

# M4P63 Algebra IV

Lectured by Dr John Britnell  
Typed by David Kurniadi Angdinata

Spring 2020

**Syllabus**

# Contents

<b>1</b>	<b>Modules over a ring</b>	<b>3</b>
1.1	Modules . . . . .	3
1.2	Homomorphisms . . . . .	4
1.3	Direct products and direct sums . . . . .	4
1.4	Exact sequences . . . . .	4
1.5	Projective modules . . . . .	6
1.6	Free modules . . . . .	7
1.7	Injective modules . . . . .	8
<b>2</b>	<b>Hom and tensor product</b>	<b>10</b>
2.1	Hom . . . . .	10
2.2	The snake lemma . . . . .	12
2.3	Tensor products . . . . .	13
2.4	Flat modules . . . . .	17
<b>3</b>	<b>Modules over a PID</b>	<b>18</b>
3.1	Free and projective modules . . . . .	18
3.2	Injective and divisible modules . . . . .	19
3.3	Flat and torsion-free modules . . . . .	19
<b>4</b>	<b>Resolutions</b>	<b>23</b>
4.1	Free resolutions . . . . .	23
4.2	Injective coresolutions . . . . .	23

# 1 Modules over a ring

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.

## 1.1 Modules

**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  $(x^2 + 3x - 2) * v = M^2 v + 3Mv - 2v$ .
- 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  $r*s_{R^{\text{op}}}s = s*Rr$ .

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.

## 1.2 Homomorphisms

**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*

$$\text{Im } f \leq M_2, \quad \text{Ker } f \leq M_1, \quad \text{Im } f \cong M / \text{Ker } f.$$

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

## 1.3 Direct products and direct sums

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

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

and surjective maps

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

## 1.4 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.**  $\alpha$  is injective and  $\beta$  is surjective.

Lecture 2  
Monday  
13/01/20

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

**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

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

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

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

□

---

<sup>1</sup>Exercise

## 1.5 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  $\beta \circ \delta = f \circ \epsilon$ , we have

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

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

□

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

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

## 1.6 Free modules

**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 an  $R$ -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.*

$\Rightarrow$  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

## 1.7 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

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ f \downarrow & \begin{array}{c} \nearrow g \\ \nwarrow \rho \end{array} & \downarrow \delta \\ M & \xrightarrow[\epsilon]{\rho} & Y \end{array}$$

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  $x \in I$ . The proof requires Zorn's lemma.

**Lemma 1.19** (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.*

*Proof.*

$\Leftarrow$  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

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

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

## 2 Hom and tensor product

### 2.1 Hom

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

**Definition 2.1.** 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 2.2.** 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 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 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 Hom respects direct sums.

**Proposition 2.3.** 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 2.4.** 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 2.5.** *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 the map defined by

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

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 2.6.** *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

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

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 2.7.** 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 2.8.** 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.  $\square$

## 2.2 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 2.9** (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  $\phi \circ f = g \circ \alpha$ , and so  $(g \circ \alpha)(a) = 0$ , 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.  $\square$

## 2.3 Tensor products

**Definition 2.10.** 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,

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

**Example.** 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  $y \in \mathbb{Z}_3$ ,

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

**Theorem 2.11** (Universal property of tensor products). *Let  $A$  be a right  $R$ -module and  $B$  a left  $R$ -module. Let  $C$  be an abelian group. Let  $f : A \times B \rightarrow C$  be a map, not necessarily a homomorphism, which is  $\mathbb{Z}$ -linear in both arguments, so*

$$f(a_1 + a_2, b) = f(a_1, b) + f(a_2, b), \quad a_1, a_2 \in A, \quad b \in B,$$

$$f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2), \quad a \in A, \quad b_1, b_2 \in B,$$

and such that

$$f(ar, b) = f(a, rb), \quad a \in A, \quad b \in B, \quad r \in R.$$

Then there is a unique homomorphism

$$\begin{aligned} g : A \otimes_R B &\longrightarrow C \\ a \otimes b &\longmapsto f(a, b) \end{aligned}$$

*Proof.* In formal group theoretic terms, the tensor product  $A \otimes_R B$  is a quotient  $F/K$ , where  $F$  is the free abelian group on the set of pure tensors  $a \otimes b$ , and  $K$  is the subgroup of  $F$  generated by elements of the form

$$(a_1 + a_2) \otimes b - a_1 \otimes b - a_2 \otimes b, \quad a \otimes (b_1 + b_2) - a \otimes b_1 - a \otimes b_2, \quad ar \otimes b - a \otimes rb.$$

The universal property of free abelian groups states that if  $F$  is free abelian on a set  $S$ , then any set map  $S \rightarrow C$ , for  $C$  an abelian group, extends uniquely to a homomorphism  $F \rightarrow C$ . In the situation under discussion, we have a map

$$g' : \{a \otimes b \mid a \in A, b \in B\} \rightarrow C.$$

So  $g'$  extends uniquely to a homomorphism  $F \rightarrow C$ . The conditions stipulated on  $f$  guarantee that  $g'(K) = 0$ . So  $g'$  induces a map  $g : F/K \rightarrow C$ , which is what we want, since  $F/K = A \otimes_R B$ . This establishes the existence of  $g$ . Since the images of the pure tensors under  $g$  are specified, it is clear that  $g$  is unique.  $\square$

**Corollary 2.12.**

1. Let  $M$  be a left  $R$ -module. Then  $R \otimes_R M \cong M$ , via the map

$$\begin{aligned} f : M &\longrightarrow R \otimes_R M \\ m &\longmapsto 1 \otimes m \end{aligned}$$

2. Let  $M$  be a right  $R$ -module. Then  $M \otimes_R R \cong M$ .

*Proof.*

1. It is clear that  $f$  is a homomorphism of abelian groups. Now  $r \otimes m = 1 \otimes rm$ , so  $R \otimes_R M$  is generated by  $\{1 \otimes m \mid m \in M\}$ , so  $f$  is surjective. For injectivity of  $f$ , we need the universal property. Define a bilinear map

$$\begin{aligned} R \times M &\longrightarrow M \\ (r, m) &\longmapsto rm \end{aligned}$$

This induces a homomorphism

$$\begin{aligned} g : R \otimes_R M &\longrightarrow M \\ r \otimes m &\longmapsto rm \end{aligned}$$

It is easy to check that  $g$  is an inverse for  $f$ , so  $f$  is bijective.

