1. Modules

Exercise 1.1. Show that an R-module homomorphism $f\colon M \to N$ is an isomorphism if and only if it is injective and surjective.

Proof. Suppose f is an isomorphism, so there exists a homomorphism $f^{-1} \in \mathrm{Hom}_R(N, M)$ such that $f \circ f^{-1} = \mathbb{1}_N$ and $f^{-1} \circ f = \mathbb{1}_M$. Suppose $f(v) = f(w)$. Then $v = f^{-1} \circ f(v) = f^{-1} \circ f(w) = w$, so f is injective. Now for $n \in N$, we have $n = f\left(f^{-1}(n)\right)$, so f is surjective.
Conversely, if f is injective, it has a left inverse as a function, and if it surjective, it has a right inverse, and these are unique and equal (by the same general property for functions). Denote this function by $f^{-1}\colon N \to M$. We claim this is an R-module homomorphism. Indeed, as f is a group homomorphism, we know the inverse is as well. Now, since $f \circ f^{-1}(rn) = rn$ and $rn = rf \circ f^{-1}(n) = f\left(rf^{-1}(n)\right)$, we have by injectivity of f that $f^{-1}(rn) = rf^{-1}(n)$, so indeed f^{-1} is an R-module homomorphism. □

Exercise 1.2. $\mathrm{Hom}_R(M, N)$ has the structure of an abelian group with

$$(f+g)(x) := f(x) + g(x)$$
$$(-f)(x) := -f(x)$$

Proof. We must check associativity, identity, inverse and commutativity when the set $\mathrm{Hom}_R(M, N)$ is equipped with the binary operator and inverse defined above. Associativity is inherited from associativity of functions. Now, let 0_N denote the identity of the abelian group N. Define a map 0 by $0(m) = 0_N$ for all $m \in M$. Then for any $f \in \mathrm{Hom}_R(M, N)$, we have

$$(f+0)(x) = f(x) + 0(x) = f(x) + 0_N = f(x)$$

and similarly, $0 + f = f$. Thus 0 is an identity for $\mathrm{Hom}_R(M, N)$. Now

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0_N$$

so $f + (-f) = 0$, and similarly, $(-f) + f = 0$.
Lastly, commutativity follows from commutativity of N. □

Exercise 1.3. For a homomorphism $f \in \mathrm{Hom}_R(M, N)$, the kernel $\ker(f) = \{x \mid f(x) = 0\}$ and the image $\mathrm{im}(f)$ are submodules.

Proof. For $x, y \in \ker f$, we have $f(x-y) = f(x) - f(y) = \mathbb{1}_R$ by f being a group homomorphism, and $f(rx) = rf(x) = r \cdot \mathbb{1}_R = \mathbb{1}_R$ by the definition of an R-module and an R-linear map, hence $\ker f$ is also closed under multiplication by elements of R. The inclusion $\ker f \to M$ is R-linear since if $x, y \in \ker f$, then $\iota(rx + y) = rx + y = r\iota(x) + \iota(y)$.
Likewise, if $x, y \in \mathrm{im}\, f$, then let $u, v \in M$ such that $f(u) = x$ and $f(v) = y$. Then $f(u - v) = f(u) - f(v) = x - y \in \mathrm{im}\, f$ and $f(ru) = rf(u) = rx \in \mathrm{im}\, f$ for all $r \in R$ and for all $x, y \in \mathrm{im}\, f$. Furthermore, for $x, y \in \mathrm{im}\, f$, $\iota(rx+y) = rx+y = r\iota(x)+\iota(y)$ so the inclusion $\mathrm{im}\, f \to N$ is R-linear. □

Exercise 1.4. R/I is a ring if I is a two-sided ideal of R.

Proof. If I is a two-sided ideal, then firstly, R/I is an abelian group under $+$ since everything is abelian hence normal. All other requirements for a ring are inherited from R. We must only check that multiplication is well-defined. If $r+I=r'+I$ and $s+I=s'+I$ then $s^{-1}\underbrace{r^{-1}r'}_{\in I}s'\in I$, so indeed $rs+I=r's'+I$. ☐

Exercise 1.5. Show that a cokernel exists and is unique up to isomorphism.

