MATH70063 ALGEBRA 4, 2026

WEEK 1

1. A bit of category theory

1.1. Basic definitions.

Definition 1.1. *A category $\mathcal{C}$ consists of the following: a collection* $\mathrm{ob}(\mathcal{C})$ *of objects, a set* $\mathrm{Hom}_{\mathcal{C}}(A,B)$ *of morphisms for every ordered pair* (A,B) *of objects, an identity morphism* $\mathrm{id}_A \in \mathrm{Hom}_{\mathcal{C}}(A,A)$ *for each object* $A \in \mathcal{C}$*, and a composition function* $\circ\colon \mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) \to \mathrm{Hom}_{\mathcal{C}}(A,C)$ *for every ordered triple* (A,B,C)*. The above data satisfies two axioms:*

(1) (Associativity): $(h \circ g) \circ f = h \circ (g \circ f)$ *for all* $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$*,* $g \in \mathrm{Hom}_{\mathcal{C}}(B,C)$*, and* $h \in \mathrm{Hom}_{\mathcal{C}}(C,D)$*.*

(2) (Unit): $\mathrm{id}_B \circ f = f = f \circ \mathrm{id}_A$ *for* $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$*.*

Definition 1.2. *A morphism* $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ *is called an* isomorphism *if there exists a morphism* $g \in \mathrm{Hom}_{\mathcal{C}}(B,A)$ *such that* $g \circ f = \mathrm{id}_A$ *and* $f \circ g = \mathrm{id}_B$*.*

Examples.

(1) The category of sets, denoted **Set**. Here morphisms are arbitrary functions. Note that the objects of this category do not form a set.

(2) The category of groups **Group**. Here morphisms are homomorphisms of groups.

(3) The category of (left) R-modules, where R is a ring, is denoted R-mod. Here morphisms are homomorphisms of R-modules. (We will discuss R-modules a lot more next week).

(4) The category of topological spaces, denoted **Top**. Here morphisms are continuous maps.

Examples.

(1) The category **Ab** of abelian groups is a full subcategory of **Group**.

(2) Every R-module can be considered as an abelian group. But this does not mean category of R-modules is a subcategory of the category of abelian groups. There's no way to look at an abelian group and say "that one is an R-module". Being an R-module involves extra structure. (Although, if $R = \mathbb{Q}$ this isn't really true...)

Definition 1.3. *A subcategory $\mathcal{D}$ of $\mathcal{C}$ is a sub-collection* $\mathrm{ob}(\mathcal{D}) \subseteq \mathrm{ob}(\mathcal{C})$ *and a subset* $\mathrm{Hom}_{\mathcal{D}}(A,B) \subseteq \mathrm{Hom}_{\mathcal{C}}(A,B)$ *for any two* $A, B \in \mathrm{ob}(\mathcal{D})$ *which contains all the identity morphisms of objects in* $\mathrm{ob}(\mathcal{D})$ *and which is closed under composition. So $\mathcal{D}$ is a category in its own right. We say that $\mathcal{D}$ is a full subcategory of $\mathcal{D}$ if* $\mathrm{Hom}_{\mathcal{D}}(A,B) = \mathrm{Hom}_{\mathcal{C}}(A,B)$ *for any two objects A, B of $\mathcal{D}$.*

Definition 1.4. *A map* $f\colon B \to C$ *is called* monic *in $\mathcal{C}$ if for any two distinct morphisms* $e_1, e_2\colon A \to B$ *we have* $f \circ e_1 \neq f \circ e_2$*; i.e., we can cancel f on the left. Similarly, f is called* epic *in $\mathcal{C}$ if for any two distinct morphisms* $g_1, g_2\colon C \to D$ *we have* $g_1 \circ f \neq g_2 \circ f$*; i.e., we can cancel f on the right.*

Exercises.

(1) Show that monic maps in the category **Set** of sets are precisely injective functions.

(2) Show that epic maps in the category **Set** of sets are precisely surjective functions.

(3) Show that the inclusion $\mathbb{Z} \subset \mathbb{Q}$ is epic in the category of rings.

(4) Show that the inclusion $\mathbb{Q} \subset \mathbb{R}$ is epic in the category of Hausdorff topological spaces (which is a full subcategory of **Top**.

(5) Describe a category with more that one object such that every map is monic and epic but any two distinct objects are not isomorphic.

Definition 1.5. *Every category $\mathcal{C}$ has an* opposite category $\mathcal{C}^{\mathrm{op}}$ *where the objects are the same as the objects in $\mathcal{C}$, but the morphisms (and compositions) are reversed, so that there is a one-to-one correspondence $f \mapsto f^{\mathrm{op}}$ between morphisms $f\colon B \to C$ in $\mathcal{C}$ and morphisms $f^{\mathrm{op}}\colon C \to B$ in $\mathcal{C}^{\mathrm{op}}$.*

Definition 1.6. *Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A* (covariant) functor $\mathcal{C} \to \mathcal{D}$ *is a rule that associates to every object C of $\mathcal{C}$ an object $F(C)$ of $\mathcal{D}$, and to every morphism $f\colon C_1 \to C_2$ in $\mathcal{C}$ a morphism $F(f)\colon F(C_1) \to F(C_2)$ in $\mathcal{D}$, such that the following conditions hold:*

(1) For each object A in $\mathrm{ob}(\mathcal{C})$, $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$,

(2) For each f in $\mathrm{Hom}_{\mathcal{C}}(A, B)$ and g in $\mathrm{Hom}_{\mathcal{C}}(B, C)$, $F(g \circ f) = F(g) \circ F(f)$.

Definition 1.7. *A* contravariant functor $F\colon \mathcal{C} \to \mathcal{D}$ *is a covariant functor from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{D}$.*

Example. For any category $\mathcal{C}$ and any object $A \in \mathrm{ob}(\mathcal{C})$, there is a contravariant functor $\mathrm{Hom}_{\mathcal{C}}(-, A)$ from $\mathcal{C}$ to **Set**.

Example. If R is a ring, then we noted that R-mod is not a subcategory of **Ab**. Instead, there is a functor $F\colon R\text{-mod} \to \mathbf{Ab}$ taking an R-module to its underlying abelian group, and a taking morphism of R-modules to the same morphism of abelian groups.

Definition 1.8. *Given two functors $F, G\colon \mathcal{C} \to \mathcal{D}$, a* natural transformation $\eta\colon F \Rightarrow G$ *is a rule that associates to every object C of $\mathcal{C}$ a morphism $\eta_C\colon F(C) \to G(C)$ in $\mathcal{D}$ such that for every morphism $f\colon C \to C'$ in $\mathcal{C}$ the following diagram commutes:*

$$\begin{array}{ccc} F(C) & \xrightarrow{F(f)} & F(C') \\ {\scriptstyle \eta_C}\downarrow & & \downarrow{\scriptstyle \eta_{C'}} \\ G(C) & \xrightarrow{G(f)} & G(C') \end{array}$$

If each $\eta_{\mathcal{C}}$ is an isomorphism, we say that η is a natural isomorphism and write $\eta\colon F \cong G$.

The set of natural transformations from F to G is written $\mathrm{Nat}(F, G)$. *(Or sometimes* $\mathrm{Hom}(F, G)$*, since natural transformations are analogous to homomorphisms between functors.)*

Examples.

(1) There are (at least) two obvious functors from **Set** to **Top**. The discrete topology functor $D\colon \mathbf{Set} \to \mathbf{Top}$ assigns to a set X the space X with the discrete topology, in which every set is open. The trivial (or indiscrete) topology functor $T\colon \mathbf{Set} \to \mathbf{Top}$ assigns to a set X the trivial topology, with only $\varnothing$ and X open. Note that the identity function gives a natural transformation $D \Rightarrow T$.

(2) For a k-vectorspace V there is a linear map $V \to V^{**}$ given by $v \mapsto (f \mapsto f(v))$. Show that this defines a natural transformation from the identity to the double dualisation functor on $\mathbf{Vect}_k$.

Definition 1.9. *We say a functor $F\colon \mathcal{C} \to \mathcal{D}$ is an* equivalence of categories *if there is a functor $G\colon \mathcal{D} \to \mathcal{C}$ and natural isomorphisms $\mathrm{id}_{\mathcal{C}} \cong GF$ and $\mathrm{id}_{\mathcal{D}} \cong FG$.*

Exercises.

(1) Define a category **Cat** whose objects are categories.

(2) For two categories $\mathcal{C}$ and $\mathcal{D}$ define the category of functors, denoted by $\mathrm{Fun}(\mathcal{C}, \mathcal{D})$ (or $[\mathcal{C}, \mathcal{D}]$), whose objects are functors from $\mathcal{C}$ to $\mathcal{D}$.

(3) Let k be a field. Let $\mathbf{fdVect}_k$ be the category whose objects are the finite dimensional k-vector spaces, and whose morphisms are linear maps. Show that $\mathbf{fdVect}_k$ is equivalent to the category $\mathbf{Mat}_k$ which is defined as follows: the objects of $\mathbf{Mat}_k$ are the non-negative integers. If $m, n \neq 0$ then the morphisms $m \to n$ are given by $m \times n$-matrices with coefficients in k. If $m = 0$ or $n = 0$ then assign a unique morphism $m \to n$ (this is the unique "zero-dimensional matrix"). Composition of morphisms is the usual matrix multiplication. You should notice that there is a choice involved in your solution.

Definition 1.10. *A functor $F\colon \mathcal{C} \to \mathcal{D}$ is called* faithful *if it is injective on* Hom*-sets, and is called* full *if it is surjective on* Hom*-sets. A functor which is both full and faithful is called* fully faithful*.*

Definition 1.11. *A* concrete *category is a category $\mathcal{C}$ together with a faithful functor to* **Set***.*

One can think of the objects of a concrete category as "sets with extra structure".

Here is a very famous lemma about functors to sets. We skipped in the lectures but it can surprisingly useful, so I'll write it down in case you find it helpful:

Proposition 1.12 (Yoneda's lemma)**.** *Let $F\colon \mathcal{C} \to \mathbf{Set}$ be a contravariant functor, and let A be an object of $\mathcal{C}$. Note that $\mathrm{Hom}_{\mathcal{C}}(-, A)\colon \mathcal{C} \to \mathbf{Set}$ is also a contravariant functor. There is a bijection of sets*

$$\mathrm{Nat}(\mathrm{Hom}_{\mathcal{C}}(-, A), F) \cong F(A).$$

Now let A and B be objects of $\mathcal{C}$. If there is a natural isomorphism of functors $\mathrm{Hom}_{\mathcal{C}}(-, A) \cong \mathrm{Hom}_{\mathcal{C}}(-, B)$, then $A \cong B$.

