MATH70063 Algebra 4 :: Lecture notes

Lecturer: Oliver Gregory

Last edited: 1st May 2025

Contents

One should call this module homological algebra.

1 Basic category theory

Definition 1.0.1. A *category* $\mathcal{C}$ is the data:

- a class $|\mathcal{C}|$ of *objects*
- a set $\mathrm{Hom}_{\mathcal{C}}(A, B)$ for each ordered pair (A, B) in $|\mathcal{C}|$ of *morphisms* (or *arrows*)
- a distinguished element $\mathrm{id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ for each $A \in |\mathcal{C}|$
- a map $\circ : \mathrm{Hom}_{\mathcal{C}}(B, C) \times \mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{C}}(A, C)$ for each ordered triples (A, B, C) in $|\mathcal{C}|$

such that

- Associativity: $(h \circ g) \circ f = h \circ (g \circ f)$ for all $f : A \to B, g : B \to C, h : C \to D$.
- Unit: $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$ for all $A, B \in |\mathcal{C}|, f : A \to B$

Example 1.0.2. 0.

$$\begin{tikzcd}
A \arrow[r, "f"'] \arrow[loop left, "\mathrm{id}_A"] \arrow[rr, bend right, "g\circ f"'] & B \arrow[r, "g"'] \arrow[loop below, "\mathrm{id}_B"] \arrow[rr, bend left, "h\circ g"] & C \arrow[r, "h"'] \arrow[loop above, "\mathrm{id}_C"] & D \arrow[loop right, "\mathrm{id}_D"]
\end{tikzcd}$$

1. The category of sets, denoted by Set: objects are sets, morphisms are functions
2. The category of groups, denoted by Grp: objects are groups, morphisms are homomorphisms
3. The category of R-modules, denoted by R-Mod: objects are R-modules, morphisms are homomorphisms
4. The category of topological spaces, denoted by Top: objects are topological spaces, morphisms are continuous maps

Definition 1.0.3. $f \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ is *monic* if $\forall e_1, e_2 : A \to B$ with $e_1 \neq e_2$ one has $f e_1 \neq f e_2$.
$f \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ is *epic* if $\forall g_1, g_2 : C \to D$ with $g_1 \neq g_2$ one has $g_1 f \neq g_2 f$.

Exercise 1.0.4. 1. Show that monic/epic maps in Set are precisely injective/surjective functions.

2. Show that $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is epic in the category of rings.

Definition 1.0.5. $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ is an *isomorphism* if $\exists g \in \mathrm{Hom}_{\mathcal{C}}(B, A) : gf = \mathrm{id}_A,\ fg = \mathrm{id}_B$.

Exercise 1.0.6. Give a category with more than one objects such that every morphism is monic and epic, but not an isomorphism.
Solution.

$$\begin{tikzcd}
A \arrow[r, "f"'] \arrow[loop left, "\mathrm{id}_A"] & B \arrow[loop right, "\mathrm{id}_B"]
\end{tikzcd}$$

Definition 1.0.7. The *opposite category* $\mathcal{C}^{\mathrm{op}}$ is the category with same objects as $\mathcal{C}$ but morphisms (and compositions) are reversed.

Definition 1.0.8. For two categories $\mathcal{C}, \mathcal{D}$, a *covariant functor* $F : \mathcal{C} \to \mathcal{D}$ is a rule that associates to every $C \in |\mathcal{C}|$ on $F(C) \in |\mathcal{D}|$, and to every $f : C_1 \to C_2$ in $\mathcal{C}$ on $F(f) : F(C_1) \to F(C_2)$ in $\mathcal{D}$ such that

1. $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}\ \ \forall A \in |\mathcal{C}|$
2. $F(gf) = F(g)F(f)\ \forall f, g$ that can be composed

Definition 1.0.9. A *contravariant functor* $\mathcal{C} \to \mathcal{D}$ is a covariant functor $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$.

Example 1.0.10. Let $\mathcal{C}$ be a category and $A \in |\mathcal{C}|$, then there is a covariant functor $\mathrm{Hom}_{\mathcal{C}}(A, -) : \mathcal{C} \to \mathrm{Set}$.

Definition 1.0.11. For $F, G : \mathcal{C} \to \mathcal{D}$, a *natural transformation* $\eta : F \Rightarrow G$ is a rule associating to every $C \in |\mathcal{C}|$ a morphism $\eta_C : F(C) \to G(C)$ in $|\mathcal{D}|$ such that $\forall f \in \mathrm{Hom}_{\mathcal{C}}(C, C')$ the diagram

$$\begin{tikzcd} F(C) \arrow[r, "F(f)"] \arrow[d, "\eta_C"'] & F(C') \arrow[d, "\eta_{C'}"] \\ G(C) \arrow[r, "G(f)"'] & G(C') \end{tikzcd}$$

commutes. If each η_C is an isomorphism, then η is called a *natural isomorphism*.

Definition 1.0.12. A functor $F : \mathcal{C} \to \mathcal{D}$ is an *equivalence of categories* if $\exists G : \mathcal{D} \to \mathcal{C}$ and natural isomorphisms $\mathrm{id}_{\mathcal{C}} \cong GF,\ \mathrm{id}_{\mathcal{D}} \cong FG$.

Exercise 1.0.13.

1. Define the category of categories, Cat, (morphisms are functors).
2. Let $\mathcal{C}, \mathcal{D}$ be two categories. Define the functor category $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ (or $[\mathcal{C}, \mathcal{D}]$). Show that the isomorphisms in $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ are precisely the natural isomorphisms.
3. Let k be a field and write fdVect_k for the category of finite dimensional k-vector spaces (morphisms are k-linear maps). Show that the fdVect_k is equivalent to Mat_k defined as follows: objects are non-negative integers and morphisms $m \to n$ are given by:
   - if $m, n \neq 0$ then $m \to n$ are $m \times n$ matrices with coefficients in k
   - if m or $n = 0$, then $m \to n$ is unique

   and compositions are given by matrix multiplications.

Week 2, lecture 1, 15th January

Definition 1.0.14. A functor $F : \mathcal{C} \to \mathcal{D}$ is *faithful/full* if the induced maps on the Hom sets $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(F(A), F(B)) : f \mapsto F(f)$ is injective/surjective. If both, then F is *fully faithful*.

1.1 Adjoint functors

Definition 1.1.1. A pair of functors $L : \mathcal{C} \to \mathcal{D}$, $R : \mathcal{D} \to \mathcal{C}$ are *adjoint* if there is a bijection

$$\tau_{\mathcal{C},\mathcal{D}} : \mathrm{Hom}_{\mathcal{D}}(L(C), D) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(C, R(D))$$

$\forall C \in |\mathcal{C}|,\ D \in |\mathcal{D}|$ which is *natural* in (C, D), i.e. $\forall f : C \to C'$ in $\mathcal{C}$ and $g : D \to D'$ in $\mathcal{D}$, the diagram

$$\begin{tikzcd} \mathrm{Hom}_{\mathcal{D}}(L(C'), D) \arrow[r, "-\circ L(f)"] \arrow[d, "\tau_{C',D}"] & \mathrm{Hom}_{\mathcal{D}}(L(C), D) \arrow[r, "g\circ -"] \arrow[d, "\tau_{C,D}"] & \mathrm{Hom}_{\mathcal{D}}(L(C), D') \arrow[d, "\tau_{C,D'}"] \\ \mathrm{Hom}_{\mathcal{C}}(C', R(D)) \arrow[r, "-\circ f"] & \mathrm{Hom}_{\mathcal{C}}(C, R(D)) \arrow[r, "R(g)\circ -"] & \mathrm{Hom}_{\mathcal{C}}(C, R(D')) \end{tikzcd}$$

commutes. In this case we say L is a *left adjoint* of R and R is a *right adjoint* of L.

Exercise 1.1.2. Show that there are two natural transformations $\eta : \mathrm{id}_{\mathcal{C}} \Rightarrow RL$ (unit) and $\varepsilon : LR \Rightarrow \mathrm{id}_{\mathcal{D}}$ (co-unit) such that $R \xrightarrow{\eta R} RLR \xrightarrow{R\varepsilon} R$ is id_R and $L \xrightarrow{L\eta} LRL \xrightarrow{\varepsilon L} L$ is id_L.

Example 1.1.3 (Equivalence of categories are adjoint pairs)**.** Let AbGrp be the category of abelian groups. Then we have the forgetful functor Forg : AbGrp $\to$ Grp that "forgets" that a group is abelian. It's the identity on objects and morphisms, so it's fully faithful. We also have a functor in the other direction: $(-)^{\mathrm{ab}} : \mathrm{Grp} \to \mathrm{AbGrp} : G \mapsto G/[G, G]$ where $[G, G]$ is the commutator subgroup.

We claim $(-)^{\mathrm{ab}}$ is the left adjoint of Forg. Let $G \in |\,\mathrm{Grp}\,|$ and $A \in |\,\mathrm{AbGrp}\,|$. We need to show

$$\begin{aligned} \tau_{G,A} : \mathrm{Hom}_{\mathrm{AbGrp}}(G^{\mathrm{ab}}, A) &\to \mathrm{Hom}_{\mathrm{Grp}}(G, A) \\ (f : G^{\mathrm{ab}} \to A) &\mapsto (\overline{f} : G \twoheadrightarrow G^{\mathrm{ab}} \xrightarrow{f} A) \end{aligned}$$

is a bijection and natural in (G, A).

$\tau_{G,A}$ is surjective: let $f : G \to A$ be a group homomorphism. Since A is abelian, f kills all commutators, so f factors uniquely through G^{ab}, i.e. $\exists! g$ such that

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, two heads] & A \\ G^{\mathrm{ab}} \arrow[ur, dotted, "g"'] & \end{tikzcd}$$

commutes. Clearly $\tau_{G,A}(g) = f$.

$\tau_{G,A}$ is injective since Forg is identity. Naturality is left as exercise.

Week 2, lecture 2, 15th January

1.2 Products and coproducts

Definition 1.2.1. Let I be an index set and a collection $\{C_i : i \in I\}$ of objects in $\mathcal{C}$. A *product* of $\{C_i : i \in I\}$ is an object $X \in |\mathcal{C}|$ together with morphisms $\pi_i : X \to C_i$ for each $i \in I$ such that the following universal property holds: $\forall Y \in |\mathcal{C}|$ and the family of morphisms $f_i : Y \to C_i, i \in I$, $\exists! f$ such that $\forall i \in I$, the diagram

$$\begin{tikzcd} & C_i \\ Y \arrow[ur, "f_i"] \arrow[r, dotted, "f"'] & X \arrow[u, "\pi_i"'] \end{tikzcd}$$

commutes. Denote the product by $\prod_{i \in I} C_i$.

Exercise 1.2.2. Show that if a product exists, then it is unique up to isomorphism.

Example 1.2.3. 1. Products in Set is the Cartesian product of sets.

2. In Grp, it's the usual product of groups.
3. In R-Mod, it's the direct product.
4. in Top, it is the Cartesian product of the underlying sets endowed with the product topology.

Definition 1.2.4. Let J be an index set and a collection $\{C_j : j \in J\}$ of objects in $\mathcal{C}$. A *coproduct* of $\{C_j : j \in J\}$ is an object $X \in |\mathcal{C}|$ together with morphisms $\iota_j : C_j \to X$ for each $j \in J$ such that $\forall Y \in |\mathcal{C}|$ with $g_j : C_j \to Y, j \in J$, $\exists! g$ such that $\forall j \in J$, the diagram

$$\begin{tikzcd} C_j \arrow[d, "\iota_j"'] \arrow[dr, "g_j"] & \\ X \arrow[r, dotted, "g"'] & Y \end{tikzcd}$$

commutes. Denote the coproduct by $\coprod_{j \in J} C_j$.

Exercise 1.2.5. Again, coproducts are unique up to isomorphism, so we can say <u>the</u> coproduct.

Example 1.2.6. 1. Coproducts in Set are disjoint unions.

2. In R-Mod they are direct sums.
3. In Grp, they are free products.
4. In top, it is the disjoint union of underlying sets endowed with disjoint union topology.

Exercise 1.2.7. Show that products/coproducts in $\mathcal{C}$ are precisely coproducts/products in $\mathcal{C}^{\mathrm{op}}$.

2 Modules

Definition 2.0.1. By *ring*, we mean an associative ring with a unit, i.e. an abelian group R with respect to + with an associative operation $\times$ such that $x(y+z) = xy + xz, (x+y)z = xz + yz$ and $\exists 1 \in R : 1x = x1 = x \ \forall x \in R$.
Denote by R^* the (group of) units of R, i.e. $x \in R : \exists y \in R : xy = yx = 1$.

Definition 2.0.2. If $R^* = R \backslash \{0\}$ then R is a *skew-field*. A commutative skew-field is a *field*.

Example 2.0.3.

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$ where except $\mathbb{Z}$ are fields
- $R[x_1, \dots, x_n]$ where R is a ring
- $\mathrm{Mat}_n(k)$ where k is a skew-field
- $\mathbb{H}$ the quaternions form a skew field

Definition 2.0.4. A *left R-module M* is an abelian group with a function $* : R \times M \to M$ which encodes the left action of R on M such that $\forall r, r_1, r_2 \in R, m, m_1, m_2 \in M$,

- $r * (m_1 + m_2) = r * m_1 + r * m_2$
- $(r_1 + r_2) * m = r_1 * m + r_2 * m$
- $1 * m = m$
- $(r_1 r_2) * m = r_1 * (r_2 * m)$

Example 2.0.5.

- $M = R^n$ is an R module with action by component-wise multiplication. Such modules are called *free with finite rank*.
- A left ideal $I \subset R$
- If $L : V \to V$ is a k-linear map of a k-vector space V, then V is a $k[x]$-module where x acts as L
- Take ring $R = \mathrm{Mat}_n(k)$, then $M = k^n$ is a left R-module with action by matrices acting on column vectors

Definition 2.0.6. A *right R-module* has the same definition as the left one, but replace $(r_1 r_2) * m = r_1 * (r_2 * m)$ by $(r_1 r_2) * m = r_2 * (r_1 * m)$.

Example 2.0.7. Again take $R = \mathrm{Mat}_n(k)$, then $M = k^n$ is also a right R-module with action by matrices acting on row vectors.

Remark 2.0.8. For left R-modules, we usually omit the $*$ sign and write rm for $r * m$, and for right R-modules, we write mr for $r * m$. In this way, we have $(r_1 r_2)m = r_1(r_2 m)$ for left R-modules and $m(r_1 r_2) = (mr_1)r_2$ for right R-modules.

Definition 2.0.9. For a ring R, the *opposite ring R^{op}* is obtained by replacing xy by yx. Then a left/right R-module is a right/left R^{op}-module.

Remark 2.0.10. If R is commutative, then $R = R^{\mathrm{op}}$, and there is no distinction between left and right R-modules.

Week 2, lecture 3, 16th January

Example 2.0.11.

- Abelian groups are precisely $\mathbb{Z}$-module
- k-vector spaces are in particular k-modules
- A representation of a group G over the field k is equivalent to a $k[G]$-module

Definition 2.0.12. A *homomorphism* $f : L \to M$ of left R-modules is a group homomorphism such that $f(rx) = rf(x) \ \forall r \in R, x \in M$.

Definition 2.0.13. $L \subset M$ is a *submodule* of M if L is a subgroup which is stable under the R-action.
Since M is an abelian group with respect to addition, we have the quotient group M/L, and since L is stable under R, we find that M/L is an R-module. This is called a *quotient module*.

Example 2.0.14. A left $I \subset R$ is precisely a submodule of R as a R-module.

Definition 2.0.15. R-Mod is the category of left R-modules with morphism being R-module homomorphisms.

Proposition 2.0.16. R-Mod has products and coproducts.

Proof. First recall Cartesian products $\prod_{i\in I} X_i = \{(x_i)_{i\in I} : x \in X_i \ \forall i \in I\}$ of sets $\{X_i : i \in I\}$. If I have left R-modules $\{M_i : i \in I\}$, consider $\prod_{i\in I} M_i$ of the underlying sets, which has a left R-action by acting coordinate-wise. As an exercise, check the universal property of products. (For a fixed $i_o \in I$, there is a surjective R-module homomorphism $\prod_{i\in I} \twoheadrightarrow M_{i_0} : (x_i)_{i\in I} \mapsto x_{i_0}$.) This is called the *direct product* of modules.
The *direct sum* $\bigoplus_{i\in I} M_i$ is the submodule of $\prod_{i\in I} M_i$ given by the condition that all but finitely many of the coordinates are zero. For a fixed $i_0 \in I$, we have an injective left R-module homomorphism $M_{i_0} \hookrightarrow \bigoplus_{i\in I} M_i : x \mapsto (x_i)_{i\in I}$ where $x_i = \begin{cases} 0 & \text{if } i \neq i_0 \\ x & \text{if } i = i_0 \end{cases}$. ◻

Remark 2.0.17. From the construction it's clear that if I is finite, then $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$.

Definition 2.0.18. A *free* R-module is a direct sum of copies of R.

Exercise 2.0.19. Show every k-module is free where k is a field.

2.1 Complexes of R-modules

Definition 2.1.1. A sequence of R-modules and R-module homomorphisms

$$\cdots \xrightarrow{f_{n-1}} A_n \xrightarrow{f_n} A_{n+1} \xrightarrow{f_{n+1}} A_{n+2} \xrightarrow{f_{n+2}} \cdots$$

is called a *complex* if $f_{n+1} \circ f_n = 0 \ \forall n$. Moreover, the sequence is *exact* if $\ker f_{n+1} = \operatorname{im} f_n \ \forall n$.

