MATH 901 LECTURE NOTES, FALL 2021

Contents

1. Category Theory 1
1.1. Categories 1
1.2. Basic notions with morphisms 5
1.3. Category-theoretic constructions of objects 6
1.4. Functors 10
1.5. Natural transformations 12
2. R-Modules 14
2.1. Kernels, images, and exact sequences 16
2.2. Homomorphisms of R-modules 19
2.3. Exact functors and left exactness of Hom 23
2.4. Tensor products 26
2.5. Projective, injective, and flat modules 37
3. Simplicity, semisimplicity, and representation theory 43
3.1. Group rings and representations 43
3.2. Simple modules and finite length modules 46
3.3. Chain conditions 50
3.4. Semisimple modules 53
3.5. Semisimple rings and the Artin-Wedderburn theorem 55
3.6. Applications to representation theory 61
4. Homological Algebra 64
4.1. The category of chain complexes of R-modules 65
4.2. Homology 68
4.3. Homotopy of chain maps 75
4.4. Projective and Injective Resolutions 76
4.5. Derived functors 82
4.6. Long exact sequence of a derived functor 86
4.7. Balancing Tor and Ext 90
Index 93

1. Category Theory

1.1. Categories.

Lecture of August 23, 2021

1.1.1. *Definition of category.*

Definition 1.1. A *category* $\mathscr{C}$ consists of the following data:

(1) a collection of *objects*, denoted $\mathrm{Ob}(\mathscr{C})$,
(2) for each pair of objects $A, B \in \mathrm{Ob}(\mathscr{C})$, a set $\mathrm{Hom}_{\mathscr{C}}(A, B)$ of *morphisms* (also known as *arrows*) from A to B,
(3) for each triple of objects $A, B, C \in \mathrm{Ob}(\mathscr{C})$, a function

$$\mathrm{Hom}_{\mathscr{C}}(A, B) \times \mathrm{Hom}_{\mathscr{C}}(B, C) \longrightarrow \mathrm{Hom}_{\mathscr{C}}(A, C)$$

written as $(\alpha, \beta) \mapsto \beta \circ \alpha$ that we call the *composition rule*.

These data are required to satisfy the following axioms:

(1) (Disjointness) the Hom sets are disjoint: if $A \neq A'$ or $B \neq B'$, then

$$\mathrm{Hom}_{\mathscr{C}}(A, B) \cap \mathrm{Hom}_{\mathscr{C}}(A', B') = \varnothing.$$

(2) (Identities) for every object A, there is an *identity morphism* $1_A \in \mathrm{Hom}_{\mathscr{C}}(A, A)$ such that $1_A \circ f = f$ and $g \circ 1_A = g$ for all $f \in \mathrm{Hom}_{\mathscr{C}}(B, A)$ and all $g \in \mathrm{Hom}_{\mathscr{C}}(A, B)$.
(3) (Associativity) composition is associative: $f \circ (g \circ h) = (f \circ g) \circ h$.

Remark 1.2. (1) The word "collection" as opposed to "set" is important here. The point is that there is no set of all sets, but by utilizing bigger collecting objects in set theory, we can sensibly talk about the collection of all sets. We'll sweep all of the set theory under the rug there, but it's worth keeping in mind that the objects of a category don't necessarily form a set. We did assume that the collections of morphisms between a pair of objects form a set, though not everyone does.
(2) The first axiom above guarantees that every morphism α in a category $\mathscr{C}$ has a well-defined *source* and *target* in $\mathrm{Ob}(\mathscr{C})$, namely, the unique A and B (respectively) such that $\alpha \in \mathrm{Hom}_{\mathscr{C}}(A, B)$.

The name arrow dovetails with the common practice of depicting a morphism $\alpha \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ as

$$A \xrightarrow{\alpha} B.$$

The composition of $A \xrightarrow{\alpha} B$ and $B \xrightarrow{\beta} C$ is $A \xrightarrow{\beta \circ \alpha} C$.

Optional Exercise 1.3. Prove that every element in a category has a unique identity morphism (i.e., a unique morphism that satisfies the hypothesis of axiom (2)).

1.1.2. *Examples of categories.* Many of our favorite objects from algebra naturally congregate in categories!

Example 1.4. (1) There is a category **Set** where
- $\mathrm{Ob}(\mathbf{Set})$ is the collection of all sets
- for two sets X, Y, $\mathrm{Hom}_{\mathbf{Set}}(X, Y)$ is the the set of functions from X to Y
- the composition rule is composition of functions

We observe that every set has an identity function, which behaves as an identity for composition, and that composition of functions is associative.

(2) There is a category **Grp** where
- $\mathrm{Ob}(\mathbf{Grp})$ is the collection of all groups
- for two sets X, Y, $\mathrm{Hom}_{\mathbf{Grp}}(X, Y)$ is the the set of group homomorphisms from X to Y
- the composition rule is composition of functions

Note that the identity function on a group is a group homomorphism, and that a composition of two group homomorphisms is a group homomorphism.

(3) There is a category **Ab** where

- Ob(**Ab**) is the collection of all abelian groups
- for two sets X, Y, $\mathrm{Hom}_{\mathbf{Ab}}(X, Y)$ is the the set of group homomorphisms from X to Y
- the composition rule is composition of functions

(4) In this class,
- A *semigroup* is a set S with an associative operation $\cdot$ that has an identity element; some may prefer the term *monoid*, but I don't.
- A *semigroup homomorphism* from semigroups $S \to T$ is a function that preserves the operation and maps the identity element to the identity element.

There is a category **Sgrp** where the objects are all semigroups and the morphisms are semigroup homomorphisms. (The composition rule is composition again.)

(5) In this class,
- A *ring* is a set R with two operations $+$ and $\cdot$ such that $(R, +)$ is abelian group, with identity 0, and $(R, \cdot)$ is a semigroup with identity 1, and such that the left and right distributive laws hold: $(r + s)t = rt + st$ and $t(r + s) = tr + ts$.
- A *ring homomorphism* is a function that preserves $+$ and $\cdot$ and sends 1 to 1.

There is a category **Ring** where the objects are all rings and the morphisms are ring homomorphisms.

(6) Let R be a ring. In this class,
- A *left R-module* is an abelian group $(M, +)$ equipped with a pairing $R \times M \to M$, written $(r, m) \mapsto rm$ or $(r, m) \mapsto r \cdot m$ such that
  (a) $r_1(r_2m) = (r_1r_2)m$,
  (b) $(r_1 + r_2)m = r_1m + r_2m$,
  (c) $r(m_1 + m_2) = rm_1 + rm_2$, and
  (d) $1m = m$.
- A *left module homomorphism* or *R-linear map* between left R-modules $\phi : M \to N$ is a homomorphism of abelian groups from $(M, +) \to (N, +)$ such that $\phi(rm) = r\phi(m)$.

There is a category $R-$**Mod** where the objects are all left R-modules and the morphisms are R-linear maps.

(7) There is a category **Fld** where the objects are all fields and the morphisms are all field homomorphisms.

(8) There is a category **Top** where the objects are all topological spaces and the morphisms are all continuous functions.

Remark 1.5. There are two special cases of the category of R-modules that are worth singling out:

- Every abelian group M is a $\mathbb{Z}$-module in a unique way, by setting
$$n \cdot m = \underbrace{m + \cdots + m}_{n-\text{times}} \quad \text{and} \quad -n \cdot m = -(\underbrace{m + \cdots + m}_{n-\text{times}}) \qquad \text{for } n \geqslant 0.$$
Thus, **Ab** is basically just $\mathbb{Z} - \mathbf{Mod}$.
- When $R = K$ happens to be a field, we are accustomed to calling K-modules *vector spaces*. Thus, we might write $K - \mathbf{Vect}$ for $K - \mathbf{Mod}$.

Lecture of August 25, 2021

Example 1.6. Here are some variations on the category $K - \mathbf{Vect}$.

(1) The collection of finite dimensional K-vector spaces with all linear transformations is a category; call it $K - \mathbf{vect}$.

(2) The collection of all n-dimensional K-vector spaces with all linear transformations is a category.
(3) The collection of all K-vector spaces (or n-dimensional vector spaces) with linear isomorphisms is a category.
(4) The collection of all K-vector spaces (or n-dimensional vector spaces) with nonzero linear transformations is not a category, since it's not closed under composition.
(5) The collection of all n-dimensional vector spaces with singular linear transformations is not a category, since it doesn't have identity maps.

Example 1.7. (1) There is a category $\mathbf{Set}_*$ of *pointed sets* where
- the objects are pairs (X, x) where X is a set and $x \in X$,
- for two pointed sets, the morphisms from (X, x) to (Y, y) are functions $f : X \to Y$ such that $f(x) = y$,
- usual composition.

(2) For a commutative ring A,
- A *commutative A-algebra* is a commutative ring R plus a homomorphism $\phi : A \to R$.
- Slightly more generally, an *A-algebra* is a ring R plus a homomorphism $\phi : A \to R$ such that $\phi(A)$ lies in the center of R: $r \cdot \phi(a) = \phi(a) \cdot r$ for any $a \in A$ and $r \in R$. (In the more general situation, A is still commutative but R may not be.)
- An *A-algebra homomorphism* between two A-algebras (R, ϕ) and (S, ψ) is a ring homomorphism $\alpha : R \to S$ such that $\alpha \circ \phi = \psi$.

The category of A-algebras is denoted $A - \mathbf{Alg}$, and the category of commutative A-algebras is $A - \mathbf{cAlg}$.

(3) Fix a field K, and define a category $\mathbf{Mat}_K$ as follows: the objects are the positive natural numbers $n \in \mathbb{N}_{>0}$, and $\mathrm{Hom}_{\mathscr{C}}(a, b)$ is the set of $b \times a$ matrices with entries in K. To see this as a category, we need a composition rule. Given $B \in \mathrm{Hom}_{\mathscr{C}}(b, c)$ and $A \in \mathrm{Hom}_{\mathscr{C}}(a, b)$, take the composition $A \circ B \in \mathrm{Hom}_{\mathscr{C}}(a, c)$ to be the product AB. Since matrix multiplication is associative, axiom (3) holds, and the $n \times n$ identity matrix serves as an identity morphism in the sense of axiom (2). Finally, if $A \in \mathrm{Hom}_{\mathscr{C}}(a, b) \cap \mathrm{Hom}_{\mathscr{C}}(a', b')$, then A is a $b \times a$ matrix and a $b' \times a'$ matrix, so $a = a'$ and $b = b'$. Notably, the morphisms in this category are not functions.

We can also make a bunch of categories in a hands-on way as follows:

Example 1.8. Let $(P, \leqslant)$ be a poset. We define a category $\mathbf{PO}(P)$ from P as follows. The objects of $\mathbf{PO}(P)$ are just the elements of P. For each pair $a, b \in P$ with $a \leqslant b$, form a symbol f_a^b. Then we set

$$\mathrm{Hom}_{\mathbf{PO}(P)}(a, b) = \begin{cases} \{f_a^b\} & \text{if } a \leqslant b \\ \varnothing & \text{otherwise.} \end{cases}$$

There is only one possible composition rule:

$$\mathrm{Hom}_{\mathbf{PO}(P)}(a, b) \times \mathrm{Hom}_{\mathbf{PO}(P)}(b, c) \longrightarrow \mathrm{Hom}_{\mathbf{PO}(P)}(a, c)$$

when $a \leqslant b$ and $b \leqslant c$ we also have $a \leqslant c$, and the unique pair on the left must map to the unique element on the right, so $f_b^c \circ f_a^b = f_a^c$; when either $a \not\leqslant b$ or $b \not\leqslant c$, there is nothing to compose!

Each morphism f_a^b is in only one Hom set (with source a and target b). Composition is associative since there is at most one function between one element sets. For any a, $f_a^a \in \mathrm{Hom}_{\mathbf{PO}(P)}(a, a)$ is the identity morphism.

For a specific example, we can think of $\mathbb{N}_{>0}$ as a category this way. Drawing all of the morphisms would be a mess, but any morphism is a composition of the ones depicted:

$$1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5 \longrightarrow \cdots .$$

Note that the objects of this category are exactly the same as in Example 1.7(3), but with much fewer morphisms!

Example 1.9. A category with one object is nothing but a semigroup.

1.1.3. *Constructions of categories.* Here are a few more basic constructions of categories:

Definition 1.10. Given a category $\mathscr{C}$, the *opposite category* $\mathscr{C}^{\mathrm{op}}$ is the category with $\mathrm{Ob}(\mathscr{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathscr{C})$, and $\mathrm{Hom}_{\mathscr{C}}(A, B) = \mathrm{Hom}_{\mathscr{C}}(B, A)$ for all $A, B \in \mathrm{Ob}(\mathscr{C})$.

That is, the opposite category is the "same category with the arrows reversed." To avoid confusion, we might write α^{op} for the morphism $B \xrightarrow{\alpha^{\mathrm{op}}} A$ in $\mathscr{C}^{\mathrm{op}}$ corresponding to $A \xrightarrow{\alpha} B$ in $\mathscr{C}$.

Definition 1.11. Given two categories $\mathscr{C}$ and $\mathscr{D}$, the *product category* $\mathscr{C} \times \mathscr{D}$ is the category with $\mathrm{Ob}(\mathscr{C} \times \mathscr{D})$ given by the collection of pairs (C, D) with $C \in \mathrm{Ob}(\mathscr{C})$ and $D \in \mathrm{Ob}(\mathscr{D})$, and $\mathrm{Hom}_{\mathscr{C}\times\mathscr{D}}((A, B), (C, D)) = \mathrm{Hom}_{\mathscr{C}}(A, C) \times \mathrm{Hom}_{\mathscr{D}}(B, D)$. We leave it to you to pin down the composition rule.

Definition 1.12. A category $\mathscr{D}$ is a *subcategory* of another category $\mathscr{C}$ provided

(1) every object of $\mathscr{D}$ is an object of $\mathscr{C}$
(2) for every $A, B \in \mathrm{Ob}(\mathscr{D})$, $\mathrm{Hom}_{\mathscr{D}}(A, B) \subseteq \mathrm{Hom}_{\mathscr{C}}(A, B)$, and
(3) for every $A \xrightarrow{\alpha} B$ and $B \xrightarrow{\beta} C$ in $\mathscr{D}$, the composition of α and β in $\mathscr{D}$ equals the composition of α and β in $\mathscr{C}$.

If equality hold in (2) (for all A, B), we say that $\mathscr{D}$ is a *full subcategory* of $\mathscr{C}$.

Example 1.13. Since every group is a set, and every homomorphism is a function, **Grp** is a subcategory of **Set**. However, since not every function between groups is a homomorphism, **Grp** is not a full subcategory of **Set**. Similarly, **Ab**, **Ring**, $R-$**Mod**, and **Top** are all subcategories of **Set**.

On the other hand, **Ab** is a full subcategory of **Grp**, and **Grp** is a full subcategory of **Sgrp**: a morphism of abelian groups is a morphism of groups that happens to be between abelian groups (and likewise for groups and semigroups)!

Lecture of August 27, 2021

1.2. **Basic notions with morphisms.**

Definition 1.14. A *diagram* in a category $\mathscr{C}$ is a directed multigraph whose vertices are objects in $\mathscr{C}$ and whose arrows/edges are morphisms in $\mathscr{C}$. A *commutative diagram* in $\mathscr{C}$ is a diagram in which for each pair of vertices A, B, any two paths from A to B compose to the same morphism.

Example 1.15. To say that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\beta} \\ C & \xrightarrow{\delta} & D \end{array}$$

commutes is to say that $\beta \circ \alpha = \delta \circ \gamma$ in $\mathrm{Hom}_{\mathscr{C}}(A, D)$.

Definition 1.16. Let $\mathscr{C}$ be any category and $A \xrightarrow{\alpha} B$ a morphism.

- α is an *isomorphism* if there exists $B \xrightarrow{\beta} A$ such that $\beta \circ \alpha = 1_A$ and $\alpha \circ \beta = 1_B$. Such an β is called the *inverse* of f.
- α has β as a *left inverse* if $\beta \circ \alpha = 1_A$. Similarly define *right inverse*.
- α is a *monomorphism* or is *monic* if for all arrows

$$C \underset{\beta_2}{\overset{\beta_1}{\rightrightarrows}} A \xrightarrow{\alpha} B$$

  if $\alpha\beta_1 = \alpha\beta_2$ then $\beta_1 = \beta_2$. That is, α can be cancelled from the left.
- α is an *epimorphism* or is *epic* if for all arrows

$$A \xrightarrow{\alpha} B \underset{\beta_2}{\overset{\beta_1}{\rightrightarrows}} C$$

  if $\beta_1\alpha = \beta_2\alpha$ then $\beta_1 = \beta_2$. That is, α can be cancelled from the right.

Remark 1.17. Note that α has a left inverse in $\mathscr{C}$ if and only if α^{op} has a right inverse in $\mathscr{C}^{\mathrm{op}}$, and that α is monic in $\mathscr{C}$ if and only if α^{op} is epic in $\mathscr{C}^{\mathrm{op}}$. We say that these are *dual* notions in category theory.

Lemma 1.18. *If α has a left inverse, then α is monic. Similarly for "right inverse" and "epic".*

Proof. If $\beta \circ \alpha = 1_A$ and γ_1, γ_2 are two morphisms from $C \to A$ such that $\alpha \circ \gamma_1 = \alpha \circ \gamma_2$, then

$$\gamma_1 = (\beta \circ \alpha) \circ \gamma_1 = \beta \circ (\alpha \circ \gamma_1) = \beta \circ (\alpha \circ \gamma_2) = (\beta \circ \alpha) \circ \gamma_2 = \gamma_2.$$

Similarly for "right inverse" and "epic". □

Example 1.19. In **Set**, the monomorphisms and left-invertible morphisms agree, and these are the injective functions. The epimorphisms and right-invertible morphisms agree, and there are the surjective functions.

Optional Exercise 1.20. For any poset P, in $\mathbf{PO}(P)$, every morphism is both monic and epic, but no nonidentity morphism has a left or right-inverse.

1.3. **Category-theoretic constructions of objects.** A property or construction is *category theoretic* if can be described just in terms of the data of the category rather than aspects of a particular category.

Example 1.21. Can we identify $\varnothing$ in **Set** without looking at the objects' and morphisms' names? We can: for every set S, there is a unique function $f : \varnothing \to S$; $\varnothing$ is the only set with this property.

Definition 1.22.
(1) An object X in a category $\mathscr{C}$ is *initial* if there for every $Y \in \mathrm{Ob}(\mathscr{C})$, there is a unique morphism $X \to Y$.
(2) An object X in a category $\mathscr{C}$ is *terminal* if there for every $Y \in \mathrm{Ob}(\mathscr{C})$, there is a unique morphism $Y \to X$.

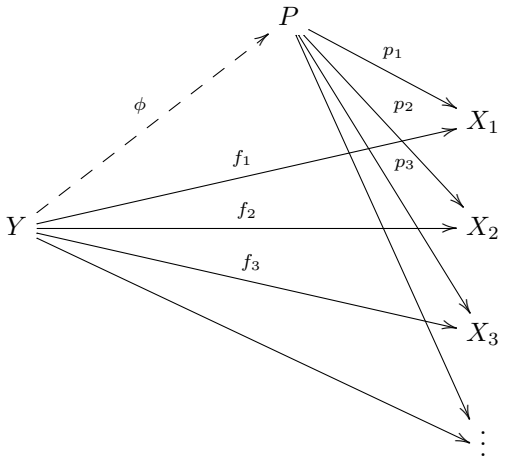
Example 1.23.
(1) We just saw that $\varnothing$ is initial in **Set**. Any singleton is terminal.
(2) A group with only one element $\{e\}$ is both initial and terminal in **Grp**.
(3) $\mathbb{Z}$ is initial in **Ring**.

1.3.1. *Definitions of product and coproduct.*

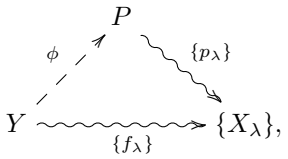
Definition 1.24. Let $\mathscr{C}$ be a category, and $\{X_\lambda\}_{\lambda \in \Lambda}$ be a family of objects. A *product* of $\{X_\lambda\}_{\lambda \in \Lambda}$ is given by an object P and a family of morphisms $\{p_\lambda : P \to X_\lambda\}_{\lambda \in \Lambda}$ that is universal in the following sense:

Given an object Y and a family of morphisms $\{f_\lambda : Y \to X_\lambda\}_{\lambda\in\Lambda}$, there is a unique morphism $\phi : Y \to P$ such that $p_\lambda \circ \phi = f_\lambda$ for all λ.

Here is a diagram for the (first few) maps involved when $\Lambda = \mathbb{N}$ is countable:



We can also take a "big picture" view of this universal property:



where the squiggly arrows are again collections of maps instead of maps. The data of Y with a family of maps to each X_λ is the sort of thing a product might be, so we may think of it as a "product candidate." In this way, we can think of a product as a "terminal product candidate."

Lecture of August 30, 2021

Remark 1.25. Note that $(P, \{p_\lambda\}_{\lambda\in\Lambda})$ is a product of $\{X_\lambda\}_{\lambda\in\Lambda}$ if and only if the function

$$\mathrm{Hom}_{\mathscr{C}}(Y, P) \longrightarrow \times_{\lambda\in\Lambda} \mathrm{Hom}_{\mathscr{C}}(Y, X_\lambda)$$

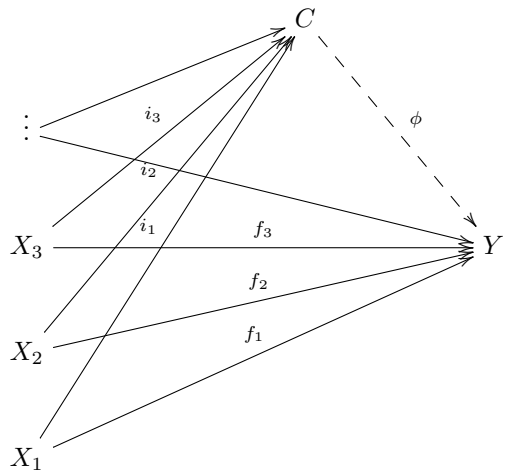
$$\phi \longmapsto (p_\lambda \circ \phi)_{\lambda\in\Lambda}$$

is a bijection for all objects Y: the universal property says that everything in the target comes from a unique thing in the source.

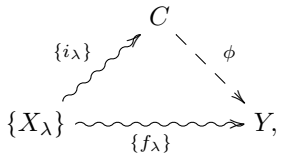
Definition 1.26. Let $\mathscr{C}$ be a category, and $\{X_\lambda\}_{\lambda\in\Lambda}$ be a family of objects. A *coproduct* of $\{X_\lambda\}_{\lambda\in\Lambda}$ is given by an object C and a family of morphisms $\{i_\lambda : X_\lambda \to C\}_{\lambda\in\Lambda}$ that is universal in the following sense:

Given an object Y and a family of morphisms $\{f_\lambda : X_\lambda \to Y\}_{\lambda\in\Lambda}$, there is a unique morphism $\phi : C \to Y$ such that $\phi \circ i_\lambda = f_\lambda$ for all λ.

Here is a diagram for the (first few) maps involved when $\Lambda = \mathbb{N}$ is countable:



We can also take a "big picture" view of the universal property:



where the squiggly arrows are now collections of maps instead of maps. We can again think of the coproduct as the "initial coproduct candidate."

Remark 1.27. Note that $(C, \{i_\lambda\}_{\lambda\in\Lambda})$ is a coproduct of $\{X_\lambda\}_{\lambda\in\Lambda}$ if and only if the function

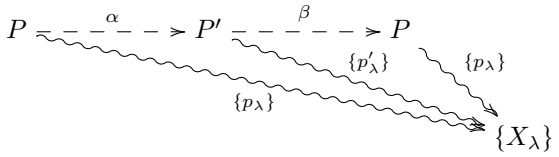
$$\mathrm{Hom}_{\mathscr{C}}(C, Y) \longrightarrow \times_{\lambda\in\Lambda} \mathrm{Hom}_{\mathscr{C}}(X_\lambda, Y)$$

$$\phi \longmapsto (\phi \circ i_\lambda)_{\lambda\in\Lambda}$$

is a bijection for all objects Y: the universal property says that everything in the target comes from a unique thing in the source.

Proposition 1.28. *If $(P, \{p_\lambda : P \to X_\lambda\}_{\lambda\in\Lambda})$ and $(P', \{p'_\lambda : P' \to X_\lambda\}_{\lambda\in\Lambda})$ are both products for the same family of objects $\{X_\lambda\}_{\lambda\in\Lambda}$ in a category $\mathscr{C}$, then there is a unique isomorphism $\alpha : P \xrightarrow{\sim} P'$ such that $p'_\lambda \circ \alpha = p_\lambda$ for all λ. The analogous statement holds for coproducts.*

Proof. We will just deal with products. The following picture is a rough guide:



Since $(P, \{p_\lambda\})$ is a product and $(P', \{p'_\lambda\})$ is an object with maps to each X_λ, there is a unique map $\beta : P' \to P$ such that $p_\lambda \circ \beta = p'_\lambda$. Switching roles, we obtain a unique map $\alpha : P \to P'$ such that $p'_\lambda \circ \alpha = p_\lambda$.

Consider the composition $\beta \circ \alpha : P \to P$. We have $p_\lambda \circ \beta \circ \alpha = p'_\lambda \circ \alpha = p_\lambda$ for all λ. The identity map $1_P : P \to P$ also satisfies the condition $p_\lambda \circ 1_P = p_\lambda$ for all λ, so by the uniqueness property of products, $\beta \circ \alpha = 1_P$. We can again switch roles to see that $\alpha \circ \beta = 1_{P'}$. Thus α is an isomorphism. The uniqueness of α in the statement is part of the universal property. □

Optional Exercise 1.29. Prove the analogous statement for coproducts.

We use the notation $\prod_{\lambda\in\Lambda} X_\lambda$ to denote the (object part of the) product of $\{X_\lambda\}$ and $\coprod_{\lambda\in\Lambda} X_\lambda$ to denote the (object part of the) coproduct of $\{X_\lambda\}$.

Observe that products and coproducts are dual notions in the same way as monic versus epic morphisms. The product of a family in $\mathscr{C}$ is the coproduct of the same family in $\mathscr{C}^{\mathrm{op}}$.

1.3.2. *Products in familiar categories.* The familiar notion of Cartesian product or direct product serves as a product in many of our favorite categories. Let's note first that given a family of objects $\{X_\lambda\}_{\lambda\in\Lambda}$ in any of the categories $\mathbf{Set}, \mathbf{Sgrp}, \mathbf{Grp}, \mathbf{Ring}, R-\mathbf{Mod}, \mathbf{Top}$, the direct product $\times_{\lambda\in\Lambda} X_\lambda$ is an object of the same category:

- for sets, this is clear;
- for semigroups, groups, and rings, take the operation coordinate by coordinate: $(x_\lambda)_{\lambda\in\Lambda} \cdot (y_\lambda)_{\lambda\in\Lambda} = (x_\lambda \cdot y_\lambda)_{\lambda\in\Lambda}$;
- for modules, addition is coordinate by coordinate, and the action is the same on each coordinate: $r \cdot (x_\lambda)_{\lambda\in\Lambda} = (r \cdot x_\lambda)_{\lambda\in\Lambda}$;
- for topological spaces, use the product topology.

Note that this is not true for fields!

Proposition 1.30. *In each of the categories* $\mathbf{Set}, \mathbf{Sgrp}, \mathbf{Grp}, \mathbf{Ring}, R-\mathbf{Mod}, \mathbf{Top}$*, given a family* $\{X_\lambda\}_{\lambda\in\Lambda}$*, the direct product* $\times_{\lambda\in\Lambda} X_\lambda$ *along with the projection maps* $\pi_\lambda : \times_{\gamma\in\Lambda} X_\gamma \to X_\lambda$ *forms a product in the category.*

Proof. We observe that in each category, the direct product is an object, and the projection maps π_λ are morphisms in the category.

Let $\mathscr{C}$ be one of these categories, and suppose that we have morphisms $g_\lambda : Y \to X_\lambda$ for all λ in $\mathscr{C}$. We need to show there is a unique morphism $\phi : Y \to \times_{\lambda\in\Lambda} X_\lambda$ such that $\pi_\lambda \circ \phi = g_\lambda$ for all λ. The last condition is equivalent to $(\phi(y))_\lambda = (\pi_\lambda \circ \phi)(y) = g_\lambda(y)$ for all λ, which is equivalent to $\phi(y) = (g_\lambda(y))_{\lambda\in\Lambda}$, so if this is a valid morphism, it is unique. Thus, it suffices to show that the map $\phi(y) = (g_\lambda(y))_{\lambda\in\Lambda}$ is a morphism in $\mathscr{C}$, which is easy to see in each case. □

1.3.3. *Coproducts in familiar categories.*

Example 1.31. Let $\{X_\lambda\}_{\lambda\in\Lambda}$ be a family of sets. The product of $\{X_\lambda\}_{\lambda\in\Lambda}$ is given by the cartesian product along with the projection maps. The coproduct of $\{X_\lambda\}_{\lambda\in\Lambda}$ is given by the "disjoint union" with the various inclusion maps. By disjoint union, we simply mean union if the sets are disjoint; in general do something like replace X_λ with $X_\lambda \times \{\lambda\}$ to make them disjoint.

Proposition 1.32. *Let* R *be a ring, and* $\{M_\lambda\}_{\lambda\in\Lambda}$ *be a family of left* R*-modules. A coproduct for the family* $\{M_\lambda\}_{\lambda\in\Lambda}$ *is* $(\bigoplus_{\lambda\in\Lambda} M_\lambda, \{\iota_\lambda\}_{\lambda\in\Lambda})$*, where*

$$\bigoplus_{\lambda\in\Lambda} M_\lambda = \{(x_\lambda)_{\lambda\in\Lambda} \mid x_\lambda \neq 0 \text{ for at most finitely many } \lambda\} \subseteq \prod_{\lambda\in\Lambda} M_\lambda$$

is the direct sum of the modules M_λ*, and* ι_λ *is the inclusion map to the* λ *coordinate.*

Lecture of September 1, 2021

Remark 1.33. If the index set Λ is finite, then the objects $\prod_{\lambda\in\Lambda} M_\lambda$ and $\bigoplus_{\lambda\in\Lambda} M_\lambda$ are identical, but the product and coproduct are not the same since one involves projection maps and the other involves inclusion maps.

Proof. Given R-module homomorphisms $g_\lambda : M_\lambda \to N$ for each λ, we need to show that there is a unique R-module homomorphism $\alpha : \bigoplus_{\lambda\in\Lambda} M_\lambda \to N$ such that $\alpha \circ \iota_\lambda = g_\lambda$. We define

$$\alpha((m_\lambda)_{\lambda\in\Lambda}) = \sum_{\lambda\in\Lambda} g_\lambda(m_\lambda).$$

Note that since $(m_\lambda)_{\lambda\in\Lambda}$ is in the direct sum, at most finitely many m_λ are nonzero, so the sum on the right hand side is finite, and hence makes sense in N. We need to check that α is R-linear; indeed,

$$\alpha((m_\lambda) + (n_\lambda)) = \alpha((m_\lambda + n_\lambda)) = \sum g_\lambda(m_\lambda + n_\lambda) = \sum g_\lambda(m_\lambda) + \sum g_\lambda(n_\lambda) = \alpha((m_\lambda)) + \alpha((n_\lambda)),$$

and the check for scalar multiplication is similar. For uniqueness of α, note that $\bigoplus_{\lambda\in\Lambda} M_\lambda$ is generated by the elements $\iota_\lambda(m_\lambda)$ for $m_\lambda \in M_\lambda$. Thus, if α' also satisfies $\alpha' \circ \iota_\lambda = g_\lambda$ for all λ, then $\alpha(\iota_\lambda(m_\lambda)) = g_\lambda(m_\lambda) = \alpha'(\iota_\lambda(m_\lambda))$ so the maps must be equal. □

Remark 1.34. For any indexing set Λ, $\coprod_{\lambda\in\Lambda} R$ is a free R-module. If $R = K$ happens to be a field, then $\prod_{\lambda\in\Lambda} K$ is free, since all vector spaces are free modules, but in general, $\prod_{\lambda\in\Lambda} R$ is not free for an infinite set Λ.

Remark 1.35.

- In **Top**, disjoint unions serve as coproducts.
- In **Sgrp** and **Grp**, coproducts exist, and are given as free products. You may see or have seen them in topology in the context of Van Kampen's theorem.
- In **Ring**, the story is more complicated. Let's note first that disjoint unions won't work, since they aren't rings. Direct sums of infinitely many rings don't have 1, so aren't rings, but even finite direct sums/products won't work, since the inclusion maps don't send 1 to 1. We will later on construct coproducts in **cRing** , the full subcategory of **Ring** consisting of commutative rings.

1.4. **Functors.**

Definition 1.36. Let $\mathscr{C}$ and $\mathscr{D}$ be categories. A *covariant functor* $F : \mathscr{C} \to \mathscr{D}$ is a mapping that assigns to each object $A \in \mathrm{Ob}(\mathscr{C})$ an object $F(A) \in \mathrm{Ob}(\mathscr{D})$ and to each morphism $\alpha \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ a morphism $F(\alpha) \in \mathrm{Hom}_{\mathscr{D}}(F(A), F(B))$ such that

(1) F preserves compositions, meaning $F(\alpha \circ \beta) = F(\alpha) \circ F(\beta)$ for all morphisms α, β in $\mathscr{C}$, and
(2) F preserves identity morphisms, meaning $F(1_A) = 1_{F(A)}$ for all objects A in $\mathscr{C}$.

A *contravariant functor* $F : \mathscr{C} \to \mathscr{D}$ is a mapping that assigns to each object $A \in \mathrm{Ob}(\mathscr{C})$ an object $F(A) \in \mathrm{Ob}(\mathscr{D})$ and to each morphism $\alpha \in \mathrm{Hom}_{\mathscr{C}}(A, B)$ a morphism $F(\alpha) \in \mathrm{Hom}_{\mathscr{D}}(F(B), F(A))$ such that

(1) F preserves compositions, meaning $F(\alpha \circ \beta) = F(\beta) \circ F(\alpha)$ for all morphisms α, β in $\mathscr{C}$, and
(2) F preserves identity morphisms, meaning $F(1_A) = 1_{F(A)}$ for all objects A in $\mathscr{C}$.

Remark 1.37. One can also interpret a contravariant functor as a covariant functor from $\mathscr{C}^{\mathrm{op}} \to \mathscr{D}$, or as a covariant functor from $\mathscr{C} \to \mathscr{D}^{\mathrm{op}}$.

Example 1.38. Here are some examples of functors.

(1) Many of the categories we considered before are sets with extra structure, and the morphisms are functions that preserve the extra structure. The *forgetful functor* from such a category $\mathscr{C}$ to **Set**, is the covariant functor that forgets that extra structure are returns the underlying set of the object. For example the forgetful functor **Grp** $\to$ **Set** sends each group to its set of elements, and each homomorphism to its corresponding function of sets. Along similar lines, a ring is a group under addition with the bonus structure of multiplication, and we can talk about the forgetful functor from **Ring** to **Grp**, etc.

(2) The *identity functor* $1_{\mathscr{C}}$ on any category $\mathscr{C}$ sends each object to itself and each morphism to itself. It is covariant.

(3) There is a covariant functor $(-)^{\times 2}$: **Set** $\to$ **Set** that sends every set S to its cartesian square $S \times S$, and every function $f : S \to T$ to the function $(f, f) : S \times S \to T \times T$ that sends $(s_1, s_2) \mapsto (f(s_1), f(s_2))$. Let's check the axioms: given $g : S \to T$ and $f : T \to U$, we need to see that $(f, f) \circ (g, g) = (f \circ g, f \circ g)$, which is clear, and that $(1_S, 1_S)$ is the identity map on $S \times S$, which is also clear.

(4) Given a group G, the subgroup $G' \leqslant G$ generated by the set of commutators $\{ghg^{-1}h^{-1} \mid g, h \in G\}$ is a normal subgroup, and the quotient $G^{\mathrm{ab}} := G/G'$ is called the *abelianization* of G. The group G^{ab} is abelian. Given a group homomorphism $\phi : G \to H$, ϕ automatically takes commutators to commutators, so it induces a homomorphism $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$. Put together, abelianization gives a covariant functor from **Grp** to **Ab**.

(5) Given any topological space X, the set of continuous functions from X to $\mathbb{R}$, $\mathrm{Cont}(X, \mathbb{R})$ is a ring with pointwise addition and multiplication. Given a continuous map $X \xrightarrow{\alpha} Y$, and a continuous map $Y \xrightarrow{f} \mathbb{R}$, the composition $X \xrightarrow{\alpha \circ f} \mathbb{R}$ is a continuous function. In this way, we get a map from $\mathrm{Cont}(Y, \mathbb{R})$ to $\mathrm{Cont}(X, \mathbb{R})$. In fact, this map is a ring homomorphism. Put together, we obtain a contravariant functor from **Top** to **Ring**.

(6) Fix a field K. Given a vector space V, the collection V^* of linear transformations from V to K is again a K-vector space, the *dual vector space* of V. If $\phi : W \to V$ is a linear transformation and $\ell : V \to K$ is in V^* then $\ell \circ \phi : W \to K$ is in W^*, so there is a map $V^* \to W^*$. You can check that this together forms a functor $(-)^*$ that is contravariant.

(7) You may be familiar with the fundamental group of a pointed topological space; this is a group $\pi_1(X, x)$ assigned to a topological space and a point in it. The rule π_1 gives a functor from pointed topological spaces to groups.

(8) The unit group functor **Ring** $\to$ **Grp** sends each ring to its group of units. A homomorphism of rings restricts to a group homomorphism on the units: if $x \in R$ is a unit, so $xy = 1$, and $\phi : R \to S$ is a group homomorphism, then $1 = \phi(xy) = \phi(x)\phi(y)$, so $\phi(x)$ is a unit; ϕ preserves multiplication as well. This is covariant.

Lecture of September 3, 2021

It follows from the definition of covariant functor that if we apply a covariant functor F to a commutative diagram, we get another commutative diagram of the same shape, e.g.:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\beta} \\ C & \xrightarrow{\delta} & D \end{array} \quad \overset{F}{\rightsquigarrow} \quad \begin{array}{ccc} F(A) & \xrightarrow{F(\alpha)} & F(B) \\ {\scriptstyle F(\gamma)}\downarrow & & \downarrow{\scriptstyle F(\beta)} \\ F(C) & \xrightarrow{F(\delta)} & F(D). \end{array}$$

If we apply a contravariant functor G to a commutative diagram, we get a commutative diagram of the same shape with the arrows reversed, e.g.:

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\beta} \\ C & \xrightarrow{\delta} & D \end{array} \qquad \overset{G}{\rightsquigarrow} \qquad \begin{array}{ccc} G(A) & \xleftarrow{G(\alpha)} & G(B) \\ {\scriptstyle G(\gamma)}\uparrow & & \uparrow{\scriptstyle G(\beta)} \\ G(C) & \xleftarrow{G(\delta)} & G(D). \end{array}$$

Remark 1.39. A composition of two covariant functors, or of two contravariant functors, is a covariant functor. The composition of a covariant functor and a contravariant functor, or vice versa, is a contravariant functor.

1.5. **Natural transformations.**

Definition 1.40. Let F and G be covariant functors $\mathscr{C} \longrightarrow \mathscr{D}$. A *natural transformation* η between F and G is a mapping that to each object A in $\mathscr{C}$ assigns a morphism $\eta_A \in \mathrm{Hom}_{\mathscr{D}}(F(A), G(A))$ such that for all $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$, the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{\eta_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow[\eta_B]{} & G(B) \end{array}$$

commutes. We sometimes write $\eta : F \implies G$.

A *natural isomorphism* is a natural transformation η where each η_A is an isomorphism.

In short, a natural transformation is a rule to turn F of whatever into G of whatever in a reasonable way.

Optional Exercise 1.41. Let $F, G : \mathscr{C} \to \mathscr{D}$ be covariant functors. Show that a natural transformation $\eta : F \implies G$ is a natural isomorphism if and only if there is another natural transformation $\mu : G \implies F$ such that $\mu \circ \eta$ is the identity natural isomorphism on F and $\eta \circ \mu$ is the identity natural transformation on G.

We can make make a similar definition for contravariant functors.

Definition 1.42. Let F and G be contravariant functors $\mathscr{C} \longrightarrow \mathscr{D}$. A *natural transformation* between F and G is a mapping that to each object A in $\mathscr{C}$ assigns a morphism $\eta_A \in \mathrm{Hom}_{\mathscr{D}}(F(A), G(A))$ such that for all $f \in \mathrm{Hom}_{\mathscr{C}}(A, B)$, the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{\eta_A} & G(A) \\ {\scriptstyle F(f)}\uparrow & & \uparrow{\scriptstyle G(f)} \\ F(B) & \xrightarrow[\eta_B]{} & G(B) \end{array}$$

commutes.

