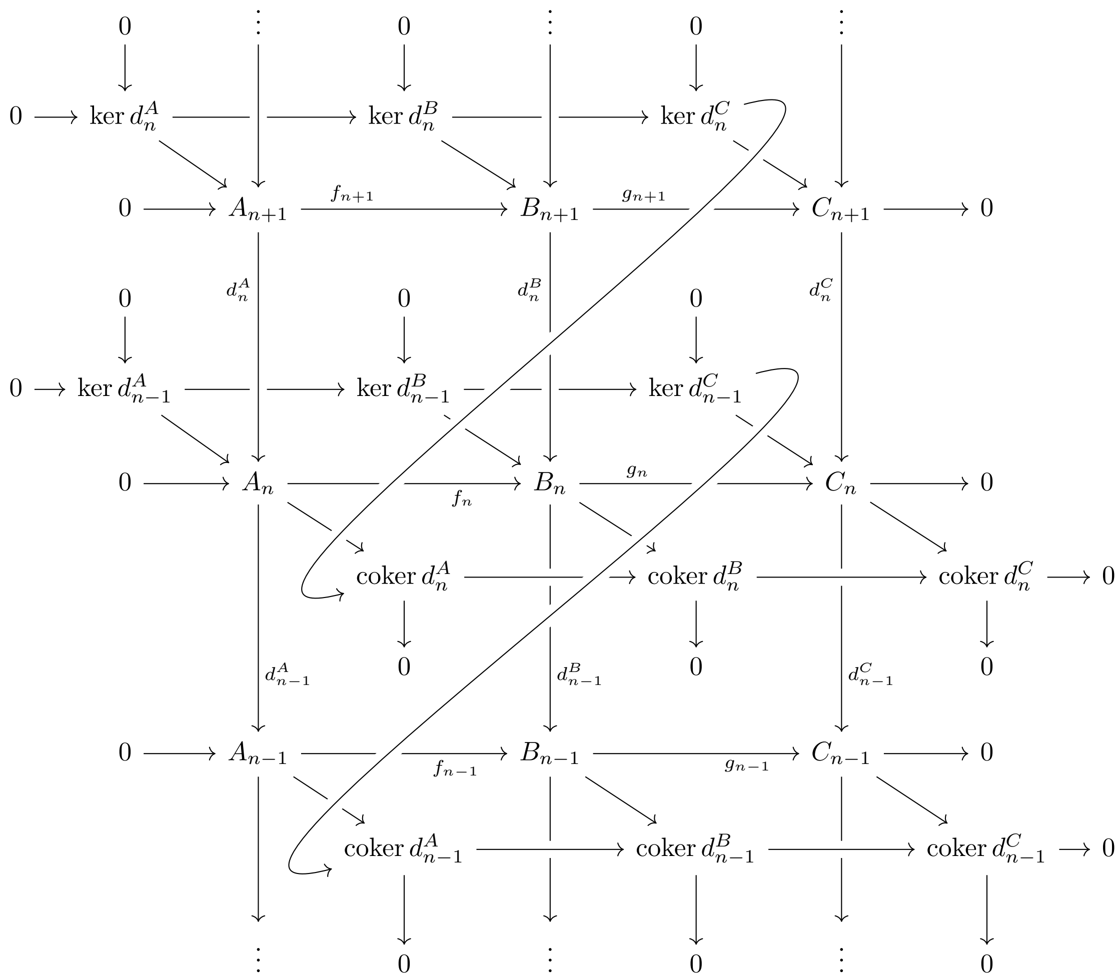
M4P63 Algebra IV

Lectured by Dr John Britnell
Typed by David Kurniadi Angdinata

Spring 2020



Syllabus

Exact sequences. Hom and tensor product. Projective and free modules. Injective and divisible modules. Torsion-free and flat modules. Projective and injective resolutions. Chain and cochain complexes. Homology and cohomology. Derived functors. Tor and torsion. Ext and extensions. Global dimension.

Contents

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 $\mathrm{Mat}_n\, k$, the $n \times n$ matrices with entries from k, a field.

1.1 Modules over rings

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

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

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 $rI \leq I$ 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 $\mathrm{Mat}_n\, k$-module, with $*$ as the usual matrix-vector multiplication.
- Let $M \in \mathrm{Mat}_n\, k$. Then we can define a left $k[x]$-module structure on k^* by letting x act as M on k^*. So $\left(x^2 + 3x - 2\right) * v = M^2 v + 3Mv - 2v$.
- 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 $M \times R \to M$ satisfying

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

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 $r *_{R^{\mathrm{op}}} s = s *_R r$.

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 $R = R^{\mathrm{op}}$.

Exercise. Show that $\mathrm{Mat}_n\, k \cong \mathrm{Mat}_n\, k^{\mathrm{op}}$.

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

1.2 Homomorphisms and submodules

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

$$\operatorname{im} f \leq M_2, \qquad \ker f \leq M_1, \qquad \operatorname{im} f \cong M/\ker f.$$

The other isomorphism theorems have R-module versions too.

1.3 Direct products and direct sums

Lecture 2
Monday
13/01/20

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

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

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

Definition 1.8. 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

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

and surjective maps

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

1.4 Exact sequences

Definition 1.9. 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 $f_n : M_n \to M_{n+1}$. Say the sequence is **exact at** M_n if

$$\operatorname{im} f_{n-1} = \ker f_n.$$

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

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

Note. α is injective and β is surjective.

The first isomorphism theorem implies that $B/\operatorname{im}\alpha \cong C$, where $\operatorname{im}\alpha \cong A$. An easy case is

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

with $\operatorname{im}\alpha = \operatorname{im}\iota_A = A \oplus 0$ and $\operatorname{im}\beta = \operatorname{im}\pi_\beta = C$. 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

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

Proposition 1.10. *A short exact sequence*

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

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

Such a σ is called a **section** of β.

Proof.

$\Longrightarrow$ 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.

$\Longleftarrow$ 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

$$\begin{tikzcd} & & A \oplus C \arrow[dd, "f"] \arrow[dr, "\pi_C"] & & \\ 0 \arrow[r] & A \arrow[ur, "\iota_A"] \arrow[dr, "\alpha"'] & & C \arrow[r] & 0 \\ & & B \arrow[ur, "\beta"'] & & \end{tikzcd}.$$

Define

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

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 $\alpha(a) \in \operatorname{im}\alpha = \ker\beta$, 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 $b - \sigma(c) \in \ker\beta = \operatorname{im}\alpha$. 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 1.11. *The short exact sequence*

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

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

Such a ρ is a **retraction** of α.

Proof.

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

$\Longleftarrow$ 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

$$\begin{array}{rccl} g & : & B & \longrightarrow & A \oplus C \\ & & b & \longmapsto & (\rho(a), \beta(c)) \end{array}.$$

□

[1] Exercise

2 Projective and injective modules

2.1 Projective modules

Lecture 3
Tuesday
14/01/20

Definition 2.1. An R-module M is **projective** if any surjective map $\beta : B \to M$ has a section. In other words, any short exact sequence

$$0 \to A \to B \to M \to 0$$

splits.

Example. The R-module R is projective. Let

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

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

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

Then σ is a section for β.

Proposition 2.2. *An R-module M is projective if and only if whenever $\beta : B \to C$ is surjective, and $f : M \to C$, there exists $g : M \to B$ such that $f = \beta \circ g$, so*

$$\begin{tikzcd} & & & M \arrow[d, "f"] \arrow[dl, dashed, "g"'] & \\ 0 \arrow[r] & A \arrow[r] & B \arrow[r, "\beta"'] & C \arrow[r] & 0 \end{tikzcd}.$$

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

Proof.

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

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

$$\begin{tikzcd} X \arrow[r, "\epsilon"] \arrow[d, "\delta"'] & M \arrow[d, "f"] \\ B \arrow[r, "\beta"'] & C \end{tikzcd}.$$

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 $\epsilon : X \to M$ is surjective. So ϵ has a section $\sigma : M \to X$. Define $g = \delta \circ \sigma : M \to B$, so

$$\begin{tikzcd} X \arrow[r, bend left, "\epsilon"] \arrow[d, "\delta"'] & M \arrow[l, dashed, bend left, "\sigma"] \arrow[d, "f"] \arrow[dl, dashed, "g"] \\ B \arrow[r, "\beta"'] & C \end{tikzcd}.$$

Since $\beta \circ \delta = f \circ \epsilon$, we have

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

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

$\square$

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

$$0 \to A \to X \to M \to 0.$$

2.2 Free modules

Definition 2.3. 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

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

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

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

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

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

Proposition 2.5. *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.

$\Longrightarrow$ 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 $F \to M$, which is clearly surjective. Then if $K = \ker \psi$, we have a short exact sequence

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

Since M is projective, there is a section σ for ψ, and so the short exact sequence splits, and $F \cong K \oplus M$. Lecture 4 Friday 17/01/20

$\Longleftarrow$ Suppose that $M \oplus N = F$, a free module with basis T. Suppose $\beta : B \to C$ is surjective, and that $f : M \to C$. Note that $f \circ \pi_M : F \to C$. 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 $\widehat{g} : F \to B$. Now define $g : M \to B$ by $g = \widehat{g} \circ \iota_M$. 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

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

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.

◻

2.3 Injective modules

Definition 2.6. Let M be an R-module. Then M is **injective** if whenever $\alpha : M \to B$ is an injective map, it has a retraction $\rho : B \to M$, so $\rho \circ \alpha = \mathrm{id}_M$. Equivalently, every short exact sequence

$$0 \to M \to B \to C \to 0$$

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 $\alpha : M \to N$ is a injective map. Then $\operatorname{im}\alpha$ is a submodule, or subspace, of N. Take a basis for $\operatorname{im}\alpha$, and extend to a basis for N. The basis vectors not in $\operatorname{im}\alpha$ form a basis for a complementary subspace U, so $N = \operatorname{im}\alpha \oplus U$. Now $\pi_{\operatorname{im}\alpha}$ is surjective, and $\alpha : M \to \operatorname{im}\alpha$ is an isomorphism. This gives a retraction $N \to M$.

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 $\alpha : \mathbb{Z} \to \mathbb{Q}$. But $\mathbb{Z}$ is not a quotient of $\mathbb{Q}$, [2] so no retraction exists for α.

Proposition 2.7. *An R-module M is injective if and only if whenever $\alpha : A \to B$ is injective, and $f : A \to M$, there exists $g : B \to M$ such that $f = g \circ \alpha$.*

Proof.

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

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

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "f"'] & B \arrow[d, "\delta"] \\ M \arrow[r, "\epsilon"'] & Y \end{tikzcd},$$

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 $\gamma : B \oplus M \to (B \oplus M)/K$ 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 $\rho : Y \to M$. Define $g : B \to M$ by $g = \rho \circ \delta$, so

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "f"'] & B \arrow[d, "\delta"] \arrow[dl, dashed, "g"'] \\ M \arrow[r, bend right, "\epsilon"'] & Y \arrow[l, dashed, bend right, "\rho"'] \end{tikzcd},$$

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

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

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

∎

[2] 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.

Lecture 5 Monday 20/01/20

Proposition 2.8 (Baer's criterion for injectivity)**.** *Let M be an R-module. Then M is injective if and only if every R-module map $f : I \to M$, where I is a left ideal of R, has the form $f(x) = xm$ for some $m \in M$. Equivalently, every map $I \to M$ extends to a map $R \to M$.*

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 $f : I \to M$ extends to $f^+ : R \to M$. 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 2.9 (Zorn's lemma)**.** *Let X be a non-empty set, partially ordered by $\le$. If every chain, or totally ordered subset, in X has an upper bound in X, then X has a maximal element.*

Proof.

$\Longleftarrow$ Suppose $\alpha : A \to B$, where α is injective. Suppose $f : A \to M$. We want to show there exists $g : B \to M$ such that $f = g \circ \alpha$. We have $\operatorname{im}\alpha \le B$. Define

$$X = \{(L, h) \mid \operatorname{im}\alpha \le L \le B,\ h : L \to M,\ f = h \circ \alpha\}.$$

Note that $X \ne \emptyset$ since $\left(\operatorname{im}\alpha, f \circ \alpha^{-1}\right)$ is in it. Define $\le$ on X by $(L_1, h_1) \le (L_2, h_2)$ if $L_1 \le L_2$ 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 $\operatorname{im}\alpha \le L \le B$. Define

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

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 $L_0 \ne B$. Let $b \in B \setminus L_0$. Note that $Rb \le B$. Consider

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

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 $I \to M$ 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

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

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 $\left(L_0 + Rb, h_0^+\right) \in X$, and $(L_0, h_0) < \left(L_0 + Rb, h_0^+\right)$, which contradicts the maximality of (L_0, h_0). Hence $L_0 = B$, and we are done.

$\Longrightarrow$ The converse is left as an exercise. [3]

$\square$

Example.

- Suppose R is a field. Then the only ideals of R are zero and R. Any map $0 \to M$, for M an R-module, can be extended to the zero map $R \to M$. 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

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

  If $k \ne 0, \pm 1$, then $f(k) = 1$, and so $f(x) \ne xm$ 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 $\mathbb{Z} \to \mathbb{Q}$ has no retraction.
- $\mathbb{Q}$ is injective as a $\mathbb{Z}$-module. Suppose we have a map $f : k\mathbb{Z} \to \mathbb{Q}$. 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.

[3] Exercise

3 Hom and tensor products

3.1 Hom

Lecture 6 Tuesday 21/01/20

Let A and B be two R-modules.

Definition 3.1. Define

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

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

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

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

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

Now suppose $s\in R$. We have $(rf)(sa)=rf(sa)=rsf(a)$. But for rf to be a homomorphism, we would need $(rf)(sa)=s(rf)(a)=srf(a)$. 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 3.2. *Suppose A,A_1,A_2,B,B_1,B_2,M are R-modules, and $\alpha:A\to B$.*

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

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

- *We can also define*

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

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 3.3. *Suppose $\alpha:A\to B$ is surjective. Then $\alpha^*:\mathrm{Hom}_R(B,M)\to\mathrm{Hom}_R(A,M)$ is injective.*

Proof. Suppose $f_1,f_2:B\to M$ 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 $f_1=f_2$. ☐

Proposition 3.4. *Suppose $\alpha:A\to B$ is injective. Then $\alpha_*:\mathrm{Hom}_R(M,A)\to\mathrm{Hom}_R(M,B)$ is injective.*

Proof. Suppose $f_1,f_2:M\to A$, 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 $m\in M$. ☐

Proposition 3.5. *Suppose*

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

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

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

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

$$g \in \ker \alpha^* \iff \alpha^*(g) = 0 \iff g \circ \alpha = 0 \iff g(\alpha(A)) = 0 \iff \mathrm{im}\, \alpha \le \ker g \iff \ker \beta \le \ker g,$$

Then $g \in \ker \alpha^*$ 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

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

is well-defined, since β is surjective, and f is an R-module homomorphism. Thus

$$g \in \ker \alpha^* \qquad \iff \qquad \exists f \in \mathrm{Hom}_R(C, M),\ \beta^*(f) = g \qquad \iff \qquad g \in \mathrm{im}\, \beta^*.$$

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

Lecture 7
Friday
24/01/20

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

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

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

  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 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$, so α^* is not surjective.