2. By the same argument as 1.

$\square$

**Corollary 2.13.** *Let  $A$  and  $B$  be right  $R$ -modules, and let  $C$  be a left  $R$ -module.*

1.  $(A \oplus B) \otimes_R C \cong (A \otimes_R C) \oplus (B \otimes_R C)$ , via the map

$$\begin{aligned} f : (A \oplus B) \otimes_R C &\longrightarrow (A \otimes_R C) \oplus (B \otimes_R C) \\ (a, b) \otimes c &\longmapsto (a \otimes c, b \otimes c) \end{aligned}.$$

2.  $A \otimes_R (B \oplus C) \cong (A \otimes_R B) \oplus (A \otimes_R C)$ .

*Proof.*

1. Take a bilinear map, that is  $\mathbb{Z}$ -bilinear in both arguments, and respecting  $R$ -multiplication,

$$\begin{aligned} A \oplus B \times C &\longrightarrow (A \otimes_R C) \oplus (B \otimes_R C) \\ ((a, b), c) &\longmapsto (a \otimes c, b \otimes c) \end{aligned}.$$

This induces a homomorphism  $f : (A \oplus B) \otimes_R C \rightarrow (A \otimes_R C) \oplus (B \otimes_R C)$  with the description as given above. Now take the bilinear map given by

$$\begin{aligned} A \times C &\longrightarrow (A \oplus B) \otimes_R C \\ (a, c) &\longmapsto (a, 0) \otimes c \end{aligned}.$$

This induces a homomorphism  $g_1 : A \otimes_R C \rightarrow (A \oplus B) \otimes_R C$ . Similarly, we get a homomorphism  $g_2 : B \otimes_R C \rightarrow (A \oplus B) \otimes_R C$ . Now define

$$\begin{aligned} g = g_1 \oplus g_2 : (A \otimes_R C) \oplus (B \otimes_R C) &\longrightarrow (A \oplus B) \otimes_R C \\ (x, y) &\longmapsto g_1(x) + g_2(y) \end{aligned}.$$

It is easy to check that  $f$  and  $g$  are mutually inverse, so both isomorphisms.

2. Similarly.

□

**Corollary 2.14.** *Let  $A$  be an abelian group. Then*

1.  $\mathbb{Z}_n \otimes_{\mathbb{Z}} A \cong A/nA$ , and  
2.  $A \otimes_{\mathbb{Z}} \mathbb{Z}_n \cong A/nA$ .

*Proof.*

1. Define a map by

$$\begin{aligned} f : A &\longrightarrow \mathbb{Z}_n \otimes_{\mathbb{Z}} A \\ a &\longmapsto 1 \otimes a \end{aligned}.$$

Suppose  $a_0 \in A$  such that  $a_0 = na$  for some  $a$ . Then  $f(a_0) = 1 \otimes a_0 = 1 \otimes na = n \otimes a = 0$  so  $nA \leq \text{Ker } f$ . So  $f$  induces a map

$$\bar{f} : A/nA \rightarrow \mathbb{Z}_n \otimes_{\mathbb{Z}} A.$$

Notice that the pure tensor  $k \otimes a$  is equal to  $1 \otimes ka$ , so  $\mathbb{Z}_n \otimes_{\mathbb{Z}} A$  is generated by  $\{1 \otimes a \mid a \in A\}$ . So  $\bar{f}$  is surjective. For injectivity, use the universal property. We have a bilinear map

$$\begin{aligned} g : \mathbb{Z}_n \times A &\longrightarrow A/nA \\ (k, a) &\longmapsto ka + nA \end{aligned}.$$

This is well-defined and bilinear. So extends to a homomorphism

$$\bar{g} : \mathbb{Z}_n \otimes_{\mathbb{Z}} A \rightarrow A/nA.$$

It is easy to check that  $\bar{g} \circ \bar{f} = \text{id}_{A/nA}$ , so  $\bar{f}$  is injective.

2. Similarly.

□

**Proposition 2.15.** *Let  $\alpha : A \rightarrow B$  be a homomorphism of right  $R$ -modules. Let  $M$  be a left  $R$ -module. There is a unique abelian group homomorphism*

$$\begin{aligned} \alpha' : A \otimes_R M &\longrightarrow B \otimes_R M \\ a \otimes m &\longmapsto \alpha(a) \otimes m, \quad a \in A, \quad m \in M. \end{aligned}$$

*Proof.* The set map defined by

$$\begin{aligned} f : A \times M &\longrightarrow B \otimes_R M \\ (a, m) &\longmapsto \alpha(a) \otimes m \end{aligned}$$

is linear in both arguments, and we have

$$f(ar, m) = \alpha(ar) \otimes m = \alpha(a)r \otimes m = \alpha(a) \otimes rm = f(a, rm).$$

Now by the universal property of tensor products,  $f$  gives rise to a unique homomorphism  $\alpha' : A \otimes_R M \rightarrow B \otimes_R M$  with the properties claimed.  $\square$

**Proposition 2.16.** *Suppose  $\alpha : A \rightarrow B$  is surjective. Then  $\alpha' : A \otimes_R M \rightarrow B \otimes_R M$  is surjective.*

*Proof.* Since  $\alpha$  is surjective, every pure tensor  $b \otimes m \in B \otimes_R M$  is equal to  $\alpha(a) \otimes m$  for some  $a \in A$ . So  $b \otimes m = \alpha'(a \otimes m) \in \text{Im } \alpha'$ . Since  $B \otimes_R M$  is generated by its pure tensors,  $\alpha'$  is surjective.  $\square$

An observation is that it is not true that  $A \rightarrow B$  is injective implies  $A \otimes_R M \rightarrow B \otimes_R M$  is injective.

**Example.** Let

$$\begin{aligned} \alpha : \mathbb{Z}_2 &\longrightarrow \mathbb{Z}_4 \\ 1 &\longmapsto 2, \end{aligned}$$

which is injective. Consider

$$\begin{aligned} \alpha' : \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2 &\longrightarrow \mathbb{Z}_4 \otimes_{\mathbb{Z}} \mathbb{Z}_2 \\ 1 \otimes 1 &\longmapsto 2 \otimes 1 = 1 \otimes 2 = 0. \end{aligned}$$

So  $\alpha'$  is the zero map, which is not injective.