Example 1.43. Let's describe a natural transformation of functors $\eta : (-)^{\times 2} \implies 1_{\mathbf{Set}}$, namely we take

$$\eta_S : S \times S \to S \qquad (s_1, s_2) \mapsto s_1.$$

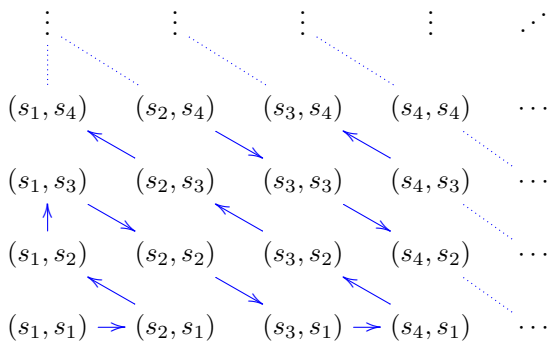
We need to check for every map $f : S \to T$ the commutativity of a diagram:

$$\begin{array}{ccc} S \times S & \xrightarrow{\eta_S} & S \\ {\scriptstyle (f,f)}\downarrow & & \downarrow{\scriptstyle f} \\ T \times T & \xrightarrow[\eta_T]{} & T. \end{array}$$

Going either down then left or right then down, (s_1, s_2) maps to $f(s_1)$, so this does commute, and we indeed have a natural transformation. This is not a natural isomorphism, since the map η_S is not always (almost never) an isomorphism of sets.

Example 1.44. Let $\mathscr{C}$ be the full subcategory of **Set** consisting of countable sets. For every $S \in \mathrm{Ob}(\mathscr{C})$, there is a $\mathscr{C}$-isomorphism, i.e., a bijection, $\eta_S : S \to S \times S$. Namely, we can take η_S as follows: enumerate S as $S = \{s_1, s_2, s_3, \dots\}$, and do the usual zigzag trick

$$\begin{aligned} s_1 &\mapsto (s_1, s_1) \\ s_2 &\mapsto (s_2, s_1) \\ s_3 &\mapsto (s_1, s_2) \\ s_4 &\mapsto (s_1, s_3) \\ s_5 &\mapsto (s_2, s_2) \\ s_6 &\mapsto (s_3, s_1) \\ &\vdots \end{aligned}$$



However, the bijections η_S do not form a natural bijection (in fact, if we just choose η_S like so for one set S, no matter what the other choices are, we can't get a natural transformation). Let $f : S \to S$ satisfy $f(s_1) = s_2$ and $f(s_2) = s_1$. Then in the diagram

$$\begin{array}{ccc} S & \xrightarrow{\eta_S} & S \times S \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle (f,f)} \\ S & \xrightarrow[\eta_S]{} & S \times S, \end{array}$$

we have $\eta_S(f(s_1)) = (s_2, s_1)$ while $(f, f)(\eta_S(s_1)) = (s_2, s_2)$, so the diagram does not commute.

Intuitively, we can blame the fact that our map η decided on a *choice* of enumeration of the set.

Example 1.45. Recall the contravariant functor $(-)^* : K - \mathbf{vect} \to K - \mathbf{vect}$; here we are restricting to finite dimensional vector spaces.

For every $V \in K - \mathbf{vect}$, there is an isomorphism $V \cong V^*$: if we fix a basis $\mathcal{B}$ for V, there is a dual basis for V^* (the $\mathcal{B}$-coordinate functions) of the same size, so they are isomorphic. However, there is no natural isomorphism $\eta : 1_{K-\mathbf{vect}} \implies (-)^*$, since $1_{K-\mathbf{vect}}$ is covariant and $(-)^*$ is contravariant. We will actually see a more compelling version of this nonnatruality statement in the homework.

Composing the dual functor with itself twice we get the covariant double-dual functor $(-)^{**} : K - \mathbf{vect} \to K - \mathbf{vect}$. We will show that there is a natural isomorphism $1_{K-\mathbf{vect}} \implies (-)^{**}$.

For every $v \in V$, there is a map $\mathrm{ev}_v : V^* \to V$ given by evaluation at v: $\mathrm{ev}_v(\ell) = \ell(v)$. So, $\mathrm{ev}_v \in V^{**}$. Since we have one for each v, there is a function $\mathrm{ev} : V \to V^{**}$ given by $\mathrm{ev}(v) = \mathrm{ev}_v$.

The map ev is a linear transformation:

$$\mathrm{ev}_{cv+w}(\ell) = \ell(cv+w) = c\ell(v) + \ell(w) = c\,\mathrm{ev}_v(\ell) + \mathrm{ev}_w(\ell).$$

It is injective, since any nonzero vector takes on a nonzero value for some linear functional. It is then a bijection since $\dim(V) = \dim(V^*) = \dim(V^{**})$.

We just need to check commutativity of the square:

$$\begin{array}{ccc} V & \xrightarrow{\mathrm{ev}} & V^{**} \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi^{**}} \\ W & \xrightarrow{\mathrm{ev}} & W^{**} \end{array}$$

This translates to

$$\mathrm{ev}_{\phi(v)} = (\mathrm{ev} \circ \phi)(v) \stackrel{?}{=} (\phi^{**} \circ \mathrm{ev})(v) = \phi^{**}(\mathrm{ev}_v)$$

in W^{**} for all $v \in V$. But, for all $\ell \in W^*$,

$$\mathrm{ev}_{\phi(v)}(\ell) = \ell(\phi(v)) = \phi^*(\ell)(v) = (\mathrm{ev}_v \circ \phi^*)(\ell) = \phi^{**}(\mathrm{ev}_v)(\ell),$$

so the equality holds.

In the homework, we will discuss some more examples from linear algebra. For example, for a pair of vector spaces $W \leqslant V$, there are isomorphisms $V \cong W \oplus V/W$, but no natural isomorphism of the sort. On the bright side, we will see that if V has an inner product, then V and V^* are naturally isomorphic in a suitable sense.

2. R-Modules

Lecture of September 8, 2021

2.0.1. *Left vs right vs both.* Recall that a left R-module is an abelian group M with an action map $R \times M \to M$ written $(r, m) \mapsto rm$ such that $r(sm) = (rs)m$, along with two distributive properties and the condition that 1 acts as the identity. A *right module* over R is defined similarly; we usually write the action as $(r, m) \mapsto mr$, and we have $(mr)s = m(rs)$, along with distributive and identity properties. The point is that when we act by a product $rs \in R$, we can think of it as an iterated action; in a left module, the left factor acts last while in a right module the right factor acts last.

Definition 2.1. If R is a ring, the *opposite ring* R^{op} is the ring with the same underlying set and same addition, but with multiplication given by $r \cdot_{R^{\mathrm{op}}} s = s \cdot_R r$.

A right R-module is exactly the same thing as a left R^{op}-module (except our convention for writing the action). In particular, if R is commutative, then a left R-module is exactly the same thing as a right R-module, and we will just say "module" in this case. By default, in general, when we say module, we will mean left R-module.

Example 2.2. Let R be a ring. The collection $M_n(R)$ of $n \times n$ matrices with entries in R forms a ring that in general is not commutative. The set R^n of column vectors of length n with entries in R is naturally a left $M_n(R)$-module. The collection of row vectors of length n with entries in R is naturally a right $M_n(R)$-module. We can also identify this latter action with a right module action on R^n by transposing any column vector into a row vector, acting, then transposing back:

$$v \cdot M = (v^T M)^T = M^T v.$$

We can think of R-module structures in a different way. To prepare, let's record a lemma.

Lemma 2.3. *If M is an abelian group, then $\mathrm{End}_{\mathbf{Ab}}(M) := \mathrm{Hom}_{\mathbf{Ab}}(M, M)$ forms a ring with pointwise addition and composition as multiplication. More generally, if M is a left R-module, then $\mathrm{End}_R(M) := \mathrm{Hom}_{R-\mathbf{Mod}}(M, M)$ forms a ring (with the aforementioned operations).*

Proof. The first statement is a special case of the first, since an abelian group is the same thing as a $\mathbb{Z}$-module, so we'll prove the second. Let $f, g \in \mathrm{End}_R(M)$. Since

$$(f+g)(rm+n) = f(rm+n) + g(rm+n) = rf(m) + f(n) + rg(m) + g(n) = r(f+g)(m) + (f+g)(n)$$

we see that $f + g \in \mathrm{End}_R(M)$. It's easy to see that $\mathrm{End}_R(M)$ is an abelian group under $+$. Associativity of multiplication is a special case of associativity of composition of functions. For distributive laws, we have

$$((f+g)h)(m) = (f+g)(h(m)) = f(h(m)) + g(h(m)) = (fh)(m) + (gh)(m)$$
$$(f(g+h))(m) = f(g(m) + h(m)) = f(g(m)) + f(h(m)) = (fg)(m) + (fh)(m);$$

for the latter distributive law, it was crucial that we are dealing with homomorphisms of abelian groups. We also have the identity map on M as a mutliplicative identity. □

Optional Exercise 2.4. Show that there is a ring isomorphism $\mathrm{End}_R(R) \cong R^{\mathrm{op}}$.

Proposition 2.5. *Let R be a ring and $(M, +)$ an abelian group. There is a bijective correspondence*

$$\{R - \textit{module actions } R \times M \to M \textit{ (with given } +)\} \longleftrightarrow \{\textit{ring homomorphisms } \rho : R \to \mathrm{End}_{\mathbb{Z}}(M)\}$$
$$\cdot \longmapsto \rho(r)(m) = r \cdot m$$
$$r \cdot m = \rho(r)(m) \longmapsfrom \rho.$$

Proof. We clearly have a bijection as long as the maps are well-defined.

Given an R-module action $\cdot$, one distributive property translates to the condition that $\rho(r)$ is $\mathbb{Z}$-linear; the identity condition means $\rho(1_R)$ is the identity function on M, which is the 1 element in $\mathrm{End}_{\mathbb{Z}}(M)$; the other distributive condition means ρ preserves addition; and the associativity condition means ρ preserves multiplication. Thus, ρ is a ring homomorphism. And conversely. □

It turns out that we often have a left module structure and a right module structure on something in a compatible way.

Definition 2.6. Let R and S be rings. An (R, S)-*bimodule* is an abelian group M equipped with a left R-module structure and a right S-module structure that commute with each other:

$$(r \cdot m) \cdot s = r \cdot (m \cdot s) \qquad \text{for all } m \in M, r \in R, s \in S.$$

Example 2.7. Here are some basic sources of bimodules:

(1) If R is a ring, then $M = R$ is an (R, R)-bimodule in the obvious way. More generally, if $\phi : A \to R$ is a ring homomorphism, then R is an (R, A)-bimodule by

$$s \cdot r \cdot a = sr\phi(a) \qquad \text{for } r, s \in R, a \in A;$$

equally well, R is an (A, R) or (A, A)-bimodule.

(2) If R is a commutative ring and M is any left module, then M is also a right module by the same action, and M is an (R, R)-bimodule with these structures. I.e., starting with an action $r \cdot m$, we

set $m \cdot s$ to be $s \cdot m$, and

$$(r \cdot m) \cdot s = s \cdot (r \cdot m) = sr \cdot m = rs \cdot m = r \cdot (s \cdot m) = r \cdot (m \cdot s).$$

(3) Every left R-module is automatically an $(R, \mathbb{Z})$-bimodule in a unique way:

$$(r \cdot m) \cdot n = \underbrace{(r \cdot m) + \cdots + (r \cdot m)}_{n \text{ times}} = r \cdot (\underbrace{m + \cdots + m}_{n \text{ times}}) = r \cdot (m \cdot n) \qquad \text{for } n \in \mathbb{Z}_{\geqslant 0},$$

and similarly for $n \leqslant 0$. Likewise, every right R-module is automatically a $(\mathbb{Z}, R)$-bimodule.

Example 2.8. For a ring R, the set of column vectors of length n, R^n, is a $(M_n(R), R)$-bimodule. However, if we take the natural left action together with the right action $v \cdot M = M^T v$ discussed above, we do not get a bimodule structure, since $(M \cdot v) \cdot N = N^T M v$ generally differs from $M \cdot (v \cdot N) = M N^T v$.

Sometimes, when we want to keep track of various module and bimodule structures, we may write something like ${}_R M_S$ to indicate that M is an (R, S)-bimodule, or ${}_R M$ to indicate that M is a left R-module.

2.1. **Kernels, images, and exact sequences.** To every homomorphism $\phi : M \to N$ in $R - \mathbf{Mod}$, the kernel $\ker(\phi) \subseteq M$ and image $\operatorname{im}(\phi) \subseteq N$ are in $R - \mathbf{Mod}$, and the inclusion maps are homomorphisms of R-modules. It is surprisingly convenient to keep track of and compare these data in terms of exact sequences.

Definition 2.9. A sequence of R-modules and R-module maps of the form

$$\cdots \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

(possible infinite, possibly not) is a *chain complex*, or just *complex* for short, if $d_i \circ d_{i+1} = 0$ for all i or, equivalently, $\operatorname{im}(d_{i+1}) \subseteq \ker(d_i)$ for all i.

A chain complex is *exact* at M_i if $\operatorname{im}(d_{i+1}) = \ker(d_i)$; it is exact if it is exact at every module that has a map in and a map out.

Lecture of September 10, 2021

Example 2.10. Let A be a $b \times a$ matrix and B be a $c \times b$ matrix of real numbers. The sequence of maps

$$\mathbb{R}^a \xrightarrow{A\cdot} \mathbb{R}^b \xrightarrow{B\cdot} \mathbb{R}^c$$

is a complex if and only if $BA = 0$; equivalently, the columns of A are in the solution space (nullspace) of B. It is exact if and only if the columns of A span the solution space of B.

Remark 2.11.
- A sequence of the form $M \xrightarrow{g} N \to 0$ is exact if and only if g is surjective.
- A sequence of the form $0 \to M \xrightarrow{f} N$ is exact if and only if f is injective.
- A sequence of the form $0 \to M \xrightarrow{h} N \to 0$ is exact if and only if h is an isomorphism.
- A sequence of the form $0 \to M \to 0$ is exact if and only if $M = 0$.

Definition 2.12.
- A *left exact sequence* is an exact sequence of the form

  $$0 \to M' \xrightarrow{i} M \xrightarrow{g} M''$$

  This means i is injective and $M' \cong \operatorname{im}(i) = \ker(g)$.
- A *right exact sequence* is an exact sequence of the form

  $$M' \xrightarrow{f} M \xrightarrow{p} M'' \to 0$$

  This means p is onto and $\operatorname{im}(f) = \ker(p)$, so, $M'' \cong M/\ker(p) = M/\operatorname{im}(f)$. We denote $M/\operatorname{im}(f) = \operatorname{coker}(f)$ and call it the *cokernel* of f. Thus in a right exact sequence as above, $M'' \cong \operatorname{coker}(f)$.

- A *short exact sequence* (*SES*) is an exact sequence of the form

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

Note that in a short exact sequence $M' \cong \ker(p)$ and $M'' \cong \operatorname{coker}(i)$. In particular, $M'' \cong M/M'$. We also say that M is an *extension* of M' and M'' if it fits in a short exact sequence as above.

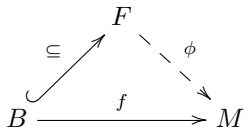
Example 2.13. Let A be a $b \times a$ matrix and B be a $c \times b$ matrix of real numbers. The sequence of maps

$$0 \to \mathbb{R}^a \xrightarrow{A\cdot} \mathbb{R}^b \xrightarrow{B\cdot} \mathbb{R}^c$$

is a left exact sequence if and only if the columns of A form a basis for the null space of B.

2.1.1. *Presentations.* Recall that a set of elements B in a module M is a *free basis* if every element of M can be written as a (finite) R-linear combination of elements of B in a unique way, and a module M is a *free module* if it admits a free basis (which almost never is unique, by the way). As mentioned before, a free module is isomorphic to a direct sum of copies of the ring (considered as a module), which we may write as R^n or $R^{\oplus\Gamma}$ for some index Γ; such a free module has as a *standard basis* $\{e_\lambda\}_{\lambda\in\Lambda}$ consisting the elements that have a 1 in the λ coordinate and 0 in each of the others. Free modules are also characterized by a universal property:

If F free with basis B, then for any module M, and any function $f : B \to M$, there is a unique module homomorphism $\phi : F \to M$ such that the diagram commutes:



i.e., any homomorphism is uniquely and freely specified by its values on the basis.

Note that a set of elements $\{m_\lambda\}_{\lambda\in\Lambda} \subseteq M$ generates M if and only if the homomorphism

$$R^\Lambda \longrightarrow M$$

$$e_\lambda \longmapsto m_\lambda$$

is surjective. The kernel of such a map consists of the set of Λ-tuples (r_λ) such that $\sum_{\lambda\in\Lambda} r_\lambda m_\lambda = 0$; this is called the module of *relations* on the elements $\{m_\lambda\}$.

Definition 2.14. A *presentation* of a module M consists of a set of elements $\{m_\lambda\}$ that generates M, and a set of relations on $\{m_\lambda\}$ that generates the whole module of relations on $\{m_\lambda\}$.

We can express the data of a presentation in terms of a right exact sequence. Namely, if $\{m_\lambda\}_{\lambda\in\Lambda}$ is a generating set of M, and $\{(r_\lambda)_\gamma\}_{\gamma\in\Gamma}$ generates the module of relations on our generating set, then

$$R^{\oplus\Gamma} \to R^{\oplus\Lambda} \to M \to 0$$

is a right exact sequence, where the standard basis of $R^{\oplus\Lambda}$ maps to $\{m_\lambda\}$ and the standard basis of $R^{\oplus\Gamma}$ maps to $\{(r_\lambda)_\gamma\}$. Conversely, a right exact sequence of the form

$$R^{\oplus\Gamma} \to R^{\oplus\Lambda} \to M \to 0$$

is equivalent to the data of a presentation.

2.1.2. *Split exact sequences.* Given modules M' and M'', we have the "trivial" SES

$$0 \to M' \xrightarrow{\iota} M' \oplus M'' \xrightarrow{\pi} M'' \to 0$$

where ι is the canonical inclusion and π is the canonical projection. The following result gives equivalent conditions for when a SES is equivalent to a split one.

Theorem 2.15 (The splitting theorem)**.** *Given a SES of left R-modules*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0,$$

the following are equivalent:

(1) *There is a commutative diagram where each vertical arrow is an isomorphism*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & M' & \xrightarrow{\iota} & M' \oplus M'' & \xrightarrow{\pi} & M'' & \longrightarrow & 0. \end{array}$$

(2) *There is an isomorphism $\theta : M \xrightarrow{\cong} M' \oplus M''$ such that $\theta \circ i = \iota$ and $\pi \circ \theta = p$.*

(3) *The map i has a left inverse q in $R-\mathbf{Mod}$.*

(4) *The map p has a right inverse j in $R-\mathbf{Mod}$.*

(5) *There are maps $q : M \to M'$ and $j : M'' \to M$ such that $q \circ i = \mathrm{id}_{M'}$, $p \circ j = \mathrm{id}_{M''}$, and $i \circ q + j \circ p = \mathrm{id}_M$.*

If these equivalent conditions hold, we call the SES a split exact sequence*.*

Proof. (1) $\Leftrightarrow$ (2) follows by definition of commutative diagram.

(1) $\Rightarrow$ (5): The main idea is that there are obvious splitting maps for the bottom SES. Define π' to be the canonical projection $\pi' : M' \oplus M'' \to M', (m', m'') \mapsto m'$ and ι'' to be the inclusion $\iota'' : M'' \to M' \oplus M'', m'' \mapsto (0, m'')$. Notice that $\pi' \circ \iota = \mathrm{id}_{M'}$ and $\pi \circ \iota'' = \mathrm{id}_{M''}$ and $i \circ \pi' + \iota'' \circ p = \mathrm{id}_{M' \oplus M''}$.

Lecture of September 13, 2021

We can use this to set $q = \pi' \circ \theta$ and $j = \theta^{-1} \circ \iota''$ and check

$$\begin{aligned} q \circ i &= \pi' \circ \theta \circ i = \pi' \circ \iota = \mathrm{id}_{M'} \\ p \circ j &= p \circ \theta^{-1} \circ \iota'' = \pi \circ \iota'' = \mathrm{id}_{M''} \end{aligned}$$

$$\begin{aligned} i \circ q + j \circ p &= i \circ \pi' \circ \theta + \theta^{-1} \circ \iota'' \circ p = \theta^{-1} \circ (\theta \circ i \circ \pi' + \iota'' \circ p \circ \theta^{-1}) \circ \theta \\ &= \theta^{-1} \circ (\iota \circ \pi' + \iota'' \circ \pi) \circ \theta = \theta^{-1} \circ \mathrm{id}_{M' \oplus M''} \circ \theta = \mathrm{id}_M. \end{aligned}$$

(5) $\Rightarrow$ (3, 4) is clear.

(3) $\Rightarrow$ (2): Given such a q, define $\theta(m) = (q(m), p(m))$. It is clear $\theta \circ i = \iota$ and $\pi \circ \theta = p$. We will now show that θ is injective: if $\theta(m) = 0$ then $p(m) = 0$ so $m \in \mathrm{im}(i)$ therefore $m = i(m')$ for some $m' \in M'$. But now $0 = q(m) = q(i(m')) = m'$ so $m' = 0$ and thus $m = 0$.

We next show that θ is surjective: $(m', m'') \in M' \oplus M''$. Since p is onto, then there exists some $u \in M$ so thar $p(u) = m''$. Let $m = i(m') + u - i(q(u))$. Then

$$\begin{aligned} \theta(m) &= (q(i(m')) + q(u) - q(i(q(u))), p(i(m')) + p(u) - p(i(q(u)))) \\ &= (m' + q(u) - q(u), m'' + 0 - 0) = (m', m''). \end{aligned}$$

Therefore θ is bijective, so it is an isomorphism.

The proof that (4) $\Rightarrow$ (2) is similar, and omitted. □

We can also use splittings to show exactness.

Proposition 2.16. *Given a complex of R-modules of the form*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0,$$

if there are maps $q : M \to M'$ and $j : M'' \to M$ such that $q \circ i = \mathrm{id}_{M'}$, $p \circ j = \mathrm{id}_{M''}$, and $i \circ q + j \circ p = \mathrm{id}_M$, then the complex is exact, and hence split exact.

Proof. Since i has a left inverse, it is injective, and since p has a right inverse, it is surjective. To show exactness in the middle, let $m \in \ker(p)$. Then

$$m = (i \circ q)(m) + (j \circ p)(m) = i(q(m)) \in \mathrm{im}(i).$$ □

Remark 2.17. The proof in the previous example actually shows that, for any ring R, a SES whose right-most term is free is split exact.

Example 2.18. Here is an example of a non-split exact sequence: Take R to be any (commutative) integral domain and $r \in R$ any non-zero, non-unit element. Then, using that R is a domain, the sequence

$$0 \to R \xrightarrow{r} R \to R/r \to 0$$

is exact (where the second map is the canonical surjection). But it cannot by split exact: If it were, then we would have an isomorphism $R \cong R \oplus R/r$ of modules and so in particular there would be an ideal I of R isomorphic as a module to R/r. But then $rI = 0$ and since R is a domain, this could only happen if $I = 0$, which would mean r is a unit.

For example

$$0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2 \to 0$$

is an exact, but not split exact, sequence of $\mathbb{Z}$-modules.

Example 2.19. Suppose $R = k$ is a field. Then every short exact sequence of R-modules

$$0 \to W \to V \to V/W \to 0$$

splits.

2.2. **Homomorphisms of R-modules.**

2.2.1. *Structure of* $\mathrm{Hom}_R(M, N)$. In general, we write $\mathrm{Hom}_R(M, N)$ for the set $\mathrm{Hom}_{R-\mathbf{Mod}}(M, N)$ of R-module morphisms between two left R-modules M and N.

It turns out that the set of homomorphisms between two R-modules has additional structure.

Proposition 2.20. *Let R be a ring, and M, N be two left R-modules.*

(1) $\mathrm{Hom}_R(M, N)$ *is an abelian group by pointwise addition, i.e.,*

$$(\alpha + \beta)(m) := \alpha(m) + \beta(m) \qquad \alpha, \beta \in \mathrm{Hom}_R(M, N),\ m \in M.$$

(2) *If R is commutative, then* $\mathrm{Hom}_R(M, N)$ *is an R-module via the action*

$$(r\alpha)(m) := r\alpha(m) = \alpha(rm) \qquad \alpha \in \mathrm{Hom}_R(M, N),\ r \in R,\ m \in M.$$

(3) *More generally,*

- *if M is a (R,S)-bimodule, then $\mathrm{Hom}_R(M,N)$ is a left S-module by the action $(s\alpha)(m) = \alpha(ms)$;*
- *if N is a (R,T)-bimodule, then $\mathrm{Hom}_R(M,N)$ is a right T-module by the action $(\alpha t)(m) = \alpha(m)t$;*
- *if M is a (R,S)-bimodule and N is a (R,T)-bimodule, then $\mathrm{Hom}_R(M,N)$ is a (S,T)-bimodule by the previous two actions.*

Proof. (1) is easy to check, and similar to what we checked with module endomorphisms.

Let's consider (2): The first thing to note is that $r\alpha(m) = \alpha(rm)$ by linearity of α. Let us check that the map $r\alpha$ defined this way is an R-module morphism:

$$(r\alpha)(m+m') = r\alpha(m+m') = r(\alpha(m)+\alpha(m')) = r\alpha(m) + r\alpha(m') = r\alpha(m) + r\alpha(m')$$

$$(r\alpha)(sm) = r\alpha(sm) = rs\alpha(m) = sr\alpha(m) = s(r\alpha(m));$$

note that commutativity of R is essential here.

The distributive rules are straightforward, and $((rs)\alpha)(m) = rs\alpha(m) = (r(s\alpha))(m)$, so $(rs)\alpha = r(s\alpha)$.

For (3), let's just focus on the first case. To see $s\alpha$ is R-linear, addition is similar to above, and

$$(s\alpha)(rm) = \alpha(rms) = r\alpha(ms) = r(s\alpha)(m).$$

Let's check the associativity property for the action: given $s, s' \in S$,

$$(ss')\alpha(m) = \alpha(mss') = s'\alpha(ms) = (s(s'\alpha))(m).$$

The other axioms are straightforward. □

The bonus module structures in case (3) are often useful, even for commutative rings. However, for many statements below we will just focus on cases (1) and (2) above for clarity.

Example 2.21. Let K be a field. Since K is commutative, $\mathrm{Hom}_K(K, K[x])$ and $\mathrm{Hom}_K(K[x], K)$ are K-vector spaces. The polynomial ring $K[x]$ is a $(K, K[x])$-bimodule. This gives $\mathrm{Hom}_K(K, K[x])$ a $K[x]$-module structure by postmultiplication: e.g., if α is the K-linear map such that $\alpha(1) = f(x)$, and $g(x) \in K[x]$, then $g(x)\alpha$ is the map that sends 1 to $f(x)g(x)$. Likewise, $\mathrm{Hom}_K(K[x], K)$ a $K[x]$-module structure by premultiplication: e.g., if α is the K-linear map such that $\alpha(x^i) = \gamma_i \in K$, then $x\alpha$ is the map that sends x^i to γ_{i+1}.

Lecture of September 15, 2021

2.2.2. *Hom as functors.*

Definition 2.22 (Covariant Hom)**.** Let R be a ring and M be an R-module. There is a covariant functor

$$\mathrm{Hom}_R(M, -) : R - \mathbf{Mod} \to \mathbf{Ab}$$

that maps each module A to $\mathrm{Hom}_R(M, A)$, and each morphism $A \xrightarrow{f} B$ to the homomorphism $\mathrm{Hom}_R(M, f)$ $=: f_*$ of "postcomposition by f":

$$\begin{array}{ccc} \mathrm{Hom}_R(M,A) & \xrightarrow{f_*} & \mathrm{Hom}_R(M,B) \\ g & \longmapsto & f \circ g \\ M \xrightarrow{g} A & & M \xrightarrow{g} A \xrightarrow{f} B. \end{array}$$

If R is commutative, then we consider $\mathrm{Hom}_R(M, -)$ as a functor from $R-\mathbf{Mod} \to R-\mathbf{Mod}$ by the same rule.

There are some things to check to verify that this is a functor.

Proof. We need to check that f_* is a valid morphism in **Ab**, or in $R-$**Mod** in the commutative case. Given $g, h \in \mathrm{Hom}_R(A, B)$, we have

$$f_*(g+h)(m) = f((g+h)(m)) = f(g(m)+h(m)) = f(g(m)) + f(h(m)) = f_*(g)(m) + f_*(h)(m).$$

If R is commutative,

$$f_*(rg)(m) = f(g(rm)) = rf(g(m)) = (rf_*)(g)(m).$$

We also need to see that these satisfy the functor axioms. We have $(1_A)_*(g) = 1_A \circ g = g$, so $(1_A)_*$ is the identity map on $\mathrm{Hom}_R(M, A)$. Given $A \xrightarrow{g} B \xrightarrow{f} C$, and $h \in \mathrm{Hom}_R(M, A)$,

$$(fg)_*(h) = f \circ g \circ h = f \circ (g_*(h)) = f^*(g^*(h)) = (f_* \circ g_*)(h). \qquad \square$$

Remark 2.23. If M is an (R, S)-bimodule, then consider $\mathrm{Hom}_R(M, -)$ as a functor from $R-$**Mod** $\to S-$**Mod** by the same rule.

Definition 2.24 (Contravariant Hom)**.** Let R be a ring and M be an R-module. There is a contravariant functor

$$\mathrm{Hom}_R(-, M) : R - \mathbf{Mod} \to \mathbf{Ab}$$

that maps each module A to $\mathrm{Hom}_R(A, M)$, and each morphism $A \xrightarrow{f} B$ to the homomorphism $\mathrm{Hom}_R(f, M)$ $=: f^*$ of "precomposition by f":

$$\begin{array}{ccc} \mathrm{Hom}_R(M, B) & \xrightarrow{f_*} & \mathrm{Hom}_R(M, A) \\ g & \longmapsto & g \circ f \\ B \xrightarrow{g} M & & A \xrightarrow{f} B \xrightarrow{g} M. \end{array}$$

If R is commutative, then we consider $\mathrm{Hom}_R(-, M)$ as a functor from $R - \mathbf{Mod} \to R - \mathbf{Mod}$ by the same rule.

There are some things to check to verify that this is a functor.

Proof. We need to check that f^* is a valid morphism in **Ab**, or in $R-$**Mod** in the commutative case. Given $g, h \in \mathrm{Hom}_R(A, B)$, we have

$$f^*(g+h)(m) = (g+h)(f(m)) = g(f(m)) + h(f(m)) = f^*(g)(m) + f^*(h)(m).$$

If R is commutative,

$$f^*(rg)(m) = rg(f(m)) = (rf^*(g))(m).$$

We also need to see that these satisfy the functor axioms. We have $(1_A)^*(g) = g \circ 1_A = g$, so $(1_A)^*$ is the identity map on $\mathrm{Hom}_R(A, M)$. Given $A \xrightarrow{g} B \xrightarrow{f} C$, and $h \in \mathrm{Hom}_R(C, M)$,

$$(fg)^*(h) = h \circ f \circ g = f^*(h) \circ g = g^*(f^*(h)) = (g^* \circ f^*)(h). \qquad \square$$

Remark 2.25. If M is an (R, S)-bimodule, then consider $\mathrm{Hom}_R(M, -)$ as a functor from $R - \mathbf{Mod} \to S^{\mathrm{op}} - \mathbf{Mod}$ by the same rule.

2.2.3. *Examples of Hom.*

Example 2.26. Let R be a ring. Then, by the universal property of free modules, since $\{1\}$ is a free basis for R as an R-module, the map

$$\begin{aligned} \mathrm{Hom}_R(R, M) &\xrightarrow{\psi_M} M \\ \phi &\longmapsto \phi(1) \end{aligned}$$

is a bijection. Moreover, this is an isomorphism of abelian groups in general, and of R-modules in the commutative case:

$$\psi_M(\alpha + \beta) = (\alpha + \beta)(1) = \alpha(1) + \beta(1) = \psi_M(\alpha) + \psi_M(\beta)$$
$$\psi_M(r\alpha) = (r\alpha)(1) = r\alpha(1) = r\psi_M(\alpha).$$

Even better, in the commutative case, the collection of isomorphisms ψ_M form a natural isomorphism $\psi : \mathrm{Hom}_R(R, -) \Rightarrow 1_{R-\mathbf{Mod}}$. For this, we need to check that, given $\beta : M \to N$, the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Hom}_R(R, M) & \xrightarrow{\beta_*} & \mathrm{Hom}_R(R, N) \\ \downarrow{\scriptstyle \psi_M} & & \downarrow{\scriptstyle \psi_N} \\ M & \xrightarrow{\beta} & N. \end{array}$$

Along either path, we get $\alpha \mapsto \beta(\alpha(1))$, so this is indeed the case.

Lecture of September 17, 2021

Example 2.27. Similarly, if $F = R^{\oplus\Lambda}$ is a free module, then $\mathrm{Hom}_R(R^{\oplus\Lambda}, M) \cong M^{\oplus\Lambda}$, where $M^{\times\Lambda} = \prod_{\lambda\in\Lambda} M$ by the map that sends a morphism to its tuple of values on the standard basis: as abelian groups, and as R-modules in the commutative case.

We can interpret the right-hand side as the values of a functor: set $F(M) = M^{\times\Lambda}$, and for $f : M \to N$, set $F(f)$ to be the map given by f on each coordinate. Interpreted like so, the isomorphisms again form a natural isomorphism.

Proposition 2.28. *Let $\{M_\lambda\}_{\lambda\in\Lambda}$ be a family of R-modules, and N be an R-module. There are isomorphisms of abelian groups*

$$\mathrm{Hom}_R(\bigoplus_{\lambda\in\Lambda} M_\lambda, N) \cong \prod_{\lambda\in\Lambda} \mathrm{Hom}_R(M_\lambda, N)$$
$$\mathrm{Hom}_R(N, \prod_{\lambda\in\Lambda} M_\lambda) \cong \prod_{\lambda\in\Lambda} \mathrm{Hom}_R(N, M_\lambda)$$

Moreover, these are isomorphisms of R-modules if R is commutative.

Proof. Since $\bigoplus_{\lambda\in\Lambda} M_\lambda$ is the coproduct of $\{M_\lambda\}_{\lambda\in\Lambda}$ in $R-\mathbf{Mod}$, we have a bijection for every R-module N

$$\begin{aligned} \mathrm{Hom}_R(\textstyle\bigoplus_{\lambda\in\Lambda} M_\lambda, N) &\longrightarrow \prod_{\lambda\in\Lambda} \mathrm{Hom}_R(M_\lambda, N) \\ \phi &\longmapsto (\phi \circ \iota_\lambda). \end{aligned}$$

We only have to observe that these maps preserve the abelian group and/or R-module structures. Similarly, since $\prod_{\lambda\in\Lambda} M_\lambda$ is the product of $\{M_\lambda\}_{\lambda\in\Lambda}$ in $R-\mathbf{Mod}$, we have a bijection for every R-module N

$$\begin{aligned} \mathrm{Hom}_R(N, \textstyle\prod_{\lambda\in\Lambda} M_\lambda) &\longrightarrow \prod_{\lambda\in\Lambda} \mathrm{Hom}_R(N, M_\lambda) \\ \phi &\longmapsto (\pi_\lambda \circ \phi), \end{aligned}$$

and one verifies the additivity / linearity of this map. □

Example 2.29. As an important special case of the previous example, if R is commutative, and $R^{\oplus\Gamma}$ and $R^{\oplus\Lambda}$ are free modules, then every R-linear homomorphism $\alpha : R^{\oplus\Gamma} \to R^{\oplus\Lambda}$ is given by left multiplication by the (possibly infinite) $\Lambda \times \Gamma$ matrix where the γ column is the Λ-tuple $(\alpha(e_\gamma))_\lambda$.

Optional Exercise 2.30. Show that when R is not necessarily commutative, if we give $\mathrm{Hom}_R(R^{\oplus\Lambda}, M)$ the R-module structure via the (R, R)-bimodule structure on $R^{\oplus\Lambda}$, the isomorphisms $\mathrm{Hom}_R(R^{\oplus\Lambda}, M) \cong M^{\times\Lambda}$ are natural isomorphisms of R-modules.

Example 2.31. Let R be a commutative ring, and consider the module R/I for some ideal I. For every module M, there is an isomorphism $\mathrm{Hom}_R(R/I, M) \cong \mathrm{ann}_M(I)$, where $\mathrm{ann}_M(I)$ is the set of elements $m \in M$ such that $Im = 0$.

Indeed, every R-module homomorphism from R/I is determined by the image of 1, so the map $\mathrm{Hom}_R(R/I, M) \to M$ of evaluation at 1 is injective. The image consists of the set of elements $m \in M$ for which the map $r \mapsto rm$ is well-defined; this is the collection of elements that satisfy $Im = 0$.

Again, we can think of the right hand side as a functor $F : R - \mathbf{Mod} \to R - \mathbf{Mod}$ where on objects $F(M) = \mathrm{ann}_M(I)$, and on morphisms $M \xrightarrow{\alpha} N$ maps to the restriction of α to $\mathrm{ann}_M(I)$. This is a natural isomorphism again.

Example 2.32. For a field K, the functor $\mathrm{Hom}_K(-, K)$ is exactly the "vector space dual" functor $(-)^*$.

2.3. **Exact functors and left exactness of Hom.**

Definition 2.33. Let R, S be rings. A covariant functor $F : R-\mathbf{Mod} \to S-\mathbf{Mod}$ is *additive* if the function

$$\begin{aligned} \mathrm{Hom}_R(M, N) &\longrightarrow \mathrm{Hom}_S(F(M), F(N)) \\ f &\longmapsto F(f) \end{aligned}$$

is a homomorphism of abelian groups. Likewise, a contravariant functor $G : R - \mathbf{Mod} \to S - \mathbf{Mod}$ is additive if the function

$$\begin{aligned} \mathrm{Hom}_R(M, N) &\longrightarrow \mathrm{Hom}_S(F(N), F(M)) \\ f &\longmapsto F(f) \end{aligned}$$

is a homomorphism of abelian groups.

Additive functors preserve a number of basic properties, e.g., zero morphisms go to zero morphisms, and the zero module maps to the zero module (since it's characterized by the fact that its identity map is its zero map).

Optional Exercise 2.34. The covariant and contravariant Hom functors are additive functors.

Definition 2.35. Let $F : R - \mathbf{Mod} \to S - \mathbf{Mod}$ be an additive covariant functor.

- F is *right exact* if whenever
$$M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$
is exact, then so is
$$F(M') \xrightarrow{F(i)} F(M) \xrightarrow{F(p)} F(M'') \to 0.$$
(Recall $F(0) = 0$ since F is additive.)
- F is *left exact* if whenever
$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$$

is exact, then so is

$$0 \to F(M') \xrightarrow{F(i)} F(M) \xrightarrow{F(p)} F(M'').$$

- F is *exact* if it is both left and right exact.

Remark 2.36. An exact functor takes any SES to a SES.

Definition 2.37. Let $G : R - \mathbf{Mod} \to S - \mathbf{Mod}$ be an additive contravariant functor.

- G is *right exact* if whenever

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M''$$

is exact, then so is

$$G(M'') \xrightarrow{G(p)} G(M) \xrightarrow{G(i)} G(M') \to 0.$$

- G is *left exact* if whenever

$$M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

is exact, then so is

$$0 \to G(M'') \xrightarrow{G(p)} G(M) \xrightarrow{G(i)} G(M').$$

- G is *exact* if it is additive and both left and right exact.

Optional Exercise 2.38. The definitions above all stay unchanged if for each condition we start with a short exact sequence. For example, a covariant additive functor F is left exact if for every short exact sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

of R-modules,

$$0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$$

is exact.

Remark 2.39. If $F, G : R - \mathbf{Mod} \to S - \mathbf{Mod}$ are naturally isomorphic additive functors, then F is exact if and only if G is exact. Indeed, given a short exact sequence

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F(M') & \xrightarrow{F(i)} & F(M) & \xrightarrow{F(p)} & F(M'') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \theta'} & & \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta''} & & \\ 0 & \longrightarrow & G(M') & \xrightarrow{G(i)} & G(M) & \xrightarrow{G(p)} & G(M'') & \longrightarrow & 0 \end{array}$$

where $\theta', \theta, \theta''$ isomorphisms. Then if the top row is exact, $G(i) = \theta F(i)(\theta')^{-1}$ is injective, $G(p) = \theta'' F(p)\theta^{-1}$ is surjective, and

$$x \in \ker G(p) = \ker(\theta'' F(p)\theta^{-1}) \iff \theta^{-1}(x) \in \ker F(p) \iff \theta^{-1}(x) \in \operatorname{im} F(i) \iff x \in \operatorname{im}(\theta F(i)(\theta')^{-1}) = \operatorname{im} G(i).$$

Similarly for "left exact" or "right exact".

Theorem 2.40. *Let M be an R-module.*

(1) *The functor $\operatorname{Hom}_R(M, -)$ is left exact.*
(2) *The functor $\operatorname{Hom}_R(-, M)$ is left exact.*

Lecture of September 20, 2021

Proof. (1) Let

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C$$

be exact. We need to show that

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

is exact.

