

# M4P63 Algebra IV

Lectured by Dr John Britnell  
Typed by David Kurniadi Angdinata

Spring 2020

**Syllabus**

## Contents

<b>1</b>	<b>Modules</b>	<b>3</b>
1.1	Modules over rings . . . . .	3
1.2	Exact sequences . . . . .	4
1.3	Projective modules . . . . .	6
1.4	Injective modules . . . . .	8
1.5	Hom . . . . .	10
1.6	The snake lemma . . . . .	12
1.7	Tensor products . . . . .	13

# 1 Modules

## 1.1 Modules over rings

Lecture 1  
Friday  
10/01/20

Let  $R$  be an **associative ring with unity**, that is an abelian group written additively with a multiplication which is associative but not necessarily commutative, with an identity 1 and distributive laws  $a(b+c) = ab+ac$  and  $(a+b)c = ac+bc$ . Then

$$R^* = \{r \in R \mid \exists s \in R, rs = 1 = sr\}$$

is the unit group of  $R$ . If  $R^* = R \setminus \{0\}$  then  $R$  is a **division ring**, or a **skew field**. In the case that  $R$  is commutative,  $R$  is a **field**.

**Example.**

- Fields  $\mathbb{C}$ ,  $\mathbb{R}$ ,  $\mathbb{Q}$ , and  $\mathbb{F}_q$ , the field with  $q = p^a$  elements with  $p$  a prime and  $a \geq 1$ .
- Skew fields  $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$  where  $i^2 = j^2 = k^2 = ijk = -1$ .
- Other rings are polynomial rings  $k[x]$  for  $k$  a field, more generally  $k[x_1, \dots, x_p]$ , and  $\text{Mat}_n k$ , the  $n \times n$  matrices with entries from  $k$ , a field.

**Definition 1.1.** Let  $R$  be a ring. A **left  $R$ -module** is an abelian group  $M$ , written additively, together with a function  $*$  :  $R \times M \rightarrow M$  satisfying

$$r*(m_1 + m_2) = r*m_1 + r*m_2, \quad (r_1 + r_2)*m = r_1*m + r_2*m, \quad (r_1 r_2)*m = r_1*(r_2*m), \quad 1*m = m.$$

We write  $rm$  for  $r*m$ .

**Example.**

- $R$  is itself a left  $R$ -module, with  $*$  as ring multiplication. More generally, let  $I$  be a left ideal of  $R$ , so  $I$  is an additive subgroup, and  $rI \subseteq I$  for all  $r \in R$ . Then  $I$  is an  $R$ -module with  $*$  as ring multiplication.
- Let  $k$  be a field. Then any vector space over  $k$  is a  $k$ -module, and vice versa.
- Any abelian group is a  $\mathbb{Z}$ -module, with  $*$  defined by  $na = a + \dots + a$  for  $n \in \mathbb{Z}^+$  and  $a \in A$ , and  $(-n)a = -(na)$ .
- Let  $k$  be a field. Let  $k^n$  be column vectors. Then  $k^n$  is a left  $\text{Mat}_n k$ -module, with  $*$  as the usual matrix-vector multiplication.
- Let  $M \in \text{Mat}_n k$ . Then we can define a left  $k[x]$ -module structure on  $k^n$  by letting  $x$  act as  $M$  on  $k^n$ . So  $(x^2 + 3x - 2)*v = M^2v + 3Mv - 2v$ .
- Let  $G$  be a group. Any representation of  $G$  over the field  $k$  is a left module for  $k[G]$ , the **group algebra**, a vector space over  $k$  with elements of  $G$  as a basis, with multiplication derived from that of  $G$ .

**Definition 1.2.** A **right  $R$ -module** is defined similarly, with the  $R$ -multiplication on the right, so  $M$  an abelian group under  $+$ , and a map  $M \times R \rightarrow M$  satisfying

$$(m_1 + m_2)*r = m_1*r + m_2*r, \quad m*(r_1 + r_2) = m*r_1 + m*r_2, \quad m*(r_1 r_2) = (m*r_1)*r_2, \quad m*1 = m.$$

Left and right modules are not quite the same. If we amend this definition by putting the ring multiplication on the left, the third axiom becomes  $(r_1 r_2)m = r_2(r_1 m)$ . But in a left module, we have  $(r_1 r_2)m = r_1(r_2 m)$ .

**Definition 1.3.** Let  $R$  be a ring. The **opposite ring**  $R^{\text{op}}$  is  $R$  with a redefined multiplication  $r*s_{R^{\text{op}}} = s*r$ .

It is easy to see that a left  $R$ -module is the same as a right  $R^{\text{op}}$ -module and vice versa. If  $R$  is commutative then  $R = R^{\text{op}}$ .

**Exercise.** Show that  $\text{Mat}_n k \cong \text{Mat}_n k^{\text{op}}$ .

Except where otherwise stated,  $R$ -modules are assumed to be left  $R$ -modules.

**Definition 1.4.** Let  $M_1$  and  $M_2$  be  $R$ -modules. A map  $f : M_1 \rightarrow M_2$  is an  $R$ -module homomorphism if

- $f$  is a group homomorphism, with respect to the  $+$  operation, and
- $f(rm) = rf(m)$ , for  $r \in R$  and  $m \in M$ .

If  $f$  is bijective, then it is an  $R$ -module isomorphism.

**Definition 1.5.** An additive subgroup  $L \leq M$  is a **submodule** if  $rL \leq L$  for  $r \in R$ . In this case we automatically get an  $R$ -module structure on the quotient  $M/L$  with multiplication given by  $r(m + L) = rm + L$ .

**Theorem 1.6** (First isomorphism theorem). *Let  $f : M_1 \rightarrow M_2$  be an  $R$ -module homomorphism. Then  $\text{Im } f \leq M_2$ ,  $\text{Ker } f \leq M_1$ , and  $\text{Im } f \cong M / \text{Ker } f$ .*

The other isomorphism theorems have  $R$ -module versions too.

Let  $S$  be a set. We have a collection of  $R$ -modules  $(M_s)_S$  indexed by  $S$ .

**Definition 1.7.** The **direct product** is

$$\prod_{s \in S} M_s = \{(m_s)_S \mid m_s \in M_s\},$$

with coordinate-wise addition and  $R$ -multiplication, so

$$(m_s)_S + (n_s)_S = (m_s + n_s)_S, \quad r(m_s)_S = (rm_s)_S.$$

If  $M_s = M$  for all  $s \in S$ , then we write  $M^S$  for  $\prod_{s \in S} M_s$ . The **direct sum** is

$$\bigoplus_{s \in S} M_s = \{(m_s)_S \mid \text{all but finitely many coordinates } m_s \text{ are zero}\} \leq \prod_{s \in S} M_s.$$

If  $S$  is finite then the direct product and the direct sum are equal.