**Proposition 2.17.** *Let*

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

*be a short exact sequence of right  $R$ -modules. Then the sequence*

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

*is exact.*

*Proof.* Since  $\beta'$  is surjective, the sequence is exact at  $C \otimes_R M$ . We show it is exact at  $B \otimes_R M$ . Since  $\beta$  is surjective, for every  $c \in C$ , there exists  $f(c) \in B$  such that  $\beta(f(c)) = c$ . Here  $f$  is a set map  $C \rightarrow B$ , which is not uniquely defined in general. Suppose that  $\beta(b) = c$ . Then  $b - f(c) \in \text{Ker } \beta = \text{Im } \alpha$ , so  $f(c) + \text{Im } \alpha = b + \text{Im } \alpha$ . Define a set map by

$$\begin{aligned} g : C \times M &\longrightarrow (B \otimes_R M) / \text{Im } \alpha' \\ (c, m) &\longmapsto f(c) \otimes m + \text{Im } \alpha'. \end{aligned}$$

Note that if  $\beta(b) = c$ , then  $b \otimes m - f(c) \otimes m = \alpha(a) \otimes m \in \text{Im } \alpha'$  for some  $a \in A$ . We can check that  $g$  is linear in both arguments. For example, for the first argument, we have  $g(c_1 + c_2, m) = f(c_1 + c_2) \otimes m + \text{Im } \alpha'$ . Now  $\beta(f(c_1 + c_2)) = c_1 + c_2 = \beta(f(c_1)) + \beta(f(c_2)) = \beta(f(c_1) + f(c_2))$  so

$$g(c_1 + c_2, m) = (f(c_1) + f(c_2)) \otimes m + \text{Im } \alpha' = f(c_1) \otimes m + f(c_2) \otimes m + \text{Im } \alpha' = g(c_1, m) + g(c_2, m).$$

Also, we have  $g(cr, m) = f(cr) \otimes m + \text{Im } \alpha'$ . But  $\beta(f(cr)) = cr = \beta(f(c)r)$ , so  $f(cr) \otimes m + \text{Im } \alpha' = f(c)r \otimes m + \text{Im } \alpha'$ . So

$$g(cr, m) = f(c)r \otimes m + \text{Im } \alpha' = f(c) \otimes rm + \text{Im } \alpha' = g(c, rm).$$



By the universal property, there is a unique homomorphism

$$\begin{aligned} \psi &: C \otimes_R M \longrightarrow (B \otimes_R M) / \text{Im } \alpha' \\ c \otimes m &\longmapsto f(c) \otimes m + \text{Im } \alpha' \end{aligned}$$

Next observe that  $(\beta' \circ \alpha')(a \otimes m) = (\beta \circ \alpha)(a) \otimes m = 0$ , since  $\text{Im } \alpha = \text{Ker } \beta$ . Since  $A \otimes_R M$  is generated by pure tensors, we have  $\beta' \circ \alpha' = 0$ . So  $\text{Im } \alpha' \leq \text{Ker } \beta'$ . Hence  $\beta'$  induces a map

$$\phi : (B \otimes_R M) / \text{Im } \alpha' \rightarrow C \otimes_R M.$$

It is easy to check that  $\phi$  and  $\psi$  are mutually inverse, and so both are isomorphisms. In particular  $\phi$  is injective, and so  $\text{Im } \alpha' = \text{Ker } \beta'$  as required.  $\square$

## 2.4 Flat modules

**Definition 2.18.** A left  $R$ -module  $M$  is **flat** if  $A \rightarrow B$  is injective implies that  $A \otimes_R M \rightarrow B \otimes_R M$  is injective.

If  $M$  is flat then any short exact sequence of right  $R$ -modules

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

corresponds to a short exact sequence of abelian groups

$$0 \rightarrow A \otimes_R M \rightarrow B \otimes_R M \rightarrow C \otimes_R M \rightarrow 0.$$

**Proposition 2.19.** *Every projective module is flat.*

This follows from two lemmas.

**Lemma 2.20.**  *$P \oplus Q$  is flat if and only if  $P$  and  $Q$  are both flat.*

*Proof.* Recall there is a canonical isomorphism

$$A \otimes_R (P \oplus Q) \cong (A \otimes_R P) \oplus (A \otimes_R Q).$$

Suppose  $\alpha : A \rightarrow B$  is injective. Then  $\alpha' : A \otimes_R (P \oplus Q) \rightarrow B \otimes_R (P \oplus Q)$  corresponds to

$$\begin{aligned} \overline{\alpha'} &: (A \otimes_R P) \oplus (A \otimes_R Q) \longrightarrow (B \otimes_R P) \oplus (B \otimes_R Q) \\ (a \otimes p, 0) &\longmapsto (\alpha(a) \otimes p, 0) \\ (0, a \otimes q) &\longmapsto (0, \alpha(a) \otimes q) \end{aligned}$$

It is clear from this that  $\overline{\alpha'}$  is injective if and only if  $A \otimes_R P \rightarrow B \otimes_R P$  and  $A \otimes_R Q \rightarrow B \otimes_R Q$  are injective, and Lemma 2.20 follows immediately.  $\square$

**Lemma 2.21.** *Every free  $R$ -module is flat.*

Lecture 11 is a problems class.

*Proof.* We know  $(A \oplus B) \otimes_R C \cong (A \otimes_R C) \oplus (B \otimes_R C)$ . Similarly,

$$\left( \bigoplus_{s \in S} A_s \right) \otimes_R C \cong \bigoplus_{s \in S} (A_s \otimes_R C).$$

So Lemma 2.20 generalises, so  $\bigoplus_{s \in S} A_s$  is flat if and only if all of the  $A_s$  is flat for  $s \in S$ . Let  $F$  be free. Then  $F = \bigoplus_{s \in S} R$ , and so  $F$  is flat if and only if  $R$  is flat. But for any  $R$ -module  $A$ , we have  $A \otimes_R R \cong A$ , so

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \text{Id} \downarrow & & \downarrow \text{Id} \\ A \otimes_R R & \xrightarrow[\alpha']{} & B \otimes_R R \end{array},$$

and it is easy to check that  $R$  is flat.  $\square$

*Proof of Proposition 2.19.* Lemma 2.20 and Lemma 2.21 imply Proposition 2.19, since a projective module is a direct summand of a free module.  $\square$

Lecture 11  
Monday  
03/02/20  
Lecture 12  
Tuesday  
04/02/20

### 3 Modules over a PID

There exist flat modules which are not projective. We will show that  $\mathbb{Q}$  as a module for  $\mathbb{Z}$  is flat, and it is easy to see it is not projective. To do this we will study the case of modules over a PID. Recall that  $R$  is an **integral domain** if  $R$  is commutative and  $rs = 0$  implies that  $r = 0$  or  $s = 0$  for  $r, s \in R$ . An integral domain is a **PID** if every ideal is  $\langle a \rangle = \{ra \mid r \in R\}$  for some  $a \in R$ .