Proof. For an R-linear map $f\colon M\to N$, define $\operatorname{coker} f := N/\operatorname{im} f$. Since $\operatorname{im} f$ is a submodule of N, $N/\operatorname{im} f$ is an R-module. Furthermore, it satisfies the diagram

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "0"'] & N \arrow[r, "q"] \arrow[d, "g"] & \operatorname{coker} f \arrow[dl, "\exists!\overline{g}"] \\ & L & \end{tikzcd}$$

since $\overline{g}$ must be defined by $\overline{g}(q(n))=g(n)$. We must check that this is well-defined. Suppose $\overline{a}=\overline{b}\in\operatorname{coker} f$, so $a-b\in\operatorname{im} f$, so $f(m)=a-b$. Then $0=gf(m)=\overline{g}(q(a)-q(b))=\overline{g}\left(\overline{a}-\overline{b}\right)=\overline{g}(a)-\overline{g}(b)$.
It is also R-linear because $\overline{g}\left(\overline{x}+\overline{y}\right)=\overline{g}\left(\overline{x+y}\right)=g(x+y)=g(x)+g(y)=\overline{g}\left(\overline{x}\right)+\overline{g}\left(\overline{y}\right)$, and $\overline{g}\left(r\overline{x}\right)=\overline{g}\left(\overline{rx}\right)=g\left(rx\right)=rg(x)=r\overline{g}(\overline{x})$.
To check uniqueness, suppose (K,q') also satisfies the above diagram. Then letting $g=q$ and $L=\operatorname{coker} f$, we get

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "0"'] & N \arrow[r, "q'"] \arrow[d, "q"] & K \arrow[dl, "\exists!\overline{q}"] \\ & \operatorname{coker} f & \end{tikzcd}$$

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "0"'] & N \arrow[r, "q"] \arrow[d, "q'"] & \operatorname{coker} f \arrow[dl, "\exists!\overline{q'}"] \\ & K & \end{tikzcd}$$

Interchanging $\operatorname{coker} f$ and K, we also get a unique map $\overline{q'}\colon\operatorname{coker} f\to K$. These have the property that $\overline{q'}\circ\overline{q}\circ q'=\overline{q'}\circ q=q'$ so by uniqueness of $\mathbb{1}_K$ in the diagram

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "0"'] & N \arrow[r, "q'"] \arrow[d, "q'"] & K \arrow[dl, "\mathbb{1}_K"] \\ & K & \end{tikzcd}$$

we get $\overline{q'}\circ\overline{q}=\mathbb{1}_K$, and likewise, $\overline{q}\circ\overline{q'}=\mathbb{1}_{\operatorname{coker} f}$. So $\overline{q}\colon\operatorname{coker} f\to K$ is an isomorphism.

☐

1.1. **Direct sum and direct product.**

Exercise 1.6. Prove uniqueness of the direct product.

Proof. Suppose A and B are both direct products with maps $\pi_{A,j}\colon A\to M_j$ and $\pi_{B,j}\colon B\to M_j$ for all j such that the universal diagram is fulfilled. Then, since we have maps $\pi_{B,j}\colon B\to M_j$ for all j, we have a unique map $u\colon B\to A$ such that $\pi_{A,j}\circ u=\pi_{B,j}$ for all j. And similarly, we have a map $v\colon A\to B$ such that $\pi_{B,j}\circ v=\pi_{A,j}$ for all j. But then $\pi_{A,j}\circ u\circ v=\pi_{A,j}$ for all j, so since $\pi_{A,j}\circ\mathbb{1}_A=\pi_{A,j}$

for all j, we get by uniqueness that $u \circ v = \mathbb{1}_A$, and similarly, interchanging A for B above, we get $v \circ u = \mathbb{1}_B$. Hence $u\colon B \to A$ is an isomorphism.

$\square$

Remark (Direct product). Note that the direct product of a family $(M_i)_{i\in I}$ is simply the universal cone over the diagram $I \to \mathrm{Mod}_R$ given by sending $i \mapsto M_i$ where I is a discrete category.

Remark (Direct sum). The direct sum is the dual of the direct product.
Given a diagram $I \to \mathrm{Mod}_R$ where I is discrete, we define the direct sum as the cone under $I \to \mathrm{Mod}_R$ and let its nadir be denoted $\bigoplus_{i\in I} M_i$ together with R-linear maps $\iota_j\colon M_j \to \bigoplus_{i\in I} M_i$.

Remark. For each $i \in I$, there is a unique map $f_j\colon M_j \to \prod_{j\in I} M_j$ with $\pi_i f_j = 0$ if $i \neq j$ and $\pi_j f_j = \mathbb{1}_{M_j}$. By the universal property, we thus get a unique map $u\colon \bigoplus_{i\in I} M_i \to \prod_{i\in I} M_i$ given by $u(x) = \sum_{i\in I} f_i(x(i))$. This map is an isomorphism when I is finite, but not necessarily when I is infinite.