- i_* is injective: Let $f \in \mathrm{Hom}_R(M, A)$ be nonzero, so $f(m) \neq 0$ for some $m \in M$. Then $i_*(f)(m) = i(f(m)) \neq 0$ since i is injective, so $i_*(f) \in \mathrm{Hom}_R(M, B)$ is nonzero.
- $\mathrm{im}(i_*) \subseteq \ker(p_*)$: Let $g \in \mathrm{Hom}_R(M, B)$ be in the image of i_*, so we can write $g = i_*(f)$ for some $f \in \mathrm{Hom}_R(M, A)$. We have $p_*(i_*(f)) = p \circ i \circ f = 0$.
- $\ker(p_*) \subseteq \mathrm{im}(i_*)$: Let $g \in \mathrm{Hom}_R(M, B)$ be in the kernel of p_*, so $p \circ g = 0$. Then, for every $m \in M$, $g(m) \in \ker(p) = \mathrm{im}(i)$. As i is injective, i induces an isomorphism from i to the image of A in B, so there is an R-module homomorphism $q : \mathrm{im}(A) \to A$ such that $i \circ q = 1_{\mathrm{im}(A)}$. Thus, we obtain an R-module map $f := q \circ g : M \to A$ such that $i_*(f) = i \circ q \circ g = g$.

(2) Let

$$A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

be exact. We need to show that

$$0 \to \mathrm{Hom}_R(C, M) \xrightarrow{p^*} \mathrm{Hom}_R(B, M) \xrightarrow{i^*} \mathrm{Hom}_R(A, M)$$

is exact.

- p^* is injective: Let $f \in \mathrm{Hom}_R(C, M)$ be nonzero, so $f(c) \neq 0$ for some $m \in M$. Then, since p is surjective, there is some $b \in B$ such that $p(b) = c$, and hence $p^*(f)(b) = f(p(b)) = f(c) \neq 0$, so $p^*(f) \neq 0$.
- $\mathrm{im}(p^*) \subseteq \ker(i^*)$: Let $g \in \mathrm{Hom}_R(B, M)$ be in the image of p_*, so we can write $g = p^*(f)$ for some $f \in \mathrm{Hom}_R(M, C)$. We have $i^*(p^*(f)) = f \circ p \circ i = 0$.
- $\ker(i^*) \subseteq \mathrm{im}(p^*)$: Let $g \in \mathrm{Hom}_R(B, M)$ be in the kernel of i^*, so $g \circ i = 0$. Thus, as $g|_{\mathrm{im}(i)} = 0$, we can factor $g = \overline{g} \circ \pi$, where $\pi : B \to B/\mathrm{im}(i) = B/\ker(p)$ is the quotient map, and $\overline{g} : B/\mathrm{im}(i) \to M$. Note that, since p is surjective, writing $p = \overline{p} \circ \pi$, the map $\overline{p} : B/\mathrm{im}(i) = B/\ker(p) \to C$ is an isomorphism, so there is a map $j : C \to B/\ker(p)$ such that $j \circ \overline{p}$ is the identity on $B/\mathrm{im}(i)$, so $j \circ p = j \circ \overline{p} = \circ \pi = \pi$. Set $f = \overline{g} \circ j$. We then have $p^*(f) = \overline{g} \circ j \circ p = \overline{g} \circ \pi = g$. Thus $g \in \mathrm{im}(p^*)$. □

Example 2.41. Neither Hom functor is exact. For example, consider the short exact sequence

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

If we apply $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$ to this sequence, we get

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

This is exact up until $\mathbb{Z}/2\mathbb{Z}$ (which agrees with the left exactness), but not at $\mathbb{Z}/2\mathbb{Z}$. Likewise, apply $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/2\mathbb{Z})$ to get

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{1} \mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \to 0.$$

This is again exact up to the last $\mathbb{Z}/2\mathbb{Z}$, but not there.

We can use left exactness to compute various Hom modules.

Example 2.42. Let R be commutative, and M be a finitely presented R-module with presentation

$$R^m \xrightarrow{A\cdot} R^n \to M \to 0.$$

Then $\mathrm{Hom}_R(M,R)$ sits in a left exact sequence

$$0 \to \mathrm{Hom}(M,R) \to \mathrm{Hom}_R(R^n,R) \xrightarrow{\mathrm{Hom}_R(A\cdot,R)} \mathrm{Hom}_R(R^m,R).$$

We have $\mathrm{Hom}_R(R^n,R)$ is free with free basis given by the coordinate functions $\{e_1^*,\dots,e_n^*\}$; likewise for $\mathrm{Hom}_R(R^m,R)$ with basis $\{\bar{e}_1^*,\dots,\bar{e}_m^*\}$ (we will write bars for basis elements in R^m). In these bases, to compute the jth column of the matrix, we have that e_j^* maps to e_j^*A, and to compute e_j^*A in terms of the given basis (to find the entry in the ith row), we observe $(e_j^*A)(\bar{e}_i)$ is A_{ji}, so the map $\mathrm{Hom}_R(A\cdot,R)$ is given by $A^T\cdot$. We get a left exact sequence

$$0 \to \mathrm{Hom}(M,R) \to R^n \xrightarrow{A^T\cdot} R^m,$$

so $\mathrm{Hom}(M,R) \cong \ker(A^T)$.

2.4. **Tensor products.**

Lecture of September 22, 2021

2.4.1. *Definition of tensor product.*

Definition 2.43. For a ring R, a right R-module M, a left R-module N, and an abelian group A, a function

$$b : M \times N \to A$$

is called *R-balanced biadditive* if the following conditions hold:

(1) $b(m+m',n) = b(m,n) + b(m',n)$ for all $m,m' \in M$, $n \in N$,
(2) $b(m,n+n') = b(m,n) + b(m,n')$ for all $m \in M$, $n,n' \in N$, and
(3) $b(mr,n) = b(m,rn)$ for all $m \in M$, $n, \in N$, and $r \in R$.

Assume R is commutative and A is an R-module (not just an abelian group). Such a pairing b is called *R-bilinear* if we also have

(4) $b(mr,n) = b(m,rn) = rb(m,n)$ for all $m \in M$, $n, \in N$, and $r \in R$.

Conditions (1) and (2) alone are the biadditive part, and condition (3) is the balancedness. Condition (4) says that the biadditive map b is an R-linear function in either argument if we fix the other one.

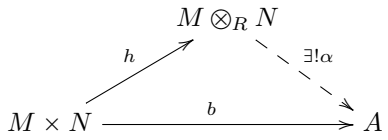
Example 2.44.
(1) If R is any ring, the map $f : R \times R \to R, f(r,s) = rs$ is R-balanced biadditive, and bilinear if R is commutative.
(2) For R commutative, an ideal I, and a left module M, the map $f : (R/I) \times M \to M/IM, f(\overline{r},m) = \overline{rm}$ is R-bilinear.
(3) For K a field, $f : K^n \times K^n \to K$ given by the usual dot product is K-bilinear. Recall that we can view K^n as a right $M_n(K)$ module via $v \cdot A = A^T v$ and as a left $M_n(K)$ module via $A \cdot v = Av$. With these structures, f is $M_n(K)$-balanced biadditive. The balanced part is the least obvious one:

$$f(v \cdot A, w) = (A^T v) \cdot w = v^T A w = v \cdot (Aw) = f(v, A \cdot w).$$

We now define tensor products using a universal property.

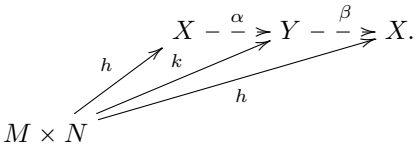
Definition 2.45. Let R be a (not necessarily commutative) ring, let M be a right R-module, let N be a left R-module.

An abelian group $M \otimes_R N$ together with an R-balanced biadditive map $h : M \times N \to M \otimes_R N$ is called a *tensor product* of M and N if it has the following universal property: for any abelian group A and R-balanced biadditive map $b : M \times N \to A$, there exists a unique abelian group homomorphism $\alpha : M \otimes_R N \to A$ such that $b = \alpha \circ h$.



Lemma 2.46. *If (X, h), (Y, k) are two tensor products for M and N, then there is a unique isomorphism of abelian groups $\alpha : X \to Y$ such that $k = \alpha \circ h$.*

Proof. The following diagram is a rough guide for the argument:



Applying the universal property of (X, h) with the R-balanced biadditive map k, we get a unique abelian group homomorphism α above that makes its triangle commute; in particular, the uniqueness statement is clear. Likewise, applying the universal property of (Y, k) with h, we get an abelian group homomorphism β that makes its triangle commute. Then, $\beta \circ \alpha$ is an abelian group homomorphism such that $(\beta \circ \alpha) \circ h = h$, and the identity map is another. By the uniqueness property of (X, h), $\beta \circ \alpha$ is the identity. A similar argument shows that $\alpha \circ \beta$ is the identity too, so α is an isomorphism. □

Theorem 2.47. *Let R be a (not necessarily commutative) ring, let M be a right R-module, let N be a left R-module. Then a tensor product $M \otimes_R N$ exists and is given by defining an abelian group $M \otimes_R N$ by generators and relations as follows:*

- *The generators are all expressions of the form $m \otimes n$ for $m \in M$ and $n \in N$.*
- *The relations are*
  1. *$(m + m') \otimes n = m \otimes n + m' \otimes n$ for all $m, m' \in M$ and $n \in N$,*
  2. *$m \otimes (n + n') = m \otimes n + m \otimes n'$ for all $m \in M$ and $n, n' \in N$, and*
  3. *$(mr) \otimes n = m \otimes (rn)$ for all $m \in M$, $n \in N$, and $r \in R$.*

Equivalently, $M \otimes_R N$ is the quotient

$$\frac{\bigoplus_{(m,n) \in M \times N} \mathbb{Z} \cdot (m \otimes n)}{(Y)}$$

where

$$Y = \{(m + m') \otimes n) - m \otimes n - m' \otimes n\} \cup \{m \otimes (n + n') - m \otimes n - m \otimes n'\} \cup \{(mr) \otimes n - m \otimes (rn)\}.$$

Further we define $h : M \times N \to M \otimes_R N$ to be the function $h(m, n) = m \otimes n$.

Then the pair $(M \otimes_R N, h)$ defined above is the tensor product of M and N.

Proof. It is immediate from the construction that h is R-balanced biadditive. Given a biadditive map $b : M \times N \to A$, define $\tilde{b} : \bigoplus_{(m,n)\in M\times N} \mathbb{Z} \cdot (m \otimes n) \to A$ to be the unique homomorphism of abelian groups sending the basis element $m \otimes n$ to $b(m, n)$. Since b is biadditive, we have

$$\tilde{b}((m + m') \otimes n - m \otimes n - m' \otimes n) = b(m + m', n) - b(m, n) - b(m', n) = 0,$$

$$\tilde{b}(m \otimes (n + n') - m \otimes n - m \otimes n) = b(m, n + n') - b(m, n) - b(m, n') = 0,$$

and

$$\tilde{b}((mr) \otimes n - m \otimes (rn)) = b(mr, n) - b(m, rn) = 0.$$

Thus $\tilde{b}(< Y >) = 0$ and so it induces a homomorphism of abelian groups

$$\alpha : M \otimes_R N \to A.$$

It is evident from the construction that $\alpha \circ h = b$. Since the image of B generates $M \otimes_A N$ as an abelian group, α is the unique homomorphism satisfying this equation.

If β is any abelian group homomorphism with $\beta \circ h = b$, we have $\beta(m \otimes n) = \beta(h(m, n)) = b(m, n) = \alpha(m \otimes n)$. Since the elements of the form $m \otimes n$ generate $M \otimes_R N$ as an abelian group, we must have $\beta = \alpha$. □

Note that the map induced by a biadditive map b sends $m \otimes n \mapsto b(m, n)$.

Remark 2.48. In this explicit construction, every element is a *sum* of *simple tensors* (elements of the form $m \otimes n$) but in general, not every element is itself a simple tensor.

Remark 2.49. While the construction of tensor products may feel easier to work with at first, it is important to keep in mind that it is hard to tell when two combinations of simple tensors are equal. In general, when we want to define a map from a tensor product, it is better to use the universal property, since we don't have to worry about well-definedness. However, to define a map into a tensor product, using the concrete description is often easier.

Optional Exercise 2.50. In $M \otimes_R N$ we have $0_M \otimes n = 0_{M\otimes_R N} = m \otimes 0_N$ for each $m \in M, n \in N$.

Lecture of September 24, 2021

Example 2.51. I claim $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/g\mathbb{Z}$ where $g = \gcd(m, n)$.

Proof. Define a function

$$b : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/g\mathbb{Z}$$

by $b(\bar{i}, \bar{j}) = \overline{ij}$. It is not hard to see that b is well-defined (exercise!) and $\mathbb{Z}$-balanced biadditive. By the universal property, it therefore induces a homomorphism of abelian groups

$$\alpha : \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/g\mathbb{Z}$$

such that $\alpha(\bar{i} \otimes \bar{j}) = \overline{ij}$.

Now define a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ by sending 1 to $1 \otimes 1$. Notice that

$$\phi(g) = g \cdot (1 \otimes 1) = g \otimes 1 = 1 \otimes g.$$

Recall that $g = im + jn$ for some $i, j \in \mathbb{Z}$. So

$$g \otimes 1 = im \otimes 1 + 1 \otimes jn = 0 \otimes 1 + 1 \otimes 0 = 0 + 0 = 0.$$

So, ϕ induces a homomorphism

$$\beta = \overline{\phi} : \mathbb{Z}/g\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$$

with $\beta(\bar{i}) = \bar{i} \otimes 1 = 1 \otimes \bar{i}$.

We have $\alpha(\beta(\bar{i})) = \alpha(\bar{i} \otimes 1) = \bar{i}$ so that $\alpha \circ \beta = \mathrm{id}$.

A typical element of $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$ has the form $\sum_t \overline{i_t} \otimes \overline{j_t}$. We have

$$\beta(\alpha(\sum_t \overline{i_t} \otimes \overline{j_t})) = \sum_t \overline{i_t} \cdot \overline{j_t} \otimes 1 = \sum_t \overline{i_t} \otimes \overline{j_t}$$

and so $\beta \circ \alpha = \mathrm{id}$. □

2.4.2. *Module structure of tensor product.*

Proposition 2.52. (1) *If R is commutative, and M and N are R-modules, then*

(a) *$M \otimes_R N$ is an R-module via the action*

$$r \cdot (\sum_i m_i \otimes n_i) = \sum_i (rm_i) \otimes n_i = \sum_i m_i \otimes (rn_i).$$

(b) *The natural map $h : M \times N \to M \otimes_R N$ is R-bilinear.*

(c) *For any R-module A and R-bilinear map $b : M \times N \to A$, there is a unique R-module homomorphism $\alpha : M \otimes_R N \to A$ such that $b = \alpha \circ h$.*

(2) *If M is an (S, R)-bimodule, and N is an R-module, then consider $M \times N$ as an S-module by the action $s(m, n) = (sm, n)$. We have*

(a) *$M \otimes_R N$ is an S-module via the action*

$$s \cdot (\sum_i m_i \otimes n_i) = \sum_i (sm_i) \otimes n_i.$$

(b) *The natural map $h : M \times N \to M \otimes_R N$ is S-linear.*

(c) *For any S-module A and S-linear R-balanced biadditive map $b : M \times N \to A$, there is a unique S-module homomorphism $\alpha : M \otimes_R N \to A$ such that $b = \alpha \circ h$.*

(3) *If M is an R-module, and N is an (R, S)-bimodule, then consider $M \times N$ as a right S-module by the action $(m, n)s = (m, ns)$. We have*

(a) *$M \otimes_R N$ is a right S-module via the action*

$$s \cdot (\sum_i m_i \otimes n_i) = \sum_i m_i \otimes (n_i s).$$

(b) *The natural map $h : M \times N \to M \otimes_R N$ is right S-linear.*

(c) *For any right S-module A and right S-linear R-balanced biadditive map $b : M \times N \to A$, there is a unique right S-module homomorphism $\alpha : M \otimes_R N \to A$ such that $b = \alpha \circ h$.*

Proof. Let's consider case (2).

For (a), the first thing we need to show that the action of an element $s \in S$ on $M \otimes_R N$ is a well-defined function. To do this, consider the map $\mu_s : M \times N \to A$ given by the rule $\mu_s(m, n) = sm \otimes n$. We claim that this is R-balanced biadditive. Indeed,

$$\mu_s(m + m', n) = (s(m + m')) \otimes n = (sm + sm') \otimes n = sm \otimes n + sm' \otimes n = \mu_s(m, n) + \mu_s(m', n),$$

similarly $\mu_s(m, n + n') = \mu_s(m, n) + \mu_s(m, n')$, and

$$\mu_s(mr, n) = smr \otimes n = sm \otimes rn = \mu_s(m, rn).$$

Thus, we obtain a well-defined map $M \otimes_R N \to M \otimes_R N$ that sends $m \otimes n \mapsto sm \otimes n$, and the given formula follows. It is easy to check that this action satisfies the module axioms.

For (b), we already know this map is additive. To see that it is S-linear, we compute

$$h(s(m,n)) = h(sm,n) = sm \otimes n = s(m \otimes n) = sh(m,n).$$

For (c), we know that since f is R-balanced biadditive map there exists a unique additive map α such that $b = \alpha \circ h$. We just need to show that this map is S-linear:

$$\alpha(s(\sum_i m_i \otimes n_i)) = \alpha(\sum_i sm_i \otimes n_i) = \sum_i \alpha(sm_i \otimes n_i) = \sum_i \alpha(h(sm_i, n_i))$$
$$= \sum_i b(sm_i, n_i) = s(\sum_i b(m_i, n_i)) = s(\sum_i \alpha(m_i \otimes n_i)) = s(\alpha(\sum_i m_i \otimes n_i)).$$

Case (3) is quite analogous. Case (1) is a special case of (2): we consider M as an (R,R)-bimodule. The extra equality in (a) follows from $rm \otimes n = mr \otimes n = m \otimes rn$. For (b) and (c), we note that R-bilinear is equivalent to R-balanced biadditive plus R-linear with respect to the module structure given in case (2). □

We can take tensor products of maps as well.

Lemma 2.53. *Let $f : M \to M'$ be a homomorphism of right R-modules and $g : N \to N'$ be a homomorphism of left R-modules. There exists a unique homomorphism of abelian groups $f \otimes g : M \otimes_R N \to M' \otimes_R N'$ such that*

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

for all $m \in M$ and $n \in N$.

If R is commutative, this map is R-linear.

If M and M' are (S,R)-bimodules, and f is also S-linear, then this map is an S-module homomorphism.

Proof. The function

$$M \times N \longrightarrow M' \otimes_R N'$$

$$(m,n) \longmapsto f(m) \otimes g(n)$$

is R-balanced biadditive (and bilinear when R is commutative), so the universal property of tensor products gives the desired R-module homomorphism, which is unique. In the bimodule case, S-linearity follows from observing that the function displayed above is S-linear on the first argument. □

Definition 2.54. Let R be a ring and M be a right R-module. There is an additive covariant functor

$$M \otimes_R - : R - \mathbf{Mod} \to \mathbf{Ab}$$

that on objects sends N to $M \otimes_R N$, and on morphisms sends $f : N \to N'$ to the map $1_M \otimes f$.

If R is commutative, we can consider $M \otimes_R -$ as a functor from $R - \mathbf{Mod} \to R - \mathbf{Mod}$.

If M is a (S,R)-bimodule, we can consider $M \otimes_R -$ as a functor from $R - \mathbf{Mod} \to S - \mathbf{Mod}$.

Proof. Well definedness of the maps comes from the lemma. Given $A \xrightarrow{g} B \xrightarrow{f} C$, we have

$$(1_M \otimes (fg))(m \otimes a) = m \otimes (fg)(a) = (1_M \otimes f)(1_M \otimes g)(m \otimes a),$$

so $(1_M \otimes (fg)) - (1_M \otimes f)(1_M \otimes g)$ vanishes on a generating set for $M \otimes_R A$, and hence is zero. Similarly for the identity property.

For additivity, we observe that

$$(1_M \otimes (f+g))(m \otimes n) = m \otimes (f+g)(n) = m \otimes f(n) + m \otimes g(n) = ((1_M \otimes f) + (1_M \otimes g))(m \otimes n),$$

and since simple tensors generate, we have $1_M \otimes (f+g) = 1_M \otimes f + 1_M \otimes g$. □

Remark 2.55. We can equally well discuss $- \otimes_R N : R^{\mathrm{op}} - \mathbf{Mod} \to \mathbf{Ab}$ (or other targets when we have more structure akin to above).

Lecture of September 27, 2021

The key to unlocking more examples of tensor will be to prove that it is right exact.

Theorem 2.56. *Let M be a right R-module. The functor $M \otimes_R - : R - \mathbf{Mod} \to \mathbf{Ab}$ is right exact.*

Proof. Let

$$A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

be exact. We need to show that

$$M \otimes_R A \xrightarrow{1_M \otimes i} M \otimes_R B \xrightarrow{1_M \otimes p} M \otimes_R C \to 0$$

is exact.

- $1_M \otimes p$ is surjective: Given $\sum_i m_i \otimes c_i \in M \otimes_R C$, we can find $b_i \in B$ such that $p(b_i) = c_i$ for all i; then $(1_M \otimes p)(\sum_i m_i \otimes b_i) = \sum_i m_i \otimes c_i$.
- $\operatorname{im}(1_M \otimes i) \subseteq \ker(1_M \otimes p)$: We have $(1_M \otimes p)(1_M \otimes i) = 1_M \otimes (pi) = 1_M \otimes 0 = 0$.
- $\ker(1_M \otimes p) \subseteq \operatorname{im}(1_M \otimes i)$: From above, the map $1_M \otimes p$ induces a surjection $\alpha : (M \otimes_R B)/\operatorname{im}(1_M \otimes i) \to M \otimes_R C$ that maps $m \otimes b \mapsto m \otimes p(b)$. We will construct an inverse for this map.

  Consider the map

  $$\begin{aligned} \mu : M \times C &\longrightarrow (M \otimes_R B)/\operatorname{im}(1_M \otimes i) \\ (m, c) &\longmapsto m \otimes b \qquad \text{for some } b \text{ with } p(b) = c. \end{aligned}$$

  To see this is well-defined, note that if $p(b) = p(b') = c$, then $p(b - b') = 0$, so $b - b' = i(a)$ for some $a \in A$, so

  $$(m \otimes b) - (m \otimes b') = m \otimes (b - b') = m \otimes i(a) \in \operatorname{im}(1_M \otimes i).$$

  We then check μ is R-balanced biadditive:

  $$\mu(m + m', c) = (m + m') \otimes b = m \otimes b + m' \otimes b = \mu(m, c) + \mu(m', c).$$

  If $p(b) = c$ and $p(b') = c'$, then $p(b + b') = c + c'$, so

  $$\mu(m, c + c') = m \otimes (b + b') = m \otimes b + m \otimes b' = \mu(m, c) + \mu(m, c'),$$

  and, if $p(b) = c$, then $p(rb) = rc$, so

  $$\mu(mr, c) = mr \otimes b = m \otimes rb = \mu(m, rc).$$

  Thus, μ induces an additive homomorphism $\beta : M \otimes_R C \to (M \otimes_R B)/\operatorname{im}(1_M \otimes i)$. By construction, we have $\beta \circ \alpha(m \otimes b) = m \otimes b$ for all simple tensors, and thus this is the identity map since simple tensors generate.

  Since α has a left inverse, it follows that α is injective, so $\operatorname{im}(1_M \otimes i)$ is equal to the kernel of $1_M \otimes p$. □

2.4.3. *Examples of tensors.*

Proposition 2.57. *Let R be a ring. There is a natural isomorphism between $R\otimes_R -$ and the identity functor on $R-\mathbf{Mod}$. In particular, for every R-module M, there is an R-module isomorphism $R\otimes_R M\cong M$ for every (left) R-module M.*

Proof. Note that R is an (R,R)-bimodule, so $R\otimes_R M$ is again an R-module. Now,

$$R\times M \longrightarrow M$$
$$(r,m)\longmapsto rm$$

is biadditive (by distributive laws), R-balanced (by associativity module axiom), and R-linear, so it induces a homomorphism of R-modules $R\otimes_R M \xrightarrow{\varphi_M} M$. By construction, φ_M is surjective. Moreover, the map

$$M \xrightarrow{f_M} R\otimes_R M$$
$$m\longmapsto 1\otimes m$$

is a homomorphism of R-modules, since

$$f_M(a+b)=1\otimes(a+b)=1\otimes a+1\otimes b$$
$$f_M(ra)=1\otimes(ra)=r\otimes a=r(1\otimes a)=rf_M(a).$$

For every $m\in M$, $\varphi_M f_M(m)=\varphi_M(1\otimes m)=1m=m$, and for every simple tensor, $f_M\varphi_M(r\otimes m)=f_M(rm)=1\otimes(rm)=r\otimes m$. This shows that φ_M is an isomorphism.

Finally, given any $f\in \mathrm{Hom}_R(M,N)$, since f is R-linear we conclude that the diagram

$$\begin{array}{ccc} R\otimes_R M & \xrightarrow{\varphi_M} & M \\ {\scriptstyle 1\otimes f}\downarrow & & \downarrow{\scriptstyle f} \\ R\otimes N & \xrightarrow[\varphi_N]{} & N \end{array}$$

commutes, as $r\otimes m\mapsto rf(m)$ either way, so our isomorphism is natural. □

Proposition 2.58. *Let R be a ring, $\{M_\lambda\}_{\lambda\in\Lambda}$ be a family of right R-modules, N be a left R-module. There is an isomorphism*

$$\phi:\left(\bigoplus_{\lambda\in\Lambda} M_\lambda\right)\otimes_R N \xrightarrow{\cong} \bigoplus_{\lambda\in\Lambda}(M_\lambda\otimes_R N)$$

that sends $(m_i)_{i\in I}\otimes n$ to $(m_i\otimes n)_{i\in I}$. This is an isomorphism of abelian groups in general, of R-modules in the commutative case, of S-modules if each M_λ is an (S,R)-bimodule, and of right S-modules if N is an (R,S)-bimodule.

Proof. Define

$$b:\left(\bigoplus_{\lambda\in\Lambda} M\right)\times N\to \bigoplus_{\lambda\in\Lambda}(M_\lambda\otimes_R N)$$

by

$$b((m_\lambda),n)=(m_\lambda\otimes n).$$

The map b is R-balanced biadditive in general, and linear with respect to the specified action in each of the other cases. Thus, it induces a morphism ϕ of the specified type.

To show ϕ is an isomorphism, we construct an inverse. For each i we define a pairing

$$b_\lambda : M_\lambda \times N \to \left(\bigoplus_{\lambda\in\Lambda} M_\lambda\right) \otimes_R N$$

by $b_\lambda(x,n) = \iota_\lambda(x)\otimes n$, where $\iota_\lambda : M_\lambda \to (\bigoplus_{\lambda\in\Lambda} M_\lambda)$ is the canonical inclusion map. Then b_λ is R-balanced biadditive in general, and linear with respect to the specified action in each of the other cases and hence induces a morphism $\psi_i : M_\lambda \otimes_R N \to (\bigoplus_{\lambda\in\Lambda} M_\lambda) \otimes_R N$.

By the universal mapping property for coproducts the maps $\psi_\lambda, \lambda \in \Lambda$ determine a morphism

$$\psi : \bigoplus_{\lambda\in\Lambda} (M_\lambda \otimes_R N) \to \left(\bigoplus_{\lambda\in\Lambda} M_\lambda\right) \otimes_R N.$$

It is easy to see that both $\psi\circ\phi$ and $\phi\circ\psi$ are the identity maps by observing that they act as the identity on simple tensors. □

Remark 2.59. The same property holds on the right side of the tensor.

Example 2.60. If $F = R^{\oplus\Lambda}$ is a free module, and M is any R-module, then $R^{\oplus\Lambda} \otimes_R M \cong M^{\oplus\Lambda}$, and this isomorphism is natural in M.

Example 2.61. As a special case, $R^{\oplus\Gamma} \otimes_R R^{\oplus\Lambda}$ is a free module on the basis $\{e_\gamma \otimes e_\lambda \mid (\gamma,\lambda) \in \Gamma\times\Lambda\}$.

Even more concretely, if K is a field, $K^m \otimes_K K^n \cong K^{m\times n}$ is isomorphic to the collection of $m\times n$ matrices, by the isomorphism that takes $e_i \otimes e_j$ to the matrix that has a 1 in the i,j entry and zeroes elsewhere. This morphism then sends $(a_1,\dots,a_m)\otimes(b_1,\dots,b_n)$ to $[a_ib_j]$, the outer product of these matrices. Observe that the simple tensors correspond exactly to the matrices of rank at most one.

Remark 2.62. Let R be a ring, M be a right R-module, and N be a left R-module. We can compute $M\otimes_R N$ by taking a presentation of M

$$R^{\oplus\Gamma} \xrightarrow{\phi} R^{\oplus\Lambda} \to M \to 0$$

and tensoring with N to get

$$N^{\oplus\Gamma} \to N^{\oplus\Lambda} \to M\otimes_R N \to 0,$$

so $M\otimes_R N$ is isomorphic to the cokernel of the map $N^{\oplus\Gamma} \to N^{\oplus\Lambda}$ induced by ϕ. We can also compute $M\otimes_R N$ by taking a presentation of M

$$R^{\oplus\Xi} \xrightarrow{\psi} R^{\oplus\Omega} \to N \to 0$$

and tensoring with M to get

$$M^{\oplus\Xi} \to M^{\oplus\Omega} \to M\otimes_R N \to 0,$$

so $M\otimes_R N$ is isomorphic to the cokernel of the map $M^{\oplus\Gamma} \to M^{\oplus\Lambda}$ induced by ψ.

Example 2.63. Let R be a commutative ring, I an ideal, and M a module. There is an isomorphism $R/I\otimes_R M \cong M/IM$. Indeed, if $I = (\{f_\gamma\})$, then we have a presentation

$$R^{\oplus\Gamma} \xrightarrow{\cdot[\{f_\gamma\}]} R \to R/I \to 0,$$

so

$$M^{\oplus\Gamma} \xrightarrow{\cdot[\{f_\gamma\}]} M \to R/I\otimes_R M \to 0$$

is exact. The image of the first map is just IM, so we obtain the isomorphism.

Lecture of September 29, 2021

Tensor is not exact in general.

Example 2.64. Consider the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{2} \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

and apply $- \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. We obtain the complex

$$0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \xrightarrow{1} \mathbb{Z}/2\mathbb{Z} \to 0,$$

which is exact at the last two $\mathbb{Z}/2\mathbb{Z}$'s but not at the first one.

The following properties are also useful properties for computing tensors.

Optional Exercise 2.65. Let R be commutative and M and N be R-modules. There is an isomorphism $M \otimes_R N \cong N \otimes_R M$.

Optional Exercise 2.66. Let R and S be rings. Let L be a right R-modules, M be an (R, S)-bimodule, and N be an S-module. Then $(L \otimes_R M) \otimes_S N \cong L \otimes_R (M \otimes_S N)$.

An important case of the tensor functor is tensoring with a ring.

Definition 2.67. Let $\phi : R \to S$ be a ring homomorphism. The functor

$$S \otimes_R - : R - \mathbf{Mod} \to S - \mathbf{Mod}$$

is called the functor of *extension of scalars* from R to S.

Observe that S is an (S, R)-bimodule, so this functor does indeed return S-modules. By the discussion above, extension of scalars turns an R-module into the S-module with the same presentation.

2.4.4. *Hom tensor adjointess.* The Hom and tensor functors are closely related.

Theorem 2.68. *Let R, S be rings, and A be an (R, S)-bimodule, B be an S-module, and C be and R-module. There is an isomorphism*

$$\mathrm{Hom}_R(A \otimes_S B, C) \cong \mathrm{Hom}_S(B, \mathrm{Hom}_R(A, C)).$$

Moreover, these isomorphisms are natural in each argument.

Proof. Take

$$\eta : \mathrm{Hom}_R(A \otimes_S B, C) \to \mathrm{Hom}_S(B, \mathrm{Hom}_R(A, C))$$

by the rule $\eta(\phi)(b)(a) = \phi(a \otimes b)$. We check

The map $\eta(\phi)(b)$ that sends $a \mapsto \phi(a \otimes b)$ for fixed b is R-linear: addition is fine and

$$\eta(\phi)(b)(ra) = \phi(ra \otimes b) = \phi(r(a \otimes b)) = r\phi(a \otimes b) = r\eta(\phi)(b)(a).$$

The map $\eta(\phi)$ that sends $b \mapsto \phi(- \otimes b)$ is S-linear: addition is fine and

$$\eta(\phi)(sb)(a) = \phi(a \otimes sb) = \phi(as \otimes b) = (s\eta(\phi)(b))(a).$$

Now take

$$\mu : \mathrm{Hom}_S(B, \mathrm{Hom}_R(A, C)) \to \mathrm{Hom}_R(A \otimes_S B, C)$$

by the rule $\mu(\psi)(a \otimes b) = \psi(b)(a)$. We need to check that $\mu(\psi)$ is well-defined and R-linear: to do this we check that the map $A \times B \to C$ given by $(a, b) \mapsto \psi(b)(a)$ is S-balanced biadditive and R-linear on the left factor (omitted).

We then see that μ and η are mutually inverse:

$$(\mu \circ \eta)(\phi)(a \otimes b) = \eta(\phi)(b)(a) = \phi(a \otimes b)$$

$$(\eta \circ \mu)(\psi)(b)(a) = \mu(\psi)(a \otimes b) = \psi(b)(a).$$

What do the naturality claims mean? First, this is a natural isomorphism as a functor of A:

$$\mathrm{Hom}_R(- \otimes_S B, C) \overset{\cong}{\Longrightarrow} \mathrm{Hom}_S(B, \mathrm{Hom}_R(-, C)),$$

and likewise for B and C. We won't write these out, but they are straghtforward. □

Hom-tensor adjunction has a nice consequence in terms of extension of scalars.

Definition 2.69. Let $\phi : R \to S$. There is a functor

$$\mathrm{Res}_\phi : S - \mathbf{Mod} \to R - \mathbf{Mod}$$

called the functor of *restriction of scalars* that maps an S-module M to the R-module that is the same abelian group as M with action $r \cdot m = \phi(r)m$, and is the identity mapping on morphisms.

When ϕ is injective, this restriction is literally just restricting the action. Evidently, this functor is exact, as it does nothing on the level of abelian groups, and exactness can be characterized there.

Proposition 2.70. *Let $\phi : R \to S$ be a ring homomorphism. Let M be an R-module and N be an S-module. There is an isomorphism*

$$\mathrm{Hom}_R(M, \mathrm{Res}_\phi(N)) \cong \mathrm{Hom}_S(S \otimes_R M, N).$$

These isomorphisms are natural in M and in N.

Proof. Consider S as an (S, R)-bimodule, where the right action is through ϕ. With this structure, $\mathrm{Hom}_S(S, N) \cong \mathrm{Res}_\phi(N)$. Thus, this follows from Hom-tensor adjunction. □

Lecture of October 1, 2021

2.4.5. *Multilinear maps.* Let R be a commutative ring. Associativity of tensor implies that for any finite set of modules $M_1, \ldots, M_n$, we can tensor them all together and it doesn't matter how we group them.

Observe that for any R-modules M and N, if M is generated by $m_1, \ldots, m_a$ and N is generated by $n_1, \ldots, n_b$, then $M \otimes_R N$ is generated by $\{m_i \otimes n_j \mid i = 1, \ldots, a; j = 1, \ldots, b\}$: we can write any element as a sum of simple tensors, and write each simple tensor $m \otimes n = (\sum_i r_i m_i) \otimes (\sum_j s_j b_j) = \sum_{i,j} r_i s_j (m_i \otimes n_j)$.

Likewise, by a straightforward induction on n, in $M_1 \otimes_R \cdots \otimes_R M_n$, every element is a sum of simple tensors, and an R-linear combination of simple tensors of generators of the modules M_i.

Definition 2.71. Let R be a commutative ring, and $M_1, \ldots, M_n, N$ be R-modules. We say that a map $\psi : M_1 \times \cdots \times M_n \to N$ is *multilinear* or *R-multilinear* if it is R-linear in each argument: i.e., for each i,

$$\psi(m_1, \ldots, rm_i + m_i', \ldots, m_n) = r\psi(m_1, \ldots, m_i, \ldots, m_n) + \psi(m_1, \ldots, m_i', \ldots, m_n).$$

Note that when $n = 2$, this is just the notion of R-bilinear.

Proposition 2.72. *There is a multilinear map*

$$h : M_1 \times \cdots \times M_n \to M_1 \otimes_R \cdots \otimes_R M_n$$

that satisfies the following universal property: for any multilinear map $\psi : M_1 \times \cdots \times M_n \to N$, there is an R-linear map $\alpha : M_1 \otimes_R \cdots \otimes_R M_n \to N$ such that $\psi = \alpha \circ h$.

Proof. For the map h, we take $h(m_1, \ldots, m_n) = m_1 \otimes \cdots \otimes m_n$. Then, if such a map α exists, we must have $\alpha(m_1 \otimes \cdots \otimes m_n) = \psi(m_1, \ldots, m_n)$; since simple tensors generate, α is unique if it exists. For existence, we can proceed by induction on n. For any fixed $m_n \in M_n$, the map ψ is a multilinear map on the first $n-1$ arguments, so by the inductive hypothesis, we obtain an R-linear map $M_1 \otimes_R \cdots \otimes_R M_{n-1} \to N$ that sends $m_1 \otimes \cdots \otimes m_{n-1} \mapsto \psi(m_1, \ldots, m_n)$. Since we have such a map for each m_n, we get a map $M_1 \otimes_R \cdots \otimes_R M_{n-1} \times M_n \to N$ that we can check to be bilinear, and this induces the desired map. □

2.4.6. *Tensor products of rings.*

Proposition 2.73. *Let A be a commutative ring, and R and S be commutative A-algebras. Then the tensor product $R \otimes_A S$ is a commutative ring, where the multiplication on simple tensors is given by $(r \otimes s) \cdot (r' \otimes s') = rr' \otimes ss'$.*

Proof. We need to show that there is a well-defined map that corresponds to this formula for multiplication. Note that the map

$$R \times S \times R \times S \longrightarrow R \otimes_A S$$

$$(r, s, r', s') \longmapsto rr' \otimes ss'$$

is multilinear over A. Thus, we get a well defined map

$$R \otimes_A S \otimes_A R \otimes_A S \longrightarrow R \otimes_A S$$

$$r \otimes s \otimes r' \otimes s' \longmapsto rr' \otimes ss'.$$

Thinking of $R \otimes_A S \otimes_A R \otimes_A S = (R \otimes_A S) \otimes_A (R \otimes_A S)$ and precomposing with the natural map from product to tensor product, we get a well defined A-bilinear map

$$(R \otimes_A S) \times (R \otimes_A S) \longrightarrow R \otimes_A S$$

$$(r \otimes s, r' \otimes s') \longmapsto rr' \otimes ss'.$$

The bilinearity of this map translates into the distributive laws. Commutativity and associativity of multiplication can be checked on simple tensors, since these generate, and for each these follow from the same properties in R and S. $1 \otimes 1$ is an evident multiplicative identity. □

Optional Exercise 2.74. If R and S are commutative rings, then $R \otimes_{\mathbb{Z}} S$ is the coproduct of R and S in the category of commutative rings. Moreover, if R and S are commutative A-algebras, then $R \otimes_A S$ is the coproduct of R and S in the category of commutative A-algebras.

Proposition 2.75. *If A is a commutative ring, and R is an A-algebra, then $A[x_1, \ldots, x_n] \otimes_A R \cong R[x_1, \ldots, x_n]$ as rings.*

Proof. Consider the map $A[x_1, \ldots, x_n] \times R \to R[x_1, \ldots, x_n]$ given by $(f(\mathbf{x}), r) \mapsto rf(\mathbf{x})$. This is A-bilinear, so we get an induced map on the tensor product. It is evidently additive, and also clearly multiplicative, so it is a ring homomorphism.

Consider the structure of $A[x_1, \ldots, x_n]$ as an A-module. Every element is an A-linear combination of monomials in a unique way, so the monomials form a free basis. Similarly for $R[x_1, \ldots, x_n]$. Thus, we have

$$A[x_1, \ldots, x_n] \otimes_A R = (\bigoplus_\alpha Ax^\alpha) \otimes_A R \cong \bigoplus_\alpha Rx^\alpha = R[x_1, \ldots, x_n],$$

where the middle isomorphism is the extension of scalars isomorphism that sends $x^\alpha \otimes 1$ to x^α, so this isomorphism is the same map considered above; hence our map is an isomorphism. □

Example 2.76. $A[x] \otimes_A A[x] = A[x, y]$.

Proposition 2.77. *If A is a commutative ring, R is an A-algebra, and $S = A[x_1, \ldots, x_n]/I$ is an A-algebra, then*

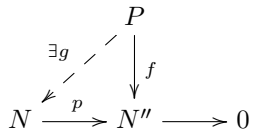
$$R \otimes_A S \cong \frac{R[x_1, \ldots, x_n]}{IR[x_1, \ldots, x_n]}.$$

Lecture of October 4, 2021

2.5. **Projective, injective, and flat modules.**

2.5.1. *Projective modules.*

Definition 2.78. An R-module P is *projective* if given any surjective homomorphism of modules $p : N \twoheadrightarrow N''$ and a homomorphism $f : P \to N''$, there is a homomorphism $g : P \to N$ such that $p \circ g = h$. In other words, given the solid arrows in the diagram



in which the bottom row is exact, there exists at least one dotted arrow that causes the triangle to commute.