Definition 2.1.2. An exact sequence of the form

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

is called a *short exact sequence*, or *ses*.

Remark 2.1.3. Giving a ses is precisely the same thing as giving an injection $\alpha : A \hookrightarrow B$, since then automatically $C = B/\alpha(A)$ and β is the natural quotient map. It's also precisely the same thing as giving a surjection $\beta : B \twoheadrightarrow C$, since then automatically $A = \ker\beta$ and α is simply inclusion.

Example 2.1.4. For two modules A, C, we always have a ses $0 \to A \xrightarrow{\alpha} A \oplus C \xrightarrow{\beta} C \to 0$ where $\alpha : a \mapsto (a, 0)$ and $\beta : (a, c) \to c$. Such a ses is called *split*.

Remark 2.1.5. Not every ses is split! cf.

$$\begin{array}{c} 0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0 \\ 1 \mapsto 2 \end{array}$$

but $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 2.1.6. For a ses of the form $(*)$, the following are equivalent:

1. The sequence is split.
2. $\exists$ an R-module homomorphism $\sigma : C \to B : \beta\sigma = \mathrm{id}_C$. In this case we say σ is a *splitting* of β.
3. $\exists$ an R-module homomorphism $\rho : B \to A : \rho\alpha = \mathrm{id}_A$. In this case we say ρ is a *retraction* of α.

Week 3, lecture 1, 22nd January

Proof. If $(*)$ is split, then $B = A \oplus C$, and the splitting is given by definition of the coproduct.
Now suppose $\exists$ such a σ. We need to construct an isomorphism $f : B \xrightarrow{\sim} A \oplus C$ such that

$$\begin{tikzcd}
& a \arrow[r, mapsto] & (a,0) \arrow[r, mapsto] & c & \\
0 \arrow[r] & A \arrow[r] & A \oplus C \arrow[r] & C \arrow[r] & 0 \\
0 \arrow[r] & A \arrow[r, "\alpha"] \arrow[u, equal] & B \arrow[r, "\beta"] \arrow[u, "f"'] & C \arrow[r] \arrow[u, equal] \arrow[l, bend left, "\sigma"] & 0
\end{tikzcd}$$

commutes. We can read off f from the diagram (assuming it commutes): the square on the right tells us the second coordinate is simply β and together with the left square we have $f : b \mapsto (\alpha^{-1}(b - \sigma\beta(b)), \beta(b))$. Indeed; first this map is well defined: α is injective and since $\beta(b - \sigma\beta(b)) = \beta(b) - \beta(\sigma(\beta(b))) = \beta(b) - \beta(b)$, we have $b - \sigma\beta(b) \in \ker\beta = \operatorname{im}\alpha$. Now

- f is injective: suppose $f(b) = 0$. Then $\beta(b) = 0$, so $b \in \operatorname{im}\alpha$ and write $\beta = \alpha(a)$ for some $a \in A$. Then $f(b) = f(\alpha(a)) = (a, 0) = 0$, so $a = 0$ and hence $b = 0$.
- f is surjective: let $a \in A, c \in C$. Then $f : \sigma(c) + \alpha(a) \mapsto (a, c)$:

$$\alpha^{-1}(\sigma(c) + \alpha(a) - \sigma\beta(\sigma(c) + \alpha(a))) = \alpha^{-1}(\alpha(a) - \sigma\beta\alpha(a)) = a - \alpha^{-1}\sigma(0) = a$$
$$\beta(\sigma(c) + \alpha(a)) = c + \beta\alpha(a) = c + 0 = c$$

The proof of the equivalence between 1 and 3 is left as an exercise. □

Exercise 2.1.7. Show that $(*)$ splits whenever C is a free R-module.

2.2 Injective and projective R-modules

Definition 2.2.1. For R-modules A, B, we say A is a *direct summand* of B if $\exists$ another R-module $C : B = A \oplus C$.

Definition 2.2.2. An R-module M is *projective* if for any ses of R-modules of the form $(*)$ and any R-module homomorphism $f : M \to C$, $\exists$ an R-module homomorphism $g : M \to B : f = \beta g$. In this case we say f *lifts* to g, or g is a *lifting* of f.

Note that if C is projective, take $f : C \to C$ to be identity, then it follows that the ses $(*)$ splits.

Lemma 2.2.3. A direct sum is projective $\iff$ each summand is projective.

Proof. $\Longleftarrow$ Let $M = \bigoplus_{s\in S} M_s$ and suppose each M_s is projective. Let $f : M \to C$ be an R-module homomorphism. Then each $f|_{M_s} = f_s : M_s \to C$ lifts to $g_s : M_s \to B$ with $f_s = \beta g_s$. Now by definition of direct sum, only finitely many coordinates of M are nonzero, then $g = \sum_{s\in S} g_s : M \to B$ is a well-defined R-module homomorphism, and clearly $f = \beta g$.

$\Longrightarrow$ Suppose M is projective and fix $s \in S$. Let $f_s : M_s \to C$ be an R-module homomorphism. We can extend this to an R-module homomorphism $f : M \to C$ by taking 0 on all summands except s, on which we take f_s. Since M is projective, f lifts to $g : M \to B$ with $f = \beta g$. Then $g_s = g|_{M_s} : M_s \to B$ is a well-defined homomorphism with $f_s = \beta g_s$.

□

Example 2.2.4. The R-module R is projective since any homomorphism from R is determined by the image of 1. Hence any free R-module is projective by lemma above.

Proposition 2.2.5 (Criterion for projectivity)**.** An R-module is projective $\iff$ it is a direct summand of a free R-module.

Proof. $\Longleftarrow$ Since free modules are projective, the desired follows immediately from 2.2.3.

$\Longrightarrow$ Any R-module M is a quotient of a free R-module F; explicitly, take F to be the R-module finitely generated by elements of M: $F = \{(r_m)_{m\in M} : r_m \in R \text{ and all but finitely many } r_m \neq 0\}$. Then there is a surjective R-module homomorphism $\varphi : F \twoheadrightarrow M : (r_m)_{m\in M} \mapsto \sum_{m\in M} r_m m$. If M is projective, then the short exact sequence $0 \to \ker\varphi \to F \to M \to 0$ splits, in particular M is a direct summand of the free module F.

□

Example 2.2.6 (Non-free projective module)**.** Let $R = \mathbb{Z}/6\mathbb{Z}$ and $M = (3) \cong \mathbb{Z}/2\mathbb{Z}$. By Chinese remainder theorem, $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, so M is a direct summand of R as an R-module, hence M is projective, but M is clearly not free since if it is, then it's copies of $\mathbb{Z}/6\mathbb{Z}$ so it has at least 6 elements, but it only has 2.

Week 3, lecture 2, 22nd January

Definition 2.2.7. An R-module M is *injective* if for any ses of R-modules of the form $(*)$ and any R-module homomorphism $f : A \to M$, $\exists$ an R-module homomorphism $g : B \to M : f = g\alpha$.

Note that if A is injective, take $f : A \to A$ to be identity, then it again follows that ses $(*)$ splits.

Lemma 2.2.8. A direct product is injective $\iff$ each factor is injective.

Proof. Write $M = \prod_{s \in S} M_S$.

$\Longleftarrow$ Suppose each M_s is injective and let $f : A \to M$ be an R-module homomorphism. Then each $f_s : A \to M \to M_s$ extends to $g_s : B \to M_s$ with $f_s = g_s\alpha$, so $\prod_{s \in S} g_s : B \to M$ is a well-defined R-module homomorphism with $g\alpha = f$.

$\Longrightarrow$ Suppose M is injective and let $f_s : A \to M_s$ for some $s \in S$. We extend this to a map $f : A \to M$ by letting all other coordinates to be 0. Then f extends to $g : B \to M$ with $g\alpha = f$. Then for each s, $g_s : B \to M \to M_s$ satisfies $g_s\alpha = f_s$.

□

Lemma 2.2.9 (Zorn's)**.** Let S be an nonempty set with partial order $\leq$. A totally ordered subset $C \subset S$ is called a *chain*. An upper bound of a subset $X \subset S$ is a $t \in S : t \geq x \ \forall x \in X$. Then if any chain in S has an upper bound, then S has a maximal element m, i.e. $x \leq m \implies m = x$.

Theorem 2.2.10 (Baer's criterion for injectivity)**.** The following are equivalent.

1. The R-module M is injective.
2. For any R-module homomorphism $f : I \to M$ where I is an ideal of R, $\exists m \in M : f$ has the form $f(x) = xm$.
3. For any ideal $I \subset R$, any R-module homomorphism $I \to M$ extends to an R-module homomorphism $R \to M$.

Proof. $2 \iff 3$: To give an R-module homomorphism $R \to M$, it's the same thing to specify the image of $1 \in R$. So if $f(x) = xm$ for $x \in I$, then f can be extended to R by $1 \mapsto m$. Conversely, any $I \to M$ which is a restriction of $f : R \to M$ is of the form $f(x) = xf(1)$.

$1 \implies 3$: If M is injective, consider the ses $0 \to I \to R \to R/I \to 0$, then by definition any R module homomorphism $I \to M$ extends to an R-module homomorphism $R \to M$.

$3 \implies 1$: Suppose we have

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

where $B \to M$ extends g. Let

$$S = \{(A', g') : A \subset A' \subset B, g' : A' \to M \text{ is a } R\text{-module homomorphism} : g'|_A = g\}$$

and define a partial order on S by: $(A', g') \leq (A'', g'')$ if $A' \subset A''$ and $g''|_{A'} = g'$. Then each chain in S has an upper bound — take the union of all submodules A' in the chain, with the corresponding g'. Hence Zorn's lemma says S has a maximal element $(A_0, g_0) \in S$.

We claim $A_0 = B$. Indeed, certainly $A_0 \subset B$, and for a contradiction suppose $\exists b \in B \backslash A_0$. Let $A_1 = \{a + xb : a \in A_0, x \in R\}$ be an R-module. Then $A_0 \subsetneq A_1$, and g_0 extends to $g_1 : A_1 \to M : a + xb \mapsto g_0(a) + xm$ by specifying $g_1(b) = m$, but any $m \in M$ will do, as long as $Rb \to M : b \mapsto m$ agrees with g_0 on $A_0 \cap Rb = \{xb \in A_0 : x \in R\}$. Note that $I = \{x \in R : xb \in A_0\}$ is an ideal of R, so by our assumption, $m \in M$ exists as above precisely when the R-module homomorphism $I \to Ib \xrightarrow{g_0} M$ has the form $x \mapsto xm$ for some $m \in M$. But this is true; and the map g_1 we wrote is well-defined, i.e. if $a + xb = a' + x'b$ then $g_0(a) + xm = g_0(a') + x'm$; indeed, $a - a' = (x' - x)b$, so $x' - x \in I$, so $g_0(a) - g_0(a') = g_1(a) - g_1(a') = g_1(a - a') = g_1((x' - x)b) = (x' - x)g_1(b) = x'm - xm$.

This contradicts that (A_0, g_0) is maximal, so $A_0 = B$, and we obtain an R-module homomorphism $B \to M$. □

Week 3, lecture 3, 23rd January

Example 2.2.11. We use Baer's criterion to verify that $\mathbb{Q}$ is an injective $\mathbb{Z}$-module by showing a $\mathbb{Z}$-module homomorphism $f : I \to \mathbb{Q}$ extends to $\mathbb{Z}$-module homomorphism $f : \mathbb{Z} \to \mathbb{Q}$ for any ideal $I \subset \mathbb{Z}$. Since $\mathbb{Z}$ is a PID, write $I = n\mathbb{Z}$. If f is the zero map or if $n = 0$ we're done. Let $y = \frac{f(n)}{n} \in \mathbb{Q}$, and define the extension $g : \mathbb{Z} \to \mathbb{Q} : z \mapsto zy$.

Exercise 2.2.12. Let $A \in |\mathcal{C}|$. Show that the contravariant functor $F_A = \mathrm{Hom}_{\mathcal{C}}(-, A) : \mathcal{C} \to \mathrm{Set}$ induces a covariant functor $\Psi : \mathcal{C} \to \mathrm{Fun}(\mathcal{C}^{\mathrm{op}}, \mathrm{Set})$.

Solution. Naturally, Ψ sends $A \in |\mathcal{C}|$ to F_A, and $f : A \to B$ in $\mathcal{C}$ to the natural transformation $\eta_f : F_A \Rightarrow F_B$ defined as follows

Week 4, lecture 1, 29th January

2.3 Hom, or what does projective/injective really mean?

Given R-modules A, B, we have an abelian group $\mathrm{Hom}_R(A, B) = \{R\text{-module homomorphisms } A \to B\}$ under addition of maps.

Proposition 2.3.1. There are canonical isomorphisms

$$\mathrm{Hom}_R\left(\bigoplus_{i \in I} A_i, B\right) \cong \prod_{i \in I} \mathrm{Hom}_R(A, B)$$

and

$$\mathrm{Hom}_R\left(A, \prod_{i \in I} B_i\right) \cong \prod_{i \in I} \mathrm{Hom}_R(A, B_i).$$

Proof. Recall the universal property that coproducts satisfy; in this case of A_i, we have that there are maps $\iota_i : A_i \to \bigoplus_{i \in I} A_i$ such that $\forall R$-modules Y with homomorphisms $\{g_i : A_i \to Y : i \in I\}$, $\exists! g : \bigoplus_{i \in I} A_i \to Y$ such that

$$\begin{tikzcd} A_j \arrow[d, "\iota_j"'] \arrow[dr, "g_j"] & \\ \bigoplus_{i \in I} A_i \arrow[r, dotted, "\exists! g"] & Y \end{tikzcd}$$

commutes. Then the first desired isomorphism is $f \mapsto (f \circ \iota_i)_{i \in I}$ with inverse $(f_i)_{i \in I} \mapsto$ the unique$f$ given by the universal property (since B is an R-module and $f_i \in \mathrm{Hom}_R(A_i, B)$ are homomorphisms).

The second one is similar. □

Corollary 2.3.2. There are canonical isomorphisms

$$\mathrm{Hom}_R(A_1 \oplus A_2, B) \cong \mathrm{Hom}_R(A_1, B) \oplus \mathrm{Hom}_R(A_2, B)$$

and

$$\mathrm{Hom}_R(A, B_1 \oplus B_2) \cong \mathrm{Hom}_R(A, B_1) \oplus \mathrm{Hom}_R(A, B_2).$$

Proof. Finite products are precisely finite coproducts. □

Remark 2.3.3. If I is infinite, then we only have

$$\mathrm{Hom}_R\left(A, \bigoplus_{i \in I} B_i\right) \subset \mathrm{Hom}_R\left(A, \prod_{i \in I} B_i\right) \cong \prod_{i \in I} \mathrm{Hom}_R(A, B_i),$$

which does not necessarily coincide with $\bigoplus_{i \in I} \mathrm{Hom}_R(A, B_i)$. For example, consider the case $A = \bigoplus_{i \in I} B_i$ where each B_i is nonzero, then id on $\bigoplus_{i \in I} B_i$ is not in $\bigoplus_{i \in I} \mathrm{Hom}_R(A, B_i)$.

Similarly,

$$\bigoplus_{i \in I} \mathrm{Hom}_R(A_i, B) \subset \mathrm{Hom}_R\left(\prod_{i \in I} A_i, B\right)$$

is not necessarily an equality; consider the case $B = \prod_{i \in I} A_i$ where each A_i is nonzero, then id is not in $\bigoplus_{i \in I} \mathrm{Hom}_R(A_i)$.

Lemma 2.3.4. Let $0 \to A_1 \to A_2 \to A_3 \to 0$ be a ses of R-modules. Then

1. The sequence of abelian groups
$$0 \to \mathrm{Hom}_R(A_3, B) \to \mathrm{Hom}_R(A_2, B) \to \mathrm{Hom}_R(A_1, B) \tag{$*$}$$
is exact.
2. The sequence of abelian groups
$$0 \to \mathrm{Hom}_R(B, A_1) \to \mathrm{Hom}_R(B, A_2) \to \mathrm{Hom}_R(B, A_3) \tag{$**$}$$
is exact.
3. Any sequence of the form $(*)$ extends to an ses, i.e. $\mathrm{Hom}_R(A_2, B) \to \mathrm{Hom}_R(A_1, B)$ is surjective, iff B is injective.
4. Any sequence of the form $(**)$ extends to an ses, i.e. $\mathrm{Hom}_R(B, A_2) \to \mathrm{Hom}_R(B, A_3)$ is surjective, iff B is projective.

Proof. Left as an exercise; simply writing down the definitions almost suffices. □

2.4 Tensor products

Definition 2.4.1. For a right module A and a left module B, let F be the free abelian group generated by all pairs (a, b) where $a \in A, b \in B$. Let $S \subset F$ generated by elements of the form $(a + a', b) - (a, b) - (a', b), (a, b + b') - (a, b) - (a, b'), (ar, b) - (a, rb)$ where $a, a' \in A, b.b' \in B, r \in R$. The *tensor product* of A, B, denoted by $A \otimes_R B$ is then the quotient group F/S. The image of a generator (a, b) in $A \otimes_R B$ is denoted by $a \otimes b$. Since we mod out S, we have
$$\begin{aligned} (a + a') \otimes b &= a \otimes b + a' \otimes b \\ a \otimes (b + b') &= a \otimes b + a \otimes b' \\ ar \otimes b &= a \otimes rb \end{aligned}$$
$\forall a, a' \in A, b.b' \in B, r \in R.$

Example 2.4.2. What is $R \otimes_R M$? It's generated by $r \otimes m = 1 \otimes rm$, hence the map $f : M \to R \otimes_R M : m \mapsto r \otimes m$ is surjective. It's also injective: define the map $g : F \to M : (r, m) \mapsto rm$, then by axioms of modules, g sends S to 0, so g defines a group homomorphism $F/S = R \otimes_R M \to M$, and $gf = \mathrm{id}_M$, so f is an isomorphism.

