Math 901 Notes

Fall 2020

Contents

Pre-requisites

I am assuming knowledge of groups, rings, modules, and ideals at the level of a first year graduate course, e.g. UNL's Math 817–818.

Chapter 1

Rings, modules, and categories

August 17, 2020

1.1 Brief reminder of rings and modules

1.1.1 Rings

In Math 818 you have studied various special classes of commutative rings: PID's, Euclidean domains, UFD's. In this class a ring will mean a unital but *not necessarily commutative* ring. In Math 902 we will study unital commutative rings exclusively.

Definition 1.1. A *ring* is a set R with two binary operations $+$ and $\cdot$ such that

- $(R, +)$ is abelian group, with identity 0
- $(R, \cdot)$ is a (possibly non-commutative) monoid with identity 1,
- the left and right distributive laws hold: $(r+s)t = rt + st$ and $t(r+s) = tr + ts$.

Definition 1.2. A *ring homomorphism* or ring map $f : R \to S$ is a function satisfying

- $f(r_1 + r_2) = f(r_1) + f(r_2)$,
- $f(r_1 r_2) = f(r_1) f(r_2)$ and
- $f(1) = 1$.

Conventions: We stipulate that throughout the course

- all rings are unital and nontrivial, meaning that $0 \neq 1$.
- all ring homomorphisms $R \to S$ are assumed to map $1_R \mapsto 1_S$
- all ideals I are assumed to be strict subsets of R (R itself an improper ideal).

If R is a ring and I is a two-sided ideal I then R/I is also a ring under the induced operations called a *quotient ring.*

Example 1.3. For a field k, the map $\rho : k \to \mathcal{M}_2(k)$ sending x to $\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}$ preserves addition and multiplication, but fails to send 1 to $1 = I_2$, so this is not a ring homomorphism according to our definition.

You've seen many examples of commutative rings before: e.g., fields, $\mathbb{Z}$, $\mathbb{Z}/n$, polynomial rings, rings of algebraic integers (such as $\mathbb{Z}[\sqrt{-5}]$), etc. Here are some non-commutative examples:

Example 1.4. For any $n \geq 1$ and ring R, the set of $n \times n$ matrices with entries in R, $\mathcal{M}_n(R)$, is ring under the usual rules for matrix addition and multiplication. This makes sense even if R is non-commutative. The multiplicative identity is I_n. The ring $\mathcal{M}_n(R)$ is non-commutative if $n > 1$.

Example 1.5 (The ring of real quaternions)**.** Let $\mathbb{H}$ be the 4-dimensional $\mathbb{R}$-vector space with basis $1, i, j, k$; that is,

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

where multiplication is defined uniquely by the following rules: multiplication between elements of $\mathbb{R}$ and elements of $\mathbb{H}$ is the same as scalar multiplication on the vector space $\mathbb{H}$, $i^2 = j^2 = k^2 = ijk = -1$, and a strong form of the associative law is satisfied $(qv) \cdot w = q(v \cdot w) = v \cdot (qw)$ for all $v, w \in \mathbb{H}$ and $q \in \mathbb{R}$. Then $(\mathbb{H}, +, \cdot)$ is a non-commutative ring and, in fact, it is a *division ring*, meaning every non-zero element has a two-sided inverse (i.e., it satisfies the axioms of a field, except for commutativity).

It may not be clear that the rules above give a well-defined multiplication on $\mathbb{H}$, but one can see that they are consistent by looking at another way of describing $\mathbb{H}$, or rather a ring isomorphic to $\mathbb{H}$: it is the $\mathbb{R}$ subspace of $\mathcal{M}_2(\mathbb{C})$ spanned by I_2, $\sqrt{-1} \cdot I_2$, $\begin{bmatrix} 0 & -\sqrt{-1} \\ \sqrt{-1} & 0 \end{bmatrix}$, and $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ (representing 1, i, j, and k in the notation above). A tedious check shows that this subspace is indeed closed under matrix multiplication and hence forms a ring and that the matrices singled out satisfy the identities postulated for $\mathbb{H}$.

Definition 1.6. Given a ring R, let R^{op} refer to the same set, same rule for + but with multiplication defined by $x \cdot_{op} y := yx$. Then R^{op} is also a ring called the *opposite ring* of R. Note that $(R^{op})^{op} = R$.

Exercise 1.7. Prove that for any ring R and integer $n \geq 1$, there is a ring isomorphism

$$\mathcal{M}_n(R)^{op} \cong \mathcal{M}_n(R^{op}).$$

1.1.2 Modules

Definition 1.8. Given a ring R, a *left R-module* is an abelian group $(M, +)$ equipped with a pairing $R \times M \to M$, written $(r, m) \mapsto rm$, such that:

- $r_1(r_2m) = (r_1r_2)m$,
- $(r_1 + r_2)m = r_1m + r_2m$,
- $r(m_1 + m_2) = rm_1 + rm_2$, and
- $1m = m$.

A *right R-module* is defined analogously, starting with a pairing $M \times R \to M$ written as $(m, r) \mapsto mr$.

The default is that "module" means "left module".

A submodule of a module is a subset that contains 0 and is closed under + and scaling (on the left or on the right, as appropriate).

Remark 1.9. Every left R-module M is also a right R^{op}-module via $m \cdot r = r \cdot m$, and vice versa. When R is commutative, since $R = R^{op}$, every left R-module M is also a right R-module by the preceding reasoning. So for R commutative, we usually just say "module" to mean both the left and the right R-module structures.

Example 1.10. A left $\mathbb{Z}$-module M is the same thing as an abelian group. We can deduce this from the exercise above by recalling that for any ring A, there is a unique ring homomorphism $\mathbb{Z} \to A$. It follows that for any abelian group M there is a unique ring homomorphism $\mathbb{Z} \to \mathrm{End}_{Ab}(M)$ giving it a $\mathbb{Z}$-module structure.

Example 1.11. For a field k, a k-module is a k vector space. More generally, if D is a division ring (e.g., a field or the quaternions), then every left D-module has a basis and hence is isomorphic to a possibly infinite direct sum of copies of D regarded as a left module over itself. The proof of this fact is identical to the proof for fields. In other words, every left module over a division ring is a free module. Since D^{op} is also a division ring, every right D-module is free too.

Here is a partial converse:

Exercise 1.12. If $R \neq 0$ and every left R-module is free, then R is a division ring.

Tip: You might start by showing that if every non-zero element x of R has a left inverse, then every element has a two-side inverse. I.e., If for all $0 \neq x \in R$, there exists a $y \in R$ such that $yx = 1$, then for all $x \neq 0$, there is a y such that $xy = 1 = yx$.

The following exercise shows that a module structure on an abelian group can be thought of as a ring homomorphism. This point of view will prove fruitful later.

Exercise 1.13. Show that a giving a pairing as in the definition for left module above is equivalent to specifying a ring homomorphism $R \to \mathrm{End}_{Ab}(M)$. Similarly, giving a pairing as in the definition for right module above is equivalent to specifying a ring homomorphism $R^{op} \to \mathrm{End}_{Ab}(M)$. In particular, a right R-module is exactly the same thing as a left R^{op}-module.

Definition 1.14. An *R-module homomorphism*, also called an *R-map*, is a function between left (or right) R-modules that preserves $+$ and commutes with scaling, i.e, $f : M \to N$ is an R-module homomorphism if

- $f(m_1 + m_2) = f(m_1) + f(m_2)$ for all $m_1, m_2 \in M$
- $f(rm) = rf(m)$ for any $r \in R, m \in M$.

The set of all R-module homomorphisms between two R-modules M, N is denoted $\mathrm{Hom}_R(M, N)$. We see below that this set is in its turn an R^{op}-module. We denote $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$.

Proposition 1.15. [1] *If R is a ring and M, N are left R-modules then the set $\mathrm{Hom}_R(M, N)$ of R-module homomorphisms from M to N is an abelian group with the addition*

$$(f + g)(x) \quad = \quad f(x) + g(x) \qquad \textit{for } f, g \in \mathrm{Hom}_R(M, N).$$

If R is commutative, this group has a left R-module structure given by the scalar multiplication

$$(sf)(x) \quad = \quad sf(x) \qquad \textit{for } f \in \mathrm{Hom}_R(M, N), s \in R.$$

Proof. The fact that $\mathrm{Hom}_R(M, N)$ forms an abelian group with respect to addition of functions is easy to check.

Next I will check that the rule for sf gives an element of $\mathrm{Hom}_R(M, N)$. Indeed, sf preserves $+$

$$(sf)(x+y) = sf(x+y) = s(f(x)+f(y)) = sf(x)+sf(y) = (sf)(x)+(sf)Y(Y) \text{ for all } x, y \in M$$

and is R-linear

$$(sf)(rx) = sf(rx) = srf(x) = r(sf(x)) = (r(sf))(x).$$

Notice that the reasoning would not work if R were not commutative, hence in that case the rule for sf would not yield an R-module homomorphism.

One can easily check that distributivity and associativity hold for the two operations defined above. □

Exercise 1.16. 1. Show there is an isomorphism of abelian groups $\mathrm{Hom}_R(R, M) \cong M$ given by $f \mapsto f(1)$. If R is commutative, show it is an R-module isomorphism.

[1] This replaces an earlier erroneous statement about an R^{op} module structure on $\mathrm{Hom}_R(M, N)$.

2. Set $\mathrm{End}_R(R) = \mathrm{Hom}_R(R, R)$, where R is regarded as a left module over itself in the standard way. Prove that for any ring R, we have an isomorphism of rings $\mathrm{End}_R(R) \cong R^{op}$. More generally, show that there are ring isomorphisms

$$\mathrm{End}_R(R^n) \cong \mathcal{M}_n(R)^{op} \cong \mathcal{M}_n(R^{op}).$$

August 19, 2020

1.2 Categories and functors

1.2.1 Definition and first examples

The importance of category theory lies in the following:

- Category theory gives a unified treatment to similar notions or result when they apply to different classes of objects, for example, there is a first isomorphism theorem for groups, rings, modules, vector spaces.

- Often mathematical objects are defined by universal properties involving maps and diagrams. An example of this that should be familiar from Math 818 is the universal mapping property of a quotient group/ring/module. Category theory gives a unified framework for manipulating maps and diagrams and objects defined from such diagrams by universal mapping properties.

- Functors (which are maps between categories) are the principal way of relating an area of mathematics to another. For example, you may have learned in topology about the "fundamental group" $\pi_1(X)$ of a (pointed) topological space X. This gives in fact a map $\pi_1 : \langle\langle \text{Top*} \rangle\rangle \to \langle\langle \text{Groups} \rangle\rangle, X \mapsto \pi_1(X)$, which is an example of a functor, and a very neat way of relating topological spaces to groups.

Definition 1.17. A *category* $\mathcal{C}$ consists of the following data:

1. *Objects:* a class of *objects*, written $\mathfrak{ob}\mathcal{C}$;

2. *Morphisms:* for each pair of objects $X, Y \in \mathfrak{ob}\mathcal{C}$, there is a set, written $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ and referred to as the *set of morphisms from* X *to* Y;

3. *Compositions:* for each triple of objects $X, Y, Z \in \mathfrak{ob}\mathcal{C}$ a function

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z) \to \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

written as $(g, f) \mapsto f \circ g$ and referred to the *composition rule.*

This data is required to satisfy the following axioms:

1. if either $X \neq X'$ or $Y \neq Y'$, then $\mathrm{Hom}_{\mathcal{C}}(X, Y) \cap \mathrm{Hom}_{\mathcal{C}}(X', Y') = \emptyset$;

2. composition is associative: $(f \circ g) \circ h = f \circ (g \circ h)$ whenever $h \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, $g \in \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ and $f \in \mathrm{Hom}_{\mathcal{C}}(Z, Q)$ for some objects $X, Y, Z, Q \in \mathfrak{ob}\mathcal{C}$;
3. for each X there is an element $\mathrm{id}_X \in \mathrm{Hom}_{\mathcal{C}}(X, X)$, referred to as *the identity morphism* of X, such that $\mathrm{id}_X \circ g = g$ and $f \circ \mathrm{id}_X = f$ for all objects Y and Z and all morphisms $f \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ and all $g \in \mathrm{Hom}_{\mathcal{C}}(Z, X)$.

Remark 1.18. Some comments:

1. The objects of category form a "class" — in set theory a class is a collection that is in some sense "bigger" than a set, so that every set is a class by not vice versa, and that it is OK to talk about the "class of all sets" without running into paradoxes (the class of all sets is not a set).
2. It's easy to overlook the first axiom, but it is needed. Roughly, it says that the source and target of a morphism are part of the data determining it. In most examples it is obviously satisfied.
3. A standard argument shows that in a category $\mathcal{C}$, id_X is the only element of $\mathrm{Hom}_{\mathcal{C}}(X, X)$ that satisfies its defining property: If $e \in \mathrm{Hom}_{\mathcal{C}}(X, X)$ has the same two defining properties as id_X, then $\mathrm{id}_X = \mathrm{id}_X \circ e = e$. So, the existence of identity morphisms is part of the axioms, not part of the data defining a category.

Example 1.19. Some standard examples of categories:

- Let $\langle\langle\mathrm{Sets}\rangle\rangle$ denote the category of sets: its objects are sets, the set of morphisms between any two objects is the set of functions between these sets, and the composition rule is the usual rule for composing functions. Note that id_X is the identity function. Isomorphisms are bijections.
- Let $\langle\langle\mathrm{Rings}\rangle\rangle$ denote the category of rings. It's objects are (untial) rings and a morphisms are (unital) ring homomorphism.
- Let $\langle\langle\mathrm{Groups}\rangle\rangle$ denote the category of groups. A morphism is defined to be a group homomorphism.
- Let $\langle\langle\mathrm{Top}\rangle\rangle$ denote the category of topological spaces. Morphisms are continuous maps. Note that an isomorphism is called a homeomorphism for historical reasons. Important: Not every continuous bijection is a homeomorphism!
- For a fixed ring R, let $\langle\langle{}_R\mathrm{Mod}\rangle\rangle$ denote the category of left R-modules. Morphisms are defined to be left R-modules homomorphisms. A particular case is $R = \mathbb{Z}$, where $\langle\langle{}_{\mathbb{Z}}\mathrm{Mod}\rangle\rangle = \langle\langle\mathrm{Ab}\rangle\rangle$ is the category of Abelian groups.

In each of the above examples, the objects are sets equipped with extra structure (a group law, a topology, etc.), and the morphisms are functions that respect the structure in a suitable sense (respect the group law, are continuous, etc.). Let us refer to such a category as a "concrete category". (There is actually a rigorous definition of this term, which we will not discuss here.) Here is an example of a "non-concrete" category:

Example 1.20. Let $(P, \leq)$ be a quasi-poset. This means that $\leq$ satisfies the reflexive and transitive properties

$$a \leq b \text{ and } b \leq c \Rightarrow a \leq c$$

and

$$a \leq a.$$

A quasi-poset is a poset provided $\leq$ is also antisymmetric: $a \leq b$ and $b \leq a \Rightarrow a = b$.

We can regard a quasi-poset as forming a category $\mathbf{PO}(P)$ as follows:

Set $\mathfrak{ob}\mathbf{PO}(P) = P$. For any pair of objects $a, b \in P$, the set $\mathrm{Hom}_{\mathbf{PO}(P)}(a, b)$ is either a one-element set or empty, depending on whether $a \leq b$ or not. In order to give a name to the morphisms, let a form a distinct symbol $f_{a,b}$ for each pair of elements of $\mathcal{P}$ satisfying $a \leq b$. So

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

The rule for composition

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

is the only one possible: If both inputs are non-empty (i.e., if $a \leq b$ and $b \leq c$), then so is the target (by the first axiom of a quasi-poset), and we set

$$f_b^c \circ f_a^b := f_a^c.$$

The first axiom of a quasi-poset ensures that this is well-defined. If either input is empty, then so is the product, and there exists a unique function from the empty set to any other set.

Now let's check the axioms: suppose $\mathrm{Hom}_{\mathrm{PO}(P)}(a, b) \cap \mathrm{Hom}_{\mathrm{PO}(P)}(c, d) \neq \emptyset$, then $f_a^b = f_c^d$, but because we have chosen these symbols to be distinct we conclude that $a = c, b = d$.

Composition is associative for a formal reason: there is exactly one function between any two one-element sets.

The set $\mathrm{Hom}_{\mathbf{PO}(P)}(a, a)$ is non-empty (by the second axiom of a quasi-poset) and its unique element (namely, f_a^a) serves as the required two-sided identity.

Here is a sort of converse to the above example:

Exercise 1.21. Suppose $\mathcal{C}$ is a category with the properties that $\mathfrak{ob}\mathcal{C}$ is a set (as opposed to a proper class) and every Hom set has at most one element. Show that the rule

$$X \leq Y \iff \mathrm{Hom}_{\mathcal{C}}(X, Y) \neq \emptyset$$

makes $\mathfrak{ob}\mathcal{C}$ into a quasi-poset.

Example 1.22. Take $\mathcal{C}$ to be any non empty category and fix $A \in \mathfrak{ob}\mathcal{C}$. Define a new category $\mathcal{C}_A$ whose objects are certain morphisms in $\mathcal{C}$ and whose morphisms are certain diagrams of $\mathcal{C}$. In detail, set

$$\mathfrak{ob}\mathcal{C}_A = \{f : A \to Z \mid Z \in \mathcal{C}\} = \bigcup_{Z \in \mathcal{C}} \operatorname{Hom}_{\mathcal{C}}(A, Z)$$

$\operatorname{Hom}_{\mathcal{C}_A}(f, g) = \{$ commutative diagrams $\begin{tikzcd} & A \arrow[dl, "f"'] \arrow[dr, "g"] & \\ X \arrow[rr, "h"] & & Y \end{tikzcd}$ in $\mathcal{C}, i.e., h \circ f = g.\}$,

and define compositions by

$$\begin{tikzcd} & A \arrow[dl, "g"'] \arrow[dr, "\ell"] & \\ Y \arrow[rr, "j"] & & Z \end{tikzcd} \circ \begin{tikzcd} & A \arrow[dl, "f"'] \arrow[dr, "g"] & \\ X \arrow[rr, "h"] & & Y \end{tikzcd} = \begin{tikzcd} & A \arrow[dl, "f"'] \arrow[dr, "\ell"] & \\ X \arrow[rr, "j \circ h"] & & Z \end{tikzcd} .$$

Exercise 1.23. Show that the definitions above satisfy the axioms of a category.

August 21, 2020

1.2.2 Types of morphisms

Some more terminology and notation that illustrates how category theory is the science of arrows and diagrams:

Definition 1.24. A *diagram* in a category $\mathcal{C}$ is a directed multigraph whose vertices are objects in $\mathcal{C}$ and whose arrows are morphisms in $\mathcal{C}$. A *commutative diagram* in $\mathcal{C}$ is a diagram in which for each pair of vertices A and B, any two paths from A to B are equal; that is, the composites are the same morphism.

Example 1.25. If G is a group, $a, b \in G$ and $\mu_a, \mu_b \in \operatorname{Hom}_{\langle\langle \text{Groups} \rangle\rangle}(G, G)$ are the homomorphism given by left multiplication by a, b respectively, then the diagram below commutes if and only if $ab = ba$:

$$\begin{tikzcd} G \arrow[r, "\mu_a"] \arrow[d, "\mu_b"] & G \arrow[d, "\mu_b"] \\ G \arrow[r, "\mu_a"] & G \end{tikzcd}$$

Definition 1.26. A morphism $f : X \to Y$ in a category $\mathcal{C}$ is called an *isomorphism* provided there exists a morphism $g : Y \to X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$.

A morphism $f : X \to Y$ in a category $\mathcal{C}$ is called a *monomorphism* provided that for any $Z \in \mathfrak{ob}\mathcal{C}$ and any morphisms $\alpha, \beta : Z \to X$ such that $f \circ \alpha = f \circ \beta$ one has $\alpha = \beta$.

A morphism $f : X \to Y$ in a category $\mathcal{C}$ is called an *epimorphism* provided there for any $Z \in \mathfrak{ob}\mathcal{C}$ and any morphisms $\alpha, \beta : Y \to Z$ such that $\alpha \circ f = \beta \circ f$ one has $\alpha = \beta$.

Remark 1.27. For each category $\mathcal{C}$ there is an opposite category $\mathcal{C}^{op}$ for which

- $\mathfrak{ob}\mathcal{C}^{op} = \mathfrak{ob}\mathcal{C}$ and
- $Hom_{\mathcal{C}^{op}}(X,Y) = \mathrm{Hom}_{\mathcal{C}}(Y,X)$, that is, for each morphism $f : X \to Y$ in $\mathcal{C}$ there is a morphism $f^{op} : Y \to X$ in $\mathcal{C}^{op}$.

Intuitively, $\mathcal{C}^{op}$ is the category obtained from $\mathcal{C}$ by reversion all the arrows. We now see that f is a monomorphism in $\mathcal{C}$ if and only if f^{op} is an epimorphism in $\mathcal{C}^{op}$. Thus we say that monomorphism and epimorphism are dual notions (obtained by reversing arrows). The importance of this fact is that whenever we have a theorem about monomorphisms it can be translated into a dual theorem about epimorphisms in the opposite category.

Example 1.28.

- The identity morphism is always an isomorphism.
- The isomorphisms in $\langle\langle\mathrm{Sets}\rangle\rangle$ are all the bijections.
- P is a poset iff the only isomorphisms in $\mathrm{PO}(P)$ are the identity homomorphisms.

Remark 1.29. The usual argument shows that if f is an isomorphism, then there is only one g satisifying these conditions and hence we write this g asf^{-1}. Namely, say $f \circ h = \mathrm{id}_Y$ and $h \circ f = \mathrm{id}_X$ also hold. Then

$$h = h \circ \mathrm{id}_Y = h \circ (f \circ g) = (h \circ f) \circ g = \mathrm{id}_X \circ g = g.$$

Example 1.30.

- In $\langle\langle\mathrm{Sets}\rangle\rangle$ the monomorphisms are the injections and the epimorphisms are the surjections.
- All morphisms in $\mathrm{PO}(P)$ are both monomorphisms and epimorphismsm.

Remark 1.31. In $\langle\langle\mathrm{Sets}\rangle\rangle$ it is true that a morphims f is an isomorphism iff it is both a monomorphim and an epimorphism. This is no longer true in other categories: for example if P is a poset, in $\mathrm{PO}(P)$ all morphisms are both mono- and epi- but only the identity morphisms are iso-.

Exercise 1.32. What are the monomorphisms and epimorphisms in $\langle\langle\mathrm{Rings}\rangle\rangle$? Is it true in $\langle\langle\mathrm{Rings}\rangle\rangle$ that f is an isomorphism if and only if it is both a monomorphism and an epimorphism?

Definition 1.33. For a category $\mathcal{C}$ and $X \in \mathfrak{ob}\mathcal{C}$, we write $\mathrm{End}_{\mathcal{C}}(X)$ for $\mathrm{Hom}_{\mathcal{C}}(X,X)$. The elements of this set are called *endomorphisms* of X. Endomorphisms that are isomorphisms are called *automorphisms*, and the set of all automorphisms of a given object X is written $\mathrm{Aut}_{\mathcal{C}}(X)$.

Remark 1.34. For any object X of a category $\mathcal{C}$, the axioms of a category imply that $\mathrm{End}_{\mathcal{C}}(X)$ is a monoid (aka, a semigroup that has an identity element) under the composition law $f \circ g$. The set $\mathrm{Aut}_{\mathcal{C}}(X)$ is the subset of units of this monoid and it forms a group under composition.

In fact all monoids can be recovered as the endomorphisms of some category:

Exercise 1.35. Show that there is a bijection between categories with exactly one object and monoids (semigroups with identity).

1.2.3 Universal properties, product, coproduct

Many of the concepts introduced in Math 817/818 have an explicit description and an accompanying description in terms of a universal property (e.g. the universal property for quotient groups/rings/vector spaces will be recalled below). The explicit description may be very useful in concrete computations, but as a rule it is the universal property that clarifies the true nature of the construction and may be more useful in abstract arguments.

Also, deeper relationships become apparent when the constructions are viewed in terms of their universal properties. For example, we will see that cartesian products of sets and disjoint unions of sets are really dual constructions (in the sense that reversing arrows transforms the universal property for one into that for the other.

Definition 1.36. A *terminal object* in a category $\mathcal{C}$ is an object T such that for every object F of $\mathcal{C}$, the set $\mathrm{Hom}_{\mathcal{C}}(F, T)$ has precisely one element.

An *initial object* of $\mathcal{C}$ is an object I of $\mathcal{C}$ such that the set $\mathrm{Hom}_{\mathcal{C}}(I, Y)$ has exactly one element for all objects Y.

Example 1.37.

- Does $\langle\langle \text{Ab} \rangle\rangle$ have a initial/terminal object? Yes, it's the 0 abelian group.
- How about $\langle\langle \text{Sets} \rangle\rangle$? The final object is a singleton set and the initial object is the empty set.
- How about $\langle\langle \text{Rings} \rangle\rangle$? The final object is the 0 ring and $\mathbb{Z}$ is the initial object.

Initial and final objects in categories are unique in a strong sense:

Exercise 1.38. Show that in any category any two initial objects are isomorphic through a unique isomorphism and any two final objects are isomorphic through a unique isomorphism.

A property or construction is *category-theoretic* if it can be defined or described using nothing other than the structure of the category to which the object belongs.

We say that a construction satisfies a *universal property* when it may be viewed as an initial or terminal object of a category. Since being initial/final amounts to the existence and uniqueness of certain morphisms, the explanation of a universal property may follow the pattern, "object X is universal with respect to the following property: for any Y such that..., there exists a unique morphism $Y \to X$ (or $X \to Y$) such that...."

We now give several examples of category-theoretic universal constructions.

Quotient

Let $\sim$ be an equivalence relation defined on a set A and let

$$\pi : A \to A/\sim$$

be the quotient map $a \mapsto \overline{a}$, where $\overline{a} = \{b \in A \mid b \sim a\}$ is the coset of a with respect to $\sim$.

Lemma 1.39. *The pair $(A/\sim, \pi)$ is universal with respect to the property of mapping A to a set in such a way that equivalent elements have the same image. That is, if $f : A \to X$ is a function such that $a \sim a' \Rightarrow f(a) = f(a')$, then there is a unique function $h : A/\sim \to X$ that makes the following diagram commute:*

$$\begin{tikzcd}
& A \arrow[dl, "\pi"'] \arrow[dr, "f"] & \\
A/\sim \arrow[rr, "h"] & & X
\end{tikzcd}$$

Proof. We will show that π is the initial object of the full subcategory of $\langle\langle \text{Sets} \rangle\rangle_A$ from Example 1.22 whose objects are functions $f : A \to X$ in $\mathcal{C}$ such that $a \sim a' \Rightarrow f(a) = f(a')$ and whose morphisms are the same as in $\langle\langle \text{Sets} \rangle\rangle_A$.

Consider $f : A \to X$ a morphism in $\mathcal{C}$. Then $\text{Hom}_{\mathcal{C}_A}(\pi, f)$ consists of commutative diagrams

$$\begin{tikzcd}
& A \arrow[dl, "\pi"'] \arrow[dr, "f"] & \\
A/\sim \arrow[rr, "h"] & & X.
\end{tikzcd}$$

Note that π is initial iff each $f \in \text{Hom}_{\mathcal{C}}(A, X)$ determines a unique such diagram, i.e there is a unique $h \in \text{Hom}_{\mathcal{C}}(A/\sim, X)$ such that $h \circ \pi = f$. Uniqueness follows because this identity allows us to write down the rule for h explicitly

$$h(\overline{a}) = f(a).$$

It remains to show that h is well defined. Notice that this follows from

$$a \sim a' \Rightarrow f(a) = f(a') \Rightarrow h(\overline{a}) = h(\overline{a'})$$

by the restriction imposed on objects in our category. □

August 24, 2020

Product and coproduct

Definition 1.40. In a category $\mathcal{C}$, given a family of objects $\{X_i\}_{i \in I}$, a *product* of the family is given by an object P and a family of morphisms $\{g_i : P \to X_i\}_{i \in I}$ that is universal in the following sense:

Given an object Y and a family of morphisms $\{f_i : Y \to X_i\}_{i \in I}$, there exists a unique morphism $\alpha : Y \to P$ such that $g_i \circ \alpha = f_i$ for all i.

Here is a schematic representation for this definition in the case when $I = \mathbb{N}$ is countably infinite.

$$\begin{tikzcd}
 & X_1 & \\
 & X_2 & \\
P \arrow[uur, "g_1"] \arrow[ur, "g_2"'] \arrow[dr, "g_n"] \arrow[ddr] & & Y \arrow[uul, "f_1"'] \arrow[ul, "f_2"] \arrow[ll, dashed, red, "\exists!\ \alpha"] \arrow[dl, "f_n"'] \arrow[ddl] \\
 & X_n & \\
 & \vdots &
\end{tikzcd}$$

Remark 1.41. $(P, \{g_i : P \to X_i\})$ is the product of the family in the definition if and only if the function

$$\mathrm{Hom}_{\mathcal{C}}(Y, P) \to \prod_i \mathrm{Hom}_{\mathcal{C}}(Y, X_i), \qquad \alpha \mapsto \{g_i \circ \alpha\}_{i \in I}$$

is a bijection of sets, where the notation $\prod$ in the codomain refers to the cartesian product of sets.

Definition 1.42. A *coproduct* of family of objects $\{X_i\}_{i \in I}$ is given by an object C and a family of morphisms $g_i : X_i \to C$ that is universal in the sense that given an object Y and morphisms $f_i : X_i \to Y$ for each i, there exists a unique morphism $\alpha : C \to Y$ such that $\alpha \circ g_i = f_i$ for all i.

Here is the diagram representation of the definition of coproduct. Note that all arrows are reversed with respect to the previous diagram, thus product and coproduct are dual notions.

$$\begin{tikzcd}
 & X_1 \arrow[ddl, "g_1"'] \arrow[ddr, "f_1"] & \\
 & X_2 \arrow[dl, "g_2"] \arrow[dr, "f_2"'] & \\
C \arrow[rr, dashed, red, "\exists!\ \alpha"] & & Y \\
 & X_n \arrow[ul, "g_n"'] \arrow[ur, "f_n"] & \\
 & \vdots \arrow[uul] \arrow[uur] &
\end{tikzcd}$$

Remark 1.43. $(C, \{g_i : X_i \to C\})$ is a coproduct of the family in the definition above if and only if the function

$$\mathrm{Hom}_{\mathcal{C}}(C, Y) \xrightarrow{\cong} \prod_i \mathrm{Hom}_{\mathcal{C}}(X_i, Y) \qquad \alpha \mapsto \{g_i \circ \alpha\}_{i\in I}$$

is a bijection of sets, where again $\prod$ denotes cartesian product of sets.

Example 1.44. In any category $\mathcal{C}$, for any object X, the product of the one-element family $\{X\}$ consisting of just X is $P = X$ itself along with the identity map $P \xrightarrow{\mathrm{id}} X$. Likewise, the coproduct of $\{X\}$ is $C = X$ with the map $X \xrightarrow{\mathrm{id}} C$.

Example 1.45. In $\langle\langle\text{Sets}\rangle\rangle$, the product of any collection of sets exists and is given by $(\prod_{i\in I} X_i, \pi_i)$ the cartesian product along with the projection maps π_i from a cartesian product of sets onto each of the factors.

The coproduct is given by $(\coprod_{i\in I} X_i, \iota_i)$, where $\coprod_{i\in I} X_i$ is the disjoint union of sets and $\iota_i : X_i \to \coprod_{i\in I} X_i$ is the inclusion map. By disjoint union we mean the ordinary union if the collection happens to be pairwise disjoint, but otherwise one must first replace each set by a bijective copy of it to make them pairwise disjoint, and then form the ordinary union.

There is no guarantee that a product or coproduct of a given family of objects exists. But when one does exist, it is unique up to unique isomorphism:

Proposition 1.46. *If $(P, \{g_i : P \to X_i\}_{i\in I})$ and $(P', \{g'_i : P' \to X_i\}_{i\in I})$ are both products for the same family $\{X_i\}_{i\in I}$ of objects in some category $\mathcal{C}$, then there is a unique isomorphism $\alpha : P \xrightarrow{\cong} P'$ such that $g'_i \circ \alpha = g_i$ for all i. The analogous statement holds for coproducts.*

Proof. We'll just prove the statement concerning products. Using that $(P, \{g_i\})$ is a product and letting $(P', \{g'_i\})$ play the role of the "test" object in the definition of a product, we obtain a unique morphism $\alpha : P \xrightarrow{\cong} P'$ such that $g'_i \circ \alpha = g_i$ for all i. We need to show α is an isomorphism.