The second part of the lemma can be deduced from the first part by setting $F = \mathrm{Hom}_{\mathcal{C}}(-, B)$. It says that if you know how all the morphisms into an object A work, then you actually know the object A perfectly.

I'm going to leave the prove of Yoneda's lemma to an exercise sheet.

1.2. **Adjoint functors.**

Definition 1.13. *A pair of functors $L\colon \mathcal{C} \to \mathcal{D}$ and $R\colon \mathcal{D} \to \mathcal{C}$ are called* adjoint *if there is a set bijection for all $C \in \mathrm{ob}(\mathcal{C})$ and $D \in |\mathcal{D}|$:*

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

which is natural in C and D in the sense that for all $f\colon C \to C'$ in $\mathcal{C}$ and $g\colon D \to D'$ in $\mathcal{D}$ the following diagram commutes:

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathcal{D}}(L(C'), D) & \xrightarrow{-\circ L(f)} & \mathrm{Hom}_{\mathcal{D}}(L(C), D) & \xrightarrow{g\circ -} & \mathrm{Hom}_{\mathcal{D}}(L(C), D') \\
\downarrow{\scriptstyle \tau_{C',D}} & & \downarrow{\scriptstyle \tau_{C,D}} & & \downarrow{\scriptstyle \tau_{C,D'}} \\
\mathrm{Hom}_{\mathcal{C}}(C', R(D)) & \xrightarrow{-\circ f} & \mathrm{Hom}_{\mathcal{C}}(C, R(D)) & \xrightarrow{R(g)\circ -} & \mathrm{Hom}_{\mathcal{C}}(C, R(D'))
\end{array}$$

In this case, we say that L is left adjoint to R, or R is right adjoint to L.

Exercises.

(1) Let $U : \mathbf{Top} \to \mathbf{Set}$ be the underlying set functor. Determine (and prove) whether there are adjunctions involving U and the discrete/trivial topology functors D and T above.

(2) Show that right adjoints are unique in the sense if R_1, R_2 are both right adjoints of a functor L, then there is a natural isomorphism $R_1 \cong R_2$. The same goes for left adjoints. (This is a guided exercise on Problem Sheet 1, the best way to do it is probably to use Yoneda's lemma!).

(3) Show that there are two natural transformations

$$\eta\colon \mathrm{id}_{\mathcal{C}} \Rightarrow RL \qquad \text{and} \qquad \epsilon\colon LR \Rightarrow \mathrm{id}_{\mathcal{D}}$$

such that the composition $R \xRightarrow{\eta R} RLR \xRightarrow{R\epsilon} R$ is id_R and $L \xRightarrow{L\eta} LRL \xRightarrow{\epsilon L} L$ is id_L. η is called the *unit* of the adjunction, and ϵ is called the *co-unit*.

(4) Show that if you have two functors R and L, with natural transformations η, and ϵ satisfying the conditions in the previous part, then R and L must be an adjunction.

Example. Let **Ab** be the category of abelian groups (morphisms are group homomorphisms). There is a "forgetful" functor

$$F \ : \ \mathbf{Ab} \to \mathbf{Group}$$

which forgets that an abelian group is abelian (F is just the identity on objects and morphisms). It is obviously fully faithful.

There is also a functor in the other direction

$$(-)^{\mathrm{ab}} \ : \ \mathbf{Group} \to \mathbf{Ab}$$

which sends G to its abelianisation $G^{\mathrm{ab}} := G/[G,G]$. Here $[G,G]$ is the commutator subgroup; the subgroup of G generated by all commutators $aba^{-1}b^{-1}$.

I claim that $(-)^{\mathrm{ab}}$ is left adjoint to F. We need to show that for every group G and every abelian group A, the map

$$(*) \qquad \begin{aligned} &\mathrm{Hom}_{\mathbf{Ab}}(G^{\mathrm{ab}}, A) \to \mathrm{Hom}_{\mathbf{Group}}(G, A) \\ &(f : G^{\mathrm{ab}} \to A) \mapsto (\overline{f} : G \overset{s}{\twoheadrightarrow} G^{\mathrm{ab}} \xrightarrow{f} A) \end{aligned}$$

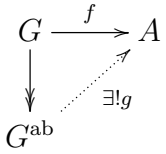
is a bijection, and natural in (G, A).

To see that $(*)$ is injective, consider two group homomorphisms $f, g : G^{\mathrm{ab}} \to A$ such that $\overline{f} = \overline{g}$. Then $f \circ s = g \circ s$ where s is the quotient map $s : G \twoheadrightarrow G^{\mathrm{ab}}$. But s is a surjective group homomorphism, so s is epic in **Group** (exercise!). Hence $f = g$ and $(*)$ is injective.

To see surjectivity, let $f : G \to A$ be a group homomorphism. Then f kills commutators because A is abelian:

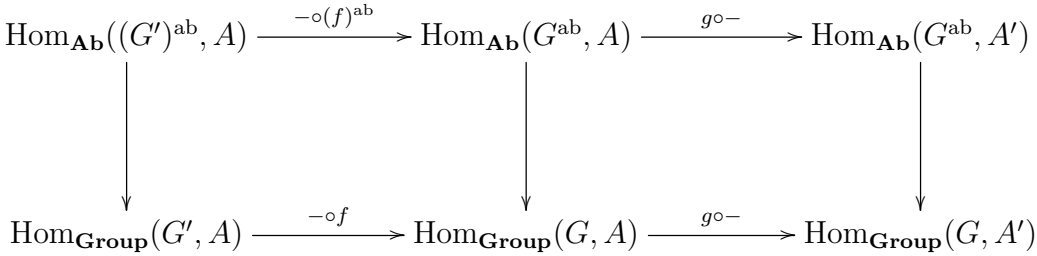
$$\begin{aligned} f(aba^{-1}b^{-1}) &= f(a)f(b)f(a)^{-1}f(b)^{-1} \\ &= f(a)f(a)^{-1}f(b)f(b)^{-1} \\ &= e\,. \end{aligned}$$

So f factors[1] through the quotient $G/[G,G] =: G^{\mathrm{ab}}$:



Clearly $g \mapsto f$ under $(*)$, so $(*)$ is also a surjection.

To see naturality, stare at the diagram

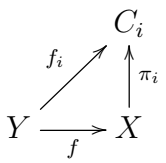


until it commutes.

WEEK 2

1.3. **Products and coproducts.**

Definition 1.14. *Let I be an index set, not necessarily finite, and let C_i, $i \in I$, be objects in a category $\mathcal{C}$. A* product *of $\{C_i : i \in I\}$ is an object $X \in \mathrm{ob}(\mathcal{C})$ together with morphisms $\pi_i \colon X \to C_i$, $i \in I$, such that for every object $Y \in \mathrm{ob}(\mathcal{C})$ and every family of morphisms $f_i \colon Y \to C_i$ there exists a unique morphism $f \colon Y \to X$ such that the following diagram commutes for all $i \in I$:*



Exercise. Show that if a product of $\{C_i : i \in I\}$ exists, then it is unique up to unique isomorphism.

In view of this, we generally refer to *the* product of $\{C_i : i \in I\}$, and denote it by $\prod_{i \in I} C_i$, or $C_1 \times C_2 \times \cdots$.

Examples.

[1] In fact it factors *uniquely* through the quotient. This is the same as the argument for injectivity of $(*)$.

(1) The product in **Set** is the usual Cartesian product of sets. In detail, supposes that we have sets X_i where i is an element of a set I. The product $\prod_{i\in I} X_i$ is defined as the set of all functions

$$f\colon I \longrightarrow \cup_{i\in I} X_i$$

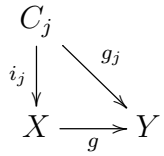
such that $f(i) \in X_i$ for all $i \in I$. This means that the set $\prod_{i\in I} X_i$ consists of 'vectors' $(x_i)_{i\in I}$, where $x_i \in X_i$ for all $i \in I$. (Here we write x_i for $f(i)$, where $i \in I$.)

(2) The product in the category of groups is the usual product of groups.

(3) The product in the category of R-modules, where R is a ring, is the direct product.

(4) The product in the category of topological spaces is the Cartesian product of underlying sets, equipped with the product topology.

Definition 1.15. *Let J be an index set, not necessarily finite, and let C_j, $j \in J$, be objects in a category $\mathcal{C}$. A* coproduct *of $\{C_j : j \in J\}$ is an object $X \in \mathrm{ob}(\mathcal{C})$ together with morphisms $i_j\colon C_j \to X$, $j \in J$, such that for every object $Y \in \mathrm{ob}(\mathcal{C})$ and every family of morphisms $g_j\colon C_j \to Y$ there exists a unique morphism $g\colon X \to Y$ such that the following diagram commutes for all $j \in J$:*



Exercise. Show that if a coproduct of $\{C_j : j \in J\}$ exists, then it is unique up to unique isomorphism.

In view of this, we generally refer to *the* coproduct of $\{C_j : j \in J\}$, and denote it by $\coprod_{j\in J} C_j$.

Examples.

(1) The coproduct in **Set** is the disjoint union.

(2) The coproduct in the category of vector spaces over k is the direct sum. Supposes that we have vector spaces V_i for $i \in I$. Then $\bigoplus_{i\in I} V_i$ is defined as the set of all functions

$$f\colon I \longrightarrow \cup_{i\in I} V_i$$

such that $f(i) \in V_i$ for all $i \in I$, and for each i, only finitely many $f(i)$ are nonzero.

(3) The coproduct in the category of R-modules, where R is a ring, is the direct sum (same definition as above)

(4) The coproduct in the category of groups is the free product.

Exercise. Show that coproducts in $\mathcal{C}$ are precisely products in $\mathcal{C}^{\mathrm{op}}$ (and vice versa!).

Remark. Products and coproducts are examples of limites and colimits (which also generalise kernels and cokernels, intersections and unions, etc etc). The **mastery material** is on limits and colimits.