Remark 2.4.3. In general, $A \times B \to A \otimes_R B : (a, b) \mapsto a \otimes b$ is nowhere near injective or surjective. For example, $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$. Indeed, $2(a \otimes b) = 2a \otimes b = 0$, and $3(a \otimes b) = a \otimes 3b = 0$.

Week 4, lecture 2, 29th January

Remark 2.4.4. If $f : A \to A'$ is a (right) R-module map, then there is a natural map $f \otimes \mathrm{id} : A \otimes_R B \to A' \otimes_R B : x \otimes y \mapsto f(x) \otimes y$. Indeed, write $A \otimes_R B = F/S$ and $A' \otimes_R B = F'/S'$, then f defines a group homomorphism $F \to F' : (a, b) \mapsto (f(a), b)$, so it remains to show f sends S to S', but
$$\begin{aligned} f((x + x', y) - (x, y) - (x', y)) &= (f(x + x'), y) - (f(x), y) - (f(x'), y) \\ &= (f(x) + f(x'), y) - (f(x), y) - (f(x'), y) \in S \end{aligned}$$
and similarly for the other two relations.

If we have a left R-module map $g : B \to B'$, we also by a similar argument have $\mathrm{id} \times g : A \otimes_R B \to A \otimes_R B' : x \otimes y \mapsto x \otimes g(y)$.

Hence $\otimes_R$ is covariant in each argument.

Definition 2.4.5. The universal property of the tensor product is that if there is a function $f : A \times B \to C$ which is linear in each argument and satisfies $f(ar, b) = f(a, rb)\ \forall a \in A, b \in B, r \in R$, then f is uniquely written as $f = g\phi$ for some homomorphism $g : A \otimes_R B \to C$.

Lemma 2.4.6. Let $\{M_i : i \in I\}$ be a family of left R-modules. Then there is a canonical isomorphism
$$A \otimes_R \left(\bigoplus_{i \in I} M_i \right) \cong \bigoplus_{i \in I} (A \otimes_R M_i).$$

Proof. The natural map

$$A \times \left(\bigoplus_{i \in I} A \right) \to \bigoplus_{i \in I} A \otimes_R M_i$$

satisfies the universal property, hence factors through

$$A \otimes_R \left(\bigoplus_{i \in I} M_i \right) \to \bigoplus_{i \in I} (A \otimes_R M_i) .$$

Now, the maps

$$A \otimes_R M_i \to A \otimes_R \left(\bigoplus_{i \in I} M_i \right)$$

gives

$$\bigoplus_{i \in I} (A \otimes_R M_i) \to A \otimes_R \left(\bigoplus_{i \in I} M_i \right)$$

by the universal property of coproducts. They are inverses of each other again by universal property. $\square$

Lemma 2.4.7. Let $0 \to A_1 \xrightarrow{\alpha} A_2 \xrightarrow{\beta} A_3 \to 0$ be a ses of right R-modules. For any left R-module B, the sequence of abelian groups

$$A_1 \otimes_R B \xrightarrow{\alpha \otimes \mathrm{id}} A_2 \otimes_R B \xrightarrow{\beta \otimes \mathrm{id}} A_3 \otimes_R B \to 0$$

is exact.

Proof. Omitted in lecture, see notes. $\square$

Example 2.4.8. Let A be an abelian group and $n \in N$. Define $A/n = A \otimes_{\mathbb{Z}} \mathbb{Z}/n$. Consider the ses $0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n \to 0$. Then by the lemma, we have the exact sequence $0 \to A[n] \to A \xrightarrow{\times n} A \to A/n \to 0$ where $A[n] = \{a \in A : na = 0\}$.

Definition 2.4.9. A left R-module B is *flat* if $- \otimes_R B$ preserves short exact sequences of right R-modules, i.e. it preserves injections.

Example 2.4.10. We just saw that $\mathbb{Z}/n$ is not a flat $\mathbb{Z}$-module.

Proposition 2.4.11. Projective modules are flat.

Proof. 2.4.6 tells us that a direct sum of modules is flat $\iff$ each summand is flat, and in particular free modules are flat, but by 2.2.5 projective modules are precisely a summand of a free module. $\square$

2.5 Modules over integral domains

Let R be an integral domain, i.e. a commutative ring such that $ab = 0 \implies a = 0$ or $b = 0$ $\forall a, b \in R$.

Definition 2.5.1. An element $m \in M$ is a *torsion element* if $rm = 0$ for some $r \in R \backslash \{0\}$. Denote the set of torsion elements by $M_{\text{tors}} = \{m \in M : m \text{ is a torsion element}\}$, which is a submodule of M. If $M_{\text{tors}} = 0$ we say M is *torsion-free*. If $M_{\text{tors}} = M$ we say M is *torsion*.

Example 2.5.2. $\mathbb{Z}$ and $\mathbb{Q}$ are torsion-free. $\mathbb{Z}/n, \mathbb{Q}/z$ are torsion.

Lemma 2.5.3. Projective R-modules are torsion-free.

Proof. Free modules are torsion-free since R has no zero divisors, so their submodules are torsion-free, and by 2.2.5 projective modules are precisely summands of free modules. $\square$

Definition 2.5.4. An element $x \in M$ is *(infinitely) divisible* if for every $r \in R \backslash \{0\}$, one can write $x = ry$ for some $y \in M$. Denote the set of divisible elements by $M_{\div} = \{m \in M : m \text{ is divisible}\}$, which is a submodule of M. If $M_{\div} = M$ we say M is divisible.

Example 2.5.5. $\mathbb{Q}, \mathbb{Q}/\mathbb{Z}$ are divisible, $\mathbb{Z}, \mathbb{Z}/n$ are not.

Lemma 2.5.6. Injective R-modules are divisible.

Proof. Let $m \in M, r \in R \backslash \{0\}$. We need to show $\exists s \in M : m = rs$. Note that the principal ideal $I = rR$ and R are isomorphic as R-modules: $R \to I : x \mapsto rx$. The R-module map $R \to M : x \mapsto xm$ composed with the inverse of that map give an R-module map $f : I \to M : rx \mapsto xm$.

Consider the inclusion $I \hookrightarrow R$. Since M is injective, by 2.2.10 f extends to an R-module map $F : R \to M$. I claim $F(1)$ works as te desired s. Indeed, $rs = rF(1) = F(r) = f(r) = m$. □

Week 5, lecture 1, 5th February

2.5.1 Modules over principal ideal domains

Theorem 2.5.7. Let R be a PID.

1. Every submodule of a free R-module is free.
2. Every submodule of R^n is isomorphic to R^m for some $m \leq n$.

Proof. 1. Let M be a free R-module and write M as $\bigoplus_{s \in S} R_s$ where each R_s is a copy of R. Write 1_s for the identity of R_s.

The well-ordering theorem says any set can be well-ordered, i.e. there is a total order such that every nonempty subset has a least element. This allows us to do transfinite induction: a statement is true for all $s \in S$ if it's true for the least element of S and its truth for all $x < s$ implies its truth for s.

Let N be a submodule of M. Define $N_t = N \cap \bigoplus_{s \leq t} R_s$ (we've already used the total order to do this). Consider the projection of M to the tth summand $\bigoplus_{s \in S} R_s \twoheadrightarrow R_t = R$ and restrict this to N_t to obtain an R-module map $f_t : N_t \to R$. Then the image $f_t(N_t)$ is a R-submodule of R, i.e. an ideal. But R is a PID, so $f_t(N_t) = Ra_t$ for some $a_t \in R$. If $a_t \neq 0$, choose $n_t \in N_t : f_t(n_t) = a_t$. If $a_t = 0$, choose $n_t = 0$. Define N'_t as the submodule of N_t generated by n_s for $s \leq t$.

Claim: $N'_t = N_t \; \forall t \in S$. We prove this by transfinite induction. The statement is clearly true when t is the least element of S. Now suppose $N'_s = N_s \; \forall s < t$. Clearly $N'_t \subset N_t$. Any $n \in N_t$ can be written as $n = rn_t + (n - rn_t)$ where $n - rn_t$ is a finite linear combination of $1_s \in R_s$ for $s < t$. Let q be the largest index used in this finite combination. Then $n - rn_t \in N_q$, so by inductive hypothesis $n - rn_t \in N'_q$. Hence $n \in N'_t$, i.e. $N_t \subset N'_t$.

Hence N is generated by the n_s for $s \in S$. It remains to show every element of N can be uniquely written as a finite linear combination of $n_s : s \in S$. For a contradiction, suppose $0 = \sum_{s \in T} r_s n_s$ where $T \subset S$ is finite and $r_s n_s \neq 0 \; \forall s \in T$. Then $a_s \neq 0$. Choose t to be the largest element of T, then f_t kills all terms except possibly $r_t n_t \mapsto r_t a_t$, but $f_t(0) = 0$ so $r_t a_t = 0$, hence $r_t = 0$, a contradiction.

2. Let $K = \operatorname{Frac} R$. Then $R \subset K$ so $R^n \subset K^n$. Let $N = \bigoplus_{s \in S} R \subset R^n$. Then $N \subset N \otimes_R K \subset R^n \otimes_R K = K^n$. Hence $N \otimes_R K$ is a K-subspace of K^n, so it has a K-basis with size $\leq n$, but a K-basis of $N \otimes_R K$ is in bijection with S, so $|S| \leq n$.

□

Corollary 2.5.8. If R is a PID, then projective modules are precisely free modules.

Proof. This follows from 2.2.5 and the theorem above. □

Theorem 2.5.9. If R is a PID, then injective modules are precisely divisible modules.

Proof. We saw last time 2.5.6, so it remains to show any divisible module M is injective. We use 2.2.10 and let $f : I \to M$ be a R-module map where $I \subset R$ is an ideal. Since R is a PID, write $I = aR$ for some $a \in R$. Since M is divisible, write $f(a) = as$ for some $s \in M$. Then $f : I \to M$ extends to $R \to M$ by $1 \mapsto s$. □

Example 2.5.10. The $\mathbb{Z}$-modules $\mathbb{Q}/\mathbb{Z}$, $\mathbb{R}/\mathbb{Z}$, $\mathbb{Q}$ are clearly divisible, hence injective.

Week 5, lecture 2, 5th February

The lecture was not recorded; it covered Theorem 0.4 and its proof which is available in the given notes for week 5. The theorem is as the following:

Theorem 2.5.11. If R is a PID, then flat modules are precisely torsion-free modules.

Week 5, lecture 3, 6th February

2.6 Enough injectives

Theorem 2.6.1 (R-Mod has enough injectives)**.** Let R be a ring. Every R-module is isomorphic to a submodule of an injective R-module.

Proof. 1. Claim: for every nonzero abelian group G, $\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}) \neq 0$. Moreover, $\forall 0 \neq x \in G$, $\exists f \in \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}) : f(x) \neq 0$.

   Let $C = \langle x \rangle \subset G$. If C is finite, there is a injective homomorphism $C \hookrightarrow \mathbb{Q}/\mathbb{Z}$ by $x \mapsto \frac{1}{|C|}$. If C is infinite, consider the homomorphism via $x \mapsto \frac{1}{2}$. In both cases the image of x is nonzero so we have a nontrivial homomorphism $C \to \mathbb{Q}/\mathbb{Z}$. Then since $\mathbb{Q}/\mathbb{Z}$ is injective, this extends to a nonzero homomorphism $G \to \mathbb{Q}/\mathbb{Z}$.

   For the second part, consider R as a right R-module and let $S = \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$. Then S can be considered as a left R-module by the action $rf(x) = f(xr)$.

2. Claim: S is an injective R-module.

   Consider the canonical isomorphism of abelian groups for a R-module M

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

   which works like this: a map $m \mapsto \phi_m$ on the left goes to $m \mapsto \phi_m(1)$ on the right, and a map ϕ on the right goes to $m \mapsto (r \mapsto \phi(rm))$ on the left. Moreover, the isomorphism is functional, i.e. if $M \to N$ is an R-module map, the diagram

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

   commutes. Since $\mathbb{Q}/\mathbb{Z}$ is injective, for any injective R-module map $M \hookrightarrow N$, any $M \to \mathbb{Q}/\mathbb{Z}$ extends to $N \to \mathbb{Q}/\mathbb{Z}$, i.e. $(*)$ is surjective, hence $(**)$ is surjective as well.

3. Claim: for any M, $\mathrm{Hom}_R(M, S) \neq 0$. Moreover, for any $0 \neq m \in M$, $\exists f \in \mathrm{Hom}_R(M, S) : f(m) \neq 0$.

   This is immediate now.

4. Now let $I(M)$ be the product of copies of S indexed by $\mathrm{Hom}_R(M, S)$, so by 2.2.8 $I(M)$ is injective. Consider the canonical map $M \to I(M)$ by sending m to the element whose coordinate with index $f \in \mathrm{Hom}_R(M, S)$ is $f(m)$. Then rm is sent to the element whose coordinate with index $f \in \mathrm{Hom}_R(M, S)$ is $f(rm) = rf(m)$, so $M \to I(M)$ is a left R-module map. It follows from step 3 that this map is injective.

□

3 Homology and cohomology

3.1 Resolutions

Let R be a ring. A *chain complex* $A_\bullet$ of R-modules is a sequence $\cdots \xrightarrow{d} A_{n+1} \xrightarrow{d} A_n \xrightarrow{d} A_{n-1} \xrightarrow{d} \cdots$ such that $d^2 = 0$, i.e. $\mathrm{im}\, d \subset \ker d$. A complex can be finite, infinite or semi-infinite. A *map of chain complexes* $f_\bullet : A_\bullet \to B_\bullet$ is a collection of R-module maps $f_n : A_n \to B_n$ such that $df_n = f_{n-1}d\ \forall n$, i.e. the diagram

$$\begin{tikzcd}
\cdots \arrow[r, "d"] & A_{n+1} \arrow[r, "d"] \arrow[d, "f_{n+1}"] & A_n \arrow[r, "d"] \arrow[d, "f_n"] & A_{n-1} \arrow[r, "d"] \arrow[d, "f_{n-1}"] & \cdots \\
\cdots \arrow[r, "d"] & B_{n+1} \arrow[r, "d"] & B_n \arrow[r, "d"] & BA_{n-1} \arrow[r, "d"] & \cdots
\end{tikzcd}$$

commutes.

A *cochain complex* of R-modules is a complex in reverse: $\cdots \xrightarrow{d} C^{n-1} \xrightarrow{d} C^n \xrightarrow{d} C^{n+1} \xrightarrow{d} \cdots$, denoted by $C^\bullet$, and *maps of cochain complexes* are what you think.

Week 6, lecture 1, 12th February

Definition 3.1.1. Let $A_\bullet$ be a chain complex. The nth *homology group* is

$$H_n(A_\bullet) = \ker(d : A_n \to A_{n-1})/\operatorname{im}(d : A_{n+1} \to A_n).$$

Similarly define cohomology group of cochain complexes.

Note that $A_\bullet$ is exact $\iff H_n(A_\bullet) = 0\ \forall n$.

Proposition 3.1.2. If $f_\bullet : A_\bullet \to B_\bullet$ is a map of complexes, then we get an induced map $f_* : H_n(A_\bullet) \to H_n(B_\bullet)$.

Proof. First let's see how $f_\bullet$ induces a map $\ker(d : A_n \to A_{n-1}) \to \ker(d : B_n \to B_{n-1})$. Let $a \in \ker(d : A_n \to A_{n-1})$, i.e. $a \in A_n$ and $d(a) = 0$. Then $d(f_n(a)) = f_{n-1}(d(a)) = 0$, i.e. $f_n(a) \in \ker(d : B_n \to B_{n-1})$ as desired.

It remains to see we have a map $\operatorname{im}(d : A_{n+1} \to A_n) \to \operatorname{im}(d : B_{n+1} \to B_n)$. Let $a \in \operatorname{im}(d : A_{n+1} \to A_n)$, i.e. $a \in A_n$ and $a = d(a')$ for some $a' \in A_{n+1}$. Hence $f_n(a) = f_n(d(a')) = d(f_{n+1}(a')) \in \operatorname{im}(d : B_{n+1} \to B_n)$ as desired. □

Definition 3.1.3. $f_\bullet : A_\bullet \to B_\bullet$ is a *quasi-isomorphism* if the induced maps of nth homology groups f_* are isomorphisms $\forall n$.

Definition 3.1.4. A *left resolution* of an R-module M is a (right bounded) chain complex of R-modules $\cdots \xrightarrow{d} P_2 \xrightarrow{d} P_1 \xrightarrow{d} P_0$ together with a map $P_0 \to M$ such that the complex $\cdots \xrightarrow{d} P_2 \xrightarrow{d} P_1 \xrightarrow{d} P_0 \to M \to 0$ is exact. Denote a left resolution by $P_\bullet \to M$. If each P_i is projective then $P_\bullet \to M$ is a *projective resolution* of M.