Interchanging the roles, we also have a unique map $\beta : P' \xrightarrow{\cong} P$ such that $g_i \circ \beta = g'_i$ for all i. Consider the composition $\beta \circ \alpha : P \to P$. It satisfies $g_i \circ (\beta \circ \alpha) = g_i$ for all i. But the identify map $\mathrm{id}_P : P \xrightarrow{=} P$ also satisfies $g_i \circ \mathrm{id}_P = g_i$ for all i, and so the uniqueness part of the definition of product implies that $\beta \circ \alpha = \mathrm{id}_P$. A similar argument shows that $\alpha \circ \beta = \mathrm{id}_{P'}$. So, α is an isomorphism. □

Exercise 1.47. Prove the analogue for coproducts.

Example 1.48. The following table summarizes the structure of products and coproducts in various caregories

Category	Product	Coproduct
$\langle\langle$Sets$\rangle\rangle$	cartesian product	disjoint union
$\langle\langle$Groups$\rangle\rangle$	cartesian product	free product (we won't discuss this notion)
$\langle\langle$Rings$\rangle\rangle$	cartesian product	none
$\langle\langle$Comm Rings$\rangle\rangle$	cartesian product	tensor product (we will define this soon)
$\langle\langle {}_R$Mod$\rangle\rangle$	cartesian product	direct sum

Remark 1.49. In $\langle\langle$Rings$\rangle\rangle$, the product of a family of rings is the cartesian product, which is a ring with the component-wise rules for addition and multiplication.

However there is no coproduct in this category. Here is a failed attempt at finding a coproduct. If R and S are ring, a reasonable guess for a potential coproduct would be that $C = R \times S$, with component-wise rules for addition and multiplication, along with the inclusion maps $i : R \to C, j : S \to C$ defined by $i(r) = (r, 0)$ and $j(s) = (0, s)$. This is not in fact a coproduct since i, j are not ring homomorphismsm since they don't send 1 to 1 (if R and S are non-zero rings).

As we will see, in the subcategory $\langle\langle$CommRings$\rangle\rangle$ of commutative rings the coproduct of a pair of commutative rings exists, and it is given by the "tensor product" construction.

Some terminology:

Definition 1.50. Given a category $\mathcal{C}$ and and subclass S of $\mathfrak{ob}\mathcal{C}$, the *full subcategory on* S is the category $\mathcal{D}$ with $\mathfrak{ob}\mathcal{D} = S$ and for any $X, Y \in S$, $\mathrm{Hom}_{\mathcal{D}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y)$.

For example, $\langle\langle$Comm Rings$\rangle\rangle$ is the full-subcategory of $\langle\langle$Rings$\rangle\rangle$ consisting of the commutative rings, and $\langle\langle$Ab$\rangle\rangle$ is the full subcategory of $\langle\langle$Groups$\rangle\rangle$ consisting of groups that are abelian.

Remark 1.51. Beware that the product and coproduct of a family can change when you pass from a full subcategory to a larger category. Given two non-zero abelian groups A and B, their coproduct in $\langle\langle$Ab$\rangle\rangle$ differs from their coproduct in $\langle\langle$Groups$\rangle\rangle$. You'll encounter this in the homework.

For a ring R, the category $\langle\langle {}_R$Mod$\rangle\rangle$ has arbitrary products and coproducts.

Proposition 1.52 (Products and Coproducts in $\langle\langle {}_R$Mod$\rangle\rangle$)**.** *Let R be a ring, N a left R-module and $\{M_i\}_{i\in I}$ a collection of left R-modules.*

1. *A product for the family $\{M_i\}_{i\in I}$ is $(P = \prod_{i\in I} M_i, \pi_i)$, where P is the cartesian product of the M_i which is a left R-module with the componentwise addition and scalar multiplication and the map π_i is the projections from the cartesian product onto the i-th factor.*

   Equivalently, the function

   $$\beta : \mathrm{Hom}_R(N, \prod_{i\in I} M_i) \to \prod_{i\in I} \mathrm{Hom}_R(N, M_i) \quad \beta(G) = (\pi_i \circ G)_{i\in I}$$

   is a bijection and in fact an isomorphism of abelian group for arbitrary R and of R-modules if R is commutative.

2. A coproduct for the family $\{M_i\}_{i\in I}$ is given by (C, ι_i) where C is the direct sum

$$C = \bigoplus_{i\in I} X_i = \{(x_i)_{i\in I} \mid x_i \neq 0 \textit{ for only finitely many } i\}$$

and $\iota_i : M_i \to C$ is the inclusion that takes $m \in M_i$ to the sequence with m in the i-th coordinate and 0 elsewhere.

Equivalently, the function

$$\alpha : \operatorname{Hom}_R(\bigoplus_{i\in I} M_i, N) \to \prod_{i\in I} \operatorname{Hom}_R(M_i, N) \quad \alpha(F) = (F \circ \iota_i)_{i\in I}$$

is a bijection and in fact an isomorphism of abelian groups for R arbitrary and of R-modules if R is commutative.

Remark 1.53. If the index set I is finite then $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$, so $P = C$, but the product and coproduct constructions are still different because the maps they involve are projections on one hand and inclusions on the other. If the index set I is infinite then $\bigoplus_{i\in I} X_i$ is a proper submodule of $\prod_{i\in I} X_i$.

Note also that α would not be well-defined if we replaced $\bigoplus_I M_i$ with $\prod_I M_i$, and β would not be well-defined if we replaced $\prod_I M_i$ with $\bigoplus_I M_i$.

Proof. (1) One needs to show that (P, π_i) satisfies the universal mapping property of the product: given R-maps $g_i : N \to M_i$ for each i, there is a unique R-map $G : N \to \prod_i M_i$ such that $\pi_j \circ G = g_j$ for all j. Indeed, the condition that $\pi_j \circ G = g_j$ yields that such a map must be given by

$$G(n) = (g_i(n))_{i\in I}.$$

In order for this map to verify the definition of product, one needs to check that G is an R-module homomorphism. This follows because each of the g_i are R-module homomorphisms.

As for the fact that β as defined above is a bijection, this follows by the existence and uniqueness of G, given a tuple of morphisms $(g_i)_{i\in I} \in \prod_{i\in I} \operatorname{Hom}_R(N, M_i)$. Both the domain and codomain of β are abelian groups and left R-modules if R is commutative by Proposition 1.72. Now we check that β is an group homomorphism:

$$\beta(G + H) = (\pi_i \circ (G + H))_{i\in I} = (\pi_i \circ G)_{i\in I} + (\pi_i \circ H)_{i\in I}$$

because π_i are group homomorphisms and

$$\beta(sG) = (\pi_i \circ (sG))_{i\in I} = (s(\pi_i \circ G))_{i\in I} = s(\pi_i \circ G)_{i\in I} \text{ for } s \in R$$

where the second equality follows from

$$(\pi_i \circ (sG))(n) = \pi_i\left((sg_j(n))_{j\in I}\right) = sg_i(n) = s(\pi_i \circ G)(n).$$

(2) One needs to show that (C, ι_i) satisfies the universal mapping property of the coproduct: Given an R-map $f_i : M_i \to N$ for each i, there exists a unique R-map $F : \bigoplus_{i \in I} M_i \to N$ such that for each j the composition $M_j \xrightarrow{\iota_j} \bigoplus_{i \in I} M_i \xrightarrow{F} N$ is f_j.

We show that this map can be define by

$$F((m_i)_{i \in I}) = \sum_{i \in I} f_i(m_i).$$

Note that this definition makes sense since $(m_i)_{i \in I}$ is an element of the direct sum C and thus there are only a finite number of nonzero summands in the summation displayed above, so we are dealing with a finite sum, which is well defined in a group.

One needs to check that F is indeed an R-module homomorphism, which I leave as an exercise. The uniqueness of F holds since $\bigoplus_{i \in I} M_i$ is generated by the subset $\cup_i \iota_i(M_i)$. The map α is the inverse of the map sending $(f_i)_{i \in I}$ to F, hence a bijection. I will leave the check that α is a morphism of abelian groups and if R is commutative of R-modules as an exercise. □

The important takeaway that one should remember from the previous proposition is that there are abelian groups and if R is commutative R-module homomorphisms between the following Hom sets.

$$\mathrm{Hom}_R(\bigoplus_{i \in I} M_i, N) \cong \prod_{i \in I} \mathrm{Hom}_R(M_i, N) \tag{1.2.1}$$

$$\mathrm{Hom}_R(N, \prod_{i \in I} M_i) \cong \prod_{i \in I} \mathrm{Hom}_R(N, M_i) \tag{1.2.2}$$

In other words, Hom takes direct sum in the source and direct product in the target to direct products of hom sets.

Exercise 1.54. Let $(P, \leq)$ be a quasi-poset, regarded as a category as described above. Under what conditions do products/coproducts exist for a pair of objects in this category? Describe them in terms of the order relation.

August 26, 2020

1.2.4 Functors

One can think of functors as homomorphisms of categories.

Definition 1.55. Given two categories $\mathcal{C}$ and $\mathcal{D}$, a *covariant functor*, sometimes called just a *functor*, from $\mathcal{C}$ to $\mathcal{D}$, written as

$$F : \mathcal{C} \to \mathcal{D}$$

consists of the following data:

1. a function $F : \mathfrak{ob}\mathcal{C} \to \mathfrak{ob}\mathcal{D}$ of classes (yes this makes sense, or so I am told) and
2. for each pair of objects $X, Y \in \mathfrak{ob}\mathcal{C}$, a function of sets
$$F_(X, Y) : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y)).$$

This data must satisfy

1. for all $X \in \mathfrak{ob}\mathcal{C}$, we have $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ and
2. $F(f \circ g) = F(f) \circ F(g)$, whenever $f \circ g$ is defined.

Remark 1.56. It *is* necessary to include the axiom $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$.

Remark 1.57. A functor takes commutative diagrams to commutative diagrams.

Remark 1.58. The composition of functors is a functor: If $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{E}$ are functors, then we may define $G \circ F : \mathcal{C} \to \mathcal{D}$ on objects by $(F \circ G)(X) = F(G(X))$ and on morphisms by composing
$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \xrightarrow{F} \mathrm{Hom}_{\mathcal{D}}(F(X), F(Y)) \xrightarrow{G} \mathrm{Hom}_{\mathcal{E}}(G(F(X)), G(F(Y))).$$

The axioms are not hard to check.

Definition 1.59. Given two categories $\mathcal{C}$ and $\mathcal{D}$, a *contravariant functor* from $\mathcal{C}$ to $\mathcal{D}$ consists of the following data:

1. a function $F : \mathfrak{ob}\mathcal{C} \to \mathfrak{ob}\mathcal{D}$ of classes and
2. for each pair of objects $X, Y \in \mathfrak{ob}\mathcal{C}$, a function $F : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{\mathcal{D}}(F(Y), F(X))$ of sets. (Note the order is backwards from the definition of a covariant functor.)

This data must satisfy

1. for all $X \in \mathfrak{ob}\mathcal{C}$, we have $F(\mathrm{id}_X) = \mathrm{id}_{F(X)}$ and
2. $F(f \circ g) = F(g) \circ F(f)$, whenever $f \circ g$ is defined. (Again, note that this is backwards.)

Remark 1.60. A contravariant functor also takes commutative diagrams to commutative diagrams, but reverses all the arrows.

Example 1.61. For any $\mathcal{C}$ we have the evident identity functor.

More generally, if $\mathcal{D}$ is a full subcategory of $\mathcal{C}$, then we have an inclusion functor $\mathcal{D} \hookrightarrow \mathcal{C}$.

Example 1.62. There are "forgetful" functors from $\langle\langle$Groups$\rangle\rangle$ to $\langle\langle$Sets$\rangle\rangle$, from $\langle\langle$Rings$\rangle\rangle$ to $\langle\langle$Sets$\rangle\rangle$, from $\langle\langle$Top$\rangle\rangle$ to $\langle\langle$Sets$\rangle\rangle$, etc. The first sends a group to its underlying set (i.e., forget the group operation) and a homomorphism to the underlying function. And similarly for the other examples.

Note that none of these categories are full subcategories of $\langle\langle$Sets$\rangle\rangle$.

Example 1.63. Fix a positive integer n and define a functor $F : \langle\langle \text{Rings} \rangle\rangle \to \langle\langle \text{Rings} \rangle\rangle$ on objects by

$$F(R) = \mathcal{M}_n(R)$$

and given an ring homomorphism $f : R \to R'$ we define

$$F(f) : \mathcal{M}_n(R) \to \mathcal{M}_n(R').$$

to be map given by applying f to each entry of an $n \times n$ matrix.

The case $n = 1$ is (very nearly) the identity functor.

Example 1.64. The assignment of a (unital) ring R to its groups of units $R^\times$ determines a functor

$$F : \langle\langle \text{Rings} \rangle\rangle \to \langle\langle \text{Groups} \rangle\rangle\,, \qquad F(R) = R^\times, \quad F(f) = f|_{R^\times}.$$

The required rule for morphisms sends a ring homomorphism $f : R \to S$ to its restriction to $R^\times$, which does indeed land in $S^\times$ and gives a group homomorphism. The two axioms for being a functor are easy to check.

Example 1.65. For a group G, let G' denote its derived subgroup

$$G' = \{aba^{-1}b^{-1} \mid a, b \in G\} \text{ and let } G^{ab} = G/G.'$$

This construction gives a functor

$$F : \langle\langle \text{Groups} \rangle\rangle \to \langle\langle \text{Ab} \rangle\rangle \qquad F(G) = G^{ab}.$$

If $f : G \to H$ is a homomorphism of groups, then $f(G') \subseteq H'$ and hence by the universal mapping property of the quotient f induces a map $\overline{f} : G^{ab} \to H^{ab}$. We define $F(f) = \overline{f}$ to be this induced map. The axioms of a functor are easy to check.

Exercise 1.66. Recall that a quasi-poset $(P, \leq)$ may be interpreted as a very special kind of category. If $(P', \leq)$ is another poset, also interpreted as a category, show that a covariant functor from $(P, \leq)$ to $(P', \leq)$ is the same thing as an order preserving function.

Definition 1.67. An *additive category* is a category $\mathcal{A}$ such that:

1. each Hom set $\text{Hom}_{\mathcal{A}}(X, Y)$ is endowed with the extra structure of an abelian group (usually written with additive notation)

2. for all objects the composition pairing

$$\text{Hom}_{\mathcal{A}}(X, Y) \times \text{Hom}_{\mathcal{A}}(Y, Z) \to \text{Hom}_{\mathcal{A}}(X, Z)$$

is a group homomorphism; that is, we have

$$(f + g) \circ h = f \circ h + g \circ h \text{ and } f' \circ (g' + h') = f' \circ g' + f' \circ h',$$

for all morphisms f, g, h, f', g', h' such that the compositions are defined.

3. $\mathcal{C}$ has a "zero object", written 0, that is both terminal and initial.

4. Every pair of objects X, Y has a product denoted $X \oplus Y$.

Example 1.68. The following are examples of additive categories

1. $\langle\langle$Ab$\rangle\rangle$ with 0 being the trivial group

2. $\langle\langle {}_R$Mod$\rangle\rangle$ for any ring R, with 0 being the 0 module

3. Any full subcategory of an additive category that contains the 0 object and is closed under finite products. For example, for a ring R, the category of all finitely generated left R-modules is additive.

Remark 1.69. Notice that the second axiom of an additive category implies that the endomorphism sets $\mathrm{End}_{\mathbb{A}}(X)$ are in fact rings with respect to $+$ and $\circ$.

August 28, 2020

Definition 1.70. Given two additive categories $\mathcal{A}, \mathcal{B}$ a functor $F : \mathcal{A} \to \mathcal{B}$ is called an *additive functor* if for all objects $X, Y \in \mathfrak{ob}\mathcal{A}$, the function

$$F_{X,Y} : \mathrm{Hom}_{\mathcal{A}}(X, Y) \to \mathrm{Hom}_{\mathcal{B}}(F(X), F(Y))$$

is a homomorphism of abelian groups.

A contravariant functor between additive categories is *additive* if

$$F_{X,Y} : \mathrm{Hom}_{\mathcal{A}}(X, Y) \to \mathrm{Hom}_{\mathcal{B}}(F(Y), F(X))$$

is a homomorphism of abelian groups for all X, Y.

Exercise 1.71. Prove that if F is an additive functor then $F(X \oplus Y) \cong F(X) \oplus F(Y)$ and $F(0) \cong 0$.

Module structure on $\mathrm{Hom}_R(M, N)$

For left R-modules M, N the set $\mathrm{Hom}_R(M, N)$ is an abelian group and it is furthermore an R-module if R is commutative.

Proposition 1.72. *If R is a ring and M, N are left R-modules then the set $\mathrm{Hom}_R(M, N)$ of R-module homomorphisms from M to N is an abelian group with the addition*

$$(f + g)(x) \quad = \quad f(x) + g(x) \qquad \text{for } f, g \in \mathrm{Hom}_R(M, N).$$

If R is commutative, this group has a left R-module structure given by the scalar multiplication

$$(sf)(x) \quad = \quad sf(x) \qquad \text{for } f \in \mathrm{Hom}_R(M, N), s \in R.$$

Proof. The fact that $\operatorname{Hom}_R(M,N)$ forms an abelian group with respect to addition of functions is easy to check. Next I will check that the rule for sf gives an element of $\operatorname{Hom}_R(M,N)$. Indeed, sf preserves $+$

$$(sf)(x+y) = sf(x+y) = s(f(x)+f(y)) = sf(x)+sf(y) = (sf)(x)+(sf)Y(Y) \text{ for } x,y \in M$$

and is R-linear

$$(sf)(rx) = sf(rx) = srf(x) = r(sf(x)) = (r(sf))\,(x) \text{ for } x \in M.$$

Notice that the reasoning would not work if R were not commutative, hence in that case the rule for sf would not yield an R-module homomorphism.

One can easily check that distributivity and associativity hold for the two operations defined above. □

Remark 1.73. If R, S are rings we say that M is an $R-S$-bimodule if M is a left R module and a right S module and these two structures satisfy the following associative property $(rm)s = r(ms)$. For example R is an $R-R$ bimodule with respect to the internal multiplication. Any left R-module M is also a right R^{op} module but this *does not necessarily make Minto an $R-R^{op}$ bimodule* since the two multiplications need not satisfy the property $(rm)s = r(ms)$.

If R, S are rings, M is an $R-S$-bimodule and N is a left R-module then $\operatorname{Hom}_R(M,N)$ has a left S-module structure with scalar multiplication given by $(sf)(x) = f(xs)$.

If R, S are rings, M is a left R-module and N is an $R-S$-bimodule then $\operatorname{Hom}_R(M,N)$ has a right S-module structure with scalar multiplication given by $(fs)(x) = f(x)s$.

Example 1.74. We can see that for any abelian group A, $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, A) \cong A$ by checking that $f \mapsto f(1)$ is an isomorphism. In particular, $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}) = \operatorname{End}_{\mathbb{Z}}(\mathbb{Z}) \cong \mathbb{Z}$ and $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}/n)$.

Next we compute $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m,\mathbb{Z}/n)$. Similar to above, any element f of this set is completely determined by $f(\overline{1})$. Now we know that $m\overline{1} = \overline{0}$ in $\mathbb{Z}/m$, hence $mf(\overline{1}) = f(m\overline{1}) = f(\overline{0}) = \overline{0}$ in $\mathbb{Z}/n$. Thus

$$\begin{aligned}
\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/m,\mathbb{Z}/n) &\cong \{\overline{t} \in \mathbb{Z}/n \mid m\overline{t} = \overline{0}\} \\
&= \{\overline{t} \in \mathbb{Z}/n \mid n \mid mt\} = \{\overline{t} \in \mathbb{Z}/n \mid \frac{n}{\gcd(m,n)} \mid t\} \\
&= \langle \frac{n}{\gcd(m,n)} \rangle \mathbb{Z}/n \cong \mathbb{Z}/\gcd(m,n),
\end{aligned}$$

where the last isomorphism is due to the fact that any cyclic group with d elements is isomorphic to $\mathbb{Z}/d$ (here $d = \gcd(m,n)$.)

Note that we can use equations (1.2.1) to extend this to Hom between any two finitely generated $\mathbb{Z}$-modules, for example

$$\begin{gathered}
\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z} \oplus \mathbb{Z}/2, \mathbb{Z}/3 \oplus \mathbb{Z}/4) \\
\cong \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Z}/3) \oplus \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2,\mathbb{Z}/3) \oplus \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}\,\mathbb{Z}/4) \oplus \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/2,\mathbb{Z}/4) \\
\cong \mathbb{Z}/3 \oplus 0 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/2.
\end{gathered}$$

We will use this to build two functors: one which is covariant $\mathrm{Hom}(M, -)$ and one which is contravariant $\mathrm{Hom}_R(-, N)$.

The covariant Hom functor

The following additive functor will be very important to us:

Proposition 1.75. *Fix a ring R and a left R-module M. We define a functor*

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

as follows:

- *on objects, for any N, let $\mathrm{Hom}_R(M, N)$ be the set of R-module homomorphisms regarded as a abelian group as usual.*
- *given a morphism $g : N \to N'$ of left R-modules, let $\mathrm{Hom}_R(M, g)$ to be left composition by g (sometimes written as g_*), i.e.*

$$\mathrm{Hom}_R(M, g) : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'), \quad \mathrm{Hom}_R(M, g)(\alpha) = g \circ \alpha.$$

The rules above give rise to an additive covariant functor.

When R is commutative, this rule can be viewed as an additive functor

$$\mathrm{Hom}_R(M, -) : \langle\langle {}_R Mod \rangle\rangle \to \langle\langle {}_R Mod \rangle\rangle .$$

Proof. We check the requirements in Definition 1.55:

1. $\mathrm{Hom}_R(M, \mathrm{id}_X)(\alpha) = \mathrm{id}_X \circ \alpha = \alpha$ whenever the composition is defined, thus $\mathrm{Hom}_R(M, \mathrm{id}_X)(\alpha)$ is the identity map on $\mathrm{Hom}_R(M, X)$.
2. $\mathrm{Hom}_R(M, f \circ g)(\alpha) = (f \circ g) \circ \alpha = f \circ (g \circ \alpha) = \mathrm{Hom}_R(M, f)(g \circ \alpha)$
$= \mathrm{Hom}_R(M, f)(\mathrm{Hom}_R(M, g)(\alpha)) = (\mathrm{Hom}_R(M, f) \circ \mathrm{Hom}_R(M, g))(\alpha)$

Furthermore $\mathrm{Hom}_R(M, g)$ is indeed a morphism of abelian groups since

$$\mathrm{Hom}_R(M, g)(\alpha + \beta) = g \circ (\alpha + \beta) = g \circ \alpha + g \circ \beta = \mathrm{Hom}_R(M, g)(\alpha) + \mathrm{Hom}_R(M, g)(\beta).$$

If R is commutative, we have a left R-module structure on $\mathrm{Hom}(M, N)$ as in Proposition 1.72 and we can make the functor discussed above into a functor

$$\mathrm{Hom}_R(M, -) : \langle\langle {}_R \mathrm{Mod} \rangle\rangle \to \langle\langle {}_R \mathrm{Mod} \rangle\rangle .$$

The only issue is whether $\mathrm{Hom}_R(M, g)$ is an R-module map. This is true since

$\mathrm{Hom}_R(M, g)(s\alpha) = g \circ (s\alpha) = g(s\alpha) = s(g \circ \alpha) = s\, \mathrm{Hom}_R(M, g)(\alpha)$ by the R-linearity of g.

□

August 31, 2020

Example 1.76. Let's study the functor $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, -)$. We have that for any $\mathbb{Z}$-module M, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \cong N$ via the map $f \mapsto f(1)$. Moreover for a $\mathbb{Z}$-module map $g : N \to N'$ I claim that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, g) : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, N')$ is "the same" as $g : N \to N'$. More specifically, the following diagram commutes

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \arrow[r, "\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},g)"] \arrow[d, "\cong"] & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, N') \arrow[d, "\cong"] \\
N \arrow[r, "g"] & N'.
\end{tikzcd}$$

We say in this situation that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, -)$ is naturally isomorphic to the identity functor on $\langle\langle {}_{\mathbb{Z}}\mathrm{Mod}\rangle\rangle$. A formal definition for this notion will be given later.

Now let's study the functor $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/2)$. Let's consider the quotient homomorphism

$$\pi : \mathbb{Z} \to \mathbb{Z}/2, \pi(x) = \overline{x}.$$

Then $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \pi) : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}/2)$ fits in the commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/2) \arrow[r, "\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2,\pi)"] \arrow[d, "\cong"] & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}/2) \arrow[d, "\cong"] \\
0 \arrow[r] & \mathbb{Z}/2.
\end{tikzcd}$$

This shows that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \pi)$ is the map that sends every element of its domain to $0 \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}/2)$. Note that in this example the functor $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, -)$ sends a surjective morphism (epimorphism) to a non surjective morphism.

The contravariant Hom functor

So far all the examples of functors that we have seen have been covariant. The following is an example of a contravariant functor:

Proposition 1.77. *Fix a ring R and a left R-module N. We define a functor*

$$\mathrm{Hom}_R(-, N) : \langle\langle {}_R Mod\rangle\rangle \to \langle\langle Ab\rangle\rangle$$

as follows:

- *on objects, for any M, let $\mathrm{Hom}_R(M, N)$ be the set of R-module homomorphisms regarded as a abelian group as usual.*
- *given a morphism $g : M \to M'$ of left R-modules, let $\mathrm{Hom}_R(g, N)$ to be right composition by g (sometimes written as g^*), i.e. the map*

$$\mathrm{Hom}_R(g, N) : \mathrm{Hom}_R(M', N) \to \mathrm{Hom}_R(M, N) \quad \mathrm{Hom}_R(g, N)(\alpha) = \alpha \circ g.$$

Then this rule defines an additive contravariant functor.

Moreover, if R is commutative, we may interpret $\operatorname{Hom}_R(-,N)$ *as a contravariant functor from* $\langle\langle_R Mod\rangle\rangle$ *to itself.*

Proof. Note that $\operatorname{Hom}_R(g,N)$ does indeed map $\operatorname{Hom}_R(M',N)$ to $\operatorname{Hom}_R(M,N)$: Given $\alpha \in \operatorname{Hom}_R(M',N)$, the function $\operatorname{Hom}_R(g,N)(\alpha) = \alpha \circ g$ is an R-module homomorphism since it is a composition of two such maps.

The two axioms for being a contra-variant functor are easy to check:

1. We have $\operatorname{Hom}_R(\mathrm{id}_M, N) = \mathrm{id}_{\operatorname{Hom}_R(M,N)}$ since $\operatorname{Hom}_R(\mathrm{id}_M, N)(\alpha) = \alpha \circ \mathrm{id}_M = \alpha$ for all $\alpha \in \operatorname{Hom}_R(M,N)$ and
2. $\operatorname{Hom}_R(g \circ f, N) = \operatorname{Hom}_R(f,N) \circ \operatorname{Hom}_R(g,N)$ for all composable g, f since

$$\operatorname{Hom}_R(g \circ f, N)(\alpha) = \alpha \circ (g \circ f) = (\alpha \circ g) \circ f = \operatorname{Hom}_R(f, \operatorname{Hom}_R(g,N)).$$

Furthermore $\operatorname{Hom}_R(g,N)$ is indeed a morphism of abelian groups since

$$\operatorname{Hom}_R(g,N)(\alpha+\beta) = (\alpha+\beta) \circ g = \alpha \circ g + \beta \circ g = \operatorname{Hom}_R(g,N)(\alpha) + \operatorname{Hom}_R(g,N)(\beta).$$

If R is commutative then $\operatorname{Hom}_R(g,N)$ is an R-module map since

$$\operatorname{Hom}_R(g,N)(s\alpha) = (s\alpha) \circ g = s\operatorname{Hom}_R(M,g)(\alpha).$$

□

Example 1.78. Let's compute $\operatorname{Hom}_{\mathbb{Z}}(\mu_d, \mathbb{Z}/d) : \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/d) \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/d)$, where $\mu_d : \mathbb{Z} \to \mathbb{Z}$ is the map $\mu_d(x) = dx$. We can write a commutative diagram

$$\begin{tikzcd}
\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/d) \arrow[r, "\operatorname{Hom}_{\mathbb{Z}}(\mu_d, \mathbb{Z}/d)"] \arrow[d, "\cong"] & \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/d) \arrow[d, "\cong"] \\
\mathbb{Z}/d \arrow[r, "0"] & \mathbb{Z}/d.
\end{tikzcd}$$

where the vertical maps send $f \mapsto f(1)$ by setting the bottom horizontal map to be the induced map $\overline{\mu_d} : \mathbb{Z}/d \to \mathbb{Z}/d$ which maps $\overline{\mu_d}(\overline{x}) = \overline{dx} = \overline{0}$, i.e the zero map. This shows that the contravariant Hom can take monomorphsms (injective homomorphisms) to maps that are not monomorphisms nor epimorphisms.

Example 1.79. A special case of the above occurs when $R = k$ is a field and $N = k$. Then $\operatorname{Hom}_k(-,k)$ is the functor sending a k-vector space V to its dual $V^* := \operatorname{Hom}_k(V,k)$, that is the vector space of linear functionals on V. Note that if V is finite dimensional, then V^* has the same dimension as V and hence V and V^* are isomorphic. But, there is no "natural" isomorphism from V to V^*. More on that later.

1.2.5 Natural Transformations

Definition 1.80. Given two categories $\mathcal{C}$ and $\mathcal{D}$ and two functors $F, G : \mathcal{C} \to \mathcal{D}$ between them, a *natural transformation* from F to G, sometimes written as

$$\eta : F \Rightarrow G,$$

consists of the following data:

> For each $X \in \mathfrak{ob}\mathcal{C}$ a morphism
>
> $$\eta_X : F(X) \to G(X)$$
>
> in $\mathcal{D}$ (i.e., $\eta_X \in \mathrm{Hom}_{\mathcal{D}}(F(X), G(X))$).

This data are required to satisfy the following condition:

> For all $X, Y \in \mathfrak{ob}\mathcal{C}$ and all $f : X \to Y$, we have
>
> $$\begin{cases} \eta_Y \circ F(f) = G(f) \circ \eta_X & \text{if } F \text{ is covariant} \\ \eta_X \circ F(f) = G(f) \circ \eta_Y & \text{if } F \text{ is contravariant} \end{cases}$$
>
> i.e the applicable diagram commutes
>
> $$\begin{tikzcd} F(X) \arrow[r, "F(f)"] \arrow[d, "\eta_X"] & F(Y) \arrow[d, "\eta_Y"] \\ G(X) \arrow[r, "G(f)"] & G(Y) \end{tikzcd}$$
>
> or
>
> $$\begin{tikzcd} F(X) \arrow[d, "\eta_X"] & F(Y) \arrow[l, "F(f)"'] \arrow[d, "\eta_Y"] \\ G(X) & G(Y). \arrow[l, "G(f)"] \end{tikzcd}$$

A natural transformation η of functors is called a *natural isomorphism* if η_X is an isomorphism for all objects X.

Example 1.81. We have seen in Example 1.76 that there is a natural isomorphism of functors between the identity functor on $\langle\langle \mathrm{Ab} \rangle\rangle$ and the functor $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, -)$.

Example 1.82. Fix a field k and let $\langle\langle \mathrm{Vect}_k \rangle\rangle$ be the category of k-vector spaces and $D : \langle\langle \mathrm{Vect}_k \rangle\rangle \to \langle\langle \mathrm{Vect}_k \rangle\rangle$ be the functor $\mathrm{Hom}_k(-, k)$. Then there is a natural transformation

$$\eta : \mathrm{id}_{\langle\langle \mathrm{Vect}_k \rangle\rangle} \Rightarrow D \circ D$$

given by the collection of k-vector space maps

$$\eta_V : V \to D(D(V))$$

defined as follows:

> For $v \in V$, let $\eta_V(v) : \mathrm{Hom}_k(\mathrm{Hom}_k(V, k), k))$ be "evaluation at v": for $\gamma \in \mathrm{Hom}_k(V, k)$, we have $\eta_V(v)(\gamma) = \gamma(v)$.

Since the dual of a finite dimensional vector space is again finite dimensional, D retricts to an endo-functor on the category $\left\langle\left\langle \mathrm{Vect}_k^{fd} \right\rangle\right\rangle$ of finite dimensional vector spaces. On the homework you will prove that this restriction is a natural isomorphism. (You should also check it is a natural transformation carefully.)

Definition 1.83. An *equivalence* between two categories $\mathcal{C}$ and $\mathcal{D}$ consists of a pair of functors

$$F : \mathcal{C} \to \mathcal{D} \text{ and } G : \mathcal{D} \to \mathcal{C}$$

and a pair of natural isomorphisms $\eta : \mathrm{id}_{\mathcal{C}} \Rightarrow G \circ F$ and $\eta' : \mathrm{id}_{\mathcal{D}} \Rightarrow F \circ G$.