2. Modules over a Ring

2.1. **Definitions and examples.** See [1, Ch.1, §1]

Let R be an associative ring with unit. Recall that this means that R is an abelian group with respect to addition (the group operation is denoted by $+$) that has an associative operation of multiplication (denoted by $\times$) such that

$$x(y+z) = xy + xz, \quad (x+y)z = xz + yz,$$

for any $x, y, z \in R$. We denote the unit in R by 1, so that $1 \times x = x \times 1 = x$ for any $x \in R$. Note that we do not require the multiplication in R to be commutative.

Let R^* denote the set of invertible elements in R, that is, the set of elements $x \in R$ for which there exists $y \in R$ such that $xy = 1$ and $yx = 1$. The set R^* is a group. If $R^* = R \setminus \{0\}$, then R is called a skew-field. If, moreover, R is commutative, then R is called a field.

Key examples of rings: the integers $\mathbb{Z}$; the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q$; polynomial rings $k[x_1, \ldots, x_n]$, where k is a field; the ring of square matrices $\mathrm{Mat}_n(k)$; the skew-field of quaternions $\mathbb{H}$.

The central concept of this course is that of a *module*.

Definition 2.1. *A left R-module M is an abelian group (written additively) with a function $\star : R \times M \to M$, called the left action of R, satisfying*

$$r \star (m_1 + m_2) = r \star m_1 + r \star m_2, \quad (r_1 + r_2) \star m = r_1 \star m + r_2 \star m,$$
$$1 \star m = m, \quad (r_1 r_2) \star m = r_1 \star (r_2 \star m),$$

for any $r, r_1, r_2 \in R$ and $m, m_1, m_2 \in M$.

Unless explicitly mentioned, all our modules are left modules.

Examples.

- $M = R^n$ with the coordinate-wise left action of R, i.e. $r \in R$ sends $(r_1, \ldots, r_n)$ to $(rr_1, \ldots, rr_n)$. These left R-modules are called *free of finite rank*.
- Any left ideal $I \subset R$ (i.e. a subgroup of R closed under left multiplication by the elements of R) is a left R-module.
- Given a linear transformation $L : V \to V$ of a vector space V over a field k one turns V into a $k[x]$-module by making x act by L.
- Take $R = \mathrm{Mat}_n(k)$ and $M = k^n$ identified with column vectors. The left action of R on M is defined by applying a square matrix to a column vector.

If there are left modules, there should be also right modules! Their definition is obtained by replacing the property $(r_1 r_2) \star m = r_1 \star (r_2 \star m)$ by

$$(r_1 r_2) \star m = r_2 \star (r_1 \star m).$$

An example of a right $\mathrm{Mat}_n(k)$-module is the vector space of row vectors k^n, on which square matrices act by right multiplication.

From now on we shall denote the action of R on a left module by rm and the action of R on a right module by mr. Thus for the left modules we have $(r_1 r_2)m = r_1(r_2 m)$, whereas for the right modules we have $m(r_1 r_2) = (mr_1)r_2$.

The *opposite* ring R^{op} of R is obtained by replacing the multiplication xy by yx. A right R-module is therefore the same as a left R^{op}-module. If R is commutative, then R^{op} is the same as R, and there is no difference between left and right modules.

Some familiar classes of objects can be interpreted as modules over a specific ring:

- Abelian groups = modules over the (commutative) ring $\mathbb{Z}$.
- Vector spaces over a field k = modules over field k.
- Representations of a group G over a field k = modules over the *group algebra* $k[G]$. This is the vector space over k with basis e_g, $g \in G$, with multiplication given by $e_g \cdot e_h = e_{gh}$.

A homomorphism (or simply a map) of left R-modules $f : L \to M$ is a homomorphism of groups that preserves the action of R: $f(rx) = rf(x)$ for any $r \in R$ and $x \in L$. An isomorphism (respectively an injective, respectively a surjective map) of R-modules is a bijective (respectively an injective, respectively a surjective) map of R-modules.

The category of left R-modules is denoted R-**mod**, and the category of left R-modules is denoted **mod**-R. This is relatively standard, but in the litturature you will see all sorts of different notations for this category.

A subgroup $L \subset M$ stable under the action of R is called a *submodule* of M. Since M is an abelian group under $+$, we can form the quotient group M/L. But L is R-stable, so we have a well defined action of R on M/L, which is called a *quotient module*.

For example, a left R-submodule of R is the same as a left ideal of R.

The collection of R-modules forms a category whose morphisms are R-module homomorphisms. Let's show that this category has all products and coproducts:

Let S be a set. Suppose we are given a left R-module M_s for each $s \in S$. The *direct product* $\prod_{s\in S} M_s$ of modules M_s as the product of sets M_s indexed by S, so that its elements are written as $(m_s)_{s\in S}$, where $m_s \in M_s$. The addition is defined coordinate-wise. The action of $r \in R$ multiplies each coordinate by r. For a fixed element $s_0 \in S$ the surjective map $\prod_{s\in S} M_s \to M_{s_0}$ that forgets all coordinates other than the s_0-coordinate is a map of R-modules. If all M_s are isomorphic to a given module M, we denote the direct product by M^S, because this is the same as the set of all functions $S \to M$.

The *direct sum* $\oplus_{s\in S} M_s$ is the submodule of $\prod_{s\in S} M_s$ given by the condition that all but finitely many coordinates are zero. For a fixed element $s_0 \in S$ the injective map $M_{s_0} \to \oplus_{s\in S} M_s$ that sends $m \in M_{s_0}$ to $(m_s)_{s\in S}$, where $m_s = 0$ if $s \neq s_0$ and $m_{s_0} = m$, is a map of R-modules. If S is finite, then there is no difference between the direct sum and the direct product.

Exercise. Check that the direct product just defined is a product in the category of R-modules. Check that the direct sum just defined is a coproduct in the category of R-modules.

A *free* module is a direct sum of copies of the left R-module R. In the particular case when the indexing set S is finite, a free module is isomorphic to R^n for some positive integer n.

Exercise. Show that there is an adjunction $F\colon \mathbf{Set} \leftrightarrows R\text{-}\mathbf{mod} : U$ where $F(S) = \oplus_{s\in S} R$ is the free module on R, and $U(M) = M$ is the underlying set of M.

Exercise. Let k be a field. Show that every k-module is free. (For finitely generated k-modules this is not too hard, for arbitrary k-modules you will need the axiom of choice.)

2.2. **Complexes of R-modules.** A sequence (finite or infinite) of modules and maps

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

is called a *complex* if $f_{n+1}f_n = 0$ whenever this is defined. A complex is called *exact* if $\ker(f_{n+1}) = \mathrm{im}(f_n)$ for all n. An exact complex of the form

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \tag{1}$$

is called a *short exact sequence*. To give a short exact sequence is the same as to give an injective map $\alpha : A \to B$ (then $C = B/\alpha(A)$), or a surjective map $\beta : B \to C$ (then $A = \ker(\beta)$). The map α gives an isomorphism of A with $\alpha(A)$, so we usually identify A with the submodule $\alpha(A) \subset B$, and identify C with the quotient module $B/\alpha(A)$.

An example of an exact sequence (and of a short exact sequence) is

$$0 \longrightarrow A \xrightarrow{\alpha} A \oplus C \xrightarrow{\beta} C \longrightarrow 0$$

where $\alpha(x) = (x, 0)$ and $\beta((x, y)) = y$. Such exact sequences are called *split*. Not all exact sequences are split, for example this sequence of abelian groups (=$\mathbb{Z}$-modules) is not:

$$0 \longrightarrow \mathbb{Z}/2 \xrightarrow{\alpha} \mathbb{Z}/4 \xrightarrow{\beta} \mathbb{Z}/2 \longrightarrow 0 \tag{2}$$

Here α is the unique non-zero homomorphism. It sends $1 \in \mathbb{Z}/2$ to $2 \in \mathbb{Z}/4$, and identifies $\mathbb{Z}/2$ with the unique subgroup of $\mathbb{Z}/4$ of order 2.

Proposition 2.2. *A short exact sequence*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0 \tag{3}$$

of left R-modules is split if and only if there is a map of R-modules $\sigma : C \to B$ such that $\beta\sigma = \mathrm{id}_C$. (Such a map is called a **section** *of β.) Equivalently, if there is a map $\rho : B \to A$ such that $\rho\alpha = \mathrm{id}_A$. (Such a map is called a* **retraction** *of α.)*

Proof. If the sequence is split, then σ and ρ are the obvious maps.

Now suppose that σ exists. We need to construct an isomorphism $f\colon B \xrightarrow{\sim} A \oplus C$ so that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{(\mathrm{id}_A, 0)} & A \oplus C & \xrightarrow{(0, \mathrm{id}_C)} & C & \longrightarrow & 0 \\ & & {\scriptstyle \mathrm{id}_A}\uparrow{\scriptstyle \cong} & & {\scriptstyle f}\uparrow{\scriptstyle \cong} & & {\scriptstyle \mathrm{id}_C}\uparrow{\scriptstyle \cong} & & \\ 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \end{array}$$

Let $f : B \to A \oplus C$ be the map

$$f(b) = (\alpha^{-1}(b - \sigma\beta(b)), \beta(b)).$$

It is well defined because $b - \sigma\beta(b) \in \ker(\beta) = \mathrm{im}(\alpha)$ and α is injective. We need to prove that f is both injective and surjective.

f is injective: If $f(b) = 0$, then $\beta(b) = 0$, and since $\ker(\beta) = \alpha(A)$ we have $b = \alpha(a)$ for some $a \in A$. But f sends $\alpha(a)$ to $(a, 0)$, so if this is 0, then $b = 0$.

f is surjective: Let $a \in A$ and $c \in C$. Then $f(\sigma(c) + \alpha(a)) = (a, c)$.

The remainder of the Proposition is proved in the next Exercise. □

Exercises.

(1) Prove the second claim of Proposition 2.2.

(2) Show that sequence (3) is split when C is a free R-module.

2.3. **Injective and projective modules.** See [1, Ch. 1, §2,3]

Definition 2.3. *Let A and B be R-modules. We call A a* **direct summand** *of B if there is an R-module C such that there is an isomorphism of R-modules $A \oplus C \cong B$.*

For example, if $M = \oplus_{s\in S} M_s$ is a direct sum of modules, then each M_s is a direct summand of M.

It follows from proposition 2.2 that A is a direct summnand of B if and only if there is a map $p\colon B \to A$ and a map $s\colon A \to B$ such that $ps = \mathrm{id}_A$ (execise: understand this).