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

Proposition 3.6. *Let*

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

be exact. Then

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

is exact.

Proof. We already know that α injective implies that α_* is injective, so the sequence is exact at $\mathrm{Hom}_R(M, A)$. We show that $\ker \beta_* = \mathrm{im}\, \alpha_*$. Suppose $g \in \mathrm{Hom}_R(M, B)$. Then

$$g \in \ker \beta_* \qquad \iff \qquad (\beta \circ g)(M) = 0 \qquad \iff \qquad \mathrm{im}\, g \le \ker \beta \qquad \iff \qquad \mathrm{im}\, g \le \mathrm{im}\, \alpha.$$

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

$$g \in \ker \beta_* \qquad \iff \qquad \mathrm{im}\, g \le \mathrm{im}\, \alpha \qquad \iff \qquad g \in \mathrm{im}\, \alpha_*.$$

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

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

- Let
$$\begin{array}{cccc} \beta & : & \sum_{q \in \mathbb{Q}} \mathbb{Z} & \longrightarrow & \mathbb{Q} \\ & & e_q & \longmapsto & q \end{array}.$$
In general $\beta : \sum_{m \in M} R \to M$ 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 $\beta_* : \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \sum_{q \in \mathbb{Q}} \mathbb{Z}\right) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q})$. Claim that $\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Q}, \sum_{q \in \mathbb{Q}} \mathbb{Z}\right)$ is trivial. Suppose $f : \mathbb{Q} \to \sum_{q \in \mathbb{Q}} \mathbb{Z}$ 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 $\mathbb{Q} \to \mathbb{Z} e_{q_1}$ exists. But $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q})$ is not trivial, so β_* is not surjective.

- Let
$$0 \to \mathbb{Z}_2 \to \mathbb{Z}_4 \to \mathbb{Z}_2 \to 0$$
be a short exact sequence of $\mathbb{Z}$-modules. Then we have
$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) & \xrightarrow{\alpha_*} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_4) & \xrightarrow{\beta_*} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_2, \mathbb{Z}_2) \\ & & \cong & & \cong & & \cong \\ & & \mathbb{Z}_2 & & \mathbb{Z}_2 & & \mathbb{Z}_2 \end{array}.$$
But there is no short exact sequence of abelian groups
$$0 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \to \mathbb{Z}_2 \to 0,$$
and so β_* cannot be surjective.

Proposition 3.7. *Let M be an R-module. Then M is injective if and only if for every injective map $\alpha : A \to B$, we get $\alpha^* : \mathrm{Hom}_R(B, M) \to \mathrm{Hom}_R(A, M)$ is surjective.*

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

Proposition 3.8. *Let M be an R-module. Then M is projective if and only if whenever $\beta : B \to C$ is surjective, the map $\beta_* : \mathrm{Hom}_R(M, B) \to \mathrm{Hom}_R(M, C)$ is surjective.*

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

3.2 The snake lemma

Lecture 8 Monday 27/01/20

Let $\alpha : A \to B$ be an R-module homomorphism. The **cokernel** of α is $B / \mathrm{im}\, \alpha$, written $\mathrm{coker}\, \alpha$. The sequence
$$0 \to \ker \alpha \to A \xrightarrow{\alpha} B \to \mathrm{coker}\, \alpha \to 0$$
is exact.

Lemma 3.9 (The snake lemma)**.** *Suppose we have a commutative diagram*
$$\begin{tikzcd} & A \arrow[r, "\alpha"] \arrow[d, "f"] & B \arrow[r, "\beta"] \arrow[d, "g"] & C \arrow[r] \arrow[d, "h"] & 0 \\ 0 \arrow[r] & X \arrow[r, "\phi"'] & Y \arrow[r, "\psi"'] & Z & \end{tikzcd},$$
where the rows are exact. Then we obtain an exact sequence
$$\ker f \xrightarrow{\alpha} \ker g \xrightarrow{\beta} \ker h \xrightarrow{\delta} \mathrm{coker}\, f \xrightarrow{\overline{\phi}} \mathrm{coker}\, g \xrightarrow{\overline{\psi}} \mathrm{coker}\, h.$$

Proof.

- The maps $\alpha : \ker f \to \ker g$ and $\beta : \ker g \to \ker h$ are obtained simply by restricting α and β respectively. Observe that if $a \in \ker f$ 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 $\alpha(a) \in \ker g$, which is what we wanted.

- The maps $\overline{\phi} : \operatorname{coker} f \to \operatorname{coker} g$ and $\overline{\psi} : \operatorname{coker} g \to \operatorname{coker} h$ are induced from ϕ and ψ by
$$\overline{\phi}(x + \operatorname{im} f) = \phi(x) + \operatorname{im} g, \qquad \overline{\psi}(y + \operatorname{im} g) = \psi(g) + \operatorname{im} h.$$
Check that these maps make sense. Suppose $x_1 + \operatorname{im} f = x_2 + \operatorname{im} f$. Then $x_1 - x_2 \in \operatorname{im} f$, so there exists $a \in A$ such that $f(a) = x_1 - x_2$. Now
$$\phi(x_1) - \phi(x_2) = \phi(x_1 - x_2) = (\phi \circ f)(a) = (g \circ \alpha)(a) \in \operatorname{im} g.$$
So $\phi(x_1) + \operatorname{im} g = \phi(x_2) + \operatorname{im} g$. So $\overline{\phi}$ is well-defined, and $\overline{\psi}$ 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 $c \in \ker h$. Then $(h \circ \beta)(b) = 0$, so $(\psi \circ g)(b) = 0$. Hence $g(b) \in \ker \psi = \operatorname{im} \phi$. Define
$$\delta(c) = x + \operatorname{im} f, \qquad \phi(x) = g(b), \qquad \beta(b) = c.$$
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 $b_1 - b_2 \in \ker \beta = \operatorname{im} \alpha$. 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 $x_1 + \operatorname{im} f = x_2 + \operatorname{im} f$. So δ is well-defined.

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

3.3 Tensor products

Definition 3.10. 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
$$l_1 \otimes m + l_2 \otimes m = (l_1 + l_2) \otimes m, \qquad l_1, l_2 \in L, \qquad m \in M,$$
$$l \otimes m_1 + l \otimes m_2 = l \otimes (m_1 + m_2), \qquad l \in L, \qquad m_1, m_2 \in M,$$
$$(lr) \otimes m = l \otimes (rm), \qquad l \in L, \qquad m \in M, \qquad r \in R.$$

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
$$l = \sum_{i=1}^p a_i s_i, \qquad m = \sum_{i=1}^q b_j t_j, \qquad s_i \in S, \qquad t_i \in T, \qquad a_i, b_i \in \mathbb{Z},$$
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 $y \in \mathbb{Z}_3$,

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

Lecture 9 Tuesday 28/01/20

Theorem 3.11 (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 $f : A \times B \to C$ be a map, not necessarily a homomorphism, which is $\mathbb{Z}$-linear in both arguments, so*

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

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

and such that

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

Then there is a unique homomorphism

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

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

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

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

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

So g' extends uniquely to a homomorphism $F \to C$. The conditions stipulated on f guarantee that $g'(K) = 0$. So g' induces a map $g : F/K \to C$, 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. □

Corollary 3.12.

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

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

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

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

This induces a homomorphism

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

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

2. By the same argument as 1.

□

Corollary 3.13. *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*
$$\begin{array}{rcrcl} f & : & (A \oplus B) \otimes_R C & \longrightarrow & (A \otimes_R C) \oplus (B \otimes_R C) \\ & & (a,b) \otimes c & \longmapsto & (a \otimes c, b \otimes c) \end{array}.$$

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,
$$\begin{array}{rcl} A \oplus B \times C & \longrightarrow & (A \otimes_R C) \oplus (B \otimes_R C) \\ ((a,b), c) & \longmapsto & (a \otimes c, b \otimes c) \end{array}.$$
This induces a homomorphism $f : (A \oplus B) \otimes_R C \to (A \otimes_R C) \oplus (B \otimes_R C)$ with the description as given above. Now take the bilinear map given by
$$\begin{array}{rcl} A \times C & \longrightarrow & (A \oplus B) \otimes_R C \\ (a,c) & \longmapsto & (a,0) \otimes c \end{array}.$$
This induces a homomorphism $g_1 : A \otimes_R C \to (A \oplus B) \otimes_R C$. Similarly, we get a homomorphism $g_2 : B \otimes_R C \to (A \oplus B) \otimes_R C$. Now define
$$\begin{array}{rcrcl} g = g_1 \oplus g_2 & : & (A \otimes_R C) \oplus (B \otimes_R C) & \longrightarrow & (A \oplus B) \otimes_R C \\ & & (x,y) & \longmapsto & g_1(x) + g_2(y) \end{array}.$$
It is easy to check that f and g are mutually inverse, so both isomorphisms.

2. Similarly.

$\square$

Corollary 3.14. *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
$$\begin{array}{rcrcl} f & : & A & \longrightarrow & \mathbb{Z}_n \otimes_{\mathbb{Z}} A \\ & & a & \longmapsto & 1 \otimes a \end{array}.$$
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 $nA \leq \ker f$. So f induces a map
$$\overline{f} : A/nA \to \mathbb{Z}_n \otimes_{\mathbb{Z}} A.$$
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 $\overline{f}$ is surjective. For injectivity, use the universal property. We have a bilinear map
$$\begin{array}{rcrcl} g & : & \mathbb{Z}_n \times A & \longrightarrow & A/nA \\ & & (k,a) & \longmapsto & ka + nA \end{array}.$$
This is well-defined and bilinear. So extends to a homomorphism
$$\overline{g} : \mathbb{Z}_n \otimes_{\mathbb{Z}} A \to A/nA.$$
It is easy to check that $\overline{g} \circ \overline{f} = \mathrm{id}_{A/nA}$, so $\overline{f}$ is injective.

2. Similarly.

$\square$

Lecture 10 Friday 31/01/20

Proposition 3.15. *Let $\alpha : A \to B$ be a homomorphism of right R-modules. Let M be a left R-module. There is a unique abelian group homomorphism*

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

Proof. The set map defined by

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

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 $\alpha' : A \otimes_R M \to B \otimes_R M$ with the properties claimed. ☐

Proposition 3.16. *Suppose $\alpha : A \to B$ is surjective. Then $\alpha' : A \otimes_R M \to B \otimes_R M$ 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 $b \otimes m = \alpha'(a \otimes m) \in \operatorname{im} \alpha'$. Since $B \otimes_R M$ is generated by its pure tensors, α' is surjective. ☐

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

Example. Let

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

which is injective. Consider

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

So α' is the zero map, which is not injective.

Proposition 3.17. *Let*

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

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

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

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 $C \to B$, which is not uniquely defined in general. Suppose that $\beta(b) = c$. Then $b - f(c) \in \ker \beta = \operatorname{im} \alpha$, so $f(c) + \operatorname{im} \alpha = b + \operatorname{im} \alpha$. Define a set map by

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

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

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

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

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

By the universal property, there is a unique homomorphism

$$\begin{array}{rrcl} \psi & : & C \otimes_R M & \longrightarrow & (B \otimes_R M) / \operatorname{im} \alpha' \\ & & c \otimes m & \longmapsto & f(c) \otimes m + \operatorname{im} \alpha' \end{array}.$$

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

$$\phi : (B \otimes_R M) / \operatorname{im} \alpha' \to C \otimes_R M.$$

It is easy to check that ϕ and ψ are mutually inverse, and so both are isomorphisms. In particular ϕ is injective, and so $\operatorname{im} \alpha' = \ker \beta'$ as required. □

3.4 Flat modules

Definition 3.18. A left R-module M is **flat** if $A \to B$ is injective implies that $A \otimes_R M \to B \otimes_R M$ is injective.

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

$$0 \to A \to B \to C \to 0$$

corresponds to a short exact sequence of abelian groups

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

Proposition 3.19. *Every projective module is flat.*

This follows from two lemmas.

Lemma 3.20. *$P \oplus Q$ 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 $\alpha : A \to B$ is injective. Then $\alpha' : A \otimes_R (P \oplus Q) \to B \otimes_R (P \oplus Q)$ corresponds to

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

It is clear from this that $\overline{\alpha'}$ is injective if and only if $A \otimes_R P \to B \otimes_R P$ and $A \otimes_R Q \to B \otimes_R Q$ are injective, and Lemma 3.20 follows immediately. □

Lemma 3.21. *Every free R-module is flat.*

Lecture 11 is a problems class.

Lecture 11 Monday 03/02/20

Lecture 12 Tuesday 04/02/20

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 3.20 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 in A, we have $A \otimes_R R \cong A$, so

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, phantom, "\cong"] & B \arrow[d, phantom, "\cong"] \\ A \otimes_R R \arrow[r, dashed, "\alpha'"'] & B \otimes_R R \end{tikzcd},$$

and it is easy to check that R is flat. □

Proof of Proposition 3.19. Lemma 3.20 and Lemma 3.21 imply Proposition 3.19, since a projective module is a direct summand of a free module. □

4 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.

4.1 Free and projective modules

Proposition 4.1. *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 $F_1 \le F_2$, 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 $|B_1| \le |B_2|$. In particular, if $M \le R^n$, then $M \cong R^m$ for some $m \le n$. For this, we will need the well-ordering theorem.

Theorem 4.2 (Well-ordering theorem)**.** *Let X be a set. There exists a well-order $\le$ on X, that is a total order such that every non-empty subset of X has a least element.*

Corollary 4.3 (Transfinite induction)**.** *Let X be a non-empty set well-ordered by $\le$. 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 $\le$ be a well-order on S. For $s \in S$, let π_s be the projection map $F \to R$ onto the s-coordinate. Let e_s be the element of F with one in coordinate s, and zero elsewhere. Suppose $U \le F$ is an R-submodule of F. Define R_t to be the submodule of F generated by $\{e_s \mid s \le t\}$, so

$$R_t = \mathrm{sp}\{e_s \mid s \le t\}.$$

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

$$U_t = U \cap R_t.$$

So $t_1 < t_2$ implies that $U_{t_1} \le U_{t_2}$. 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

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

- Claim that B generates U. We will actually prove that $B_t = \{u_s \mid s \le t\}$ 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 $\pi_{t_0}(u) = r a_{t_0}$. Hence $\pi_{t_0}(u - r u_{t_0}) = 0$. So $u - r u_{t_0}$ has zero in the t_0-coordinate, so $u - r u_{t_0} \in \mathrm{sp}\{e_s \mid s < t_0\}$. Clearly $u - r u_{t_0} \in U$. We have $u - r u_{t_0} = \sum_{i=1}^q r_i e_{s_i}$, where $s_i < t_0$, and $s_1 < \dots < s_q$. Then

$$u - r u_{t_0} \in U \cap R_{s_q} = U_{s_q} = \mathrm{sp}\, B_{s_q},$$

by the inductive hypothesis. Hence $u \in \mathrm{sp}\left(B_{s_q} \cup \{u_{t_0}\}\right) \subseteq \mathrm{sp}\, B_{t_0}$. 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 $a_{s_k} \ne 0$, 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 $|B| \le |S|$. □

Lecture 13 is a problems class.