Remark 1.84. Equivalence of categories really is an equivalence relation, but I won't prove that.

Example 1.85 (Concrete linear algebra is equivalent to abstract linear algebra)**.** For each natural number n, the categories $\mathcal{M}_n(k)$ of and $\langle\langle \mathrm{Vect}_k^n \rangle\rangle$ of n-dimensional k-vector spaces are equivalent.

Example 1.86. In operator algebras, the category of commutative, unital C^*-algebras is equivalent to the opposite of the category of compact Hausdorff spaces.

September 2, 2020

1.3 Projective and injective modules

1.3.1 Exact sequences and exact functors

Definition 1.87. 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* if $d_i \circ d_{i+1} = 0$ for all i or, equivalently, $\mathrm{Im}(d_{i+1}) \subseteq \mathrm{Ker}(d_i)$ for all i.

A chain complex is an *exact sequence* if $\mathrm{Im}(d_{i+1}) = \mathrm{Ker}(d_i)$ for all i.

Remark 1.88. A sequence of the form $M \xrightarrow{g} N \to 0$ is exact if and only if g is surjective, and a sequence of the form $0 \to M \xrightarrow{f} N$ is exact iff f is injective.

Definition 1.89. 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 $M' \cong \mathrm{Im}(i) = \mathrm{Ker}(g)$.

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 $\operatorname{Im}(f) = \operatorname{Ker}(p)$, so, $M'' \cong M/\operatorname{Ker}(p) = M/\operatorname{Im}(f)$. 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* 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 $M' \cong \operatorname{Ker}(p)$ and $M \cong \operatorname{coker}(i)$. We also say that M is an "extension" of M' and M'' if it fits in a short exact sequence as above.

Given modules M' and M'', we have the "trivial" s.e.s.

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

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

Theorem 1.90 (The splitting theorem)**.** *Given a s.e.s. of left R-modules*

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

TFAE:

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

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "i"] \arrow[d, "id"] & M \arrow[r, "p"] \arrow[d, "\theta"] & M'' \arrow[r] \arrow[d, "id"] & 0 \\
0 \arrow[r] & M' \arrow[r, "\iota"] & M' \oplus M'' \arrow[r, "\pi"] & M'' \arrow[r] & 0.
\end{tikzcd}$$

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

3. *There is a map $q : M \to M'$ such that $q \circ i = id_{M'}$ (we say i is a "split injection" in this case).*

4. *There is a map $j : M'' \to M$ such that $p \circ j = id_{M''}$ (we say p is a "split surjection" in this case).*

5. *There are maps $q : M \to M'$ and $j : M'' \to M$ such that $q \circ i = id_{M'}$, $p \circ j = id_{M''}$, and $i \circ q + j \circ p = id_M$.*

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

Proof. (1) ⇔ (2) follows by definition of commutative diagram.

(1) ⇒ (5): The main idea is that there are obvious splitting maps for the bottom s.e.s. 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 $i \circ \pi' + \iota'' \circ p = \mathrm{id}_{M' \oplus M''}$.

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

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

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

(5) ⇒ (3, 4) is clear.

(3) ⇒ (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 h is bijective, so it is an isomorphism.

The proof that (4) ⇒ (2) is similar, and omitted. □

September 4, 2020

Example 1.91. Suppose $R = k$ is a field. Then every short exact sequence of R-modules splits. We could verify any of the four equivalent conditions directly; I'll do (3). Given a surjection $p : V \twoheadrightarrow V''$ of k-vector spaces, pick a basis B of V''. For each $w \in B$ pick any element $\tilde{w}$ of V such that $p(\tilde{w}) = w$. The function $w \mapsto \tilde{w}$ from B to V extends uniquely to a k-linear map $j : V'' \to V$ such that $j(w) = \tilde{w}$ for all $w \in B$. The composition $p \circ j$ is the identity on V'' since it is the identity on the basis B by construction.

Remark 1.92. The proof in the previous example actually shows that, for any ring R, a s.e.s. whose right-most term is free is split exact.

Example 1.93. 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.

Exact functors

Definition 1.94. For any rings R and S, a covariant additive functor $F : \langle\langle_R\text{Mod}\rangle\rangle \to \langle\langle_S\text{Mod}\rangle\rangle$ (or "right" modules) is called *right exact* if whenever

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

is exact, then so is

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

(Recall $F(0) = 0$ since F is additive.)

F is *left exact* if whenever

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

is exact, then so is

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

We say F is *exact* if it is additive and both left and right exact.

Remark 1.95. An exact functor takes any s.e.s. to a s.e.s.

Remark 1.96. A contravariant functor $F : \mathcal{C} \to \mathcal{D}$ is the same as a covariant functor $F : \mathcal{C}^{op} \to D$. Applying the definitions above to the latter yields corresponding definitions for exactness of contravariant functors.

Definition 1.97. For any rings R and S, a contravariant additive functor $F : \langle\langle_R\text{Mod}\rangle\rangle \to \langle\langle_S\text{Mod}\rangle\rangle$ (or "right" modules) is called *right exact* if whenever

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

is exact, then so is

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

(Recall $F(0) = 0$ since F is additive.)

F is *left exact* if whenever

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

is exact, then so is

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

We say F is *exact* if it is additive and both left and right exact.

Proposition 1.98. *If R is commutative and M, N are R-modules the covariant and contravariant* Hom *functors* $\mathrm{Hom}_R(M, -) : \langle\langle {}_R\mathit{Mod} \rangle\rangle \to \langle\langle {}_R\mathit{Mod} \rangle\rangle$ *and* $\mathrm{Hom}_R(-, N) : \langle\langle {}_R\mathit{Mod} \rangle\rangle \to \langle\langle {}_R\mathit{Mod} \rangle\rangle$ *are left exact.*

More generally, if R, S are rings and M, N are $R - S$ bimodules, the functors $\mathrm{Hom}_R(M, -) : \langle\langle {}_R\mathit{Mod} \rangle\rangle \to \langle\langle {}_S\mathit{Mod} \rangle\rangle$ *and* $\mathrm{Hom}_R(-, N) : \langle\langle {}_R\mathit{Mod} \rangle\rangle \to \langle\langle \mathit{Mod}_S \rangle\rangle$ *(where $\langle\langle \mathit{Mod}_S \rangle\rangle$ means right S modules) are left exact.*

Proof. Homework. □

Remark 1.99. Examples 1.76 and 1.78 show that these functors are in general *not* right exact and hence not exact.

1.3.2 Projective modules

We now examine the question: for which R-modules P is the functor $\mathrm{Hom}_R(P, -)$ exact? This really is asking when $\mathrm{Hom}_R(P, -)$ is right exact because we know that this functor is always left exact.

So the question is: given a surjective map of R-modules $p : N \twoheadrightarrow N''$ when is the map

$$\mathrm{Hom}_R(P, p) : \mathrm{Hom}_R(P, N) \to \mathrm{Hom}_R(P, N'')$$

onto? It is onto iff given $f : M \to N''$, there is a $g : M \to N$ such that $p \circ g = f$. This motivates:

Definition 1.100. 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

$$\begin{tikzcd}
& P \arrow[dl, dashed, "\exists g"'] \arrow[d, "f"] & \\
N \arrow[r, "p"] & N'' \arrow[r] & 0
\end{tikzcd}$$

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

Proposition 1.101. *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. □

Remark 1.102. Examples 1.107, 1.108 show that the converse is not true: there exist projective modules which are not free.

Example 1.103. The module $\mathbb{Z}/n$ for $n \geq 2$ is not a projective $\mathbb{Z}$-module. Consider the diagram as in the definition in which $P = \mathbb{Z}/n$, $N = \mathbb{Z}$, $N' = \mathbb{Z}/n$, p is the canonical surjection, and f is the identity map. The only R-map from $\mathbb{Z}/n$ to $\mathbb{Z}$ is the zero map and so no such g exists as in the definition.

Definition 1.104. An R-module F is free if it is isomorphic to a (finite or infinite) direct sum of copies of R, i.e., $F \cong \bigoplus_{i \in I} R$. A module F is free if and only if it has a basis, i.e. a generating set that is also R-linearly independent.

Proposition 1.105. *For a ring R and module P, the following are equivalent:*

1. *P is projective,*

2. *the functor $\mathrm{Hom}_R(P, -)$ (from R-modules to abelian groups) 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 $p : N \twoheadrightarrow P$ is split surjective, 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 (justify this as an exercise!). The definition of "projective" is just a long-winded version 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 1.90. Note that given an onto map $p : N \twoheadrightarrow P$, we may form the short exact sequence $0 \to \mathrm{Ker}(p) \to N \xrightarrow{p} P \to 0$.

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

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 $P \oplus \mathrm{Ker}(p) \cong F$, 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 1.106. 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.

September 7, 2020

Example 1.107. Let

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

the ring of polynomial functions defined on the circle, and let P be the ideal $(x, 1-y)$. We show that P is projective as an R-module but not free.

To see that P is projective, one notices that that the map

$$q : R^2 \xrightarrow{(x,1-y)} P$$

is a split surjection, with splitting $j : P \to R^2$ given by

$$j(r) = \left(\frac{(1+y)r}{2x}, \frac{r}{2}\right)^T$$

since

$$(q \circ j)(r) = x\frac{(1+y)r}{2x} + (1-y)\frac{r}{2} = \frac{(1+y)r}{2} + \frac{(1-y)r}{2} = r.$$

The only issue remaining is the well-definedness of the map j, specifically whether dividing by x makes sense. In fact since $r \in P = (x, 1-y)$ we have $r = \alpha x + \beta(1-y)$ so $(1+y)r = \alpha x(1+y) + \beta(1-y^2) = ax(1+y) + \beta x^2 = x(\alpha(1+y) + \beta x)$ and we see that it make sense to write $(1+y)r/2x = (\alpha(1+y) + \beta x)/2 \in R$.

To see that P is not free, first notice (or take as an exercise) that an ideal of a commutative ring R is free as an R-module if and only if it is principal. Now see that P is not principal because if $P = (r)$ then $x = \alpha r$ and $1 - y = \beta r$, so $x^2 + y^2 - 1 = (\alpha x - \beta(1+y))r$ in $\mathbb{R}[x, y]$, which can only occur if one of the factors is a unit, since $x^2 + y^2 - 1$ is irreducible e.g by Eisenstein's criterion. Either way, we obtain $P = R$, which is a contradiction.

P is an algebraic version of the Möbius strip.

Example 1.108. 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 $j(r) = (xr, yr, zr)^T$. 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.

The following technical result is sometimes useful:

Lemma 1.109. *Let R be a ring and $\{M_i\}_{i\in I}$ a family of R-modules. The coproduct (direct sum) $\bigoplus_{i\in I} M_i$ of this family is projective if and only if each M_i is projective.*

Proof. There is a natural isomorphism (i.e. a natural transformation η of functors such that η_X is an isomorphism for all X)

$$\operatorname{Hom}_R(\bigoplus_{i\in I} M_i, -) \overset{\cong}{\Longrightarrow} \prod_{i\in I} \operatorname{Hom}_R(M_i, -).$$

Here "natural" means that if $g : N \to N'$ is and R-module homomorphism then there is a commutative diagram

$$\begin{tikzcd}
\operatorname{Hom}_R(\bigoplus_{i\in I} M_i, N) \arrow[r, "\operatorname{Hom}_R(\bigoplus_{i\in I} M_i, g)"] \arrow[d, "\cong"] & \operatorname{Hom}_R(\bigoplus_{i\in I} M_i, N') \arrow[d, "\cong"] \\
\prod_{i\in I} \operatorname{Hom}_R(M_i, N) \arrow[r, "\prod_{i\in I} \operatorname{Hom}_R(M_i, g)"] & \prod_{i\in I} \operatorname{Hom}_R(M_i, N')
\end{tikzcd}$$

from which we see that the top map is surjective if and only if the bottom map is surjective if and only if each $\operatorname{Hom}_R(M_i, g)$ is surjective. □

1.3.3 Injective modules

Injective is the dual notion for projective.

Definition 1.110. An R-module E is *injective* if given solid arrows as in the diagram

$$\begin{tikzcd}
0 \arrow[r] & N' \arrow[r, "i"] \arrow[d, "f"] & N \arrow[dl, dashed, "\exists g"] \\
& E &
\end{tikzcd}$$

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

Exercise 1.111. Show that if V is a k-vector space then V is injective as a k-module. However, this does not generalize to free R-modules. For example, show that $\mathbb{Z}$ is not an injective $\mathbb{Z}$-module.

Proposition 1.112. *The following are equivalent for an R-module E:*

1. *E is injective,*

2. *the functor $\operatorname{Hom}_R(-, E)$ (from R-modules to abelian groups) 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 $j : E \hookrightarrow M$ is split.*

September 9, 2020

In the proof we'll use the following notion

Definition 1.113. A *pushout* of a diagram

$$\begin{tikzcd}
A \arrow[r, "i"] \arrow[d, "j"] & B \\
C &
\end{tikzcd}$$

in a category $\mathcal{C}$ is a triple (D, f, g) so that the diagram below commutes

$$\begin{tikzcd}
A \arrow[r, "i"] \arrow[d, "j"] & B \arrow[d, "f"] \\
C \arrow[r, "g"] & D
\end{tikzcd}$$

and satisfies the following universal property: for any other commutative diagram as above with D replaced by Y there is a unique dotted map that makes the big diagram below commute

$$\begin{tikzcd}
A \arrow[r, "i"] \arrow[d, "j"] & B \arrow[d, "f"'] \arrow[ddr, "f'"] & \\
C \arrow[r, "g"] \arrow[drr, "g'"'] & D \arrow[dr, dashed] & \\
& & Y.
\end{tikzcd}$$

Exercise 1.114. Show that in the category $\langle\langle {}_R\mathrm{Mod} \rangle\rangle$ the pushout exists and is given (in the notation of Definition 1.113) as an object by

$$D = \frac{B \bigoplus C}{\{(i(a), -j(a)) \mid a \in A\}}$$

with maps f, g given by the inclusions of the two summands into $B \oplus C$ followed by the quotient map $B \oplus C \to D$.

Proof of Proposition 1.112. 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 $\mathrm{Hom}_R(i, E) : \mathrm{Hom}_R(N, E) \to \mathrm{Hom}_R(N', E)$ (exercise!). Likewise, the equivalence of (3) and (4) follows from the Splitting Theorem 1.90.

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

$$\begin{tikzcd}
0 \arrow[r] & E \arrow[r, "j"] \arrow[d, "\mathrm{id}_E"] & M \arrow[dl, dashed, "\exists q"] \\
& E &
\end{tikzcd}$$

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 pushout module

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

(I leave it to you to check that the denominator is a submodule of $E \oplus N$.) 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 pushout diagram below commutes

$$\begin{tikzcd}
N' \arrow[r, "i"] \arrow[d, "f"] & N \arrow[d, "h"] \\
E \arrow[r, "j"] & M
\end{tikzcd}$$

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 one-to-one and hence $a = 0$.

By assumption (i.e. statement (4)), there is a map $q : M \twoheadrightarrow E$ such that $q \circ j = \mathrm{id}_M$. 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. □

Lemma 1.115. *An arbitrary product of injective modules is injective.*

Proof. This holds since there is a natural isomorphism

$$\mathrm{Hom}_R(-, \prod_i E_i) \overset{\cong}{\Longrightarrow} \prod_i \mathrm{Hom}_R(-, E_i)$$

and a product of functors is exact if and only if each of them is. □

Example 1.116. Suppose R is an integral domain and E is an injective R-module. I claim E must have the following property: for all $x \in E$ and $0 \neq r \in R$, there is an element $y \in E$ such that $ry = x$ i.e., every element of E can be divided by every non-zero element of R'. To see this, just apply the definition to the diagram

$$\begin{tikzcd}
0 \arrow[r] & R \arrow[r, "r"] \arrow[d, "x"] & R \arrow[dl, dashed, "\exists g"] \\
& E &
\end{tikzcd}$$

We give this necessary condition a suggestive name – "divisible".

Definition 1.117. An R-module E is called *divisible* if it satisfies for all $x \in E$ and $0 \neq r \in R$, there is an element $y \in E$ such that $ry = x$.

Theorem 1.118 (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*

$$\begin{tikzcd}
0 \arrow[r] & J \arrow[r, "\iota"] \arrow[d, "f"] & R \arrow[dl, dashed, "\exists g"] \\
 & E &
\end{tikzcd}$$

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

$$\begin{tikzcd}
0 \arrow[r] & N' \arrow[r, "i"] \arrow[d, "f"] & N \arrow[dl, dashed, "\exists g"] \\
 & E &
\end{tikzcd}$$

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 $(M_1, h_1) \leq (M_2, h_2)$ 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 $(M, h) \geq (M_i, h_i)$ for all i.

By Zorn's Lemma, $\mathcal{S}$ has a maximal element (M, h). It suffices to prove $M = N$. If not pick $x \in N \setminus M$ 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

$$\begin{tikzcd}
I \arrow[r, "\subseteq"] \arrow[d, "x"] & R \arrow[d, "x"] \\
M \arrow[r, "\subseteq"] & T
\end{tikzcd}$$

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

$$\begin{tikzcd}
I \arrow[r, "\subseteq"] \arrow[d, "x"] & R \arrow[d, "x"] \arrow[ddr, "\beta"] & \\
M \arrow[r, "\subseteq"] \arrow[drr, "h"'] & T \arrow[dr, dashed] & \\
 & & E
\end{tikzcd}$$

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. More concretely, 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. □

September 11, 2020

Corollary 1.119. *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

$$\begin{tikzcd}
0 \arrow[r] & (r) \arrow[r, "\iota"] \arrow[d, "f"] & R \arrow[dl, dashed, "\exists g"] \\
 & E &
\end{tikzcd}$$

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

1.4 Tensor product

1.4.1 Tensor product as an abelian group

Definition 1.121. 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-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 $r \in R$.

Example 1.122. Examples of bilinear maps include

- $f : R \times R \to R, f(r,s) = rs$
- for an R-module M, $f : R^2 \times M \to M^2, f((r,s), m) = (rm, sm)$
- for a right ideal I and a left module M, $f : (R/I) \times M \to M/IM, f(\overline{r}, m) = \overline{rm}$

We now define tensor products using a universal property.

Definition 1.123. 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-biadditive map $h : M \times N \to M \otimes_R N$ is called the tensor product of M and N if it has the following universal property: for any abelian group A and R-biadditive map $f : M \times N \to A$, there exists a unique group homomorphism $g : M \otimes_R N \to A$ such that $f = g \circ h$.

$$\begin{tikzcd}
M \times N \arrow[r, "f"] \arrow[d, "h"] & A \\
M \otimes_R N \arrow[ur, dashed, "\exists! g"'] &
\end{tikzcd}$$

Remark 1.124. The tensor product of M and N is unique up to isomorphism. (This justifies the slightly abusive language "the" tensor product instead of "a" tensor product in the definition above.)

Theorem 1.125. *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*.*

Remark 1.126. It is important to note that while expressions of the form $m \otimes n$, called simple tensors, are elements of $M \otimes_R N$, not every element of $M \otimes_R N$ has this form. Instead, every element of $M \otimes_R N$ is a finite sum of simple tensors

$$m_1 \otimes n_1 + m_2 \otimes n_2 + \cdots + m_k \otimes n_k.$$

Proof of Theorem 1.125. It is immediate from the construction that h is R-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. □

Exercise 1.127. In $M \otimes_R N$ we have $0_M \otimes n = 0_{M\otimes_R N} = m \otimes 0_N$ for each $m \in M, n \in N$.

September 14, 2020

Example 1.128. I claim $\mathbb{Z}/m \otimes_{\mathbb{Z}} \mathbb{Z}/n \cong \mathbb{Z}/g$ where $g = gcd(m,n)$.

Proof. Define a function

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

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

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

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

Now define a homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/m \otimes_{\mathbb{Z}} \mathbb{Z}/n$ 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

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

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 $\mathbb{Z}/m \times \mathbb{Z}/n$ 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 $\beta \circ \alpha = \mathrm{id}$. □

1.4.2 Tensor product as a module

We have not required in Definition 1.123 that $M \otimes_R N$ be a module. Indeed, this is not always the case but we will see below that is is an R-module if R is commutative. First we give a more general statement.

Proposition 1.129. *If R, S is are rings M is an $S - R$ bimodule and N is a left R-module, then:*

0. *The abelian group $M \times N$ becomes a left S-module with the following rule for scaling:*

$$s(m, n) = (sm, n).$$

1. *The abelian group $M \otimes_R N$ becomes a left S-module with the following rule for scaling:*

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

2. The map $h : M \times N \to M \otimes_R N$ given by $h(m, n) = m \otimes n$ is an S-module homomorphism.

3. Given any left S-module A and S-linear map $b : M \times N \to A$, there exists a unique S-module homomorphism $g : M \otimes_R N \to A$ such that $g \circ h = b$.

If R, S is are rings M is a right R-module and N is an $R - S$-bimodule, then:

0'. The abelian group $M \times N$ becomes a right S-module with the following rule for scaling:

$$(m, n) = (m, ns).$$

(1') The abelian group $M \otimes_R N$ becomes a right S-module with the following rule for scaling:

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

(2') The map $h : M \times N \to M \otimes_R N$ given by $h(m, n) = m \otimes n$ is an S-module homomorphism.

(3') Given any right S-module A and S-linear map $b : M \times N \to A$, there exists a unique S-module homomorphism $g : M \otimes_R N \to A$ such that $g \circ h = b$.

Proof. We only show (1), (2), (3).

For (1) we first need to verify that this scalar multiplication is well-defined (Remember in $M \otimes_R N$ one there are relations e.g $(m" + m') \otimes n = m \otimes n + m' \otimes n$ and one needs to be concerned whether multiplying either side by a give element $s \in S$ produces the same result.) An equivalent way of thinking about scalar multiplication by a fixed element s is as a group homomorphism $M \otimes_R N \to M \otimes_R N$ given by $u \mapsto su$. If we can show that this map is well defined then we'll be done.

Fix $s \in S$ and define a map $f_s : M \times N \to M \otimes_R N$ by $f_s(m, n) = (sm) \otimes n$. One can check that f_s is R-biadditive. Then there exists a unique group homomorphism $g_s : M \otimes_R N \to M \otimes_R N$ given by $g_s(m \otimes n) = (sm) \otimes n$. In particular the multiplication is well-defined! It is then easy to see that the rest of the module properties hold.

(2) The map is already a group homomorphism. We check that it is S-linear.

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

(3) Existence and uniqueness of such a group homomorphism g is guaranteed by the definition of tensor product. We now show it is also S-linear using the S-linearity of b:

$$\begin{aligned} g(s(\sum_{i=1}^k m_i \otimes n_i)) &= g(\sum_{i=1}^k sm_i \otimes n_i) = \sum_{i=1}^k g(h(sm_i, n_i)) = \sum_{i=1}^k b(sm_i, n_i) \\ &= s\left(\sum_{i=1}^k b(m_i, n_i)\right) = s\left(\sum_{i=1}^k g(m_i \otimes n_i)\right). \end{aligned}$$

□

We now focus on the case to when R is commutative. Recall that any R-module M is an $R-R$ bimodule. Hence we deduce:

Corollary 1.130. *If R is a commutative ring and M and N are R-modules, then:*

1. *The abelian group $M \otimes_R N$ becomes an R-module with the following rule for scaling:*
$$r \cdot \left(\sum_i m_i \otimes n_i \right) := \sum_i r m_i \otimes n_i = \sum_i m_i \otimes n_i r.$$

2. *The map $h : M \times N \to M \otimes_R N$ given by $h(m, n) = m \otimes n$ is R-bilinear.*

3. *Given any R-module A and R-bilinear pairing $b : M \times N \to A$, there exists a unique R-module homomorphism $g : M \otimes_R N \to A$ such that $g \circ h = b$.*

Remark 1.131. When R is not commutative, the proof fails because the rule for scaling is not well-defined. If we let $f_r(m, n) = (mr, n)$ then $f_r(ms, n) = msr \otimes n$ need not equal $f_r(m, sn) = mr \otimes sn = mrs \otimes n$ since sr need not equal rs.

Example 1.132. Let R be a ring. Then:

1. If M is a left R-module, then $R \otimes_R M \cong M$ as left R-modules via the map $r \otimes m \mapsto rm$

2. Let M be an $R-S$ bimodule, let N be an $S-T$ bimodule, and let P be a left T -module. Then $(M \otimes_S N) \otimes_T P \cong M \otimes_S (N \otimes_T P)$ as left R-modules.

3. If R is commutative, and M and N are R-modules, then $M \otimes_R N \cong N \otimes_R M$ as R-modules via the map $m \otimes n \mapsto n \otimes m$.

Remark 1.133. A special case of (1) yields the isomorphism $R \otimes_R R \cong R$, $r \otimes s \mapsto rs$.

Exercise 1.134. Show that if R, S are commutative rings, the tensor product $R \otimes_{\mathbb{Z}} S$ is the (object of the) coproduct of R, S in the category of rings.

1.4.3 Functoriality, extension of scalars, and localization

Let's discuss the functorality of $- \otimes_R -$ now.

Proposition 1.135. *For a ring R, right R-modules M, M' and left R-modules N, N', and R-module homomorphisms $f : M \to M'$ and $g : N \to N'$, there are homomorphisms of abelian groups*

$$f \otimes id_N : M \otimes_R N \to M' \otimes_R N$$

and

$$id_M \otimes g : M \otimes_R N \to M \otimes_R N'$$

given on generators by $(f \otimes id)(m \otimes n) = f(m) \otimes n$ *and* $(id \otimes g)(m \otimes n) = m \otimes g(n)$.

For a fixed M*, the following assignments denoted* $M \otimes_R - : \langle\langle {}_R Mod \rangle\rangle \to \langle\langle Ab \rangle\rangle$ *form a right exact additive covariant functor:*

- *objects: a left* R*-module* N *maps to* $M \otimes_R N$ *and*
- *morphisms: a homomorphism* g *of left* R*-modules maps to* $id_M \otimes g$

For a fixed N*, the following assignments denoted* $- \otimes_R N : \langle\langle Mod_R \rangle\rangle \to \langle\langle Ab \rangle\rangle$ *form a right exact additive covariant functor:*

- *objects: a right* R*-module* M *maps to* $M \otimes_R N$ *and*
- *morphisms: a homomorphism* f *of right* R*-modules maps to* $f \otimes id_N$

If R *is commutative,* $f \otimes id$ *and* $id \otimes g$ *are* R*-module homomorphisms and* $M \otimes_R -$ *and* $- \otimes_R N$ *are functors* $\langle\langle {}_R Mod \rangle\rangle \to \langle\langle {}_R Mod \rangle\rangle$.

Proof. The fact that these rules define functors is left as an exercise.

The functor $M \otimes_R -$ is additive; i.e, we have $\mathrm{id}_M \otimes_R (f+g) = \mathrm{id}_M \otimes_R f + \mathrm{id}_M \otimes_R g$. To see this, note the the left map sends a generator $m \otimes n$ to $m \otimes (f(n) + g(n))$ and the right map sends it to $m \otimes f(n) + m \otimes g(n)$, and these are equal. Similarly $- \otimes_R N$ is additive.

I'll just show $M \otimes -$ is right exact: Let $N' \xrightarrow{g} N \xrightarrow{p} N'' \to 0$ be a right exact sequence of left R-modules. We need to show

$$M \otimes N' \xrightarrow{\mathrm{id}_M \otimes g} M \otimes N \xrightarrow{\mathrm{id}_M \otimes p} M \otimes N'' \to 0$$

is also right exact.

The surjectivity of $\mathrm{id}_M \otimes p$ holds since given a generator $m \otimes n''$ of $M \otimes N''$, we have $n'' = p(n)$ for some n (since p is surjective) and thus $m \otimes n'' = (\mathrm{id}_M \otimes p)(m \otimes n)$. Since a set of generators is contained in its image, $\mathrm{id}_M \otimes p$ is onto.

Reasoning more generally, if F is a covariant additive functor , and the composition of $M' \xrightarrow{g} M \xrightarrow{p} M''$ is the 0 map, then the composition of $F(M') \xrightarrow{F(g)} F(M) \xrightarrow{F(p)} F(M'')$ is automatically the 0 map too, since

$$F(p) \circ F(g) = F(p \circ g) = F(0) = 0.$$

So, given a chain complex

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

so long as F is additive, we have $\mathrm{Im}(F(g)) \subseteq \mathrm{Ker}(F(p))$.

Since the functor $M \otimes_R -$ is additive, the argument above gives $\mathrm{Im}(\mathrm{id}_M \otimes g) \subseteq \mathrm{Ker}(\mathrm{id}_M \otimes p)$. It remains only to prove the opposite containment.

September 16, 2020

Since $\operatorname{Im}(\mathrm{id}_M \otimes g) \subseteq \operatorname{Ker}(\mathrm{id}_M \otimes p)$, $\mathrm{id}_M \otimes p$ induces a map we will write as

$$\phi : T \to M \otimes N''$$

where

$$T := \operatorname{coker}(M \otimes N' \xrightarrow{\mathrm{id}_M \otimes g} M \otimes N) = (M \otimes N)/\operatorname{Im}(\mathrm{id}_M \otimes g).$$

The kernel of ϕ is $\operatorname{Ker}(\mathrm{id}_M \otimes p)/\operatorname{Im}(\mathrm{id}_M \otimes g)$ and so it suffices to prove ϕ is injective. (In fact, it's an isomorphism.)

Define a function

$$b : M \times N'' \to T$$

by

$$b(m, n'') = \overline{m \otimes n}$$

where n is chosen so that $p(n) = n''$. This is independent of choice of n since if $p(n_2) = n''$ then $n - n_2 = g(n')$ and hence

$$\overline{m \otimes n - m \otimes n_2} = \overline{m \otimes g(n')} = 0 \in T.$$

It is easy to check that b is R-biadditive and hence induces a map

$$\psi : M \otimes_R N'' \to T.$$

I claim this map is inverse to $\psi \circ \phi = \mathrm{id}$ and hence ϕ is injective.

For $\overline{m \otimes n} \in T$ we have

$$\psi(\phi(\overline{m \otimes n})) = \phi(m \otimes p(n)) = m \otimes n$$

and since such elements generate T, we see that $\psi \circ \phi$ is the identity.

□

Remark 1.136. Here is how *not* to prove Ker ⊆ Im:

> "Say $(\mathrm{id}_M \otimes p)(m \otimes n) = m \otimes p(n) = 0$. Then $p(n) = 0$. **This deduction is flawed**. So $n = g(n')$ by exactness of the original sequence, and hence $m \otimes n = (\mathrm{id}_M \otimes g)(m \otimes n')$." **Also it does not suffice to prove this for simple tensors.**

Remark 1.137. Tensoring is not in general left exact. Indeed, consider the left exact sequence of $\mathbb{Z}$-modules

$$0 \to \mathbb{Z} \xrightarrow{\cdot n} \mathbb{Z} \to \mathbb{Z}/n$$

and tensor with $\mathbb{Z}/n$. It does not matter if we do so on the left or right by Example 1.132 (2). We obtain

$$0 \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n \xrightarrow{\cdot n \otimes \mathrm{id}_{\mathbb{Z}_n}} \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n \to \mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Z}/n.$$

But $(\cdot n \otimes \mathrm{id}_{\mathbb{Z}_n})(m, \overline{k}) = (nm, \overline{k}) = (m, n\overline{k}) = 0$ so $\cdot n \otimes \mathrm{id}_{\mathbb{Z}_n} : \mathbb{Z}/n \to \mathbb{Z}/n$ is the zero map which is no longer injective.

Definition 1.138. A left R-module N is called *(left) flat* if the functor $-\otimes_R N : \langle\langle \mathrm{Mod}_R \rangle\rangle \to \langle\langle \mathrm{Ab} \rangle\rangle$ is exact. Equivalently, an R module N is flat iff $-\otimes_R N$ preserves injections.

Similarly, a right R-module M is *(right) flat* if $M\otimes_R -$ is exact/preserves injections.

When R is commutative, the the natural isomorphism $M\otimes_R - \cong -\otimes_R M$ shows that M is left-flat if and only if it is right flat, and we just say M is "flat" in this case.

Example 1.139. Remark 1.137 shows that $\mathbb{Z}/n$ is not flat as a $\mathbb{Z}$-module. However $\mathbb{Z}/n$ is flat as a $\mathbb{Z}/n$-module since the functor $\mathbb{Z}/n \otimes_{\mathbb{Z}/n} -$ is naturally isomorphic to the identity functor on $\mathbb{Z}/n$-modules.