Proposition 2.79. *Every free R-module is projective.*

Proof. Suppose P is free with basis B and let a diagram as in the definition be given. Since p is surjective, for each $b \in B$, we can find an element $n_b \in N$ such that $f(b) = p(n_b)$. Since B is a basis, the assignment $b \mapsto n_b$ extends uniquely to an R-module homomorphism $g : P \to N$. The triangle commutes since $p \circ g$ and f agree on B. □

We will see soon that the converse is false.

Proposition 2.80. *For a ring R and module P, the following are equivalent:*

1. *P is projective,*
2. *the functor $\mathrm{Hom}_R(P, -)$ is exact,*
3. *every short exact sequence of the form $0 \to N' \to N \to P \to 0$ is split,*
4. *every surjective R-module homomorphism $p : N \twoheadrightarrow P$ has a right inverse, and*
5. *P is a summand of a free R-module; i.e., there is an R-module Q such that $F = P \oplus Q$ is a free R-module.*

Proof. Since $\mathrm{Hom}_R(P, -)$ is left exact for any module P, $\mathrm{Hom}_R(P, -)$ is exact if and only if it preserves surjections. The definition of "projective" is just an unpackaging of the property that $\mathrm{Hom}_R(P, -)$ preserves surjections. The equivalence of (1) and (2) is thus essentially by definition.

The equivalence of (3) and (4) follows from the Splitting Theorem. Note that given an surjective map $p : N \twoheadrightarrow P$, we may form the short exact sequence $0 \to \ker(p) \to N \xrightarrow{p} P \to 0$.

Suppose (1) holds and $p : N \twoheadrightarrow P$ is onto. Applying the definition with $f = \mathrm{id}_P$ and $p = p$ gives an R-linear map g such that $p \circ f = \mathrm{id}_P$. So (1) $\Rightarrow$ (4).

To see (1) implies (4), let $p : N \twoheadrightarrow P$ be surjective, and consider the identity map on P. By (1), the identity map factors through p, so p has a right inverse.

Assume (3) holds. By choosing a generating set for P (e.g., all of P) we may find a surjection $p : F \twoheadrightarrow P$ with F a free R-module. This map splits by assumption, and thus $P \oplus \ker(p) \cong F$, so that (5) holds. So (3) $\Rightarrow$ (5).

Assume (5) holds. Say $F = P \oplus Q$ is free, and let a diagram as in the definition be given. Let $\pi : F \twoheadrightarrow P$ be the canonical surjection. Since F is projective (by the example above), there is a $h : F \to N$ so that $p \circ h = f \circ \pi$. Define $g : P \to N$ to be $h \circ \iota$ where $\iota : P \to F$ sends x to $(x, 0)$. Then $p(g(x)) = p(h(x, 0)) = f(\pi(x, 0)) = f(x)$. So P is projective (i.e. (1) holds). □

Remark 2.81. The proof of (5) $\Rightarrow$ (1) shows more than advertised: it shows that if P is a summand of projective R-module, then P is projective.

Example 2.82. Let $R = \mathbb{Z}[\sqrt{-5}]$ and let P be the ideal $(2, 1 + \sqrt{-5})$. We claim P is projective as an R-module, but not free.

It's not free since an ideal in an integral domain is free as a module if and only if it is principal (exercise). And you should have seen in 818 that this ideal is not principal.

To prove it is projective I will prove it is a summand of a free module. Let

$$\pi : R^2 \twoheadrightarrow P$$

be the map given by the row vector $[2, 1 + \sqrt{-5}]$; that is $\pi(x, y) = 2x + (1 + \sqrt{-5})y$, which is clearly onto. Define $j : P \to R^2$ to be the map

$$j(z) = (-z, 3z/(1 + \sqrt{-5})).$$

The target of j really is R^2 since for $z = 2\alpha + (1 + \sqrt{-5})\beta$ we have

$$j(z) = (-z, (1 - \sqrt{-5})\alpha + 3\beta) \in R^2,$$

using that $3 \cdot 2 = (1 - \sqrt{-5})(1 + \sqrt{-5})$. We have

$$\pi(j(z)) = -2z + 3z = z;$$

that is, p is a split surjection with splitting j. It follows that

$$R^2 \cong P \oplus \ker(\pi),$$

and hence P is projective.

Example 2.83. Let

$$R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$$

and let P be the kernel of the map

$$\pi : R^3 \xrightarrow{[x,y,z]} R.$$

π is in fact a split surjection, since $\pi \circ j = \mathrm{id}_R$ where $j(r) = (xr, yr, zr)$. This also follows because R is projective. So we have

$$R^3 \cong P \oplus R$$

and in particular this shows P is projective.

It's not free; can you prove it? Tip: Hairy Ball Theorem.

Lecture of October 6, 2021

The following technical result is sometimes useful:

Optional Exercise 2.84. Let R be a ring and $\{M_\lambda\}_{\lambda\in\Lambda}$ a family of R-modules. The coproduct (direct sum) $\bigoplus_{\lambda\in\Lambda} M_\Lambda$ of this family is projective if and only if each M_λ is projective.

2.5.2. *Injective modules.* Injective is the dual notion for projective.

Definition 2.85. An R-module E is *injective* if given solid arrows as in the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & N' & \xrightarrow{i} & N \\ & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle \exists g} & \\ & & E & & \end{array}$$

in which the top row is exact, there exists at least one dotted arrow that causes the triangle to commute.

Example 2.86. If K is a field, then K is an injective K-module. Given a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & W & \xrightarrow{i} & V \\ & & {\scriptstyle f}\downarrow & \swarrow & \\ & & K & & \end{array}$$

of K vector spaces, there is a splitting q of i, and we can take $f \circ q$ as the desired map.

Example 2.87. $\mathbb{Z}$ is not an injective $\mathbb{Z}$-module: there is no $\mathbb{Z}$-linear map making the diagram commute below

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{2} & \mathbb{Z} \\ & & {\scriptstyle 1}\downarrow & \swarrow & \\ & & \mathbb{Z} & & \end{array}$$

since such a map would send 2 to 1.

Proposition 2.88. *The following are equivalent for an R-module E:*

(1) *E is injective,*
(2) *the functor $\mathrm{Hom}_R(-, E)$ is exact,*
(3) *every short exact sequence of the form $0 \to E \to N \to N'' \to 0$ is split, and*
(4) *every injective R-module homomorphism of the form $j : E \to M$ has a left inverse.*

Proof. As with the previous proposition, the equivalence of (1) and (2) is essentially by definition, since $\mathrm{Hom}_R(-, E)$ is left exact for any module E, so this functor is right exact if and only if it takes injections $i : N' \to N$ to surjections $\mathrm{Hom}_R(i, E) : \mathrm{Hom}_R(N, E) \to \mathrm{Hom}_R(N', E)$. Likewise, the equivalence of (3) and (4) follows from the Splitting Theorem.

The proof of (1) $\Rightarrow$ (4) is very similar to the analogous proof for the proposition involving projective modules above: if E is injective and $j : E \to M$ is an injective R-linear map, then

$$\begin{array}{ccccc} 0 & \longrightarrow & E & \xrightarrow{j} & M \\ & & {\scriptstyle \mathrm{id}_E}\downarrow & \swarrow{\scriptstyle \exists q} & \\ & & E & & \end{array}$$

can be completed, and $q \circ j = \mathrm{id}_E$ for any such completion.

Assume (4) and let a diagram as in the definition of "injective" be given. Form the module

$$M = \frac{E \oplus N}{\{(f(n'), -i(n')) \mid n' \in N'\}}.$$

(This is called a *pushout* of E and N.) Let $j : E \to M$ be the map sending a to the class of $(a, 0)$ and let $h : N \to M$ be the map sending n to the class of $(0, n)$. Then the diagram below commutes

$$\begin{array}{ccc} N' & \xrightarrow{i} & N \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle h} \\ E & \xrightarrow{j} & M \end{array}$$

and I claim that j is injective. The former is clear by construction of M: given $n' \in N'$, we have $j(f(n')) - h(i(n')) = (f(n'), -i(n')) = 0 \in M$. If $j(a) = \overline{(a, 0)} = 0$ in M, then there is an $n' \in N'$ such that $f(n') = a$ and $i(n') = 0$. But i is injective and hence $a = 0$.

By assumption (i.e. statement (4)), there is a map $q : M \twoheadrightarrow E$ such that $q \circ j = \mathrm{id}_E$. Define $g : N \to E$ as $g := q \circ h$. Then $g \circ i = q \circ h \circ i = q \circ j \circ f = \mathrm{id}_E \circ f = f$.

This proves E is injective. □

Optional Exercise 2.89. If $\{M_\lambda\}_{\lambda \in \Lambda}$ is a collection of modules, then $\prod_{\lambda \in \Lambda} M_\lambda$ is injective if and only if each M_λ is injective.

Example 2.90. If K is a field and R is a K-algebra, then $\mathrm{Hom}_K(R, K)$ is an injective R-module. Indeed, $\mathrm{Hom}_R(-, \mathrm{Hom}_K(R, K)) \overset{\cong}{\Longrightarrow} \mathrm{Hom}_K(R \otimes_R -, K) \overset{\cong}{\Longrightarrow} \mathrm{Hom}_K(-, K)$, which is exact, since K is an injective K-vector space.

Example 2.91. Suppose R is an integral domain and E is an injective R-module. The E is *divisible*: for every $x \in E$ and $r \in R \smallsetminus 0$, there is a $y \in E$ such that $x = ry$. To see this, just apply the definition to the diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & R & \xrightarrow{r} & R \\ & & {\scriptstyle x}\downarrow & \swarrow_{\exists g} & \\ & & E & & \end{array}$$

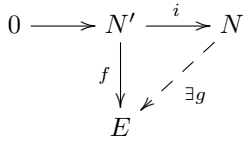
Theorem 2.92 (Baer's criterion)**.** *For any ring R, an R-module E is injective if and only if every diagram of the form represented below in solid arrows*

$$\begin{array}{ccccc} 0 & \longrightarrow & J & \xrightarrow{\iota} & R \\ & & {\scriptstyle f}\downarrow & \swarrow_{\exists g} & \\ & & E & & \end{array}$$

where J is an ideal of R and ι is the inclusion map, can be completed by some dashed homomorphism g to a commutative diagram.

Proof. One direction is immediate from the definition.

Suppose each diagram as in the statement can be completed and let a diagram



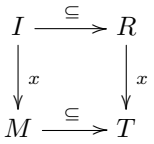
as in the definition of "injective" be given. For simplicity of notation, we may assume i is the inclusion of a submodule N' of N into N. We need to show that given an R-map $g : N' \to E$, there is an R-map $g : N \to E$ such that $g|_{N'} = f$.

Consider pairs (M, h) such that $N' \subseteq M \subseteq N$ and $h : M \to E$ is an R-map such that $h|_{N'} = f$. Let $\mathcal{S}$ be the collection of all such pairs, and partially order it by $(M_1, h_1) \leqslant (M_2, h_2)$ if and only if $M_1 \subseteq M_2$ and $h_2|_{M_1} = h_1$. The set $\mathcal{S}$ is non-empty since (N', f) belongs to it.

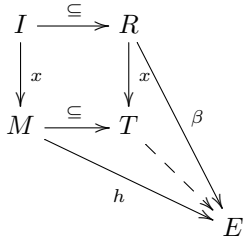
Let us show $\mathcal{S}$ satisfies the hypotheses of Zorn's Lemma. Suppose $\{(M_i, h_i)\}_{i\in I}$ is a totally ordered subset of $\mathcal{S}$. Then $M := \cup_{i\in I} M_i$ is a submodule of N (since the collection is totally ordered) and the function $h : M \to E$ defined as $h(m) = h_i(m)$ for any i such that $m \in M_i$ is a well-defined R-map (again, since the collection is totally ordered). So $(M, h) \in \mathcal{S}$ and $(M, h) \geqslant (M_i, h_i)$ for all i.

By Zorn's Lemma, $\mathcal{S}$ has a maximal element (M, h). It suffices to prove $M = N$. If not pick $x \in N \smallsetminus M$ and let $T = M + Rx$. I will show h can be extended to T, arriving at a contradiction:

Set $I = \{r \in R \mid rx \in M\}$. The map $R \xrightarrow{x} T$ (sending r to tx) restricts to a map $I \xrightarrow{x} M$ by definition of I, and so we have a commutative square



By assumption the map $\alpha : I \to E$ given as the composition $I \xrightarrow{x} M \xrightarrow{h} E$ extends to a map $\underline{:}R \to E$. This gives a diagram



in which the inner square and the outer quadrilateral both commute. I claim there is an R-map $\gamma : T \to E$ (the dashed arrow in the diagram) causing both triangles to commute. It is given abstractly by the fact that the square in this diagram is a push-out. Define $\gamma : T \to E$ by $\gamma(m + rx) = h(m) + \beta(r)$ for $m \in M$ and $r \in R$. I leave it to you to prove γ is well-defined (note that $m + rx$ can equal $m' + r'x$ without $m' = m$ and $r = r'$) and an R-map. Granting this, we clearly have $\gamma|_M = h$. So $(M, h) < (T, \gamma)$ in $\mathcal{S}$, a contradiction. It must be the $M = N$, and so we have proven E is injective. □

Lecture of October 8, 2021

Corollary 2.93. *For a PID, E is an injective R-module if and only if it is divisible.*

Proof. We already proved one direction (for any domain). Assume E is divisible. By Baer's Criterion and the fact that every ideal in R is principal by assumption, we just need to show every diagram of the form

$$\begin{array}{ccccc} 0 & \longrightarrow & Rr & \xrightarrow{\iota} & R \\ & & \downarrow{\scriptstyle f} & \swarrow_{\exists g} & \\ & & E & & \end{array}$$

can be completed, where r is any element of R. If $r = 0$, we may take $g = 0$. If $r \neq 0$, then let $f(r) = x \in E$. Since E is divisible there is $y \in E$ such that $x = ry$, Now define $g : R \to E$ by $g(u) = uy$ and notice that $(g \circ \iota)(r) = g(r) = ry = x = f(r)$ hence $g \circ \iota = f$ for any element of (r) since this is true for the generator r. □

Example 2.94. Using the above criterion, $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$, and $\mathbb{C}^\times$ are injective $\mathbb{Z}$-modules.

Not every divisible module is injective.

Example 2.95. Let K be a field, $R = K[x, y]$, and $Q = K(x, y)$ be the fraction field. Since Q is divisible, Q/R is as well. However, Q/R is not injective.

Let $I = (x, y)$, and consider the map $f : I \to Q/R$ given by $f(ax + by) = a[\frac{1}{y}]$. To see that this is well defined, note that if $ax + by = cx + dy$, then $(a - c)x = (d - b)y$, so $y|(a - c)$, as $K[x, y]$ is a UFD; then $f(ax + by) - f(cx + dy) = (a - c)[\frac{1}{y}] = 0$. It is easy to see that f is R-linear.

We claim that f cannot be extended to $g : R \to Q/R$. Indeed, given an extension g, write $g(1) = [\frac{a}{b}]$ with $a, b \in R$ and a/b in lowest terms (which makes sense since R is a UFD). Note that b cannot be a unit, since then $a/b \in R$, so $[\frac{a}{b}] = 0$, so g is the zero map and hence f is the zero map, which it is not. We have $0 = f(y) = g(y) = yg(1) = y[\frac{a}{b}]$, so $\frac{ya}{b} \in R$. Thus $b|y$ in R, so without loss of generality, $b = y$. We also have $[\frac{1}{y}] = f(x) = g(x) = xg(1) = x[\frac{a}{y}]$, which means that $\frac{1-ax}{y} \in R$, so $y|(1 - ax)$, which is a contradiction.

Note that every R-module admits a surjection from a projective R-module: there is a surjection from a free module. The dual statement is true for injectives as well.

Proposition 2.96. *Let M be an R-module. There exists an injective module E and an injective homomorphism $i : M \to E$.*

Proof. First, we deal with the case that $R = \mathbb{Z}$.

Observe that if $\mathbb{Z}x$ is a nonzero cyclic group, there is a nonzero additive map $M \to \mathbb{Q}/\mathbb{Z}$: map x to $[1/n]$ for some n that divides the order of x if finite, or to an arbitrary $[1/n]$ if infinite. Now, for an arbitrary abelian group A, for any nonzero x we have

$$0 \to \mathbb{Z}x \to A \to A/\mathbb{Z}x \to 0$$

exact, so since $\mathbb{Q}/\mathbb{Z}$ is injective, we can extend any map from $\mathbb{Z}x \to \mathbb{Q}/\mathbb{Z}$ to a map from A. For every nonzero $a \in A$, fix an additive map $\phi_a : A \to \mathbb{Q}/\mathbb{Z}$ and let $\phi : A \to \prod_{a \in A \smallsetminus 0} \mathbb{Q}/\mathbb{Z}$ be given by $\phi(x) = (\phi_a(x))_{a \in A \smallsetminus 0}$. By construction this is an injective homomorphism, and $\mathbb{Q}/\mathbb{Z}$ is an injective module.

Now let R be arbitrary, and M be an R-module. Considering M as an abelian group, there is an injective abelian group D and additive map $j : M \to D$ by the case above. By left exactness of Hom, there is an injection $\mathrm{Hom}_{\mathbb{Z}}(R, M) \xrightarrow{j_*} \mathrm{Hom}_{\mathbb{Z}}(R, D)$. This map is R-linear:

$$rj_*(\alpha)(s) = r(j\alpha)(s) = j\alpha(sr) = j(r\alpha)(s) = j_*(r\alpha)(s).$$

Furthermore, there is an injection $M \cong \mathrm{Hom}_R(R, M) \subseteq \mathrm{Hom}_{\mathbb{Z}}(R, M)$. Put together, we obtain an R-linear injection $M \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$.

It remains to see that $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module. But

$$\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, D)) \xRightarrow{\cong} \mathrm{Hom}_{\mathbb{Z}}(R \otimes_R -, D) \xRightarrow{\cong} \mathrm{Hom}_{\mathbb{Z}}(-, D)$$

is exact, so this is the case. □

2.5.3. *Flat modules.*

Definition 2.97. An R-module N is *flat* if for every injective homomorphism of right R-modules $M \xrightarrow{f} M'$, the induced map $M \otimes_R N \xrightarrow{f \otimes 1_N} M' \otimes_R N$ is injective.

Since tensor is right exact, a module N is flat if and only if $- \otimes_R N$ is an exact functor.

Optional Exercise 2.98. Given a family of R-modules $\{M_\lambda\}_{\lambda \in \Lambda}$, $\bigoplus_\lambda M_\lambda$ is flat if and only if every M_λ is flat.

All projectives are flat.

Theorem 2.99. *Every projective R-module is flat.*

Proof. First, recall that $- \otimes_R R$ is naturally isomorphic to the identity functor, and thus exact. This shows that R is flat, and thus any free module, being a direct sum of copies of R, must also be flat. Finally, every projective module is a direct summand of a free module. Direct summands of flat modules are flat, so every projective module is flat. □

Proposition 2.100. *If R is a commutative ring, and S is any multiplicatively closed set, then $S^{-1}R$ is a flat R-module.*

Proof. You showed on the homework that the functor $- \otimes_R S^{-1}R$ is naturally isomorphic to the localization functor, which is exact. □

3. Simplicity, semisimplicity, and representation theory

3.1. **Group rings and representations.** We will take a brief aside to discuss an important class of examples of modules.

3.1.1. *Representations.*

Definition 3.1. Let G be a group. A *representation* of G over a field K is a K-vector space V equipped with a group homomorphism $\rho : G \to \mathrm{Aut}_K(V)$. More generally, a representation of G over a ring R is an R-module V equipped with group homomorphism $\rho : G \to \mathrm{Aut}_R(V)$. We may also say that G *acts linearly* on V.

One often simply says that V is a representation of G if the homomorphism ρ is understood.

Remark 3.2. We can think of this data in a number of different ways.

(1) Given a representation (V, ρ), the map

$$G \times V \longrightarrow V$$
$$(g, m) \longmapsto g \cdot v := \rho(g)(v)$$

satisfies the properties

(a) $e \cdot v = v$
(b) $gh \cdot v = g \cdot (h \cdot v)$
(c) $g \cdot (v + w) = (g \cdot v) + (g \cdot w)$
(d) $g \cdot rv = r(g \cdot v)$,

In particular, the first two conditions say that G acts on V in the sense of group action on a set, and the last two say that the action of any element is by an R-linear map. Conversely, any such function ψ yields a representation (V, ρ).

(2) If $V = R^n$ is free, then $\mathrm{Aut}_R(V) \cong \mathrm{GL}_n(R)$, where $\mathrm{GL}_n(R)$ is the group of $n \times n$ invertible matrices with entries in R. By a slight abuse of notation, we will say that a group homomorphism $G \to \mathrm{GL}_n(V)$ is a representation of G.

Example 3.3. (1) For any group G, and any R-module V, there is the *trivial representation* $\rho : G \to \mathrm{Aut}_R(V)$ where $\rho(g) = 1_V$ for all $g \in G$. In this action, every element acts trivially on M.

(2) Any representation on $V = R$ is determined by specifying a group homomorphism $\rho : G \to \mathrm{Aut}_R(R) \cong R^\times$.

For example, if $G = C_n = \langle g \rangle$ (the multiplicative cyclic group of order n) and $R = \mathbb{C}$, there are n possible such homomorphisms, determined by $\rho(g) = e^{\frac{2\pi k i}{n}}$ where $0 \leqslant k \leqslant n-1$.

Another important example of a rank 1 representation is the *sign representation* of the symmetric group S_n, given by the group homomorphism which assigns to each permutation its sign, regarded as an element of the arbitrary ring R.

(3) The symmetric group S_n acts on a free R-module with basis $b_1, \ldots, b_n$ by permuting coordinates: $\rho(\sigma)(b_i) = b_{\sigma(i)}$. For a concrete example, S_3 acts on $\mathbb{R}^3$, where, for example $(132) \cdot (a_1, a_2, a_3) = (a_2, a_3, a_1)$.

(4) Let $G = D_{2n}$, symmetries of the equilateral polygon on n vertices. Then G acts linearly on $V = \mathbb{R}^2$ by rotations and reflections. If G is generated by r (rotation by $2\pi/n$) and l (reflection about the y-axis), then the associated group homomorphism $\rho : G \to \mathrm{GL}_2(\mathbb{R})$ maps

$$\rho(r) = \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix} \qquad \rho(l) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

(5) Let $R = K$ be a field,$V = K^2$, and let $G = (K, +)$. We see that the assignment

$$\rho : G \to \mathrm{GL}_2(K) \quad \rho(\lambda) = \begin{bmatrix} 1 & 0 \\ \lambda & 1 \end{bmatrix}$$

is a representation. In particular, if $K = \mathbb{F}_p$, this is a representation of C_p.

Definition 3.4. If $\rho : G \to \mathrm{Aut}_R(V)$ and $\omega : G \to \mathrm{Aut}_R(W)$ are R-linear representations of G on V and W respectively then a *G-equivariant map* from V to W is an R-module homomorphism $f : V \to W$ such that $f(gv) = gf(v)$ for all $v \in V$. Equivalently the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \phi(g)}\downarrow & & \downarrow{\scriptstyle \psi(g)} \\ V & \xrightarrow{f} & W \end{array}$$

Definition 3.5. If $\rho : G \to \mathrm{Aut}_R(V)$ is a representation, a submodule $W \leqslant V$ is *G-stable* if $\rho(g)(W) \subseteq W$ for all $g \in G$.

Example 3.6. For $G = S_n$ acting by permuting a basis as above, $\{(\lambda, \dots, \lambda) \mid \lambda \in K\}$ and

$$\{(\lambda_1, \dots, \lambda_n) \mid \lambda_1 + \cdots + \lambda_n = 0\}$$

are stable subspaces.

Example 3.7. For $G = (K, +)$ acting on K^2 as above, $\{(0, \lambda) \mid \lambda \in K\}$ is a stable subspace.

Proposition 3.8. *Fix a group G and a ring R. The collection of left R-linear representations of G and G-equivariant maps between them forms a category which we will denote* $\mathbf{Rep}_R(G)$.

Lecture of October 13, 2021

3.1.2. *Group rings and modules.*

Definition 3.9. For any ring R and group G, we define the *group ring* $R[G]$ as follows: As a set, $R[G]$ is the free left R-module with basis G; that is,

$$R[G] = \left\{ \sum_g r_g g \mid r_g = 0_R \text{ for all by a finite number of } g's \right\}.$$

We define addition as module addition; that is,

$$\left(\sum_g r_g g\right) + \left(\sum_h s_h h\right) = \sum_{f \in G} (r_f + s_f) f.$$

Multiplication is the unique pairing that obeys the distributive laws and is such that R is a subring, $1_R G$ is a subgroup of $(R[G]^\times, \cdot)$, and every element of R commutes with every element of G. In general, we have

$$\left(\sum_g r_g g\right) \cdot \left(\sum_h s_h h\right) = \sum_{f \in G} \left(\sum_{\substack{(g,h) \in G \times G \\ gh = f}} r_g s_h \right) f.$$

where the inner sum is over pairs of group elements whose product is f.

Remark 3.10. As a matter of notation, the element $1_R g$ will be written as just g and the element $r e_G$ as just r, so that we will regard G and R as subsets of $R[G]$. They overlap in the one element $1_R e_G$ which will be written as just 1.

Remark 3.11. When R is commutative (in particular when R is a field), $R[G]$ is an R-algebra called the *group R-algebra* of G.

Optional Exercise 3.12. For any ring R and $G = C_n$, prove there is a ring isomorphism

$$R[C_n] \cong R[x]/(x^n - 1).$$

Proposition 3.13 (Universal Mapping Property of group rings)**.** *Let R, A be rings and G a group. Given a ring homomorphism $\iota : R \to A$ and a group homomorphism $f : G \to (A^\times, \cdot)$, such that for every $r \in R, g \in G$ we have that $\iota(r)$ and $f(g)$ commute in $(A, \cdot)$, there is a unique ring homomorphism $\alpha : R[G] \to A$ such that $\alpha|_R = \iota$ and $\alpha|_G = f$. Explicitly, α is given by*

$$\alpha\left(\sum_g r_g g\right) = \sum_g \iota(r_g) f(g).$$

Proof. Most of this follows from noticing that $R[G]$ is a coproduct. Indeed, we can vie $R[G]$ as an internal direct sum $R[G] = \bigoplus_{g\in G} Rg$ and hence it is the coproduct for the family $\{Rg\}_{g\in G}$ where each $Rg \cong R$. For each $g \in G$ set up an R-module homomorphism $f_g : Rg \to A$ by mapping $f_g(r_g g) = \iota(r_g)f(g)$. Then the definition of coproduct gives a unique R-module homomorphism

$$\alpha : R[G] = \bigoplus_{g\in G} Rg \to A \text{ such that } \alpha|_{Rg} = f_g.$$

From the way we defined the maps f_g we can deduce that $\alpha|_R = \iota$ and $\alpha|_G = f$ and

$$\alpha\left(\sum_g r_g g\right) = \sum_g \iota(r_g)f(g).$$

It remains to check that this map is in fact a ring homomorphism, i.e. it preserves multiplication. This can be done using the formula for α above and the fact that $\iota(R)$ and $f(G)$ commute in A. □

Remark 3.14. If we assumed that A is an R-algebra in the proposition above, then we would not need the commutativity condition as $\iota(R)$ is in the center of A so it commutes with everything.

Lemma 3.15. *Let R be a ring, V a left R-module, and G a group. There is a bijection*

$$\left\{ \begin{array}{c} R\text{-linear representations} \\ \text{of } G \text{ on } V \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} R[G]\text{-module structures on } V \\ \text{(extending given action of } R) \end{array} \right\}.$$

Moreover, if V and W are representations, then $\psi : V \to W$ is G-equivariant if and only if it is $R[G]$-linear.

Proof. Given an $R[G]$-module structure on V, for every $g \in G$, there is a map $m_g : V \to V$ given by $v \mapsto g\cdot v$. We have $m_g(rv) = g(rv) = rg(v) = rm_g(v)$, so m_g is R-linear. Moreover, the map $\rho : G \to \mathrm{End}_R(V)$ that sends $g \mapsto m_g$ preserves multiplication and identity: $\rho(gh)(v) = ghv = g(hv) = \rho(g)\rho(h)(v)$ and $\rho(e)(v) = v$. Thus, we obtain an R-linear representation $\rho : G \to \mathrm{Aut}_R(V)$.

Conversely, recall that a module structure on an abelian group is equivalent to a ring homomorphism to its endomorphism ring over $\mathbb{Z}$. Given a representation $\rho : G \to \mathrm{Aut}_R(V)$ by considering $\mathrm{Aut}_R(V) \subseteq \mathrm{End}_{\mathbb{Z}}(V)$ we get a group homomorphism f to the unit subgroup of $\mathrm{End}_{\mathbb{Z}}(V)$. The action of R on V gives a ring homomorphism $\iota : R \to \mathrm{End}_{\mathbb{Z}}(V)$. For $r \in R$ and $g \in G$, we have

$$(f(g) \circ \iota(r))(v) = f(g)(rv) = \rho(g)(rv) = r\rho(g)(v) = (\iota(r) \circ f(g))(v)$$

for all $v \in V$. Thus, by the universal property, we get a well-defined ring homomorphism $R[G] \to \mathrm{End}_{\mathbb{Z}}(V)$, and hence an $R[G]$-module structure, which is easily seen to follow the formula above.

We leave the final claim as an exercise. □

Remark 3.16. We can think of these bijections as yielding mutually inverse functors $F : \mathbf{Rep}_R(G) \to R[G] - \mathbf{Mod}$ and $F^{-1} : R[G] - \mathbf{Mod} \to \mathbf{Rep}_R(G)$.

3.2. **Simple modules and finite length modules.**

3.2.1. *Simple modules.* Now we proceed to discuss some smallness conditions on modules. The first key notion is that of a simple module. Simple modules are the atoms in module theory.

Definition 3.17. An R-module M is *simple* if there are no nonzero proper submodules of M.

Lemma 3.18. *Let M be a nonzero R-module. The following are equivalent:*

(1) *M is simple*
(2) *$Rm = M$ for all $m \in M \smallsetminus 0$*
(3) *$M \cong R/I$ for some maximal left ideal I.*

Proof. If M is simple, and $m \neq 0$, then $0 \neq Rm \subseteq M$ implies $Rm = M$, so (1) implies (2). Conversely, if $0 \neq N \subsetneqq M$, and $m \in N$ is nonzero, then Rm is nonzero and contained in N, hence not equal to M, so (2) implies (1).

For a left ideal I, the submodules of R/I are in bijective correspondence with the left R-submodules of R that contain I, i.e., the left ideals that contain I. It is then clear that if I is a maximal left ideal, then R/I is simple, so (3) implies (1). On the other hand, if M is simple then it is cyclic (since (1) implies (2)), so $M \cong R/I$ for some left ideal I, and if $I \subsetneqq J$ for some proper left ideal J, then $0 \neq J/I \subsetneqq R/I$; thus (1) implies (3). □

Example 3.19.
(1) If K is a field, a K-vector space is simple if and only if it is 1-dimensional. Moreover, if R is a K-algebra, then any R-module that is 1-dimensional as a vector space is a simple R-module as well.
(2) If R is commutative, then an R-module M is simple if and only if M is isomorphic to a field.
(3) Let $R = \mathbb{R}[D_{2n}]$, and V be the natural 2-dimensional representation by reflections and rotations. Then V is a simple R-module, since there are no D_{2n}-stable subspaces.
(4) Let K be a field, or more generally a division ring, and let $R = M_n(K) \cong \mathrm{End}_K(K^n)$. The module $M = K^n$ of column vectors is a simple R-module Indeed, if $v = (a_1, \dots, a_n) \neq 0$, say $a_i \neq 0$; then $a_i^{-1} E_{ij} v = e_i \in M$, and since M is generated by the standard vectors e_i, $M = Rv$.

Lemma 3.20 (Schur's Lemma)**.** *Let R be a ring, and M, N be two simple R-modules. Then every nonzero R-module homomorphism $\phi : M \to N$ is an isomorphism. In particular, $\mathrm{End}_R(M)$ is a division ring.*

Proof. For the first assertion, let $f : M \to N$ be R-linear and nonzero. Then $\ker(f) \neq M$, so $\ker(f) = 0$ by simplicity, and $\mathrm{im}(f) \neq 0$, so $\mathrm{im}(f) = N$.

For the second, recall that $\mathrm{End}_R(M)$ is a ring. If $f \in \mathrm{End}_R(M)$ is nonzero, then by the first part, it is an isomorphism, so it has a two-sided inverse in $\mathrm{End}_R(M)$. □

3.2.2. *Finite length modules.* Given a short exact sequence

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

we may think of the middle module B as built out of A and C; we call B an *extension* of A and C. Suppose that a module has a finite sequence of submodules

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

we call such a sequence a *filtration*. Then M_1 is an extension of M_0 and M_1/M_0, M_2 is an extension of $M_1 = M_1/M_0$ and M_2/M_1, and so on. We might think of M as built from $M_1/M_0, M_2/M_1, \dots, M_n/M_{n-1}$ like so.

A module has finite length if it can be built from finitely many simple modules in this way.

Definition 3.21. A module M has *finite length* if it has a filtration of the form

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

with M_{i+1}/M_i simple for each i; such a filtration is called a *composition series* of *length* n. We say a composition series is *strict* if $M_i \neq M_{i+1}$ for all i. Two composition series are *equivalent* if the collections

of composition factors M_{i+1}/M_i are the same up to reordering. The *length* of a finite length module M, denoted $\ell(M)$, is the minimum of the lengths of a composition series of M. If M has does not have finite length, we say that M has infinite length, or $\ell(M) = \infty$.

Example 3.22. Let K be a field and $V = K^2$. Then any filtration of the form $0 \subseteq W \subseteq V$ where W is a line through the origin is a strict composition series.

Remark 3.23. Let

$$0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$$

be a short exact sequence. Given filtrations / composition series / strict composition series

$$A_\bullet : \qquad 0 = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_n = A$$

and

$$C_\bullet : \qquad 0 = C_0 \subseteq C_1 \subseteq C_2 \subseteq \cdots \subseteq C_n = C$$

we can make a filtration / composition series / strict composition series of B by

$$0 = i(A_0) \subseteq i(A_1) \subseteq i(A_2) \subseteq \cdots \subseteq i(A_n) = i(A) = p^{-1}(C_0) \subseteq p^{-1}(C_1) \subseteq p^{-1}(C_2) \subseteq \cdots \subseteq p^{-1}(C_n) = B.$$

Conversely, given a filtration / composition series / strict composition series of B that contains $i(L)$ as a term, we can obtain filtrations / composition series / strict composition series of A and C by applying i^{-1} to the terms up through $i(L)$ and applying p to the terms from $i(L)$ on. However, not every filtration / composition series of a module will contain a fixed submodule as a term.

Theorem 3.24 (Jordan-Holder theorem)**.** *Let M be a module of finite length.*

1. *If $L \subseteq M$ is a proper submodule, then $\ell(L) < \ell(M)$.*
2. *If $L \subseteq M$ is a nonzero submodule and $\overline{M} = M/L$, then $\ell(\overline{M}) < \ell(M)$.*
3. *Any filtration of M can be refined to a composition series.*
4. *All strict composition series for M are equivalent, and hence have the same length.*

Proof. If $m := \ell(M)$, consider a strict composition series of M of length m, say

$$M_\bullet : \qquad 0 = M_0 \subsetneqq M_1 \subsetneqq M_2 \subsetneqq \cdots \subsetneqq M_m = M.$$

(1) Consider the filtration

$$L_\bullet : \qquad 0 = M_0 \cap L \subseteq M_1 \cap L \subseteq M_2 \cap L \subseteq \cdots \subseteq M_m \cap L = L.$$

By the Second Isomorphism Theorem, its composition factors satisfy

$$\frac{M_{i+1} \cap L}{M_i \cap L} = \frac{M_{i+1} \cap L}{(M_{i+1} \cap L) \cap M_i} \cong \frac{M_{i+1} \cap L + M_i}{M_i}.$$

The right hand side is a submodule of M_{i+1}/M_i, which by assumption is simple, so our filtration is in fact a composition series of length n. Then for any i either

$$\frac{M_{i+1} \cap L}{M_i \cap L} = 0 \quad \text{or} \quad \frac{M_{i+1} \cap L}{M_i \cap L} \cong \frac{M_{i+1}}{M_i}.$$

We claim that the latter case does not hold for all i: if it did, we would have $0 = M_0 = M_0 \cap L$, and inductively $M_{i+1} \cap L = M_{i+1}$ for all i and in particular for $i = m - 1$, we have $M = M \cap L$, contradicting that L is proper. Thus, for some i, the first case holds. We can then skip that i and obtain a composition series of length less than n, so $\ell(L) < m$.

Lecture of October 20, 2021

(2) Consider the filtration

$$\overline{M}_\bullet : \qquad 0 = \frac{M_0 + L}{L} \subseteq \frac{M_1 + L}{L} \subseteq \cdots \subseteq \frac{M_n + L}{L} = \overline{M}.$$

The factors satisfy

$$\frac{(M_{i+1} + L)/L}{(M_i + L)/L} \cong \frac{M_{i+1} + L}{M_i + L} \cong \frac{M_{i+1} + (M_i + L)}{M_i + L} \cong \frac{M_{i+1}}{M_{i+1} \cap (M_i + L)},$$

and since $M_i \subseteq M_{i+1} \cap (M_i + L)$, these are quotient modules of the simple module M_{i+1}/M_i, so this is a composition series. Then for any i either

$$\frac{(M_{i+1} + L)/L}{(M_i + L)/L} = 0 \quad \text{or} \quad \frac{M_{i+1}}{M_{i+1} \cap (M_i + L)} \cong \frac{M_{i+1}}{M_i}.$$

We claim that the latter case does not hold for all i: if it did, we would have then $M_{i+1} \cap (M_i + L) = M_i$ for all i, so

$$\frac{M_{i+1} + L}{M_{i+1}} \cong \frac{L + M_i}{(L + M_i) \cap M_{i+1}} = \frac{L + M_i}{M_i}$$

for all i, and hence $L \cong (L + M_0)/M_0 \cong (L + M_n)/M_n \cong 0$, contradicting that $L \neq 0$. Thus, for some i, the first case holds, and we can skip that i to obtain a composition series of length less than n, so $\ell(\overline{M}) < m$.

(3) We proceed by induction on length again. Given a filtration of M, we can suppose that there is some nonzero proper submodule L in the filtration, since otherwise we could just take any composition series. Then L and $\overline{M}$ has length less than M. The filtration up to L can be refined to a strict composition series by the induction hypothesis, and the filtration from L to M taken mod L can be refined to a strict composition series for $\overline{M}$; pulling back as in the remark above, we get the strict composition series we want.

(4) We show by induction on m that for any module of length m, all of its strict composition series are equivalent. Assume that $\ell(M) = m$. If $m = 1$, the claim is clear since we are dealing with a simple module. Suppose that

$$N_\bullet : \qquad 0 = N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_n = M$$

is another strict composition series for M, so $n \geqslant m$. If $N_{n-1} = M_{m-1}$, then since $\ell(M_{m-1}) \leqslant m-1$ the two composition series we have for M_{m-1} are equivalent by induction, so the two given series are equivalent.

If $N_{n-1} \neq M_{m-1}$, since M/M_{m-1} is simple, M_{m-1} is not properly contained in N_{n-1}, so the image of M_{m-1} in M/N_{n-1} is nonzero, so equals all of M, which means that $N_{n-1} + M_{m-1} = M$. Set $K = N_{n-1} \cap M_{m-1}$. By the second isomorphism theorem, we then have

$$\frac{M}{M_{m-1}} = \frac{M_{m-1} + N_{n-1}}{M_{m-1}} \cong \frac{N_{n-1}}{K}$$

and similarly $M/N_{n-1} \cong M_{m-1}/K$, and both of these modules are simple.

Fix a strict composition series for K:

$$K_\bullet : \qquad 0 = K_0 \subsetneqq K_1 \subsetneqq \cdots \subsetneqq K_k = K$$

and extend to a strict composition series for M_{m-1}:

$$K'_\bullet : \qquad 0 = K_0 \subsetneqq K_1 \subsetneqq \cdots \subsetneqq K_k = K \subsetneqq M_{m-1}.$$

Since we also have the strict composition series

$$M_{\bullet\leqslant m-1}: \qquad 0 = M_0 \subsetneqq M_1 \subsetneqq M_2 \subsetneqq \cdots \subsetneqq M_{m-1}$$

of length $m-1$, we must have that $k = m-2$ and $K'_\bullet$ is equivalent to $M_{\bullet\leqslant n-1}$. Thus, the composition factors of $M_{\bullet\leqslant m-1}$ are those of K plus one copy of $M_{m-1}/K \cong M/N_{n-1}$.