**Example.** The ring  $\mathbb{Z}$  is an example of a PID.

#### 3.1 Free and projective modules

**Proposition 3.1.** *Let  $R$  be a PID. Then every projective  $R$ -module is free. Equivalently, every summand of a free module is free.*

In fact we will show that any submodule of a free module is free. Moreover, if  $F_1 \leq F_2$ , where  $F_1$  and  $F_2$  are free, and if  $B_1$  and  $B_2$  are bases for  $F_1$  and  $F_2$  respectively, then  $|B_1| \leq |B_2|$ . In particular, if  $M \leq R^n$ , then  $M \cong R^m$  for some  $m \leq n$ . For this, we will need the well-ordering theorem.

**Theorem 3.2** (Well-ordering theorem). *Let  $X$  be a set. There exists a well-order  $\leq$  on  $X$ , that is a total order such that every non-empty subset of  $X$  has a least element.*

**Corollary 3.3** (Transfinite induction). *Let  $X$  be a non-empty set well-ordered by  $\leq$ . Let  $x_0$  be the least element of  $X$ . Let  $S \subseteq X$ . If  $x_0 \in S$ , and  $s < t$  implies  $s \in S$  implies that  $t \in S$ , then  $S = X$ .*

*Proof.* Let  $F = \bigoplus_{s \in S} R$ . Let  $\leq$  be a well-order on  $S$ . For  $s \in S$ , let  $\pi_s$  be the projection map  $F \rightarrow R$  onto the  $s$ -coordinate. Let  $e_s$  be the element of  $F$  with one in coordinate  $s$ , and zero elsewhere. Suppose  $U \leq F$  is an  $R$ -submodule of  $F$ . Define  $R_t$  to be the submodule of  $F$  generated by  $\{e_s \mid s \leq t\}$ , so

$$R_t = \text{sp}\{e_s \mid s \leq t\}.$$

So if  $t_1 \leq t_2$  then  $R_{t_1} \leq R_{t_2}$ . Let

$$U_t = U \cap R_t.$$

So  $t_1 < t_2$  implies that  $U_{t_1} \leq U_{t_2}$ . Consider  $\pi_s(U_s)$ . This is an ideal of  $R$ . Hence there exists  $a_s \in R$  such that  $\pi_s(U_s) = \langle a_s \rangle$ , since  $R$  is a PID. For each  $s$ , let  $u_s \in U_s$  be such that  $\pi_s(u_s) = a_s$ . In cases where  $a_s = 0$ , assume  $u_s = 0$ . Let

$$B = \{u_s \mid s \in S, u_s \neq 0\}.$$

- Claim that  $B$  generates  $U$ . We will actually prove that  $B_t = \{u_s \mid s \leq t\}$  generates  $U_t$ , using transfinite induction. If  $s_0$  is the least element of  $S$ , it is easy to see that  $B_{s_0} = \{u_{s_0}\}$  generates  $U_{s_0}$ . Suppose  $B_t$  generates  $U_t$  for all  $t < t_0$ . Let  $u \in U_{t_0}$ . Then  $\pi_{t_0}(u) = ra_{t_0}$ . Hence  $\pi_{t_0}(u - ru_{t_0}) = 0$ . So  $u - ru_{t_0}$  has zero in the  $t_0$ -coordinate, so  $u - ru_{t_0} \in \text{sp}\{e_s \mid s < t_0\}$ . Clearly  $u - ru_{t_0} \in U$ . We have  $u - ru_{t_0} = \sum_{i=1}^q r_i e_{s_i}$ , where  $s_i < t_0$ , and  $s_1 < \dots < s_q$ . Then

$$u - ru_{t_0} \in U \cap R_{s_q} = U_{s_q} = \text{sp } B_{s_q},$$

by the inductive hypothesis. Hence  $u \in \text{sp}(B_{s_q} \cup \{u_{t_0}\}) \subseteq \text{sp } B_{t_0}$ . Hence  $B_{t_0}$  generates  $U_{t_0}$ , as required.

- Next we show the linear independence of  $B$ . Suppose we have a linear combination of elements of  $B$  equal to zero. Say  $\sum_{i=1}^k r_i u_{s_i} = 0$ . Assume  $s_1 < \dots < s_k$ . We have

$$\pi_{s_k} \left( \sum_{i=1}^k r_i u_{s_i} \right) = \sum_{i=1}^k r_i \pi_{s_k}(u_{s_i}).$$

Now  $u_{s_i} \in U_{s_i} \subseteq R_{s_i}$ , and so  $\pi_{s_k}(u_{s_i}) = 0$  if  $s_i < s_k$ . Hence  $r_k \pi_{s_k}(u_{s_k}) = 0$ , so  $r_k a_{s_k} = 0$ . But  $a_{s_k} \neq 0$ , and  $R$  is an integral domain. So  $r_k = 0$ . It follows easily that  $r_i = 0$  for all  $i$ , so  $B$  is linearly independent.

We have shown that  $B$  is a basis for  $U$ . Hence  $U$  is free. Since the elements of  $B$  are indexed by a subset of  $S$ , we have  $|B| \leq |S|$ . □

Lecture 13 is a problems class.

Lecture 13  
Friday  
07/02/20

### 3.2 Injective and divisible modules

**Definition 3.4.** Let  $R$  be an integral domain, and  $M$  an  $R$ -module. Let  $m \in M$ . Say that  $m$  is **infinitely divisible** if for all  $r \in R \setminus \{0\}$  there exists  $l \in M$  such that  $rl = m$ .

**Proposition 3.5.** *The divisible elements of  $M$  form a submodule  $D(M)$ .*

*Proof.* Easy. □

**Definition 3.6.** If  $D(M) = M$ , then  $M$  is **divisible**.

**Proposition 3.7.** *Let  $R$  be an integral domain. Then if an  $R$ -module  $M$  is injective then it is divisible.*

*Proof.* Recall that for an integral domain  $R$ , and  $a \in R \setminus \{0\}$ , the map

$$\begin{aligned} f : R &\longrightarrow \langle a \rangle \\ r &\longmapsto ra \end{aligned}$$

is an isomorphism. Suppose  $M$  is an injective  $R$ -module. Let

$$\begin{aligned} g : R &\longrightarrow M \\ 1 &\longmapsto m \end{aligned}.$$

Then  $g \circ f^{-1}$  is a homomorphism  $\langle a \rangle \rightarrow M$ , and  $(g \circ f^{-1})(a) = g(1) = m$ . Now by Baer's criterion, there is a map  $h : R \rightarrow M$  extending  $g \circ f^{-1}$ . Now  $ah(1) = h(a) = (g \circ f^{-1})(a) = m$ . Hence there exists  $l \in M$  such that  $al = m$ . So  $m$  is a divisible element, and so  $M$  is divisible. □

**Proposition 3.8.** *Let  $R$  be a PID. If  $M$  is a divisible  $R$ -module then  $M$  is injective.*

So divisible equals injective when  $R$  is a PID.