Definition 2.4. *An R-module M is called* **projective** *if for any short exact sequence (3) and any map of R-modules $f : M \to C$ there is a map of R-modules $g : M \to B$ such that $f = \beta g$. One says that f 'lifts' to g, or that g is a 'lifting' of f.*

If C is projective, then (3) has a section and so is split.

Lemma 2.5. *A direct sum is projective if and only if each summand is projective.*

Proof. Let $M = \oplus_{s\in S} M_s$ and $f : M \to C$. If M_s is projective for each $s \in S$, then the restriction of f to each M_s (embedded into M in the obvious way), call it $f_s : M_s \to C$, lifts to $g_s : M_s \to B$. By definition each element of the direct sum has only finitely many non-zero coordinates, hence $g := \sum_{s\in S} g_s$ is a well defined function $M \to B$. It is clear that $\beta g = f$.

Conversely, assume that M is projective. A map $f_s : M_s \to C$ for one element $s \in S$ extends trivially to a map $f : M \to C$ whose restriction to any other summand is zero. It lifts to a map $g : M \to B$. Restricting to M_s we get a lifting of f_s. □

WEEK 3

Proposition 2.6 (Criterion of projectivity)**.** *A module is projective if and only if it is a direct summand of a free module.*

Proof. Any module M is a quotient of the free module F freely generated as an R-module by the elements of M. In other words, F consists of $(r_m)_{m\in M}$, where each $r_m \in R$ and only finitely many r_m can be non-zero. There is a natural map of R-modules $F \to M$ sending $(r_m)_{m\in M} \in F$ to $\sum_{m\in M} r_m m \in M$. When M is projective, there is a section. By Proposition 2.2 M is a direct summand of F.

The R-module R is projective, because one element (namely, 1) can be lifted. By Lemma 2.5 all free modules are projective. Again by Lemma 2.5 a direct summand of a free module is projective. □

The fact that every R-module is a quotient of a projective R-module is usually stated as 'the category of left R-modules has enough projectives'.

Example (Projective modules are not always free)**.** Let $R = \mathbb{Z}/6$ and let M be the principal ideal of R generated by 3, so that $M \cong \mathbb{Z}/2$. The abelian group $\mathbb{Z}/6$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/3$. One checks that this gives an isomorphism of $\mathbb{Z}/6$-modules $\mathbb{Z}/6 \cong \mathbb{Z}/2 \oplus \mathbb{Z}/3$. Hence $\mathbb{Z}/2$ is a projective $\mathbb{Z}/6$-module. Since 2 is not a power of 6, it is certainly not free.

An R-module M is called *injective* if for any exact sequence (3) and for any map of R-modules $f : A \to M$ there is a map of R-modules $g : B \to M$ such that $f = g\alpha$. One says that g 'extends' f.

The theory of injective modules is in a certain sense 'dual' to the theory of projective modules. If A is injective, then (3) has a retraction and so is split.

Lemma 2.7. *A direct product is injective if and only if each factor is injective.*

Proof. Let $M = \prod_{s \in S} M_s$ be a direct product of R-modules and let $f : A \to M$ be a map of R-modules. If M_s is injective for each $s \in S$, then the s-coordinate of f, which is a map $f_s : A \to M_s$, is such that there exists $g_s : B \to M_s$ with the property $g_s\alpha = f_s$. The product (which can be infinite) $g := \prod_{s \in S} g_s$ is a well defined function $B \to M$. It is clear that $g\alpha = f$.

Conversely, assume that M is injective. A map $f_s : A \to M_s$ for one element $s \in S$ extends trivially to a map $f : A \to M$ (all coordinates zero except s). Then there is a map $g : B \to M$ such that $g\alpha = f$. The s-coordinate g_s of g has the desired property $g_s\alpha = f_s$. □

Theorem 2.8 (Baer's criterion of injectivity)**.** *A left R-module M is injective if and only if for any map of left R-modules $f : I \to M$, where I is a left ideal of R, there is an element $m \in M$ such that f has the form $f(x) = xm$.*

Equivalently, M is injective if and only if for any left ideal I of R, any map of left R-modules $I \to M$ extends to a map of left R-modules $R \to M$.

Proof. To see the equivalence of two properties we note that to give a map of left R-modules $R \to M$ is the same as to specify the image of $1 \in R$. So if $f(x) = xm$ for any $x \in I$, then f can be extended to R by sending 1 to m. Conversely, any map $I \to M$ which is a restriction of some map $F : R \to M$ has the form $F(x) = xF(1)$.

Now let's prove the theorem. If M is injective, then any $f : I \to M$ extends to a map of R-modules $R \to M$, so one direction is clear.

The proof of the converse uses *Zorn's lemma*. Let us recall its statement. Let S be a non-empty set with a partial order $\leq$. A totally ordered subset $C \subset S$ is called a *chain*. An *upper bound* of a subset of S is an element $t \in S$ such that $t \geq x$ for any x in this subset. Zorn's lemma states that if any chain in S has an upper bound, then S has a maximal element, that is, an element $m \in S$ such that $m \leq x$ for $x \in S$ implies $m = x$.

Let $A \subset B$ be left R-modules and let $g : A \to M$ be a map of left R-modules. To show that M is injective we need to show that g extends to a map of R-modules $B \to M$. Let S be the set of pairs (A', g'), where A' is a submodule of B containing A and $g' : A' \to M$ is a map of R-modules whose restriction to A is g. We make S a partially ordered set: $(A', g') \leq (A'', g'')$ if $A' \subset A''$ and the restriction of g'' to A' is g'. Each chain in S has an upper bound: take the union of the submodules A' in this chain; this is a submodule of B together with a map of R-modules to M which extends g: $A \to M$. By Zorn's lemma S has a maximal element. Call it (A_0, g_0).

Let us prove that $A_0 = B$. Otherwise there is a $b \in B$, $b \notin A_0$. Let A_1 be the set of all sums $a + xb$, where $a \in A_0$ and $x \in R$. This is clearly an R-module and $A_0 \subsetneq A_1$. To deduce a contradiction it is enough to extend g_0 to $g_1 \colon A_1 \to M$, for which we need to define the image $m = g_1(b) \in M$. Any m will do provided the map $Rb \to M$ sending b to m agrees with g_0 on $A_0 \cap Rb = \{xb \in A_0 | x \in R\}$. We note that the set of $x \in R$ such that $xb \in A_0$ is a left ideal $I \subset R$. Thus the required $m \in M$ exists precisely when the map of left R-modules $I \to Ib \xrightarrow{g_0} M$ has the form $x \mapsto xm$ for some $m \in M$. Indeed, define the map $g_1 \colon A_1 = A_0 + Rb \to M$ by sending $a + xb$ to $g_0(a) + xm$, where $a \in A_0$ and $x \in R$. We need to check that g_1 is well defined, i.e. if $a + xb = a' + x'b$ for $a, a' \in A_0$ and $x, x' \in R$, then $g_0(a) + xm = g_0(a') + x'm$. But $a - a' = (x' - x)b$, hence $x - x' \in I$ and in this case $g_0(a) - g_0(a') = g_0(a - a') = g_0((x' - x)b) = (x' - x)m$, so g_1 is indeed well defined. It is clearly a map of left R-modules, so we get the desired contradiction. □

Exercises.

(1) Let $R = k[\![x]\!]$ be a power series ring over a field k. Let $M = k[x^{-1}]$ be the polynomial ring in x^{-1}, thought of as an R-module in the following way: for i, j natural numbers $x^i \cdot x^{-j} = x^{i-j}$ if $i \geq j$, and $x^i \cdot x^{-j} = 0$ otherwise. For a power series $f = \sum \alpha_i x^i$ we extend $f \cdot x^{-j} = \sum \alpha_i x^i \cdots x^{-j}$. Check that this is well-defined (i.e. the sum is finite) and makes M into an R-module. (Another way to define this is $M = (k[\![x]\!]_x)/k[\![x]\!]$, inverting x then factoring out by the powerseries.) Use Baer's criterion to show that M is an injective R-module. If you want to read more about injective modules like this you can search for "Matlis duality".

(2) Let n be a natural number and set $R = \mathbb{Z}/n\mathbb{Z}$. Using Baer's criterion and a bit of number theory, show that $M = \mathbb{Z}/n\mathbb{Z}$ is an injective R-module. Rings R such that the free module R is injective are called self-injective.

0.1. Hom (or "what does projective/injective really mean?") See [1, Ch. 2, §2,4]

Let A and B be left R-modules. We denote by $\mathrm{Hom}_R(A, B)$ the set of maps of R-modules $A \to B$. It is an abelian group under addition of maps (check this!). If R is a commutative ring then $\mathrm{Hom}_R(A, B)$ is an R-module: if $f \in \mathrm{Hom}_R(A, B)$ and $r \in R$ then rf is the map $rf(a) = rf(a) = f(ra)$. This doesn't work if R is non-commutative (check this too!).

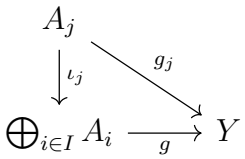
Proposition 2.9. *There are canonical isomorphisms*

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

and

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

Proof. This follows immediately from the universal property of products and coproducts. For example, remember that there are maps (the obvious inclusions) $\iota_i \colon A_i \to \bigoplus_{i \in I} A_i$ such that for every R-module Y and every family of R-module homomorphisms $g_i \colon A_i \to Y$, $i \in I$, there exists a unique morphism $g \colon \bigoplus_{i \in I} A_i \to Y$ such that the following diagram commutes for all $j \in I$:



The first isomorphism is given by $f \mapsto (f \circ \iota_i)_{i\in I}$. The inverse sends $(f_i)_{i\in I}$ to the unique R-module map $f\colon \bigoplus_{i\in I} A_i \to B$ making the diagrams

$$\begin{array}{ccc} A_j & & \\ \downarrow{\scriptstyle \iota_j} & \searrow^{f_j} & \\ \bigoplus_{i\in I} A_i & \xrightarrow[f]{} & B \end{array}$$

commute. The argument for the second isomorphism is similar. □

Corollary 2.10. *There are canonical isomorphisms*

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

and

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

Proof. Finite products are the same as finite coproducts in the category of R-modules and the category of abelian groups. □

Remark. There is a map

$$\bigoplus_{i\in I} \mathrm{Hom}_R(A, B_i) \to \mathrm{Hom}_R\Big(A, \bigoplus_{i\in I} B_i\Big)$$

but this may not be an isomorphism if I is infinite. Consider the case $A = \bigoplus_{i\in I} B_i$ where each B_i is non-zero. Then the identity map on A is not in the image of the map is if I is infinite. Modules A such that the above map is an isomorphism for all families $\{B_i\}$ are sometimes called compact.