**Example.** Let  $M = \mathbb{Z}_2$ , as a  $\mathbb{Z}$ -module, and let  $S = \mathbb{N}$ . Then  $\bigoplus_{s \in \mathbb{N}} \mathbb{Z}_2$  is a countable  $\mathbb{Z}$ -module but  $\prod_{s \in \mathbb{N}} \mathbb{Z}_2 = \mathbb{Z}_2^{\mathbb{N}}$  is uncountable.

When  $|S| = 2$ , generally we write  $M_1 \oplus M_2$  for the direct sum or product. There are natural injective maps

$$\begin{aligned} \iota_A : A &\longrightarrow A \oplus B & \iota_B : B &\longrightarrow A \oplus B \\ a &\longmapsto (a, 0) & b &\longmapsto (0, b) \end{aligned},$$

and surjective maps

$$\begin{aligned} \pi_A : A \oplus B &\longrightarrow A & \pi_B : A \oplus B &\longrightarrow B \\ (a, b) &\longmapsto a & (a, b) &\longmapsto b \end{aligned}.$$

## 1.2 Exact sequences

**Definition 1.8.** Suppose we have a sequence of  $R$ -modules

$$\dots \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \dots,$$

with maps  $f_n : M_n \rightarrow M_{n+1}$ . Say the sequence is **exact at  $M_n$**  if

$$\text{Im } f_{n-1} = \text{Ker } f_n.$$

The sequence is **exact** if it is exact everywhere. A **short exact sequence** is an exact sequence

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0.$$

Note that  $\alpha$  is injective and  $\beta$  is surjective. The first isomorphism theorem implies that  $B / \text{Im } \alpha \cong C$ , where  $\text{Im } \alpha \cong A$ . An easy case is

$$B \cong A \oplus C,$$

with  $\text{Im } \alpha = A \oplus 0$  and  $\text{Im } \beta = C$ , so  $\alpha = \iota_A$  and  $\beta = \pi_B$ . We say that the short exact sequence **splits** in this case.

Lecture 2  
Monday  
13/01/20

**Example.** A non-split short exact sequence of  $\mathbb{Z}$ -modules, or abelian groups, is

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0.$$

**Proposition 1.9.** A short exact sequence

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

is split if and only if there exists an  $R$ -module homomorphism  $\sigma : C \rightarrow B$  such that  $\beta \circ \sigma = \text{id}_C$ .

Such a  $\sigma$  is called a **section** of  $\beta$ .

*Proof.*

$\Rightarrow$  Suppose that the short exact sequence is split. So assume  $B = A \oplus C$ , with  $\alpha = \iota_A$  and  $\beta = \pi_C$ . Now  $\iota_C$  is a section for  $\beta$ .

$\Leftarrow$  For the converse, suppose that  $\sigma$  is a section for  $\beta$ . We want  $f : A \oplus C \xrightarrow{\sim} B$  such that  $f \circ \iota_A = \alpha$  and  $\beta \circ f = \pi_C$ , so

$$\begin{array}{ccccccc} & & & A \oplus C & & & \\ & \nearrow \iota_A & & \downarrow f & \nwarrow \pi_C & & \\ 0 & \longrightarrow & A & & C & \longrightarrow & 0 \\ & \searrow \alpha & & \downarrow \beta & \nearrow & & \\ & & & B & & & \end{array}$$

Define

$$\begin{aligned} f : A \times C &\longrightarrow B \\ (a, c) &\longmapsto \alpha(a) + \sigma(c) \end{aligned}$$

Need to check the following.

- $f$  is an  $R$ -module homomorphism. <sup>1</sup>
- $f$  is injective. Suppose  $f(a, c) = 0$ . Then  $\alpha(a) + \sigma(c) = 0$ . Now  $\alpha(a) \in \text{Im } \alpha = \text{Ker } \beta$ , so  $\beta(\alpha(a) + \sigma(c)) = \beta(\sigma(c)) = c$ . Since  $\alpha(a) + \sigma(c) = 0$ , we have  $c = 0$ . Hence  $\alpha(a) = 0$ , and so  $a = 0$  since  $\alpha$  is injective. We have shown that  $f$  is injective.
- $f$  is surjective. Let  $b \in B$ . Let  $c = \beta(b)$ . We have  $(\beta \circ \sigma)(c) = c = \beta(b)$ , so  $b - \sigma(c) \in \text{Ker } \beta = \text{Im } \alpha$ . So there exists  $a \in A$  with  $\alpha(a) = b - \sigma(c)$ . Then  $b = \alpha(a) + \sigma(c) = f(a, c)$ .
- $f \circ \iota_A = \alpha$  and  $\beta \circ f = \pi_C$ . Immediate from the construction of  $f$ .

□

**Proposition 1.10.** The short exact sequence

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

is split if and only if there exists  $\rho : B \rightarrow A$  such that  $\rho \circ \alpha = \text{id}_A$ .

Such a  $\rho$  is a **retraction** of  $\alpha$ .

*Proof.*

$\Rightarrow$  Once again, if the short exact sequence is split then the existence of  $\rho$  is clear.

$\Leftarrow$  Suppose that  $\rho$  is a retraction for  $\alpha$ . We define  $f : B \xrightarrow{\sim} A \oplus C$  such that  $f \circ \alpha = \iota_A$  and  $\pi_C \circ f = \beta$ . Do this by

$$\begin{aligned} g : B &\longrightarrow A \oplus C \\ b &\longmapsto (\rho(b), \beta(b)) \end{aligned}$$

Details are omitted.

□

---

<sup>1</sup>Exercise

### 1.3 Projective modules

**Definition 1.11.** An  $R$ -module  $M$  is **projective** if any surjective map  $\beta : B \rightarrow M$  has a section. In other words, any short exact sequence

$$0 \rightarrow A \rightarrow B \rightarrow M \rightarrow 0$$

splits.

**Example.** The  $R$ -module  $R$  is projective. Let

$$0 \rightarrow A \rightarrow B \xrightarrow{\beta} R \rightarrow 0$$

be a short exact sequence. Since  $\beta$  is surjective, there exists  $b \in B$  such that  $\beta(b) = 1$ . Now for all  $r \in R$ ,  $\beta(rb) = r$ . Now define

$$\begin{array}{ccc} \sigma & : & R \longrightarrow B \\ & & r \longmapsto rb \end{array}.$$

Then  $\sigma$  is a section for  $\beta$ .