*Proof.* We use Baer's criterion. Let  $I$  be an ideal of  $R$ , and  $f : I \rightarrow M$  an  $R$ -module homomorphism. Since  $R$  is a PID,  $I = \langle a \rangle$  for some  $a \in R$ . Suppose  $f(a) = m$ . If  $a = 0$  there is nothing to prove, since the zero map  $R \rightarrow M$  extends  $f$ . So assume  $a \neq 0$ . Since  $m$  is divisible, there exists  $l \in M$  with  $al = m$ . Now the map given by

$$\begin{aligned} R &\longrightarrow M \\ 1 &\longmapsto l \end{aligned}$$

extends  $f$ . So Baer's criterion is satisfied, and so  $M$  is injective. □

### 3.3 Flat and torsion-free modules

**Definition 3.9.** Let  $R$  be an integral domain. Let  $M$  be an  $R$ -module. Say that  $m \in M$  is a **torsion element** if there exists  $r \in R \setminus \{0\}$  such that  $rm = 0$ .

**Proposition 3.10.** *The torsion elements of  $M$  form a submodule  $T(M)$ .*

*Proof.* Easy, using the fact that integral domains are commutative. □

**Definition 3.11.** If  $T(M) = 0$ , then  $M$  is **torsion-free**. If  $T(M) = M$ , then  $M$  is a **torsion module**.

**Proposition 3.12.** *Let  $R$  be an integral domain. Let  $M$  be a flat  $R$ -module. Then  $M$  is torsion-free.*

*Proof.* Let  $a \in R \setminus \{0\}$ . Then

$$\begin{aligned} f : R &\longrightarrow R \\ 1 &\longmapsto a \end{aligned}$$

is an injective  $R$ -module homomorphism. Suppose that  $M$  is flat. Then the map

$$\begin{aligned} g : R \otimes_R M &\longrightarrow R \otimes_R M \\ r \otimes m &\longmapsto ra \otimes m = r \otimes am \end{aligned}$$

is injective. But  $R \otimes_R M$  is canonically isomorphic to  $M$ , under which the map  $g$  corresponds to  $m \mapsto am$ . Since  $g$  is injective, we have  $am \neq 0$  for  $m \neq 0$ . Hence  $m$  is not a torsion element, if  $m \neq 0$ , and so  $M$  is torsion-free. □

We now build up to the following.

**Proposition 3.13.** *Let  $R$  be a PID. If  $M$  is a torsion-free  $R$ -module then  $M$  is flat.*

The following is the strategy. We want to prove that whenever  $\alpha : A \rightarrow B$  is injective, so is  $\alpha' : A \otimes_R M \rightarrow B \otimes_R M$ , where  $M$  is torsion-free.

1. Prove this in the case that  $B$  is free, and  $A$  is a submodule of  $B$ , and  $\alpha$  is the inclusion map, by
  - first reducing the problem to the case that  $A$  and  $B$  are finitely generated, so  $B \cong \mathbb{R}^n$ , and
  - then using induction on the rank  $n$  of  $B$ .
2. Show the general case follows from 1.

**Lemma 3.14.** *Let  $R$  be a PID, let  $I = \langle a \rangle$  be an ideal of  $R$ , and let  $M$  be a torsion-free  $R$ -module. Then  $g : I \otimes_R M \rightarrow R \otimes_R M$  is injective.*

*Proof.* The homomorphism given by

$$\begin{array}{ccc} R & \longrightarrow & I \\ r & \longmapsto & ra \end{array}$$

gives a map  $f : R \otimes_R M \rightarrow I \otimes_R M$ . Now  $g \circ f$  is a map

$$\begin{array}{ccc} R \otimes_R M & \longrightarrow & R \otimes_R M \\ r & \longmapsto & ra \end{array}.$$

Now  $f$  is surjective, and  $g \circ f$  is injective, since  $R$  is an integral domain. But this implies that  $g$  is injective, as required.  $\square$

**Lemma 3.15.** *Let  $A$  be a right  $R$ -module. Let  $M$  be a left  $R$ -module. Suppose  $\sum_{i=1}^t (a_i \otimes m_i) = 0$  in  $A \otimes_R M$ . There exists a finitely generated submodule  $A_0 \leq A$  such that  $a_i \in A_0$  for all  $i$ , and  $\sum_{i=1}^t (a_i \otimes m_i) = 0$  in  $A_0 \otimes_R M$ .*

*Proof.* Recall that

$$A \otimes_R M = F_{\text{ab}}(A \times M) / K,$$

where  $K$  is generated by certain relators. If  $\sum_{i=1}^t (a_i \otimes m_i) = 0$  in  $A \otimes_R M$ , then in  $F_{\text{ab}}(A \times M)$ , we have  $\sum_{i=1}^t (a_i \otimes m_i) \in K$ . So there exist relators  $s_1, \dots, s_q$ , or their negations, such that

$$\sum_{i=1}^t (a_i \otimes m_i) = \sum_{i=1}^q s_i.$$

Only finitely many elements of  $A$  are involved in the relators  $s_1, \dots, s_q$ . Let  $A_0$  be generated by these together with  $a_1, \dots, a_t$ . Then certainly  $a_i \in A_0$  for all  $i$ . And  $\sum_{i=1}^t (a_i \otimes m_i) = \sum_{i=1}^q s_i$  in  $F_{\text{ab}}(A_0 \times M)$  so  $\sum_{i=1}^t (a_i \otimes m_i) = 0$  in  $A_0 \otimes_R M$ . Clearly  $A_0$  is finitely generated.  $\square$

**Lemma 3.16.** *Let  $F = F(S) = \bigoplus_{s \in S} R$ . Let  $U$  be a finitely generated submodule of  $F$ . Then there exists a finite  $T \subseteq S$  such that  $U \leq F(T)$ , and for any  $M$ , the map  $F(T) \otimes_R M \rightarrow F(S) \otimes_R M$  is injective.*

*Proof.* Let  $u_1, \dots, u_q$  be generators for  $U$ . Every  $u_i$  is an  $R$ -linear combination of elements of  $S$ . Since each of these linear combinations mentions only finitely many elements of  $S$ , there is a finite subset  $T \subseteq S$  such that every  $u_i$  is an  $R$ -linear combination of elements of  $T$ . So  $U \leq F(T)$ . We have

$$F(S) = F(T) \oplus F(S \setminus T),$$

and so

$$F(S) \otimes_R M \cong (F(T) \otimes_R M) \oplus (F(S \setminus T) \otimes_R M).$$

It follows that the natural map  $F(T) \otimes_R M \rightarrow F(S) \otimes_R M$  is injective.  $\square$

Lecture 15  
Tuesday  
11/02/20

Lemma 3.15 and Lemma 3.16 tell us that if  $F$  is free and  $U \leq F$ , and if  $M$  is an  $R$ -module, if  $U \otimes_R M \rightarrow F \otimes_R M$  is not injective, then there exists a finitely generated  $U_0 < U$  and a finite rank free submodule  $F_0 < F$  such that  $U_0 \otimes_R M \rightarrow F_0 \otimes_R M$  is not injective.