Lecture 13 Friday 07/02/20

4.2 Injective and divisible modules

Lecture 14 Monday 10/02/20

Definition 4.4. 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 4.5. *The divisible elements of M form a submodule $\mathrm{D}(M)$.*

Proof. Easy. ☐

Definition 4.6. If $\mathrm{D}(M) = M$, then M is **divisible**.

Proposition 4.7. *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

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

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

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

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

Proposition 4.8. *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 $f : I \to M$ 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 $R \to M$ extends f. So assume $a \neq 0$. Since m is divisible, there exists $l \in M$ with $al = m$. Now the map given by

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

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

4.3 Flat and torsion-free modules

Definition 4.9. 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 4.10. *The torsion elements of M form a submodule $\mathrm{T}(M)$.*

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

Definition 4.11. If $\mathrm{T}(M) = 0$, then M is **torsion-free**. If $\mathrm{T}(M) = M$, then M is a **torsion module**.

Proposition 4.12. *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

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

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

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

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 4.13. *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 $\alpha : A \to B$ is injective, so is $\alpha' : A \otimes_R M \to B \otimes_R M$, where M is torsion-free.

1. Prove this in the case that B is free, and A is a submodule of B, and α 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 4.14. *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 $g : I \otimes_R M \to R \otimes_R M$ is injective.*

Proof. The homomorphism given by

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

gives a map $f : R \otimes_R M \to I \otimes_R M$. 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. ☐

Lemma 4.15. *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 $A_0 \le A$ 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

$$A \otimes_R M = \mathrm{F}_{\mathrm{ab}} (A \times M) / K,$$

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 $\mathrm{F}_{\mathrm{ab}} (A \times M)$, 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 $\mathrm{F}_{\mathrm{ab}} (A_0 \times M)$ so $\sum_{i=1}^t (a_i \otimes m_i) = 0$ in $A_0 \otimes_R M$. Clearly A_0 is finitely generated. ☐

Lecture 15 Tuesday 11/02/20

Lemma 4.16. *Let $F = \mathrm{F}(S) = \bigoplus_{s \in S} R$. Let U be a finitely generated submodule of F. Then there exists a finite $T \subseteq S$ such that $U \le \mathrm{F}(T)$, and for any M, the map $\mathrm{F}(T) \otimes_R M \to \mathrm{F}(S) \otimes_R M$ 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 $U \le \mathrm{F}(T)$. We have

$$\mathrm{F}(S) = \mathrm{F}(T) \oplus \mathrm{F}(S \setminus T),$$

and so

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

It follows that the natural map $\mathrm{F}(T) \otimes_R M \to \mathrm{F}(S) \otimes_R M$ is injective. ☐

Lemma 4.15 and Lemma 4.16 tell us that if F is free and $U \leq F$, and if M is an R-module, if $U \otimes_R M \to F \otimes_R M$ is not injective, then there exists a finitely generated $U_0 < U$ and a finite rank free submodule $F_0 < F$ such that $U_0 \otimes_R M \to F_0 \otimes_R M$ is not injective.

Lemma 4.17. *Let R be a PID. Let F be free, and $U \leq F$. Let M be torsion-free. Then $U \otimes_R M \to F \otimes_R M$ 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 4.14, $U \otimes_R M \to F \otimes_R M$ is injective in this case.

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

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

We also have a short exact sequence

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

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

$$\begin{tikzcd} 0 \arrow[r] & U_1 \arrow[r] \arrow[d] & U \arrow[r] \arrow[d] & \pi_{R^{n-1}}(U) \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & R \arrow[r] & R^n \arrow[r] & R^{n-1} \arrow[r] & 0 \end{tikzcd},$$

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

$$\begin{tikzcd} & U_1 \otimes_R M \arrow[r] \arrow[d, "f"] & U \otimes_R M \arrow[r] \arrow[d, "g"] & \pi_{R^{n-1}}(U) \otimes_R M \arrow[r] \arrow[d, "h"] & 0 \\ 0 \arrow[r] & R \otimes_R M \arrow[r] & R^n \otimes_R M \arrow[r] & R^{n-1} \otimes_R M \arrow[r] & 0 \end{tikzcd}.$$

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

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

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

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

Now f is injective by Lemma 4.14, and h is injective by the inductive hypothesis. The snake lemma tells us that the sequence

$$\ker f \to \ker g \to \ker h$$

is exact at $\ker g$. So

$$0 \to \ker g \to 0$$

is exact, and so $\ker g = 0$. So g is injective, and this completes the induction.

$\square$

Proof of Proposition 4.13. Prove that if $\alpha : A \to B$ is injective, and M is torsion-free, over a PID R, then $\alpha' : A \otimes_R M \to B \otimes_R M$ is injective. There exists a free module F such that B is quotient of F. So there is a short exact sequence

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

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

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

We have a commuting diagram

$$\begin{tikzcd} & & F_A \arrow[r] \arrow[dd, hook] & \alpha A \arrow[r] \arrow[dd, hook] & 0 \\ 0 \arrow[r] & K \arrow[ur] \arrow[dr] & & & \\ & & F \arrow[r] & B \arrow[r] & 0 \end{tikzcd}.$$

Tensoring with M,

$$\begin{tikzcd} & F_A \otimes_R M \arrow[r, "\gamma"] \arrow[dd, "f"] & \alpha A \otimes_R M \arrow[r] \arrow[dd, "g"] & 0 \\ K \otimes_R M \arrow[ur, "\beta"] \arrow[dr, "\delta"'] & & & \\ & F \otimes_R M \arrow[r, "\epsilon"'] & B \otimes_R M \arrow[r] & 0 \end{tikzcd}$$

is commuting, and exact along rows. Let $u \in \ker g \leq \alpha A \otimes_R M \cong A \otimes_R M$. Since γ 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 $f(w) \in \ker \epsilon = \operatorname{im} \delta$, so $f(w) = \delta(k)$ for $k \in K \otimes_R M$. Since f is injective, by Lemma 4.17, we get $w = \beta(k) \in \operatorname{im} \beta$. So $w \in \ker \gamma$, 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.

4.4 Modules over PIDs

Lecture 16
Friday
14/02/20

For an R-module M

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

Over a PID

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

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

Example. 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, $\mathrm{D}(F) = \{0\}$. But $\mathrm{D}(\mathbb{Q}) = \mathbb{Q}$. Hence $\mathbb{Q} \ncong F$. So $\mathbb{Q}$ is an example of a flat module which is not projective.

5 Projective and injective resolutions

Definition 5.1. Let M be an R-module. A **resolution**, or **left resolution**, for M is a sequence of R-modules $A_0, A_1, A_2, \ldots$, with homomorphisms $d : A_{i+1} \to A_i$, and also a homomorphism $A_0 \to M$, such that

$$\ldots \xrightarrow{d} A_2 \xrightarrow{d} A_1 \xrightarrow{d} A_0 \to M \to 0$$

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.

Definition 5.2. A **right resolution**, or **coresolution**, for M is a sequence of R-modules $A^0, A^1, A^2, \ldots$, with homomorphisms $d : A^i \to A^{i+1}$, and $M \to A^0$, such that

$$0 \to M \to A^0 \xrightarrow{d} A^1 \xrightarrow{d} A^2 \xrightarrow{d} \ldots$$

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.

5.1 Existence of projective resolutions

Proposition 5.3. *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 exist a free module F and $K \leq F$ such that $L \cong F/K$. So we get a short exact sequence

$$0 \to K \to F \to L \to 0.$$

It follows that we can find $F_0, F_1, F_2, \ldots$, and $K_0 \leq F_0, K_1 \leq F_1, K_2 \leq F_2, \ldots$ such that

$$0 \to K_0 \to F_0 \to M \to 0, \qquad 0 \to K_1 \to F_1 \to K_0 \to 0, \qquad 0 \to K_2 \to F_2 \to K_1 \to 0, \qquad \ldots$$

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

$$\cdots \to F_2 \to F_1 \to F_0 \to M \to 0$$

is exact, and a free resolution for M. $\square$

5.2 Existence of injective resolutions

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

Proof. Start by defining $f_0 : \langle a \rangle \to \mathbb{Q}/\mathbb{Z}$. 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

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

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. 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

$$\begin{array}{rcccl} f & : & B & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & & b & \longmapsto & f_s(b) \end{array}, \qquad b \in B_s.$$

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 $\langle B, x\rangle \le A$, and $\langle B, x\rangle \cong (B \oplus \langle x\rangle) / \langle nx - b_0\rangle$, where $b_0 = nx$ in A. Define

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

so sending x to $f(b_0)/n$. We see that $\phi(nx - b_0) = 0$, so ϕ induces a map $(B \oplus \langle x\rangle) / \langle nx - b_0\rangle \to \mathbb{Q}/\mathbb{Z}$, and hence a map $f' : \langle B, x\rangle \to \mathbb{Q}/\mathbb{Z}$. 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. ☐

Lecture 17 Monday 17/02/20

Proposition 5.5. *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 $s \in S$, $f_s : A \to \mathbb{Q}/\mathbb{Z}$ such that $f_s(s) \neq 0$. Define

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

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. ☐

Proposition 5.6. *Let M be a right R-module, and let A be an abelian group. Then $\mathrm{Hom}_{\mathbb{Z}}(M, A)$ 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. ☐

Proposition 5.7. *Let M be a left R-module, and A an abelian group. Then $\mathrm{Hom}_{\mathbb{Z}}(R, A)$ is a left R-module, and there is a natural isomorphism*

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

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

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

Check the following.

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

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

- Φ is a homomorphism, since

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

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

Now define

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

Check the following.

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

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

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

- Ψ 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 $\Psi \circ \Phi = \mathrm{id}_{\mathrm{Hom}_R(M,H)}$ and $\Phi \circ \Psi = \mathrm{id}_{\mathrm{Hom}_{\mathbb{Z}}(M,A)}$. [4] Hence Φ and Ψ are isomorphisms. ☐

We are interested in the case $A = \mathbb{Q}/\mathbb{Z}$. Write $S = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. Lecture 18 Tuesday 18/02/20

Proposition 5.8. *S is injective as a left R-module.*

Proof. Let M and N be R-modules, and $\alpha : M \to N$ an injective homomorphism. By identifying M with $\mathrm{im}\,\alpha$, we may assume that $M \leq N$, and α is the inclusion map. Since $\mathbb{Q}/\mathbb{Z}$ is injective as an abelian group, any $\mathbb{Z}$-module homomorphism $M \to S$ extends to a homomorphism $N \to S$. Define

$$\begin{array}{cccc} \Theta & : & \mathrm{Hom}_{\mathbb{Z}}(N,\mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z}) \\ & & f & \longmapsto & f|_M \end{array},$$

the restriction to M. We see that Θ is surjective. Similarly, we can define

$$\begin{array}{cccc} \Theta' & : & \mathrm{Hom}_R(N,S) & \longrightarrow & \mathrm{Hom}_R(M,S) \\ & & f & \longmapsto & f|_M \end{array}.$$

Then Θ' is an abelian group homomorphism. But we know there is a naturally defined isomorphism between $\mathrm{Hom}_R(M,S)$ and $\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z})$. So we get

$$\begin{tikzcd} \mathrm{Hom}_{\mathbb{Z}}(N,\mathbb{Q}/\mathbb{Z}) \arrow[r, "\Theta"] \arrow[d, "\Psi"', "\sim"] & \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Q}/\mathbb{Z}) \arrow[d, "\sim"', "\Psi"] \\ \mathrm{Hom}_R(N,S) \arrow[r, "\Theta'"'] & \mathrm{Hom}_R(M,S) \end{tikzcd}.$$

It is easy to see that this diagram commutes. It follows that Θ' is surjective. So any R-module homomorphism $M \to S$ extends to a homomorphism $N \to S$. Hence S is injective. ☐

[4] Exercise

Proposition 5.9. *Let M be a left R-module, and $m \in M \setminus \{0\}$. Then there exists $f : M \to S$ such that $f(m) \neq 0$.*

Proof. We know there is an abelian group homomorphism $g : M \to \mathbb{Q}/\mathbb{Z}$ such that $g(m) \neq 0$. Now $\Psi(g) \in \mathrm{Hom}_R(M, S)$, and $\Psi(g)(m)(1) = g(m) \neq 0$ for $1 \in R$, so $\Psi(g)(m)$ is not the zero map. $\square$

Proposition 5.10. *Let M be a left R-module. There exists an injective R-module I such that M is isomorphic to a submodule of I. Equivalently, there exists an injection $M \to I$.*

Proof. Same as abelian groups. Let $T = M \setminus \{0\}$. Then $I = \prod_{t \in T} S$ is injective. Let f_t be a homomorphism $M \to S$ such that $f_t(t) \neq 0$. Then

$$\begin{array}{cccc} f & : & M & \longrightarrow & I \\ & & m & \longmapsto & (f_t(m))_{t \in T} \end{array}$$

is injective, and a homomorphism. $\square$

Proposition 5.11. *Every R-module admits an injective resolution.*

Thus there exist injective $I_0, I_1, I_2, \dots$ such that

$$0 \to M \to I_0 \to I_1 \to I_2 \to \dots$$

is exact.

Proof. Let M be an R-module. Then M injects into some injective module I_0. Let $C_0 = I_0 / \mathrm{im}(M \to I_0)$. Then C_0 injects into some injective I_1. This induces a map $I_0 \to I_1$ whose kernel is $\mathrm{im}(M \to I_0)$. Further terms in the sequence are constructed in an identical manner. $\square$

5.3 Uniqueness of projective resolutions

Proposition 5.12. *Let M and N be R-modules, and $\phi : M \to N$. Let (P_i) be a projective resolution for M, and (Q_i) a projective resolution for N.*

1. *There exist R-module homomorphisms $f_i : P_i \to Q_i$ such that the diagram*

$$\begin{tikzcd} \dots \arrow[r, "d_2"] & P_2 \arrow[r, "d_1"] \arrow[d, dashed, "f_2"] & P_1 \arrow[r, "d_0"] \arrow[d, dashed, "f_1"] & P_0 \arrow[r, "p"] \arrow[d, dashed, "f_0"] & M \arrow[r] \arrow[d, "\phi"] & 0 \\ \dots \arrow[r, "d_2'"'] & Q_2 \arrow[r, "d_1'"'] & Q_1 \arrow[r, "d_0'"'] & Q_0 \arrow[r, "q"'] & N \arrow[r] & 0 \end{tikzcd}$$

commutes.

