, ..., a_k)) = a_1 + a_2 + ... + a_k$$

is an isomorphism (of R-modules): $N_1 \times N_2 \times ... \times N_k \cong N_1 + N_2 + ... + N_k$.

(2) $N_j \cap (N_1 + N_2 + ... + N_{j-1} + N_{j+1} + ... + N_k) = 0$ for all $j \in \{1, 2, ..., k\}$.

(3) Every $x \in N_1 + N_2 + ... + N_k$ can be written uniquely in the form $a_1 + a_2 + ... + a_k$ with $a_i \in N_i$.

Proof. To prove that (1) implies (2), suppose for some j (2) fails to hold and let $a_j \in N_j \cap (N_1 + N_2 + ... + N_{j-1} + N_{j+1} + ... + N_k)$ with $a_j \neq 0$. Then $a_j \in N_j$ and $a_j \in N_1 + N_2 + ... + N_{j-1} + N_{j+1} + ... + N_k$, hence $a_j = a_1 + a_2 + ... + a_{j-1} + a_{j+1} + ... + a_k$ for some $a_i \in N_i$. Subtracting a_j from both sides gives $0 = a_1 + a_2 + ... + a_{j-1} - a_j + a_{j+1} + ... + a_k$, which is equivalent to $\pi(0) = (a_1, a_2, ..., a_{j-1}, -a_j, a_{j+1}, ..., a_k)$. Note that this would be a nonzero element of $\ker \pi$, which gives a contradiction.

Assume now that (2) holds. If for some module elements $a_i, b_i \in N_i$ we have:

$$a_1 + a_2 + ... + a_k = b_1 + b_2 + ... + b_k$$

then for each j we have:

$$a_j - b_j = (b_1 - a_1) + (b_2 - a_2) + ... + (b_{j-1} - a_{j-1}) + (b_{j+1} - a_{j+1}) + ... + (b_k - a_k).$$

The left belongs to N_j and the right side belongs to $(N_1 + N_2 + ... + N_{j-1} + N_{j+1} + ... + N_k)$, hence $a_j - b_j \in N_j \cap (N_1 + N_2 + ... + N_{j-1} + N_{j+1} + ... + N_k)$. It must be the case then that $a_j - b_j = 0$; i.e., $a_j = b_j$ for all j. Thus (2) implies (3).

Finally, to see that (3) implies (1), observe first that the map π is clearly a surjective R-module homomorphism. Then (3) simply implies π is injective, hence is an isomorphism, completing the proof. □

Definition 2.3.4. If an R-module M is the sum of submodules $N_1, N_2, ..., N_k$ of M satisfying the conditions of the proposition above, then M is said to be the (internal) *direct sum* of $N_1, N_2, ..., N_k$, written:

$$M = N_1 \oplus N_2 \oplus ... \oplus N_k.$$

Note 2.3.1. Part (1) of Proposition 2.3.3 is the statement that the internal direct sum of $N_1, N_2, ..., N_k$ is isomorphic to their external direct sum (from Definition 2.3.2), which is the reason we identify them and use the same notation for both.

Definition 2.3.5. An R-module F is said to be *free* on the subset A of F if for every nonzero element x of F, there exist unique nonzero elements $r_1, r_2, ..., r_n$ of R and unique $a_1, a_2, ..., a_n$ in A such that $x = r_1 a_1 + r_2 a_2 + ... + r_n a_n$, for some $n \in \mathbf{Z}^+$. In this situation we say A is a *basis* or *set of free generators* for F. If R is a commutative ring the cardinality of A is called the *rank* of F.

Note 2.3.2. To avoid confusion, we reiterate Definition 2.3.1 and Definition 2.3.5 as follows: An R-module M is called:

- *free* if $M \cong R^n = \bigoplus_{i=1}^n R$. In other words, the map $\phi : R^n \to M$ is an R-module isomorphism. n is called the *rank* of M and it can be infinite.

- *finitely generated* if M has a finite generating set. In other words, the map $\phi : R^n \to M$ is only surjective.

The difference boils down to whether $\ker \phi = 0$ or not. Furthermore, in the case of a direct sum between two modules, the module elements will be unique, whereas in the case of free modules the module elements and ring elements must be unique.