Definition 1.140. Recall that for a ring R, left ideal I and left R-module M, we write IM for the set of all expressions of the form

$$IM = \{a_1m_1 + \cdots + a_jm_j \mid j \geq 0, a_i \in I, m_i \in M\}.$$

Then IM is a submodule of M.

Corollary 1.141 (of Proposition 1.135)**.** *Let I be a two-sided ideal of R, with M a left R-module. Then $R/I\otimes_R M \cong M/IM$ as left R/I-modules via the map $\overline{r}\otimes m \mapsto \overline{rm}$.*

Proof. Consider the s.e.s.

$$0 \to I \to R \to R/I \to 0$$

and apply $-\otimes_R M$ to get the right exact sequence

$$I\otimes_R M \to R\otimes_R M \to R/I\otimes_R M \to 0.$$

Recall from Example 1.132 (1) that $R\otimes_R M \cong M$ as left R-modules via $\varphi(r\otimes m) = rm$. Use this isomorphism to construct a commutative diagram where the first vertical map, $\varphi'(i\otimes m) = im$ is obviously surjective and the last map is $\varphi''(\overline{r}\otimes m) = \overline{rm}$. I will skip showing that any of these maps are well defined left R-module homomorphisms and also that the diagram commutes.

$$\begin{tikzcd}
 & I\otimes_R M \arrow[r, "\iota"] \arrow[d, "\varphi'"] & R\otimes_R M \arrow[r, "\pi"] \arrow[d, "\varphi", "\cong"'] & R/I\otimes_R M \arrow[r] \arrow[d, "\varphi''"] & 0 \\
0 \arrow[r] & IM \arrow[r, "i"] & M \arrow[r, "p"] & M/IM \arrow[r] & 0
\end{tikzcd}$$

To establish φ'' is surjective, let $\bar{m} \in M/IM$ with $m \in M$. Then $\overline{m} = \varphi''(\overline{1}\otimes m)$.

Now if $u \in R/I\otimes_R M$ is such that $\varphi''(u) = 0$ then let $v \in R\otimes_R M$ be such that $\pi(v) = u$. Then $p(\varphi(v)) = 0$ so $\varphi(v) \in \mathrm{Ker}(p) = \mathrm{Im}(i) = IM = \varphi'(I\otimes_R M)$ and so there exists $w \in I\otimes_R M$ such that $i(\varphi'(w)) = \varphi(v) = 0$. This implies that $\varphi(\iota(w)) = \varphi(v)$, but since φ is injective this forces $v = \iota(w)$. But now we can deduce $u = \pi(v) = \pi(\iota(w)) = 0$. We have established φ'' is injective.

The last two paragraphs are an example of **diagram chase**. □

Remark 1.142. For a commutative ring R and ideals I and J, the special case $M = R/J$ of the result above gives an isomorphism of R-modules

$$R/I \otimes_R R/J \cong (R/J)/(I(R/J)) = (R/J)/((I+J)/J) \cong R/(I+J).$$

September 18, 2020

Extension of scalars

Definition 1.143 (Module structure via extension of scalars)**.** Let $g : R \to S$ be a map of rings and M a left R-module. The map g allows us to view S as a right R-module via $s \cdot r := sg(r)$ and in fact S is an $S - R$ bimodule. We check the required condition

$$s'(s \cdot r) = s'(sg(r)) = (s's)g(r) = (s's) \cdot r,$$

where we have used associativity of multiplication in S in the middle.

By Proposition 1.129 the abelian group $S \otimes_R M$ is a left S-module.

Definition 1.144. Given $g : R \to S$ a map of rings, extension of scalars along g is the functor $S \otimes_R - : \langle\langle {}_R\text{Mod}\rangle\rangle \to \langle\langle {}_S\text{Mod}\rangle\rangle$ that takes

- a left R-module M to the left R-module $S \otimes_R M$
- an R-module homomorphism $f : M \to N$ to an S-module homomorphism $id_S \otimes f : S \otimes_R M \to S \otimes_R N$ given by $(id_S \otimes f)(s \otimes m) = s \otimes f(m)$.

Definition 1.145. Let R be a commutative ring. A subset S of R is multiplicatively closed if $1 \in S$ and $s, t \in S \Rightarrow st \in S$. Define a new set $S^{-1}R$ called the *localization of R at S* as follows:

$$S^{-1}R = \left\{\frac{r}{s} \mid r \in R, s \in S\right\} / \sim$$

where $\sim$ is the equivalence relation $\frac{r}{s} \sim \frac{r'}{s'}$ if and only if $t(rs' - r's) = 0$ for some $t \in S$. This set is a ring with respect to the operations

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'} \qquad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}.$$

As a simple example, if R is a domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is the field of fractions of R.

For an R-module M define

$$S^{-1}M = \left\{\frac{m}{s} \mid m \in M, s \in S\right\} / \sim$$

where $\sim$ is the equivalence relation $\frac{m}{s} \sim \frac{m'}{s'}$ if and only if $t(ms' - m's) = 0$ for some $t \in S$. Then $S^{-1}M$ is an $S^{-1}R$ module via the operations

$$\frac{m}{s} + \frac{m'}{s'} = \frac{ms' + m's}{ss'} \qquad \frac{r}{s} \cdot \frac{m}{s'} = \frac{rm}{ss'}.$$

If $f : M \to N$ is a morphism of R-modules, we define $S^{-1}f : S^{-1}M \to S^{-1}N$ by $(S^{-1}f)(m/s) \mapsto f(m)/s$. Then $S^{-1}f$ is a well-defined $S^{-1}R$-module homomorphism.

The rules above determine a functor $S^{-1}(-) : \langle\langle {}_R\mathrm{Mod}\rangle\rangle \to \langle\langle {}_{S^{-1}R}\mathrm{Mod}\rangle\rangle$ called *localization at S*. The axioms of a functor are easy to check.

Proposition 1.146. *The extension of scalars functor $S^{-1}R \otimes_R -$ along the canonical map $g : R \to S^{-1}R, g(r) = \frac{r}{1}$ is naturally isomorphic to the localization functor $S^{-1}(-)$ as follows: for each M there is an isomorphism*

$$\eta_M : S^{-1}R \otimes_R M \xrightarrow{\cong} S^{-1}M$$

of $S^{-1}R$-modules that sends $\frac{r}{s} \otimes m$ to $\frac{rm}{s}$.

Proof. Define $b : S^{-1}R \times M \to S^{-1}M$ by $b(\frac{r}{s}, m) = \frac{rm}{s}$. Then b is easily seen to be well-defined and R-bilinear and hence it induces a R-module map

$$\eta_M : S^{-1}R \otimes_R M \to S^{-1}M$$

We need to know that η_M is a morphism not just of R-modules but of $S^{-1}R$ modules. Let's check: Since η_M is R-linear we have

$$\eta_M((r'/s')\sum_i (r_i/s_i) \otimes m_i) = \eta_M(\sum_i r'r_i/(s's_i) \otimes m) =$$
$$\sum_i r'r_i m/(ss') = (r'/s')\sum_i r_i m/s_i = (r'/s')\eta_M(\sum_i r_i/s_i \otimes m).$$

To show η_M is a bijection, we define a map f going the other direction by $f(m/s) = \frac{1}{s} \otimes m$. One should check f is well-defined, but I'll leave that to you. The composition $f \circ g$ sends a generator $\frac{r}{s} \otimes m$ to $\frac{1}{s} \otimes rm = \frac{r}{s} \otimes m$ and hence is the identity. The other composition sends m/s to m/s.

Finally, so show that the map η_M determines a natural isomorphism, we need to verify that if $f : M \to M'$ is an R-module homomorphism, then we have $S^{-1}(f) \circ \eta_M = \eta_{M'} \circ \mathrm{id} \otimes f$. This follows immediately from the formulas:

$$\eta_{M'}(\mathrm{id} \otimes f)(r/s \otimes m) = \frac{rf(m)}{s} = \frac{f(rm)}{s} = S^{-1}(f)(\eta_M(r/s \otimes m)).$$

□

Proposition 1.147. *The localization functor as well as the extension of scalars functor along the canonical map $g : R \to S^{-1}R$ are exact and hence $S^{-1}R$ is a flat R-module.*

Proof. The localization functor was proven exact on homework. If two functors are naturally isomorphic one is exact if and only if the other is. □

Example 1.148. $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.

1.4.4 Hom-tensor adjointness and $\otimes$ distributes over $\oplus$

A useful property of tensor products is that they commute with arbitrary coproducts:

Proposition 1.149. *For any commutative ring R, a family of R-modules $\{M_i : i \in I\}$, and another R-module N, there is an R-module isomorphism*

$$\phi : \left(\bigoplus_{i\in I} M_i\right) \otimes N \xrightarrow{\cong} \bigoplus_{I} (M_i \otimes_R N)$$

that sends $(m_i)_{i\in I} \otimes n$ to $(m_i \otimes n)_{i\in I}$, and similarly there is an R-module isomorphism

$$N \otimes_R \left(\bigoplus_{i\in I} M_i\right) \cong \left(\bigoplus_{i\in I} N \otimes_R M_i\right).$$

Remark 1.150. I am being lazy here by assuming R is commutative. With the evident modifications, the proposition is true for non-commtuative rings and suitable bimodules.

Proof. Define

$$b : \left(\bigoplus_{I} M\right) \times N \to \bigoplus_{I} M_i \otimes_R N$$

by

$$b((m_i)_i, n) = (m_i \otimes n)_i.$$

I leave it to you to check that b is R-bi-linear and hence induces an R-module homomorphism ϕ as in the statement.

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

$$b_i : M_i \times N \to \left(\bigoplus_{i\in I} M_i\right) \otimes N$$

by $b_i(x, n) = \iota_i(x) \otimes n$, where $\iota_i : M_i \hookrightarrow \left(\bigoplus_{i\in I} M_i\right)$ is the canonical inclusion map. Then b_i is R-bi-linear and hence induces an R-map $\psi_i : M_i \otimes_R N \to \left(\bigoplus_{i\in I} M_i\right) \otimes N$.

By the universal mapping property for coproducts the maps $\psi_i, i \in I$ determine an R-map

$$\psi : \bigoplus_{i}(M_i \otimes_R N) \to \left(\bigoplus_{i\in I} M_i\right) \otimes N.$$

It is easy to see that both $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps. □

September 21, 2020

We now come to adjointness.

Definition 1.151. Let $\mathcal{C}$, $\mathcal{D}$ be categories, and let $F : \mathcal{C} \to \mathcal{D}$, $G : \mathcal{D} \to \mathcal{C}$ be functors. We say that F and G are adjoint (and we say that G is right-adjoint to F and F is left-adjoint to G) if there are natural isomorphisms

$$\mathrm{Hom}_{\mathcal{C}}(X, G(Y)) \cong \mathrm{Hom}_{\mathcal{D}}(F(X), Y).$$

We show below that Hom and $\otimes$ are adjoint functors.

Theorem 1.152 (Hom-Tensor Adjointness)**.** *Let R, S, T be rings, and let ${}_RM_T$, ${}_SN_R$, and ${}_SL$ be modules/bimodules as indicated by the subscripts. Then there is a natural isomorphism of left T-modules*

$$\mathrm{Hom}_S(N \otimes_R M, L) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, L))$$

given by sending an S-map $\phi : N \otimes_R M \to L$ to the R-map $f_\phi : M \to \mathrm{Hom}_S(N, L)$ given as $f_\phi(m)(n) = \phi(n \otimes m)$. The inverse map sends θ to the unique map $g_\theta : N \otimes_R M \to L$ so that $g_\theta(n \otimes m) = \theta(m)(n)$.

Proof. Many of the details of this proof will be omitted.

Let's denote the proposed inverse map by g. We will first show that the map g is well-defined. Fix $m \in \mathrm{Hom}_R(M, \mathrm{Hom}_S(N, L))$. Define $b_\theta : N \times M \to L$ by $b_\theta(n, m) = \theta(m)(n)$. One can check that b_θ is R-biadditive. Then by the universal property, there exists a unique g_θ as in the statement. One can then check that g_θ is S-linear using that θ is S-linear. Finally one can check that g is T-linear.

Similar checks are required for f.

Now we will show that f and g are inverses. Indeed:

$$\begin{aligned}(f \circ g)(\theta)(m)(n) &= f_{g_\theta}(m)(n) = g_\theta(n \otimes m) = \theta(m)(n) \\ (g \circ f)(\phi)(n \otimes m) &= g_{f_\phi}(n \otimes m) = f_\theta(m)(n) = \theta(n \otimes m).\end{aligned}$$

Thus these maps are isomorphism of T-modules. □

There are a lot of nice properties of adjoint functor such as:

- applying a right adjoint functor to a product of objects yields the product of the images;

- applying a left adjoint functor to a coproduct of objects yields the coproduct of the images;

- every additive right adjoint functor between two abelian categories is left exact;

- every additive left adjoint functor between two abelian categories is right exact.

We will not explore these properties here.

Chapter 2

Representation theory

2.1 Group representations as $R[G]$-modules

2.1.1 Linear group representatios

Recall from Math 817 that the most important aspect of group theory is that groups have actions on various sets: the group itself, its cosets, some groups are even defined as transformations of Euclidean space (e.g. the dihedral group) so they act on it.

Also in 817 you have seen Cayley's Theorem that every group can be embedded in a permutation group (more precisely, a group G can be viewed as a subgroup of the permutations on the underlying set of G). More generally, a group G acting on a set X gives rise to a group homomorphism $\rho : G \to \mathrm{Perm}(X) = \mathrm{Aut}_{\langle\langle \mathrm{Sets} \rangle\rangle}(X)$.

In this chapter we study the scenario in which a group acts on a set V with additional algebraic structure, such as a module or vector space and the action of the group preserves this structure. When this happens, we say that G acts "linearly" on V. Here is the official definition.

Definition 2.1. Let R be a ring, V a left R-module, and G a group. An *R-linear representation* or *R-linear action* of G on V is an action of G on V, i.e., a pairing $G \times V \to V$, written $(g, v) \mapsto gv$, such that

1. $e_G v = v$ for all $v \in V$ and
2. $(gh)v = g(hv)$ for all $g, h \in G, v \in V$

that is also R-linear, in the sense that

4. $g(v + u) = gv + gu$ for all $g \in G, u, v \in V$and
5. $g(rv) = rg(v)$ for all $g \in G, v \in V, r \in R$.

Remark 2.2. Sometimes we abusively say V is a G-representation to mean that there is some unspecified linear action of G on V.

Remark 2.3. Often we will specialize to the case of *k-linear representations* when $R = k$ is a field and thus V is a k-vector space.

Example 2.4. $G = S_n$ acts k-linearly on k^n by permuting the entries:

$$\sigma \cdot (a_1, \dots, a_n) = (a_{\sigma(1)}, \dots, a_{\sigma(n)}).$$

Lemma 2.5. *Specifying an R-linear representation of G on V is equivalent to specifying a group homomorphism $\rho : G \to \mathrm{Aut}_R(V)$, where $\mathrm{Aut}_R(V)$ is the group of R-linear automorphisms of V.*

Proof. Given an R-linear representation of G on V as in Definition 2.1 we set

$$\rho : G \to \mathrm{Aut}_R(V), \quad \rho(g)(v) = gv.$$

Properties 3 and 4 in Definition 2.1 say that $\rho(g)$ is an R-module homomorphism. Its inverse is $\rho(g^{-1})$, hence $\rho(g)$ is really an automorphism. Properties 1 and 2 in Definition 2.1 say that ρ is a group homomorphism.

Conversely, given ρ we define a representation by setting $gv = \rho(g)(v)$. □

Remark 2.6. When $V = R^n$ is a free R-module of rank n then $\mathrm{Aut}_R(V) \cong GL_n(R)$, the group of invertible $n \times n$ matrices with entries in R.

Example 2.7.

1. For any group G and commutative ring R we can take $V = R$ and $\rho(g) = \mathrm{id}_R$ for all $g \in G$. This representation is called the *trivial representation.*

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 $0 \leq k \leq n-1$.

   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. 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 $\rho : G \hookrightarrow GL_2(\mathbb{R})$ maps

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

4. Let $R = \mathbb{F}_p, V = R^2$ and let $G = C_p = \langle g \rangle$. We see that the assignment

$$\rho : G \to \mathrm{End}_{\mathbb{F}_p}(\mathbb{F}_p^2) \cong GL_2(\mathbb{F}_p) \quad \rho(g^r) = \begin{bmatrix} 1 & 0 \\ \overline{r} & 1 \end{bmatrix}$$

is a representation.The fact that this map is well defined is very much dependent on the choice of R as the field $\mathbb{F}_p$: in any other characteristic it would not work, because the matrix shown would no longer have order p.

September 23, 2020

Definition 2.8. If $\phi : G \to \mathrm{Aut}_R(V)$ and $\psi : G \to \mathrm{Aut}_R(W)$ 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:

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "\phi(g)"'] & W \arrow[d, "\psi(g)"] \\ V \arrow[r, "f"] & W \end{tikzcd}$$

Example 2.9. For the representations of $G = S_n$ on $V = k^n$ given by permuting the entries of an n-tuple, the only equivariant maps $f : V \to V$ are the scaling maps $f(a_1, \ldots, a_n) = c(a_1, \ldots, a_n)$ where $c \in k$.

Proposition 2.10. *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 $\langle\langle Rep_R(G)\rangle\rangle$.*

Proof. The verification of the axioms is left as an exercise. The composition we use in the category $\langle\langle {}_RG\text{-Rep}\rangle\rangle$ is the ususal composition of functions and the identity morphisms are the identity functions id_V. □

2.1.2 Group rings and their modules

Next we will turn representations into modules. First we define a suitable ring.

Definition 2.11. Given a commutative ring R, an *R-algebra* is defined to be a (not necessarily commutative) unital ring A equipped with a ring homomorphism $R \to A$, called the structure map, whose image lies in the center of A.

An *R-algebra homomorphism* between R-algebras A, B with structure maps $\alpha : R \to A, \beta : R \to B$ are the ring homomorphisms $\gamma : A \to B$ that satisfy $\gamma \circ \alpha = \beta$.

Proposition 2.12. *Fix a commutative ring R. The collection of R-algebras and R-algebra homomorphisms forms a category denoted $\langle\langle R\text{-Algebras}\rangle\rangle$.*

Proof. Exercise. □

Next we see how to construct R-algebras from a group in a concrete way.

Definition 2.13. 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

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

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

Remark 2.14. As a matter of notation, the element $1_R g$ will be written as just g and the element re_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 2.15. When R is commutative (in particular when R is a field), $R[G]$ is an R-algebra called the *group R-algebra* of G.

Exercise 2.16. For any ring R and $G = C_n$, prove there is a ring isomorphism

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

Proposition 2.17 (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 2.18. 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.

Exercise 2.19. Show that if R is commutative then forming the group R-algebra is a functor $R[-] : \langle\langle\text{Groups}\rangle\rangle \to \langle\langle R\text{-Algebras}\rangle\rangle$.

September 25, 2020

Example 2.20. (The regular representation) Fix a group G and a ring R. The (left) *regular representation* of G on $R[G]$ is given by the action $g \cdot v = gv$ for any $v \in R[G]$, where the right hand side denotes multiplication in $R[G]$. Note that this extends the action of the group G on itself by left multiplication.

Equivalently the group ring $R[G]$ is given the structure of an R-linear representation of G by means of the map

$$\rho : G \to \mathrm{Aut}_R(R[G]), \quad \rho(g) = \alpha_g,$$

where $\alpha_g : R[G] \to R[G]$ is the morphism given by Proposition 2.17 applied for $A = R[G]$, $\iota = R \hookrightarrow R[G]$ and $f : G \to R[G]^\times, f(g') = gg'$.

Example 2.21. Let's analyze the regular representation of the cyclic group $C_n = \langle g \rangle$ further. $R[C_n]$ is a free R-module with basis $1, g, g^2, \ldots, g^{n-1}$ and thus $\mathrm{Aut}_R(R[C_n]) \cong GL_n(R)$. Let's determine the group homomorphism $\rho : C_n \to GL_n(R)$ corresponding to the regular representation: $g \in C_n$ acts by cyclically permuting the basis elements, so

$$\rho(g) = \begin{bmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \end{bmatrix}.$$

Now recall that $R[C_n] \cong R[x]/(x^n - 1)$ via $g \mapsto x$ and realize that if we look at the multiplication map by x $R[x]/(x^n-1) \xrightarrow{\cdot x} R[x]/(x^n-1)$ as an R-linear map between free R-modules, this map is represented by the same matrix.

Remark 2.22. In a similar way to the example above we see that if G is a finite group then the map ρ corresponding to the regular representation takes every element of G to a permutation matrix.

Example 2.23. Take $R = \mathbb{R}$ and $G = Q_8$, where $Q_8 = \{\pm e, \pm i, \pm j, \pm k\}$ is the *group* of quaternions. Recall the of real quaternion algebra $\mathbb{H}$ from Example 1.5:

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d, \in R, i^2 = j^2 = k^2 = ijk = -1\}.$$

We give this a structure of a Q_8, $\mathbb{R}$-linear representation via multiplication by the images of elements of Q_8 under the map $f : Q_8 \to \mathbb{H}$ that maps elements of Q_8 to elements having the same name in $\mathbb{H}$. That is, $q \in Q_8$ acting on $v \in \mathbb{H}$ is $f(q)v$. More formally, the inclusion $\iota : \mathbb{R} \hookrightarrow \mathbb{H}$, which is a ring homomorphism together with the group homomorphism $f : Q_8 \to (H^\times, \cdot)$ from above give by Proposition 2.17 gives a ring homomorphism

$$\rho : \mathbb{R}[Q_8] \to \mathbb{H},$$

which is equivalent to the action by multiplication described above.

It would be forgivable to assume this map is an isomorphism based on the terminology, but notice that the source is 8 dimensional as an $\mathbb{R}$-vector space and the image is only 4-dimensional. Note that $(1_\mathbb{R})(-e)$ and $(-1_\mathbb{R})e$ are different elements of $\mathbb{R}[Q_8]$ that get mapped to the same element of the target. What is true is that the kernel of α is the $\mathbb{R}$-linear span of $-e + e$, $-i + i$, $-j + j$, $-k + k$, which does indeed form a two-sided ideal of the source. The first isomorphism theorem gives a ring isomorphism

$$\overline{\alpha} : \mathbb{R}[Q_8]/I \xrightarrow{\cong} \mathbb{H}.$$

Notice that the representation $\mathbb{H}$ is thus a *module* over the group ring $\mathbb{R}[Q_8]$. We see below that this is true for all representations.

Modules over group rings

We are now ready to translate group representations in the language of modules. We start by defining two mutually inverse functions

$$\langle\langle \mathrm{Rep}_R(G) \rangle\rangle \to \left\langle\left\langle {}_{R[G]}\mathrm{Mod} \right\rangle\right\rangle \text{ and } \left\langle\left\langle {}_{R[G]}\mathrm{Mod} \right\rangle\right\rangle \to \langle\langle \mathrm{Rep}_R(G) \rangle\rangle .$$

Lemma 2.24. *Assume R is a ring, V is a left R-module, and G is a group. Given a group homomorphism $\rho : G \to \mathrm{Aut}_R(V)$, i.e. an R-linear representation of G on V, there is a unique structure on $(V, +)$ of a left $R[G]$-module denoted V^ρ such that*

$$\left(\sum_{g \in G} r_g g\right) m = \sum_{g \in G} r_g \cdot \alpha(g)(m).$$

(In particular $r \cdot m$ is the original rule for scaling when $r \in R$ and $g \cdot m = \rho(g)(m)$.)

Conversely, if M is a left $R[G]$-module, then we may regard M as a left R-module via restriction of scalars to $R \subseteq R[G]$, and the map $\rho_M : G \to \mathrm{Aut}_R(M)$ defined by $\rho_M(g)(m) = gm$ is a group homomorphism.

Moreover, these two constructions are mutually inverse in the evident sense.

Proof. Recall that, if S is a ring, to give an S-module structure on a set N is equivalent to giving a bi-additive pairing $S \times N \to N, s \times n \mapsto sn$ which is in turn equivalent to giving an S-module homomorphism $S \to \mathrm{End}_{\langle\langle \mathrm{Ab} \rangle\rangle}(N, +), s \mapsto (n \mapsto sn)$ (see Exercise 1.13).

Given V, $\iota : R \hookrightarrow R[G]$ and $\rho : G \to \mathrm{Aut}_R(V)$ as in the statement, note that $\mathrm{Aut}_R(V) \leq \mathrm{Aut}_{Ab}(V) = \mathrm{End}_{\langle\langle \mathrm{Ab} \rangle\rangle}(V, +)^{\times} \leq \mathrm{End}_{\langle\langle \mathrm{Ab} \rangle\rangle}(V, +)$, so we can instead think of ρ as a group homomorphism

$$\rho : G \to \mathrm{End}_{\langle\langle \mathrm{Ab} \rangle\rangle}(V, +).$$

However, the fact that $\rho(g) \in \mathrm{Aut}_R(M)$ means $\rho(g)$ and $\iota(r)$ commute in $\mathrm{End}_{Ab}(M, +)$ for all $g \in G$ and $r \in R$. By Proposition 2.17 we obtain a ring map $\alpha : R[G] \to \mathrm{End}_{Ab}(M, +)$ which makes $(M, +)$ into a left $R[G]$-module. Tracking through the constructions we see that $r \cdot m$ and $g \cdot m$ are as advertised in the statement. □

September 28, 2020

We can augment these functions to functors to prove:

Theorem 2.25. *The categories $\langle\langle \mathit{Rep}_R(G) \rangle\rangle$ and $\left\langle\left\langle {}_{R[G]}\mathit{Mod} \right\rangle\right\rangle$ are isomorphic.*

Proof. Define a functor $F : \langle\langle \mathrm{Rep}_R(G) \rangle\rangle \to \left\langle\left\langle {}_{R[G]}\mathrm{Mod} \right\rangle\right\rangle$ on objects to map $V \mapsto V^{\rho}$ as in the first part of Lemma 2.24. On G-equivariant morphisms $f : V \to W$ define $F(f) : V^{\rho} \to W^{\tau}$ to be $F(f) = f$. We need to show that f is indeed an $R[G]$-module homomorphism, not just an R-module homomorphism. So we compute using R-linearity and G-equivaraince of f

$$f\left(\left(\sum r_g g\right) v\right) = f\left(\sum r_g \rho(g)(v)\right) = \sum r_g \tau(g)(f(v)) = \left(\sum r_g g\right) f(v).$$

Define $G : \left\langle\left\langle {}_{R[G]}\mathrm{Mod} \right\rangle\right\rangle \to \langle\langle \mathrm{Rep}_R(G) \rangle\rangle$ to be the functor that forgets the $R[G]$-module structure but remembers ρ_M as in the second part of Lemma 2.24. Let $\phi : M \to N$ be an $R[G]$-module homomorphism and set $G(\phi) = \phi$. It is clear that ϕ is also an R-module homomorphism. We need to show ϕ is G-equivariant. This follows using the $R[G]$-linearity of ϕ, i.e. $\phi(gm) = g\phi(m)$ for all $m \in M$.

It remains to see that F and G are mutually inverse functors. On objects this is given by Lemma 2.24 and on morphisms both F and G act as the identity so their composition also acts as the identity.

□

Summarizing the information from this section, we have 3 equivalent ways of describing R-linear representations of G on V:

- an R-linear action of G on the R-module V,
- a group homomorphism $\rho : G \to \mathrm{Aut}_R(V)$, and
- a left $R[G]$-module structure on V (that extends the R-linear structure and the G-action)

2.2 Semisimple modules and representations

In this section we aim to:

- decompose representations as direct sums of "simpler" representations
- classify all the indecomposable representations of a given group.

2.2.1 Decomposing representations by Maschke's theorem

We come now to our first non-trivial result, and one that is fundamental to the study of representations of finite groups over fields of characteristic zero, or characteristic not dividing the group order. This surprising result says that in this situation representations always break apart as direct sums of smaller representations.

Corollary 2.26. *The category $\langle\langle Rep_R(G)\rangle\rangle$ has coproducts. The coproduct of a family of R-linear G-representations $(V_1, \rho_1), (V_2, \rho_2)$ is the* direct sum representation

$$(V_1 \oplus V_2, \rho_1 \oplus \rho_2)$$

together with the inclusion maps ι_1, ι_2 of the summands V_1, V_2 into $V_1 \oplus V_2$. The action of G on $V_1 \oplus V_2$ is componentwise: $g \cdot (v_1, v_2) = (g \cdot v_1, g \cdot v_2)$ or equivalently

$$(\rho_1 \oplus \rho_2)(g)(v_1, v_2) = (\rho_1(g)(v_1), \rho_2(g)(v_2)).$$

Proof. We use the isomorphism of categories in Theorem 2.25 and the fact that $\left\langle\left\langle {}_{R[G]}\mathrm{Mod}\right\rangle\right\rangle$ admits coproducts. One can see that the representation $(V_1 \oplus V_2, \rho_1 \oplus \rho_2)$ satisfies, using notation from Lemma 2.24,

$$(V_1 \oplus V_2)^{\rho_1 \oplus \rho_2} = V_1^{\rho_1} \oplus V_2^{\rho_2}$$

in the category of $R[G]$-modules and use that the right hand side is a coproduct in that category. □

Definition 2.27. Let V be an R-linear representation of a group G. An R-submodule W of V is a *subrepresentation* if W is stable under the action of G, that is $g \cdot w \in W$ for all $w \in W$.

Remark 2.28. If W is a subrepresentation of V then V/W can be given a structure of *quotient representation* with respect to the R-linear action $g \cdot \overline{v} = \overline{g \cdot v}$. This is independent of choice of representative because W is stable under the G action on V.

Example 2.29. Let C_2 act on $\mathbb{R}^2$ by reflection over the x-axis. Specifically we have $\rho : C_2 = \langle g \rangle \to GL_2(\mathbb{R}), \rho(e) = I_2, \rho(g) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. Observe that the subrepresentations are $V_0 = \{0\}, V_1 = \operatorname{Span}\{e_1\}, V_2 = \operatorname{Span}\{e_2\}, V = \mathbb{R}^2$ and that V decomposes as $V = V_1 \oplus V_2$.

Exercise 2.30. Show that if W as above is a subrepresentation of a representation (V, ρ) then ρ induces a group homomorphism $\rho_W : G \to \operatorname{Aut}_R(W)$ by restriction $\rho_W(g) = \rho(G)|_W$ and W^{ρ_W} is an $R[G]$-submodule of V^ρ.

We do now require the ring R to be a field, and in this situation we will often use the symbol k instead of R.

Theorem 2.31 (Maschke's Theorem - representation theoretic version)**.** *Let V be a k-linear representation of a finite group G such that $\operatorname{char}(k) \nmid |G|$ (i.e. $|G|$ is invertible in k). Let W be a subrepresentation of V. Then there exists a subrepresentation U of V such that $V = W \oplus U$ as representations.*

September 30, 2020

Proof. Let $i : W \hookrightarrow V$ be the inclusion map. Then we have a short exact sequence

$$0 \to W \xrightarrow{i} V \xrightarrow{q} V/W \to 0$$

which splits because the modules in this sequence are k-vector spaces, hence free k-modules. In particular, W/V is free, hence projective by Proposition 1.101 and thus there is a splitting map $s' : V/W \to V$ by Proposition 1.105. Set $U' = s'(V/W)$. Then $V/W \cong s(V/W)$ and $V = W \oplus U'$ by the Splitting Theorem.

However, although V/W is a representation with respect to the action $g \cdot \overline{v} = \overline{g \cdot v}$ which makes q a G-equivariant map, U' need not be a subrepresentation of V because U' need not be stable under the action of G and s' need tot be G-equivariant. In other words, we have split the short exact sequence in the category of k-vector spaces but not in the category of k-linear G-representations.