Now,

$$K''_\bullet: \qquad 0 = K_0 \subsetneqq K_1 \subsetneqq \cdots \subsetneqq K_{m-2} = K \subsetneqq N_{n-1}$$

is a strict composition series for N_{n-1}, so $n = m$. Then, $K''_\bullet$ is equivalent to the strict composition series

$$N_{\bullet\leqslant n-1}: \qquad 0 = N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_{n-1}.$$

Thus, the composition factors of $N_{\bullet\leqslant n-1}$ are those of K plus one copy of $N_{n-1}/K \cong M/M_{n-1}$.

It follows that the composition series $M_\bullet$ and $N_\bullet$ are equivalent. □

Example 3.25. (1) If K is a field, then a K-vector space of dimension n is a K-module of length n.

(2) If R is a K-algebra, and M is an R-module that as a K-vector space has dimension n, then $\ell(M) \leqslant n$, since the vector space dimension of a proper submodule is strictly smaller.

(3) The ring $R = K[x]$ does not have finite length as a module over itself.

(4) $\mathbb{Z}/p^n$ has length n as a $\mathbb{Z}$-module, with strict composition series

$$0 \subseteq \langle \overline{p^{n-1}} \rangle \subseteq \cdots \subseteq \langle \overline{p} \rangle \subseteq \mathbb{Z}/p^n.$$

3.3. **Chain conditions.**

Definition 3.26. We say a poset $(P, \leqslant)$ satisfies the *ascending chain condition* or *ACC* if every totally ordered nonempty subset of P has a maximum element. Similarly, $(P, \leqslant)$ satisfies the *descending chain condition* or *DCC* if every totally ordered nonempty subset of P has a minimum element.

Remark 3.27. For a poset $(P, \leqslant)$, the following are equivalent:

(1) Every totally ordered nonempty subset has a maximum element (i.e., P has ACC)

(2) Every totally ordered subset indexed by $\mathbb{N}$, $p_1 \leqslant p_2 \leqslant p_3 \leqslant \cdots$ has a maximum element (i.e., $\exists k : p_k = p_{k+1} = \cdots$)

(3) Every nonempty subset of P has a maximum element.

Indeed, (3) $\Rightarrow$ (1) $\Rightarrow$ (2) is clear. Given a totally ordered nonempty subset with no maximum, one can inductively keep choosing larger elements and obtain a countable such subset, so (2) $\Rightarrow$ (1). If any totally ordered nonempty subset of P has a maximum element, then the same property holds for any nonempty subset Q of P, so by Zorn's Lemma, such a Q has a maximum element. The analogous equivalences hold with DCC.

Note that the condition (3) asserts that any nonempty subset of P has an element that is maximal *within the subset*, not maximal *within* P.

Definition 3.28. Let R be a ring and M be an R-module.

(1) We say that M is *Noetherian* if the poset of submodules of M partially ordered by containment has ACC.

(2) We say that M is *Artinian* if the poset of submodules of M partially ordered by containment has DCC.

(3) We say that R is *left Noetherian* if R is Noetherian as a left R-module; i.e., the poset of left ideals of R under containment has ACC.
(4) We say that R is *left Artinian* if R is Artinian as a left R-module; i.e., the poset of left ideals of R under containment has DCC.

If R is commutative, left ideals and right ideals are the same, so we will just say R is Noetherian or Artinian.

Example 3.29. (1) A division ring D is both left Noetherian and left Artinian.
(2) If R is a PID but not a field (e.g., $R = \mathbb{Z}$ or $R = K[x]$), then R is Noetherian but not Artinian. To see R is Noetherian, note that any ideal is of the form $I = (p_1^{e_1} \cdots p_t^{e_t})$ for some irreducible elements p_i and positive integers e_i. An ideal contains I if it corresponds to a product of the same irreducibles with smaller or equal multiplicities; there are only finitely many of these so an ascending chain must stablilize. To see R is not Artinian, take some irreducible p and take the chain
$$(p) \supsetneqq (p^2) \supsetneqq (p^3) \supsetneqq (p^4) \supsetneqq \cdots .$$
(3) A polynomial ring in infinitely many variables is neither Noetherian nor Artinian: there is an ascending chain
$$(x_1) \subsetneqq (x_1, x_2) \subsetneqq (x_1, x_2, x_3) \subsetneqq (x_1, x_2, x_3, x_4) \subsetneqq \cdots$$
and take a descending chain as in the last example.
(4) The $\mathbb{Z}$-module $M = \dfrac{\mathbb{Z}[\frac{1}{2}]}{\mathbb{Z}}$, where $\mathbb{Z}[\frac{1}{2}]$ is the subring of $\mathbb{Q}$ generated by $\mathbb{Z}$ and $\frac{1}{2}$, is Artinian but not Noetherian. Suppose that $N \subseteq M$ is generated by $\{[\frac{a_\lambda}{2^{n_\lambda}}]\}$, where each a_λ is odd (we can write any element in $\mathbb{Z}[\frac{1}{2}]$ like so). Observe that for each λ, there are integers s, t such that $sa_\lambda + t2^{n_\lambda} = 1$, so $s[\frac{a_\lambda}{2^{n_\lambda}}] = [\frac{1}{2^{n_\lambda}}]$. Thus, N is generated by $\{[\frac{1}{2^{n_\lambda}}]\}$. Thus, the submodules of M are M itself, 0, and $M_i = \dfrac{\mathbb{Z} \cdot \frac{1}{2^n}}{\mathbb{Z}}$ for $i > 0$. We have $0 \subsetneqq M_1 \subsetneqq M_2 \subsetneqq \cdots$ so M is not Noetherian. However, any descending chain is either always equal to M, or else has some M_i as a term, and there are finitely many submodules of such an M_i, so must stabilize.
(5) The subring of $M_2(\mathbb{Q})$ given as
$$\left\{ \begin{bmatrix} a & 0 \\ b & c \end{bmatrix} \mid a \in \mathbb{Z}, b, c \in \mathbb{Q} \right\}$$
is left Noetherian but not right Noetherian.

Optional Exercise 3.30. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. Then M has ACC (resp DCC) if and only if M' and M'' have ACC (resp. DCC).

The Noetherian condition is intimately tied to finite generation.

Proposition 3.31. *Let M be an R-module. Then M has ACC if and only if every submodule of M is finitely generated.*

Proof. Suppose that $N \subseteq M$ is not finitely generated. Then we can construct an ascending chain of submodules of M given by setting $N_0 = 0$, and $N_{i+i} = N_i + n_{i+1}$ for some $n_{i+1} \in N \setminus N_i$; we can do this since each N_i is a finitely generated submodule of N, so is not equal to N.

Now suppose that every submodule of M is finitely generated. Given a countable ascending chain of submodules

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq M_4 \subseteq \cdots$$

let $N = \bigcup_{n\in\mathbb{N}} M_n$; this is a submodule of M. Take a finite generating set $\{n_1, \ldots, n_t\}$ for N. For each $i = 1, \ldots, t$, we have $n_i \in M_j$ for some j. Since there are finitely many n_i's there is some M_j that contains them all. But then $M_j = N$, so the chain stabilizes (i.e., achieves a maximum element). □

Proposition 3.32. *Let R be left Noetherian. Then a module is finitely generated if and only if it is left Noetherian. In particular, in a left Noetherian ring, every submodule of a finitely generated module is finitely generated.*

Proof. For the first statement, the "if" implication holds in general without the hypothesis on R. For the other implication, observe that there are short exact sequences

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

for all $n > 0$. So, by the exercise above and induction on n, every finitely generated free module is Noetherian. Now, if M is finitely generated, there is a short exact sequence of the form

$$0 \to K \to R^n \to M \to 0$$

so by the exercise above again, M is Noetherian.

The second statement follows from the first as a submodule of a Noetherian module is Noetherian, again by the exercise. □

Now we tie these chain conditions to length.

Proposition 3.33. *A module M has finite length if and only if it is both Noetherian and Artinian.*

Proof. Assume that M has finite length. Suppose that M is not Noetherian. Then there is a chain

$$M_0 \subsetneqq M_1 \subsetneqq M_2 \subsetneqq \cdots$$

Since each M_i is a submodule of M, its length is finite, and is a nonnegative integer. Then $\ell(M_0) < \ell(M_1) < \ell(M_2) < \cdots \leqslant \ell(M)$, which yields a contradiction. The argument that M is Artinian is similar.

Now assume that M is both Noetherian and Artinian. We will construct a composition series for M. We can assume that $M \neq 0$. Consider the collection of proper submodules of M. This is nonempty, so has a maximal element M^1 by the Noetherian hypothesis. We must have M/M^1 is simple, or else there is a module in between M^1 and M. Using Noetherianity again, if $M^1 \neq 0$ (we're done otherwise), there is a maximal proper submodule of M^1; call it M^2. This process yields a descending chain with simple quotients, and this must stop (i.e., yield $M^i = 0$ for some i) by the Artinian hypothesis. Thus, there is a composition series for M. □

Lecture of October 25, 2021

3.4. **Semisimple modules.** We now study an important condition that is somewhat orthogonal (yet somewhat related) to our chain conditions. The condition of finite length, and to some extent the Noetherian and Artinian conditions, were related to how a module is made out of building blocks, or how big it is in terms of its pieces. The condition of semisimplicity says that a module is composed of basic building blocks in the simplest possible way.

Definition 3.34. For any ring R, a left R-module M is called *semisimple* if it is a (possibly infinite) direct sum of simple modules. The empty direct sum is allowed, so that the 0 module *is* considered to be semisimple.

Example 3.35. Let M be a finitely generated $\mathbb{Z}$-module. Then by the FTFGAG, M is isomorphic to $\mathbb{Z}^r \oplus \mathbb{Z}/p_1^{e_1} \oplus \cdots \oplus \mathbb{Z}/p_n^{e_n}$ for some $r \geqslant 0$, $n \geqslant 0$, primes p_i and positive integers e_i. Such a module is semisimple if and only if $r = 0$ and $e_i = 1$ for all i.

Example 3.36. Every module over a division ring D is semisimple because any such module has a basis, hence it is a free module.

Lemma 3.37. *Let D be a division ring and set $R = M_n(D)$ for some $n \geqslant 1$. I claim R is semisimple as a left module over itself.*

Proof. For each $1 \leqslant i \leqslant n$, let I_i denote the subset of R consisting of matrices whose only nonzero entires belong to the i-th column. The rules for matrix addition and multiplication show that I_i is a left ideal (i.e., a left submodule) of R. Moreover, there is evident bijection between I_i and D^n (column vectors) and this bijection is an isomorphism of left R-modules. We proved D^n is simple as an R-module and hence so is I_i. Finally, R is the internal direct sum of $I_1, \ldots, I_n$:

$$R = I_1 \oplus \cdots \oplus I_n$$

because each matrix X is uniquely a sum of the form $X_1 + \cdots + X_n$ with $X_i \in M_i$. □

Optional Exercise 3.38. Let $\{M_\lambda\}_{\lambda \in \Lambda}$ be an infinite collection of nonzero modules. Then $\bigoplus_{\lambda \in \Lambda} M_\lambda$ is not finitely generated.

Remark 3.39. As a consequence of the above exercise, a module is a finitely generated semisimple module if and only if it is a finite direct sum of simple modules. In this case if we write $M = M_1 \oplus \cdots \oplus M_n$ as a sum of simple modules, there is a strict composition series

$$0 \subset M_1 \subset M_1 \oplus M_2 \subset \cdots \subset M_1 \oplus \cdots \oplus M_{n-1} \subset M$$

so M has finite length, namely length n, and the composition factors are the modules M_i.

Proposition 3.40 (Krull-Schmidt for semisimple modules)**.** *Let M be a finitely generated semisimple module. Given two direct sum decompositions as simple modules*

$$M = M_1 \oplus \cdots \oplus M_m = N_1 \oplus \cdots \oplus N_n$$

then $m = n$, and there is a permutation σ such that $M_{\sigma(i)} \cong N_i$ for all i.

Proof. Follows from the previous remark and the Jordan-Holder theorem. □

Theorem 3.41 (Equivalent conditions for semisimple modules)**.** *For any ring R and left R-module M, the following are equivalent:*

(1) *M is semisimple,*
(2) *every submodule of M is a summand; i.e., for every submodule N of M there is a submodule N' such that $M = N \oplus N'$ is the internal direct sum of N and N',*
(3) *every injective R-map $i : M' \to M$ is split has a left inverse,*
(4) *every SES of the form $0 \to M' \to M \to M'' \to 0$ is split exact,*
(5) *every surjective R-map $p : M \to M''$ has a right inverse.*

Proof. The equivalence of (3), (4), and (5) is given by the Splitting Theorem.

(2) $\Rightarrow$ (3) holds since given an injective map i as in (3), we have by (2) that $i(M')$ is a summand of M, hence there is a projection homomorphism $\pi : M \to i(M')$ that splits the inclusion of the summand into M, that is $\pi|_{i(M')} = \mathrm{id}_{i(M')}$. Now $i : M' \to i(M')$ is an isomorphism so we may consider the R-module homomorphism $i^{-1} : i(M') \to M'$ and set $q : M \to M'$ to be $q = i^{-1} \circ \pi$. Then

$$q \circ i = i^{-1} \circ \pi \circ i = i^{-1} \circ \pi_{i(M')} \circ i = i^{-1} \circ i = \mathrm{id}_{M'}.$$

(3) $\Rightarrow$ (2) holds since we can split the inclusion $N \to M$ and thus also the SES

$$0 \to N \to M \to M/N \to 0.$$

Therefore the Splitting Theorem yields $M = N \oplus s(M/N)$ where s denotes the splitting of the quotient map $M \to M/N$.

The hard part is proving (1) $\Leftrightarrow$ (2). (1) $\Rightarrow$ (2) Assume (1), so that $M = \oplus_{\lambda \in \Lambda} M_\lambda$ for some collection of simple submodules M_λ, and let $N \subseteq M$ be any submodule. (It is important to note that it does not necessarily follow that N is a sum of some subcollection of the M_λ) . Consider the collection $\mathcal{S}$ of subsets Γ of Λ such that $N \cap M_\Gamma = 0$ where we define $M_\Gamma := \oplus_{\lambda \in \Gamma} M_\lambda$. View $\mathcal{S}$ as a poset by inclusion. It is nonempty since $J = \varnothing$ belongs to $\mathcal{S}$. If $\{\Gamma_\alpha\}$ is a totally ordered subcollection of $\mathcal{S}$, let $\Gamma = \cup_\alpha \Gamma_\alpha$. I claim $M_\Gamma \cap N = 0$. If not, there is a nonzero element $(m_\gamma) \in M_\Gamma \cap N$. But since $m_\gamma = 0$ for all but a finite number of γ's and since the collection of Γ_α's was totally ordered, there is some α such that $(m_\gamma) \in M_{\Gamma_\alpha} \cap N$, a contradiction. We may thus apply Zorn's Lemma to get a maximal $\Gamma \in \mathcal{S}$.

I claim M is the internal direct sum of N and M_Γ. We have $N \cap M_\Gamma = 0$ since $\Gamma \in \mathcal{S}$ and so it suffices to prove $N + M_\Gamma = M$. Since $M = \sum_{\lambda \in \Lambda} M_\lambda$, the latter is equivalent to proving that $M_\lambda \subseteq N + M_\Gamma$ for all $\lambda \in \Lambda$. If this fails for some λ, then since $M_\lambda \cap (N + M_\Gamma)$ is a proper submodule of M_λ, which is simple, and hence $M_\lambda \cap (N + M_\Gamma) = 0$. But then $N \cap (M_\Gamma \oplus M_\lambda) = 0$ (if $n \in N$ and $n = m + m'$, with $m \in M_\Gamma$ and $m' \in M_\lambda$, then $m' = n - m$ so $m' = 0$ and $n = m$, and then $n = 0$.) So, $\Gamma \cup \{\lambda\}$ is a member of $\mathcal{S}$ that strictly contains Γ, a contradiction. It must be thar $M = N \oplus M_\Gamma$.

Lecture of October 27, 2021

(2) $\Rightarrow$ (1) Now assume that every submodule of M is a summand. We proceed in three steps:

(i) We claim that every submodule T of M inherits this property; i.e., every submodule of T is a summand of T. For say $U \subseteq T$ is a submodule. By assumption on M, we have $M = U \oplus V$ (internal direct sum) for some V. Since $U \subseteq T$, it follows that $T = U + (V \cap T)$. (Given $t \in T$, we have $t = u + v$ for some $u \in U, v \in V$. Since $U \subseteq T$, $v = t - u \in V \cap T$.) Since $U \cap (V \cap T) = 0$, this shows $T = U \oplus (V \cap T)$.

(ii) We claim that every nonzero submodule T of M contains a simple summand. Pick $0 \neq x \in T$ and apply Zorn's Lemma to show that there is a maximal submodule U of T with respect to the property that $x \notin U$. We have $T = U \oplus W$ by (i) for some $W \neq 0$. If W is not simple, then W contains a nonzero, proper submodule W_1 and hence, by using (i) again, we get that $W = W_1 \oplus W_2$ for some proper nonzero submodule W_2.

These properties implies that $(U \oplus W_1) \cap (U \oplus W_2) = U$. One containment is clear. If v belongs to the left side, then $v = u + w_1 = u' + w_2$. It follows that $w_1 - w_2 = u - u' \in U \cap W = 0$ and so $w_1 = w_2 \in W_1 \cap W_2 = 0$, and hence $w_1 = w_2 = 0$. So, either $x \notin U \oplus W_1$ or $x \notin U \oplus W_2$, and either way we reach a contradiction to the maximality of U.

(iii) Let $\mathscr{G}$ be the set of all simple submodules of M, and let

$$\mathscr{F} = \{\Omega \subseteq \mathscr{G} \mid \text{for all distinct } \omega_0, \omega_1, \ldots, \omega_t \in \Omega, \omega_0 \cap (\omega_1 + \cdots + \omega_t) = 0\}.$$

Equivalently, the module generated by the modules in Ω their direct sum. The set $\mathscr{F}$ is partially ordered by inclusion. It is nonempty, since $\varnothing \in \mathscr{F}$ (or some singleton is in there by (ii)). Given a chain $\{\Omega_\alpha\}$ in $\mathscr{F}$, $\bigcup_\alpha \Omega_\alpha$ is again an element of $\mathscr{F}$, so there is a maximal element in $\mathscr{F}$; call it Ω. Let U be the direct sum of Ω.

We claim that $U = M$. By hypothesis we have $M = U \oplus V$ for some V. If $V = 0$ we are done. Otherwise by (ii) (and (i) again) we have $V = S \oplus V'$ for some simple submodule S. But then $\Omega \cup \{U\} \in \mathscr{F}$, contradicting maximality of Ω. □

Corollary 3.42. *If M semisimple, so is every submodule and quotient module of M.*

Proof. Say $N \subseteq M$ is a submodule. By the claim marked (i) in the proof of Theorem 3.41 every submodule of N is a summand, and hence N is semisimple by Theorem 3.41 (2) $\Rightarrow$ (1).

Given a surjection $M \twoheadrightarrow P$, it splits by Theorem 3.41, so that P is isomorphic to a submodule of M, namely the image of P under the splitting map. Hence P is semisimple by the case already proven. □

A major source of semisimple modules comes from group rings.

3.5. **Semisimple rings and the Artin-Wedderburn theorem.**

3.5.1. *Semisimple rings.*

Definition 3.43. A ring R is *left semisimple* if R is semisimple as a left module over itself. R is *right semisimple* if R is semisimple as a right modules over itself.

Remark 3.44. Recall that submodules of R are left ideals and the simple ones are the minimal (nonzero) left ideals. So, R is left semisimple if and only if R is the internal direct sum of some collection of minimal left ideals I_j:

$$R = \bigoplus_{j \in J} I_j.$$

Moreover, R is f.g. as a module over itself, and so this must be a finite direct sum. So, R is left semisimple if and only if R decomposes as an internal direct sum of the form $R = I_1 \oplus \cdots \oplus I_m$ for some finite collection $I_1, \ldots, I_m$ of minimal left ideals.

Example 3.45. For any $n \geqslant 0$ and division ring D, the matrix ring $M_n(D)$ is left semisimple. This was shown earlier. It is also right semisimple.

Example 3.46. If $R = K_1 \times \cdots \times K_t$ is a finite product of fields, then each K_i is a simple R-module, and R is the direct sum of these, so R is (left) semisimple.

Proposition 3.47. *For a ring R, the following conditions are equivalent:*

(1) *R is a left semisimple ring.*
(2) *Every left R-module is semisimple.*

(3) *Every SES of left R-modules is split.*
(4) *Every injection $i : M' \hookrightarrow M$ of left R-modules splits.*
(5) *Every surjection $p : M \twoheadrightarrow M''$ of left R-modules splits.*
(6) *Every left R-module is projective.*
(7) *Every left R-module is injective.*

Proof. The equivalence of (2)–(5) follows from Proposition 3.41. The equivalence of (4) and (7) follows from the characterization of injective modules in Proposition 2.88 and the equivalence of (5) and (6) follows from the characterization of projective modules in Proposition 2.80. The implication (2) $\Rightarrow$ (1) is obvious.

Now for (1) $\Rightarrow$ (2): Assume (1) and let M be any left R-module. It follows from the definition that an arbitrary coproduct of semisimple modules is again semisimple, and so the free module $\bigoplus_\Lambda R$ is semisimple for any indexing set Λ. By choosing a generating set of M , we may find a surjection of the form $p : \oplus_\Lambda R \twoheadrightarrow M$. By Corollary 3.42, it follows that M is semisimple since it is a quotient of a semisimple module $M \cong \oplus_\Lambda R/\ker(p)$. □

Lecture of October 29, 2021

Proposition 3.48. *Let R be a left semisimple ring and write $R = I_1 \oplus \cdots \oplus I_m$ as an internal direct sum with $I_1, \ldots, I_m$ minimal left ideals. Let $J_1, \ldots, J_n$ be a complete list of representatives of isomorphism classes as left R-modules taken from the list $I_1, \ldots, I_m$; so, for each i with $1 \leqslant i \leqslant m$, there is a unique j with $1 \leqslant j \leqslant l$ so that $I_i \cong J_j$ as left R-modules.*

Then every R-module is isomorphic to $J_1^{\oplus\Lambda_1} \oplus \cdots \oplus J_n^{\oplus\Lambda_n}$ for some index sets $\Lambda_1, \ldots, \Lambda_n$.

If M is finitely generated, M is isomorphic to $J_1^{\oplus e_1} \oplus \cdots \oplus J_n^{\oplus e_n}$ for a unique list $e_1, \ldots, e_n$ of nonnegative integers.

Proof. If M is finitely generated there is a surjection $R^a \twoheadrightarrow M$. Using Proposition 3.47 this surjection splits, so that $R^n \cong M \oplus N$ for some N, and each of M and N is semisimple and finitely generated. So $M = \oplus_{i=1}^s M_i$ and $N = \oplus_{j=1}^s N_j$ with M_i, N_j simple. Clearly R^n is isomorphic to a finite direct sum of copies of the J_i's, and so the result follows from the Krull-Schmidt Theorem for semisimple modules.

In the general case, we know that M is a direct sum of simple modules; if some simple summand N of M is not isomorphic to one of the J_i, then N is a finitely generated counterexample to the f.g. case. □

In short, if R is left semisimple, and we know the simple decomposition of R itself, then we have a complete classification of *all* R-modules: they are just direct sums of the simple summands of R!

Much of the interest in semisimple rings arises from the following:

Theorem 3.49 (Maschke's Theorem)**.** *If K is a field and G is a finite group such that* $\mathrm{char}(K)$ *does not divide $|G|$, then the group ring $K[G]$ is left semisimple.*

Proof. Let $i : N \to M$ be any injection of left $K[G]$-modules. It suffices to prove that there is an $K[G]$-linear map $p : M \to N$ such that $p \circ i = \mathrm{id}_N$. By restriction of scalars along the inclusion $K \subseteq K[G]$, we may regard i as a K-linear map between K-vector spaces. As such it admits a K-linear splitting $f : M \twoheadrightarrow N$ (since K is semisimple). There is no reason that f will be $K[G]$-linear, but we can modify it so that it becomes so: Define $p : M \to N$ by

$$p(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1} f(gm).$$

Note that the formula makes sense since $|G|$ is invertible in K by assumption.

Then p is still a K-linear map (since f is K-linear and the group action is K-linear). For any $h \in G$ we have

$$p(hm) = \frac{1}{|G|}\sum_{g\in G} g^{-1}f(ghm) = \frac{1}{|G|}\sum_{x\in G} hx^{-1}f(xm) = hp(m),$$

where the second equality is given by identifying x with gh. These conditions ensure that p is $K[G]$-linear. Finally,

$$p(i(n)) = \frac{1}{|G|}\sum_{g\in G} g^{-1}f(gi(n)) = \frac{1}{|G|}\sum_{g\in G} g^{-1}f(i(gn)) = \frac{1}{|G|}\sum_{g\in G} g^{-1}gn = \frac{1}{|G|}\sum_{g\in G} n = n$$

where the second equality uses that i is $K[G]$-linear and the third one uses that $f \circ i = \mathrm{id}$. □

Remark 3.50. The proof actually shows that $K[G]$ is semisimple provided K is and $|G|$ is invertible in K.

Example 3.51. The group ring $R = \mathbb{F}_p[C_p]$ does not satisfy the hypotheses of Maschke's theorem, since the order of the group is zero in the field. In fact, $\mathbb{F}_p[C_p]$ is not semisimple: let $V = \mathbb{F}_p^2$ be the $C_p = \langle g\rangle$ representation $g^n \mapsto \begin{bmatrix} 1 & 0 \\ \lambda n & 1 \end{bmatrix}$; i.e., as a $\mathbb{F}_p[C_p]$-module, we have $g \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ a+b \end{bmatrix}$. We claim that $U = \left\{ \begin{bmatrix} 0 \\ b \end{bmatrix} \right\}$ is the unique nonzero proper submodule of V. Let $W \subseteq V$ be a nonzero submodule and suppose that $U \neq W$. Then, there is some element $v = \begin{bmatrix} a \\ b \end{bmatrix} \in W$ with $a \neq 0$. Then v and gv are linearly independent, so we must have $W = V$. It follows that V is not semisimple: it is not simple since $0 \subsetneqq U \subsetneqq V$, but V is not a direct sum of simple modules.

Let G be a finite group and K a field. The representation of G corresponding to $K[G]$ viewed as a left module over itself can be described explicitly as following: As a K-vector space, $K[G]$ has G as a basis: $K[G] = \oplus_{g\in G} k \cdot g$. G acts on this vector space by permuting the basis via left multiplication: $h \cdot (\sum_g c_g g) = \sum_g c_g(hg)$. This is sometimes called the *(left) regular representation of G*.

Corollary 3.52 (Corollary of Maschke's Theorem)**.** *If G is a finite group and K is a field such that* $\mathrm{char}(K) \nmid |G|$*, then every K-linear representation of G is a direct sum of irreducible representations, and every finite dimensional representation is uniquely a finite direct sum of irreducible ones.*

Moreover, every irreducible representation arises as a summand of the left regular representation.

Example 3.53. Let $G = C_3$. We can use Maschke's Theorem and the theory of semisimple rings so far to classify every representation of G over $\mathbb{R}$ or over $\mathbb{C}$ (or more generally over any field of characteristic not equal to 3). In any case, the left regular representation V of C_3 is the three-dimensional representation with basis $\{1, g, g^2\}$ such that $g \cdot 1 = g, g \cdot g = g^2, g \cdot g^2 = 1$, i.e.,

$$g \mapsto \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

in this basis. Also in any case, the subspace W spanned by $1 + g + g^2$, which is the vector $(1, 1, 1)$ in these coordinates, is a 1-dimensional G-stable subspace, so a simple subrepresentation. Moreover, this is the trivial representation, since this vector is fixed by g. Then V/W obtains the structure of a representation. We can take $1 + W, g + W$ as a basis for V/W, and $g \cdot (1 + W) = g + W$, and $g \cdot (g + W) = g^2 + W = -1 - g + W$, i.e., in our coordinates,

$$g \mapsto \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

A G-stable subspace must correspond to an eigenvector of g (which is equivalently an eigenvector of g^{-1}). The characteristic equation of this matrix shows that the eigenvalues are precisely the primitive cube roots of unity.

If $K = \mathbb{R}$ (or more generally if there are no primitive cube roots of unity), then the 2-dimensional representation V/W we just found is simple since there are no stable subspaces. If $K = \mathbb{C}$ (or more generally if there are primitive cube roots of unity), let ω be a primitive cube root of unity. The 2-dimensional representation V/W has ω and ω^2 as eigenvalues, and there are corresponding eigenvectors, so V/W is a direct sum of two 1-dimensional stable subspaces T, T' such that $g \cdot t = \omega t$ for all $t \in T$ and $g \cdot t' = \omega^2 t'$ for all $t' \in T'$.

Lecture of November 1, 2021

We conclude that *every* real representation of C_3 is isomorphic to a direct sum of copies of the trivial representation and copies of V/W. That is, for any such representation U, there is a basis of U, $\{e_\alpha\}_{\alpha \in A}$, $\{e'_\beta, e''_\beta\}_{\beta \in B}$, such that $g \cdot e_\alpha = e_\alpha$, $g \cdot e'_\beta = e''_\beta$, and $g \cdot e''_\beta = -e'_\beta - e''_\beta$.

We conclude that *every* complex representation of C_3 is isomorphic to a direct sum of copies of the trivial representation, T, and T'. That is, for any such representation U, there is a basis of U, $\{e_\alpha\}_{\alpha \in A}$, $\{e'_\beta\}_{\beta \in B}$, $\{e''_\gamma\}_{\gamma \in C}$, such that $g \cdot e_\alpha = e_\alpha$, $g \cdot e'_\beta = \omega e'_\beta$, and $g \cdot e''_\gamma = e''_\gamma$.

3.5.2. *Artin-Wedderburn Theorem.* We will now give a classification of *all* left semisimple rings. To start, we collect some examples.

Lemma 3.54. *If R and S are left semisimple, so is the product ring $R \times S$.*

Proof. Say we have internal direct sum decompositions $R = I_1 \oplus \cdots \oplus I_m$ and $S = J_1 \oplus \cdots \oplus J_n$ involving minimal left ideals. Then for all a and b, $I_a \times \{0\}$ and $\{0\} \times J_b$ are minimal left ideals of $R \times S$ and they determine an internal direct sum decomposition of $R \times S$. □

Example 3.55. The previous lemma and Lemma 3.37 show that for any integer $m \geqslant 0$, list of division rings $D_1, \ldots, D_m$ and positive integers $n_1, \ldots, n_m$, the ring

$$R = \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_m}(D_m)$$

is left semisimple.

The Artin-Wedderburn Theorem asserts that the last example accounts for *all* examples!

Theorem 3.56 (Artin-Wedderburn Theorem)**.** *Let R be a left semisimple ring. Then for some $m \geqslant 0$, positive integers $n_1, \ldots, n_m$, and division rings $D_1, \ldots, D_m$, there is a ring isomorphism*

$$R \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_m}(D_m).$$

Moreover,

1. *m is the number of isomorphism classes of simple left R-modules.*
2. *Say $M_1, \ldots, M_m$ are simple modules forming a complete set of representatives of these isomorphism classes. Then, after reordering, $D_i \cong \mathrm{End}_R(M_i)^{\mathrm{op}}$ and*
3. *n_j is the number of times summands isomorphic to M_j occur in the decomposition of R into a direct sum of simple left modules.*

Moreover, the data $(m; n_1, \ldots, n_m; D_1, \ldots, D_m)$ is unique up to a permutation of $\{1, \ldots, m\}$ and isomorphisms of division rings.

Example 3.57. We saw before that the module decomposition in terms of simple modules is $\mathbb{R}[C_3] = W \oplus U$, where W is the one-dimensional trivial representation, and U is the 2-dimensional representation given by $g \mapsto \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$. On the other hand, as rings,

$$\mathbb{R}[C_3] \cong \mathbb{R}[g]/(g^3 - 1) \cong \mathbb{R}[g]/(g-1) \times \mathbb{R}[g]/(g^2 + g + 1) \cong \mathbb{R} \times \mathbb{C}.$$

To reconcile these decompositions by the Artin-Wedderburn Theorem, one can check that $\mathrm{End}_{\mathbb{R}[C_3]}(W) \cong \mathbb{R}$ and $\mathrm{End}_{\mathbb{R}[C_3]}(V/W) \cong \mathbb{C}$.

We have $\mathrm{End}_{\mathbb{R}[C_3]}(W) \cong \mathbb{R}$. To compute the endomorphism ring of V/W, observe that an $\mathbb{R}$-linear endomorphism of V/W is $\mathbb{R}[C_3]$-linear if and only if it commutes with the action of g. We can write any $\mathbb{R}$-linear endomorphism of V/W as a 2×2 matrix; for it to commute with g means it commutes with $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}$. We have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} - \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} b+c & -a-b+d \\ d-a+c & -b-c \end{bmatrix},$$

so the matrices we seek are of the form

$$\begin{bmatrix} a & -c \\ c & a-c \end{bmatrix} = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + c \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}.$$

Any pair of matrices in this set commutes (since the two vectorspace generators do) so they form a commutative ring and hence a field by Schur's Lemma; any matrix in this collection is algebraic over the subring of scalar matrices (since both generators are). It follows that this collection of matrices is isomorphic as a ring to $\mathbb{C}$.

Lecture of November 3, 2021

Lemma 3.58. *Let M be an R-module. The map*

$$\begin{aligned} \mathrm{End}_R(M^{\oplus n}) &\xrightarrow{\Theta} \mathrm{Mat}_n(\mathrm{End}_R(M)) \\ \phi &\longmapsto [\pi_i \phi \iota_j]_{i,j} \end{aligned}$$

is a ring isomorphism, where ι_k and π_k denote the natural inclusion and projection maps.

Proof. It is clear that this map is additive, as each ι_i and π_j is. Observe that $\pi_j \iota_i$ is the identity on M if $i = j$, and the zero map otherwise and that $1_{M^{\oplus n}} = \sum_k \iota_k \pi_k$.

The map

$$\begin{aligned} \mathrm{End}_R(M^{\oplus n}) &\xleftarrow{\zeta} \mathrm{Mat}_n(\mathrm{End}_R(M)) \\ \textstyle\sum_{i,j} \iota_i \alpha_{i,j} \pi_j &\longleftarrow [\alpha_{i,j}]_{i,j} \end{aligned}$$

is a two-sided inverse for Θ:

$$\zeta(\Theta(\phi)) = \zeta([\pi_i \phi \iota_j]_{i,j}) = \sum_{i,j} \iota_i \pi_i \phi \iota_j \pi_j = (\sum_i \iota_i \pi_i) \phi (\sum_j \iota_j \pi_j) = \phi, \quad \text{and}$$

$$\Theta(\zeta([\alpha_{i,j}]_{i,j}))_{k,\ell} = \Theta(\sum_{i,j} \iota_i \alpha_{i,j} \pi_j)_{k,\ell} = \pi_k (\sum_{i,j} \iota_i \alpha_{i,j} \pi_j) \iota_\ell = \sum_{i,j} (\pi_k \iota_i) \alpha_{i,j} (\pi_j \iota_\ell) = \alpha_{k,\ell}.$$

To see that Θ respects multiplication, we have

$$[\Theta(\psi)\Theta(\phi)]_{i,j} = \sum_k (\pi_i \psi \iota_k)(\pi_k \phi \iota_j) = \pi_i \psi \phi \iota_j = \Theta(\psi\phi)_{i,j}.$$

□

Optional Exercise 3.59. Let D be a division ring. Then $\mathrm{End}_{\mathrm{Mat}_n(D)}(D^n) \cong D^{\mathrm{op}}$, where D^n is the simple module of column vectors.

We now come to the main theorem regarding semisimple rings

Proof. Since R is left semisimple, we have $R \cong I_1 \oplus \cdots \oplus I_t$ with each I_i is simple (in fact a minimal ideal). Group by isomorphism to rewrite this as $R \cong M_1^{\oplus n_1} \oplus \cdots \oplus M_m^{\oplus n_m}$ with each M_i simple, $n_j \geqslant 1$, and such that M_i is not isomorphic to M_j for all $i \neq j$. We compute the endomorphisms of both sides:

$$\begin{aligned}
\mathrm{End}_R(R) &= \mathrm{Hom}_R(\bigoplus_{i=1}^m M_i^{\oplus n_i}, \prod_{j=1}^m M_j^{\oplus n_j}) \cong \prod_j \mathrm{Hom}_R(M_i^{\oplus n_i}, \prod_i M_i^{\oplus n_j}) \\
&\cong \prod_{i=1}^m \prod_{j=1}^m \mathrm{Hom}_R(M_i^{\oplus n_i}, M_j^{\oplus n_j}) \\
&= \prod_{i=1}^m \mathrm{Hom}_R(M_i^{\oplus n_i}, M_i^{\oplus n_i}) \\
&= \prod_{i=1}^m \mathrm{End}_R(M_i^{\oplus n_i}) \cong \prod_{i=1}^m \mathrm{Mat}_{n_i}(\mathrm{End}_R(M_i)).
\end{aligned}$$

Above the second line follows from the first by properties of Hom, the third follows because Schur's lemma gives that $\mathrm{Hom}_R(M_i, M_j) = 0$, and consequently $\mathrm{Hom}_R(M_i^{\oplus n_i}, M_j^{\oplus n_j}) = 0$, when $i \neq j$. The final isomorphism is the previous lemma.

On the one hand, we have $\mathrm{End}_R(R) \cong R^{\mathrm{op}}$ by a problem from the homework. On the other hand, applying Schur's Lemma again, $D_i' := \mathrm{End}_R(M_i)$ is a division ring for all i.

Combining these gives

$$R^{\mathrm{op}} \cong \mathrm{Mat}_{n_1}(D_1') \times \cdots \times \mathrm{Mat}_{n_m}(D_m')$$

and hence, also by a homework problem, we have

$$R \cong \left(\mathrm{Mat}_{n_1}(D_1') \times \cdots \times \mathrm{Mat}_{n_m}(D_m')\right)^{\mathrm{op}} \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_m}(D_m)$$

with $D_i := (D_i')^{\mathrm{op}} = \mathrm{End}_R(M_i)^{\mathrm{op}}$.

This shows that given a decomposition of R as a left semisimple module, there is a ring decomposition as a product of matrix rings over division rings, and the data of division rings and matrix sizes is related to the data of simple modules and multiplicities by the formulas (1)–(3). We just need to prove uniqueness.

Say we are given an isomorphism of rings $R \cong \prod_{i=1}^k \mathrm{Mat}_{t_i}(Q_i)$ for some division rings $Q_1, \ldots, Q_k$. Then since $\mathrm{Mat}_{t_i}(Q_i)$ decomposes as a direct sum of t_i copies of $N_i := Q_i^{t_i}$, and N_i is a simple $\mathrm{Mat}_{t_i}(Q_i)$-module, hence also a simple R-module, we have a semisimple R-module decomposition of R as

$$M_1^{\oplus n_1} \oplus \cdots \oplus M_m^{\oplus n_m} \cong R \cong N_1^{\oplus t_1} \oplus \cdots \oplus N_k^{\oplus t_k}.$$

By Krull-Schmidt, we must have $m = k$, and after a permutation, $M_i \cong N_i = Q_i^{\oplus t_i}$ and $n_i = t_i$ for each i.

Moreover, we have

$$D_i \cong \mathrm{End}_R(M_i)^{\mathrm{op}} \cong \mathrm{End}_R(N_i)^{\mathrm{op}}.$$

We recall that $N_i \cong Q_i^{\oplus n_i}$, with the natural column vector action from $\mathrm{Mat}_{n_i}(Q_i)$, and the trivial action from the other factors. Thus,

$$\mathrm{End}_R(N_i)^{\mathrm{op}} = \mathrm{End}_{\mathrm{Mat}_{n_i}(Q_i)}(Q_i^{\oplus n_i})^{\mathrm{op}} \cong Q_i,$$

using the exercise above. □

Corollary 3.60. *A ring is left semisimple if and only if it is right semisimple.*

Proof. The claim is equivalent to showing R is left semisimple if and only R^{op} is, which in turn follows from just one of the implications. If R is left semisimple, then $R \cong \prod_i \mathrm{Mat}_{n_i}(D_i)$, so $R^{\mathrm{op}} \cong \prod_i \mathrm{Mat}_{n_i}(D_i)^{\mathrm{op}} \cong \prod_i \mathrm{Mat}_{n_i}(D_i^{\mathrm{op}})$ so R^{op} is left semisimple. □

Henceforth, we just say that R is *semisimple* if it is left semisimple.

3.6. **Applications to representation theory.** Let us start by restating the Artin-Wedderburn theorem in the context of group rings.

Theorem 3.61 (Artin-Wedderburn for group rings)**.** *If G is a finite group and K is a field such that $\mathrm{char}(K) \nmid |G|$, then there is an isomorphism of rings*

$$K[G] \cong \mathrm{Mat}_{n_1}(D_1) \times \cdots \times \mathrm{Mat}_{n_m}(D_m),$$

where $D_1, \ldots, D_m$ are division rings. Furthermore, each D_i contains K (up to isomorphism) as a subring of its center and the above isomorphism is K-linear. In particular, $\dim_K(D_i) < \infty$.