Remark 3.1.5. To have a right bounded chain complex $P_\bullet$ with a homomorphism $P_0 \to M$ is precisely the same data as a morphism of complexes

$$\begin{tikzcd}
\cdots \arrow[r, "d"] & P_2 \arrow[r, "d"] \arrow[d] & P_1 \arrow[r, "d"] \arrow[d] & P_0 \arrow[r] \arrow[d] & 0 \arrow[r] & \cdots \\
\cdots \arrow[r, "d"] & 0 \arrow[r, "d"] & 0 \arrow[r, "d"] & M \arrow[r] & 0 \arrow[r] & \cdots
\end{tikzcd}$$

and to ask for the complex $P_\bullet$ to be exact precisely means $H_n(P_\bullet) = 0\ \forall n \geq 1$ and $H_0(P_\bullet) = P_0/\operatorname{im}(d : P_1 \to P_0)$ where $\operatorname{im}(d : P_1 \to P_0) = \ker(P_0 \to M)$ since the diagram commutes. But also $P_0 \to M$ is asked to be surjective to have a left resolution, so $H_0(P_\bullet) \cong M$. Hence to ask for a left resolution is precisely asking for a right bounded complex quasi-isomorphic to M (the complex with M in degree 0 and 0 elsewhere).

The idea is then, if I want to study a module M which might be complicated, then I should find a left resolution of M where each of the P_i's are hopefully better behaved (i.e. projective). This idea of replacing stuff we don't understand by complexes of things we do understand gets us quite far and deep.

Definition 3.1.6. A *right resolution* of an R-module M is a (left bounded) cochain complex of R-modules $I^0 \xrightarrow{d} I^1 \xrightarrow{d} I^2 \xrightarrow{d} \cdots$ together an R-module map $M \to I^0$ such that $0 \to M \to I^0 \xrightarrow{d} I^1 \xrightarrow{d} I^2 \xrightarrow{d} \cdots$ is exact. Denote this by $M \to I^\bullet$. If each I^i is injective then $M \to I^\bullet$ is an *injective resolution* of M.

Example 3.1.7.

1. The ses of abelian groups $0 \to \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$ exhibits the 2-term complex $\mathbb{Z} \xrightarrow{\times n} \mathbb{Z}$ (together with the map $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$) as a projective resolution of the finite abelian group $\mathbb{Z}/n\mathbb{Z}$.
2. The ses $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ exhibits the 2-term complex $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ (together with the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$) as an injective resolution of the abelian group $\mathbb{Z}$.
3. Let k be a field and consider k as a $k[x]/(x^n)$-module by x acting as 0. Then

$$\cdots \xrightarrow{\times x^{n-1}} k[x]/(x^n) \xrightarrow{\times x} k[x]/(x^n) \xrightarrow{\times x^{n-1}} k[x]/(x^n) \xrightarrow{\times x} k[x]/(x^n)$$

is an exact sequence. Together with the projection $k[x]/(x^n) \twoheadrightarrow k$, this is a projective resolution of k.

Lemma 3.1.8. Every module has a projective and injective resolution.

Proof. We know any module M has a surjective map $\varepsilon : P_0 \twoheadrightarrow M$ where P_0 is free (hence projective). Define $M_0 = \ker \varepsilon$ and take a surjective map $P_1 \twoheadrightarrow M_0$ where P_1 is free (hence projective). Let $d : P_1 \to P_0$ be $P_1 \twoheadrightarrow M_0 \hookrightarrow P_0$. Then $\operatorname{im}(d : P_1 \to P_0) = M_0 = \ker(\varepsilon : P_0 \twoheadrightarrow M)$. This gives the first part of a projective resolution. Now define $M_1 = \ker(d : P_1 \to P_0)$ and repeat.

The injective part is left as an exercise (use that every module is isomorphic to a submodule of an injective module (2.6.1)). □

Proposition 3.1.9. Suppose $P_\bullet \to M$ is a projective resolution of M. Let $f : M \to N$ be an R-module map. Then

1. For any left resolution $Q_\bullet \to N$, there exists R-module maps $f_n : P_n \to Q_n$ $\forall n$ such that

$$\begin{tikzcd} \cdots \arrow[r] & P_2 \arrow[r, "d"] \arrow[d, dashed, "f_2"] & P_1 \arrow[r, "d"] \arrow[d, dashed, "f_1"] & P_0 \arrow[r] \arrow[d, dashed, "f_0"] & M \arrow[r] \arrow[d, "f"] & 0 \\ \cdots \arrow[r] & Q_2 \arrow[r, "d"] & Q_1 \arrow[r, "d"] & Q_0 \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

   commutes.

2. If $g_\bullet : P_\bullet \to Q_\bullet$ is another map of complexes that the above diagram commutes, then there are maps $s_n : P_n \to Q_{n+1}$ such that $f_n - g_n = s_{n-1}d + ds_n$ $\forall n \geq 1$ and $f_0 - g_0 = ds_0$.

Proof. Read the notes. $\square$

Remark 3.1.10. Part 2 says $f_\bullet$ is "unique up to homotopy". More precisely, a *chain homotopy* $s : f_\bullet \Rightarrow g_\bullet$ between two chain complex maps $f_\bullet, g_\bullet : C_\bullet \to D_\bullet$ is a sequence of R-module maps $s_n : C_n \to D_{n+1}$ $\forall n$ such that

$$\begin{tikzcd} \cdots \arrow[r, "d"] & C_{n+1} \arrow[r, "d"] \arrow[d, bend right, "f_{n+1}"'] \arrow[d, bend left, "g_{n+1}"] & C_n \arrow[r, "d"] \arrow[dl, "s_n"] \arrow[d, bend right, "f_n"'] \arrow[d, bend left, "g_n"] & C_{n-1} \arrow[r, "d"] \arrow[dl, "s_{n-1}"'] \arrow[d, bend right, "f_{n-1}"'] \arrow[d, bend left, "g_{n-1}"] & \cdots \\ \cdots \arrow[r, "d"] & D_{n+1} \arrow[r, "d"] & D_n \arrow[r, "d"] & D_{n-1} \arrow[r, "d"] & \cdots \end{tikzcd}$$

commutes.

Lemma 3.1.11. Let $f_\bullet, g_\bullet : A_\bullet \to B_\bullet$ be maps of complexes. If $f_\bullet$ and $g_\bullet$ are homotopic, then they induce the same maps f_*, g_* on homology.

Proof. Exercise. It suffices to prove if $f_\bullet$ is homotopic to zero then f_* is 0 on homology. $\square$

Suppose I have maps of complexes $A_\bullet \to B_\bullet \to C_\bullet$. We say it is a *ses of complexes* and write $0 \to A_\bullet \to B_\bullet \to C_\bullet \to 0$ if for each n, $0 \to A_n \to B_n \to C_n \to 0$ is a ses of modules.

Lemma 3.1.12. An ses of complexes induces a long exact sequence on homology

$$\begin{tikzcd} \cdots \arrow[r] & H_n(A_\bullet) \arrow[r] & H_n(B_\bullet) \arrow[r] & H_n(C_\bullet) \arrow[dll] \\ & H_{n-1}(A_\bullet) \arrow[r] & H_{n-1}(B_\bullet) \arrow[r] & H_{n-1}(C_\bullet) \arrow[dll] \\ & \cdots \arrow[r] & \cdots \arrow[r] & \cdots \arrow[dll] \\ & H_0(A_\bullet) \arrow[r] & H_0(B_\bullet) \arrow[r] & H_0(C_\bullet) \arrow[r] & 0 \end{tikzcd}$$

Proof. We use the snake lemma: a commutative diagram with exact rows

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

induces an exact sequence

$$\ker f \longrightarrow \ker g \longrightarrow \ker h \longrightarrow \operatorname{coker} f \longrightarrow \operatorname{coker} g \longrightarrow \operatorname{coker} h.$$

To prove the snake lemma, consider

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & \ker f \arrow[r] \arrow[d] & \ker g \arrow[r] \arrow[d] & \ker h \arrow[d] \arrow[dddll, rounded corners] & \\
 & L \arrow[r] \arrow[d, "f"] & M \arrow[r] \arrow[d, "g"] & N \arrow[r] \arrow[d, "h"] & 0 \\
0 \arrow[r] & L' \arrow[r] \arrow[d] & M' \arrow[r] \arrow[d] & N' \arrow[d] & \\
 & \operatorname{coker} f \arrow[r] \arrow[d] & \operatorname{coker} g \arrow[r] \arrow[d] & \operatorname{coker} h \arrow[d] & \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where each column is exact. We apply it to

$$\begin{tikzcd}
 & A_1/d(A_2) \arrow[r] \arrow[d, "d"] & B_1/d(B_2) \arrow[r] \arrow[d, "d"] & C_1/d(C_2) \arrow[r] \arrow[d, "d"] & 0 \\
0 \arrow[r] & A_0 \arrow[r] & B_0 \arrow[r] & C_0 &
\end{tikzcd}$$

and obtain

$$H_1(A_\bullet) \longrightarrow H_1(B_\bullet) \longrightarrow H_1(C_\bullet) \longrightarrow H_0(A_\bullet) \longrightarrow H_0(B_\bullet) \longrightarrow H_0(C_\bullet) \longrightarrow 0$$

where $H_0(B_\bullet) \to H_0(C_\bullet)$ is surjective since $B_0 \to C_0$ is surjective. Now we do the snake to

$$\begin{tikzcd}
 & A_2/d(A_3) \arrow[r] \arrow[d, "d"] & B_2/d(B_3) \arrow[r] \arrow[d, "d"] & C_2/d(C_3) \arrow[r] \arrow[d, "d"] & 0 \\
0 \arrow[r] & \ker(A_1 \to A_0) \arrow[r] & \ker(B_1 \to B_0) \arrow[r] & \ker(C_1 \to C_0) &
\end{tikzcd}$$

and obtain

$$H_2(A_\bullet) \longrightarrow H_2(B_\bullet) \longrightarrow H_2(C_\bullet) \longrightarrow H_1(A_\bullet) \longrightarrow H_1(B_\bullet) \longrightarrow H_1(C_\bullet) \longrightarrow 0.$$

If we can glue the two together and proceed similarly we are done. It remains to see that the arrows we glue are indeed the same, which can be done by staring at the two commutative diagrams of exact rows above. □

Week 6, lecture 3, 13th February

3.2 Derived functors

Let $\mathcal{C}, \mathcal{C}'$ be abelian categories. (Typically $\mathcal{C} = R$-Mod and $\mathcal{C}' = \mathbb{Z}$-Mod = AbGrp). Suppose $\mathcal{C}$ has enough projectives (i.e. every object is a surjective image of a projective object). Let $F : \mathcal{C} \to \mathcal{C}'$ be a functor such that if $0 \to A \to B \to C \to 0$ is an ses in $\mathcal{C}$ then $F(A) \to F(B) \to F(C) \to 0 \quad (*)$ in $\mathcal{C}'$ is exact. In this case we say F is *right exact*. We now want to see how far is $(*)$ away from an ses.

Definition 3.2.1. Define $L_nF : A \mapsto H_n(F(P_\bullet))$ where $P_\bullet \to A$ is a projective resolution of A in $\mathcal{C}$. This is called the nth *left derived functor* of L.

Note that A doesn't have a unique projective resolution, so how is the above well-defined? i.e. How can $L_nF(A)$ be independent of $P_\bullet$?

Theorem 3.2.2. 1. $L_0F = F$.

2. If $Q_\bullet \to A$ is another projective resolution of A, then $A \mapsto H_N(F(P_\bullet))$ and $A \mapsto H_N(F(Q_\bullet))$ are naturally isomorphic functors.

3. For any ses $0 \to A \to B \to C \to 0$ in $\mathcal{C}$ we get a long exact sequence in $\mathcal{C}'$ of the form

$$\begin{tikzcd}
\cdots \arrow[r] & L_nF(A) \arrow[r] & L_nF(B) \arrow[r] & L_nF(C) \arrow[dll] \\
& L_{n-1}F(A) \arrow[r] & L_{n-1}F(B) \arrow[r] & L_{n-1}F(C) \arrow[dll] \\
& \cdots \arrow[r] & \cdots \arrow[r] & \cdots \arrow[dll] \\
& L_1F(A) \arrow[r] & L_1F(B) \arrow[r] & L_1F(C) \arrow[dll] \\
& F(A) \arrow[r] & F(B) \arrow[r] & F(C) \arrow[r] & 0.
\end{tikzcd}$$

Proof. 1. Consider the ses $0 \to \mathrm{im}(P_1 \to P_0) \to P_0 \to A \to 0$. Since F is right exact, we have the exact sequence $F(\mathrm{im}(P_1 \to P_0)) \to F(P_0) \to F(A) \to 0$. Clearly $P_1 \twoheadrightarrow \mathrm{im}(P_1 \to P_0)$, so again since F is right exact, $F(P_1) \twoheadrightarrow F(\mathrm{im}(P_1 \to P_0))$, hence the exact sequence $F(P_1) \to F(P_0) \to F(A) \to 0$. This shows $H_0(F(P_\bullet)) = F(A)$ as desired.

2. By 3.1.9 and 3.1.11, there is a well-defined map $H_n(F(P_\bullet)) \to H_n(F(Q_\bullet))$. But P and Q are symmetrical so we also have a map $H_n(F(Q_\bullet)) \to H_n(F(P_\bullet))$. Moreover, if we compose the two maps of complexes which induce the two above maps we get identity. Hence $H_n(F(P_\bullet)) \cong H_n(F(Q_\bullet))$.

3. Postponed for a second because we need a lemma.

□

Lemma 3.2.3 (Horseshoe)**.** Let $0 \to A \to B \to C \to 0$ be an ses and $P_\bullet \to A$, $R_\bullet C$ be projective resolutions. Define $Q_n = P_n \oplus R_n$ for each n. Then one can define maps $Q_n \to Q_{n-1}$ for $n \geq 1$ and $Q_0 \to B$ such that $Q_\bullet \to B$ is a projective resolution and we have a commutative diagram with exact rows

$$\begin{tikzcd}
\vdots \arrow[r, hook] \arrow[d, "d"] & \vdots \arrow[r, two heads] \arrow[d, "d"] & \vdots \arrow[d, "d"] \\
P_1 \arrow[r, hook] \arrow[d, "d"] & Q_1 \arrow[r, two heads] \arrow[d, "d"] & R_1 \arrow[d, "d"] \\
P_0 \arrow[r, hook] \arrow[d, two heads] & Q_0 \arrow[r, two heads] \arrow[d] & R_0 \arrow[d, two heads] \\
A \arrow[r, hook] & B \arrow[r] & C
\end{tikzcd}$$

Proof. Construct a map $Q_0 \to B$: on P_0 we have $P_0 \twoheadrightarrow A \hookrightarrow B$; on R_0 we have $R_0 \twoheadrightarrow C$, but R_0 is projective, this lifts to a map $R_0 \to B$. Now we can use the snake lemma on

$$\begin{tikzcd}
& P_0 \arrow[r] \arrow[d] & Q_0 \arrow[r] \arrow[d] & R_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A \arrow[r] & B \arrow[r] & C
\end{tikzcd}$$

and see $\mathrm{coker}(Q_0 \to B) = 0$, so $Q_0 \twoheadrightarrow B$. Now iterate for $Q_1 = P_1 \oplus R_1$ and so on. □

Week 7, lecture 1, 19th February

3.3 Ext and Tor functors

3.3.1 First principles

Definition 3.3.1. Let R be a ring.

1. Let B be a left R-module. Then the ith left derived functor of $- \otimes_R B$: right R-modules $\to$ abelian groups is called $\mathrm{Tor}_i^R(-, B)$.

2. Let A be a right R-module. Then the ith right derived functor of $\mathrm{Hom}_R(A, -)$: left R-modules $\to$ abelian groups is called $\mathrm{Ext}_R^i(A, -)$.

Remark 3.3.2. Given a right module A, I could've considered $F(-) = A \otimes_R -$: left R-modules $\to$ abelian groups and taken the ith left derived functor. It turns out that $L_i F(B) = \mathrm{Tor}_i^R(A, B)$. This is called the "balancing of Tor". Similarly, given a left module B, I could've considered $G(-) = \mathrm{Hom}_R(-, B)$: right R-modules $\to$ abelian groups and taken the ith right derived functor. It turns out that $R^i G(A) = \mathrm{Ext}_R^i(A, B)$. This is called the "balancing of Ext". Depending on what A, B are, this might makes calculations easier.