**Lemma 3.17.** *Let  $R$  be a PID. Let  $F$  be free, and  $U \leq F$ . Let  $M$  be torsion-free. Then  $U \otimes_R M \rightarrow F \otimes_R M$  is injective.*

*Proof.* We assume that  $F = R^n$ . We do this by induction on  $n$ .

Base case. Let  $n = 1$ . So  $F$  is  $R$ , and  $U$  is an ideal of  $R$ . By Lemma 3.14,  $U \otimes_R M \rightarrow F \otimes_R M$  is injective in this case.

Inductive hypothesis.  $U \leq F = R^{n-1}$  implies that  $U \otimes_R M \rightarrow F \otimes_R M$  is injective.

Inductive step. Assume  $U \leq F = R^n$ . Write  $R^n = R \oplus R^{n-1}$ . So we have a short exact sequence

$$0 \rightarrow R \rightarrow R^n \rightarrow R^{n-1} \rightarrow 0.$$

We also have a short exact sequence

$$0 \rightarrow U_1 \rightarrow U \rightarrow \pi_{R^{n-1}}(U) \rightarrow 0,$$

where  $U_1 = U \cap (R \oplus 0^{n-1})$ . Identifying  $R$  with  $R \oplus 0^{n-1}$ , we get a commuting diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & U_1 & \longrightarrow & U & \longrightarrow & \pi_{R^{n-1}}(U) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & R & \longrightarrow & R^n & \longrightarrow & R^{n-1} \longrightarrow 0 \end{array},$$

where the vertical maps are inclusions, and the rows are exact. Tensoring everything with  $M$ , we get a new commuting diagram

$$\begin{array}{ccccccc} U_1 \otimes_R M & \longrightarrow & U \otimes_R M & \longrightarrow & \pi_{R^{n-1}}(U) \otimes_R M & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \downarrow h \\ 0 & \longrightarrow & R \otimes_R M & \longrightarrow & R^n \otimes_R M & \longrightarrow & R^{n-1} \otimes_R M \longrightarrow 0 \end{array}.$$

The initial zero in the bottom row comes from the fact that

$$0 \rightarrow R \rightarrow R^n \rightarrow R^{n-1} \rightarrow 0$$

is split, since  $R^n = R \oplus R^{n-1}$ , and so

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

Now  $f$  is injective by Lemma 3.14, and  $h$  is injective by the inductive hypothesis. The snake lemma tells us that the sequence

$$\text{Ker } f \rightarrow \text{Ker } g \rightarrow \text{Ker } h$$

is exact at  $\text{Ker } g$ . So

$$0 \rightarrow \text{Ker } g \rightarrow 0$$

is exact, and so  $\text{Ker } g = 0$ . So  $g$  is injective, and this completes the induction.  $\square$

*Proof of Proposition 3.13.* Prove that if  $\alpha : A \rightarrow B$  is injective, and  $M$  is torsion-free, over a PID  $R$ , then  $\alpha' : A \otimes_R M \rightarrow B \otimes_R M$  is injective. There exists a free module  $F$  such that  $B$  is quotient of  $F$ . So there is a short exact sequence

$$0 \rightarrow K \rightarrow F \xrightarrow{\delta} B \rightarrow 0.$$

Now  $A \cong \alpha A = \text{Im } \alpha$ . Let  $F_A$  be the  $\delta$ -preimage of  $\alpha A$ . Then  $K < F_A$ , and we have another short exact sequence

$$0 \rightarrow K \rightarrow F_A \rightarrow \alpha A \rightarrow 0.$$

We have a commuting diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & K & \longrightarrow & F_A & \longrightarrow & \alpha A \longrightarrow 0 \\ & & \parallel & & \downarrow & & \downarrow \\ 0 & \longrightarrow & K & \longrightarrow & F & \longrightarrow & B \longrightarrow 0 \end{array}.$$

Tensoring with  $M$ ,

$$\begin{array}{ccccccc} K \otimes_R M & \xrightarrow{\beta} & F_A \otimes_R M & \xrightarrow{\gamma} & \alpha A \otimes_R M & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow g & & \\ K \otimes_R M & \xrightarrow{\delta} & F \otimes_R M & \xrightarrow{\epsilon} & B \otimes_R M & \longrightarrow & 0 \end{array}$$

is commuting, and exact along rows. Let  $u \in \text{Ker } g \leq \alpha A \otimes_R M \cong A \otimes_R M$ . Since  $\gamma$  is surjective, there is  $w \in F_A \otimes_R M$  with  $\gamma(w) = u$ . So  $(g \circ \gamma)(w) = 0$ . So  $(\epsilon \circ f)(w) = 0$ . So  $f(w) \in \text{Ker } \epsilon = \text{Im } \delta$ , so  $f(w) = \delta(k)$  for  $k \in K \otimes_R M$ . Since  $f$  is injective, by Lemma 3.17, we get  $w = \beta(k) \in \text{Im } \beta$ . So  $w \in \text{Ker } \gamma$ , so  $u = 0$ . Hence  $g$  is injective, as required.  $\square$

We have shown that if  $R$  is a PID, and if  $M$  is torsion-free, then  $M$  is flat. For an  $R$ -module  $M$

$$\text{free} \implies \text{projective} \implies \text{flat} \implies \text{torsion-free}, \quad \text{injective} \implies \text{divisible}.$$

Over a PID

$$\text{free} \iff \text{projective} \implies \text{flat} \iff \text{torsion-free}, \quad \text{injective} \iff \text{divisible}.$$

**Example.** Do we have projective if and only if flat, over a general ring, or over a PID? The answer is no.

The  $\mathbb{Z}$ -module  $\mathbb{Q}$  is torsion-free, so flat. Is  $\mathbb{Q}$  projective? Is  $\mathbb{Q}$  free, since  $\mathbb{Z}$  is a PID? Consider a free  $\mathbb{Z}$ -module  $F = \bigoplus_{s \in S} \mathbb{Z}$ . Let  $s_0 \in S$ . Then let

$$x = (x_s)_{s \in S} = \begin{cases} 1 & s = s_0 \\ 0 & \text{otherwise} \end{cases} \in F.$$

It is clear there are no  $y \in F$  such that  $2y = x$ . So  $x$  is not a divisible element of  $F$ . Indeed,  $D(F) = \{0\}$ . But  $D(\mathbb{Q}) = \mathbb{Q}$ . Hence  $\mathbb{Q} \not\cong F$ . So  $\mathbb{Q}$  is an example of a flat module which is not projective.