Similarly,

$$\bigoplus_{i\in I} \mathrm{Hom}_R(A_i, B) \to \mathrm{Hom}_R\Big(\prod_{i\in I} A_i, B\Big)$$

need not be an isomorphism.

Note that the group $\mathrm{Hom}_R(R, M)$ is canonically isomorphic to M via the map sending $f\colon R \to M$ to $f(1)$.

Let

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0 \tag{1}$$

be an exact sequence of left R-modules.

Lemma 2.11.

(1) The sequence

$$0 \to \mathrm{Hom}_R(A_3, B) \to \mathrm{Hom}_R(A_2, B) \to \mathrm{Hom}_R(A_1, B)$$

is exact.

(2) B is injective if and only if

$$0 \to \mathrm{Hom}_R(A_3, B) \to \mathrm{Hom}_R(A_2, B) \to \mathrm{Hom}_R(A_1, B) \to 0$$

is exact for every short exact sequence (1).

Proof. You can directly check that (i) always works, and (ii) follows from the definition of injective. Check this! □

Lemma 2.12.

(1) The sequence

$$0 \to \mathrm{Hom}_R(B, A_1) \to \mathrm{Hom}_R(B, A_2) \to \mathrm{Hom}_R(B, A_3)$$

is exact.

(2) B is projective if and only if

$$0 \to \mathrm{Hom}_R(B, A_1) \to \mathrm{Hom}_R(B, A_2) \to \mathrm{Hom}_R(B, A_3) \to 0$$

is exact for every short exact sequence (1).

Proof. Once again can directly check that (i) always works, and (ii) follows from the definition of projective. Check this! □

WEEK 4

0.2. Tensor product. Now we would like to define the tensor product. This is an abelian group associated to two R-modules (one left one right) that "classifies bilinear maps".

Let A be a right R-module and B a left R-module. If R is a commutative ring then we don't need to think about left or right: we just take two R-modules.

Let F be the free abelian group generated by pairs (a, b) with $a \in A$, $b \in B$.

(Note this this not the abelian group $A \oplus B$ *consisting* of pairs (a, b). It is freely generated by them, so it contains things like $2(a, b) - 5(a', b')$. Typically F will have infinitely many generators.)

Let $S \subseteq F$ be the subgroup generated by all elements of the form

$$(a + a', b) - (a, b) - (a', b), \quad (a, b + b') - (a, b) - (a, b'),$$

and also by the elements

$$(ar, b) - (a, rb).$$

for all $r \in R$. In particular, we have relations $n(a, b) = (na, b) = (a, nb)$, where $a \in A, b \in B, n \in \mathbb{Z}$.

Define

$$A \otimes_R B = F/S.$$

The image of the generator $(a, b) \in F$ in $A \otimes_R B$ is denoted by $a \otimes b$. From the definition we obtain the relations

$$(a + a') \otimes b = a \otimes b + a' \otimes b, \qquad a \otimes (b + b') = a \otimes b + a \otimes b',$$

$$ar \otimes b = a \otimes rb,$$

for all $a, a' \in A$, $b, b' \in B$, and $r \in R$.

Remark. Let us calculate $R \otimes_R M$, where R is a right module over itself, and M is a left R-module. The abelian group $R \otimes_R M$ is generated by elements $r \otimes m = 1 \otimes rm$, so the map

$$f \colon M \to R \otimes_R M, \qquad m \mapsto 1 \otimes m$$

is surjective. Let us prove that f is injective, and hence an isomorphism. Let F be the free abelian group with generators (r, m), $r \in R$, $m \in M$. Define

$$g \colon F \to M$$

as the map sending the generator (r, m) to $rm \in M$ (this makes sense because F is a free abelian group). We then check that the following elements of F go to 0: $(r + r', m) - (r, m) - (r', m)$, $(r, m + m') - (r, m) - (r, m')$, and $(r, m) - (1, rm)$, for any $r, r' \in R$ and any $m, m' \in M$. Then g sends the subgroup $S \subseteq F$ generated by these elements to 0, hence g descends to a homomorphism $F/S = R \otimes_R M \longrightarrow M$. The composition $m \longmapsto 1 \otimes m \longmapsto m$ is id_M, thus we have an isomorphism

$$f\colon M \xrightarrow{\sim} R \otimes_R M.$$

Let us denote by

$$\varphi\colon A \times B \to A \otimes_R B$$

the function sending (a, b) to $a \otimes b$. In general, φ is neither surjective nor injective. This is one reason why the tensor product $A \otimes_R B$ is so different from the usual product of two abelian groups $A \times B$. When Emmy Noether invented the tensor product she did not like this fact, and said that A and B should be considered part of the data of $A \otimes_R B$, so that you can recover them. Now this is not considered an issue.

In the case $R = \mathbb{Z}$ we obtain the tensor product of abelian groups G_1 and G_2, denoted by $G_1 \otimes_{\mathbb{Z}} G_2$. For example, as a particular case of the canonical isomorphism $R \otimes_R M \cong M$, we obtain a canonical isomorphism $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}$. Similarly, $\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/2 \cong \mathbb{Z}/2$. Sometimes the result of tensor multiplication can be counter-intuitive. For example, $\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/3 = 0$. This follows from the relations $2(a \otimes b) = 2a \otimes b = 0 \otimes b = 0$ and $3(a \otimes b) = a \otimes 3b = a \otimes 0 = 0$, hence $a \otimes b = 0$ for all $a \in A$ and $b \in B$.

From the definition of tensor product we see that if $f\colon A \to A'$ is a map of right R-modules, then there is a natural map

$$f \otimes \mathrm{id}\colon A \otimes_R B \to A' \otimes_R B$$

sending $x \otimes y$ to $f(x) \otimes y$.

Indeed, write $A \otimes_R B = F/S$ and $A' \otimes_R B = F'/S'$. Then f defines a map $F \to F'$ sending each generator (a, b) to $(f(a), b)$. We claim that this map sends S to S'. For example, $(x + x', y) - (x, y) - (x', y)$ goes to $(f(x) + f(x'), y) - (f(x), y) - (f(x'), y) \in S'$, and $(xr, y) - (x, ry)$ goes to $(f(x)r, y) - (f(x), ry) \in S'$. Thus we obtain a map $F/S \to F'/S'$, which is the desired map $f \otimes \mathrm{id}\colon A \otimes_R B \to A' \otimes_R B$.

There is a similar construction for the second argument. We conclude that tensor product is a covariant functor in each argument.

The universal property of the tensor product states that if there is a function

$$f\colon A \times B \to C$$

which is linear in each argument and satisfies $f(ar, b) = f(a, rb)$ (for example, the function $\varphi\colon A \times B \to A \otimes_R B$ above), then f can be written uniquely as $f = g \circ \varphi$ for a homomorphism

$$g\colon A \otimes_R B \to C.$$

This is an immediate consequence of the definition $A \otimes_R B = F/S$.

Remark. If M is a right R-module and N is a left R-module then $M \otimes_R N$ is an abelian group. Any way of trying to make it an R-module will fail in general (although it might succeed in specific situations). If R is commutative, then left and right R-modules are essentially the same thing, and the tensor product of two R-modules produces an R-module (check this!).

Example. Let k be a field and let U, V, W be finite dimensional k-vector spaces. Assume $V \neq 0$ and set $R = \mathrm{End}_k(V)$ (so R is isomorphic to a matrix algebra, which in particular means it is very non-commutative).

The vector space $\mathrm{Hom}_k(U, V)$ is a left R-module using post-composition: $r \cdot f = r \circ f$ for $r \in R$ and $f \in \mathrm{Hom}_k(U, V)$. Likewise $\mathrm{Hom}_k(V, W)$ is a right R-module using pre-composition: $g \cdot r = g \circ r$ for $r \in R$ and $g \in \mathrm{Hom}_k(V, W)$.

Exercise: prove that the map $\mathrm{Hom}_k(V, W) \otimes_R \mathrm{Hom}_k(U, V) \to \mathrm{Hom}_k(U, W)$ given by $g \otimes f \mapsto g \circ f$ is an isomorphism.

This example should hopefully make it clear that the tensor product of two R-modules doesn't need to be an RF module, because in this example the result $\mathrm{Hom}_k(U, W)$ has nothing to do with V.

Proposition 2.13 (The tensor-hom adjunction)**.** *If R is a commutative ring and A, B, C re R-modules, then there is a natural isomorphism*

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

Proof. I'll leave this one to the exercise sheet. □

Remark. The previous preposition says that $- \otimes_R B$ is left adjoint to $\mathrm{Hom}_R(B, -)$.

Example. Let A be an abelian group and let n be a positive integer. The is an exact sequence

$$0 \longrightarrow A[n] \longrightarrow A \xrightarrow{n} A \longrightarrow A/nA \longrightarrow 0, \tag{3}$$

where

$$A[n] = \{a \in A \mid na = 0\}.$$

This need not be trivial, for example the case $A = \mathbb{Z}/n$.

We can view this as a tensor product of A with the short exact sequence The short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/n \longrightarrow 0.$$

That is, we can check that $A/nA \cong A \otimes_{\mathbb{Z}} \mathbb{Z}/n$. and tensor the short exact sequence with A to get

$$0 \longrightarrow A[n] \longrightarrow A \otimes_{\mathbb{Z}} \mathbb{Z} \longrightarrow A \otimes_{\mathbb{Z}} \mathbb{Z} \longrightarrow A/nA \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0.$$

We will later come back to where this extra term $A[n]$ comes from, in terms of the tensor product.

There is a canonical isomorphism

$$A \otimes_R (B \oplus C) \cong (A \otimes_R B) \oplus (A \otimes_R C).$$

More generally, we have the following lemma.