Moroever, we have:

1. *m is the number of irreducible k-linear representation of G (up to isomorphism),*
2. *the D_i's are the opposite rings of the endomorphism rings of these representations,*
3. *the n_j's give the number of times each irreducible representation occurs in the decomposition of the regular representation of G,*
4. *the numbers $n_1 \cdot \dim_k(D_1), \ldots, n_m \cdot \dim_k(D_m)$ give the dimensions of these representations, and*
5. *$n_1^2 \cdot \dim_k(D_1) + \cdots + n_m^2 \cdot \dim_k(D_m) = |G|$.*

Proof. This mostly follows from Artin-Wedderburn and Maschke's Theorem. What needs to be noted is that each division ring here contains a copy of K in its center. Indeed, we recall that each D_i is given as the opposite ring of $\mathrm{End}_{K[G]}(M_i)$ for some simple module M_i. For $\lambda \in K$, we have the map $M_i \xrightarrow{\lambda \cdot} M_i$ which commutes with any $K[G]$-linear map from M_i to itself. □

Lecture of November 5, 2021

Corollary 3.62. *Let G be a finite group, and K be a field such that $\mathrm{char}(K) \nmid |G|$. Then G is abelian if and only if $K[G]$ is isomorphic to a product of fields.*

Lemma 3.63. *Let G be any group and K any field. Given two group homomorphisms $\rho_1, \rho_2 : G \to K^\times = \mathrm{GL}_1(K)$, the associated $K[G]$-modules M_1 and M_2 are isomorphic if and only if $\rho_1 = \rho_2$.*

Proof. Suppose that $\alpha : M_1 \to M_2$ is an isomorphism of $K[G]$-modules. Identifying $M_1 = M_2 = K$ as vector spaces, we have $\alpha(k) = ck$ for some $c \neq 0$. Then,

$$c\rho_1(g)(k) = \alpha\rho_1(g)(k) = \rho_2(g)\alpha(k) = \rho_2(g)(ck) = c\rho_2(g)(k)$$

for all $k \in K$, so $\rho_1(g)(k) = \rho_2(g)(k)$ for all $k \in K$. □

Proposition 3.64. *If D is a division ring that contains $\mathbb{R}$ in its center and $\dim_{\mathbb{R}}(D) = 2$, then $D \cong \mathbb{C}$.*

Proof. Pick $x \in D \smallsetminus \mathbb{R}$. Then $\mathbb{R} \subsetneqq \mathbb{R}[x] \subseteq D$, and since $\mathbb{R}[x]$ is an $\mathbb{R}$-vectorspace, we must have $\mathbb{R}[x] = D$ for dimension reasons. Thus D is commutative and is a field. Since D is a finite extension of $\mathbb{R}$, it is algebraic, so $\mathbb{R} \subsetneqq D \subseteq \mathbb{C}$, and we must have $D = \mathbb{C}$. □

Example 3.65. Let $k = \mathbb{R}$ and $G = S_3$. We find all the simple modules over the ring $\mathbb{R}[S_3]$ or, equivalently, all irreducible $\mathbb{R}$-linear representations of S_3. We also find the Artin-Wedderburn decomposition of $\mathbb{R}[S_3]$.

The one dimensional represenatations are given by group homomorphisms of the form $S_3 \to \mathbb{R}^\times$, and any such map factors as

$$S_3 \twoheadrightarrow S_3^{\mathrm{ab}} \to \mathbb{R}^\times.$$

Note that $S_3^{\mathrm{ab}} = S_3/A_3 \cong C_2$ and there are two group homomorphisms $C_2 \to \mathbb{R}^\times$, sending the generator to either 1 or -1 (the only elements of $\mathbb{R}^\times$ of order 1 or 2). This gives two representations: $M_1 = \mathbb{R}$ with S_3 acting trivially and $M_2 = \mathbb{R}$ with S_3 acting by the sign representation. These are not isomorphic by the previous lemma.

We have that $1 = \dim_{\mathbb{R}}(M_1) = n_1 \cdot \dim_{\mathbb{R}}(D_1)$ so $n_1 = 1$ and $\dim_{\mathbb{R}}(D_1) = 1$, and likewise $1 = \dim_{\mathbb{R}}(M_2) = n_2 \cdot \dim_{\mathbb{R}}(D_2)$ so $n_2 = 1$ and $\dim_{\mathbb{R}}(D_2) = 1$. So, the Artin-Wedderburn decomposition starts as

$$\mathbb{R}[S_3] \cong \mathbb{R} \times \mathbb{R} \times \cdots .$$

Note that there are no further factors of $\mathbb{R}$, since we found all of the one-dimensional simple modules.

Recall also that S_3 acts on $\mathbb{R}^3$ by permuting the basis (corresponding to the group homomorphism $S_3 \to \mathrm{GL}_3(\mathbb{R})$ sending a permutation to its associated permutation matrix). The subspace $M_3 = \{(a, b, c) \in \mathbb{R}^3 \mid a + b + c = 0\}$ is a subrepresenation of $\mathbb{R}^3$ of dimension 2. We claim it is irreducible: Say $0 \neq (a, b, c) \in M_3$.

By applying a permutation and scaling appropriately we obtain an element of the form $(1, x, -1-x) \in M_3$ and hence $(1, -1-x, x) \in M_3$. Adding these gives $(2, -1, -1) \in M_3$ and hence $(-1, 2, -1) \in M_3$. The latter two are linearly independent and so must span M_3. This proves (a, b, c) generates M_3 as a left $\mathbb{R}[S_3]$-module and hence that M_3 is simple. Note that M_3 is not isomorphic to either M_1 nor M_2 by dimension considerations.

We have that $2 = \dim \mathbb{R}(M_3) = n_3 \cdot \dim_{\mathbb{R}}(D_3)$, so there are two possibilities.

(1) One possibility is $n_3 = 1$ and $\dim_{\mathbb{R}}(D_3) = 2$, in which case $D_3 \cong \mathbb{C}$, so the Artin-Wedderburn decomposition reads as
$$\mathbb{R}[S_3] \cong \mathbb{R} \times \mathbb{R} \times \mathbb{C} \times S$$
for some S. We must have $\dim_{\mathbb{R}}(S) = 2$. We know that S cannot have any one-dimensional simple modules (since we already accounted for all of the one-dimensional simple modules for $\mathbb{R}[S_3]$), so S cannot be $\mathbb{R} \times \mathbb{R}$. Then, for dimension reasons, we must have that $S \cong D_4$ with $\dim_{\mathbb{R}}(D_4) = 2$, so $S \cong \mathbb{C}$. But then
$$\mathbb{R}[S_3] \cong \mathbb{R} \times \mathbb{R} \times \mathbb{C} \times \mathbb{C}$$
would be commutative, which it is not, as S_3 is not abelian.

(2) The other possibility is $n_3 = 2$ and $D_3 = \mathbb{R}$. We obtain the AW decomposition
$$\mathbb{R}[S_3] \cong \mathbb{R} \times \mathbb{R} \times \mathrm{Mat}_2(\mathbb{R}).$$

(Alternatively, we could compute the endomorphism ring of M_3 and see that it contains only scalars.)

We have found the AW decomposition of $\mathbb{R}[S_3]$. As a consequence, we have identified all of the irreducible real representations of S_3.

3.6.1. *Algebraically closed fields.* When working over an algebraically closed field, the Artin-Wedderburn Theorem takes a simpler form.

Corollary 3.66 (Artin-Wedderburn for group rings over algebraically closed fields)**.** *If G is a finite group and K is an algebraically closed field such that* $\mathrm{char}(K) \nmid |G|$*, then there is an isomorphism of rings*

$$k[G] \cong \mathrm{Mat}_{n_1}(K) \times \cdots \times \mathrm{Mat}_{n_m}(K).$$

Moroever, we have:

(1) *m is the number of irreducible K-linear representation of G (up to isomorphism),*
(2) *the D_i's are the opposite rings of the endomorphism rings of these representations,*
(3) *the n_j's give the number of times each irreducible representation occurs in the decomposition of the regular representation of G,*
(4) *the n_j's also give the dimensions of these representations, and*
(5) $n_1^2 + \cdots + n_m^2 = |G|$.

Proof. The point is that in this setting, for each irreducible representation M_i, $D_i \cong \mathrm{End}_{K[G]}(M_i)^{\mathrm{op}}$ is equal to K. Let $\theta \in \mathrm{End}_{K[G]}(M_i)$. In particular, θ is a K-linear endomorphism of the finite dimensional vector space M_i. Since K is algebraically closed, θ has an eigenvaluse, say λ. Then $\theta - \lambda 1_{M_i}$ is a $K[G]$-linear endomorphism of M_i that is not injective, so by Schur's Lemma is must be 0. Thus, $\theta = \lambda 1_{M_i}$. □

Lecture of November 8, 2021

Example 3.67. Let $k = \mathbb{C}$ and consider the alternating group $G = A_4$ of order 12. We find all the simple modules over the ring $\mathbb{C}[A_4]$ or, equivalently, all irreducible $\mathbb{C}$-linear representations of A_4. We also find the Artin-Wedderburn decomposition of $\mathbb{C}[A_4]$.

As before we start by finding 1-dimensional representations given by group homomorphisms of the form $A_4 \to \mathbb{C}^\times$. Any such map factors as

$$A_4 \twoheadrightarrow A_4^{\mathrm{ab}} \cong C_3 \to \mathbb{C}^\times$$

and thus there are three nonisomorphic 1-dimensional representations given by $\rho_i : C_3 = \langle g \rangle \to \mathbb{C}^\times$, $\rho_i(g) = e^{\frac{2\pi i}{3}}$, with $i = 0, 1, 2$. Note that ρ_0 corresponds to the trivial representation. Also ρ_1 and ρ_2 make essential use of the fact that we are working over $\mathbb{C}$ as opposed to, say, $\mathbb{R}$ where there are no primitive cubic roots of 1.

With respect to the Artin-Wedderburn decomposition we have so far

$$\mathbb{C}[A_4] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_{n_4}(\mathbb{C}) \times \cdots \times \mathrm{Mat}_{n_m}(\mathbb{C}).$$

where $n_3, \ldots, n_m \geqslant 2$ because we have already found all the 1-dimensional representations ($n_i = 1$) above. Counting dimensions we obtain

$$12 = 1 + 1 + 1 + \sum_{i=4}^{m} {n_i}^2.$$

It is easy to see there is only one solution: $m = 4$ and $n_4 = 3$. Hence there is a unique up to isomorphism $\mathbb{C}$-linear irreducible representation of A_4 which is a 3 dimensional $\mathbb{C}$-vector space.

To exhibit such a representation, let A_4 act on $V = \mathbb{C}^4$ by permuting the standard basis elements and thus any vector in V. The subspace $W \subseteq V$ given by

$$W = \{(a, b, c, d) \mid a + b + c + d = 0\}$$

is an A_4-stable subspace. This is an irreducible representation: if $v \in W \smallsetminus 0$, after permuting and scaling, we can write $v = (1, x, y, -1 - x - y)$. We also have $(1, -1 - x - y, x, y)$ and $(1, y, -1 - x - y, x)$ in $\langle v \rangle$, so

the sum $(3,-1,-1,-1) \in \langle v \rangle$. Then $(-1,3,-1,-1)$ and $(-1,-1,3,-1)$ are also in $\langle v \rangle$, and these are three linearly independent vectors, so we must have $\langle v \rangle = W$.

Remark 3.68. Let's consider what the Artin-Wedderburn Theorem says about complex representations of finite abelian groups: the group ring must be a product of copies of $\mathbb{C}$, so every irreducible representation is one-dimensional. Thus, every representation is a sum of one-dimensional representations. Concretely, this means that there is a basis in which every group element acts as a diagonal matrix.

This special case actually just follows from basic facts in linear algebra. Let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be a representation. Then every $g \in G$ has finite order, so $g^k - 1$ for some k. This implies that the matrix $\rho(g)$ satisfies $\rho(g)^k = I_n$, so its minimal polynomial divides $x^k - 1$. This polynomial splits into distinct linear factors over $\mathbb{C}$, so $\rho(g)$ is diagonalizable for every $g \in G$. (So far, we've only used that G is finite.) Now, since g is abelian, we have $gh = hg$ for all $g, h \in G$, so $\rho(g)\rho(h) = \rho(h)\rho(g)$; i.e., the matrices commute. Commuting diagonalizable matrices are simultaneously diagonalizable; i.e., there is a basis as above.

Proposition 3.69. *Let G be a finite group. The number of one-dimensional complex representations of G (up to isomorphism) is $|G^{\mathrm{ab}}|$. Thus, in the Artin-Wedderburn decomposition of $\mathbb{C}[G]$, there are exactly $|G^{\mathrm{ab}}|$ copies of $\mathbb{C}$.*

Proof. We have that $\mathrm{Hom}_{\mathbf{Grp}}(G, \mathbb{C}^\times) \cong \mathrm{Hom}_{\mathbf{Ab}}(G^{\mathrm{ab}}, \mathbb{C}^\times)$, and by the discussion above, there are $|G^{\mathrm{ab}}|$ distinct one-dimensional representations of G^{ab}. □

Proposition 3.70. *For any finite group G, the number of irreducible complex representations (up to isomorphism) is equal to the number of conjugacy classes.*

Proof. We have

$$\mathbb{C}[G] \cong \mathrm{Mat}_{n_1}(\mathbb{C}) \times \cdots \times \mathrm{Mat}_{n_m}(\mathbb{C})$$

and m is the number of irreducible complex representations up to isomorphism. A key point is that the center of the right side is $\mathbb{C}I_{n_1} \times \cdots \times \mathbb{C}I_{n_m}$, which has dimension m as a complex vector space. Since this ring isomorphism is $\mathbb{C}$-linear, it induces a $\mathbb{C}$-linear isomorphism of the centers, and thus we just need to show that $\dim_{\mathbb{C}}(Z(\mathbb{C}[G]))$ is equal to the number of conjugacy classes.

Let $C_1, \ldots, C_h$ denote the conjugacy classes of G (i.e., the orbits for the action of G on itself by conjugation). For each i set $z_i = \sum_{g \in C_i} g \in \mathbb{C}[G]$. Then for all $x \in G$, $xz_ix^{-1} = \sum_{g \in C_i} xgx^{-1} = z_i$ and it follows that $z_i \in Z(\mathbb{C}[G])$. Since that z_i's are sums of disjoint subsets of a basis of $\mathbb{C}[G]$, they are linearly independent. Now say $\sum_g c_g g$ belongs to the center. Then for each $x \in G$,

$$\sum_g c_g xgx^{-1} = x(\sum_g c_g g)x^{-1} = \sum_g c_g g$$

and it follows that $c_g = c_h$ whenever g, h are conjugate. This proves that $Z(\mathbb{C}[G])$ is spanned by $z_1, \ldots, z_h$. We conclude that $h = \dim_{\mathbb{C}}(Z(\mathbb{C}[G])) = m$. □

Lecture of November 10, 2021

4. Homological Algebra

Homological algebra is the study of homology - a measure for the nonexactness of chain complexes which we shall define below.

4.1. **The category of chain complexes of R-modules.** Let's define "chain complex" carefully.

Definition 4.1. For a ring R, a *chain complex* of left R-modules is a pair consisting of

- a family of left R-modules indexed by $\mathbb{Z}$, $\{M_i\}_{i\in\mathbb{Z}}$
- a family of R-module homomorphisms $\{d_i : M_i \to M_{i-1}\}_{i\in\mathbb{Z}}$ such that $d_{i-1} \circ d_i = 0$ for all i, i.e., "$d^2 = 0$".

Such a pair is usually written as $(M_\bullet, d)$ or $(M_\bullet, d^M)$ or just $M_\bullet$. The map d (really, the family of maps) is called the *differential* of the chain complex. We may say that the *homological degree* of M_i is i.

Example 4.2. Infinitely many of the modules M_i in a chain complex could be zero of course. So, for example, a short exact sequence

$$0 \to M_2 \to M_1 \to M_0 \to 0$$

will be regarded as a chain complex with $M_i = 0$ for all $i \notin \{0, 1, 2\}$.

Example 4.3. For those who have taken (or will take) a course in algebraic topology, given a topological space X, we form a chain complex $C_\bullet(X) := C_\bullet(X; \mathbb{Z})$ over the ring $\mathbb{Z}$, called the *singular chain complex* associated to X, as follows.

- Define $C_n(X)$ to be the free $\mathbb{Z}$-module with basis given by the set of all continuous functions $\Delta^n \to X$ where Δ^n is the standard topological n-simplex:

  $$\Delta^n := \{(r_0, \ldots, r_n) \in \mathbb{R}^{n+1} \mid r_i \geqslant 0, \sum_i r_i = 1\}.$$

  For $n < 0$, $C_n(X) := 0$.
- The map $d_n : C_n(X) \to C_{n-1}(X)$ is the unique homomorphism of abelian groups sending a basis element $g : \Delta^n \to X$ to $\sum_{i=0}^n (-1)^i g \circ \alpha_i^n$ where $\alpha_i^n : \Delta^{n-1} \to \Delta^n$ is the map $(r_0, \ldots, r_{n-1}) \mapsto (r_0, \ldots, r_{i-1}, 0, r_i, \ldots, r_{n-1})$.

Since the singular chain complex associated to X is huge (the modules C_n are usually not finitely generated), in practice it is more convenient to work with X being a simplicial complex (union of simplices) and $C_\bullet(X)$ being the *simplicial chain complex* of X. This complex has

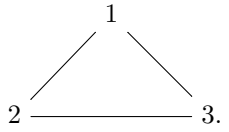
$$C_n(X) = \text{ the free } \mathbb{Z} \text{ module with basis given by the } n\text{-dimensional simplices of } X$$

and $d_n : C_n(X) \to C_{n-1}(X)$ is given by sending

$$d_n(\{r_0, \ldots, r_{n-1}\}) = \sum_{i=0}^{n} (-1)^i \{r_0, \ldots, \hat{r_i}, \ldots, r_n\}$$

where the hat indicates removing one vertex to get an $n-1$-dimensional simplex.

For a very concrete example, let's take X to be the following (hollow) triangle



This gives the simplicial chain complex

$$C_\bullet(X) : 0 \xrightarrow{d_2} \mathbb{Z}^3 \xrightarrow{d_1} \mathbb{Z}^3 \xrightarrow{d_0} 0,$$

where the maps $d_i = 0$ for $i \neq 0$ and the map d_1 is given by the following matrix

$$d_1 = \begin{bmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & -1 \end{bmatrix}$$

with respect to the ordered bases $\{1,2\},\{1,3\},\{2,3\}$ and $\{1\},\{2\},\{3\}$. Here $\{i\}$ denotes the map $\{i\} : \Delta^0 \to X$ which maps Δ^0 to the vertex i of X and $\{i,j\}$ denotes the map $\{i,j\} : \Delta^1 \to X$ which maps Δ^1 to the edge $[i,j]$ of X.

Definition 4.4. A *chain map* from one chain complex of left R-modules $(M_\bullet, d^M)$ to another $(N_\bullet, d^N)$ is a family of left R-module homomorphisms $f_i : M_i \to N_i$, for $i \in \mathbb{Z}$, such that $d^N_i \circ f_i = f_{i-1} \circ d^M_i$ for all i. We often write a chain map as just $f : (M_\bullet, d^M) \to (N_\bullet, d^N)$, or even just $f : M_\bullet \to N_\bullet$.

Pictorially, a chain map is a commutative diagram of the form

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & M_{i+1} & \longrightarrow & M_i & \longrightarrow & M_{i-1} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & N_{i+1} & \longrightarrow & N_i & \longrightarrow & N_{i-1} & \longrightarrow & \cdots \end{array}$$

in which both rows are complexes and all squares commute.

Example 4.5. Straightforward examples of maps between chain complexes include:

- the identity map $\mathrm{id}_{M_\bullet} : (M_\bullet, d^M) \to (M_\bullet, d^M)$, $f_i = \mathrm{id}_{M_i}$
- the zero map $0 : (M_\bullet, d^M) \to (N_\bullet, d^N)$, $f_i = 0$

Example 4.6. If $f : X \to Y$ is a continuous map between topological spaces, there is an induced chain map $f_* : (C_\bullet(X), d) \to (C_\bullet(Y), d)$ between associated singular chain complexes defined by composition with f in the evident way.

Example 4.7. Consider the complexes $(M_\bullet, d^M)$, $(N_\bullet, d^N)$, $(N'_\bullet, d^{N'})$ of $\mathbb{Z}$-modules given by

$$M_\bullet = \qquad 0 \longrightarrow \mathbb{Z} \xrightarrow{\begin{bmatrix} 1 \\ -1 \end{bmatrix}} \mathbb{Z}^2 \xrightarrow{\begin{bmatrix} 1 & 1 \end{bmatrix}} \mathbb{Z} \longrightarrow 0 \ ,$$

$$N_\bullet = \qquad 0 \longrightarrow \mathbb{Z} \xrightarrow{1} \mathbb{Z} \longrightarrow 0 \longrightarrow 0$$

$$N'_\bullet = \qquad 0 \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{1} \mathbb{Z} \longrightarrow 0$$

where we consider the last column to be homological degree -1. The map $f : (N_\bullet, d^N) \to (M_\bullet, d^M)$ given by $f_2 = 1$, $f_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is not a chain map, since the square with f_1 and f_0 does not commute: one composition in the 0,1 square is zero and the other isn't. However, the map $f : (N'_\bullet, d^{N'}) \to (M_\bullet, d^M)$ given by $f_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $f_0 = 1$ is a chain map; the 1,2 square has both compositions zero, and the both compositions in the 0,1 square are multiplication by 1 on $\mathbb{Z}$. Also, the map $f : (M_\bullet, d^M) \to (N_\bullet, d^N)$ given by $f_2 = 1$, $f_1 = \begin{bmatrix} 1 & 0 \end{bmatrix}$ is a chain map.

Proposition 4.8. *For any ring R, chain complexes and chain maps of left R-modules form a category, written $R-$* **Comp** *.*

Proof. We need to give a rule for composing morphisms and check that it satisfies the axioms. Of course, composition will take place degree-by-degree. We should check that a composition of chain maps is a chain map, and that composition is associative. Let $f : (L_\bullet, d^L) \to (M_\bullet, d^M)$ and $g : (M_\bullet, d^M) \to (N_\bullet, d^N)$ be chain maps. Then

$$(g \circ f)_i d^L_{i+1} = g_i f_i d^L_{i+1} = g_i d^M_{i+1} f_{i+1} = d^N_{i+1} g_{i+1} f_{i+1} = d^N_{i+1}(g \circ f)_{i+1}.$$

Associativity of composition follows directly from the same fact for module maps. □

Lecture of November 12, 2021

The category $R-$ **Comp** has many similarities to $R-$ **Mod**. These similarities are axiomatized in the definition of *abelian category*, which we won't pursue here. Rather, let's just notice a few.

Remark 4.9.

- Given any two chain maps $f, g : (M_\bullet, d^M) \to (N_\bullet, d^N)$, the sum $(f+g)_i = f_i + g_i$ is a chain map. Under this operation, the set $\mathrm{Hom}_{R-\mathbf{Comp}}((M_\bullet, d^M), (N_\bullet, d^N))$ is an abelian group.
- There is an initial and terminal "0 object": the chain complex consisting entirely of 0 modules with 0 differential.
- For any two elements in $R-$ **Comp**, the product and coproduct exist, and are given by isomorphic objects. Namely, for chain complexes $(M_\bullet, d^M), (N_\bullet, d^N)$ the product is the chain complex $(M_\bullet \oplus N_\bullet, d^M \oplus d^N)$ for which the modules are $M_i \oplus N_i$ and the differential is

  $$d^M_i \oplus d^N_i = \left[\begin{array}{c|c} d^M_i & 0 \\ \hline 0 & d^N_i \end{array}\right] : M_i \oplus N_i \to M_{i-1} \oplus N_{i-1}.$$

  We also call this the *direct sum* of these complexes.
- We can also talk about the kernel and cokernel of a chain map:
  - the *kernel* of $f : (M_\bullet, d^M) \to (N_\bullet, d^N)$ is the complex $(K_\bullet, d^K)$ with $K_i = \ker(f_i)$ and $d^K_i = d^i_M|_{K_i}$.
  - the *cokernel* of $f : (M_\bullet, d^M) \to (N_\bullet, d^N)$ is the complex $(C_\bullet, d^K)$ with $C_i = \mathrm{coker}(f_i)$ and d^C_i is map induced by d on the quotient modules $C_i \to C_{i-1}$.

Example 4.10. Let's return to the complexes of $\mathbb{Z}$-modules from before. We can compute $\mathrm{Hom}_{R-\mathbf{Comp}}((N_\bullet, d^N), (M_\bullet, d^M))$. For a chain map f, we need to specify $f_2 = \begin{bmatrix} a \end{bmatrix}$ and $f_1 = \begin{bmatrix} b \\ c \end{bmatrix}$. The commutativity of the square forces $\begin{bmatrix} a \\ -a \end{bmatrix} = \begin{bmatrix} b \\ c \end{bmatrix}$, so we conclude that this hom group is $\mathbb{Z}$.

Let's also compute a direct sum: $(N_\bullet \oplus N'_\bullet, d^N \oplus d^{N'})$ is the complex

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\begin{bmatrix} 1 \\ 0 \end{bmatrix}} \mathbb{Z}^2 \xrightarrow{\begin{bmatrix} 0 & 1 \end{bmatrix}} \mathbb{Z} \longrightarrow 0.$$

We can define exact sequences in $R-$ **Comp**.

Definition 4.11. A *short exact sequence* of chain complexes is a sequence of chain complexes of chain maps of the form

$$0 \to (M'_\bullet, d') \to (M_\bullet, d) \to (M''_\bullet, d'') \to 0$$

that is an exact sequence of R-modules in each degree. Pictorially, a short exact sequence of chain complexes is a commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & M'_{i+1} & \longrightarrow & M'_i & \longrightarrow & M'_{i-1} & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & M_{i+1} & \longrightarrow & M_i & \longrightarrow & M_{i-1} & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & M''_{i+1} & \longrightarrow & M''_i & \longrightarrow & M''_{i-1} & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

in which each row is a complex and each column is a short exact sequence of modules. (One might add horizontal arrows between the 0 modules along the top and the bottom, but they are redundant and just add clutter.)

Example 4.12. Returning to our same running examples, there is a short exact sequence

$$\begin{array}{ccccccccc}
0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{1} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \begin{bmatrix} 1 \\ 0 \end{bmatrix}} & & \downarrow{\scriptstyle 1} & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\begin{bmatrix} 1 \\ -1 \end{bmatrix}} & \mathbb{Z}^2 & \xrightarrow{\begin{bmatrix} 1 & 1 \end{bmatrix}} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle \begin{bmatrix} 0 & 1 \end{bmatrix}} & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{1} & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

4.2. **Homology.**

Definition 4.13. Given a chain complex $M_\bullet = (M_\bullet, d)$ of left R modules, its *homology* is the sequence of left R-modules indexed by $\mathbb{Z}$ defined by

$$H_i(M_\bullet) = H_i(M_\bullet, d) := \frac{\ker(d_i : M_i \to M_{i-1})}{\operatorname{im}(d_{i+1} : M_{i+1} \to M_i)}$$

for $i \in \mathbb{Z}$. We also give names to the modules in the numerator and denominator above

$$Z_i := \ker(d_i : M_i \to M_{i-1}) \text{ is called the module of } i\text{-cycles}$$

$$B_i := \operatorname{im}(d_{i+1} : M_{i+1} \to M_i) \text{ is called the module of } i\text{-boundaries.}$$

Remark 4.14. A chain complex $M_\bullet$ is exact if and only if $H_i(M_\bullet) = 0$ for all i.

Example 4.15. For a module M, we write $M[0]$ for the complex with $M[0]_i = 0$ for all $i \neq 0$ and $M[0]_0 = M$. The differential is (necessarily) the 0 map in each degree. The homology modules of $M[0]$ is $H_i(M[0]) = 0$ for $i \neq 0$ and $H_0(M[0]) \cong M$.

Example 4.16. The homology of a complex with just two nonzero modules located in degrees 0 and 1,

$$\cdots 0 \to M_1 \xrightarrow{d_1} M_0 \to 0 \to \cdots,$$

is $H_i(M, d) = 0$ for all $i \neq 0, 1$, $H_0(M, d) = \operatorname{coker}(d_1)$ and $H_1(M, d) = \ker(d_1)$.

Example 4.17. If $(V_\bullet, d)$ is a complex of K-vector spaces, then, by the rank nullity theorem

$$\dim_K H_i(V_\bullet, d) = \dim_K(V_i) - \operatorname{rank}(d_{i+1}) - \operatorname{rank}(d_i).$$

Example 4.18 (Homology groups in topology)**.** The homology of the singular chain complex $C_\bullet(X)$ of a topological space X are known as the *homology groups* of X.

Let's compute the homology groups of the simplicial complex X from Example 4.3 where the relevant chain complex is

$$\cdots 0 \to C_1(X) = \mathbb{Z}^3 \xrightarrow{d_1} C_0(X) = \mathbb{Z}^3 \to 0 \to \cdots,$$

To compute the homology let's perform row reduction on the matrix of the differential d_1:

$$\begin{bmatrix} 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & -1 \end{bmatrix} \xrightarrow{R_1+R_2\to R_2} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & -1 & -1 \end{bmatrix} \xrightarrow{R_2+R_3\to R_3} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \xrightarrow{C_2-C_1-C_3\to C_2} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

The row and column operations amount to performing changes of basis on the free modules $C_0(X) = \mathbb{Z}^3$ and $C_1(X) = \mathbb{Z}^3$. The last matrix above gives a new description for the differential d_1 with respect to the ordered bases $\{1,2\}, \{1,3\} - \{1,2\} - \{2,3\}, \{2,3\}$ and $\{1\}, \{1\} + \{2\}, \{1\} + \{2\} + \{3\}$. We now see that

$$\begin{aligned} H_1(C_\bullet(X)) &= \ker(d_1) = \mathbb{Z}(\{1,3\} - \{1,2\} - \{2,3\}) \cong \mathbb{Z} \\ H_0(C_\bullet(X)) &= \operatorname{coker}(d_1) = \frac{\mathbb{Z}\{1\} \oplus \mathbb{Z}(\{1\} + \{2\}) \oplus \mathbb{Z}(\{1\} + \{2\} + \{3\})}{\mathbb{Z}\{1\} \oplus \mathbb{Z}(\{1\} + \{2\})} \\ &\cong \mathbb{Z}(\{1\} + \{2\} + \{3\}) \cong \mathbb{Z}. \end{aligned}$$

Now suppose that Y is the simplicial complex obtained by filling in the triangle X with a 2-dimensional simplex. Then $C_\bullet(Y)$ is

$$\cdots 0 \to C_2(Y) = \mathbb{Z} \xrightarrow{d_2} C_1(X) = \mathbb{Z}^3 \xrightarrow{d_1} C_0(X) = \mathbb{Z}^3 \to 0 \to \cdots,$$

where $d_2 = \begin{bmatrix} 1 & -1 & 1 \end{bmatrix}^T$ with respect to the bases $\{1,2,3\}$ and $\{1,2\}, \{1,3\}, \{2,3\}$, i.e. $\operatorname{im}(d_2) = \mathbb{Z}(\{1,2\} - \{1,3\} + \{2,3\})$.

From the computations above we see that $\ker(d_1) = \mathbb{Z}(\{1,3\} - \{1,2\} - \{2,3\})$. Hence $H_1(C_\bullet(Y)) = 0$ since $\ker(d_1) = \operatorname{im}(d_2)$ and $H_2(C_\bullet(Y)) = 0$ because d_2 is injective.

The topological significance of the computations above is that

- the rank of H_0 measures the number of connected components: both for X and for Y there is one connected component and $H_0 \cong \mathbb{Z}$ has rank one;
- the rank of H_1 measures the number of 1-dimensional "holes": X has one such hole (X is homotopic to the circle S^1) and $H_1(C_\bullet(X)) \cong \mathbb{Z}$ but Y has no such holes and $H_1(C_\bullet(Y)) = 0$;
- the rank of H_2 measures the number of 2-dimensional "holes" etc.

Definition 4.19 (Induced map in homology)**.** Given a chain map $f : (M_\bullet, d) \to (N_\bullet, d)$ for each i write $H_i(f) : H_i(M_\bullet) \to H_i(N_\bullet)$ for the map induced by f in the following manner: given $z \in \ker(d_i : M_i \to M_{i-1})$, we define $H_i(f)(\overline{z}) = \overline{f(z)}$.

Remark 4.20. The function $H_i(f)$ is indeed a well-defined R-linear map: Note, first of all, that for $z \in \ker(d_i : M_i \to M_{i-1})$ we have $d_i(f_i(z)) = f_{i-1}(d_i(z)) = f_{i-1}(0) = 0$, and hence $f_i(z) \in \ker(d_i : N_i \to N_{i-1})$. Thus, we have a well-defined element $\overline{f_i(z)}$ of $H_i(N_\bullet)$. Moreover, if $\overline{z} = \overline{y}$ in $H_i(M_\bullet)$ for elements $y, z \in \ker(d_i : M_i \to M_{i-1})$, then $y - z = d^M_{i+1}(w)$ for some $w \in M_{i+1}$. It follows that

$$f_i(y) - f_i(z) = f_i(y - z) = f_i(d^M_{i+1}(w)) = d^N_{i+1}(f_{i+1}(w)),$$

since f is a chain map, and hence $\overline{f_i(y)} = \overline{f_i(z)}$ holds in $H_i(N_\bullet)$. This proves $H_i(f)$ is well-defined. It is easy to see that it is an R-module homomorphism.

Lecture of November 15, 2021

Definition 4.21. A chain map $f : M_\bullet \to N_\bullet$ is a *quasi-isomorphism* if $H_i(f)$ is an isomorphism for all $i \in \mathbb{Z}$.

Example 4.22. The chain map

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{2} & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \bar{1}} & & \downarrow & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots
\end{array}$$

is a quasi-isomorphism.

Example 4.23. Admitting a quasi-isomorphism is stronger than having isomorphic homology in each degree. Consider the complexes

$$M_\bullet \qquad 0 \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{2} \mathbb{Z}/4\mathbb{Z} \longrightarrow 0$$

$$N_\bullet \qquad 0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{2} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

Observe that $H_1(M_\bullet) = \langle [2]_4 \rangle \cong \mathbb{Z}/2\mathbb{Z}$, $H_0(M_\bullet) = \langle [1]_2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$, $H_1(N_\bullet) = \langle [1]_2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$, and $H_0(N_\bullet) = \langle [1]_2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$. There is no chain map $f : M_\bullet \to N_\bullet$ for which $H_1(f)$ is an isomorphism, since $f_1([2]_4) = 0$, so $H_1(f) = 0$. Likewise, there is no chain map $f : N_\bullet \to M_\bullet$ for which $H_0(f)$ is an isomorphism, since $2f_0([1]_2) = 0$ implies $f_0([1]_2) \in \langle [2]_4 \rangle$ and hence $H_0(f) = 0$.

Next we promote homology to being a functor.

Lemma 4.24. *For each fixed i, $H_i(-)$ is an additive functor*

$$H_i(-) : R - \mathbf{Comp} \to R - \mathbf{Mod}.$$

Recall that this means $H_i(f \circ g) = H_i(f) \circ H_i(g)$, $H_i(\mathrm{id}) = \mathrm{id}$, and $H_i(f + g) = H_i(f) + H_i(g)$.

Proof. These follow easily from Definition 4.19. □

However, the homology functors are not exact.

Example 4.25. Consider the following short exact sequence of complexes K-vector spaces (where each row is a complex, and the vertical maps are chain maps)

$$\begin{array}{lccccccc}
M'_\bullet: & & 0 & \longrightarrow & 0 & \longrightarrow & K^a & \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle i} & \\
M_\bullet: & 0 & \longrightarrow & K^b & \xrightarrow{\cong} & K^b & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle p} & \\
M''_\bullet: & 0 & \longrightarrow & K^b & \xrightarrow{p} & K^c & \longrightarrow & 0
\end{array}$$

Then applying H_0 yields

$$K^a \longrightarrow 0 \longrightarrow 0$$

and applying H_1 yields

$$0 \longrightarrow 0 \longrightarrow \ker(p) \cong K^a.$$

Note that neither of these is exact.

4.2.1. *The long exact sequence of homology.*

Proposition 4.26 (Snake Lemma)**.** *For a ring R, suppose*

$$\begin{array}{ccccccc}
 & & M' & \xrightarrow{i} & M & \xrightarrow{p} & M'' \longrightarrow 0 \\
 & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\
0 & \longrightarrow & N' & \xrightarrow{j} & N & \xrightarrow{q} & N''
\end{array}$$

is a commutative diagram of left R-modules such that each row is an exact sequence. Then there is an exact sequence of the form

$$\ker(f') \xrightarrow{i|} \ker(f) \xrightarrow{p|} \ker(f'') \xrightarrow{\partial} \operatorname{coker}(f') \xrightarrow{\overline{j}} \operatorname{coker}(f) \xrightarrow{\overline{q}} \operatorname{coker}(f'').$$

which can be visualized in relation to the previous diagram as follows

$$\begin{array}{ccccc}
\ker f' & \longrightarrow & \ker f & \longrightarrow & \ker f'' \\
\downarrow & & \downarrow & & \downarrow \\
M' & \longrightarrow & M & \longrightarrow & M'' \\
{\scriptstyle f'}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle f''}\downarrow \\
N' & \longrightarrow & N & \longrightarrow & N'' \\
\downarrow & & \downarrow & & \downarrow \\
\operatorname{coker} f' & \longrightarrow & \operatorname{coker} f & \longrightarrow & \operatorname{coker} f''
\end{array} \qquad \partial$$

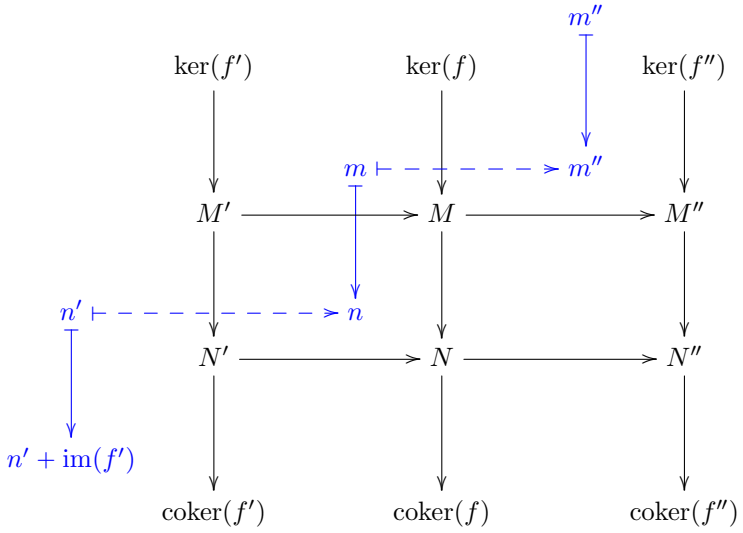
The map ∂ is called the connecting homomorphism*, as is given as follows: For $m'' \in \ker(f'')$, pick $m \in M$ such that $p(m) = m''$. Then $qf(m) = 0$ and hence $f(m) = j(n')$ for a element $n' \in N'$. Set*

$$\partial(m) = n' + \operatorname{im}(f') \in \operatorname{coker}(f').$$

Moreover, if i is injective and if q is surjective they lead to an exact sequence

$$0 \to \ker(f') \xrightarrow{i|} \ker(f) \xrightarrow{p|} \ker(f'') \xrightarrow{\partial} \operatorname{coker}(f') \xrightarrow{\overline{j}} \operatorname{coker}(f) \xrightarrow{\overline{q}} \operatorname{coker}(f'') \to 0.$$

The map ∂ can be illustrated as follows:



Proof. One needs to show many things.

- Well-definedness of $i|$ and $p|$, specifically the fact that the images of these maps land in $\ker(f)$ and $\ker(f'')$ respectively:

  To show this for $i|$, consider $u \in \ker(f')$. Then $i|(u) = i(u)$ and $f(i(u)) = j(f'(u)) = j(0) = 0$ by the commutativity of the given diagram. Thus $i|(u) \in \ker(f)$ as desired. The same argument works for $p|$.
- Well-definedness of $\bar{j}$ and $\bar{q}$, specifically independence of coset representative.

  To show this for $\bar{q}$, consider $n - \tilde{n} \in \mathrm{im}(f)$. Then we have $q(n) - q(\tilde{n}) = q(n - \tilde{n}) \in q(\mathrm{im}(f)) = f''(\mathrm{im}(p)) \subseteq \mathrm{im}(f'')$ yields that $\bar{q}(n + \mathrm{im}(f)) = q(n) + \mathrm{im}(f'') = q(\tilde{(n)}) + \mathrm{im}(f'') = \bar{q}(\tilde{n} + \mathrm{im}(f))$. The same argument works for $\bar{k}$.
- Exactness at $\ker(f)$:

  It is clear that $\mathrm{im}(i|) \subseteq \ker(p|)$. If $m \in \ker(p|) = \ker(f) \cap \ker(p)$, then $m = i(m')$ for some $m' \in M'$, and $j(f'(m')) = f(i(m')) = f(m) = 0$, and since j is injective, $f'(m') = 0$, so $m' \in \ker(f')$.
- Exactness at $\mathrm{coker}(f)$:

  It is clear that $\mathrm{im}(\bar{j}) \subseteq \ker(\bar{q})$. If $\bar{n} \in \ker(\bar{q})$, then $q(n) \in \mathrm{im}(f'')$, so there is some m'' such that $q(n) = f''(m'')$. We can write $m'' = p(m)$ for some $m \in M$. Then $q(n) = f''(p(m)) = q(f(m))$ so $q(n - f(m)) = 0$. Thus $n - f(m) = j(n')$ for some $n' \in N'$, so $\bar{n} = \bar{j}(\overline{n'})$.