Example 3.3.3. 1. Let A be an abelian group. Compute $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$. We saw $P_\bullet = (\mathbb{Z} \xrightarrow{\times n} \mathbb{Z})$ together with $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ is a projective resolution of $\mathbb{Z}/n\mathbb{Z}$. To compute $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A)$, we need to compute the homology of $P_\bullet \otimes_R A$, i.e. the homology of $A \xrightarrow{\times n} A$. So we find that

$$\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) = \begin{cases} A/n & \text{if } i = 0 \\ A[n] & \text{if } i = 1 \\ 0 & \text{if } i \geq 2 \end{cases}$$

A similar calculation gives

$$\mathrm{Ext}_{\mathbb{Z}}^i(\mathbb{Z}/n\mathbb{Z}, A) = \begin{cases} A[n] & \text{if } i = 0 \\ A/n & \text{if } i = 1 \\ 0 & \text{if } i \geq 2 \end{cases}$$

2. Let $n \geq 2$ and k be a field. Consider k as a $k[x]/(x^n)$-module via x acting as 0. Compute $\mathrm{Tor}_i^{k[x]/(x^n)}(k, k[x]/(x^n))$. We saw that

$$\cdots \xrightarrow{\times x^{n-1}} k[x]/(x^n) \xrightarrow{\times x} k[x]/(x^n) \xrightarrow{\times x^{n-1}} k[x]/(x^n) \xrightarrow{\times x} k[x]/(x^n)$$

together with $k[x]/(x^n) \twoheadrightarrow k$ is a projective resolution of k by $k[x]/(x^n)$-modules. We need to compute the homology of $P_\bullet \otimes_{k[x]/(x^n)} k[x]/(x^n)$, i.e. of

$$\cdots \xrightarrow{\times x^{n-1} = 0} k[x]/(x^{n-1}) \xrightarrow{\times x} k[x]/(x^{n-1}) \xrightarrow{\times x^{n-1} = 0} k[x]/(x^{n-1}) \xrightarrow{\times x} k[x]/(x^{n-1}).$$

We find that

$$\begin{aligned} \mathrm{Tor}_i^{k[x]/(x^n)}(k, k[x]/(x^n)) &= \begin{cases} \ker\left(k[x]/(x^{n-1}) \xrightarrow{\times x} k[x]/(x^{n-1})\right) & \text{if } i \text{ is odd} \\ \mathrm{coker}\left(k[x]/(x^{n-1}) \xrightarrow{\times x} k[x]/(x^{n-1})\right) & \text{if } i \text{ is even} \end{cases} \\ &= \begin{cases} k[x]/(x^{n-2}) & \text{if } i \text{ is odd} \\ k & \text{if } i \text{ is even} \end{cases} \end{aligned}$$

Proposition 3.3.4. If P is a projective right R-module, then $\mathrm{Tor}_i^R(P, B) = 0 \; \forall i \geq 1$ and all left R-modules B. If Q is a projective left R-module, then $\mathrm{Ext}_R^i(Q, A) = 0 \; \forall i \geq 1$ and all right R-modules A.

Proof. The 1-term complex P together with the identity map $P \to P$ is a projective resolution of P. $\square$

Proposition 3.3.5.

- A left R-module B is flat iff $\mathrm{Tor}_1^R(A, B) = 0 \; \forall$ right R-modules A (which implies $\mathrm{Tor}_n^R(A, B) = 0 \; \forall n \geq 1$ as well).

- A left R-module B is injective iff $\mathrm{Ext}_R^1(A, B) = 0 \; \forall$ right R-modules A (which implies $\mathrm{Ext}_R^n(A, B) = 0 \; \forall n \geq 1$ as well).

- A right R-module A is projective iff $\mathrm{Ext}_R^1(A, B) = 0 \; \forall$ left R-modules B (which implies $\mathrm{Ext}_R^n(A, B) = 0 \; \forall n \geq 1$ as well).

Proof.

- Recall that by definition, B is flat iff $-\otimes_R B$ preserves ses's, and Tor, as the derived functor of $-\otimes_R B$, measures how far away $-\otimes_R B$ is from being exact.
- We saw B is injective iff $\mathrm{Hom}_R(-, B)$ is exact by 2.3.4.
- This similarly follows from 2.3.4.

□

3.3.2 For abelian groups

Proposition 3.3.6. For any abelian groups A, B, we have $\mathrm{Tor}_i^{\mathbb{Z}}(A, B) = 0\ \forall i \geq 2$ and $\mathrm{Ext}_{\mathbb{Z}}^i(A, B) = 0\ \forall i \geq 2$.

Proof. We know $\exists$ a surjective homomorphism $F \twoheadrightarrow B$ where F is a free abelian group. Let F' be the kernel. Since $\mathbb{Z}$ is a PID and F' is a submodule of F, F' is free. By 2.5.8, $F' \to F$ together with $F \twoheadrightarrow B$ is then a projective resolution of B. It is a 2-term complex, so all left derived functors L_i vanish for $i \geq 2$.

Now by 2.6.1, let I be an injective abelian group such that there is an injection $B \hookrightarrow I$. Then I is divisible by 2.5.9, hence I/B is divisible and injective, so $I \to I/B$ together with $B \hookrightarrow I$ is an injective resolution of B. It is a 2-term complex, so all right derived functors R_i vanish for $i \geq 2$. □

Week 7, lecture 2, 19th February

Example 3.3.7.

1. We already know for any $i \geq 1$, $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}, B) = \mathrm{Tor}_i^{\mathbb{Z}}(A, \mathbb{Z}) = \mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Q}, B) = \mathrm{Tor}_i^{\mathbb{Z}}(A, \mathbb{Q}) = 0$ since $\mathbb{Z}$ is a free $\mathbb{Z}$-module and $\mathbb{Q}$ is flat since it's torsion-free (2.5.11).
2. I claim $\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, A) = A_{\mathrm{tors}}$. Two ways of seeing this:
   (a) (Imagine you know colimits) Consider $\mathbb{Q}/\mathbb{Z}$ as the colimit $\varinjlim_n \mathbb{Z}/n\mathbb{Z}$, then
   $$\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, A) = \varinjlim_n \mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/n, A) = \varinjlim_n A[n] = A_{\mathrm{tors}}.$$
   (b) We first claim that in general $\mathrm{Tor}_1^{\mathbb{Z}}(A, B) = \mathrm{Tor}_1^{\mathbb{Z}}(A, B_{\mathrm{tors}})$. Indeed, consider the ses $0 \to B_{\mathrm{tors}} \to B \to B/B_{\mathrm{tors}} \to 0$ which by 3.2.2 and previous proposition induces the long exact sequence
   $$0 \to \mathrm{Tor}_1^{\mathbb{Z}}(A, B_{\mathrm{tors}}) \to \mathrm{Tor}_1^{\mathbb{Z}}(A, B) \to \mathrm{Tor}_1^{\mathbb{Z}}(A, B/B_{\mathrm{tors}}) \to A \otimes_{\mathbb{Z}} B_{\mathrm{tors}} \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B/B_{\mathrm{tors}} \to 0,$$
   but B/B_{tors} is flat since it's a torsion-free $\mathbb{Z}$-module (2.5.11), hence by 3.3.5 $\mathrm{Tor}_1^{\mathbb{Z}}(A, B/B_{\mathrm{tors}}) = 0$ and so $\mathrm{Tor}_1^{\mathbb{Z}}(A, B_{\mathrm{tors}}) \xrightarrow{\sim} \mathrm{Tor}_1^{\mathbb{Z}}(A, B)$.
   Now consider the ses $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ which induces
   $$\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Q}, A_{\mathrm{tors}}) \to \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, A_{\mathrm{tors}}) \to A_{\mathrm{tors}} \to \mathbb{Q} \otimes_{\mathbb{Z}} A_{\mathrm{tors}},$$
   where $\mathbb{Q}$ is flat so $\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Q}, A_{\mathrm{tors}}) = 0$ and by the same argument in 2.4.3, $\mathbb{Q} \otimes_{\mathbb{Z}} A_{\mathrm{tors}} = 0$, hence $\mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, A_{\mathrm{tors}}) = \mathrm{Tor}_1^{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, A) = A_{\mathrm{tors}}$.

By elementary group theory, if A is a finitely generated abelian group, then $A \cong \mathbb{Z}^n \times F$ for some $n \geq 0$ and F a product of finite cyclic groups. But $\mathrm{Tor}_i^{\mathbb{Z}}(-, B)$ is an additive functor, so we are reduced to computing $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}, B)$, which is 0 by 2.5.8 and 3.3.4, and $\mathrm{Tor}_i^{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, B)$ for various n, which we already did in 3.3.3. Similarly for $\mathrm{Ext}_{\mathbb{Z}}^i$. However, (again imagine you know colimits) we used that Tor and colimits interchange in 2(a) before, which, considering colimits of finitely generated abelian groups, gives us the full picture of $\mathrm{Tor}_i^{\mathbb{Z}}(A, B)$, but the same is not true for $\mathrm{Ext}_{\mathbb{Z}}^i$.

3.3.3 Ext as the group of extensions

Suppose we have a commutative diagram of ses of R-modules

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

If A is an R-module, then we get connecting homomorphisms

$$\partial : \mathrm{Hom}_R(A, N) \to \mathrm{Ext}^1_R(A, L),\ \ \partial' : \mathrm{Hom}_R(A, N') \to \mathrm{Ext}^1_R(A, L')$$

and a commutative square

$$\begin{tikzcd} \mathrm{Hom}_R(A, N) \arrow[r, "\partial"] \arrow[d, "h_*"] & \mathrm{Ext}^1_R(A, L) \arrow[d, "f_*"] \\ \mathrm{Hom}_R(A, N')' \arrow[r, "\partial"] & \mathrm{Ext}^1_R(A, L') \end{tikzcd}$$

Definition 3.3.8. An ses of R-modules $0 \to A \to B \to C \to 0$ is also called an *extension* of C by A.

Definition 3.3.9. We say two extensions of C by A, $0 \to A \to B \to C \to 0$ and $0 \to A \to B' \to C \to 0$, are *equivalent* if there is a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "="] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d, "="] & 0 \\ 0 \arrow[r] & A \arrow[r] & B' \arrow[r] & C \arrow[r] & 0 \end{tikzcd}$$

(then $B \xrightarrow{\sim} B'$).
This is an equivalence relation on the set of extensions of C by A.

Definition 3.3.10. Given two extensions $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ and $0 \to A \xrightarrow{\alpha'} B' \xrightarrow{\beta'} C$, the *Baer sum* is the extension $0 \to A \to X \to C \to 0$ where X is the homology of the complex $A \xrightarrow{(\alpha, -\alpha')} B \oplus B' \xrightarrow{\beta - \beta'} C$.
$A \to X$ is induced by $(\alpha, 0)$ and $X \to C$ is induced by β.

Lemma 3.3.11. The Baer sum turns the set of equivalence classes of extensions of C by A into an abelian group. The zero element is the equivalence class of split extensions, i.e. $0 \to A \to A \oplus C \to C \to 0$. The inverse is ... (left as an exercise)

Week 7, lecture 3, 20th February

Example 3.3.12. Calculate the Baer sum of $0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$ with itself. By definition, this is $0 \to \mathbb{Z} \to X \to \mathbb{Z}/2\mathbb{Z} \to 0$ where X is the homology of $\mathbb{Z} \xrightarrow{(\times 2, \times(-2))} \mathbb{Z} \oplus \mathbb{Z} \xrightarrow{\text{1st pos mod 2 } - \text{ 2nd pos mod 2}} \mathbb{Z}/2\mathbb{Z}$, i.e.

$$X = \frac{\{(x, y) \in \mathbb{Z} \oplus \mathbb{Z} : x - y \equiv 0 \bmod 2\}}{\{(2x, -2x) \in \mathbb{Z} \oplus \mathbb{Z} : x \in \mathbb{Z}\}} = \frac{\langle (1, -1), (2, 0) \rangle}{\langle (2, -2) \rangle} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}.$$

Hence the Baer sum is

$$0 \to \mathbb{Z} \xrightarrow{(0, \times 2)} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z} \xrightarrow{p_1} \mathbb{Z}/2\mathbb{Z} \to 0,$$

the usual split extension.

Definition 3.3.13. The *class* of an extension $0 \to A \to B \to C \to 0$ is the image of $\mathrm{id}_C \in \mathrm{Hom}_R(C, C)$ under $\partial : \mathrm{Hom}_R(C, C) \to \mathrm{Ext}^1_R(C, A)$. As an exercise, show that equivalent extensions have the same class.

Theorem 3.3.14. Now we have a well-defined map

$$\begin{aligned} \{\text{extensions of } C \text{ by } A\}/\text{equivalence} &\to \mathrm{Ext}^1_R(C, A) \\ (0 \to A \to B \to C \to 0) &\mapsto \partial(\mathrm{id}_C) \end{aligned}$$

This is a group isomorphism.

Proof. Let $x \in \mathrm{Ext}^1_R(C, A)$, choose an injection $A \hookrightarrow I$ where I is an injective R-module, and let $M = A/I$. We have the ses $0 \to A \to I \xrightarrow{\mu} M \to 0$, which induces $\mathrm{Hom}_R(C, I) \xrightarrow{\mu_*} \mathrm{Hom}_R(C, M) \to \mathrm{Ext}^1_R(C, A) \to \mathrm{Ext}^1_R(C, I)$, but I is injective, so $\mathrm{Ext}^1_R(C, I) = 0$ by 3.3.5. Let $\phi : C \to M$ be an R-module map such that ϕ is mapped to x, and $X \subset I \oplus C$ given by $\ker(I \oplus C \xrightarrow{\mu - \phi} M)$. Then we have a commutative diagram of ses's

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] & I \arrow[r, "\mu"] & M \arrow[r] & 0 \\ 0 \arrow[r] & A \arrow[r] \arrow[u, equal] & X \arrow[r] \arrow[u] & C \arrow[r] \arrow[u, "\phi"] & 0 \end{tikzcd}$$

and a commutative square

$$\begin{tikzcd}
\mathrm{Hom}_R(C, M) \arrow[r, "\partial'"] & \mathrm{Ext}^1_R(C, A) \\
\mathrm{Hom}_R(C, C) \arrow[r, "\partial"] \arrow[u, "\phi_*"] & \mathrm{Ext}^1_R(C, A) \arrow[u, equal]
\end{tikzcd}$$

So $\partial(\mathrm{id}_C) = (\partial' \circ \phi_*)(\mathrm{id}_C) = \partial'(\phi) = x$. Hence $0 \to A \to X \to C \to 0$ is an extension of C by A whose class is $x \in \mathrm{Ext}^1_R(C, A)$. We've proved surjection.

If $\phi' \in \mathrm{Hom}_R(C, M)$ is another lifting of x, then $\phi' = \phi + \mu\rho$ for some $\rho : C \to I$. The automorphism of $I \otimes C$ via $(a, b) \mapsto (a + \rho(b), b)$ identifies X_ϕ and $X_{\phi'}$. Compatibility can be seen with maps $X \to C$ and $A \to X$; so the extension of C by A constructed from ϕ' is equivalent to the extension constructed from ϕ. We've proved injection.

Week 8, lecture 1, 26th February

Now that we proved the map is bijective, to show it's a group isomorphism, it remains to show that it takes the Baer sum of extensions to the sum of classes.

Suppose $x_1, x_2 \in \mathrm{Ext}^1_R(C, A)$ come from $\phi_1, \phi_2 \in \mathrm{Hom}_R(C, C)$ (i.e. $x_i = \partial(\phi_i)$) and let $0 \to A \to B \to C \to 0$ and $0 \to A \to B' \to C \to 0$ be corresponding extensions. Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] & I \arrow[r, "\mu"] & M \arrow[r] & 0 \\
0 \arrow[r] & A \oplus A \arrow[r] \arrow[u, "(x,y)\mapsto x+y"'] & B \oplus B' \arrow[r] \arrow[u] & C \oplus C \arrow[r] \arrow[u, "(x,y)\mapsto\phi_1(x)+\phi_2(y)"'] & 0
\end{tikzcd}$$

which we claim commutes. Indeed, let $A_0 = \ker(A \oplus A \to A) = \{(x, -x) \in A \oplus A\}$, which is a copy of A, and hence the diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] & I \arrow[r, "\mu"] & M \arrow[r] & 0 \\
0 \arrow[r] & (A \oplus A)/A_0 \arrow[r] \arrow[u, equal] & (B \oplus B')/A_0 = \arrow[r] \arrow[u] & C \oplus C \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

commutes. Now consider $C = \{(x, x) : x \in C\} \subset C \oplus C$ and let X be its preimage in $(B \oplus B')/A_0$. Then we have

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] & I \arrow[r, "\mu"] & M \arrow[r] & 0 \\
0 \arrow[r] & A \arrow[r] \arrow[u, equal] & X \arrow[r] \arrow[u] & C \arrow[r] \arrow[u] & 0
\end{tikzcd}$$

where the bottom row is the Baer sum of the two extension we started off with. Restricting $C \oplus C \to M$ gives the map $\phi_1 + \phi_2 : C \to M$, i.e. the class of the bottom row is $x_1 + x_2 \in \mathrm{Ext}^1_R(C, A)$. $\square$

3.4 Group rings

Let G be a group. The *group ring* (with integer coefficients) $\mathbb{Z}[G]$ of G is a free $\mathbb{Z}$-module with generators $g \in G$, with multiplication given by the condition that on generators g, h, we have $gh \in \mathbb{Z}[G]$ is the generator $gh \in G$, and extended by linearity.

The elements of $\mathbb{Z}[G]$ are written as $\sum_{g \in G} a_g g$ where $a_g \in \mathbb{Z}$. The unit in $\mathbb{Z}[G]$ is $1 := 1e$ where e is the identity of G.

(!) $\mathbb{Z}[G]$ is a ring, but it's only commutative if G is abelian.

The generators of $\mathbb{Z}[G]$ associated to $g \in G$ are called the *canonical generators*.

Example 3.4.1.
1. Let $G = C_n$ be the cyclic group with generator s. Then $\mathbb{Z}[G] = \mathbb{Z} \oplus \mathbb{Z}s \oplus \cdots \oplus \mathbb{Z}s^{n-1}$ with multiplication given by $s \sum_{i=0}^{n-1} a_i s^i = a_{n-1} + \sum_{i=1}^{n-1} a_{i-1} s^i$.
2. Let $G = \mathbb{Z}$ with generator t. Then $\mathbb{Z}[G] = \cdots \oplus \mathbb{Z}t^{-1} \oplus \mathbb{Z} \oplus \mathbb{Z}t \oplus \mathbb{Z}t^2 \oplus \cdots$ with t acting as $t \cdot t^i = t^{i+1}$; hence $\mathbb{Z}[G] = \mathbb{Z}((t))$ (Laurent series ring).