Lemma 2.14 (Lemma 0.5)**.** *If M_i, $i \in I$, are left R-modules, then there is a canonical isomorphism*

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

Proof. On the one hand, the natural map $A \times \left(\bigoplus_{i\in I} M_i\right) \longrightarrow \bigoplus_{i\in I}(A \otimes_R M_i)$ satisfies the assumptions of the universal property of the tensor product, hence factors through a homomorphism

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

On the other hand, the natural maps

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

give rise to the homomorphism

$$\nu : \bigoplus_{i\in I}(A \otimes_R M_i) \longrightarrow A \otimes_R \left(\bigoplus_{i\in I} M_i\right)$$

Direct calculation shows that $\mu\nu$ and $\nu\mu$ are the identity maps. □

Lemma 2.15 (Lemma 0.6)**.** *Let*

$$0 \longrightarrow A_1 \xrightarrow{\alpha} A_2 \xrightarrow{\beta} A_3 \longrightarrow 0 \tag{2}$$

be an exact sequence of right R-modules. For any left R-module B, the sequence of abelian groups

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

is exact.

Proof. Let Q be the quotient of $A_2 \otimes_R B$ by the image of $\alpha \otimes \mathrm{id}$. We have a natural map

$$u : Q \longrightarrow A_3 \otimes_R B.$$

It is enough to show that it is an isomorphism.

Since β is surjective, we can choose a set-theoretic section of $A_2 \to A_3$, i.e. a function (not necessarily a homomorphism and not necessarily respecting the action of R)

$$s : A_3 \to A_2$$

such that $\beta s = \mathrm{id}_{A_3}$.

Now define a function

$$A_3 \times B \longrightarrow Q$$

by sending a pair (a, b), where $a \in A_3$ and $b \in B$, to the element of Q which is the coset of $s(a) \otimes b$. This map does not depend on the choice of s, because a different set-theoretic section will change $s(a) \otimes b$ by $(\alpha(x), b)$, where $x \in A_1$, and in Q this is $\alpha(x) \otimes b = 0$. Similar calculations show that our function $A_3 \times B \to Q$ is bilinear and sends (ar, b) and (a, rb) to the same element of Q. For example, linearity in the first argument follows from the fact that for any $a, a' \in A_3$ we have $s(a + a') - s(a) - s(a') \in \alpha(A_1)$, because β sends this element to zero, hence $s(a + a') \otimes b - s(a) \otimes b - s(a') \otimes b$ is in the image of $\alpha \otimes \mathrm{id}$.

By the universal property of the tensor product, the function $A_3 \times B \to Q$ factors through a homomorphism of abelian groups

$$v : A_3 \otimes_R B \longrightarrow Q.$$

By construction we have

$$uv = \mathrm{id}_{A_3\otimes_R B}.$$

For any $x \in A_2$ we have $\beta(x - s\beta(x)) = 0$, so $x - s\beta(x) \in \alpha(A_1)$, and this implies that

$$vu = \mathrm{id}_Q.$$

Thus v is the inverse of u, so u is an isomorphism. □

Definition 2.16. *A left R-module B is called* flat *if $- \otimes_R B$ preserves short exact sequences of right R-modules.*

So we just saw that $\mathbb{Z}/n$ is not flat as an abelian group.

Lemma 2.17. *A direct sum of R-modules $M = \bigoplus_{i \in I} M_i$ is flat if and only if each M_i is flat.*

Proof. By definition $M = \bigoplus_{i \in I} M_i$ is flat if and only if for every short exact sequence of right R-modules

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0$$

the induced sequence

$$0 \longrightarrow A_1 \otimes_R \Big(\bigoplus_{i \in I} M_i\Big) \longrightarrow A_2 \otimes_R \Big(\bigoplus_{i \in I} M_i\Big) \longrightarrow A_3 \otimes_R \Big(\bigoplus_{i \in I} M_i\Big) \longrightarrow 0$$

is exact. By Lemma 0.5, this sequence is

$$0 \longrightarrow \bigoplus_{i \in I} (A_1 \otimes_R M_i) \longrightarrow \bigoplus_{i \in I} (A_2 \otimes_R M_i) \longrightarrow \bigoplus_{i \in I} (A_3 \otimes_R M_i) \longrightarrow 0.$$

This sequence is exact if and only if

$$0 \longrightarrow A_1 \otimes_R M_i \longrightarrow A_2 \otimes_R M_i \longrightarrow A_3 \otimes_R M_i \longrightarrow 0$$

is exact for each $i \in I$, i.e. if and only if each M_i is a flat R-module. □

Proposition 2.18. *Projective modules are flat.*

Proof. Lemma 0.10 says that a direct sum of modules is flat if and only if each summand is flat. The isomorphism

$$M \cong R \otimes_R M$$

shows that R is flat. Lemma 0.10 therefore implies that all free modules are flat. But every projective module is a summand of a free module. □

We will see later that the converse is not true.

Lemma 2.19. *If M is a flat left R-module, then for any non-zero divisor $a \in R$ and non-zero $m \in M$ we have $am \neq 0$.*

Proof. Consider the injective map $R \to R$ of right R-modules sending 1 to a. If M is flat, then the induced map $R \otimes_R M \longrightarrow R \otimes_R M$ is also injective. The identification $m \mapsto 1 \otimes m$ of M with $R \otimes_R M$ allows us to rewrite this map as the map $M \to M$ sending m to am. □

3. Modules over Integral Domains

3.1. **Torsion and divisible submodules.** See [1, Ch. VII, §1]

Let R be an integral domain, that is, a commutative ring with unit such that $ab = 0$ implies $a = 0$ or $b = 0$.

An element $m \in M$ is a torsion element if $rm = 0$ for some $r \in R$, $r \neq 0$. Define M_{tors} as the subset of torsion elements in M; this is a submodule. If $M_{\text{tors}} = 0$, then M is called torsion-free. If $M = M_{\text{tors}}$, then M is called a torsion module.

Examples. Abelian groups $\mathbb{Z}$ and $\mathbb{Q}$ are torsion-free, whereas $\mathbb{Z}/n$ and $\mathbb{Q}/\mathbb{Z}$ are torsion groups (as long as $n \neq 0$).

Lemma 3.1. *Flat (and hence also projective) modules over integral domains are torsion-free.*

Proof. If r is a nonzero element of R then $R \xrightarrow{r} R$ is an injective map of R-modules. If F is flat then applying $F \otimes_R -$ shows that $F \xrightarrow{r} F$ is injective as well, so F is torision free. □

An element $x \in M$ is (infinitely) divisible if for any $r \in R$, $r \neq 0$, we can write $x = ry$ for some $y \in M$. Define M_{div} as the subset of infinitely divisible elements in M; this is a submodule. If $M = M_{\text{div}}$, then M is called an infinitely divisible module. Often the word "infinitely" is omitted.

Examples. Abelian groups $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{Q}$ are divisible, whereas $\mathbb{Z}$ and $\mathbb{Z}/n$ are not. Despite what I said in the lecture, $\mathbb{Z}/n$ is not a divisible $\mathbb{Z}$-module even when n is a prime, although it is a divisible $\mathbb{Z}/n$-module in this case.

Lemma 3.2. *Injective modules are divisible.*

Proof. Let $m \in M$ and let $r \in R$, $r \neq 0$. We need to show that there is an $s \in M$ such that $m = rs$.

We note that the principal ideal $I = rR$ and the ring R are isomorphic as R-modules: the map $x \mapsto rx$ is an isomorphism

$$R \xrightarrow{\sim} I$$

since R has no zero divisors.

The map of R-modules $R \to M$ sending x to xm composed with the inverse of the isomorphism $R \xrightarrow{\sim} I$ gives a map of R-modules

$$f : I \to M$$

such that $f(rx) = xm$ for any $x \in R$.

Consider the natural inclusion of the principal ideal I into R. Since M is injective, $f : I \to M$ extends to a map of R-modules

$$F : R \to M.$$

We claim that $s = F(1)$ does the job. Indeed,

$$rs = rF(1) = F(r) = f(r) = m.$$

□

WEEK 5

3.2. **Modules over principal ideal domains.** A principal ideal domain (PID) is an integral domain where every ideal is principal. The crucial example for this section is the category of $\mathbb{Z}$-modules, that is, abelian groups.

Theorem 3.3. *If R is a PID, then every submodule of a free module is free. Every submodule of R^n is isomorphic to R^m for some $m \leq n$.*

Proof. Let S be the indexing set of the free R-module $\oplus_{s\in S} R$, and let M be a submodule of $\oplus_{s\in S} R$. Given a subset $T \subseteq S$ write $M_T = M \cap \oplus_{s\in T} R$. We are going to use Zorn's lemma to show that $M = M_S$ is free.

Consider the set of pairs (T, B) such that $T \subseteq S$ and M_T is free on the basis $B \subseteq M_T$. Partially order this set by $(T, B) \leq (T', B')$ if $T \subseteq T'$ and $B \subseteq B'$.

This partially ordered set is nonempty since $M_\varnothing = 0$ is free.

We claim that, given a chain $\{(T_i, B_i)\}$, with each M_{T_i} a free module free on B_i, then setting $T = \bigcup T_i$, the module M_T is free on the basis $B = \bigcup B_i$. First, B spans M_T since any element of M_T belongs to M_{T_i} for some i, so it is spanned by B_i. Secondly, if there is a finite sum $\sum r_j b_j = 0 \in M_T$ for some $r_j \in R$, $b_j \in B$, then since the sum is finite there is a B_i containing all of the b_j, and so $\sum r_j b_j = 0 \in M_{T_i}$, contradicting the fact that B_i is a basis.

By Zorn's lemma, there is a maximal element (T, B) in the partially ordered set. If $T \neq S$ then there is some $t \in S \smallsetminus T$. Consider $\pi_s \colon M_{T\cup\{t\}} \to R$, the projection of $\bigoplus_{s\in S} R$ onto the t factor, restricted to $M_{T\cup\{t\}}$. Note that $\ker(\pi_t) = M_T$.

Since R-submodules of R are precisely the ideals of R, and all ideals are principal by assumption, we see that $\mathrm{im}(\pi_t) = Ra_t$ for some $a_t \in R$. Since R is a domain, Ra_t is a free module (either zero or isomorphic to R). Therefore the sequence

$$0 \to M_T \to M_{T\cup\{t\}} \to Ra_t \to 0$$

is split, and $M_{T\cup\{t\}} \cong M_T \oplus Ra_t$ is a free module on a basis $B \cup \{a_t\}$ (or just B if $a_t = 0$). This contradicts minimality of (T, B), unless $T = S$ as was our goal.