Lecture 16  
Friday  
14/02/20

## 4 Resolutions

### 4.1 Free resolutions

**Definition 4.1.** Let  $M$  be an  $R$ -module. A **resolution**, or **left resolution**, for  $M$  is a sequence of  $R$ -modules  $A_0, A_1, \dots$ , with homomorphisms  $d : A_{i+1} \rightarrow A_i$ , and also a homomorphism  $A_0 \rightarrow M$ , such that

$$\dots \xrightarrow{d} A_1 \xrightarrow{d} A_0 \rightarrow M \rightarrow 0$$

is an exact sequence, where  $d$  is the **differential**. If all of the modules  $A_i$  have a property  $\mathcal{P}$ , we call this a  **$\mathcal{P}$ -resolution**. So we can talk about free resolutions, projective resolutions, flat resolutions. We do not use the term injective resolution in this context. A **right resolution**, or **coresolution**, for  $M$  is a sequence of  $R$ -modules  $A^0, A^1, \dots$ , with homomorphisms  $d : A^i \rightarrow A^{i+1}$ , and  $M \rightarrow A^0$ , such that

$$0 \rightarrow M \rightarrow A^0 \xrightarrow{d} A^1 \xrightarrow{d} \dots$$

is exact. If the modules  $A^i$  have a property  $\mathcal{P}$ , we can refer to a **right  $\mathcal{P}$ -resolution**. An injective resolution always means a right injective resolution.

**Proposition 4.2.** *Let  $M$  be an  $R$ -module. Then  $M$  has free, projective, and flat resolutions.*

*Proof.* Since free implies projective implies flat, it is enough to show that free resolutions exist. Use the fact that for any module  $L$ , there exists a free module  $F$  and  $K \leq F$  such that  $L \cong F/K$ . So we get a short exact sequence

$$0 \rightarrow K \rightarrow F \rightarrow L \rightarrow 0.$$

It follows that we can find  $F_0, F_1, \dots$ , and  $K_0 \leq F_0, K_1 \leq F_1, \dots$  such that

$$0 \rightarrow K_0 \rightarrow F_0 \rightarrow M \rightarrow 0, \quad 0 \rightarrow K_1 \rightarrow F_1 \rightarrow K_0 \rightarrow 0, \dots$$

are all exact. Since  $K_i \leq F_i$ , we may consider the maps  $F_{i+1} \rightarrow K_i$  as maps  $F_{i+1} \rightarrow F_i$  with image  $K_i$ . But  $K_i$  is the kernel of the map  $F_i \rightarrow K_{i-1}$ , so the sequence

$$\dots \rightarrow F_1 \rightarrow F_0 \rightarrow M \rightarrow 0$$

is exact, and a free resolution for  $M$ . □

### 4.2 Injective coresolutions

Injective coresolutions exist too, but the proof is more intricate. It involves making use of properties of the abelian group  $\mathbb{Q}/\mathbb{Z}$ .

**Proposition 4.3.** *Let  $A$  be an abelian group, and let  $a \in A \setminus \{0\}$ . There is a homomorphism  $f : A \rightarrow \mathbb{Q}/\mathbb{Z}$  such that  $f(a) \neq 0$ .*

*Proof.* Start by defining  $f_0 : \langle a \rangle \rightarrow \mathbb{Q}/\mathbb{Z}$ . If  $a$  has finite order  $t$ , then  $f_0 : a \mapsto 1/t + \mathbb{Z}$ . If  $a$  has infinite order, then  $f_0 : a \mapsto \frac{1}{2} + \mathbb{Z}$ . We will use Zorn's lemma. Let  $X$  be the set

$$\{(B, f) \mid B \leq A, a \in B, f : B \rightarrow \mathbb{Q}/\mathbb{Z}, f \text{ extends } f_0\}.$$

Then  $X$  is non-empty, since  $(\langle a \rangle, f_0) \in X$ . Define a partial order  $\leq$  on  $X$  by  $(B_1, f_1) \leq (B_2, f_2)$  if  $B_1 \leq B_2$  and  $f_2$  extends  $f_1$ . Let  $\{(B_s, f_s) \mid s \in S\}$  be a chain in  $X$ , where  $S$  is a suitable indexing set. Then  $\{B_s \mid s \in S\}$  is a chain of subgroups of  $A$ . So the union  $B = \bigcup_{s \in S} B_s$  is a subgroup of  $A$ , containing  $a$ . Define

$$f : B \rightarrow \mathbb{Q}/\mathbb{Z}, \quad b \mapsto f_s(b), \quad b \in B_s.$$

This is well-defined since if  $b \in B_t$  then  $f_s(b) = f_t(b)$ . Now  $(B, f)$  is an upper bound for  $\{B_s \mid s \in S\}$  in  $X$ . So by Zorn's lemma,  $X$  has a maximal element, which we will call  $(B, f)$ . We show that  $B = A$ . Since  $f(a) = f_0(a)$ , this will complete the proof. Suppose  $x \in A \setminus B$ . Then let  $I < \mathbb{Z}$  be defined by

$$I = \{k \mid kx \in B\}.$$

Since  $\mathbb{Z}$  is a PID, we have  $I = n\mathbb{Z}$  for some  $n$ . We have  $\langle B, x \rangle \leq A$ , and  $\langle B, x \rangle \cong B \oplus \langle x \rangle / \langle nx - b_0 \rangle$ , where  $b_0 = nx$  in  $A$ . Define

$$\begin{aligned} \phi &: B \oplus \langle x \rangle \longrightarrow \mathbb{Q}/\mathbb{Z} \\ (b, kx) &\longmapsto f(b) + \frac{kf(b_0)}{n}, \end{aligned}$$

so sending  $x$  to  $f(b_0)/n$ . We see that  $\phi(nx - b_0) = 0$ , so  $\phi$  induces a map  $B \oplus \langle x \rangle / \langle nx - b_0 \rangle \rightarrow \mathbb{Q}/\mathbb{Z}$ , and hence a map  $f' : \langle B, x \rangle \rightarrow \mathbb{Q}/\mathbb{Z}$ . But  $f'(a) = f_0(a)$ , so  $(\langle B, x \rangle, f)$  is an element of  $X$  greater than  $(B, f)$ , contradicting maximality of  $(B, f)$ . Hence  $B = A$  as required.  $\square$