2. *Let $g_i : P_i \to Q_i$ be such that the diagram*

$$\begin{tikzcd} \dots \arrow[r, "d_2"] & P_2 \arrow[r, "d_1"] \arrow[d, bend right, "g_2"'] \arrow[d, bend left, "f_2"] & P_1 \arrow[r, "d_0"] \arrow[d, bend right, "g_1"'] \arrow[d, bend left, "f_1"] & P_0 \arrow[r, "p"] \arrow[d, bend right, "g_0"'] \arrow[d, bend left, "f_0"] & M \arrow[r] \arrow[d, "\phi"] & 0 \\ \dots \arrow[r, "d_2'"'] & Q_2 \arrow[r, "d_1'"'] & Q_1 \arrow[r, "d_0'"'] & Q_0 \arrow[r, "q"'] & N \arrow[r] & 0 \end{tikzcd}$$

commutes. Then there exist homomorphisms $s_i : P_i \to Q_{i+1}$ such that

$$g_i - f_i = \begin{cases} s_{i-1} \circ d_{i-1} + d_i' \circ s_i & i > 0 \\ d_0' \circ s_0 & i = 0 \end{cases},$$

so

$$\begin{tikzcd} \dots \arrow[r, "d_2"] & P_2 \arrow[r, "d_1"] \arrow[dl, dashed, "s_2"'] & P_1 \arrow[r, "d_0"] \arrow[dl, dashed, "s_1"'] & P_0 \arrow[r, "p"] \arrow[dl, dashed, "s_0"'] & M \arrow[r] \arrow[d, "\phi"] & 0 \\ \dots \arrow[r, "d_2'"'] & Q_2 \arrow[r, "d_1'"'] & Q_1 \arrow[r, "d_0'"'] & Q_0 \arrow[r, "q"'] & N \arrow[r] & 0 \end{tikzcd}.$$

Proof.

1. The map $q : Q_0 \to N$ is surjective. There is a map $p : P_0 \to N$, given by composing $P_0 \to M$ with ϕ. Since P_0 is projective there exists $f_0 : P_0 \to Q_0$ such that $p = q \circ f_0$. Suppose the maps $f_0, \dots, f_{t-1}$ have been constructed, so

$$\begin{tikzcd} \dots \arrow[r, "d_t"] & P_t \arrow[r, "d_{t-1}"] \arrow[d, dashed, "f_t"] & P_{t-1} \arrow[r, "d_{t-2}"] \arrow[d, "f_{t-1}"] & P_{t-2} \arrow[r] \arrow[d, "f_{t-2}"] & \dots \\ \dots \arrow[r, "d'_t"'] & Q_t \arrow[r, "d'_{t-1}"'] & Q_{t-1} \arrow[r, "d'_{t-2}"'] & Q_{t-2} \arrow[r] & \dots \end{tikzcd}.$$

Observe that $d'_{t-2} \circ f_{t-1} \circ d_{t-1} = f_{t-2} \circ d_{t-2} \circ d_{t-1}$, since the existing squares of the diagram commute. But $d_{t-2} \circ d_{t-1} = 0$. So $d'_{t-2} \circ f_{t-1} \circ d_{t-1} = 0$, so $\operatorname{im}(f_{t-1} \circ d_{t-1}) \le \ker d'_{t-2} = \operatorname{im} d'_{t-1}$. Now the map $d'_{t-1} : Q_t \to \operatorname{im} d'_{t-1}$ is obviously surjective, and P_t is projective. So there is a map $f_t : P_t \to Q_t$ such that $f_{t-1} \circ d_{t-1} = d'_{t-1} \circ f_t$. Now inductively, maps f_i exist for all i.

2. We want s_i such that $g_i - f_i = d'_i \circ s_i + s_{i-1} \circ d_{i-1}$. Let $h_i = g_i - f_i$. We see that the diagram

$$\begin{tikzcd} \dots \arrow[r, "d_2"] & P_2 \arrow[r, "d_1"] \arrow[d, "h_2"] & P_1 \arrow[r, "d_0"] \arrow[d, "h_1"] & P_0 \arrow[r, "p"] \arrow[d, "h_0"] & M \arrow[r] \arrow[d, "0"] & 0 \\ \dots \arrow[r, "d'_2"'] & Q_2 \arrow[r, "d'_1"'] & Q_1 \arrow[r, "d'_0"'] & Q_0 \arrow[r, "q"'] & N \arrow[r] & 0 \end{tikzcd}$$

commutes, since we want $h_i \circ d_i = d'_i \circ h_{i+1}$, but we have

$$h_i \circ d_i = g_i \circ d_i - f_i \circ d_i = d'_i \circ g_{i+1} - d'_i \circ f_{i+1} = d'_i \circ h'_{i+1},$$

so we are fine.

Base case. Let $x \in P_0$. Then $(q \circ h_0)(x) = (0 \circ p)(x) = 0$ so $\operatorname{im} h_0 \le \ker q = \operatorname{im} d'_0$. We have a surjective map $d'_0 : Q_1 \to \operatorname{im} d'_0$, and a map $h_0 : P_0 \to \operatorname{im} d'_0$. Since P_0 is projective, there exists $s_0 : P_0 \to Q_1$ such that $h_0 = d'_0 \circ s_0$.

Inductive step. Suppose we have maps $s_0, \dots, s_{t-1}$, with $s_i : P_i \to Q_{i+1}$, and $h_i = d'_i \circ s_i + s_{i-1} \circ d_{i-1}$ for $i = 1, \dots, t-1$, so

$$\begin{tikzcd} \dots \arrow[r, "d_{t+1}"] & P_{t+1} \arrow[r, "d_t"] \arrow[d, "h_{t+1}"'] & P_t \arrow[r, "d_{t-1}"] \arrow[d, "h_t"'] \arrow[dl, dashed, "s_t"'] & P_{t-1} \arrow[r, "d_{t-2}"] \arrow[d, "h_{t-1}"'] \arrow[dl, "s_{t-1}"'] & P_{t-2} \arrow[r, "d_{t-3}"] \arrow[d, "h_{t-2}"'] \arrow[dl, "s_{t-2}"'] & \dots \\ \dots \arrow[r, "d'_{t+1}"'] & Q_{t+1} \arrow[r, "d'_t"'] & Q_t \arrow[r, "d'_{t-1}"'] & Q_{t-1} \arrow[r, "d'_{t-2}"'] & Q_{t-2} \arrow[r, "d'_{t-3}"'] & \dots \end{tikzcd}.$$

Look at $h_t - s_{t-1} \circ d_{t-1}$. We want to show that the image of this map is contained in $\operatorname{im} d'_t = \ker d'_{t-1}$. So check

$$\begin{aligned} d'_{t-1} \circ (h_t - s_{t-1} \circ d_{t-1}) &= d'_{t-1} \circ h_t - d'_{t-1} \circ s_{t-1} \circ d_{t-1} \\ &= h_{t-1} \circ d_{t-1} - (h_{t-1} - s_{t-2} \circ d_{t-2}) \circ d_{t-1} \\ &= h_{t-1} \circ d_{t-1} - h_{t-1} \circ d_{t-1} + s_{t-2} \circ d_{t-2} \circ d_{t-1}. \end{aligned}$$

Now $d_{t-2} \circ d_{t-1} = 0$, so we have $d'_{t-1} \circ (h_t - s_{t-1} \circ d_{t-1}) = 0$. So $h_t - s_{t-1} \circ d_{t-1} \in \ker d'_{t-1}$. Now we have the situation

$$\begin{tikzcd} & P_t \arrow[d, "h_t - s_{t-1} \circ d_{t-1}"] \arrow[dl, dashed, "s_t"'] \\ Q_{t+1} \arrow[r, "d'_t"'] & \operatorname{im} d'_t \end{tikzcd},$$

and since P_t is projective, there exists s_t such that $d'_t \circ s_t = h_t - s_{t-1} \circ d_{t-1}$, so $h_t = d'_t \circ s_t + s_{t-1} \circ d_{t-1}$ as required.

□

5.4 Uniqueness of injective resolutions

The following is the equivalent result for injectives.

Proposition 5.13. *Let M and N be R-modules, and $\phi : M \to N$ a homomorphism. Let (I_t) be an injective resolution for M, and (J_t) another injective resolution for N. Then*

- *there exist maps $f_i : I_i \to J_i$ such that the diagram*

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "i"] \arrow[d, "\phi"] & I_0 \arrow[r, "d_0"] \arrow[d, dashed, "f_0"] & I_1 \arrow[r, "d_1"] \arrow[d, dashed, "f_1"] & I_2 \arrow[r, "d_2"] \arrow[d, dashed, "f_2"] & \dots \\ 0 \arrow[r] & N \arrow[r, "j"'] & J_0 \arrow[r, "d'_0"'] & J_1 \arrow[r, "d'_1"'] & J_2 \arrow[r, "d'_2"'] & \dots \end{tikzcd}$$

  commutes, and

- *if (g_i) is another set of maps $g_i : I_i \to J_i$ such that the diagram*

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "i"] \arrow[d, "\psi"] & I_0 \arrow[r, "d_0"] \arrow[d, bend right, "f_0"'] \arrow[d, bend left, "g_0"] & I_1 \arrow[r, "d_1"] \arrow[d, bend right, "f_1"'] \arrow[d, bend left, "g_1"] & I_2 \arrow[r, "d_2"] \arrow[d, bend right, "f_2"'] \arrow[d, bend left, "g_2"] & \dots \\ 0 \arrow[r] & N \arrow[r, "j"'] & J_0 \arrow[r, "d'_0"'] & J_1 \arrow[r, "d'_1"'] & J_2 \arrow[r, "d'_2"'] & \dots \end{tikzcd}$$

  commutes, then there exist maps $s_i : I_{i+1} \to J_i$ such that

$$g_i - f_i = \begin{cases} s_i \circ d_i + d'_{i-1} \circ s_{i-1} & i > 0 \\ s_0 \circ d_0 & i = 0 \end{cases},$$

  so

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "i"] \arrow[d, "\psi"] & I_0 \arrow[r, "d_0"] & I_1 \arrow[r, "d_1"] \arrow[dl, dashed, "s_0"'] & I_2 \arrow[r, "d_2"] \arrow[dl, dashed, "s_1"'] & \dots \arrow[dl, dashed, "s_2"'] \\ 0 \arrow[r] & N \arrow[r, "j"'] & J_0 \arrow[r, "d'_0"'] & J_1 \arrow[r, "d'_1"'] & J_2 \arrow[r, "d'_2"'] & \dots \end{tikzcd}.$$

Proof. Very similar to Proposition 5.12. □

Lecture 19 is a problems class. Lecture 19 Friday 21/02/20

6 Complexes and homology

6.1 Chain complexes

Lecture 20 Monday 24/02/20

Definition 6.1. A **chain complex** is a series $A_* = (A_i)$, with maps $d_i^A = d_i = d : A_{i+1} \to A_i$ such that $d^2 = 0$, that is $d_{i+1} \circ d_i = 0$, or $\operatorname{im} d_{i+1} \leq \ker d_i$.

Definition 6.2. A **cochain complex** is a series $A^* = \left(A^i\right)$ with maps $d_i^A = d_i = d : A^i \to A^{i+1}$ such that $d^2 = 0$, or $\operatorname{im} d_i \leq \ker d_{i+1}$.

Let A_* and B_* be chain complexes. Let $f = (f_i)$ be a family of R-module homomorphisms $f_i : A_i \to B_i$. Say that f is a **map of chain complexes** if $f \circ d = d \circ f$, that is $f_i \circ d_i^A = d_i^B \circ f_{i+1}$. So

$$\begin{tikzcd}
\dots \arrow[r, "d_{n+1}"] & A_{n+1} \arrow[r, "d_n"] \arrow[d, "f_{n+1}"] & A_n \arrow[r, "d_{n-1}"] \arrow[d, "f_n"] & A_{n-1} \arrow[r, "d_{n-2}"] \arrow[d, "f_{n-1}"] & \dots \\
\dots \arrow[r, "d_{n+1}"'] & B_{n+1} \arrow[r, "d_n"'] & B_n \arrow[r, "d_{n-1}"'] & A_{n-1} \arrow[r, "d_{n-2}"'] & \dots
\end{tikzcd}$$

commutes. Say that f **has property** $\mathcal{P}$ if all f_i have property $\mathcal{P}$, where $\mathcal{P}$ is injective, surjective, etc. A sequence

$$A_* \xrightarrow{f} B_* \xrightarrow{g} C_*$$

is **exact** at B_* if

$$A_n \xrightarrow{f_n} B_n \xrightarrow{g_n} C_n$$

is exact at B_n for all n. A sequence of chain complexes is **exact** if it is exact everywhere. An **exact sequence**

$$0 \to A_* \to B_* \to C_* \to 0$$

is a short exact sequence of chain complexes.

6.2 Homology groups

Definition 6.3. Let A_* be a chain complex. The n**-th homology group** of A_* is $\ker d_{n-1} / \operatorname{im} d_n$. We write $\mathrm{H}_n(A_*)$. Also write $\mathrm{H}_*(A_*) = (\mathrm{H}_n(A_*))$.

Definition 6.4. Let A^* be a cochain complex. The n**-th cohomology group** of A^* is $\ker d_n / \operatorname{im} d_{n-1}$. We write $\mathrm{H}^n(A^*)$, and $\mathrm{H}^*(A^*) = (\mathrm{H}^n(A^*))$.