To fix the problem above we now modify s' to be equivariant. Let $s : V/W \to V$ be given by

$$s(\overline{v}) = \frac{1}{|G|} \sum_{g \in G} g \cdot s'(g^{-1} \cdot \overline{v}).$$

It is easy to see that this map is k-linear. We check that s splits q. Indeed,

$$\begin{aligned} (q \circ s)(\overline{v}) &= q\left(\frac{1}{|G|} \sum_{g \in G} g \cdot s'(g^{-1} \cdot \overline{v}) \right) \\ &= \frac{1}{|G|} \sum_{g \in G} q(g \cdot s'(g^{-1} \cdot \overline{v})) \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{|G|}\sum_{g\in G}\overline{g\cdot s'(g^{-1}\cdot\overline{v})}\\
&= \frac{1}{|G|}\sum_{g\in G} g\cdot\overline{s'(g^{-1}\cdot\overline{v})}\\
&= \frac{1}{|G|}\sum_{g\in G} g\cdot\underbrace{(q\circ s')}_{\mathrm{id}_{V/W}}(g^{-1}\cdot\overline{v})\\
&= \frac{1}{|G|}\sum_{g\in G} g\cdot g^{-1}\cdot\overline{v} = \frac{1}{|G|}\sum_{g\in G}\overline{v} = \overline{v}.
\end{aligned}
$$

We check that s is G-equivariant: for $h\in G$ we compute

$$
\begin{aligned}
s(h\cdot\overline{v}) &= \frac{1}{|G|}\sum_{g\in G} g\cdot s'(g^{-1}\cdot h\cdot\overline{v}) = \frac{1}{|G|}\sum_{g\in G} g\cdot s'((h^{-1}g)^{-1}\cdot\overline{v})\\
&= h\cdot\frac{1}{|G|}\sum_{h^{-1}g\in G} h^{-1}g\cdot s'((h^{-1}g)^{-1}\cdot\overline{v}) = h\cdot s(\overline{v}).
\end{aligned}
$$

Now set $U = s(V/W)$ and observe that U is a subrepresentation of V by the calculation above and $V = W\oplus U$ as before. □

Definition 2.32. An R-linear representation V of a group G is called *irreducible* or *simple* if $V\neq 0$ and V does not have any non-zero, proper subrepresentations.

Example 2.33. There are three irreducible $\mathbb{R}$-linear representations of $S_3 = D_6$:

- the trivial representation
- the sign representation
- $\mathbb{R}^2$ with the natural action of D_6 by reflections and rotations

The trivial and sign representations are irreducible because they have dimension 1 as vector spaces and any 1-dimensional vector space is irreducible. The 2-dimensional representation is simple because, visibly, no 1- dimensional subspace is invariant under the group action of D_6.

We will show eventually that these are all the irreducible representations of S_3 up to isomorphism.

Corollary 2.34 (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 finite dimensional k-linear representation of G is a finite direct sum of irreducible representations.*

Proof. The basic idea is that if V is a non-simple representation then V decomposes into proper subrepresentations $V = U\oplus W$ by Maschke's theorem. This process can be repeated if U or W are non-simple. One needs to be concerned whether there this procedure terminates. It does because at each step the number of summands increases and by dimension counting this can happen at most $\dim_k(V)$ times before we reach summands that are either irreducible or 1-dimensional, hence also irreducible for dimension reasons. □

In the following sections we will to imitate the decomposition of k-linear representations, i.e., $k[G]$-modules from the previous section for modules over arbitrary rings. We start by considering the building blocks.

2.2.2 Simple modules

Definition 2.35. A left R-module M is called (left) *simple* if it is non-zero and it has no non-zero, proper submodules.

Lemma 2.36. *M is a simple left R-module if and only if M is isomorphic to R/I, where I is a maximal left ideal.*

Proof. Suppose M is a simple left R-module. Since M is non-zero, there is a $0 \neq m \in M$. The submodule generated by m must be all of M (since M is simple), and so M is cyclic and hence $M \cong R/I$ for a proper left ideal I. By the lattice theorem there are no left ideals with $I \subset J \subset R$ and thus I is a maximal left ideal.

The converse follows also by the lattice theorem. □

Exercise 2.37. Prove uniquness: If $R/I \cong R/J$ for any two maximal left ideals I and J, then $I = J$. (This holds in fact without the "maximal" assumption.)

Example 2.38. If R is commutative, then an ideal I is maximal if and only if R/I is a field. (Note that in the non-commutative case, R/I would not even be a ring unless I happens to be a two-sided ideal.) So the simple R-modules in this case are the quotient fields of R.

In particular, if R is a PID, the simple R-modules are those of the form R/p with p a prime element. In particular, for $R = k[x]$ the simple modules are those of the form $R/p(x)$ with $p(x)$ an irreducible polynomial. And the simple $\mathbb{Z}$-modules are $\mathbb{Z}/p$ for p a prime integer.

Lemma 2.39. *For a division ring D and integer $n \geq 1$, let $R = \mathcal{M}_n(R)$ be the ring of $n \times n$ matrices with entries in R and let $M = D^n$ (column vectors) viewed as a left R-module via the standard matrix multiplication. Then M is a simple R-module.*

Proof. Let $V \neq 0$ be an R-submodule of M. We wish to show $V = M$. Let $0 \neq v = \begin{bmatrix} v_1 & \cdots & v_n \end{bmatrix}^T \in V$ and suppose $v_j \neq 0$. Then $v_j^{-1} E_{ij} v = e_i \in V$ for all i, where e_i denotes the i-th standard basis vector of D^n and E_{ij} the matrix with entry 1 in position (i, j) and 0 elsewhere. Since V is a D-module and contains a basis of M it follows that $V = M$, as desired. □

October 2nd, 2020

Proposition 2.40. *Suppose G is a group and M is a non-zero left $R[G]$-module. M is simple as a left $R[G]$-module if and only if M is irreducible when viewed as a representation of G.*

Proof. To prove this, we show that the functors $F : \langle\langle \mathrm{Rep}_R(G) \rangle\rangle \to \langle\langle {}_{R[G]}\mathrm{Mod} \rangle\rangle$ and $G : \langle\langle {}_{R[G]}\mathrm{Mod} \rangle\rangle \to \langle\langle \mathrm{Rep}_R(G) \rangle\rangle$ of Theorem 2.25 take a subrepresentation of M, i.e., an R-submdule of M that is invariant under G to an $R[G]$-submodule W of M and vice-versa.

To see this, say $W \subseteq M$ is an R-submodule and is invariant under G. Then for all $w \in W$, we have $(\sum_i r_i g_i)w = \sum_i r_i(g_i w)$ belongs to W, for all elements $\sum_i r_i g_i$ of the group ring. So W is an $R[G]$-submodule.

If W is an $R[G]$-submodule, then it is closed under $+$ and scaling by R, since R is a subring of $R[G]$. Thus it is an R-module. Its invariant under the action of G since G is a subgroup of $R[G]^\times$. □

The following is a classic and easy fact about simple modules. It is reminiscent of the well known fact that any non-zero field homomorphism is injective.

Lemma 2.41 (Schur's Lemma). *Let R be any ring and M and N two simple left R-modules. Every non-zero R-module homomorphism $f : M \to N$ is an isomorphism. In particular,* $\mathrm{End}_R(M)$ *is a division ring.*

Proof. For the first assertion, if $f \neq 0$, then we have $\mathrm{Ker}(f) \neq M$ and $\mathrm{Im}(f) \neq 0$. Since each of these is a submodule, the simplicity assumptions give that $\mathrm{Ker}(f) = 0$ and $\mathrm{Im}(f) = N$, and hence that f is one-to-one and onto.

For the second, recall $\mathrm{End}_R(M)$ is ring, as shown before, and that the mutiplication rule is composition. If $f \in \mathrm{End}_R(M)$ is any non-zero element, then by the first part f has a two-sided inverse f^{-1} (which also belongs to $\mathrm{End}_R(M)$). □

2.2.3 Semisimple modules and the Krull-Schmidt theorem

Definition 2.42. For any ring R, a left R-module M is called (left) *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 2.43. Let M be a finitely general $\mathbb{Z}$-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 $r \geq 0$, $n \geq 0$, 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 2.44. Every module over a division ring D is semisimple because any such module has a basis, hence it is a free module.

Lemma 2.45. *Let D be a division ring and set $R = \mathcal{M}_n(D)$ for some $n \geq 1$. I claim R is semisimple as a left module over itself.*

Proof. For each $1 \leq i \leq n$, let I_i denote the subset of R consisting of matrices whose only non-zero 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 in Lemma 2.39 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 $X_i \in M_i$. □

Before we discuss semisimple module further, let's recall a few facts about internal direct sums.

Definition 2.46. Given an R-module M and submodules M' and M'' we say that M is the *internal direct sum* of M' and M'' and we write $M = M' \oplus M''$ if the map $\varphi : M' \oplus M'' \to M, (m', m'') \mapsto m' + m''$ is an R-module isomorphism. We also say in this setup that M' and M'' are (direct) *summands* of M.

Lemma 2.47 (Characterization of internal direct sum). *The following statements are equivalent for a R-module M and submodules M' and M'':*

1. *$M = M' \oplus M''$ (internal direct sum)*

2. *There is a split s.e.s $0 \to M' \to M \to M'' \to 0$.*

3. *Every $m \in M$ has a unique expression of the form $m = m' + m''$ for elements $m' \in M', m'' \in M''$.*

4. *$M = M' + M''$ and $M' \cap M'' = \{0\}$*

Proof. (1) ⇔ (3) is by definition and (3) ⇔ (4) is easy (left as exercise).

Finally (1) ⇔ (2) follows from the Splitting Theorem 1.90. The key point is that the splitting theorem furnishes an isomorphism $\theta : M \to N \oplus N'$ which is the inverse of the map φ in Definition 2.46. □

Remark 2.48. If one has a split s.e.s $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ with splitting s for p then there is also a split s.e.s $0 \to i(M') \to M \to s(M'') \to 0$ which yields an internal direct sum $M = i(M') \oplus s(M'')$.

Proposition 2.49 (Equivalent conditions for simple 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 $i : M' \hookrightarrow M$ is split (i.e., for each such i there is an R-map $q : M \to M'$ with $q \circ i = id_N$),*

4. *every s.e.s of the form $0 \to M' \to M \to M'' \to 0$ is split exact,*

5. *every surjective R-map $p : M \twoheadrightarrow M''$ splits (i.e., for each such p there is an R-map $j : M'' \to M$ with $p \circ j = id_N$).*

October 5, 2020

Proof. The equivalence of (3), (4), and (5) is given by the Splitting Theorem 1.90.

(2) ⇒ (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 isomorphims so we may consider the R-module homomorphism $i^{-1} : i(M') \to M'$ and set $s : M \to M'$ to be $s = i^{-1} \circ \pi$. Then

$$s \circ i = i^{-1} \circ \pi \circ i = i^{-1} \circ \pi_{i(M')} \circ i = i^{-1} \circ i = \mathrm{id}_{M'}.$$

(3) ⇒ (2) holds since we can split the inclusion $N \hookrightarrow M$ and thus also the s.e.s.

$$0 \to N \to M \to M/N \to 0.$$

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) ⇔ (2). (1) ⇒ (2) Assume (1), so that $M = \oplus_{i\in I} M_i$ for some collection of simple submodules M_i, and let $N \subseteq M$ be any submodule. *It is important to note that it does not necessarily follow that N is one of the M_i;* see Example 2.55. Consider the collection $\mathcal{S}$ of subsets J of I such that $N \cap M_J = 0$ where we define $M_J := \oplus_{j\in J} M_j$. View $\mathcal{S}$ as a poset by inclusion. It's non-empty since $J = \emptyset$ belongs to $\mathcal{S}$. If $\{J_\alpha\}$ is a totally ordered sub-collection of $\mathcal{S}$, let $J = \cup_\alpha J_\alpha$. I claim $M_J \cap N = 0$. If not, there is a non-zero element $(m_j) \in M_J \cap N$. But since $m_j = 0$ for all but a finite number of j's and since the collection of J_α's was totally ordered, there is some α such that $(m_j) \in M_{J_\alpha} \cap N$, a contradiction. We may thus apply Zorn's Lemma to get a maximal $J \in \mathcal{S}$.

I claim M is the internal direct sum of N and M_J. We have $N \cap M_J = 0$ by construction and so it suffices to prove $N + M_J = M$. Since $M = \sum_{i\in I} M_i$, the latter is equivalent to proving that $M_i \subseteq N + M_J$ for all $i \in I$. If this fails for some i, then since $M_i \cap (N + M_J)$ is a proper submodule of M_i, which is simple, and hence $M_i \cap (N + M_J) = 0$. But then $N \cap M_{J'} = 0$ where $J' = J \cup \{i\} \supset J$. Indeed, if $n \in N$ and $n = m_i + \sum_{j\in J} m_j$, then $m_i = n - \sum_j -m_j \in M_i \cap (N + M_J) = 0$. So, J' is member of $\mathcal{S}$ that strictly contains J, a contradiction. It must be the $M = N \oplus M_J$.

(2) ⇒ (1) Now assume that every submodule of M is a summand. We proceed in three steps:

(i) I 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 $T = U \oplus (V \cap T)$.

October 7, 2020

(ii) I claim that every non-zero 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 non-zero, proper submodule W_1 and hence, by using (i) again, we get that $W = W_1 \oplus W_2$ for some proper non-zero 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) For this part we consider the collection of all families $\{S_j\}_{j \in J}$ of submodules of M satisfy the two properties

- each S_j is a simple submodule of M and
- they form an internal direct sum of the submodule that they generate; i.e., $\sum_j S_i = \oplus_j S_j$. (This is equivalent to saying that for all $l \in J$ we have $S_l \cap \sum_{j \in J, j \neq l} S_j = 0$.)

Define an order relation on the collection of all such families by declaring $\{S_j\}_{j \in J} \leq \{T_i\}_{i \in I}$ iff $J \subseteq I$ and $S_j = T_j$ for all $j \in J$. Take my word for it that we may apply Zorn's Lemma to show that there is a member $\{S_j\}_{j \in J}$ of this collection that is maximal. Set $U = \oplus_j S_j = \sum_j S_j$. We need to prove $U = M$. By (i) 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 $\{S_j\}_{j \in J} \cup \{S\}$ is a larger member of the collection, a contradiction. □

Corollary 2.50. *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 Proposition 2.49 every submodule of N is a summand, and hence N is semisimple by Proposition 2.49 (2) $\Rightarrow$ (1).

Given a surjection $M \twoheadrightarrow P$, it splits by Proposition 2.49, 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. □

Let us now derive some properties of semisimple modules in the case when M is assumed to be finitely generated. These properties involve the ascending and descending chain conditions on submodules.

Definition 2.51. A module M is said to be (left) *noetherian* or to satisfy the ascending chain condition (acc) on submodules if given any ascending chain $M_1 \subseteq M_2 \subseteq \cdots$ of (left) submodules of M, there is an index n such that $M_n = M_{n+1} = \cdots$.

A module M is said to be (left) *artinian* or to satisfy the descending chain condition (dcc) on submodules if given any descending chain $M_1 \supseteq M_2 \supseteq \cdots$ of (left) submodules of M, there is an index n such that $M_n = M_{n+1} = \cdots$.

Lemma 2.52. *Let R be any ring and M a finitely generated left semisimple left R-module.Then M is both (left) noetherian and (left) artinian.*

Proof. If N is a submodule of M, then, by Proposition 2.49, $M = N \oplus T$ for some T and hence there is a surjective R-map $M \twoheadrightarrow N$ given by the evident projection. Since M is finitely generated, N is finitely generated by the images of the generators of M under this projection. It follows that every submodule of M is finitely generated.

By a standard argument it follows that M has the acc (in fact, this condition on submodules is equivalent to acc, see Exercise 2.53.) In detail if $M_0 \subseteq M_1 \subseteq \cdots M$ is a chain of submodules, then the union $M' = \cup_i M_i$ is a submodule of M and hence is finitely generated. Any finite generating set would necessarily be contained in M_i for some sufficiently large i, which gives that $M_j = M'$ for all $j \geq i$.

For dcc, suppose there was an infinite descending chain $M = M_0 \supset M_1 \supset \cdots$. For each i, there exists by (2) a submodule N_i of M_i such that $M_i = M_{i+1} \oplus N_i$ (internal direct sum), and since $M_{i+1} \neq M_i$, we have $N_i \neq 0$. We get $M = N_0 \oplus M_1 = N_0 \oplus N_1 \oplus M_2 = \cdots$, which leads to an infinite strictly ascending chain

$$N_0 \subset N_0 \oplus N_1 \subset N_0 \oplus N_1 \oplus N_2 \subset \cdots,$$

contrary to the acc. □

We have proven half of the following exercise within the proof if the Lemma above.

Exercise 2.53. Prove M has acc if and only if every (left) submodule of M is finitely generated.

Remark 2.54. It is easy to show that any finitely generated semisimple module is a *finite* direct sum of simple modules.

October 9, 2020

Example 2.55. Consider the semisimple $\mathbb{Z}$-module $M = \mathbb{Z}/(p) \oplus \mathbb{Z}/(p)$. It has many simple submodules, for example $N_1 = \{(a,a) \mid a \in \mathbb{Z}/(p)\}$ or $N_2 = \{(a,2a) \mid a \in Z/(p)\}$. One can show that

$$M = \mathbb{Z}/(p) \oplus \mathbb{Z}/(p) = N_1 \oplus N_2.$$

The following theorem will allow us to deduce from the above equality that $N_1 \cong \mathbb{Z}/(p)$ and $N_2 \cong \mathbb{Z}/(p)$ (as one can easily check directly). More importantly, the next theorem will allow to show that if N is *any* simple submodule of M then N is isomorphic to $\mathbb{Z}/(p)$.

The next theorem is a statement about the uniqueness of writing a semisimple module as a *finite* sum of simple modules.

Theorem 2.56 (Krull-Schmidt for semisimple modules)**.** *For any ring R, suppose we have an isomorphism $M_1 \oplus \cdots \oplus M_t \cong N_1 \oplus \cdots \oplus N_s$ of R-modules, with all the M_i's and N_j's simple. Then $t = s$ and, after reordering, $M_j \cong N_j$ for all j.*

Proof. Let $M = M_1 \oplus \cdots \oplus M_t$ and $N = N_1 \oplus \cdots \oplus N_s$, with all the M_i's and N_j's simple, and suppose there is an isomorphism $\phi : N \xrightarrow{\cong} M$ of R-modules. We proceed by induction on $\max\{s, t\}$ with the case $\max\{s, t\} = 1$ being obvious.

For each j, set $\alpha_j : N_1 \to M_j$ to be the composition $N_1 \hookrightarrow N \xrightarrow{\phi} M \twoheadrightarrow M_j$. Since $\phi|_{N_1} \neq 0$, for some j the map α_j must be non-zero. Since N_1 and M_j are simple, this map must be an isomorphism by Schur's Lemma. Renumber so that $j = 1$.

Let $N = N_1 \oplus N'$ and $M = M_1 \oplus M'$ where $N' = N_2 \oplus \cdots \oplus N_s$ and $M' = M_2 \oplus \cdots \oplus M_t$. We have that the composition of $N_1 \hookrightarrow N \xrightarrow{\phi} M \xrightarrow{proj} M_1$ is an isomorphism α_1. If we can somehow "cancel" N_1 and M_1 from each side and deduce that $N' \cong M'$, then we will be done by induction. This is a bit delicate; see Example 2.57.

Instead we show that

$$M = \phi(N_1) \oplus M'.$$

Indeed, let $\pi_1 : M \to M_1$ and $\pi_2 : M \to M'$ denote projections onto the respective summands. Notice that $\alpha = \pi_1 \circ \phi|_{N_1}$ is bijective can be restated as $\pi_1|_{\phi(N_1)}$ is an isomorphism. Moreover $\pi_1|M' = 0$. This shows that $\phi(N_1) \cap M' = \{0\}$.

To see that $\phi(N_1) + M' = M$, let $\phi(N_1) + M' = U$ and note that it suffices to show that $U/M' = M/M'$. Since $M/M' \cong M_1$ via the map induced by π_1, this is equivalent to showing that $\pi_1(U) = M_1$. This follows because $\pi_1(U) = \pi_1(\phi(N_1)) + \pi_1(M') = \alpha_1(N_1) + 0 = M_1$.

Now notice that there are isomorphisms

$$N' \cong N/N_1 \cong M/\phi(N_1) \cong M'$$

where the first and last isomorphisms are induced by projection onto summands and the middle isomorphism is induced by ϕ. Hence $M_2 \oplus \cdots \oplus M_t \cong N_2 \oplus \cdots \oplus N_s$ and the rest follows by the inductive hypothesis.

□

The above proof fails in general because such an isomorphism need not map the copy of R in the source isomorphically onto any of the copies of R in the target, since Schur's Lemma is not available. Beware that "cancelling summands" is thus not possible in general, as shown by the following example.

Example 2.57. Let

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

be the ring of polynomial functions defined on the sphere S^2 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 $j(r) = (xr, yr, zr)^T$. So we have

$$R^3 = R^2 \oplus R \cong P \oplus R$$

but $P \ncong R^2$ because P is not free by the Hairy Ball Theorem. If P were free, P would yield a nonvanishing vector field on the sphere S^2 - such a vector field does not exist by the Hairy Ball Theorem.

Corollary 2.58. *If M is a finitely generated semisimple module such that $M = M_1 \oplus \cdots M_n$ for some simple modules $M_1, \cdots, M_n$ and if N is any simple submodule of M then $N \cong M_i$ for some i.*

Proof. Let $M = N \oplus N'$ for some submodule N'. If N' is simple or $N' = 0$ stop, otherwise consider a simple submodule N_2 of N' and write $N' = N_2 \oplus N''$. Continuing in this way we find a finite simple decomposition $M = N \oplus N_2 \oplus \cdots \oplus N_s$ because M is finitely generated and hence it satisfies dcc thus the chain $N' \supsetneq N'' \supsetneq \cdots$ must terminate.

Applying Krull-Schmidt to $M = M_1 \oplus \cdots M_n = N \oplus N_2 \oplus \cdots \oplus N_s$ yields $N \cong M_i$ for some i. □

October 12, 2020

2.2.4 Semisimple rings and the Artin-Wedderburn theorem

Definition 2.59. A ring R is *left semi-simple* if R is semi-simple as a left module over itself. R is *right semi-simple* if R is semi-simple as a right modules over itself.

As a technical point, the 0 is ring is considered left and right semi-simple.

Remark 2.60. It is easy to see from the definition that R is right semisimple is equivalent to R^{op} is left semi-simple. It will be a consequence of the Artin-Wedderburn Theorem that, in fact, R is right semisimple is equivalent to R is left semi-simple but this is not at all obvious just from the definition.

Remark 2.61. Recall that submodules of R are left ideals and the simple ones are the minimal (non-zero) left ideals. So, R is left semi-simple 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*. In other words the decomposition above gives that $1 = i_{j_1} + \cdots + i_{j_m}$ with finitely many terms $i_{j_i} \in I_{j_i}$. So, R is left semi-simple 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 2.62. For any $n \geq 0$ and division ring D, $\mathcal{M}_n(D)$ is left semi-simple. This was shown in Lemma 2.45. It is also right semi-simple.

Semi-simple rings are very nice in that we can describe modules over them explicitly, as the next two results show.

Proposition 2.63. *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 s.e.s. 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 2.49. The equivalence of (4) and (7) follows from the characterization of injective modules in Proposition 1.112 and the equivalence of (5) and (6) follows from the characterization of projective modules in Proposition 1.105. 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 semi-simple modules is again semi-simple, and so $\bigoplus_I R$ is semi-simple for any indexing set I. By choosing a generating set of M (e.g, M itself), we may find a surjection of the form $p : \oplus_I R \twoheadrightarrow M$. By Corollary 2.50, it follows that M is semi-simple since it is a quotient of a semisimple module $M \cong \oplus_I R/\operatorname{Ker}(p)$. □

We obtain from the previous result and Krull-Smidt the following important classification theorem:

Proposition 2.64. *Let R be a left semi-simple ring such that $R = I_1 \oplus \cdots \oplus I_m$ 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 for $I_1, \ldots, I_m$; so, for each i with $1 \leq i \leq m$, there is a unique j with $1 \leq j \leq l$ so that $I_i \cong J_j$ as left R-modules.*

Then every finitely generated left R-module 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 non-negative integers.

Proof. Since M is finitely generated there is a surjection $R^n \twoheadrightarrow M$. Using Proposition 2.63 this surjection splits, so that $R^n \cong M \oplus N$ for some N, and each of M and N is semi-simple 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 semi-simple modules. □

We now come to the main theorem regarding semisimple rings

Theorem 2.65 (Artin-Wedderburn Theorem)**.** *Let R be a left semisimple ring. Then for some $m \geq 0$, positive integers $n_1, \ldots, n_m$, and division rings $D_1, \ldots, D_m$, there is a ring isomorphism*

$$R \cong \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_m}(D_m).$$

Moreover,

1. *m is the number of isomorphism classes of simple left R-modules*
2. *Say $M_1, \ldots, M_m$ are simples modules forming a complete set of representatives of these isomorphism classes. Then, after reordering, $D_i \cong \mathrm{End}_R(M_i)^{op}$ and*
3. *n_j is the number of times summands isomorphic to M_j 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 isomorphism of division rings.

For the proof we use the following lemmas.

Lemma 2.66. *If R and S are semi-simple, 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 2.67. The previous lemma and Lemma 2.45 show that for any integer $m \geq 0$, list of division rings $D_1, \ldots, D_m$ and positive integers $n_1, \ldots, n_m$, the ring

$$R = \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_m}(D_m)$$

is semi-simple. The Artin-Wedderburn Theorem asserts that these are the *only* examples! (The case $m = 0$ gives the 0 ring.)

October 14, 2020

Proof of the Artin-Wedderburn Theorem. Since R is left semi-simple, 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, $n_j \geq 1$, and such that M_i is not isomorphic to V_j for all $i \neq j$. We compute the endomorphisms of both sides:

$$\begin{aligned}
\mathrm{End}_R(R) &= \mathrm{Hom}_R(\bigoplus_{i=1}^{m} M_i^{\oplus n_i}, \prod_{j=1}^{m} M_j^{\oplus n_j}) \cong \prod_j \mathrm{Hom}_R(M_i^{\oplus n_i}, \prod_i M_i^{\oplus n_j}) \\
&\cong \prod_{i=1}^{m}\prod_{j=1}^{m} \mathrm{Hom}_R(M_i^{\oplus n_i}, M_j^{\oplus n_j}) \\
&= \prod_{i=1}^{m} \mathrm{Hom}_R(M_i^{\oplus n_i}, M_i^{\oplus n_i}) \\
&= \mathrm{End}_R(M_i^{\oplus n_i}) \cong \mathcal{M}_{n_i}(\mathrm{End}_R(M_i)).
\end{aligned}$$

Above the second line follows from the first by properties of Hom, the third follows because Schur's lemma gives $\mathrm{Hom}(M_i^{\oplus n_i}, M_j^{\oplus n_j}) = 0$ whenever $i \neq j$. Finally, by applying Schur's Lemma again, $D_i' := \mathrm{End}_R(M_i)$ is a division ring for all i.

On the one hand, we have $\mathrm{End}_R(R) \cong R^{op}$ by a problem from the homework.

Combining these gives

$$R^{op} \cong \mathcal{M}_{n_1}(D_1') \times \cdots \times \mathcal{M}_{n_m}(D_m')$$

and hence, also by a homework problem, we have

$$R \cong (\mathcal{M}_{n_1}(D_1') \times \cdots \times \mathcal{M}_{n_m}(D_m'))^{op} \cong \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_m}(D_m)$$

with $D_i := (D_i')^{op}$.

Concerning uniqueness, Schur's Lemma allows us to conclude the D_1, n_i and m are unique provided the decomposition of R as a product of matrix rings arises from a decomposition of R into simple modules $R \cong M_1^{\oplus n_1} \oplus \cdots \oplus M_m^{\oplus n_m}$ as above. We show this is always the case.

Say we are given an isomorphism of rings $R \cong \prod_i \mathcal{M}_{t_i}(D_i'')$. Then since $\mathcal{M}_n(D'')$ decomposes as a direct sum of n copies of D''^n, and D''^n is a simple D''-module by Lemma 2.39, hence also a simple R-module since D_n'' is a subring of $\mathcal{M}_n(D'')$ (viewed as the ring of D'' multiples of the identity matrix) and $\mathcal{M}_n(D'')$ can be identified with an ideal of R, hence any R-module is also a D''-module. This leads to a decomposition of R into simple modules. Specifically we have

$$M_1^{\oplus n_1} \oplus \cdots \oplus M_m^{\oplus n_m} \cong R \cong (D_i''^{t_1})^{\oplus t_1} \oplus \cdots \oplus (D_m''^{t_m'})^{\oplus t_m'}$$

Applying Krull-Schmidt gives $m = m'$, $M_i \cong D_i''^{t_i}$ and $n_i = t_i$, thus $M_i \cong D_i''^{n_i}$ and

$$D_i \cong \mathrm{End}_R(M_i^{\oplus n_i})^{op} \cong \mathrm{End}_R(D_i''^{\oplus n_i})^{op} \cong \mathrm{End}^{op}_{\mathcal{M}_{n_i}(D_i'')}(D_i''^{\oplus n_i})^{op} \cong D_i'',$$

with the last isomorphism due to a homework problem. So, every decomposition into a product of matrix rings does indeed arise from the construction of the theorem and thus Krull-Schmidt gives the uniqueness statement. □

2.2.5 Applications to representation theory

Returning to the setup of Maschke's Theorem, let's discuss what our knowledge on semisimple rings and modules implies for representation theory.

Theorem 2.68 (Representations of finite groups – nonmodular case)**.** *Let G be a finite group and let k be a field such that* $\mathrm{char}(k) \nmid |G|$*. Then*

1. *(Maschke's Theorem) the group ring $k[G]$ is semisimple*
2. *every irreducible k-linear representation of G is a direct summand of the left regular representation $k[G]$*
3. *there is an isomorphism of rings*

   $$k[G] \cong \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_m}(D_m),$$

   where $D_1, \cdots, D_m$ are division rings. Furthermore, each D_i contains a field isomorphic to k as a subring of its center and the above isomorphism is k-linear. In particular, $\dim_k(D_i) < \infty$.
4. *m is the number of distinct isomorphism classes of irreducible k-linear representation of G,*
5. *a complete set of isomorphism classes of irreducible representations is given by $M_i = D_i^{n_i}, 1 \leq i \leq m$ and the dimensions of these irreducible representations are $\dim_k(M_i) = n_i \cdot \dim_k(D_i)$,*
6. *the n_j's give the number of times each irreducible representation occurs in the decomposition of the regular representation of G.*
7. $$|G| = n_1^2 \dim_k(D_1) + \cdots + n_m^2 \dim_k(D_m).$$
8. *(Molien's Theorem) if k is algebraically closed, then $D_i = k$ for $1 \leq i \leq m$ thus there exist unique $m; n_1, \ldots n_m$ such that*

   $$k[G] \cong \mathcal{M}_{n_1}(k) \times \cdots \times \mathcal{M}_{n_m}(k)$$
9. *if k is algebraically closed and $n_1, \ldots n_m$ are the dimensions of the irreducible k-linear representations of G then*

   $$|G| = n_1^2 + \cdots + n_m^2.$$

Proof. (1) is a restatement of Maschke's Theorem 2.31.

(2) follows from Proposition 2.40 and Proposition 2.64.

(3)–(6) are restatements of the Artin-Wedderburn theorem. I will comment on some of the additional information. In general, for any ring R and module M, if R contains a field k in its center, then so too does the ring $\mathrm{End}_R(M)$. In detail, for $a \in k$, the map $\lambda_a : M \to M$ defined by $\lambda_a(m) = am$ is an element of the center of $\mathrm{End}_R(M)$ (since $l_a(rm) = arm = ram = l_r(am)$, $l_a(m + m') = a(m + m') = am + am'$, and for $\alpha \in \mathrm{End}_R(M)$ we have $l_a\alpha(m) = a\alpha(m) = \alpha(am) = \alpha l_a(m)$). Moreover, the map $a \mapsto \lambda_a$ is readily seen to be a ring map $k \to \mathrm{End}_R(M)$, and since k is a field this map is injective.

We thus see that each D_i occurring in the Artin-Wedderburn Theorem applied to $k[G]$ contains k in its center. Tracking through the proof, one can check that the isomorphism

$$k[G] \cong \mathcal{M}_{n_1}(D_1) \times \cdots \times \mathcal{M}_{n_m}(D_m)$$

is indeed k-linear. Since $\dim_k(k[G]) = |G| < \infty$, we must have $\dim_k(D_i) < \infty$ for all i.

Statement (5) follows by the observation at the end of the proof of the Artin-Wedderburn Theorem that $M_i \cong D_i^{n_i}$. Taking vector space dimension yields $\dim_k(M_i) = n_i \cdot \dim_k(D_i)$.

(7) follows by computing k-vector space dimension for both sides of the isomorphism displayed in (6).

For (8) recall that $D_i \cong \mathrm{End}_{k[G]}(M_i)^{op}$ where M_i are irreducible representations that are finite dimensional k-vector spaces. We show that $\mathrm{End}_{k[G]}(M_i) \cong k$ by showing that any endomorphism

$$\theta \in \mathrm{End}_{k[G]}(M_i) \text{ is given by } \theta(v) = \lambda v \text{ for some } \lambda \in k \text{ and for all } v \in V.$$

Indeed, consider θ as a k-linear transformation on M_i. Then θ has an eigenvalue $\lambda \in k$ since k is algebraically closed. Then $(\theta - \lambda\mathrm{id}_{M_i}) : M_i \to M_i$ is a $k[G]$-linear endomorphism of M_i which is not injective, so by Schur's Lemma $\theta - \lambda\mathrm{id}_{M_i} = 0$, i.e. $\theta = \lambda\mathrm{id}_{M_i}$.