(!) Sometimes people call a $\mathbb{Z}[G]$-module a G-module.

Definition 3.4.2. For a $\mathbb{Z}[G]$-module M, define $M^G = \{m \in M : gm = m \; \forall g \in G\}$.

Definition 3.4.3. A $\mathbb{Z}[G]$-module M is *trivial* if the G-action on M is trivial, i.e. every $g \in G$ acts as the identity. M^G is then the maximal trivial $\mathbb{Z}[G]$-submodule of M, and M is trivial $\iff M = M^G$.

Definition 3.4.4. For a $\mathbb{Z}[G]$-module M, define $M_G = M / \langle m - gm : m \in M, g \in G \rangle$. This is the largest G-invariant quotient module of M.

Week 8, lecture 2, 26th February

Proposition 3.4.5.

1. The kernel I of the map $\sigma : \mathbb{Z}[G] \to \mathbb{Z} : \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g$, which is a 2-sided ideal called the *augmentation ideal*, has a $\mathbb{Z}$-basis $\{1 - g : g \in G \backslash \{e\}\}$. In particular, $\mathbb{Z}[G]_G = \mathbb{Z}[G]/I \cong \mathbb{Z}$.
2. Let G be finite and define $N = \sum_{g \in G} g \in \mathbb{Z}[G]$, the *norm element*. Then N is in the centre of $\mathbb{Z}[G]$ and $\mathbb{Z}[G]^G = \mathbb{Z}N$.
   (!) Note that if G is not finite, say $G = \mathbb{Z}$, then $\mathbb{Z}[\mathbb{Z}]^{\mathbb{Z}} = 0$.

Proof.

1. σ is a $\mathbb{Z}[G]$-module map where $\mathbb{Z}$ is a trivial $\mathbb{Z}[G]$-module, so I is indeed a 2-sided ideal. The part about the basis is clear.
2. Note that $gN = g\left(\sum_{g \in G} g\right) = \sum_{g \in G} g = N$.

$\square$

Definition 3.4.6. For a $\mathbb{Z}[G]$-module M, the nth *group cohomology* of G with M coefficients is $H^n(G, M) = \operatorname{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M)$. Similarly, the nth group homology of G with M coefficients is $H_n(G, M) = \operatorname{Tor}^{\mathbb{Z}[G]}_n(\mathbb{Z}, M)$.

Example 3.4.7.

1. $H^0(G, M) = \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) = M^G$.
2. $H_0(G, M) = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M = M_G$.
3. Cohomology of cyclic groups:
   - let $G = \mathbb{Z}$ with generator t. Then $0 \to \mathbb{Z}[\mathbb{Z}] \xrightarrow{1-t} \mathbb{Z}[\mathbb{Z}]$ together with $\sigma : \mathbb{Z}[\mathbb{Z}] \twoheadrightarrow \mathbb{Z}$ is a projective resolution of $\mathbb{Z}$ by $\mathbb{Z}[\mathbb{Z}]$-modules. So
   $$H_i(\mathbb{Z}, M) = \begin{cases} M_G & \text{if } i = 0 \\ M^G & \text{if } i = 1 \\ 0 & \text{if } i \geq 2 \end{cases}, \qquad \text{and } H^i(\mathbb{Z}, M) = \begin{cases} M^G & \text{if } i = 0 \\ M_G & \text{if } i = 1 \\ 0 & \text{if } i \geq 2 \end{cases}$$
   - now let $G = C_m$ with generator s. Then $\cdots \to \mathbb{Z}[C_m] \xrightarrow{N} \mathbb{Z}[C_m] \xrightarrow{1-s} \mathbb{Z}[C_m]$ where $N = 1 + s + \cdots + s^{m-1}$ together with $\sigma : \mathbb{Z}[C_m] \twoheadrightarrow \mathbb{Z}$ is a projective resolution of $\mathbb{Z}$ by $\mathbb{Z}[C_m]$-modules. So

     Theorem 3.4.8. (a)
     $$H^n(C_m, M) = \begin{cases} M^G & \text{if } n = 0 \\ \dfrac{\ker(M \xrightarrow{N} M)}{(1-s)M} & \text{if } n \geq 1 \text{ is odd} \\ M^G/NM & \text{if } n \geq 2 \text{ is even} \end{cases}$$
     (b)
     $$H_n(C_m, M) = \begin{cases} M_G & \text{if } n = 0 \\ M^G/NM & \text{if } n \geq 1 \text{ is odd} \\ \dfrac{\ker(M \xrightarrow{N} M)}{(1-s)M} & \text{if } n \geq 2 \text{ is even} \end{cases}$$

Week 8, lecture 3, 27th February

Proposition 3.4.9.

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \left\{ (a_1, a_2, \dots) \in \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z} : \forall m : m \mid n,\ a_n \equiv a_m \bmod m \right\}.$$

This is a ring under component-wise addition and multiplication. Denote it by $\widehat{\mathbb{Z}}$. If you know the (now mysterious) mastery material, you can write $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ with respect to the map $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\bmod m} \mathbb{Z}/m\mathbb{Z}$ (note that the condition is equivalent to $a_n \mapsto a_m$ under this map).

Proof. Given $a \in \widehat{\mathbb{Z}}$, define $\phi_a : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ by $\frac{m}{n} \mapsto a_n \frac{m}{n}$. We first show ϕ_a is indeed a group homomorphism. Indeed,

$$\phi_a\left(\frac{m_1}{n_1} + \frac{m_2}{n_2}\right) = \phi_a\left(\frac{n_2 m_1 + n_1 m_2}{m_1 m_2}\right) = a_{n_1 n_2}\frac{n_2 m_1 + n_1 m_2}{m_1 m_2}$$

and

$$\phi_a\left(\frac{m_1}{n_1}\right) + \phi_a\left(\frac{m_2}{n_2}\right) = a_{n_1}\frac{m_1}{n_1} + a_{n_2}\frac{m_2}{n_2} = \frac{a_{n_1} n_2 m_1 + a_{n_2} n_1 m_2}{n_1 n_2},$$

but $a_{n_1 n_2} \equiv a_{n_1} \bmod n_1$ and $\equiv a_{n_2} \bmod n_2$, i.e. $a_{n_1 n_2} = a_{n_1} + s n_1 = a_{n_2} + t n_2$ for some $s, t \in \mathbb{Z}$, hence

$$\begin{aligned} \frac{a_{n_1} n_2 m_1 + a_{n_2} n_1 m_2}{n_1 n_2} &= \frac{(a_{n_1 n_2} - s n_1) n_2 m_1 + (a_{n_1 n_2} - t n_2) n_1 m_2}{n_1 n_2} = a_{n_1 n_2}\frac{n_2 m_1 + n_1 m_2}{m_1 m_2} - \frac{s n_1 n_2 m_1}{n_1 n_2} - \frac{t n_1 n_2 m_2}{n_1 n_2} \\ &= a_{n_1 n_2}\frac{n_2 m_1 + n_1 m_2}{m_1 m_2} - s m_1 - t m_2 = a_{n_1 n_2}\frac{n_2 m_1 + n_1 m_2}{m_1 m_2} \end{aligned}$$

since $s m_1 + t m_2 \in \mathbb{Z}$.

Now clearly $a \mapsto \phi_a$ is by construction a homomorphism. It remains to show it's a bijection. We do this by writing down the inverse. Given $\psi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$, define $a_\psi = \left(\psi(1), 2\psi\left(\frac{1}{2}\right), 3\psi\left(\frac{1}{3}\right), \dots\right) \in \prod_{n=1}^{\infty} \mathbb{Z}/n\mathbb{Z}$. First see that indeed $a_\psi \in \widehat{\mathbb{Z}}$. Indeed, if $m \mid n$, write $n = mx$ for some $x \in \mathbb{Z}$, then

$$a_n - a_m = n\psi\left(\frac{1}{n}\right) - m\psi\left(\frac{1}{m}\right) = mx\psi\left(\frac{1}{mx}\right) - m\psi\left(\frac{1}{m}\right) \equiv 0 \bmod m.$$

The fact that $\psi \mapsto a_\psi$ is a homomorphism follows from that ψ is a homomorphism.

It remains to see the two homomorphisms we defined are inverses:

$$\phi_{a_\psi}\left(\frac{m}{n}\right) = n\psi\left(\frac{1}{n}\right)\frac{m}{n} = m\psi\left(\frac{1}{n}\right) = \psi\left(\frac{m}{n}\right)$$

and

$$a_{\phi_a} = \left(a_1 \cdot 1, 2\left(a_2\frac{1}{2}\right), 3\left(a_3\frac{1}{3}\right), \dots\right) = (a_1, a_2, a_3, \dots) = a.$$

□

Again if you know the mastery material, $\mathrm{Hom}_{\mathbb{Z}}\left(\varinjlim A_i, B\right) \cong \varprojlim \mathrm{Hom}_{\mathbb{Z}}(A_i, B)$. Also, we worked out in coursework 1 that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$. Combining these two facts we easily have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}\left(\varinjlim \mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z}\right) = \varprojlim \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$.

How is this useful? Consider the ses $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ which by $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ induces the long $0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to \cdots$, where we just calculated $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = \widehat{\mathbb{Z}}$, and by 3.3.5 and 2.5.9 $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = 0$, and since a $\mathbb{Z}$-homomorphism $\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ is given by its image of 1, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$. Hence we have an ses $0 \to \widehat{\mathbb{Z}} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z} \to 0$. Consider $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}/\mathbb{Z})$ as a $\mathbb{Q}$-vector space. Then one has $\mathrm{Tor}^{\mathbb{Z}}_1(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}) \to \widehat{\mathbb{Z}} \otimes \mathbb{Q} \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z} \otimes \mathbb{Q}$, but $\mathrm{Tor}^{\mathbb{Z}}_1(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}) = 0$ by 3.3.5 and 2.5.11, and any tensor product with a torsion is 0, hence $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Q}/\mathbb{Z}) \cong \widehat{\mathbb{Z}} \otimes \mathbb{Q} = \mathbb{A}_{\mathbb{Q}}$ (the ring of adèles of $\mathbb{Q}$).

Week 9, lecture 1, 5th March

3.5 Standard resolution

Let $P_n = \mathbb{Z}[G^{n+1}]$ with canonical generators $(g_0, \dots, g_n)$ where $g_i \in G$. Make P_n a $\mathbb{Z}[G]$-module via $g(g_0, \dots, g_n) = (gg_0, \dots, gg_n)$.

Lemma 3.5.1. For $n \geq 1$, P_n is a free $\mathbb{Z}[G]$-module, and $P_n = \mathbb{Z}[G] \otimes_{\mathbb{Z}} Q_n$ where Q_n is the free abelian group generated by $(e, a_1, a_1a_2, \dots, a_1a_2\cdots a_n)$ for every $(a_1, \dots, a_n) \in G^n$.

Proof. For each $a = (a_1, \dots, a_n) \in G^n$ define $P_n(a)$ as the $\mathbb{Z}[G]$-submodule of P_n generated as an abelian group by $(g, ga_1, ga_1a_2, \dots, ga_1a_2\cdots a_n)$ $\forall g \in G$. So

$$P_n(a) = \bigoplus_{g\in G} \mathbb{Z}(g, ga_1, \dots, ga_1\cdots a_n) = \mathbb{Z}[G](e, a_1, \dots, a_1\cdots a_n),$$

i.e. $P_n(a) \cong \mathbb{Z}[G]$. By definition of P_n,

$$P_n = \bigoplus_{a\in G} P_n(a) \cong \bigoplus_{a\in G} \mathbb{Z}[G],$$

so P_n is a free $\mathbb{Z}[G]$-module and $P_n \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} Q_n$. $\square$

Define $d : P_n \to P_{n-1}$ by

$$(g_0, \dots, g_n) \mapsto \sum_{i=0}^{n} (-1)^i (g_0, \dots, g_{i-1}, g_{i+1}, \dots, g_n).$$

Lemma 3.5.2. $\cdots \to \mathbb{Z}[G^3] \xrightarrow{d} \mathbb{Z}[G^2] \xrightarrow{d} \mathbb{Z}[G] \xrightarrow{\sigma} \mathbb{Z} \to 0$ is an exact complex, i.e. $P_\bullet$ together with $\sigma : \mathbb{Z}[G] \to \mathbb{Z}$ is a projective resolution of $\mathbb{Z}$ by $\mathbb{Z}[G]$-modules.

Proof. It's easy to check $d^2 = 0$, so $P_\bullet$ is a complex. To prove exactness, it suffices to show id : $P_\bullet \to P_\bullet$ is chain homotopic to the zero map. We construct maps $s_n : P_n \to P_{n+1}$ such that id $= s_{n-1}d + ds_n$ $\forall n > 1$. Fix $h \in G$ and let $s_n : (g_0, \dots, g_n) \mapsto (h, g_0, \dots, g_n)$. $\square$

Remark 3.5.3.

1. When we defined chain homotopies for complex of R-modules (3.1.10), we said that s_n's are R-module homomorphism. Here we have a complex of $\mathbb{Z}[G]$-modules, but the s_n's are only $\mathbb{Z}$-module homomorphisms. But this is okay because for any ring R, the forgetful functor R-Mod $\to$ AbGrp is exact and faithful.

2. If G is a finite group, define $S_n : (g_0, \dots, g_n) \mapsto \sum_{h\in G}(h, g_0, \dots, g_n)$ which *is* a $\mathbb{Z}[G]$-module map and we have $S_{n-1}d + dS_n = \sum_{h\in G}$ id = multiplication by m where $m = |G|$, i.e. multiplication by m is chain homotopic to the zero map, i.e. $\times m$ kills $H^n(G, \mathbb{Z})$ for all $n \geq 1$.

We now want to calculate $H^1(G, M)$ and $H^2(G, M)$ for a general G (we've seen that $H^0(G, M) = M^G$ and $H^i(G, M)$ for cyclic G in 3.4.7). Let R be a ring and A an abelian group. Consider R as a left R-module. For any left R-module M, we have $\mathrm{Hom}_R(R \otimes_{\mathbb{Z}} A, M) = \mathrm{Hom}_{\mathbb{Z}}(A, M)$. Indeed, an R-module map $R \otimes_{\mathbb{Z}} A \to M$ is uniquely determined by its values on $1 \otimes a$ for $a \in A$. Conversely, if $f : A \to M$ is a group homomorphism, then we get an R-module map $R \otimes_{\mathbb{Z}} A \to M : r \otimes a \mapsto rf(a)$. So in particular,

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P_n, M) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G] \otimes_Z Q_n, M) = \mathrm{Hom}_{\mathbb{Z}}(Q_n, M).$$

Now $P_\bullet$ with $\mathbb{Z}[G] \xrightarrow{\sigma} \mathbb{Z}$ is a projective resolution of $\mathbb{Z}$, so $H^n(G, M)$ is computed by cohomology of

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, M) \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_2, M) \to \cdots,$$

which is the same as

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(Q_0, M) \to \mathrm{Hom}_{\mathbb{Z}}(Q_1, M) \to \mathrm{Hom}_{\mathbb{Z}}(Q_2, M) \to \cdots$$

by calculation above. Now $Q_0 = \mathbb{Z}$ so $\mathrm{Hom}_{\mathbb{Z}}(Q_0, M) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M) = M$.

Week 9, lecture 2, 5th March

A homomorphism $Q_n \to M$ is uniquely determined by its values on the generators $(e, g_1, \cdots, g_1 \cdots g_n)$ for $g_i \in G$, i.e.

$$\mathrm{Hom}_{\mathbb{Z}}(Q_n, M) = \{f : G^n \to M\} := \mathrm{Fun}(G^n, M)$$

via

$$((e, g_1, \ldots, g_1 \cdots g_n) \mapsto f(g_1, \ldots, g_n)) \quad \leftarrow\!\shortmid \quad f,$$

so $H^n(G, M)$ is the cohomology of

$$0 \to M \xrightarrow{d} \mathrm{Fun}(G, M) \xrightarrow{d} \cdots \xrightarrow{d} \mathrm{Fun}(G^n, M) \to \cdots$$

Now it remains understand the differential d.

Lemma 3.5.4. $d : \mathrm{Fun}(G^n, m) \to \mathrm{Fun}(G^{n+1}, M)$ sends $f : G^n \to M$ to $df : G^{n+1} \to M$ whose value on $(g_1, \ldots, g_{n+1})$ is as follows:

- $n = 0$: d sends an element m of $M = \mathrm{Fun}(G^0, M)$ to the map $dm : G \to M : g \mapsto gm - m$.
- $n = 1$: $df : G^2 \to M : (g_1, g_2) \mapsto g_1 f(g_2) - f(g_1 g_2) + f(g_1)$.
- $n = 2$: $df : G^3 \to M : (g_1, g_2, g_3) \mapsto g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2)$,
- In general:

$$\begin{aligned} df : (g_1, \ldots, g_{n+1}) \mapsto g_1 f(g_2, \ldots, g_{n+1}) - f(g_1 g_2, g_3, \ldots, g_{n+1}) + f(g_1, g_2 g_3, g_4, \ldots, g_{n+1}) - \cdots \\ + (-1)^n f(g_1, g_2, \ldots, g_n g_{n+1}) + (-1)^{n+1} f(g_1, \ldots, g_n) \end{aligned}$$

Theorem 3.5.5. 1. $H^0(G, M) = \ker(m \mapsto (g \mapsto gm - m)) = \{m \in M : gm = m \ \forall g \in G\} = M^G$ as seen.