**Proposition 1.12.** An  $R$ -module  $M$  is projective if and only if whenever  $\beta : B \rightarrow C$  is surjective, and  $f : M \rightarrow C$ , there exists  $g : M \rightarrow B$  such that  $f = \beta \circ g$ , so

$$\begin{array}{ccccccc} & & & & M & & \\ & & & & \downarrow f & & \\ & & g & \swarrow & & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{\beta} & C \longrightarrow 0 \end{array}.$$

Such a  $g$  is called a **lift** of  $f$ .

*Proof.*

$\Leftarrow$  Suppose that whenever  $\beta : B \rightarrow C$  is surjective and  $f : M \rightarrow C$  then there exists  $g : M \rightarrow B$  with  $f = \beta \circ g$ . Suppose  $\beta : B \rightarrow M$  is a surjective map. Define  $f : M \rightarrow M$  to be  $\text{id}_M$ . Then there exists  $g : M \rightarrow B$  such that  $f = \beta \circ g$ , so  $\text{id}_M = \beta \circ g$ . So  $g$  is a section for  $\beta$ , and so  $M$  is projective.

$\Rightarrow$  For the converse, suppose  $\beta : B \rightarrow C$  is surjective, and  $f : M \rightarrow C$ . We construct a module  $X$  to complete a commuting square

$$\begin{array}{ccc} X & \xrightarrow{\epsilon} & M \\ \delta \downarrow & & \downarrow f \\ B & \xrightarrow{\beta} & C \end{array}.$$

Let  $X$  be the submodule of  $B \oplus M$  defined by

$$X = \{(b, m) \mid \beta(b) = f(m)\}.$$

The maps  $\delta$  and  $\epsilon$  are just  $\pi_B$  and  $\pi_M$  respectively, in their restrictions to  $X$ . It is clear that  $X \leq B \oplus M$ , and that the square above commutes. Now suppose that  $M$  is projective. Since  $\beta$  is surjective, we see that for all  $m \in M$  there exists  $b \in B$  with  $\beta(b) = f(m)$ . It follows that  $\epsilon : X \rightarrow M$  is surjective. So  $\epsilon$  has a section  $\sigma : M \rightarrow X$ . Define  $g = \delta \circ \sigma : M \rightarrow B$ , so

$$\begin{array}{ccc} X & \xrightarrow{\epsilon} & M \\ \delta \downarrow & \swarrow \sigma & \downarrow f \\ B & \xrightarrow{\beta} & C \end{array}.$$

Since  $\beta \circ \delta = f \circ \epsilon$ , for all  $m \in M$  we have

$$(\beta \circ g)(m) = (\beta \circ \delta \circ \sigma)(m) = (f \circ \epsilon \circ \sigma)(m) = (f \circ \text{id}_M)(m) = f(m).$$

So  $\beta \circ g = f$  as required.

□

Such an  $X$  is the **pullback** of  $\beta$  and  $f$ , and there is a short exact sequence

$$0 \rightarrow A \rightarrow X \rightarrow M \rightarrow 0.$$

**Definition 1.13.** An  $R$ -module  $M$  is **free** if  $M$  is a direct sum of copies of  $R$ , so

$$M = \bigoplus_{s \in S} R.$$

A **basis** for a module  $M$  is a set  $T$  of elements such that every element  $m \in M$  has a unique expression as

$$m = \sum_{i=1}^m r_i t_i, \quad r_i \in R, \quad t_i \in T.$$

If  $M = \bigoplus_{s \in S} R$ , then  $M$  has a basis consisting of elements with exactly one coordinate one, and the rest zero. On the other hand, if  $M$  has a basis  $T$  then it is straightforward to show that  $M \cong \bigoplus_{t \in T} R$ .

**Proposition 1.14.** Let  $F$  be a free  $R$ -module with basis  $T$ . Let  $M$  be some  $R$ -module, and let  $\psi : T \rightarrow M$  be a set map. Then  $\psi$  extends uniquely to a  $R$ -module homomorphism  $\psi : F \rightarrow M$ .

*Proof.* Each element of  $F$  has a unique expression as  $\sum_i r_i t_i$  for  $r_i \in R$  and  $t_i \in T$ . Now define

$$\begin{array}{ccc} \psi & : & F \longrightarrow M \\ & & \sum_i r_i t_i \longmapsto \sum_i r_i \psi(t_i) \end{array}.$$

It is easy to check that this respects  $+$  and  $R$ -multiplication. □

**Proposition 1.15.** A module  $M$  is projective if and only if there exists  $N$  such that  $M \oplus N$  is free, so projective modules are direct summands of free modules.

*Proof.*

$\implies$  Suppose  $M$  is projective. Let  $F$  be the free module with basis  $\{b_m \mid m \in M\}$ . Now the map  $b_m \mapsto m$  extends to an  $R$ -module homomorphism  $F \rightarrow M$ , which is clearly surjective. Then if  $K = \text{Ker } \psi$ , we have a short exact sequence

$$0 \rightarrow K \rightarrow F \xrightarrow{\psi} M \rightarrow 0.$$

Since  $M$  is projective, there is a section  $\sigma$  for  $\psi$ , and so the short exact sequence splits, and  $F \cong K \oplus M$ .

$\Leftarrow$  Suppose that  $M \oplus N = F$ , a free module with basis  $T$ . Suppose  $\beta : B \rightarrow C$  is surjective, and that  $f : M \rightarrow C$ . Note that  $f \circ \pi_M : F \rightarrow C$ . For each  $t \in T$ , let  $b_t \in B$  be such that  $\beta(b_t) = (f \circ \pi_M)(t)$ . The set map

$$\begin{array}{ccc} T & \longrightarrow & B \\ t & \longmapsto & b_t \end{array}$$

extends to a homomorphism  $\hat{g} : F \rightarrow B$ . Now define  $g : M \rightarrow B$  by  $g = \hat{g} \circ \iota_M$ . We need to show  $f = \beta \circ g$ . Take  $m \in M$ . Then  $\iota_M(m) = (m, 0) \in F$  can be written as  $\sum_i r_i t_i$ , where  $t_i \in T$  and  $r_i \in R$ . Applying  $\pi_M$ ,  $m = \sum_i r_i m_{t_i}$ . Then

$$g(m) = (\hat{g} \circ \iota_M)(m) = \hat{g}\left(\sum_i r_i t_i\right) = \sum_i r_i b_{t_i}.$$

So

$$(\beta \circ g)(m) = \beta\left(\sum_i r_i b_{t_i}\right) = \sum_i r_i \beta(b_{t_i}) = \sum_i r_i f(m_{t_i}) = f\left(\sum_i r_i m_{t_i}\right) = f(m).$$

Hence  $\beta \circ g = f$ . So  $M$  is projective. □

Lecture 4  
Friday  
17/01/20

## 1.4 Injective modules

**Definition 1.16.** Let  $M$  be an  $R$ -module. Then  $M$  is **injective** if whenever  $\alpha : M \rightarrow B$  is an injective map, it has a retraction  $\rho : B \rightarrow M$ , so  $\rho \circ \alpha = \text{id}_M$ . Equivalently, every short exact sequence

$$0 \rightarrow M \rightarrow B \rightarrow C \rightarrow 0$$

splits.