**Proposition 4.4.** *For every abelian group  $A$ , there is an injective abelian group  $I$  such that  $A$  is isomorphic to a subgroup of  $I$ .*

*Proof.* We know that  $\mathbb{Q}/\mathbb{Z}$  is injective, as a  $\mathbb{Z}$ -module, since it is divisible, and  $\mathbb{Z}$  is a PID. So  $\prod_{s \in S} \mathbb{Q}/\mathbb{Z}$  is also injective. Take  $S = A \setminus \{0\}$ . Then define, for each  $s \in S$ ,  $f_s : A \rightarrow \mathbb{Q}/\mathbb{Z}$  such that  $f_s(s) \neq 0$ . Define

$$\begin{aligned} f &: A \longrightarrow \prod_{s \in S} \mathbb{Q}/\mathbb{Z} \\ a &\longmapsto (f_s(a))_{s \in S}. \end{aligned}$$

Now if  $s \in A \setminus \{0\}$ , then  $f_s(s) \neq 0$ , so  $f(s) \neq 0$ . So  $f$  is injective. It is easy to check that  $f$  is a homomorphism.  $\square$

**Proposition 4.5.** *Let  $M$  be a right  $R$ -module, and let  $A$  be an abelian group. Then  $\text{Hom}_{\mathbb{Z}}(M, A)$  is a left  $R$ -module, with the  $R$ -action defined by  $(rf)(m) = f(mr)$ .*

*Proof.* This is clearer if we write the map  $f$  on the right instead of the left. Then the proposition becomes  $(m)(rf) = (mr)f$ , and it is easy to see this works.  $\square$

**Proposition 4.6.** *Let  $M$  be a left  $R$ -module, and  $A$  an abelian group. Then  $\text{Hom}_{\mathbb{Z}}(R, A)$  is a left  $R$ -module, and there is a natural isomorphism*

$$\text{Hom}_R(M, \text{Hom}_{\mathbb{Z}}(R, A)) \cong \text{Hom}_{\mathbb{Z}}(M, A).$$

*Proof.* Write  $H = \text{Hom}_{\mathbb{Z}}(R, A)$ . Define

$$\begin{aligned} \Phi &: \text{Hom}_R(M, H) \longrightarrow \text{Hom}_{\mathbb{Z}}(M, A) \\ f &\longmapsto (m \mapsto f(m)(1)), \quad m \in M, \quad 1 \in R. \end{aligned}$$

Check the following.

- $\Phi(f)$  is a homomorphism, since

$$\begin{aligned} \Phi(f)(m_1 + m_2) &= f(m_1 + m_2)(1) \\ &= (f(m_1) + f(m_2))(1) \\ &= f(m_1)(1) + f(m_2)(1) && \text{definition of } + \text{ in } \text{Hom}_{\mathbb{Z}}(R, A) \\ &= \Phi(f)(m_1) + \Phi(f)(m_2). \end{aligned}$$

- $\Phi$  is a homomorphism, since

$$\begin{aligned} \Phi(f_1 + f_2)(m) &= (f_1 + f_2)(m)(1) \\ &= (f_1(m) + f_2(m))(1) && \text{definition of } + \text{ in } \text{Hom}_{\mathbb{Z}}(M, A) \\ &= f_1(m)(1) + f_2(m)(1) \\ &= \Phi(f_1)(m) + \Phi(f_2)(m) \\ &= (\Phi(f_1) + \Phi(f_2))(m) && \text{definition of } + \text{ in } \text{Hom}_{\mathbb{Z}}(M, A), \end{aligned}$$

so since  $m$  was arbitrary,  $\Phi(f_1 + f_2) = \Phi(f_1) + \Phi(f_2)$ .

Lecture 17  
Monday  
17/02/20



Now define

$$\begin{aligned} \Psi &: \text{Hom}_{\mathbb{Z}}(M, A) \longrightarrow \text{Hom}_R(M, H) \\ p &\longmapsto (m \mapsto (r \mapsto p(rm))) \end{aligned}, \quad m \in M, \quad r \in R.$$

Check the following.

- $\Psi(p)(m)$  is a homomorphism, since

$$\begin{aligned} \Psi(p)(m)(r_1 + r_2) &= p((r_1 + r_2)m) = p(r_1m + r_2m) \\ &= p(r_1m) + p(r_2m) = \Psi(p)(m)(r_1) + \Psi(p)(m)(r_2). \end{aligned}$$

- $\Psi(p)$  is an  $R$ -module homomorphism, since

$$\begin{aligned} \Psi(p)(m_1 + m_2)(r) &= p(r(m_1 + m_2)) = p(rm_1 + rm_2) = p(rm_1) + p(rm_2) \\ &= \Psi(p)(m_1)(r) + \Psi(p)(m_2)(r) = (\Psi(p)(m_1) + \Psi(p)(m_2))(r), \end{aligned}$$

so  $\Psi(p)(m_1 + m_2) = \Psi(p)(m_1) + \Psi(p)(m_2)$ , and for  $h \in H$ , we have  $(sh)(r) = h(rs)$ , by definition of the  $R$ -module structure on  $H$ , so

$$s\Psi(p)(m)(r) = \Psi(p)(m)(rs) = p(rsm) = \Psi(p)(sm)(r),$$

so  $s\Psi(p)(m) = \Psi(p)(sm)$ .

- $\Psi$  is a homomorphism, since

$$\begin{aligned} \Psi(p_1 + p_2)(m)(r) &= (p_1 + p_2)(rm) = p_1(rm) + p_2(rm) \\ &= \Psi(p_1)(m)(r) + \Psi(p_2)(m)(r) = (\Psi(p_1) + \Psi(p_2))(m)(r), \end{aligned}$$

so  $\Psi(p_1 + p_2) = \Psi(p_1) + \Psi(p_2)$ .

Then  $\Psi \circ \Phi = \text{id}_{\text{Hom}_R(M, H)}$  and  $\Phi \circ \Psi = \text{id}_{\text{Hom}_{\mathbb{Z}}(M, A)}$ .<sup>4</sup> Hence  $\Phi$  and  $\Psi$  are isomorphisms.  $\square$

We are interested in the case  $A = \mathbb{Q}/\mathbb{Z}$ . Write  $S = \text{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ . We will show

- $S$  is injective, as a left  $R$ -module, and
- there exists, for every  $m \in M \setminus \{0\}$ , an  $R$ -module homomorphism  $f : M \rightarrow S$  such that  $f(m) \neq 0$ .

---

<sup>4</sup>Exercise