(9) follows by computing k-vector space dimension for both sides of the isomorphism displayed in (8). □

October 16, 2020

Corollary 2.69. *If R is a commutative semisimple ring then R is a product of fields. In particular, if G is a finite abelian group and k is a field such that $\mathrm{char}(k) \nmid |G|$ then $k[G]$ is a product of fields.*

Proof. Studying the Artin-Wedderburn decomposition of R we see that R is commutative if and only if $n_i = 1$ and D_i is a field for $1 \leq i \leq m$. □

Let's see Theorem 2.68 in action. For our examples will need the following

Lemma 2.70. *Given two group homomorhisms $\rho_1, \rho_2 : G \to k^\times = GL_1(k)$, the associated $k[G]$-modules $M_1 = k$ and $M_2 = k$ are isomorphic if and only if $\rho_1 = \rho_2$. Hence M_1 and M_2 are isomorphic as G-representations if and only if $\rho_1 = \rho_2$*

Proof. For the first assertion, let $\alpha : M_1 \to M_2$ be any homomorphism of $k[G]$-modules. As a k-vector space, each M_i is just k and since α is k-linear, there is a $c \in k$ such that we have $\alpha(x) = cx$ for all $x \in M_1 = k$. Let $g \in G$ be such that $\rho_1(g) \neq \rho_2(g)$. Then we obtain a contradiction

$$c\rho_1(g) = \alpha(g \cdot_{M_1} 1) = g \cdot_{M_2} \alpha(1) = \rho_2(g)c = c\rho_2(g).$$

□

Lemma 2.71. *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 $x \in D \setminus \mathbb{R}$. Then $\mathbb{R} \subsetneq \mathbb{R}[x] \subseteq D$, and since $\mathbb{R}[x]$ is an $\mathbb{R}$ vector space we see that $\mathbb{R}[x] = D$ by a dimension argument. Hence D is commutative and thus D is a field. Since D is an algebraic extension of $\mathbb{R}$ it is contained in the algebraic closure of $\mathbb{R}$, which is $\mathbb{C}$. Thus we have $\mathbb{R} \subsetneq D \subseteq \mathbb{C}$, which yields $D = \mathbb{C}$ for dimension reasons. □

Example 2.72. 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 $\mathbb{R}[S_3]$.

As with any group G and field k, the one dimensional ones are given by group homomorphisms of the form $S_3 \to \mathbb{R}^\times$, and any such map factors as

$$S_3 \twoheadrightarrow S_3^{ab} \to \mathbb{R}^\times.$$

Note that $S_3^{ab} = S_3/A_3 \cong C_2$ and there are two group homomorophisms $\rho_1, \rho_2 : C_2 \to \mathbb{R}^\times$, 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 according to the sign rule: $\sigma \cdot z = \mathrm{sgn}(\sigma)z$. These are the trivial representation and the sign representation, respectively. It is easy to see that these are not isomorphic cf. Lemma 2.70 since $\rho_1 \neq \rho_2$.

These two one dimensional representations must correspond to two factors of $\mathbb{R}$ in the AW decomposition:

$$\mathbb{R}[S_3] \cong \mathbb{R} \times \mathbb{R} \times ??.$$

Recall that $S_3 = D_6$ acts on $\mathbb{R}^2$ by rotations and reflections. We have shown that $\mathbb{R}^2$ is an irreducible representation with respect to this action. We call this representation $M_3 = \mathbb{R}^2$. So $2 = \dim(M_3) = n_3 \cdot \dim_{\mathbb{R}}(D_3)$. We have two possibilities:

1. $n_3 = 2, D_3 = \mathbb{R}$ in which case we obtain the AW decomposition

$$\mathbb{R}[S_3] \cong \mathbb{R} \times \mathbb{R} \times \mathcal{M}_2(\mathbb{R}).$$

2. $n_3 = 1, \dim_{\mathbb{R}}(D_3) = 2$ which yields by Lemma 2.71 that $D_3 \cong \mathbb{C}$ and in which case we obtain the AW decomposition

$$\mathbb{R}[S_3] \cong \mathbb{R} \times \mathbb{R} \times \mathbb{C} \times ??$$

By dimension counting we see that ?? must be a divison ring D_4 such that $\dim_R(D_4) = 2$, hence $D_4 \cong \mathbb{C}$. But this gives $\mathbb{R}[S_3] \cong \mathbb{R} \times \mathbb{R} \times \mathbb{C} \times \mathbb{C}$, which is a contradiction since $\mathbb{R}[S_3]$ is not commutative whereas the product of fields on the right of the isomorphism is commutative.

Thus case 2 is impossible and we have found the AW decomposition

$$\mathbb{R}[S_3] \cong \mathbb{R} \times \mathbb{R} \times \mathcal{M}_2(\mathbb{R}).$$

Furthermore, we have found all isomorphism classes of irreducible representations: any irreducible $\mathbb{R}$-linear representation of S_3 is isomorphic to the trivial representation M_1 or the sign representation M_2 or the *standard representation* M_3.

Example 2.73. 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

$$A_4 \twoheadrightarrow A_4^{ab} \cong C_3 \to \mathbb{C}^\times$$

and thus there are three non-isomorphic 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

$$\mathbb{C}[A_4] \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathcal{M}_{n_4}(\mathbb{C}) \times \cdots \times \mathcal{M}_{n_m}(\mathbb{C}).$$

where $n_3, \ldots, n_m \geq 2$ because we have already found all the 1-dimensional representations ($n_i = 1$) above. Counting dimensions we obtain

$$12 = 1 + 1 + 1 + \sum_{i=3}^{m} {n_i}^2.$$

It is easy to see there is only one solution $m = 3$ and $n_3 = 3$. Hence there is a unique up to isomorphism $|C$-linear irreducible representation of A_4 which is a 3 dimensional $\mathbb{C}$-vector space. We give an example of such a representation: let A_4 act on $V = \mathbb{C}^4$ by permuting the standard basis elements and thus the coordinates of any vector in V. We see that the vector subspace

$$W = \{(a, a, a, a) \mid a \in \mathbb{C}\} \cong \mathbb{C}$$

is invariant under this action, hence a subrepresentation of V. It follows that the quotient vector space V/W is also a $\mathbb{C}$-linear representation of A_4 and $\dim_{\mathbb{C}}(V/W) = 3$.

October 19, 2020

2.3 Character theory

2.3.1 Characters

Definition 2.74. Assume that k is a field and V is a k-linear representation of a group G via the group homomorphism $\rho : G \to \mathrm{GL}(V)$. The *character* χ_V of the representation V is the function $\chi : G \to k$ given by

$$\chi_V(g) = \mathrm{trace}(\rho(g)), \text{ for each } g \in G.$$

The dimension of V, $\dim_k V$, is called the *degree* of the character.

Example 2.75. Below is the character of the standard representation of $S_3 = D_6$ acting on $\mathbb{R}^2$. The leftmost arrows represent the map $\rho : S_3 \to GL_2(\mathbb{R})$ and the rightmost arrows represent the character function $g \mapsto \chi(g)$.

$$\begin{array}{ccccc}
() & \mapsto & \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} & \mapsto & 2 \\
(1,2) & \mapsto & \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} & \mapsto & 0 \\
(1,3) & \mapsto & \begin{bmatrix}-1 & 0\\ -1 & 1\end{bmatrix} & \mapsto & 0 \\
(2,3) & \mapsto & \begin{bmatrix}1 & -1\\ 0 & -1\end{bmatrix} & \mapsto & 0 \\
(1,2,3) & \mapsto & \begin{bmatrix}0 & -1\\ 1 & -1\end{bmatrix} & \mapsto & -1 \\
(1,3,2) & \mapsto & \begin{bmatrix}-1 & 1\\ -1 & 0\end{bmatrix} & \mapsto & -1
\end{array}$$

We often write the values of the character as a vector: for the character above we would write

$$\chi = (2, 0, 0, 0, -1, -1).$$

Note that the values of the character are the same for all 2-cycles and separately for all 3-cycles. This is not a coincidence but a consequence of the fact that all cycles of a given length in S_n belong to the same conjugacy class.

Lemma 2.76. *The character of a finite representation of a group G is constant on each conjugacy class of G.*

Proof. Suppose $g' = hgh^{-1}$ in G. Then $\rho(G') = \rho(h)\rho(g)\rho(h)^{-1}$ in $GL(V)$, i.e. $\rho(g')$ and $\rho(g)$ are conjugate matrices. But conjugate matrices have the same trace ($\mathrm{trace}(PAP^{-1}) = \mathrm{trace}(A)$) thus

$$\chi_V(g') = \mathrm{trace}(\rho(g')) = \mathrm{trace}(\rho(h)\rho(g)\rho(h)^{-1}) = \mathrm{trace}(\rho(g)) = \chi_V(g).$$

□

Thus we can summarize the character by just writing values for one representative of each conjugacy class. We will see later that the character is constant also on each isomorphism class of representations. This leads to forming a character table.

Definition 2.77. The *character table* of a group G is a table whose rows are indexed by the isomorphism types of simple representations of G, whose columns are indexed by the conjugacy classes of G and whose entries are the values of the characters of the simple representations on representatives of the conjugacy classes.

It is usual to index the first column of a character table by the (conjugacy class of the) identity, and to put the character of the trivial representation as the top row. With this convention the top row of every character table will be a row of 1's.

Example 2.78. The character table for S_3 is the following:

g	$e = ()$	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Above χ_1, χ_2, χ_3 denote the characters of the trivial, sign, and standard representations respectively.

We will see that the character table has remarkable properties, among which are that it is always square, and its rows (and also its columns) satisfy certain orthogonality relations. Our next main goal is to state and prove these results. To do this, we need a few ways of constructing new representations from old.

Definition 2.79. Given a commutative ring R and R-modules M, N that are R-linear representations of a group G then the following are also R-linear representations of G:

- $M \oplus N$ with action $g \cdot (m, n) = (g \cdot m, g \cdot n)$ – the *direct sum representation*
- $M \otimes_R N$ with action $g \cdot \sum_i m_i \otimes n_i = \sum_i (g \cdot m_i) \otimes (g \cdot n_i)$ the *tensor product representation*
- $\mathrm{Hom}_R(M, N)$ with action $(g \cdot f)(m) = g \cdot f(g^{-1}m)$
- $M^* = \mathrm{Hom}_R(M, R)$ with action $(g \cdot f)(m) = f(g^{-1}m)$ –the *dual* or *contragradient representation*

October 19, 2020

Here are a few properties for characters:

Proposition 2.80. *Let V, M, N be finite dimensional k-linear representations of a group G or, equivalently, $k[G]$-modules. Then*

(1) $\chi(e_G) = (\dim_k V) \cdot 1_k$

(1') *if* $\mathrm{char}(k) = 0$ *then* $\chi(e_G) = \dim_k V$.

(2) *if* M *and* N *are isomorphic representations then* $\chi_M = \chi_N$

(3) $\chi_{M \oplus N} = \chi M + \chi N$

(4) $\chi_{M \otimes_R N} = \chi M \cdot \chi N$

(5) $\chi_{V^*}(g) = \chi_V(g^{-1})$ *for all* $g \in G$.

(5') *If* $k = \mathbb{C}$ *and* G *is finite, then* $\chi_{V^*}(g) = \chi_V(g^{-1}) = \overline{\chi_V(g)}$ *for all* $g \in G$, *where the overline denotes complex conjugate.*

(6) $\chi_{\mathrm{Hom}_R(M,N)} = \chi_{M^*} \cdot \chi_N$.

(6') *If* $k = \mathbb{C}$ *and* G *is finite, then* $\chi_{\mathrm{Hom}_R(M,N)} = \overline{\chi_M} \cdot \chi_N$

Proof. I only prove parts (1) and (2) and partially (5), leaving the rest as exercises.

(1) The map $\rho : G \to GL_{\dim_k V}(k)$ takes e_G to the identity matrix $I_{\dim_k V}$. The trace of this matrix is $(\dim_k V) \cdot 1_k$.

(2) Suppose that M and N are the representations of G given by $\rho_M : G \to \mathrm{Aut}_R(M)$, $\rho_N : G \to \mathrm{Aut}_R(N)$ and there is a G-equivariant isomorphism of R-modules $\alpha : M \to N$. Then we have $\alpha\rho_M(g) = \rho_N(g)\alpha$ for all $g \in G$, thus

$$\chi_N(g) = \mathrm{trace}\,\rho_N(g) = \mathrm{trace}(\alpha\rho_M(g)\alpha^{-1}) = \mathrm{trace}\,\rho_M(g) = \chi_M(g).$$

(5') Taking $\chi_{V^*}(g) = \chi_V(g^{-1})$ granted by (5), let's prove the second assertion. If G is finite and $\rho : G \to \mathrm{GL}(V)$ gives the representation V, then $\rho(g)^n = \mathrm{id}_V^*$ for $n = |g|$, the order of g. It follows that the eigenvalues of $\rho(g)$ are n-th roots of unity and hence $\lambda_i^{-1} = \overline{\lambda_i}$ for each eigenvalue λ_i. Now we compute

$$\chi_{V^*}(g) = \chi_V(g^{-1}) = \mathrm{trace}(\rho(g)^{-1}) = \sum_{i=1}^{\dim(V)} \lambda_i^{-1} = \sum_{i=1}^{\dim(V)} = \overline{\lambda_i} = \overline{\mathrm{trace}(\rho(g))} = \overline{\chi_V(g)}.$$

(6') follows from (5') and (6).

□

2.3.2 Orthogonality relations and character tables

Definition 2.81. A *class function* on a group G with values in a field k is a function $f : G \to k$ that is constant on each conjugacy class of G. The set of class functions is denoted $k^{cc(G)}$.

By Lemma 2.76, characters of representations of G are class functions.

Remark 2.82. The set of class functions $k^{cc(G)}$ is a k-vector space with respect to addition of functions and scalar multiplication of functions by complex numbers. Its dimension is equal to the number of conjugacy classes of G.

This vector space is endowed with a bilinear form by means of

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1}).$$

We restrict now to *complex* representations, that is, $k = \mathbb{C}$ of finite groups G.

If $k = \mathbb{C}$ then the bilinear form above is in fact an inner product, and even more, a Hermitian form and is given by

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)}.$$

Definition 2.83. A *Hermitian inner product* on a complex vector space V is a complex-valued bilinear form $\langle -, - \rangle : V \times V \to \mathbb{C}$ which is antilinear in the second slot, and is positive definite. That is, it satisfies the following properties, for all $u, v \in V$ and $\alpha \in \mathbb{C}$, where $\overline{z}$ denotes the complex conjugate of z.

1. $< u + v, w >=< u, w > + < v, w >$
2. $< u, v + w >=< u, v > + < u, w >$
3. $< \alpha u, v >= \alpha < u, v >$
4. $< u, \alpha v >= \overline{\alpha} < u, v >$
5. $< u, v >= \overline{< v, u >}$
6. $< u, u >\geq 0$, with equality only if $u = 0$. (Note that $< u, u >\in \mathbb{R}$ by 5.)

The theory of vector spaces endowed with inner products tells us that an orthonormal basis must exist for the vector space $\mathbb{C}^{cc(G)}$ with respect to the inner product defined above. We now give an explicit description of such a basis.

Theorem 2.84 (Row orthogonality relations)**.** *Let G be a finite group and k an algebraically closed field such that $|G| \in k^\times$. If V, W are irreducible k-linear representations of G with characters χ_V, χ_W then*

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & \textit{if } V \cong W \\ 0 & \textit{otherwise.} \end{cases}$$

To prove this we need to make a few definitions.

Definition 2.85. Let G be a group, R a ring, and let M be an R-linear representation of G. The invariant submodule of M is $M^G = \{m \in M \mid g \cdot m = m, \ \forall g \in G\}$.

Lemma 2.86. *Let G be a finite group, k a field such that* $\mathrm{char}(k) \nmid |G|$, *and let M be a k-linear representation of G. The inclusion $M^G \hookrightarrow M$ is a split $k[G]$-module map, with splitting given by*

$$\phi : M \to M^G, \ \phi(m) = \frac{1}{|G|} \sum_{g \in G} g \cdot m$$

Proof. Homework. □

Proof of Theorem 2.84. Let $M = \mathrm{Hom}_k(V, W)$, which is a k-linear representation of G as described in Definition 2.79. I claim that $M^G = \mathrm{Hom}_{k[G]}(V, W)$. Denote $N = \mathrm{Hom}_{k[G]}(V, W)$. It is clear that N is a k-linear subspace of M. We show that N is fixed by the action of G on M. This will show both that N is a $k[G]$ module and that $N = M^G$. Indeed, let $f \in N$ and $g \in G$ then, utilizing that f commutes with the G action, we have

$$(g \cdot f)(v) = g \cdot f(g^{-1} \cdot v) = g \cdot g^{-1} \cdot f(v) = f(v), \ \forall v \in V.$$

From Lemma 2.86 we conclude that $M \cong M^G \oplus M/M^G$ and

$$\frac{1}{|G|} \sum_{g \in G} g|_{M^G} = \mathrm{id}_{M^G} \quad \text{whereas } \frac{1}{|G|} \sum_{g \in G} g|_{M/M^G} = 0$$

and thus trace $\left(\frac{1}{|G|} \sum_{g \in G} \rho(g)\right) = \mathrm{trace}(\mathrm{id}_{M^G}) = \dim_k M^G$. However,

$$\begin{aligned}
\mathrm{trace}\left(\frac{1}{|G|} \sum_{g \in G} \rho(g)\right) &= \frac{1}{|G|} \sum_{g \in G} \mathrm{trace}(\rho(g)) = \frac{1}{|G|} \sum_{g \in G} \chi_M(g) \\
&= \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{Hom}_k(V,W)}(g) = \frac{1}{|G|} \sum_{g \in G} \chi_V(g)\overline{\chi_W(g)} \\
&= \langle \chi_V, \chi_W \rangle
\end{aligned}$$

Combining everything obtained so far with Schur's Lemma we have

$$\langle \chi_V, \chi_W \rangle = \dim_k M^G = \dim_k \mathrm{Hom}_{k[G]}(V, W) = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{otherwise.} \end{cases}$$

Above we have used the fact that if $V \ncong W$ then $\mathrm{Hom}_{k[G]}(V, W) = 0$ by Schur's Lemma and if $V \cong W$ then $\mathrm{Hom}_{k[G]}(V, W) = \mathrm{End}_{k[G]}(V) \cong k$ as in the proof of part (8) of Theorem 2.68. □

October 23, 2020

Corollary 2.87. *Let G be a finite group and let $\chi_1, \ldots, \chi_m$ be the characters corresponding to a complete set of representatives for the irreducible complex representations of G. Then $\{\chi_1, \ldots, \chi_m\}$ is an orthonormal basis for the vector space spanned by all characters of G.*

Proof. We see that $\{\chi_1, \ldots, \chi_m\}$ is a spanning set because every representation can be decomposed as a sum of irreducible representations. By Proposition 2.80 (3) then every character can be written as a linear combination of irreducible characters.

Theorem 2.84 gives linear independence and orthonormality. □

We are now able to show that the character determines the representation up to isomorphism type:

Proposition 2.88. *Let G be a finite group and let k be an algebraically closed field of characteristic 0. Then M and N are isomorphic finite dimensional representations of G if and only if $\chi_M = \chi_N$.*

Proof. Let a complete set of representatives of isomorphism classes of irreducible G-representations be given by $V_1, \ldots, V_m$ and consider decompositions

$$M \cong V_1^{r_1} \oplus \cdots \oplus V_m^{r_m} \qquad N \cong V_1^{s_1} \oplus \cdots \oplus V_m^{s_m}.$$

Then $\langle \chi_M, \chi_{V_i} \rangle = r_i$ and $\langle \chi_N, \chi_{V_i} \rangle = s_i$. Thus

$$\begin{aligned} \chi_M = \chi_N \quad &\Longleftrightarrow \quad \langle \chi_M, \chi_{V_i} \rangle = \langle \chi_N, \chi_{V_i} \rangle, \ \forall i \\ &\Longleftrightarrow \quad r_i = s_i, \ \forall i \ \Longleftrightarrow \ M \cong N. \end{aligned}$$

□

Constructing character tables

We will use the technique of lifting representations from quotient groups.

Lemma 2.89. *If H is a normal subgroup of a group G, $q : G \to G/H$ is the quotient map and $\overline{\rho} : G/H \to \mathrm{Aut}_k(V)$ is a group homomorphism making a k-vector space V into a k-linear representation of G/H, then $\rho = \overline{\rho} \circ q : G \to \mathrm{Aut}_k(V)$ makes V into a k-linear representation of G. Furthermore the representation given by ρ is irreducible if and only if the representation given by $\overline{\rho}$ is irreducible.*

Proof. Exercise. □

Example 2.90. We compute the character table for complex representations of the Klein four group

$$G = C_2 \times C_2 = \{e, a, b, c\}.$$

Since the group is abelian, each element is a separate conjugacy class. We now determine the isomorphism types of irreducible representations.

Set $V_1 = \mathbb{C}$ to be the trivial representation.

Each of the elements a, b, c generates a normal subgroup H isomorphic to C_2 such that $G/H \cong C_2$. For example, if $H = \langle a \rangle$ then $G/H = \{\overline{e} = \overline{a}, \overline{b} = \overline{c}\} \cong C_2$. There are only two isomorphism types of irreducible representations of $C_2 = S_2$ and they are both 1-dimensional: the trivial representation and the sign representation. Let's take $\overline{\rho} : G/H \to (\mathbb{C}^\times, \cdot)$ to be the sign representation $\overline{\rho}(\overline{e}) = \overline{\rho}(\overline{a}) = 1, \overline{\rho}(\overline{b}) = \overline{\rho}(\overline{c}) = -1$. By Lemma 2.89, this lifts to a unique irreducible 1-dimensional representation $V_2 = \mathbb{C}$ with action of G given by $\rho(e) = \rho(a) = 1, \rho(b) = \rho(c) = -1$.

We get two more irreducible representations $V_3 = \mathbb{C}$ and $V_4 = \mathbb{C}$ by lifting the sign representations from $G/\langle b \rangle$ and $G/\langle c \rangle$ respectively. At this point we have found all the irreducible representations because the sum of squares of the dimensions of V_i is $1^2 + 1^2 + 1^2 + 1^2 = 4 = |G|$.

Denote the character of V_i by χ_i. Then the character table of the Klein four group is

	e	a	b	c
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1.

Example 2.91. We compute the character table for complex representations of the quaternion group

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

The conjugacy classes of Q_8 are $\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}$ and $\{\pm k\}$. Since $H = Z(Q_8) = \{\pm 1\}$ is a normal subgroup, and Q_8/H is isomorphic to the Klein four group, we can lift the characters from the previous example.

This yields four characters as follows:

	1	-1	$\pm i$	$\pm j$	$\pm k$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1

Because the above four representations have dimension 1 and their characters are distinct they are not pairwise isomorphic; see Lemma 2.70. However we have not found all the isomorphism types of irreducible representations of Q_8 because $1^2+1^2+1^2+1^2 = 4 < 8 = |Q_8|$. In fact we see that in order to have equality we must add a a 2-dimensional representation $1^2 + 1^2 + 1^2 + 1^2 + 2^2 = 8 = |Q_8|$. Denote χ_5 the character of this 2-dimensional representation.

The row orthogonality relations applied to the table below

	1	-1	$\pm i$	$\pm j$	$\pm k$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	x	y	z	$w,$

yield

$$\begin{cases} 2+\overline{x}+2\overline{y}+2\overline{z}+2\overline{w}=0 \\ 2+\overline{x}+2\overline{y}-2\overline{z}-2\overline{w}=0 \\ 2+\overline{x}-2\overline{y}+2\overline{z}-2\overline{w}=0 \\ 2+\overline{x}-2\overline{y}-2\overline{z}+2\overline{w}=0 \end{cases}$$

with unique solution $x=-2$, $y=z=w=0$.

Example 2.92. We compute the character table for complex representations of the dihedral group D_8. This is entirely analogous to Q_8: the center of D_8, $Z(D_8)=\{1,r^2\}$, has order two and the quotient of D_8 by its center is isomorphic to the Klein four group. Since these were the only facts we used in the previous example along with $|Q_8|=|D_8|=8$, the same arguments apply verbatim to show that the character table of Q_8 is also

	$\{1\}$	$\{r^2\}$	$\{r,r^3\}$	$\{l,lr^2\}$	$\{lr,lr3\}$
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	$0.$

Remark 2.93. The above examples show that it is possible for two non-isomorphic groups to have the same character table.

Chapter 3

Homological algebra

October 26, 2020

Homological algebra is the study of homology - a measure for the non exactness of chain complexes which we shall define below.

3.1 Chain complexes and their homology

3.1.1 The category of chain complexes of R-modules

Let's define "chain complex" carefully.

Definition 3.1. For a ring R, a *chain complex of left R-modules* is a pair consisting of

- a family of left R-modules indexed by $\mathbb{Z}$, $\{M_i\}_{i\in\mathbb{Z}}$ (M_i is in *homological degree* i)
- 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.

Example 3.2. 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 $i \notin \{0, 1, 2\}$.

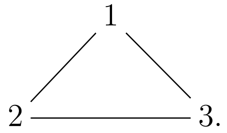
Example 3.3. For those who have taken (or will take) a course in algebraic topology, given a topological space X, we form a chain complex $C_\bullet(X) := C_\bullet(X;\mathbb{Z})$ over the ring $\mathbb{Z}$, called the *singular chain complex* associated to X, as follows.

- 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. (That is, $\Delta^n := \{(r_0, \dots, r_n) \in \mathbb{R}^{n+1} \mid r_i \geq 0, \sum_i r_i = 0\}$.) 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 $(r_0, \dots, r_{n-1}) \mapsto (r_0, \dots, r_{i-1}, 0, r_i, \dots, r_{n-1})$.

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 $C_n(X)$ = the free $\mathbb{Z}$ module with basis given by the n-dimensional simplices of X and $d_n : C_n(X) \to C_{n-1}(X)$ is given by sending an n-simplex $\{r_0, \dots, r_{n-1}\}$ to $d_n(\{r_0, \dots, r_{n-1}) = \sum_{i=0}^n (-1)^i \{r_0, \dots, \hat{r_i}, \dots, R_n\}$ 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 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 3.4. 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 $d_i^N \circ f_i = f_{i-1} \circ d_i^M$ 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

$$\begin{tikzcd}
\cdots \arrow[r] & M_{i+1} \arrow[r] \arrow[d] & M_i \arrow[r] \arrow[d] & M_{i-1} \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & N_{i+1} \arrow[r] & N_i \arrow[r] & N_{i-1} \arrow[r] & \cdots
\end{tikzcd}$$

in which both rows are complexes and all squares commute.

Example 3.5. 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 3.6. 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.

Theorem 3.7. *For any ring R, chain complexes and chain maps of left R-modules form an additive category, written $\langle\langle R\text{-complexes}\rangle\rangle$.*

- *The rule for adding morphisms is $(f + g)_i = f_i + g_i$.*
- *The rule for composing morphisms is given by component-wise composition: $(f \circ g)_i := f_i \circ g_i$.*
- *The 0 object is the chain complex consisting entirely of 0 modules with 0 differential.*
- *Products in this category are given by direct sums of complexes, which are formed componentwise, i,e, for the family of 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 $d_i^M \oplus d_i^N = \left[\begin{array}{c|c} d_i^M & 0 \\ \hline 0 & d_i^N \end{array}\right] : M_i \oplus N_i \to M_{i+1} \oplus N_{i+1}$.*

In fact, $\langle\langle R\text{-complexes}\rangle\rangle$ is what's known as an *abelian category.* I will not define this term carefully, but basically such a category behaves like the category of S-modules for a ring S in that there are notions of kernel, cokernel, etc. and the first, second, third isomorphism theorems and similar results hold.

The kernel of a chain map $f : (M_\bullet, d^M) \to (N_\bullet, d^N)$ is the complex for which the module indexed by i is $\mathrm{Ker}(f_i)$ and whose differential is induced from d^M by $d_i^M|_{\mathrm{Ker}(f_i)}$, and similarly for images and cokernels.

We can define exact sequences in any abelian category and we shall do so in $\langle\langle R\text{-complexes}\rangle\rangle$.

Definition 3.8. 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 s.e.s. of chain complexes is a commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
\cdots \arrow[r] & M'_{i+1} \arrow[r] \arrow[d] & M'_i \arrow[r] \arrow[d] & M'_{i-1} \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & M_{i+1} \arrow[r] \arrow[d] & M_i \arrow[r] \arrow[d] & M_{i-1} \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & M''_{i+1} \arrow[r] \arrow[d] & M''_i \arrow[r] \arrow[d] & M''_{i-1} \arrow[r] \arrow[d] & \cdots \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

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.)

October 28, 2020

3.1.2 Snake lemma

Proposition 3.9 (Snake Lemma). *For a ring R, suppose*

$$\begin{tikzcd}
 & M' \arrow[r, "i"] \arrow[d, "f'"] & M \arrow[r, "p"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "j"] & N \arrow[r, "q"] & N'' &
\end{tikzcd}$$

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

$$\mathrm{Ker}(f') \overset{i|}{\to} \mathrm{Ker}(f) \overset{p|}{\to} \mathrm{Ker}(f'') \overset{\partial}{\to} \mathrm{coker}(f') \overset{\bar{j}}{\to} \mathrm{coker}(f) \overset{\bar{q}}{\to} \mathrm{coker}(f'').$$

which can be visualized in relation to the previous diagram as follows

$$\begin{tikzcd}
 & \mathrm{Ker}(f') \arrow[r, "i|"] \arrow[d] & \mathrm{Ker}(f) \arrow[r, "p|"] \arrow[d] & \mathrm{Ker}(f'') \arrow[d] \arrow[dddll, rounded corners, "\partial"] & \\
 & M' \arrow[r, "i"] \arrow[d, "f'"] & M \arrow[r, "p"] \arrow[d, "f"] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "j"] \arrow[d] & N \arrow[r, "q"] \arrow[d] & N'' \arrow[d] & \\
 & \mathrm{coker}(f') \arrow[r, "\overline{j}"] & \mathrm{coker}(f) \arrow[r, "\overline{q}"] & \mathrm{coker}(f'') &
\end{tikzcd}$$

Above $i|$ and $p|$ denote the restrictions of i and p to $\mathrm{Ker}(f)$ *and* $\mathrm{Ker}(g)$ *respectively and $\overline{j}$ and $\overline{q}$ are the quotients of j and q. E.g., the map $\overline{q} : \mathrm{coker}(f) \to \mathrm{coker}(f'')$ sends $\overline{q}(n + \mathrm{Im}(f)) = q(n) + \mathrm{Im}(f'')$.*

The map ∂ is given as follows: For $m'' \in \mathrm{Ker}(f'')$, pick $m \in M$ such that $p(m) = m''$. Such an m exists, but is not unique, since p is onto. Then $qf(m) = 0$ and hence $f(m) = j(n')$ for a (unique, since j is injective) element $n' \in N'$. We set

$$\partial(m) = n' + \mathrm{Im}(f') \in \mathrm{coker}(f').$$

Moreover, if i is injective then $i|$ is injective and if q is surjective then $\overline{q}$ is surjective. When both of these hold, they lead to an exact sequence

$$0 \to \mathrm{Ker}(f') \xrightarrow{i|} \mathrm{Ker}(f) \xrightarrow{p|} \mathrm{Ker}(f'') \xrightarrow{\partial} \mathrm{coker}(f') \xrightarrow{\overline{j}} \mathrm{coker}(f) \xrightarrow{\overline{q}} \mathrm{coker}(f'') \to 0.$$

Proof. One needs to show:

- well-definedness of $i|$ and $p|$, specifically the fact that the images of these maps land in $\mathrm{Ker}(f)$ and $\mathrm{Ker}(f'')$ respectively.

To show this for $i|$, consider $u \in \mathrm{Ker}(f')$. Then $i|(u) = i(u)$ and $f(i(u)) = j(f'(u)) = j(0) = 0$ by the commutativity of the given diagram. Thus $i|(u) \in \mathrm{Ker}(f)$ as desired.

- well-definedness of $\overline{j}$ and $\overline{q}$, specifically independence of coset representative.

To show this for $\overline{j}$, consider $n - \tilde{n} \in \mathrm{Im}(f)$. Then we have $q(n) - q(\widetilde{(n)}) = q(n - \tilde{n}) \in q(\mathrm{Im}(f)) = f''(\mathrm{Im}(p)) \subseteq \mathrm{Im}(f'')$ yields that $\overline{q}(n + \mathrm{Im}(f)) = q(n) + \mathrm{Im}(f'') = q(\widetilde{(n)}) + \mathrm{Im}(f'') = \overline{q}(\tilde{n} + \mathrm{Im}(f))$.