Theorem 2.3.6. *For any set A there is a free R-module $F(A)$ on the set A where $F(A)$ satisfies the following universal property: if M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\phi : F(A) \to M$ such that $\phi(a) = \varphi(a)$ for all $a \in A$, that is, the following diagram commutes:*

$$\begin{tikzcd} A \arrow[r, "\text{inclusion}"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\phi"] \\ & M \end{tikzcd}$$

Proof. Let $F(A) = \{0\}$ if $A = \emptyset$. If A is nonempty let $F(A)$ be the collection of all set functions $f : A \to R$ such that $f(a) = 0$ for all but finitely many $a \in A$. Make $F(A)$ into an R-module by pointwise addition of functions and pointwise multiplication of a ring element times a function. It is an easy matter to check that all R-module axioms hold. Identify A as a subset of $F(A)$ by $a \mapsto f_a$, where f_a is the function which is 1 at a and zero elsewhere. We can, in this way, think of $F(A)$ as all finite R-linear combinations of elements of A by identifying each function f with the sum $r_1a_1 + r_2a_2 + ... + r_na_n$, where f takes on the value r_i at a_i and is zero at all other elements of A. To establish the universal property of $F(A)$ suppose $\varphi : A \to M$ is a map of the set A into the R-module M. Define $\phi : F(A) \to M$ by

$$\phi : \sum_{i=1}^{n} r_i a_i \mapsto \sum_{i=1}^{n} r_i \varphi(a_i).$$

By the uniqueness of the expression for the elements of $F(A)$ as linear combinations of the a_i we see easily that ϕ is a well defined R-module homomorphism. By definition, the restriction of ϕ to A equals φ. Finally, since $F(A)$ is generated by A, once we know the values of an R-module homomorphism on A its values on every element of $F(A)$ are uniquely determined, so ϕ is the unique extension of φ to all of $F(A)$. □

Corollary 2.3.7.

(1) If F_1 and F_2 are free modules on the same set A, there is a unique isomorphism between F_1 and F_2 which is the identity map on A.

(2) If F is any free R-module with basis A, then $F \cong F(A)$. In particular, F enjoys the same universal property with respect to A as $F(A)$ does in Theorem 2.3.6.

Proof. Exercise. □

2.4 Tensor Products of Modules

Definition 2.4.1. Let R be a ring, let A be a right R-module, let B be a left R-module, and let G be an (additive) abelian group. A function $f : A \times B \to G$ is called *R-biadditive* if, for all $a, a' \in A$, $b, b' \in B$, and $r \in R$ we have

(1) $f(a + a', b) = f(a, b) + f(a', b)$,

(2) $f(a, b + b') = f(a, b) + f(a, b')$,

(3) $f(ar, b) = f(a, rb)$.

If R is commutative and A, B, and M are R-modules, then a function $f : A \times B \to M$ is called *R-bilinear* if f is R-biadditive and also

(4) $f(ar, b) = f(a, rb) = rf(a, b)$.

Example 2.4.1.

(1) If R is a ring, then its multiplication $\mu : R \times R \to R$ is R-biadditive; the first two axioms from Definition 2.4.1 are the right and left distributive laws, while the third axiom is associativity:

$$\mu(ar, b) = (ar)b = a(rb) = \mu(a, rb).$$

If R is a commutative ring, then μ is R-bilinear, for $(ar)b = a(rb) = r(ab)$.

(2) If we regard a left R-module M as its underlying abelian group, then the scalar multiplication $\sigma : R \times M \to M$ is $\mathbf{Z}$-bilinear.

(3) Recall from Proposition 2.2.2 that $\mathrm{Hom}_R(M, N)$ is an R-module if R is commutative and we define $(r\varphi)(m) = r(\varphi(m))$ for all $m \in M$. With this definition we can see that *evaluation* $e : M \times \mathrm{Hom}_R(M, N) \to N$ given by $(m, \varphi) \mapsto \varphi(m)$ is R-bilinear.

Definition 2.4.2. Given a ring R, a left R-module A, and a right R-module B, then their *tensor product* is an abelian group $A \otimes_R B$ and an R-biadditive function

$$h : A \times B \to A \otimes_R B$$

such that, for every abelian group G and every R-biadditive function $f : A \times B \to G$, there exists a unique $\mathbf{Z}$-homomorphisms $\tilde{f} : A \otimes_R B \to G$ making the following diagram commute:

$$\begin{tikzcd} A \times B \arrow[rr, "h"] \arrow[dr, "f"'] & & A \otimes_R B \arrow[dl, dashed, "\tilde{f}"] \\ & G & \end{tikzcd}$$

Definition 2.4.3. Let R and S be rings and let M be an abelian group. Then M is an *(R, S)-bimodule*, denoted by ${}_RM_S$, if M is a left R-module and a right S-module, and the two scalar multiplications are related by an associative law:

$$r(ms) = (rm)s$$

for all $r \in R$, $m \in M$, and $s \in S$. If M is an (R, S)-bimodule, it is permissible to write rms with no parentheses, for the definition of bimodules says that the two possible associations agree.

Example 2.4.2.

(1) Every ring R is an (R,R)-bimodule; the extra identity is just the associativity of multiplication in R. More generally, if $S \subseteq R$ is a subring, then R is an (R,S)-bimodule.

(2) Every two-sided ideal in a ring R is an (R,R)-bimodule.

(3) If M is a left R-module, then M is an $(R,\mathbf{Z})$-bimodule. The "reverse" holds if M were a right R-module.