  Lecture of November 17, 2021
- Well-definedness of ∂:

  First, given $m'' \in \ker(f'')$, p is surjective, so we can write $p(m) = m''$. Then $0 = f''(p(m)) = q(f(m))$, so $n = f(m) \in \ker(q) = \mathrm{im}(j)$, and hence we can choose n' such that $j(n') = n$.

  To see that $\partial(m'')$ is independent of the choice of m occurring in its construction, suppose m_1 and m_2 satisfy $p(m_1) = m'' = p(m_2)$, and let n_1', n_2' be the unique elements satisfying $j(n_1') = f(m_1)$ and $j(n_2') = f(m_2)$. Then $p(m_1 - m_2) = 0$ and hence by exactness of the top row, there is a m' such that $i(m') = m_1 - m_2$. By the commutativity of the left square we get

$$j(f'(m')) = fi(m') = f(m_1) - f(m_2) = j(n_1') - j(n_2') = j(n_1' - n_2').$$

Since j is injective, it follows that $f'(m') = n_1' - n_2'$ and hence that $n_1' + \operatorname{im}(f') = n_2' + \operatorname{im}(f')$. So, we have proven ∂ is a well-defined function.

The fact that ∂ is R-linear follows from noting that if $p(m_1) = m_1''$ and $p(m_2) = m_2''$, then we have $p(rm_1 + m_2) = rm_1'' + m_2''$, and likewise with j.

- $\operatorname{im}(p|) = \ker(\partial)$:

  If $m'' \in \ker(f'')$ satisfies $m'' = p(x)$ for some $x \in \ker(f)$, then in the construction of ∂ we may take $m = x$ and it follows that $f(m) = 0$ and hence $\partial(m') = 0$. This proves $\operatorname{im}(p|) \subseteq \ker(f'')$. If $\partial(m'') = 0$, then, using the same letters as in the construction of ∂, $n' = f'(m')$ for some $m' \in M'$. Then $p(m - i(m')) = p(m) = m''$ and $f(m - i(m')) = f(m) - jf'(m') = 0$, which proves that $m'' \in \operatorname{im}(p|)$. This proves the other containment.
- $\operatorname{im}(\partial) = \ker \bar{j}$:

  For $m'' \in M''$, write $\partial(m'') = n' + \operatorname{im}(f')$; then, in the construction, $j(n') = n \in \operatorname{im}(f)$, so $\operatorname{im}(\partial) \subseteq \ker \bar{j}$. If $\bar{j}(n' + \operatorname{im}(f')) = 0$, then $j(n') \in \operatorname{im}(f)$, so write $n = j(n') = f(m)$. Then $f''(p(m)) = q(f(m)) = q(j(n')) = 0$, so $p(m) \in \ker(f'')$, and $\partial(p(m)) = n' + \operatorname{im}(f)$ by definition, which proves that $n' + \operatorname{im}(f) \in \operatorname{im}(\partial)$.
- Exactness at $\ker(f')$ and $\operatorname{coker}(f'')$ given exactness at M' and N'':

  Clear, since the restriction of an injective map is injective, and the map induced on a quotient by a surjective map is surjective. □

Example 4.27. Given an $m \times n$ matrix A and a prime p, write $\bar{A}$ for the reduction of A modulo p. In general, there may be solutions of $\bar{A}v = 0$ that are not of the form $v = \bar{w}$ for any w such that $Aw = 0$. We can use the Snake Lemma to understand the difference: there is a chain map of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}^n & \xrightarrow{p} & \mathbb{Z}^n & \xrightarrow{p} & \mathbb{F}_p^n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle \bar{A}} & & \\ 0 & \longrightarrow & \mathbb{Z}^m & \xrightarrow{p} & \mathbb{Z}^m & \xrightarrow{p} & \mathbb{F}_p^m & \longrightarrow & 0, \end{array}$$

which by the snake lemma yields an exact sequence

$$0 \to \ker(A) \xrightarrow{p} \ker(A) \to \ker(\bar{A}) \xrightarrow{\partial} \operatorname{coker}(A) \xrightarrow{p} \operatorname{coker}(A) \to \operatorname{coker}(\bar{A}) \to 0.$$

This gives a short exact sequence

$$0 \to \frac{\ker(A)}{p \ker(A)} \to \ker(\bar{A}) \to \operatorname{im}(\partial) \to 0,$$

so the image of the connecting map measures how many solutions mod p do not come from solutions in $\mathbb{Z}$. We also have an isomorphism $\operatorname{im}(\partial) \cong \ker(\operatorname{coker}(A) \xrightarrow{p} \operatorname{coker}(A))$.

The connecting homomorphism is given by the formula $\partial(v) = [\frac{1}{p} A\tilde{v}]$, where $\tilde{v}$ is a lift of v: any vector in $\mathbb{Z}$ whose coordinates are representatives for the coordinates of v.

Lecture of November 19, 2021

Theorem 4.28 (Long exact sequence in homology)**.** *If $0 \to M_\bullet' \xrightarrow{j} M_\bullet \xrightarrow{p} M_\bullet'' \to 0$ is a short exact sequence of chain complexes of left R-modules, then there is a long exact sequence of left R-modules of the form*

$$\cdots \to H_i(M_\bullet') \xrightarrow{H_i(j)} H_i(M_\bullet) \xrightarrow{H_i(p)} H_i(M_\bullet'') \xrightarrow{\partial_i} H_{i-1}(M_\bullet') \xrightarrow{H_{i-1}(j)} H_{i-1}(M_\bullet) \xrightarrow{H_{i-1}(p)} \cdots$$

also often drawn as

$$\cdots \longrightarrow H_i(M'_\bullet) \longrightarrow H_i(M_\bullet) \longrightarrow H_i(M''_\bullet) \xrightarrow{\partial_i} H_{i-1}(M'_\bullet) \longrightarrow H_{i-1}(M_\bullet) \longrightarrow H_{i-1}(M''_\bullet) \xrightarrow{\partial_{i-1}} H_{i-2}(M'_\bullet) \longrightarrow H_{i-2}(M_\bullet) \longrightarrow H_{i-2}(M''_\bullet) \dashrightarrow H_0(M'_\bullet) \longrightarrow H_0(M_\bullet) \longrightarrow H_0(M''_\bullet) \dots$$

where the map ∂_i is defined as follows:

Given $z \in \ker(d_i : M''_i \to M''_{i-1})$, since p is onto, we may find a $w \in M_i$ such that $p_i(w) = z$. For any choice of such a w, we have $p(d(w)) = d(p(w)) = d(z) = 0$ and hence, by the exactness in the middle of the original s.e.s., there is a unique $u \in M'_{i-1}$ such that $j(u) = d(w)$. We have $jd(u) = d(j(u)) = d(d(w)) = 0$ and thus, since j is one-to-one, $u \in \ker(d_{i-1})$. We set $\partial_i(\overline{z}) = \overline{u} \in H_{i-1}(M'_\cdot)$.

Proof. The theorem follows from several applications of the Snake Lemma:

- First we note that for any n, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M'_n & \longrightarrow & M_n & \longrightarrow & M''_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_n^{M'}} & & \downarrow{\scriptstyle d_n^{M}} & & \downarrow{\scriptstyle d_n^{M''}} & & \\ 0 & \longrightarrow & M'_{n-1} & \longrightarrow & M_{n-1} & \longrightarrow & M''_{n-1} & \longrightarrow & 0, \end{array}$$

  so by the Snake Lemma we get exact sequences

$$0 \to Z_n(M'_\bullet) \to Z_n(M_\bullet) \to Z_n(M''_\bullet)$$

$$M'_n/B_n(M'_\bullet) \to M_n/B_n(M_\bullet) \to M''_n/B_n(M''_\bullet) \to 0.$$

- Next we observe that since the boundaries B_n are contained in the kernel of the differential d_n and since the image of d_n is contained in Z_n, the universal mapping property of the quotient gives that the differentials d_n for the three complexes induce vertical maps as follows

$$\begin{array}{ccccccccc} & & M'_n/B_n(M'_\bullet) & \longrightarrow & M_n/B_n(M_\bullet) & \longrightarrow & M''_n/B_n(M''_\bullet) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \overline{d}_n^{M'}} & & \downarrow{\scriptstyle \overline{d}_n^{M}} & & \downarrow{\scriptstyle \overline{d}_n^{M''}} & & \\ 0 & \longrightarrow & Z_{n-1}(M'_\bullet) & \longrightarrow & Z_{n-1}(M_\bullet) & \longrightarrow & Z_{n-1}(M''_\bullet) & & \end{array}$$

- observe that the kernel of $\overline{d}_n$ is H_n and the cokernel of $\overline{d}_n$ is H_{n-1} therefore the Snake Lemma applied to the diagram in the previous bullet point yields a six term exact sequence

$$H_n(M'_\bullet) \to H_n(M_\bullet) \to H_n(M''_\bullet) \xrightarrow{\partial} H_{n-1}(M'_\bullet) \to H_{n-1}(M_\bullet) \to H_{n-1}(M''_\bullet)$$

  Comparing the description of ∂ given by the Snake Lemma and the description of ∂_n above one sees that these maps are the same. □

Corollary 4.29 (Two out of three exactness)**.** *If $0 \to M'_\bullet \to M_\bullet \to M''_\bullet \to 0$ is a short exact sequence of chain complexes of left R-modules and if any two of the three complexes are exact, then the third complex is also exact.*

Proof. Recall that a complex is exact if and only if all its homology modules are equal to 0. Now if two of the three given complexes are exact (say $M_\bullet$ and $M''_\bullet$ are exact for concreteness), it means that in the long exact sequence in homology we have two zeros surrounding each of the homology modules of the third complex ($M'_\bullet$) as follows:

$$\cdots \xrightarrow{H_i(p)} 0 \xrightarrow{\partial_i} H_{i-1}(M'_\bullet) \xrightarrow{H_{i-1}(j)} 0 \xrightarrow{H_{i-1}(p)} \cdots$$

The presence of the 0 homology modules implies that $\partial_i = 0 = H_{i-1}(p)$, and the exactness yields $H_{i-1}(M'_\bullet) = \ker(H_{i-1}(j)) = \operatorname{im}(\partial_i) = 0$ for any $i \in \mathbb{Z}$. Thus $M'_\bullet$ is exact. □

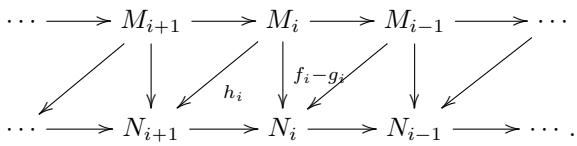
4.3. **Homotopy of chain maps.**

Definition 4.30. Suppose $M_\bullet$ and $N_\bullet$ are two chain complexes of R-modules and $f, g : M_\bullet \to N_\bullet$ are two chain maps joining them. We say f and g are *homotopic* (or sometimes *chain homotopic*), written $f \simeq_{\text{htpc}} g$, if there is a family of R-maps $h_i : M_i \to N_{i+1}$, $i \in \mathbb{Z}$, such that

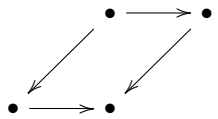
$$d^N_{i+1} \circ h_i + h_{i-1} \circ d^M_i = f_i - g_i$$

for all i. (Succinctly, $dh + hd = f - g$.) Such a family of maps $\{h_i\}_{i\in\mathbb{Z}}$ is called a *chain homotopy* joining f to g. A chain map is called *null-homotopic* if $f \simeq_{\text{htpc}} 0$.

Here is a picture of a chain homotopy



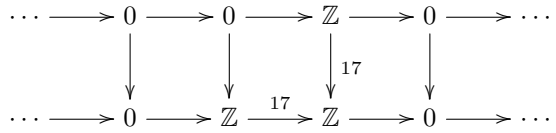
The squares commute but the triangles do not. Rather, the sum of the two compositions in each rhombus



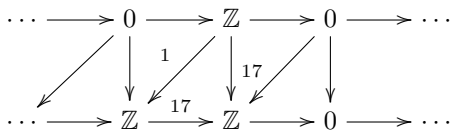
occuring in this diagram is equal to the difference of f and g.

Example 4.31. If $f, g : X \to Y$ are continuous maps between topoogical spaces that are homotopic in the sense of topology, then the induced maps on singular chain complexes $f_*, g_* : C_\bullet(X) \to C_\bullet(Y)$ are chain homotopic.

Example 4.32. I claim the chain map pictured below is null homotopic:



A null-homotopy is given by the diagram



The main point of chain homotopy is given by the following result:

Proposition 4.33. *Homotopic chain maps induce the same map on homology: If f and g are chain maps from $(M_\bullet, d^M)$ to $(N_\bullet, d^N)$ and they are homotopic, then $H_i(f) = H_i(g)$ for all i.*

In particular, a null homotopic map induces the 0 map on homology.

Proof. We prove the second assertion first. Suppose f is null-homotopic. For any i, let $\overline{z} \in H_i(M)$ be a class represented by an element $z \in \ker(d_i : M_i \to M_{i-1})$. Since f is null-homotopic, there is a h such that $d^N h + h d^M = f$. So $f(z) = d^N(h(z)) + h(d^M(z)) = d^N(h(z))$ since $d(z) = 0$. This gives $f(z) \in \mathrm{im}(d)$ and hence $\overline{f(z)} = 0$ in $H_i(N_\bullet)$.

If $f \simeq_{\mathrm{htpc}} g$, then $f - g$ is null-homotopic, so that $H_i(f - g) = 0$, by what we just proved. Since H_i is additive, we have $0 = H_i(f - g) = H_i(f) - H_i(g)$. □

Example 4.34. The converse of this proposition is false. For example, the chain map of $\mathbb{Z}$-modules pictured as

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle 2} & & \downarrow & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \xrightarrow{2} & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots
\end{array}$$

induces the 0 map on all homology groups, but it is not null homotopic. Indeed, the only possible homotopy would be 0 in all degrees except one, in which it would be a map $h_0 : \langle \mathbb{Z}/2\mathbb{Z} \rangle \to \mathbb{Z}/4\mathbb{Z}$. The only possibilities for h_0 are the 0 map and the map of multiplication by 2, but neither works.

Lecture of November 22, 2021

4.4. **Projective and Injective Resolutions.**

4.4.1. *Free and Projective resolutions.*

Definition 4.35. Let M be an R-module. A *free resolution* of M is a chain complex $F_\bullet$ of free R-modules

$$\cdots F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \to 0 \cdots$$

along with a map $\pi : F_0 \to M$ such that the augmented complex

$$\cdots F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\pi} M \to 0 \cdots$$

is exact. Similarly, a *projective resolution* is a complex of projective modules that satisfies the same conditions.

In particular, a free or projective resolution of M is a chain complex such that $H_i(P_\bullet) = 0$ for $i \neq 0$ and $H_0(P_\bullet) \cong M$.

Free resolutions always exist:

Lemma 4.36. *Every R-module admits a free resolution.*

Proof. Let M be an R-module. There is a surjection π from a free module F_0 onto M (given by mapping a free basis of a free module to a generating set for M). Then, $\ker(\pi) \subseteq F_0$ is a module, and there is a surjection π_1 from a free module F_1 onto $\ker(\pi)$; let $d_1 : F_1 \to F_0$ be the composition of π_1 and the inclusion map. Take a surjection from a free module onto $\ker(d_1)$, and continue like so. □

A free or projective resolution can be thought of as an approximation of M by free/projective modules via a sort of inclusion/exclusion method: A crude approximation of M is a free module F_0 that surjects onto

it. Such an approximation is too big, so we want to subtract the kernel of π, and we take a free module that surjects onto the kernel for $F_1 \xrightarrow{d_1} F_0$. But we might consider this as subtracting too much, since F_1 may properly surject onto, so be bigger than, the kernel. And so on.

They need not be unique.

Example 4.37. For a ring R, a free resolution of the free module R is $0 \to R \to 0$, with the map $\pi : R \xrightarrow{1} R$. We could also take $0 \to R \xrightarrow{\begin{bmatrix} 1 \\ -1 \end{bmatrix}} R^2 \to 0$, with the map $\pi : R^2 \xrightarrow{\begin{bmatrix} 1 & 1 \end{bmatrix}} R$.

Example 4.38. Let K be a field, and $R = K[x, y]$ be a polynomial ring over K. Take $M = R/(x, y)$. There is a surjection $\pi : R \to M$. The kernel of π is generated by x and y, so we can take $d_1 : R^2 \xrightarrow{\begin{bmatrix} x & y \end{bmatrix}} R$. We need to find the kernel of d_1: if $xf + yg = 0$ in R, then $xf = -yg$, and since R is a UFD, we have $f = yh, g = -xh$ for some $h \in R$. Thus, $\ker(d_1) = R \cdot \begin{bmatrix} y \\ -x \end{bmatrix}$, so we can take

$$0 \to R \xrightarrow{\begin{bmatrix} y \\ -x \end{bmatrix}} R^2 \xrightarrow{\begin{bmatrix} x & y \end{bmatrix}} R \to 0$$

as a free resolution.

Example 4.39. Let K be a field, and $R = K[x, y]/(xy)$. Take $M = R/(x)$. There is a surjection $\pi : R \to M$. The kernel of this is generated by (x), so we can take $d_1 : R \xrightarrow{x} R$. The kernel of this consists of the elements killed by x in R, which is (y), so we can take $d_2 : \xrightarrow{y} R$. It's now clear this keeps repeating:

$$\cdots \to R \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \to 0.$$

4.4.2. *Injective resolutions.*

Definition 4.40. For a ring R and R-module M, an *injective resolution* of M is complex of the form

$$\cdots \to 0 \to E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \xrightarrow{d^2} \cdots,$$

(with E^0 in homological degree zero) such that each E^i is injective for all i, together with an R-map $M \xrightarrow{i} E^0$ such that the augmented sequence

$$0 \to M \xrightarrow{i} E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \xrightarrow{d^2} \cdots$$

is an exact complex.

Remark 4.41. The notation above follows *cohmological indexing*, in which we write a complex

$$\cdots \to M_2 \xrightarrow{d_2} M_1 \xrightarrow{d_1} M_0 \xrightarrow{d_0} M_{-1} \xrightarrow{d_{-1}} M_{-2} \to \cdots$$

as

$$\cdots \to N^{-2} \xrightarrow{d^{-2}} N^{-1} \xrightarrow{d_{-1}} N^0 \xrightarrow{d^0} N^1 \xrightarrow{d^1} N^2 \to \cdots,$$

where $N^i = M_{-i}$ and $d^i = d_{-i}$.

Lecture of November 29, 2021

Injective resolutions also exist.

Proposition 4.42. *Every R-module admits an injective resolution.*

Proof. Given a module M, by a result above we can find an injective R-linear map $j : M \to E^0$ with E^0 injective. Let $N = \operatorname{coker}(j) = E^0/\operatorname{im}(j)$ and apply this result again to obtain a injective R-module map $N \to E^1$ with E^1 injective. Let $E^0 \to E^1$ be the composition of $E^0 \to N \to E^1$. Then we have a l.e.s $0 \to N \to E^1 \to E^2$. Repeating this process (by taking the cokernel of $E^1 \to E^2$ and injecting it into an injective R-module, etc.), we build a (possibly never-ending) injective resolution of M. □

Example 4.43. Let us find an injective resolution of $\mathbb{Z}$ as a module over itself. We have the evident embedding $\mathbb{Z} \to \mathbb{Q}$ and we know $\mathbb{Q}$ is injective since it is divisible. The cokernel is $\mathbb{Q}/\mathbb{Z}$, which is injective since it too is divisible. Thus

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 \to \cdots$$

is an injective resolution of $\mathbb{Z}$.

Example 4.44. Let's find an injective resolution of $\mathbb{Z}/n\mathbb{Z}$ as a $\mathbb{Z}$-module. We have

$$0 \to \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \to E^1 \to 0 \to \cdots$$

where E^1 is the quotient of $\mathbb{Q}/\mathbb{Z}$ by the subgroup generated by $1/n + \mathbb{Z}$. In other words $E^1 = \frac{\mathbb{Q}}{\mathbb{Z}+\mathbb{Z}\cdot\frac{1}{n}}$. Then E^1 is divisible and hence injective.

Definition 4.45. Let M and N be R-modules, and $P_\bullet$ and $Q_\bullet$ be two complexes such that $P_i = 0$ and $Q_i = 0$ for all $i < 0$. Suppose we have maps $P_0 \xrightarrow{p} M$ and $Q_0 \xrightarrow{q} N$. We say that a chain map $\tilde{f} : P_\bullet \to Q_\bullet$ *lifts* an R-module map $f : M \to N$ if the diagram of complexes

$$\begin{array}{ccc} P_\bullet & \xrightarrow{\tilde{f}} & Q_\bullet \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ M & \xrightarrow{f} & N \end{array}$$

commutes. Equivalently, such a map is a lift if the diagram

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \xrightarrow{p} & M & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle \tilde{f}_2} & & \downarrow{\scriptstyle \tilde{f}_1} & & \downarrow{\scriptstyle \tilde{f}_0} & & \downarrow{\scriptstyle f} & & & & \\ \cdots & \longrightarrow & Q_2 & \longrightarrow & Q_1 & \longrightarrow & Q_0 & \xrightarrow{q} & M & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

commutes.

Similarly, in cohomological notation, if $P^\bullet$ and $Q^\bullet$ be two complexes such that $P^i = 0$ and $Q^i = 0$ for all $i < 0$ and we have maps $M \xrightarrow{p} P^0$ and $N \xrightarrow{q} Q^0$, we say that a chain map $\tilde{f} : P^\bullet \to Q^\bullet$ *lifts* an R-module map $f : M \to N$ if the diagram of complexes

$$\begin{array}{ccc} P^\bullet & \xrightarrow{\tilde{f}} & Q^\bullet \\ {\scriptstyle p}\uparrow & & \uparrow{\scriptstyle q} \\ M & \xrightarrow{f} & N \end{array}$$

commutes.

Theorem 4.46. *Let M and N be R-modules, $f : M \to N$ an R-module homomorphism. Consider two complexes*

$$P_\bullet = \quad \cdots \to P_2 \to P_1 \to P_0 \to 0 \to 0 \to \cdots$$
$$Q_\bullet = \quad \cdots \to Q_2 \to Q_1 \to Q_0 \to 0 \to 0 \to \cdots$$

with maps $P_0 \xrightarrow{p} M$ and $Q_0 \xrightarrow{q} N$. Suppose that P_i is projective for all i and that the augmentation of $Q_\bullet$,

$$\cdots \to Q_2 \to Q_1 \to Q_0 \xrightarrow{q} N \to 0 \to \cdots,$$

is exact.

Then there is a lift $\tilde{f} : P_\bullet \to Q_\bullet$ of f. Moreover, $\tilde{f}$ is unique up to homotopy: if $\tilde{f}' : P_\bullet \to Q_\bullet$ is another lift of f, then $\tilde{f} \simeq_{\mathrm{htpc}} \tilde{f}'$.

Proof. For existence, as illustrated below,

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P_2 & \xrightarrow{d_2^P} & P_1 & \xrightarrow{d_1^P} & P_0 & \xrightarrow{p} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tilde{f}_2} & & \downarrow{\scriptstyle \tilde{f}_1} & & \downarrow{\scriptstyle \tilde{f}_0} & & \downarrow{\scriptstyle f} & & \\
\cdots & \longrightarrow & Q_2 & \xrightarrow{d_2^Q} & Q_1 & \xrightarrow{d_1^Q} & Q_0 & \xrightarrow{q} & N & \longrightarrow & 0,
\end{array}$$

we need to construct maps $\tilde{f}_i : P_i \to Q_i$ for $i \geqslant 0$ such that $q\tilde{f}_0 = fp$ and $d_i^Q \tilde{f}_i = \tilde{f}_{i-1} d_i^P$ for $i \geqslant 1$. To construct $\tilde{f}_0$, we merely use the definition of projective and the diagram

$$\begin{array}{ccccc}
 & & P_0 & & \\
 & {\scriptstyle \exists \tilde{f}_0} \swarrow & \downarrow{\scriptstyle fp} & & \\
Q_0 & \xrightarrow{q} & N & \longrightarrow & 0.
\end{array}$$

Suppose we have constructed maps $\tilde{f}_0, \ldots, \tilde{f}_n$ for some $n \geqslant 0$ so that $d_i^Q \tilde{f}_i = \tilde{f}_{i-1} d_i^P$ for $1 \leqslant i \leqslant n$. (When $n = 0$, the condition is vacuous.) Then $d_n^Q \tilde{f}_n d_{n+1}^P = \tilde{f}_{n-1} d_n^P d_{n+1}^P = 0$, so $\operatorname{im}(\tilde{f}_n d_{n+1}^P) \subseteq Z_n(Q_\bullet) = B_n(Q_\bullet)$, using exactness of $Q_\bullet$. Use the definition of projective again with the diagram

$$\begin{array}{ccccc}
 & & P_{n+1} & & \\
 & {\scriptstyle \exists \tilde{f}_{n+1}} \swarrow & \downarrow{\scriptstyle \tilde{f}_n d_{n+1}^P} & & \\
Q_{n+1} & \xrightarrow{d_{n+1}^Q} & B_n(Q_\bullet) & \longrightarrow & 0
\end{array}$$

to construct $\tilde{f}_{n+1}$ such that $d_{n+1}^Q \tilde{f}_{n+1} = \tilde{f}_n d_n^P$ holds too. This proves existence.

Lecture of December 1, 2021

For uniqueness, suppose $\tilde{f}'$ is another such chain map. Observe that $\tilde{f} - \tilde{f}'$ is a chain map from $P_\bullet \to Q_\bullet$ that extends the zero map from M to N. Thus, it suffices to prove that if $\tilde{f} : P_\bullet \to Q_\bullet$ is a lift of the zero map, then $\tilde{f}$ is null-homotopic. That is,

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & P_2 & \xrightarrow{d_2^P} & P_1 & \xrightarrow{d_1^P} & P_0 & \xrightarrow{p} & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tilde{f}_2} & \swarrow{\scriptstyle h_1} & \downarrow{\scriptstyle \tilde{f}_1} & \swarrow{\scriptstyle h_0} & \downarrow{\scriptstyle \tilde{f}_0} & & \downarrow{\scriptstyle 0} & & \\
\cdots & \longrightarrow & Q_2 & \xrightarrow{d_2^Q} & Q_1 & \xrightarrow{d_1^Q} & Q_0 & \xrightarrow{q} & N & \longrightarrow & 0,
\end{array}$$

we need to show there are maps $h_i : P_i \to Q_{i+1}$ for $i \geqslant 0$ such that $d_{i+1}^Q h_i + h_{i-1} d_i^P = \tilde{f}_i$ for all $i \geqslant 0$. (In the latter equation, when $i = 0$ we have $h_{-1} = 0$.)

Since $q \circ \tilde{f}_0 = 0p = 0$, the image of $\tilde{f}_0$ is contained in $\ker(q) = \operatorname{im}(d_1^Q) = B_0(Q_\bullet)$ and so since P_0 is projective, considering the diagram

$$\begin{array}{ccccc} & & & & P_0 \\ & & \overset{\exists h_0}{\swarrow} & & \downarrow \tilde{f}_0 \\ Q_1 & \xrightarrow{d_1^Q} & B_0(Q_\bullet) & \longrightarrow & 0. \end{array}$$

there is a map $h_0 : P_0 \to Q_1$ such that $d_1^Q \circ h_0 = g_0$ as needed.

We will proceed inductively again. When we separate out the "new part" in the null-homotopy equation, we get $d_{n+1}^Q h_n = \tilde{f}_n - h_{n-1} d_n^P$, so we want to use the projective lifting property to the map on the right; to do that, it should be in the image of the differential through which we want to lift it. Hence, we will be interested in showing that the image such a map consists of boundaries.

So, as part of the base case of our induction, we observe that

$$d_1^Q(\tilde{f}_1 - h_0 d_1^P) = d_1^Q \tilde{f}_1 - d_1^Q h_0 d_1^P = \tilde{f}_0 d_1^P - d_1^Q h_0 d_1^P = d_1^Q h_0 d_1^P - d_1^Q h_0 d_1^P = 0,$$

so $\operatorname{im}(\tilde{f}_1 - h_0 d_1^P) \subseteq Z_1(Q_\bullet) = B_1(Q_\bullet)$.

Suppose maps $h_0, \ldots, h_n$ have been constructed for some $n \geqslant 0$ with $d_{n+1}^Q h_n + h_{n-1} d_n^P = \tilde{f}_n$, and that $\operatorname{im}(\tilde{f}_{n+1} - h_n d_{n+1}^P) \subseteq B_{n+1}(Q_\bullet)$.

Since P_{n+1} is projective, considering the diagram

$$\begin{array}{ccccc} & & & & P_{n+1} \\ & & \overset{\exists h_{n+1}}{\swarrow} & & \downarrow \tilde{f}_{n+1} - h_n d_{n+1}^P \\ Q_{n+2} & \xrightarrow{d_{n+2}^Q} & B_{n+1}(Q_\bullet) & \longrightarrow & 0, \end{array}$$

there is a map $h_{n+1} : P_{n+1} \to Q_{n+2}$ such that $d_{n+2}^Q \circ h_{n+1} = \tilde{f}_{n+1} - h_n d_{n+1}^P$. Then

$$d_{n+2}^Q(\tilde{f}_{n+2} - h_{n+1} d_{n+2}^P) = \tilde{f}_{n+1} d_{n+2}^P - d_{n+2}^Q h_{n+1} d_{n+2}^P = (\tilde{f}_{n+1} - d_{n+2}^Q h_{n+1}) d_{n+2}^P = h_n d_{n+1}^P d_{n+2}^P = 0.$$

Again using exactness of $Q_\bullet$, we see that $\operatorname{im}(\tilde{f}_{n+2} - h_{n+1} d_{n+2}^P) \subseteq B_{n+2}(Q_\bullet)$. Thus, by induction, we can construct such a map h. □

Definition 4.47. Given two chain complexes $(M_\bullet, d)$ and $(N_\bullet, d)$, a chain map $f : M_\bullet \to N_\bullet$ is called a *homotopy equivalence*, written $f : M_\bullet \xrightarrow{\simeq} N_\bullet$, if there is a chain map $g : N_\bullet \to M_\bullet$ such that both compositions are homotopic to the identity map: $f \circ g \simeq_{\text{htpc}} \mathrm{id}_N$ and $g \circ f \simeq_{\text{htpc}} \mathrm{id}_M$.

Remark 4.48. If $f : M_\bullet \to N_\bullet$ is a homotopy equivalence, then f is a quasi-isomorphism. Indeed, using Proposition 4.33 we see that $H_i(f) \circ H_i(g) = H_i(f \circ g) = H_i(\mathrm{id}_N) = \mathrm{id}_{H_i(M_\bullet)}$ and $H_i(g) \circ H_i(f) = H_i(g \circ f) = H_i(\mathrm{id}_M) = \mathrm{id}_{H_i(N_\bullet)}$.

Example 4.49. Let M be an R-module and let

$$\cdots \to P_2 \to P_1 \to P_0 \to 0 \to \cdots$$

along with $\pi : P_0 \twoheadrightarrow M$ form a projective resolution of M. We may interpret this as an example of a quasi-isomorphism: The map π induces a chain map

$$\pi : P_\bullet \to M[0]$$

which is the map π in degree 0 and (necessarily) the zero map in all other degrees. (By abuse of notation, we call the chain map π too.) Here is a picture of the chain map π:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & M & \longrightarrow & 0 & \longrightarrow & \cdots . \end{array}$$

On homology we have $H_i(P_\bullet) = 0$ for all $i \neq 0$ and $H_i(M[0]) = 0$ for all $i \neq 0$, so that $H_i(\pi)$ is an isomorphism, vacuouly, for all $i \neq 0$. In degree 0, the map

$$H_0(\pi) : H_0(P_\bullet) \to H_0(M)$$

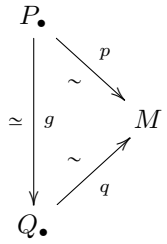
is the isomorphism $\overline{\pi} : \operatorname{coker}(d_0) = P_0/\operatorname{im}(d_0) = P_0/\ker(\pi) \xrightarrow{\cong} M$ induced by π. So π is indeed a quasi-isomorphism.

However, I clam that π is not a homotopy equivalence in general. If it were, there would be a chain map $g : M \to P_\bullet$ such that $\pi \circ g \simeq_{\text{htpc}} \text{id}_M$ (and also for the other composition). Note that the chain map g is really just a map $g_0 : M \to P_0$. Let h be a homotopy realizing $\pi \circ g \simeq_{\text{htpc}} \text{id}_M$. Since $M = M[0]$ is only nonzero in degree 0, h has to be the zero map. It follows that $\pi \circ g = \text{id}_M$ and hence the composition

$$M \xrightarrow{g_0} P_0 \xrightarrow{\pi} M$$

is the identity. That is, M is isomorphic to a summand of P_0 and hence M itself is projective. But, of course M is an arbitrary module so it need not be projective.

Corollary 4.50. *Any two projective resolutions of the same module are homotopy equivalent: if $p : C_\bullet \xrightarrow{\sim} M$ and $q : Q_\bullet \xrightarrow{\sim} M$ are two projective resolutions of a module M, then there is a homotopy equivalence $g : P_\bullet \xrightarrow{\simeq} Q_\bullet$ such that the triangle diagram of chain complexes*



commutes. (Equvialently, g is a lift of the identity map on M.) Moreover, g is unique up to homotopy.

Proof. Applying the previous result to the identity map on M gives a chain map $g : P_\bullet \to Q_\bullet$ such that $q \circ g = p$. Moreover, g is unique up to homotopy by the uniqueness clause of the previous result.

By interchanging the roles of $P_\bullet$ and $Q_\bullet$ we get a chain map $f : Q_\bullet \to P_\bullet$ such that $p \circ f = q$. The composition $f \circ g$ is a chain endomorphism of $P_\bullet$ such that $p \circ f \circ g = p$. Since we also have $p \circ id_{P_\bullet} = p$, the uniqueness clause of the previous result gives that $f \circ g$ is homotopic to $\text{id}_{C_\bullet}$. Similarly, $g \circ f$ is homotopic to $\text{id}_{Q_\bullet}$. □

I'll skip the proof of the following two statements. Both the statements and the proofs are given by flipping the orientation of all the arrows involved in the previous two statements and proofs.

Theorem 4.51. *Let M and N be R-modules, $f : M \to N$ an R-module homomorphism, and $i : M \xrightarrow{\sim} E^\bullet$ and $j : N \xrightarrow{\sim} F^\bullet$ injective resolutions. Then there is a lift $\tilde{f} : E^\bullet \to F^\bullet$ of f, and such a lift is unique up to homotopy.*

Corollary 4.52. *Any two injective resolutions of the same module are homotopy equivalent via a chain map that is unique up to homotopy.*

Optional Exercise 4.53. If g is a homotopy equivalence, and F is an additive covariant functor, then $F(g)$ is a homotopy equivalence.

4.5. **Derived functors.**

Definition 4.54. Let R and S be rings and $F : R-\mathbf{Mod} \to S-\mathbf{Mod}$ be a right exact covariant functor. For each $j \geqslant 0$, we define a functor $\mathbb{L}_j F : R-\mathbf{Mod} \to S-\mathbf{Mod}$ as follows:

For every R-module fix a projective resolution $P_\bullet^M \xrightarrow{p_M} M$, and for every R-module homomorphism $f : M \to N$, fix a chain map $\tilde{f} : P_\bullet^M \to P_\bullet^N$ lifting f.

- On objects, for an R-module M, we set $\mathbb{L}_j F(M) := H_j(F(P_\bullet))$.
- On morphisms, for $f : M \to N$, we set $\mathbb{L}_j F(f) := H_j(F(\tilde{f}))$.

We call $\mathbb{L}_j F$ the *jth left derived functor* of F.

Lecture of December 3, 2021

In fact, this definition is *not* well defined! However, it is well-defined up to natural isomorphism, and we follow the standard abuse of notation by calling it "the" derived functor rather than "a" derived functor.

Proposition 4.55. *Let R and S be rings and $F : R-\mathbf{Mod} \to S-\mathbf{Mod}$ be a right exact covariant functor. The functor $\mathbb{L}_j F$ is well-defined up to natural isomorphism; i.e., for two choices of projective resolutions and lifts of maps, there is a natural isomorphism between the functors resulting from the definition.*

Proof. For every R-module fix two projective resolutions $P_\bullet^M \xrightarrow{p_M} M$ and $Q_\bullet^M \xrightarrow{q_M} M$, and for every R-module homomorphism $f : M \to N$, fix chain maps $\tilde{f} : P_\bullet^M \to P_\bullet^N$ and $\tilde{f}' : Q_\bullet^M \to Q_\bullet^N$ lifting f. Set $\mathbb{L}_j F(M) := H_j(F(P_\bullet^M))$ with $\mathbb{L}_j F(f) := H_j(F(\tilde{f}))$ and $\mathbb{L}'_j F(M) := H_j(F(Q_\bullet^M))$ with $\mathbb{L}'_j F(f) := H_j(F(\tilde{f}'))$.

For any module M, there is a homotopy equivalence $g_M : P_\bullet^M \xrightarrow{\simeq_{\text{htpc}}} Q_\bullet^M$ that lifts the identity map on M. Then $F(e_M) : F(P_\bullet^M) \to F(Q_\bullet^M)$ is a homotopy equivalence, and hence a quasi-isomorphism; i.e., we define our natural isomorphism η via $\eta_M = H_j(F(e_M))$.

Let $f : M \to N$ be a morphism. We need to show that the square

$$\begin{array}{ccc} \mathbb{L}_j F(M) & \xrightarrow{\mathbb{L}_j F(f)} & \mathbb{L}_j F(N) \\ {\scriptstyle \eta_M}\downarrow & & \downarrow{\scriptstyle \eta_N} \\ \mathbb{L}'_j F(M) & \xrightarrow{\mathbb{L}'_j F(f)} & \mathbb{L}'_j F(N) \end{array}$$

commutes. To do so, consider the square of chain maps:

$$\begin{array}{ccc} P_\bullet^M & \xrightarrow{\tilde{f}} & P_\bullet^N \\ {\scriptstyle e_M}\downarrow & & \downarrow{\scriptstyle e_N} \\ Q_\bullet^M & \xrightarrow{\tilde{f}'} & Q_\bullet^N. \end{array}$$

This does not necessarily commute, but $\tilde{f}' \circ g_M$ and $g_N \circ \tilde{f}$ both lift f: since

$$\begin{array}{ccccc} P_\bullet^M & \xrightarrow{g_M} & Q_\bullet^M & \xrightarrow{\tilde{f}'} & Q_\bullet^N \\ \downarrow{\scriptstyle p_M} & & \downarrow{\scriptstyle q_M} & & \downarrow{\scriptstyle q_N} \\ M & \xrightarrow{1_M} & M & \xrightarrow{f} & N \end{array}$$

commutes, we have that $\tilde{f}' \circ g_M$ lifts f, and similarly for the other composition. By homotopy uniqueness of lifts for projective resolutions, we have $\tilde{f}' \circ e_M \simeq_{\text{htpc}} e_N \circ \tilde{f}$. Since additive functors preserve homotopies, we have $F(\tilde{f}' \circ e_M) \simeq_{\text{htpc}} F(e_N \circ \tilde{f})$ Homotopic maps induce the same map on homology, so we have

$$H_j(F(\tilde{f}')) \circ H_j(F(e_M)) = H_j(F(\tilde{f}' \circ e_M)) = H_j(F(e_N \circ \tilde{f})) = H_j(F(e_N)) \circ H_j(F(\tilde{f})).$$

This is exactly the commutativity of the square. □

Optional Exercise 4.56. Let R and S be rings and $F : R - \mathbf{Mod} \to S - \mathbf{Mod}$ be a right exact covariant functor. Then $\mathbb{L}_j F$ is additive.

Here is the key example of a left derived functor.

4.5.1. *The Tor functor.*

Definition 4.57. For a ring R, right R-module N and left R-module M, we define

$$\operatorname{Tor}_j^R(N, M) := \mathbb{L}_j(N \otimes_R -)(M)$$

to be the j-th left derived functor of the functor $N \otimes_R - : R - \mathbf{Mod} \to \mathbf{Ab}$. So, for each j, $\operatorname{Tor}_j^R(N, M)$ is an abelian group. When R is commutative, $N \otimes_R -$ can be viewed as taking values in $R - \mathbf{Mod}$ and hence $\operatorname{Tor}_j^R(N, M)$ is an R-module; analogously when N is a bimodule.