Let S be the indexing set of a free submodule $M \subseteq R^n$. Let K be the field of fractions of R, and note that $M \otimes_R K$ is a K-vector space with a basis whose elements are in an natural bijection with S. Also $M \otimes_R K \subseteq K^n$ is a K-vector subspace, and it follows that S is finite and $|S| \leq n$. □

Remark. Almost the same proof shows that if R is a (possibly non-commutative) ring such that every ideal of R is a projective module, then any submodule of a projective module is projective. Rings with this property are called *hereditary* and they are extremely important in representation theory. You can ignore this remark as far as the course content goes.

Corollary 3.4. *If R is a PID, then projective modules and free modules are the same thing.*

Proof. We have seen that projective modules are summands of free modules. Then apply the theorem. □

Theorem 3.5. *If R is a PID, then injective modules and divisible modules are the same thing.*

Proof. We saw last time that all injective modules are divisible, so we need to show that any divisible module M is injective. Let us use Baer's criterion. So let $f : I \to M$ be a map of R-modules, where $I \subset R$ is an ideal. Since R is a PID, we have $I = aR$ for some $a \in R$. As M is divisible we can write $f(a) = as$ for some $s \in M$. Then $f : I \to M$ extends to a map of R-modules $R \to M$ which sends 1 to s. □

In particular, the abelian groups $\mathbb{Q}/\mathbb{Z}$, $\mathbb{R}/\mathbb{Z}$ and $\mathbb{Q}$ are divisible, hence injective.

Theorem 3.6. *If R is a PID, then flat modules and torsion-free modules are the same thing.*

Proof. We know from Lemma 3.1 that flat modules are torsion-free, so let us prove the converse. Let $A \subset B$ be a submodule and let M be a torsion-free R-module. We need to prove that $A \otimes_R M \to B \otimes_R M$ is an injective map.

Step 1: It is enough to prove our claim in the case when B is free. Indeed, we know that any module is a quotient of a free module F, so there is an exact sequence

$$0 \longrightarrow K \longrightarrow F \longrightarrow B \longrightarrow 0$$

If we denote the inverse image of A in F by A', we obtain a commutative diagram of R-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K & \longrightarrow & F & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

This sequence is split exact since B is free. So it will stay split exact if we tensor it with M. This gives rise to a commutative diagram of abelian groups

$$\begin{array}{ccccccccc} & & K \otimes_R M & \longrightarrow & A' \otimes_R M & \longrightarrow & A \otimes_R M & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K \otimes_R M & \longrightarrow & F \otimes_R M & \longrightarrow & B \otimes_R M & \longrightarrow & 0 \end{array}$$

By assumption the middle vertical map is injective. Now a digram chase gives us that the right vertical map is injective too.

Step 2: It is enough to prove our claim in the case when $B = R$. By Step 1 it is enough to consider an inclusion $A \subset F$, where F is a free R-module. Any $x \in A \otimes_R M$ is a finite sum $\sum_{i=1}^{n} a_i \otimes m_i$, so $x \in A_0 \otimes_R M$, where $A_0 \subset A$ is the submodule generated by $a_1, \ldots, a_n$. Let R^n be the free submodule of F generated by the generators of F that show up in $a_1, \ldots, a_n$. Then $A_0 \subset R^n$ and $F = R^n \oplus F'$, where F' is the R-module generated by the generators of F not contained in R^n. Since $A \otimes_R F \cong (A \otimes_R R^n) \oplus (A \otimes_R F')$, it is enough to show that $A_0 \otimes_R M \to R^n \otimes_R M$ is injective.

Write $R^n = R \oplus R^{n-1}$ and $A_1 = A_0 \cap R$. Let A_2 be the image of A_0 in R^{n-1} under the projection map. We obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & A_0 & \longrightarrow & A_2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & R & \longrightarrow & R^n & \longrightarrow & R^{n-1} & \longrightarrow & 0 \end{array}$$

and hence a commutative diagram

$$\begin{array}{ccccccc} & & A_1 \otimes_R M & \longrightarrow & A_0 \otimes_R M & \longrightarrow & A_2 \otimes_R M \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & R \otimes_R M & \longrightarrow & R^n \otimes_R M & \longrightarrow & R^{n-1} \otimes_R M \longrightarrow 0 \end{array}$$

because the bottom exact sequence of the previous diagram is split. By the assumption of Step 2 the left vertical map is injective. Arguing by induction we assume that the right vertical map is injective. Then a diagram chase (or the Snake Lemma) gives the injectivity of the middle vertical map.

Step 3: End of proof. Now A is an ideal in R. Since R is a PID, we have $A = aR$. We need to prove the injectivity of the natural map $\alpha : aR \otimes_R M \to R \otimes_R M$. The map of R-modules $R \to aR$, $r \mapsto ar$, gives rise to $\beta : R \otimes_R M \to aR \otimes_R M$. This map is clearly surjective. The composition $\alpha\beta$ is the map $R \otimes_R M \to R \otimes_R M$, which is identified with the map $M \to M$ given by $m \mapsto am$. Since M is torsion-free, this map is injective. Now $\alpha\beta$ is injective and β is surjective, and this implies that α is injective. □

Now we can justify the example of a module that is flat but not projective given above: the abelian group $\mathbb{Q}$ is torsion-free, hence flat. But $\mathbb{Q}$ is divisible, so it is not a direct summand of a free abelian group, hence $\mathbb{Q}$ is not projective.

3.3. **Enough injectives.** We are now ready to show that the category of R-modules has enough injectives.

Theorem 3.7. *Let R be a (not necessarily commutative) ring. Every left R-module is isomorphic to a submodule of an injective module.*

Proof. We proceed in several steps.

Step 1: For every non-zero abelian group G we have $\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z}) \neq 0$; moreover, for any non-zero $x \in G$ there is an $f \in \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$ such that $f(x) \neq 0$.

Indeed, let $C \subset G$ be the cyclic subgroup generated by x. It can be finite or infinite. If C is finite, then there is an injective homomorphism $C \to \mathbb{Q}/\mathbb{Z}$ (e.g., sending x to $1/|C|$). If C is infinite, then consider the homomorphism sending x to $1/2 \in \mathbb{Q}/\mathbb{Z}$. In each case the image of x is non-zero, so it is a non-zero homomorphism $C \to \mathbb{Q}/\mathbb{Z}$. By the injectivity of $\mathbb{Q}/\mathbb{Z}$ (Theorem 3.5) it extends to a non-zero homomorphism $G \to \mathbb{Q}/\mathbb{Z}$.

Consider R as a *right* R-module. Then the abelian group $S = \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ can be equipped with the structure of a *left* R-module by making $r \in R$ send a homomorphism $f(x)$ to $f(xr)$. Indeed, the action of $b \in R$ sends $f(x)$ to $f(xb)$, and then the action of $a \in R$ sends $f(xb)$ to $f(xab)$, which is the same as the action of ab.

Step 2. The R-module S is injective.

For any R-module M we have a canonical isomorphism of abelian groups

$$\mathrm{Hom}_R(M, S) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}). \tag{4}$$

The map from left to right is obtained by evaluating at $1 \in R$: a map of R-modules $M \to \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$, $m \mapsto f_m$, goes to the homomorphism $m \mapsto f_m(1)$. The map from right to left attaches to a homomorphism $\phi(x) : M \to \mathbb{Q}/\mathbb{Z}$ the map of left R-modules which sends $m \in M$ to the homomorphism $F_m : R \to \mathbb{Q}/\mathbb{Z}$, $r \mapsto \phi(rm)$. (Note that for $x \in R$, the element $xm \in M$ goes to $F_{xm} : r \mapsto \phi(rxm)$ which equals xF_m for the left

R-module structure on $\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ defined above, so sending m to F_m is indeed a map of left R-modules.) It is easy to check that both compositions are the identity maps.

The isomorphism (4) is functorial, that is, for any map of R-modules $M \to N$ we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}_R(N, S) & \longrightarrow & \mathrm{Hom}_R(M, S) \\ \downarrow \cong & & \downarrow \cong \\ \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}) \end{array}$$

Since $\mathbb{Q}/\mathbb{Z}$ is injective as an abelian group, for any injective map of R-modules $M \to N$ any map $M \to \mathbb{Q}/\mathbb{Z}$ extends to a map $N \to \mathbb{Q}/\mathbb{Z}$. In other words, the natural map $\mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ (the restriction to $M \subset N$) is surjective. The diagram gives that the natural map $\mathrm{Hom}_R(N, S) \to \mathrm{Hom}_R(M, S)$ is surjective, hence S is injective as a left R-module.

Step 3. For any M we have $\mathrm{Hom}_R(M, S) \neq 0$; moreover, for any non-zero $m \in M$ there exists an $f \in \mathrm{Hom}_R(M, S)$ such that $f(m) \neq 0$.

This follows directly from Steps 1 and 2.

Now let $I(M)$ be the product of copies of S indexed by the elements of $\mathrm{Hom}_R(M, S)$. Since any product of injective modules is injective, $I(M)$ is injective. There is a canonical map $M \to I(M)$ that sends $m \in M$ to the element of $I(M)$ whose coordinate corresponding to $f \in \mathrm{Hom}_R(M, S)$ is $f(m)$. Then rm is sent to the element of $I(M)$ whose f-coordinate is $f(rm) = rf(m)$, so this is a map of left R-modules.

Step 4. This map is injective.

Indeed, let $m \in M$ be non-zero. By Step 3 there exists an $f \in \mathrm{Hom}_R(M, S)$ such that $f(m) \neq 0$. Hence this m goes to a non-zero element of $I(M)$. □

4. Resolutions and Derived Functors

4.1. **Projective and injective resolutions.** Let R be a ring (not necessarily commutative). A *chain complex* of R-modules is a complex

$$\ldots \xrightarrow{d} A_{n+1} \xrightarrow{d} A_n \xrightarrow{d} A_{n-1} \xrightarrow{d} \ldots$$

Being a complex means that $d^2 = 0$, or in other words $\operatorname{im} d \subset \ker d$. The complex can be finite, infinite, or semi-infinite. A map of chain complexes $f_\bullet \colon A_\bullet \to B_\bullet$ is a collection of maps of R-modules $f_n : A_n \to B_n$ commuting with the differentials d, so that $df_n = f_{n-1}d$ for all n. That is, a map of chain complexes $f_\bullet \colon A_\bullet \to B_\bullet$ is a commutative diagram

$$\begin{array}{ccccccccc} \ldots & \xrightarrow{d} & A_{n+1} & \xrightarrow{d} & A_n & \xrightarrow{d} & A_{n-1} & \xrightarrow{d} & \ldots \\ & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\ \ldots & \xrightarrow{d} & B_{n+1} & \xrightarrow{d} & B_n & \xrightarrow{d} & B_{n-1} & \xrightarrow{d} & \ldots \end{array}$$

A *cochain complex* of R-modules is a complex

$$\ldots \xrightarrow{d} C^{n-1} \xrightarrow{d} C^n \xrightarrow{d} C^{n+1} \xrightarrow{d} \ldots$$

Maps of cochain complexes are, again, defined as families of maps commuting with d.