(4) If R is commutative, then every left (or right) R-module is an (R,R)-bimodule. In more detail, if $M = {}_RM$, define a new scalar multiplication $M \times R \to M$ by $(m,r) \mapsto rm$. To see that M is a right R-module, we must show that $m(rr') = (mr)r'$, that is $(rr')m = r'(rm)$, and this is so because $rr' = r'r$. Finally, M is an (R,R)-bimodule because both $r(mr')$ and $(rm)r'$ equal to $(rr')m$.

Proposition 2.4.4 (Extending Scalars)**.** *Let S be a subring of a ring R.*

(1) Given a bimodule ${}_RA_S$ and a left module ${}_SB$, then the tensor product $A \otimes_S B$ is a left R-module, where

$$r(a \otimes b) = (ra) \otimes b.$$

Similarly, given A_S and ${}_SB_R$, the tensor product $A \otimes_S B$ is a right R-module, where $(a \otimes b)r = a \otimes (br)$.

(2) The ring R is an (R,S)-bimodule and, if M is a left S-module, then $R \otimes_S M$ is a left R-module.

2.5 Exact Sequences

Definition 2.5.1.

(1) The pair of homomorphisms $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is said to be <u>*exact*</u> (at Y) if $\operatorname{im}\alpha = \ker\beta$.

(2) A sequence $... \to X_{n-1} \to X_n \to X_{n+1} \to ...$ of homomorphisms is said to be an <u>*exact sequnce*</u> if it is exact at every X_n between a pair of homomorphisms.

Proposition 2.5.2. *Let A, B, and C be R-modules over some ring R. Then*

(1) The sequence $0 \to A \xrightarrow{\psi} B$ is exact (at A) if and only if ψ is injective.

(2) The sequence $B \xrightarrow{\varphi} C \to 0$ is exact (at C) if and only if φ is surjective.

Proof. The (uniquely defined) homomorphism $0 \to A$ has image 0 in A. This will be the kernel of ψ if and only if ψ is injective.

Similarly, the kernel of the (uniquely defined) zero homomorphism $C \to 0$ is all of C, which is the image of φ if and only if φ is surjective. □

Corollary 2.5.3. *The sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is exact if and only if ψ is injective, φ is surjective, and $\operatorname{im}\psi = \ker\varphi$; i.e., B is an extension of C by A.*

Definition 2.5.4. The exact sequence $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ is called <u>*short exact sequence*</u>.

Example 2.5.1.

(1) Given modules A and C we can always form their direct sum $B = A \oplus B$ and the sequence

$$0 \to A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \to 0$$

where $\iota(a) = (a, 0)$ and $\pi(a, c) = c$ is a short exact sequence. It follows that there always exists at least one extension of C by A.

(2) Consider the two $\mathbf{Z}$-modules $A = \mathbf{Z}$ and $C = \mathbf{Z}/n\mathbf{Z}$:

$$0 \longrightarrow \mathbf{Z} \xrightarrow{\iota} \mathbf{Z} \oplus (\mathbf{Z}/n\mathbf{Z}) \xrightarrow{\varphi} \mathbf{Z}/n\mathbf{Z} \longrightarrow 0$$

This is one extension of $\mathbf{Z}/n\mathbf{Z}$ by $\mathbf{Z}$. Another extension is given by the short exact sequence:

$$0 \longrightarrow \mathbf{Z} \xrightarrow{n} \mathbf{Z} \xrightarrow{\pi} \mathbf{Z}/n\mathbf{Z} \longrightarrow 0$$

where n denotes the map $x \mapsto nx$ given by multiplication by n, and π denotes the natural projection. Note that the modules in the middle of the previous two exact sequences are not isomorphic even though the respective "A" and "C" terms are isomorphic. Thus there are (at least) two "inequivalent" ways of extending $\mathbf{Z}/n\mathbf{Z}$ by $\mathbf{Z}$.

(3) If $\varphi : B \to C$ is any homomorphism we may form an exact sequence:

$$0 \longrightarrow \ker\varphi \xrightarrow{\iota} B \xrightarrow{\varphi} \operatorname{im}\varphi \longrightarrow 0$$

where ι is the inclusion map. In particular, if φ is surjective, the sequence $\varphi : B \to C$ may be extended to a short exact sequence with $A = \ker\varphi$.

(4) Let M be an R-module and S a set of generators for M. Let $F(S)$ be the free R-module on S. Then

$$0 \longrightarrow K \xrightarrow{\iota} F(S) \xrightarrow{\varphi} M \longrightarrow 0$$

is the short exact sequence where φ is the unique R-module homomorphism which is the identity on S (c.f. Theorem 2.3.6) and $K = \ker\varphi$.

Definition 2.5.5. Let $0 \to A \to B \to C \to 0$ and $0 \to A' \to B' \to C' \to 0$ be two short exact sequences of modules.

(1) A *homomorphism of short exact sequences* is a triple (α, β, γ) of module homomorphisms such that the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

The homomorphism is an *isomorphism of short exact sequences* if α,β,γ are all isomorphisms, in which case the extensions B and B' are said to be *isomorphism extensions*.