**Example.** Let  $k$  be a field. Then  $k$ -modules are vector spaces. Every  $k$ -module is injective. Suppose  $M$  and  $N$  are  $k$ -vector spaces and  $\alpha : M \rightarrow N$  is a injective map. Then  $\text{Im } \alpha$  is a submodule, or subspace, of  $N$ . Take a basis for  $\text{Im } \alpha$ , and extend to a basis for  $N$ . The basis vectors not in  $\text{Im } \alpha$  form a basis for a complementary subspace  $U$ , so  $N = \text{Im } \alpha \oplus U$ . Now  $\pi_{\text{Im } \alpha}$  is surjective, and  $\alpha : M \rightarrow \text{Im } \alpha$  is an isomorphism. This gives a retraction  $N \rightarrow M$ .

If  $R$  is a general ring, the module  $R$  need not be injective.

**Example.** Let  $R = \mathbb{Z}$ . Then  $R$ -modules are abelian groups. There exists an injective  $\alpha : \mathbb{Z} \rightarrow \mathbb{Q}$ . But  $\mathbb{Z}$  is not a quotient of  $\mathbb{Q}$ ,<sup>2</sup> so no retraction exists for  $\alpha$ .

**Proposition 1.17.** An  $R$ -module  $M$  is injective if and only if whenever  $\alpha : A \rightarrow B$  is injective, and  $f : A \rightarrow M$ , there exists  $g : B \rightarrow M$  such that  $f = g \circ \alpha$ .

*Proof.*

$\Leftarrow$  Suppose that whenever  $\alpha : A \rightarrow B$  is injective, and  $f : A \rightarrow M$ , there exists  $g : B \rightarrow M$  such that  $f = g \circ \alpha$ . Suppose that  $\alpha : M \rightarrow B$  is injective. We have a map  $M \rightarrow M$ , namely  $\text{id}_M$ . There exists  $g : B \rightarrow M$  such that  $\text{id}_M = g \circ \alpha$ . So  $g$  is a retraction for  $\alpha$ , and so  $M$  is injective.

$\Rightarrow$  For the converse, suppose  $\alpha : A \rightarrow B$  is injective, and  $M$  is an injective module, with  $f : A \rightarrow M$ . We define a module  $Y$  completing a square

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ f \downarrow & & \downarrow \delta \\ M & \xrightarrow{\epsilon} & Y \end{array}$$

with  $\epsilon \circ f = \delta \circ \alpha$ . Let  $Y$  be a quotient of  $B \oplus M$ , by the kernel

$$K = \{(\alpha(a), -f(a)) \mid a \in A\}.$$

Let  $\gamma : B \oplus M \rightarrow (B \oplus M)/K$  be the canonical quotient map. Then we define  $\delta = \gamma \circ \iota_B$  and  $\epsilon = \gamma \circ \iota_M$ . By construction, we have

$$\begin{aligned} (\epsilon \circ f)(a) &= (\gamma \circ \iota_M \circ f)(a) = \gamma(0, f(a)) = (0, f(a)) + K \\ &= (\alpha(a), 0) + K = \gamma(\alpha(a), 0) = (\gamma \circ \iota_B \circ \alpha)(a) = (\delta \circ \alpha)(a). \end{aligned}$$

Hence  $\epsilon \circ f = \delta \circ \alpha$ . Claim that  $\epsilon$  is injective. Suppose  $\epsilon(m) = 0$ . Then  $\iota_M(m) \in K$ , so  $(0, m) = (\alpha(a), -f(a))$  for some  $a \in A$ . But  $\alpha(a) = 0$  implies that  $a = 0$ , and so  $m = -f(0) = 0$ . Since  $M$  is injective,  $\epsilon$  has a retraction  $\rho : Y \rightarrow M$ . Define  $g : B \rightarrow M$  by  $g = \rho \circ \delta$ , so

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ f \downarrow & \swarrow g & \downarrow \delta \\ M & \xleftarrow{\rho} & Y \\ & \searrow \epsilon & \end{array}$$

We know that  $(\epsilon \circ f)(a) = (\delta \circ \alpha)(a)$  for all  $a \in A$ . So

$$f(a) = (\text{id}_M \circ f)(a) = (\rho \circ \epsilon \circ f)(a) = (\rho \circ \delta \circ \alpha)(a) = (g \circ \alpha)(a),$$

so  $f = g \circ \alpha$  as required. □

---

<sup>2</sup>Exercise



We know that projectives are direct summands of free modules. We might hope for a dual version of this for injective modules. But there is no straightforward way of doing this.

**Proposition 1.18** (Baer's criterion for injectivity). *Let  $M$  be an  $R$ -module. Then  $M$  is injective if and only if every  $R$ -module map  $f : I \rightarrow M$ , where  $I$  is a left ideal of  $R$ , has the form  $f(x) = xm$  for some  $m \in M$ . Equivalently, every map  $I \rightarrow M$  extends to a map  $R \rightarrow M$ .*

Why are these two conditions equivalent? If  $f(x) = xm$  for  $x \in I$ , then we can extend  $f$  to  $R$  by  $f(r) = rm$ . Conversely, suppose that  $f : I \rightarrow M$  extends to  $f^+ : R \rightarrow M$ . Let  $m = f^+(1)$ . Then for all  $r \in R$ ,  $f^+(r) = rm$ , and so  $f(x) = xm$  for  $x \in I$ .

*Proof.* The proof requires Zorn's lemma. Let  $X$  be a non-empty set, partially ordered by  $\leq$ . If every chain, or totally ordered subset, in  $X$  has an upper bound in  $X$ , then  $X$  has a maximal element.