2.
$$H^1(G, M) = \frac{\{f : G \to M : g_1 f(g_2) - f(g_1 g_2) + f(g_1) = 0 \ \forall g_1, g_2 \in G\}}{\{gm - m : m \in M, g \in G\}} = \frac{\text{1-cocycles}}{\text{trivial 1-cocycles}}$$

3.
$$\begin{aligned} H^2(G, M) &= \frac{\{f : G^2 \to M : g_1 f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0 \ \forall g_1, g_2, g_3 \in G\}}{\{g_1 f(g_2) - f(g_1 g_2) + f(g_1) : f : G \to M, g_1, g_2 \in G\}} \\ &= \frac{\text{2-cocycles}}{\text{trivial 2-cocycles}} \end{aligned}$$

Remark 3.5.6. • Note that $f : G \to M$ is a 1-cocycle if $f(g_1 g_2) = f(g_1) + \underline{g_1} f(g_2) \ \forall g_1, g_2 \in G$. If we covered the underlined g_1 then this looks like definition of homomorphism. So such f is also called *crossed homomorphism* in other places.

- 2-cocycles are sometimes called *factor sets* (?!).
- If M is a trivial $\mathbb{Z}[G]$-module then 1-cocycles are indeed precisely group homomorphisms, and hence $H^1(G, M) = \frac{\mathrm{Hom}_{\mathrm{Grp}}(G,M)}{0} = \mathrm{Hom}_{\mathrm{Grp}}(G, M)$. For example, if G is finite then $H^1(G, \mathbb{Z}) = 0$.

3.6 Inflation-restriction sequence

Given a group homomorphism $f : H \to G$, a $\mathbb{Z}[G]$-module M is a $\mathbb{Z}[H]$-module via f. Functoriality gives a group homomorphism $\mathrm{Res} = \mathrm{Res}_H^G : H^n(G, M) \to H^n(H, M)$.

For example, if $H \leq G$, then $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module (verify), so a free $\mathbb{Z}[G]$-module gives a free $\mathbb{Z}[H]$-module, hence $P_\bullet$ (the standard resolution) is also a free resolution on $\mathbb{Z}$ as $\mathbb{Z}[H]$-modules. So $H^n(H, M)$ is computed using $\mathrm{Hom}_{\mathbb{Z}[H]}(P_\bullet, M)$. In this case, the restriction map Res_H^G is the map induced by $\mathrm{Hom}_{\mathbb{Z}[G]}(P_\bullet, M) \to \mathrm{Hom}_{\mathbb{Z}[H]}(P_\bullet, M)$. If further $H \trianglelefteq G$, then if M is a $\mathbb{Z}[G]$-module, then M^H is a $\mathbb{Z}[G/H]$-module (verify).

Definition 3.6.1. Let $H \trianglelefteq G$, the inflation map is

$$\mathrm{Inf} = \mathrm{Inf}_H^G : H^n(G/H, M^H) \xrightarrow{\text{induced by } G \to G/H} H^n(G, M^H) \xrightarrow{\text{induced by } M^H \hookrightarrow M} H^n(G, M).$$

Week 9, lecture 3, 6th March

On H^1, inf on 1-cocycles goes as follows. Let $\varphi : G/H \to M^H$. We get a function $\varphi' : G \twoheadrightarrow G/H \xrightarrow{\varphi} M^H \hookrightarrow M$. It satisfies the cocycle condition, so is a 1-cocycle for G, and $\inf(\varphi) = \varphi' \in H^1(G, M)$.

Lemma 3.6.2 (Shapiro's)**.** Let $H \le G$ and M be a $\mathbb{Z}[H]$-module. Define

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} M = \mathrm{Ind}_H^G(M) \qquad \text{and} \qquad \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], M) = \mathrm{CoInd}_H^G(M).$$

(Verify that if $[G : H] < \infty$ then $\mathrm{Ind}_H^G(M) = \mathrm{CoInd}_H^G(M)$.)
Then

$$H_*\left(G, \mathrm{Ind}_H^G(M)\right) \cong H_*(H, M) \qquad \text{and} \qquad H^*\left(G, \mathrm{CoInd}_H^G(M)\right) \cong H^*(H, M)$$

Proof. Let $P_\bullet$ be a projective resolution of $\mathbb{Z}$ by $\mathbb{Z}[G]$-modules. Then

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P_n, \mathrm{CoInd}_H^G(M)) = \mathrm{Hom}_{\mathbb{Z}[G]}(P_n, \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], M)) \cong \mathrm{Hom}_{\mathbb{Z}[H]}(P_n, M).$$

□

So (let M be a $\mathbb{Z}[G]$-module) we have a commutative diagram

$$\begin{tikzcd} H^n(G, M) \arrow[r, "\mathrm{Res}"] \arrow[d] & H^n(H, M) \\ H^n\left(G, \mathrm{Ind}_H^G(M)\right) \arrow[ur, "\mathrm{Shapiro}"'] & \end{tikzcd}$$

Theorem 3.6.3 (Main theorem of inflation-restriction)**.** Let $H \trianglelefteq G$, then

$$0 \to H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M)$$

is an exact sequence.

Example 3.6.4. Let D_{2n} be the dihedral group of size $2n$. The cyclic group C_n (rotations) is a normal subgroup, with quotient C_2 (reflection). Consider the exact sequence

$$0 \to C_n \to D_{2n} \to C_2 \to 0.$$

Let M be a trivial $\mathbb{Z}[D_{2n}]$-module. Then the inflation-restriction sequence gives

$$0 \to H^1(C_2, M) \xrightarrow{\mathrm{Inf}} H^1(D_{2n}, M) \xrightarrow{\mathrm{Res}} H^1(C_n, M)$$

and as calculated in 3.4.7, we have $H^1(C_2, M) = M^{C_2} = \{m \in M : gm = m \ \forall g \in C_2\} = M[2]$ and similarly $H^1(C_n, M) = M[n]$. Then for example if M is torsion-free, e.g. $\mathbb{Z}$, then these are 0 and so $H^1(D_{2n}, M) = 0$.

Proof of 3.6.3. We first prove Inf is injective. Let $c : G/H \to M^H$ be a 1-cocycle such that $c : G \to M$ is a trivial 1-cocycle. (...exercise)

Now we show $\mathrm{im}\,\mathrm{Inf} = \ker \mathrm{Res}$. Let $c : G \to M$ be a 1-cocycle such that $\exists m \in M : c(h) = hm - m \ \forall h \in H$. Then $c' : G \to M : g \mapsto c(g) - (gm - m)$ is a 1-cocycle which differs from c by a trivial 1-cocycle, i.e. its class in $H^1(G, M)$ is the same as c. Now $c'(h) = c(h) - (hm - m) = 0 \ \forall h \in H$, so $c'(gh) = gc'(h) + c'(g) = c'(g) \forall g, h \in H$, i.e. c' is a well-define function $G/H \to M$. But $gH = Hg$ since H is normal, so $\forall h \in H, g \in G$, $c'(g) = c'(hg) = hc'(g) + c'(h) = hc'(g)$, i.e. $c' : G/H \to M^H$, so $c' \in H^1(G/H, M^H)$. □

Week 10, lecture 1, 12th March

3.7 Application to group theory

Let G, H be groups. **The question**: can one classify all groups E such that H is a normal subgroup of E and $E/H = G$? That is, can we classify all short exact sequences of the form $0 \to H \to E \to G \to 1$? So far we've only done ses's of abelian categories, but Grp isn't one.

Definition 3.7.1. An ses of the above form is called a *(group) extension* of G by H. We say two extensions of G by H are *equivalent* if $\exists$ a group homomorphism $\varphi : E \to E'$ such that the diagram

$$\begin{tikzcd} 0 \arrow[r] & H \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d, "\varphi"] & G \arrow[r] \arrow[d, equal] & 1 \\ 0 \arrow[r] & H \arrow[r] & E' \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

commutes. (Verify that this condition actually forces φ into an isomorphism).

In such a situation, E acts on H by conjugation. If H is abelian, this action is trivial, so get a well-defined action of $E/H \cong G$ on H. Indeed, define this action via $(g, h) \mapsto \widehat{g}h\widehat{g}^{-1}$ where $\widehat{g} \in E$ is such that $\widehat{g} \equiv g \bmod h$. Then H is a $\mathbb{Z}[G]$-module. Verify that equivalent extensions induce the same $\mathbb{Z}[G]$-structure on H.

We now focus on **the sub-question** where H is abelian: let G be a group and A a $\mathbb{Z}[G]$-module. Can we classify all groups E containing A as a normal subgroup such that the $\mathbb{Z}[G]$-module structure on A is the same as the G-action induced by conjugation by E? i.e. Can we classify all extensions of the form $0 \to A \to E \to G \to 1$ up to equivalence?

It's a priori an unsatisfying focus from general subgroups to abelian ones. But we will see that an answer to this sub-question is quite often enough to bootstrap up to one to the question we started with.

In analogy to the case of R-modules, we can imagine that there is a distinguished class of "trivial" extensions which we might call "split". (!) It is not enough to just consider $A \times G$ as the split ones. Indeed, the elements of A and G commute in $A \times G$, so the $\mathbb{Z}[G]$-module structure on A given by conjugation is trivial. This is where semidirect products arise (from a stronger motivation then in the usual introduction to group theory).

Definition 3.7.2. Let G be a group and A a $\mathbb{Z}[G]$-module. The *semidirect product* $A \rtimes G$ is defined as the set $A \times G$ with binary operation $(a, g) \cdot (b, h) = (a + gb, gh)$. In particular, if A is a trivial $\mathbb{Z}[G]$-module, then $A \rtimes G = A \times G$.

Exercise 3.7.3. Verify that: this satisfies the group axioms with the unit $(0, e)$ and inverse of (a, g) being $\left(-g^{-1}a, g^{-1}\right)$; and $A \cong A \times \{e\} \subset A \rtimes G$ is a normal subgroup and the action of G on A by conjugations in $A \times G$ coincides with the G-action on A that we were given.

Definition 3.7.4. An extension $0 \to A \xrightarrow{\alpha} E \xrightarrow{\beta} G \to 1$ is *split* if β has a section, i.e. a group homomorphism $\sigma : G \to E : \beta \circ \sigma = \mathrm{id}_G$.

Proposition 3.7.5. An extension $0 \to A \xrightarrow{\alpha} E \xrightarrow{\beta} G \to 1$ is split $\iff$ it is equivalent to $0 \to A \hookrightarrow A \rtimes G \to G \to 1$ for some $\mathbb{Z}[G]$-module structure on A.

Proof.

- $\Longleftarrow$: Let $\sigma : g \mapsto (0, g)$.
- $\Longrightarrow$: Let

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\alpha"] & E \arrow[r, shift left, "\beta"] & G \arrow[l, bend left, "\sigma"] \arrow[r] & 1 \end{tikzcd}$$

be a split extension. Then E contains $A \cong \alpha(A)$ and $\delta(G)$ as subgroups. Any $x \in E$ can be written uniquely as $(\alpha(y), \beta(x))$ where $y \in A$ is the unique element such that $x\sigma(\beta(x))^{-1} = \alpha(y)$. The map $E \to A \times G : x \mapsto (y, \beta(x))$ is then a bijection. Verify that this bijection sends group law on E to group law on $A \rtimes G$.

$\square$

Week 10, lecture 2, 12th March

Example 3.7.6.

1. Let k be a field. Then we have $0 \to \mathrm{SL}_n(k) \to \mathrm{GL}_n(k) \xrightarrow{\det} k^* \to 1$, which is split by $\sigma : k^* \to \mathrm{GL}_n(k) : a \mapsto \begin{pmatrix} a & 0 \\ 0 & I_{n-1} \end{pmatrix}$. In other words, $\mathrm{GL}_n(k) = \mathrm{SL}_n(k) \rtimes k^\times$.
2. Let $A = \mathbb{Z}/n\mathbb{Z}$ and $G = C_2$. If the generator of C_2 acts on A as -1, then $A \rtimes G = D_{2n}$.
3. Let Q_8 be the group of invertible elements of the ring of integers of quaternions $R = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}ij$ where $i^2 = j^2 = -1$ and $ij = -ji$. We have $Q_8 = \{\pm 1, \pm i, \pm j, \pm ij\}$. The subgroup $\{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}$ is normal, so we have $0 \to \mathbb{Z}/4\mathbb{Z} \xrightarrow{\alpha} Q_8 \xrightarrow{\beta} C_2 \to 1$. It's not a split extension (the only element of order 2 in $\mathbb{Q}_8$ is $-1 \in \mathbb{Z}/4\mathbb{Z}$, so β cannot have an section).

Theorem 3.7.7. Let G be a group and A a $\mathbb{Z}[G]$-module. The set of equivalence classes of extensions of the form $0 \to A \xrightarrow{\alpha} E \xrightarrow{\beta} G \to 1$ such that the induced action of G on A is the same as that the given $\mathbb{Z}[G]$-module structure is in bijection with $H^2(G, A)$. The class of split extensions corresponds to $0 \in H^2(G, A)$ under this bijection.

Proof. Let's first map an extension to a 2-cocycle. $\beta(E) = G$, so there is a set-theoretic map $s : G \to E$ such that $\beta \circ s = \mathrm{id}_G$. For any $g, h \in G$, we have $s(g)s(h)s(gh)^{-1} \in \ker\beta = \operatorname{im}\alpha$. Let $\phi(g, h) \in A$ be the unique (since α is injective) element such that $\alpha(\phi(g, h)) = s(g)s(h)s(gh)^{-1}$. Notice that $\phi(g, e) = \phi(e, g) = 0\ \forall g \in G$. We claim that $\phi : G^2 \to A$ is a 2-cocycle, i.e. $\forall f, g, h \in G$, we have $f\phi(g, h) + \phi(f, gh) = \phi(h, g) = \phi(fg, h)$ (verifying this is left as an exercise). Also, we claim that two extensions with the same 2-cocycle are equivalent. Indeed, we have a bijection $E \to A \times G : x \mapsto (y, \beta(x))$ where y is the unique element such that $\alpha(y) = x(s(\beta(x)))^{-1}$. Under this bijection, the group law on E gives the group law on $A \times G$ given by

$$(a, g) \cdot (b, h) = (a + gb + \phi(g, h), gh), \tag{$*$}$$

which is evidently determined by ϕ. Conversely, if we have a 2-cocycle $\phi : G^2 \to A$, then $(*)$ defines a group structure E on $A \times G$. It remains to check that if $\phi, \psi : G^2 \to A$ are two 2-cocyles then $E = E_\phi$ and $E' = E_\psi$ are equivalent if $\phi - \psi$ is a trivial 2-cocycle, i.e.

$$\phi(g, h) - \psi(g, h) = g(c(h)) - c(gh) + c(g) \tag{$**$}$$

for some function $c : G \to A$. Indeed, an equivalence of E and E' is precisely an isomorphism $\mu : E \xrightarrow{\sim} E'$ such that $\beta = \beta'\mu$. So μs is a (set-theoretic) section of β'. Any two set-theoretic sections of β' differ by a map $c : G \to A$, so the isomorphism $\mu : E \xrightarrow{\sim} E'$ maps $(a, g) \mapsto (a + c(g), g)$, transforming $(*)$ for ϕ into $(*)$ for ψ. We have

$$a + g(b) + \phi(g, h) + c(gh) = a + c(g) + g(b) + g(c(h)) + \psi(g, h)$$

which shows that a set-theoretic μ is a group homomorphism (hence a group isomorphism) precisely when $(**)$ holds. $\square$

Week 10, lecture 3, 13th March

Theorem 3.7.8 (Schur–Zassenhaus)**.** Let E be a finite group of order mn where $(m, n) = 1$. If H is a normal subgroup of E of order n, then $E \cong H \rtimes E/H$.

Remark 3.7.9.

1. The theorem doesn't really determine E uniquely. e.g. if $H = C_3$ and $E/H = C_2$, then $E \cong C_3 \rtimes C_2$ but there are two such groups, C_6 and $D_6 \cong S_3$, depending on which C_2 action on C_3 one chooses.
2. The theorem says if an extension $0 \to H \to E \to G \to 1$ of a group G of order m by a group H of order n with $(m, n) = 1$, then it's split.
3. The coprime condition is necessary. Indeed, $0 \to C_2 \to C_4 \to C_2 \to 0$ is not split.

Lemma 3.7.10 (Frattini's argument)**.** Let G be a finite group with H a normal subgroup. If S is a p-Sylow subgroup of H, then $G = N_G(S)H$.

Proof. Let $g \in G$. We want to write g as $g = nh$ where $n \in N_G(S)$ and $h \in H$. Consider $g^{-1}Sg$ which, since H is normal, is a subgroup of H, and $|g^{-1}Sg| = |S|$, so also a p-Sylow subgroup of H. Recall that all p-Sylow subgroups of H are conjugate to one another, i.e. $\exists h \in H : g^{-1}Sg = h^{-1}Sh$, so $S = gh^{-1}Shg^{-1}$, i.e. $gh^{-1} \in N_G(S)$. $\square$

Proof of 3.7.8. Let $G = E/H$. It suffices to show that E contains a subgroup of order m. Indeed, that subgroup will be isomorphic to G under $E \twoheadrightarrow G$. (If G' is a subgroup of E of order m, then $G' \cap H$ is trivial by Lagrange and $(n, m) = 1$.) We prove this statement by induction on n. If $n = 1$ then clearly E itself is a subgroup of order $m = mn$, so suppose $|H| = n > 1$ and the statement is true for all normal subgroups of order $< n$. The proof is in 4 steps.