Let $A_\bullet$ be a chain complex of R-modules. The n-th *homology group* $H_n(A_\bullet)$ is defined as the quotient of $\ker[A_n \to A_{n-1}]$ by $\mathrm{im}[A_{n+1} \to A_n]$. One defines the *cohomology groups* of a cochain complex similarly (cohomology is the homology of a cochain complex). A chain complex is exact if and only if all its homology groups are zero; a cochain complex is exact if and only if all its cohomology groups are zero.

We note that a map of chain complexes $f = (f_n) : A_\bullet \to B_\bullet$ induces maps on homology groups $f_* = (f_{n*}) : H_n(A_\bullet) \to H_n(B_\bullet)$. Indeed, let $a \in \ker[A_n \to A_{n-1}]$, i.e. $d(a) = 0$. So $df_n(a) = f_{n+1}d(a) = 0$ (where we have used that $f_\bullet$ is a map of chain complexes), so $f_n(a) \in \ker[B_n \to B_{n-1}]$. Now let $a \in \mathrm{im}[A_{n+1} \to A_n]$, i.e. $a = d(a')$ for some $a' \in A_{n+1}$. Then $f_n(a) = f_n d(a') = df_{n+1}(a')$, so $f_n(a) \in \mathrm{im}[B_{n+1} \to B_n]$. Hence we get an induced map $H_n(A^\bullet) \to H_n(B^\bullet)$.

Definition 4.1. *A* **left resolution** *of an R-module M is a (right bounded) chain complex of R-modules*

$$\ldots \xrightarrow{d} P_n \xrightarrow{d} \ldots \xrightarrow{d} P_1 \xrightarrow{d} P_0$$

together with a map $P_0 \to M$ such that the complex

$$\ldots \xrightarrow{d} P_n \xrightarrow{d} \ldots \xrightarrow{d} P_1 \xrightarrow{d} P_0 \longrightarrow M \longrightarrow 0$$

is exact. A left resolution is denoted by $P_\bullet \to M$. If each P_n is projective, the resolution $P_\bullet \to M$ is called projective.

A map of complexes $f = (f_n)$ is called a *quasi-isomorphism* if the induced map $f_{n*} \colon H_n(A_\bullet) \to H_n(B_\bullet)$ is an isomorphism for all n.

Remark. Let me make a remark about what is going on here. Note that to have a chain complex $P_\bullet$ with a homomorphism $P_0 \to M$ is precisely the same data as a morphism of complexes

$$\begin{array}{ccccccccccc}
\ldots & \xrightarrow{d} & P_2 & \xrightarrow{d} & P_1 & \xrightarrow{d} & P_0 & \xrightarrow{d} & 0 & \longrightarrow & \ldots \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \\
\ldots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & M & \longrightarrow & 0 & \longrightarrow & \ldots
\end{array}$$

where M is in degree 0. To ask for the complex $P_\bullet$ to be exact precisely means that $H_n(P_\bullet) = 0$ for all $n \neq 0$ and $H_0(P_\bullet) = P_0/\mathrm{im}(P_1 \xrightarrow{d} P_0) = \mathrm{coker}(P_1 \xrightarrow{d} P_0) \cong M = H_0(M)$. So a left resolution is precisely a complex concentrated in nonnegative degrees which is quasi-isomorphic to the complex with M concentrated in degree 0.

Definition 4.2. *A* **right resolution** *of an R-module M is a (left bounded) cochain complex of R-modules*

$$I^0 \xrightarrow{d} I^1 \xrightarrow{d} \ldots \xrightarrow{d} I^n \xrightarrow{d} \ldots$$

together with a map $M \to I^0$ such that the complex

$$0 \longrightarrow M \longrightarrow I^0 \xrightarrow{d} I^1 \xrightarrow{d} \ldots \xrightarrow{d} I^n \xrightarrow{d} \ldots$$

is exact. A right resolution is denoted by $M \to I^\bullet$. If each I^n is injective, the resolution $M \to I^\bullet$ is called injective.

A similar remark as before explains that giving a right resolution of a module M is precisely the same as giving a (left bounded) complex which is quasi-isomorphic to the complex with M concentrated in degree 0.

Examples. (1) The short exact sequence

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

shows that the 2-term complex $\mathbb{Z} \xrightarrow{\times n} \mathbb{Z}$ together with the surjection $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ is a projective resolution of the finite abelian group $\mathbb{Z}/n\mathbb{Z}$.

(2) The short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

shows that the 2-term complex $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ together with the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ is an injective resolution of the abelian group $\mathbb{Z}$. The same sequence can be viewed as a flat resolution of $\mathbb{Q}/\mathbb{Z}$ (this is an odd situation: we can't usually view complexes as resolutions in two ways like this).

(3) Let k be a field. Consider k as an $k[x]/(x^n)$-module by x acting as 0. Then

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

is an exact sequence. Together with the surjection $k[x]/(x^n) \twoheadrightarrow k$, we get a resolution of k by projective $k[x]/(x^n)$-modules.

One of the big ideas of homological algebra is the following: in order to study a (potentially badly behaved) module M, one should view it as a complex concentrated in degree 0 and then replace it by a quasi-isomorphic complex of easier (e.g. projective or injective) modules. This simple idea will take us very far. The following lemma says that this is always possible:

Lemma 4.3. *Every module has projective and injective resolutions.*

Proof. We know that for any M there is a surjective map $\epsilon : P_0 \to M$, where P_0 is free, hence projective. Define $M_0 = \ker(\epsilon)$. Take a surjective map $P_1 \to M_0$ with P_1 projective. Now let $d : P_1 \to P_0$ be the composition $P_1 \to M_0 \to P_0$. It is easy to see that $\mathrm{im}[P_1 \to P_0] = M_0 = \ker[P_0 \to M]$. This gives the first bit of our resolution and proves the exactness at P_0. Now define $M_1 = \ker[P_1 \to P_0]$ and repeat the procedure to construct P_2, and so on.

An injective resolution is built in exactly the same way, using the theorem from last week that says every module injects into an injective module. □

Proposition 4.4. *Suppose that we are given a projective resolution $P_\bullet \to M$ and a map of R-modules $f\colon M \to N$. Then for any left resolution $Q_\bullet \to N$ there exist maps of R-modules $f_n\colon P_n \to Q_n$, $n \geq 0$, making the following diagram commutative*

$$\begin{array}{ccccccccccc}
\ldots & \longrightarrow & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f} & & \\
\ldots & \longrightarrow & Q_2 & \xrightarrow{d_2} & Q_1 & \xrightarrow{d_1} & Q_0 & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

If $g_\bullet = (g_n) : P_\bullet \to Q_\bullet$ is another map of complexes making the diagram commutative, then there are maps $s_n : P_n \to Q_{n+1}$ such that $f_n - g_n = s_{n-1}d_n + d_{n+1}s_n$ for $n \geq 1$ and $f_0 - g_0 = d_1 s_0$.

Proof. Consider the surjective map $Q_0 \to N$. By the definition of a projective module the composition $P_0 \to M \to N$ can be lifted to $f_0 : P_0 \to Q_0$. This builds the first square of the diagram and shows that it is commutative. Now consider $P_1 \to P_0 \to Q_0$. The

image of this map goes to 0 in N, so it can be viewed as a map $P_1 \to \ker[Q_0 \to N]$. Consider the surjective map $Q_1 \to \ker[Q_0 \to N]$. Since P_1 is projective, we get a map $f_1 : P_1 \to Q_1$ which builds the second square and shows that it is commutative. Iterating this procedure constructs all vertical maps one by one and proves the commutativity of respective squares.

To prove the second statement, we consider the zero map $M \to N$ and prove that for any map of complexes $f_\bullet \colon P_\bullet \to Q_\bullet$ making the diagram commutative there are maps $s_n : P_n \to Q_{n+1}$ such that $f_n = s_{n-1}d_n + d_{n+1}s_n$ for $n \geq 1$ and $f_0 = d_1 s_0$. Indeed, in this case f_0 sends P_0 to $\ker[Q_0 \to N]$. Since P_0 is projective, f_0 lifts to a map $s_0 : P_0 \to Q_1$. This gives $f_0 = d_1 s_0$. Now $f_1 - s_0 d_1$ sends P_1 to $\ker[Q_1 \to Q_0]$, hence, by the projectivity of P_1, it lifts to $s_1 : P_1 \to Q_2$. We obtain $f_1 - s_0 d_1 = d_2 s_1$, which is $f_1 = s_0 d_1 - d_2 s_1$. Now continue by iterating this contruction. □

Exercise. State and prove the analogous statement for injective resolutions.

The second statement of Proposition 4.4 is usually phrased as follows: a map of complexes $f_\bullet : P_\bullet \to Q_\bullet$ making the above diagram commutative is *unique up to homotopy*. More precisely, a **chain homotopy** $s : f_\bullet \Rightarrow g_\bullet$ between two maps of chain complexes $f_\bullet, g_\bullet : C_\bullet \to D_\bullet$ is a sequence of R-module maps $s_n : C_n \to D_{n+1}$ for each n such that

$$f_n - g_n = ds_n + s_{n-1}d$$

for all n.

Lemma 4.5. *Maps of chain complexes $f, g : A_\bullet \to B_\bullet$ that are chain homotopic (i.e. there exists a chain homotopy $s : f \Rightarrow g$) induce equal maps of homology groups, i.e. $f_* = g_*$.*

Proof. Exercise. Note that it suffices to prove that if a map of complexes $f : A_\bullet \to B_\bullet$ is homotopic to the zero map then it induces the zero map on each homology group. □

References

[1] H. Cartan and S. Eilenberg. *Homological algebra*. Princeton University Press, 1956.

[2] E. Riehl, *Category theory in context*, Aurora Dover Modern Math Originals, Dover, Mineola, NY, 2016.

[3] C. Weibel. *An introduction to homological algebra*. Cambridge University Press, 1994.