$\Leftarrow$  Suppose  $\alpha : A \rightarrow B$ , where  $\alpha$  is injective. Suppose  $f : A \rightarrow M$ . We want to show there exists  $g : B \rightarrow M$  such that  $f = g \circ \alpha$ . We have  $\text{Im } \alpha \leq B$ . Define

$$X = \{(L, h) \mid \text{Im } \alpha \leq L \leq B, h : L \rightarrow M, f = h \circ \alpha\}.$$

Note that  $X \neq \emptyset$  since  $(\text{Im } \alpha, f \circ \alpha^{-1})$  is in it. Define  $\leq$  on  $X$  by  $(L_1, h_1) \leq (L_2, h_2)$  if  $L_1 \leq L_2$  and  $h_2$  extends  $h_1$ , so  $h_2|_{L_1} = h_1$ . Suppose  $\{(L_s, h_s) \mid s \in S\}$  is a chain in  $X$ . Set  $L = \bigcup_{s \in S} L_s$ . Then  $\text{Im } \alpha \leq L \leq B$ . Define

$$\begin{aligned} h &: L \longrightarrow M \\ l &\longmapsto h_s(l), \quad l \in L_s. \end{aligned}$$

This does not depend on the choice of  $s$ . Then  $(L, h)$  is an upper bound for the chain  $\{(L_s, h_s) \mid s \in S\}$ . Hence  $X$  has a maximal element,  $(L_0, h_0)$ . We want to show that  $L_0 = B$ . Then we may set  $g = h_0$ . Suppose that  $L_0 \neq B$ . Let  $b \in B \setminus L_0$ . Note that  $Rb \leq B$ . Consider

$$L_0 + Rb = \{l + rb \mid l \in L_0, r \in R\} \leq B.$$

We would like to extend  $h_0$  to  $h_0^+$  by specifying an image for  $h_0^+(b)$ . The problem is that  $Rb \cap L_0$  may not be  $\{0\}$ , and if  $rb \in L_0$  then we require  $rh_0^+(b) = h_0(rb)$ , otherwise  $h_0^+$  will not be well-defined. Note that  $I = \{r \in R \mid rb \in L_0\}$  is a left ideal for  $R$ . Suppose that  $M$  has the condition from Baer's criterion, so every map  $I \rightarrow M$  has the form  $x \mapsto xm$  for some  $m \in M$ . Note that  $\{xb \mid x \in I\}$  is a submodule of  $L_0$ . Define a map

$$\begin{aligned} \delta &: I \longrightarrow M \\ x &\longmapsto h_0(xb). \end{aligned}$$

This is an  $R$ -module homomorphism. So  $\delta(x) = xm$  for some  $m \in M$ . Hence  $h_0(xb) = xm$  for all  $x \in I$ . So we can safely define  $h_0^+(b) = m$ . Now  $(L_0 + Rb, h_0^+) \in X$ , and  $(L_0, h_0) < (L_0 + Rb, h_0^+)$ , which contradicts the maximality of  $(L_0, h_0)$ . Hence  $L_0 = B$ , and we are done.

$\Rightarrow$  The converse is left as an exercise. <sup>3</sup>

□

### Example.

- Suppose  $R$  is a field. Then the only ideals of  $R$  are zero and  $R$ . Any map  $0 \rightarrow M$ , for  $M$  an  $R$ -module, can be extended to the zero map  $R \rightarrow M$ . Hence any  $R$ -module is injective.
- Let  $\mathbb{Z}$  be a module for itself. The ideals of  $\mathbb{Z}$  are  $k\mathbb{Z}$  for  $k \in \mathbb{Z}$ . Define

$$\begin{aligned} f &: k\mathbb{Z} \longrightarrow \mathbb{Z} \\ km &\longmapsto m. \end{aligned}$$

If  $k \neq 0, \pm 1$ , then  $f(k) = 1$ , and so  $f(x) \neq xm$  for  $m \in \mathbb{Z}$ , since one is not divisible by  $k$  in  $\mathbb{Z}$ . So Baer's criterion fails, and  $\mathbb{Z}$  is not injective. We already knew that  $\mathbb{Z} \rightarrow \mathbb{Q}$  has no retraction.

- $\mathbb{Q}$  is injective as a  $\mathbb{Z}$ -module. Suppose we have a map  $f : k\mathbb{Z} \rightarrow \mathbb{Q}$ . Let  $q = f(k)$ . Then  $f(kt) = qt = (q/k)kt$ . So  $f(x) = x(q/k)$  for all  $x$ , so  $\mathbb{Q}$  satisfies Baer's criterion.

---

<sup>3</sup>Exercise

## 1.5 Hom

Let  $A$  and  $B$  be two  $R$ -modules.

**Definition 1.19.** Define

$$\text{Hom}_R(A, B) = \{R\text{-module homomorphisms } A \rightarrow B\}.$$

We can define a natural addition on  $\text{Hom}_R(A, B)$  by defining  $f_1 + f_2$  by

$$(f_1 + f_2)(a) = f_1(a) + f_2(a), \quad f_1, f_2 \in \text{Hom}_R(A, B).$$

This gives  $\text{Hom}_R(A, B)$  the structure of an abelian group. Why does  $\text{Hom}_R(A, B)$  not carry an  $R$ -module structure in general? The only obvious candidate for  $rf$  is

$$(rf)(a) = rf(a) = f(ra), \quad r \in R, \quad f \in \text{Hom}_R(A, B).$$

Now suppose  $s \in R$ . We have  $(rf)(sa) = rf(sa) = rsf(a)$ . But for  $rf$  to be a homomorphism, we would need  $(rf)(sa) = s(rf)(a) = sfr(a)$ . If  $R$  is non-commutative, then  $rs$  may not be  $sr$ , and so  $rf$  is not an  $R$ -module homomorphism in general. Clearly, however, if  $R$  is commutative then  $rf$  is an  $R$ -module homomorphism, and  $\text{Hom}_R(A, B)$  has an  $R$ -module structure. The following are observations.