1. WLOG, H is a minimal normal subgroup. Indeed, suppose H is not a minimal normal subgroup, i.e. $\exists$ another normal subgroup $1 \neq H_0 \trianglelefteq E$ with $H_0 \subsetneqq H$. Consider $H/H_0 \trianglelefteq E/H_0$. Then $|H/H_0| \mid |H| = n$, so $|H/H_0|$ and $|E/H| = m$ are coprime, so by inductive hypothesis $\exists$ a subgroup $\overline{H} \leq E/H_0 : |\overline{H}| = m$. Let $\widehat{H} \leq E$ with $\widehat{H}/H_0 = \overline{H}$, then $|\widehat{H}/H_0| = |\overline{H}| = m$, and $|H_0| \mid |H| = n$, so $|H_0|$ and $|\widehat{H}/H_0|$ are coprime, so again by inductive hypothesis $\exists H' \leq \widehat{H}$ such that $|H'| = |\widehat{H}/H_0| = m$.

2. WLOG, H is a p-group. Indeed, suppose H is not a p-group; let S be a p-Sylow subgroup of H. By Frattini's argument, write $E = N_E(S)H$, so $E/H = N_E(S)/(H \cap N_E(S))$. Since $|H \cap N_E(S)| \mid |H| = n$, and $|N_E(S)/(H \cap N_E(S))| = |E/H| = m$, we have $|N_E(S)/(H \cap N_E(S))|$ and $|H \cap N_E(S)|$ are coprime. Since $S \subsetneqq H$ and H is a minimal normal subgroup of E, we must have S is not a normal subgroup of E. In particular $S \neq N_E(S)$. We have $|N_E(S)| < |E|$. By the inductive hypothesis, $\exists H' \leq N_E(S) : |H'| = |N_E(S)/(H \cap N_E(S))| = |E/H| = m$.

3. Minimal normal subgroups H which are p-groups are abelian. Indeed, recall from group theory: it follows from orbit–stabiliser theorem that since H is a p-group, $Z(H)$ is nontrivial. Clearly $Z(H) \trianglelefteq E$. But H is minimal, so we must have $H = Z(H)$, i.e. H is abelian.

4. We have seen that extensions of the form $0 \to H \to E \to G \to 1$ are classified by $H^2(G, H)$. But we've seen in 3.4.7 that this is 0, so all these extensions are split.

□

Week 11, lecture 1, 19th March

3.8 Lyndon–Hochschild–Serre spectral sequence

By 3.6.3, if we have $H \trianglelefteq G$ and M a $\mathbb{Z}[G]$-module, then we have the exact sequence

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G, M) \xrightarrow{\text{Res}} H^1(G/H, M)^{G/H} \longrightarrow H^2(G/H, M^H) \xrightarrow{\text{Inf}} H^2(G, M).$$

But it doesn't go on. What about higher degrees?

Definition 3.8.1. A *double (cochain) complex* $(A^{\bullet,\bullet}, d', d'')$ is a commutative diagram

$$\begin{tikzcd}
 & \vdots & \vdots & \vdots & \\
\cdots \arrow[r, "d'"] & A^{i-1,j+1} \arrow[r, "d'"] \arrow[u, "d''"] & A^{i,j+1} \arrow[r, "d'"] \arrow[u, "d''"] & A^{i+1,j+1} \arrow[r, "d'"] \arrow[u, "d''"] & \cdots \\
\cdots \arrow[r, "d'"] & A^{i-1,j} \arrow[r, "d'"] \arrow[u, "d''"] & A^{i,j} \arrow[r, "d'"] \arrow[u, "d''"] & A^{i+1,j} \arrow[r, "d'"] \arrow[u, "d''"] & \cdots \\
\cdots \arrow[r, "d'"] & A^{i-1,j-1} \arrow[r, "d'"] \arrow[u, "d''"] & A^{i,j+1} \arrow[r, "d'"] \arrow[u, "d''"] & A^{i+1,j+1} \arrow[r, "d'"] \arrow[u, "d''"] & \cdots \\
 & \vdots \arrow[u, "d''"] & \vdots \arrow[u, "d''"] & \vdots \arrow[u, "d''"] &
\end{tikzcd}$$

where each row and column is a complex.

Definition 3.8.2. Let $(A^{\bullet,\bullet}, d', d'')$ be a double complex. The *total complex* is the complex $\operatorname{Tot} A^{\bullet,\bullet} = A^\bullet$ given by

$$A^n = \bigoplus_{i+j=n} A^{i,j}$$

with $d : A^n \to A^{n+1}$ given by

$$d = \sum_{i+j=n} d'^{i,j} + (-1)^n d''^{i,j}.$$

Example 3.8.3. Let G be a group, $H \trianglelefteq G$, $P^\bullet$ a projective resolution of the trivial $\mathbb{Z}[G]$-module $\mathbb{Z}$. We've seen that then $P^\bullet$ is also a projective resolution of $\mathbb{Z}$ by $\mathbb{Z}[H]$-modules. Let $Q^\bullet$ be a projective resolution of $\mathbb{Z}$ by $\mathbb{Z}[G/H]$-modules. Let M be a $\mathbb{Z}[G]$-module. Then G acts on $\operatorname{Hom}_{\mathbb{Z}[H]}(P^\bullet, M)$ by $gf(x) = g(f(g^{-1}x))$. Since H acts trivially, we consider $\operatorname{Hom}_{\mathbb{Z}[H]}(P^\bullet, M)$ as an $\mathbb{Z}[G/H]$-module. We get a double complex

$$A^{\bullet,\bullet} = \operatorname{Hom}_{\mathbb{Z}[G/H]}\left(Q^\bullet, \operatorname{Hom}_{\mathbb{Z}[H]}(P^\bullet, M)\right) \text{ with } d' = \operatorname{Hom}_{\mathbb{Z}[G/H]}(d_Q, \text{id}),\ d'' = \operatorname{Hom}_{\mathbb{Z}[G/H]}(\text{id}, d_P^*).$$

Note that $A^{i,j} = 0$ whenever i or j is negative (in this case we say it's "first quadrant"). In particular, $\operatorname{Tot} A^{\bullet,\bullet}$ is concentrated in nonnegative degrees.

Given a double complex $A^{\bullet,\bullet}$, we get a sequence of double complexes $F^i A^{\bullet,\bullet}$ given by setting all columns to the left of the ith column in $A^{\bullet,\bullet}$ to be 0. Taking total complexes gives a sequence of (sub)complexes $F^i A^\bullet := \operatorname{Tot} F^i A^{\bullet,\bullet}$, i.e.

$$F^i A^n = \bigoplus_{\substack{i'+j=n \\ i' \geq i}} A^{i',j}.$$

This sequence is sometimes called a *filtration*. e.g. $F^0 A^\bullet = A^\bullet$, $F^i A^\bullet = 0$ whenever $i > n$.

Proposition 3.8.4. Let $A^{\bullet,\bullet}$ be a first quadrant double complex. Then $\exists$ objects $E_r^{i,j}$ for $i, j, r \geq 0$ such that the following holds:

1. We have $E_0^{i,j} = A^{i,j}$ $\forall i, j$.
2. For each r, $\exists$ maps $d_r^{i,j} : E_r^{i,j} \to E_r^{i+r,j+1-r}$ such that

$$\cdots \longrightarrow E_r^{i-r,j-1+r} \xrightarrow{d_r^{i-r,j-1+r}} E_r^{i,j} \xrightarrow{d_r^{i,j}} E_r^{i+r,j+1-r} \xrightarrow{d_r^{i+r,j+1-r}} E_r^{i+2r,j+2-2r} \longrightarrow \cdots$$

   is a complex.
3. Each $E_{r+1}^{i,j}$ is H^i of the above complex.
4. For $r = 0$, $d_0^{i,j} = (-1)^i d''^{i,j}$.
5. For $r = 1$, $d_1^{i,j}$ is the map induced by $d'^{i,j}$.
6. The terms $E_r^{i,j}$ stabilise for $r \gg 0$. We call the stabilisation $E_\infty^{i,j}$.
7. There is a filtration of $H^n(\operatorname{Tot} A^{\bullet,\bullet})$ whose successive quotients are the $E_\infty^{i,j}$ for $i + j = n$. We say that spectral sequence *converges* to $H^*(\operatorname{Tot} A^{\bullet,\bullet})$.

The objects $E_r^{i,j}$ for a fixed r forms what's called the *E_r-page*.

Proof. For the full proof, see Stacks project, 012K. The gist is: let $A^\bullet = \operatorname{Tot} A^{\bullet,\bullet}$ with filtration $F^i A^\bullet$ as above. Define

$$Z_r^{i,j} = \frac{F^i A^{i+j} \cap d^{-1}\left(F^{i+r} A^{i+j+1}\right) + F^{i+1,i+j}}{F^{i+1} A^{i+j}}$$

and

$$B_r^{i,j} = \frac{F^i A^{i+j} \cap d\left(F^{i-r+1} A^{i+j-1}\right) + F^{i+1,i+j}}{F^{i+1} A^{i+j}}.$$

Then $E_r^{i,j} = Z_r^{i,j} / B_r^{i,j}$ and $d_r^{i,j}$ is $z + F^{i+1} A^{i+j} \mapsto dz + F^{i+r+1} A^{i+j+1}$. $\square$

Week 11, lecture 2, 19th March

The $E_\infty^{i,j}$ along the $i + j = n$ line are successive quotients of a filtration on $H^n(A^\bullet)$. Knowing the $E_\infty^{i,j}$ gives us information about $H^n(A^\bullet)$. Sometimes we can completely determine $H^n(A^\bullet)$ this way.

Example 3.8.5 (3.8.3 continued)**.** The spectral sequence $E_r^{i,j}$ we get from $A^{\bullet,\bullet}$ is called the *Lyndon–Hochschild–Serre spectral sequence*. It converges to $H^*(G, M)$. The E_1-page looks like $\operatorname{Hom}_{\mathbb{Z}[G/H]}(Q^\bullet, H^*(H, M))$. The E_2-page is $H^i\left(G/H, H^j(H, M)\right)$. One often writes the shorthand notation $H^{i+j}(G, M)$.

Suppose we have a first quadrant spectral sequence and we know the E_2-page. We get the E_3-page by taking cohomology of the complexes on the E_2-page:

$$\begin{tikzcd}
\ker\left(E_2^{0,2} \to E_2^{2,1}\right) \arrow[ddrrr] & \ker\left(E_2^{1,2} \to E_2^{3,1}\right) & \cdots & \\
\ker\left(E_2^{0,1} \to E_2^{2,0}\right) & \ker\left(E_2^{1,1} \to E_2^{3,0}\right) & \cdots & \\
E_2^{0,0} & E_2^{1,0} & E_2^{2,0}/d_2^{0,1}\left(E_2^{0,1}\right) & \cdots
\end{tikzcd}$$

where the two red rows have no space for a nonzero arrow to come out, i.e. they are already stabilised, $E_3^{i,j} = E_\infty^{i,j}$ for the red. But by property 7, $E_\infty^{i,j}$ for $i+j=n$ are successive quotients of a filtration on $H^n(\operatorname{Tot} A^{\bullet,\bullet})$. In particular, fix $i+j=1$, we immediately get an ses,

$$0 \longrightarrow E_2^{1,0} \longrightarrow H^1(\operatorname{Tot} A^{\bullet,\bullet}) \longrightarrow \ker\left(E_2^{0,1} \to E_2^{2,0}\right) \longrightarrow 0$$

and for $i+j=2$ we have an injection

$$E_2^{2,0}/d_2^{0,1}\left(E_2^{0,1}\right) \hookrightarrow H^2(\operatorname{Tot} A^{\bullet,\bullet})$$

Sticking them together we get the "5-term low-degree exact sequence"

$$0 \longrightarrow E_2^{1,0} \longrightarrow H^1(\operatorname{Tot} A^{\bullet,\bullet}) \longrightarrow E_2^{0,1} \longrightarrow E_2^{2,0} \longrightarrow H^2(\operatorname{Tot} A^{\bullet,\bullet}).$$

Example 3.8.6 (3.8.3 continued)**.** The calculation before and the above deduction gives us

$$0 \longrightarrow H^1\left(G/H, M^H\right) \longrightarrow H^1(G,H) \longrightarrow H^1(H,M)^{G/H} \longrightarrow H^2(G/H, M^H) \longrightarrow H^2(G,M)$$

which looks precisely like the sequence we started this subsection with! It remains as an exercise to see that the maps are indeed inflation and restriction.

Exercise 3.8.7. Let $H \trianglelefteq G$ and M a $\mathbb{Z}[G]$-module. Suppose $H^i(H,M) = 0\ \forall i = 1,\dots,n$ for some $n \geq 1$. Show that $H^i(G,M) \cong H^i\left(G/H, M^H\right)\ \forall i = 1,\dots,n-1$, and that there is an exact sequence

$$0 \longrightarrow H^n\left(G/H, M^H\right) \xrightarrow{\text{Inf}} H^n(G,M) \xrightarrow{\text{Res}} H^n(G/H,M)^{G/H} \longrightarrow H^{n+1}\left(G/H, M^H\right) \xrightarrow{\text{Inf}} H^{n+1}(G,M).$$

Example 3.8.8. Let m be an odd integer. Let's use the Lyndon–Hochschild–Serre spectral sequence to compute $H^*(D_{2m},\mathbb{Z})$ where $\mathbb{Z}$ is the trivial $\mathbb{Z}[D_{2m}]$-module. We already saw in 3.6.4 with the inflation-restriction sequence that $H^1(D_{2m},\mathbb{Z}) = 0$. We know D_{2m} is an extension of the form $0 \to C_m \to D_{2m} \to C_2 \to 0$. So the E_2-page of the Lyndon–Hochschild–Serre spectral sequence is $E_2^{i,j} = H^i\left(C_2, H^j(C_m,\mathbb{Z})\right)$, where by calculation in 3.4.7,

$$H^j(C_m,\mathbb{Z}) \cong \begin{cases} \mathbb{Z} & \text{if } j=0 \\ 0 & \text{if } j \text{ is odd} \\ \mathbb{Z}/m\mathbb{Z} & \text{if } j>0 \text{ is even.} \end{cases}$$

Since we assumed m is odd, $|C_2|$ is coprime to m, so $E_2^{i,j} = H^i\left(C_2, H^j(C_m,\mathbb{Z})\right) = 0\ \forall i,j$ except possibly $i=0$ or $j=0$. To find $E_2^{i,j}$ for $i=0$ or $j=0$ we need to understand how C_2 acts on $H^j(C_m,\mathbb{Z})$. The C_2-action on C_m is induced by conjugations in D_{2m}. We saw that this action is the nontrivial one (the generator acts as -1; otherwise we would have $C_{2m} = C_2 \times C_m$ instead of D_{2m}). Look at Example 6.7.10 on page 191 in Weibel's book to see that C_2 acts as $(-1)^j$ on $H^{2j}(C_m,\mathbb{Z})$. So we find that

$$E_2^{0,j} = H^0\left(C_2, H^j(C_m,\mathbb{Z})\right) = \begin{cases} \mathbb{Z} & \text{if } j=0 \\ 0 & \text{if } j \text{ is odd} \\ \mathbb{Z}/m\mathbb{Z} & \text{if } j>0 \text{ and } j \equiv 0 \bmod 4 \\ 0 & \text{if } j>0 \text{ and } j \equiv 2 \bmod 4 \end{cases}$$

and

$$E_2^{i,0} = H^i(C_2,\mathbb{Z}) = \begin{cases} 0 & \text{if } i \text{ is odd} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } i \text{ is even} \end{cases}$$

We can thus see the E_2-page as follows:

$$\begin{tikzcd}
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\
\mathbb{Z}/m\mathbb{Z} & 0 & 0 & 0 \arrow[drr] & 0 & 0 & \cdots \\
0 & 0 & 0 & 0 & 0 & 0 & \cdots \\
0 & 0 & 0 \arrow[drr] & 0 & 0 & 0 & \cdots \\
0 \arrow[drr] & 0 & 0 & 0 & 0 & 0 & \cdots \\
\mathbb{Z} & 0 & \mathbb{Z}/2\mathbb{Z} & 0 & \mathbb{Z}/2\mathbb{Z} & 0 & \cdots
\end{tikzcd}$$

In particular, note that the d_2-differentials either begin or end on a zero, so they are all the zero map, i.e. their kernels are everything and the E_3-page (and the E_4-page, and so on) are the same. This means $E_2^{i,j} = E_\infty^{i,j}\ \forall i, j$ already stabilises.

Looking at the $i + j = n$ lines, we immediately read off

$$H^n(D_{2m}, \mathbb{Z}) \cong \begin{cases} \mathbb{Z} & \text{if } n = 0 \\ 0 & \text{if } n \text{ is odd} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } n \equiv 2 \bmod 4 \end{cases}$$

since these lines have at most one nontrivial entry. What about $0 < i + j = n \equiv 0 \bmod 4$? We get an extension

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow H^n(D_{2n}, \mathbb{Z}) \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0,$$

where $(2, m) = 1$ so this splits, and since $H^n(D_{2n}, \mathbb{Z})$ is abelian, so in this case

$$H^n(D_{2m}, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/2m\mathbb{Z}.$$

What happens if m is even?