Example. Let $A_i = \mathbb{Z}^3$ for all i, and let $d(a,b,c) = (0,0,a)$. Certainly $d^2 = 0$, so this is a chain complex. Then

$$\ker d = \{(0,b,c)\} = 0 \oplus \mathbb{Z}^2, \qquad \operatorname{im} d = \{(0,0,a)\} = 0^2 \oplus \mathbb{Z}.$$

Now

$$\ker d_{n-1} / \operatorname{im} d_n = \left\{(0,b,0) + 0^2 \oplus \mathbb{Z}\right\}.$$

Proposition 6.5. *A map of chain complexes $f : A_* \to B_*$ induces a map on the homology,*

$$f_* : \mathrm{H}_*(A_*) \to \mathrm{H}_*(B_*),$$

given by

$$\begin{array}{cccc} f_{*i} & : & \mathrm{H}_i(A_*) & \longrightarrow & \mathrm{H}_i(B_*) \\ & & x + \operatorname{im} d_i^A & \longmapsto & f_i(x) + \operatorname{im} d_i^B \end{array}.$$

Proof. Let $x \in \ker d_{i-1}^A$. Then $\left(f_{i-1} \circ d_{i-1}^A\right)(x) = 0$, so $\left(d_{i-1}^B \circ f_i\right)(x) = 0$. Hence $f_i(x) \in \ker d_{i-1}^B$. So f_i certainly induces a map $\overline{f_i} : \ker d_{i-1}^A \to \ker d_{i-1}^B / \operatorname{im} d_i^B$. So there exists $y \in A_{i+1}$ with $d_i^A(y) = x$. Now $f_i(x) = \left(f_i \circ d_i^A\right)(y) = \left(d_i^B \circ f_{i+1}\right)(y) \in \operatorname{im} d_i^B$, so $\overline{f_i}(x) = 0$. Hence $\operatorname{im} d_i^A \leq \ker \overline{f_i}$ so $\overline{f_i}$ induces a map

$$\ker d_{i-1}^A / \operatorname{im} d_i^A = \mathrm{H}_i(A_*) \to \ker d_{i-1}^B / \operatorname{im} d_i^B = \mathrm{H}_i(B_*).$$

∎

Let A_* and B_* be chain complexes, and let f and g be maps between them. We say that f and g are **equal up to homotopy** if there exist maps $s_i : A_i \to B_{i+1}$ such that

$$g_i - f_i = s_{i-1} \circ d_{i-1}^A + d_i^B \circ s_i.$$

Proposition 6.6. *If $f, g : A_* \to B_*$ are equal up to homotopy, then $f_* = g_*$, so f and g induce the same map on homology.*

Proof. Exercise. [5] ☐

6.3 The long exact sequence in homology

Proposition 6.7. *Let*

$$0 \to A_* \xrightarrow{f} B_* \xrightarrow{g} C_* \to 0$$

be a short exact sequence. This induces a long exact sequence

$$\dots \to \mathrm{H}_{n+1}(A_*) \to \mathrm{H}_{n+1}(B_*) \to \mathrm{H}_{n+1}(C_*) \to \mathrm{H}_n(A_*) \to \mathrm{H}_n(B_*) \to \mathrm{H}_n(C_*) \to \dots.$$

Proof. We have a commuting diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & A_{n+1} \arrow[r, "f_{n+1}"] \arrow[d, "d_n^A"] & B_{n+1} \arrow[r, "g_{n+1}"] \arrow[d, "d_n^B"] & C_{n+1} \arrow[r] \arrow[d, "d_n^C"] & 0 \\
0 \arrow[r] & A_n \arrow[r, "f_n"'] & B_n \arrow[r, "g_n"'] & C_n \arrow[r] & 0
\end{tikzcd}.$$

Notice $\operatorname{im} d_n \leq \ker d_{n-1}$, so we can change this to

$$\begin{tikzcd}
0 \arrow[r] & A_{n+1} \arrow[r, "f_{n+1}"] \arrow[d, "d_n^A"] & B_{n+1} \arrow[r, "g_{n+1}"] \arrow[d, "d_n^B"] & C_{n+1} \arrow[r] \arrow[d, "d_n^C"] & 0 \\
0 \arrow[r] & \ker d_{n-1}^A \arrow[r, "f_n"'] & \ker d_{n-1}^B \arrow[r, "g_n"'] & \ker d_{n-1}^C
\end{tikzcd}.$$

Now $\operatorname{im} d_{n+1} \leq \ker d_n$, so the maps $A_{n+1} \to \ker d_{n+1}$ induce maps $A_{n+1} / \operatorname{im} d_{n+1} \to \ker d_{n-1}$. So we get a diagram

$$\begin{tikzcd}
 & A_{n+1}/\operatorname{im} d_{n+1}^A \arrow[r, "f_{n+1}"] \arrow[d, "\overline{d_n^A}"] & B_{n+1}/\operatorname{im} d_{n+1}^B \arrow[r, "g_{n+1}"] \arrow[d, "\overline{d_n^B}"] & C_{n+1}/\operatorname{im} d_{n+1}^C \arrow[r] \arrow[d, "\overline{d_n^C}"] & 0 \\
0 \arrow[r] & \ker d_{n-1}^A \arrow[r, "f_n"'] & \ker d_{n-1}^B \arrow[r, "g_n"'] & \ker d_{n-1}^C
\end{tikzcd}.$$

We are now in the position to apply the snake lemma, so

$$\ker \overline{d_n^A} \to \ker \overline{d_n^B} \to \ker \overline{d_n^C} \to \operatorname{coker} \overline{d_n^A} \to \operatorname{coker} \overline{d_n^B} \to \operatorname{coker} \overline{d_n^C}$$

is an exact sequence. Then

$$\ker \overline{d_n^A} = \ker d_n^A / \operatorname{im} d_{n+1}^A = \mathrm{H}_{n+1}(A_*), \qquad \operatorname{coker} \overline{d_n^A} = \ker d_{n-1}^A / \operatorname{im} d_n^A = \mathrm{H}_n(A_*).$$

Similarly for B_* and C_*. So we have an exact sequence

$$\mathrm{H}_{n+1}(A_*) \to \mathrm{H}_{n+1}(B_*) \to \mathrm{H}_{n+1}(C_*) \to \mathrm{H}_n(A_*) \to \mathrm{H}_n(B_*) \to \mathrm{H}_n(C_*).$$

Since consecutive values of i give a sequence overlapping in three terms we can glue them together, to give the long exact sequence in the proposition. ☐

[5] Exercise

7 Derived functors

7.1 Covariant and contravariant functors

Lecture 21 Tuesday 25/02/20

The following are two variations.

Definition 7.1. A **covariant functor** F from the category of left or right R-modules to the category of abelian groups is a map from R-modules to abelian groups such that if $\phi : M \to N$ is an R-module homomorphism then there exists an abelian group homomorphism

$$F(\phi) : F(M) \to F(N),$$

which respects identity maps, so $F(\mathrm{id}_M) = \mathrm{id}_{F(M)}$, and respects composition, so

$$F(\phi_1 \circ \phi_2) = F(\phi_1) \circ F(\phi_2).$$

The map F on homomorphisms is **additive** if $F(\phi_1 + \phi_2) = F(\phi_1) + F(\phi_2)$. If

$$0 \to A \to B \to C \to 0$$

be a short exact sequence, then F is **right exact** if

$$F(A) \to F(B) \to F(C) \to 0$$

is exact, **left exact** if

$$0 \to F(A) \to F(B) \to F(C)$$

is exact. Then F is **exact** if both left and right exact.

Definition 7.2. A **contravariant functor** F from the category of left or right R-modules to the category of abelian groups is a map from R-modules to abelian groups such that if $\phi : M \to N$ is an R-module homomorphism then there exists an abelian group homomorphism

$$F(\phi) : F(N) \to F(M),$$

which respects identity maps, so $F(\mathrm{id}_M) = \mathrm{id}_{F(M)}$, and respects composition, so

$$F(\phi_1 \circ \phi_2) = F(\phi_2) \circ F(\phi_1).$$

Similarly, if

$$0 \to A \to B \to C \to 0$$

be a short exact sequence, then F is **right exact** if

$$F(C) \to F(B) \to F(A) \to 0$$

is exact, and **left exact** if

$$0 \to F(C) \to F(B) \to F(A)$$

is exact.

Example. Some functors we have seen. Fix a left R-module M.

- $F(A) = \mathrm{Hom}_R(M, A)$, where

$$F(\phi) \quad : \quad \begin{array}{rcl} F(A) = \mathrm{Hom}_R(M, A) & \longrightarrow & F(B) = \mathrm{Hom}_R(M, B) \\ f & \longmapsto & \phi \circ f \end{array}, \qquad \phi : A \to B,$$

  is covariant, left exact, and exact if and only if M is projective.

- $F(A) = \mathrm{Hom}_R(A, M)$, where

$$F(\phi) \quad : \quad \begin{array}{rcl} F(B) = \mathrm{Hom}_R(B, M) & \longrightarrow & F(A) = \mathrm{Hom}_R(A, M) \\ f & \longmapsto & f \circ \phi \end{array}, \qquad \phi : A \to B,$$

  is contravariant, left exact, and exact if and only if M is injective.

- For a right R-module A, $F(A) = A \otimes_R M$ is covariant, right exact, and exact if and only if M is flat.

7.2 Left derived functors

Let F be the functor $F(A) = A \otimes_R M$, where M is a fixed R-module. Let $P_* \to A$ be a projective resolution for A. So $P_* = (P_i)_{i \geq 0}$ for projective P_i, and

$$\dots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\phi} A \to 0$$

is exact. Consider the sequence

$$\dots \to P_2 \to P_1 \to P_0 \to 0.$$

This is no longer exact, but it is a chain complex. And if we apply F, we get a chain complex $F(P_*)$,

$$\dots \to F(P_2) \to F(P_1) \to F(P_0) \to 0.$$

Define **left derived functors**

$$\mathrm{L}_n F(A) = \mathrm{H}_n(F(P_*)).$$

Theorem 7.3.

1. $\mathrm{L}_n F(A)$ *does not depend on the choice of resolution* P_*.
2. $\mathrm{L}_n F$ *is an additive functor from right* R*-modules to abelian groups.*
3. $\mathrm{L}_0 F(A) = F(A)$.

Lecture 22 Friday 28/02/20

Proof.

1. Let $P_* \to A$ and $Q_* \to A$ be projective resolutions. Then there exist maps of chain complexes $f : P_* \to Q_*$ and $g : Q_* \to P_*$. So $g \circ f : P_* \to P_*$, so

$$\begin{tikzcd} \dots \arrow[r, "d_2"] & P_2 \arrow[r, "d_1"] \arrow[d, "g_2 \circ f_2"] & P_1 \arrow[r, "d_0"] \arrow[d, "g_1 \circ f_1"] & P_0 \arrow[r] \arrow[d, "g_0 \circ f_0"] & A \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ \dots \arrow[r, "d_2"'] & P_2 \arrow[r, "d_1"'] & P_1 \arrow[r, "d_0"'] & P_0 \arrow[r] & A \arrow[r] & 0 \end{tikzcd},$$

and $g \circ f$ is equal to id up to homotopy. Apply F to everything. Since F is right exact,

$$\begin{tikzcd} \dots \arrow[r, "F(d_2)"] & F(P_2) \arrow[r, "F(d_1)"] \arrow[d, "F(g_2)\circ F(f_2)"] & F(P_1) \arrow[r, "F(d_0)"] \arrow[d, "F(g_1)\circ F(f_1)"] & F(P_0) \arrow[r] \arrow[d, "F(g_0)\circ F(f_0)"] & F(A) \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\ \dots \arrow[r, "F(d_2)"'] & F(P_2) \arrow[r, "F(d_1)"'] & F(P_1) \arrow[r, "F(d_0)"'] & F(P_0) \arrow[r] & F(A) \arrow[r] & 0 \end{tikzcd}.$$

The diagram remains commutative, since F preserves composition. Now

$$g_i \circ f_i - \mathrm{id} = s_{i-1} \circ d_{i-1} + d_i \circ s_i,$$

for suitable maps s_i. Then

$$F(g_i) \circ F(f_i) - \mathrm{id} = F(s_{i-1}) \circ F(d_{i-1}) + F(d_i) \circ F(s_i).$$

So $F(g_i) \circ F(f_i)$ is id up to homotopy. Hence $F(g) \circ F(f)$ induces the identity on homology $\mathrm{H}_*(F(P_*))$. Also $F(f) \circ F(g)$ induces the identity on $\mathrm{H}_*(F(Q_*))$. Now we have

$$\overline{F(f_i)} : \mathrm{H}_i(F(P_*)) \to \mathrm{H}_i(F(Q_*)), \qquad \overline{F(g_i)} : \mathrm{H}_i(F(Q_*)) \to \mathrm{H}_i(F(P_*)),$$

and $\overline{F(f_i)} \circ \overline{F(g_i)} = \mathrm{id}$ and $\overline{F(g_i)} \circ \overline{F(f_i)} = \mathrm{id}$, so $\overline{F(f_i)}$ and $\overline{F(g_i)}$ are isomorphisms. So

$$\mathrm{H}_n(F(P_*)) \cong \mathrm{H}_n(F(Q_*)),$$

as required. This argument tells us nothing about $\mathrm{H}_0(F(P_*))$.

2. Let $\phi : A \to B$. Let $P_* \to A$ and $Q_* \to B$ be projective resolutions. Then there exists $f : P_* \to Q_*$ such that
$$\begin{tikzcd} P_* \arrow[r] \arrow[d, "f"'] & A \arrow[r] \arrow[d, "\phi"] & 0 \\ Q_* \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$
commutes. Then F is covariant and right exact. So
$$\begin{tikzcd} F(P_*) \arrow[r] \arrow[d, "F(f)"'] & F(A) \arrow[r] \arrow[d, "F(\phi)"] & 0 \\ F(Q_*) \arrow[r] & F(B) \arrow[r] & 0 \end{tikzcd}$$
is commutative, where $F(f) = (F(f_i))$. If $g : P_* \to Q_*$ is such that
$$\begin{tikzcd} P_* \arrow[r] \arrow[d, "g"'] & A \arrow[r] \arrow[d, "\phi"] & 0 \\ Q_* \arrow[r] & B \arrow[r] & 0 \end{tikzcd}$$
commutes, then $\overline{f}$ and $\overline{g}$, the induced maps on homology, are equal. So there exists a map $\overline{F(f_i)} : \mathrm{L}_i F(A) \to \mathrm{L}_i F(B)$, and is independent of the choice of f. So we can write $\mathrm{L}_n F(\phi) = \overline{F(f_i)}$. Then $\mathrm{L}_n F$ preserves identity and compositions and is additive, since F is an additive functor. [6]

3. We have a short exact sequence
$$0 \to \operatorname{im} d_0 \xrightarrow{\subseteq} P_0 \xrightarrow{\phi} A \to 0.$$
Since F is right exact, we get an exact sequence
$$F(\operatorname{im} d_0) \to F(P_0) \to F(A) \to 0.$$
Now $d_0 : P_1 \to \operatorname{im} d_0$ is surjective, and F preserves surjectivity. So $F(d_0) : F(P_1) \to F(\operatorname{im} d_0)$ is surjective. So
$$F(P_1) \to F(P_0) \to F(A) \to 0$$
is exact. So, setting $P_{-1} = 0$, we get $\mathrm{L}_0 F(P_*) = F(P_0) / \operatorname{im} F(d_0) = F(A)$.