**Proposition 1.20.** Suppose  $A, A_1, A_2, B, B_1, B_2, M$  are  $R$ -modules, and  $\alpha : A \rightarrow B$ .

- $\text{Hom}_R(A_1 \oplus A_2, B) \cong \text{Hom}_R(A_1, B) \oplus \text{Hom}_R(A_2, B)$ .
- $\text{Hom}_R(A, B_1 \oplus B_2) \cong \text{Hom}_R(A, B_1) \oplus \text{Hom}_R(A, B_2)$ .
- Then we can define

$$\begin{array}{ccc} \alpha_* : \text{Hom}_R(M, A) & \longrightarrow & \text{Hom}_R(M, B) \\ f & \longmapsto & \alpha \circ f \end{array}, \quad f : M \rightarrow A.$$

- We can also define

$$\begin{array}{ccc} \alpha^* : \text{Hom}_R(B, M) & \longrightarrow & \text{Hom}_R(A, M) \\ g & \longmapsto & g \circ \alpha \end{array}, \quad g : B \rightarrow M.$$

Thus  $\text{Hom}$  is a bifunctor between the category of  $R$ -modules and the category of abelian groups, additive in both arguments, covariant in the second argument and contravariant in the first argument.

- Bi means  $\text{Hom}$  takes two arguments.
- Functor means that homomorphisms between  $R$ -modules turn into abelian group homomorphisms.
- Covariant means the homomorphism goes in the same direction.
- Contravariant means the direction gets reversed.
- Additive in both arguments means  $\text{Hom}$  respects direct sums.

**Proposition 1.21.** Suppose  $\alpha : A \rightarrow B$  is surjective. Then  $\alpha^* : \text{Hom}_R(B, M) \rightarrow \text{Hom}_R(A, M)$  is injective.

*Proof.* Suppose  $f_1, f_2 : B \rightarrow M$  are such that  $\alpha^*(f_1) = \alpha^*(f_2)$ . Then  $f_1 \circ \alpha = f_2 \circ \alpha$ , so  $(f_1 \circ \alpha)(a) = (f_2 \circ \alpha)(a)$  for all  $a \in A$ . Let  $b \in B$ . Then  $b = \alpha(a)$  for some  $a$ , since  $\alpha$  is surjective, so  $f_1(b) = (f_1 \circ \alpha)(a) = (f_2 \circ \alpha)(a) = f_2(b)$ , so  $f_1 = f_2$ .  $\square$

**Proposition 1.22.** Suppose  $\alpha : A \rightarrow B$  is injective. Then  $\alpha_* : \text{Hom}_R(M, A) \rightarrow \text{Hom}_R(M, B)$  is injective.

*Proof.* Suppose  $f_1, f_2 : M \rightarrow A$ , and  $\alpha_*(f_1) = \alpha_*(f_2)$ . Then  $\alpha \circ f_1 = \alpha \circ f_2$ , so  $(\alpha \circ f_1)(m) = (\alpha \circ f_2)(m)$  for all  $m \in M$ . But  $\alpha$  is injective, so this implies  $f_1(m) = f_2(m)$  for all  $m \in M$ .  $\square$

**Proposition 1.23.** *Suppose*

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

*is a short exact sequence of  $R$ -modules. Then we have an exact sequence*

$$0 \rightarrow \operatorname{Hom}_R(C, M) \xrightarrow{\beta^*} \operatorname{Hom}_R(B, M) \xrightarrow{\alpha^*} \operatorname{Hom}_R(A, M).$$

*Proof.* This is exact at  $\operatorname{Hom}_R(C, M)$ , since  $\beta^*$  is injective. Claim that the sequence is also exact at  $\operatorname{Hom}_R(B, M)$ , so it is an exact sequence. It is not necessarily a short exact sequence since  $\alpha^*$  is not generally surjective. Let  $g : B \rightarrow M$ . We have

$$g \in \operatorname{Ker} \alpha^* \iff \alpha^*(g) = 0 \iff g \circ \alpha = 0 \iff g(\alpha(A)) = 0 \iff \operatorname{Im} \alpha \leq \operatorname{Ker} g \iff \operatorname{Ker} \beta \leq \operatorname{Ker} g,$$

Then  $g \in \operatorname{Ker} \alpha^*$  if and only if for all  $b_1, b_2 \in B$ ,  $\beta(b_1) = \beta(b_2)$  implies that  $g(b_1) = g(b_2)$ , which is if and only if

$$\begin{array}{ccc} f & : & C \longrightarrow M \\ & c & \longmapsto g(b) \end{array}, \quad \beta(b) = c$$

is well-defined, since  $\beta$  is surjective, and  $f$  is an  $R$ -module homomorphism. Thus

$$g \in \operatorname{Ker} \alpha^* \iff \exists f \in \operatorname{Hom}_R(C, M), \beta^*(f) = g \iff g \in \operatorname{Im} \beta^*.$$

Hence  $\operatorname{Ker} \alpha^* = \operatorname{Im} \beta^*$ . So the sequence is exact at  $\operatorname{Hom}_R(B, M)$ . □

**Example.** These examples show that  $\alpha : A \rightarrow B$  is injective does not imply  $\alpha^* : \operatorname{Hom}_R(B, M) \rightarrow \operatorname{Hom}_R(A, M)$  is surjective.

Lecture 7  
Friday  
24/01/20

- The inclusion  $\alpha : \mathbb{Z} \rightarrow \mathbb{Q}$  is a  $\mathbb{Z}$ -module homomorphism. Let  $M = \mathbb{Z}$ . Then we get  $\alpha^* : \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) \rightarrow \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$ . Then  $\alpha$  is injective, but  $\alpha^*$  is not surjective. Why is this? In fact  $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$ . Suppose

$$\begin{array}{ccc} f & : & \mathbb{Q} \longrightarrow \mathbb{Z} \\ & 1 & \longmapsto k \neq 0 \end{array}.$$

Suppose  $p \nmid k$ . Then there is no possible image for  $1/p \in \mathbb{Q}$ , since we would require  $pf(1/p) = f(1) = k$ . But  $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$ , so  $\alpha^*$  is not surjective.

- Let  $\alpha : k\mathbb{Z} \rightarrow \mathbb{Z}$  be the inclusion, so  $\alpha$  is injective and not surjective. Let  $M = \mathbb{Z}$ . So we get  $\alpha^* : \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \rightarrow \operatorname{Hom}_{\mathbb{Z}}(k\mathbb{Z}, \mathbb{Z})$ . Suppose that  $g \in \operatorname{Im} \alpha^*$ . Then  $g = f \circ \alpha$ , where  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ . Then  $g(k) = f(k) = kf(1)$ , so  $\operatorname{Im} g \leq k\mathbb{Z}$ . But there exists  $g \in \operatorname{Hom}_{\mathbb{Z}}(k\mathbb{Z}, \mathbb{Z})$  such that  $g(k) = 1$ . So this  $g \notin \operatorname{Im} \alpha^*$ , so  $\alpha^*$  is not surjective.

