

M4P63 Algebra IV

Lectured by Dr John Britnell
Typed by David Kurniadi Angdinata

Spring 2020

Syllabus

Contents

1	Modules over a ring	3
1.1	Modules	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
1.8	Modules over a PID	18

1 Modules over a ring

1.1 Modules

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^{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^{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 α is injective and β 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 σ is called a **section** of β .

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 ι_C is a section for β .

\Leftarrow For the converse, suppose that σ is a section for β . 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. ¹
- 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 α 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 ρ is a **retraction** of α .

Proof.

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

\Leftarrow Suppose that ρ is a retraction for α . 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.

□

¹Exercise

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 β 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 σ is a section for β .

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

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

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 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 β , 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 δ and ϵ are just π_B and π_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 β 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 ϵ has a section $\sigma : M \rightarrow X$. Define $g = \delta \circ \sigma : M \rightarrow B$, so

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

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 β 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 ψ 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 σ for ψ , 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 π_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. □

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} ,² so no retraction exists for α .

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 id_M . There exists $g : B \rightarrow M$ such that $\text{id}_M = g \circ \alpha$. So g is a retraction for α , 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 ϵ 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, ϵ 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. □

²Exercise

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 α 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. ³

□

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.

³Exercise

1.5 Hom

Let A and B be two R -modules.

Definition 1.20. Define

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

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

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

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

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

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 $\mathrm{Hom}_R(A, B)$ has an R -module structure. The following are observations.

Proposition 1.21. Suppose $A, A_1, A_2, B, B_1, B_2, M$ are R -modules, and $\alpha : A \rightarrow B$.

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

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

- We can also define

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

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 1.22. Suppose $\alpha : A \rightarrow B$ is surjective. Then $\alpha^* : \mathrm{Hom}_R(B, M) \rightarrow \mathrm{Hom}_R(A, M)$ 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 α 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 1.23. Suppose $\alpha : A \rightarrow B$ is injective. Then $\alpha_* : \mathrm{Hom}_R(M, A) \rightarrow \mathrm{Hom}_R(M, B)$ 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 α is injective, so this implies $f_1(m) = f_2(m)$ for all $m \in M$. \square

Proposition 1.24. *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 β^* 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 α^* 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 β 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 α is injective, but α^* 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 α^* is not surjective.

- Let $\alpha : k\mathbb{Z} \rightarrow \mathbb{Z}$ be the inclusion, so α 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 α^* is not surjective.

Proposition 1.25. *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 α injective implies that α_* 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 β 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 β_* 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 β_* cannot be surjective.

Proposition 1.26. 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 α^* is surjective. \square

Proposition 1.27. 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 β_* is surjective. \square

1.6 The snake lemma

Let $\alpha : A \rightarrow B$ be an R -module homomorphism. The **cokernel** of α 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 1.28 (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 α and β 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 ϕ and ψ 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** δ defined? Since β 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 ϕ is injective, and so $f(a) = x_1 - x_2$, and so $x_1 + \text{Im } f = x_2 + \text{Im } f$. So δ is well-defined.

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

1.7 Tensor products

Definition 1.29. 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 1.30 (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 1.31.

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 1.32. *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 1.33. *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 1.34. *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 1.35. *Suppose $\alpha : A \rightarrow B$ is surjective. Then $\alpha' : A \otimes_R M \rightarrow B \otimes_R M$ is surjective.*

Proof. Since α 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, α' 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 α' is the zero map, which is not injective.

Proposition 1.36. *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 β' is surjective, the sequence is exact at $C \otimes_R M$. We show it is exact at $B \otimes_R M$. Since β 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 β' induces a map

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

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

Definition 1.37. 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 1.38. Every projective module is flat.

This follows from two lemmas.

Lemma 1.39. $P \oplus Q$ 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 1.39 follows immediately. \square

Lemma 1.40. 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 1.39 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 in 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 1.38. Lemma 1.39 and Lemma 1.40 imply Proposition 1.38, since a projective module is a direct summand of a free module. \square

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.

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

1.8 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.

Proposition 1.41. *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 1.42 (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 1.43 (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 π_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 $|B| \leq |S|$. \square

Definition 1.44. 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 1.45. *The torsion elements of M form a submodule $T(M)$.*

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

Definition 1.46. If $T(M) = 0$, then M is **torsion-free**. If $T(M) = M$, then M is a **torsion module**.

Definition 1.47. 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 1.48. *The divisible elements of M form a submodule $D(M)$.*

Proof. Easy. □

Definition 1.49. If $D(M) = M$, then M is **divisible**.

Proposition 1.50.

- *If R is a PID then M is injective if and only if M is divisible.*
- *If R is a PID then M is flat if and only if M is torsion-free.*

Lecture 13 is a problems class.

Lecture 13
Friday
07/02/20