$\square$

[6] Exercise

7.3 The long exact sequence of left derived functors

Proposition 7.4 (Horseshoe lemma)**.** *Suppose*

$$0 \to A \to B \to C \to 0$$

is an exact sequence of R-modules. Suppose $P_* \to A$ and $R_* \to C$ are projective resolutions. Define $Q_i = P_i \oplus R_i$. Then there exist maps $Q_{i+1} \to Q_i$ and $Q_0 \to B$ such that $Q_* \to B$ is a projective resolution, and such that

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\dots \arrow[r] & P_2 \arrow[r] \arrow[d, "\iota"] & P_1 \arrow[r] \arrow[d, "\iota"] & P_0 \arrow[r] \arrow[d, "\iota"] & A \arrow[r] \arrow[d] & 0 \\
\dots \arrow[r, dashed] & Q_2 \arrow[r, dashed] \arrow[d, "\pi"] & Q_1 \arrow[r, dashed] \arrow[d, "\pi"] & Q_0 \arrow[r, dashed] \arrow[d, "\pi"] & B \arrow[r, dashed] \arrow[d] & 0 \\
\dots \arrow[r] & R_2 \arrow[r] \arrow[d] & R_1 \arrow[r] \arrow[d] & R_0 \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 & 0 &
\end{tikzcd}$$

commutes, where if $x \in P_i$ and $y \in R_i$ then $\iota(x) = (x, 0)$ and $\pi(x, y) = y$.

Note. Q_i is a direct sum of projectives, so is itself projective.

Proof. We have the setup

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & \\
P_0 \arrow[r, "\phi"] \arrow[d, "\iota"'] & A \arrow[r] \arrow[d, "f"] & 0 \\
Q_0 \arrow[d, "\pi"'] & B \arrow[d, "g"] & \\
R_0 \arrow[r, "\psi"'] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 & 0 &
\end{tikzcd} .$$

Since $B \to C$ is surjective, and R_0 is projective, there exists $h : R_0 \to B$ such that $g \circ h = \psi$. Now define

$$\begin{array}{cccc} \chi & : & Q_0 & \longrightarrow & B \\ & & (x, y) & \longmapsto & (f \circ \phi)(x) + h(y) \end{array}, \qquad x \in P_0, \qquad y \in R_0.$$

This construction guarantees that the squares are commutative. It is easy to see that χ is surjective, so

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & \\
P_0 \arrow[r, "\phi"] \arrow[d, "\iota"'] & A \arrow[r] \arrow[d, "f"] & 0 \\
Q_0 \arrow[r, dashed, "\chi"] \arrow[d, "\pi"'] & B \arrow[r, dashed] \arrow[d, "g"] & 0 \\
R_0 \arrow[r, "\psi"'] \arrow[ur, dashed, "h"] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 & 0 &
\end{tikzcd} .$$

Now we have a short exact sequence

$$0 \to \ker \phi \xrightarrow{\iota} \ker \chi \xrightarrow{\pi} \ker \psi \to 0,$$

by the snake lemma. So now we can iterate, replacing A, B, C with these kernels, to construct a map $Q_1 \to Q_0$, and so on. $\square$

Proposition 7.5. *Let F be an additive functor, and let A and B be R-modules. There is a canonical isomorphism $F(A) \oplus F(B) \to F(A \oplus B)$.*

Proof. Let $M = A \oplus B$. Consider functions

$$p_1 : \begin{array}{ccc} M & \longrightarrow & M \\ (a,b) & \longmapsto & (a,0) \end{array}, \qquad p_2 : \begin{array}{ccc} M & \longrightarrow & M \\ (a,b) & \longmapsto & (0,b) \end{array}.$$

Then $p_i^2 = p_i$, $p_1 \circ p_2 = p_2 \circ p_1 = 0$, and $p_1 + p_2 = \mathrm{id}_M$. If q_1 and q_2 are maps on a module M satisfying these relations, then $M = q_1(M) \oplus q_2(M)$. ☐

Lecture 23 Monday 02/03/20

Proposition 7.6. *Let*

$$0 \to A \to B \to C \to 0$$

be a short exact sequence of right R-modules. This gives rise to a long exact sequence

$$\dots \to \mathrm{L}_n F(A) \to \mathrm{L}_n F(B) \to \mathrm{L}_n F(C) \to \dots \to \mathrm{L}_0 F(A) \to \mathrm{L}_0 F(B) \to \mathrm{L}_0 F(C) \to 0.$$

Proof. Let $P_* \to A$ be a projective resolution and $R_* \to C$ be a projective resolution. By the horseshoe lemma, there exists a projective resolution $Q_* \to B$ such that

$$0 \to P_* \to Q_* \to R_* \to 0$$

is a split short exact sequence of chain complexes, that is $Q_i = P_i \oplus R_i$. Since $Q_i = P_i \oplus R_i$, and since F is an additive functor, we have $F(Q_i) = F(P_i) \oplus F(R_i)$. So

$$0 \to F(P_*) \to F(Q_*) \to F(R_*) \to 0$$

is a short exact sequence. Therefore we get a long exact sequence on homology,

$$\dots \to \mathrm{H}_n(F(P_*)) \to \mathrm{H}_n(F(Q_*)) \to \mathrm{H}_n(F(R_*)) \to \dots.$$

Since $\mathrm{H}_n(F(P_*)) = \mathrm{L}_n F(A)$ this gives the long sequence that we need. Since $\mathrm{L}_0 F(A) = F(A)$, and F is right exact, the sequence terminates

$$\mathrm{L}_0 F(A) \to \mathrm{L}_0 F(B) \to \mathrm{L}_0 F(C) \to 0,$$

as required. ☐

7.4 General derived functors

Proposition 7.7.

- *Let F be any covariant, right exact, additive functor from left or right R-modules to abelian groups. Then the left derived functors $\mathrm{L}_n F$ can be defined in just the same way as we did for the case $F(A) = A \otimes_R M$. All of the results we have proved follow in the more general case, by the same arguments.*
- *If F is a covariant, left exact, additive functor from R-modules to abelian groups, then we can define* ***right derived functors*** $\mathrm{R}^i F$ *in a similar manner. Instead of working with a projective resolution, we use an injective resolution,*

  $$0 \to A \to I_0 \to I_1 \to I_2 \to \dots.$$

  By similar arguments, we show that $\mathrm{R}^i F(A)$ is independent of the choice of injective resolution. All of the results we proved for left derived functors have natural analogies for right derived functors. The argument requires a version of the horseshoe lemma for injective resolutions, which is exactly what one might expect.
- *We can even construct derived functors for contravariant functors. If F is contravariant and right exact, so*

  $$0 \to A \to I_0 \to I_1 \to I_2 \to \dots$$

  is exact implies that

  $$\dots \to F(I_2) \to F(I_1) \to F(I_0) \to F(A) \to 0$$

  is exact, we get a left derived functor, which is defined using an injective resolution. If F is contravariant and left exact, we get a right derived functor, which is defined using a projective resolution.

8 Tor and Ext

8.1 Balancing theorems

Definition 8.1. Let F be the functor $F(A) = A \otimes_R B$. Then F is covariant, right exact, and additive. So $\mathrm{L}_n F$ exists. Define

$$\mathrm{Tor}_i^R(A, B) = \mathrm{L}_i F(A).$$

Fact. Let F' be the functor $F'(B) = A \otimes_R B$. Then F' is covariant, right exact, and additive. So $\mathrm{L}_n F'$ exists. We have

$$\mathrm{L}_i F'(B) \cong \mathrm{L}_i F(A) = \mathrm{Tor}_i^R(A, B).$$

Definition 8.2. Let F be the functor $F(B) = \mathrm{Hom}_R(A, B)$. Then F is covariant, left exact, and additive, so $\mathrm{R}^n F$ exists. Define

$$\mathrm{Ext}_R^i(A, B) = \mathrm{R}^i F(B).$$

Fact. Let F' be the functor $F'(A) = \mathrm{Hom}_R(A, B)$. Then F' is contravariant, left exact, and additive, so $\mathrm{R}^n F'$ exists. We have

$$\mathrm{R}^i F'(A) \cong \mathrm{R}^i F(B) = \mathrm{Ext}_R^i(A, B).$$

The two facts above are the **balancing theorems** for Tor and Ext. Their proof is beyond the scope of the course.

8.2 Tor, flatness, and torsion

The following is an observation. Suppose A is projective. Then a projective resolution for A is

$$0 \to \dots \to 0 \to A \xrightarrow{\mathrm{id}} A \to 0.$$

So $\mathrm{L}_i F(A) = 0$ for $i \geq 1$, and $\mathrm{L}_0 F(A) = F(A)$, for F possessing left derived functors. Similarly, if A is injective, then an injective resolution is

$$0 \to A \xrightarrow{\mathrm{id}} A \to 0 \to \dots \to 0,$$

so $\mathrm{R}^i F(A) = 0$ for $i \geq 1$, and $\mathrm{R}^0 F(A) = F(A)$, for F possessing right derived functors. In fact the property $\mathrm{Tor}_i^R(A, B) = 0$ for all $i \geq 0$ characterises flat modules, so either A or B is flat.

Proposition 8.3. *Let $F(A) = A \otimes_R B$. Then $\mathrm{L}_i F(A) = \mathrm{Tor}_i^R(A, B) = 0$ for all $i \geq 1$ and for all A if and only if B is flat.*

Similarly if $F'(B) = A \otimes_R B$, then $\mathrm{L}_i F'(B) = 0$ for all $i \geq 1$ and for all B if and only if A is flat. Lecture 24 Tuesday 03/03/20

Proof.

$\Longleftarrow$ If B is flat then $F(A) = A \otimes_R B$ is exact, so

$$0 \to L \to M \to N \to 0$$

is exact implies that

$$0 \to F(L) \to F(M) \to F(N) \to 0$$

is exact, or F maps kernels to kernels and cokernels to cokernels. Let $P_* \to A$ be a projective resolution. Then

$$\dots \to P_2 \to P_1 \to P_0 \to 0$$

is exact everywhere except P_0. So

$$\dots \to F(P_2) \to F(P_1) \to F(P_0) \to 0$$

is exact everywhere except $F(P_0)$. So $\mathrm{L}_n F(P_*) = 0$ for $n \geq 1$. But $\mathrm{L}_n F(P_*) = \mathrm{Tor}_n^R(A, B)$.

$\Longrightarrow$ Conversely, suppose $\mathrm{Tor}_i^R(A, B) = 0$ for all A. Let

$$0 \to L \to M \to N \to 0$$

be exact. This gives a long exact sequence of homology groups

$$\begin{tikzcd} \dots \arrow[r] & \mathrm{L}_1 F(L) \arrow[r] & \mathrm{L}_1 F(M) \arrow[r] & \mathrm{L}_1 F(N) \arrow[r] \arrow[d, phantom, "\cong" rotate=-90] & L \otimes_R B \arrow[r] & M \otimes_R B \arrow[r] & N \otimes_R B \arrow[r] & 0 \\ & & & \mathrm{Tor}_1^R(N, B) & & & & \end{tikzcd}.$$

Since $\mathrm{Tor}_1^R(N, B) = 0$, we get a short exact sequence

$$0 \to L \otimes_R B \to M \otimes_R B \to N \otimes_R B \to 0.$$

So $F(A) = A \otimes_R B$ is left exact, and so B is flat.

$\square$

Proposition 8.4. *Let A and B be abelian groups. Then*

$$\mathrm{Tor}_n^{\mathbb{Z}}(A, B) = 0, \qquad n > 1.$$

Proof. A is a quotient of some free module K, say

$$K \xrightarrow{f} A \to 0.$$

Now $\ker f \leq K$, and since $\mathbb{Z}$ is a PID, $\ker f$ is free, since it is a submodule of a free module. So

$$\dots \to 0 \to \ker f \to K \to A \to 0$$

is a projective resolution for A. Since all of the modules above P_1 in the resolution are zero, clearly $\mathrm{H}_n(P_*) = 0$ for $n > 1$. $\square$

Fact.

$$\mathrm{Tor}_1^{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z}) = \mathrm{T}(A) = \{a \in A \mid a \text{ has finite order}\}.$$

The proof is omitted.

8.3 Baer sums of extensions

Proposition 8.5. *Let A and B be abelian groups. Then*

$$\mathrm{Ext}_{\mathbb{Z}}^n(A, B) = 0, \qquad n > 1.$$

Proof. Problem sheet question. $\square$

More generally, $\mathrm{Ext}_R^1(A, C)$ tells us about **extensions** of C by A, that is B such that

$$0 \to A \to B \to C \to 0.$$

Let B_1 and B_2 be two extensions of C by A. Write $B_1 \sim B_2$ if there exists a **map of extensions** $f : B_1 \to B_2$ such that

$$\begin{tikzcd} & & B_1 \arrow[dd, "f"] \arrow[dr, "\beta_1"] & & \\ 0 \arrow[r] & A \arrow[ur, "\alpha_1"] \arrow[dr, "\alpha_2"'] & & C \arrow[r] & 0 \\ & & B_2 \arrow[ur, "\beta_2"'] & & \end{tikzcd}$$

commutes.

Proposition 8.6. *Any such f is an isomorphism.*

Proof.

- f is surjective. Suppose $y \in B_2$. Then $\beta_2(y) \in C$, and β_1 is surjective, so $\beta_2(y) = \beta_1(x)$ for some $x \in B_1$. Now $f(x) - y \in \ker \beta_2 = \operatorname{im} \alpha_2$, so $f(x) - y = \alpha_2(a)$ for some $a \in A$. So $f(x) - y = (f \circ \alpha_1)(a)$, and so $y = f(x) - (f \circ \alpha_1)(a) = f(x - \alpha_1(a))$.
- f is injective. Suppose $f(x) = f(y)$ for $x, y \in B_1$. Then $f(x - y) = 0$, so $(\beta_2 \circ f)(x - y) = 0$, so $\beta_1(x - y) = 0$. So $x - y \in \ker \beta_1 = \operatorname{im} \alpha_1$, so $x - y = \alpha_1(a)$ for some $a \in A$. Now $\alpha_2(a) = (f \circ \alpha_1)(a) = f(x - y) = 0$. But α_2 is injective, so $a = 0$, so $x - y = 0$.