Corollary 1.7. *Summarizing, we have bijections*

$$\mathrm{Hom}_R\left(N, \prod_{i\in I} M_i\right) \overset{\approx}{\to} \prod_{i\in I} \mathrm{Hom}_R(N, M_i)$$
$$u \mapsto (\pi_i u)_{i\in I}$$

where we send $(\pi_i u)_{i\in I}(j) = \pi_j u\colon N \overset{u}{\to} \prod_{i\in I} M_i \overset{\pi_j}{\to} M_j$ *and*

$$\mathrm{Hom}_R\left(\bigoplus_{i\in I} M_i, N\right) \overset{\approx}{\to} \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$$
$$u \mapsto (u\iota_i)_{i\in I}$$

which are in fact isomorphisms of abelian groups.

Exercise 1.8. Show that the above bijections are isomorphisms of abelian groups.

Proof. Since they are bijections between abelian groups, we must simply show that they are homomorphisms.
Now,

$$u + v \mapsto (\pi_i(u+v))_{i\in I} = (\pi_i u + \pi_i v)_{i\in I}$$

and $(\pi_i u + \pi_i v)(j) = (\pi_i u)(j) + (\pi_i v)(j)$ so $u + v \mapsto (\pi_i u) + (\pi_i v)$ by the definition of addition in the direct product, hence this is indeed a homomorphism.
For the direct sum, we similarly have

$$u + v \mapsto ((u+v)\iota_i)_{i\in I} = (u\iota_i + v\iota_i)_{i\in I}$$

and $(u\iota_i + v\iota_i)_{i\in I}(j) = (u\iota_i)_{i\in I}(j) + (v\iota_i)_{i\in I}(j)$, so $u + v \mapsto (u\iota_i)_{i\in I} + (v\iota_i)_{i\in I}$ which is indeed a homomorphism by the additive structure on the direct product which the direct sum inherits.

$\square$

Exercise 1.9. Show that cyclic left R-modules (of R?) are precisely those of the form R/I for some left ideal $I \subset R$.

Proof. Suppose M is a cyclic left R-module. Then $M = Rx$ for some $x \in M$.

$\square$

1.2. **Generation and free modules.**

Exercise 1.10. Show that an R-module is free if and only if it has a basis.

Proof. Suppose M is a free R-module. Let X be a generating set and $\mu\colon X \to M$ the map satisfying the universal property that for any R-module N and any map $f\colon X \to N$, there exists a unique R-linear map $\tilde{f}\colon M \to N$ such that $\tilde{f}\mu = f$.

$$\begin{tikzcd} X \arrow[r, "\mu"] \arrow[dr, "f"'] & M \arrow[d, dashed, "\exists! \tilde{f}"] \\ & N \end{tikzcd}$$

We claim M has $\mu(X)$ as a basis. Suppose there exists a finite linear combination $\sum_{i=1}^n r_i x_i = 0$ with $x_i \in \mu(X)$ and $r_i \in R$ such that not all r_i are 0. Then let $N = \bigoplus_X R$ and $f\colon X \to \bigoplus_X R$ be the inclusion $x \mapsto \iota_x(\mathbb{1}_R)$. By uniqueness, we must have that $0 = \tilde{f}(\mu(x_i)) = \iota_x(\mathbb{1}_R)$, so $\tilde{f}\left(\sum r_i x_i\right) = \sum r_i \tilde{f}\mu(x_i') = \sum r_i f(x_i') = \sum r_i \iota_{x_i'}(\mathbb{1}_R)$, but by definition then $0 = \left(\sum r_i f(x_i')\right)(j) = \left(\sum r_i \iota_{x_i'}(\mathbb{1}_R)\right)(j) = \sum r_i \iota_{x_i'}(\mathbb{1}_R)(j) \sum r_i \mathbb{1}_R \delta_{i,j} = r_j$ for all j, hence we obtain linear indepence.
Conversely, suppose M has $X \subset M$ as a basis. Let $\mu\colon X \to M$ be the inclusion. We claim this is a free R-module.
Suppose N is any other R-module and we have any (not necessarily an R-module homomorphism) map $f\colon X \to N$. If $\tilde{f}\mu = f$, then we must have $\tilde{f}(x) = f(x)$ for all $x \in X$. Now, for any linear combination $\sum r_i x_i \in M$, we have by linearity, $\tilde{f}\left(\sum r_i x_i\right) = \sum r_i \tilde{f}(x_i) = \sum r_i f(x_i)$, so $\tilde{f}$ is indeed uniquely determined by f. $\square$

Exercise 1.11. Complete the proof that every commutative ring R has invariant basis number.