**Proposition 1.24.** *Let*

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

*be exact. Then*

$$0 \rightarrow \operatorname{Hom}_R(M, A) \xrightarrow{\alpha_*} \operatorname{Hom}_R(M, B) \xrightarrow{\beta_*} \operatorname{Hom}_R(M, C)$$

*is exact.*

*Proof.* We already know that  $\alpha$  injective implies that  $\alpha_*$  is injective, so the sequence is exact at  $\operatorname{Hom}_R(M, A)$ . We show that  $\operatorname{Ker} \beta_* = \operatorname{Im} \alpha_*$ . Suppose  $g \in \operatorname{Hom}_R(M, B)$ . Then

$$g \in \operatorname{Ker} \beta_* \iff (\beta \circ g)(M) = 0 \iff \operatorname{Im} g \leq \operatorname{Ker} \beta \iff \operatorname{Im} g \leq \operatorname{Im} \alpha.$$

Note there exists  $\alpha^{-1} : \operatorname{Im} \alpha \rightarrow A$ . If  $\operatorname{Im} g \leq \operatorname{Im} \alpha$ , then  $\alpha^{-1} \circ g : M \rightarrow A$ . If  $f = \alpha^{-1} \circ g$ , then  $\alpha \circ f = g$ , so  $g \in \operatorname{Im} \alpha_*$ . Conversely, if  $g \in \operatorname{Im} \alpha_*$ , then  $g = \alpha \circ f$  for some  $f \in \operatorname{Hom}_R(M, A)$  and so  $\operatorname{Im} g \leq \operatorname{Im} \alpha$ . So

$$g \in \operatorname{Ker} \beta_* \iff \operatorname{Im} g \leq \operatorname{Im} \alpha \iff g \in \operatorname{Im} \alpha_*.$$

Hence  $\operatorname{Ker} \beta_* = \operatorname{Im} \alpha_*$ . So the sequence is exact at  $\operatorname{Hom}_R(M, B)$ . □

**Example.** These examples show that  $\beta : B \rightarrow C$  is surjective does not imply  $\beta_* : \text{Hom}_R(M, B) \rightarrow \text{Hom}_R(M, C)$  is surjective.

- Let

$$\begin{array}{ccc} \beta & : & \sum_{q \in \mathbb{Q}} \mathbb{Z} \longrightarrow \mathbb{Q} \\ & & e_q \longmapsto q \end{array}.$$

In general  $\beta : \sum_{m \in M} R \rightarrow M$  defined by mapping the basis vector  $e_m$  to  $m$ , is a surjective homomorphism, so  $\beta$  is surjective. Let  $M = \mathbb{Q}$ . So we get  $\beta_* : \text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \sum_{q \in \mathbb{Q}} \mathbb{Z}) \rightarrow \text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q})$ . Claim that  $\text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \sum_{q \in \mathbb{Q}} \mathbb{Z})$  is trivial. Suppose  $f : \mathbb{Q} \rightarrow \sum_{q \in \mathbb{Q}} \mathbb{Z}$  is not zero. Suppose  $f(q_0) \neq 0$ . Then there exist  $q_1, \dots, q_t \in \mathbb{Q}$  and  $a_1, \dots, a_t \in \mathbb{Z}$  such that  $f(q_0) = \sum_{i=1}^t a_i e_{q_i}$ . Now the projection of  $\sum_{q \in \mathbb{Q}} \mathbb{Z}$  onto  $\mathbb{Z}e_{q_1}$  is a non-trivial  $\mathbb{Z}$ -module homomorphism. But  $\mathbb{Z}e_{q_1} \cong \mathbb{Z}$ , and so no non-trivial map  $\mathbb{Q} \rightarrow \mathbb{Z}e_{q_1}$  exists. But  $\text{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q})$  is not trivial, so  $\beta_*$  is not surjective.

- Let

$$0 \rightarrow \mathbb{Z}_2 \rightarrow \mathbb{Z}_4 \rightarrow \mathbb{Z}_2 \rightarrow 0$$

be a short exact sequence of  $\mathbb{Z}$ -modules. Then we have

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) & \xrightarrow{\alpha_*} & \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_4) & \xrightarrow{\beta_*} & \text{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) \\ & & \text{IR} & & \text{IR} & & \text{IR} \\ & & \mathbb{Z}_2 & & \mathbb{Z}_2 & & \mathbb{Z}_2 \end{array}.$$

But there is no short exact sequence of abelian groups

$$0 \rightarrow \mathbb{Z}_2 \rightarrow \mathbb{Z}_2 \rightarrow \mathbb{Z}_2 \rightarrow 0,$$

and so  $\beta_*$  cannot be surjective.

**Proposition 1.25.** Let  $M$  be an  $R$ -module. Then  $M$  is injective if and only if for every injective map  $\alpha : A \rightarrow B$ , we get  $\alpha^* : \text{Hom}_R(B, M) \rightarrow \text{Hom}_R(A, M)$  is surjective.

*Proof.*  $M$  is injective if and only if for all injective  $\alpha : A \rightarrow B$ , for all  $f \in \text{Hom}_R(A, M)$ , there exists  $g \in \text{Hom}_R(B, M)$  such that  $f = g \circ \alpha$ , so  $f = \alpha^*(g)$ . This is if and only if for all injective  $\alpha : A \rightarrow B$ ,  $f \in \text{Im } \alpha^*$  for all  $f \in \text{Hom}_R(A, M)$ , which is if and only if  $\alpha^*$  is surjective.  $\square$

**Proposition 1.26.** Let  $M$  be an  $R$ -module. Then  $M$  is projective if and only if whenever  $\beta : B \rightarrow C$  is surjective, the map  $\beta_* : \text{Hom}_R(M, B) \rightarrow \text{Hom}_R(M, C)$  is surjective.

*Proof.*  $M$  is projective if and only if whenever  $\beta : B \rightarrow C$  is surjective, and  $f \in \text{Hom}_R(M, C)$ , there exists  $g \in \text{Hom}_R(M, B)$  such that  $f = \beta \circ g$ . This is if and only if whenever  $\beta : B \rightarrow C$  is surjective, and  $f \in \text{Hom}_R(M, C)$ , then  $f \in \text{Im } \beta_*$ , which is if and only if  $\beta_*$  is surjective.  $\square$

## 1.6 The snake lemma

Let  $\alpha : A \rightarrow B$  be an  $R$ -module homomorphism. The **cokernel** of  $\alpha$  is  $B/\text{Im } \alpha$ , written  $\text{Coker } \alpha$ . The sequence

$$0 \rightarrow \text{Ker } \alpha \rightarrow A \xrightarrow{\alpha} B \rightarrow \text{Coker } \alpha \rightarrow 0$$

is exact.