Explicitly,

$$\operatorname{Tor}_j^R(N, M) = H_j(\cdots \xrightarrow{\mathrm{id}_N \otimes d_3} N \otimes_R P_2 \xrightarrow{\mathrm{id}_N \otimes d_2} N \otimes_R P_1 \xrightarrow{\mathrm{id}_N \otimes d_1} N \otimes_R P_0 \to 0 \to \cdots)$$

where $P_\bullet \xrightarrow{\sim} M$ is a projective resolution of M.

Lecture of December 6, 2021

Example 4.58. Let's compute $\operatorname{Tor}_j^{\mathbb{Z}}(N, \mathbb{Z}/n\mathbb{Z})$ for any $\mathbb{Z}$-module N and integers $n \geqslant 1$, and j.

We have the projective resolution $\cdots \to 0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} (\to \mathbb{Z}/n\mathbb{Z}) \to 0$ of $\mathbb{Z}/n\mathbb{Z}$ and so $\operatorname{Tor}_j^R(N, \mathbb{Z}/n\mathbb{Z})$ is the homology of the complex

$$\cdots 0 \to N \otimes_{\mathbb{Z}} \mathbb{Z} \xrightarrow{\mathrm{id}_N \otimes n} N \otimes_{\mathbb{Z}} \mathbb{Z} \to 0$$

(where the two nonzero terms lie in degrees 0 and 1). This complex is isomorphic to the complex

$$\cdots 0 \to N \xrightarrow{n} N \to 0$$

and hence

$$\operatorname{Tor}_0^R(N, \mathbb{Z}/n\mathbb{Z}) \cong N/nN \cong N \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z},$$

$$\operatorname{Tor}_1^R(N, \mathbb{Z}/n\mathbb{Z}) \cong \ker(N \xrightarrow{n} N) = \{x \in N \mid n \cdot x = 0\},$$

and

$$\operatorname{Tor}_j^R(N, \mathbb{Z}/n\mathbb{Z}) = \mathbb{L}_j F(\mathbb{Z}/n\mathbb{Z}) = 0$$

for all $j \notin \{0, 1\}$.

Note that $\operatorname{Tor}_1^R(N, \mathbb{Z}/n\mathbb{Z})$ is the n-torsion submodule of N — this explains the notation Tor.

Example 4.59. Let $R = k[x, y]$ for a field k and let M be an R-module. Let's compute $\operatorname{Tor}_*^R(M, R/(x, y))$. The kernel of the canonical surjection $R \twoheadrightarrow R/(x, y)$ is the ideal (x, y) and from before we saw how to resolve (x, y) freely. This gives the resolution

$$\cdots \to 0 \to R \xrightarrow{\begin{bmatrix} -y \\ x \end{bmatrix}} R^2 \xrightarrow{\begin{bmatrix} x & y \end{bmatrix}} R \to R/(x, y) \to 0.$$

It follows that $\operatorname{Tor}_*^R(M, R/(x, y))$ is the homology of the complex

$$\cdots \to 0 \to M \xrightarrow{\begin{bmatrix} -y \\ x \end{bmatrix}} M^{\oplus 2} \xrightarrow{\begin{bmatrix} x & y \end{bmatrix}} M \to 0 \to \cdots.$$

So $\operatorname{Tor}_2^R(M, R/(x, y)) = \{m \in M \mid xm = 0 = ym\}$. The module $\operatorname{Tor}_1^R(M, R/(x, y))$ is a bit more complicated: It consists of pairs (m, n) in $M \oplus M$ such that $xm + yn = 0$, modulo the "obvious" pairs that satisfy this condition, namely those of the form $(-yt, xt)$ for some $t \in M$.

Returning to the general situation of a right exact covariant functor F, let's compute a "formula" for the 0th left derived functor $\mathbb{L}_0 F(M)$.

Proposition 4.60. *For any covariant right exact functor F and R-module M, there is a natural isomorphism*

$$\mathbb{L}_0 F(M) \cong F(M)$$

In particular,

$$\operatorname{Tor}_0^R(N, M) \cong N \otimes_R M$$

for all right R-modules N and left R-modules M.

Proof. Let $P_\bullet \xrightarrow{\sim} M$ be a projective resolution for M. Since $P_1 \xrightarrow{d_1} P_0 \xrightarrow{p} M \to 0$ is right exact, so is

$$F(P_1) \xrightarrow{F(d_1)} F(P_0) \xrightarrow{F(p)} F(M) \to 0.$$

The homology in degree 0 of $F(P_\bullet)$ is the cokernel of $F(P_1) \xrightarrow{F(d_1)} F(P_0)$, which is isomorphic to $F(M)$ via $H_0(F(p))$.

The check of naturality is left as an exercise. □

The following proposition is a first justification of the idea that derived functors measure the failure of exactness.

Proposition 4.61. *If F is an exact covariant functor, then $\mathbb{L}_i F \equiv 0$ for all $i > 0$.*

Proof. If $P_\bullet$ is a projective resolution of a module M, then $P_\bullet \xrightarrow{p} M \to 0$ is exact, and so is $F(P_\bullet) \xrightarrow{F(p)} F(M)$. Thus, $H_i(F(P_\bullet)) \cong 0$ for $i > 0$. □

A large part of the magic of Tor comes from the following fact, called balancedness of Tor. For every R-module M, there is a right exact functor

$$- \otimes_R M : R^{\mathrm{op}} - \mathbf{Mod} \to \mathbf{Ab}.$$

We can take the left derived functors of this; let's say

$$\operatorname{Tor}'^R_i(-, M) := \mathbb{L}_i(- \otimes_R M).$$

Then Balancedness of Tor states that for every right R-module N and every left R-module M, there is an isomorphism $\mathrm{Tor}_i^R(N,M) \cong \mathrm{Tor}'^R_i(N,M)$. Concretely, if $P_\bullet$ is a projective resolution of M and $Q_\bullet$ is a projective resolution of N, then

$$H_i(P_\bullet \otimes_R N) \cong H_i(M \otimes_R Q_\bullet).$$

Maybe we'll prove this later if we have time.

4.5.2. *Right derived functors.*

Definition 4.62. Let R and S be rings and $F : R-\mathbf{Mod} \to S-\mathbf{Mod}$ be a left exact covariant functor. For each $j \geqslant 0$, we define a functor $\mathbb{R}^jF : R-\mathbf{Mod} \to S-\mathbf{Mod}$ as follows:

For every R-module fix an injective resolution $M \xrightarrow{\varepsilon^M} E^\bullet_M$, and for every R-module homomorphism $f : M \to N$, fix a chain map $\tilde{f} : E^\bullet_M \to E^\bullet_N$ lifting f.

- On objects, for an R-module M, we set $\mathbb{R}^jF(M) := H^j(F(E^\bullet_M))$.
- On morphisms, for $f : M \to N$, we set $\mathbb{R}^jF(f) := H^j(F(\tilde{f}))$.

We call $\mathbb{R}^jF$ the *jth right derived functor* of F.

Definition 4.63. Let R and S be rings and $G : R-\mathbf{Mod} \to S-\mathbf{Mod}$ be a left exact contravariant functor. Recall that such a functor turns right exact sequences into left exact sequences. For each $j \geqslant 0$, we define a functor $\mathbb{R}^jG : R-\mathbf{Mod} \to S-\mathbf{Mod}$ as follows:

For every R-module fix a projective resolution $P^M_\bullet \xrightarrow{p_M} M$, and for every R-module homomorphism $f : M \to N$, fix a chain map $\tilde{f} : P^M_\bullet \to P^N_\bullet$ lifting f.

- On objects, for an R-module M, we set $\mathbb{R}^jG(M) := H^j(G(P^M_\bullet))$.
- On morphisms, for $f : M \to N$, we set $\mathbb{R}^jG(f) := H^j(G(\tilde{f}))$.

We call $\mathbb{R}^jG$ the *jth right derived functor* of F.

The following summarizes properties analogous to those worked out carefully above for right exact covariant functors:

Proposition 4.64. *Let R, S, F, and G be as in the definitions above.*

- *The functors $\mathbb{R}^iF$ and $\mathbb{R}^iG$ are well-defined up to natural isomorphism.*
- *We have canonical isomorphisms $\mathbb{R}^0F(M) \cong F(M)$ and $\mathbb{R}^0G(M) \cong G(M)$.*
- *If F or G is exact, $\mathbb{R}^{>0}F \equiv 0$ or $\mathbb{R}^{>0}G \equiv 0$, respectively.*

4.5.3. *The* Ext *functor.*

Definition 4.65. For a pair of left R-modules M and N, we define

$$\mathrm{Ext}^j_R(M,-)^I = \mathbb{R}^j\mathrm{Hom}_R(M,-)$$

and

$$\mathrm{Ext}^j_R(-,N)^{II} = \mathbb{R}^j\mathrm{Hom}_R(-,N).$$

Both $\mathrm{Ext}^j_R(M,N)^I$ and $\mathrm{Ext}^j_R(M,N)^{II}$ are abelian groups in general and R-modules when R is commutative.

There is a balancedness statement for Ext as well: for every pair of R-modules M and N, $\mathrm{Ext}^j_R(M,N)^I \cong \mathrm{Ext}^j_R(M,N)^{II}$. Then one just writes

$$\mathrm{Ext}^j_R(M,N) := \mathrm{Ext}^j_R(M,N)^I = \mathrm{Ext}^j_R(M,N)^{II}.$$

For now we'll keep the superscripts.

Lecture of December 8, 2021

Example 4.66. Let's compute $\mathrm{Ext}^*_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})^I$ and $\mathrm{Ext}^*_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})^{II}$.

For the latter, we start with the free resolution $\cdots 0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} (\to \mathbb{Z}/m\mathbb{Z}) \to 0$ of $\mathbb{Z}/m$ and apply $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/n\mathbb{Z})$ to obtain

$$\cdots \leftarrow 0 \leftarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \xleftarrow{m} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \leftarrow 0$$

which is isomorphic to

$$\cdots \leftarrow 0 \leftarrow \mathbb{Z}/n\mathbb{Z} \xleftarrow{m} \mathbb{Z}/n\mathbb{Z} \leftarrow 0.$$

The two nonzero homology modules are both isomorphic to $\mathbb{Z}/g\mathbb{Z}$ where $g = gcd(m, n)$. So

$$\mathrm{Ext}^i_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})^{II} \cong \begin{cases} \mathbb{Z}/g\mathbb{Z} & i = 0, 1 \\ 0 & i \geqslant 2. \end{cases}$$

For the former, we will use the following fact: For any integer j there is a short exact sequence

$$0 \to \mathbb{Z}/j\mathbb{Z} \xrightarrow{\overline{1} \mapsto \overline{1/n}} \mathbb{Q}/\mathbb{Z} \xrightarrow{j} \mathbb{Q}/\mathbb{Z} \to 0.$$

This holds since $\mathbb{Q}/\mathbb{Z}$ is divisible and the kernel of multiplication by j is $\{\overline{\frac{i}{j}} \mid 0 \leqslant i \leqslant j-1\}$, which is generated by $\overline{1/n}$.

In particular, we have an injective resolution

$$0 \to \mathbb{Z}/n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \xrightarrow{n} \mathbb{Q}/\mathbb{Z} \to 0 \to \cdots$$

of $\mathbb{Z}/n\mathbb{Z}$. Applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, -)$ gives

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{n} \mathrm{Hom}_{\mathbb{Z}}(Z/m\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to 0 \to \cdots .$$

Now, the only elements of $\mathbb{Q}/\mathbb{Z}$ have have order a multiple of m are the elements $\frac{j}{m} + \mathbb{Z}$ for $0 \leqslant j < m$, and they form a cyclic subgroup of order m. It follows that

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}$$

and that the previous complex is isomorphic to

$$\cdots \to 0 \to \mathbb{Z}/m\mathbb{Z} \xrightarrow{n} \mathbb{Z}/m\mathbb{Z} \to 0 \to \cdots$$

This gives

$$\mathrm{Ext}^i_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})^I \cong \begin{cases} \mathbb{Z}/g\mathbb{Z} & i = 0, 1 \\ 0 & i \geqslant 2. \end{cases}$$

4.6. **Long exact sequence of a derived functor.** Our next goal is to explain how we can use derived functors to extend a left exact or right exact sequence obtained from a functor into a long exact sequence.

The technical ingredient we need is a method to lift short exact sequences to resolutions.

Lemma 4.67. *Let*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

be a short exact sequence.

Then there exist projective resolutions $P_\bullet^A \to A$, $P_\bullet^B \to B$, $P_\bullet^C \to C$ *and lifts* $P_\bullet^A \xrightarrow{\tilde{f}} P_\bullet^B$, $P_\bullet^B \xrightarrow{\tilde{g}} P_\bullet^C$ *such that*

$$0 \to P_i^A \xrightarrow{\tilde{f}_i} P_i^B \xrightarrow{\tilde{g}_i} P_i^C \to 0$$

is exact for all i.

Likewise, there exist injective resolutions $A \to E_A^\bullet$, $B \to E_B^\bullet$, $C \to E_C^\bullet$ *and lifts* $E_A^\bullet \xrightarrow{\tilde{f}} E_B^\bullet$, $E_B^\bullet \xrightarrow{\tilde{g}} E_C^\bullet$ *such that*

$$0 \to E_A^i \xrightarrow{\tilde{f}_i} E_B^i \xrightarrow{\tilde{g}_i} E_C^i \to 0$$

is exact for all i.

Proof. Start with any projective resolutions for A and C, $P_\bullet^A \to A$ and $P_\bullet^C \to C$. For all i, set $P_i^B := P_i^A \oplus P_i^C$ for all i, $\tilde{f}_i : P_i^A \to P_i^A \oplus P_i^C$ to be the inclusion map, and $\tilde{g}_i : P_i^A \oplus P_i^C \to P_i^C$ to be the projection map. Clearly

$$0 \to P_i^A \xrightarrow{\tilde{f}_i} P_i^B \xrightarrow{\tilde{g}_i} P_i^C \to 0$$

is exact for all i.

We need to construct differentials (including an augmentation) on P_i^B that make $P_i^B \to B$ an exact complex and $\tilde{f}$ and $\tilde{g}$ chain maps. Since P_0^C is projective and $g : B \to C$ is surjective, we can lift

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_0^A & \xrightarrow{\tilde{f}_0} & P_0^B & \xrightarrow{\tilde{g}_0} & P_0^C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle p_A} & & & \swarrow{\scriptstyle \gamma} & \downarrow{\scriptstyle p_C} & & \\
0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0,
\end{array}$$

so $g\gamma = p_C$. Set $p_B : P_0^B (= P_0^A \oplus P_0^C) \to B$ to be $fp_A \oplus \gamma$.

Then the diagram commutes:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_0^A & \xrightarrow{\tilde{f}_0} & P_0^B & \xrightarrow{\tilde{g}_0} & P_0^C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle p_A} & & \downarrow{\scriptstyle p_B} & & \downarrow{\scriptstyle p_C} & & \\
0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0;
\end{array}$$

the left square is clear, and for the right

$$p_C \tilde{g}_0(u, w) = p_C(w) = g\gamma(w); \quad gp_b(u, w) = g(fp_A(u) + \gamma(w)) = g\gamma(w).$$

By the Snake Lemma,

$$\operatorname{coker}(p_A) \to \operatorname{coker}(p_B) \to \operatorname{coker}(p_C) \to 0$$

is exact, so p_B is surjective. Also,

$$0 \to \ker(p_A) \to \ker(p_B) \to \ker(p_C) \to \operatorname{coker}(A)$$

is exact, so

$$0 \to \ker(p_A) \to \ker(p_B) \to \ker(p_C) \to 0$$

is.

We can now proceed inductively on i (precisely, that we have constructed $d_1^B, \ldots, d_i^B$ such that $H_j(P_\bullet^B) = 0$ for $i = 0, \ldots, i$, the maps $\tilde{f}$ and $\tilde{g}$ are chain maps up through the ith spot, and that the ith induced maps

on cycles also form a short exact sequence), at each step applying essentially the previous case to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P^A_{i+1} & \xrightarrow{\tilde{f}_{i+1}} & P^B_{i+1} & \xrightarrow{\tilde{g}_{i+1}} & P^C_{i+1} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d^A_{i+1}} & & & & \downarrow{\scriptstyle d^C_{i+1}} & & \\ 0 & \longrightarrow & Z_i(P^A_\bullet) & \xrightarrow{\tilde{f}_i} & Z_i(P^B_\bullet) & \xrightarrow{\tilde{g}_i} & Z_i(P^C_\bullet) & \longrightarrow & 0. \end{array}$$

The injective case is similar. □

Theorem 4.68. *Let*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

be a short exact sequence.

(1) *Let $F : R-\mathbf{Mod} \to S-\mathbf{Mod}$ be a covariant right exact functor. Then there is a long exact sequence*

$$\cdots \to \mathbb{L}_i F(A) \xrightarrow{\mathbb{L}_i F(f)} \mathbb{L}_i F(B) \xrightarrow{\mathbb{L}_i F(g)} \mathbb{L}_i F(C) \xrightarrow{\partial_i} \mathbb{L}_{i-1} F(A) \to \cdots \to \mathbb{L}_1 F(C) \xrightarrow{\partial_1} F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \to 0.$$

(2) *Let $F : R-\mathbf{Mod} \to S-\mathbf{Mod}$ be a covariant left exact functor. Then there is a long exact sequence*

$$0 \to F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \xrightarrow{\partial_1} \mathbb{R}^1 F(A) \to \cdots \to \mathbb{R}^{i-1} F(C) \xrightarrow{\partial_{i-1}} \mathbb{R}^i F(A) \xrightarrow{\mathbb{R}^i F(f)} \mathbb{R}^i F(B) \xrightarrow{\mathbb{R}^i F(g)} \mathbb{R}^i F(C) \to \cdots$$

(3) *Let $G : R-\mathbf{Mod} \to S-\mathbf{Mod}$ be a contravariant left exact functor. Then there is a long exact sequence*

$$0 \to G(C) \xrightarrow{G(g)} G(B) \xrightarrow{G(f)} G(A) \xrightarrow{\partial_1} \mathbb{R}^1 G(C) \to \cdots \to \mathbb{R}^{i-1} G(A) \xrightarrow{\partial_{i-1}} \mathbb{R}^i G(C) \xrightarrow{\mathbb{R}^i G(g)} \mathbb{R}^i G(B) \xrightarrow{\mathbb{R}^i G(f)} \mathbb{R}^i G(A) \to \cdots$$

Proof. For (1), take projective resolutions $P^A_\bullet \to A$, $P^B_\bullet \to B$, $P^C_\bullet \to C$ and lifts $P^A_\bullet \xrightarrow{\tilde{f}} P^B_\bullet$, $P^B_\bullet \xrightarrow{\tilde{g}} P^C_\bullet$ such that

$$0 \to P^A_i \xrightarrow{\tilde{f}_i} P^B_i \xrightarrow{\tilde{g}_i} P^C_i \to 0$$

is exact for all i. Observe that these sequences are all split exact, since P^C_i is projective. Then

$$0 \to F(P^A_i) \xrightarrow{F(\tilde{f}_i)} F(P^B_i) \xrightarrow{F(\tilde{g}_i)} F(P^C_i) \to 0$$

is split exact for all i, as well. That is,

$$0 \to F(P^A_\bullet) \xrightarrow{F(\tilde{f})} F(P^B_\bullet) \xrightarrow{F(\tilde{g})} F(P^C_\bullet) \to 0$$

is a short exact sequence of complexes. We obtain a long exact sequence in homology. Applying the definitions, this is exactly the long exact sequence above.

(2) and (3) are similar. □

We apply these to Ext and Tor.

Theorem 4.69. *Let*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

be a short exact sequence of R-modules.

(1) *For any right R-module N, there is a long exact sequence*

$$\cdots \to \operatorname{Tor}^R_i(N, A) \xrightarrow{\operatorname{Tor}^R_i(N,f)} \operatorname{Tor}^R_i(N, B) \xrightarrow{\operatorname{Tor}^R_i(N,g)} \operatorname{Tor}^R_i(N, C) \xrightarrow{\partial_i} \operatorname{Tor}^R_{i-1}(N, A) \to \cdots$$
$$\cdots \to \operatorname{Tor}^R_1(N, C) \xrightarrow{\partial_1} N \otimes_R A \xrightarrow{N \otimes_R f} N \otimes_R B \xrightarrow{N \otimes_R g} N \otimes_R C \to 0.$$

(2) *For any R-module M, there is a long exact sequence (thinking of* Ext *as* Ext^I*)*

$$0 \to \mathrm{Hom}_R(M,A) \xrightarrow{\mathrm{Hom}_R(M,f)} \mathrm{Hom}_R(M,B) \xrightarrow{\mathrm{Hom}_R(M,g)} \mathrm{Hom}_R(M,C) \xrightarrow{\partial_1} \mathrm{Ext}^1_R(M,A) \to \cdots$$

$$\cdots \to \mathrm{Ext}^{i-1}_R(M,C) \xrightarrow{\partial_{i-1}} \mathrm{Ext}^i_R(M,A) \xrightarrow{\mathrm{Ext}^i_R(M,f)} \mathrm{Ext}^i_R(M,B) \xrightarrow{\mathrm{Ext}^i_R(M,g)} \mathrm{Ext}^i_R(M,C) \to \cdots$$

(3) *For any R-module M, there is a long exact sequence (thinking of* Ext *as* Ext^{II}*)*

$$0 \to \mathrm{Hom}_R(C,M) \xrightarrow{\mathrm{Hom}_R(g,M)} \mathrm{Hom}_R(B,M) \xrightarrow{\mathrm{Hom}_R(f,M)} \mathrm{Hom}_R(A,M) \xrightarrow{\partial_1} \mathrm{Ext}^1_R(C,M) \to \cdots$$

$$\cdots \to \mathrm{Ext}^{i-1}_R(A,M) \xrightarrow{\partial_{i-1}} \mathrm{Ext}^i_R(C,M) \xrightarrow{\mathrm{Ext}^i_R(g,M)} \mathrm{Ext}^i_R(B,M) \xrightarrow{\mathrm{Ext}^i_R(g,M)} \mathrm{Ext}^i_R(A,M) \to \cdots$$

In particular, the long exact sequences give us the correction term for failure of left exactness of Tor / right exactness of Ext: they are given by connecting maps in the corresponding long exact sequences.

Here is an application of the long exact sequence.

Proposition 4.70. *Let R be a ring, and M be an R-module. The following are equivalent:*

(1) *M is projective.*
(2) *$\mathrm{Ext}^i_R(M,N) = 0$ for all $i > 0$ and all R-modules N.*
(3) *$\mathrm{Ext}^1_R(M,N) = 0$ for all $i > 0$ and all R-modules N.*

Proof. If M is projective, then $\mathrm{Hom}_R(M,-)$ is exact. Hence, its (nontrivial) right derived functors all vanish, as shown above.

If $\mathrm{Ext}^1_R(M,N) = 0$ for all $i > 0$, we claim that $\mathrm{Hom}_R(M,-)$ is exact. Indeed, given a short exact sequence

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

the long exact sequence of $\mathrm{Ext}^i_R(M,-)$ starts

$$0 \to \mathrm{Hom}_R(M,A) \xrightarrow{\mathrm{Hom}_R(M,f)} \mathrm{Hom}_R(M,B) \xrightarrow{\mathrm{Hom}_R(M,g)} \mathrm{Hom}_R(M,C) \to \mathrm{Ext}^1_R(M,A) \to \cdots .$$

By assumption, we then have that

$$0 \to \mathrm{Hom}_R(M,A) \xrightarrow{\mathrm{Hom}_R(M,f)} \mathrm{Hom}_R(M,B) \xrightarrow{\mathrm{Hom}_R(M,g)} \mathrm{Hom}_R(M,C) \to 0$$

is exact. Thus, $\mathrm{Hom}_R(M,-)$ is an exact functor, and M is projective. □

Remark 4.71. In this argument, we showed that M is projective if and only if $\mathrm{Ext}^{>0}(M,N)^I \equiv 0$ for all N; no balancing of Ext was used. Note that if M is projective, we clearly also have $\mathrm{Ext}^{>0}(M,N)^{II} \equiv 0$ for all N, since we can take a projective resolution for M that only lives in degree 0.

Lecture of December 10, 2021

Similarly,

Proposition 4.72. *Let R be a ring, and M be an R-module. The following are equivalent:*

(1) *N is injective.*
(2) *$\mathrm{Ext}^i_R(M,N) = 0$ for all $i > 0$ and all R-modules M.*
(3) *$\mathrm{Ext}^1_R(M,N) = 0$ for all $i > 0$ and all R-modules M.*

Here is a slightly more subtle fact.

Proposition 4.73. *Let L and N be R-modules. If $\mathrm{Ext}^1_R(N,L) = 0$ then every short exact sequence of the form*

$$X_\bullet : \qquad 0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

splits.

Proof. Recall that $X_\bullet$ splits if and only if there is some $q : M \to L$ such that $qf = 1_L$; equivalently, $1_L \in \mathrm{im}(\mathrm{Hom}_R(f, L))$. Consider the long exact sequence of $\mathrm{Ext}^i_R(-, L)$:

$$0 \to \mathrm{Hom}_R(N, L) \xrightarrow{\mathrm{Hom}_R(g,L)} \mathrm{Hom}_R(M, L) \xrightarrow{\mathrm{Hom}_R(f,L)} \mathrm{Hom}_R(L, L) \xrightarrow{\partial} \mathrm{Ext}^1_R(N, L) \to \cdots .$$

From the assumption, we have $\partial = 0$, so $\mathrm{Hom}_R(f, L)$ is surjective, and the claim follows. □

4.7. **Balancing Tor and Ext.** Our last goal is to balance Tor and Ext. We'll just deal with Ext, but Tor is similar.

Definition 4.74. Given a module M and a projective resolution $P_\bullet \to M$, we denote by $\Omega_i(M)$ the $i-1$ module of cycles of the exact complex (augmented resolution)

$$\cdots \to P_2 \to P_1 \to P_0 \to M \to 0.$$

We call this the ith *syzygy* module of M.

The modules $\Omega_i(M)$ depend on the choice of projective resolution (but there is a uniqueness type statement given by Schanuel's Lemma). Note that $\Omega_0(M) = M$ and that for all $i \geqslant 0$ we have a short exact sequence

$$0 \to \Omega_{i+1}(M) \to P_i \to \Omega_i(M) \to 0.$$

Similarly, given an injective resolution $M \to E^\bullet$, we define the *cosyzygy* modules $\Omega^i(M)$, and have $\Omega^0(M) = M$ and

$$0 \to \Omega^i(M) \to E_i \to \Omega^{i+1}(M) \to 0.$$

Lemma 4.75. (1) *Let F be a right exact covariant functor. Then for all $i \geqslant 0$ and all $j > 0$ there are isomorphisms*

$$\mathbb{L}_j F(\Omega_{i+1}(M)) \cong \mathbb{L}_{j+1} F(\Omega_i(M)).$$

Hence, $\mathbb{L}_k F(M) \cong \mathbb{L}_1 F(\Omega_{k-1}(M))$ for all $k > 0$.

(2) *Let F be a left exact covariant functor. Then for all $i \geqslant 0$ and $j > 0$ there are isomorphisms*

$$\mathbb{R}^j F(\Omega^{i+1}(M)) \cong \mathbb{R}^{j+1} F(\Omega^i(M)).$$

Hence $\mathbb{R}^k F(M) \cong \mathbb{R}^1 F(\Omega^{k-1} M)$ for all $k > 0$.

(3) *Let G be a left exact contravariant functor. Then for all $i \geqslant 0$ and $j > 0$ there are isomorphisms*

$$\mathbb{R}^j G(\Omega_{i+1}(M)) \cong \mathbb{R}^{j+1} G(\Omega_i(M)).$$

Hence $\mathbb{R}^k G(M) \cong \mathbb{R}^1 G(\Omega_{k-1} M)$ for all $k > 0$.

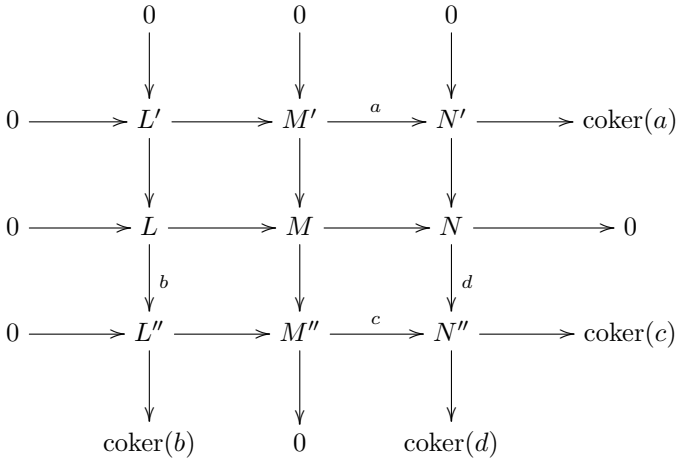
Proof. Take the long exact sequence of $\mathbb{L}_j F$ from the short exact sequence above. We get

$$\cdots \mathbb{L}_{j+1} F(P_i) \to \mathbb{L}_{j+1} \Omega_i(M) \to \mathbb{L}_j \Omega_{i+1}(M) \to \mathbb{L}_j F(P_i) \to \cdots .$$

For $j > 0$, we have $\mathbb{L}_j F(P_i) = 0$ since P_i is projective (so it is a projective resolution of itself). The isomorphisms follow.

The other cases are similar. □

Lemma 4.76. *Given a commutative diagram with each row and column exact of the form*



we have $\operatorname{coker}(a) \cong \operatorname{coker}(b)$ *and* $\operatorname{coker}(c) = \operatorname{coker}(d)$.

Proof. Since M surjects onto N and onto M'', we have

$$\operatorname{im}(c) = \operatorname{im}(M \to M'' \to N'') = \operatorname{im}(M \to N \to N'') = \operatorname{im}(d),$$

so $\operatorname{coker}(c) = \operatorname{coker}(d)$.

We can apply the Snake Lemma to the bottom two rows to get

$$M' \xrightarrow{a} N' \to \operatorname{coker}(b) \to 0$$

exact, so $\operatorname{coker}(c) \cong \operatorname{coker}(b)$. □

Theorem 4.77. *Let M, N be R-modules. Then $\operatorname{Ext}^n_R(M,N)^I \cong \operatorname{Ext}^n_R(M,N)^{II}$. (I.e., $\mathbb{R}^n\operatorname{Hom}_R(M,-)(N) \cong \mathbb{R}^n(\operatorname{Hom}_R(-,N)(M))$.*

Proof. For $n = 0$, we have $\operatorname{Hom}_R(M,N)$ for both sides.

Fix a projective resolutions $P_\bullet \to M$ and injective resolution $Q_\bullet \to N$. We have the short exact sequences

$$0 \to \Omega_{i+1}(M) \xrightarrow{\alpha} P_i \xrightarrow{\beta} \Omega_i(M) \to 0$$

for all $i \geqslant 0$. Apply $\operatorname{Hom}_R(-, E^j)$ yields a short exact sequence

$$0 \to \operatorname{Hom}_R(\Omega_i(M), E^j) \xrightarrow{\beta^*} \operatorname{Hom}_R(P_i, E^j) \xrightarrow{\alpha^*} \operatorname{Hom}_R(\Omega_{i+1}(M), E^j) \to 0.$$

From the functor $\operatorname{Hom}_R(-, \Omega^j(N))$ we get the long exact sequence

$$\begin{aligned} 0 \to \operatorname{Hom}_R(\Omega_i(M),\Omega^j(N)) &\xrightarrow{\beta^*} \operatorname{Hom}_R(P_i, \Omega^j(N)) \xrightarrow{\alpha^*} \operatorname{Hom}_R(\Omega_{i+1}(M), \Omega^j(N)) \\ &\to \operatorname{Ext}^1_R(\Omega_i(M), \Omega^j(N)) \to \operatorname{Ext}^1_R(P_i, \Omega^j(N)) \to \cdots . \end{aligned}$$

Note that the last term is zero, since P_i is projective.

Now, we also have the short exact sequences

$$0 \to \Omega^j(N) \xrightarrow{\gamma} E^j \xrightarrow{\zeta} \Omega^{j+1}(N) \to 0,$$

which yield short exact sequences

$$0 \to \operatorname{Hom}_R(P_i, \Omega^j(N)) \xrightarrow{\gamma_*} \operatorname{Hom}_R(P_i, E^j) \xrightarrow{\zeta_*} \operatorname{Hom}_R(P_i, \Omega^{j+1}(N)) \to 0$$

and long exact sequences

$$0 \to \mathrm{Hom}_R(\Omega_i(M),\Omega^j(N)) \xrightarrow{\gamma_*} \mathrm{Hom}_R(\Omega_i(M), E^j) \xrightarrow{\zeta_*} \mathrm{Hom}_R(\Omega_i(M), \Omega^{j+1}(N))$$
$$\to \mathrm{Ext}^1_R(\Omega_i(M), \Omega^j(N)) \to \mathrm{Ext}^1_R(\Omega_i(M), E^j) \to \cdots .$$

Again, the last term here is zero.

Thus, there is a diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_R(\Omega_i(M), \Omega^j(N)) & \xrightarrow{\beta^*} & \mathrm{Hom}_R(P_i, \Omega^j(N)) & \xrightarrow{\alpha^*} & \mathrm{Hom}_R(\Omega_{i+1}(M), \Omega^j(N)) & \longrightarrow & \mathrm{Ext}^1_R(\Omega_i(M), \Omega^j(N))^{II} \longrightarrow 0 \\
 & & \downarrow{\scriptstyle \gamma_*} & & \downarrow{\scriptstyle \gamma_*} & & \downarrow{\scriptstyle \gamma_*} & & \\
0 & \longrightarrow & \mathrm{Hom}_R(\Omega_i(M), E^j) & \xrightarrow{\beta^*} & \mathrm{Hom}_R(P_i, E^j) & \xrightarrow{\alpha^*} & \mathrm{Hom}_R(\Omega_{i+1}(M), E^j) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \zeta_*} & & \downarrow{\scriptstyle \zeta_*} & & \downarrow{\scriptstyle \zeta_*} & & \\
0 & \longrightarrow & \mathrm{Hom}_R(\Omega_i(M), \Omega^{j+1}(N)) & \xrightarrow{\beta^*} & \mathrm{Hom}_R(P_i, \Omega^{j+1}(N)) & \xrightarrow{\alpha^*} & \mathrm{Hom}_R(\Omega_{i+1}(M), \Omega^{j+1}(N)) & \longrightarrow & \mathrm{Ext}^1_R(\Omega_i(M), \Omega^{j+1}(N))^{II} \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathrm{Ext}^1_R(\Omega_i(M), \Omega^j(N))^I & & 0 & & \mathrm{Ext}^1_R(\Omega_{i+1}(M), \Omega^j(N))^I & & \\
 & & \downarrow & & & & \downarrow & & \\
 & & 0 & & & & 0 & &
\end{array}$$

Furthermore, this diagram commutes, as in each square the two maps are given by precomposing and postcomposing by the same pair of maps.

From the lemma, we see immediately that

$$\mathrm{Ext}^1_R(\Omega_i(M), \Omega^j(N))^I \cong \mathrm{Ext}^1_R(\Omega_i(M), \Omega^j(N))^{II},$$

so taking $i = j = 0$, we have

$$\mathrm{Ext}^1_R(M, N)^I \cong \mathrm{Ext}^1_R(M, N)^{II}.$$

We also have

$$\mathrm{Ext}^1_R(\Omega_{i+1}(M), \Omega^j(N))^I \cong \mathrm{Ext}^1_R(\Omega_i(M), \Omega^{j+1}(N))^{II},$$

so combined with the previous isomorphism,

$$\mathrm{Ext}^1_R(\Omega_{i+1}(M), \Omega^j(N))^I \cong \mathrm{Ext}^1_R(\Omega_i(M), \Omega^{j+1}(N))^I,$$

and inductively

$$\mathrm{Ext}^1_R(\Omega_{n-1}(M), \Omega^0(N))^I \cong \mathrm{Ext}^1_R(\Omega_0(M), \Omega^{n-1}(N))^I$$

for all n. Thus,

$$\mathrm{Ext}^n_R(M, N)^I \cong \mathrm{Ext}^1_R(\Omega_{n-1}(M), \Omega^0(N))^I \cong \mathrm{Ext}^1_R(\Omega_0(M), \Omega^{n-1}(N))^I$$
$$\cong \mathrm{Ext}^1_R(\Omega_0(M), \Omega^{n-1}(N))^{II} \cong \mathrm{Ext}^n_R(M, N)^{II}.$$

Thus, the isomorphism holds for all n. □

Index

$(-)^*$, 11
1_A, 2
$1_{\mathscr{C}}$, 11
A-algebra, 4
A-algebra homomorphism, 4
$A - \mathbf{Alg}$, 4
$A - \mathbf{cAlg}$, 4
B_i, 68
$F \implies G$, 12
G-equivariant map, 44
G-stable, 44
G^{ab}, 11
$K - \mathbf{Vect}$, 3
$K - \mathbf{vect}$, 3
$M \otimes_R -$, 30
$M_n(R)$, 14
R-balanced biadditive, 26
R-bilinear, 26
R-linear map, 3
R-multilinear, 35
$R - \mathbf{Comp}$, 67
$R - \mathbf{Mod}$, 3
R^n, 14
R^{op}, 14
$R^{\oplus\Gamma}$, 17
V^*, 11
Z_i, 68
$\mathrm{GL}_n(R)$, 44
$\mathrm{Hom}_R(-, M)$, 21
$\mathrm{Hom}_R(M, -)$, 20
Ob, 1
$\coprod_{\lambda\in\Lambda} X_\lambda$, 9
$\ell(M)$, 48
Ab, 2
Fld, 3
Grp, 2
$\mathbf{PO}(P)$, 4
Ring, 3
Set, 2
$\mathbf{Set}_*$, 4
Top, 3
cRing, 10
$\mathrm{Cont}(X, \mathbb{R})$, 11
$\mathrm{Hom}_R(M, N)$, 19
$\mathrm{Hom}_R(M, f)$, 20
$\mathrm{Hom}_R(f, M)$, 21
$\mathrm{Hom}_{\mathscr{C}}(A, B)$, 2
Res_ϕ, 35
$\mathscr{C} \times \mathscr{D}$, 5
$\mathscr{C}^{\mathrm{op}}$, 5
$\mathrm{End}_R(M)$, 15
$\mathrm{End}_{\mathbf{Ab}}(M)$, 15
$\mathrm{im}(\phi)$, 16
$\ker(\phi)$, 16
$\prod_{\lambda\in\Lambda} X_\lambda$, 9
${}_RM_S$, 16
e_λ, 17
$f \otimes g$, 30
$f \otimes g$, 30
f^*, 21
f_*, 20
$m \otimes n$, 27
(left) regular representation of G, 57

abelian category, 67
abelianization, 11
ACC, 50
acts linearly, 43
additive, 23
arrows, 2
Artinian, 50
ascending chain condition, 50

bimodule, 15
boundaries, 68

category, 1
category theoretic, 6
chain complex, 16, 65
cohmological indexing, 77
cokernel, 16, 67
commutative A-algebra, 4
commutative diagram, 5
complex, 16
composition, 2
composition series, 47
connecting homomorphism, 71
contravariant functor, 10
contravariant Hom functor, 21
coproduct, 7
covariant functor, 10
covariant Hom functor, 20
cycles, 68

DCC, 50
descending chain condition, 50
diagram, 5
differential, 65
direct sum, 67
divisible, 40
dual, 6

dual vector space, 11

epic, 6
epimorphism, 6
equivalent, 47
exact, 16, 24
extension, 17, 47
extension of scalars, 34

filtration, 47
finite length, 47
flat, 43
forgetful functor, 11
free basis, 17
free module, 17
free resolution, 76
full subcategory, 5

homological degree, 65
homology, 68

identity functor, 11
identity morphism, 2
initial, 6
injective, 39
injective resolution, 77
inverse, 6
isomorphism, 6

kernel, 67
Krull-Schmidt, 53

left R-module, 3
left Artinian, 51
left exact, 23, 24
left exact sequence, 16
left inverse, 6
left module homomorphism, 3
left Noetherian, 51
left semisimple, 55
length, 48

Maschke's Theorem, 56
monic, 6
monoid, 3
monomorphism, 6
morphisms, 2
multilinear, 35

natural isomorphism, 12
natural transformation, 12
Noetherian, 50

objects, 1
opposite category, 5
opposite ring, 14

pointed sets, 4
presentation, 17
product, 6
product category, 5
projective resolution, 76
pushout, 40

quasi-isomorphism, 70

relations, 17
representation, 43
restriction of scalars, 35
right exact, 23, 24
right exact sequence, 16
right inverse, 6
right module, 14
right semisimple, 55
ring, 3
ring homomorphism, 3

semigroup, 3
semigroup homomorphism, 3
semisimple, 53, 61
SES, 17
short exact sequence, 17, 67
sign representation, 44
simple, 46
simple tensors, 28
singular chain complex, 65
source, 2
split exact sequence, 18
standard basis, 17
strict, 47
subcategory, 5

target, 2
tensor product, 27
tensor product of maps, 30
terminal, 6
trivial representation, 44

vector spaces, 3