$\square$

Hence the relation $\sim$ is an equivalence relation. Write $\mathrm{E}_C(A)$ for the set of $\sim$-equivalence classes. We will put an abelian group structure on $\mathrm{E}_C(A)$. Let B_1 and B_2 be extensions, so

$$0 \to A \xrightarrow{\alpha_1} B_1 \xrightarrow{\beta_1} C \to 0, \qquad 0 \to A \xrightarrow{\alpha_2} B_2 \xrightarrow{\beta_2} C \to 0.$$

Define maps α^* and β^* by

$$\begin{array}{cccccc} \alpha^* & : & A & \longrightarrow & B_1 \oplus B_2 \\ & & a & \longmapsto & (\alpha_1(a), -\alpha_2(a)) \end{array}, \qquad \begin{array}{cccccc} \beta^* & : & B_1 \oplus B_2 & \longrightarrow & C \\ & & (b_1, b_2) & \longmapsto & \beta_1(b_1) - \beta_2(b_2) \end{array}.$$

Now $\beta^* \circ \alpha^* = 0$. So

$$0 \to A \xrightarrow{\alpha^*} B_1 \oplus B_2 \xrightarrow{\beta^*} C \to 0$$

is a chain complex. Define

$$H = \mathrm{H}(B_1, B_2),$$

the **Baer sum** of $[B_1]$ and $[B_2]$, to be the homology group at $B_1 \oplus B_2$, that is $H = \ker \beta^* / \operatorname{im} \alpha^*$. More explicitly,

$$H = \{(b_1, b_2) \in B_1 \oplus B_2 \mid \beta_1(b_1) = \beta_2(b_2)\} / \{(\alpha_1(a), -\alpha_2(a)) \mid a \in A\}.$$

Clearly H is an R-module. Now define maps

$$\begin{array}{ccccc} \alpha & : & A & \longrightarrow & H \\ & & a & \longmapsto & (\alpha_1(a), 0) + \operatorname{im} \alpha^* \end{array}, \qquad \begin{array}{ccccc} \beta & : & H & \longrightarrow & C \\ & & (b_1, b_2) + \operatorname{im} \alpha^* & \longmapsto & \beta_1(b_1) \end{array}.$$

Lecture 25 Friday 06/03/20

Note. $(b_1, b_2) \in \ker \beta^*$, so $\beta_1(b_1) = \beta_2(b_2)$. Also $(\alpha_1(a), 0) = (0, \alpha_2(a)) + (\alpha_1(a), -\alpha_2(a))$, so $(\alpha_1(a), 0) + \operatorname{im} \alpha^* = (0, \alpha_2(a)) + \operatorname{im} \alpha^*$.

Proposition 8.7.

$$0 \to A \xrightarrow{\alpha} H \xrightarrow{\beta} C \to 0$$

is a short exact sequence.

Proof.

- First check that β is well-defined. If $(b_1, b_2) \in (b_1', b_2') + \operatorname{im} \alpha^*$ then $(b_1, b_2) = (b_1', b_2') + (\alpha_1(a), -\alpha_2(a))$ for some $a \in A$. So

  $$\beta((b_1, b_2) + \operatorname{im} \alpha^*) = \beta_1(b_1) = \beta_1(b_1 - \alpha_1(a)) = \beta((b_1', b_2') + \operatorname{im} \alpha^*),$$

  since $\beta_1 \circ \alpha_1 = 0$.
- Next check α is injective. Suppose $\alpha(a) = (0, 0) + \operatorname{im} \alpha^*$. Then $(\alpha_1(a), 0) = \alpha^*(a')$ for some a'. So $(\alpha_1(a), 0) = (\alpha_1(a'), -\alpha_2(a'))$. Since α_1 and α_2 are injective, $a = a' = 0$.
- Next, show β is surjective. Take $c \in C$. Then $c = \beta_1(b_1)$ for some $b_1 \in B_1$. Since β_2 is surjective, there exists $b_2 \in B_2$ with $\beta_2(b_2) = \beta_1(b_1) = c$. Now $(b_1, b_2) \in \ker \beta^*$, and $\beta((b_1, b_2) + \operatorname{im} \alpha^*) = \beta_1(b_1) = c$.

- Finally, show that
$$0 \to A \to H \to C \to 0$$
is exact, that is $\ker \beta = \operatorname{im} \alpha$. It is clear that $\operatorname{im} \alpha \leq \ker \beta$, since $\beta_1 \circ \alpha_1 = 0$. For the reverse containment, let $(b_1, b_2) + \operatorname{im} \alpha^* \in \ker \beta$. So $(b_1, b_2) \in \ker \beta^*$, so $\beta_1(b_1) = \beta_2(b_2)$. And $\beta_1(b_1) = 0$, so $\beta_2(b_2) = 0$ as well. But $\ker \beta_i = \operatorname{im} \alpha_i$ for $i = 1, 2$, so there exist $a_1, a_2 \in A$ with $\alpha_1(a_1) = b_1$ and $\alpha_2(a_2) = b_2$. Now
$$\begin{aligned} (b_1, b_2) &= (\alpha_1(a_1), \alpha_2(a_2)) = (\alpha_1(a_1 + a_2), 0) + (-\alpha_1(a_2), \alpha_2(a_2)) \\ &\in (\alpha_1(a_1 + a_2), 0) + \operatorname{im} \alpha^* = \alpha(a_1 + a_2) \in \operatorname{im} \alpha. \end{aligned}$$

□

We have shown that H is an extension of C by A.

Proposition 8.8. *If $B_1 \sim B_1'$ and $B_2 \sim B_2'$ then $\mathrm{H}(B_1, B_2) \sim \mathrm{H}(B_1', B_2')$, where $B \sim B'$ if there exists a map of extensions $f : B \to B'$ such that*

$$\begin{tikzcd} & & B \arrow[dd, "f"] \arrow[dr] & & \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & C \arrow[r] & 0 \\ & & B' \arrow[ur] & & \end{tikzcd}$$

commutes.

Proof. Suppose $f_1 : B_1 \to B_1'$ and $f_2 : B_2 \to B_2'$ are maps of extensions. Then there exists a map of chain complexes

$$\begin{tikzcd} & & B_1 \oplus B_2 \arrow[dd, "(f_1, f_2)"] \arrow[dr] & & \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & C \arrow[r] & 0 \\ & & B_1' \oplus B_2' \arrow[ur] & & \end{tikzcd} .$$

This induces a map on homology, $\overline{f} : \mathrm{H}(B_1, B_2) \to \mathrm{H}(B_1', B_2')$. It is easy to check

$$\begin{tikzcd} & & \mathrm{H}(B_1, B_2) \arrow[dd, "\overline{f}"] \arrow[dr] & & \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & C \arrow[r] & 0 \\ & & \mathrm{H}(B_1', B_2') \arrow[ur] & & \end{tikzcd}$$

commutes, so $\mathrm{H}(B_1, B_2) \sim \mathrm{H}(B_1', B_2')$. □

Write $[B]$ for the equivalence class of B. If $H = \mathrm{H}(B_1, B_2)$, write $[H] = [B_1] + [B_2]$, or $[H] = [B_1] +_{\mathrm{B}} [B_2]$.

Proposition 8.9. *$+$ gives an abelian group operation on the set $\mathrm{E}_C(A)$ of equivalence classes of extensions.*

Proof.

- Check $+$ is commutative. This follows easily from the facts that
$$\alpha(a) = (\alpha_1(0), 0) + \operatorname{im} \alpha^* = (0, \alpha_2(a)) + \operatorname{im} \alpha^*, \qquad \beta((b_1, b_2) + \operatorname{im} \alpha^*) = \beta_1(b_1) = \beta_2(b_2).$$

- Associativity is an exercise. [7]

- The identity is $[A \oplus C]$, the **split extension**. Let
$$0 \to A \xrightarrow{\alpha} A \oplus C \xrightarrow{\beta} C \to 0, \qquad 0 \to A \xrightarrow{\alpha'} B \xrightarrow{\beta'} C \to 0.$$
There is a map $\pi : A \oplus C \to A$ such that $\pi \circ \alpha = \mathrm{id}_A$. Consider a map
$$\begin{array}{rccc} f & : & \mathrm{H}(B, A \oplus C) & \longrightarrow & B \\ & & (b_1, b_2) + \operatorname{im} \alpha^* & \longmapsto & b_1 + \alpha'(a) \end{array}, \qquad \beta'(b_1) = \beta(b_2), \qquad b_2 = (a, c) \in A \oplus C.$$
It is easy to check this gives a map of extensions.

[7] Exercise

- Inverses. Suppose
$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0.$$
Then the inverse of $[B]$ is given by the extension
$$0 \to A \xrightarrow{\alpha} B \xrightarrow{-\beta} C \to 0.$$

$\square$

8.4 Ext and classes of extensions

Lecture 26 Monday 09/03/20

Definition 8.10. Let
$$0 \to A \to B \to C \to 0$$
be an extension of C by A. The **class** of this extension is simply defined as $\eta(\mathrm{id}_C)$ in the long exact sequence
$$0 \to \mathrm{Hom}_R(C, A) \to \mathrm{Hom}_R(C, B) \to \mathrm{Hom}_R(C, C) \xrightarrow{\eta} \mathrm{Ext}^1_R(C, A) \to \dots.$$

Proposition 8.11.

- *Equivalent extensions have the same class.*
- *The map between equivalence classes of extensions and* $\mathrm{Ext}^1_R(C, A)$ *is a bijection.*
- *In fact class is an isomorphism* $(\mathrm{E}_C(A), +_{\mathrm{B}}) \to \mathrm{Ext}^1_R(C, A)$.

Lemma 8.12. *Suppose*
$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & X \arrow[r] & Y \arrow[r] & Z \arrow[r] & 0 \end{tikzcd}$$
commutes, where the rows are exact. We get long exact sequences
$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ext}^0_R(C, L) \arrow[r] \arrow[d] & \mathrm{Ext}^0_R(C, M) \arrow[r] \arrow[d] & \mathrm{Ext}^0_R(C, N) \arrow[r] \arrow[d] & \mathrm{Ext}^1_R(C, L) \arrow[r] \arrow[d] & \dots \\ 0 \arrow[r] & \mathrm{Ext}^0_R(C, X) \arrow[r] & \mathrm{Ext}^0_R(C, Y) \arrow[r] & \mathrm{Ext}^0_R(C, Z) \arrow[r] & \mathrm{Ext}^1_R(C, X) \arrow[r] & \dots \end{tikzcd},$$
where the vertical arrows are given by the functoriality of $\mathrm{Ext}^1_R(C, \cdot)$. *This diagram commutes.*

Proof. Omitted. $\square$

Proof of Proposition 8.11. We show that class gives a map $\mathrm{E}_C(A) \to \mathrm{Ext}^1_R(C, A)$, which is bijective.

- Every element of $\mathrm{Ext}^1_R(C, A)$ is the class of an extension. Take $x \in \mathrm{Ext}^1_R(C, A)$. Let I be an injective module containing A as a submodule. Then
$$0 \to A \to I \to I/A \to 0$$
is a short exact sequence, which gives a long exact sequence
$$0 \to \mathrm{Hom}_R(C, A) \to \mathrm{Hom}_R(C, I) \to \mathrm{Hom}_R(C, I/A) \xrightarrow{\mu} \mathrm{Ext}^1_R(C, A) \to \mathrm{Ext}^1_R(C, I) \to \dots.$$
Then $\mathrm{Ext}^1_R(C, I) = 0$ since I is injective. So μ is surjective. Let $\phi \in \mathrm{Hom}_R(C, I/A)$ be such that $\mu(\phi) = x$, and let
$$X_\phi = \{(i, c) \in I \oplus C \mid i + A = \phi(c)\}$$
be the pullback via ϕ, so
$$\begin{tikzcd} & & X_\phi \arrow[r, "\pi_C"] \arrow[d, "\pi_I"] & C \arrow[r] \arrow[d, "\phi"] & 0 \\ 0 \arrow[r] & A \arrow[ur, "\iota_I"] \arrow[r, "\le"'] & I \arrow[r] & I/A \arrow[r] & 0 \end{tikzcd}.$$

From Lemma 8.12, there is a commuting square

$$\begin{tikzcd} \mathrm{Hom}_R\left(C, C\right) \arrow[dr, "\eta"] \arrow[d, "\overline{\phi}"'] & \\ \mathrm{Hom}_R\left(C, I/A\right) \arrow[r, "\mu"'] & \mathrm{Ext}^1_R\left(C, A\right) \end{tikzcd} .$$

For $f \in \mathrm{Hom}_R\left(C, C\right)$, $\overline{\phi}\left(f\right) = \phi \circ f$. So the class of the extension

$$0 \to A \to B \to C \to 0$$

is $\eta\left(\mathrm{id}_C\right) = \mu\left(\phi \circ \mathrm{id}_C\right) = \mu\left(\phi\right) = x$.

- Extensions giving the same class are equivalent. Suppose that ψ is another element of $\mathrm{Hom}_R\left(C, I/A\right)$ such that $\mu\left(\psi\right) = x$. Tracing back through the definition of the connecting homomorphism, in the proof of the snake lemma, it can be shown that $\psi = \phi + q \circ f$, where $f : C \to I$, and q is the quotient map $I \to I/A$. Now it is easy to show that the map given by

$$\begin{array}{ccc} I \oplus C & \longrightarrow & I \oplus C \\ \left(i, c\right) & \longmapsto & \left(i + f\left(c\right), c\right) \end{array}$$

is bijective, and it maps $X_\phi \to X_\psi$. The diagram

$$\begin{tikzcd} & & X_\phi \arrow[dr] \arrow[dd, "f"] & & \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & C \arrow[r] & 0 \\ & & X_\psi \arrow[ur] & & \end{tikzcd}$$

commutes, and so the extensions are equivalent. We need to show that every extension arises as X_ϕ for some ϕ. Suppose

$$0 \to A \xrightarrow{\alpha} B \to C \to 0$$

is an extension. Let $A \le I$ where I is injective. Then there exists $\lambda : B \to I$ such that $\left(\lambda \circ \alpha\right)\left(a\right) = a$ for all $a \in A$. We have $\lambda' : C \cong B/\alpha\left(A\right) \to I/A$. We get short exact sequences

$$\begin{tikzcd} & & B \arrow[r] \arrow[dd, "\lambda"] & C \arrow[r] \arrow[dd, "\lambda'"] & 0 \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & & \\ & & I \arrow[r] & I/A \arrow[r] & 0 \end{tikzcd} .$$

Now we have $B \cong X_{\lambda'}$, since this is the same construction as before.

Lecture 27 Tuesday 10/03/20

- Equivalent extensions have the same class. Suppose

$$\begin{tikzcd} & & B_1 \arrow[dr] \arrow[dd, "f"] & & \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & C \arrow[r] & 0 \\ & & B_2 \arrow[ur] & & \end{tikzcd}$$

commutes. We get maps

$$\begin{tikzcd} \mathrm{Hom}_R\left(C, C\right) \arrow[r, bend left, "\mu_1"] \arrow[r, bend right, "\mu_2"'] & \mathrm{Ext}^1_R\left(C, A\right) \end{tikzcd}$$

commuting. So $\mu_1 = \mu_2$. Hence the extensions B_1 and B_2 have the same class.