Proof. By Zorn's lemma, every commutative ring R has a maximal ideal $I \leq R$. Then R/I is a field. Let now M be a free R-module with basis $\{x_i\}_{i \in J}$.
We claim M/IM is an R/I module. Define $\overline{r} \cdot \overline{x} = \overline{rx}$ where multiplication of rx is done in M over R, and define $\overline{v} + \overline{w} = \overline{v + w}$.
Suppose $\overline{r} = \overline{r'}$ and $\overline{x} = \overline{x'}$. So $r' - r \in I$ and $x' - x \in IM$. Then $r'x' - rx' \in IM$ and $rx' - rx \in IM$, so $r'x' - rx = r'x' - rx' + rx' - rx \in IM$, hence $\overline{r'x'} = \overline{rx}$ is well defined. Similarly, if $\overline{v} = \overline{v'}$ and $\overline{w} = \overline{w'}$ then $v - v', w - w' \in IM$, so $v + w - (v' + w') \in IM$, hence $\overline{v + w} = \overline{v' + w'}$.

The properties for M/IM being an R/I-module are then inherited from M as an R-module.

But as R/I is a field, M/IM is a vector space over R/I, hence its dimension is well-defined. Now, suppose $\sum \overline{r_i} \cdot \overline{x_i} = 0$ in M/IM. Then $\overline{\sum r_i x_i} = 0$, hence $\sum r_i x_i \in IM$. But then there exists a linear combination $\sum s_i x_i$ such that $s_i \in I$ for all i, and such that $\sum r_i x_i = \sum s_i x_i$. Then $\sum (r_i - s_i) x_i = 0$ and linear independence of $\{x_i\}_{i \in J}$ gives $r_i = s_i$ for all i, hence $\overline{r_i} = \overline{0}$. So $\{\overline{x_i}\}_{i \in J}$ is linearly independent over R/I as well. Hence as it clearly also spans M/IM, we have that $\dim_{R/I} M/IM = |J|$. Thus an bases for M over R have the same cardinality, so R has invariant basis number. $\square$

Exercise 1.12. Find a free non commutative ring R with bases of different cardinalities.

1.3. **Free modules over PID.**

1.4. **Structure theorem for modules over PID.**

1.5. **Exact sequences.**

Exercise 1.13. In the 2-out-of-3 lemma, what can you say about a third map if two of the h_1, h_2, h_3 are just injective (or just surjective)?

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "h_1"] & M \arrow[r, "g"] \arrow[d, "h_2"] & M'' \arrow[r] \arrow[d, "h_3"] & 0 \\ 0 \arrow[r] & N' \arrow[r, "f'"] & N \arrow[r, "g'"] & N'' \arrow[r] & 0 \end{tikzcd}$$

Solution. Suppose h_1 and h_3 are injective. By the same argument as the one in the notes, h_2 is also injective.
Similarly, if h_1 and h_3 are surjective, the same argument as in the notes shows that h_2 is surjective.
Suppose h_1, h_2 are injective. Let $h_3(m) = 0$. Then by surjectivity of g, let $m' \in M$ such that $g(m') = m$. Then $g'h_2(m') = 0$ so there exists $m'' \in M'$ such that $f'h_1(m'') = h_2(m')$, so $h_2 f(m'') = h_2(m')$. But h_2 is injective, so $m' = f(m'')$. Thus $m = g(m') = gf(m'') = 0$ by exactness. So h_3 is injective. If h_2 is surjective, then letting $n \in N''$, there exists $n' \in N$ with $g'(n') = n$ so by surjectivity of h_2, there exists $m \in M$ such that $h_2(m) = n'$. Then $h_3(g(m)) = n$, so h_3 is surjective.

Exercise 1.14. Show that if $0 \to N' \xrightarrow{f} N \xrightarrow{g} N''$ is an exact sequence of R-modules and g is surjective, then g_* need not be surjective.

1.6. **Projective modules.**

Definition 1.15. An R-module P is projective if for every R-linear map $f\colon P \to M$ and every R-linear surjective map $q\colon N \to M$ of R-modules, there exists an R-linear map $h\colon P \to N$ such that

$$\begin{tikzcd} & P \arrow[d, "f"] \arrow[dl, "\exists h"'] \\ N \arrow[r, two heads, "q"] & M \end{tikzcd} \tag{Ω}$$

commutes.

Exercise 1.16. Show that h in (Ω) is not necessarily unique.

Proof. a $\square$

Exercise 1.17. Let R be a commutative ring and A an R-algebra. Then a left A-module is the same thing as an R-module M together with a homomorphism of R-algebras

$$A \to \mathrm{End}_{RMod}(M)$$