- well-definedness of ∂

(See Jill Clayborn in the opening scene from *It's My Turn* https://www.youtube.com/watch?v=etbcKWEKnvg explaining the construction of the map ∂ and the proof of why it's well-defined (independent of the choice of m), given below based on some not-at-all annoying questioning from a student.)

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 it is an R-map is proven similarly.

- exactness of the six-term sequence

The proof that the six-term sequence is indeed an exact sequence is tedious (although no one step is difficult), and I'm going to skip most of it. Let's just show that $\operatorname{Im}(p|) = \operatorname{Ker}(\partial)$:

If $m'' \in \operatorname{Ker}(f'')$ satisfies $m' = p(x)$ for some $x \in \operatorname{Ker}(f)$, then in the construction of ∂ we may take $m = x$ and it follows that $f(m) = 0$ and hence $\partial(m') = 0$. This proves $\operatorname{Im}(p|) \subseteq \operatorname{Ker}(f'')$. If $\partial(m'') = 0$, then in the construction $n' = f'(m')$ for some 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.

The "moreover" part of the statement is clear since $i|$ and $\overline{q}$ are obtained from i and q respectively. □

The snake lemma is very useful in computing homology leading to the long exact sequence in Theorem 3.18.

October 30, 2020

3.1.3 Homology of a chain complex

Definition 3.10. 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

$$H_i(M_\bullet) = H_i(M_\bullet, d) := \frac{\operatorname{Ker}(d_i : M_i \to M_{i-1})}{\operatorname{Im}(d_{i+1} : M_{i+1} \to M_i)}$$

for $i \in \mathbb{Z}$. We also give names to the modules in the numerator and denominator above

$$Z_i := \operatorname{Ker}(d_i : M_i \to M_{i-1}) \text{ is called the module of } i\text{-cycles}$$

$$B_i := \operatorname{Im}(d_{i+1} : M_{i+1} \to M_i) \text{ is called the module of } i\text{-boundaries.}$$

Remark 3.11. A chain complex $M_\bullet$ is exact if and only if $H_i(M_\bullet) = 0$ for all i.

Example 3.12. 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 3.13. The homology of a complex with just two non-zero 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 $H_1(M,d) = \operatorname{Ker}(d_1)$.

Example 3.14 (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 3.3 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

$$\begin{aligned} H_1(C_\bullet(X)) &= \operatorname{Ker}(d_1) = \mathbb{Z}(\{1,3\} - \{1,2\} - \{2,3\}) \cong \mathbb{Z} \\ H_0(C_\bullet(X)) &= \operatorname{coker}(d_1) = \frac{\mathbb{Z}\{1\} \oplus \mathbb{Z}(\{1\} + \{2\}) \oplus \mathbb{Z}(\{1\} + \{2\} + \{3\})}{\mathbb{Z}\{1\} \oplus \mathbb{Z}(\{1\} + \{2\})} \\ &\cong \mathbb{Z}(\{1\} + \{2\} + \{3\}) \cong \mathbb{Z}. \end{aligned}$$

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 $\operatorname{Ker}(d_1) = \mathbb{Z}(\{1,3\} - \{1,2\} - \{2,3\})$. Hence $H_1(C_\bullet(Y)) = 0$ since $\operatorname{Ker}(d_1) = \operatorname{Im}(d_2)$ 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.

We see from this example that computing homology can be made into an algorithmic procedure, however it is not something that one would typically want to do by hand. We will turn our attention to alternate methods for computing homology below.

Definition 3.15 (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 $z \in \operatorname{Ker}(d_i : M_i \to M_{i-1})$, we define $H_i(f)(\overline{z}) = \overline{f(z)}$.

Remark 3.16. The function $H_i(f)$ is indeed a well-defined R-map: Note, first of all, that for $z \in \operatorname{Ker}(d_i : M_i \to M_{i-1})$ we have $d_i(f_i(z)) = f_{i-1}(d_i(z)) = f_{i-1}(0) = 0$, and hence $f_i(z) \in \operatorname{Ker}(d_i : N_i \to N_{i-1})$. 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 $y, z \in \operatorname{Ker}(d_i : M_i \to M_{i-1})$, 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.

Next we promote homology to being a functor.

Lemma 3.17. *For each fixed i, $H_i(-)$ is an additive functor*

$$H_i(-) : \langle\langle R\text{-}\mathit{complexes}\rangle\rangle \to \langle\langle {}_R\mathit{Mod}\rangle\rangle .$$

Recall that this means $H_i(f \circ g) = H_i(f) \circ H_i(g)$, $H_i(id) = id$ and $H_i(f \pm f') = H_i(f) \pm H_i(f')$.

Proof. The three formulas listed above follow easily from Definition 3.15. □

November 2, 2020

Long exact sequence in homology

Theorem 3.18 (Long exact sequence in homology)**.** *If $0 \to M'_\bullet \overset{j}{\to} M_\bullet \overset{p}{\to} M''_\bullet \to 0$ 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

$$\begin{tikzcd}
\cdots \arrow[r] & H_i(M'_\bullet) \arrow[r] & H_i(M_\bullet) \arrow[r] & H_i(M''_\bullet) \arrow[dll, "\partial_i" description] \\
& H_{i-1}(M'_\bullet) \arrow[r] & H_{i-1}(M_\bullet) \arrow[r] & H_{i-1}(M''_\bullet) \arrow[dll, "\partial_{i-1}" description] \\
& H_{i-2}(M'_\bullet) \arrow[r] & H_{i-2}(M_\bullet) \arrow[r] & H_{i-2}(M''_\bullet) \arrow[dll, dashed] \\
& H_0(M'_\bullet) \arrow[r] & H_0(M_\bullet) \arrow[r] & H_0(M''_\bullet) \ldots
\end{tikzcd}$$

where the map ∂_i *is defined as follows:*

Given $z \in \operatorname{Ker}(d_i : M''_i \to M''_{i-1})$*, 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,* $u \in \operatorname{Ker}(d_{i-1})$*. 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 consider the following complexes of kernels and cokernels respectively, which are exact by the Snake Lemma

$$0 \to Z_n(M'_\bullet) \to Z_n(M_\bullet) \to Z_n(M''_\bullet)$$

$$M'_n/B_n(M'_\bullet) \to M_n/B_n(M_\bullet) \to M''_n/B_n(M''_\bullet) \to 0$$

- next 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 a follows

$$\begin{tikzcd}
 & M'_n/B_n(M'_\bullet) \arrow[r] \arrow[d, "\overline{d}_n^{M'}"] & M_n/B_n(M_\bullet) \arrow[r] \arrow[d, "\overline{d}_n^{M}"] & M''_n/B_n(M''_\bullet) \arrow[r] \arrow[d, "\overline{d}_n^{M''}"] & 0 \\
0 \arrow[r] & Z_{n-1}(M'_\bullet) \arrow[r] & Z_{n-1}(M_\bullet) \arrow[r] & Z_{n-1}(M''_\bullet) &
\end{tikzcd}$$

- 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

$$H_n(M'_\bullet) \to H_n(M_\bullet) \to H_n(M''_\bullet) \overset{\partial}{\to} H_{n-1}(M'_\bullet) \to H_{n-1}(M_\bullet) \to H_{n-1}(M''_\bullet)$$

  Comparing the description of ∂ given by the Snake Lemma and the description of ∂_n above one sees that these maps are the same.

□

Example 3.19. The long exact sequence in homology is used in topology to compute the homology groups of quotient spaces. Let X be the simplicial complex of Example 3.3 and let A be the subset formed by the three vertices. Then there is an obvious inclusion $A \subseteq X$, which leads to an inclusion of chain complexes $C_\bullet(A) \hookrightarrow C_\bullet(X)$. Ler $D_\bullet$ be the cokernel of this inclusion, leading to a s.e.s of chain complexes

$$0 \to C_\bullet(A) \xrightarrow{i} C_\bullet(X) \xrightarrow{\pi} D_\bullet \to 0.$$

We could compute $D_\bullet$ explicitly and find its homology. Instead, let's compute the homology of $D_\bullet$ by using nothing but the l.e.s. in homology: for $i < 0$ or $i \geq 2$ we have s.e.s

$$0 = H_i(X) \to H_i(D_\bullet) \to H_{i-1}(A) = 0$$

which yield $H_i(D_\bullet) = 0$ for $i \geq 2$ and $i < 0$. Now for the more interesting portion of the l.e.s:

$$0 = H_1(A) \to H_1(X) \to H_1(D_\bullet) \to H_0(A) \xrightarrow{H_0(i)} H_0(X) \to H_0(D_\bullet) \to 0.$$

Substituting the known homology groups for X, A (see Example 3.14) we have:

$$0 \to \mathbb{Z} \to H_1(D_\bullet) \xrightarrow{\partial_1} \mathbb{Z}^3 \xrightarrow{H_0(i)=\begin{bmatrix}1 & 1 & 1\end{bmatrix}} \mathbb{Z} \to H_0(D_\bullet) \to 0.$$

Since the map $H_0(i)$ is surjective, we deduce $H_0(D_\bullet) = 0$. Also the kernel of this map is $K = \mathbb{Z}(\{1\} - \{2\}) \oplus \mathbb{Z}(\{1\} - \{3\}) \cong \mathbb{Z}^2$. By the exactness of the above l.e.s, $K = \operatorname{Im}(\partial_1)$, so we can write a s.e.s.

$$0 \to \mathbb{Z} \to H_1(D_\bullet) \xrightarrow{\partial_1} K \cong \mathbb{Z}^2 \to 0.$$

Finally, since $\mathbb{Z}^2$ is free, hence projective, the s.e.s above splits and yields $H_1(D_\bullet) \cong \mathbb{Z} \oplus \mathbb{Z}^2 \cong \mathbb{Z}^3$.

The importance of this computation to topology is that it recovers the (reduced) homology groups of the quotient space X/A. This is defined as the space obtained from X by collapsing all the points of A to a single point. In our example this results in X/A being a bouquet of 3 circles.

Then the reduced homology groups of X/A (also called the relative homology groups of X with respect to A) are given by $\widetilde{H_i}(X/A) = H_i(X, A) = H_i(D_\bullet) = \begin{cases} \mathbb{Z}^3 & i = 1, \\ 0 & \text{otherwise.} \end{cases}$ Finally, the reduced homology groups relate to the ordinary homology groups by $\widetilde{H_i}(X/A) = \begin{cases} H_0(X/A)/\mathbb{Z} & i = 0, \\ H_i(X/A) & \text{otherwise} \end{cases}$, hence we deduce

$$H_i(X/A) = \begin{cases} \mathbb{Z} & i = 0, \\ \mathbb{Z}^3 & i = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 3.20 (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 $H_{i-1}(M'_\bullet) = \operatorname{Ker}(H_{i-1}(j)) = \operatorname{Im}(\partial_i) = 0$ for any $i \in \mathbb{Z}$. Thus $M'_\bullet$ is exact. □

November 4, 2020

3.1.4 Comparing chain maps through homotopy

Definition 3.21. 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

$$\begin{tikzcd}
\cdots \arrow[r] & M_{i+1} \arrow[r] \arrow[d] \arrow[dl] & M_i \arrow[r] \arrow[d, "f_i-g_i"] \arrow[dl, "h_i"'] & M_{i-1} \arrow[r] \arrow[d] \arrow[dl] & \cdots \arrow[dl] \\
\cdots \arrow[r] & N_{i+1} \arrow[r] & N_i \arrow[r] & N_{i-1} \arrow[r] & \cdots .
\end{tikzcd}$$

The squares commute but the triangles do not. Rather, the sum of the two compositions in each rhombus

$$\begin{tikzcd}
 & \bullet \arrow[r] \arrow[dl] & \bullet \arrow[dl] \\
\bullet \arrow[r] & \bullet &
\end{tikzcd}$$

occuring in this diagram is equal to the difference of f and g.

Example 3.22. 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 3.23. I claim the chain map pictured below is null homotopic:

$$\begin{tikzcd}
\cdots \arrow[r] & 0 \arrow[r] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d, "17"] & 0 \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & \mathbb{Z} \arrow[r, "17"] & \mathbb{Z} \arrow[r] & 0 \arrow[r] & \cdots
\end{tikzcd}$$

A null-homotopy is given by the diagram

$$\begin{tikzcd}
\cdots \arrow[r] & 0 \arrow[r] \arrow[d] \arrow[dl] & \mathbb{Z} \arrow[r] \arrow[d, "17"] \arrow[dl, "1"'] & 0 \arrow[r] \arrow[d] \arrow[dl] & \cdots \\
\cdots \arrow[r] & \mathbb{Z} \arrow[r, "17"] & \mathbb{Z} \arrow[r] & 0 \arrow[r] & \cdots
\end{tikzcd}$$

The main point of chain homotopy is given by the following result:

Proposition 3.24. *Homotopic chain maps induced 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 $z \in \operatorname{Ker}(d_i : M_i \to M_{i-1})$. 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 $f(z) \in \operatorname{Im}(d)$ and hence $\overline{f(z)} = 0$ in $H_i(N_\bullet)$.

If $f \simeq_{\text{htpc}} g$, 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 3.25. The converse of this proposition is false. For example, the chain map of $\mathbb{Z}$-modules pictured as

$$\begin{tikzcd}
\cdots \arrow[r] & 0 \arrow[r] \arrow[d] & \langle 2 \rangle \mathbb{Z}/4 \arrow[r] \arrow[d, "inc"] & 0 \arrow[r] \arrow[d] & \cdots \\
\cdots \arrow[r] & \mathbb{Z}/4 \arrow[r, "2"] & \mathbb{Z}/4 \arrow[r] & 0 \arrow[r] & \cdots
\end{tikzcd}$$

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 $h_0 : \langle 2 \rangle \to \mathbb{Z}/4$. The only possibilities for h_0 are the 0 map and the inclusion map. Neither works.

Remark 3.26. Homotopy is an equivalence relation on chain maps. The quotient of $\langle\langle R\text{-complexes}\rangle\rangle$ by this equivalence relation is the *homotopy category* of R-complexes.

3.2 Resolutions

3.2.1 Free and projective resolutions

Definition 3.27. A *free resolution* of an R-module M is a chain complex of the form

$$\cdots \to F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \to 0 \to \cdots ,$$

such that each F_i is a free R-module, along with a map $\pi : F_0 \to M$ such that the augmented sequence

$$\cdots \to F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\pi} M \to 0 \to \cdots$$

is an exact complex. (We allow for the possibility that $F_i = 0$ for some of the i's.)

A *projective resolution* of an R-module M is a chain complex of the form

$$\cdots \to P_3 \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to 0 \to \cdots ,$$

such that each P_i is a projective R-module, along with a map $\pi : P_0 \to M$ such that the augmented sequence

$$\cdots \to P_3 \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\pi} M \to 0 \to \cdots$$

is an exact complex. (We allow for the possibility that $P_i = 0$ for some of the i's.)

We shall see below that free resolutions generalize the notion of presentation for a module. An important fact is that all R modules have free, and hence projective, resolutions.

Proposition 3.28. *Every (left) R-module has a free resolution.*

Proof. Given an R-module M and a subset $S \subseteq M$ that generates it, we may find a free module F_0 of rank equal to the cardinaltiy of S and a surjective R-map $\pi : F_0 \twoheadrightarrow M$, given by sending a basis of F_0 bijectively onto S. Write $\Omega^1_R(M)$ for the kernel of this surjection, so that we have the s.e.s.

$$0 \to \Omega^1_R(M) \xrightarrow{\iota} F_0 \xrightarrow{\pi} M \to 0.$$

The module $\Omega^1_R(M)$ is known as a module of *first syzygies* of M. Note that it is not unique, but rather depends on the choice of generators of M. The module $\Omega^1_R(M)$ gives the collection of all *relations* on this set of generators.

Repeating this process, starting with $\Omega^1_R(M)$ gives another surjective R-module $F_1 \twoheadrightarrow \Omega^1(M)$ with F_1 free. This gives the right exact sequence

$$F_1 \xrightarrow{g} F_0 \xrightarrow{\pi} M \to 0$$

where g is the composition of $F_1 \twoheadrightarrow \Omega^1(M) \hookrightarrow F_0$. (It is right exact since π is onto and the image of g is the kernel of π, by construction.) A basis of F_0 gives the generators of M and a basis of F_1 gives a set of generators on the relations among these generators of M.

Why stop here? Let $\Omega^2_R(M) = \operatorname{Ker}(g)$ (the module of "second syzygies" of M) and map a free module onto $\Omega^2(M)$, to obtain the exact sequence

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

Repeating ad infinitum yields the exact sequence

$$\cdots \to F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \to M \to 0,$$

with each F_i a free R-module. The kernel of d_n is sometimes written $\Omega^n_R(M)$ and referred to as the module of n-th syzygies. (But, again, it depends on the choices of generators made along the way.) A basis of F_0 gives a list of generators of M, a basis of F_1 gives a list of generators of the module $\Omega^1_R(M)$ of all relations on the chosen generators of M, a basis of F_2 gives a list of generators of the module $\Omega^2_R(M)$ of all relations among the relations on the generators of M, etc.

This construction terminates (i.e., $F_{i+1} = 0$ for some $i \geq 0$) if and only if for some sequence of choices made along the way, $\Omega^i_R(M) = \operatorname{Ker}(F_{i-1} \to F_{i-2})$ happens to be a free module. In that case we obtain a *finite* resolution. However, not all modules have finite resolutions. □

Remark 3.29. Recall that M is finitely presented if F_0 and F_1 can both be taken to have finite rank, say $F_0 = R^p, F_1 = R^q$. Then map $F_1 \to F_0$ is given by a $p \times q$ matrix A that "presents" M. The rows of A correspond to generators $m_1, \dots, m_p$ of M and each column $(a_{1,j}, \dots, a_{p,j})$, for $1 \leq j \leq q$, gives the relation $a_{1,j}m_1 + \cdots + a_{p,j}m_p = 0$ among these generators. Moreover, every relation on these generators is an R-linear combination of these q relations; i.e., if $(b_1, \dots, b_p)^T$ is such that $\sum b_i m_i = 0$ then $(b_1, \dots, b_p)^T$ is an R-linear combination of the columns of A.

November 6, 2020

Example 3.30. Let $R = k[x, y]$ for a field k and $M = (x, y)$. Then M is generated by x and y and we have a surjection

$$R^2 \xrightarrow{\pi} M \to 0$$

where π is given by the 1×2 matrix (x, y). The module $\Omega^1_R(M)$ is the submodule

$$\left\{ \begin{bmatrix} f(x,y) \\ g(x,y) \end{bmatrix} \mid xf + yg = 0 \right\}$$

of R^2.

If $\begin{bmatrix} f(x,y) \\ g(x,y) \end{bmatrix}$ belongs to $\Omega^1(M)$, then $xf(x,y) = -yg(x,y)$. Using that R is a UFD and x, y are non-associate irreducible elements, it follows that $g = xh$ and hence that $f = -yh$, for some $h \in R$; that is, $(f,g)^T = h(-y,x)^T$ and hence the kernel of π is generated by the single $(-y,x)^T$. This gives us the right exact sequence

$$R \xrightarrow{\begin{bmatrix} -y \\ x \end{bmatrix}} R^2 \xrightarrow{(x,y)} M \to 0$$

In fact, the map $\begin{bmatrix} -y \\ x \end{bmatrix} : R \to R^2$ is injective since R is a domain, and so the process "stops" here. In other words, $\Omega^1(M)$ is free of rank one in this example, and we have the exact sequence

$$0 \to R \xrightarrow{\begin{bmatrix} -y \\ x \end{bmatrix}} R^2 \xrightarrow{(x,y)} M \to 0.$$

Formally, we have that the complex

$$\cdots \to 0 \to R \xrightarrow{\begin{bmatrix} -y \\ x \end{bmatrix}} R^2 \to 0 \to \cdots$$

together with the map $\pi : R^2 \xrightarrow{(x,y)} M$ form a free resolution of M. We will usually just say, a bit inaccurately, that

$$\cdots \to 0 \to R \xrightarrow{\begin{bmatrix} -y \\ x \end{bmatrix}} R^2 \xrightarrow{(x,y)} M \to 0$$

is a free resolution of M.

Since every free module is projective, every free resolution is a projective resolution, but not vice versa. One might wonder why we talk about projective resolutions and not just free ones. It turns out that the larger collection of projective resolutions enjoys all of the same former properties as the collection of free resolutions, and modules sometimes have "smaller" projective resolutions than free ones. This is illustrated by Example 3.31 below; in that example, the module has a finite projective resolution but no finite free resolution.

Example 3.31. Let $R = \mathbb{Z}[\sqrt{-5}]$. Recall that $I = (2, 1+\sqrt{-5})$ is an ideal of R which, when regarded as just a module, is projective but not free. If we set $M = R/I$, then

$$0 \to I \xrightarrow{\iota} R \xrightarrow{\pi} M \to 0$$

is a projective resolution, but not a free one. (Again, I am abusing terminology a bit.)

We can form a free resolution of M, of course, and it would start as

$$R^2 \xrightarrow{(2,1+\sqrt{-5})} R \to M \to 0.$$

The module $\Omega^2_R(M)$ contains the elements $(-1-\sqrt{-5},2)^T$ and $(-3,1-\sqrt{-5})^T$.

It can in fact be shown that no free resolution of M terminates after a finite number of steps.

Example 3.32. Let $R = k[x,y]/(xy)$ and $M = R/x$. Then one can show that the $\operatorname{Ann}_R(x) = (y)$ and $\operatorname{Ann}_R(y) = (x)$ and hence

$$\cdots \to R \xrightarrow{x} R \xrightarrow{y} R \xrightarrow{x} R \xrightarrow{\pi} M \to 0$$

is a free resolution of M. It can be shown that M does not admit any free or even projective resolution with $P_i = 0$ for some $i \geq 0$. That is, the R-module M has "infinite projective dimension".

3.2.2 Injective resolutions

Definition 3.33. For a ring R and R-module M, an *injective resolution* of M is complex of the form

$$\cdots \to 0 \to E^0 \xrightarrow{d^0} E^1 \xrightarrow{d^1} E^2 \xrightarrow{d^2} \cdots,$$

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.

It is more difficult to motivate the concept of an injective resolution. But they exist. To show this, we first need to show that for an arbitrary R-module M, an injective module E^0 exists such that M injects into E^0.

Theorem 3.34. *For any ring R and any R-module M, there is an injective R-module E and a one-to-one R-module homomorphism $i : M \hookrightarrow E$.*

Proof. We first prove this for the case $R = \mathbb{Z}$ then bootstrap to the general case.

Suppose $R = \mathbb{Z}$. I first show that for each $0 \neq x \in M$, there is an injective R-module E_x and a one-to-one R-module homomorphism $i_x : M \to E_x$ such that $i_x(x) \neq 0$. Let $N = \mathbb{Z} \cdot x$ be the subgroup of M generated by x. We first find an injective $\mathbb{Z}$-module E_x and a one-to-one homomorphism $j : N \hookrightarrow E_x$: If $|x| = \infty$, we take $E_x = \mathbb{Q}$ and let j be the unique group homomorphism defined by $j(x) = 1$. If $|x| = n < \infty$, we take $E_x = \mathbb{Q}/\mathbb{Z}$ and let j be the unique group homomorphism defined by $j(x) = 1/n$. Since E_x is injective, the map j extends to a map $i_x : M \to E_x$ such that $i_x|_N = j$ and hence $i_x(x) = j(x) \neq 0$.

Now set $E = \prod_{x \in M} E_x$ and define $i : M \to E$ to be the map whose x-th component is i_x. Then i is one-to-one, since for all $x \neq 0$, the x-th component of $i(x)$ is non-zero. Since a product of injective modules is injective, E is injective.

Now return to R being arbitrary. If we regard M as just an abelian group, then by the special case $R = \mathbb{Z}$ there is a one-to-one homomorphism of $\mathbb{Z}$-modules $j : M \hookrightarrow D$ with D an injective $\mathbb{Z}$-module. Apply $\operatorname{Hom}_{\mathbb{Z}}(R, -)$ to this map to obtain the one-to-one homomorphism

$$j_* : \operatorname{Hom}_{\mathbb{Z}}(R, M) \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(R, D).$$

of $\mathbb{Z}$-modules. (It is one-to-one since $\operatorname{Hom}_{\mathbb{Z}}(R, -)$ is left exact.) Since M is an R-module, we have a canonical map

$$\alpha : M \to \operatorname{Hom}_{\mathbb{Z}}(R, M)$$

given by $\alpha(m)(r) := rm$ and it is a homomorphism of abelian groups. Moroever, α is injective since $\alpha(m) = 0$ implies $1_R m = 0$.

Composing these maps gives the one-to-one homomorphism of abelian groups

$$\beta : M \hookrightarrow \operatorname{Hom}_{\mathbb{Z}}(R, D) \tag{3.2.1}$$

and tracking through the formulas shows that $\beta(m)(r) = j_*(rm) = j(rm)$.

Since R is a $\mathbb{Z} - R$-bimodule, the abelian group $\operatorname{Hom}_{\mathbb{Z}}(R, M)$ is a left R-module via the rule for scaling

$$(x \cdot g)(r) := g(rx),$$

for any $g \in \operatorname{Hom}_{\mathbb{Z}}(R, M)$, and $r, x \in R$. We note that β is an R-map since $\beta(xm)(r) = j(rxm)$ and $(x \cdot \beta(m))(r) = \beta(m)(rx) = j(rxm)$.

So (3.2.1) is a one-to-one homomorphism of left R-modules, and it remains to prove $\operatorname{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module.

For this I use the Hom-tensor adjointness isomorphism

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

which is a natural isomorphism of functors from R-modules to abelian groups. Since the functor $R \otimes_R -$ is naturally isomorphic to the identity functor, this gives a natural isomorphism

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

Since D is an injective $\mathbb{Z}$-module, $\operatorname{Hom}_{\mathbb{Z}}(-, D)$ is exact, and hence so too is $\operatorname{Hom}_R(-, \operatorname{Hom}_{\mathbb{Z}}(R, D))$. This proves $\operatorname{Hom}_{\mathbb{Z}}(R, D)$ is an injective R-module. □

November 9, 2020

Proposition 3.35. *Every R-module admits an injective resolution.*

Proof. Given a module M, by a result above we can find a one-to-one R-map $j : M \hookrightarrow E^0$ with E^0 injective. Let $N = \operatorname{coker}(j) = E^1/\operatorname{Im}(j)$ and apply this result again to obtain a one-to-one R-module $N \hookrightarrow E^1$ with E^1 injective. Let $E^0 \to E^1$ be the composition of $E^0 \twoheadrightarrow N \hookrightarrow E^1$. 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. $\square$

Example 3.36. Let us find an injective resolution of $\mathbb{Z}$ as a module over itself. We have the evident embedding $\mathbb{Z} \hookrightarrow \mathbb{Q}$ 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 3.37. Let's find an injective resolution of $\mathbb{Z}/n$ as a $\mathbb{Z}$-module. We have

$$0 \to \mathbb{Z}/n \to \mathbb{Q}/\mathbb{Z} \to E^1 \to 0 \to \cdots$$

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.

Remark 3.38. Warning! In general, quotients of injective modules need not be injective and so things aren't as simple as the above example indicates. There are actually very few examples in which one can explicitly describe the injective resolution of a module. But, as we shall see, it is valuable to know that injective resolutions exist even though they can rarely be described explicitly.

3.2.3 Uniqueness of resolutions up to homotopy

As I have repeatedly mentioned, free, projective, and injective resolutions of modules are not unique. For example, the construction outlined above to produce the free resolution of a module depends on infinitely many choices, since we must choose generating sets for $M, \Omega^1_R(M), \Omega^2_R(M), \ldots$. However, there is a version of uniqueness that holds: such resolutions are unique "up to homotopy".

Theorem 3.39. *Let M and N be R-modules, $f : M \to N$ an R-module homomorphism. Consider two complexes*

$$\overbrace{\cdots \to P_2 \to P_1 \to P_0}^{P_\bullet} \to M \to 0$$

$$\underbrace{\cdots \to Q_2 \to Q_1 \to Q_0}_{Q_\bullet} \to N \to 0$$

such that P_i is projective for all i and the second complex displayed above is exact.

Then there is a chain map $\tilde{f} : P_\bullet \to Q_\bullet$ causing the square diagram

$$\begin{tikzcd}
P_\bullet \arrow[r, "\tilde{f}"] \arrow[d, "p", "\sim"'] & Q_\bullet \arrow[d, "q", "\sim"'] \\
M \arrow[r, "f"] & N
\end{tikzcd}$$

of chain complexes to commute. Moreover, $\tilde{f}$ is unique up to homotopy: if $\tilde{f}' : P_\bullet \to Q_\bullet$ is another chain map causing this square to commute, then $\tilde{f} \simeq_{\text{htpc}} \tilde{f}'$.

Proof. For existence, we need to construct maps $\tilde{f}_i : P_i \to Q_i$ for $i \geq 0$ such that $q \circ \tilde{f}_0 = f \circ p$ and $d_i^Q \circ \tilde{f}_i = \tilde{f}_{i-1} \circ d_i^P$ for $i \geq 1$. To construct $\tilde{f}_0$, we merely use the definition of projective and the diagram

$$\begin{tikzcd}
 & P_0 \arrow[dl, dashed, "\exists \tilde{f}_0"'] \arrow[d, "f \circ p"] & \\
Q_0 \arrow[r, "q"] & N \arrow[r] & 0.
\end{tikzcd}$$

Suppose we have consructed maps $\tilde{f}_0, \dots, \tilde{f}_n$ for some $n \geq 0$ so that $d_i^Q \circ \tilde{f}_i = \tilde{f}_{i-1} \circ d_i^P$ for $1 \leq i \leq n$. (When $n = 0$, the condition is vacuous.) Let $\Omega_R^{n+1}(N) = \operatorname{Ker}(Q_n \to Q_{n-1})$. Use the definition of projective again with the diagram

$$\begin{tikzcd}
 & P_{n+1} \arrow[dl, dashed, "\exists \tilde{f}_{n+1}"'] \arrow[d, "\tilde{f}_n \circ d_{n+1}^P"] & \\
Q_{n+1} \arrow[r, "d_{n+1}|"] & \Omega_R^{n+1}(N) \arrow[r] & 0
\end{tikzcd}$$

to contruct $\tilde{f}_{n+1}$ such that $d_{n+1}^Q \circ \tilde{f}_{n+1} = \tilde{f}_n \circ d_n^P$ holds too. This proves existence.

November 11, 2020

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 $g : P_\bullet \to Q_\bullet$ is a chain map such that $qg = 0$, then g is null homotopic. That is, we need to show there are maps $h_i : P_i \to Q_{i+1}$ for $i \geq 0$ such that $d_{i+1}^Q \circ h_i + h_{i-1} \circ d_i^P = g_i$ for all $i \geq 0$. (In the latter equation, when $i = 0$ we have $h_{-1} = 0$.)

Since $q \circ g_0 = 0$, the image of g_0 is contained in $\operatorname{Ker}(q) = \operatorname{Im}(d_1^Q)$ and so since P_0 is projective, there is a map $h_0 : P_0 \to Q_1$ such that $(d_1^Q|^{\operatorname{Im}(d_1^Q)}) \circ h_0 = g_0|^{\operatorname{Im}(d_1^Q)}$ and hence $d_1^Q \circ h_0 = g_0$ as needed. Suppose maps $h_0, \dots, h_n$ have be constructed for $n \geq 0$, and consider the map $g_{n+1} - h_n \circ d_{n+1}^P : P_{n+1} \to Q_n$. By induction the image of this map is contained in $\operatorname{Im}(d_{n+1}^Q)$ and so, since P_{n+1} is projective, there is a map $h_{n+1} : P_{n+1} \to Q_{n+2}$ such that $d_{n+2}^Q \circ h_{n+1} = g_{n+1} - h_n \circ d_{n+1}^P$ and hence $d_{n+2}^Q \circ h_{n+1} + h_n \circ d_{n+1}^P = g_{n+1}$. □

We now give a way to compare chain complexes:

Definition 3.40. 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: $f \circ g \simeq_{\text{htpc}} \text{id}_N$ and $g \circ f \simeq_{\text{htpc}} \text{id}_M$.