**Lemma 1.27** (The snake lemma). Suppose we have a commutative diagram

$$\begin{array}{ccccccc} A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ \downarrow f & & \downarrow g & & \downarrow h & & \\ 0 & \longrightarrow & X & \xrightarrow{\phi} & Y & \xrightarrow{\psi} & Z \end{array},$$

where the rows are exact. Then we obtain an exact sequence

$$\text{Ker } f \xrightarrow{\bar{\alpha}} \text{Ker } g \xrightarrow{\bar{\beta}} \text{Ker } h \xrightarrow{\delta} \text{Coker } f \xrightarrow{\bar{\phi}} \text{Coker } g \xrightarrow{\bar{\psi}} \text{Coker } h.$$

Lecture 8  
Monday  
27/01/20

*Proof.*

- The maps  $\bar{\alpha} : \text{Ker } f \rightarrow \text{Ker } g$  and  $\bar{\beta} : \text{Ker } g \rightarrow \text{Ker } h$  are obtained simply by restricting  $\alpha$  and  $\beta$  respectively. Observe that if  $a \in \text{Ker } f$  then  $f(a) = 0$ , so  $(\phi \circ f)(a) = 0$ . But  $\phi \circ f = g \circ \bar{\alpha}$ , and so  $(g \circ \bar{\alpha})(a) = 0$ , so  $\bar{\alpha}(a) \in \text{Ker } g$ , which is what we wanted.
- The maps  $\bar{\phi} : \text{Coker } f \rightarrow \text{Coker } g$  and  $\bar{\psi} : \text{Coker } g \rightarrow \text{Coker } h$  are induced from  $\phi$  and  $\psi$  by

$$\bar{\phi}(x + \text{Im } f) = \phi(x) + \text{Im } g, \quad \bar{\psi}(y + \text{Im } g) = \psi(y) + \text{Im } h.$$

Check that these maps make sense. Suppose  $x_1 + \text{Im } f = x_2 + \text{Im } f$ . Then  $x_1 - x_2 \in \text{Im } f$ , so there exists  $a \in A$  such that  $f(a) = x_1 - x_2$ . Now

$$\phi(x_1) - \phi(x_2) = \phi(x_1 - x_2) = (\phi \circ f)(a) = (g \circ \alpha)(a) \in \text{Im } g.$$

So  $\phi(x_1) + \text{Im } g = \phi(x_2) + \text{Im } g$ . So  $\bar{\phi}$  is well-defined, and  $\bar{\psi}$  is shown to be well-defined by a similar argument.

- How is the **connecting homomorphism**  $\delta$  defined? Since  $\beta$  is surjective, for all  $c \in C$ , there exists  $b \in B$  with  $\beta(b) = c$ . Suppose  $c \in \text{Ker } h$ . Then  $(h \circ \beta)(b) = 0$ , so  $(\psi \circ g)(b) = 0$ . Hence  $g(b) \in \text{Ker } \psi = \text{Im } \phi$ . Define

$$\delta(c) = x + \text{Im } f, \quad \phi(x) = g(b), \quad \beta(b) = c.$$

Check this is well-defined. Suppose  $b_1, b_2, x_1, x_2$  are such that  $\phi(x_1) = g(b_1)$  and  $\phi(x_2) = g(b_2)$ , and  $\beta(b_1) = \beta(b_2) = c$ . We have  $b_1 - b_2 \in \text{Ker } \beta = \text{Im } \alpha$ . So  $b_1 - b_2 = \alpha(a)$  for some  $a \in A$ . Then

$$(\phi \circ f)(a) = (g \circ \alpha)(a) = g(b_1 - b_2) = g(b_1) - g(b_2) = \phi(x_1) - \phi(x_2) = \phi(x_1 - x_2).$$

But  $\phi$  is injective, and so  $f(a) = x_1 - x_2$ , and so  $x_1 + \text{Im } f = x_2 + \text{Im } f$ . So  $\delta$  is well-defined.

Exactness of the sequence is an exercise, on problem sheet.  $\square$

## 1.7 Tensor products

**Definition 1.28.** Let  $M$  be a left  $R$ -module, and let  $L$  be a right  $R$ -module. The **tensor product**  $L \otimes_R M$  is an abelian group generated as an abelian group by a set of **pure tensors**

$$\{l \otimes m \mid l \in L, m \in M\},$$

subject to the relations

$$\begin{aligned} l_1 \otimes m + l_2 \otimes m &= (l_1 + l_2) \otimes m, & l_1, l_2 \in L, & m \in M, \\ l \otimes m_1 + l \otimes m_2 &= l \otimes (m_1 + m_2), & l \in L, & m_1, m_2 \in M, \\ (lr) \otimes m &= l \otimes (rm), & l \in L, & m \in M, r \in R. \end{aligned}$$

The following are observations.

- In general, not every element of  $L \otimes_R M$  is a pure tensor. A general element of  $L \otimes_R M$  is a  $\mathbb{Z}$ -linear combination of pure tensors.
- If  $R$  is commutative,  $L$  can be a left module, since left and right modules are the same. Also, in this case,  $L \otimes_R M$  has an  $R$ -module structure, by  $r(l \otimes m) = rl \otimes m$ .
- Suppose that  $S$  is a set of generators for  $L$ , as an abelian group, and  $T$  is a set of generators for  $M$ , as an abelian group. Then a smaller generating set for  $L \otimes_R M$  is  $\{s \otimes t \mid s \in S, t \in T\}$ . This is because if

$$l = \sum_{i=1}^p a_i s_i, \quad m = \sum_{j=1}^q b_j t_j, \quad s_i \in S, \quad t_j \in T, \quad a_i, b_j \in \mathbb{Z},$$

then, from the relations,

$$l \otimes m = \sum_{i=1}^p \sum_{j=1}^q a_i b_j s_i \otimes t_j.$$

- Tensor products can be counter intuitive, such as  $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3 = 0$ . Why? Observe that for  $x \in \mathbb{Z}_2$ ,  $x3 = 3x = x$ . So for all  $x \in \mathbb{Z}_2$  and  $y \in \mathbb{Z}_3$ ,

$$x \otimes y = x3 \otimes y = x \otimes 3y = x \otimes 0 = x \otimes y - x \otimes y = 0.$$