It remains to show that it is a group homomorphism. Let

$$0 \to A \to B_i \to C \to 0, \qquad i = 1, 2.$$

Suppose $B_i = X_{\phi_i}$ for $\phi_i : C \to I/A$, where I is an injective containing A. From the arguments earlier, we have

$$\begin{tikzcd} & & B_i \arrow[r] \arrow[d, "\rho_i"] & C \arrow[r] \arrow[d, "\phi_i"] & 0 \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & & \\ & & I \arrow[r] & I/A \arrow[r] & 0 \end{tikzcd} .$$

Use the diagram above for $i = 1, 2$ to construct a new commuting diagram

$$\begin{tikzcd} 0 \arrow[r] & A \oplus A \arrow[r] \arrow[d, "+"] & B_1 \oplus B_2 \arrow[r] \arrow[d, "\rho_1+\rho_2"] & C \oplus C \arrow[r] \arrow[d, "\phi_1+\phi_2"] & 0 \\ 0 \arrow[r] & A \arrow[r] & I \arrow[r] & I/A \arrow[r] & 0 \end{tikzcd} .$$

Define

$$A^+ = \{(a, a) \mid a \in A\} \le A \oplus A, \qquad A^- = \{(a, -a) \mid a \in A\} \le A \oplus A, \qquad C^+ = \{(c, c) \mid c \in C\} \le C \oplus C.$$

Quotienting by A^-, $(A \oplus A)/A^- \cong A$, since $(a_1, a_2) = (a_1 + a_2, 0) - (a_2, -a_2)$. Then

$$\begin{tikzcd} & & (B_1 \oplus B_2)/A' \arrow[r] \arrow[d] & C \oplus C \arrow[r] \arrow[d, "\phi_1+\phi_2"] & 0 \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & & \\ & & I \arrow[r] & I/A \arrow[r] & 0 \end{tikzcd} ,$$

where A' is the image of A^- in $B_1 \oplus B_2$, so if

$$A \xrightarrow{\alpha_1} B_1 \xrightarrow{\beta_1} C, \qquad A \xrightarrow{\alpha_2} B_2 \xrightarrow{\beta_2} C,$$

then $A' = \{(\alpha_1(a), -\alpha_2(a))\}$. Let $X \le (B_1 \oplus B_2)/A'$ be the preimage of C^+ in the map $(B_1 \oplus B_2)/A' \to C \oplus C$. Then

$$0 \to A \to X \to C^+ \to 0$$

is exact, and we have $C^+ \cong C$. We get

$$\begin{tikzcd} & & X \arrow[r] \arrow[d] & C \arrow[r] \arrow[d, "\phi_1+\phi_2"] & 0 \\ 0 \arrow[r] & A \arrow[ur] \arrow[dr] & & & \\ & & I \arrow[r] & I/A \arrow[r] & 0 \end{tikzcd} ,$$

identifying the maps

$$\begin{array}{cccccc} \phi_1 + \phi_2 & : & C \oplus C & \longrightarrow & I/A \\ & & (c, c) & \longmapsto & \phi_1(c) + \phi_2(c) \end{array}, \qquad \begin{array}{cccccc} \phi_1 + \phi_2 & : & C & \longrightarrow & I/A \\ & & c & \longmapsto & \phi_1(c) + \phi_2(c) \end{array},$$

so $X = X_{\phi_1+\phi_2}$. Recall from the definition of the Baer sum,

$$0 \to A \xrightarrow{(\alpha_1, -\alpha_2)} B_1 \oplus B_2 \xrightarrow{\beta_1-\beta_2} C \to 0,$$

and $H = \ker(\beta_1 - \beta_2) / \operatorname{im}(\alpha_1, -\alpha_2)$. But $\operatorname{im}(\alpha_1, -\alpha_2)$ is precisely the module A', and $\ker(\beta_1 - \beta_2)$ is the preimage of C^+ in $B_1 \oplus B_2$. So $X = H$, and so $[X_{\phi_1}] + [X_{\phi_2}] = [X_{\phi_1+\phi_2}]$. $\square$

We have shown that elements of $\mathrm{Ext}_R^1(C, A)$ corresponds to equivalence classes of extensions. Since the identity in $\mathrm{E}_C(A)$ is the class of split extensions, it follows that $0 \in \mathrm{Ext}_R^1(C, A)$ corresponds to split extensions $C \oplus A$.

Example. Take $R = \mathbb{Z}$. Calculate $\mathrm{Ext}_R^1(\mathbb{Z}_n, H)$ for H an abelian group. Use the functor $F(A) = \mathrm{Hom}_{\mathbb{Z}}(A, H)$. This is contravariant, so we need a projective resolution of $\mathbb{Z}_n$. This is given by

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \to \mathbb{Z}_n \to 0.$$

This gives a long exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, H) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, H) \xrightarrow{n} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, H) \to \mathrm{Ext}_R^1(\mathbb{Z}_n, H) \to 0,$$

since $\mathrm{Ext}_n^i(\mathbb{Z}, H) = 0$ for $i > 1$ since $\mathbb{Z}$ is projective. Now

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, H) \cong H_n = \{h \in H \mid nh = 0\}, \qquad \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, H) \cong H.$$

So

$$0 \to H_n \to H \xrightarrow{n} H \to \mathrm{Ext}_R^1(\mathbb{Z}_n, H) \to 0,$$

so $\mathrm{Ext}_R^1(\mathbb{Z}_n, H) \cong H/nH$.

Lecture 28 is a problems class. Lecture 28 Friday 13/03/20

9 Dimension

9.1 Projective, injective, and flat dimensions

Lecture 29 Monday 16/03/20

Definition 9.1. Let M be a R-module. The **projective dimension** $\mathrm{pd}\, M$ is the smallest d such that there exists a projective resolution $P_* \to M$ such that $P_{d+1} \to 0$, or infinity if no such d exists. The **injective dimension** $\mathrm{id}\, M$ is similar for injective resolutions. The **flat dimension** is similar for flat resolutions.

Every projective is flat, so $\mathrm{fd}\, M \le \mathrm{pd}\, M$.

Example.

- $\mathbb{Z}$ as a module for itself. Then $\mathbb{Z}$ is projective, and flat, so a projective or flat resolution is
$$0 \to \mathbb{Z} \to \mathbb{Z} \to 0,$$
so $\mathrm{fd}\, \mathbb{Z} = \mathrm{pd}\, \mathbb{Z} = 0$. Since $\mathbb{Z}$ is not injective, an injective resolution is
$$0 \to \mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \to 0,$$
so $\mathrm{id}\, \mathbb{Z} = 1$.
- $\mathbb{Q}$ as a module for $\mathbb{Z}$. This is flat but not projective, so $\mathrm{fd}\, \mathbb{Q} = 0$ and $\mathrm{pd}\, \mathbb{Q} = 1$.

Proposition 9.2. *The following are equivalent.*

1. $\mathrm{pd}\, M \le d$.
2. $\mathrm{Ext}_R^{d+1}(M, N) = 0$ *for all* N.

Proof.

$\implies$ Assume 1. Then there exists a projective resolution
$$0 \to P_d \to \dots \to P_0 \to M \to 0.$$
Let F be the functor $F(A) = \mathrm{Hom}_R(A, N)$. Then $\mathrm{Ext}_R^*(M, N)$ is calculated from the chain complex
$$0 \to F(P_d) \to \dots \to F(P_{d-1}) \to F(P_0) \to 0,$$
so clearly $\mathrm{Ext}_R^n(M, N) = \mathrm{L}_n F(P_*) = 0$ for $n > d$.

$\impliedby$ For the converse, suppose that $\mathrm{Ext}_R^{d+1}(M, N) = 0$ for all N. Suppose
$$P_{d-1} \to P_{d-2} \to \dots \to P_0 \to M \to 0$$
is exact. Let K_{d-1} be the kernel of $P_{d-1} \to P_{d-2}$, the $(d-1)$-dimensional **syzygy** of M. So
$$0 \to K_{d-1} \to P_{d-1} \to P_{d-2} \to \dots \to P_0 \to M \to 0.$$
A fact is that
$$\mathrm{Ext}_R^{d+1}(M, N) \cong \mathrm{Ext}_R^1(K_{d-1}, N).$$
Suppose $\mathrm{Ext}_R^{d+1}(M, N) = 0$. Then $\mathrm{Ext}_R^1(K_{d-1}, N) = 0$. So K_{d-1} is projective. Hence
$$0 \to K_{d-1} \to P_{d-1} \to P_{d-2} \to \dots \to P_0 \to M \to 0$$
is a projective resolution. So $\mathrm{pd}\, M \le d$.

∎

Proposition 9.3. *The following are equivalent.*

- $\operatorname{id} N \leq d$.
- $\operatorname{Ext}_R^{d+1}(M, N) = 0$ *for all* M.

Proof. Similar to Proposition 9.2. Use the **cosyzygy**. ☐

Proposition 9.4. *The following are equivalent.*

- $\operatorname{fd} M \leq d$.
- $\operatorname{Tor}_{d+1}^R(M, N) = 0$ *for all* N.

Fact. Any flat resolution for M can be used to calculate Tor.

Proof. Using the fact, the proof is the same as above. ☐

9.2 Global dimension

We will be interested in defining dimension for the ring R.

Definition 9.5. Claim that

$$\sup\{\operatorname{pd} M \mid M \text{ a left } R\text{-module}\} = \sup\{\operatorname{id} M \mid M \text{ a left } R\text{-module}\} = \sup\left\{d \;\middle|\; \exists M, N,\ \operatorname{Ext}_R^d(M, N) \neq 0\right\},$$

where the supremums are in $\mathbb{N} \cup \{\infty\}$. This number is the **left global dimension** $\operatorname{lgd} R$ of R. The **right global dimension** $\operatorname{rgd} R$ is defined similarly, but using right modules.

There exist rings R such that $\operatorname{lgd} R \neq \operatorname{rgd} R$.

Definition 9.6. Say that R satisfies the **ascending chain condition on right ideals** if whenever $I_0 \leq I_1 \leq \dots$ is a chain of right ideals, there exists d such that $I_d = I_{d+1} = \dots$. The condition that R satisfies the **ascending chain condition on left ideals** is similar. If R satisfies the ascending chain condition on both left and right ideals, it is **noetherian**.

Fact. For any noetherian ring R, $\operatorname{lgd} R = \operatorname{rgd} R$.

Definition 9.7. So in this context we can refer to **global dimension**, $\operatorname{gd} R$. Claim that

$$\sup\{\operatorname{fd} N \mid N \text{ a left } R\text{-module}\} = \sup\{\operatorname{fd} M \mid M \text{ a right } R\text{-module}\} = \sup\left\{d \;\middle|\; \exists M, N,\ \operatorname{Tor}_d^R(M, N) \neq 0\right\}.$$

This number is the **weak global dimension** $\operatorname{wgd} R$.

Since $\operatorname{fd} M \leq \operatorname{pd} M$, $\operatorname{wgd} R \leq \operatorname{gd} R$.

9.3 Krull dimension

Lecture 30
Tuesday
17/03/20

The following is another ring dimension. Let R be a commutative ring.

Definition 9.8. The **Krull dimension** $\dim R$ is the length of the longest chain of prime ideals of R, where $I \leq R$ is **prime** if $I \neq R$, and $ab \in I$ implies that $a \in I$ or $b \in I$.

In particular, any maximal ideal of R is prime.

Example. Let V be an **affine variety** in F^n, defined by the zeros of a set of polynomials in $F[x_1, \dots, x_n]$. Then V corresponds to an ideal I_V in $F[x_1, \dots, x_n]$, and V is **irreducible** if I_V is prime. Then

$$\dim F[x_1, \dots, x_n] / I_V = \dim V.$$

Fact. $\dim R \leq \operatorname{gd} R$.

Definition 9.9. A ring is **local** if it has a unique maximal ideal, so the non-units of R form an ideal. Let $I \leq R$ be a prime ideal. The **localisation** of R at I is the ring

$$\left\{ \frac{r}{q} \;\middle|\; r \in R, \; q \in R \setminus I \right\}.$$

The unique maximal ideal is

$$\left\{ \frac{i}{q} \;\middle|\; i \in I, \; q \in R \setminus I \right\},$$

so this ring is local. This is a basic tool in algebraic geometry.

Theorem 9.10 (Serre)**.** *Let R be a noetherian local ring such that $\dim R$ is finite. Then*

$$\dim R = \operatorname{gd} R.$$

Example. $R = F[x_1, \dots, x_n]$ corresponds to the zero variety. This is not local, but $\dim R = \operatorname{gd} R = n$. The fact that $\operatorname{gd} R = n$ is **Hilbert's syzygy theorem**.

- Let $n = 3$. Note that F is a module for R, by the multiplication $x_i \lambda = 0$ for all x_i and $\lambda \in F$. Let us calculate a projective resolution, keeping track of the syzygies. If

  $$0 \to K_1 \to R \to F \to 0,$$

  then

  $$\begin{aligned} K_1 &= \ker \begin{pmatrix} R & \longrightarrow & F \\ x_i & \longmapsto & 0 \\ 1 & \longmapsto & 1 \end{pmatrix} \\ &= \langle x_1, x_2, x_3 \rangle \leq R. \end{aligned}$$

  If

  $$0 \to K_2 \to R^3 \to K_1 \to 0,$$

  then

  $$\begin{aligned} K_2 &= \ker \begin{pmatrix} R^3 & \longrightarrow & K_1 \\ (r_1, r_2, r_3) & \longmapsto & r_1 x_1 + r_2 x_2 + r_3 x_3 \end{pmatrix} \\ &= \{(r_1, r_2, r_3) \mid r_1 x_1 + r_2 x_2 + r_3 x_3 = 0\} \\ &= \langle (0, x_3, -x_2), (-x_3, 0, x_1), (x_2, -x_1, 0) \rangle \leq R^3. \end{aligned}$$

  If

  $$0 \to K_3 \to R^3 \to K_2 \to 0,$$

  then

  $$\begin{aligned} K_3 &= \ker \begin{pmatrix} R^3 & \longrightarrow & K_2 \\ (r_1, r_2, r_3) & \longmapsto & (r_3 x_2 - r_2 x_3, r_1 x_3 - r_3 x_1, r_2 x_1 - r_1 x_2) \end{pmatrix} \\ &= \langle (x_1, x_2, x_3) \rangle \cong R. \end{aligned}$$

  Our projective resolution is

  $$0 \to R \to R^3 \to R^3 \to R \to F \to 0.$$

- Generally for arbitrary n, this construction gives

  $$P_j = R^{\binom{n}{j}}.$$

  Generators of $K_j \leq P_{j-1}$ correspond to subsets of size j of $\{1, \dots, n\}$. The generator corresponding to a subset S of size j will have a coordinate for each subset T of size $j - 1$. This coordinate is zero if $T \not\subseteq S$ and $\pm x_i$ if $S = T \cup \{i\}$.

This is an example of a **Koszul complex**, and is a technique used for calculating syzygies explicitly in certain situations.