Lemma 3.41. *If $f : M_\bullet \to N_\bullet$ is a homotopy equivalence, then the induced map in homology $H_i(f) : H_i(M_\bullet) \to H_i(N_\bullet)$ is an isomorphism for each i. Indeed, using Proposition 3.24 we see that $H_i(f) \circ H_i(g) = H_i(f \circ g) = H_i(id_N) = id_{H_i(M_\bullet)}$ and $H_i(g) \circ H_i(f) = H_i(g \circ f) = H_i(id_M) = id_{H_i(N_\bullet)}$.*

Definition 3.42. A chain map $f : M_\bullet \to N_\bullet$ such that $H_i(f)$ is an isomorphism for each $i \in \mathbb{Z}$ is called a *quasi-isomorphism* and denoted $f : M_\bullet \xrightarrow{\sim} N_\bullet$. Moreover $M_\bullet$ and $N_\bullet$ are called quasi-isomorphic complexes denoted $M_\bullet \simeq N_\bullet$.

Any homotopy equivalence is a quasi-isomorphism. But there exist quasi-isomorphisms that are not homotopy equivalences.

Example 3.43. 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:

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

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 $\overline{\pi} : \text{coker}(d_0) = P_0/\operatorname{Im}(d_0) = P_0/\operatorname{Ker}(\pi) \xrightarrow{\cong} M$ 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 non-zero 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 identify. 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 3.44. *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*

$$\begin{tikzcd}
P_\bullet \arrow[dr, "p", "\sim"'] \arrow[dd, "g", "\simeq"'] & \\
& M \\
Q_\bullet \arrow[ur, "\sim", "q"'] &
\end{tikzcd}$$

commutes. Morever, 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 $\mathrm{id}_{C_\bullet}$. Similarly, $g \circ f$ is homotopic to $\mathrm{id}_{Q_\bullet}$. $\square$

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 3.45. *Let M and N be R-modules, $f : M \to N$ an R-module homomorphism, and $i : M \xrightarrow{\sim} E^\bullet$ and $j : N \xrightarrow{\sim} F^\cdot$ injective resolutions. Then there is a chain map $\tilde{f} : E^\bullet \to F^\cdot$ causing the square diagram*

$$\begin{tikzcd}
M \arrow[r, "i", "\sim"'] \arrow[d, "f"] & E^\bullet \arrow[d, "\tilde{f}"] \\
N \arrow[r, "j", "\sim"'] & F^\cdot
\end{tikzcd}$$

of chain complexes to commute. Moreover, $\tilde{f}$ is unique up to homotopy.

Corollary 3.46. *Any two injective resolutions of the same module are homotopy equivalent via a chain map that is unique up to homotopy.*

3.3 Derived functors

3.3.1 Definition on objects and examples

Left derived functors

Definition 3.47. Let R and S be rings and $F : \langle\langle {}_R\mathrm{Mod} \rangle\rangle \to \langle\langle {}_S\mathrm{Mod} \rangle\rangle$ be a right exact covariant functor. For each $j \geq 0$ and R-module M, we define an S-module $\mathbb{L}_j F(M)$, known as the *j-th left derived functor of F* (evaluated at M) as follows: choose a projective resolution $\pi : P_\bullet \xrightarrow{\sim} M$ of M, apply F to $P_\bullet$ to obtain the complex $F(P_\bullet)$ (with differential given by $F(d^P)$), and set

$$\mathbb{L}_j F(M) := H_j(F(P_\bullet)).$$

November 13, 2020

Proposition 3.48. *The modules $\mathbb{L}_j F(M)$ are independent, up to a canonical isomorphism, of the choice of projective resolution involved in their definition.*

Proof. Let $P_\bullet$ and $Q_\bullet$ be resolutions of M. Then by Corollary 3.44 there is a unique homotopy equivalence $g : P_\bullet \xrightarrow{\simeq_{\text{htpc}}} Q_\bullet$ causing the evident triangle to commute. Since F is additive, it takes id_M to id_M and commutes with $+$ and compositions so it follows that $F(g) : F(P_\bullet) \to F(Q_\bullet)$ is also a homotopy equivalence. Taking homology thus gives an isomorphism

$$H_j(F(P_\bullet)) \xrightarrow{\cong} H_j(F(Q_\bullet)).$$

So, $\mathbb{L}_j F(M)$ is well-defined up to a canonical isomorphism. □

Remark 3.49. To be truly precise, Definition 3.47 should say: Given F, upon choosing, once and for all, a projective resolution of each R-module, these definitions determine a functor $\mathbb{L}_j F(-)$ for each $j \geq 0$. Given another choice of projective resolutions we technically would get a different functor $\mathbb{L}_j F(-)$ for each j. But, for each j, the two functors so obtained are naturally isomorphic in a canonical way, as shown (partially) by the Proposition above.

The Tor functor

Definition 3.50. For a ring R, right R-module N and left R-module M, we define

$$\mathrm{Tor}_j^R(N, M) := \mathbb{L}_j(N \otimes_R -)(M)$$

to be the j-th left derived functor of the functor $N \otimes_R - : \langle\langle {}_R\mathrm{Mod} \rangle\rangle \to \langle\langle \mathbb{Z}\text{-modules} \rangle\rangle$. So, for each j, $\mathrm{Tor}_j^R(N, M)$ is an abelian group. When R is commutative, $N \otimes_R -$ can be viewed as taking values in $\langle\langle {}_R\mathrm{Mod} \rangle\rangle$ and hence $\mathrm{Tor}_j^R(N, M)$ is an R-module.

Explicitly,

$$\mathrm{Tor}^i_R(N, M) = H_j(\cdots \xrightarrow{\mathrm{id}_N \otimes d_3} N \otimes_R P_2 \xrightarrow{\mathrm{id}_N \otimes d_2} N \otimes_R P_1 \xrightarrow{\mathrm{id}_N \otimes d_1} N \otimes_R P_0 \to 0 \to \cdots)$$

where $P_\bullet \xrightarrow{\sim} M$ is a projective resolution of M.

Example 3.51. Let's compute $\mathrm{Tor}_j^{\mathbb{Z}}(N, \mathbb{Z}/n)$ for any $\mathbb{Z}$-module N and integers $n \geq 1$, and j.

We have the projective resolution $\cdots \to 0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n \to 0$ of $\mathbb{Z}/n$ and so $\mathrm{Tor}_j^R(N, \mathbb{Z}/n)$ 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 non-zero 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

$$\mathrm{Tor}_0^R(N, \mathbb{Z}/n) \cong N/nN \cong N \otimes_{\mathbb{Z}} \mathbb{Z}/n$$

(as the Proposition below tells us),

$$\mathrm{Tor}_1^R(N, \mathbb{Z}/n) \cong \mathrm{Ker}(N \xrightarrow{n} N) = \{x \in N \mid n \cdot x = 0\},$$

and

$$\mathrm{Tor}_j^R(N, \mathbb{Z}/n) = \mathbb{L}_j F(\mathbb{Z}/n) = 0$$

for all $j \notin \{0, 1\}$.

Note that $\mathrm{Tor}_1^R(N, \mathbb{Z}/n)$ is the n-torsion submodule of N — this explains the notation Tor.

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 3.52. *For any right exact functor F and R-module M, there is a canonical isomorphism*

$$\mathbb{L}_0 F(M) \cong F(M)$$

In particular,

$$\mathrm{Tor}_0^R(N, M) \cong N \otimes_R M$$

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 $F(P_1) \xrightarrow{F(d_1)} F(P_0)$, i.e., $F(M)$. This proves both statements. □

Example 3.53. 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

$$\cdots \to 0 \to R \xrightarrow{\begin{bmatrix} -y \\ x \end{bmatrix}} R^2 \xrightarrow{(x,y)} R \to R/(x, y) \to 0.$$

It follows that $\operatorname{Tor}_*^R(M, R/(x, y))$ is the homology of the complex

$$\cdots \to 0 \to M \xrightarrow{\begin{bmatrix} -y \\ x \end{bmatrix}} M^{\oplus 2} \xrightarrow{(x,y)} M \to 0 \to \cdots .$$

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 $t \in M$.

Proposition 3.54. *If F is a flat right R-module, then $\operatorname{Tor}_j^R(F, M) = 0$ for all $j \neq 0$ and all left R-modules M.*

Proof. This holds since $F \otimes_R -$ is an exact functor. In detail, if $P_\bullet$ is a projective resolution of M then $P_\bullet \xrightarrow{p} M \to 0$ is an exact complex. Applying the exact functor $F \otimes_R -$ yields the exact complex $F \otimes_R P_\bullet \xrightarrow{\mathrm{id}_F \otimes p} F \otimes_R M$. This gives that

$$\operatorname{Tor}_j^R(F, M) = H_j(F \otimes_R P) = \begin{cases} F \otimes_R M & j = 0 \\ 0 & j \neq 0. \end{cases}$$

□

Remark 3.55. It is also true that $\operatorname{Tor}_j^R(N, F) = 0$ for all $j \neq 0$ whenever F is flat. This will follow from the balancedness of Tor, a property to be stated later.

Remark 3.56. The converse of Proposition 3.54 is also true, namely if $\operatorname{Tor}_j^R(F, M) = 0$ for all $j \neq 0$ and all R-modules M, then F is a flat R-module. We will prove this later.

November 16, 2020

Right derived functors

Definition 3.57. Let R and S be rings and $F : \langle\langle {}_R\mathrm{Mod} \rangle\rangle \to \langle\langle {}_S\mathrm{Mod} \rangle\rangle$ be a left exact covariant functor. For each $j \geq 0$ and R-module M, we define an S-module $\mathbb{R}^j F(M)$, called the *j-th right derived functor of F* (evaluated on M) as follows: Choose an injective resolution $i : M \xrightarrow{\sim} E^\bullet$ of M, apply F to $E^\bullet$ to obtain the complex $F(E^\bullet)$, and set

$$\mathbb{R}^j F(M) = H^j(F(E^\bullet)) = \frac{\operatorname{Ker}(F(E^j) \xrightarrow{F(d^j)} F(E^{j+1}))}{\operatorname{Im}(F(E^{j-1}) \xrightarrow{F(d^{j-1})} F(E^j))}.$$

Definition 3.58. Let R and S be rings and $G : \langle\langle {}_R\mathrm{Mod}\rangle\rangle \to \langle\langle {}_S\mathrm{Mod}\rangle\rangle$ be a left exact *contra-variant* functor. (Recall this means that G is additive and takes right exact sequences to left exact sequences.) For each $j \geq 0$ and R-module M, we define an S-module $\mathbb{R}^j G(M)$, called the *j-th right derived functor of* G (evaluated at M as follows: Choose a projective resolution $p : P_\bullet \xrightarrow{\sim} M$ of M, apply G to $P_\bullet$ to obtain the complex $G(P_\bullet)$. Since G is contravariant, this complex takes the form

$$\cdots \to 0 \to G(P_0) \xrightarrow{G(d_0)} G(P_1) \xrightarrow{G(d_1)} G(P_2) \xrightarrow{G(d_2)} \cdots$$

We set

$$\mathbb{R}^j F(M) = H^j(F(P_\bullet)) = \frac{\mathrm{Ker}(G(P_j) \xrightarrow{G(d_{j+1})} G(P_{j+1})}{\mathrm{Im}(G(P_{j-1}) \xrightarrow{G(d_j)} G(P_j)}.$$

The following summarizes properties analogous to those worked out carefully above for right exact covariant functors:

Proposition 3.59. *Let R, S, F and G be as in the definitions above.*

- *The modules $\mathbb{R}^j F(M)$ and $\mathbb{R}^j G(M)$ are independent, up to canonical isomorphism, of the choice of injective/projective resolution.*
- *We have canonical isomorphisms $\mathbb{R}^0 F(M) \cong F(M)$ and $\mathbb{R}^0 G(M) \cong G(M)$.*

The Ext functor

Definition 3.60. For a pair of left R-modules M and N, we write

$$\mathrm{Ext}^j_R(M,N)^I = \mathbb{R}^j \operatorname{Hom}_R(M,-)(N)$$

where F in Definition 3.57 is taken to be the left-exact covariant functor $F := \operatorname{Hom}_R(M,-)$.

We define

$$\mathrm{Ext}^j_R(M,N)^{II} = \mathbb{R}^j \operatorname{Hom}_R(-,N)(M)$$

where G in Definition 3.58 is taken to be the left exact contravariant functor $G := \operatorname{Hom}_R(-,N)$.

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.

Definition 3.61. By the balancedness of Ext, which I will formally state later, there is a canonical isomorphism $\mathrm{Ext}^j_R(M,N)^I \cong \mathrm{Ext}^j_R(M,N)^{II}$. 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 I'll keep the superscripts.

Example 3.62. Let's compute $\mathrm{Ext}^*_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n)^I$ and $\mathrm{Ext}^*_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n)^{II}$.

For the latter, we start with the free resolution $\cdots 0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m \to 0$ of $\mathbb{Z}/m$ and apply $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}/n)$ to obtain

$$\cdots \to 0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n) \xrightarrow{m} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/n) \to 0$$

which is isomorphic to

$$\cdots \to 0 \to \mathbb{Z}/n \xrightarrow{m} \mathbb{Z}/n \to 0.$$

The two non-zero homology modules are both isomorphic to $\mathbb{Z}/g$ where $g = gcd(m, n)$. So

$$\mathrm{Ext}^i_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n)^{II} \cong \begin{cases} \mathbb{Z}/g & i = 0, 1 \\ 0 & i \geq 2. \end{cases}$$

For the former, we will use the following fact: For any integer j there is a short exact sequence

$$0 \to \mathbb{Z}/j \xrightarrow{\overline{1} \mapsto \overline{1/n}} \mathbb{Q}/\mathbb{Z} \xrightarrow{j} \mathbb{Q}/\mathbb{Z} \to 0.$$

This holds since $\mathbb{Q}/\mathbb{Z}$ is divisible and the kernel of multiplicaition by j is $\{\overline{\frac{i}{j}} \mid 0 \leq i \leq j-1\}$, which is generated by $\overline{1/n}$.

In particular, we have an injective resolution

$$0 \to \mathbb{Z}/n \to \mathbb{Q}/\mathbb{Z} \xrightarrow{n} \mathbb{Q}/\mathbb{Z} \to 0 \to \cdots$$

of $\mathbb{Z}/n$. Applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, -)$ gives

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Q}/\mathbb{Z}) \xrightarrow{n} \mathrm{Hom}_{\mathbb{Z}}(Z/m, \mathbb{Q}/\mathbb{Z}) \to 0 \to \cdots.$$

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 $0 \leq j < m$, and they form a cyclic subgroup of order m. It follows that

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/m) \cong \mathbb{Z}/m$$

and that the previous complex is isomorphic to

$$\cdots \to 0 \to \mathbb{Z}/m \xrightarrow{n} \mathbb{Z}/m \to 0 \to \cdots$$

This gives

$$\mathrm{Ext}^i_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n)^{I} \cong \begin{cases} \mathbb{Z}/g & i = 0, 1 \\ 0 & i \geq 2. \end{cases}$$

November 18, 2020

3.3.2 Definition on maps and long exact sequence

Definition 3.63. Given a right exact functor $F : \langle\langle {}_R\text{Mod}\rangle\rangle \to \langle\langle {}_S\text{Mod}\rangle\rangle$, R-modules M and N, an R-map $f : M \to N$, and an integer $j \geq 0$, we define an S-module homomorphism

$$\mathbb{L}_j F(f) : \mathbb{L}_j F(M) \to \mathbb{L}_j F(N)$$

as follows: Given projective resolutions $p : P_\bullet \xrightarrow{\sim} M$ and $q : Q_\bullet \xrightarrow{\sim} M$, apply Theorem 3.39 to obtain a chain map $\tilde{f} : P_\bullet \to Q_\bullet$ such that $q \circ \tilde{f} = f \circ p$. Then $F(\tilde{f}) : F(P_\bullet) \to F(Q_\bullet)$ is a chain map and hence it induces a map on homology

$$\mathbb{L}_j F(M) = H_j(F(P_\bullet)) \xrightarrow{F(\tilde{f})} H_j(F(Q_\bullet)) = \mathbb{L}_j F(M)$$

which is, by definition, $\mathbb{L}_j F(f)$.

We will take the following fact on faith.

Proposition 3.64. *The rules introduced above make $\mathbb{L}_j F(-)$, for each $j \geq 0$, into an additive covariant functor $\mathbb{L}_j F(-) : \langle\langle {}_R\mathit{Mod}\rangle\rangle \to \langle\langle {}_S\mathit{Mod}\rangle\rangle$.*

Likewise we define $\mathbb{R}^j F$ on morphisms for both covariant and contravariant left exact functors. I will define the latter, leaving the former to your imagination.

Definition 3.65. Given a left exact contravariant functor $G : \langle\langle {}_R\text{Mod}\rangle\rangle \to \langle\langle {}_S\text{Mod}\rangle\rangle$, R-modules M and N, an R-map $f : M \to N$, and an integer $j \geq 0$, we define an S-module homomorphism

$$\mathbb{R}_j G(f) : \mathbb{R}_j F(N) \to \mathbb{R}_j F(M)$$

as follows: Given projective resolutions $p : P_\bullet \xrightarrow{\sim} M$ and $q : Q_\bullet \xrightarrow{\sim} M$, apply Theorem 3.39 to obtain a chain map $\tilde{f} : P_\bullet \to Q_\bullet$ such that $q \circ \tilde{f} = f \circ p$. Then $G(\tilde{f}) : G(Q_\bullet) \to G(P_\bullet)$ is a chain map and hence it induces a map on homology

$$\mathbb{R}_j F(N) = H_j(G(Q_\bullet) \xrightarrow{F(\tilde{f})} H_j(G(P_\bullet)) = \mathbb{L}_j R(M)$$

which is, by definition, $\mathbb{R}_j G(f)$.

We have a similar fact.

Proposition 3.66. *The rules introduced above make $\mathbb{R}_j G(-)$, for each $j \geq 0$, into an additive contravariant functor $\mathbb{R}_j G(-) : \langle\langle {}_R\mathit{Mod}\rangle\rangle \to \langle\langle {}_S\mathit{Mod}\rangle\rangle$.*

Long exact sequence of derived functors

Akin to how a shot exact sequence of complexes gives rise to a long exact sequence in homology (see Theorem 3.18), short exact sequences of R-modules give rise to long exact sequences involving derived functors.

Theorem 3.67. *Let $F : \langle\langle {}_R Mod\rangle\rangle \to \langle\langle {}_S Mod\rangle\rangle$ be a right exact additive covariant functor for some rings R and S. Given a s.e.s. of left R-modules $0 \to M' \to M \to M'' \to 0$ there is a long exact sequence of the form*

$$\cdots \mathbb{L}_{i+1}F(M') \to \mathbb{L}_{i+1}F(M) \to \mathbb{L}_{i+1}F(M'') \to \mathbb{L}_iF(M') \to \mathbb{L}_iF(M) \to \mathbb{L}_iF(M'') \to \mathbb{L}_{i-1}F(M') \cdots$$

also pictured as

$$\begin{tikzcd}
\cdots \arrow[r] & \mathbb{L}_{i+1}F(M'_\bullet) \arrow[r] & \mathbb{L}_{i+1}F(M_\bullet) \arrow[r] & \mathbb{L}_{i+1}F(M''_\bullet) \arrow[dll, "\partial_i"] & \\
 & \mathbb{L}_iF(M'_\bullet) \arrow[r] & \mathbb{L}_iF(M_\bullet) \arrow[r] & \mathbb{L}_iF(M''_\bullet) \arrow[dll, "\partial_{i-1}"] & \\
 & \mathbb{L}_{i-1}F(M'_\bullet) \arrow[r] & \mathbb{L}_{i-1}F(M_\bullet) \arrow[r] & \mathbb{L}_{i-1}F(M''_\bullet) \arrow[dll, dashed] & \\
 & \mathbb{L}_0F(M'_\bullet) = F(M') \arrow[r] & \mathbb{L}_0F(M_\bullet) = F(M) \arrow[r] & \mathbb{L}_0F(M''_\bullet) = F(M'') \arrow[r] & 0.
\end{tikzcd}$$

Proof. For the existence of such a long exact sequence, we apply the Horseshoe Lemma (a result we shall not prove - see Lemma 10.53 on p.839 of Rotman's book *Advanced Modern Algebra* 2nd edition for a proof) to obtain from projective resolutions $P'_\bullet \overset{\sim}{\to} M'$ and $P''_\bullet \overset{\sim}{\to} M''$ a projective resolution $P_\bullet \overset{\sim}{\to} M$ that makes the short exact sequence of chain complexes pictured below exact:

$$\begin{tikzcd}
0 \arrow[r] & P'_\bullet \arrow[r, "\tilde{i}"] \arrow[d, "\sim"', "p'"] & P_\bullet \arrow[r, "\tilde{q}", "\sim"'] \arrow[d, "p"] & P''_\bullet \arrow[r] \arrow[d, "\sim"', "p'"] & 0 \\
0 \arrow[r] & M' \arrow[r, "i"] & M \arrow[r, "q"] & M'' \arrow[r] & 0.
\end{tikzcd}$$

By defintion, $\mathbb{L}_qF(M') = H_q(F(P'_\bullet))$ etc.

I claim that

$$0 \to F(P_\bullet) \to F(P'_\bullet) \to F(P''_\bullet) \to 0$$

is a short exact sequence of chain complexes. For each i,

$$0 \to P'_i \to P_i \to P''_i \to 0$$

is a split exact sequence since P''_i is projective. Since applying an additive functor to a split eaxct sequence yields a split eaxct sequence by a midterm problem, the sequence

$$0 \to F(P'_i) \to F(P_i) \to F(P''_i) \to 0$$

is exact (since it is split exact). This proves the claim.

The desired long exact sequence follows since short exact sequnces of chain complexes induce long exact sequences on homology by Theorem 3.18. □

Example 3.68. Let X be a right R-module and $0 \to M' \to M \to M'' \to 0$ a s.e.s. of left R-modules. Then there is a long exact sequence of abelian groups of the form

$$\begin{aligned} \cdots \to \operatorname{Tor}_2^R(X, M') \to \operatorname{Tor}_2^R(X, M) \to \operatorname{Tor}_2^R(X, M'') \\ \to \operatorname{Tor}_1^R(X, M') \to \operatorname{Tor}_1^R(X, M) \to \operatorname{Tor}_1^R(X, M'') \\ \to X \otimes_R M' \to X \otimes_R M \to X \otimes_R M'' \to 0. \end{aligned}$$

If R is commutative, this becomes a long exact sequence of R-modules.

The long exact sequence of Tor allows us to prove the converse to Proposition 3.54

Proposition 3.69. *If F is a right R-module such that $\operatorname{Tor}_j^R(F, M) = 0$ for all $j \neq 0$ and all left R-modules M, then F is flat.*

Proof. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. The long exact sequence of Tor from Example 3.68 with $X = F$ is really a short exact sequence as follows due to the hypothesis:

$$0 = \operatorname{Tor}_1^R(F, M'') \to F \otimes_R M' \to F \otimes_R M \to F \otimes_R M'' \to 0.$$

This shows that the functor $F \otimes_R -$ is left exact and hence F is flat. □

November 20, 2020

Similar arguments to those given above prove:

Theorem 3.70. *Suppose $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of left R-modules. If $F : \langle\langle {}_R Mod \rangle\rangle \to \langle\langle {}_S Mod \rangle\rangle$ is a left exact covariant functor there is a long exact sequence*

$$0 \to F(M') \to F(M) \to F(M'') \to \mathbb{R}^1 F(M') \to \mathbb{R}^1 F(M) \to \mathbb{R}^1 F(M'') \to \mathbb{R}^2 F(M') \to \cdots$$

and if F is a left exact contravariant functor there is along exact suquenece

$$0 \to F(M'') \to F(M) \to F(M') \to \mathbb{R}^1 F(M'') \to \mathbb{R}^1 F(M) \to \mathbb{R}^1 F(M') \to \mathbb{R}^2 F(M'') \to \cdots.$$

Example 3.71. Let X be a left R-module and $0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$ a s.e.s. of left R-modules. Then there are long exact sequence of abelian groups

$$\begin{aligned} 0 \to \operatorname{Hom}_R(X, M') \xrightarrow{i_*} \operatorname{Hom}_R(X, M) \xrightarrow{p_*} \operatorname{Hom}_R(X, M'') \\ \to \operatorname{Ext}_R^1(X, M')^I \to \operatorname{Ext}_R^1(X, M)^I \to \operatorname{Ext}_R^1(X, M'')^I \to \\ \to \operatorname{Ext}_R^2(X, M')^I \to \operatorname{Ext}_R^2(X, M)^I \to \operatorname{Ext}_R^2(X, M'')^I \to \\ \cdots \end{aligned}$$

and

$$\begin{aligned}
&0 \to \mathrm{Hom}_R(M'', X) \xrightarrow{p^*} \mathrm{Hom}_R(M, X) \xrightarrow{i^*} \mathrm{Hom}_R(M'', X) \\
&\qquad \to \mathrm{Ext}^1_R(M'', X)^{II} \to \mathrm{Ext}^1_R(M, X)^{II} \to \mathrm{Ext}^1_R(M', X)^{II} \to \\
&\qquad \to \mathrm{Ext}^2_R(M'', X)^{II} \to \mathrm{Ext}^2_R(M, X)^{II} \to \mathrm{Ext}^2_R(M', X)^{II} \to \\
&\cdots .
\end{aligned}$$

Remark 3.72. In the long exact sequences above the maps that are singled out with notation are

$$\begin{aligned}
i_*(f) \quad &= \mathrm{Hom}_R(X, i)(f) = i \circ f \\
p_*(f) \quad &= \mathrm{Hom}_R(X, p)(f) = p \circ f \\
i^*(g) \quad &= \mathrm{Hom}_R(i, X)(g) = i \circ g \\
p^*(g) \quad &= \mathrm{Hom}_R(X, p)(g) = p \circ g.
\end{aligned}$$

We can use Ext to characterize projective and injective modules as follows:

Proposition 3.73. *Let R be a ring and let M be a left R-module. Then the following are equivalent:*

1. *M is projective*
2. *$\mathrm{Ext}^i_R(M, N) = 0$ for all $i \geq 1$ and all left R-modules N*
3. *$\mathrm{Ext}^1_R(M, N) = 0$ for all left R-modules N*

Proof. (1) ⇒ (2) If M is projective then a projective resolution of M is given by

$$P_\bullet : \cdots \to 0 \to 0 \to M \to 0,$$

i.e. $P_0 = M$ and $P_i = 0$ for $i \geq 1$ and the map $\pi : P_0 = M \to M$ is id_M. Applying $\mathrm{Hom}_R(-, N)$ for an arbitrary left R-module N gives

$$\mathrm{Hom}_r(P_\bullet, N) : \mathrm{Hom}_R(0, N) \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(0, N) \to \mathrm{Hom}_R(0, N) \to \cdots ,$$

$$\text{i.e.,} \qquad 0 \to \mathrm{Hom}_R(M, N) \to 0 \to 0 \to \cdots ,$$

thus $\mathrm{Ext}^i_R(M, N) = 0$ for all $i \geq 1$ and all left R-modules N.

(2) ⇒ (3) is clear.

(3) ⇒ (1) follows because $\mathrm{Ext}^1_R(M, N) = 0$ for all left R-modules N implies that the functor $\mathrm{Hom}_R(M, -)$ is eaxct. In detail, consider a s.e.s of left R-modules

$$0 \to N' \to N \to N'' \to 0.$$

Then the corresponding l.e.s. shows that the sequence remains exact after applying $\mathrm{Hom}_R(M, -)$ since $\mathrm{Ext}^1_R(M, N') = 0$:

$$0 \to \mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'') \to \mathrm{Ext}^1_R(M, N') = 0.$$

Now Proposition 1.105 (2) ⇒ (1) yields that M is projective. □

Proposition 3.74. *Let R be a ring and let N be a left R-module. Then the following are equivalent:*

1. *N is injective*
2. *$\operatorname{Ext}_R^i(M, N) = 0$ for all $i \geq 1$ and all left R-modules M*
3. *$\operatorname{Ext}_R^1(M, N) = 0$ for all left R-modules M*

Proof. The proof is very similar to the previous one. For (1) ⇒ (2) one observes that N has an injective resolution $0 \to N \to 0 \to 0 \to \cdots$ with only one non zero injective module in it. For (3) ⇒ (1) one uses the l.e.s. of $\operatorname{Ext}_R(-, N)$ to show that the functor $\operatorname{Hom}_R(-, N)$ is exact and then Proposition 1.112 applies to conclude that N is injective. □

Balancedness

Recall we defined $\operatorname{Tor}_j^R(M, N)$ as the j-th right derived functor of $M \otimes_R -$ evaluated at N. Let's temporarily rename this by introducing a superscript "I":

$$\operatorname{Tor}_j^R(M, N)^I := \mathbb{L}_j(M \otimes_R -)(N).$$

Now define

$$\operatorname{Tor}_j^R(M, N)^{II} := \mathbb{L}_j(- \otimes_R N)(M),$$

so that $\operatorname{Tor}_j^R(M, N)^{II} = H_j(P_\bullet \otimes_R N)$ where $P_\bullet \xrightarrow{\sim} M$ is a projective resolution of M.

The following theorem shows that the above functors are naturally isomorphic. In practical terms, this says that we can compute $\operatorname{Tor}_j^R(M, N)$ using either a projective resolution of M or a projective resolution of N. (Of course we will use whichever is easier to come by, understand or work with in a given situation).

This result is not easy to prove. We will take it on faith.

Theorem 3.75 (Balancedness of Tor and Ext)**.** *Let R be a ring.*

1. *Given a right R-module M and a left R-module N, there is an isomorphism*

   $$\operatorname{Tor}_j^R(M, N)^I \cong \operatorname{Tor}_j^R(M, N)^{II}$$

   of abelian groups that is natural in both arguments. If R is commutative, it is an isomorphisms of R-modules. We write this common abelian group (or R-module) as just $\operatorname{Tor}_j^R(M, N)$.

2. *Given left R-modules M and N, there is an isomorphism*

   $$\operatorname{Ext}_R^j(M, N)^I \cong \operatorname{Ext}_R^j(M, N)^{II}$$

   of abelian groups that is natural in both arguments. If R is commutative, it is an isomorphisms of R-modules. We write this common abelian group (or R-module) as just $\operatorname{Ext}_R^j(M, N)$.

Using this we can state a more fully fleshed out characterization for flat modules.

Proposition 3.76. *Let R be a commutative ring and let F be an R-module. The following are equivalent:*

1. *N is flat*
2. $\operatorname{Tor}_i^R(F, N) = 0$ *for all $i \geq 1$ and all R-modules N*
3. $\operatorname{Tor}_i^R(F, N) = 0$ *for all R-modules N*
4. $\operatorname{Tor}_i^R(M, F) = 0$ *for all $i \geq 1$ and for all R-modules M*
5. $\operatorname{Tor}_1^R(M, F) = 0$ *for all R-modules M.*

Proof. We have proven (1) ⇒ (2) in Proposition 3.54 and (3) ⇒ (1) in Proposition 3.69. Together with (2) ⇒ (3), which is obvious, this shows that (1) $\iff$ (2) $\iff$ (3).

To see that (1) ⇒ (4), one argues similarly to Proposition 3.54, but uses a projective resolution for M to compute $\operatorname{Tor}_i^R(M, F)$. In detail, given $P_\bullet \xrightarrow{\sim} M$ a projective resolution of M, the complex $P_\bullet \otimes_R F \to 0$ is exact everywhere except for homological degree 0 since the functor $- \otimes_R F$ is exact due to the flatness of F. This yields that $\operatorname{Tor}_i^R(M, F) = 0$ for all $i \geq 1$ and for all R-modules M.

To see that (5) ⇒ (1), one takes a s.e.s of R-modules $0 \to M' \to M \to M'' \to 0$ and uses the following l.e.s of derived functors for $- \otimes_R F$:

$$0 \to M' \otimes_R F \to M \otimes_R F \to M'' \otimes_R F \to \operatorname{Tor}_1^R(M', F) \to \operatorname{Tor}_1^R(M, F) \to \operatorname{Tor}_1^R(M'', F) \to \cdots$$

Since $\operatorname{Tor}_1^R(M', F) = 0$, this yields a s.e.s

$$0 \to M' \otimes_R F \to M \otimes_R F \to M'' \otimes_R F \to 0$$

thus proving that the functor $- \otimes_R F$ is exact and hence F is flat.

Since (4) ⇒ (5) is obvious, this shows that (1) $\iff$ (4) $\iff$ (5). □

3.3.3 Where next?

If you are interested in learning more about homological algebra, Charles Weibel's textbook *"An Introduction To Homological Algebra"* is the gold standard reference for this topic. It gives a modern prespective and is written by an expert. But it may be a bit rough going for beginners, the treatment being at times quite terse. Much more user friendly and still very thorough is the second edition of Joseph Rotman's book of the same name (which is different from the recommended textbook for this course). Like everything by Rotman, it's a wonderful and enlightening read, with occasional tendencies towards verbosity.